

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 ІТ-інфраструктури мережі наукової
бібліотеки»

Виконав студент 4-го курсу групи КІ-4
спеціальності 123 «Комп'ютерна інженерія»

 Г.О. Борейченко

Керівник доцент кафедри КІ та КБ, к.пед.н.

 О.С. Головня

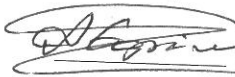
Рецензент доцент кафедри КН, к.пед.н.

 О.В. Коротун

Житомир – 2022

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Борейченко Гліб Олегович

Тема роботи: «Проект IT-інфраструктури мережі наукової бібліотеки»

затверджена Наказом університету від 1 березня 2022 р. № 127/с

Термін здачі студентом закінченої роботи 10 червня 2022 р.

Вихідні дані роботи: предметом дослідження є розробка і побудова мережі наукової бібліотеки, об'єктом дослідження даної кваліфікаційної роботи є розробка мережі наукової бібліотеки.

Обладнання та програмне забезпечення:

1. Операційна система Ubuntu Server
2. Програмний мережевий емулятор GNS3
3. Клієнт протоколів SFTP та SCP – WinSCP

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Головня О.С.	10.03.2022р. 	10.03.2022р. 
2	Головня О.С.	10.04.2022р. 	10.04.2022р. 
3	Головня О.С.	14.05.2022р. 	14.05.2022р. 

Студент  Гліб Боре́йченко

Керівник  Олена Головня

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примі- тка
1	Аналіз отриманого завдання	02.09.2021 р.	
2	Складання календарного плану	05.09.2021 р.	
3	Аналіз літературних джерел	03.10.2021 р.	
4	Написання вступу до роботи	11.10.2021 р.	
5	Вибір технологій для розробки	30.11.2021 р.	
6	Вибір мережевої архітектури	31.03.2022 р.	
7	Вибір серверної ОС для роботи	01.04.2022 р.	
8	Проектування топології та адресації	03.05.2022 р.	
9	Вибір апаратного забезпечення мережі	10.05.2022 р.	
10	Налагодження обладнання для мережі	16.05.2022 р.	
11	Перевірка працездатності	17.05.2022 р.	
12	Організація мережі на Ubuntu Server	20.05.2022 р.	
13	Налагодження захисту мережі	01.06.2022 р.	
14	Формулювання загального висновку	14.06.2022 р.	
15	Захист	Згідно з розкладом	

Студент  Гліб Боре́йченко

Керівник  Олена Головня

АНОТАЦІЯ

В даній кваліфікаційній роботі розглянуто питання забезпечення функціонування робочої IT-інфраструктури бібліотеки. У процесі виконання кваліфікаційної роботи був проведений аналіз можливостей мереж наукових бібліотек, на базі якого було розроблено проєкт для полегшеного та прискореного доступу до мережі наукової бібліотеки та кращого отримання даних з застосуванням інформаційних технологій.

Обсяг пояснювальної записки складає сто тридцять сім сторінок друкованого тексту. Кількість рисунків складає сто тридцять три. Кількість таблиць вісім. Обсяг списку використаних джерел складає тридцять найменувань розміщених на трьох сторінках.

Метою кваліфікаційної роботи є розробка проєкту IT-інфраструктури мережі наукової бібліотеки.

Під час розробки кваліфікаційної роботи було досягнуто наступних результатів. Досліджено особливості проектування інформаційних мереж. Створено структуру комп'ютерної мережі і на її базі спроектовано робочу топологію мережі. Вибрано апаратне забезпечення для роботи над проєктом. Вибрано основні технології для втілення проєкту і показано поступну розробку мережі. Забезпечено захист інформаційної мережі. Проведено тестування мережі і наведено результати.

Ключові слова: КОРПОРАТИВНА МЕРЕЖА, МЕРЕЖІ, МЕРЕЖЕВІ ПРОТОКОЛИ, НАУКОВА БІБЛІОТЕКА, СЕРВЕР, ОС UBUNTU.

					КІК.КР.Б – 123 – 07 – ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проєкт IT-інфраструктури мережі наукової бібліотеки	Літ.	Арк.	Аркушів
Розроб.		Бореченко І.О.	<i>[Підпис]</i>	20.06				
Керівник		Головня О.С.	<i>[Підпис]</i>	20.06				
Реценз.		Коротун О.В.	<i>[Підпис]</i>	20.06			4	137
Н. контр.		Головня О.С.	<i>[Підпис]</i>	20.06		ФІКТ, Гр. КІ-4		
Затверд.		Сфіменко А.А.	<i>[Підпис]</i>	20.06				

ANNOTATION

The qualification work focuses on the issues of ensuring the functioning of the working IT infrastructure of the library. An analysis of the capabilities of scientific library networks was conducted, on the basis of which a project was developed for easier and faster access to the network of the scientific library and better data keeping using information technology.

The volume of the explanatory note is one hundred and thirty-seven pages of printed text. The number of drawings is one hundred and thirty-three. The number of tables is eight. The volume of the list of used sources makes thirty names placed on three pages.

The purpose of the qualification work is to build a project of IT-infrastructure of the scientific library network.

The following results were achieved during the development of the qualification work. Peculiarities of information networks design are investigated. The structure of the computer network is created and the working topology of the network is designed on its basis. Hardware selected to work on the project. The main technologies for the project implementation are selected and the step-by-step network development is shown. Information network protection is provided. The network was tested and the results are given.

Keywords: CORPORATE NETWORK, NETWORKS, NETWORK PROTOCOLS, OS UBUNTU, SCIENTIFIC LIBRARY, SERVER.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	8
ВСТУП.....	9
РОЗДІЛ 1 ПЛАНУВАННЯ СТРУКТУРИ МЕРЕЖІ.....	12
1.1 Особливості проєктування корпоративної мережі.....	12
1.2 Етапи проєктування корпоративної мережі.....	14
1.3 Аналіз завдань	14
1.4 Побудова функціональної моделі мережі	15
1.5 Побудова технічної моделі мережі	16
1.6 Інформаційні потоки у мережі бібліотеки	17
1.7 Основні технології та протоколи	18
РОЗДІЛ 2 ПРОЄКТУВАННЯ МЕРЕЖІ.....	29
2.1 Управління мережею	29
2.2 Розміщення сервера	31
2.3 Мережева архітектура	33
2.4 Мережеві ресурси	34
2.5 Розширення мережі.....	35
2.6 Огляд ОС для розробки комп'ютерної мережі	36
2.7 Обґрунтування вибору Ubuntu Server.....	44
2.8 Проектування топології комп'ютерної мережі та розробка системи адресації	46
2.9 Апаратне забезпечення комп'ютерної мережі.....	54

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ	58
3.1 Налагодження обладнання мережі.....	58
3.2 Перевірка працездатності мережі	64
3.3 Встановлення і налаштування ОС Ubuntu Server.....	67
3.4 Організація мережі на ОС Ubuntu Server	70
3.5 Налагодження захисту мережі.....	86
ВИСНОВКИ.....	96
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	98
ДОДАТКИ.....	101

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Модель OSI (Open Systems Interconnection Basic Reference Model) – базова еталонна модель взаємодії відкритих систем

Модель TCP/IP (Transmission Control Protocol /Internet Protocol) – стек протоколів

UDP (User Datagram Protocol) - протокол датаграм користувача

YAML (Yet Another Markup Language) - мова опису розмітки

TCP (Transmission Control Protocol) - протокол керування передачею

DNS (Domain Name System) - система доменних імен

SSH (Secure SHell) - безпечний командний рядок

UFW (Uncomplicated Firewall) – брандмауер на Ubuntu Server

OSPF (Open Shortest Path First) – протокол динамічної маршрутизації

LACP (Link Aggregation Control Protocol) – протокол агрегації каналів

PVST (Per-VLAN Spanning Tree) – модифікація протоколу STP

HSRP (Hot Standby Router Protocol) – протокол Cisco

VPN (Virtual Private Network) - віртуальна приватна мережа

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Інформація є головним компонентом розвитку людства. З часом суспільство постійно збільшувало наявний обсяг знань і досвіду. В умовах безперервного збільшення обсягу даних виникла нагальна потреба в їх оптимізації, ефективному зберіганні та забезпеченню ефективного доступу до них. Саме на цьому етапі формуються перші бібліотеки як осередки накопичених суспільством знань і навичок. Однак з плином часу змінюються і способи роботи з великими обсягами нових знань. При цьому новітні інформаційні технології і їх стрімке поширення спричиняє фундаментальну зміну в аспектах суспільного життя і зокрема в зберіганні отриманих знань та навичок. Оскільки єдиним завданням бібліотек є надання необхідних даних і інформації своїм читачам це спонукає бібліотеки йти в ногу з технічним прогресом.

Виходячи з потреб часу, бібліотека як установа, яка зберігає та обробляє великий масив даних, повинна забезпечувати інформаційні потреби своїх користувачів. Це неможливо зробити без створення інформаційно-комп'ютерних бібліотечних мереж. Така мережа має забезпечувати вільний доступ до науково-технічної інформації кожному своєму користувачу, надавати доступ до потрібних їм джерел інформації, задовольняти їхні інтереси у пошуку необхідних даних.

Основним завданням бібліотеки завжди було збирати, зберігати, поширювати, виробляти та використовувати загальнодоступну інформацію, наукові праці тощо. Наукова бібліотека – це бібліотека, зосереджена на розвитку науки, створена для інформаційних потреб наукових і навчальних установ та окремих осіб пов'язаних з дослідницькою або навчальною роботою. Таким чином, наукові бібліотеки й наукові фонди відрізняються від інших бібліотек різним відношенням користувачів до потрібної інформації та знань. Діяльність наукових бібліотек спрямована на задоволення інформаційних потреб читачів, пов'язаних з науково-дослідною роботою, з розширенням професійних знань і підвищенням кваліфікації осіб з вищою освітою у всіх сферах виробничої діяльності. Однак слід пам'ятати, що в наш час спосіб створення і зберігання знань та навичок

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

зазнав значних змін, що призвело до відповідного зрушення у соціальній комунікації в цій галузі. З одного боку, ця зміна забезпечує доступ до інформаційних ресурсів, що належать до інших тем інформаційного простору, у тому числі представлених у всесвітній мережі інтернет. З іншого боку, забезпечує такі інформаційні ресурси, як бази даних, цифрові документи та інтернет-портали, за своїми фізичними стінами. Разом з тим, сучасні бібліотеки стали центрами концентрації та розподілу інформаційного потоку.

Сьогодні бібліотечні послуги засновані не лише на фондах бібліотечної літератури, а й на електронних і віртуальних носіях. Сьогодні бібліотеки надають нові можливості для доступу до інформації незалежно від часу та місця документа та користувача. Таким чином, щоб задовольнити інформаційні, освітні та культурні потреби користувачів, сьогодні бібліотеки не лише надають документальні знання, інформацію, що зберігається у їхніх колекціях або на жорстких дисках серверів. Вони виходять за межі своїх фізичних кордонів, переходячи з реального простору у віртуальний.

Стрімке розповсюдження нових комунікаційних технологій призвело до системних змін в інформаційній сфері. Створений глобальний інформаційний простір має забезпечити людей швидким обміном даними та доступом до глобальних інформаційних ресурсів, задовольнити потреби користувачів в інформаційних продуктах та послугах. Таким чином, значення науково-бібліотечної галузі як системи зберігання інформації зросло. Однак, підвищення ролі наукових бібліотек потребує втілення нових методів для формування інформаційного простору та самої бібліотеки, що реалізується на основі комп'ютерних технологій.

Розвиток сучасних технологій, а також зростання кількості інформації та даних якими обмінюються користувачі у мережі дедалі більше впливають на сьогодення. Комунікативні технології мають вирішальне значення для зв'язку між різними суспільними установами й структурами, громадянським суспільством і системами поширення інформації тощо. Розвиток таких технологій займає центральне місце в процесі поширення знань, розвитку освіти, науки та культури. У результаті сьогодні наукові бібліотеки стають інформаційним центром

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

не тільки для наукових і навчальних працівників, а й для більшості населення. В умовах постійного обміну даними, коли інформація стає товаром і коли складно перевірити її на правдивість, саме наукові бібліотеки полегшують і узагальнюють результати інформаційного пошуку. Здійснений аналіз дає змогу дійти висновку, що впровадження інформаційно-мережевих технологій, створення власних електронних ресурсів є необхідним елементом на етапі розвитку обробки знань і їх подальшого розвитку. Новітні електронні технології дали поштовх в процесі зберігання наукових робіт, документів, технічних робіт, електронних носіїв та їх подальшій обробці. Нарешті вони дали змогу розширити кількість користувачів за межами наукових бібліотек.

Метою кваліфікаційної роботи є розробка проєкту ІТ-інфраструктури мережі наукової бібліотеки.

Визначена мета обумовлює наступні завдання:

- Дослідити особливості проєктування інформаційних мереж;
- Окреслити структуру комп'ютерної мережі;
- Вибрати основні технології для втілення проєкту;
- Вибрати апаратне забезпечення для роботи над проєктом;
- Спроекувати мережу наукової бібліотеки;
- Забезпечити захист інформаційної мережі;
- Провести тестування мережі;
- Проаналізувати напрями удосконалення мережі.

Об'єктом дослідження даної кваліфікаційної роботи є розробка мережі наукової бібліотеки.

Предметом дослідження є розробка і побудова мережі наукової бібліотеки.

У процесі виконання кваліфікаційної роботи було розроблено проєкт для полегшеного та прискореного доступу до наукової бібліотеки та швидшого і кращого отримання інформації з застосуванням новітніх інформаційних технологій.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ПЛАНУВАННЯ СТРУКТУРИ МЕРЕЖІ

1.1 Особливості проектування корпоративної мережі

Будь-яка організація складається з менших робочих підрозділів, які виконують певні функції та в свою чергу мають свою структуру. Такі підрозділи функціонально пов'язані між собою, виконують окремі види робіт в рамках єдиного бізнес-проекту, а також інформаційно, обмінюючись документами, факсами, письмовими та усними розпорядженнями й так далі, крім того, ці елементи взаємодіють із зовнішніми системами, причому їх взаємодія також може бути як інформаційною, так і функціональною. Такий опис можна застосувати абсолютно для всіх організацій, незалежно від їх виду діяльності. Це можуть бути банки, промислові об'єкти, урядові організації, комерційні фірми тощо. Такий узагальнений погляд на структуру підприємств допомагає зрозуміти принципи побудови корпоративних комп'ютерних мереж в масштабі всієї організації [26, с. 18].

Корпоративна мережа обслуговує одне велике підприємство і за своїм масштабом повинна забезпечувати безперебійну роботу по всьому підприємству або будівлі в якій розміщена виробнича потужність. Зазвичай побудована на протоколі TCP/IP. Структура корпоративної мережі виглядає наступним чином: є декілька підмереж, можуть бути представлені в якості віртуальних локальних мереж, які обслуговують певний підрозділ, розташований в одному або декількох приміщеннях, які можуть бути на значному віддаленні один від одного; підмережі пов'язані між собою за допомогою серверів доступу; також мають доступ до зовнішньої мережі. В якості серверів доступу можуть використовуватися мости, комутатори, маршрутизатори, шлюзи доступу [29].

При проектуванні корпоративної мережі корисно мати уявлення про неї у вигляді багатоповерхової піраміди. Хоча поверхи цієї піраміди пов'язані та впливають один на інший, зазвичай кожний окремий поверх може проектуватися спеціалістами й фірмами окремо для того, щоб забезпечити автономність роботи окремих сегментів мережі.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

В залежності від напрямку руху в цій піраміді: зверху вниз – від рівня програм до апаратної платформи або знизу вверх – від апаратної складової до програм; всі фірми розробники комп'ютерних мереж можна умовно розділити на три групи.

Перша група – фірми, які займаються розробкою мереж лише з платформ одного-двох виробників апаратного забезпечення. Плюси й мінуси в такому підході розробки очевидні. Неякісна апаратна складова, що призводить до частих поломок і як результат неефективної роботи підприємства [29].

Друга група – фірми, які орієнтуються тільки на одну СУБД або певний програмний додаток для роботи з даними, наприклад розроблений компанією “Oracle” або “Informix”. В такому разі при спробі використання декількох апаратних платформ обмеження будуть диктуватись використаною СУБД [29].

Третя група – фірми, які можуть пропонувати будь-які рішення на всіх рівнях розробки корпоративної мережі і які не мають прив'язки до певної програмної платформи або мережних конфігурацій. У таких розробників єдиним критерієм вибору рішення є досягнення максимального ефекту в межах наявних ресурсів і можливостей. Звісно, мінусом такої розробки є висока вартість послуг, час і обов'язкова наявність кваліфікованих працівників які мають досвід роботи з відповідними додатками та платформами [29].

Як бачимо, є можливість будувати різні конфігурації, які дозволяють достатньо легко розв'язувати проблеми, пов'язані з тим, що клієнт або користувач вже використовує (наприклад певну СУБД) і не бажає здійснювати перекваліфікацію свого персоналу для роботи з іншою базою даних.

При цьому, при проєктуванні будь-якого рівня розробки характеристики інших рівнів, які впливають на прийняття проєктних рішень, беруться у вигляді вихідних даних. Наприклад при проєктуванні програмних утиліт враховується швидкість, яку може забезпечити сучасне комунікаційне обладнання по вартості, яке може забезпечити підприємство. Або ж припустімо, розробники транспорт-

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

ного рівня мережі орієнтуються на середні дані про трафік, який можуть створити наявні на підприємстві програмні додатки і які можуть бути введені в експлуатацію в найближчому майбутньому.

1.2 Етапи проєктування корпоративної мережі

Проєктування корпоративних мереж можна розділити на певні етапи. Аналіз завдань – перед створенням мережі необхідно провести інформаційне обстеження організації або підприємства. Побудова функціональної моделі мережі – за результатами обстеження вибрати архітектуру системи й апаратно-програмні засоби її реалізації. Побудова технічної моделі мережі – за результатами інформаційного обстеження вибрати й розробити ключові компоненти інформаційної мережі. Втім, такий розділ на етапи не є обов’язковим і слугує виключно для гнучкого процесу розробки мережі.

1.3 Аналіз завдань

Аналіз завдань, які стоять перед мережею, насамперед визначається головними завданнями проєкту і пріоритетами, які ставить перед собою розробник такої мережі. Чітке і точне визначення основних задач допоможе уникнути реалізації непотрібних параметрів і виникнення помилок при проєктуванні мережі, що значно зекономить кошти підприємства. Детальний аналіз вимог до мережі є основою для написання якісного технічного завдання на базі якого розробники зможуть розробити проєкт мережі. Нарешті, чітке розуміння цілей проєкт допоможе сформулювати якісну оцінку для тестування розробленої комп’ютерної мережі [30].

На цьому етапі формуються основні цілі підприємства, для якого розробляється проєкт, наприклад скорочення циклу виробництва, більш оперативне обслуговування клієнтів або підвищення продуктивності шляхом більш ефективної взаємодії працівників. Відбувається пошук і детальний аналіз подібних систем, які застосовуються на подібних підприємствах або фірмах, аналізуються їх сильні й слабкі сторони, збирається весь необхідний досвід для успішного проєктування системи.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Для виконання аналізу вимог до корпоративної мережі необхідно:

- Оцінити поточний стан локальних мереж і робочих станцій на підприємстві, що допоможе виявити, які проблеми потребують вирішення;
- Визначити цілі та переваги від майбутньої корпоративної мережі, що допоможе правильно її спроектувати;
- Оцінити необхідність оновлення застарілого обладнання;
- Зробити закупівлю нового обладнання, якщо це необхідно, виходячи з можливостей розробника і клієнта;
- Написати ефективне технічне завдання;
- Описати критерії для оцінювання якості майбутньої мережі.

1.4 Побудова функціональної моделі мережі

Мережа виробництва призначена для того, щоб виконувати виконавчі функції, тому необхідно оцінити її роль у всій структурі підприємства. Для успішної побудови корпоративної мережі потрібно насамперед побудувати функціональну модель, із якої можна потім отримати технічну і фізичну модель мережі.

Така модель описує ділові процедури, послідовність і взаємозв'язок всіх робіт на підприємстві. Звісно, вся увага в ході написання цього дипломного проекту буде концентруватись саме на комп'ютерній системі, але для дохідливого розуміння роботи мережі наукової бібліотеки необхідно розглянути також таку модель.

Архітектура комп'ютерних програм і платформ грає ключову роль у діловій архітектурі підприємства. Всі фірми базуються на швидкості й зручності управління даними на програмах і архітектурі мереж. Саме тому, успішний аналіз вимог і успішна побудова корпоративної мережі потребують від технічного спеціаліста також навичок бізнесмена [30].

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

1.5 Побудова технічної моделі мережі

Після розробки функціональної моделі мережі і визначення того, які процедури і параметри потребують оновлення або змін, необхідно побудувати технічну модель мережі. Технічна модель докладно описує, яке комп'ютерне обладнання потрібно використовувати для досягнення цілей описаних у функціональній моделі. Для того, щоб побудувати технічну модель потрібно проаналізувати наявне устаткування, визначити системні вимоги, оцінити теперішній і спрогнозувати майбутній стан техніки.

Розробник також повинен забезпечити необхідний набір функцій і необхідний час доступу до мережі. Наприклад, якщо мережа повинна бути доступна вночі і в будні дні, то у відповідних налаштуваннях параметрів необхідно мати додаткові диски пам'яті і джерела безперебійного струму. Необхідно вирішити достатньо наявних дискових ресурсів чи необхідний додатковий дисковий масив [29].

Далі потрібно визначити, які технології будуть залучені в проєкт мережі. Потрібно визначити перспективи застосування таких технологій, як довго вони будуть залишатись актуальними, надавати перевагу платформам і технологіям які мають постійну технічну підтримку. Необхідно оцінити, чи зможе наявна мережа пристосуватись до майбутніх технологічних новинок.

Після того, як вибрана технічна модель, яка описує мережу в загальних параметрах, створюється фізична модель, яка містить чіткий опис певних апаратних продуктів, їх кількості, технічних параметрів і способів їх взаємодії.

Встановлення і налаштування системи. Даний етап являє собою координацію постачання апаратних складових, управління конфігуруванням, налаштування обладнання, навчання персоналу (якщо це необхідно).

Тестування комп'ютерної мережі. На цьому етапі проводяться тестування конфігурації проєкту.

Експлуатація створеної мережі. Цей етап не має чітко визначених часових рамок, являє собою безперервний процес. Можна додати, що хоча процес є без-

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

перервним, але так чи інакше буде відбуватися зміна персоналу, саме тому необхідно мати чітку фізичну і технічну модель комп'ютерної мережі для більш гнучкої роботи.

1.6 Інформаційні потоки у мережі бібліотеки

Розглянемо організаційну структуру підрозділів наукової бібліотеки. На чолі бібліотеки стоїть організаційний відділ, яким керує директор. До складу бібліотеки входять серверний відділ і п'ять окремих відділів: відділ комплектування, наукової обробки документів і організації каталогів; інформаційно-бібліографічний; відділ інформаційних технологій та комп'ютерного забезпечення; відділ обслуговування навчальною літературою; відділ обслуговування науковою та художньою літературою. Крім цього в структурі бібліотеки є п'ять філій, які знаходяться у різних навчальних корпусах.

Кожний з вищезгаданих підрозділів і філій знаходяться у підпорядкуванні згідно з рисунком 1.1. Серверний відділ надає інформаційну і технічну підтримку підрозділам бібліотеки.

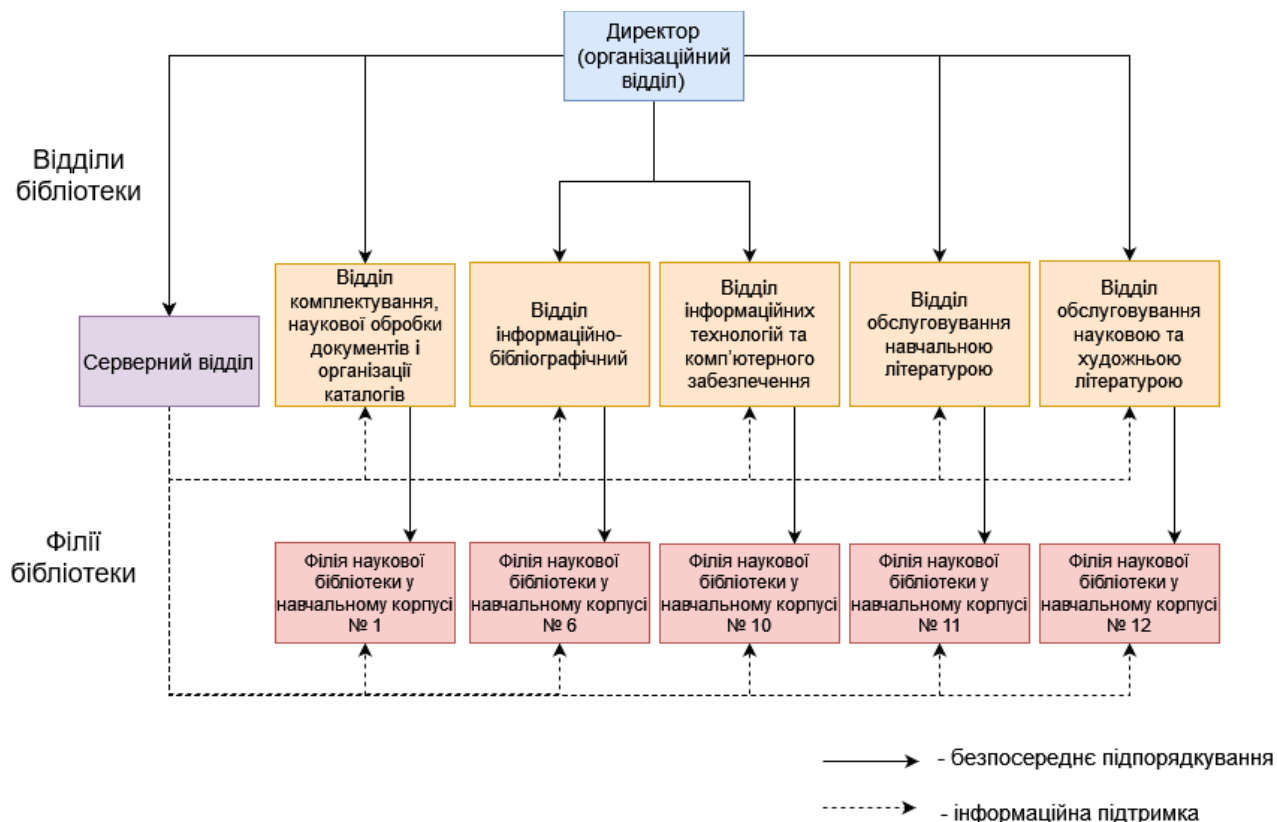


Рисунок 1.1 – Організаційна структура наукової бібліотеки

Таким чином, було детально розглянуто організаційну структуру наукової бібліотеки. Організаційна структура бібліотеки складається з організаційного апарату, серверного відділу, п'яти окремих відділів і п'яти бібліотечних філій для роботи бібліотечного персоналу. Беручи до уваги вищезгадане, дана структура бібліотеки не є принциповою і може змінюватись відповідно до вимог організації. Наприклад, у майбутньому може збільшитись кількість відділів або філій бібліотеки, з'явитися декілька організаційних відділів тощо.

1.7 Основні технології та протоколи

1.7.1 Технологія VLAN

Однією з надважливих функцій, що реалізуються в технології Ethernet, є технологія віртуальних локальних мереж (VLAN). Для об'єднання кінцевих пристроїв і серверів мережі ця технологія використовує комутатори. Зв'язок комп'ютерів, що належать до однієї VLAN, можливий тільки з пристроями цієї ж мережі, тому мережа функціонує як декілька індивідуальних, не з'єднаних одна з одною локальних мереж LAN. Різні виробники мають різні підходи до створення таких мереж, тому важко дати загальне визначення мережі VLAN [3]. На рисунку 1.2 показано приклад мережі VLAN, яка складається з чотирьох робочих станцій і двох комутаторів.

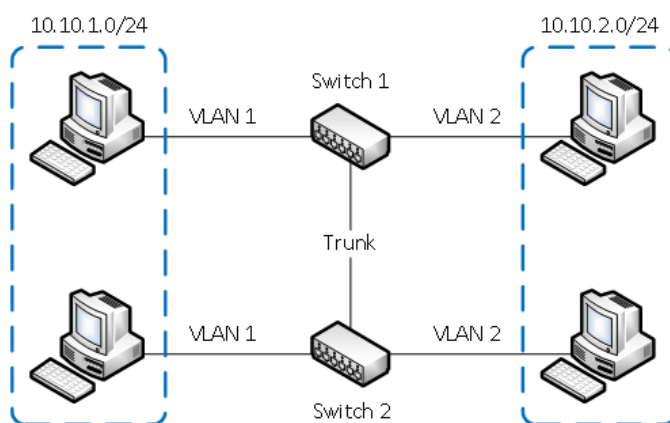


Рисунок 1.2 - Мережа VLAN

Віртуальною локальною мережею (Virtual Local Area Network, VLAN) називається група вузлів мережі трафік якої, зокрема широкомовний, на каналному рівні повністю ізольований від трафіку інших вузлів мережі.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

До появи VLAN для створення окремої мережі використовувались фізично ізольовані сегменти коаксіального кабелю або не пов'язані між собою сегменти побудовані на застарілих повторювачах і мостах. Потім ці мережі пов'язувались маршрутизаторами в єдину мережу. Така структура мережі створює бар'єри на шляху небажаного трафіку із однієї мережі в іншу. Будь-яка зміна сегментів мережі спричиняє зміни у налаштуваннях мережних пристроїв, що є надзвичайно незручним у великих мережах – це потребує великих затрат часу і може спричинити багато помилок у конфігуруванні мережі. Саме тому перевагою технології віртуальних мереж є те, що вона дозволяє створювати повністю ізольовані сегменти мережі шляхом логічного конфігурування комутаторів, не вдаючись до зміни фізичної структури [3].

Також існує можливість більш гнучкого об'єднання користувачів у групи (наприклад, по відділах) замість фізичного розподілу за місцеперебування.

Спрощення пошуку проблеми в мережі, оскільки більшість проблем локалізуються саме в одній області пристроїв.

На рис. 1.3 приведений приклад проєктування мережі VLAN у фізичній мережі. В цьому випадку створюються три мережі VLAN, в яких робочі станції сполучені одна з одною через комутатори, а самі комутатори сполучені один з одним через маршрутизатор [30].

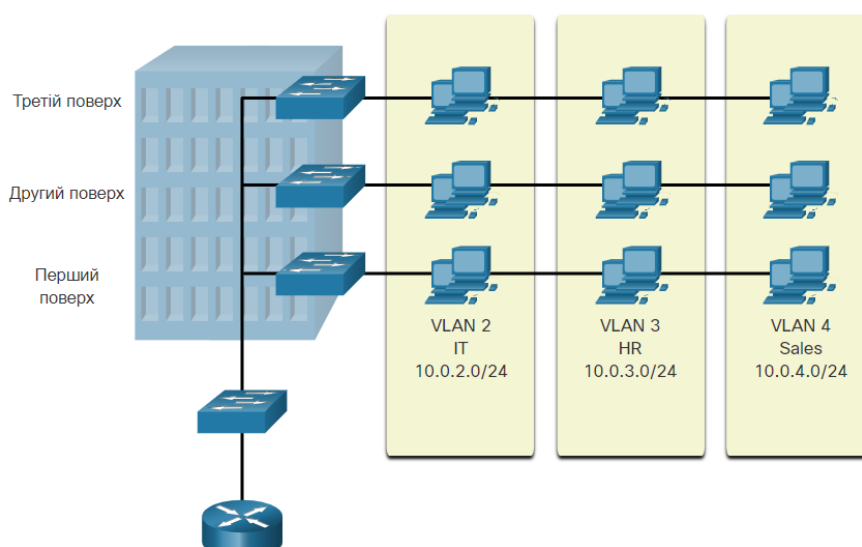


Рисунок 1.3 – Приклад проєктування віртуальної локальної мережі

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

1.7.2 Протокол IPv4

В кожній мережі, яка лежить на шляху розподілу пакетів, протокол IP звертається до транспортних засобів цієї мережі для передачі пакета даних на маршрутизатор, який веде до наступної мережі або на вузол-адресат. Підтримка інтерфейсів з відповідними технологіями підмереж є однією з важливих функцій протоколу IP. В ці функції також входить підтримка інтерфейсів з протоколами транспортного рівня, зокрема протоколами TCP, який забезпечує надійну доставку даних мережею TCP/IP [9].

Протокол IP підтримує обробку кожного пакету як незалежної одиниці обміну, яка не пов'язана з іншими пакетами. В протоколі IP немає механізмів для забезпечення безперебійної доставки даних. Якщо під час транспортування пакета відбувається помилка, то протокол IP нічого не зробить для її виправлення. Наприклад, якщо на проміжному маршрутизаторі пакет був відхилений через помилку, то модуль IP не намагається заново послати втрачений пакет даних. Тобто протокол реалізує доставку пакетів даних «по можливості».

Є прямий зв'язок між кількістю полів заголовка пакета і складністю протоколу, який працює з цим заголовком. Чим простіший заголовок, тим простіший відповідний протокол. Більша частина дій протоколу пов'язана саме з обробкою службової інформації, яка переноситься в полях заголовка пакета.

Поле номера версії займає 4 біти, що характеризує версію протоколу IP. Зараз широко використовується версія IPv4, хоча все частіше зустрічається і нова версія IPv6. Значення довжини заголовка IP-пакета також займає 4 біти. Зазвичай заголовок має довжину у 20 байтів, але при додаванні службової інформації це значення збільшується шляхом додаткових байтів в полі параметрів [9].

Система адресації IPv6 внесла значні зміни в протокол IP. Насамперед збільшилась розрядність адреси. Замість 4 байт версії IPv4 у новій версії під адресу відведено 16 байтів, що дає можливість пронумерувати надзвичайно велику кількість вузлів мережі. Головною метою зміни системи адресації було не механічне збільшення адресного простору, а збільшення ефективності роботи стека TCP/IP в цілому.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

1.7.3 Протокол OSPF

Протокол OSPF (Open Shortest Path First) заснований на алгоритмі вибору найкоротшого шляху для пакетів даних, які передаються мережею. OSPF розбиває процедуру побудови таблиці маршрутизації на два етапи [8].

Перший етап включає побудову і підтримку бази даних про стан зв'язку у мережі. Зв'язок у мережі може бути представлений у вигляді графа, в якому вершинами є маршрутизатори і підмережі, а ребрами – зв'язки між ними. Кожний маршрутизатор обмінюється зі своїми сусідами тією інформацією про структуру мережі до якої він має доступ. Для контролю за станом топології мережі маршрутизатори, на яких налаштований протокол OSPF передають один одному особливі сповіщення HELLO кожні 10 секунд. Невеликий об'єм таких повідомлень дозволяє часте тестування стану сусідів і зв'язку з ними [8]. Якщо повідомлення перестають поступати від якогось пристрою, то маршрутизатор робить відповідний висновок про стан роботи зв'язку в мережі, після чого вносить зміни у свою топологію мережі. Одночасно він розсилає повідомлення LSA про відповідні зміни у мережі навколишнім пристроям, які також вносять зміни у свої бази даних і своєю чергою теж розсилають повідомлення LSA своїм сусідам у мережі.

Другий етап включає знаходження оптимальних маршрутів і генерації таблиці маршрутизації. Задача знаходження оптимального шляху є достатньо складною. В протоколі OSPF для розв'язання цієї задачі використовується алгоритм Дейкстри, який знаходить найкоротший шлях від однієї вершини графу до всіх інших вершин. Тобто кожний маршрутизатор мережі шукає оптимальні маршрути від своїх інтерфейсів до всіх відомих йому підмереж. В кожному знайденому таким чином маршруті зберігається тільки один крок – до наступного маршрутизатора. Дані про цей крок потрапляють в таблицю маршрутизації.

Якщо стан зв'язку в мережі змінився і відбулося коригування графа мережі, то кожний маршрутизатор знову шукає оптимальні маршрути і коригує свою таблицю маршрутизації. Аналогічний процес відбувається і в тому випадку, коли в мережі з'являється новий зв'язок або новий пристрій, який повідомляє про себе

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

за допомогою розсилки повідомлень HELLO. При роботі протоколу OSPF побудова таблиць маршрутизації до нового узгодженого стану відбувається швидше, ніж у мережах, які працюють на дистанційно-векторних протоколах (RIP, IGRP, BGP, EIGRP). Цей час складається з часу розповсюдження через мережу оголошення LSA та часу роботи алгоритму Дейкстри. Проте обчислювальна складність цього алгоритму висуває високі вимоги до потужності процесорів маршрутизаторів. Якщо ж стан мережі не змінюється, то оголошення про зв'язки не генеруються, топологічні бази даних та таблиці маршрутизації не коригуються, що заощаджує пропускну спроможність мережі та обчислювальні ресурси маршрутизаторів. Однак у цього правила є виняток: кожні 30 хвилин маршрутизатори OSPF обмінюються всіма записами бази даних топологічної інформації, тобто синхронізують їх для надійнішої роботи мережі. Оскільки цей період досить великий, то цей виняток анітрохи не позначається на завантаженні мережі.

При пошуку оптимальних маршрутів протокол OSPF за замовчуванням використовує метрику, яка враховує пропускну спроможність каналів зв'язку. Крім того, допускається застосування двох інших метрик для врахування затримки та надійності передачі пакетів каналами зв'язку. Для кожної з метрик протокол OSPF будує окрему таблицю маршрутизації [16, с. 364].

1.7.4 Протокол LACP

LACP (Link Aggregation Control Protocol) – протокол управління агрегацією ліній зв'язку у мережі. Протокол LACP виконує дві основні функції: створення групи портів LAG (link aggregation group) і постійний моніторинг стану портів і ліній зв'язку, які входять у групу LAG [12].

Ці функції взаємопов'язані: якщо в результаті моніторингу з'ясовується, що порт або лінія зв'язку стали непрацездатними, склад групи LAG може динамічно змінитися, порт, який не відповідає або вийшов з ладу, з неї видаляється, а новий додається. Для виконання цих функцій вузли постійно обмінюються повідомленнями протоколу LACP. Протокол LACP вузла може перебувати у двох станах - активному, коли він періодично генерує повідомлення LACP, і пасивному, коли

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

він тільки приймає повідомлення LACP від активного сусіда [6]. Обидва з'єднанні між собою вузла мережі можуть знаходитись і в активному стані, але якщо вони обидва знаходяться у пасивному стані, то сесія LACP просто не буде відбуватись. Стан LACP вузла конфігурується адміністратором. Для об'єднання кількох фізичних портів протоколом LACP в одну групу LAG має бути виконано кілька умов:

- порти повинні підтримувати одну й ту саму швидкість, наприклад, порт 1 Гбіт/с та порт 10 Гбіт/с об'єднати не можна;
- порти повинні працювати у режимі full-duplex;
- кількість портів, що об'єднуються, не повинна перевищувати максимальну кількість портів для груп LAG даного вузла.

1.7.5 Протокол PVST

Протокол STP, призначений для видалення петель комутації, був розроблений достатньо давно [4]. На той час технології, які пізніше будуть впроваджені у мережевих пристроях, зокрема комутаторах, ще не були розроблені. Це стосується і технологій агрегації каналів та VLAN. Розробка і впровадження високошвидкісних технологій, орієнтованих на використання високопродуктивних комутаторів, та досвід експлуатації класичного протоколу STP показали, що закладені часові та інші параметри роботи протоколу не задовольняють сучасні умови. Це призвело до розробки покращених протоколів на базі STP. Класичний протокол STP та його модифікація RSTP були орієнтовані на використання у мережі, яка не розділяється на VLAN. Фірмою Cisco були розроблені фірмові модифікації згаданих протоколів, такі як PVST/PVST+/RPVST+, для використання у мережі, яка може розділятися на декілька VLAN [4].

PVST (Per-VLAN Spanning Tree) - протокол Cisco Systems, який для кожного VLAN будує окреме дерево. Він передбачає використання ISL (Inter Switch Link) для створення транків і дозволяє порту бути заблокованим для одних VLAN та розблокованим для інших.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

PVST+ (Per-VLAN Spanning Tree Plus) - протокол компанії Cisco Systems з функціональністю аналогічною PVST. Однак замість протоколу ISL він використовує відкритий стандарт 802.1Q. Розрізняють два види протоколу PVST+: PVST+ - заснований на протоколі STP, з деякими удосконаленнями та протокол Rapid PVST+ – заснований на протоколі RSTP з деякими удосконаленнями [5].

1.7.6 Протокол HSRP

Протокол HSRP (Hot Standby Router Protocol) є одним із перших протоколів динамічного резервування шлюзу, що розроблений у 1997 році фірмою Cisco Systems Inc. для широкомовних мереж із множинним доступом до середовища передачі даних [2].

Протокол HSRP працює відповідно до моделі активний/резервний (або активний/пасивний). Протокол HSRP дозволяє взаємодіяти двом або більше маршрутизаторам, виступаючи у ролі єдиного стандартного маршрутизатора. Але у кожний конкретний момент лише один маршрутизатор активно підтримує трафік кінцевого користувача. Пакети, надіслані мережними пристроями на стандартний маршрутизатор, надходять на цей активний маршрутизатор. Інші маршрутизатори, що перебувають у стані очікування (HSRP Standby), чекають, поки відмовить активний маршрутизатор HSRP, і вони почнуть працювати.

Щоб протокол HSRP належно працював, на кожному маршрутизаторі слід виконати деякі дії. Обидва маршрутизатори потребують налаштування конфігурації HSRP, включаючи віртуальну IP-адресу. Щоб провести переговори та вирішити, який маршрутизатор зараз має бути активним, а який резервним, маршрутизатори обмінюються повідомленнями HSRP. Маршрутизатори продовжують обмінюватись повідомленнями, щоб резервний маршрутизатор міг дізнатися про відмову поточного активного маршрутизатора і замінити його [2].

Протокол HSRP забезпечує балансування навантаження на мережу внаслідок переваги різних маршрутизаторів як активних в різних підмережах. Про-

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

токол HSRP може бути налаштований так, щоб в одній мережі VLAN переважним на роль активного був один маршрутизатор, а в іншій мережі VLAN - інший маршрутизатор, який балансує трафік.

1.7.7 Технологія VPN

Віртуальні приватні мережі (Virtual Private Network) використовуються у всьому світі, щоб забезпечити зашифровані підключення до Інтернету. Це надає можливість користуватися мережею Інтернет з підвищеною конфіденційністю. До цього VPN може замінити справжню IP-адресу на іншу з іншого регіону, що дозволяє отримувати інформацію, доступ до якої раніше був заблокований [18].

Сервіси VPN використовують різноманітні мережеві протоколи. Старіші протоколи, такі як PPP і PPTP, вважаються менш безпечними. Ось деякі з типів протоколів безпеки [28].

IP Security (IP Sec). Популярний протокол, який захищає дані на транспортному рівні. Він вважається дуже безпечним і якісним для захисту вхідного та вихідного трафіку. Але для нього потрібно багато процесорної потужності, що може вплинути на продуктивність пристрою. Крім того, деякі алгоритми безпеки, використовувані в IPSec в минулому, були зламані кіберзлочинцями. Нові версії IPSec використовують складніші алгоритми захисту.

Layer 2 Tunneling Protocol (L2TP)/IPSec. L2TP – це протокол VPN, який сам по собі не шифрує дані. Ось чому він працює в парі з шифруванням IPSec. Одна з його основних переваг – доступність на більшості пристроїв та операційних систем. Має високий рівень безпеки. З мінусів, протокол використовує процес подвійної інкапсуляції, що може призвести до сповільнення з'єднання.

Secure Sockets Layer (SSL) та Transport Layer Security (TLS). SSL був протоколом шифрування VPN, який зазвичай використовувався до 2015 року. Він перетворився на TLS для шифрування даних, які передаються на сервер SSL VPN. Однією з причин того, що SSL був значною мірою замінений у VPN, є велика кількість вразливостей, виявлених у протоколі.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Point-to-Point Tunneling Protocol (PPTP). PPTP був найпершим із протоколів безпеки й вперше випущений у Windows 95. Він швидкий тому, що протокол забезпечує низький рівень шифрування.

Secure Shell (SSH). Протокол SSH широко використовується для зашифрованого підключення. Легко налаштовується, навіть користувачами без відповідного досвіду.

Secure Socket Tunneling Protocol (SSTP). Цей розроблений Microsoft протокол вважається надзвичайно безпечним і простим у використанні, але він не працює на інших платформах, крім Windows.

Internet Key Exchange, Version 2 (IKEv2). Цей протокол заснований на IPSec. Вважається досить безпечним і швидким. Один мінус – його можуть заблокувати брандмауери.

Open VPN. Це, мабуть, найпопулярніший наразі протокол VPN. Він поєднує в собі високу безпеку і швидкість. Оскільки він має відкритий вихідний код, численна спільнота продовжує підтримувати та оновлювати протокол [28].

Отже, VPN потрібний у корпоративній мережі, щоб підвищити безпеку вашої особистої інформації та конфіденційності в Інтернеті. Крім того, існують інші ризики для безпеки мережі. Наприклад, доступ до інформації співробітників може бути скомпрометований у разі порушення даних. Злочинці можуть використовувати відкриту інформацію для створення фішингових електронних листів. Якщо ви відкриєте один з цих підроблених листів, вся мережа компанії може стати жертвою атаки програм-вимагачів. Так, у 2015-2016 роках в Україні були знайдені віруси, що замасковані під програми-вимагачі. Їх виявили у системах, які належать українській владі, та організаціях, які виконують важливі функції виконавчої влади. Крім того, жертвою таких атак стали фірми, що керують сайтами державних установ та державні банки.

Деякі пропонувані на ринку програми VPN можуть сповільнювати роботу вашого інтернет-з'єднання. Це може статися, якщо сервери VPN територіально віддалені. Для кращої продуктивності необхідно вибирати VPN сервери, розта-

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

шовані ближче до вашого місцеперебування. Звісно, деякі рішення лише тимчасово можуть покращувати роботу такої технології, але ніяк не розв'язувати проблеми у масштабі цілої фірми або організації. Тому для кращої працездатності існує ціла низка платних сервісів VPN саме для корпоративного використання [18].

Висновки з першого розділу

Отже, в першому розділі було описано процес обміну інформацією в організаціях, суть якого буде пізніше втілено у розробці мережі наукової бібліотеки. Було широко розкрито поняття корпоративної мережі, з чого вона складається, для чого потрібна, переваги використання у повсякденній роботі. Таким чином, було встановлено основні етапи проектування корпоративної мережі: аналіз завдань, побудова функціональної моделі мережі, побудова технічної моделі мережі. Отримані результати свідчать про важливість побудови правильної архітектури комп'ютерної мережі, яка забезпечить достатню швидкість і зручність управління. Така структура повинна забезпечувати послідовність і взаємозв'язок між всіма структурними підрозділами на підприємстві або організації. У результаті успішного планування комп'ютерної мережі дозволить успішне розширення і її модернізацію. Дозволить зменшити або виключити помилки при роботі організації у майбутньому.

Також у першому розділі було детально розглянуто організаційну структуру наукової бібліотеки. Організаційна структура бібліотеки складається з організаційного апарату, серверного відділу і п'яти окремих відділів для роботи бібліотечного персоналу. Структура бібліотеки може змінюватись відповідно до вимог організації. Наприклад, у майбутньому може збільшитись кількість відділів або філій бібліотеки, з'явитися декілька організаційних відділів тощо.

Здійснений аналіз дає змогу дійти висновку які саме основні технології й мережеві протоколи необхідні для успішного втілення спроектованої нами мережі. Технологія VLAN для гнучкої організації мережі і її робочих станцій, серверу.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

Також було проаналізовано протокол динамічної маршрутизації OSPF. Протокол який працює на технології відстеження стану каналу. Після аналізу особливостей роботи протоколу зроблено висновок, що при роботі протоколу OSPF побудова таблиць маршрутизації відбувається швидше, ніж у мережах, які працюють на дистанційно-векторних протоколах (RIP, IGRP, BGP, EIGRP).

Для агрегації каналів вибрали протокол LACP. Для видалення петель комутації вибрали мережевий протокол PVST, який кращий ніж попередні протоколи, розроблені на базі протоколу STP. Протокол динамічного резервування шлюзу HSRP. Нарешті розглянули доцільність реалізації VPN, її переваги та недоліки, які види технологій VPN існують на ринку. Для реалізації в кваліфікаційній роботі вибрали OpenVPN через його масовість і доступність документації.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТУВАННЯ МЕРЕЖІ

2.1 Управління мережею

Локальна комп'ютерна мережа (Local Area Network) – це декілька комп'ютерів в межах однієї території (знаходяться в одному приміщенні або декількох близько розташованих споруд) та під'єднаних до єдиної лінії зв'язку. На сьогодні більшість комп'ютерних мереж – це локальні комп'ютерні мережі, які розміщуються всередині тільки однієї будівлі фірми і засновані на комп'ютерній моделі клієнт-сервер. Мережне з'єднання складається з двох комп'ютерів і шляху між ними. Також можна створити мережу, використовуючи безпроводні технології [16, с. 25].

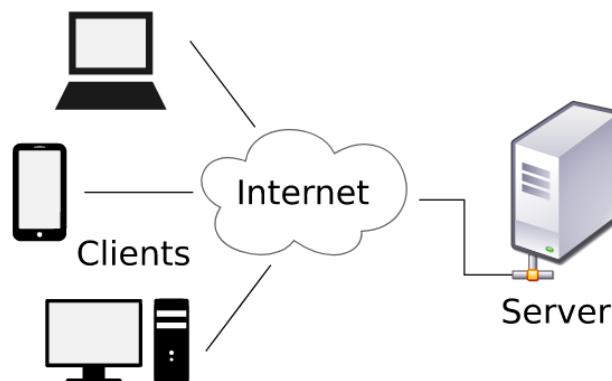


Рисунок 2.1 – Модель клієнт-сервер

Архітектура клієнт-сервер є одним з архітектурних шаблонів програмного забезпечення та є панівною концепцією у створенні розподілених мережних застосунків і передбачає взаємодію та обмін даними між ними. В моделі клієнт-сервер зв'язок в мережі ділиться на дві області – сторону клієнта і сторону сервера. При цьому клієнт робить запит на інформацію із сервера. Сервер своєю чергою виконує запити клієнта.

Найчастіше кожна сторона в такій моделі може виконувати функції як сервера, так і клієнта. Сервери є незалежними один від одного. Клієнти також функціонують паралельно і незалежно один від одного. Немає жорсткої прив'язки клієнтів до серверів. Більш ніж типовою є ситуація, коли один сервер одночасно обробляє запити від різних клієнтів. При створенні комп'ютерної мережі наукової бібліотеки потрібно насамперед вибрати різні компоненти, що

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

визначають яке саме програмне забезпечення й обладнання можна використати при побудові корпоративної мережі.

Кожна організація формує власні потреби до конфігурації мережі, які визначаються характером її потреб для розв'язання певних завдань. У першу чергу необхідно визначити, яка кількість працівників буде залучена у розробці проекту і подальшій експлуатації мережі, її технічній підтримці. Від цього насправді будуть залежати всі наступні етапи створення мережі.

Кількість робочих станцій, які будуть введені в експлуатацію у корпоративній мережі, буде напряду залежати від кількості співробітників. Другим фактором є ієрархія, яка існує в структурі організації. У випадку бібліотеки це директор і організаційний відділ, голови підлеглих відділів і філій та весь інший персонал з різним рівнем доступу. Для невеликої фірми з горизонтальною структурою, де всі співробітники мають доступ до даних один одного, оптимальним і найдешевшим рішенням є проста однорангова мережа. Однак для організації, яка оперує великою кількістю інформації та побудованій на вертикальній структурі із суворою ієрархією, де точно відомо, який рівень доступу має бути встановлено для кожного співробітника, слід орієнтуватись на дорожчий варіант мережі – з виділеним сервером. Тому тільки в такій мережі існує можливість адміністрування прав доступу. Згідно з організаційною структурою проєктованої мережі, цю роль займає серверний відділ бібліотеки.

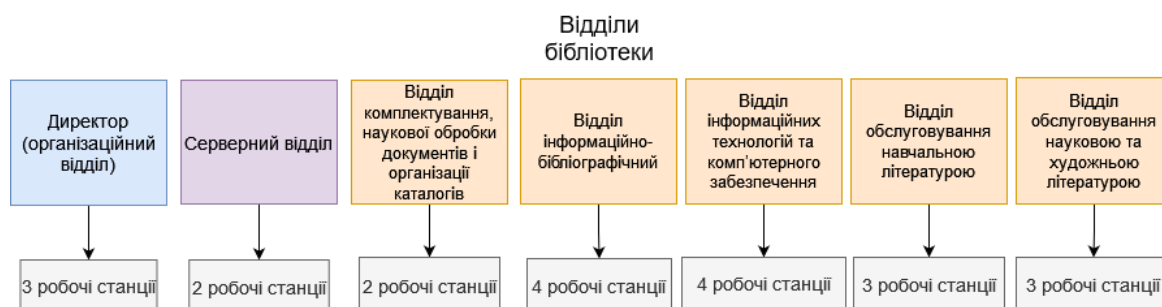


Рисунок 2.2 – кількість робочих станцій

В цьому випадку у бібліотеці є двадцять робочих станцій, які потрібно об'єднати у корпоративну мережу. Причому вони об'єднані в наступні групи:

- Директор і організаційний відділ бібліотеки – 3 робочі станції
- Серверний відділ – 2 робочі станції

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

- Відділ комплектування – 2 робочі станції
- Відділ інформаційно-бібліографічний – 4 робочі станції
- Відділ інформаційних технологій – 4 робочі станції
- Відділ навчальної літератури – 3 робочі станції
- Відділ наукової та художньої літератури — 3 робочі станції

Одним з головних етапів планування є створення попередньої схеми корпоративної мережі. При цьому залежно від типу мережі виникає питання обмеження довжини кабельного сегмента. Це може бути несуттєвим для невеликого офісу фірми, однак якщо мережа охоплює декілька поверхів будівлі, може постати така проблема. У проєктованій мережі бібліотеки різні відділи знаходяться на одному поверсі, але інші філії можуть знаходитись на різних поверхах або навіть в іншій будівлі, що збільшує вартість кабельного оснащення.

Розглянувши методи управління мережею, перейдемо до установки сервера, оскільки при вертикальній структурі мережі необхідно мати розмежований доступ до інформації.

2.2 Розміщення сервера

На відміну від налаштування однорангової мережі, при проєктуванні мережі з сервером виникає питання його доцільного розміщення.

На вибір місця розміщення сервера впливає декілька факторів:

- Через високий рівень шуму сервер бажано установити окремо від решти робочих станцій;
- Необхідно забезпечити постійний доступ до сервера для технічного обслуговування;
- Забезпечити безпечний рівень вологості для електроніки серверного відділу;
- Якщо у структурній моделі передбачено декілька серверних шаф, то необхідно забезпечити потрібну температуру у приміщенні;
- Для захисту інформації на сервері необхідно обмежити доступ до нього і до приміщення, в якому він розміщений.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Сервер розташований у серверному відділі бібліотеки (позначений цифрою 3 на рис. 2.3) тому, що тільки це приміщення задовольняє необхідні потреби. Тобто рівень шуму в приміщенні мінімальний, тому що серверна кімната розташована якомога далі від інших відділів бібліотеки. Іноді для зниження шуму використовують шумоізоляцію, але цей варіант є дорогим і більше притаманний великим обчислювальним центрам.

Приміщення ізольоване від інших і перебуває під охороною. Отже, доступ до сервера буде обмеженим. Серверний відділ захищений фізично – має двері та немає доступу ззовні.

Системний адміністратор зможе безперебійно слідкувати за роботою серверу і здійснювати обслуговування сервера, як при вводі в експлуатацію сервера. Доступність є необхідною складовою гнучкої мережі.

Для забезпечення безпечного рівня вологості при побудові серверної кімнати можна використати вологоізоляційні матеріали й компоненти.

В разі, якщо в майбутньому буде розширення мережі та знадобляться додаткові серверні шафи, то для забезпечення необхідної температури знадобиться контролер температури та кондиціонери.

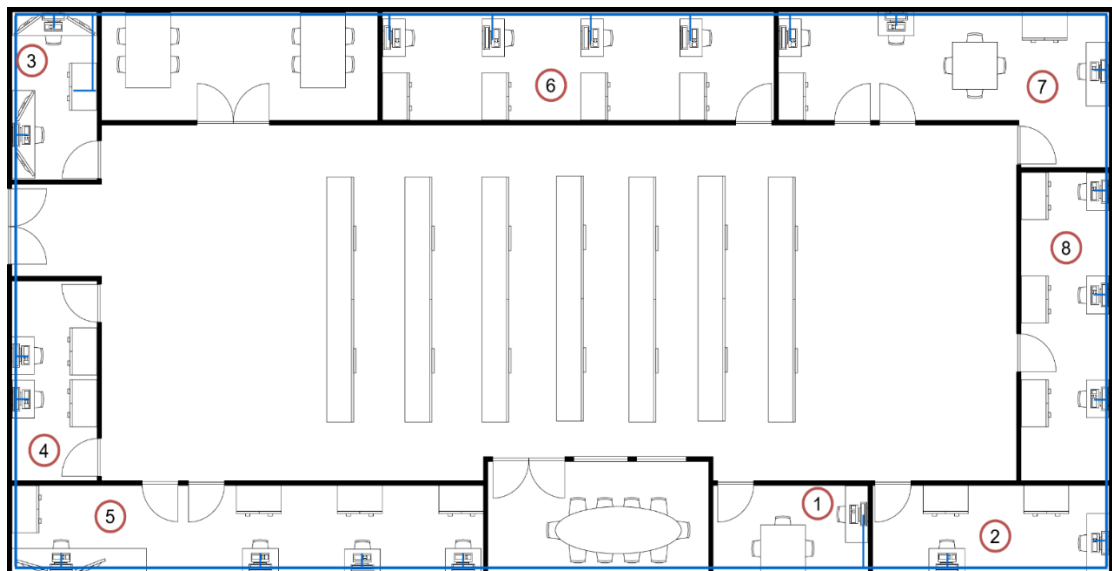


Рисунок 2.3 – структурний план приміщення

На структурному плані приміщення (рис. 2.3) відділи бібліотеки пронумеровані наступним чином:

1. Директор;
2. Організаційний відділ;
3. Серверний відділ;
4. Відділ комплектування, наукової обробки документів і організації каталогів;
5. Інформаційно – бібліографічний відділ;
6. Відділ інформаційних технологій та комп'ютерного забезпечення;
7. Відділ обслуговування навчальною літературою;
8. Відділ обслуговування науковою та художньою літературою.

2.3 Мережева архітектура

Мережева архітектура – це сукупність топології, методу доступу і стандартів необхідних для створення працездатної мережі.

Вибір топології визначається зокрема планом приміщення, в якому проєктується робоча мережа. Крім того, велике значення мають затрати на покупку і налаштування мережевого обладнання, що є надважливим питанням для організації, оскільки від різної мережевої архітектури змінюється вартість обладнання.

Топологія типу «зірка» являє собою структуру, де кожна робоча станція з'єднані окремим сегментом кабелю з центральним концентратором. Найчастіше використовується в корпоративних і домашніх мережах. Основною перевагою такої топології є її стійкість, оскільки через пошкодження одного кабелю вийти з ладу може тільки одна робоча станція. Також така топологія є легкою в установці, керуванні й усуненні неполадок. З іншої сторони, в разі пошкодження центрального пристрою – вся мережа втрачає працездатність.

Ще однією перевагою даної архітектури є простота розширення мережі, оскільки при використанні додаткових комутаторів з'являється можливість підключення великої кількості робочих станцій.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

2.4 Мережеві ресурси

Наступним важливим аспектом планування мережі є спільне використання мережевих ресурсів (принтерів, модемів, факсів).

Перелічені ресурси можуть застосовуватись як в однорангових, так і в мережах з виділеним сервером. Однак у випадку однорангової мережі одразу виявляються її недоліки. Щоб працювати з такими компонентами, їх необхідно спочатку встановити на робочу станцію, налаштувати драйвери, програмне забезпечення, провести діагностику роботи. При вимкненні цієї станції всі компоненти й відповідні служби та налаштування стануть недоступні для колективного використання.

Тимчасом як в мережах з сервером такий комп'ютер існує заздалегідь. Мережевий сервер ніколи не вимикається, крім коротких перерв для технічного обслуговування або діагностики. Таким чином забезпечується щоденний доступ робочих станцій до мережевої периферії.

Для злагодженої роботи бібліотеки наявно два принтери для організаційного відділу і по одному на кожний з п'яти відділів наукової бібліотеки. Така кількість необхідна для мінімально комфортних умов роботи колективу.

Тепер виникає питання підключення принтерів до корпоративної мережі. Для цього існує декілька способів.

Перший, підключення до робочої станції, яка знаходиться до нього найближче, в результаті чого вибрана станція стає сервером для друку. Недолік такого способу в тому, що при виконанні завдань на друк продуктивність робочої станції знижується, що негативно вплине на роботу прикладних програм при інтенсивному використанні принтерів. Крім цього, якщо машина буде вимкнена або вийде з ладу, сервер друку стане недоступним для інших вузлів мережі.

Другий спосіб, пряме підключення до сервера. Принтер підключається до порту сервера за допомогою спеціального кабелю. В такому випадку він постійно доступний для всіх робочих станцій мережі. Недолік такого рішення обумовлений обмеженням в довжині принтерного кабелю, який забезпечує передачу даних. Звісно кабель можна протягнути на відстань десять і більше метрів,

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

але його необхідно прокладати в спеціальних перекриттях, що значно підвищить витрати на організацію мережі.

Третій спосіб, підключення до мережі через спеціальний мережевий інтерфейс. Принтер налаштовується з мережевим інтерфейсом і під'єднується до мережі як робоча станція. Інтерфейс в такому випадку працює як мережевий адаптер, а принтер реєструється на сервері як вузол корпоративної мережі. Програмне забезпечення сервера виконує передачу даних для друку через мережу напряду на під'єднаний мережевий принтер.

Четвертий спосіб, підключення до виділеного сервера друку. Альтернативою третьому варіанту є використання спеціалізованих серверів друку. Такий сервер є мережевим інтерфейсом, скомпонованим в окремому корпусі, з одним або декількома роз'ємами (портами) для підключення принтерів. Однак у цьому випадку використання сервера друку є непрактичним.

У нашому випадку у зв'язку з нерентабельністю установки спеціального мережного принтера або покупкою окремої мережевої картки для принтера, найкращим способом під'єднання принтера є підключення до робочої станції. На це рішення вплинув ще й той факт, що принтери згідно зі структурним плану бібліотеки, розташовані біля тих робочих станцій, потреба яких у принтері є найбільшою.

2.5 Розширення мережі

Під час побудови комп'ютерної мережі, неважливо локальної чи корпоративної, рано чи пізно постає питання розширення мережі або додавання нових пристроїв. Зазвичай це не викликає великих труднощів і користувач з мінімальними навичками або кваліфікований співробітник може самостійно провести відповідне налаштування. Але якщо є більше пристроїв ніж доступних портів Ethernet, користувачі мають декілька варіантів для розширення: Ethernet-комутатор, мережевий концентратор, ретранслятор (repeater). Мережеві концентратори та ретранслятори вже давно застаріли та майже не застосовуються у побудові мереж унаслідок витіснення більш досконалим пристроєм – мережевим комутатором.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

Мережевий комутатор (network switch) – пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного або декількох сегментів мережі. На відміну від концентратора, який розширює трафік від одного пристрою до всіх інших, комутатор передає дані тільки безпосередньо до одержувача, виключення становить широкомовний трафік (FF:FF:FF:FF:FF:FF) всім вузлам мережі. Це підвищує продуктивність і безпеку мережі, виключає можливість, коли інші сегменти мережі обробляють дані, які їм не призначались.



Рисунок 2.4 – Ethernet-комутатор

2.6 Огляд ОС для розробки комп'ютерної мережі

2.6.1 Windows Server

Операційна система ОС (Operating system, OS) – це комплексна програма, яка виконує роль інтерфейсу (панелі взаємодій) між користувачем і обладнанням комп'ютера. Усі додатки комп'ютера, такі як текстові та графічні редактори, електронні таблиці, бази даних, інтернет-браузери тощо, не можуть працювати та виконувати свої завдання без програмного середовища операційної системи, яка надає для них необхідні сервіси.

Важливо позначати відмінність серверної операційної системи від операційної системи звичайного комп'ютера (desktop OS, тобто настільної ОС). У настільній ОС працюють такі програми, як MS Word, Excel, PowerPoint, Visio, Adobe Photoshop та багато інших, які використовуються для повсякденної роботи, а також ігри та розважальні програми для відпочинку. Настільна ОС відповідає за підключення комп'ютера користувача до локальної мережі LAN та

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

до мережі Інтернет, а також до інших пристроїв через різні протоколи та програми. Також варто додати, що пропрієтарна настільна ОС зазвичай має набагато меншу вартість, ніж серверна ОС.

Серверна ОС використовує набагато більший обсяг пам'яті для обчислювальної активності і обробки даних, а також може виконувати функції вебсервера, додатків серверів і серверів електронної пошти та багатьох інших серверів, необхідних для роботи ІТ-систем підприємств.

Windows Server є частиною сімейства мережевого програмного забезпечення Windows Network, яке розвивалося спільно з ОС Windows. Остання версія ОС Windows Server 2022 може працювати як сервери підприємств, так і хмарними серверами (Microsoft Azure), створюючи гібридні обчислювальні середовища. Хмарні ресурси можуть бути залучені в разі необхідності при встановленні навантажень на власну ІТ-систему. Windows Server 2022 також має розширені функції безпеки.



Рисунок 2.5 – логотип Windows Server

Серед плюсів нової версії можна навести такі як:

Підтримка гібридної хмари. ІТ-систему підприємства на Windows Server можна розширити в хмарне середовище Azure і отримати там додаткові функції та сервіси, а також збільшити обсяг накопичувачів та обчислювальну потужність сервера.

Безпека. Можливість захисту від шкідливого ПЗ і проникнення у віртуальні машини.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Розробка програм. Підтримка технологій контейнерів Kubernetes для розробки нових сервісів і додатків, а також нові можливості розгортання та масштабування додатків у гібридній хмарі на базі Azure.

Підтримка Linux. Windows Server 2022 містить удосконалену версію підсистеми підтримки Windows Subsystem for Linux (WSL). Тому розробники на базі Windows Server 2022 мають можливість розробляти програми для ОС Linux безпосередньо в середовищі Windows, в якій можуть працювати віртуальні машини Linux. Крім того, розробники можуть писати програми на популярній мові команди Bash, а також Ruby і Python.

Підтримка системи управління контейнерами Kubernetes. Контейнерні технології отримують всю більшу популярність, оскільки вони використовуються замість віртуальних машин, яким потрібна окрема ОС. Ці контейнери можна зберігати у вигляді образів і при необхідності повторно використовувати при розробці програми замість того, щоб писати код заново.

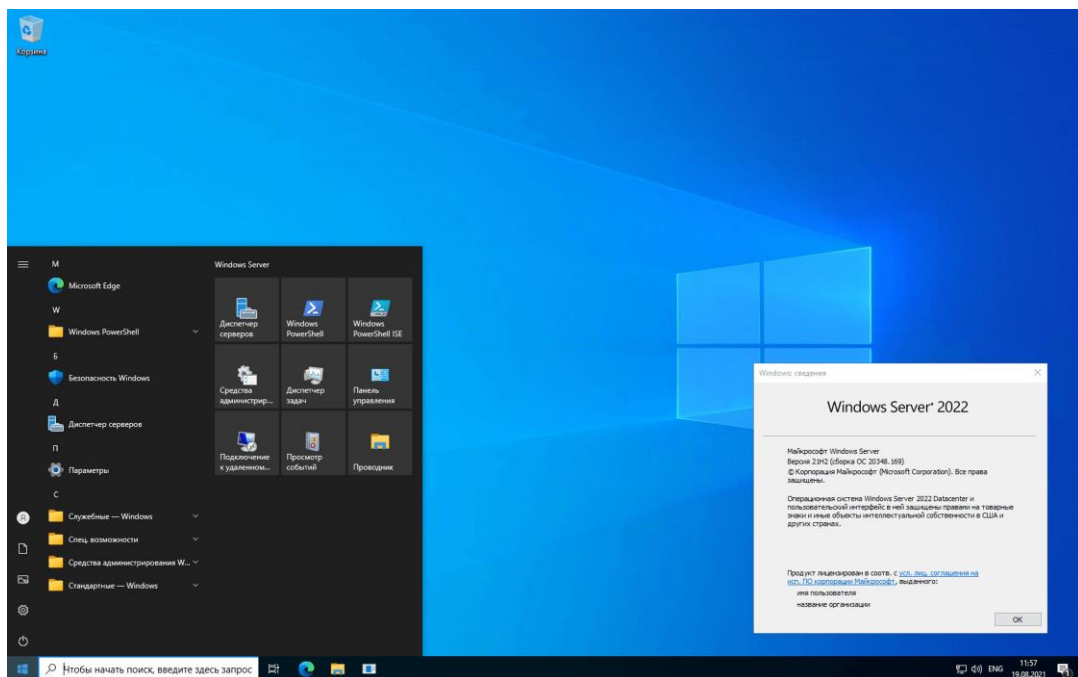


Рисунок 2.6 – ОС Windows Server

У Windows Server 2022 є також Центр адміністрування серверів WAC (Центр адміністрування Windows). Він встановлюється в ІТ-системі замовника та дозволяє адмініструвати локальні та хмарні екземпляри Windows Server 2022,

		Борейченко Г.О.			KIK.KP.B – 123 – 07 – ПЗ	Арк.
		Головня О.С.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

комп'ютери під керуванням ОС Windows 10, кластери та мережну інфраструктуру. WAC також може адмініструвати сервери для об'єктів ІТ-систем для обліку засобів підвищеної безпеки та мобільних рішень, які дозволяють надавати або відкривати доступ у залежності від відповідних політик, ризиків, місця розташування та інших факторів.

Windows Server 2022 має нові інтелектуальні можливості, зокрема System Insights, для прогнозової аналітики, які дозволяють запобігати проблемам у парках серверів підприємств. Модель машинного інтелекту враховує навантаження та події в системі, а також може спрогнозувати нестачу вільного місця у системах зберігання даних. Крім того, машинний інтелект надає аналітичні звіти про роботу серверів і допомагає скоротити експлуатаційні витрати.

2.6.2 Unix-подібні системи

Red Hat Enterprise Linux (RHEL) – досить популярний дистрибутив серверної ОС, розроблений на базі ОС Linux компанією Red Hat, перша версія, якої була випущена на ринку в 2003 році. Хоча RHEL належить до класу відкритого ПЗ і його вихідний програмний код є безкоштовним і доступним всім охочим, однак виконувані коди RHEL отримуються за плату. Раз в два роки Red Hat випускає версію RHEL у двійковому коді з підтримкою протягом десяти років, при чому Red Hat відстежує критичні помилки Linux і оновлює вже випущені версії серверної ОС.



Рисунок 2.7 – логотип Red Hat

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

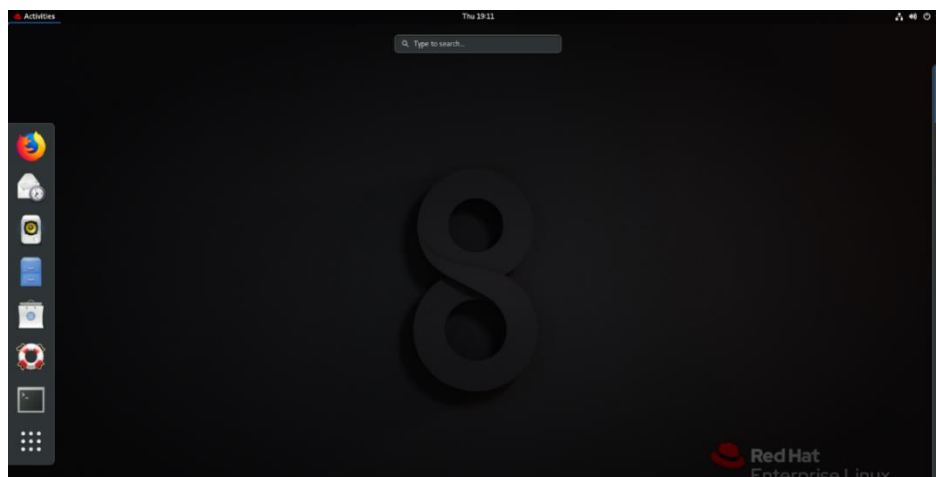


Рисунок 2.8 – робочий стіл ОС Red Hat

Крім того, Red Hat має найбільший внесок у розроблення ОС Linux за обсягом програмного коду. Остання версія RHEL 9 була представлена 18 травня 2022 року. Вона орієнтована для роботи на гібридній основі та має ефективні інструменти для забезпечення надійності, стабільності та доступності. Вона містить наступні оновлення:

- Система розумного моніторингу та управління в рамках сервісу Red Hat Insights.
- Розширений набір інструментів для роботи з контейнерами.
- Покращений інтерфейс, який підходить як для новачків, так і для експертів.

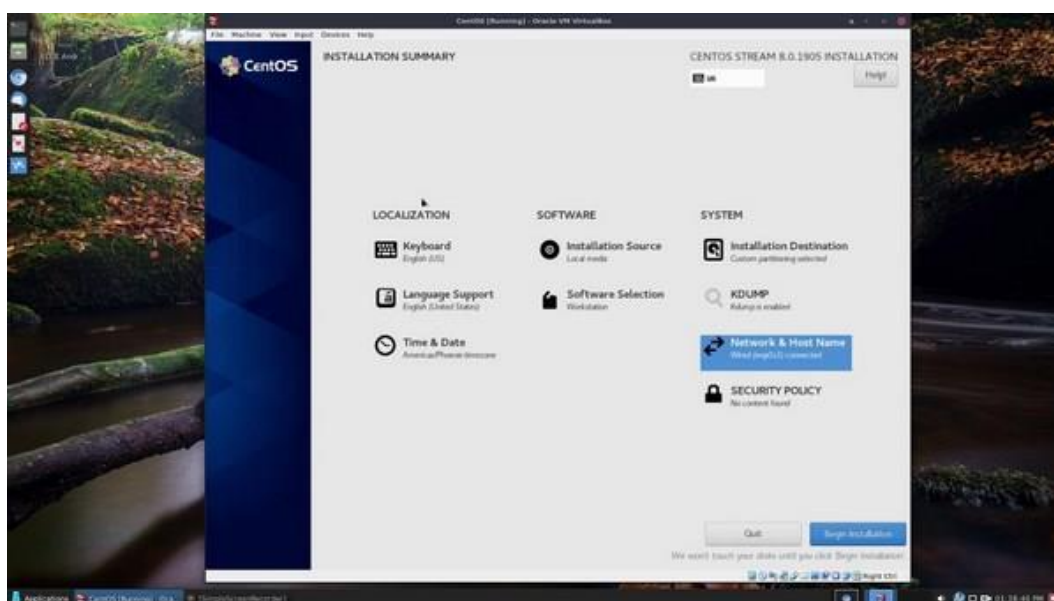


Рисунок 2.9 – робочий стіл CentOS

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

CentOS – це ще один дистрибутив Linux, являє собою вільну ОС корпоративного класу, що підтримується спільнотою розробників. Розробка CentOS почалася в 2006 році під назвою Tao Linux (клон Red Hat Enterprise Linux), потім було прийнято назву CentOS. У січні 2014 року компанія Red Hat об’явила, що вона буде спонсорувати цей проєкт. В результаті володіння товарними знаками CentOS було передано Red Hat. При цьому більшість розробників CentOS працюють в спеціальному підрозділі компанії Red Hat паралельно з командою розробників Red Hat Enterprise Linux.

Однак, з того моменту відбулися важливі зміни у підтримці цієї ОС. Зокрема, в 2021 році компанія Red Hat заявила, що невдовзі зупинить підтримку CentOS. Натомість планується запропонувати користувачам проєкт CentOS Stream зі схожими функціями.

CentOS функціонально сумісний із Red Hat Enterprise Linux та побудований із програмними блоками RHEL. Відповідно до життєвого циклу Red Hat Enterprise Linux, CentOS версії 5, 6 і 7 підтримуватиметься до 10 років.

Oracle Linux (Oracle Enterprise Linux, Unbreakable Linux) — відкритий дистрибутив ОС Linux, який після реєстрації можна безкоштовно завантажити з сайту компанії Oracle. Oracle також надає послуги платної технічної підтримки організацій, що користуються дистрибутивом. Oracle Linux створений у 2006 році на основі Red Hat Enterprise Linux. Oracle Linux на 100% сумісний з Red Hat Enterprise Linux на рівні двійкового коду. Пропонована копія дистрибутиву від Red Hat, Oracle встановила вартість послуг з технічної підтримки на Oracle Linux нижче, ніж у Red Hat. 31 березня 2020 р. було випущено оновлення ядра ОС Unbreakable Enterprise Kernel 6 для Oracle Linux, яке надає нові функції з відкритим вихідним кодом і критично важливими для бізнесу рішеннями щодо оптимізації роботи та безпеки корпоративних ІТ-систем, як на майданчику підприємства, так і у хмарі.

В травні 2022 року вийшла нова beta-версія системи Unbreakable Enterprise Kernel 7.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

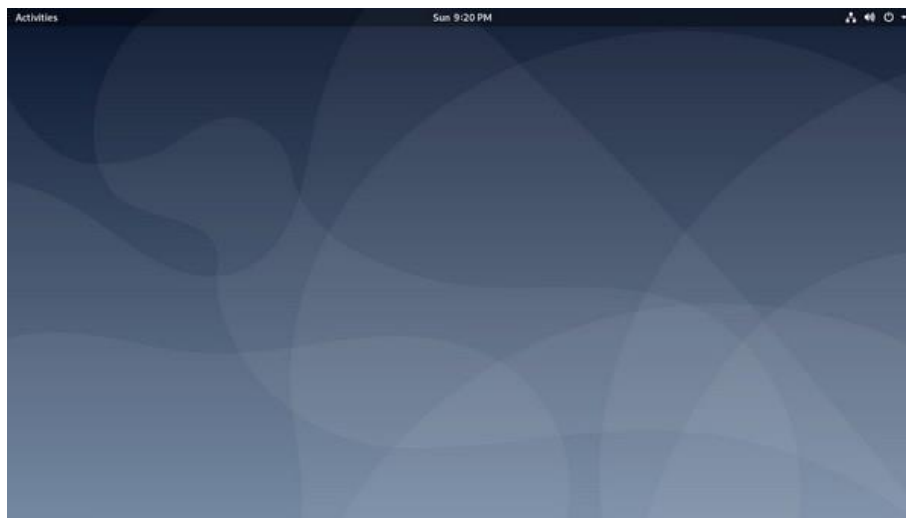


Рисунок 2.10 – робочий стіл Oracle Linux

2.6.3 Ubuntu server

ОС Ubuntu – популярна ОС з відкритим кодом на базі Linux для комп’ютерів, ноутбуків, планшетів, телефонів та віртуальних машин, а також для серверів. Основним розробником і спонсором є компанія Canonical, однак ця ОС розвивається та підтримується вільною спільнотою розробників. Ubuntu поширюється безкоштовно і містить повний набір усіх необхідних для роботи додатків, а всі інші утиліти в стандартній поставці можна завантажити з Інтернету. Також в Ubuntu Server існують програми платної підтримки. Документація по операційній системі Ubuntu Linux створюється спільнотою forum.ubuntu.com.

За власними підрахунками компанії Canonical, Ubuntu використовується приблизно 20 мільйонами користувачів і займає 1-е місце в списку популярних дистрибутивів Linux для вебсерверів. Ubuntu надається з підбіркою програмного забезпечення для різних типів серверів і робочих станцій, а також має версії для різних процесорних архітектур: x86, AMD, ARM. Крім того, з 2013 року розпочато розробку спеціальної версії Ubuntu для смартфонів на архітектурі ARM та x86. Існує також редакція Ubuntu Core, призначена для пристроїв Інтернету речей (IoT) та роботів.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

```

[ 11.155011] systemd[1]: Finished udev Coldplug all Devices.
[ OK ] Finished udev Coldplug all Devices.
[ 11.160031] systemd[1]: Finished Load Kernel Modules.
[ OK ] Finished Load Kernel Modules.
[ 11.167703] systemd[1]: Mounting FUSE Control File System...
Mounting FUSE Control File System...
[ 11.176221] systemd[1]: Mounting Kernel Configuration File System...
Mounting Kernel Configuration File System...
[ 11.188472] systemd[1]: Starting Apply Kernel Variables...
Starting Apply Kernel Variables...
[ 11.198444] systemd[1]: Starting udev Wait for Complete Device Initialization...
Starting udev Wait for Complete Device Initialization...
[ 11.203342] systemd[1]: Mounted Kernel Configuration File System.
[ OK ] Mounted Kernel Configuration File System.
[ 11.213882] systemd[1]: Mounted FUSE Control File System.
[ OK ] Mounted FUSE Control File System.
[ 11.225801] systemd[1]: Started Journal Service.
[ OK ] Started Journal Service.
Starting Flush Journal to Persistent Storage...
[ 11.282744] systemd-journald[350]: Received client request to flush runtime journal.
[ OK ] Finished Load/Save Random Seed.
[ OK ] Finished Create System Users.
Starting Create Static Device Nodes in /dev...
[ 11.389241] systemd-journald[350]: File /var/log/journal/a4bcd4a1df224716bf5be3972a737e71/system...
journal corrupted or uncleanly shut down, renaming and replacing.
[ OK ] Activated swap /swap.img.
[ OK ] Finished Set the console keyboard layout.
[ OK ] Finished Apply Kernel Variables.
[ OK ] Finished Create Static Device Nodes in /dev.
Starting udev Kernel Device Manager...
[ OK ] Finished Flush Journal to Persistent Storage.
[ OK ] Started udev Kernel Device Manager.
[ OK ] Started Dispatch Password Requests to Console Directory Watch.
[ OK ] Reached target Local Encrypted Volumes.
[ OK ] Listening on Load/Save RF Kill Switch Status /dev/rfkill Watch.
[ OK ] (1 of 2) A start job is running for /dev/disk...-fe75-49bd-963e-85a0e6fe6ce7 (8s / 1min 30s)

```

Рисунок 2.11 – завантаження Ubuntu Server

Насамперед вся серія серверних систем Windows пропонує зручність адміністрування на основі великої кількості вже розроблених для цього програм та утиліт. Але те, що для звичайного користувача може вважатися гнучкістю у користуванні, для інших є скоріше обмеженням у функціоналі і виборі рішень для користувача. Тоді як Ubuntu розвивалась з відкритого підходу до розробки (open-source). Разом з тим саме сервери під управлінням Linux активно використовують для роботи з MySQL і Postgre. До того ж, в системі легко розгортати системи управління трафіку і налагоджувати маршрутизацію у мережі. Основні аспекти саме цього дистрибутиву Linux можна описувати дуже довго. Це і менша потреба в апаратних ресурсах (у разі використання інтерфейсу командного рядка) і консольна система для роботи з серверами тощо. Завдяки цьому дружній інтерфейс для звичайного користувача. Беручи до ваги, все вище згадане, можемо виділити основні переваги та недоліки ОС Ubuntu Server.

Переваги серверної системи Ubuntu Linux:

- Без додаткової плати за ліцензію, оскільки операційна система безкоштовна. Більш надійний захист системи – рідко стикається з шкідливими програмами.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

- Невимогливість до апаратного забезпечення клієнта та низьке споживання ресурсів у разі використання інтерфейсу командного рядка (без GUI).
- Завдяки низьким вимогам до інфраструктури демонструє чудові показники продуктивності.
- Системні адміністратори мають свободу та можливість вільно налаштувати систему відповідно до своїх побажань.
- Безперебійне використання програмного забезпечення з відкритим кодом.

Недоліки серверної системи Ubuntu Linux:

- Робота через командний рядок замість графічного інтерфейсу вимагає певного досвіду у користувача.
- Деякі сторонні програми можуть не мати підтримки.

2.7 Обґрунтування вибору Ubuntu Server

В якості операційної системи було вирішено використовувати Ubuntu Server. Ця система підтримує роботу з великою місткістю оперативної пам'яті і великою кількістю процесорів. Також вона містить засоби організації доменів і механізми розподілу навантаження на серверну структуру.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Таблиця 2.1 – Порівняльна характеристика різних ОС

Характеристика	Windows Server	Red Hat	Cent OS	Ubuntu Server
Перший рік випуску	2003	2000	2002	2004
Остання версія	Windows Server 2022	Red Hat 8.5	Cent OS 8.5	Ubuntu Server 22.04
Архітектура	Windows NT	Linux kernel		
Вартість	Ліцензійна плата за користувача, ПЗ з закритим кодом	Платна, з відкритим кодом	Безкоштовна, ПЗ з відкритим кодом	Безкоштовна, ПЗ з відкритим кодом
Захист	Схильна до спроб злому та кіберзагроз	Захищена від шкідливого ПЗ та кіберзагроз		
Підтримка	Спільнота та довгострокова підтримка клієнтів, великий обсяг документації	Велика спільнота програмістів і системних адміністраторів, розвинута документація		
Режим роботи	Графічний інтерфейс (Windows Shell)	Командний рядок, графічний інтерфейс Gnome, KDE інші		
Досвід користувача	Зручний для початківців	Досвід адміністрування на Linux системах		
Підтримувані БД	Microsoft SQL, Microsoft Access	PostgreSQL, MySQL, MariaDB, MongoDB та інші		
Підтримувані скрипти	ASP and ASP.NET	Python, PHP, Perl та інші		
Підтримуване ПЗ	Специфічне windows орієнтоване ПЗ	Apache, Tomcat		Веб-сервери: nginx, Apache тощо

Таблиця 2.2 – Характеристика різних версій Ubuntu Server

Характеристика	18.04 LTS	20.04 LTS	22.04 LTS
Кодова назва	Bionic Beaver	Focal Fossa	Jammy Jellyfish
Дата виходу	26 квітня 2018	23 квітня 2020	21 квітня 2022
Підтримка до	квітень 2023	квітень 2025	21 квітня 2027
Підтримується	Досі підтримується	Досі підтримується	Поточний випуск
Мінімальна опера- тивна пам'ять	1 Гб	4 Гб	4 Гб
Мінімальна пам'ять на диску	1.5 Гб	25 Гб	25 Гб

Здійснений аналіз дає змогу дійти висновку, що серверна операційна система Linux Ubuntu Server найкраще підходить для вирішення завдань в межах даної кваліфікаційної роботи, а саме створення мережі наукової бібліотеки.

2.8 Проектування топології комп'ютерної мережі та розробка системи адресації

При проектуванні мережі була використана трирівнева ієрархічна модель мережі Cisco, в якій використовуються три рівні:

- Рівень ядра (Core layer);
- Рівень розподілу (Distribution layer);
- Рівень доступу (Access layer).

Загальна топологія спроектованої мережі представлена на рисунку 2.12. Де номерами позначено: 1 – Директор, 2 – Організаційний відділ, 3 – Серверний відділ, 4 – відділ комплектування документів, 5 – інформаційно-бібліографічний відділ, 6 – відділ інформаційних технологій, 7 – відділ навчальної літератури, 8 – відділ наукової та художньої літератури.

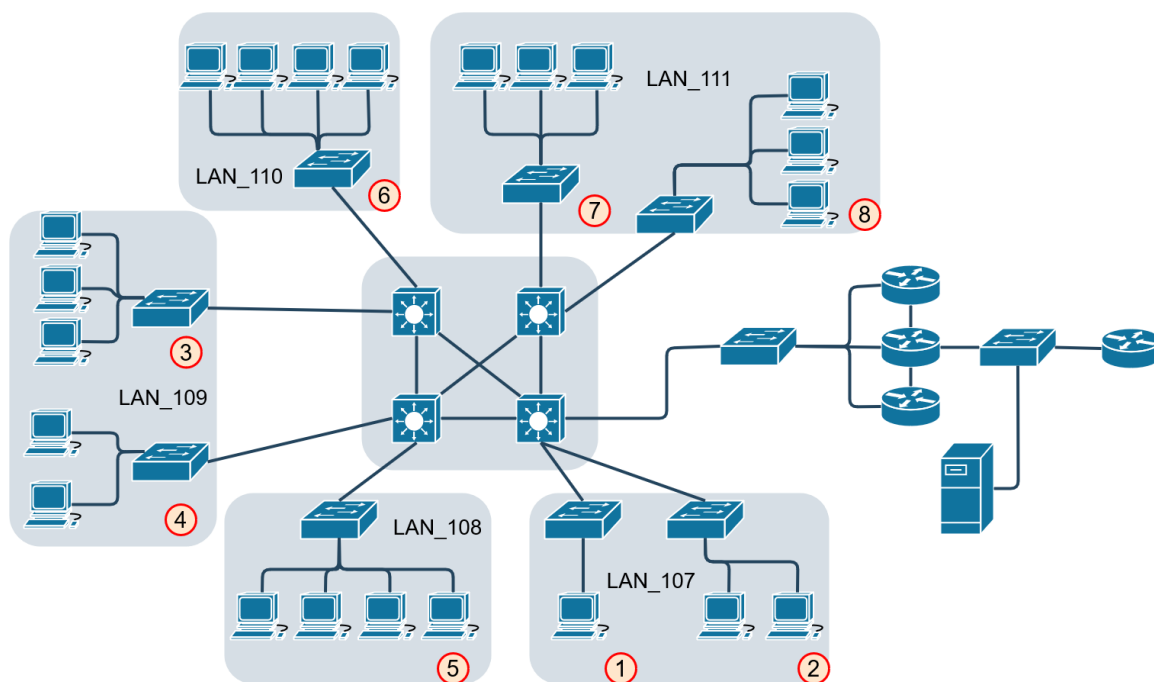


Рисунок 2.12 – Загальна топологія спроектованої мережі

Загальна топологія мережі спроектованої на GNS3 представлена на
 рисунку 2.13.

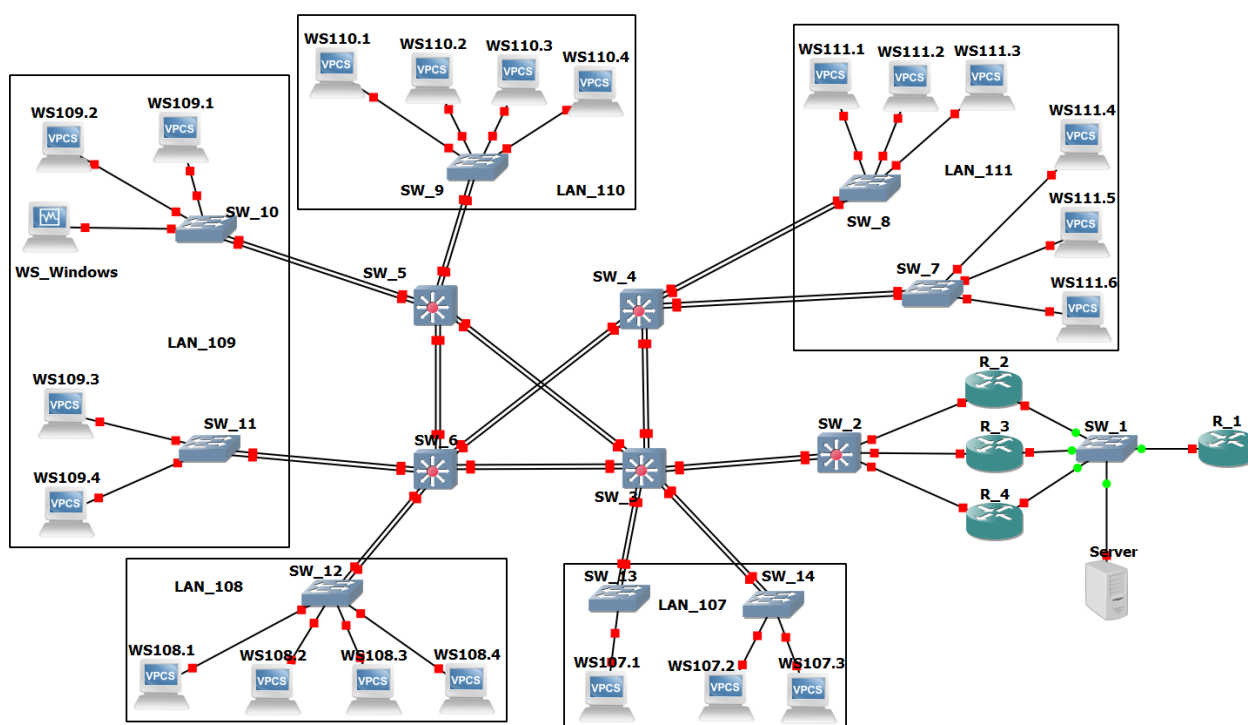


Рисунок 2.13 – Загальна топологія спроектованої мережі

У загальному в мережі використано чотирнадцять комутаторів та чотири маршрутизатора. Мережа складається з п'яти VLAN, які розподілені на різні комутатори.

Рівень ядра складається з трьох маршрутизаторів та чотирьох комутаторів, які з'єднані між собою за допомогою витой пари Gigabit Ethernet.

Рівень розподілу складається зі з'єднаних між собою агрегованими каналами комутаторами за допомогою витой пари Fast Ethernet для забезпечення високої швидкості на даному рівні.

Рівень доступу представлений комутаторами з під'єднаними до них кінцевих вузлів, які відносяться до різних віртуальних локальних мереж (VLAN), саме з'єднання комутаторів до рівня розподілу забезпечуються агрегованими каналами з витих пар Gigabit Ethernet, а з'єднання до кінцевих вузлів – витую парою Fast Ethernet.

Розглянемо детальніше спроектовану мережу. Загальна структура мережі показана в додатку А.

До комутаторів SW_13, SW_14 підключений VLAN107, який має три кінцевих вузла.

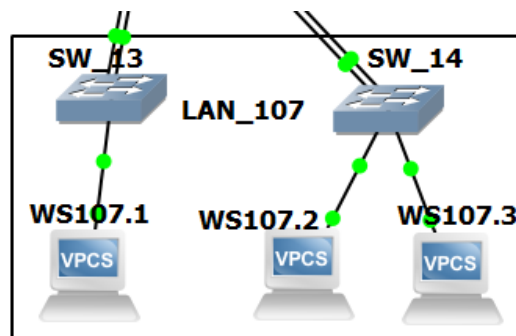


Рисунок 2.14 - Комутатори SW_13, SW_14 та підключені три кінцевих вузла

До комутатора SW_12 підключений VLAN108, який має чотири кінцевих вузла.

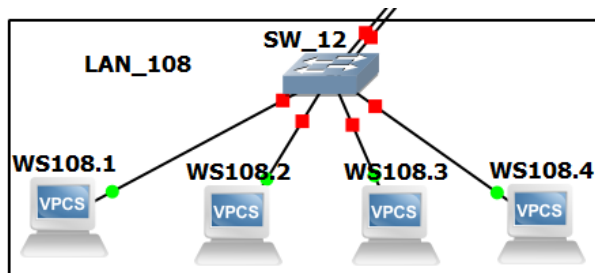


Рисунок 2.15 - Комутатор SW_12 та підключені чотири кінцевих вузла

До комутаторів SW_10, SW_11 підключений VLAN109, який має п'ять кінцевих вузлів.

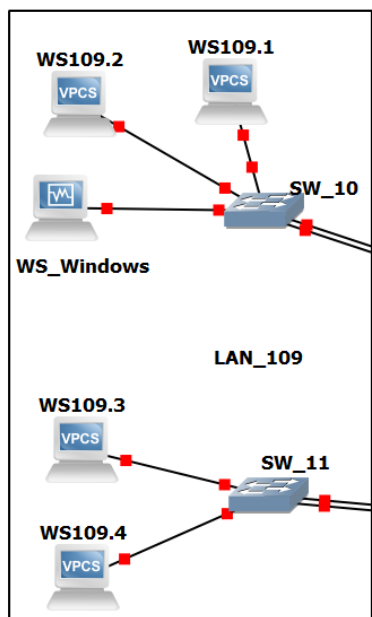


Рисунок 2.16 - Комутатори SW_10, SW_11 та підключені п'ять кінцевих вузла

До комутатора SW_9 підключений VLAN110, який має чотири кінцевих вузла.

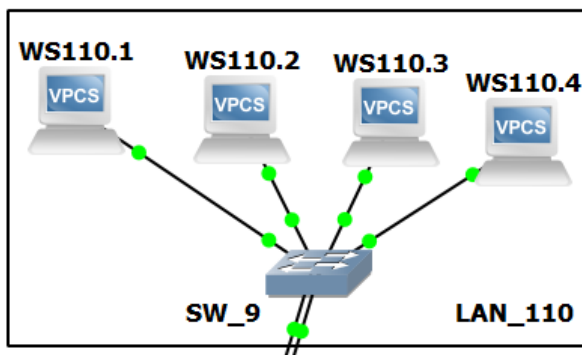


Рисунок 2.17 – Комутатор SW_9 та підключені чотири кінцевих вузла

До комутаторів SW_8, SW_7 підключений VLAN111, який має шість кінцевих вузлів.

		Борейченко Г.О.			KIK.KP.B – 123 – 07 – ПЗ	Арк.
		Головня О.С.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

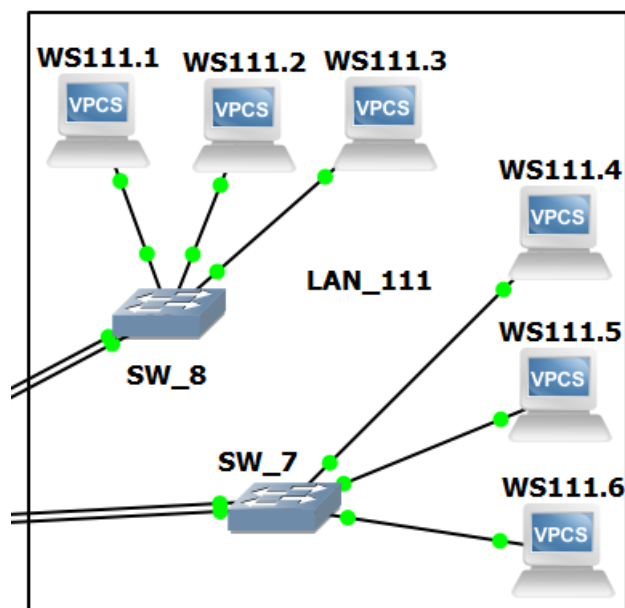


Рисунок 2.18 - Комутатори SW_8, SW_7 та підключені шість кінцевих вузлів

Загалом сумарна кількість кінцевих вузлів кожної VLAN наведено в таблиці 2.3:

Таблиця 2.3 – Загальна кількість кінцевих вузлів кожної VLAN

Номер VLAN	Загальна кількість кінцевих вузлів
107	3
108	4
109	4
110	4
111	6

На рівні ядра використано три маршрутизатора R_2, R_3 та R_4 для балансування навантаження між трьома каналами, які підключені до них з комутатора SW_2.

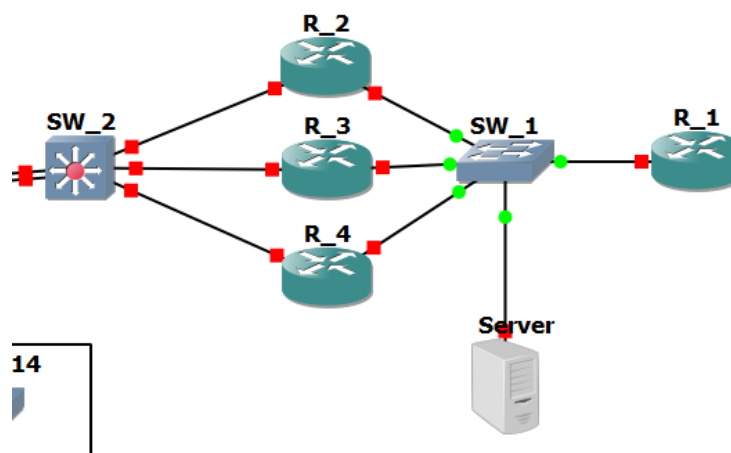


Рисунок 2.19 - маршрутизатори R_2, R_3 та R_4

Пріоритети кожної VLAN наведено в таблиці 2.4

Таблиця 2.4 - HSRP пріоритети для кожної VLAN

VLAN	R_2	R_3	R_4
VLAN107	96	105	100
VLAN108	96	105	100
VLAN109	100	96	105
VLAN110	105	100	96
VLAN111	105	100	96

Адресація пристроїв мережі на рівні ядра наведена в таблиці 2.5

Таблиця 2.5 - Адресація пристроїв мережі на рівні ядра

Пристрій мережі	Інтерфейс	IPv4-адреса	Маска мережі	Префікс мережі
Маршрутизатор R_1	Ethernet1/0	194.4.7.1	255.255.255.192	/26
Маршрутизатор R_2	Ethernet1/0	194.4.7.2		
Маршрутизатор R_3	Ethernet1/0	194.4.7.3		
Маршрутизатор R_4	Ethernet1/0	194.4.7.4		

Для зменшення навантаження на мережу та збільшення балансування на маршрутизаторах R_2, R_3, R_4 було створено і налаштовано інтерфейси для кожної VLAN відповідно. Кожний інтерфейс має свою IP-адресу, маску підмережі та префікс мережі. Адресація вказаних пристроїв мережі наведена в таблиці 2.6:

Таблиця 2.6 - Адресація на рівні розподілу і рівні доступу

Пристрій мережі	Інтерфейс	IPv4-адреса	Маска мережі	Префікс мережі
Маршрутизатор R_4_7_2	Ethernet0/0.107	193.4.107.126	255.255.255.128	/25
	Ethernet0/0.108	193.4.108.126		
	Ethernet0/0.109	193.4.109.126		
	Ethernet0/0.110	193.4.110.126		
	Ethernet0/0.111	193.4.111.126		
Маршрутизатор R_4_7_3	Ethernet0/0.107	193.4.107.125		
	Ethernet0/0.108	193.4.108.125		
	Ethernet0/0.109	193.4.109.125		
	Ethernet0/0.110	193.4.110.125		
	Ethernet0/0.111	193.4.111.125		
Маршрутизатор R_4_7_4	Ethernet0/0.107	193.4.107.125		
	Ethernet0/0.108	193.4.108.124		
	Ethernet0/0.109	193.4.109.124		
	Ethernet0/0.110	193.4.110.124		
	Ethernet0/0.111	193.4.111.124		

Адресація всіх створених VLAN загальної мережі наведена в таблиці 2.7:

Таблиця 2.7 - Адресація всіх VLAN загальної мережі

VLAN	Призначення	IPv4-адреса
VLAN107	Префікс	/25
	Маска префіксу	255.255.255.128
	Інверсна маска префіксу	0.0.0.127
	Мережа	193.4.107.0
	Шлюз по-замовчуванню	193.4.107.123
	Мінімальна адреса діапазону	193.4.107.1
	Максимальна адреса діапазону	193.4.107.126
VLAN108	Префікс	/25
	Маска префіксу	255.255.255.128
	Інверсна маска префіксу	0.0.0.127
	Мережа	193.4.108.0
	Шлюз по-замовчуванню	193.4.108.123
	Мінімальна адреса діапазону	193.4.108.1
	Максимальна адреса діапазону	193.4.108.126
VLAN109	Префікс	/25
	Маска префіксу	255.255.255.128
	Інверсна маска префіксу	0.0.0.127
	Мережа	193.4.109.0
	Шлюз по-замовчуванню	193.4.109.123
	Мінімальна адреса діапазону	193.4.109.1
	Максимальна адреса діапазону	193.4.109.126

VLAN110	Префікс	/25
	Маска префіксу	255.255.255.128
	Інверсна маска префіксу	0.0.0.127
	Мережа	193.4.110.0
	Шлюз по-замовчуванню	193.4.110.123
	Мінімальна адреса діапазону	193.4.110.1
	Максимальна адреса діапазону	193.4.110.126
VLAN111	Префікс	/25
	Маска префіксу	255.255.255.128
	Інверсна маска префіксу	0.0.0.127
	Мережа	193.4.111.0
	Шлюз по-замовчуванню	193.4.111.123
	Мінімальна адреса діапазону	193.4.111.1
	Максимальна адреса діапазону	193.4.111.126

2.9 Апаратне забезпечення комп'ютерної мережі

Після вибору архітектури мережі, системних і програмних рішень для її проектування настав час розглянути вибір апаратного обладнання для організації роботи мережі. При виборі моделі комутатора основними критеріями виступають: кількість портів, швидкість передачі портів, керований або некерований комутатор.

У даній мережі, яка розробляється у рамках кваліфікаційної роботи використовуються дві моделі комутатора, а саме:

- Cisco Switch Catalyst 2960: WS-C2960-24-S. Дана модель використовується на рівні розподілу та на рівні ядра мережі, так як там швидкість передачі трафіку грає дуже важливу роль;
- Cisco Switch Catalyst 2950: 2950-24 на двадцять чотири порти Gigabit Ethernet, який гарантує високу швидкість та можливість реалізації агрегації портів для будь-якої мережі. Дана модель використовується на рівні доступу, так як гарантує підключення десяти кінцевих вузлів, та забезпечує високу швидкість передачі трафіку на рівень розподілу.

Прошивка комутаторів Cisco Catalyst 2960 випускається в образах LAN Base та Lan Lite Image. Версія LAN Base має розширені можливості, включаючи покращену безпеку (ACLs), захист DHCP Snooping та додаткові функції контролю доступу - Web authentication та розширення 802.1x, додаткові можливості установок якості обслуговування QoS, підтримка надлишкового живлення RPS та великої кількості SFP-портів. Функції Flex Links та Link State Tracking, збільшена кількість підтримуваних VLANs (до 256), IPv6 Host, MLD Snooping, LLDP-MED, RSPAN, MVR, DHCP Option 82, та IP SLA (responder) та інше.



Рисунок 2.20 - Комутатор Cisco Catalyst 2960



Рисунок 2.21 – Порти комутатора Cisco Catalyst 2960



Рисунок 2.22 - Комутатор Cisco Catalyst 2950

При виборі моделі маршрутизатора потрібно враховувати, як він маршрутизує пакети в складній мережі з різними видами топологій. Маршрутизатор має містити достатню кількість портів, забезпечувати необхідну швидкість передачі даних та швидкість їх обробки. Для даної мережі було обрано маршрутизатор Cisco 2600.



Рисунок 2.23 - Маршрутизатор Cisco 2600

Висновки з другого розділу

Отже, в рамках другого розділу було детальніше розглянуто планування структури майбутньої мережі наукової бібліотеки. Було згадано, які існують комп'ютерні моделі мереж, в якості шаблону була вибрана найпоширеніша архітектурна модель клієнт-сервер. Далі перейшли до питання управління мережею. Якщо проектується мережа на базі моделі клієнт-сервер, то необхідно визначити точну кількість робочих станцій у мережі бібліотеки й в кожному її відділі. Далі розмістити сервер, забезпечити його умови роботи, підтримку працездатності і його захист. Таким чином, у рамках другого розділу розробили чіткий структурний план приміщення наукової бібліотеки, де буде проходити

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

корпоративна мережа. Нарешті, розібравшись з планом розміщення серверу і робочих станцій, перейшли до топології мережі. Також згадали про мережеві ресурси, які необхідні для нормальної роботи будь-якої організації і які необхідно правильно налаштувати для злагодженої роботи мережі (принтери, модеми, факси та інші).

Також в даному розділі ми розглянули питання що таке ОС, чим відрізняється операційна система звичайного комп'ютера від серверної операційної системи. Розглянули найбільш використовувані серверні операційні системи. Дали коротку характеристику таким популярним системам як Windows Server, Red Hat, Ubuntu Server, CentOS Server. Таким чином у розглянутих нами ОС є як свої плюси, так і недоліки. Наприклад, Ubuntu Server і CentOS мають безкоштовну основу і деякі платні програми підтримки, у той час як Windows Server і Red Hat мають платну ліцензію. Windows отримує частіші оновлення системи, хоча має меншу захищеність від шкідливого ПЗ, ніж Ubuntu Server.

Оскільки, в рамках виконання даної кваліфікаційної роботи нам необхідна ОС для побудови серверної інфраструктури, то нам необхідна насамперед, популярна і безкоштовна ОС, яка має велику кількість документації та літератури для обробки. Беручи до уваги захищеність системи, найкращим вибором для нас є Ubuntu Server.

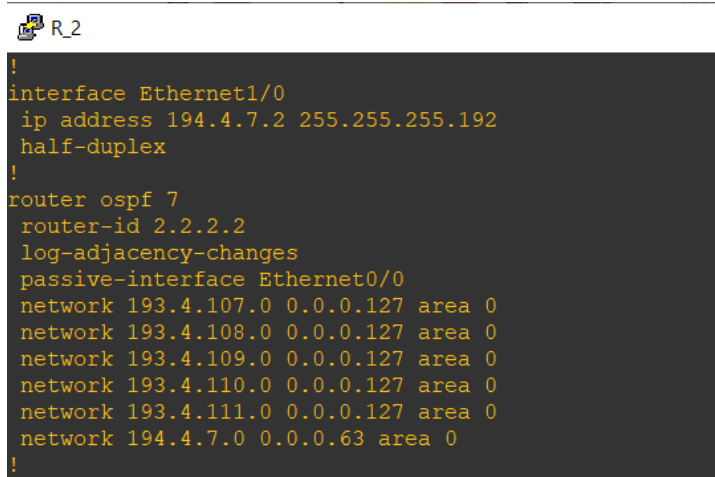
Також у цьому розділі було виконано проектування топології комп'ютерної мережі та розподілено відповідні IP-адреси. Мережа була побудована згідно концепції трирівневої ієрархічної моделі Cisco. Було побудовано і налаштовано рівень ядра, рівень розподілу і доступу. У загальному в мережі використано чотирнадцять комутаторів та чотири маршрутизатора. Мережа складається з п'яти VLAN, які розподілені на різні комутатори.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ

3.1 Налагодження обладнання мережі

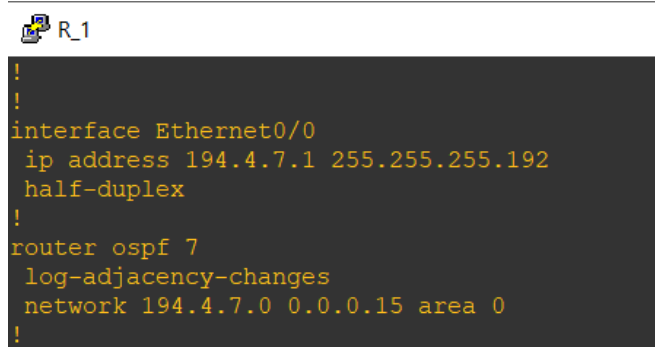
Перш за все у даній мережі було налаштовано адресацію інтерфейсів, підінтерфейсів маршрутизаторів та роботу протоколу OSPF. Розглянемо лістинг налаштування на прикладі маршрутизатора R_2 рисунок 3.1 та маршрутизатора R_1 рисунок 3.2 [8].



The screenshot shows the configuration for router R_2. It starts with the configuration of the Ethernet1/0 interface, setting the IP address to 194.4.7.2 with a subnet mask of 255.255.255.192 and setting it to half-duplex. Then, the OSPF process is configured with router-id 2.2.2.2, logging adjacency changes, and making Ethernet0/0 a passive interface. Finally, several networks are advertised into area 0: 193.4.107.0, 193.4.108.0, 193.4.109.0, 193.4.110.0, 193.4.111.0, and 194.4.7.0.

```
! R_2
!
interface Ethernet1/0
 ip address 194.4.7.2 255.255.255.192
 half-duplex
!
router ospf 7
 router-id 2.2.2.2
 log-adjacency-changes
 passive-interface Ethernet0/0
 network 193.4.107.0 0.0.0.127 area 0
 network 193.4.108.0 0.0.0.127 area 0
 network 193.4.109.0 0.0.0.127 area 0
 network 193.4.110.0 0.0.0.127 area 0
 network 193.4.111.0 0.0.0.127 area 0
 network 194.4.7.0 0.0.0.63 area 0
!
```

Рисунок 3.1 – налаштування маршрутизатора R_2



The screenshot shows the configuration for router R_1. It starts with the configuration of the Ethernet0/0 interface, setting the IP address to 194.4.7.1 with a subnet mask of 255.255.255.192 and setting it to half-duplex. Then, the OSPF process is configured with logging adjacency changes and advertising the 194.4.7.0 network into area 0.

```
! R_1
!
interface Ethernet0/0
 ip address 194.4.7.1 255.255.255.192
 half-duplex
!
router ospf 7
 log-adjacency-changes
 network 194.4.7.0 0.0.0.15 area 0
!
```

Рисунок 3.2 – налаштування маршрутизатора R_1

Було вирішено використовувати в мережі п'ять різних VLAN, тому було реалізовано InterVlan Routing та налаштовано підінтерфейси на маршрутизаторах R_2, R_3, R_4 (рис. 3.3).

```

R_2
!
interface Ethernet0/0.107
 encapsulation dot1Q 107
 ip address 193.4.107.126 255.255.255.128
 standby 107 ip 193.4.107.123
 standby 107 priority 96
 standby 107 preempt
 standby 107 track Ethernet1/0
!
interface Ethernet0/0.108
 encapsulation dot1Q 108
 ip address 193.4.108.126 255.255.255.128
 standby 108 ip 193.4.108.123
 standby 108 priority 96
 standby 108 preempt
 standby 108 track Ethernet1/0
!
interface Ethernet0/0.109
 encapsulation dot1Q 109
 ip address 193.4.109.126 255.255.255.128
 standby 109 ip 193.4.109.123
 standby 109 preempt
 standby 109 track Ethernet1/0
!
interface Ethernet0/0.110
 encapsulation dot1Q 110
 ip address 193.4.110.126 255.255.255.128
 standby 110 ip 193.4.110.123
 standby 110 priority 105
 standby 110 preempt
 standby 110 track Ethernet1/0
!
interface Ethernet0/0.111
 encapsulation dot1Q 111
 ip address 193.4.111.126 255.255.255.128
 standby 111 ip 193.4.111.123
 standby 111 priority 105
 standby 111 preempt
 standby 111 track Ethernet1/0
!

```

Рисунок 3.3 – налаштування маршрутизатора R_2

Далі для забезпечення надійності мережі між маршрутизаторами R_2, R_3, R_4 було налаштовано протокол HSRP [2]. Розглянемо виконання команди show standby і show standby brief на прикладі рисунків 3.4 – 3.8.

```

R_3
R_3#
R_3#show standby
Ethernet0/0.107 - Group 107
  State is Active
    2 state changes, last state change 00:05:45
  Virtual IP address is 193.4.107.123
  Active virtual MAC address is 0000.0c07.ac6b
    Local virtual MAC address is 0000.0c07.ac6b (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.391 secs
  Preemption enabled
  Active router is local
  Standby router is 193.4.107.124, priority 100 (expires in 7.412 sec)
  Priority 105 (configured 105)
    Track interface Ethernet1/0 state Up decrement 10
  Group name is "hsrp-Et0/0.107-107" (default)
Ethernet0/0.108 - Group 108
  State is Active
    2 state changes, last state change 00:05:44
  Virtual IP address is 193.4.108.123
  Active virtual MAC address is 0000.0c07.ac6c
    Local virtual MAC address is 0000.0c07.ac6c (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.475 secs
  Preemption enabled
  Active router is local
  Standby router is 193.4.108.124, priority 100 (expires in 8.942 sec)
  Priority 105 (configured 105)
    Track interface Ethernet1/0 state Up decrement 10
  Group name is "hsrp-Et0/0.108-108" (default)
Ethernet0/0.109 - Group 109
  State is Listen
    3 state changes, last state change 00:04:34
  Virtual IP address is 193.4.109.123
  Active virtual MAC address is 0000.0c07.ac6d
    Local virtual MAC address is 0000.0c07.ac6d (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption enabled
  Active router is 193.4.109.124, priority 105 (expires in 7.467 sec)
  Standby router is 193.4.109.126, priority 100 (expires in 8.277 sec)
  Priority 96 (configured 96)
    Track interface Ethernet1/0 state Up decrement 10
  Group name is "hsrp-Et0/0.109-109" (default)

```

Рисунок 3.4 – Виконання команди show standby на R_3

```

R_3
Ethernet0/0.110 - Group 110
  State is Standby
    4 state changes, last state change 00:04:26
  Virtual IP address is 193.4.110.123
  Active virtual MAC address is 0000.0c07.ac6e
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.311 secs
  Preemption enabled
  Active router is 193.4.110.126, priority 105 (expires in 9.323 sec)
  Standby router is local
  Priority 100 (default 100)
    Track interface Ethernet1/0 state Up decrement 10
  Group name is "hsrp-Et0/0.110-110" (default)
Ethernet0/0.111 - Group 111
  State is Standby
    4 state changes, last state change 00:04:48
  Virtual IP address is 193.4.111.123
  Active virtual MAC address is 0000.0c07.ac6f
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.791 secs
  Preemption enabled
  Active router is 193.4.111.126, priority 105 (expires in 8.786 sec)
  Standby router is local
  Priority 100 (default 100)
    Track interface Ethernet1/0 state Up decrement 10
  Group name is "hsrp-Et0/0.111-111" (default)

```

Рисунок 3.5 – продовження команди show standby на R_3

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_2#show standby brief
          P indicates configured to preempt.
          |
Interface   Grp   Pri P State   Active             Standby             Virtual IP
Et0/0.107   107   96 P Listen  193.4.107.125     193.4.107.124     193.4.107.123
Et0/0.108   108   96 P Listen  193.4.108.125     193.4.108.124     193.4.108.123
Et0/0.109   109   100 P Standby 193.4.109.124     local              193.4.109.123
Et0/0.110   110   105 P Active  local              193.4.110.125     193.4.110.123
Et0/0.111   111   105 P Active  local              193.4.111.125     193.4.111.123

```

Рисунок 3.6 – Виконання команди show standby brief на R_2

```

R_3#show standby brief
          P indicates configured to preempt.
          |
Interface   Grp   Pri P State   Active             Standby             Virtual IP
Et0/0.107   107   105 P Active  local              193.4.107.124     193.4.107.123
Et0/0.108   108   105 P Active  local              193.4.108.124     193.4.108.123
Et0/0.109   109   96 P Listen  193.4.109.124     193.4.109.126     193.4.109.123
Et0/0.110   110   100 P Standby 193.4.110.126     local              193.4.110.123
Et0/0.111   111   100 P Standby 193.4.111.126     local              193.4.111.123

```

Рисунок 3.7 – Виконання команди show standby brief на R_3

```

R_4#show standby brief
          P indicates configured to preempt.
          |
Interface   Grp   Pri P State   Active             Standby             Virtual IP
Et0/0.107   107   100 P Standby 193.4.107.125     local              193.4.107.123
Et0/0.108   108   100 P Standby 193.4.108.125     local              193.4.108.123
Et0/0.109   109   105 P Active  local              193.4.109.126     193.4.109.123
Et0/0.110   110   96 P Listen  193.4.110.126     193.4.110.125     193.4.110.123
Et0/0.111   111   96 P Listen  193.4.111.126     193.4.111.125     193.4.111.123

```

Рисунок 3.8 – Виконання команди show standby brief на R_4

Створення і перевірка VLAN на комутаторах на рис. 3.9 [3].

```

SW_4(config)#Vlan 107
SW_4(config-vlan)# name LAN_107
SW_4(config-vlan)#
SW_4(config-vlan)#Vlan 108
SW_4(config-vlan)# name LAN_108
SW_4(config-vlan)#
SW_4(config-vlan)#Vlan 109
SW_4(config-vlan)# name LAN_109
SW_4(config-vlan)#
SW_4(config-vlan)#Vlan 110
SW_4(config-vlan)# name LAN_110
SW_4(config-vlan)#
SW_4(config-vlan)#Vlan 111
SW_4(config-vlan)# name LAN_111
SW_4(config-vlan)#ex
SW_4(config)#do wr
Building configuration...
Compressed configuration from 3369 bytes to 1550 bytes[OK]
SW_4(config)#do show vlan

```

VLAN	Name	Status	Ports
1	default	active	Et1/2, Et1/3, Et2/2, Et2/3 Et3/0, Et3/1, Et3/2, Et3/3
107	LAN_107	active	
108	LAN_108	active	
109	LAN_109	active	
110	LAN_110	active	
111	LAN_111	active	

Рисунок 3.9 – створення і перевірка VLAN на комутаторі SW_4

Налаштування протоколу PVST на рис. 3.10 [4].

```
SW_5(config-if)#ex
SW_5(config)#spanning-tree mode pvst
SW_5(config)#spanning-tree vlan 1,107-111 priority 16384
SW_5(config)#
```

Рисунок 3.10 – Задання пріоритету комутатору SW_5

Налаштування портів комутатора та агрегації з використанням протоколу LACP на рис. 3.11 [6].

```
SW_3
SW_3(config-if)#
SW_3(config-if)#interface e2/0
SW_3(config-if)# switchport
SW_3(config-if)# switchport trunk encapsulation dot1q
SW_3(config-if)# switchport trunk allowed vlan 107-111
SW_3(config-if)# switchport mode trunk
SW_3(config-if)# channel-protocol lacp
SW_3(config-if)# channel-group 4 mode active
SW_3(config-if)#
SW_3(config-if)#interface e2/1
SW_3(config-if)# switchport
SW_3(config-if)# switchport trunk encapsulation dot1q
SW_3(config-if)# switchport trunk allowed vlan 107-111
SW_3(config-if)# switchport mode trunk
SW_3(config-if)# channel-protocol lacp
SW_3(config-if)# channel-group 4 mode active
SW_3(config-if)#
SW_3(config-if)#interface e2/2
SW_3(config-if)# switchport
SW_3(config-if)# switchport trunk encapsulation dot1q
SW_3(config-if)# switchport trunk allowed vlan 107
SW_3(config-if)# switchport mode trunk
SW_3(config-if)# channel-protocol lacp
SW_3(config-if)# channel-group 2 mode active
SW_3(config-if)# spanning-tree guard root
SW_3(config-if)#
```

Рисунок 3.11 – Агрегація каналів з використанням протоколу LACP на SW_3

Наступний крок – це налаштування транкових каналів, через які буде рухатись трафік різних VLAN, та налаштування VLAN для кінцевих вузлів. Розглянемо налаштування port-channel на SW_3 на рис. 3.12.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

```

SW_3(config-if)#
SW_3(config-if)#interface Port-channel1
SW_3(config-if)# switchport
SW_3(config-if)# switchport trunk encapsulation dot1q
SW_3(config-if)# switchport trunk allowed vlan 107
SW_3(config-if)# switchport mode trunk
SW_3(config-if)#
SW_3(config-if)#interface Port-channel2
SW_3(config-if)# switchport
SW_3(config-if)# switchport trunk encapsulation dot1q
SW_3(config-if)# switchport trunk allowed vlan 107
SW_3(config-if)# switchport mode trunk
SW_3(config-if)#
SW_3(config-if)#interface Port-channel3
SW_3(config-if)# switchport
SW_3(config-if)# switchport trunk encapsulation dot1q
SW_3(config-if)# switchport trunk allowed vlan 107-111
SW_3(config-if)# switchport mode trunk
SW_3(config-if)#

```

Рисунок 3.12 – Налаштування транкових каналів на SW_3

Розглянемо налаштування належності кінцевих вузлів до VLAN та налаштування засобів захисту STP на комутаторі SW_8 на рис. 3.13 [5].

```

SW_8
!
interface Ethernet0/1
 switchport access vlan 111
 switchport mode access
 duplex auto
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree link-type point-to-point
!
interface Ethernet0/2
 switchport access vlan 111
 switchport mode access
 duplex auto
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree link-type point-to-point
!
interface Ethernet0/3
 switchport access vlan 111
 switchport mode access
 duplex auto
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree link-type point-to-point
!

```

Рисунок 3.13 – Налаштування належності кінцевих вузлів до VLAN та налаштування засобів захисту STP

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Перевірка працездатності мережі

Перевіримо наявність зв'язку між кінцевими вузлами в одній VLAN та зв'язок між кінцевими вузлами різних VLAN на рис. 3.15 – 3.21.

```
WS111.2
111.2> ping 193.4.111.5
84 bytes from 193.4.111.5 icmp_seq=1 ttl=64 time=4.159 ms
84 bytes from 193.4.111.5 icmp_seq=2 ttl=64 time=3.719 ms
84 bytes from 193.4.111.5 icmp_seq=3 ttl=64 time=4.081 ms
84 bytes from 193.4.111.5 icmp_seq=4 ttl=64 time=3.770 ms
84 bytes from 193.4.111.5 icmp_seq=5 ttl=64 time=3.498 ms

111.2>
111.2>
111.2>

WS111.5
WS111.5> ping 193.4.111.2
84 bytes from 193.4.111.2 icmp_seq=1 ttl=64 time=3.358 ms
84 bytes from 193.4.111.2 icmp_seq=2 ttl=64 time=4.224 ms
84 bytes from 193.4.111.2 icmp_seq=3 ttl=64 time=3.965 ms
84 bytes from 193.4.111.2 icmp_seq=4 ttl=64 time=4.178 ms
84 bytes from 193.4.111.2 icmp_seq=5 ttl=64 time=3.378 ms

WS111.5>
WS111.5>
```

Рисунок 3.15 – перевірка зв'язку між SW_8 і SW_7 (VLAN_111)

```
WS107.1
WS107.1> ping 193.4.107.2
84 bytes from 193.4.107.2 icmp_seq=1 ttl=64 time=3.444 ms
84 bytes from 193.4.107.2 icmp_seq=2 ttl=64 time=3.047 ms
84 bytes from 193.4.107.2 icmp_seq=3 ttl=64 time=4.166 ms
84 bytes from 193.4.107.2 icmp_seq=4 ttl=64 time=3.603 ms
84 bytes from 193.4.107.2 icmp_seq=5 ttl=64 time=3.651 ms

WS107.1>

WS107.2
WS107.2> ping 193.4.107.1
84 bytes from 193.4.107.1 icmp_seq=1 ttl=64 time=4.257 ms
84 bytes from 193.4.107.1 icmp_seq=2 ttl=64 time=2.699 ms
84 bytes from 193.4.107.1 icmp_seq=3 ttl=64 time=2.985 ms
84 bytes from 193.4.107.1 icmp_seq=4 ttl=64 time=4.121 ms
84 bytes from 193.4.107.1 icmp_seq=5 ttl=64 time=4.339 ms

WS107.2>
```

Рисунок 3.16 – перевірка зв'язку між SW_13 і SW_14 (VLAN_107)

```
WS109.2
WS109.2> ping 193.4.109.3
84 bytes from 193.4.109.3 icmp_seq=1 ttl=64 time=1.688 ms
84 bytes from 193.4.109.3 icmp_seq=2 ttl=64 time=2.006 ms
84 bytes from 193.4.109.3 icmp_seq=3 ttl=64 time=1.816 ms
84 bytes from 193.4.109.3 icmp_seq=4 ttl=64 time=1.821 ms
84 bytes from 193.4.109.3 icmp_seq=5 ttl=64 time=1.634 ms

WS109.2>
WS109.2>
WS109.2>
WS109.2>
WS109.2>

WS109.3
WS109.3> show ip

NAME       : WS109.3[1]
IP/MASK    : 193.4.109.3/25
GATEWAY    : 193.4.109.123
DNS        :
MAC        : 00:50:79:66:68:02
LPORT     : 10029
RHOST:PORT : 127.0.0.1:10030
MTU       : 1500

WS109.3>
```

Рисунок 3.17 – перевірка зв'язку між SW_10 і SW_11 (VLAN_109)

```
WS109.1
WS109.1> ping 193.4.110.2
84 bytes from 193.4.110.2 icmp_seq=1 ttl=63 time=24.593 ms
84 bytes from 193.4.110.2 icmp_seq=2 ttl=63 time=17.974 ms
84 bytes from 193.4.110.2 icmp_seq=3 ttl=63 time=16.062 ms
84 bytes from 193.4.110.2 icmp_seq=4 ttl=63 time=25.539 ms
84 bytes from 193.4.110.2 icmp_seq=5 ttl=63 time=15.080 ms

WS109.1> show ip

NAME       : WS109.1[1]
IP/MASK    : 193.4.109.1/25
GATEWAY    : 193.4.109.123
DNS        :
MAC        : 00:50:79:66:68:00
LPORT     : 10025
RHOST:PORT : 127.0.0.1:10026
MTU       : 1500

WS110.2
WS110.2> ping 193.4.109.1
84 bytes from 193.4.109.1 icmp_seq=1 ttl=63 time=25.342 ms
84 bytes from 193.4.109.1 icmp_seq=2 ttl=63 time=21.251 ms
84 bytes from 193.4.109.1 icmp_seq=3 ttl=63 time=21.700 ms
84 bytes from 193.4.109.1 icmp_seq=4 ttl=63 time=24.311 ms
84 bytes from 193.4.109.1 icmp_seq=5 ttl=63 time=22.755 ms

WS110.2>
WS110.2>
WS110.2>
WS110.2>
WS110.2>
WS110.2>
WS110.2>
WS110.2>
WS110.2>
```

Рисунок 3.18 – перевірка зв'язку між VLAN_109 і VLAN_110

WS107.1	WS111.1
WS107.1> ping 193.4.111.1	WS111.1> ping 193.4.107.1
84 bytes from 193.4.111.1 icmp_seq=1 ttl=63 time=17.425 ms	84 bytes from 193.4.107.1 icmp_seq=1 ttl=63 time=19.632 ms
84 bytes from 193.4.111.1 icmp_seq=2 ttl=63 time=23.331 ms	84 bytes from 193.4.107.1 icmp_seq=2 ttl=63 time=20.562 ms
84 bytes from 193.4.111.1 icmp_seq=3 ttl=63 time=25.227 ms	84 bytes from 193.4.107.1 icmp_seq=3 ttl=63 time=26.314 ms
84 bytes from 193.4.111.1 icmp_seq=4 ttl=63 time=24.821 ms	84 bytes from 193.4.107.1 icmp_seq=4 ttl=63 time=26.794 ms
84 bytes from 193.4.111.1 icmp_seq=5 ttl=63 time=15.763 ms	84 bytes from 193.4.107.1 icmp_seq=5 ttl=63 time=17.966 ms
WS107.1>	WS111.1>
WS107.1>	WS111.1>

Рисунок 3.19 – перевірка зв'язку між VLAN_107 і VLAN_111

WS111.1	WS110.2
WS111.1>	WS110.2>
WS111.1> ping 193.4.110.2	WS110.2> ping 193.4.111.1
84 bytes from 193.4.110.2 icmp_seq=1 ttl=63 time=32.033 ms	84 bytes from 193.4.111.1 icmp_seq=1 ttl=63 time=24.190 ms
84 bytes from 193.4.110.2 icmp_seq=2 ttl=63 time=23.515 ms	84 bytes from 193.4.111.1 icmp_seq=2 ttl=63 time=19.670 ms
84 bytes from 193.4.110.2 icmp_seq=3 ttl=63 time=17.774 ms	84 bytes from 193.4.111.1 icmp_seq=3 ttl=63 time=14.238 ms
84 bytes from 193.4.110.2 icmp_seq=4 ttl=63 time=16.605 ms	84 bytes from 193.4.111.1 icmp_seq=4 ttl=63 time=22.208 ms
84 bytes from 193.4.110.2 icmp_seq=5 ttl=63 time=34.605 ms	84 bytes from 193.4.111.1 icmp_seq=5 ttl=63 time=16.794 ms
WS111.1>	WS110.2>

Рисунок 3.20 – перевірка зв'язку між VLAN_111 і VLAN_110

WS109.1	WS107.1
WS109.1>	WS107.1>
WS109.1> ping 193.4.107.1	WS107.1> ping 193.4.109.1
84 bytes from 193.4.107.1 icmp_seq=1 ttl=63 time=23.740 ms	84 bytes from 193.4.109.1 icmp_seq=1 ttl=63 time=18.113 ms
84 bytes from 193.4.107.1 icmp_seq=2 ttl=63 time=27.965 ms	84 bytes from 193.4.109.1 icmp_seq=2 ttl=63 time=17.258 ms
84 bytes from 193.4.107.1 icmp_seq=3 ttl=63 time=20.799 ms	84 bytes from 193.4.109.1 icmp_seq=3 ttl=63 time=14.688 ms
84 bytes from 193.4.107.1 icmp_seq=4 ttl=63 time=20.593 ms	84 bytes from 193.4.109.1 icmp_seq=4 ttl=63 time=22.673 ms
84 bytes from 193.4.107.1 icmp_seq=5 ttl=63 time=22.144 ms	84 bytes from 193.4.109.1 icmp_seq=5 ttl=63 time=17.596 ms
WS109.1>	WS107.1>

Рисунок 3.21 – перевірка зв'язку між VLAN_109 і VLAN_107

Перевіримо роботу протоколу HSRP, а саме відключимо інтерфейс Ethernet0/0 на маршрутизаторі R_3 (рис. 3.22). Через відключення даного інтерфейсу пріоритет маршрутизатора має декрементуватись на 10 одиниць і активним маршрутизатором стане R_4 (рис. 3.25).

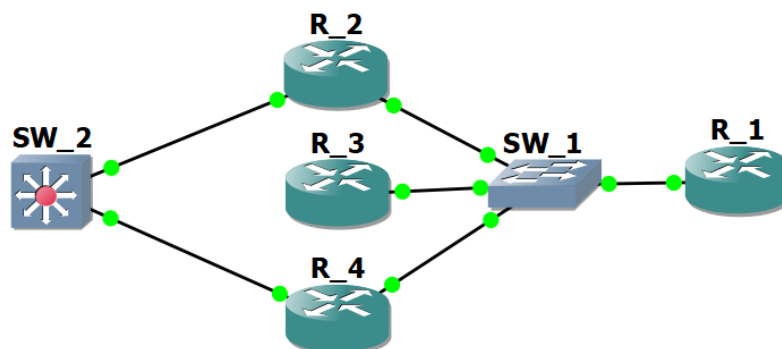


Рисунок 3.22 – відключимо інтерфейс Ethernet0/0 на маршрутизаторі R_3

```

R_3#show standby
Ethernet0/0.107 - Group 107
  State is Active
    2 state changes, last state change 00:12:00
  Virtual IP address is 193.4.107.123
  Active virtual MAC address is 0000.0c07.ac6b
    Local virtual MAC address is 0000.0c07.ac6b (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.250 secs
  Preemption enabled
  Active router is local
  Standby router is 193.4.107.124, priority 100 (expires in 7.191 sec)
  Priority 105 (configured 105)
    Track interface Ethernet1/0 state Up decrement 10
  Group name is "hsrp-Et0/0.107-107" (default)

```

Рисунок 3.23 – Виконання команди show standby на маршрутизаторі R_3 до відключення інтерфейсу

```

R_4#show standby
Ethernet0/0.107 - Group 107
  State is Standby
    4 state changes, last state change 00:11:01
  Virtual IP address is 193.4.107.123
  Active virtual MAC address is 0000.0c07.ac6b
    Local virtual MAC address is 0000.0c07.ac6b (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.446 secs
  Preemption enabled
  Active router is 193.4.107.125, priority 105 (expires in 9.560 sec)
  Standby router is local
  Priority 100 (default 100)
    Track interface Ethernet1/0 state Up decrement 10
  Group name is "hsrp-Et0/0.107-107" (default)

```

Рисунок 3.24 – Виконання команди show standby на маршрутизаторі R_4 до відключення інтерфейсу

```

R_4#show standby
Ethernet0/0.107 - Group 107
  State is Active
    8 state changes, last state change 00:00:37
  Virtual IP address is 193.4.107.123
  Active virtual MAC address is 0000.0c07.ac6b
    Local virtual MAC address is 0000.0c07.ac6b (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.738 secs
  Preemption enabled
  Active router is local
  Standby router is 193.4.107.126, priority 96 (expires in 9.688 sec)
  Priority 100 (default 100)
    Track interface Ethernet1/0 state Up decrement 10
  Group name is "hsrp-Et0/0.107-107" (default)

```

Рисунок 3.25 – Виконання команди show standby на маршрутизаторі R_4 після відключення інтерфейсу

Перевірка показала, що протокол спрацював успішно.

Перевіримо таблицю маршрутизації на маршрутизаторі R_1 за допомогою команди show ip route (рис. 3.26).

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_1#
R_1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    193.4.107.0/25 is subnetted, 1 subnets
O       193.4.107.0 [110/20] via 194.4.7.4, 00:15:03, Ethernet0/0
           [110/20] via 194.4.7.3, 00:15:13, Ethernet0/0
           [110/20] via 194.4.7.2, 00:13:59, Ethernet0/0
    193.4.111.0/25 is subnetted, 1 subnets
O       193.4.111.0 [110/20] via 194.4.7.4, 00:15:03, Ethernet0/0
           [110/20] via 194.4.7.3, 00:15:13, Ethernet0/0
           [110/20] via 194.4.7.2, 00:13:59, Ethernet0/0
    193.4.110.0/25 is subnetted, 1 subnets
O       193.4.110.0 [110/20] via 194.4.7.4, 00:15:05, Ethernet0/0
           [110/20] via 194.4.7.3, 00:15:15, Ethernet0/0
           [110/20] via 194.4.7.2, 00:14:00, Ethernet0/0
    193.4.109.0/25 is subnetted, 1 subnets
O       193.4.109.0 [110/20] via 194.4.7.4, 00:15:07, Ethernet0/0
           [110/20] via 194.4.7.3, 00:15:17, Ethernet0/0
           [110/20] via 194.4.7.2, 00:14:12, Ethernet0/0
    193.4.108.0/25 is subnetted, 1 subnets
O       193.4.108.0 [110/20] via 194.4.7.4, 00:15:07, Ethernet0/0
           [110/20] via 194.4.7.3, 00:15:17, Ethernet0/0
           [110/20] via 194.4.7.2, 00:14:03, Ethernet0/0
    194.4.7.0/26 is subnetted, 1 subnets
C       194.4.7.0 is directly connected, Ethernet0/0
R_1#

```

Рисунок 3.26 – Виконання команди show ip route на маршрутизаторі R_1

3.3 Встановлення і налаштування ОС Ubuntu Server

Встановлення і налаштування ОС Ubuntu Server на VirtualBox (рис. 3.27):

Рисунок 3.27 – налаштування профілю і логіну ОС

Починаючи з Ubuntu 18.04 налаштування і перевірка конфігурації мережевих інтерфейсів відбувається не в звичному каталозі /etc/network/interfaces, а в каталозі /etc/netplan (рис. 3.28). Після встановлення системи в ньому буде згенеровано відповідний конфігураційний файл, який необхідно відредагувати (рис. 3.29).

```
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ sudo ls /etc/netplan
01-netconf.yaml
ubuntu@ubuntu:~$ sudo nano /etc/netplan/01-netconf.yaml
```

Рисунок 3.28 – відкриття каталогу /etc/netplan

```
GNU nano 4.8 /etc/netplan/01-netconf.yaml
# This is the network config written by 'subiquity'
network:
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      dhcp6: no
      addresses: [194.4.7.5/26]
      gateway4: 194.4.7.1
  version: 2
```

Рисунок 3.29 – зміна ір конфігурації

```
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ sudo netplan apply
ubuntu@ubuntu:~$
```

Рисунок 3.30 – активація ір конфігурації

За допомогою команди `ip address` перевіримо ір-адресу (рис. 3.31).

```
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a5:9a:0f brd ff:ff:ff:ff:ff:ff
    inet 194.4.7.5/26 brd 194.4.7.63 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea5:9a0f/64 scope link
        valid_lft forever preferred_lft forever
```

Рисунок 3.31 – перевірка ір-адреси

За допомогою команди `ping` перевіримо зв'язок з маршрутизатором R_1 (рис. 3.32).

```
ubuntu@ubuntu:~$ ping 194.4.7.1
PING 194.4.7.1 (194.4.7.1) 56(84) bytes of data.
64 bytes from 194.4.7.1: icmp_seq=1 ttl=255 time=97.3 ms
64 bytes from 194.4.7.1: icmp_seq=2 ttl=255 time=8.42 ms
64 bytes from 194.4.7.1: icmp_seq=3 ttl=255 time=2.60 ms
64 bytes from 194.4.7.1: icmp_seq=4 ttl=255 time=7.59 ms
64 bytes from 194.4.7.1: icmp_seq=5 ttl=255 time=9.63 ms
64 bytes from 194.4.7.1: icmp_seq=6 ttl=255 time=12.6 ms
64 bytes from 194.4.7.1: icmp_seq=7 ttl=255 time=6.37 ms
64 bytes from 194.4.7.1: icmp_seq=8 ttl=255 time=9.55 ms
64 bytes from 194.4.7.1: icmp_seq=9 ttl=255 time=2.85 ms
64 bytes from 194.4.7.1: icmp_seq=10 ttl=255 time=4.36 ms
^C
--- 194.4.7.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9035ms
rtt min/avg/max/mdev = 2.604/16.127/97.298/27.224 ms
ubuntu@ubuntu:~$
```

Рисунок 3.32 – перевірка зв'язку між Сервером і маршрутизатором R_1

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

Далі зайдемо в робочу станцію WS_Windows і перевіримо зв'язок з сервером (рис. 3.33). Проведемо підключення по SSH за допомогою утиліти putty (рис. 3.34).

```
C:\Users\Student>ping 194.4.7.5

Pinging 194.4.7.5 with 32 bytes of data:
Reply from 194.4.7.5: bytes=32 time=18ms TTL=62
Reply from 194.4.7.5: bytes=32 time=29ms TTL=62
Request timed out.
Reply from 194.4.7.5: bytes=32 time=24ms TTL=62

Ping statistics for 194.4.7.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 29ms, Average = 23ms

C:\Users\Student>_
```

Рисунок 3.33 – перевірка зв'язку між робочою станцією WS_Windows і Сервером

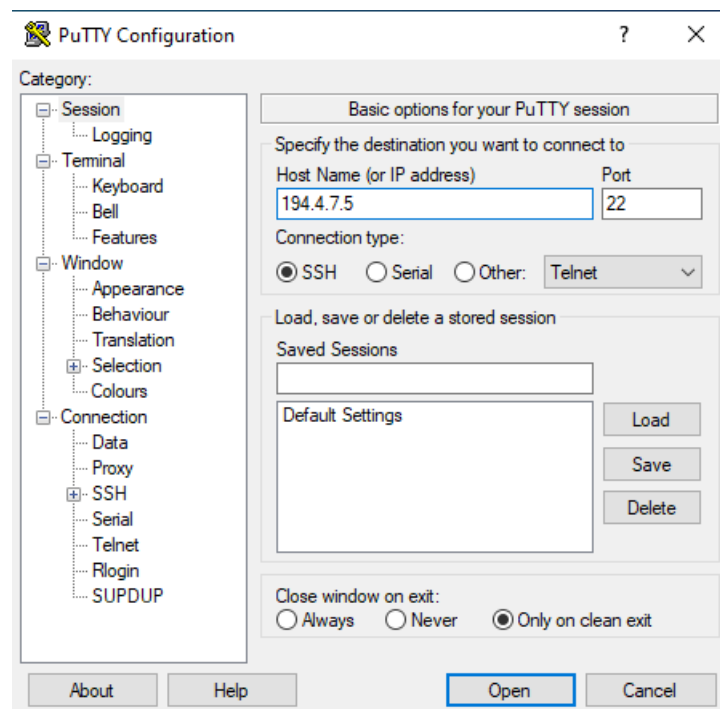


Рисунок 3.34 – підключення до сервера Ubuntu Server через програму putty на робочій станції WS_Windows

```

ubuntu@ubuntu: ~
login as: ubuntu
ubuntu@194.4.7.5's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-117-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Wed 15 Jun 2022 07:07:54 PM UTC

System load:  0.33               Processes:            123
Usage of /:   23.5% of 18.57GB   Users logged in:     1
Memory usage: 25%               IPv4 address for enp0s3: 194.4.7.5
Swap usage:   0%

* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

42 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Wed Jun 15 18:28:17 2022
ubuntu@ubuntu:~$

```

Рисунок 3.35 – успішне підключення до сервера Ubuntu Server через програму putty на робочій станції WS_Windows

3.4 Організація мережі на ОС Ubuntu Server

3.4.1 Захист за допомогою брандмауера

Ядро Linux забезпечує вбудований механізм фільтрації пакетів під назвою netfilter, який використовується для фільтрації трафіку, що надходить або виходить з системи. Усі сучасні системи брандмауера Linux використовують сітковий фільтр вбудований у ядро системи. Iptables – це добре відомий і популярний інтерфейс користувача для налаштування та керування правилами фільтрації для netfilter. Це повноцінне рішення брандмауера, яке легко налаштовується і є дуже гнучким. Однак iptables потребує зусиль з боку користувача, щоб освоїти процес складного налаштування. Для спрощення конфігурації iptables були розроблені різні додаткові інструменти для роботи з брандмауером.

UFW є інтерфейсом iptables, призначений для спрощення процесу налаштування брандмауера. Оскільки ми шукаємо простий і нескладний спосіб захистити нашу мережу, то такий інструмент як UFW підходить для виконання завдань у рамках цієї кваліфікаційної роботи.

		Борейченко Г.О.			KIK.KP.B – 123 – 07 – ПЗ	Арк.
		Головня О.С.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Зазвичай UFW попередньо встановлено в системах Ubuntu. Якщо це не так, його необхідно встановити за допомогою наступної команди (рис. 3.36).

```
ubuntu@ubuntu:~$ sudo apt-get install UFW
Reading package lists... Done
Building dependency tree
Reading state information... Done
5: Unable to locate package UFW
```

Рисунок 3.36 – встановлення UFW

Перевіримо статус UFW (рис. 3.37).

```
ubuntu@ubuntu:~$ sudo ufw status
Status: inactive
ubuntu@ubuntu:~$
```

Рисунок 3.37 – перевірка статусу UFW

Щоб дозволити підключення по SSH, необхідно додати нове правило до брандмауера (рис. 3.38). Дозволимо лише трафік TCP через HTTP (порт 80).

```
ubuntu@ubuntu:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
ubuntu@ubuntu:~$ sudo ufw allow http/tcp
Rules updated
Rules updated (v6)
ubuntu@ubuntu:~$
```

Рисунок 3.38 – додавання нових правил UFW

Заборонимо вхідний FTP-трафік (рис. 3.39).

```
ubuntu@ubuntu:~$ sudo ufw deny ftp
Rules updated
Rules updated (v6)
ubuntu@ubuntu:~$
```

Рисунок 3.39 – додавання нових правил UFW

Перевіримо всі додані правила перед запуском брандмауера (рис. 3.40).

```
ubuntu@ubuntu:~$ sudo ufw show added
Added user rules (see 'ufw status' for running firewall):
ufw allow 22/tcp
ufw allow 80/tcp
ufw deny 21/tcp
ubuntu@ubuntu:~$ _
```

Рисунок 3.40 – перевірка доданих правил UFW

Тепер увімкнемо брандмауер (рис. 3.41).

```
ubuntu@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
ubuntu@ubuntu:~$
```

Рисунок 3.41 – увімкнення UFW

Перевіримо статус ufw (рис. 3.42).

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

```
ubuntu@ubuntu:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22/tcp ALLOW IN Anywhere
80/tcp ALLOW IN Anywhere
21/tcp DENY IN Anywhere
22/tcp (v6) ALLOW IN Anywhere (v6)
80/tcp (v6) ALLOW IN Anywhere (v6)
21/tcp (v6) DENY IN Anywhere (v6)
```

Рисунок 3.42 – перевірка статусу роботи UFW

Отримаємо нумерований список доданих правил (рис. 3.43).

```
ubuntu@ubuntu:~$ sudo ufw status numbered
Status: active

To Action From
--
[ 1] 22/tcp ALLOW IN Anywhere
[ 2] 80/tcp ALLOW IN Anywhere
[ 3] 21/tcp DENY IN Anywhere
[ 4] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 5] 80/tcp (v6) ALLOW IN Anywhere (v6)
[ 6] 21/tcp (v6) DENY IN Anywhere (v6)
```

Рисунок 3.43 – виведення нумерованого списку доданих правил UFW

3.4.2 Захист віддаленого доступу

Для захисту віддаленого доступу було обрано OpenVPN. Перед налаштуванням програми на Ubuntu необхідно встановити брандмауер, що було зроблено у попередньому розділі. Перевіримо статус і додамо виключення для порту 993, де пізніше налаштуємо сервер OpenVPN (рис. 3.44).

```
ubuntu@ubuntu:~$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
993/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
993/tcp (v6) ALLOW Anywhere (v6)
```

Рисунок 3.44 – виведення списку доданих правил UFW

Проведемо завантаження орепвнрп з репозиторію (рис. 3.45).

```
ubuntu@ubuntu:~$ wget https://git.io/vpn -O openvpn-install.sh
--2022-06-15 15:41:54-- https://git.io/vpn
Resolving git.io (git.io)... 140.82.112.21
Connecting to git.io (git.io)|140.82.112.21|:443... connected.
HTTP request sent, awaiting response... 302 Found
```

Рисунок 3.45 – завантаження орепвнрп з репозиторію

Запустимо скрипт на виконання.

```
ubuntu@ubuntu:~$ sudo bash openvpn-install.sh
```

Рисунок 3.46 – запуск завантаженого скрипта

Після запуску скрипта необхідно провести основні налаштування VPN сервера. А саме протокол по якому буде працювати сервер, в нашому випадку – це протокол UDP [28]. Далі порт, на якому буде працювати OpenVPN – порт 993. Який саме сервер будемо використовувати, CloudFlare самий популярний тому вибираємо його. Далі вказуємо ім'я користувача (рис. 3.47).

```
Which protocol should OpenVPN use?
 1) UDP (recommended)
 2) TCP
Protocol [1]: 1

What port should OpenVPN listen to?
Port [1194]: 993

Select a DNS server for the clients:
 1) Current system resolvers
 2) Google
 3) 1.1.1.1
 4) OpenDNS
 5) Quad9
 6) AdGuard
DNS server [1]: 3

Enter a name for the first client:
Name [client]: client-01

OpenVPN installation is ready to begin.
Press any key to continue...
```

Рисунок 3.47 – налаштування OpenVPN

```
Finished!

The client configuration is available in: /root/client-01.ovpn
New clients can be added by running this script again.
ubuntu@ubuntu:~$
```

Рисунок 3.48 – успішне налаштування OpenVPN

Далі необхідно налаштувати клієнт OpenVPN для робочої станції Windows на якій будемо користуватись OpenVPN (рис. 3.49). Для цього необхідно завантажити інсталяційний файл з офіційного веб-сайту [17].

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

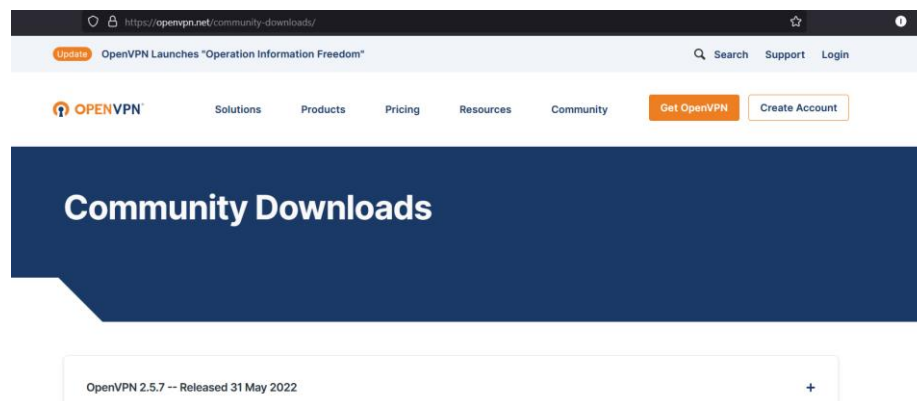


Рисунок 3.49 – завантаження інсталяційного пакету OpenVPN для Windows з офіційного сайту

За допомогою програми WinSCP завантажимо файл конфігурації з Ubuntu Server на робочу станцію Windows (рис. 3.50).

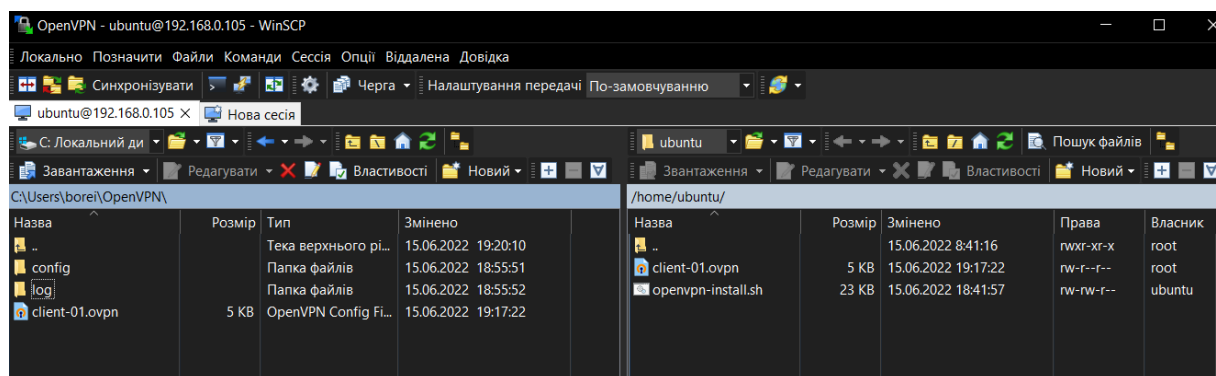


Рисунок 3.50 – завантаження у WinSCP

Запустимо програму і додамо конфігураційний файл (рис. 3.51). Після запуску програма вимагає конфігураційний файл, який завантажили з Ubuntu Server на робочу станцію Windows. Після відкриття файлу сервер OpenVPN повинен успішно запуститись (рис. 3.52) [28].

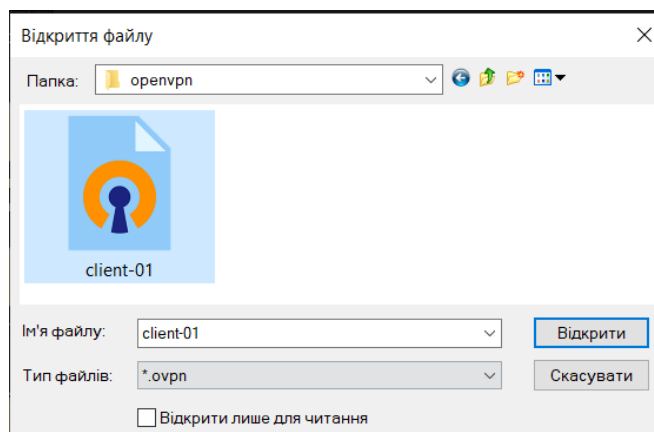


Рисунок 3.51 – конфігураційний файл OpenVPN

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

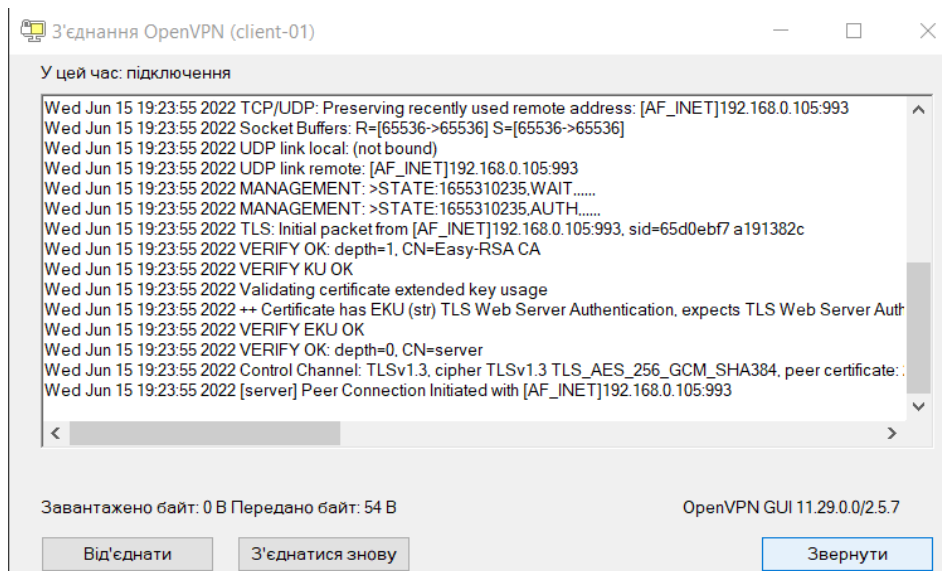


Рисунок 3.52 – успішний запуск OpenVPN на робочій станції Windows

Перевірка роботи OpenVPN до запуску програми (рис. 3.53) і після зміни- лась IP-адреса і країна (рис. 3.54).

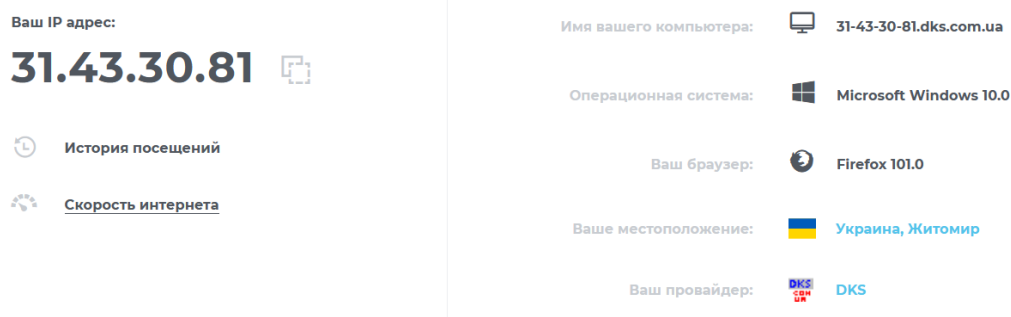


Рисунок 3.53 – перевірка IP-адреси до налаштування OpenVPN

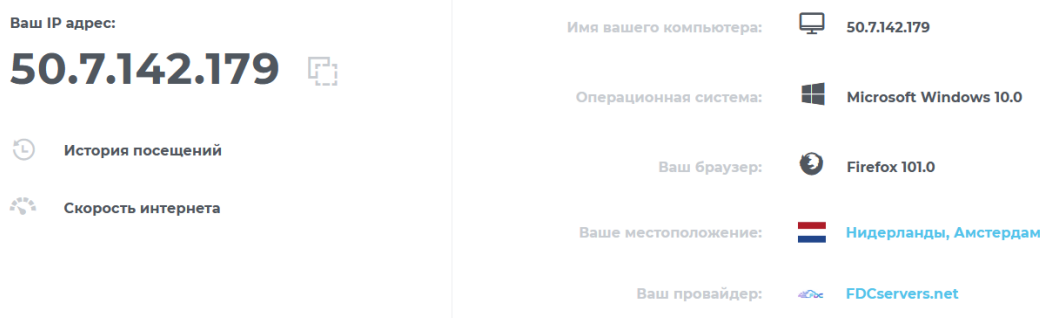


Рисунок 3.54 – перевірка IP-адреси після налаштування OpenVPN

3.4.3 Захист від мережних атак

Програма Fail2ban працює шляхом моніторингу конфігураційних файлів журналу безпеки. Вона використовує регулярні вирази, які називаються фільт-

		Борейченко Г.О.			KIK.KP.B – 123 – 07 – ПЗ	Арк.
		Головня О.С.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

рами, для виявлення записів журналу, які відповідають певним критеріям, наприклад як невдалі спроби входу або підключення до серверу. Установка fail2ban за замовчуванням надає різні фільтри, які можуть бути знайдено в каталозі /etc/fail2ban/filter.d. Завжди можна створити власні фільтри і використовувати їх для виявлення записів журналу, які відповідають вашим критеріям. Однак існуючого потенціалу програми достатньо для захисту сервера у даній кваліфікаційній роботі.

Як тільки fail2ban виявить підозрілий хост або робочу станцію, яка намагається підключитись до сервера, і яка не відповідає налаштованим фільтрам fail2ban, програма налаштує параметри брандмауера так, щоб відхилити відповідну IP-адресу від підключення до системи.

Вона доступна у сховищі пакетів Ubuntu, тому ми можемо встановити її за допомогою команди, як показано нижче на рисунку 3.55.

```
ubuntu@ubuntu:~$ sudo apt-get install fail2ban
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Рисунок 3.55 – встановлення Fail2ban

Створимо копію файлу конфігурації fail2ban для локальних змін (рис. 3.56).

```
ubuntu@ubuntu:~$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ _
```

Рисунок 3.56 – створення локальної копії у директорії /etc/fail2ban

Відкриємо новий файл конфігурації у редакторі:

```
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ sudo nano /etc/fail2ban/jail.local_
```

Рисунок 3.57 – відкриття файлу конфігурації fail2ban у редакторі nano

Далі необхідно змінити налаштування, наведені в розділі [DEFAULT] (далі рис. 3.58). Для цього необхідно розкоментувати відповідні рядки, як це показано на рисунку 3.58. Додати свою IP-адресу до списку ігнорованих IP-адрес. Bantime – час, на який блокується хост користувача, findtime – час, на який приймається виклик хоста, maxretry – кількість невдалих спроб входу для блокування робочої станції.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

```

GNU nano 4.8 /etc/fail2ban/jail.local
# will not ban a host which matches an address in this list. Several addresses
# can be defined using space (and/or comma) separator.
ignoreip = 127.0.0.1/8 ::1 10.0.2.15

# External command that will take an tagged arguments to ignore, e.g. <ip>,
# and return true if the IP is to be ignored. False otherwise.
#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime = 10m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 10m

# "maxretry" is the number of failures before a host get banned.
maxretry = 5

```

Рисунок 3.58 – налаштування файлу конфігурації fail2ban у редакторі nano

Далі встановлюємо свою адресу електронної пошти, оскільки хотіли б отримувати сповіщення електронною поштою про заборону дій у вашій системі (рис. 3.59).

```

# Some options used for actions

# Destination email address used solely for the interpolations in
# jail.{conf,local,d/*} configuration files.
destemail = boreichenkoglib@gmail.com

# Sender email address used solely for some actions
sender = root@<fq-hostname>

# E-mail action. Since 0.8.1 Fail2Ban uses sendmail MTA for the
# mailing. Change mta configuration parameter to mail if you want to
# revert to conventional 'mail'.
mta = sendmail

```

Рисунок 3.59 – встановлення адреси електронної пошти

Служба SSH вимкнена за замовчуванням, її необхідно увімкнути (рис. 3.60).

```

[sshd]
enabled = true_
# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode = normal
port = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s

```

Рисунок 3.60 – увімкнення SSH

Перезапустимо службу fail2ban та перевіримо iptables на наявність правил, створених fail2ban (рис. 3.61).

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ubuntu@ubuntu:~$ sudo service fail2ban restart
ubuntu@ubuntu:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT

```

Рисунок 3.61 – перевірка доданих налаштувань fail2ban

3.4.4 Моніторинг активності мережі

Коли ми говоримо про сервер, його мережеве з'єднання з навколишньою мережею є найважливішим ресурсом. Особливо у хмарній мережі, коли це єдиний канал зв'язку для доступу клієнта до сервера і навпаки. Неправильно налаштовані комп'ютерні мережі є ненадійним каналом зв'язку. Ви можете втратити деякі дані під час передачі, дані можуть бути скомпроментовані або зловмисник може змінити вихідні дані і отримати доступ до них, перш ніж вони дійдуть до адресата.

Сервер Ubuntu, як і Linux загалом, надає безліч утиліт для полегшення роботи моніторингу та адміністрування мережі. Цей розділ охоплює деякі вбудовані інструменти для моніторингу трафіку мережі та його продуктивності. Ми також розглянемо кілька додаткових інструментів для моніторингу мережі.

Почнемо з основних мережевих команд, `ifconfig` і `ping`. `Ifconfig` зазвичай використовується для читання мережі конфігурації та отримання деталей підключення мережевих інтерфейсів. Окрім основного використання, `ifconfig` може також використовуватися для налаштування мережевого інтерфейсу.

Ми почнемо з часто використовуваної команди, тобто `ifconfig`. Переважно використовуємо цю команду, щоб прочитати деталі конфігурації мережі, такі як IP-адреса. При виклику без будь-яких параметрів `ifconfig` відображає деталі всієї активної мережі та інтерфейси наступним чином (рис. 3.62).

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

```

ubuntu@ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 194.4.7.5 netmask 255.255.255.192 broadcast 194.4.7.63
    inet6 fe80::a00:27ff:fea5:9a0f prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:a5:9a:0f txqueuelen 1000 (Ethernet)
    RX packets 86 bytes 8378 (8.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 100 bytes 13938 (13.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 5091 bytes 362535 (362.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5091 bytes 362535 (362.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Рисунок 3.62 – запуск команди ifconfig

Якщо потрібна лише швидка мережева статистика, можна використати ifconfig з прапорцем -s, наступним чином (рис. 3.63).

```

ubuntu@ubuntu:~$ ifconfig -s

```

Iface	MTU	RX-OK	RX-ERR	RX-DRP	RX-OVR	TX-OK	TX-ERR	TX-DRP	TX-OVR	Flg
enp0s3	1500	99	0	0 0		107	0	0	0	BMRU
lo	65536	5411	0	0 0		5411	0	0	0	LRU

Рисунок 3.63 – швидка статистика ifconfig

Іншою часто використовуваною командою є ping (рис. 3.64). Він надсилає запити ICMP до вказаного хоста і чекає відповіді. Якщо запитати ім'я хоста, ping отримає його IP-адресу від DNS. Це також дозволяє підтвердити, що DNS працює належним чином. Пінг також дає необхідні дані про затримку при пересиланні даних.

```

ubuntu@ubuntu:~$ ping www.google.com -c 4
PING www.google.com (142.251.39.68) 56(84) bytes of data:
64 bytes from bud02s39-in-f4.1e100.net (142.251.39.68): icmp_seq=1 ttl=114 time=100 ms
64 bytes from bud02s39-in-f4.1e100.net (142.251.39.68): icmp_seq=2 ttl=114 time=142 ms
64 bytes from bud02s39-in-f4.1e100.net (142.251.39.68): icmp_seq=3 ttl=114 time=76.3 ms
64 bytes from bud02s39-in-f4.1e100.net (142.251.39.68): icmp_seq=4 ttl=114 time=69.5 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3410ms
rtt min/avg/max/mdev = 69.476/96.959/141.539/28.200 ms
ubuntu@ubuntu:~$

```

Рисунок 3.64 – пінгування серверу www.google.com

За допомогою netstat можна отримати список усіх мережевих сокетів і їхні відповідні процеси, що використовують ці з'єднання у системі Ubuntu Server. З різними параметрами можна легко відокремлювати активні або слухаючі з'єднання і навіть окремі з'єднання за допомогою різних протоколів. Крім того,

netstat надає детальні таблиці маршрутизації та інформацію про мережеву статистику. Зазвичай використовується наступний синтаксис команди (рис. 3.65).

```
ubuntu@ubuntu:~$ sudo netstat -pltn
[sudo] password for ubuntu:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN      676/systemd-resolve
tcp        0      0 0.0.0.0:22            0.0.0.0:*               LISTEN      872/sshd: /usr/sbin
tcp6       0      0 :::80                 :::*                   LISTEN      895/apache2
tcp6       0      0 :::22                 :::*                   LISTEN      872/sshd: /usr/sbin
udp        0      0 127.0.0.53:53          0.0.0.0:*               676/systemd-resolve
udp        0      0 0.0.0.0:5353          0.0.0.0:*               687/avahi-daemon: r
udp        0      0 0.0.0.0:33006         0.0.0.0:*               687/avahi-daemon: r
udp6       0      0 :::56923              :::*                   687/avahi-daemon: r
udp6       0      0 :::5353               :::*                   687/avahi-daemon: r
ubuntu@ubuntu:~$
```

Рисунок 3.65 – команда netstat

Таблиця маршрутизації може бути викликана за допомогою прапорця -r (рис. 3.66).

```
ubuntu@ubuntu:~$ sudo netstat -r
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default _gateway 0.0.0.0 UG 0 0 0 enp0s3
194.4.7.0 0.0.0.0 255.255.255.192 U 0 0 0 enp0s3
ubuntu@ubuntu:~$
```

Рисунок 3.66 – команда netstat

Інша команда, lsof (рис. 3.67), виводить список усіх відкритих файлів. Він включає файли, які використовуються для мережевих підключень. Використаємо команду з прапорцем -i, щоб відобразити всі мережеві файли, як показано нижче:

```
ubuntu@ubuntu:~$ sudo lsof -i
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
systemd-r 676 systemd-resolve 12u IPv4 21675 0t0 UDP localhost:domain
systemd-r 676 systemd-resolve 13u IPv4 21676 0t0 TCP localhost:domain (LISTEN)
avahi-dae 687 avahi 12u IPv4 23294 0t0 UDP *:mdns
avahi-dae 687 avahi 13u IPv6 23295 0t0 UDP *:mdns
avahi-dae 687 avahi 14u IPv4 23296 0t0 UDP *:33006
avahi-dae 687 avahi 15u IPv6 23297 0t0 UDP *:56923
sshd 872 root 3u IPv4 27069 0t0 TCP *:ssh (LISTEN)
sshd 872 root 4u IPv6 27071 0t0 TCP *:ssh (LISTEN)
apache2 895 root 4u IPv6 27196 0t0 TCP *:http (LISTEN)
apache2 896 www-data 4u IPv6 27196 0t0 TCP *:http (LISTEN)
apache2 897 www-data 4u IPv6 27196 0t0 TCP *:http (LISTEN)
sshd 5864 root 4u IPv4 95319 0t0 TCP ubuntu:ssh->193.4.109.5:49674 (ESTABLISHED)
sshd 6015 ubuntu 4u IPv4 95319 0t0 TCP ubuntu:ssh->193.4.109.5:49674 (ESTABLISHED)
ubuntu@ubuntu:~$
```

Рисунок 3.67 – команда lsof

Далі, щоб отримати статистику мережевого трафіку, скористаємося командою «sar» (рис. 3.68 – 3.69). Щоб просто показати всю мережеву статистику, введемо команду sar наступним чином.

```
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ sar -n ALL 1 5 | less
```

Рисунок 3.68 – команда sar

```
Linux 5.4.0-100-generic (ubuntu)      06/11/2022      _x86_64_      (2 CPU)
12:48:28 PM   IFACE  rxpck/s  txpck/s    rxkB/s    txkB/s   rxcmp/s   txcmp/s  rxmcst/s
12:48:29 PM   enp0s8      0.00    0.00      0.00      0.00      0.00      0.00      0.00
12:48:29 PM      lo      0.00    0.00      0.00      0.00      0.00      0.00      0.00
12:48:29 PM   enp0s3      0.00    0.00      0.00      0.00      0.00      0.00      0.00
```

Рисунок 3.69 – команда sar

Існує ще одна утиліта з назвою «collectl», яка схожа на «sar». Таким же чином як «sar», також потрібно буде окремо встановити цю команду. Після виклику команди collectl з прапорцем -s і значенням sn, отримали статистику мережі (рис. 3.70).

```
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ collectl -s sn
waiting for 1 second sample...
#<-----Network-----><-----Sockets----->
#  KBIn  PktIn  KBOuT  PktOut  Tcp  Udp  Raw  Frag
0      2      0      0  544    0    0    0
0      2      1      2  532    0    0    0
0      1      0      1  544    0    0    0
0      2      0      1  544    0    0    0
0      2      0      1  544    0    0    0
0      2      0      1  544    0    0    0
0      1      0      1  532    0    0    0
```

Рисунок 3.70 – утиліта collectl

3.4.5 Отримання привілеїв адміністратора Ubuntu Server

Обліковий запис root у Linux має повний доступ до системи без жодних обмежень і його слід використовувати лише для адміністративних завдань. Завжди можна створити новий обліковий запис користувача з меншими привілеями. Але бувають випадки, коли вам потрібні додаткові привілеї root, щоб додати нового користувача або змінити якесь системне налаштування. Ви можете використовувати команду sudo, щоб тимчасово отримати додаткові привілеї для однієї команди. У цьому розділі детально розглянемо, як надати привілеї sudo новоствореному користувачеві.

Виконаймо такі дії, щоб отримати права root за допомогою команди sudo, якщо потрібно, додамо нового користувача (рис. 3.71).

```
ubuntu@ubuntu:~$ sudo adduser glib
[sudo] password for ubuntu:
Adding user `glib' ...
Adding new group `glib' (1001) ...
Adding new user `glib' (1001) with group `glib' ...
Creating home directory `/home/glib' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for glib
Enter the new value, or press ENTER for the default
  Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
```

Рисунок 3.71 – створення нового користувача glib

Зробимо користувача членом групи sudo командою (рис. 3.72).

```
ubuntu@ubuntu:~$ sudo adduser glib sudo
Adding user `glib' to group `sudo' ...
Adding user glib to group sudo
Done.
ubuntu@ubuntu:~$
```

Рисунок 3.72 – додавання користувача до групи

Тепер користувач є членом групи sudo, а отже має права адміністратора.

Усі правила доступу до sudo налаштовані у файлі (рис. 3.74), розташованому за адресою /etc/sudoers (рис. 3.73). Цей файл містить весь список користувачів і груп, яким дозволено використовувати команду sudo.

```
ubuntu@ubuntu:~$ sudo nano /etc/sudoers
```

Рисунок 3.73 – відкриття файлу /etc/sudoers у редакторі nano

```
GNU nano 4.8 /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/s
# Host alias specification
#
# User alias specification
#
# Cmnd alias specification
#
# User privilege specification
root    ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL
```

Рисунок 3.74 – правила доступу до sudo налаштовані у файлі /etc/sudoers

Все, що нам потрібно зробити, це додати нового користувача до групи `sudo`, і цей користувач автоматично отримає привілеї `sudo`. Після отримання членства в групі `sudo` користувачу потрібно вийти і увійти знову, щоб зміни вступили в силу. По суті, оболонку користувача потрібно перезапустити з новими привілеями.

3.4.6 Налаштування аутентифікації з відкритим ключем Ubuntu Server

Bruteforce – одна з найпоширеніших загроз для користувачів у мережі. Для захисту від необхідно вимкнути аутентифікацію за пароллями в SSH, а замість неї використовувати аутентифікацію по ключам. Однією з популярних програм для реалізації протоколу SSH є програма OpenSSH [27]. В разі якщо вона не встановлена на сервері, її можна встановити командою (рис. 3.75).

```
ubuntu@ubuntu:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:8.2p1-4ubuntu0.5).
0 upgraded, 0 newly installed, 0 to remove and 102 not upgraded.
ubuntu@ubuntu:~$
```

Рисунок 3.75 – встановлення OpenSSH (серверна версія)

Запустити демона `sshd` на сервері Ubuntu і налаштувати автоматичний запуск демона при кожному вході в систему (рис. 3.76).

```
ubuntu@ubuntu:~$ sudo systemctl start sshd
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ sudo systemctl enable sshd
```

Рисунок 3.76 – налаштування демона `sshd`

Спочатку для нового користувача необхідно створити каталог для зберігання ключів і надати необхідні дозволи (рис. 3.77).

```
ubuntu@ubuntu:~$ mkdir .ssh
mkdir: cannot create directory '.ssh': File exists
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ touch .ssh/authorized_keys
ubuntu@ubuntu:~$ chmod 700 .ssh
ubuntu@ubuntu:~$ chmod 600 .ssh/authorized_keys
ubuntu@ubuntu:~$
```

Рисунок 3.77 – створення каталогу `.ssh` для зберігання публічних ключів і надання дозволів на їх використання

Після цього можна згенерувати відповідні ключі SSH (рис. 3.78).

```

ubuntu@ubuntu:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ubuntu/.ssh/id_rsa): .ssh/authorized_keys
.ssh/authorized_keys already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in .ssh/authorized_keys
Your public key has been saved in .ssh/authorized_keys.pub
The key fingerprint is:
SHA256:3tjxhvsSWgD4rQ1TpMX9xzhaiRfx0d28eMGL7c+Lf7k ubuntu@ubuntu
The key's randomart image is:
+---[RSA 3072]-----+
|      . . .      |
|      + . . . +   |
|      = 0 =+0+    |
|     o o . B *.+   |
|    +S..+ = =     |
|   +..+=+ 0       |
|  =00+00 ..       |
|   . 0 .0 .00     |
|   .0...E*        |
+---[SHA256]-----+
ubuntu@ubuntu:~$ _

```

Рисунок 3.78 – генерація ключів

Тепер можна під'єднатись до серверу використовуючи ключ SSH (рис. 3.79 – 3.80).

```

glib@ubuntu:/home/ubuntu$ ssh ubuntu@ubuntu
The authenticity of host 'ubuntu (127.0.1.1)' can't be established.
ECDSA key fingerprint is SHA256:5XcDTFeto6R3tsBnxIjoKrcIdrm7tnoQ9KAzsr38jS4.
Are you sure you want to continue connecting (yes/no/[fingerprint])?

```

Рисунок 3.79 – підключення до серверу

```

glib@ubuntu:/home/ubuntu$ ssh ubuntu@ubuntu
The authenticity of host 'ubuntu (127.0.1.1)' can't be established.
ECDSA key fingerprint is SHA256:5XcDTFeto6R3tsBnxIjoKrcIdrm7tnoQ9KAzsr38jS4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ubuntu' (ECDSA) to the list of known hosts.
ubuntu@ubuntu's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-100-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat 11 Jun 2022 02:03:21 PM UTC

```

Рисунок 3.80 – успішне підключення до серверу

3.4.7 Захист облікових записів користувачів Ubuntu Server

В цьому розділі буде розглянуто методи для покращення захищеності облікових записів користувачів у системі Ubuntu Server. Спершу необхідно встановити політику надійних паролів, виконавши такі дії.

Відкриваємо конфігураційний файл `/etc/pam.d/common-password` за допомогою редактора GNU nano (рис. 3.81).

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

```

GNU nano 4.8 /etc/pam.d/common-password
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.
#
# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old `OBSOLETE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
password [success=1 default=ignore] pam_unix.so obscure sha512
# here's the fallback if no module succeeds
password requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password required pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config

```

Рисунок 3.81 – відкриття файлу /etc/pam.d/common-password

Додаємо параметр мінімальний розмір паролю (рис. 3.82).

```

# here are the per-package modules (the "Primary" block)
password [success=1 default=ignore] pam_unix.so obscure sha512 minlen=5
# here's the fallback if no module succeeds

```

Рисунок 3.82 – налаштування файлу common-password

Для того, щоб налаштувати захист домашнього каталогу системи, необхідно перевірити і обмежити дозволи користувачам і групі за допомогою наступної команди (рис. 3.83).

```

ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ ls -ld /home/ubuntu
drwxr-xr-x 4 ubuntu ubuntu 4096 Jun 11 10:43 /home/ubuntu
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ chmod 750 /home/ubuntu
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ _

```

Рисунок 3.83 – перевірка дозволів і обмеження дозволів для безпеки

Далі необхідно змінити дозволи для додавання користувача за замовчуванням шляхом редагування файлу /etc/adduser.conf. В файлі необхідно змінити рядок DIR_MODE=0755 на DIR_MODE=0750 (рис. 3.84).

```
# If DIR_MODE is set, directories will be created with the specified
# mode. Otherwise the default mode 0755 will be used.
DIR_MODE=0750

# If SETGID_HOME is "yes" home directories for users with their own
# group the setgid bit will be set. This was the default for
# versions << 3.13 of adduser. Because it has some bad side effects we
# no longer do this per default. If you want it nevertheless you can
# still set it here.
SETGID_HOME=no
```

Рисунок 3.84 – редагування файлу adduser.conf

Вимкнемо доступ SSH для користувача root, виконавши наступний крок. Відкриємо файл /etc/ssh/sshd_config і змінимо значення PermitRootLogin на PermitRootLogin no (рис. 3.85).

```
GNU nano 4.8 /etc/ssh/sshd_config Modified

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no_
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
```

Рисунок 3.85 – редагування файлу adduser.conf

3.5 Налашдування захисту мережі

3.5.1 Захист фізичного і віддаленого доступу

Налаштування паролю для зберігання в зашифрованому вигляді і додавання нового користувача для наступних налаштувань. (рис. 3.86) [1]

```
R_1(config)#enable secret cisco
R_1(config)#username admin privill
R_1(config)#username admin privi
R_1(config)#username admin privilege 15 secret cisco
R_1(config)#service pass
R_1(config)#service password-encryption
```

Рисунок 3.86 – налаштування паролів на маршрутизаторі R_1

Далі проведемо налаштування SSH і створення ключів для підключення. Обмежимо час введення логіна і паролю, зробимо всі спроби входу тільки за паролем. Вказуємо SSH в якості протокола віддаленого доступу (рис. 3.87).

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				86
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_1(config)#ip domain-name R1
R_1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R_1.R1

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R_1(config)#
*Mar  1 01:47:47.882: %SSH-5-ENABLED: SSH 1.99 has been enabled
R_1(config)#ip ssh ver
R_1(config)#ip ssh version 2
R_1(config)#ip ssh time
R_1(config)#ip ssh time-out 15
R_1(config)#ip ssh log
R_1(config)#ip ssh logging events
R_1(config)#line vty 0 4
R_1(config-line)#tran
R_1(config-line)#transport input ssh
R_1(config-line)#exec-time
R_1(config-line)#exec-timeout 5 0

```

Рисунок 3.87 – налаштування SSH на маршрутизаторі R_1

Далі дозволимо доступ до маршрутизатора тільки з відповідної підмережі (рис. 3.88).

```

R_1(config)#ip access-list standard SSH ACCESS
R_1(config-std-nacl)#permit host 194.4.7.0
R_1(config-std-nacl)#exit
R_1(config)#line vty 0 4
R_1(config-line)#access-class SSH-ACCESS in

```

Рисунок 3.88 – обмеження доступу для ір-адрес на маршрутизаторі R_1

Для захисту від підбору паролів (Brute Force) необхідно налаштувати тимчасове блокування повторної аутентифікації. (рис. 3.89) [1]

```

R_1(config)#login delay 5
R_1(config)#login block
R_1(config)#login block-for 60 atte
R_1(config)#login block-for 60 attempts 3 wit
R_1(config)#login block-for 60 attempts 3 within 30
R_1(config)#

```

Рисунок 3.89 – налаштування захисту від підбору паролів на R_1

3.5.2 Налаштування AAA

Для налаштування AAA було вибрано протокол Tacsacs+. Для належного налаштування додали до топології мережі підключення до мережі Інтернет, додали новий комутатор SW_15, утиліту TacsacsGUI для GNS3 і робочу станцію WS_webterm для налаштування і входу в акуант Tacsacs (рис. 3.89) [24].

		Борейченко Г.О.			KIK.KP.B – 123 – 07 – ПЗ	Арк.
		Головня О.С.				87
Змн.	Арк.	№ докум.	Підпис	Дата		

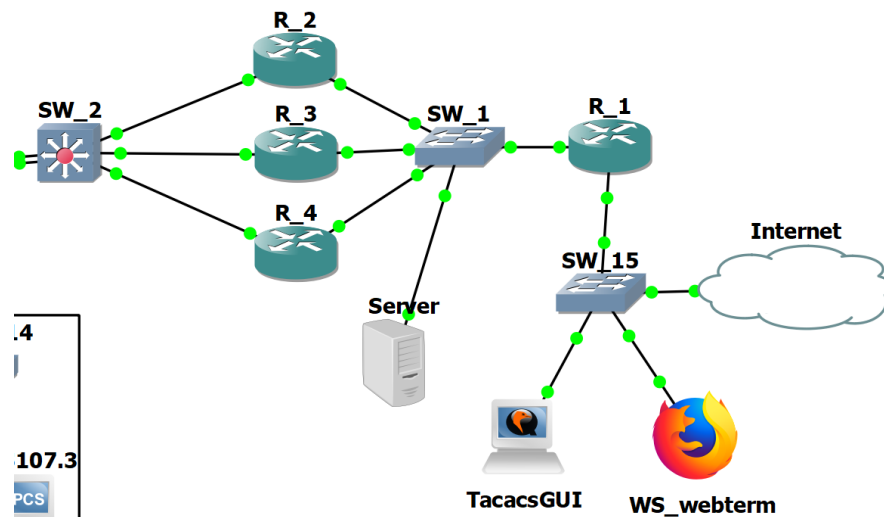


Рисунок 3.89 – налаштування AAA

Для початку перейдемо до початкового меню Тасас GUI (рис. 3.90).

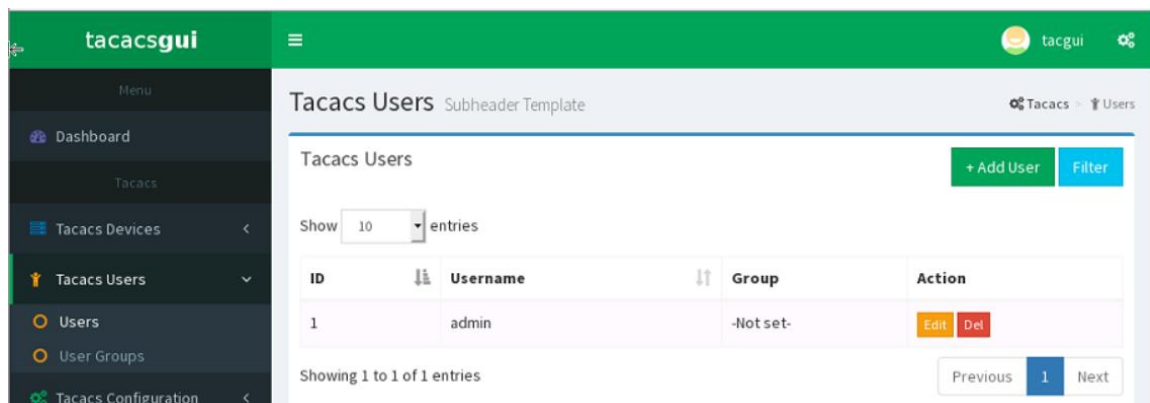


Рисунок 3.90 – початкове меню Тасас GUI

Створили користувачів з різними Privilege level (рис. 3.91).

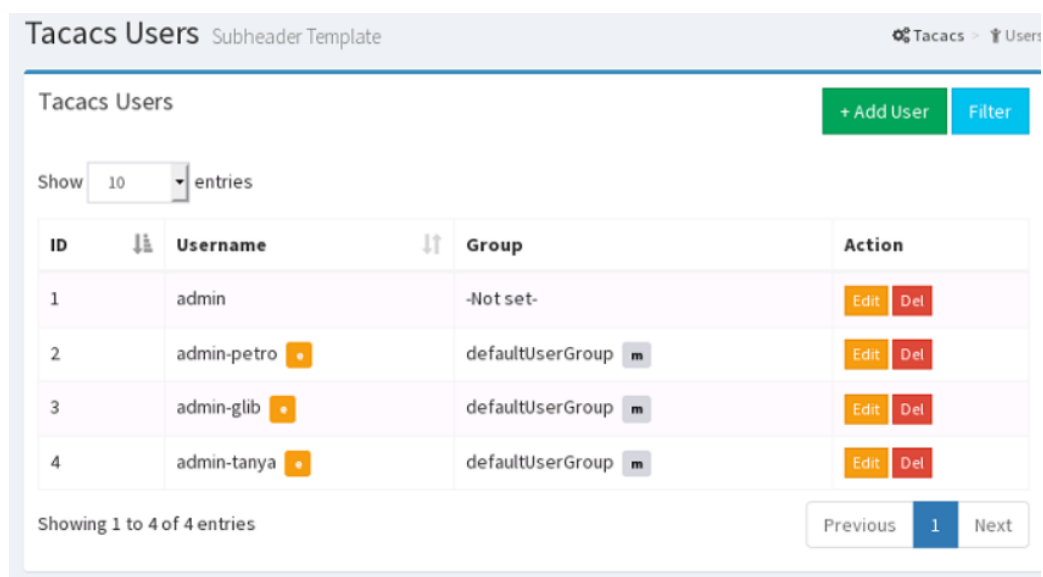


Рисунок 3.91 – створені користувачі в Тасас GUI

Додали нову групу для пристроїв (рис. 3.92).

Рисунок 3.92 – створена група пристроїв у Tacsacs GUI

Далі додали новий пристрій – маршрутизатор R_1 (рис. 3.93) і зберегли налаштування (рис. 3.94).

Рисунок 3.93 – новий пристрій у Tacsacs GUI

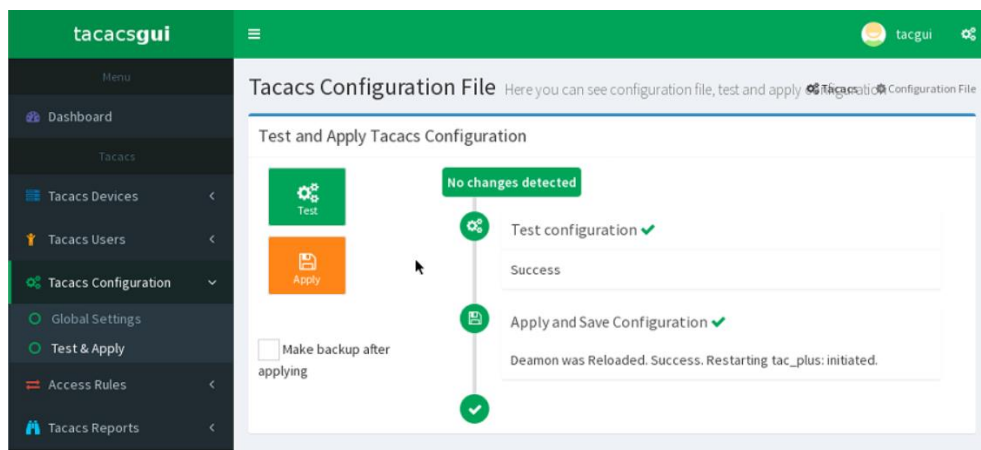


Рисунок 3.94 – успішне зберігання налаштувань

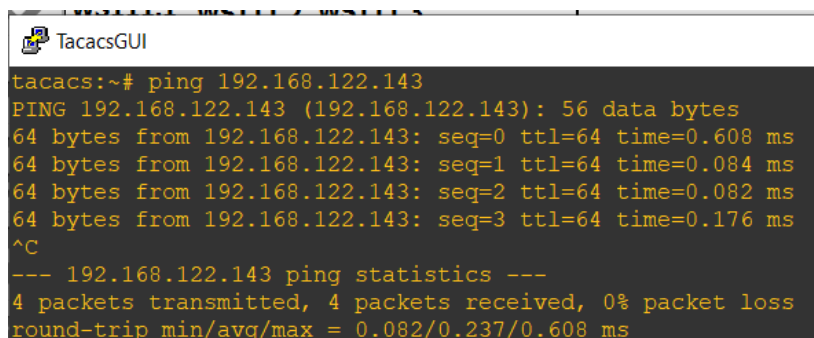


Рисунок 3.95 – перевірка зв'язку між сервером tacacs і маршрутизатором R_1

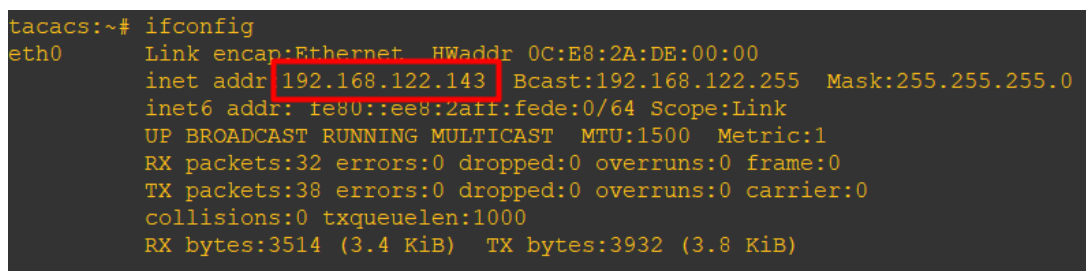


Рисунок 3.96 – ір-адреса сервера tacacs

Проведемо налаштування Authentication (рис. 3.97).

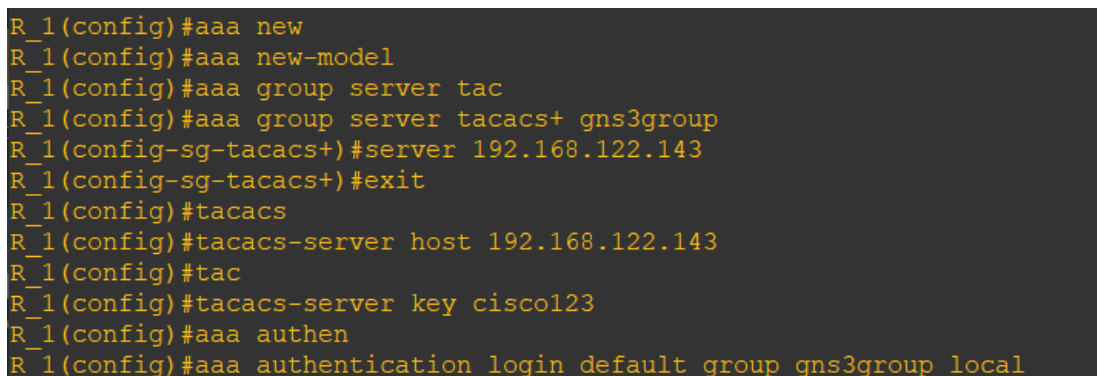


Рисунок 3.97 – налаштування Authentication

В результаті при спробі підключення до маршрутизатора успішно підключаємось до нового користувача (рис. 3.98). Але знак «>» говорить про те, що ми в режимі користувача. Причина у відсутності налаштувань авторизації.

```
R_1#telnet 192.168.122.200
Trying 192.168.122.200 ... Open

User Access Verification

Username: admin-petro
Password:

R_1>
```

Рисунок 3.98 – вхід з користувача admin-petro на маршрутизатор R_1
Далі проведемо налаштування авторизації (рис. 3.99).

```
R_1(config)#aaa authorization exec default group gns3group local
R_1(config)#aaa author
R_1(config)#aaa authorization config
R_1(config)#aaa authorization config-com
R_1(config)#aaa authorization config-command
R_1(config)#aaa authorization commands 1 default group gns3group local
R_1(config)#aaa authorization commands 15 default group gns3group local
R_1(config)#aaa authori
R_1(config)#aaa authorization console
```

Рисунок 3.99 – налаштування Authorization

Успішно заходимо під користувачем admin-glib (рис. 3.100) і бачимо, що одразу переходимо на режим privileged exec mode. Налаштування спрацювали.

```
R_1#telnet 192.168.122.200
Trying 192.168.122.200 ... Open

User Access Verification

Username: admin-glib
Password:

R_1#
```

Рисунок 3.100 – вхід з користувача admin-glib на маршрутизатор R_1
Далі проведемо налаштування обліку (рис. 3.101).

```
R_1(config)#aaa accounting exec default start-stop group gns3group
R_1(config)#aaa acc
R_1(config)#aaa accounting comm
R_1(config)#aaa accounting commands 1 default start
R_1(config)#aaa accounting commands 1 default start-stop group gns3group
R_1(config)#aaa accounting commands 15 default start-stop group gns3group
R_1(config)#
```

Рисунок 3.101 – налаштування Accounting

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

3.5.3 Захист локальної мережі

При включенні інтерфейса комутатора порт проходить три етапи: listening, learning і після цього переходить у стан forwarding або blocking. Це займає близько 30 секунд і є необхідним для того щоб комутатор зміг перевірити, хто до нього підключений робоча станція чи інший комутатор.

Фактично функція PortFast змінює у роботі протоколу STP наступне: порт пропускає стан роботи listening і learning; при зміні статусу порту, не відправляється повідомлення про зміну стану порту TCN BPDU (topology change notification BPDU). Це дозволяє швидче переводити порт у стан forwarding. Крім того, вимкнення повідомлень TCN BPDU дозволяє знизити навантаження на Root Bridge (кореневий комутатор STP), якому довелося б обробляти кожне увімкнення/вимкнення портів. Налаштовувати PortFast необхідно на рівні розподілу на портах, до яких підключені робочі станції, щоб завадити утворенням петель (рис. 3.102).

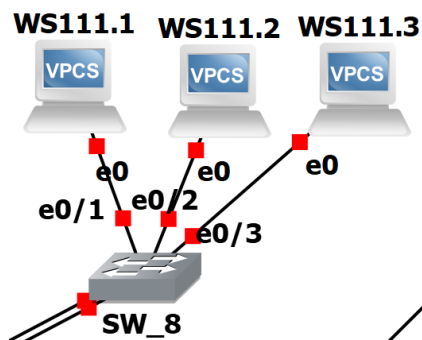


Рисунок 3.102 – налаштування PortFast на комутаторі рівня розподілу SW_8

```
SW_8
!
interface Ethernet0/1
 switchport access vlan 111
 switchport mode access
 duplex auto
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree link-type point-to-point
!
interface Ethernet0/2
 switchport access vlan 111
 switchport mode access
 duplex auto
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree link-type point-to-point
!
```

Рисунок 3.103 – налаштування PortFast

		Борейченко Г.О.			KIK.KP.B – 123 – 07 – ПЗ	Арк.
		Головня О.С.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

Одним із найпоширеніших видів взлому локальних мереж є підміна кореневого комутатора. Організувати захист від таких атак досить просто. Для цього потрібно скористатися функцією BPDU Guard на всіх портах користувача, крім тих портів, до яких підключено інші комутатори. Це дозволить блокувати пакети BPDU там, де їх не повинно бути. Налаштуємо BPDU Guard на портах які під'єднані до робочих станцій (рис. 3.104) для протидії сценарію взлому локальної мережі шляхом підміни кореневого комутатора:

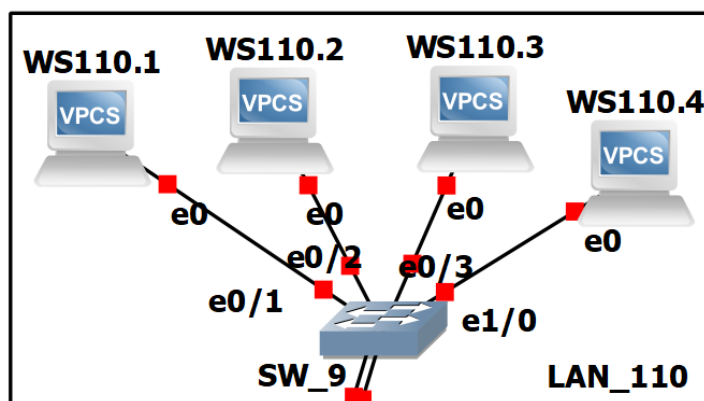


Рисунок 3.104 – налаштування bpduguard на комутаторі рівня розподілу SW_9 на портах, які під'єднані до робочих станцій

```
SW_9
!
interface Ethernet0/1
 switchport access vlan 110
 switchport mode access
 duplex auto
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree link-type point-to-point
!
interface Ethernet0/2
 switchport access vlan 110
 switchport mode access
 duplex auto
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree link-type point-to-point
!
```

Рисунок 3.105 – налаштування bpduguard

За допомогою налаштування BPDU Guard (рис. 3.105) нам вдалося ліквідувати вразливість пов'язану з розсилкою BPDU пакетів на рівні розподілу, що могло би призвести до перебудови STP топології та зміни кореневого комута-

тора. Щоб уникнути цієї вразливості на комутаторах рівня ядра (рис. 3.106) мережі необхідно активувати додаткову функцію – Root Guard (рис. 3.107). Вмикається цей захист на портах, до комутаторів доступу, де ми забороняємо будь-яку появу кореневого комутатора.

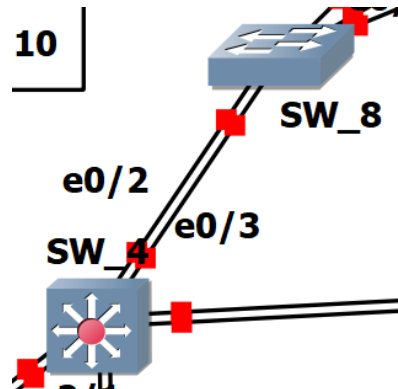


Рисунок 3.106 – налаштування guard root на комутаторі рівня ядра SW_4 на портах, які ведуть до комутатора рівня розподілу SW_8

Налаштуємо Root Guard на рівні ядра:

```
SW_4
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 111
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 2 mode active
 spanning-tree guard root
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 111
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 2 mode active
 spanning-tree guard root
!
```

Рисунок 3.107 – налаштування guard root

Висновки з третього розділу

У третьому розділі було проведено налаштування мережевих пристроїв побудованої мережі і проведено тестування для перевірки правильності цих налаштувань. Спершу провели налаштування інтерфейсів маршрутизаторів і комутаторів мережі. Налаштували VLAN і ір-адреси. Також налаштували протокол ди-

		Борейченко Г.О.			KIK.KP.B – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		94

намічної маршрутизації OSPF, який працює на технології відстеження стану каналу. Вибрали саме цей протокол тому, що при роботі OSPF побудова таблиць маршрутизації відбувається швидше, ніж у мережах, які працюють на дистанційно-векторних протоколах (RIP, IGRP, BGP, EIGRP). Налаштували протокол динамічного резервування шлюзу HSRP і перевірили його роботу. Для агрегації каналів налаштували протокол LACP. Для видалення петель комутації налаштували мережевий протокол PVST+, який має більше удосконалень ніж попередні протоколи розроблені на базі протоколу кістякового дерева STP. Далі провели перевірку зв'язку між рівнем ядра, розподілу, доступу і різними VLAN.

Встановили і налаштували ОС Ubuntu Server. Провели базові налаштування IP-адреси в системі. Провели перевірку зв'язку з іншими вузлами мережі. Для реалізації технології VPN на Ubuntu Server вибрали OpenVPN через його популярність і доступність документації. Разом з тим було налаштовано підключення SSH з ключем, замість звичної автентифікації паролем. Також дозволили лише одному користувачу з правом root доступ до сервера. Також налаштували брандмауер і заблокували всі порти, крім кількох необхідних.

Сервери, які відкриті для загальнодоступної мережі, завжди можуть бути вразливими до зовнішніх атак. Таким чином необхідно збільшити захищеність серверу і зменшити можливість атак. Це можна зробити якщо розробник відстежує журнали програм та журнали доступу до серверу, тоді можна знайти повторювані систематичні спроби входу, які можуть говорити що мали місце атаки методом грубої сили або інші. Для відслідковування такої підозрілої активності на Ubuntu Server встановили і налаштували спеціальну утиліту - Fail2ban.

Накінець провели налагодження захисту мережі. Провели налаштування фізичного і віддаленого доступу до маршрутизаторів. Для налаштування AAA вибрали протокол TACACS. Перевагою цього протоколу є те, що він шифрує всі дані, а не тільки пароль як протокол RADIUS [19]. Має зручніший інтерфейс і простіший у налаштуванні. Наприкінці налагодили захист локальної мережі на рівні комутаторів рівня ядра і розподілу. Налаштували такі корисні функції, як PortFast, BPDU Guard і root guard.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

Згідно з метою кваліфікаційної роботи була розроблена і побудована ІТ-інфраструктура мережі наукової бібліотеки. Підсумовуючи роботу можна сказати, що було досягнуто всі завдання, які були поставлені на початку роботи.

Було досліджено особливості проектування інформаційних мереж. До того ж, було ширше розкрито поняття корпоративної мережі, з чого вона складається, для чого потрібна, переваги використання у повсякденній роботі. Таким чином, було встановлено основні етапи проектування корпоративної мережі: аналіз завдань, побудова функціональної моделі мережі, побудова технічної моделі мережі. Отже, побудова правильної архітектури комп'ютерної мережі може забезпечити достатню швидкість і зручність використання для користувачів. Така структура повинна забезпечувати послідовність і взаємозв'язок між всіма структурними підрозділами на підприємстві або організації. У результаті успішне планування комп'ютерної мережі дозволить її успішне розширення і модернізацію. Дозволить зменшити або виключити помилки при роботі організації у майбутньому.

Також на початку кваліфікаційної роботи було створено та розглянуто організаційну структуру наукової бібліотеки і базуючись на ній детально окреслено структуру майбутньої комп'ютерної мережі.

Таким чином, здійснене дослідження дало змогу дійти висновку, які саме основні технології й мережеві протоколи необхідні для успішного втілення спроектованої нами мережі.

Після вибору архітектури мережі, системних і програмних рішень для її проектування настав час розглянути вибір апаратного обладнання для організації роботи мережі. Було вибрано відповідні комутатори та маршрутизатори для подальшого налаштування. Під час побудови комп'ютерної мережі, неважливо локальної чи корпоративної, рано чи пізно постає питання розширення мережі або додавання нових пристроїв, тому проаналізувати напрями удосконалення мережі.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		96

Врешті спроектували чіткий структурний план мережі наукової бібліотеки. Розібрались з планом розміщення серверу і робочих станцій і перейшли до налагодження топології мережі. Насамперед виконали загальне проектування топології комп'ютерної мережі та розподілили відповідні IP-адреси. Мережа була побудована згідно концепції трирівневої ієрархічної моделі Cisco. Було побудовано і налаштовано рівень ядра, рівень розподілу і доступу.

Розглянувши проектування мережі перейшли до практичної реалізації. Найперше було проведено налаштування мережевих пристроїв побудованої мережі. Після цього провели тестування для перевірки правильності цих налаштувань. Далі провели перевірку зв'язку між рівнем ядра, розподілу, доступу і різними VLAN мережі.

Додали сервер на ОС Ubuntu Server. Провели налаштування брандмауера, віддаленого доступу і захисту від мережних атак. Дослідили варіанти моніторингу мережі. Зробили аутентифікацію за ключем. Налаштували захист облікових записів користувачів.

Разом з тим провели налагодження захисту мережі. А саме налаштування фізичного і віддаленого доступу до маршрутизаторів. Далі налаштували систему аутентифікації авторизації та обліку подій. Наприкінці налагодили захист локальної мережі на рівні комутаторів рівня ядра і розподілу.

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		97

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Basic Router Configuration. [Електронний ресурс] – Режим доступу до ресурсу:
https://www.cisco.com/c/en/us/td/docs/routers/access/800M/software/800M_SCG/routconf.html
2. Catalyst 3750-X and 3560-X Switch Software Configuration Guide - Configuring HSRP. [Електронний ресурс] – Режим доступу до ресурсу:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swhsrp.html
3. Configure Port to VLAN Interface Settings on a Switch through the CLI. [Електронний ресурс] – Режим доступу до ресурсу:
<https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5653-configure-port-to-vlan-interface-settings-on-a-switch-throug.html>
4. Configure STP Settings on a Switch through the CLI.Cisco. [Електронний ресурс] – Режим доступу до ресурсу:
<https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5760-configure-stp-settings-on-a-switch-through-the-cli.html>
5. Configuring PVST+ and RPVST+ [Електронний ресурс] – Режим доступу до ресурсу:
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/routers/ncs5xx/ncs520/configuration/guide/LAN-switch/17-1-1/b-lanswitch-17-1-1-ncs520/b-lanswitch-17-1-1-ncs520_chapter_0110.html.xml
6. Etherchannel on Cisco IOS Catalyst Switch. [Електронний ресурс] – Режим доступу до ресурсу: <https://networklessons.com/switching/etherchannel-cisco-ios-catalyst-switch>

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				98
Змн.	Арк.	№ докум.	Підпис	Дата		

7. Hudson, A. and Hudson, P., 2018. Ubuntu unleashed. Indianapolis, Ind.: Sams.
8. IP Routing: OSPF - Configuring OSPF [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html
9. IPv4 Addressing Guide [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_ipv4/configuration/xe-3s/ipv4-xe-3s-book/configuring_ipv4_addresses.html
10. LaCroix, J., 2018. Mastering Ubuntu Server - Second Edition. 2th ed. [Place of publication not identified]: Packt Publishing.
11. LaCroix, J., 2020. Mastering Ubuntu Server - Third Edition. 3th ed. [S.l.]: Packt Publishing.
12. Link Aggregation Control Protocol. [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/gigeth.html
13. Odom, W. and Hogg, S., 2020. CCNA routing and switching.
14. Odom, W. and Knott, T., 2019. Networking basics. Indianapolis, IN: Cisco Press.
15. Odom, W., 2017. Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide. 8th ed.
16. Olifer, N. and Olifer, V., 2010. Computer networks. Saint Petersburg: Willy Saint Petersburg.
17. OpenVPN. 2022. Community Downloads | OpenVPN. [Електронний ресурс] – Режим доступу до ресурсу: <https://openvpn.net/community-downloads/>
18. OpenVPN. 2022. Ubuntu VPN Software Package For Access Server | OpenVPN. [Електронний ресурс] – Режим доступу до ресурсу: <https://openvpn.net/vpn-software-packages/ubuntu/>

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				99
Змн.	Арк.	№ докум.	Підпис	Дата		

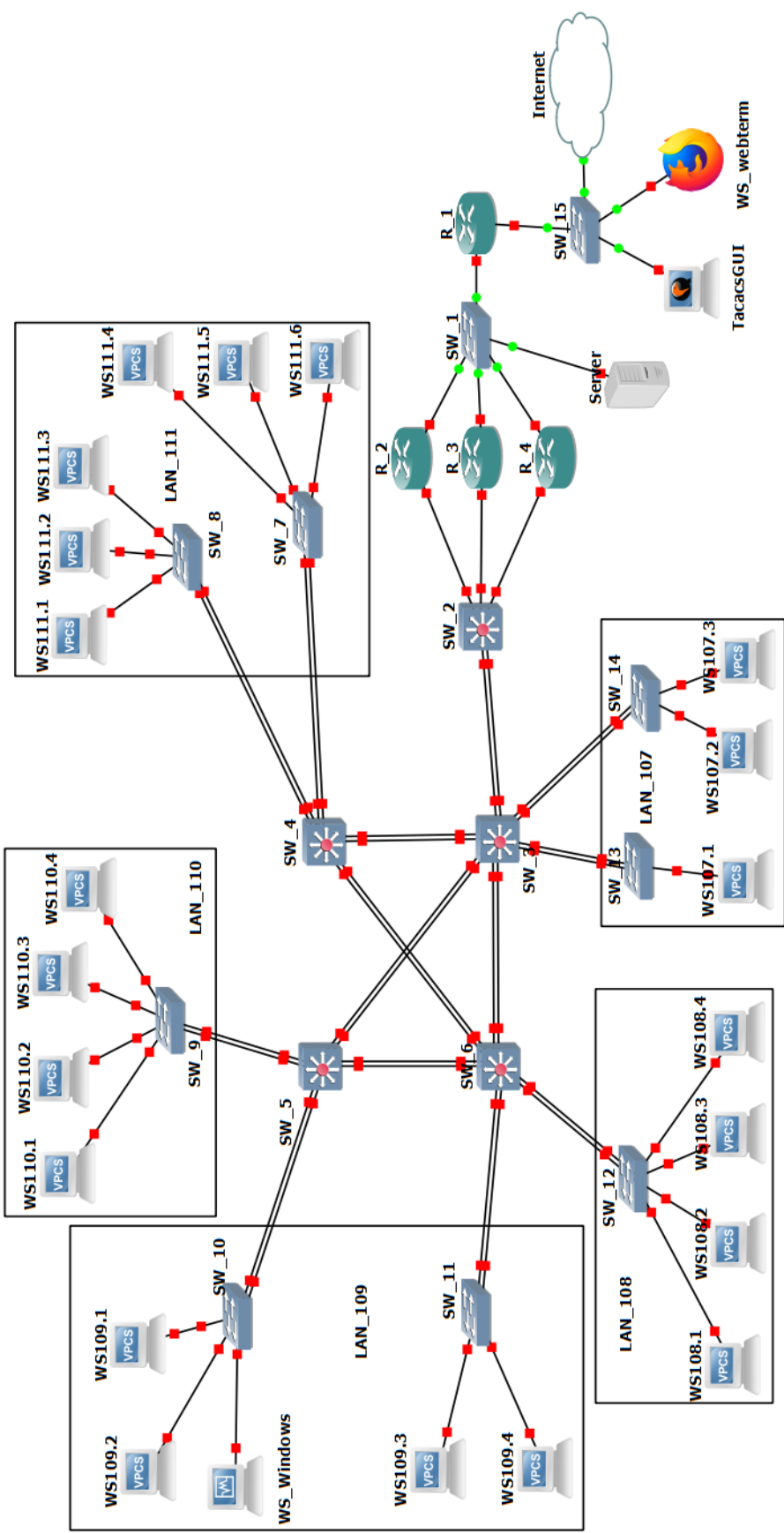
- 19.RADIUS Protocol. [Електронний ресурс] – Режим доступу до ресурсу:
<https://networkradius.com/doc/3.0.10/introduction/RADIUS.html>
- 20.Rankin, K. and Hill, B., 2021. The official Ubuntu server book.
- 21.Sawant, U., 2020. Ubuntu Server cookbook. 10th ed. Birmingham, UK: Packt Publishing.
- 22.Schroder, C., 2021. Linux cookbook. 10th ed. Sebastopol, Calif.: O'Reilly.
- 23.Stutz, M., 2019. The Linux cookbook. 6th ed. San Francisco: Starch Press.
- 24.TACACS+ Configuration Guide [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/xe-16/sec-usr-tacacs-xe-16-book/sec-cfg-tacacs.html
- 25.Tanenbaum, A. and Boschung, H., 2019. Modern operating systems.
- 26.Tanenbaum, A. and Wetherall, D., 2017. Computer networks. 4th ed.
- 27.Ubuntu. 2022. Service - OpenSSH | Ubuntu. [Електронний ресурс] – Режим доступу до ресурсу: <https://ubuntu.com/server/docs/service-openssh>
- 28.Ubuntu. 2022. Service - OpenVPN | Ubuntu. [Електронний ресурс] – Режим доступу до ресурсу: <https://ubuntu.com/server/docs/service-openvpn>
- 29.What Is an Enterprise Network. Cisco. 2022.[Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-an-enterprise-network.html>
- 30.Навчальний курс Cisco CCNAv7: Introduction to Networks [Електронний ресурс] – Режим доступу до ресурсу: www.netacad.com

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		100

ДОДАТКИ

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				101
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток А – Топологія комп'ютерної мережі



		Борейченко Г.О.		
		Головня О.С.		
Змн.	Арк.	№ докум.	Підпис	Дата

Додаток Б – Параметри з'єднань інтерфейсів пристроїв

Пристрій	Інтерфейс при-строю	Підключення до інтерфейсу	Підключення до при-строю
Маршрутизатор R1	E0/0	E0	Комутатор SW_1
	E1/0	E0	Комутатор SW_15
Маршрутизатор R2	E0/0	E0/0	Комутатор SW_2
	E1/0	E1	Комутатор SW_1
Маршрутизатор R3	E0/0	E0/1	Комутатор SW_2
	E1/0	E2	Комутатор SW_1
Маршрутизатор R4	E0/0	E0/2	Комутатор SW_2
	E1/0	E3	Комутатор SW_1
Комутатор SW_1	E0	E0/0	Маршрутизатор R_1
	E1	E1/0	Маршрутизатор R_2
	E2	E1/0	Маршрутизатор R_3
	E3	E1/0	Маршрутизатор R_4
	E4	E0	SERVER
Комутатор SW_2	E0/0	E0/0	Маршрутизатор R_2
	E0/1	E0/0	Маршрутизатор R_3
	E0/2	E0/0	Маршрутизатор R_4
	E0/3	E0/3	Комутатор SW_3
	E1/0	E1/0	Комутатор SW_3
Комутатор SW_3	E0/0	E0/0	Комутатор SW_4
	E0/1	E0/1	Комутатор SW_4
	E0/2	E0/0	Комутатор SW_14
	E0/3	E0/3	Комутатор SW_2
	E1/0	E1/0	Комутатор SW_2
	E1/1	E1/1	Комутатор SW_6

	E1/2	E1/2	Комутатор SW_6
	E1/3	E0/3	Комутатор SW_14
	E2/0	E2/0	Комутатор SW_5
	E2/1	E2/1	Комутатор SW_5
	E2/2	E0/0	Комутатор SW_13
	E2/3	E0/2	Комутатор SW_13
Комутатор SW_4	E0/0	E0/0	Комутатор SW_3
	E0/1	E0/1	Комутатор SW_3
	E0/2	E0/0	Комутатор SW_8
	E0/3	E1/0	Комутатор SW_8
	E1/0	E0/0	Комутатор SW_7
	E1/1	E1/0	Комутатор SW_7
	E2/0	E2/0	Комутатор SW_6
	E2/1	E2/1	Комутатор SW_6
Комутатор SW_5	E0/0	E0/0	Комутатор SW_6
	E0/1	E0/1	Комутатор SW_6
	E0/2	E0/0	Комутатор SW_10
	E0/3	E0/3	Комутатор SW_10
	E1/0	E0/0	Комутатор SW_9
	E1/1	E1/1	Комутатор SW_9
	E2/0	E2/0	Комутатор SW_3
	E2/1	E2/1	Комутатор SW_3
Комутатор SW_6	E0/0	E0/0	Комутатор SW_5
	E0/1	E0/1	Комутатор SW_5
	E0/2	E0/0	Комутатор SW_12
	E0/3	E1/1	Комутатор SW_12

		Борейченко Г.О.		
		Головня О.С.		
Змн.	Арк.	№ докум.	Підпис	Дата

KIK.KP.B – 123 – 07 – ПЗ

Арк.

104

	E1/0	E0/0	Комутатор SW_11
	E1/1	E1/1	Комутатор SW_3
	E1/2	E1/2	Комутатор SW_3
	E1/3	E0/3	Комутатор SW_11
	E2/0	E2/0	Комутатор SW_4
	E2/1	E2/1	Комутатор SW_4
Комутатор SW_7	E0/0	E1/0	Комутатор SW_4
	E1/0	E1/1	Комутатор SW_4
	E0/1	E0	Робоча станція WS111.4
	E0/2	E0	Робоча станція WS111.5
	E0/3	E0	Робоча станція WS111.6
Комутатор SW_8	E0/0	E0/2	Комутатор SW_4
	E1/0	E0/3	Комутатор SW_4
	E0/1	E0	Робоча станція WS111.1
	E0/2	E0	Робоча станція WS111.2
	E0/3	E0	Робоча станція WS111.3
Комутатор SW_9	E0/0	E1/0	Комутатор SW_5
	E1/1	E1/1	Комутатор SW_5
	E0/1	E0	Робоча станція WS110.1

		Борейченко Г.О.		
		Головня О.С.		
Змн.	Арк.	№ докум.	Підпис	Дата

KIK.KP.B – 123 – 07 – ПЗ

Арк.

105

	E0/2	E0	Робоча станція WS110.2
	E0/3	E0	Робоча станція WS110.3
	E1/0	E0	Робоча станція WS110.4
Комутатор SW_10	E0/0	E0/2	Комутатор SW_5
	E0/3	E0/3	Комутатор SW_5
	E0/1	E0	Робоча станція WS109.1
	E0/2	E0	Робоча станція WS109.2
	E1/0	E0	Робоча станція WS_Windows
Комутатор SW_11	E0/0	E1/0	Комутатор SW_6
	E0/3	E1/3	Комутатор SW_6
	E0/1	E0	Робоча станція WS109.3
	E0/2	E0	Робоча станція WS109.4
Комутатор SW_12	E0/0	E0/2	Комутатор SW_6
	E1/1	E0/3	Комутатор SW_6
	E0/1	E0	Робоча станція WS108.1
	E0/2	E0	Робоча станція WS108.2

	E0/3	E0	Робоча станція WS108.3
	E1/0	E0	Робоча станція WS108.4
Комутатор SW_13	E0/0	E2/2	Комутатор SW_3
	E0/2	E2/3	Комутатор SW_3
	E0/1	E0	Робоча станція WS107.1
Комутатор SW_14	E0/0	E0/2	Комутатор SW_3
	E0/3	E1/3	Комутатор SW_3
	E0/1	E0	Робоча станція WS107.2
	E0/2	E0	Робоча станція WS107.3
Комутатор SW_15	E0	E1/0	Маршрутизатор R_1
	E1	Nat0	Internet
	E2	Eth0	Робоча станція WS_webterm
	E3	Port1	TacacsGUI

Додаток В – Параметри адресації пристроїв мережі

Пристрій	Інтерфейс при-строю	ІР-адреса	Маска підме-режі	Префікс
Маршрутизатор R_1	E0/0	194.4.7.1	255.255.255.192	/26
	E1/0	192.168.122.200	255.255.255.0	/24
Маршрутизатор R_2	E0/0	-		
	E1/0	194.4.7.2	255.255.255.192	/26
Маршрутизатор R_3	E0/0	-		
	E1/0	194.4.7.3	255.255.255.192	/26
Маршрутизатор R_4	E0/0	-		
	E1/0	194.4.7.4	255.255.255.192	/26
Server	Мережний адаптер	194.4.7.5	255.255.255.192	/26
	Шлюз за замовчуванням	194.4.7.1		
TacacsGUI	Port1	192.168.122.143	255.255.255.0	
Робоча станція WS_webterm	Eth0	DHCP		
Робоча станція WS107.1	Мережний адаптер	193.4.107.1	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.107.123	255.255.255.128	/25
Робоча станція WS107.2	Мережний адаптер	193.4.107.2	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.107.123	255.255.255.128	/25
Робоча станція	Мережний адаптер	193.4.107.3	255.255.255.128	/25

WS107.3	Шлюз за замовчуванням	193.4.107.123	255.255.255.128	/25
Робоча станція WS108.1	Мережний адаптер	193.4.108.1	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.108.123	255.255.255.128	/25
Робоча станція WS108.2	Мережний адаптер	193.4.108.2	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.108.123	255.255.255.128	/25
Робоча станція WS108.3	Мережний адаптер	193.4.108.3	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.108.123	255.255.255.128	/25
Робоча станція WS108.4	Мережний адаптер	193.4.108.4	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.108.123	255.255.255.128	/25
Робоча станція WS109.1	Мережний адаптер	193.4.109.1	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.109.123	255.255.255.128	/25
Робоча станція WS109.2	Мережний адаптер	193.4.109.2	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.109.123	255.255.255.128	/25
Робоча станція WS_Windows	Мережний адаптер	193.4.109.5	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.109.123		

Робоча станція WS109.3	Мережний адаптер	193.4.109.3	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.109.123	255.255.255.128	/25
Робоча станція WS109.4	Мережний адаптер	193.4.109.4	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.109.123	255.255.255.128	/25
Робоча станція WS110.1	Мережний адаптер	193.4.110.1	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.110.123	255.255.255.128	/25
Робоча станція WS110.2	Мережний адаптер	193.4.110.2	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.110.123	255.255.255.128	/25
Робоча станція WS110.3	Мережний адаптер	193.4.110.3	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.110.123	255.255.255.128	/25
Робоча станція WS110.4	Мережний адаптер	193.4.110.4	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.110.123	255.255.255.128	/25
Робоча станція WS111.1	Мережний адаптер	193.4.111.1	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.111.123	255.255.255.128	/25
Робоча станція	Мережний адаптер	193.4.111.2	255.255.255.128	/25

WS111.2	Шлюз за замовчуванням	193.4.111.123	255.255.255.128	/25
Робоча станція WS111.3	Мережний адаптер	193.4.111.3	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.111.123	255.255.255.128	/25
Робоча станція WS111.4	Мережний адаптер	193.4.111.4	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.111.123	255.255.255.128	/25
Робоча станція WS111.5	Мережний адаптер	193.4.111.5	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.111.123	255.255.255.128	/25
Робоча станція WS111.6	Мережний адаптер	193.4.111.6	255.255.255.128	/25
	Шлюз за замовчуванням	193.4.111.123	255.255.255.128	/25

Маршрутизатор R_1:

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R_1
!
boot-start-marker
boot-end-marker
!
enable secret 5
$1$XNQl$IDdS/8wqPJ2nuS3y2iS7/.
!
aaa new-model
!
!
aaa group server tacacs+ gns3group
server 192.168.122.143
!
aaa authentication login default group
gns3group local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group
gns3group local
aaa authorization commands 1 default
group gns3group local
aaa authorization commands 15 default
group gns3group local
aaa accounting exec default start-stop
group gns3group
aaa accounting commands 1 default
start-stop group gns3group
aaa accounting commands 15 default
start-stop group gns3group
!
!
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
    
```

Маршрутизатор R_2:

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
archive
log config
hidekeys
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
no ip address
half-duplex
!
interface Ethernet0/0.107
encapsulation dot1Q 107
ip address 193.4.107.126
255.255.255.128
standby 107 ip 193.4.107.123
standby 107 priority 96
standby 107 preempt
standby 107 track Ethernet1/0
!
interface Ethernet0/0.108
    
```

		Борейченко Г.О.			KIK.KP.B – 123 – 07 – ПЗ	Арк.
		Головня О.С.				112
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip domain name R1
login block-for 60 attempts 3 within 30
login delay 5
!
multilink bundle-name authenticated
!
username admin privilege 15 secret 5
$1$9dZZ$HkShMrgQzlJmzm7Cz061u1
archive
 log config
  hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 15
ip ssh logging events
ip ssh version 2
!
interface Ethernet0/0
 ip address 194.4.7.1 255.255.255.192
 half-duplex
!
interface Ethernet1/0
 ip address 192.168.122.200
 255.255.255.0
 half-duplex
!
router ospf 7
 log-adjacency-changes
 network 194.4.7.0 0.0.0.15 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ip access-list standard SSH_ACCESS
 permit 194.4.7.0
!
no cdp log mismatch duplex
!
!
!
!
!

```

```

encapsulation dot1Q 108
 ip address 193.4.108.126
 255.255.255.128
 standby 108 ip 193.4.108.123
 standby 108 priority 96
 standby 108 preempt
 standby 108 track Ethernet1/0
!
interface Ethernet0/0.109
 encapsulation dot1Q 109
 ip address 193.4.109.126
 255.255.255.128
 standby 109 ip 193.4.109.123
 standby 109 preempt
 standby 109 track Ethernet1/0
!
interface Ethernet0/0.110
 encapsulation dot1Q 110
 ip address 193.4.110.126
 255.255.255.128
 standby 110 ip 193.4.110.123
 standby 110 priority 105
 standby 110 preempt
 standby 110 track Ethernet1/0
!
interface Ethernet0/0.111
 encapsulation dot1Q 111
 ip address 193.4.111.126
 255.255.255.128
 standby 111 ip 193.4.111.123
 standby 111 priority 105
 standby 111 preempt
 standby 111 track Ethernet1/0
!
interface Ethernet1/0
 ip address 194.4.7.2 255.255.255.192
 half-duplex
!
router ospf 7
 router-id 2.2.2.2
 log-adjacency-changes
 passive-interface Ethernet0/0
 network 193.4.107.0 0.0.0.127 area 0
 network 193.4.108.0 0.0.0.127 area 0

```

		Борейченко Г.О.		
		Головня О.С.		
Змн.	Арк.	№ докум.	Підпис	Дата

KIK.KP.Б – 123 – 07 – ПЗ

Арк.

113

```

tacacs-server host 192.168.122.143
tacacs-server key 7
121A0C0411045D5679
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
access-class SSH-ACCESS in
exec-timeout 5 0
transport input ssh
End

```

Маршрутизатор R_3:

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!

```

```

network 193.4.109.0 0.0.0.127 area 0
network 193.4.110.0 0.0.0.127 area 0
network 193.4.111.0 0.0.0.127 area 0
network 194.4.7.0 0.0.0.63 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
End

```

Маршрутизатор R_4:

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_4
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
!

```

```

ip tcp synwait-time 5
!
interface Ethernet0/0
no ip address
half-duplex
!
interface Ethernet0/0.107
encapsulation dot1Q 107
ip address 193.4.107.125
255.255.255.128
standby 107 ip 193.4.107.123
standby 107 priority 105
standby 107 preempt
standby 107 track Ethernet1/0
!
interface Ethernet0/0.108
encapsulation dot1Q 108
ip address 193.4.108.125
255.255.255.128
standby 108 ip 193.4.108.123
standby 108 priority 105
standby 108 preempt
standby 108 track Ethernet1/0
!
interface Ethernet0/0.109
encapsulation dot1Q 109
ip address 193.4.109.125
255.255.255.128
standby 109 ip 193.4.109.123
standby 109 priority 96
standby 109 preempt
standby 109 track Ethernet1/0
!
interface Ethernet0/0.110
encapsulation dot1Q 110
ip address 193.4.110.125
255.255.255.128
standby 110 ip 193.4.110.123
standby 110 preempt
standby 110 track Ethernet1/0
!
interface Ethernet0/0.111
encapsulation dot1Q 111

```

```

!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
!
interface Ethernet0/0
no ip address
half-duplex
!
interface Ethernet0/0.107
encapsulation dot1Q 107
ip address 193.4.107.124
255.255.255.128
standby 107 ip 193.4.107.123
standby 107 preempt
standby 107 track Ethernet1/0
!
interface Ethernet0/0.108
encapsulation dot1Q 108
ip address 193.4.108.124
255.255.255.128
standby 108 ip 193.4.108.123
standby 108 preempt
standby 108 track Ethernet1/0
!
interface Ethernet0/0.109
encapsulation dot1Q 109
ip address 193.4.109.124
255.255.255.128
standby 109 ip 193.4.109.123

```

```

ip address 193.4.111.125
255.255.255.128
standby 111 ip 193.4.111.123
standby 111 preempt
standby 111 track Ethernet1/0
!
interface Ethernet1/0
ip address 194.4.7.3 255.255.255.192
half-duplex
!
router ospf 7
router-id 3.3.3.3
log-adjacency-changes
passive-interface Ethernet0/0
passive-interface Ethernet0/0.107
passive-interface Ethernet0/0.108
passive-interface Ethernet0/0.109
passive-interface Ethernet0/0.110
passive-interface Ethernet0/0.111
network 193.4.107.0 0.0.0.127 area 0
network 193.4.108.0 0.0.0.127 area 0
network 193.4.109.0 0.0.0.127 area 0
network 193.4.110.0 0.0.0.127 area 0
network 193.4.111.0 0.0.0.127 area 0
network 194.4.7.0 0.0.0.63 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15

```

```

standby 109 priority 105
standby 109 preempt
standby 109 track Ethernet1/0
!
interface Ethernet0/0.110
encapsulation dot1Q 110
ip address 193.4.110.124
255.255.255.128
standby 110 ip 193.4.110.123
standby 110 priority 96
standby 110 preempt
standby 110 track Ethernet1/0
!
interface Ethernet0/0.111
encapsulation dot1Q 111
ip address 193.4.111.124
255.255.255.128
standby 111 ip 193.4.111.123
standby 111 priority 96
standby 111 preempt
standby 111 track Ethernet1/0
!
interface Ethernet1/0
ip address 194.4.7.4 255.255.255.192
half-duplex
!
router ospf 7
router-id 4.4.4.4
log-adjacency-changes
passive-interface Ethernet0/0
network 193.4.107.0 0.0.0.127 area 0
network 193.4.108.0 0.0.0.127 area 0
network 193.4.109.0 0.0.0.127 area 0
network 193.4.110.0 0.0.0.127 area 0
network 193.4.111.0 0.0.0.127 area 0
network 194.4.7.0 0.0.0.63 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex

```

		Борейченко Г.О.		
		Головня О.С.		
Змн.	Арк.	№ докум.	Підпис	Дата

KIK.KP.Б – 123 – 07 – ПЗ

Арк.

116

```

logging synchronous
line vty 0 4
login
!
!
End
Комутатор SW_2:
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1,107-111 priority
16384
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Port-channel6
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
!

```

```

!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
End
Комутатор SW_3:
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_3
!
logging discriminator EXCESS severity
drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1,107-111 priority
4096
!

```

		Борейченко Г.О.			KIK.KP.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		117

<pre> interface Ethernet0/0 switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk duplex auto ! interface Ethernet0/1 switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk duplex auto ! interface Ethernet0/2 switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk duplex auto ! interface Ethernet0/3 switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk duplex auto channel-group 6 mode on ! interface Ethernet1/0 switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk duplex auto channel-group 6 mode on ! interface Vlan1 no ip address shutdown ! interface Vlan107 no ip address ! interface Vlan108 no ip address ! interface Vlan109 no ip address </pre>	<pre> ! ! ! vlan internal allocation policy ascending ! ip tcp synwait-time 5 ! ! interface Port-channel6 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk ! interface Port-channel5 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk ! interface Port-channel4 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk ! interface Port-channel3 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk ! interface Port-channel2 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 107 switchport mode trunk ! interface Port-channel1 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 107 switchport mode trunk ! </pre>
--	--

```

!
interface Vlan110
  no ip address
!
interface Vlan111
  no ip address
!
!
no ip http server
!
control-plane
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
!
end

```

Комутатор SW_4:

```

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_4
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
!
no ip domain-lookup

```

```

interface Ethernet0/0
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 107-111
  switchport mode trunk
  duplex auto
  channel-protocol lacp
  channel-group 5 mode active
!
interface Ethernet0/1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 107-111
  switchport mode trunk
  duplex auto
  channel-protocol lacp
  channel-group 5 mode active
!
interface Ethernet0/2
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 107
  switchport mode trunk
  duplex auto
  channel-protocol lacp
  channel-group 1 mode active
!
interface Ethernet0/3
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 107-111
  switchport mode trunk
  duplex auto
  channel-group 6 mode on
  spanning-tree guard root
!
interface Ethernet1/0
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 107-111
  switchport mode trunk
  duplex auto
  channel-group 6 mode on
  spanning-tree guard root
!
interface Ethernet1/1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 107-111
  switchport mode trunk

```

		Борейченко Г.О.			KIK.KP.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		119

```

no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1,107-111 priority
8192
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Port-channel6
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
!
interface Port-channel5
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
!
interface Port-channel2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 111
switchport mode trunk
!
interface Port-channel1
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 111
switchport mode trunk
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
duplex auto
channel-protocol lacp

```

```

duplex auto
channel-protocol lacp
channel-group 3 mode active
!
interface Ethernet1/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 3 mode active
!
interface Ethernet1/3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 1 mode active
!
interface Ethernet2/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 4 mode active
!
interface Ethernet2/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 4 mode active
!
interface Ethernet2/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 2 mode active
spanning-tree guard root

```

```

channel-group 5 mode passive
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 5 mode passive
!
interface Ethernet0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 2 mode active
spanning-tree guard root
!
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 2 mode active
spanning-tree guard root
!
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 1 mode active
spanning-tree guard root
!
interface Ethernet1/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 1 mode active

```

```

!
interface Ethernet2/3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 2 mode active
spanning-tree guard root
!
!
interface Vlan1
no ip address
shutdown
!
interface Vlan107
ip address 193.4.107.1 255.255.255.128
shutdown
!
interface Vlan108
ip address 193.4.108.1 255.255.255.128
shutdown
!
interface Vlan109
ip address 193.4.109.1 255.255.255.128
shutdown
!
interface Vlan110
ip address 193.4.110.1 255.255.255.128
shutdown
!
interface Vlan111
ip address 193.4.111.1 255.255.255.128
shutdown
!
no ip http server
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15

```

```

spanning-tree guard root
!
interface Ethernet2/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 6 mode passive
!
interface Ethernet2/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 6 mode passive
!
interface Vlan1
no ip address
shutdown
!
interface Vlan107
ip address 193.4.107.1 255.255.255.128
shutdown
!
interface Vlan108
ip address 193.4.108.1 255.255.255.128
shutdown
!
interface Vlan109
ip address 193.4.109.1 255.255.255.128
shutdown
!
interface Vlan110
ip address 193.4.110.1 255.255.255.128
shutdown
!
interface Vlan111
ip address 193.4.111.1 255.255.255.128
shutdown
!
!
no ip http server

```

```

logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

Комутатор SW_5:

```

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_5
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1,107-111 priority
16384
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Port-channel6
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 110

```

		Борейченко Г.О.			KIK.KP.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		122

<pre> control-plane ! ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous line aux 0 exec-timeout 0 0 privilege level 15 logging synchronous line vty 0 4 login ! end Комутатор SW_6: version 15.1 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption service compress-config ! hostname SW_6 ! boot-start-marker boot-end-marker ! ! no aaa new-model no ipv6 cef ipv6 multicast rpf use-bgp no ip icmp rate-limit unreachable ! no ip domain-lookup ip cef ! spanning-tree mode pvst spanning-tree extend system-id spanning-tree vlan 1,107-111 priority 16384 ! ! ! </pre>	<pre> switchport mode trunk ! interface Port-channel5 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk ! interface Port-channel4 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk ! interface Port-channel2 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 110 switchport mode trunk ! interface Port-channel1 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 109 switchport mode trunk ! interface Ethernet0/0 switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk duplex auto channel-protocol lacp channel-group 5 mode passive ! interface Ethernet0/1 switchport trunk encapsulation dot1q switchport trunk allowed vlan 107-111 switchport mode trunk duplex auto channel-protocol lacp channel-group 5 mode passive ! interface Ethernet0/2 switchport trunk encapsulation dot1q </pre>
--	---

```

!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
interface Port-channel5
no ip address
!
interface Port-channel3
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
!
interface Port-channel2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 109
switchport mode trunk
!
interface Port-channel1
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 108
switchport mode trunk
!
interface Port-channel6
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
!
interface Ethernet0/0
no switchport
no ip address
channel-protocol lacp
channel-group 5 mode active
!
interface Ethernet0/1
no switchport
no ip address
channel-protocol lacp
channel-group 5 mode active

```

```

switchport trunk allowed vlan 109
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 1 mode active
spanning-tree guard root
!
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 109
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 1 mode active
spanning-tree guard root
!
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 110
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 6 mode active
spanning-tree guard root
!
interface Ethernet1/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 110
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 6 mode active
spanning-tree guard root
!
interface Ethernet2/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 4 mode passive
!
interface Ethernet2/1
switchport trunk encapsulation dot1q

```

```

!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 108
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 1 mode active
 spanning-tree guard root
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 108
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 1 mode active
 spanning-tree guard root
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 109
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 2 mode active
 spanning-tree guard root
!
interface Ethernet1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 107-111
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 3 mode passive
!
interface Ethernet1/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 107-111
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 3 mode passive
!
switchport trunk allowed vlan 107-111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 4 mode passive
!
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan107
 ip address 193.4.107.1 255.255.255.128
 shutdown
!
interface Vlan108
 ip address 193.4.108.1 255.255.255.128
 shutdown
!
interface Vlan109
 ip address 193.4.109.1 255.255.255.128
 shutdown
!
interface Vlan110
 ip address 193.4.110.1 255.255.255.128
 shutdown
!
interface Vlan111
 ip address 193.4.111.1 255.255.255.128
 shutdown
!
!
no ip http server
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15

```

```

interface Ethernet1/3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 109
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 2 mode active
spanning-tree guard root
!
interface Ethernet2/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 6 mode passive
!
interface Ethernet2/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107-111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 6 mode passive
!
!
interface Vlan1
no ip address
shutdown
!
interface Vlan107
ip address 193.4.107.1 255.255.255.128
shutdown
!
interface Vlan108
ip address 193.4.108.1 255.255.255.128
shutdown
!
interface Vlan109
ip address 193.4.109.1 255.255.255.128
shutdown
!
interface Vlan110
ip address 193.4.110.1 255.255.255.128

```

```

logging synchronous
line vty 0 4
login
!
end

```

Комутатор SW_7:

```

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_7
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 111
switchport mode trunk
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 111
switchport mode trunk
duplex auto
channel-protocol lacp

```

		Борейченко Г.О.			KIK.KP.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		126

```

shutdown
!
interface Vlan111
ip address 193.4.111.1 255.255.255.128
shutdown
!
!
no ip http server
!
!
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

Комутатор SW_8:

```

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_8
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!

```

```

channel-group 1 mode passive
!
interface Ethernet0/1
switchport access vlan 111
switchport mode access
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree link-type point-to-point
!
interface Ethernet0/2
switchport access vlan 111
switchport mode access
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree link-type point-to-point
!
interface Ethernet0/3
switchport access vlan 111
switchport mode access
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree link-type point-to-point
!
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 1 mode passive
!
interface Vlan1
no ip address
shutdown
!
interface Vlan111
ip address 193.4.111.1 255.255.255.128
shutdown
!
!
no ip http server

```

		Борейченко Г.О.			KIK.KP.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		127

```

ip cef
!
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
interface Port-channel2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 110,111
switchport mode trunk
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 110,111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 2 mode passive
!
interface Ethernet0/1
switchport access vlan 111
switchport mode access
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree link-type point-to-point
!
interface Ethernet0/2
switchport access vlan 111
switchport mode access
duplex auto
spanning-tree portfast

```

```

!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

Комутатор SW_9:

```

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_9
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Port-channel6

```

		Борейченко Г.О.			KIK.KP.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		128

```

spanning-tree bpduguard enable
spanning-tree link-type point-to-point
!
interface Ethernet0/3
switchport access vlan 111
switchport mode access
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree link-type point-to-point
!
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 110,111
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 2 mode passive
!
!
interface Vlan1
no ip address
shutdown
!
interface Vlan110
ip address 193.4.110.1 255.255.255.128
shutdown
!
interface Vlan111
ip address 193.4.111.1 255.255.255.128
shutdown
!
!
no ip http server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15

```

```

switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 110
switchport mode trunk
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 110
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 6 mode passive
!
interface Ethernet0/1
switchport access vlan 110
switchport mode access
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree link-type point-to-point
!
interface Ethernet0/2
switchport access vlan 110
switchport mode access
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree link-type point-to-point
!
interface Ethernet0/3
switchport access vlan 110
switchport mode access
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree link-type point-to-point
!
interface Ethernet1/0
switchport access vlan 110
switchport mode access
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree link-type point-to-point

```

```

logging synchronous
line vty 0 4
login
!
end

```

Комутатор SW_10:

```

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_10
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!

```

```

!
interface Ethernet1/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 110
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 6 mode passive
!
interface Vlan1
no ip address
shutdown
!
interface Vlan110
ip address 193.4.110.1 255.255.255.128
shutdown
!
!
no ip http server
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

Комутатор SW_11:

```

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_11
!

```

<pre> ! interface Port-channel1 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 109 switchport mode trunk ! interface Ethernet0/0 switchport trunk encapsulation dot1q switchport trunk allowed vlan 109 switchport mode trunk duplex auto channel-protocol lacp channel-group 1 mode passive ! interface Ethernet0/1 switchport access vlan 109 switchport mode access duplex auto spanning-tree portfast spanning-tree bpduguard enable spanning-tree link-type point-to-point ! interface Ethernet0/2 switchport access vlan 109 switchport mode access duplex auto spanning-tree portfast spanning-tree bpduguard enable spanning-tree link-type point-to-point ! interface Ethernet0/3 switchport trunk encapsulation dot1q switchport trunk allowed vlan 109 switchport mode trunk duplex auto channel-protocol lacp channel-group 1 mode passive ! interface Ethernet1/0 switchport access vlan 109 switchport mode access duplex auto spanning-tree portfast </pre>	<pre> boot-start-marker boot-end-marker ! no aaa new-model no ip icmp rate-limit unreachable ! ip cef ! ! no ip domain-lookup no ipv6 cef ipv6 multicast rpf use-bgp ! ! spanning-tree mode pvst spanning-tree extend system-id ! vlan internal allocation policy ascending ! ip tcp synwait-time 5 ! interface Port-channel2 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 109 switchport mode trunk ! interface Ethernet0/0 switchport access vlan 109 switchport trunk encapsulation dot1q switchport mode trunk duplex auto channel-protocol lacp channel-group 2 mode passive ! interface Ethernet0/1 switchport access vlan 109 switchport mode access duplex auto spanning-tree portfast spanning-tree bpduguard enable spanning-tree link-type point-to-point ! interface Ethernet0/2 </pre>
---	--

```

spanning-tree bpduguard enable
spanning-tree link-type point-to-point
!
!
interface Vlan1
no ip address
shutdown
!
interface Vlan109
ip address 193.4.109.1 255.255.255.128
shutdown
!
!
no ip http server
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

Комутатор SW_12:

```

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_12
!
boot-start-marker
boot-end-marker
!
!

```

```

switchport access vlan 109
switchport mode access
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree link-type point-to-point
!
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 109
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 2 mode passive
!
!
interface Vlan1
no ip address
shutdown
!
interface Vlan109
ip address 193.4.109.1 255.255.255.128
shutdown
!
!
no ip http server
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end

```

		Борейченко Г.О.			KIK.KP.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		132

```

no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Port-channel1
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 108
switchport mode trunk
!
interface Ethernet0/0
shutdown
duplex auto
channel-protocol lacp
channel-group 1 mode passive
!
interface Ethernet0/1
switchport access vlan 108
switchport mode access
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree link-type point-to-point
!
interface Ethernet0/2
switchport access vlan 108
switchport mode access
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable

```

Комутатор SW_13:

```

version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW_13
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
no ip domain-lookup
!
no ipv6 cef
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Port-channel1
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107
switchport mode trunk
!
interface Port-channel2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107
switchport mode trunk
!
interface Ethernet0/0
switchport trunk encapsulation dot1q

```

		Борейченко Г.О.			KIK.KP.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		133

spanning-tree link-type point-to-point ! interface Ethernet0/3 switchport access vlan 108 switchport mode access duplex auto spanning-tree portfast spanning-tree bpduguard enable spanning-tree link-type point-to-point ! interface Ethernet1/0 switchport access vlan 108 switchport mode access duplex auto spanning-tree portfast spanning-tree bpduguard enable spanning-tree link-type point-to-point ! interface Ethernet1/1 shutdown duplex auto channel-protocol lacp channel-group 1 mode passive ! ! interface Vlan1 no ip address shutdown ! interface Vlan108 ip address 193.4.108.1 255.255.255.128 shutdown ! ! no ip http server ! ! control-plane ! ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous	switchport trunk allowed vlan 107 switchport mode trunk duplex auto channel-protocol lacp channel-group 2 mode passive ! interface Ethernet0/1 switchport access vlan 107 switchport mode access duplex auto spanning-tree portfast edge spanning-tree bpduguard enable spanning-tree link-type point-to-point ! interface Ethernet0/2 switchport trunk encapsulation dot1q switchport trunk allowed vlan 107 switchport mode trunk duplex auto channel-protocol lacp channel-group 2 mode passive ! interface Vlan1 no ip address shutdown ! interface Vlan107 ip address 193.4.107.1 255.255.255.128 shutdown ! ip forward-protocol nd no ip http server ! control-plane ! ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous line aux 0 exec-timeout 0 0 privilege level 15 logging synchronous
---	---

```

line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

Комутатор SW_14:

```

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_14
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Port-channel1
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 107
switchport mode trunk

```

```

line vty 0 4
login
transport input all
!
End

```

Робоча станція WS_webterm

```

# DHCP config for eth0
auto eth0
iface eth0 inet dhcp

```

		Борейченко Г.О.			KIK.KP.B – 123 – 07 – ПЗ	Арк.
		Головня О.С.				135
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 107
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 1 mode passive
!
interface Ethernet0/1
 description LANG
 switchport access vlan 107
 switchport mode access
 duplex auto
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree link-type point-to-point
!
interface Ethernet0/2
 description LANG
 switchport access vlan 107
 switchport mode access
 duplex auto
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree link-type point-to-point
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 107
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 1 mode passive
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan107
 ip address 193.4.107.1 255.255.255.128
 shutdown
!
!

```

		Борейченко Г.О.		
		Головня О.С.		
Змн.	Арк.	№ докум.	Підпис	Дата

KIK.KP.B – 123 – 07 – ПЗ

Арк.

136

```

no ip http server
!
control-plane
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
!
end

```

		Борейченко Г.О.			КІК.КР.Б – 123 – 07 – ПЗ	Арк.
		Головня О.С.				137
Змн.	Арк.	№ докум.	Підпис	Дата		