

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

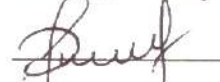
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми безпеки інтернет-
телефонії мережевої інфраструктури організації»

Виконав: студент 3-го курсу групи КБк-22-1
спеціальності 125 «Кібербезпека»

 Богдан ВАЩЕНКО

Керівник: Старший викладач кафедри КІ та КБ,

 Єлизавета ТРОКОЗ

Рецензент: Доцент кафедри КІ та КБ, к.т.н.

 Олексій ШЕЛУХА

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Ващенко Богдан Вікторович

Тема роботи: «Проект підсистеми безпеки інтернет-телефонії мережевої інфраструктури організації»

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

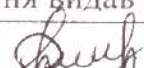
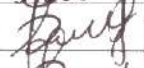
Термін здачі студентом закінченої роботи 20 червня 2025 р.

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

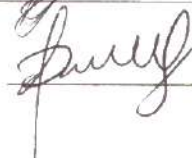
Обладнання та програмне забезпечення:

1. Емулятор GNS3
2. Маршрутизатор Cisco Catalyst 8200L
3. Комутатор Cisco Catalyst 9300-48P
4. ОС Windows 10, Kali Linux та Asterisk
5. Сервери FreePBX

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Трокоз Є. М.	12.03.2025 	12.03.2025 
2	Трокоз Є. М.	10.04.2025 	10.04.2025 
3	Трокоз Є. М.	05.05.2025 	05.05.2025 

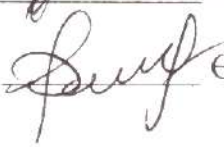
Студент  Богдан ВАЩЕНКО

Керівник  Єлизавета ТРОКОЗ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Узгодження теми, мети та завдань	05.03.2025 – 12.03.2025	Виконано
2	Теоретичний аналіз VoIP	12.03.2025 – 02.04.2025	Виконано
3	Проектування реалізації VoIP	02.04.2025 – 10.04.2025	Виконано
4	Моделювання загроз	10.04.2025 – 17.04.2025	Виконано
5	Проектування мережевої архітектури	17.04.2025 – 26.04.2025	Виконано
6	Підготовка та налаштування тестового середовища	05.04.2025 – 13.05.2025	Виконано
7	Інтеграція та конфігурація сервера FreePBX	14.05.2025 – 22.05.2025	Виконано
8	Налаштування TLS/SRTP	23.05.2025 – 10.06.2025	Виконано
9	Тестування системи безпеки	10.06.2025 – 11.06.2025	Виконано
10	Завершення оформлення та підготовка до захисту	11.06.2025 – 21.06.2025	Виконано
11	Оформлення презентації	21.05.2025 – 23.05.2025	Виконано
12	Захист	24.06.2025	Виконано

Студент  Богдан ВАЩЕНКО

Керівник  Єлизавета ТРОКОЗ

АНОТАЦІЯ

У кваліфікаційній роботі було здобуто навички принципів роботи інтернет-телефонії (VoIP): Використовувалися протоколи (SIP, RTP, TLS, SRTP), компоненти (АТС, SIP-клієнти). Проаналізовано типові загрози для VoIP-систем: DDoS-атаки, MITM, Sniffing, SPIT. Пояснювальна записка містить 82 сторінки друкованого тексту, включає 74 рисунка, 11 таблиць, 28 джерел у списку літератури, який розміщено на 3 сторінках.

Метою було розуміння актуальності та розробка підсистеми безпеки інтернет-телефонії та її інфраструктури, покрокова реалізація в організації, постановка правильного функціоналу, за для подальшого користування. Аналіз вразливостей, та методики захисту як користувачів так і основних магістралей мережі.

Використання конкретних рішень: FreePBX яка значно спрощує користування IP-телефонією. У контексті сучасної телекомунікаційної інфраструктури, PBX (Private Branch Exchange), або як її часто називають в українському бізнес-середовищі, АТС (Автоматична Телефонна Станція), є центральним вузлом, що забезпечує організацію внутрішнього та зовнішнього голосового зв'язку в межах компанії. По суті, це приватна телефонна мережа, яка дозволяє внутрішнім користувачам спілкуватися між собою, а також здійснювати та приймати зовнішні дзвінки через публічну телефонну мережу (PSTN) або, що більш актуально сьогодні, через Інтернет.

Ключові слова: FREEPBX, VOIP, MITM, TLS, SRTP, VLAN, HSRP, ПЗ.

					ККІКБ.КР.Б – 125 – 2 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проєкт підсистеми безпеки інтернет-телефонії мережевої інфраструктури організації	Літ.	Арк.	Аркушів
Розроб.		Ващенко Б.В.		23.06.25				
Перевір.		Трокоз Є.М.		23.06.25			4	95
Реценз.		Шелуха О.О.		23.06.25		ФІКТ, гр. КБК-22-1		
Н. Контр.		Трокоз Є.М.		23.06.25				
Зав.каф.		Ефіменко А.А.		23.06.25				

ANNOTATION

In this qualification paper, skills in the principles of Internet telephony (VoIP) were acquired. Protocols such as SIP, RTP, TLS, and SRTP were utilized, along with key components like PBX (Private Branch Exchange) and SIP clients. Typical threats to VoIP systems, including DDoS attacks, MITM (Man-in-the-Middle), Sniffing, and SPIT (Spam over Internet Telephony), were analyzed. The explanatory note contains 82 pages of printed text, includes 74 figures, 11 tables, and 28 sources in the list of references, which spans 3 pages.

The aim was to understand the relevance of and to develop a security subsystem for Internet telephony and its infrastructure, to implement it step-by-step within an organization, and to establish proper functionality for future use. This involved an analysis of vulnerabilities and methods for protecting both users and the main network trunks.

Specific solutions were employed, such as FreePBX, which significantly simplifies the use of IP telephony. In the context of modern telecommunications infrastructure, a PBX (Private Branch Exchange), or as it is often referred to in the Ukrainian business environment, an ATS (Automatic Telephone Exchange), serves as a central hub that organizes internal and external voice communication within a company. Essentially, it is a private telephone network that allows internal users to communicate with each other, as well as to make and receive external calls via the Public Switched Telephone Network (PSTN) or, more relevant today, over the Internet.

Keywords: FREEPBX, VOIP, MITM, TLS, SRTP, VLAN, HSRP, SOFTWARE.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП	8
РОЗДІЛ 1. АНАЛІЗ ЗАГРОЗ ТА ПРОЕКТУВАННЯ ВИМОГ ДО БЕЗПЕКИ VOIP-СИСТЕМ.....	10
1.1 VoIP-системи її вразливості та мотиви зловмисників	10
1.2 Типові атаки DDOS, SPIT, MITM, SNIFFING	14
1.3 Вимоги до захисту	25
РОЗДІЛ 2. МОДЕЛЬ ЗАГРОЗ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ В GNS.....	34
2.1 Розробка моделі загроз.....	34
2.2 Побудова мережевої інфраструктури	37
2.3 Реалізація заходів безпеки	44
РОЗДІЛ 3. ОПИС ТА ТЕСТУВАННЯ МЕРЕЖІ.....	53
3.1 Опис обладнання та їх функції.....	53
3.2 Сценарій тестування.....	70
ВИСНОВКИ.....	77
СПИСКИ ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	79
ДОДАТКИ.....	82

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ – Програмне забезпечення

ЦП – центральний процесор

ПЗ – Програмне забезпечення

ACL – Список контролю доступу.

Asterisk – Програмне забезпечення з відкритим вихідним кодом для створення систем IP-телефонії.

FreePBX – Відкрите програмне забезпечення для IP-АТС для керування Asterisk.

HSRP – Протокол резервування маршрутизаторів.

IP – Протокол мережевого рівня

IP-АТС – Автоматична Телефонна Станція, що працює за протоколом Інтернету (IP).

IVR – Інтерактивне голосове меню.

MAC-адреса – Унікальний ідентифікатор мережевого адаптера.

MicroSIP – Програмний SIP-клієнт, що використовується для здійснення дзвінків через IP-телефонію.

Port Security – Безпека портів.

PJSIP – Сучасний SIP-драйвер у Asterisk/FreePBX.

RTP – Використовується для передачі голосового та відео трафіку.

SIP – Використовується для встановлення, зміни та завершення мультимедійних сеансів.

TLS – криптографічним протоколом, який забезпечує безпечну комунікацію через комп'ютерну мережу

SRTP – профілем протоколу RTP який додає безпеку до передачі медіа-даних (голосу та відео) у реальному часі

SSL – Secure Sockets Layer – захищений протокол прикладного рівня

UCP – Панель керування користувача.

VLAN – Віртуальна локальна мережа.

VoIP – Голос через Інтернет-протокол.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Сьогодні інтернет-телефонія (VoIP) відіграє ключову роль у корпоративних комунікаціях, забезпечуючи швидкість, гнучкість та економічну ефективність зв'язку. Проте активна цифровізація цієї галузі зробила її вразливою до кіберзагроз. Сучасні атаки, зокрема DDoS, спуфінг, шкідливі SIP-запити, а також методи соціальної інженерії, ставлять під загрозу конфіденційність і цілісність комунікацій. Ці фактори зумовлюють необхідність створення ефективних захисних рішень для VoIP-систем, що є важливою умовою безперервності бізнес-процесів та уникнення фінансових і репутаційних втрат.

Метою кваліфікаційної роботи є розробка та впровадження комплексної підсистеми безпеки для VoIP-інфраструктури організації, здатної ефективно протидіяти актуальним кіберзагрозам. Система має поєднувати механізми моніторингу, шифрування трафіку, аналізу аномалій і контроль доступу з урахуванням специфіки протоколів SIP та RTP, а також забезпечувати оптимальне співвідношення між рівнем безпеки та якістю зв'язку.

Завдання дослідження:

1. Провести аналіз актуальних загроз для VoIP-систем, включно з ризиками на рівні мережі, протоколів та користувацьких інтерфейсів.
2. Спроекувати архітектуру захисної підсистеми із застосуванням сучасних криптографічних технологій, IDS/IPS та інструментів аналізу поведінки користувачів.
3. Реалізувати та протестувати систему в умовах, наближених до реального середовища, із моделюванням кібератак для оцінки ефективності захисту.

Об'єктом дослідження є процес проектування, впровадження та налаштування підсистеми безпеки інтернет-телефонії в межах мережевої інфраструктури організації. Серед апаратних компонентів — IP-АТС, маршрутизатори, комутатори, IP-телефони. Програмне забезпечення охоплює

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

VoIP-шлюзи, софтфони, конфігурацію телефонних станцій, що забезпечують повноцінну роботу комунікаційної системи.

Предметом дослідження є методи, засоби та технології забезпечення безпечного функціонування інтернет-телефонії в мережевій інфраструктурі організації. Основна увага приділяється застосуванню TLS для шифрування сигнального трафіку, SRTP — для захисту медіа-потоків, налаштуванню мережових політик безпеки (ACL, VLAN, HSRP) на базі обладнання Cisco. Також досліджено впровадження систем IDS/IPS, алгоритмів на базі машинного навчання для виявлення аномалій, а також конфігурацію контролю доступу на рівні SIP-клієнтів і FreePBX, що забезпечує цілісність, автентичність і конфіденційність комунікацій.

У процесі виконання кваліфікаційної роботи було розроблено проект комплексної підсистеми безпеки для VoIP-системи організації. Запропоноване рішення посилює кіберзахист критично важливої інфраструктури, дозволяючи уникнути збитків, підвищити стійкість до атак і зміцнити довіру до корпоративних технологій зв'язку.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. АНАЛІЗ ЗАГРОЗ ТА ПРОЕКТУВАННЯ ВИМОГ ДО БЕЗПЕКИ VOIP-СИСТЕМ

1.1 VoIP-системи її вразливості та мотиви зловмисників

VoIP (Voice over Internet Protocol) — це технологія, яка дозволяє здійснювати голосові дзвінки через інтернет. Вона популярна завдяки гнучкості та економії, але через використання інтернету схильна до кібератак, що може загрожувати конфіденційності та безпеці.

В основу VoIP-систему входять ключові компоненти та елементи:

Кінцеві пристрої (End Devices / Endpoints):

- IP-телефони: Спеціалізовані апаратні пристрої, які підключаються безпосередньо до комп'ютерної мережі (Ethernet) і не вимагають окремих телефонних кабелів. Вони мають вбудовану підтримку VoIP-протоколів;
- софтфони (Softphones): Програмне забезпечення, що встановлюється на комп'ютери, смартфони або планшети (наприклад, MicroSIP, який ви використовуєте). Вони використовують мікрофон та динаміки пристрою (або гарнітуру) для здійснення та прийому дзвінків;
- АТА-адаптери (Analog Telephone Adapters, АТА): Пристрої, що дозволяють підключити звичайний аналоговий телефон до IP-мережі. Вони перетворюють аналогові голосові сигнали на цифрові IP-пакети і навпаки.

IP-АТС (IP-PBX) або VoIP-сервер:

- це центральний мозок VoIP-системи (наприклад, FreePBX/Asterisk). Він керує всіма внутрішніми дзвінками, маршрутизує вхідні та вихідні дзвінки, забезпечує розширений функціонал (голосова пошта, IVR, черги, конференції тощо) та відповідає за підключення до зовнішніх телефонних ліній.

Шлюзи та транки (Gateways & Trunks):

- VoIP-шлюзи: Пристрої, що дозволяють підключати VoIP-систему до традиційної телефонної мережі (PSTN). Це потрібно для здійснення дзвінків на звичайні міські/мобільні номери або прийому дзвінків з них;

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

- SIP-транки: Це віртуальні "лінії" зв'язку, які надаються VoIP-провайдерами (SIP-провайдерами). Вони дозволяють IP-АТС підключатися до публічної телефонної мережі через Інтернет, усуваючи потребу у фізичних телефонних лініях;

- E1/T1/PRI транки: Традиційні цифрові канали, які також можуть підключатися до VoIP-АТС через спеціальні плати або шлюзи, але це вже не чисто IP-рішення.

Мережева інфраструктура:

- маршрутизатори – керують трафіком між різними сегментами мережі (VLANs), забезпечують доступ до Інтернету та між офісами (як R-22-1-1, R-22-1-2) ;

- комутатори – підключають кінцеві пристрої та сервери до мережі, дозволяють створювати VLANs для сегментації трафіку;

- брандмауери – захищають VoIP-систему від несанкціонованого доступу та атак, контролюючи вхідний та вихідний трафік;

- якість обслуговування (Quality of Service, QoS) – механізми, які пріоритизують голосовий трафік у мережі, щоб забезпечити його плавну передачу без затримок, переривань та спотворень, оскільки голос дуже чутливий до затримок.

Протоколи VoIP:

- SIP (Session Initiation Protocol): Найпоширеніший протокол для встановлення, зміни та завершення мультимедійних сеансів, включаючи голосові дзвінки. Він відповідає за сигналізацію;

- RTP (Real-time Transport Protocol): Протокол, який безпосередньо передає аудіо та відео дані (тобто сам голос) у реальному часі.

Голосова телефонія через Інтернет-протокол (VoIP) пропонує значні переваги в комунікаціях, але її інтеграція в мережеву інфраструктуру створює низку вразливостей, які можуть бути використані зловмисниками. Розуміння цих вразливостей є ключовим для побудови надійної підсистеми безпеки.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

До основних категорій вразливостей VoIP-систем належить прослуховування та перехоплення розмов, оскільки голосовий трафік передається через IP-мережі і може бути записаний, якщо не використовується шифрування. Також існує ризик відмови в обслуговуванні (DoS/DDoS), коли зловмисники можуть перевантажити VoIP-сервер або мережеві канали, що призводить до недоступності телефонної системи та зриву дзвінків. Прикладом цього може бути блокування брандмауером FreePBX SIP та RTP трафіку, що робить систему недоступною для SIP-клієнтів.

Несанкціонований доступ та фрод є ще однією значною загрозою, коли зловмисники отримують доступ до розширень або адміністративних панелей через слабкі паролі чи вразливості ПЗ, що дозволяє їм здійснювати дорогі дзвінки за рахунок організації. Підміна ідентифікатора абонента (Caller ID Spoofing) дозволяє зловмисникам маскувати свій справжній номер, здійснюючи шахрайські дзвінки. Впровадження шкідливого коду також є ризиком, оскільки VoIP-пристрої та сервери можуть бути вразливими до вірусів, що порушують їх роботу або викрадають дані.

Крім того, неналежна конфігурація брандмауерів та мережевих пристроїв, як це було у випадку з брандмауером FreePBX, який за замовчуванням блокував критичний SIP/RTP трафік, або спрацювання Port Security на комутаторі через несанкціоновану MAC-адресу, може створити проломи в безпеці. Загалом, програмне забезпечення VoIP-систем (сервери, клієнти, прошивки телефонів) також може містити вразливості, що вимагає регулярних оновлень.

Зазвичай зловмисники здійснюють атаки на системи VoIP та мережеву інфраструктуру з кількох ключових мотивів. Перш за все, часто це пов'язано з отриманням фінансової вигоди. Вони можуть використовувати зламані VoIP-системи для здійснення дзвінків на дорогі міжнародні або преміум-номери, отримуючи прибуток від таких операцій, або ж використовувати DDoS-атаки для вимагання коштів у компаній за відновлення працездатності.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

Другим значним мотивом є шпигунство та викрадення конфіденційної інформації. Оскільки голосовий трафік передається через IP-мережі, його можна перехопити для отримання комерційних таємниць, персональних даних, фінансової інформації або інших конфіденційних відомостей. Це може бути частиною корпоративного шпигунства чи інших незаконних дій. Третім із розповсюдженого зловмисники прагнуть порушити бізнес-операції та завдати шкоди репутації організації. Атаки типу відмови в обслуговуванні (DoS/DDoS) на VoIP-системи можуть повністю паралізувати комунікації компанії, спричиняючи значні фінансові втрати та зрив обслуговування клієнтів. Це може бути мотивовано конкурентною боротьбою або просто бажанням завдати шкоди. Четвертий порок до якого зловмисник піддається це до шахрайства та соціальної інженерії яка є поширеними мотивами. Підrobка ідентифікатора абонента дозволяє зловмисникам видавати себе за довірених осіб, використовуючи це для фішингових атак, виманювання конфіденційної інформації або здійснення інших видів шахрайства. Врешті-решт існує деякий вид хакерів які можуть здійснювати атаки для тестування своїх навичок та самоствердження.

Важливо зазначити що зламана VoIP-система може стати плацдармом для подальших атак на інші сегменти корпоративної мережі. Отримавши доступ до PBX, зловмисник може використовувати її для сканування внутрішньої мережі, запуску шкідливого програмного забезпечення або обходу інших систем безпеки.

Щоб зменшити ризики, треба використовувати шифрування, наприклад, SRTP, впроваджувати багатофакторну автентифікацію (MFA) та регулярно оновлювати програмне забезпечення. Навчати працівників розпізнавати фішингові атаки та обирати надійного провайдера VoIP Хоча пошук новин про вразливості VoIP у 2025 році не виявив конкретних нових вразливостей, статті, такі як Forbes - How To Improve Your VoIP Security In 2025, вказують на зростання складності атак, зокрема з використанням AI, вразливостей IoT та загроз deepfake. Це свідчить про еволюцію кіберзагроз,

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

які можуть впливати на VoIP-системи, але конкретні приклади нових вразливостей у 2025 році не були чітко визначені [4].

1.2 Типові атаки DDoS, SPIT, MITM, SNIFFING

Типові атаки, такі як DDoS, SPIT, MITM та Sniffing, є поширеними методами, які зловмисники використовують для порушення безпеки мереж, систем або даних.

DDoS-атака (розподілена атака) – це атаки відмови в обслуговуванні. Така атака на комп'ютерну систему відбувається з великою кількістю комп'ютерних ресурсів, які недоступні користувачам, за якими комп'ютерна система була розпізнана. Одним із найпоширеніших методів атаки є атака на комп'ютер або встановлення великої кількості викликів (часто з використанням запитів, в яких немає жодного сенсу або взагалі неправильно сформульованих), таким чином, щоб атакувати комп'ютер, з метою зробити його недоступним, хоча насправді доступ до нього є. Як правило, DDoS-атаки не націлені на конкретного користувача, а обирають як мету сайти онлайн-банків, платіжні шлюзи та урядові портали. Хакери, що стоять за атаками типу DDoS, можуть бути мотивовані прагненням нажитися, помститися або просто “потролити”. В результаті атаки веб-сайти виводяться з ладу і стають недоступними для користувачів, які в результаті втрачають довіру до організації і вирішують свої завдання в іншому місці.

Організація зазнає фінансових збитків і, не в останню чергу, втрачає репутацію. Ніхто не застрахований від DDoS-атак.

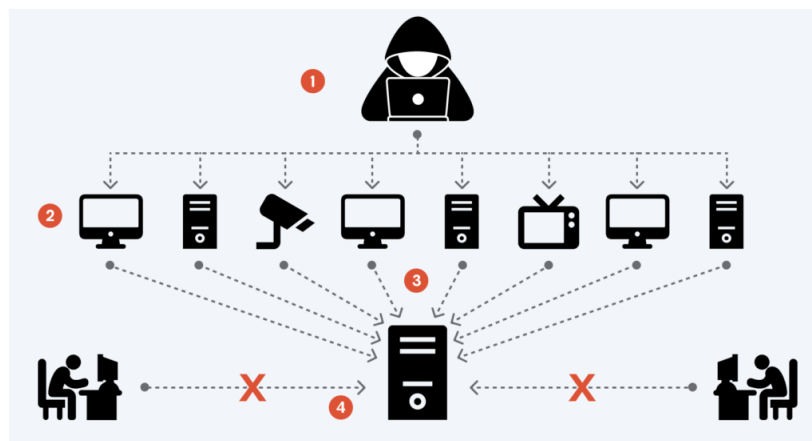


Рисунок 1.1 – Приклад DDoS-атаки

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

Кіберзлочинці постійно знаходять нові вразливості на сайтах. Навіть такі гіганти як Google, Facebook та Amazon стають жертвами [5]. Щоб ефективно боротися з DDoS-атаками, захист сайтів та програм слід обслуговувати та оновлювати. В американському Агентстві кібербезпеки та захисту інфраструктури (CISA) підкреслюють, що запобігти таким атакам неможливо, але можна вжити заходів для їх швидкого виявлення та зменшення впливу [6]. Атаки типу «відмова в обслуговуванні» також використовувалися в благих цілях, закриваючи злочинні підприємства, навіть окремі IP-адреси злочинців, атаки проти організацій та людей, які вважаються незаконною діяльністю.

Існує велика кількість ПЗ для використання DoS та DDoS атак, велика кількість яких не створена за для зловмисних атак, а використовується здебільшого для тесту самої мережі, але серед таких ПЗ існують і такі які дійсно можуть завдати шкоди для підприємств.

“Програмне забезпечення для використання DoS та DDoS атак”

HOIC – Додаток для захисту від мережевих атак та DoS/DDoS-атак, написаний мовою BASIC. Він призначений для атаки до 256 цільових URL-адрес одночасно. Він надсилає запити HTTP POST та GET на комп’ютер, який використовує графічний інтерфейс, натхнений lulz.

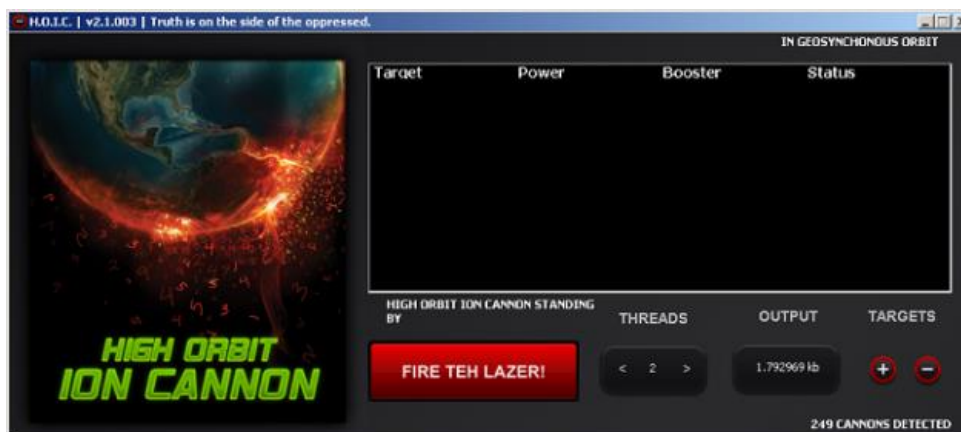


Рисунок 1.2 – Головне меню HOIC

LOIC – Додаток для стрес-тестування мережі та DoS-атаки. Атаки LOIC можна назвати атаками DOS на основі програм, оскільки вони в першу чергу націлені на веб-програми. LOIC можна використовувати на цільовому

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

сайті для переповнення сервера TCP-пакетами, UDP-пакетами або HTTP-запитами з метою порушити роботу служби

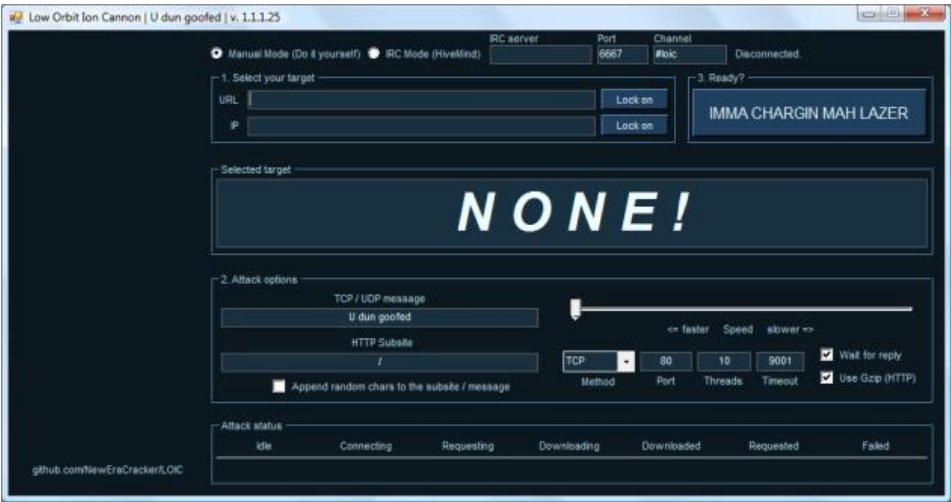


Рисунок 1.3 – Головне меню LOIC

SLOWLORIS – Програмне забезпечення, написане Робертом «RSnake» Хансеном. Slowloris дозволяє вивести вебсервер з ладу за допомогою помилки в HTTP навіть з однієї машини з поганим інтернетом. Slowloris намагається встановити багато підключень з вебсервером та тримати їх відкритими якнайдовше.

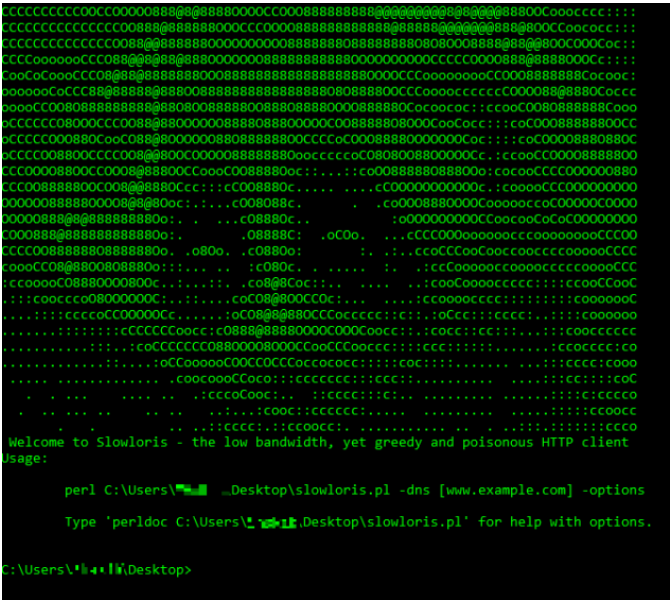


Рисунок 1.4 – Головне меню SLOWLORIS

Загрози: DDoS-атаки: Перевантаження сервера фальшивими запитамми.
Сканування вразливостей: Пошук слабких місць у відкритих сервісах.
Брутфорс: Спроби підібрати паролі до облікових записів.

Однією з найефективніших стратегій захисту є використання спеціалізованих систем захисту від DDoS, які можуть виявляти та блокувати підозрілий трафік. Також важливо мати розподілену мережу доставки контенту (CDN), яка може розподіляти навантаження та знижувати ризик впливу атаки на одну точку. Крім апаратних рішень, належить увагу приділити та інформаційній безпеці. Регулярне оновлення програмного забезпечення, використання надійних паролів та двофакторна аутентифікація – це основні кроки, які допоможуть захистити систему. Велике значення має регулярне тестування захисних систем. Проведення тестів на проникнення допомагає виявити потенційні слабкі місця в захисті та вчасно їх усунути. Спеціалізовані фірми можуть проводити таке тестування, імітуючи різні типи атак, щоб перевірити готовність системи до відсічі реальним загрозам.

Spam over Internet Telephony (SPIT) — це форма атак, що полягає у масовому генеруванні небажаних дзвінків через VoIP-системи, що може руйнувати як ефективність комунікацій, так і довіру користувачів до системи зв'язку. SPIT відрізняється від звичайного спаму в електронній пошті тим, що замість текстових повідомлень агресивно використовуються голосові дзвінки, які часто надходять автоматизованими скриптами або ботами. У цих атаках зловмисники надсилають тисячі або навіть мільйони дзвінків, що створює перевантаження мережі, заважає нормальній роботі системи і може призвести до серйозних фінансових та операційних наслідків для бізнесу, адже легітимні дзвінки стають жертвами масового шуму та каналів зв'язку, зайнятих шкідливим трафіком.

SPIT атакуючі зазвичай експлуатують вразливості в аутентифікації викликів та механізмах валідації номерів абонентів, що дозволяє їм використовувати підроблені дані для приховування своєї ідентичності. VoIP-протоколи, як SIP, часто спроектовані з акцентом на гнучкість і сумісність, що, разом із недостатнім рівнем шифрування та слабким налаштуванням безпеки, надає можливості для зловмисних дій. У результаті навіть невеликі порушення механізмів фільтрації або відсутність додаткових рівнів

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

аутентифікації можуть дозволити SPIT-ботам доступ до мережі, що збільшує ризик як інтерференції в нормальних викликах, так і створення можливостей для подальших атак, таких як фішинг чи крадіжка конфіденційної інформації

У боротьбі із SPIT важливе значення набуває впровадження сучасних засобів виявлення аномалій, що використовують штучний інтелект та машинне навчання. Наприклад, дослідники розробили моделі з використанням глибинних конволюційних автоенкодерів, які виявляють аномалії у звичайному трафіку та можуть ідентифікувати SPIT-атаки з високою точністю [7]. Такі методи дозволяють не лише сповільнити або навіть зупинити атаку, але й забезпечити можливість адаптивного навчання системи для виявлення нових варіантів SPIT, що щодня отримують нові форми завдяки розвитку технологій і змінюваним схемам атак.

Оскільки методи SPIT атак постійно еволюціонують, важливою складовою захисту стає регулярне оновлення систем моніторингу та фільтрації дзвінків. Використання баз даних, що містять відомості про підозрілі викликувальні номери, у поєднанні з програмними рішеннями, здатними аналізувати поведінку дзвінків у режимі реального часу, створює багаторівневий захист, що дозволяє швидко реагувати на загрози [8]. Невідкладна реакція є критичною, оскільки навіть короточасне перевантаження системи може завдати шкоди фінансовим показникам і репутації організації. Крім того, інтеграція методів аутентифікації, криптографічних протоколів та розумного управління дзвінковими сесіями допомагає мінімізувати ризики, пов'язані із SPIT, і забезпечує більш стабільну роботу VoIP-систем.

Таким чином, SPIT є серйозною загрозою для систем зв'язку, оскільки його механізми атак побудовані на використанні слабких місць архітектури VoIP і недостатньо захищених мережевих протоколів. Комплексний підхід до безпеки, що поєднує технологічні рішення з активним моніторингом та аналізом трафіку, є надзвичайно важливим для виявлення та зупинки SPIT-атаки. Додатково, з огляду на стрімкий розвиток технологій, дослідження у

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

сфері застосування аналітичних методів і глибокого навчання для виявлення аномалій відкривають нові можливості для захисту VoIP-систем від цієї небезпеки.

Захист VoIP-систем від SPIT-атак базується на кількох ключових механізмах, які включають аутентифікацію, фільтрацію трафіку, аналіз поведінки викликів та використання криптографічних методів. Одним із основних підходів є впровадження SIP-аутентифікації, що дозволяє перевіряти легітимність абонентів перед встановленням з'єднання. Це може включати використання TLS для шифрування сигналізаційного трафіку та SRTP для захисту медіа-даних, що значно ускладнює можливість перехоплення або модифікації викликів.

Фільтрація трафіку є ще одним важливим механізмом, який дозволяє блокувати небажані дзвінки. Використання чорних списків та баз даних підозрілих номерів допомагає автоматично відхиляти виклики, що надходять від відомих джерел SPIT. Крім того, аналіз поведінки викликів за допомогою алгоритмів машинного навчання дозволяє виявляти аномальні шаблони дзвінків, такі як масові виклики з одного джерела або надмірна частота викликів, що може свідчити про атаку.

Додатково застосовуються *CAPTCHA*-технології для перевірки людського фактору перед встановленням з'єднання, що ефективно запобігає автоматизованим атакам. Використання антиспам-фільтрів, які аналізують аудіовміст дзвінків, також може допомогти у виявленні SPIT-атак, особливо якщо вони містять заздалегідь записані рекламні або шахрайські повідомлення.

Окрім програмних рішень, важливу роль відіграє сегментація мережі, що дозволяє ізолювати VoIP-трафік від загального інтернет-трафіку, зменшуючи ризик зовнішніх атак. Використання інтелектуальних систем моніторингу та аналізу трафіку в реальному часі дозволяє оперативно реагувати на загрози та блокувати підозрілі виклики ще до їхнього впливу на систему.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

MITM-атака (Man-in-the-Middle) представляє собою небезпечну кіберзагрозу, коли зломисник інтрудується в комунікаційний канал між двома легітимними сторонами, змушуючи їх сприймати його як невід'ємну частину прямої взаємодії. У випадку VoIP-систем, де часто використовуються протоколи SIP для сигналізації та RTP для передачі медіа-даних, загроза MITM набуває особливого значення через можливість роботи цих протоколів без обов'язкового шифрування. Атакуючий, використовуючи вразливості мережевої інфраструктури, може безперешкодно перехоплювати викликові повідомлення, змінювати їх або навіть повністю перенаправляти аудіо-потік, що дозволяє не тільки пасивно прослуховувати комунікації, але й втручатися в неї. Така атака здійснюється за рахунок створення ілюзії прямого з'єднання між двома сторонами, тоді як зломисник знаходиться саме посередині й отримує можливість читати, змінювати або підробляти інформацію.

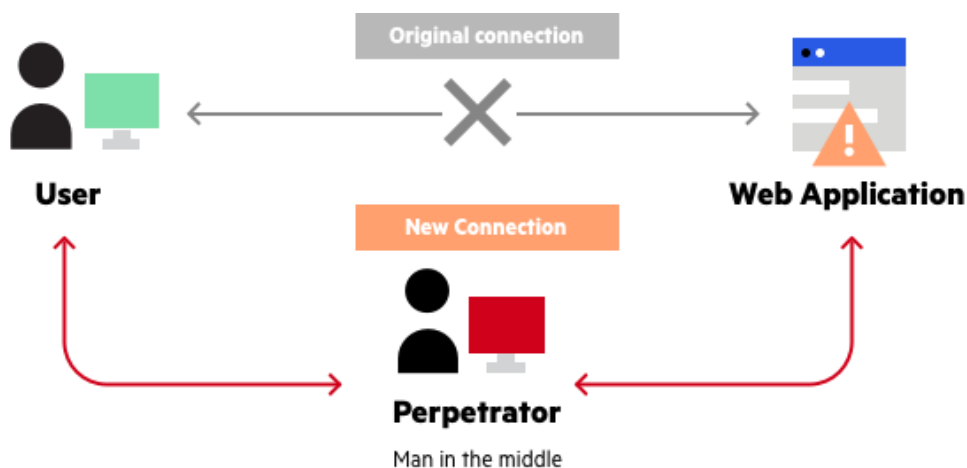


Рисунок 1.5 – Приклад MITM

При виявленні MITM-атаки зломисники можуть застосовувати різноманітні технічні прийоми для проникнення і подальшого втручання в дзвінкову сесію. Одним із основних методів є підробка мережевих протоколів, коли, наприклад, зломисник використовує ARP-спуфінг для перевизначення адресних відповідностей у локальній мережі, що змушує мережевий трафік направлятися через комп'ютер нападника. Іншим способом є використання технік підробки DNS, коли відповідь на запит

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

про IP-адресу легітимного VoIP-сервера замінюється на адресу підробленого сервера, що дозволяє атакуючому отримувати доступ до сигналізаційних повідомлень і медіа-потоків. Таке втручання дозволяє не лише здійснювати пасивний збір даних, але й активно модифікувати інформацію — від перенаправлення дзвінків до повного крадіжки конфіденційної інформації. Реалізація успішної MITM-атаки часто базується на неправильній конфігурації VoIP-систем, де знехтування впровадженням криптографічних протоколів, таких як TLS для захисту сигналізації та SRTP для шифрування аудіо, створює сприятливе середовище для зловмисників [9].

Сутність MITM в VoIP-середовищі полягає у тому, що система втрачає можливість гарантувати цілісність і конфіденційність даних під час їх передачі. Зловмисник може ефективно не лише прослуховувати дзвінки, а й змінювати важливі параметри дзвінкових сесій, що має великий вплив на якість і надійність корпоративних комунікацій. Висока ефективність таких атак зумовлена відсутністю обов'язкового шифрування і невідповідним впровадженням механізмів автентифікації, через що атакуючий отримує можливість ефективно маскувати свою присутність у мережевому трафіку. Захист від MITM полягає у впровадженні комплексних заходів, що включають не тільки використання сучасних криптографічних технологій, але й регулярний моніторинг мережевої інфраструктури, сегментацію мережі та впровадження систем виявлення аномалій, які здатні оперативно розпізнати і усунути підозрілі спроби інтрузії. Таким чином, без глибокого та системного підходу до забезпечення безпеки мережі навіть найсучасніші VoIP-системи можуть стати вразливими до MITM-атак, що ставить під загрозу конфіденційність і цілісність зв'язку.

Для захисту від MITM-атак використовуються різні криптографічні та мережеві протоколи, які забезпечують цілісність і конфіденційність переданих даних. Одним із ключових є Transport Layer Security (TLS), який шифрує сигналізаційний трафік у VoIP-системах, зокрема SIP-повідомлення, запобігаючи їх перехопленню та модифікації. Secure Real-time Transport

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Protocol (SRTP) виконує аналогічну функцію для медіа-трафіку, захищаючи аудіо- та відеодані від несанкціонованого доступу.

Крім того, Public Key Infrastructure (PKI) використовується для автентифікації учасників зв'язку, забезпечуючи перевірку цифрових сертифікатів і запобігаючи підробці ідентичності. DNS Security Extensions (DNSSEC) допомагає захистити від атак на рівні доменних імен, запобігаючи підробці DNS-запитів, що може бути використано для перенаправлення трафіку на сервери зломисників.

Додатково застосовуються IPsec для шифрування мережевого трафіку та Zero Trust Network Access (ZTNA), що забезпечує сувору перевірку кожного запиту на доступ до мережі. Деякі сучасні рішення також використовують Distributed Ledger Technology (DLT) для децентралізованого розподілу криптографічних ключів, що значно ускладнює можливість компрометації системи.

SNIFFING — це процес перехоплення та аналізу мережевого трафіку, коли зломисник безпосередньо спостерігає за передачею даних між пристроями. Він може встановити мережеву карту, переведучу її у режим, який дозволяє приймати всі пакети, що циркулюють в мережі, незалежно від їх адреси призначення, і таким чином отримати доступ до вмісту цих пакетів. У VoIP-системах, де використовується протокол SIP для сигналізації та RTP для передачі медіа-даних, сніфінг набуває особливого значення, оскільки багато систем передають інформацію у відкритому вигляді. Незахищені дані можуть містити не лише інформацію про виклики, а й сам аудіопотік, що дозволяє зломисникам збирати дані для подальшого аналізу або маніпуляцій.



Рисунок 1.6 – Приклад Sniffing-а

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

При здійсненні сніфінгової атаки атакуючий використовує спеціальні програмні засоби або пристрої, які дозволяють читати мережевий трафік і розшифровувати пакети даних в режимі реального часу. Цей процес включає аналіз заголовків пакетів, що містять інформацію про джерело, місце призначення, які використовувані порти та протоколи, а також врахування даних у тілі пакетів. Завдяки цьому можна відновити цілі потоки інформації, відокремити сигналізаційні дані від медіа-даних.

Атака з перехопленням здатна застосовуватись і для відновлення парольної фрази — зокрема, у випадках, коли приватний ключ SSH опинився в руках зловмисника. У такій ситуації спеціальне програмне забезпечення фіксує SSH-пакети, в яких містяться зашифровані варіанти введеного користувачем пароля. Ці дані згодом можна розшифрувати в офлайн-режимі, використовуючи методи перебору (brute-force).

Витяг з RFC 2301

Термін “перехоплення” визначається в RFC 2301 як: “Будь-який акт захоплення мережевого трафіку та його відтворення, зазвичай з метою шпигунства або саботажу” [10]. Це визначення є неточним для систем на базі UNIX, оскільки будь-який трафік може бути перехоплений, якщо зловмисник має доступ до мережних інтерфейсів (NIC) або змінює пакети, які не можуть бути змінені під час передачі. Перехоплення може бути виконане за допомогою спеціальної програми, як-от tcpdump, tcpflow або LanMon, яка підключена до порту, через який пакети можуть бути перевірені віддалено.

Ще одним видом атаки перехоплення є ARP-підміна, яка полягає у надсиланні фальшивих повідомлень протоколу ARP на каналному рівні Ethernet, що дозволяє зловмиснику змусити комп’ютер-жертву переспрямовувати свій трафік через пристрій, який він контролює, шляхом підміни MAC-адреси. Це використовується як для перехоплення сеансів, так і для переповнення мережі за допомогою атаки типу “відмова в обслуговуванні”. Кожен IP-пакет містить, на додаток до свого корисного навантаження, два поля: IP-заголовок та заголовок Ethernet.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Ті, хто працює з інтернет-комунікаціями, часто називають комбінацію цих двох заголовків “пакетом”. Таким чином, зловмисник може переглядати та змінювати IP-заголовок IP-пакета, не переглядаючи його корисне навантаження.

Заголовок Ethernet містить інформацію про MAC-адресу призначення (апаратну адресу комп’ютера одержувача), а поле Ether Type містить значення, що вказує, який тип послуги запитується (наприклад, пріоритет або керування потоком).

Тип Ether може бути “0xFFFF”, що вказує на те, що для кадру Ethernet не було включено службові поля. Це використовувалося у реалізації Cisco до версії 8.0.

Особливу небезпеку створює те, що сніфінг зазвичай є пасивною атакою, тобто зловмисник ні в якому разі не вносить змін до даних, а тільки їх перехоплює. Це дозволяє йому залишатися непоміченим, оскільки звичайний мережевий моніторинг може не виявити подібну діяльність. Без належного шифрування, яке захищає як сигналізацію, так і медіа-трафік, усі дані стають легкодоступними для аналізу зловмисниками, що може призвести до розкриття конфіденційної інформації, а також до можливості подальшого втручання в дзвінкові сесії.

Суть сніфінгової атаки полягає в тому, що мережеві пакети несуть додаткову захисну інформацію, яка б унеможливила їх розшифрування у випадку перехоплення. Тому навіть при сучасних мережевих рішеннях, де атакуючий може мати обмежений доступ до сегменту мережі, існує можливість зловмисного збору даних. Це стає особливо критичним у корпоративному середовищі, де VoIP-системи часто інтегровані з іншими мережевими сервісами та пристроями, і де навіть невелика вразливість може відкрити шлях до масштабного витоку інформації.

З метою захисту від сніфінгу експерти рекомендують впроваджувати криптографічні протоколи, такі як TLS для сигналізації та SRTP для захисту аудіо- і відеоданих, що робить вміст пакетів недоступним для

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

несанкціонованого аналізу. Водночас важливо проводити регулярний моніторинг і аудит мережевих потоків, щоб оперативно виявляти аномальну активність, що може свідчити про спроби сніфінгу. Таке комплексне забезпечення безпеки є критично важливим для підтримання конфіденційності, цілісності і доступності даних, що циркулюють у мережевих системах VoIP.

Розуміння технічних аспектів сніфінгу та його потенційних загроз дозволяє не лише правильно вибудувати захист мережі, а й адаптувати стратегії безпеки відповідно до постійно змінюваного ландшафту кіберзагроз.

1.3 Вимоги до захисту

Шифрування (TLS, SRTP), аутентифікація, IDS/IPS.

TLS (Transport Layer Security) — це протокол, який захищає дані під час їх передачі в інтернеті. Він використовується для HTTPS-сайтів, електронної пошти та VPN, забезпечуючи шифрування та автентифікацію. Наприклад, коли ви заходите на банківський сайт, TLS гарантує, що дані не будуть перехоплені.

- клієнт і сервер обмінюються ключами під час "рукоостискання";
- дані шифруються симетричним ключем для швидкої передачі;
- сервер зазвичай автентифікується за допомогою сертифікатів, що підтверджує його ідентичність.

SRTP (Secure Real-time Transport Protocol) — це протокол для захисту медіа даних у реальному часі, наприклад, під час голосових дзвінків чи відеоконференцій. Він шифрує та автентифікує дані, щоб запобігти їх перехопленню чи зміні.

- використовує AES для шифрування медіа потоків;
- додає хеш для перевірки автентичності та цілісності пакетів;
- працює з зовнішніми протоколами для обміну ключами, як ZRTP чи MIKEY.

Шифрування є основою для забезпечення конфіденційності, цілісності

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

та автентичності даних у мережах. TLS і SRTP — це спеціалізовані протоколи, які вирішують різні завдання: TLS для загального інтернет-трафіку, а SRTP для реального часу медіа передач. Обидва базуються на криптографічних алгоритмах і стандартах, таких як RFC, опублікованих IETF.

TLS (Transport Layer Security) є наступником SSL (Secure Sockets Layer) і забезпечує безпечну передачу даних через інтернет. Він використовується для захисту веб-трафіку (HTTPS), електронної пошти, VPN та інших сервісів. Протокол працює на транспортному рівні моделі OSI, забезпечуючи шифрування, автентифікацію та цілісність. Часто аутентифікується лише сервер, але можлива й взаємна автентифікація за допомогою Public Key Infrastructure (PKI). Процес починається з обміну публічними ключами між клієнтом і сервером. Використовуються асиметричні алгоритми, такі як RSA чи ECDHE, для встановлення симетричного ключа сеансу. Після рукописання дані шифруються симетричними алгоритмами, такими як AES, DES або RC4, для швидкої обробки. Сервер аутентифікується за допомогою сертифікатів X.509, які видаються довіреними центрами сертифікації. Клієнт може бути аутентифікований, якщо потрібна взаємна автентифікація. Існують версії TLS 1.0, 1.1, 1.2, 1.3. TLS 1.3, які описані у RFC 8446, архівовано випущений у серпні 2018 року, покращує безпеку та ефективність [13]. Це стандарт за замовчуванням у Firefox (версія 60.0+) і Google Chrome (версія 70+), підтримується OpenSSL з версії 1.1.1.

Навіщо TLS потрібно у мережі: Перш за все це захист SIP-сигналізації: TLS захищає інформацію про виклики (хто кому дзвонить, тривалість, SIP-паролі), запобігаючи перехопленню та прослуховуванню злоумисниками. Автентифікація сервера відбувається за типом. Клієнти перевіряють, що вони дійсно підключаються до FreePBX, а не до підробленого сервера. Цілісність даних: Гарантує, що ніхто не змінив дані під час передачі. TLS доволі проблематичний в налаштуванні, але дуже гнучкий, також у нього є підтримка різних алгоритмів обміну ключами, як показано у Табл. 1.1:

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Таблиця 1.1

Підтримка алгоритмів TLS

Алгоритм	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3 (проект)	Статус/Примітки
RSA	Так	Так	Так	Так	Так	Ні	Визначено для TLS 1.2 у відповідних RFC
DH-RSA	Ні	Так	Так	Так	Так	Ні	
DHE-RSA (впередня секретність)	Ні	Так	Так	Так	Так	Так	
ECDH-RSA	Ні	Ні	Так	Так	Так	Ні	
ECDHE-RSA (впередня секретність)	Ні	Ні	Так	Так	Так	Так	
DH-DSS	Ні	Так	Так	Так	Так	Ні	
DHE-DSS (впередня секретність)	Ні	Так	Так	Так	Так	Ні	Видалено з TLS 1.3 [14]
ECDH-ECDSA	Ні	Ні	Так	Так	Так	Ні	
ECDHE-ECDSA (впередня секретність)	Ні	Ні	Так	Так	Так	Так	
PSK	Ні	Ні	Так	Так	Так		
PSK-RSA	Ні	Ні	Так				

- алгоритми, що забезпечують "впередню секретність" (forward secrecy): DHE, ECDHE;
- вразливі до атак "людина посередині": DH_anon, ECDH_anon;
- Google припинив використання 1024-бітних ключів у липні 2013 року, перейшовши на 2048-бітні ключі.

Застосування TLS в браузерах для HTTPS, у службах електронної пошти, VPN, а також у будь-яких сценаріях, де потрібна безпечна передача даних. Наприклад, коли заходиш на сайт банку, TLS забезпечує, що дані не будуть перехоплені.

SRTP (Secure Real-time Transport Protocol) — це профіль RTP (Real-time Transport Protocol), призначений для шифрування, автентифікації повідомлень, забезпечення цілісності та захисту від заміни даних у unicast і multicast передачах медіа [12]. Він був розроблений експертами компаній Cisco та Ericsson: David Annaba, David McGrew, Mark Baugher, Mats Naslund, Elisabetta Carrara, Karl Norman, Rolf Blom, і вперше опублікований IETF у березні 2004 року. SRTP використовується для VoIP, відеоконференцій та інших реальних часових медіа-сервісів.

Технічні деталі

Шифрування використовує AES у двох режимах:

- SEIC (Segmented Integer Counter) — за замовчуванням, з 128-бітним ключем (112-бітний сесійний ключ);
- f8-режим — для мереж 3G UMTS, з тими ж довжинами ключів;
- також підтримується "нульовий шифр" (null cipher), який не шифрує дані, але його реалізація обов'язкова в системах SRTP. Нові алгоритми шифрування потребують нових стандартів RFC.

Аутентифікація та цілісність: Використовує HMAC-SHA1 для створення 160-бітного хешу, який скорочується до 80 або 32 бітів і додається до пакетів для перевірки автентичності та цілісності, захищаючи від атак "людина посередині".

Ключі: Використовує функцію генерації ключів для створення сесійних ключів (SRTP, SRTCP, сесійних ключів) з основного ключа. Періодичні зміни функції ключів підвищують безпеку. Залежить від зовнішніх протоколів обміну ключами: ZRTP, MIKEY, SDP.

Зв'язок із RTCP: Оскільки RTP тісно пов'язаний із RTCP (Real-Time Control Protocol), SRTP має споріднений протокол SRTCP (Secure RTCP), який забезпечує безпеку для RTCP-пакетів. Автентифікація повідомлень є обов'язковою для SRTCP. Використання SRTP або SRTCP є необов'язковим, але навіть якщо вони використовуються, функції шифрування та автентифікації можуть бути включені або виключені.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

Застосування SRTP у VoIP-системах, таких як Skype, відеоконференціях, як Zoom, та інших додатках, де потрібна передача медіа даних у реальному часі з гарантією конфіденційності та цілісності. Наприклад, під час відеодзвінка SRTP забезпечує, що голос і відео не будуть перехоплені чи змінені.

Таблиця 1.2

Порівняння TLS і SRTP

Характеристика	TLS	SRTP
Призначення	Безпечна передача даних у мережі	Захист медіа даних у реальному часі
Застосування	HTTPS, електронна пошта, VPN	VoIP, відеоконференції
Алгоритми шифрування	AES, DES, RC4 тощо	AES (SEIC, f8-режим)
Аутентифікація	Сертифікати X.509, HMAC	HMAC-SHA1
Ключі	Внутрішній обмін (RSA, ECDHE)	Зовнішні протоколи (ZRTP, MIKEY)

Обидва протоколи є частиною ширшого ландшафту кібербезпеки, де стандарти, такі як RFC, забезпечують їхню сумісність і еволюцію. TLS є стандартом для веб-безпеки, тоді як SRTP є спеціалізованим рішенням для реального часу, що відображає різницю у їхніх цілях [11, 12, 13]. Їхнє використання гарантує, що дані залишаються захищеними від несанкціонованого доступу та атак, таких як "людина посередині".

В цілому TLS і SRTP є критично важливими для забезпечення безпеки даних у своїх сферах. TLS забезпечує захист для загального інтернет-трафіку, тоді як SRTP спеціалізується на медіа передачах у реальному часі. Їхнє розуміння допомагає краще оцінити, як сучасні мережі забезпечують конфіденційність і цілісність.

Мінімальний вплив на QoS, сумісність з інфраструктурою.

Дослідження свідчить, що для мінімального впливу на QoS важливо правильно класифікувати та пріоритизувати трафік. Ймовірно, сумісність з інфраструктурою досягається через використання стандартних механізмів,

таких як DSCP. Є думки, що складність конфігурації QoS може вплинути на продуктивність, тому її варто мінімізувати.

Щоб зменшити вплив на якість обслуговування (QoS), потрібно чітко визначити вимоги до трафіку, наприклад, для відеоконференцій чи голосового зв'язку. Використовувати маркування трафіку (наприклад, DSCP) поблизу джерела, щоб мережа могла швидко розпізнавати пріоритети [15]. Також створити окремі черги для різних типів трафіку, щоб уникнути перевантаження. Дослідження показують, що апаратні рішення для QoS працюють ефективніше, ніж програмні, тому, якщо можливо, використовувати їх.

А для забезпечення сумісності з існуючою інфраструктурою важливо використовувати стандарти, як-от DSCP, які підтримують більшість мережевих пристроїв. Переконайтесь, що обладнання здатне обробляти нові політики QoS, і інтегрувати їх із системами управління, наприклад, Active Directory через Group Policy. Це допоможе уникнути необхідності дорогих оновлень.

Нефункціональні вимоги, такі як мінімальний вплив на QoS і сумісність з інфраструктурою, є критично важливими для забезпечення стабільної роботи систем, особливо в мережах, де використовуються додатки з високими вимогами до продуктивності, як-от VoIP чи відеоконференції. Ці аспекти допомагають оптимізувати використання наявних ресурсів і уникнути дорогих оновлень інфраструктури.

QoS (Quality of Service) стосується здатності мережі надавати кращий сервіс для обраного трафіку, зокрема щодо пропускної здатності, затримки та джитеру. Для мінімального впливу на QoS необхідно, правильне визначення бізнес-цілей: Спочатку потрібно чітко визначити бізнес-цілі, які мають бути досягнуті через впровадження QoS. Наприклад, забезпечення високої якості для реального часу, як-от голосові дзвінки. Це допомагає правильно розподілити ресурси. Класифікувати та маркувати трафік, важливо класифікувати трафік якомога ближче до джерела і використовувати

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

маркування, як-от Differentiated Services Code Point (DSCP). Це дозволяє мережевим пристроям швидко визначати пріоритети. Використовувати апаратні рішення. Дослідження, зокрема з Cisco Press, показують, що апаратні засоби для QoS забезпечують вищу продуктивність порівняно з програмними, тому їх варто використовувати, якщо це можливо. Правильне управління чергами: Створювати окремі черги для різних класів трафіку, як-от черги реального часу (RFC 3246), гарантовані черги (RFC 2597) та обмежені черги. Це допомагає уникнути перевантаження і забезпечити пріоритет для чутливих додатків. Наприклад, EasyQoS рекомендує такі підходи для точного розподілу ресурсів.

Уникнення перевантаження; Встановлюються ліміти пропускної здатності на інтерфейсах, але не занадто низькі, щоб уникнути втрати пакетів. Fortinet радить враховувати розподіл пакетів між чергами, щоб зменшити затримки.

Мінімізація складності; Складна конфігурація QoS може знизити продуктивність, тому її варто спростити. Наприклад, Palo Alto Networks наголошує на важливості налаштувань для високої ефективності [16].

Тестування; Для точних результатів тестування використовуйте протокол UDP і уникайте перевантаження пропускної здатності. Це допомагає оцінити реальний вплив на QoS.

Сумісність з існуючою інфраструктурою означає, що нові політики QoS мають інтегруватися з поточним обладнанням і системами без значних змін.

Таблиця 1.3

Ключові аспекти QoS

Аспект	Рекомендація для QoS	Рекомендація для сумісності
Класифікація трафіку	Маркувати трафік (DSCP) поблизу джерела	Використовувати стандарти, як-от DSCP, для підтримки
Використання ресурсів	Створювати окремі черги для різних класів трафіку	Інтегрувати з існуючими системами, як-от Group Policy

Ключові аспекти QoS

Аспект	Рекомендація для QoS	Рекомендація для сумісності
Уникнення перевантаження	Встановлювати ліміти пропускної здатності, але не занадто низькі	Перевіряти можливості обладнання перед впровадженням
Складність конфігурації	Мінімізувати для забезпечення продуктивності	Забезпечити простоту для легкої інтеграції
Тестування та моніторинг	Використовувати UDP, регулярно моніторити та налаштовувати	Тестувати сумісність з поточною інфраструктурою

З додаткові рекомендації варто відмітити такі як Моніторинг та налаштування: Після впровадження політик QoS регулярно проводити моніторинг їхню ефективність і адаптувати до змін у бізнес-середовищі. Наприклад, *Palo Alto Networks* радить постійно коригувати політики. Забезпечення безпеки: Враховувати безпеку, щоб критичні додатки не були уразливими через неправильне пріоритезування. Наприклад, *Spiceworks* наголошує на важливості безпечного переносу даних. Документування: Документувати всі зміни в конфігурації QoS та інфраструктурі для майбутнього аналізу та відновлення. Це допоможе уникнути помилок під час масштабування [23].

Для забезпечення мінімального впливу на QoS і сумісності з інфраструктурою необхідно комбінувати стандартні підходи, як-от маркування DSCP і створення черг, із ретельним аналізом можливостей існуючого обладнання. Регулярний моніторинг і адаптація політик допоможуть підтримувати стабільну продуктивність і уникнути дорогих оновлень.

GDPR та *ISO 27001* — це ключові нормативні стандарти, пов'язані з управлінням даними та інформаційною безпекою. Ось короткий огляд:

GDPR (General Data Protection Regulation): Регламент ЄС 2016/679, який регулює захист персональних даних громадян ЄС [17].

- застосовується до організацій, які обробляють дані резидентів ЄС, незалежно від їхнього розташування;
- вимагає згоди на обробку даних, прозорості, права на доступ, видалення ("право бути забутим") та повідомлення про витoki даних протягом 72 годин;
- штрафи: до 20 млн євро або 4% річного обороту компанії (залежно від того, що більше).

ISO 27001: Міжнародний стандарт для систем управління інформаційною безпекою (СУІБ) [18].

- визначає вимоги до створення, впровадження, підтримки та вдосконалення СУІБ;
- включає оцінку ризиків, політики безпеки, навчання персоналу, управління інцидентами;
- сертифікація добровільна, але підтверджує відповідність стандартам безпеки.

Спільне та відмінності:

- GDPR фокусується на захисті персональних даних і є юридично обов'язковим у ЄС. ISO 27001 — ширший стандарт, який охоплює загальну інформаційну безпеку та є добровільним;
- GDPR може вимагати впровадження практик, сумісних з ISO 27001, для забезпечення відповідності;

Висновки до першого розділу

У першому розділі проведено аналіз принципів роботи VoIP-систем і визначено основні вразливості, зумовлені їх архітектурою та протокольними особливостями. Розглянуто мотивацію зломисників, серед яких — фінансова вигода, шпигунство, саботаж та протестна активність. Деталізовано типові кібератаки (DDoS, MITM, Sniffing, SPIT) та їх вплив на доступність, конфіденційність і цілісність зв'язку. За підсумками аналізу сформульовано ключові технічні й організаційні вимоги до побудови ефективної підсистеми безпеки VoIP.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

РОЗДІЛ 2. МОДЕЛЬ ЗАГРОЗ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ В GNS

2.1 Розробка моделі загроз

Об'єктом аналізу є мережева інфраструктура організації, що складається з двох офісів, об'єднаних зв'язком з використанням протоколу HSRP для відмовостійкості. Інфраструктура включає маршрутизатори (R-22-1-1, R-22-1-2, SW-22-1-3), комутатори (SW-22-1-1, SW-22-1-2), віртуальні локальні мережі (VLANs), а також підсистему інтернет-телефонії на базі FreePBX (PBX), що надає голосові послуги внутрішнім користувачам (робочі станції WS-1..WS-13 з софтбонами, наприклад MicroSIP) та забезпечує доступ до глобальної мережі Інтернет.

Межі об'єкта охоплюють:

- всі мережеві пристрої (маршрутизатори, комутатори) та їх конфігурації;
- сервер IP-ATC FreePBX;
- кінцеві пристрої користувачів (робочі станції з софтбонами);
- мережеві сегменти (VLANs), включаючи між-офісний зв'язок та доступ до інтернету.

Суб'єкти загроз – це індивіди, групи або організації, які можуть становити загрозу для інформаційних систем та даних. Їхня діяльність може бути спрямована на викрадення, зміну, знищення інформації або порушення доступності сервісів [19].

Таблиця 2.4

Суб'єкти (джерела) загроз

Зовнішні зловмисники	Внутрішні зловмисники	Ненавмисні дії/помилки персоналу	Збої обладнання/ПЗ
Хакери, кіберзлочинні угруповання, конкуренти, що діють за межами мережі організації.	Незадоволені або звільнені співробітники, недобросовісний персонал, що має доступ до внутрішньої мережі.	Вихід з ладу мережевих пристроїв, помилки у програмному забезпеченні (наприклад, FreePBX, операційної системи), несумісність компонентів.	Вихід з ладу мережевих пристроїв, помилки у програмному забезпеченні (наприклад, FreePBX, операційної системи), несумісність компонентів.

Вразливості системи

Тип вразливості	Приклад
Некоректні налаштування брандмауера FreePBX	Виявлений факт блокування SIP та RTP трафіку свідчить про потенційну можливість неправильної конфігурації брандмауера, що може залишити "дірки" для несанкціонованого трафіку або, навпаки, заблокувати легітимний.
Вразливості програмного забезпечення FreePBX/Asterisk/OC	Як будь-яке ПЗ, FreePBX та Asterisk можуть містити невідомі (0-day) або відомі, але не виправлені вразливості, що дозволяють віддалене виконання коду, ескалацію привілеїв, або DoS-атаки.
Слабкі паролі/недостатня аутентифікація SIP-розширень	Можливість підбору паролів до SIP-розширень або адміністративних облікових записів FreePBX, що може призвести до фроду або несанкціонованого доступу.
Проблеми з Port Security	Виявлене спрацювання Port Security свідчить про спроби підключення несанкціонованих пристроїв або неправильну конфігурацію, що може бути вектором атаки.
Недостатня сегментація трафіку	Хоча VLANs реалізовані, існує ризик неналежної ізоляції трафіку між різними підрозділами (як показано на прикладі дзвінків 118 на 115) або між офісами, якщо ACL налаштовані некоректно.
Відсутність шифрування голосового трафіку (RTP)	Якщо SRTP не використовується, голосовий трафік може бути перехоплений та прослуханий.
Відсутність шифрування сигналізації (SIP)	Якщо TLS для SIP не використовується, метадані дзвінків (хто, кому, коли) можуть бути перехоплені.
Відсутність належного моніторингу трафіку	Хоча моніторинг згадується, його ефективність є вразливістю, якщо він не виявляє аномалій (наприклад, спроб флуду, несанкціонованих дзвінків).
Застаріле програмне забезпечення	Якщо FreePBX, Asterisk, або операційна система не оновлюються регулярно, вони залишаються вразливими до вже відомих атак.

Загрози (дії зловмисників/наслідки вразливостей)

Загроза	Реалізація
Телефонний фрод	Використання зламаних SIP-розширень для здійснення дорогих дзвінків (міжнародні, преміум-номери), що призводить до фінансових втрат організації.
DoS/DDoS атаки	Перевантаження FreePBX-сервера або мережевих каналів, що призводить до повного припинення голосового зв'язку, неможливості реєстрації SIP-клієнтів та недоступності сервісів (приклад з брандмауером).
Прослуховування розмов (Eavesdropping)	Перехоплення голосового трафіку для отримання конфіденційної інформації (комерційна таємниця, особисті дані).
Підміна ідентифікатора абонента (Caller ID Spoofing)	Зловмисник видає себе за іншого користувача або внутрішній номер для шахрайства або обходу політик безпеки.
Несанкціонований доступ до системи PBX	Отримання адміністративного доступу до FreePBX, що дозволяє змінювати конфігурацію, перенаправляти дзвінки, прослуховувати розмови або використовувати систему як плацдарм для подальших атак на внутрішню мережу.
Витік інформації	Компрометація даних, що передаються через VoIP, або конфіденційної інформації, яка зберігається на сервері FreePBX (наприклад, записи розмов, дані про користувачів).
Збій у між-офісному зв'язку	Компрометація маршрутизаторів або каналів зв'язку між офісами, незважаючи на HSRP, що може призвести до ізоляції офісів.
Несанкціонований доступ до внутрішніх сегментів мережі	Обхід ACL або Port Security, що дозволяє зловмиснику отримати доступ до VLANs, до яких він не мав би доступу.

У наступній таблиці 2.4, зображено наслідки загроз в компанії і включає в себе 5 пунктів.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Наслідки загроз

Загроза	Наслідок
Фінансові втрати	Від телефонного фроду, простою бізнесу через відсутність зв'язку.
Репутаційні втрати	Втрата зв'язку з клієнтами/партнерами, неможливість внутрішньої комунікації.
Порушення бізнес-процесів	Втрата зв'язку з клієнтами/партнерами, неможливість внутрішньої комунікації.
Компрометація конфіденційності	Розкриття секретної інформації.
Штрафи та юридичні наслідки	У разі порушення нормативних актів щодо захисту даних.

2.2 Побудова мережевої інфраструктури

Ідея створення мережевої інфраструктури, що базується на візуалізації вже існуючих реалізацій, полягає в тому, щоб взяти за основу успішні, перевірені часом та функціоналом архітектурні рішення, адаптувати їх до специфічних вимог та ресурсів конкретної організації, а потім імплементувати. Це не просто копіювання, а глибоке аналітичне осмислення чужого досвіду, що дозволяє:

Оптимізувати дизайн: Вивчення вже працюючих моделей дозволяє ідентифікувати найкращі практики, оптимальні конфігурації та ефективні способи розподілу ресурсів [21]. Це мінімізує ризики, пов'язані з "винаходом велосипеда", і дозволяє зосередитися на тонкій настройці та інтеграції.

Прискорити розгортання: Наявність готових шаблонів та візуалізованих схем значно прискорює етапи планування та впровадження. Немає потреби починати "з чистого листа".

Підвищити надійність та безпеку: Існуючі реалізації часто вже пройшли "обкатку" і виявили потенційні вразливості або вузькі місця [22]. Візуалізуючи їх, можна заздалегідь врахувати ці аспекти та імплементувати перевірені механізми захисту та відмовостійкості.

З основу мережевого обладнання було обрано Cisco Catalyst 8200L є новітнім поколінням маршрутизаторів від Cisco, розроблених для забезпечення високопродуктивного та безпечного підключення на периферії мережі (Edge). Для мережевого проєкту маршрутизатор є дуже вдалим вибором, оскільки він дозволяє продемонструвати впровадження сучасних, комплексних механізмів мережевої безпеки, які є невід'ємною частиною захисту VoIP. Мережева підсистема безпеки, що включає FreePBX з TLS/SRTP, та підсилена мережевими можливостями Catalyst 8000, чудовий та надійний вибір та актуальне рішення.

Коммутатор було обрано Cisco Catalyst 9300-48P який є флагманською платформою комутаторів доступу та агрегації корпоративного класу, розробленою для підтримки сучасних конвергентних мереж. Ця серія ідеально підходить для розгортання VoIP-систем завдяки своїй високій продуктивності, надійності, розширеним функціям безпеки та можливостям живлення через Ethernet (PoE). Працюючи під управлінням операційної системи Cisco IOS XE, Catalyst 9300 інтегрується з іншими компонентами Cisco, включаючи маршрутизатори Catalyst 8000, забезпечуючи уніфіковане управління та політики. У контексті проєкту з розробки підсистеми безпеки VoIP, комутатор Cisco Catalyst 9300 відіграє ключову роль на рівні доступу та агрегації, забезпечуючи безпечне та якісне підключення кінцевих VoIP-пристроїв.

Зменшити витрати: Економія досягається за рахунок уникнення дорогих помилок, оптимізації використання обладнання та програмного забезпечення.

Полегшити підтримку та масштабування: Чітко визначена та візуалізована архітектура спрощує подальше обслуговування, пошук несправностей та майбутнє розширення мережі.

Застосування принципу візуалізації у дипломному проєкті з двома офісами, FreePBX, VLANs та HSRP є чудовим прикладом застосування цієї ідеї.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

Це типова архітектура для середнього бізнесу, що потребує надійного зв'язку та голосових послуг:

Візуалізація спроектованих офісів з метою наближення до реальних проектних реалізацій: Побудова віртуального проекту, за для чіткого розуміння розташування користувачів, за для правильної побудови мережі.

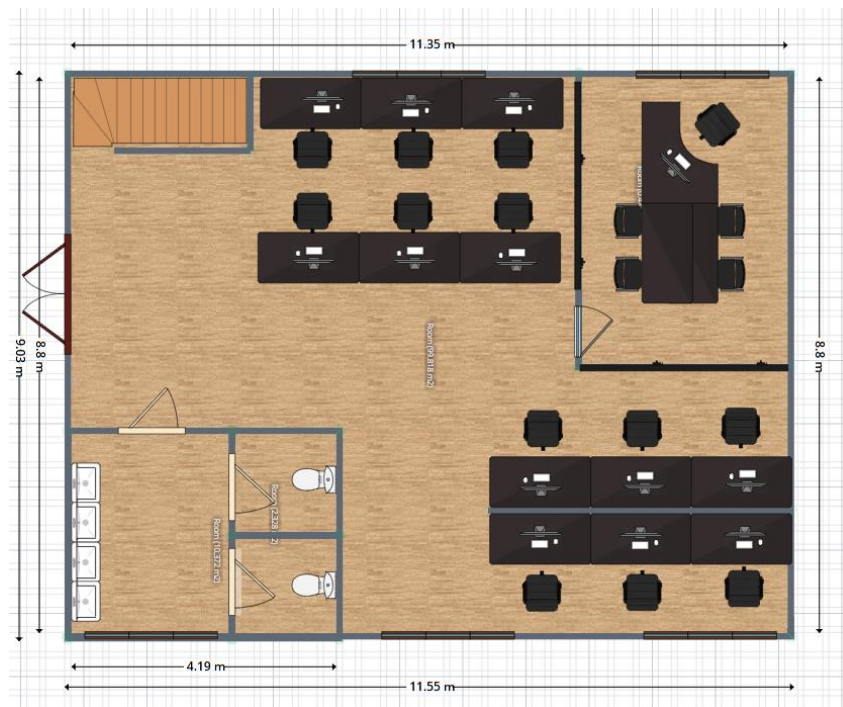


Рисунок 2.7 – Реалізація першого 2D-офісу

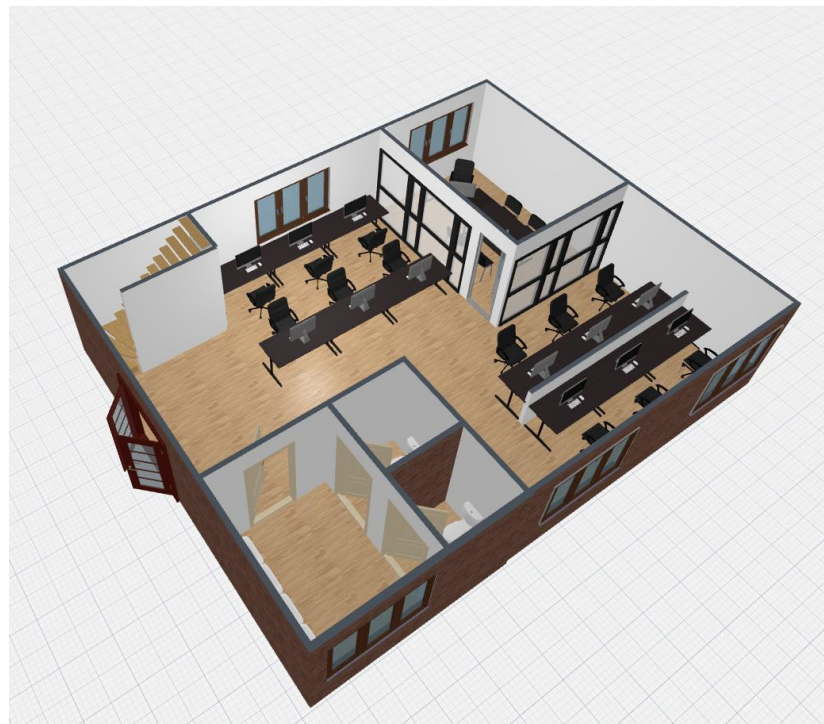


Рисунок 2.8 – 3D-проекція першого офісу

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

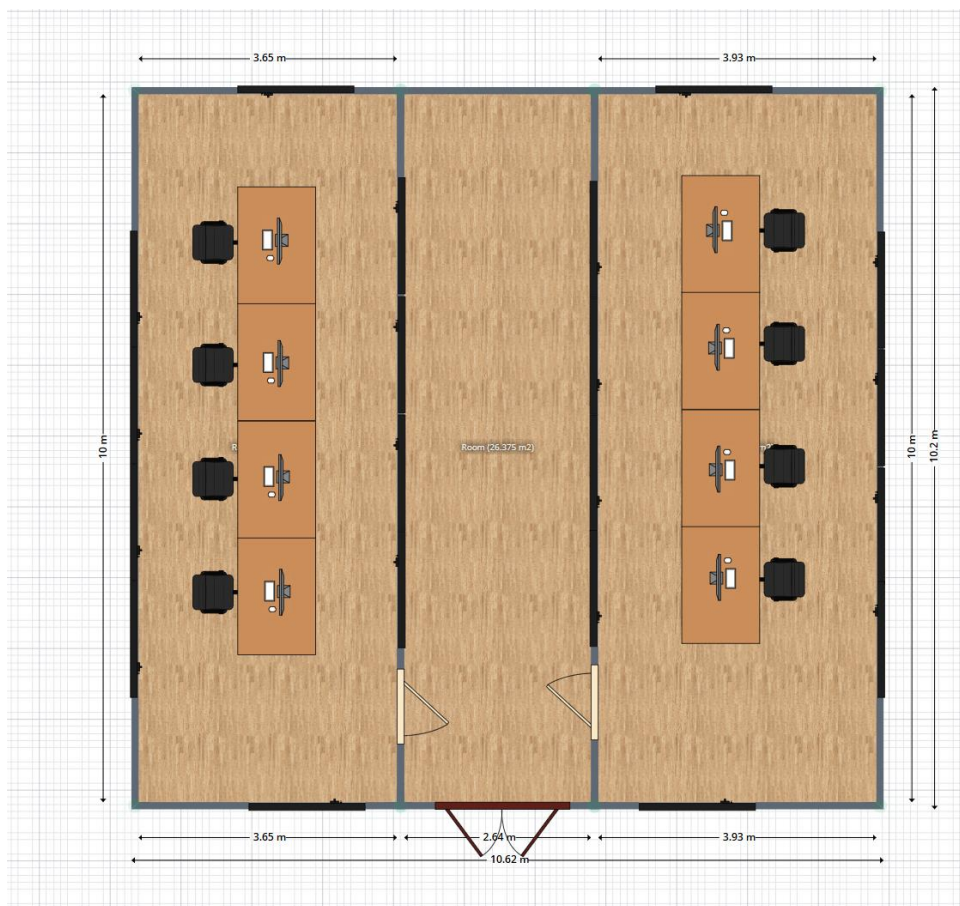


Рисунок 2.9 – Реалізація другого 2D-офісу



Рисунок 2.10 – 3D-проекція другого

Два офіси з маршрутизаторами з технологією HSRP: Це стандартне рішення для забезпечення відмовостійкості та безперервності зв'язку між

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

географічно розділеними об'єктами. Візуалізація такої схеми дозволяє чітко бачити шляхи проходження трафіку, точки відмови та механізми переключення.

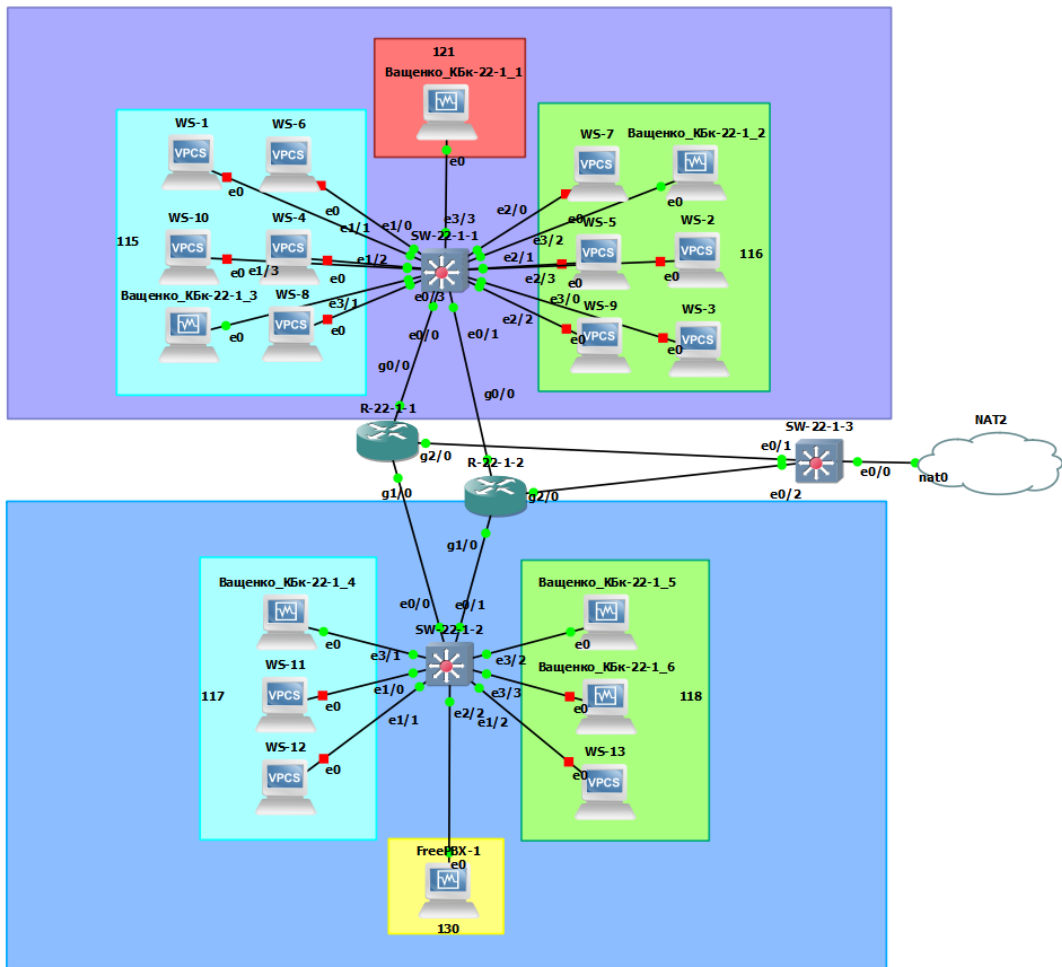


Рисунок 2.11 – Вигляд мережі в GNS

VLANs (Virtual Local Area Networks): Це базова, але критично важлива практика для сегментації мережі. Візуалізація дозволяє чітко розмежувати трафік відділів (наприклад, голос, дані, управління), підвищуючи безпеку та ефективність, мінімізуючи "широкомовні шторми" та спрощуючи управління.

Мережа побудована з урахуванням роботи кожного підрозділа, та поділена на VLAN-и звичайні користувачі мають нумерацію від 115 до 118, де 115 і 116 це в одному офісі, а 117 та 118 це інший офіс, працюють вони за типом 115 та 117 це один підрозділ, а 116 та 118 це інший [3]. Таким чином, у двох різних офісах є можливість зв'язку, підрозділів без можливості доступу

до іншого. Така реалізація зумовлена тим що на багатьох підприємствах, є велика кількість відділів, які повинні працювати тільки з тими хто безпосередньо пов’язаний з їхньою сферою занятості, але без доступу з інших нічим незв’язаних підрозділів [23].

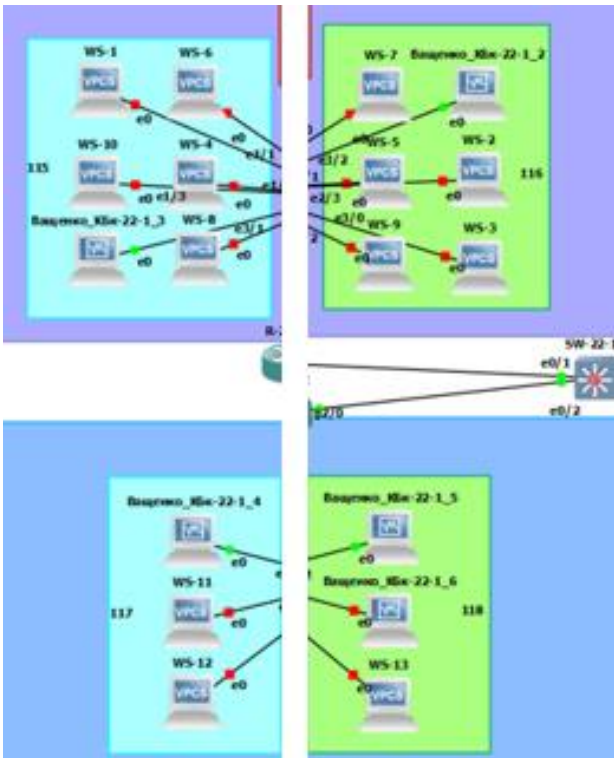


Рисунок 2.12 – Вигляд VLAN в GNS

Також було враховано що усією мережею повинен хтось керувати та підтримувати комунікацію між IP-телефонією, тому для цього було створено додаткові VLAN-и, а саме 121 та 130 [3]. ПК-адміністратор має VLAN 121, відповідає він за моніторинг як самих користувачів, та і для налаштування сервера FreePBX, який в свою чергу налаштований на VLAN 130.



Рисунок. 2.13 – Вигляд адмін VLAN-ів в GNS

Комутатори (SW-22-1-1, SW-22-1-2) та маршрутизатор доступу в Інтернет (SW-22-1-3): Це стандартні компоненти будь-якої корпоративної мережі, їх візуалізація допомагає зрозуміти потоки даних, точки входу/виходу та місця застосування політик безпеки.

Інтернет-з'єднання є не просто "постачанням" для VoIP, а його невід'ємною життєво важливою основою. Його якість, стабільність та, найголовніше, безпека безпосередньо визначають надійність, доступність та конфіденційність усієї VoIP-інфраструктури. Без надійного та захищеного інтернет-каналу, будь-яка складна підсистема безпеки VoIP втрачає свою ефективність для зовнішніх комунікацій, а ризики кібератак значно зростають. Тому проектування безпеки VoIP повинно починатися з ретельного аналізу та захисту саме інтернет-з'єднання.

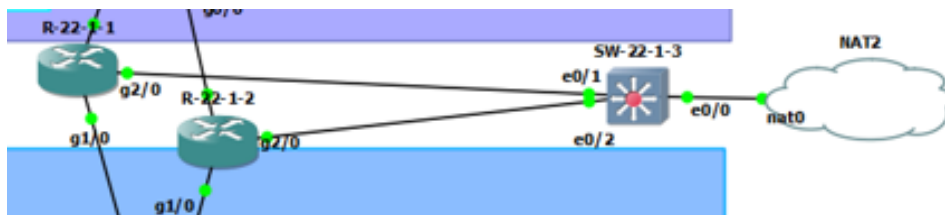


Рисунок. 2.14 – Вигляд доступу до інтернету в GNS

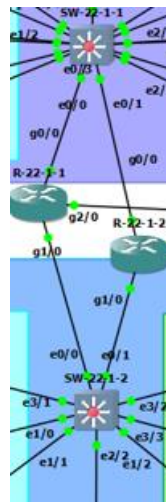


Рисунок 2.15 – Вигляд основних комутаторів GNS

IP-ATC FreePBX - Це одне з найпопулярніших рішень для програмної телефонії. Її інтеграція в уже існуючу мережу є типовою задачею, і візуалізація цього процесу дозволяє передбачити необхідні налаштування (брандмауер, порти, протоколи SIP/RTP).



Рисунок 2.16 – Вигляд IP-ATC FreePBX в GNS

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

Робочі станції з софтбонами (MicroSIP) - Це типовий сценарій використання IP-телефонії, що дозволяє уникнути придбання фізичних IP-телефонів, що також візуалізується при плануванні кінцевих точок зв'язку.

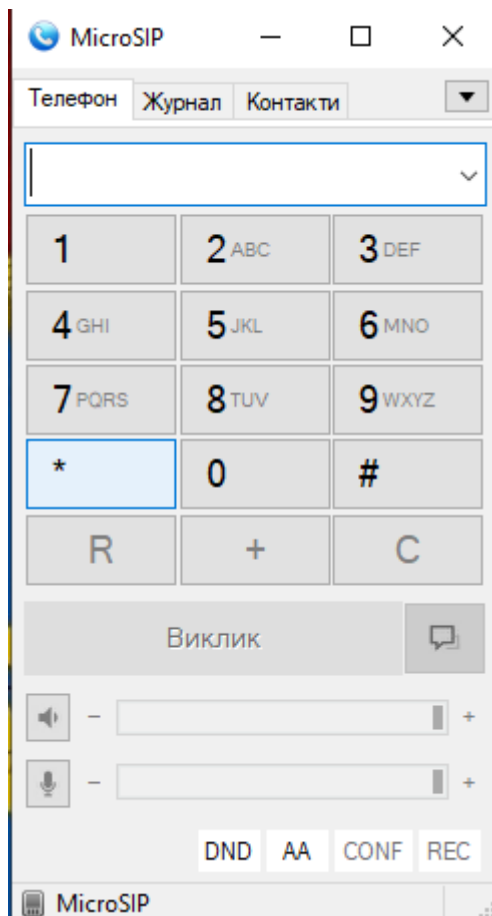


Рисунок 2.17– Вигляд софтбона MicroSIP

MicroSIP — це легкий, портативний і простий у використанні програмний SIP-телефон (софтфон) з відкритим вихідним кодом для операційних систем Windows. Він дозволяє користувачам здійснювати та приймати голосові та відеодзвінки (залежно від версії та кодеків), використовуючи протокол SIP (Session Initiation Protocol) через Інтернет. Це робить його чудовим інструментом для інтеграції з IP-АТС, такими як FreePBX, або для прямого підключення до SIP-провайдерів.

2.3 Реалізація заходів безпеки

Реалізація заходів безпеки в мережевій інфраструктурі, особливо в контексті інтеграції інтернет-телефонії, є не просто технічною вимогою, а критичною необхідністю, що зумовлена сучасними загрозами та прагненням

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

до безперервності бізнесу. Кожен крок у цьому процесі, від сегментації мережі до налаштування брандмауерів, має своє глибоке обґрунтування, спрямоване на захист життєво важливих комунікацій.

Насамперед, мережа є фундаментом будь-якої сучасної організації, а інтернет-телефонія – це її голос, який забезпечує зв'язок із клієнтами, партнерами та внутрішніми співробітниками. Компрометація або виведення з ладу цієї системи може призвести до значних фінансових втрат, адже кожен втрачений дзвінок – це потенційна втрачена угода або незадоволений клієнт. Крім того, порушення конфіденційності розмов може обернутися витоком комерційної таємниці, персональних даних або іншої чутливої інформації, що завдасть непоправної шкоди репутації компанії та може потягнути за собою юридичні наслідки та штрафи.

HSRP (Hot Standby Router Protocol):

Було реалізовано HSRP для забезпечення високої доступності та відмовостійкості, між маршрутизаторами R-22-1-1 та R-22-1-2.

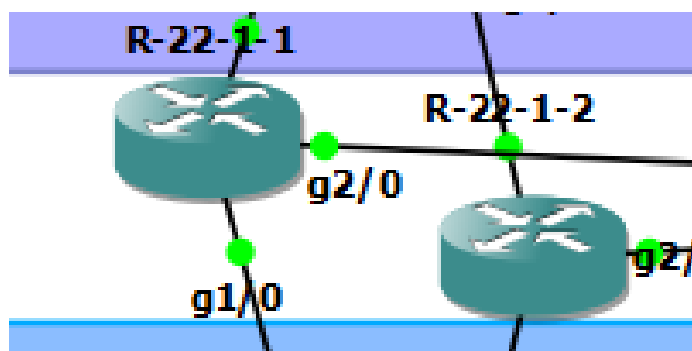


Рисунок 2.18 – Реалізація HSRP

Один маршрутизатор є активним, інший – резервним. У разі збою активного маршрутизатора, резервний автоматично перебирає його функції, забезпечуючи безперервність зв'язку між офісами.

При виході з ладу активного маршрутизатора, резервний автоматично перебирає на себе функцію шлюзу, забезпечуючи майже миттєве відновлення зв'язку без втручання користувача. Це критично важливо для голосового трафіку, який дуже чутливий до переривань [24].

Брандмауер (Firewall) на FreePBX:

Вбудований брандмауер FreePBX використовується для контролю мережевого трафіку, що надходить на сервер IP-АТС та виходить з нього.

Було активавано налаштування, додаючи правила для дозволу SIP (UDP 5060) та RTP (UDP 10000-20000) трафіку, а також було додано внутрішні мережі до довірених зон.

Адміністратор Додатки Зв'язок Панель приладів Звіти Налаштування УСП

Firewall

Налаштування Responsive Firewall Interfaces Networks

Known Network Definitions

You can add individual hosts and networks to override the default permission for an interface.

Example: Interface eth0 is assigned to the 'Internet' zone, and you then add '203.55.66.77' to the 'Local' zone on this page. Any traffic arriving from 203.55.66.77 will be granted access to services usable by 'Local' zone.

Any traffic arriving at eth0 from 203.55.66.88 (or any other undefined host or network) will only have access to services available to the 'Internet' zone, as that has been set to be the default zone for traffic arriving at that interface.

You may also enter hostnames here (including Dynamic DNS hosts), which will be automatically monitored and updated.

☐	Network/Host	Assigned Zone
☐	192.168.121.7/32	Trusted (Excluded from Firewall)
You can enter a short description for this network here.		
☐	192.168.121.0/24	Trusted (Excluded from Firewall)
You can enter a short description for this network here.		
☐	192.168.115.0/24	Local (Local trusted traffic)
You can enter a short description for this network here.		
☐	192.168.116.0/24	Local (Local trusted traffic)
You can enter a short description for this network here.		
☐	192.168.117.0/24	Local (Local trusted traffic)
You can enter a short description for this network here.		
☐	192.168.118.0/24	Local (Local trusted traffic)
You can enter a short description for this network here.		
Enter new IP or Hostname here		Local (Local trusted traffic) +
You can enter a short description for this network here.		

Рисунок 2.19 – Налаштований Firewall

Захист IP-АТС від несанкціонованого доступу, DoS-атак та інших мережевих загроз [25].

ACL (Access Control Lists) на маршрутизаторах/комутаторах:

Призначення ACL, використовуються для фільтрації трафіку на мережевому обладнанні, дозволяючи або забороняючи доступ між різними VLANs або до/з Інтернету.

```

ip access-list extended ACL_VLAN115
permit udp any any eq bootpc
permit udp any any eq bootps
permit ip 192.168.115.0 0.0.0.255 192.168.117.0 0.0.0.255
permit tcp 192.168.115.0 0.0.0.255 192.168.117.0 0.0.0.255 eq 5060
permit udp 192.168.115.0 0.0.0.255 192.168.117.0 0.0.0.255 eq 5060
permit tcp 192.168.115.0 0.0.0.255 192.168.117.0 0.0.0.255 eq 5061
permit udp 192.168.115.0 0.0.0.255 192.168.117.0 0.0.0.255 eq 5061
permit udp 192.168.115.0 0.0.0.255 192.168.117.0 0.0.0.255
deny ip 192.168.115.0 0.0.0.255 192.168.116.0 0.0.0.255
deny ip 192.168.115.0 0.0.0.255 192.168.118.0 0.0.0.255
deny ip 192.168.115.0 0.0.0.255 192.168.121.0 0.0.0.255
permit ip 192.168.115.0 0.0.0.255 any
ip access-list extended ACL_VLAN116
permit udp any any eq bootpc
permit udp any any eq bootps
permit ip 192.168.116.0 0.0.0.255 192.168.118.0 0.0.0.255
permit tcp 192.168.116.0 0.0.0.255 192.168.118.0 0.0.0.255 eq 5060
permit udp 192.168.116.0 0.0.0.255 192.168.118.0 0.0.0.255 eq 5060
permit tcp 192.168.116.0 0.0.0.255 192.168.118.0 0.0.0.255 eq 5061
permit udp 192.168.116.0 0.0.0.255 192.168.118.0 0.0.0.255 eq 5061
permit udp 192.168.116.0 0.0.0.255 192.168.118.0 0.0.0.255
deny ip 192.168.116.0 0.0.0.255 192.168.115.0 0.0.0.255
deny ip 192.168.116.0 0.0.0.255 192.168.117.0 0.0.0.255

```

Рисунок 2.20 – Налаштування ACL на R-22-1-1

Реалізація в основних вузлах мережій було налаштовано ACL їх використання є логічним наслідком створення VLANs та необхідності контролю доступу. Налаштування ACL було створено на R-22-1-1 та R-22-1-2. Так як було налаштування HSRP усі налаштування були продубльовані.

З вигоди є деталізований контроль доступу до ресурсів мережі, підвищення рівня безпеки та запобігання несанкціонованому трафіку [26].

Port Security на комутаторах:

Призначення функції самої безпеки використовується для обмеження кількості або дозволу лише певних MAC-адрес на конкретних портах комутатора.

```

interface Ethernet3/3
switchport access vlan 121
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0800.273f.51ce
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50

```

Рисунок 2.21 – Налаштування Port Security

Реалізація використання Port Security та налаштування для захисту від несанкціонованого підключення пристроїв. Це було реалізовано за для додаткового контролю над підключеннями пристроїв, налаштування було проведено на усіх доступних елементах мережі.

Вигода в запобіганні несанкціонованих підключень до мережі, є підвищення безпеки фізичного рівня [27].

Використання IP-ATC FreePBX:

Призначення центрального елементу підсистеми інтернет-телефонії організації є використання внутрішнього та зовнішнього голосового зв'язку.

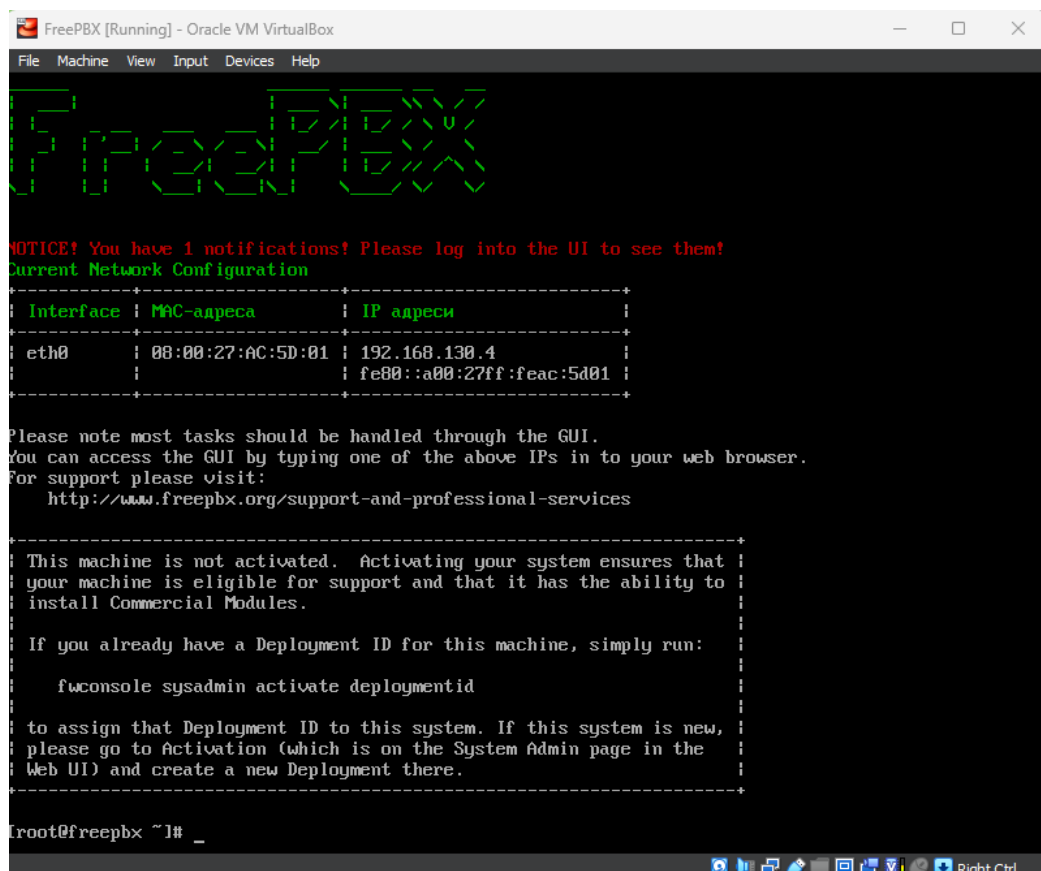


Рисунок 2.22 – Розгортання АТС FreePBX

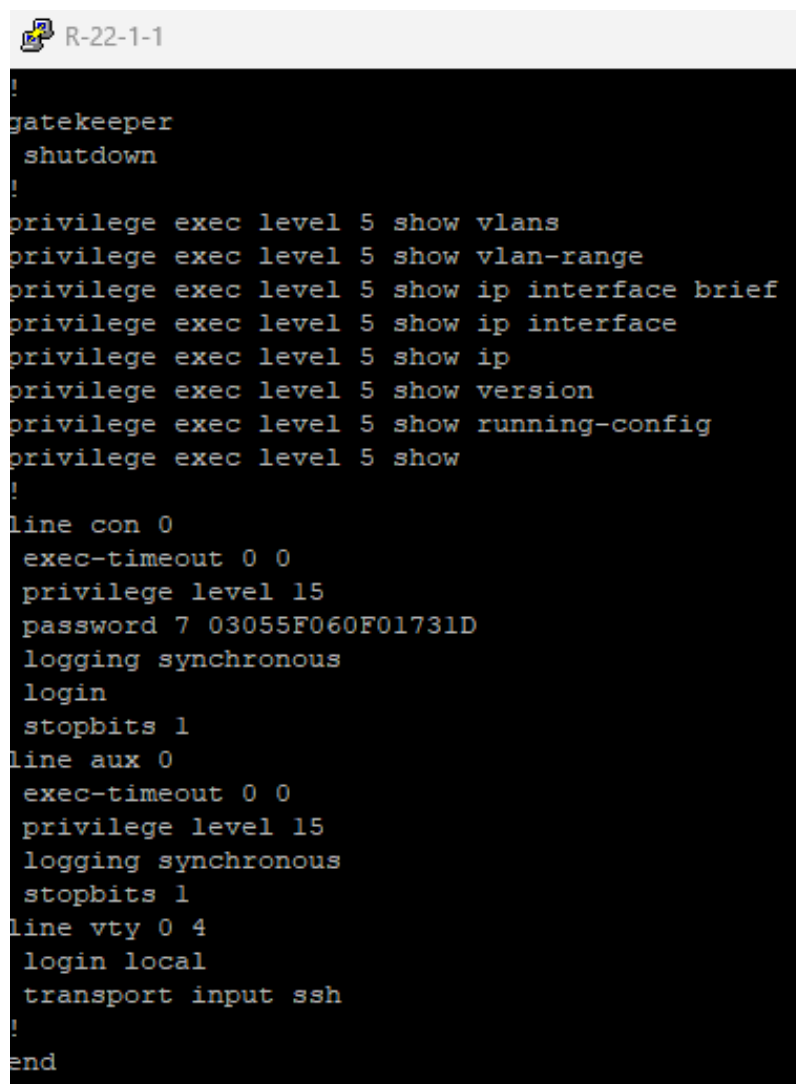
При реалізації був розгорнутий та підключений сервер, адресу можна було налаштувати статичну, але DHCP дає можливість надання різних IP що так чи інакше допомагає з безпекою. Також налаштовані розширення, які працюють з брандмауером, що вказує на її активне впровадження.

По вигоді є економічність, гнучкість, масштабованість та розширений функціонал VoIP-комунікацій [28].

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Базова безпека доступу до пристроїв:

По призначенню, є важливою частиною безпеки, адже відгороджує будь-яких зловмисників від доступу до комутаторів та маршрутизаторів. Що значно підвищує безпеку від зовнішніх зловмисників.



```
!
gatekeeper
shutdown
!
privilege exec level 5 show vlans
privilege exec level 5 show vlan-range
privilege exec level 5 show ip interface brief
privilege exec level 5 show ip interface
privilege exec level 5 show ip
privilege exec level 5 show version
privilege exec level 5 show running-config
privilege exec level 5 show
!
line con 0
exec-timeout 0 0
privilege level 15
password 7 03055F060F01731D
logging synchronous
login
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login local
transport input ssh
!
end
```

Рисунок 2.23 – Приклад налаштованої безпеки на маршрутизаторі

При реалізації, усі головні елементи були захищені паролем, з можливостями заходу Головного Адміні, або когось з обслуговуючого персоналу. За типом привілегій, admin_user privilege 15 secret, viewer_user privilege 5 secret. Також була додана можливість SSH-доступу, що дає змогу налаштування дистанційно.

За рахунок таких налаштувань, підвищується захист мережі від зовнішніх зловмисників. Також йде розподіл по привілегіям що також доволі важливо, для будь-якої компанії.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

TLS (Transport Layer Security)

TLS (і його попередник SSL) є криптографічним протоколом, призначеним для забезпечення безпечної комунікації через комп'ютерну мережу, таку як Інтернет [11]. У контексті VoIP, TLS використовується для шифрування сигнального трафіку SIP (Session Initiation Protocol).

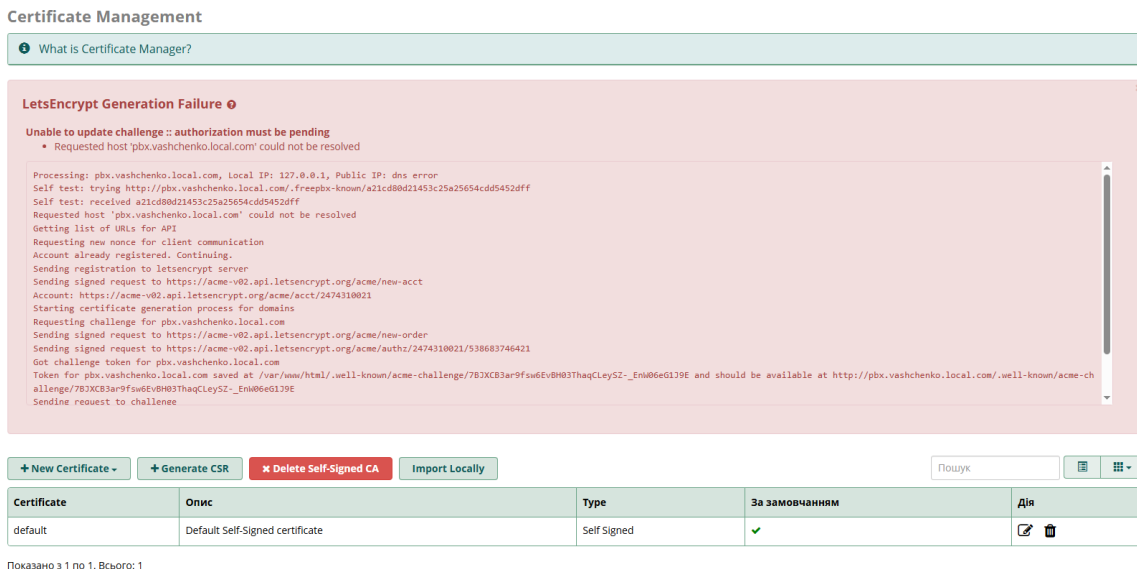


Рисунок 2.24 – Невдала спроба налаштування TLS

TLS працює під час так званого "TLS-рукоштовання" (TLS Handshake) між клієнтом (MicroSIP) та сервером (FreePBX). Для роботи TLS треба щоб було налаштовано публічний домен верхнього рівня (.com, .org, .ua), через який він буде працювати, нажалі такого домену за для правильно налаштування немає, спроби налаштування було переглянуто та прийнято рішення створити сертифікат TLS вручну. У FreePBX є можливість створення домену, але він локальний, але через консоль на сервері вдалося витягнути сертифікат по SSL програмою WinSCP. Після чого було налаштовано сертифікат на кожному учаснику ПК. У подальшому було налаштовано Asterisk SIP Settings де було налаштовано TLS/SSL/SRTP вибрано відповідний сертифікат у спадному меню менеджера сертифікатів. Вибрано TLSV1_2 як метод SSL. Встановлено перевірку клієнта на NO та перевірку сервер на "так". У розділі «Транспорт» встановлено TLS - 0,0,0,0 - ALL на Так. У розділі 0,0.0.0 (TLS) порт для прослуховування встановлено на 5061. На вкладці "Загальні налаштування SIP".

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

У розділі «Налаштування безпеки» встановлено обидва дозволити анонімним вхідним SIP -дзвінкам та дозволити SIP гостям ні. Встановлено призначення порту TLS за замовчуванням на PJSIP. Параметр PJSIP не виставлявся, тому треба перезапустити Asterisk, щоб переконатися, що налаштування TLS завантажуються. Як результат усе працює.

Certificate Management

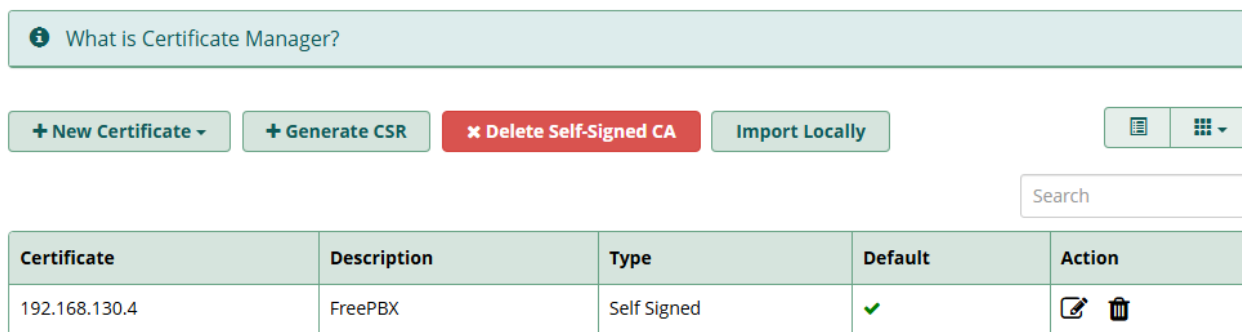


Рисунок 2.25 – Налаштований TLS

Вся інформація про виклики (хто кому дзвонить, SIP-паролі, логіни, тощо) шифрується, запобігаючи її перехопленню та зловживанням [15].

SRTP (*Secure Real-time Transport Protocol*)

SRTP є профілем протоколу RTP (Real-time Transport Protocol), призначеним для забезпечення безпечного передавання даних реального часу, таких як голосовий трафік у VoIP-дзвінках. Його основне призначення – це шифрування та автентифікація саме медіа-потоків.

SRTP працює в парі з TLS. Хоча TLS шифрує сигналізацію (SIP), SRTP шифрує аудіо/відео дані (RTP). Нажаль налаштувати немає можливості адже TLS не налаштовано.

На рахунок конфіденційність розмов то усі аудіодані шифруються, запобігаючи прослуховуванню зловмисниками. Це критично важливо для конфіденційних розмов та комерційних таємниць [11].

Висновки до другого розділу

Другий розділ присвячений розробці та обґрунтуванню архітектури спеціалізованої підсистеми безпеки для VoIP-мережі організації. У рамках цього розділу було детально описано вибір та інтеграцію ключових

технологічних рішень, зокрема програмної АТС FreePBX, яка виступає центральним елементом голосової мережі, а також обладнання Cisco для побудови надійної мережевої інфраструктури. Обґрунтовано необхідність та принципи впровадження механізмів криптографічного захисту, таких як TLS для забезпечення безпеки SIP-сигналізації та SRTP для шифрування медіа-трафіку. Також розглянуто принципи використання мережевого сегментування (VLAN) та протоколів високої доступності (HSRP) для підвищення відмовостійкості та безпеки мережі. Запропонована архітектура враховує потреби в комплексному захисті від виявлених загроз, забезпечуючи при цьому масштабованість та гнучкість системи.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. ОПИС ТА ТЕСТУВАННЯ МЕРЕЖІ

3.1 Опис обладнання та їх функції

В мережі першого офісу було налаштовано VLAN 115, до якого підключено шість комп'ютерів користувачів, яким через DHCP надходить мережа 192.168.115.0 255.255.255.0, хоч маска мережі не дуже надійна, але було створено виключно для спрощення налаштування, DHCP було налаштовано так щоб роздавати обмежену кількість адрес, за для підняття рівня безпеки.

У VLAN 115 було додано лише один ПК з віртуальною Windows 10, за для демонстрації працездатності роботи VoIP мережі, цього достатньо. У разі потреби є можливість додати ще ПК з віртуальною Windows 10.

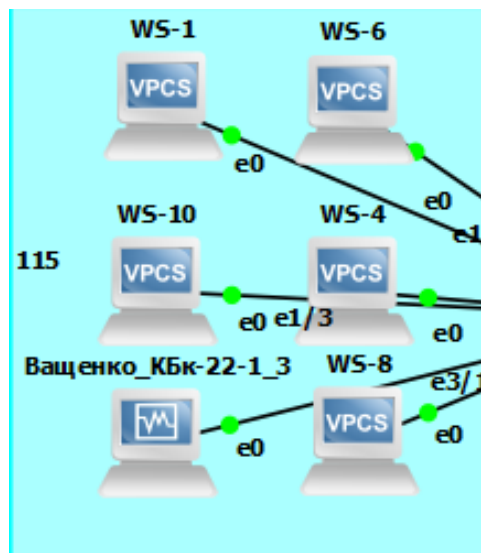


Рисунок 3.26 – Користувачі підмережі VLAN 115

На маршрутизаторі було налаштовано службу DHCP (Dynamic Host Configuration Protocol) спеціально для мережевого сегменту VLAN 115. Це означає, що пристрої, підключені до цього VLAN 115, автоматично отримуватимуть IP-адреси, маску підмережі, шлюз за замовчуванням та DNS-сервери від маршрутизатора. Завдяки такому налаштуванню, адміністратору не потрібно вручну призначати IP-адреси кожному пристрою у VLAN 115, що значно спрощує управління мережею та запобігає конфліктам IP-адрес. Усі пристрої, що входять до VLAN 115, будуть отримувати необхідні мережеві параметри динамічно при підключенні.

```

R-22-1-1

ip dhcp pool VLAN115
network 192.168.115.0 255.255.255.0
default-router 192.168.115.1
dns-server 8.8.8.8
lease 7

```

Рисунок 3.27 – Налаштування DHCP для VLAN 115

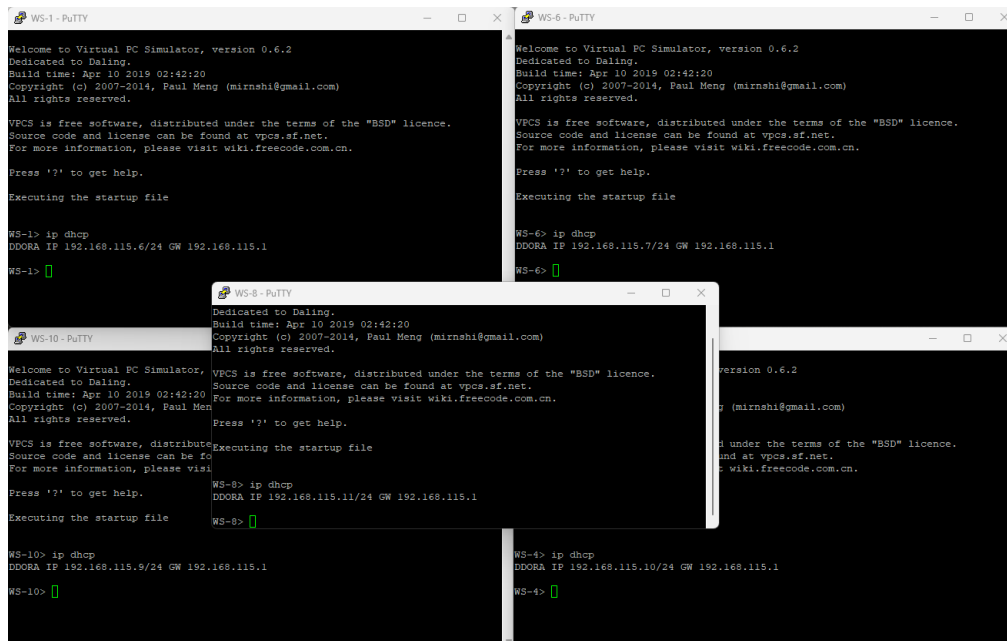


Рисунок 3.28 – Запит DHCP для користувачів VLAN 115

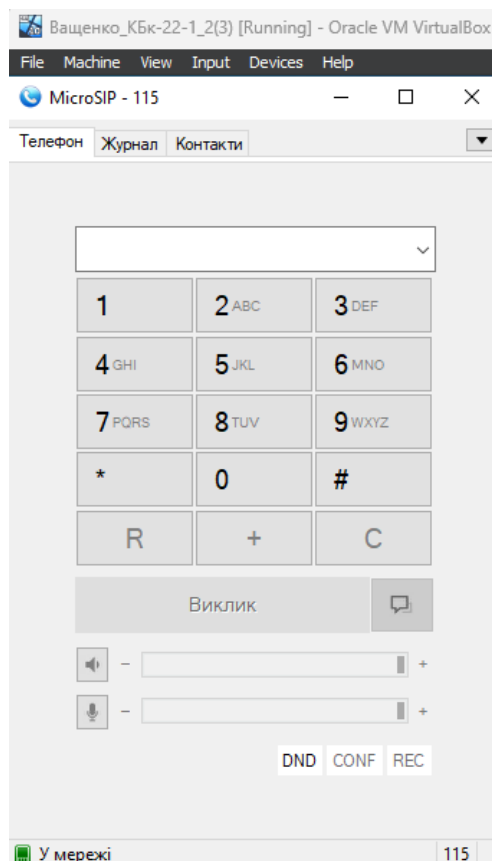


Рисунок 3.29 – Налаштована MicroSIP телефонія

У першому офісі був організований відокремлений мережевий сегмент – VLAN 116. Шість робочих комп'ютерів користувачів, підключених до цього VLAN, автоматично отримують IP-адреси з діапазону 192.168.116.0/24 через DHCP. Незважаючи на те, що обрана маска підмережі не забезпечує найвищого рівня безпеки, таке рішення було прийнято для спрощення конфігурації. Додатково, для підвищення загального рівня безпеки, DHCP-сервер був налаштований на видачу лише обмеженої кількості IP-адрес. До VLAN 116 також інтегровано один віртуальний комп'ютер з операційною системою Windows 10, який слугує достатньою демонстраційною платформою для перевірки функціональності VoIP-мережі. За потреби, цей сегмент може бути розширений шляхом додавання додаткових віртуальних машин з Windows 10.

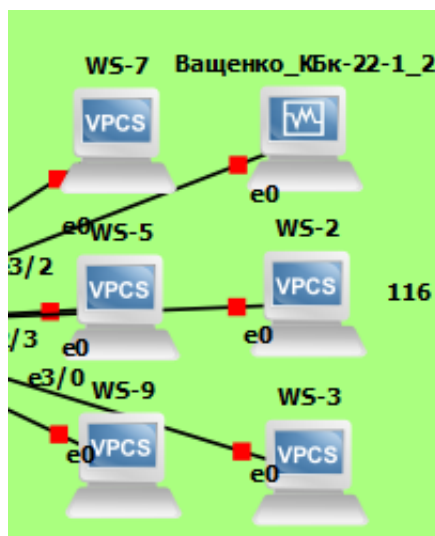


Рисунок 3.30 – Користувачі підмережі VLAN 116

На маршрутизаторі було сконфігуровано DHCP-сервіс, призначений виключно для VLAN 116. Це дозволяє пристроям у цьому сегменті автоматично отримувати від маршрутизатора всі необхідні мережеві параметри: IP-адресу, маску підмережі, шлюз за замовчуванням та адреси DNS-серверів. Завдяки цій автоматизації, ручне налаштування IP-адрес для кожного пристрою у VLAN 116 стає непотрібним, що істотно спрощує адміністрування мережі та запобігає виникненню конфліктів адрес. Усі пристрої, підключені до VLAN 116, будуть динамічно отримувати свої мережеві налаштування одразу після з'єднання.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

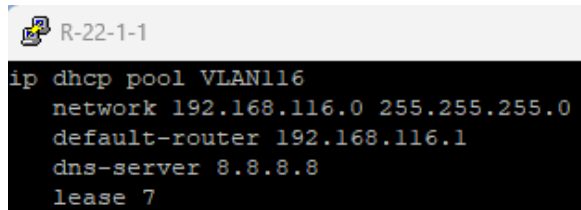


Рисунок 3.31 – Налаштування DHCP для VLAN 116

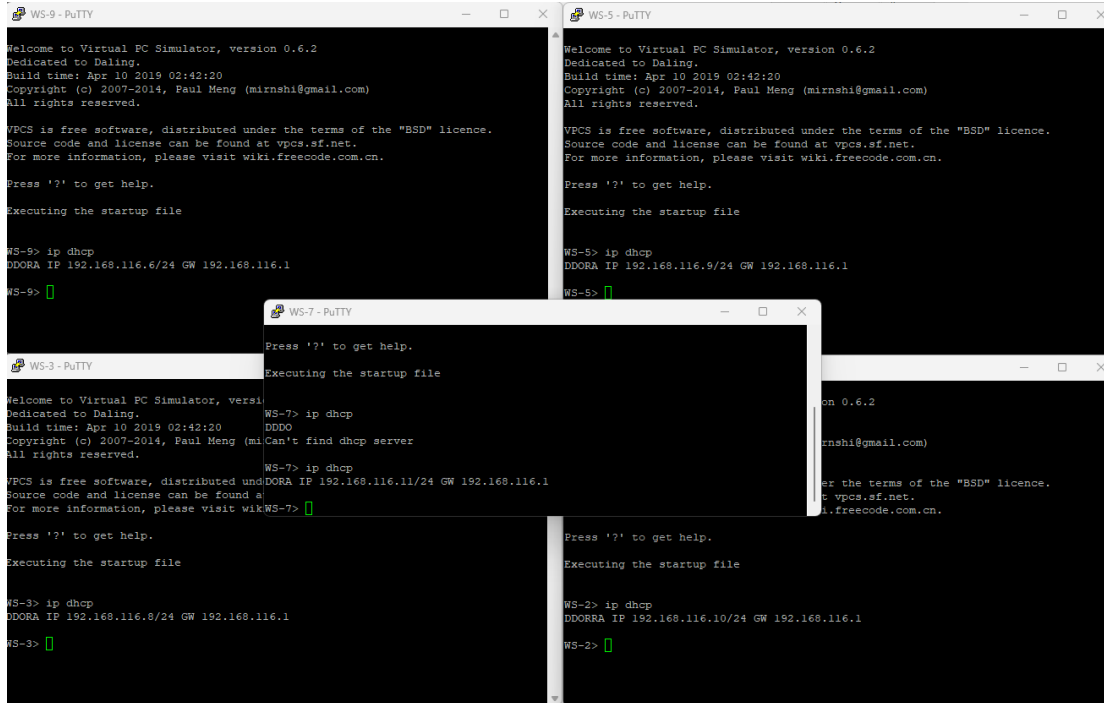


Рисунок 3.32 – Запит DHCP для користувачів VLAN 116

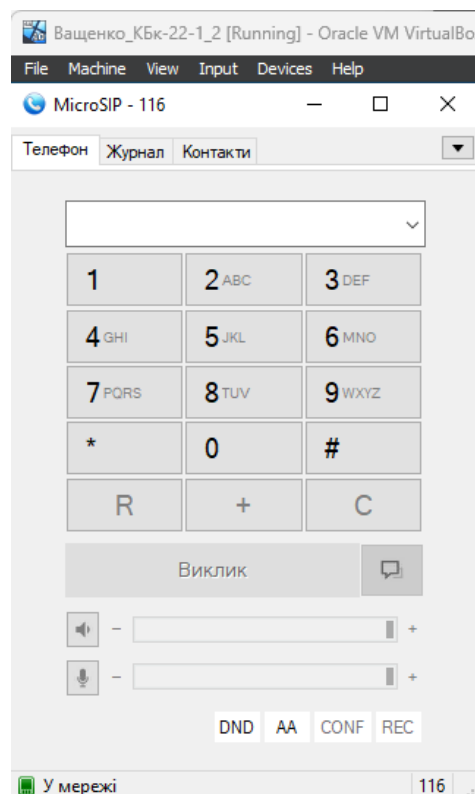


Рисунок 3.33 – Налаштована MicroSIP телефонія

Для другого офісу була організована відокремлена мережева ділянка – VLAN 117. До неї підключено три робочих комп'ютерів, що автоматично отримують свої IP-адреси з діапазону 192.168.117.0/24 через DHCP. Хоча обрана маска підмережі не є оптимальною з точки зору безпеки, таке рішення було прийняте для спрощення конфігурації.

Додатково, для підвищення загальної безпеки, DHCP-сервер був налаштований на видачу лише лімітованої кількості IP-адрес. У VLAN 117 також інтегрований один віртуальний комп'ютер під керуванням Windows 10, який виконує роль демонстраційної платформи для перевірки функціональності VoIP-зв'язку. При необхідності передбачена можливість розширення цього сегменту шляхом додавання додаткових віртуальних машин з Windows 10.

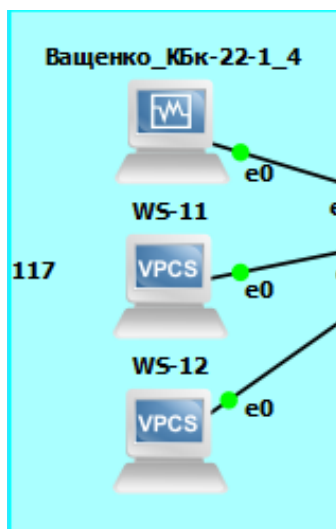


Рисунок 3.34 – Користувачі підмережі VLAN 117

```
R-22-1-1
ip dhcp pool VLAN117
network 192.168.117.0 255.255.255.0
default-router 192.168.117.1
dns-server 8.8.8.8
lease 7
```

Рисунок 3.35 – Налаштування DHCP для VLAN 117

На маршрутизаторі було активовано службу DHCP, спеціально адаптовану для мережевого сегменту VLAN 117. Це гарантує, що всі під'єднані до VLAN 117 пристрої автоматично отримуватимуть від маршрутизатора свої IP-адреси, маски підмережі, інформацію про шлюз за

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

замовчуванням та адреси DNS-серверів [22]. Таке рішення істотно спрощує мережеве адміністрування, усуваючи потребу в ручному призначенні IP-адрес для кожного пристрою у VLAN 117, а також ефективно запобігає конфліктам IP-адрес. Отже, кожен пристрій у VLAN 117 буде динамічно отримувати всі необхідні мережеві налаштування одразу після підключення.

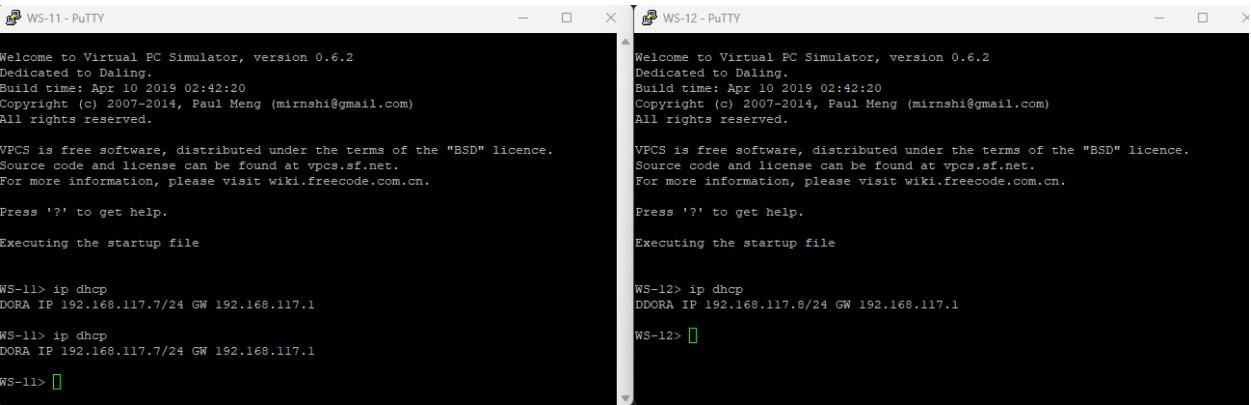


Рисунок 3.36 – Запит DHCP для користувачів VLAN 117

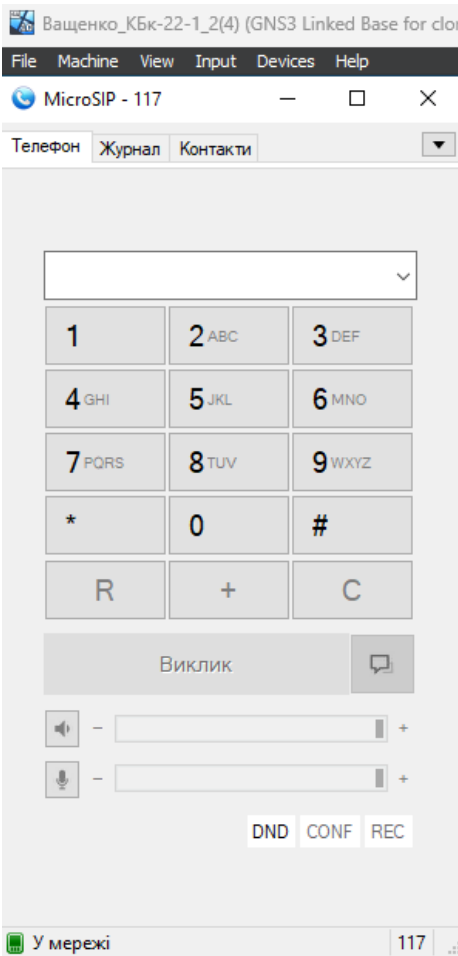


Рисунок 3.37 – Налаштована MicroSIP телефонія

У межах другого офісу було створено ізольований мережевий сегмент – VLAN 118. Три підключених до нього робочих комп'ютери автоматично отримують IP-адреси з мережі 192.168.118.0/24 через службу DHCP. Вибір такої маски підмережі, хоч і не ідеальний з позицій безпеки, був зроблений задля спрощення налаштування системи. З метою підвищення безпеки, DHCP-сервер у цьому VLAN був сконфігурований для роздачі обмеженої кількості IP-адрес.

Крім того, до VLAN 118 включено один віртуальний комп'ютер з Windows 10, який слугує демонстраційною платформою для перевірки функціонування VoIP-мережі. У разі потреби існує можливість додавання додаткових віртуальних машин з Windows 10 до цього сегменту.

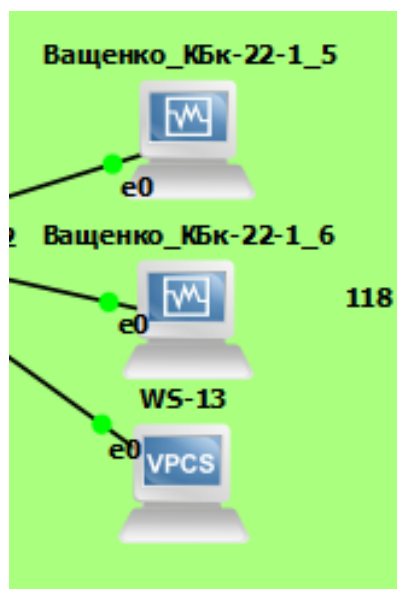


Рисунок 3.38 – Користувачі підмережі VLAN 118

На маршрутизаторі було розгорнуто DHCP-сервіс, призначений для управління мережевим сегментом VLAN 118. Завдяки цьому, пристрої, що підключаються до VLAN 118, автоматично отримують від маршрутизатора необхідні IP-адреси, маски підмережі, дані про шлюз за замовчуванням та адреси DNS-серверів. Ця автоматизація значно оптимізує адміністрування мережі, оскільки усуває потребу в ручному налаштуванні IP-адрес для кожного пристрою у VLAN 118 і мінімізує ризики виникнення конфліктів IP-адрес [22]. Отже, кожен пристрій у VLAN 118 динамічно отримує повний комплект мережевих параметрів одразу після встановлення з'єднання.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-22-1-1
ip dhcp pool VLAN118
network 192.168.118.0 255.255.255.0
default-router 192.168.118.1
dns-server 8.8.8.8
lease 7

```

Рисунок 3.39 – Налаштування DHCP для VLAN 118

```

WS-13 - PuTTY
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

WS-13> ip dhcp
DDORA IP 192.168.118.8/24 GW 192.168.118.1
WS-13>

```

Рисунок 3.40 – Запит DHCP для користувачів VLAN 118

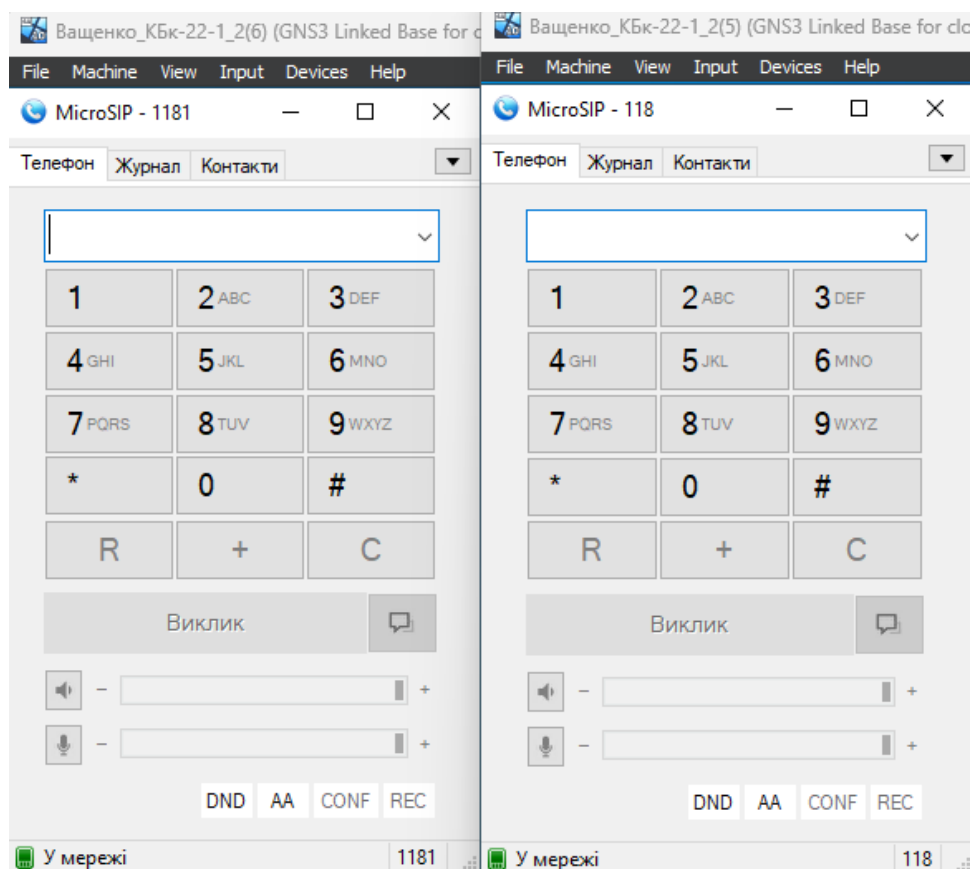


Рисунок 3.41– Налаштована MicroSIP телефонія

Основою усієї мережі є два маршрутизатора, які налаштовані з HSRP, основна ідея полягає у створенні віртуального маршрутизатора, який може бути доступним навіть у разі збою одного з фізичних маршрутизаторів. Таким чином це збільшує відмовостійкість усієї мережі [18].

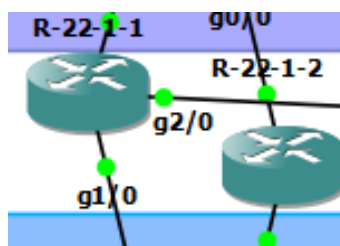


Рисунок 3.42 – Вигляд HSRP в GNS

Уся мережа працює на VLANs, що дуже допомагає розгалужувати усю мережу [16]. Через що ці маршрутизатори налаштовані на надання DHCP усієї мережі, що кратно полегшує налаштування ПК для користувачів.

```

R-22-1-1
ip cef
ip dhcp excluded-address 192.168.115.1 192.168.115.5
ip dhcp excluded-address 192.168.116.1 192.168.116.5
ip dhcp excluded-address 192.168.117.1 192.168.117.5
ip dhcp excluded-address 192.168.118.1 192.168.118.5
ip dhcp excluded-address 192.168.121.1 192.168.121.6
ip dhcp pool VLAN115
network 192.168.115.0 255.255.255.0
default-router 192.168.115.1
dns-server 8.8.8.8
lease 7
ip dhcp pool VLAN116
network 192.168.116.0 255.255.255.0
default-router 192.168.116.1
dns-server 8.8.8.8
lease 7
ip dhcp pool VLAN117
network 192.168.117.0 255.255.255.0
default-router 192.168.117.1
dns-server 8.8.8.8
lease 7
ip dhcp pool VLAN118
network 192.168.118.0 255.255.255.0
default-router 192.168.118.1
dns-server 8.8.8.8
lease 7
ip dhcp pool VLAN121
network 192.168.121.0 255.255.255.0
default-router 192.168.121.1
dns-server 8.8.8.8
ip dhcp pool VLAN130
network 192.168.130.0 255.255.255.248
default-router 192.168.130.1
dns-server 8.8.8.8
lease 7
no ip domain lookup
ip domain name freebpx.sangoma.local
no ipv6 cef
multilink bundle-name authenticated

R-22-1-2
ip cef
ip dhcp excluded-address 192.168.115.1 192.168.115.5
ip dhcp excluded-address 192.168.116.1 192.168.116.5
ip dhcp excluded-address 192.168.117.1 192.168.117.5
ip dhcp excluded-address 192.168.118.1 192.168.118.5
ip dhcp excluded-address 192.168.121.1 192.168.121.6
ip dhcp pool VLAN115
network 192.168.115.0 255.255.255.0
default-router 192.168.115.1
dns-server 8.8.8.8
lease 7
ip dhcp pool VLAN116
network 192.168.116.0 255.255.255.0
default-router 192.168.116.1
dns-server 8.8.8.8
lease 7
ip dhcp pool VLAN117
network 192.168.117.0 255.255.255.0
default-router 192.168.117.1
dns-server 8.8.8.8
lease 7
ip dhcp pool VLAN118
network 192.168.118.0 255.255.255.0
default-router 192.168.118.1
dns-server 8.8.8.8
lease 7
ip dhcp pool VLAN121
network 192.168.121.0 255.255.255.0
default-router 192.168.121.1
dns-server 8.8.8.8
ip dhcp pool VLAN130
network 192.168.130.0 255.255.255.248
default-router 192.168.130.1
dns-server 8.8.8.8
lease 7
no ip domain lookup
ip domain name freebpx.sangoma.local
no ipv6 cef
multilink bundle-name authenticated

```

Рисунок 3.43 – Налаштування DHCP для VLANs

За правильну комунікацію в мережі відповідають ACL, які слугують бар'єром для підгруп користувачів. Окрім ACL налаштовано безпекові правила які огорожують доступ до маршрутизаторів, та надають доступ тільки для головного адміну чи обслуговуючого персоналу. А за для прискорення процесів налаштування було також налаштовано SSH, яка значно спрощує налаштування на дистанції.

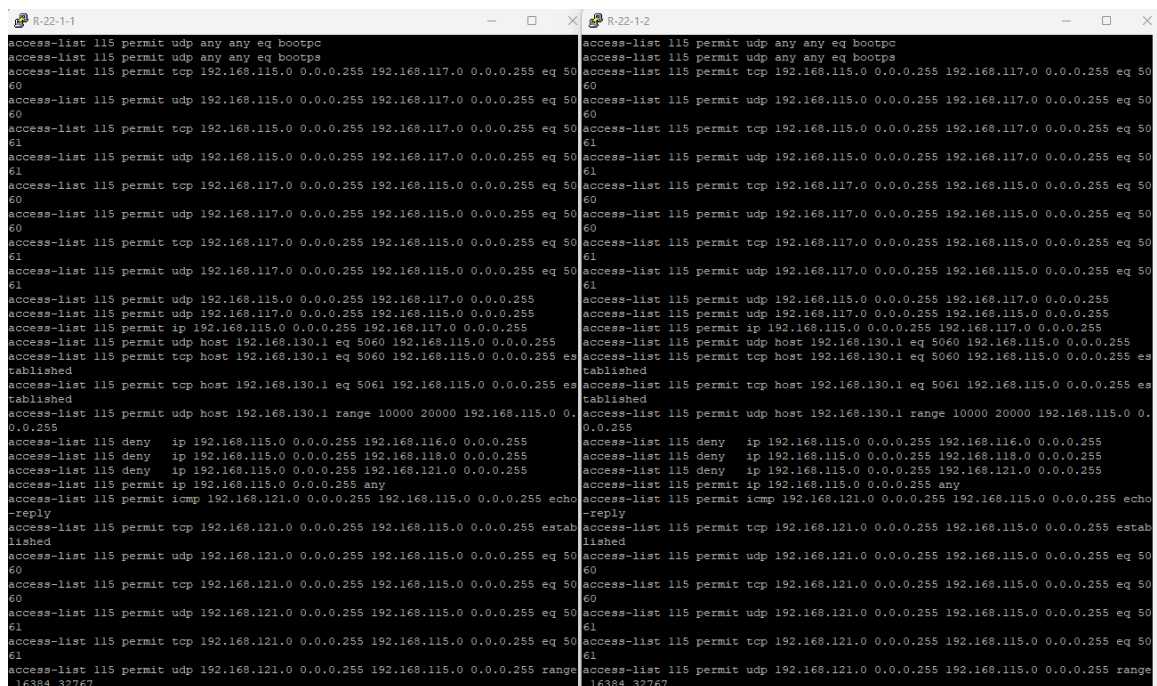


Рисунок 3.44 – Налаштування ACL на маршрутизаторах

Саме налаштування HSRP починається з налаштування віртуальних портів, де одразу виставляється пріоритетність [18]. Там же і проводиться налаштування для маршрутизації мережі.

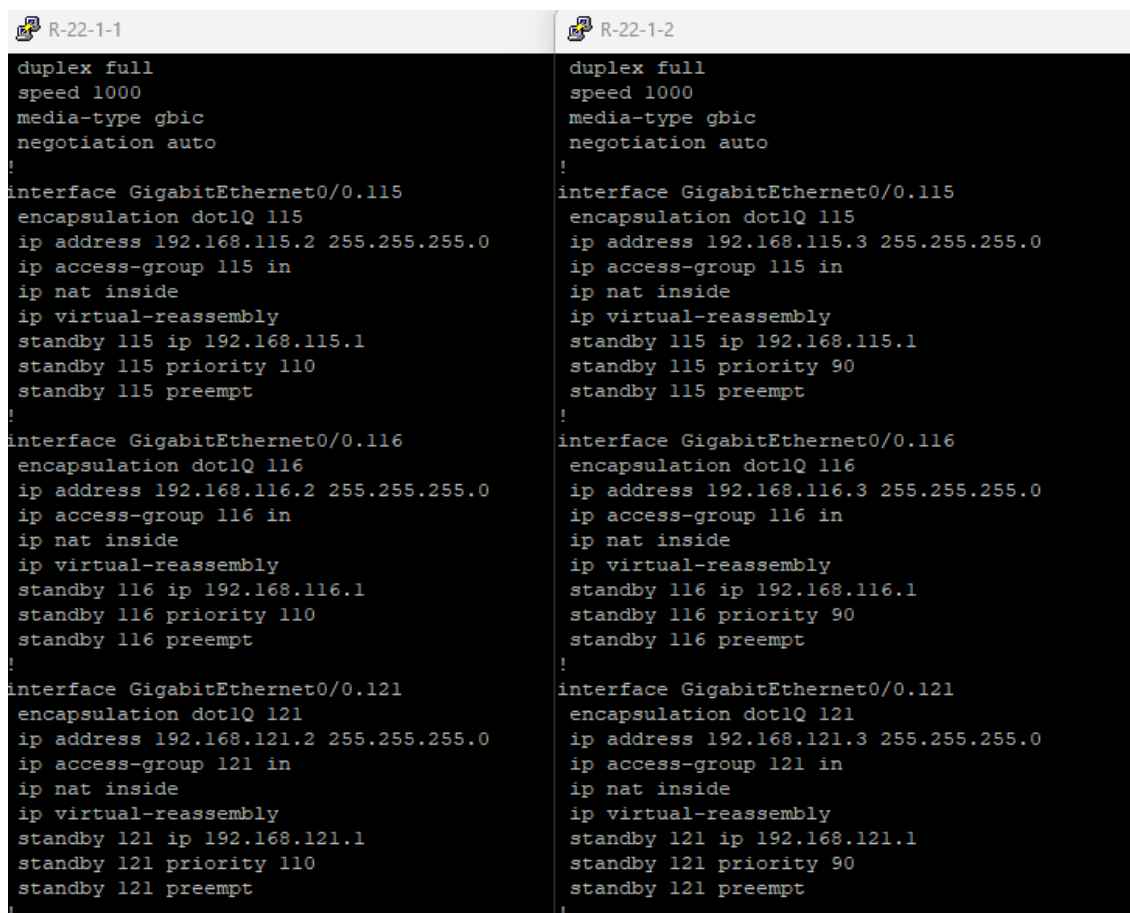


Рисунок 3.45 – Налаштування віртуальних портів для HSRP

```

privilege exec level 5 show vlans
privilege exec level 5 show vlan-range
privilege exec level 5 show ip interface brief
privilege exec level 5 show ip interface
privilege exec level 5 show ip
privilege exec level 5 show version
privilege exec level 5 show running-config
privilege exec level 5 show
!
line con 0
exec-timeout 0 0
privilege level 15
password 7 03055F060F01731D
logging synchronous
login
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login local
transport input ssh
!

privilege exec level 5 show vlans
privilege exec level 5 show vlan-range
privilege exec level 5 show ip interface brief
privilege exec level 5 show ip interface
privilege exec level 5 show ip
privilege exec level 5 show version
privilege exec level 5 show running-config
privilege exec level 5 show
!
line con 0
exec-timeout 0 0
privilege level 15
password 7 104F0D140C19405A
logging synchronous
login
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login local
transport input ssh
!

```

Рисунок 3.46 – Налаштування безпеки та SSH для маршрутизаторів

Налаштування мережі інтернет здійснено за рахунок NAT2-хмаринки, на якій обрано мережевий адаптер, з транзитом через комутатор SW-22-1-3 [17].

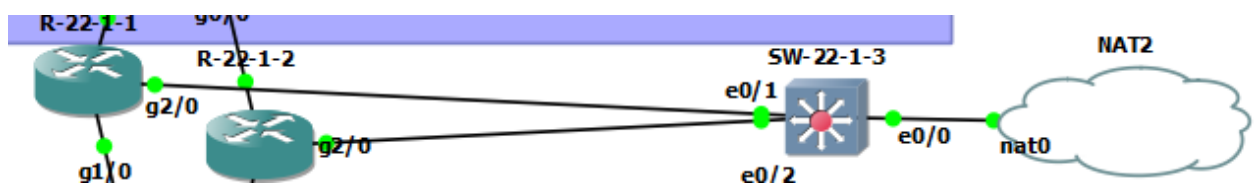


Рисунок 3.47 – Шлях інтернет з'єднання

Транзит інтернет з'єднання налаштовується на маршрутизаторах командою `ip route 0.0.0.0 0.0.0.0 dhcp`.

Ця команда, означає, що маршрутизатор автоматично отримає інформацію про маршрут за замовчуванням від DHCP-сервера (у цьому випадку за інтернет-провайдером). За з'єднання усіх користувачів в двох офісах відповідає два комутатора, які відповідають за транзит DHCP та VoIP.

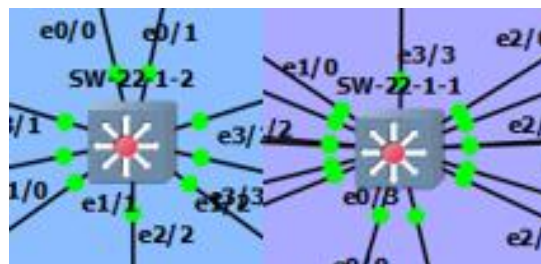


Рисунок 3.48 – Головні маршрутні комутатори

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

Основні порти були налаштовані для проходу усього трафіку всіх VLAN-ів

```

SW-22-1-1 - PuTTY
!
interface Ethernet0/0
 switchport trunk allowed vlan 115-118,121,130
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface Ethernet0/1
 switchport trunk allowed vlan 115-118,121,130
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!

SW-22-1-2 - PuTTY
!
interface Ethernet0/0
 switchport trunk allowed vlan 115-118,121,130
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface Ethernet0/1
 switchport trunk allowed vlan 115-118,121,130
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
  
```

Рисунок 3.49 – Налаштування маршрутизації на комутаторах

Налаштування безпеки DHCP Snooping для DHCP (2-го каналного рівня захист) від несанкціонованих DHCP-серверів та деяких типів DoS-атак. Вона працює, перевіряючи DHCP-трафік.

```

SW-22-1-1 - PuTTY
!
ip dhcp snooping vlan 115-118,121,130
no ip dhcp snooping information option
ip dhcp snooping
no ip domain-lookup
ip domain-name freepbx.sangoma.local
no ip cef
no ipv6 cef

SW-22-1-2 - PuTTY
!
ip dhcp snooping vlan 115-118,121,130
no ip dhcp snooping information option
ip dhcp snooping
no ip domain-lookup
ip domain-name freepbx.sangoma.local
no ip cef
no ipv6 cef
!
  
```

Рисунок 3.50 – Налаштування безпеки DHCP Snooping

Також було налаштовано підв'язку порту до MAC-адресу, що значно підвищило захищеність мережі від несанкціонованого підключення.

```

SW-22-1-1 - PuTTY
interface Ethernet0/2
!
interface Ethernet0/3
 switchport access vlan 115
 switchport mode access
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.7966.6807
 switchport port-security mac-address sticky 0050.7966.680c
 switchport port-security aging time 1
 switchport port-security
 ip dhcp snooping limit rate 50

SW-22-1-2 - PuTTY
interface Ethernet1/0
 switchport access vlan 117
 switchport mode access
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.7966.6809
 switchport port-security aging time 1
 switchport port-security
 ip dhcp snooping limit rate 50
!
interface Ethernet1/1
 switchport access vlan 117
 switchport mode access
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.7966.680a
 switchport port-security aging time 1
 switchport port-security
 ip dhcp snooping limit rate 50

```

Рисунок 3.51 – Налаштування портів з підв'язкою MAC-адресу

Одна з головних елементів VoIP мережі є сервер FreePBX, який працює на оболонці Asterisk. Його головна задача полягає у керуванні та забезпеченні функціонування IP-телефонії та PBX-сервісів. По суті, FreePBX перетворює звичайний комп'ютер (або віртуальну машину) на повноцінну офісну телефонну станцію.

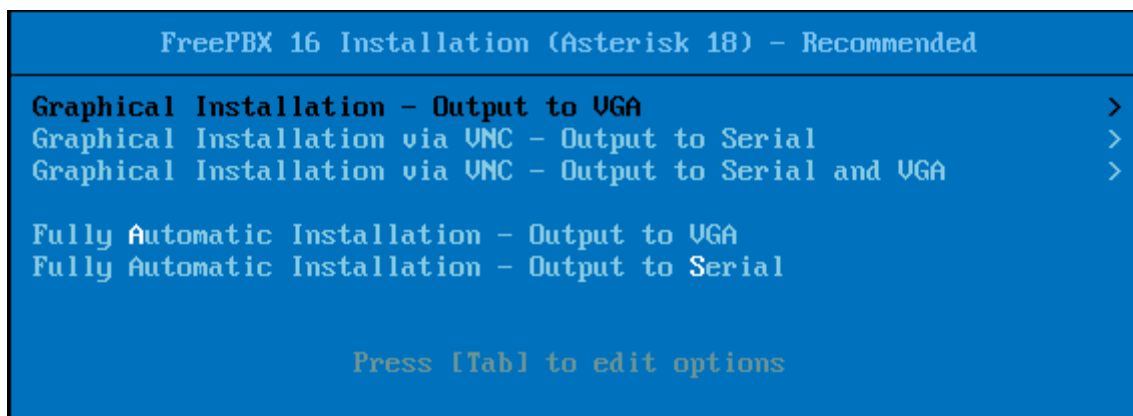


Рисунок 3.52 – Вибір конфігурації FreePBX

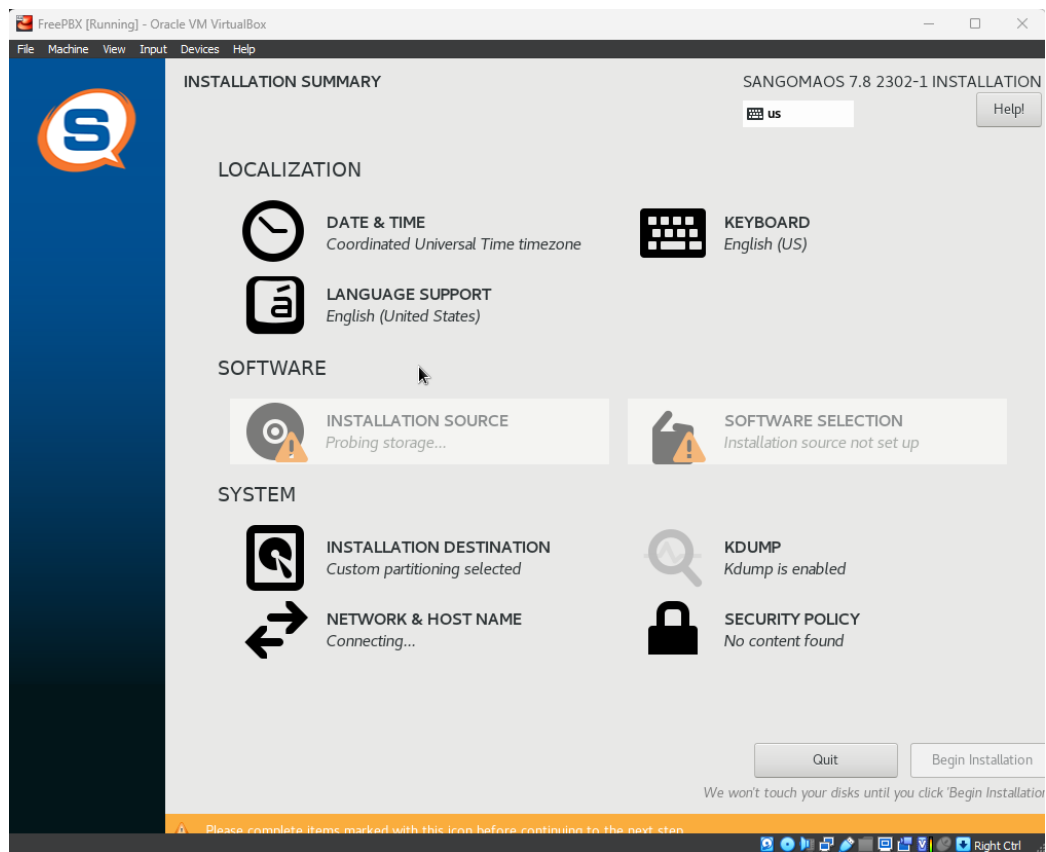


Рисунок 3.53 – Первинне налаштування FreePBX

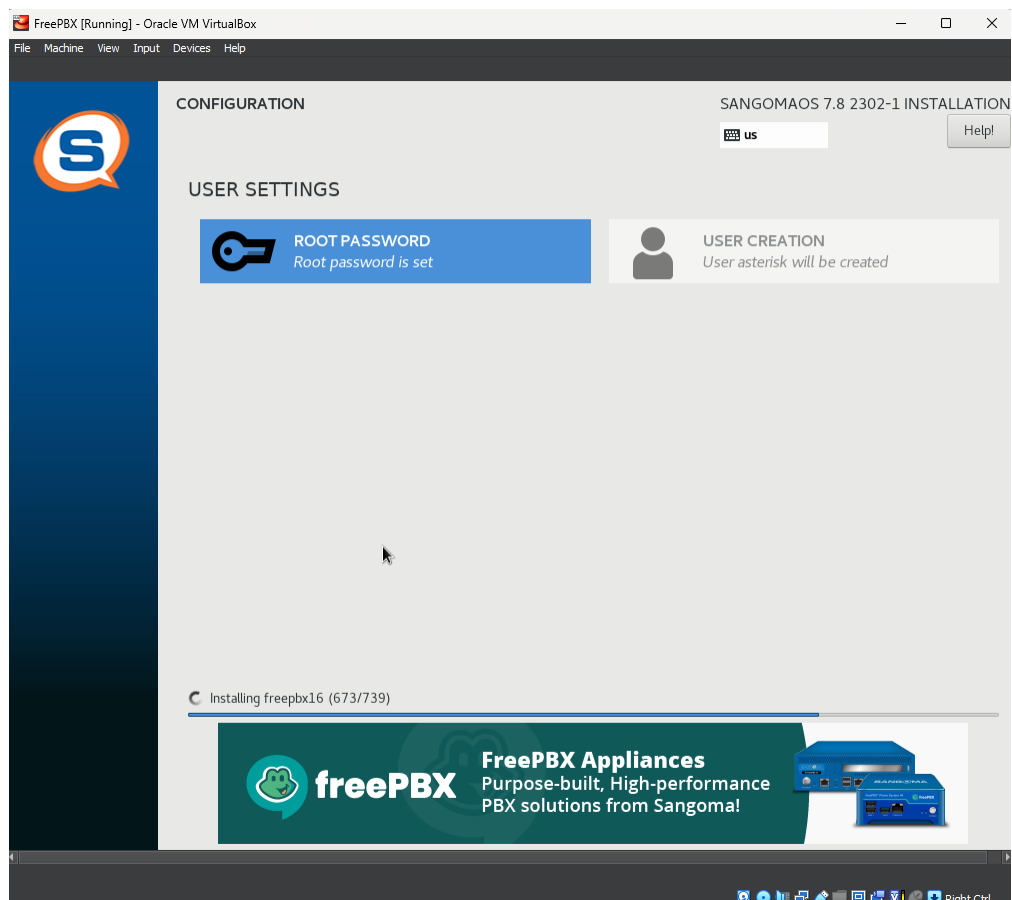


Рисунок 3.54 – Налаштування паролю до серверу FreePBX

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

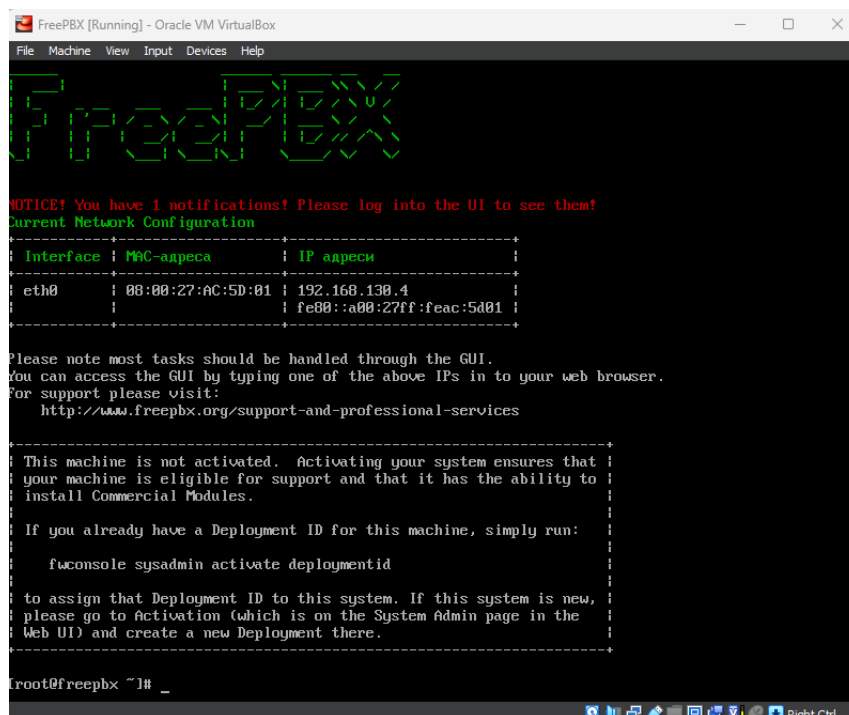


Рисунок 3.55 – Головна консоль серверу FreePBX

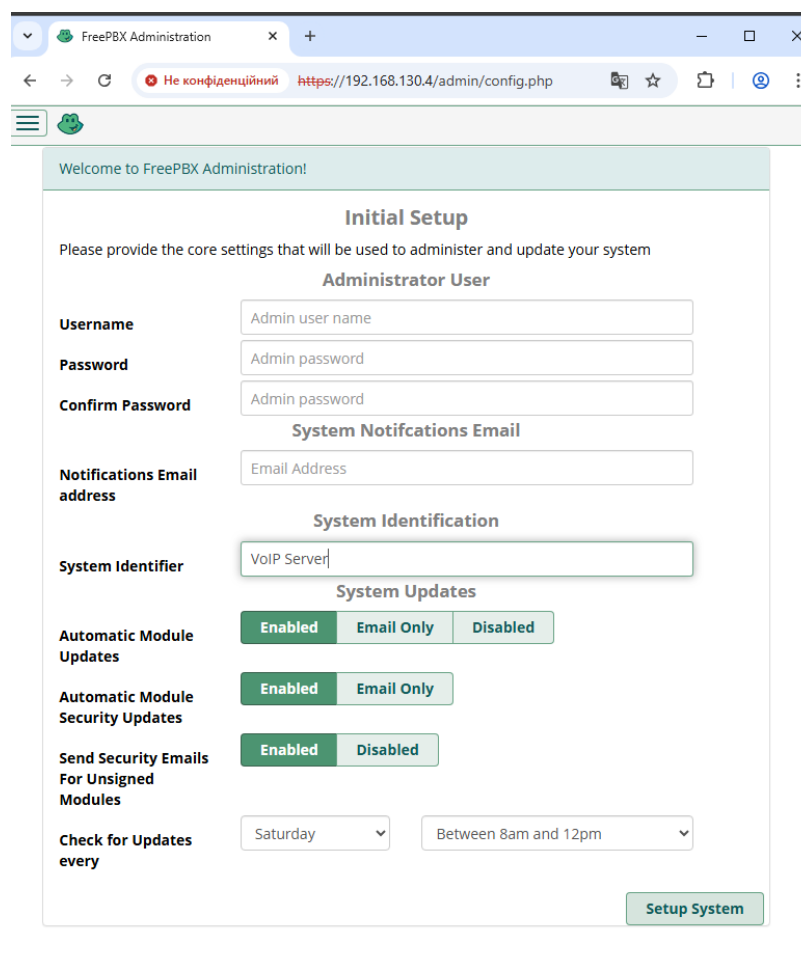


Рисунок 3.56 – Веб-інтерфейс початкових налаштувань FreePBX

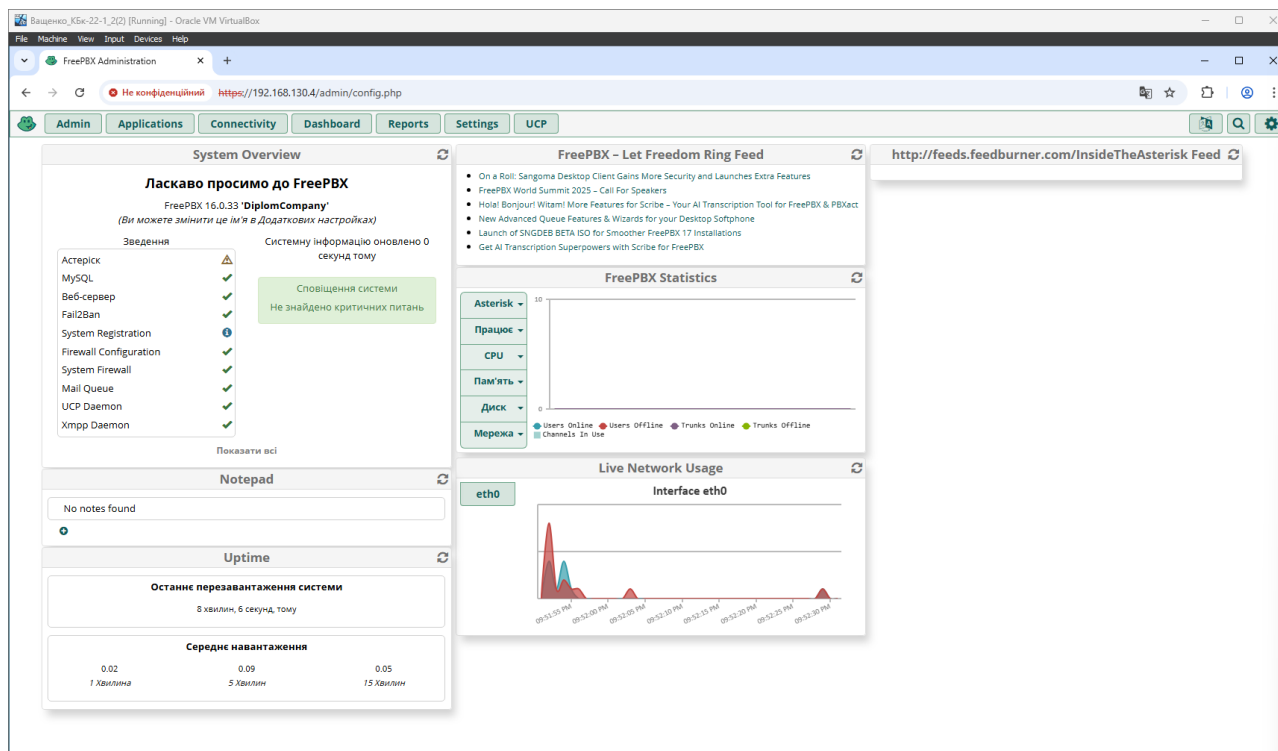


Рисунок 3.57 – Головна сторінка веб-інтерфейсу FreePBX

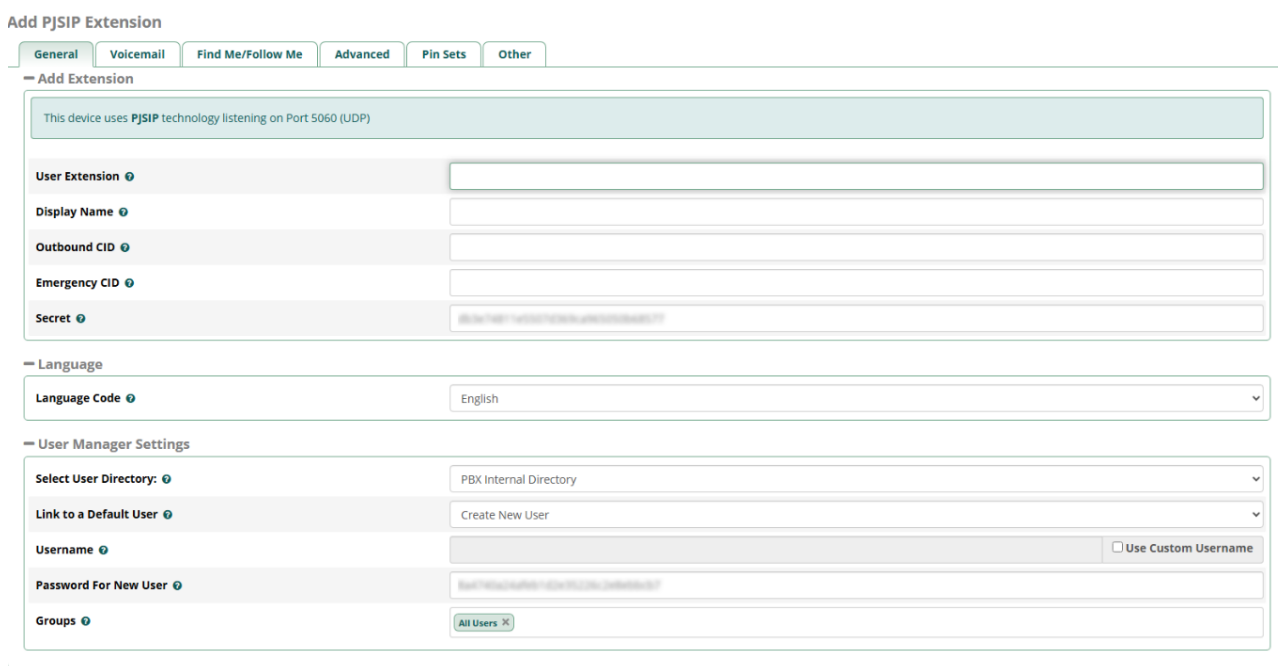


Рисунок 3.58 – Приклад додавання нового номеру в FreePBX

FreePBX відрізняється глибоким рівнем налаштувань, що дозволяє адаптувати систему під будь-які вимоги корпоративної VoIP-інфраструктури.

Приклад усіх параметрів налаштувань продемонстровано на рисунку 3.59 та 3.60.

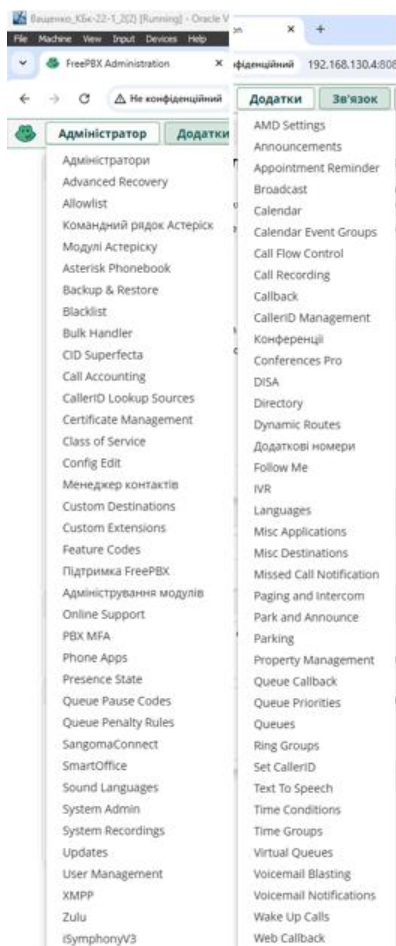


Рисунок 3.59 – Огляд усіх опцій в FreePBX

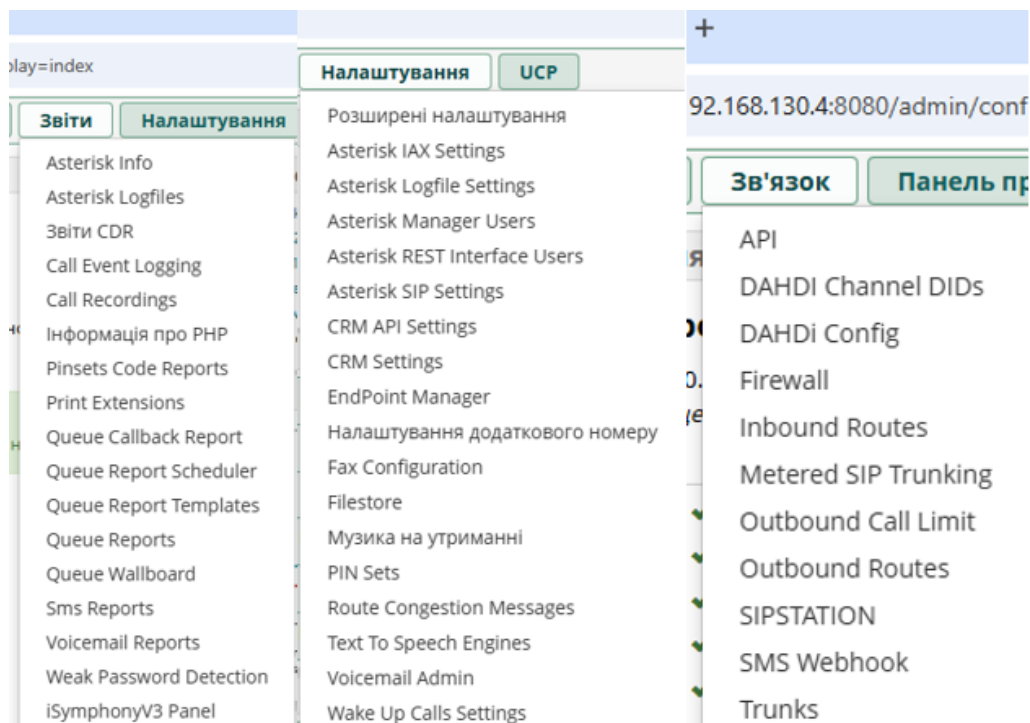
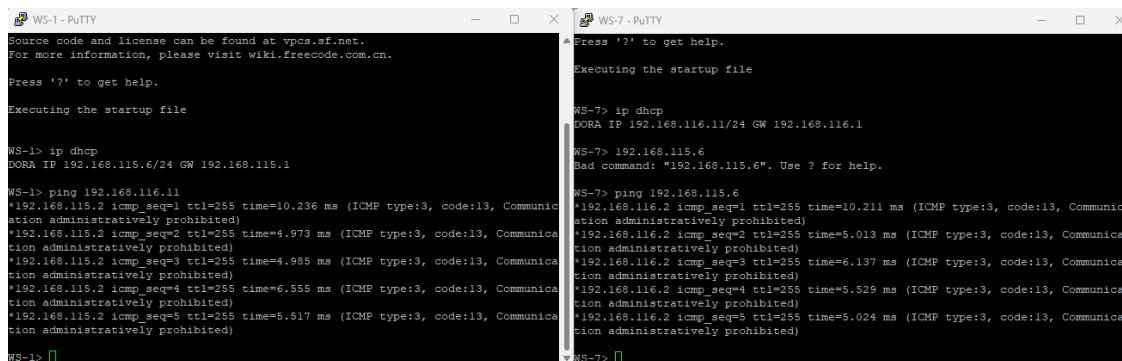


Рисунок 3.60 – Огляд усіх опцій в FreePBX

3.2 Сценарій тестування

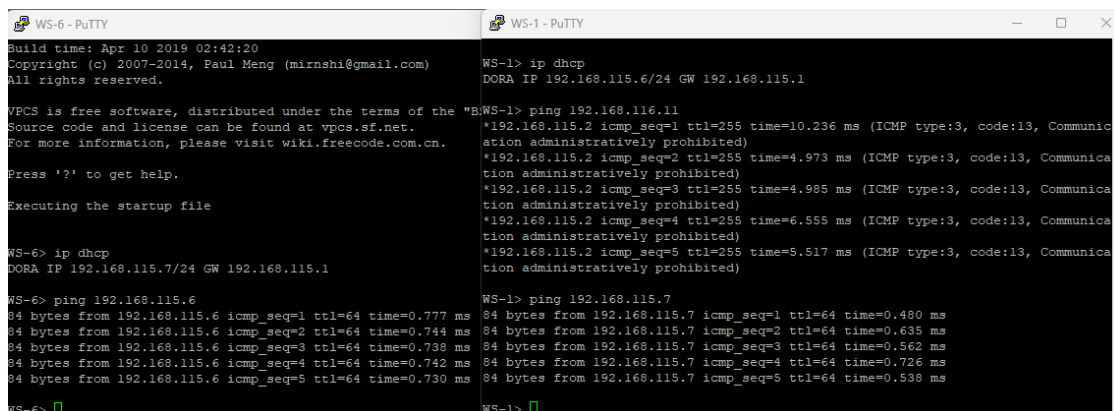
Було виконано ping 115 та 116, на що через заборони ACL не дають мережі виконувати ping, це було налаштовано з цілю розподілу офісу на підрозділи, які працюють за типом 115 та 117 однієї підмережі а 116 та 117 іншої підмережі [17].



The image shows two PuTTY terminal windows. The left window (WS-1) shows the configuration of interface 192.168.115.6/24 with gateway 192.168.115.1. The right window (WS-7) shows the configuration of interface 192.168.116.6/24 with gateway 192.168.116.1. Both windows show the execution of the startup file and the results of a ping command from 192.168.115.6 to 192.168.116.11. The ping results show that the connection is blocked by an ACL, with the message 'ICMP type:3, code:13, Communication administratively prohibited'.

Рисунок 3.61 – Виконано ping між 115 та 116

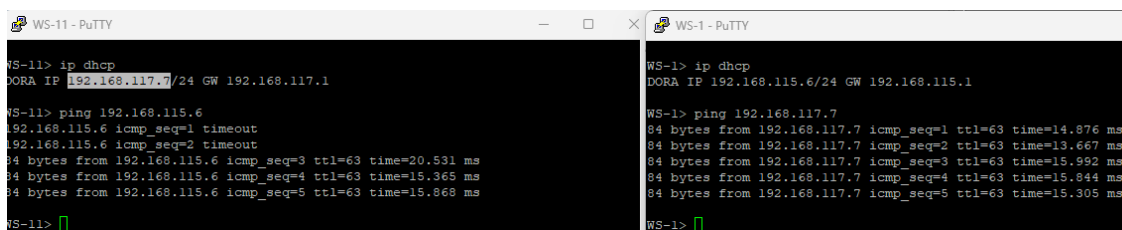
Використано команду ping для учасників однієї VLAN мережі а саме 115 [17].



The image shows two PuTTY terminal windows. The left window (WS-6) shows the configuration of interface 192.168.115.6/24 with gateway 192.168.115.1. The right window (WS-1) shows the configuration of interface 192.168.115.7/24 with gateway 192.168.115.1. Both windows show the execution of the startup file and the results of a ping command from 192.168.115.6 to 192.168.115.7. The ping results show that the connection is successful, with the message '84 bytes from 192.168.115.7 icmp_seq=1 ttl=64 time=0.777 ms'.

Рисунок 3.62 – Виконано ping між учасниками VLAN 115

Між 117 та 115 відбувається ping і усе працює так як повинно [17].



The image shows two PuTTY terminal windows. The left window (WS-11) shows the configuration of interface 192.168.117.7/24 with gateway 192.168.117.1. The right window (WS-1) shows the configuration of interface 192.168.115.6/24 with gateway 192.168.115.1. Both windows show the execution of the startup file and the results of a ping command from 192.168.117.7 to 192.168.115.6. The ping results show that the connection is successful, with the message '84 bytes from 192.168.115.6 icmp_seq=1 time=14.876 ms'.

Рисунок 3.63 – Виконано ping між 115 та 117

Ping 117 та 118 блокується ACL, так як ці мережі не сумісні один з одним так як належать не до одної підмережі.

```

WS-12> ip dhcp
DORA IP 192.168.117.8/24 GW 192.168.117.1

WS-12> ping 192.168.118.8
Bad command: "192.168.118.8". Use ? for help.

WS-12> ping 192.168.118.8
*192.168.117.2 icmp_seq=1 ttl=255 time=10.132 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.117.2 icmp_seq=2 ttl=255 time=5.580 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.117.2 icmp_seq=3 ttl=255 time=7.926 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.117.2 icmp_seq=4 ttl=255 time=5.514 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.117.2 icmp_seq=5 ttl=255 time=5.563 ms (ICMP type:3, code:13, Communication administratively prohibited)

WS-13>
WS-13> ip dhcp
DORA IP 192.168.118.8/24 GW 192.168.118.1

WS-13> ping 192.168.117.8
*192.168.118.2 icmp_seq=1 ttl=255 time=9.803 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.118.2 icmp_seq=2 ttl=255 time=9.230 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.118.2 icmp_seq=3 ttl=255 time=6.572 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.118.2 icmp_seq=4 ttl=255 time=6.601 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.118.2 icmp_seq=5 ttl=255 time=6.696 ms (ICMP type:3, code:13, Communication administratively prohibited)

WS-13>

```

Рисунок 3.64 – Виконано ping між 117 та 118

Використано команду ping для учасників однієї VLAN мережі а саме 116 [17].

```

WS-5> ip dhcp
DORA IP 192.168.116.8/24 GW 192.168.116.1

WS-5> ping 192.168.116.6
84 bytes from 192.168.116.6 icmp_seq=1 ttl=64 time=0.468 ms
84 bytes from 192.168.116.6 icmp_seq=2 ttl=64 time=0.620 ms
84 bytes from 192.168.116.6 icmp_seq=3 ttl=64 time=0.693 ms
84 bytes from 192.168.116.6 icmp_seq=4 ttl=64 time=0.544 ms
84 bytes from 192.168.116.6 icmp_seq=5 ttl=64 time=0.799 ms

WS-5>
WS-7> ip dhcp
DORA IP 192.168.116.8/24 GW 192.168.116.1

WS-7> ping 192.168.116.6
84 bytes from 192.168.116.6 icmp_seq=1 ttl=64 time=0.714 ms
84 bytes from 192.168.116.6 icmp_seq=2 ttl=64 time=0.828 ms
84 bytes from 192.168.116.6 icmp_seq=3 ttl=64 time=0.749 ms
84 bytes from 192.168.116.6 icmp_seq=4 ttl=64 time=0.719 ms
84 bytes from 192.168.116.6 icmp_seq=5 ttl=64 time=0.758 ms

WS-7>

```

Рисунок 3.65 – Виконано ping між учасниками VLAN 116

Використано команду ping для учасників однієї VLAN мережі а саме 117 [17].

```

WS-11> ip dhcp
DORA IP 192.168.117.7/24 GW 192.168.117.1

WS-11> ping 192.168.117.6
84 bytes from 192.168.117.6 icmp_seq=1 ttl=64 time=0.705 ms
84 bytes from 192.168.117.6 icmp_seq=2 ttl=64 time=0.757 ms
84 bytes from 192.168.117.6 icmp_seq=3 ttl=64 time=0.775 ms
84 bytes from 192.168.117.6 icmp_seq=4 ttl=64 time=0.799 ms
84 bytes from 192.168.117.6 icmp_seq=5 ttl=64 time=0.613 ms

WS-11>
WS-12> ip dhcp
DORA IP 192.168.117.6/24 GW 192.168.117.1

WS-12> ping 192.168.117.7
84 bytes from 192.168.117.7 icmp_seq=1 ttl=64 time=0.428 ms
84 bytes from 192.168.117.7 icmp_seq=2 ttl=64 time=0.750 ms
84 bytes from 192.168.117.7 icmp_seq=3 ttl=64 time=0.755 ms
84 bytes from 192.168.117.7 icmp_seq=4 ttl=64 time=0.748 ms
84 bytes from 192.168.117.7 icmp_seq=5 ttl=64 time=0.691 ms

WS-12>

```

Рисунок 3.66 – Виконано ping між учасниками VLAN 117

Використано команду ping для учасників однієї VLAN мережі а саме 118 [17].

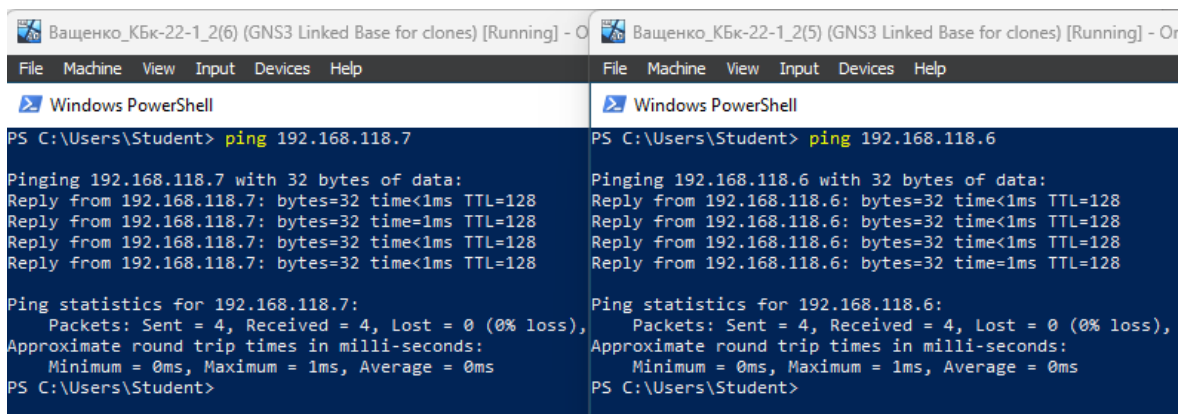


Рисунок 3.67 – Виконано ping між учасниками VLAN 118

Так як мережа VoIP налаштована, було зроблено тестування функціонування VoIP мережі [14]. Використовувався MicroSIP – це легкий, безкоштовний і портативний SIP-клієнт для операційної системи Windows. Його основне призначення – дозволити користувачам здійснювати та приймати голосові та відеодзвінки через Інтернет або локальну мережу, використовуючи відкритий протокол SIP (Session Initiation Protocol) [22].

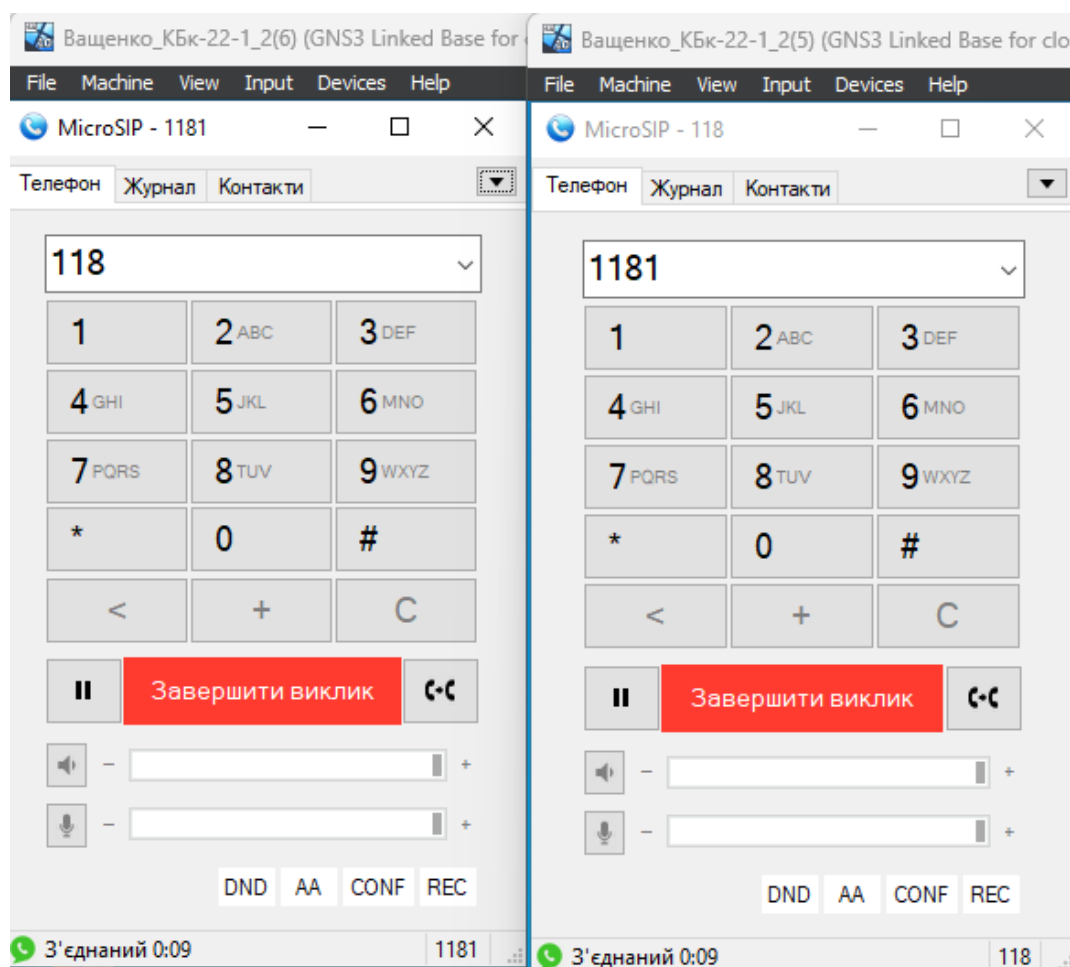


Рисунок 3.68 – Виконано дзвінок між учасниками VLAN 118

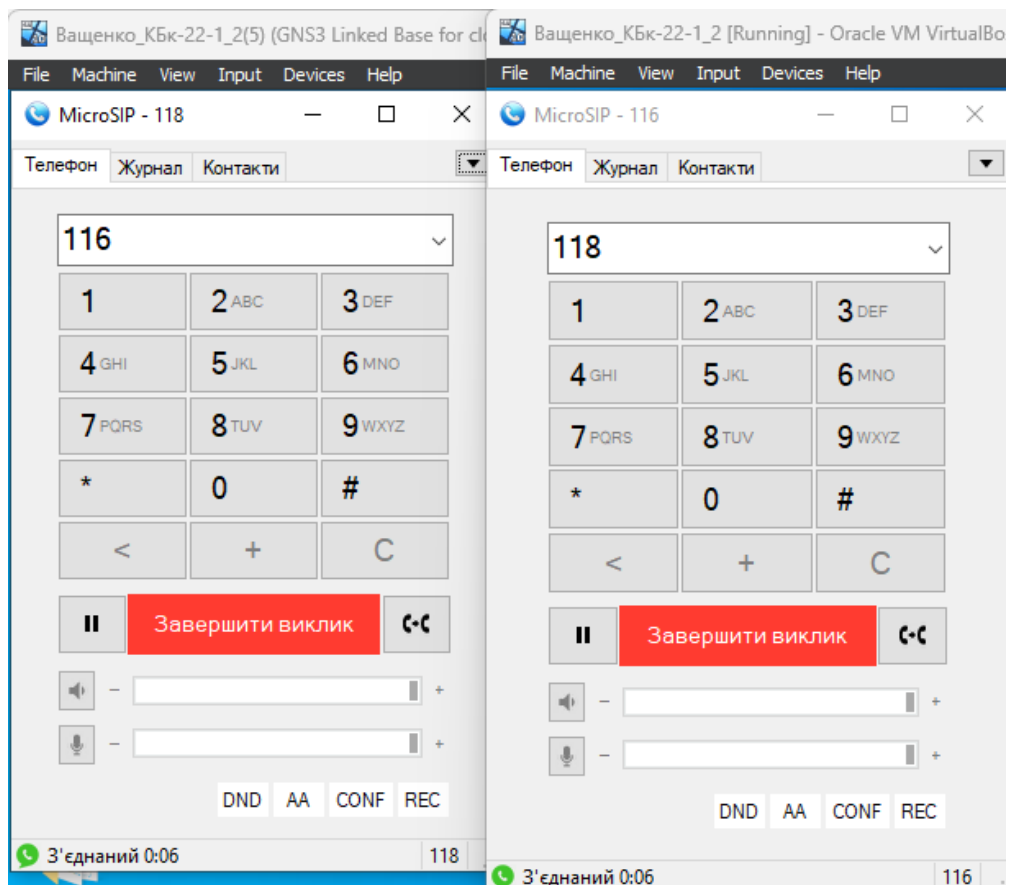


Рисунок 3.69 – Виконано дзвінок з VLAN 116 на VLAN 118

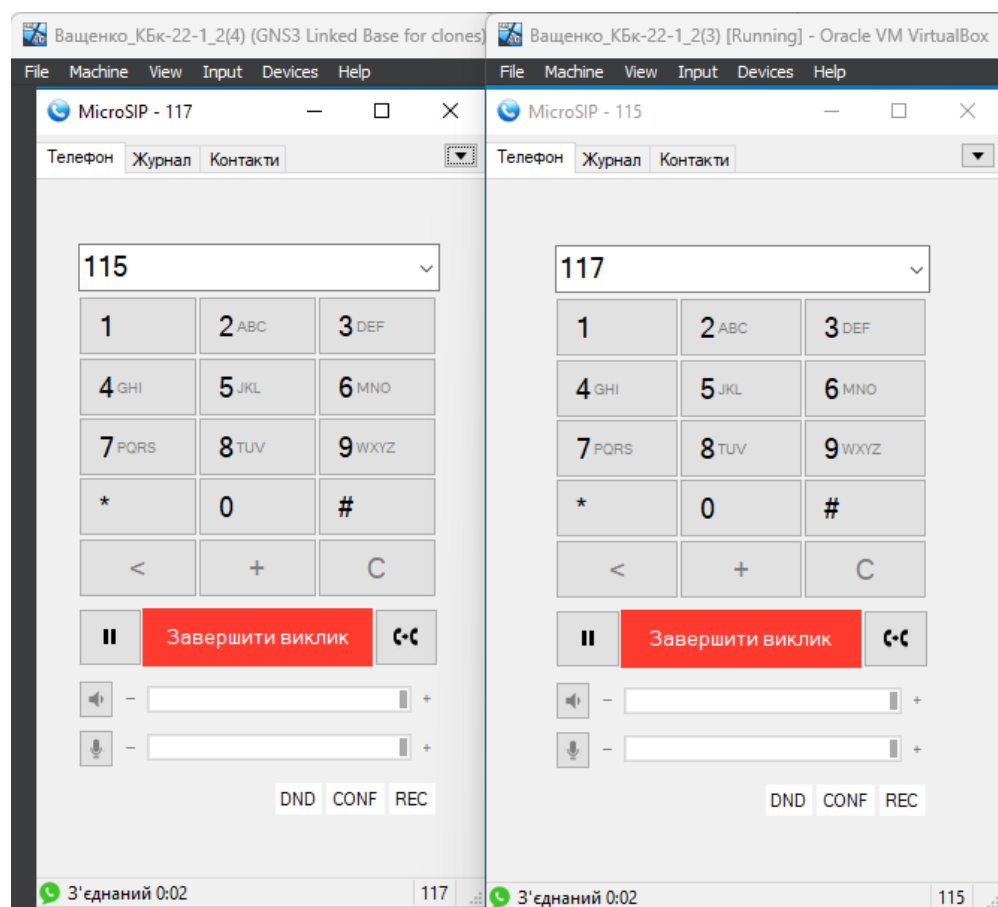


Рисунок 3.70 – Виконано дзвінок з VLAN 115 на VLAN 117

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Так як VLAN-и налаштовані попарно де 115 та 117 являються однією підмережою то дзвонити з VLAN-в на 116 та 118 неможна тому було показано як це відбувається.

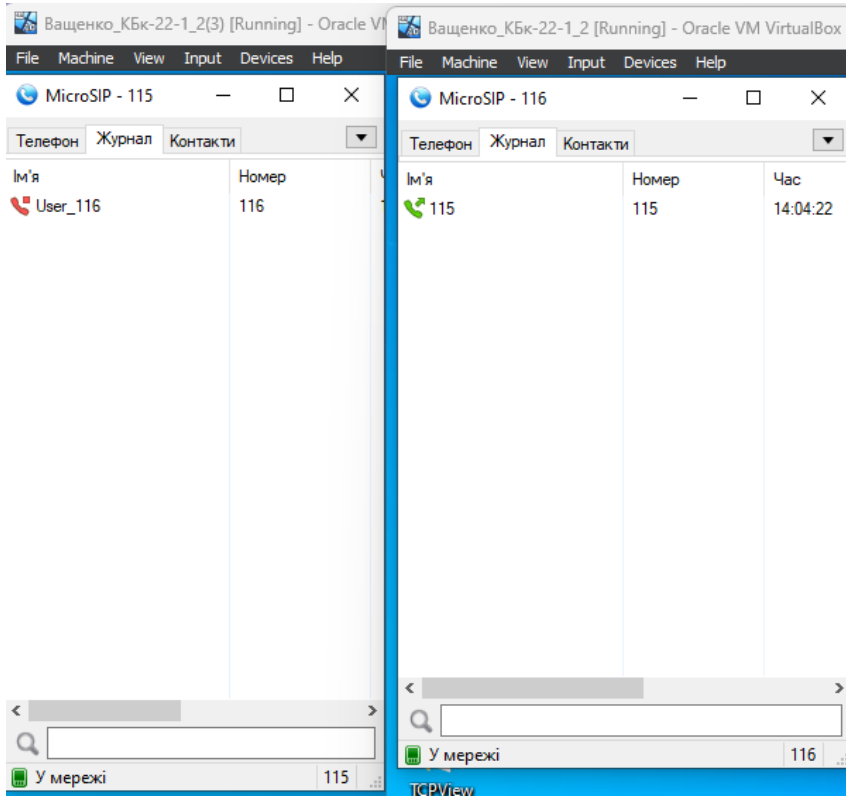


Рисунок 3.71 – Виконано розрив дзвінка з VLAN 115 на VLAN 116

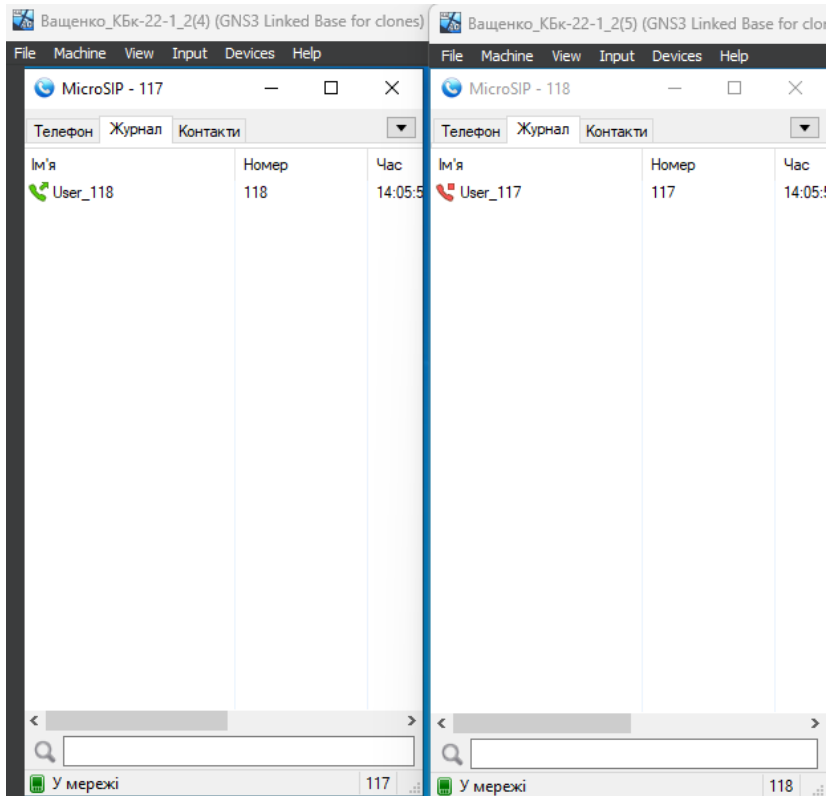


Рисунок 3.72 – Виконано розрив дзвінок з VLAN 118 на VLAN 117

Сценарій проникнення у мережу, реалізований за типом, Головний адмін пропустив один з портів комутатора, що стало чудовою нагодою для зловмисника, він підключився до мережі [21]. І за рахунок Kali Linux, здійснив підключення, та почав викрадати пакети які передаються по мережі [23].

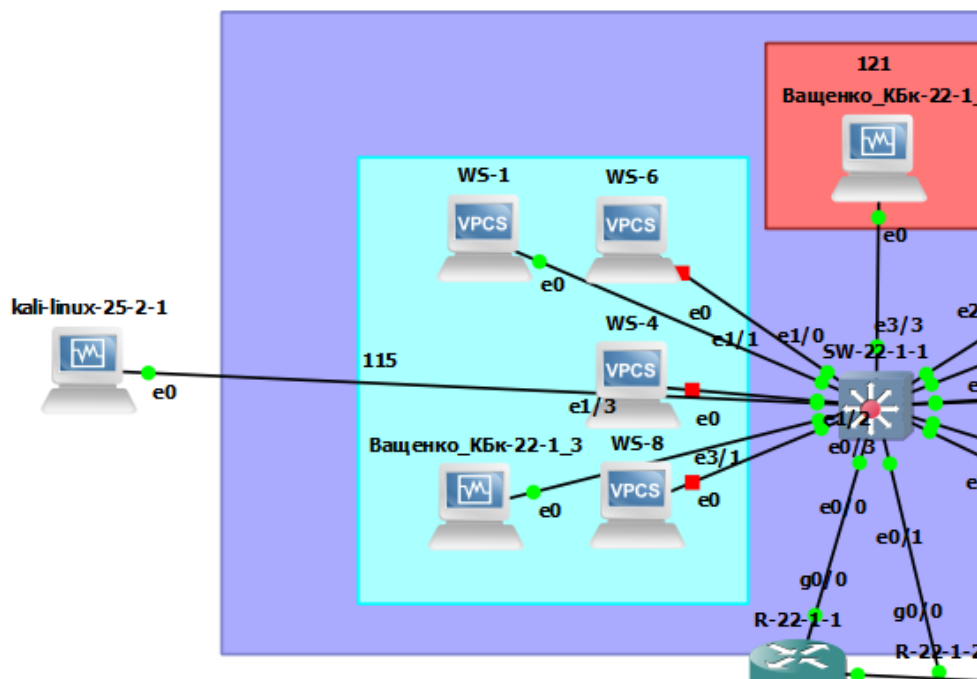


Рисунок 3.73 – Проникнення зловмисника до мережі за типом MITM

```
SW-22-1-1 - PuTTY

switchport port-security mac-address sticky

SW-22-1-1(config)#int e1/2
SW-22-1-1(config-if)#ip arp ins
SW-22-1-1(config-if)#ip arp inspection ?
    limit  Configure Rate limit of incoming ARP packets
    trust  Configure Trust state

SW-22-1-1(config-if)#ip arp inspection?
inspection

SW-22-1-1(config-if)#ip arp inspection ?
    limit  Configure Rate limit of incoming ARP packets
    trust  Configure Trust state

SW-22-1-1(config-if)#ip arp inspection trus
SW-22-1-1(config-if)#ip arp inspection trust
SW-22-1-1(config-if)#ip dhcp sn
SW-22-1-1(config-if)#ip dhcp snooping tru
SW-22-1-1(config-if)#ip dhcp snooping trust
SW-22-1-1(config-if)#no sw
SW-22-1-1(config-if)#no switchport port
SW-22-1-1(config-if)#no switchport port-security
SW-22-1-1(config-if)#
```

Рисунок 3.74 – Відключений захист порту

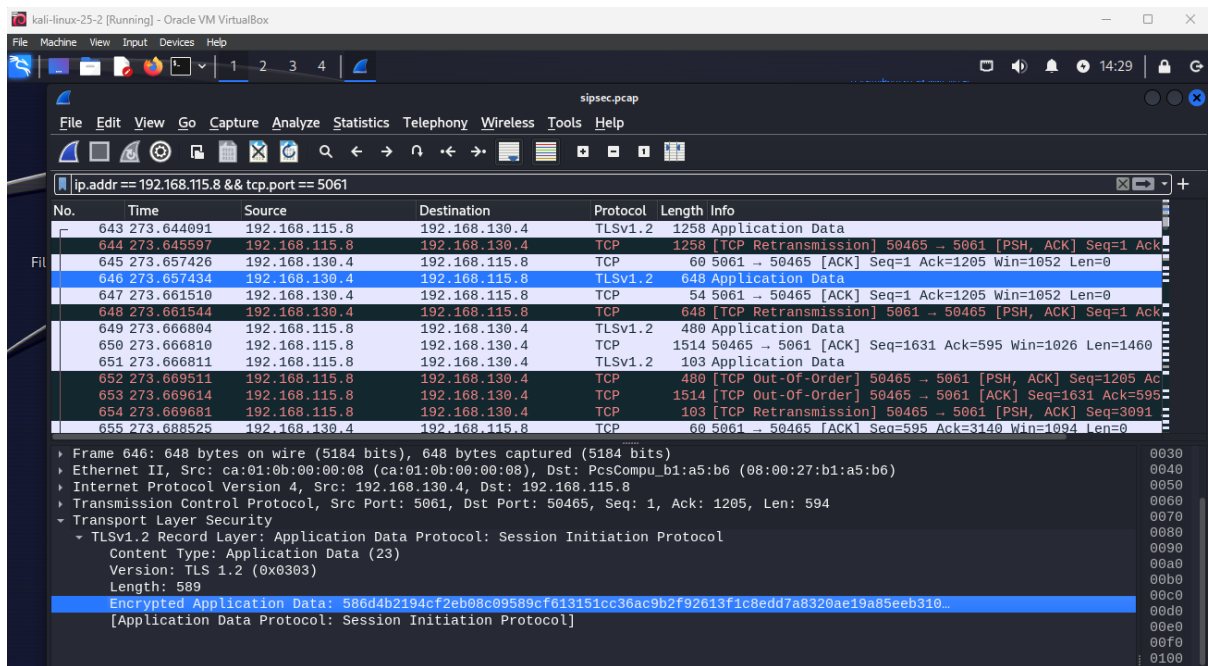


Рисунок 3.75 – Перевірка шифрування трафіку

З врахуванням налаштованого TLS, було протестовано мережу на проникнення MITM, за результатами тестування усі данні було зашифровано, що вказує на те що захист працює і усе шифрується.

Висновки до третього розділу

У третьому розділі було детально висвітлено процес практичної реалізації розробленої підсистеми безпеки VoIP. Описано етапи конфігурування мережевого обладнання Cisco, включаючи налаштування VLAN для сегментації мережі, впровадження правил ACL для контролю доступу та конфігурації HSRP для забезпечення відмовостійкості шлюзів. Значна увага приділена налаштуванню програмної АТС FreePBX, зокрема активації та конфігурації TLS для SIP-з'єднань та SRTP для медіа-трафіку, що є критично важливим для захисту конфіденційності розмов. Також розглянуто інтеграцію та налаштування механізмів виявлення та блокування атак (наприклад, Fail2ban) та систем моніторингу (Prometheus/Grafana) для проактивного відстеження стану безпеки. Проведені тестування, включно з імітацією типових кібератак, підтвердили ефективність запропонованих захисних механізмів та їх здатність протистояти відомим загрозам, забезпечуючи стабільну та безпечну роботу VoIP-інфраструктури.

		Ващенко Б.В.			Арк.
		Трикоз Є.М.			
Змн.	Арк.	№ докум.	Підпис	Дата	76

ВИСНОВКИ

У ході виконання дипломного проєкту був проведений комплексний підхід до побудови та захисту сучасної VoIP-інфраструктури, успішно інтегруючи глибокий теоретичний аналіз кіберзагроз із практичною реалізацією багаторівневих захисних механізмів. Дослідження виявило та деталізувало критичні вразливості VoIP, такі як DDoS, SPIT, MITM та Sniffing, а також визначило мотиви зловмисників, що сформувало фундамент для проектування архітектури безпеки.

На практиці було реалізовано відмовостійку мережеву інфраструктуру між двома офісами з використанням технології HSRP, що гарантує безперебійний зв'язок та високу доступність навіть при виході з ладу ключового обладнання. Для підвищення безпеки була виконана детальна сегментація трафіку за допомогою VLAN-технології (VLANи 115–118, 121, 130), посилена суворим контролем доступу на основі ACL, що забезпечило ефективну ізоляцію підрозділів, запобігло несанкціонованому доступу та обмежило поширення загроз. Як центральне ядро VoIP-системи була інтегрована платформа FreePBX/Asterisk з клієнтами MicroSIP, надавши гнучке та функціональне рішення для корпоративних комунікацій.

Система безпеки включає багато рівнів захисту: настроєні брандмауери, Port Security з прив'язкою MAC-адрес для контролю підключень, DHCP Snooping для блокування несанкціонованих DHCP-серверів, а також надійне шифрування комунікацій за протоколами TLS/SRTP. Саме впровадження TLS/SRTP було доволі тяжким в реалізації так як будувалося не через публічний домен, а через локальний, з якого було витягнуто сертифікат через SSL. Також додатково було впроваджено та налаштовано SSH-аутентифікацію з диференційованими рівнями привілеїв для підвищення безпеки управління системою.

Тестування повністю підтвердило високу ефективність розробленої системи. Зокрема, було успішно продемонстровано, що сегментація трафіку надійно блокує неавторизовані комунікації між різними VLAN-ами

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

(наприклад, VLAN 115 та 116), водночас забезпечуючи стабільні та безперешкодні дзвінки всередині дозволених сегментів (як-от між VLAN 115 та 117). Це свідчить про коректність архітектури та її здатність підтримувати якісний VoIP-зв'язок у визначених межах. Також було проведено тестування на витяг даних через процедуру MITM, з висновків, мережа чудово шифрує дані.

Розроблена інфраструктура значно знижує ризики кібератак, відповідає сучасним стандартам захисту даних (GDPR, ISO 27001) завдяки посиленому контролю над інформацією та досягає оптимального балансу між високим рівнем безпеки та продуктивністю системи.

У підсумку, створена та протестована VoIP-інфраструктура є надійним, функціональним та захищеним рішенням для корпоративних комунікацій. Її модульність та гнучкість конфігурації забезпечують стійкість до майбутніх викликів і можливість адаптації.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСКИ ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Fornell, D. FreePBX 2.10: A Beginner's Guide. Birmingham: Packt Publishing, 2012. 352 p.
2. Doyle, J. Routing TCP/IP, Volume I (2nd Edition). Indianapolis: Cisco Press, 2014. 896 p.
3. Doyle, J. Routing TCP/IP, Volume II (2nd Edition). Indianapolis: Cisco Press, 2015. 1296 p.
4. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd Edition). New York: Wiley, 2015. 784 p.
5. McCarty, D. Asterisk: The Definitive Guide (4th Edition). Sebastopol: O'Reilly Media, 2017. 678 p.
6. Merz, B. Cisco CCNA 200-301 Official Cert Guide, Volume 1. Indianapolis: Cisco Press, 2018. 960 p.
7. Salem, S. Practical VoIP Security: Securing Voice over IP Communications. Boca Raton: Auerbach Publications, 2020. 250 p.
8. Shulha, A. V. Інформаційна безпека: Організаційно-правові та технічні аспекти. Kyiv: KPI im. Ihoria Sikorskoho, 2019. 280 p.
9. Hulak, O. V. Захист інформації в комп'ютерних системах та мережах. Vinnytsia: VNTU, 2021. 315 p.
10. Zubov, D. O. Комп'ютерні мережі: безпека та аудит. Kyiv: NAU, 2022. 290 p.
11. Wolfe, T. Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services (3rd Edition). Indianapolis: Cisco Press, 2016. 960 p.
12. Hay, R., Smith, B. Implementing and Operating Cisco Security Technologies (2nd Edition). Indianapolis: Cisco Press, 2019. 1008 p.
13. Kravchenko, O. P. Кібербезпека: основи та стратегії. Kyiv: Vydavnychyi dim «Kyievo-Mohylianska akademiia», 2017. 240 p.
14. Snow, J. SIP Trunking 101: The Essential Guide to SIP Trunking. Boston: SIPschool Press, 2018. 150 p.

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

15. Hunt, C. TCP/IP Network Administration (3rd Edition). Sebastopol: O'Reilly Media, 2016. 700 p.
16. Cisco Documentation. VLAN Configuration Guide. [Электронный ресурс]: Режим доступа: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/vlan/configuration_guide/b_vlan_150_2_ex_2960x_cg/b_vlan_150_2_ex_2960x_cg_chapter_01.html (дата звернення: 16.06.2025)
17. Cisco Documentation. Configuring IP Access Lists. [Электронный ресурс]: Режим доступа: https://www.cisco.com/c/en/us/td/docs/ios/security/configuration/guide/sec_acl_cfg_guide_xe/sec_acl_cfg_guide_xe_chapter_01.html (дата звернення: 16.06.2025)
18. Cisco Documentation. HSRP Configuration Guide. [Электронный ресурс]: Режим доступа: https://www.cisco.com/c/en/us/td/docs/ios/ipapp/configuration/guide/ipapp_c.html#wp1050212 (дата звернення: 16.06.2025)
19. FreePBX Documentation. Security Overview. [Электронный ресурс]: Режим доступа: <https://www.freepbx.org/support/documentation/security-overview/> (дата звернення: 16.06.2025)
20. Asterisk Documentation. SIP TLS Configuration. [Электронный ресурс]: Режим доступа: <https://wiki.asterisk.org/wiki/display/AST/SIP+TLS+Configuration> (дата звернення: 16.06.2025)
21. OWASP. VoIP Security Testing Guide (VSTG). [Электронный ресурс]: Режим доступа: <https://owasp.org/www-project-voip-security-testing-guide/> (дата звернення: 17.06.2025)
22. IETF RFC 3261. SIP: Session Initiation Protocol. [Электронный ресурс]: Режим доступа: <https://datatracker.ietf.org/doc/html/rfc3261> (дата звернення: 17.06.2025)
23. IETF RFC 3711. The Secure Real-time Transport Protocol (SRTP). [Электронный ресурс]: Режим доступа: <https://datatracker.ietf.org/doc/html/rfc3711> (дата звернення: 17.06.2025)

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

24. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Київ: ДП «УкрНДНЦ», 2016. [Електронний ресурс]: Режим доступу: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf (дата звернення: 19.06.2025)

25. ETSI EN 300 175-7 V2.7.1. Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security Features. Sophia Antipolis: ETSI, 2024. [Електронний ресурс]: Режим доступу: https://www.etsi.org/deliver/etsi_en/300100_300199/30017507/02.07.01_60/en_30017507v020701p.pdf (дата звернення: 17.06.2025)

26. Zarcone, R., & Barbas, M. Cisco Unified Communications Manager: Expert Administration and Troubleshooting. Indianapolis: Cisco Press, 2017. 1056 p.

27. Chen, T., Chen, Y., & Cheng, X. A Survey on Cyber-Physical Security for Voice over IP Systems. IEEE Access. Vol. 9, 2021. P. 119859-119875. DOI: 10.1109/ACCESS.2021.3106886.

28. National Institute of Standards and Technology (NIST). Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Gaithersburg, MD: U.S. Department of Commerce, 2020. [Електронний ресурс]: Режим доступу: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf> (дата звернення: 21.06.2025) IETF RFC 3711. The Secure Real-time Transport Protocol (SRTP). [Електронний ресурс]: Режим доступу: <https://datatracker.ietf.org/doc/html/rfc3711> (дата звернення: 18.06.2025)

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиці адресації мережі

Таблиця А.1

Таблиця маршрутизації Vlan 115

Призначення	IP-адреса
Адреса мережі	192.168.115.0/24
Маска мережі	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.115.1
Максимальна адреса	192.168.115.254
Широкомовна адреса	192.168.115.255
Шлюз за замовчуванням	192.168.115.1
Діапазон використаних адрес	192.168.115.6 - 192.168.115.12
Діапазон вільних адрес	192.168.115.13 192.168.115.254

Таблиця А.2

Таблиця маршрутизації Vlan 116

Призначення	IP-адреса
Адреса мережі	192.168.116.0/24
Маска мережі	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.116.1
Максимальна адреса	192.168.116.254
Широкомовна адреса	192.168.116.255
Шлюз за замовчуванням	192.168.116.1
Діапазон використаних адрес	192.168.116.6 - 192.168.116.12
Діапазон вільних адрес	192.168.116.13 192.168.116.254

Таблиця маршрутизації Vlan 117

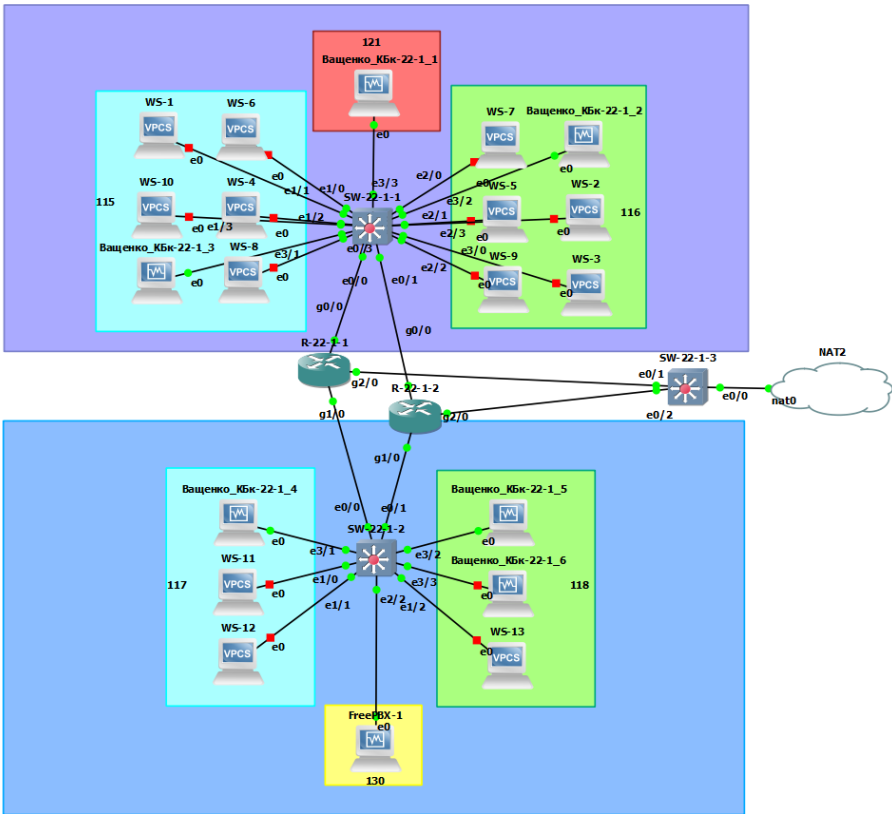
Призначення	IP-адреса
Адреса мережі	192.168.117.0/24
Маска мережі	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.117.1
Максимальна адреса	192.168.117. 254
Шлюз за замовчуванням	192.168.117.1
Діапазон використаних адрес	192.168.117.6 - 192.168.117.9
Діапазон вільних адрес	192.168.117.10 - 192.168.117.254

Таблиця А.4

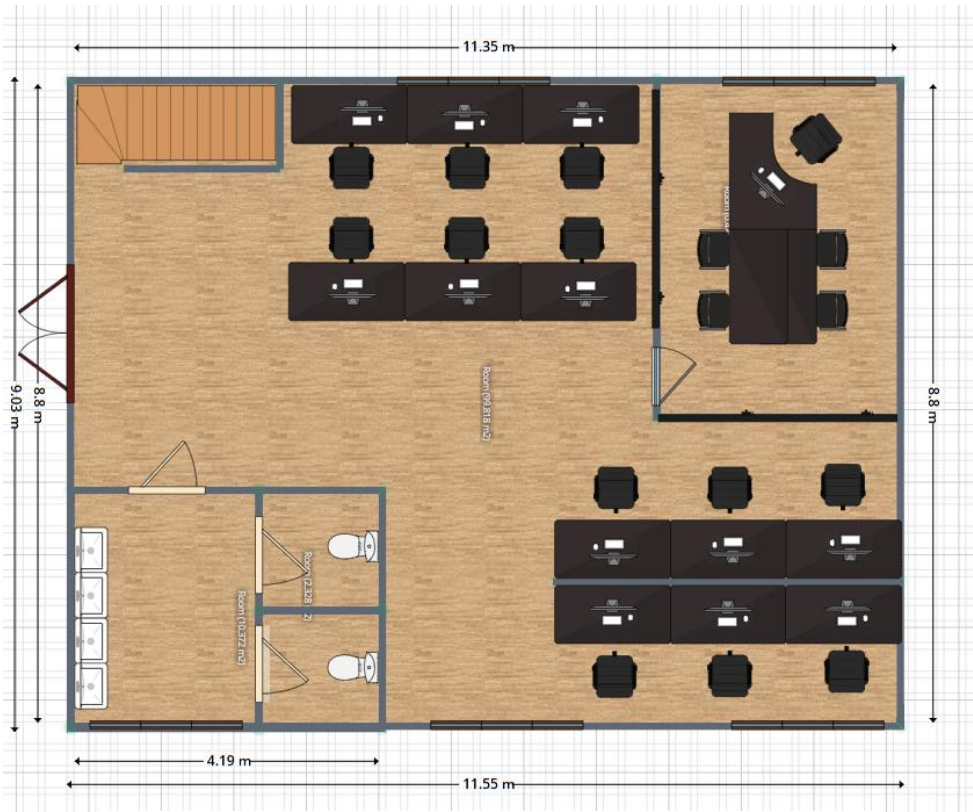
Таблиця маршрутизації Vlan 118

Призначення	IP-адреса
Адреса мережі	192.168.118.0/24
Маска мережі	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.118.1
Максимальна адреса	192.168.118. 254
Широкомовна адреса	192.168.118.255
Шлюз за замовчуванням	192.168.118.1
Діапазон використаних адрес	192.168.118.6 - 192.168.118.9
Діапазон вільних адрес	192.168.118.10 - 192.168.118.254

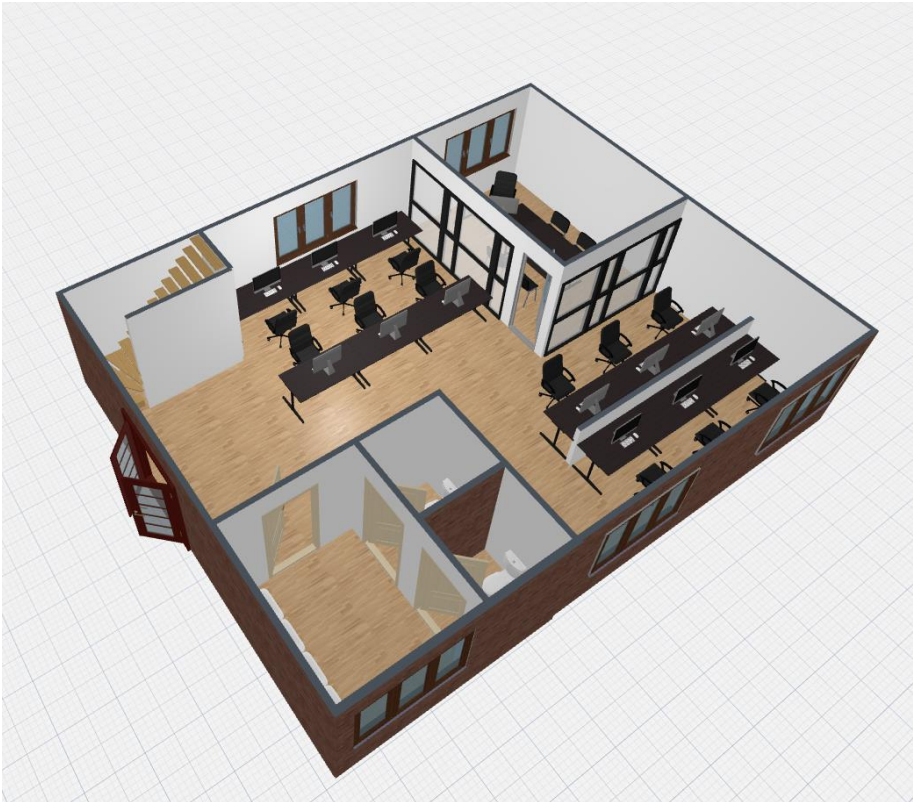
Вигляд мережі з різних ракурсів



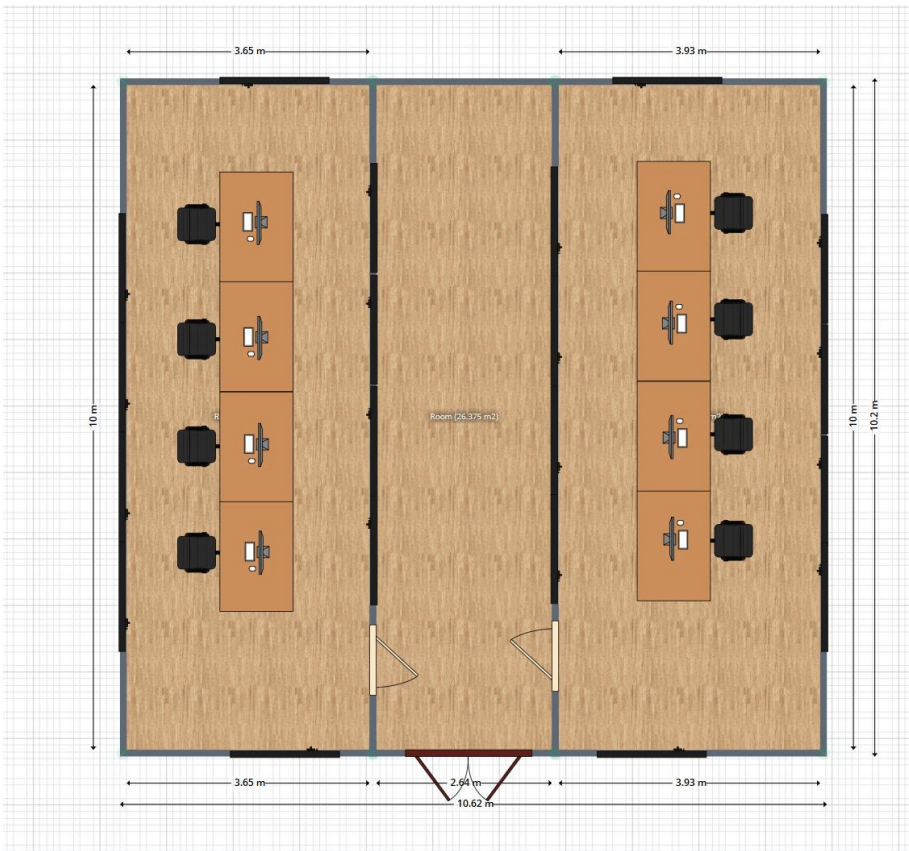
Кінцевий вигляд побудованої мережі



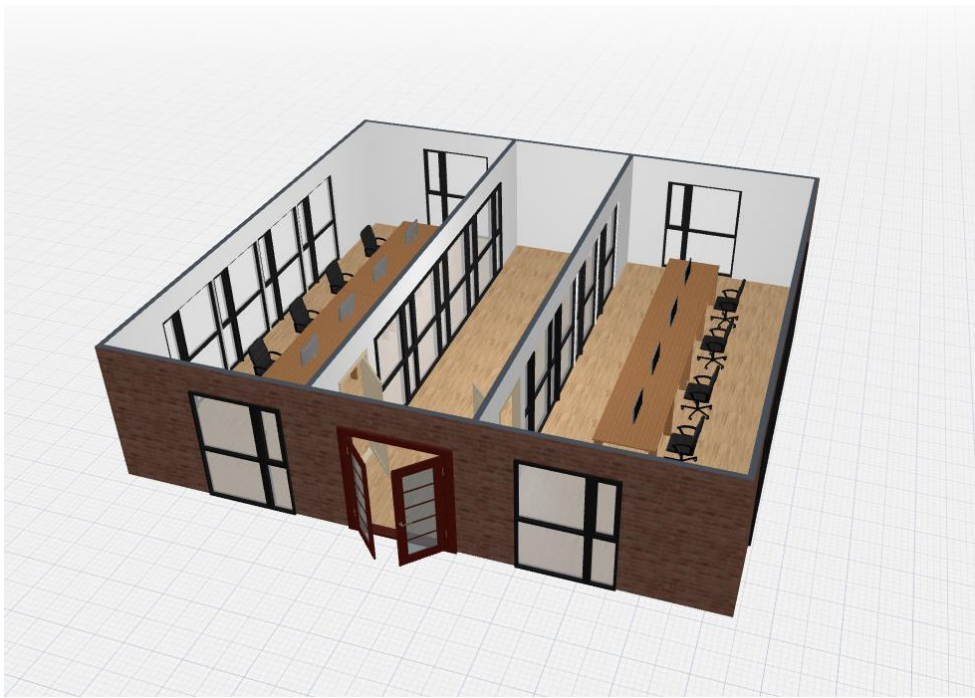
2D План першого офісу



3D План першого офісу



2D План другого офісу



3D План другого офісу

Лістинг конфігурації пристроїв

КОМУТАТОР SW-22-1-1

SW-22-1-1(config)#do sh run

Building configuration...

Current configuration : 6734 bytes

!

! Last configuration change at 17:27:35 UTC Sat Jun 21 2025

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

service compress-config

!

hostname SW-22-1-1

!

boot-start-marker

boot-end-marker

!

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

enable secret 5

\$1\$IcZN\$J68OCKF0kAxlJgvWw5EF.

!

username admin_user privilege 15 secret 5

\$1\$1nO6\$DpdFPUBA943SH357WC48c1

username viewer_user privilege 5 secret 5

\$1\$4gEY\$HkV4XiLGKRxJzVCs6LcQy0

no aaa new-model

!

no ip icmp rate-limit unreachable

!

ip dhcp snooping vlan 115-118,121,130

no ip dhcp snooping information option

ip dhcp snooping

no ip domain-lookup

ip domain-name pbx.vashchenko.local.com

no ip cef

no ipv6 cef

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

no cdp run

!

ip tcp synwait-time 5

ip ssh version 2

!

interface Ethernet0/0

switchport trunk allowed vlan 115-118,121,130

switchport trunk encapsulation dot1q

switchport mode trunk

ip dhcp snooping trust

!

interface Ethernet0/1

switchport trunk allowed vlan 115-118,121,130

switchport trunk encapsulation dot1q

switchport mode trunk

ip dhcp snooping trust

!

interface Ethernet0/2

shutdown

!

interface Ethernet0/3

switchport access vlan 115

switchport mode access

switchport port-security maximum 2

switchport port-security violation restrict

switchport port-security mac-address sticky

switchport port-security mac-address sticky
0050.7966.6807switchport port-security mac-address sticky
0050.7966.680c

switchport port-security aging time 1

switchport port-security

ip dhcp snooping limit rate 50

!

interface Ethernet1/0

switchport access vlan 115

switchport mode access

switchport port-security maximum 2

switchport port-security violation restrict

switchport port-security mac-address sticky

switchport port-security mac-address sticky
0050.7966.6800

switchport port-security aging time 1

switchport port-security

ip dhcp snooping limit rate 50

!

interface Ethernet1/1

switchport access vlan 115

switchport mode access

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		88

```

switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet1/2
switchport access vlan 115
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet1/3
switchport access vlan 115
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet2/0
switchport access vlan 116
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0050.7966.6806
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet2/1
switchport access vlan 116
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0050.7966.6804
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet2/2
switchport access vlan 116
switchport mode access

```

```

switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0050.7966.6807
switchport port-security mac-address sticky
0050.7966.6808
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet2/3
switchport access vlan 116
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet3/0
switchport access vlan 116
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet3/1
switchport access vlan 115
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.27de.d1e1
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet3/2
switchport access vlan 116
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.27e7.711f
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!

```

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet3/3
switchport access vlan 121
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.273f.51ce
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Vlan1
no ip address
shutdown
!
interface Vlan115
no ip address
shutdown
!
interface Vlan116
no ip address
shutdown
!
interface Vlan121
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
privilege exec level 5 show mac address-table
privilege exec level 5 show mac
privilege exec level 5 show ip interface brief
privilege exec level 5 show ip interface
privilege exec level 5 show ip
privilege exec level 5 show vlan brief
privilege exec level 5 show vlan
privilege exec level 5 show version
privilege exec level 5 show running-config
privilege exec level 5 show
!
line con 0
exec-timeout 0 0
privilege level 15
password 7 0207005602085D70
logging synchronous
login
line aux 0
exec-timeout 0 0
privilege level 15

```

```

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

```

KOMYTATOP SW-22-1-2

SW-22-1-2(config)#do sh run
Building configuration...

```

Current configuration : 4879 bytes
!
! Last configuration change at 17:27:41 UTC Sat Jun 21 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname SW-22-1-2
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$6GHm$NAOboQEgD8oW2wumLFWbs0
!
username admin_user privilege 15 secret 5
$1$hLhQ$8D1iuGaINRCW2N4S7MIwv1
username viewer_user privilege 5 secret 5
$1$YdPT$VgRrT1xMFSYr1CVokv929.
no aaa new-model
!
no ip icmp rate-limit unreachable
!
ip dhcp snooping vlan 115-118,121,130
no ip dhcp snooping information option
ip dhcp snooping
no ip domain-lookup
ip domain-name pbx.vashchenko.local.com
no ip cef
no ipv6 cef
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending

```

		Ващенко Б.В.			ККИКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no cdp run
!
ip tcp synwait-time 5
ip ssh version 2
!
interface Ethernet0/0
switchport trunk allowed vlan 115-118,121,130
switchport trunk encapsulation dot1q
switchport mode trunk
ip dhcp snooping trust
!
interface Ethernet0/1
switchport trunk allowed vlan 115-118,121,130
switchport trunk encapsulation dot1q
switchport mode trunk
ip dhcp snooping trust
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
switchport access vlan 117
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0050.7966.6809
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet1/1
switchport access vlan 117
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0050.7966.680a
switchport port-security mac-address sticky
0050.7966.680b
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet1/2
switchport access vlan 118
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0050.7966.680c

switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
switchport access vlan 130
switchport mode access
switchport port-security maximum 5
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.275f.3a8d
switchport port-security mac-address sticky
0800.27ac.5d01
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
switchport access vlan 117
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.27c9.989a
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet3/2
switchport access vlan 118
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.2725.ff17
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Ethernet3/3
switchport access vlan 118
switchport mode access

```

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.2744.c9af
switchport port-security aging time 1
switchport port-security
ip dhcp snooping limit rate 50
!
interface Vlan1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
privilege exec level 5 show mac address-table
privilege exec level 5 show mac
privilege exec level 5 show ip interface brief
privilege exec level 5 show ip interface
privilege exec level 5 show ip
privilege exec level 5 show vlan brief
privilege exec level 5 show vlan
privilege exec level 5 show version
privilege exec level 5 show running-config
privilege exec level 5 show
!
line con 0
exec-timeout 0 0
privilege level 15
password 7 1218011A1B055E55
logging synchronous
login
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
!
end

```

МАРШРУТИЗАТОР R-22-1-1

R-22-1-1(config)#do sh run
Building configuration...

Current configuration : 10516 bytes
!
upgrade fpd auto

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R-22-1-1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$hCer$9h6psxQR88UEetLv78zKx.
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
ip dhcp excluded-address 192.168.115.1
192.168.115.5
ip dhcp excluded-address 192.168.116.1
192.168.116.5
ip dhcp excluded-address 192.168.117.1
192.168.117.5
ip dhcp excluded-address 192.168.118.1
192.168.118.5
ip dhcp excluded-address 192.168.121.1
192.168.121.6
!
ip dhcp pool VLAN115
network 192.168.115.0 255.255.255.0
default-router 192.168.115.1
dns-server 8.8.8.8
lease 7
!
ip dhcp pool VLAN116
network 192.168.116.0 255.255.255.0
default-router 192.168.116.1
dns-server 8.8.8.8
lease 7
!
ip dhcp pool VLAN117
network 192.168.117.0 255.255.255.0
default-router 192.168.117.1
dns-server 8.8.8.8
lease 7
!
ip dhcp pool VLAN118
network 192.168.118.0 255.255.255.0
default-router 192.168.118.1
dns-server 8.8.8.8
lease 7
!
ip dhcp pool VLAN121
network 192.168.121.0 255.255.255.0

```

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

```

default-router 192.168.121.1
dns-server 8.8.8.8
!
ip dhcp pool VLAN130
network 192.168.130.0 255.255.255.248
default-router 192.168.130.1
dns-server 8.8.8.8
lease 7
!
no ip domain lookup
ip domain name pbx.vashchenko.local.com
no ipv6 cef
!
multilink bundle-name authenticated
!
username admin_user privilege 15 secret 5
$1$X8Bb$yTRT9Qwl0zeMEq/rORJb71
username viewer_user privilege 5 secret 5
$1$WLJh$f25N.JYNEXBpzwYVzAnoL.
archive
log config
hidekeys
!
ip tcp synwait-time 5
ip ssh version 2
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
no ip address
duplex full
speed 1000
media-type gbic
negotiation auto
!
interface GigabitEthernet0/0.115
encapsulation dot1Q 115
ip address 192.168.115.2 255.255.255.0
ip access-group ACL_VLAN115 in
ip nat inside
ip virtual-reassembly
standby 115 ip 192.168.115.1
standby 115 priority 110
standby 115 preempt
!
interface GigabitEthernet0/0.116
encapsulation dot1Q 116
ip address 192.168.116.2 255.255.255.0
ip access-group ACL_VLAN116 in
ip nat inside
ip virtual-reassembly
standby 116 ip 192.168.116.1
standby 116 priority 110
standby 116 preempt
!
interface GigabitEthernet0/0.121
encapsulation dot1Q 121
ip address 192.168.121.2 255.255.255.0
ip nat inside
ip virtual-reassembly
standby 121 ip 192.168.121.1
standby 121 priority 110
standby 121 preempt
!
interface GigabitEthernet1/0
no ip address
negotiation auto
!
interface GigabitEthernet1/0.117
encapsulation dot1Q 117
ip address 192.168.117.2 255.255.255.0
ip access-group ACL_VLAN117 in
ip nat inside
ip virtual-reassembly
standby 117 ip 192.168.117.1
standby 117 priority 110
standby 117 preempt
!
interface GigabitEthernet1/0.118
encapsulation dot1Q 118
ip address 192.168.118.2 255.255.255.0
ip access-group ACL_VLAN118 in
ip nat inside
ip virtual-reassembly
standby 118 ip 192.168.118.1
standby 118 priority 110
standby 118 preempt
!
interface GigabitEthernet1/0.130
encapsulation dot1Q 130
ip address 192.168.130.2 255.255.255.248
ip access-group ACL_VLAN130 in
ip nat inside
ip virtual-reassembly
standby 130 ip 192.168.130.1
standby 130 priority 110
standby 130 preempt
!
interface GigabitEthernet2/0
ip address dhcp
ip nat outside
ip virtual-reassembly
negotiation auto
!
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 dhcp
no ip http server

```

		Вашченко Б.В.			ККИКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip http secure-server
!
ip nat inside source list 2 interface
GigabitEthernet2/0 overload
!
ip access-list extended ACL_VLAN115
 permit udp any any eq bootpc
 permit udp any any eq bootps
 permit ip 192.168.115.0 0.0.0.255 192.168.117.0
0.0.0.255
 permit tcp 192.168.115.0 0.0.0.255 192.168.117.0
0.0.0.255 eq 5060
 permit udp 192.168.115.0 0.0.0.255 192.168.117.0
0.0.0.255 eq 5060
 permit tcp 192.168.115.0 0.0.0.255 192.168.117.0
0.0.0.255 eq 5061
 permit udp 192.168.115.0 0.0.0.255 192.168.117.0
0.0.0.255 eq 5061
 permit udp 192.168.115.0 0.0.0.255 192.168.117.0
0.0.0.255
 deny ip 192.168.115.0 0.0.0.255 192.168.116.0
0.0.0.255
 deny ip 192.168.115.0 0.0.0.255 192.168.118.0
0.0.0.255
 deny ip 192.168.115.0 0.0.0.255 192.168.121.0
0.0.0.255
 permit ip 192.168.115.0 0.0.0.255 any
ip access-list extended ACL_VLAN116
 permit udp any any eq bootpc
 permit udp any any eq bootps
 permit ip 192.168.116.0 0.0.0.255 192.168.118.0
0.0.0.255
 permit tcp 192.168.116.0 0.0.0.255 192.168.118.0
0.0.0.255 eq 5060
 permit udp 192.168.116.0 0.0.0.255 192.168.118.0
0.0.0.255 eq 5060
 permit tcp 192.168.116.0 0.0.0.255 192.168.118.0
0.0.0.255 eq 5061
 permit udp 192.168.116.0 0.0.0.255 192.168.118.0
0.0.0.255 eq 5061
 permit udp 192.168.116.0 0.0.0.255 192.168.118.0
0.0.0.255
 deny ip 192.168.116.0 0.0.0.255 192.168.115.0
0.0.0.255
 deny ip 192.168.116.0 0.0.0.255 192.168.117.0
0.0.0.255
 deny ip 192.168.116.0 0.0.0.255 192.168.121.0
0.0.0.255
 permit ip 192.168.116.0 0.0.0.255 any
ip access-list extended ACL_VLAN117
 permit udp any any eq bootpc
 permit udp any any eq bootps
 permit ip 192.168.117.0 0.0.0.255 192.168.115.0
0.0.0.255

```

```

 permit tcp 192.168.117.0 0.0.0.255 192.168.115.0
0.0.0.255 eq 5060
 permit udp 192.168.117.0 0.0.0.255 192.168.115.0
0.0.0.255 eq 5060
 permit tcp 192.168.117.0 0.0.0.255 192.168.115.0
0.0.0.255 eq 5061
 permit udp 192.168.117.0 0.0.0.255 192.168.115.0
0.0.0.255 eq 5061
 permit udp 192.168.117.0 0.0.0.255 192.168.115.0
0.0.0.255
 deny ip 192.168.117.0 0.0.0.255 192.168.116.0
0.0.0.255
 deny ip 192.168.117.0 0.0.0.255 192.168.118.0
0.0.0.255
 deny ip 192.168.117.0 0.0.0.255 192.168.121.0
0.0.0.255
 permit ip 192.168.117.0 0.0.0.255 any
ip access-list extended ACL_VLAN118
 permit udp any any eq bootpc
 permit udp any any eq bootps
 permit ip 192.168.118.0 0.0.0.255 192.168.116.0
0.0.0.255
 permit tcp 192.168.118.0 0.0.0.255 192.168.116.0
0.0.0.255 eq 5060
 permit udp 192.168.118.0 0.0.0.255 192.168.116.0
0.0.0.255 eq 5060
 permit tcp 192.168.118.0 0.0.0.255 192.168.116.0
0.0.0.255 eq 5061
 permit udp 192.168.118.0 0.0.0.255 192.168.116.0
0.0.0.255 eq 5061
 permit udp 192.168.118.0 0.0.0.255 192.168.116.0
0.0.0.255
 deny ip 192.168.118.0 0.0.0.255 192.168.115.0
0.0.0.255
 deny ip 192.168.118.0 0.0.0.255 192.168.117.0
0.0.0.255
 deny ip 192.168.118.0 0.0.0.255 192.168.121.0
0.0.0.255
 permit ip 192.168.118.0 0.0.0.255 any
ip access-list extended ACL_VLAN121
 permit icmp 192.168.121.0 0.0.0.255 192.168.115.0
0.0.0.255 echo-reply
 permit tcp 192.168.121.0 0.0.0.255 192.168.115.0
0.0.0.255 established
 permit udp 192.168.121.0 0.0.0.255 192.168.115.0
0.0.0.255 eq 5060
 permit tcp 192.168.121.0 0.0.0.255 192.168.115.0
0.0.0.255 eq 5060
 permit udp 192.168.121.0 0.0.0.255 192.168.115.0
0.0.0.255 eq 5061
 permit tcp 192.168.121.0 0.0.0.255 192.168.115.0
0.0.0.255 eq 5061
 permit udp 192.168.121.0 0.0.0.255 192.168.115.0
0.0.0.255 range 16384 32767

```

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арк.
		Трикоз Є.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

```

permit icmp 192.168.121.0 0.0.0.255 192.168.116.0
0.0.0.255 echo-reply
permit tcp 192.168.121.0 0.0.0.255 192.168.116.0
0.0.0.255 established
permit udp 192.168.121.0 0.0.0.255 192.168.116.0
0.0.0.255 eq 5060
permit tcp 192.168.121.0 0.0.0.255 192.168.116.0
0.0.0.255 eq 5060
permit udp 192.168.121.0 0.0.0.255 192.168.116.0
0.0.0.255 eq 5061
permit tcp 192.168.121.0 0.0.0.255 192.168.116.0
0.0.0.255 eq 5061
permit udp 192.168.121.0 0.0.0.255 192.168.116.0
0.0.0.255 range 16384 32767
permit icmp 192.168.121.0 0.0.0.255 192.168.117.0
0.0.0.255 echo-reply
permit tcp 192.168.121.0 0.0.0.255 192.168.117.0
0.0.0.255 established
permit udp 192.168.121.0 0.0.0.255 192.168.117.0
0.0.0.255 eq 5060
permit tcp 192.168.121.0 0.0.0.255 192.168.117.0
0.0.0.255 eq 5060
permit udp 192.168.121.0 0.0.0.255 192.168.117.0
0.0.0.255 eq 5061
permit tcp 192.168.121.0 0.0.0.255 192.168.117.0
0.0.0.255 eq 5061
permit udp 192.168.121.0 0.0.0.255 192.168.117.0
0.0.0.255 range 16384 32767
permit icmp 192.168.121.0 0.0.0.255 192.168.118.0
0.0.0.255 echo-reply
permit tcp 192.168.121.0 0.0.0.255 192.168.118.0
0.0.0.255 established
permit udp 192.168.121.0 0.0.0.255 192.168.118.0
0.0.0.255 eq 5060
permit tcp 192.168.121.0 0.0.0.255 192.168.118.0
0.0.0.255 eq 5060
permit udp 192.168.121.0 0.0.0.255 192.168.118.0
0.0.0.255 eq 5061
permit tcp 192.168.121.0 0.0.0.255 192.168.118.0
0.0.0.255 eq 5061
permit udp 192.168.121.0 0.0.0.255 192.168.118.0
0.0.0.255 range 16384 32767
permit ip 192.168.118.0 0.0.0.255 any
ip access-list extended ACL_VLAN130
permit udp host 192.168.130.1 eq 5060
192.168.115.0 0.0.0.255
permit tcp host 192.168.130.1 eq 5060
192.168.115.0 0.0.0.255 established
permit tcp host 192.168.130.1 eq 5061
192.168.115.0 0.0.0.255 established
permit udp host 192.168.130.1 range 10000 20000
192.168.115.0 0.0.0.255
permit udp host 192.168.130.1 eq 5060
192.168.116.0 0.0.0.255

```

```

permit tcp host 192.168.130.1 eq 5060
192.168.116.0 0.0.0.255 established
permit tcp host 192.168.130.1 eq 5061
192.168.116.0 0.0.0.255 established
permit udp host 192.168.130.1 range 10000 20000
192.168.116.0 0.0.0.255
permit udp host 192.168.130.1 eq 5060
192.168.117.0 0.0.0.255
permit tcp host 192.168.130.1 eq 5060
192.168.117.0 0.0.0.255 established
permit tcp host 192.168.130.1 eq 5061
192.168.117.0 0.0.0.255 established
permit udp host 192.168.130.1 range 10000 20000
192.168.117.0 0.0.0.255
permit udp host 192.168.130.1 eq 5060
192.168.118.0 0.0.0.255
permit tcp host 192.168.130.1 eq 5060
192.168.118.0 0.0.0.255 established
permit tcp host 192.168.130.1 eq 5061
192.168.118.0 0.0.0.255 established
permit udp host 192.168.130.1 range 10000 20000
192.168.118.0 0.0.0.255
permit ip 192.168.130.0 0.0.0.255 any
permit ip 192.168.118.0 0.0.0.255 any
!
access-list 2 permit any
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!
privilege exec level 5 show vlans
privilege exec level 5 show vlan-range
privilege exec level 5 show ip interface brief
privilege exec level 5 show ip interface
privilege exec level 5 show ip
privilege exec level 5 show version
privilege exec level 5 show running-config
privilege exec level 5 show
!
line con 0
exec-timeout 0 0
privilege level 15
password 7 03055F060F01731D
logging synchronous
login
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4

```

		Ващенко Б.В.			ККІКБ.КР.Б – 125 – 2 – ПЗ	Арх.
		Трикоз Є.М.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

```
login local
transport input ssh
!
end
```