Міністерство освіти і науки України
Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерних систем та мереж

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА
за спеціальністю 123 «Комп'ютерна інженерія»

Тема наукової роботи:
КОМУТАЦІЙНА МЕРЕЖА ОПЕРАТОРА ЗВ'ЯЗКУ З ОПТИМІЗАЦІЄЮ ЕНЕРГОНЕЗАЛЕЖНОГО РЕЖИМУ РОБОТИ

Виконав _____ В. В. Плінський
Керівник роботи _____ А. О. Сенько
Нормоконтроль _____ Д. І. Кузнєцов
Завідувач кафедри _____ А. І. Купін

Кривий Ріг
2024

Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерних систем та мереж

Ступінь вищої освіти магістр
Спеціальність 123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри, голова циклової комісії

_____ А. І. Купін

"____" _____ 2024 року

ЗАВДАННЯ
НА РОЗРАХУНКОВО-ГРАФІЧНУ РОБОТУ МАГІСТРА

_____
(прізвище, ім'я, по батькові)

1. Тема роботи _____
_____
_____

керівник роботи: _____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від "___"____ 20__року №__

2. Строк подання студентом роботи _____

3. Вихідні дані до роботи _____
_____
_____
_____
_____

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)_____
_____
_____
_____
_____
_____

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)_____
_____
_____
_____

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник роботи _____ _____
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка включає: 135 сторінок, 17 таблиць, 42 рисунки, 37 використаних джерела та 3 додатки.

Робота складається з чотирьох розділів.

Перший розділ присвячено розробці структури мережі оператора зв'язку, як об'єкту дослідження впливу фактору не стабільного енергопостачання на показники роботи мережі оператора. Вирішені такі завдання: вибір оптимального середовища для розробки, визначення вузлів мережі, налаштування взаємодії мережевого обладнання для забезпечення симуляції реального сценарію використання послугою Інтернет. Розглянуті сучасні протоколи динамічної маршрутизації, приклади налаштування актуального програмного забезпечення для забезпечення кінцевих споживачів доступом до глобальної мережі. Було проведене тестування, результати якого засвідчили відповідність фактичних показників до очікуваного.

У другому розділі розглянуті системи віртуалізації, як один із шляхів збільшення автономного часу роботи мережі. Було обґрунтовано доцільність використання комплексів зі створення віртуальних середовищ та зроблено огляд основних характеристик різних типів віртуалізації. Навели приклад розгортання системи та створення віртуальних машин та контейнерів у тестовому середовищі. Окремо було розглянуто сучасні рішення для реалізації веб-серверу, що забезпечує: високу швидкодію, безпеку, швидкість впровадження, зручність адміністрування. Також на базі налаштованого середовища створено базовий веб-сайт, що демонструє загальну працездатність системи.

Третій розділ присвячено дослідженню, на меті якого було визначення оптимальної технології рівня доступу, що є найбільш доцільною до застосування з вимогою енергонезалежності. За допомогою програмного комплексу зробили статистичний аналіз даних служби технічної підтримки оператора зв'язку, який довів значущість фактору тимчасового знеструмлення обладнання у загальній кількості звернень. Використали метод експертної оцінки для визначення технології, яка найкращим чином відповідає вимогам сучасного ринку послуг стаціонарного Інтернет.

У четвертому розділі розглядається приклад практичної імплементації визначеної технології у діючі мережі зв'язку. Був зроблений огляд теоретичного матеріалу та ознайомлення з сучасними практиками щодо впровадження технології пасивних оптичним мереж. Також зроблений розрахунок оптичного бюджету та складений перелік необхідного обладнання для будівництва мережі у обраній локації.

Ключові слова: МЕРЕЖЕВИЙ ЕМУЛЯТОР, МАРШРУТИЗАТОР, КОМУТАТОР, СЕРВЕР ДОСТУПУ, BGP, OSPF, DHCP, PPPOE, RADIUS, NAT, ДІАГНОСТИКА, ВІРТУАЛІЗАЦІЯ, KVM, LXC, ВЕБ СЕРВЕР, СТАТИСТИЧНИЙ АНАЛІЗ, МЕТОД ЕКСПЕРТНИХ ОЦІНОК, PON, ОПТИЧНИЙ БЮДЖЕТ.

Master’s work: 135 pages, 17 tables, 42 figures, 37 used sources and 3 additions.

The work consists of four sections.

The first section is dedicated to the development of the network structure of a telecommunications operator as the object of research into the impact of unstable power supply on the performance indicators of the operator's network. The following tasks were solved: selection of the optimal environment for development, determination of network nodes, configuration of network equipment interaction to ensure the simulation of a real scenario of Internet service usage. Modern dynamic routing protocols were reviewed, as well as examples of configuring relevant software to provide end-users with access to the global network. Testing was conducted, and the results confirmed the compliance of actual performance with expectations.

The second section examines virtualization systems as one of the ways to extend the autonomous operating time of the network. The feasibility of using virtualization environment solutions was justified, and an overview of the main characteristics of different types of virtualization was provided. An example of deploying the system and creating virtual machines and containers in a test environment was given. Modern solutions for implementing a web server that ensures high performance, security, fast deployment, and ease of administration were specifically considered. Additionally, a basic website was created within the configured environment to demonstrate the overall functionality of the system.

The third section focuses on research aimed at determining the optimal access-level technology most suitable for ensuring energy independence. Using a software suite, a statistical analysis of the telecommunications operator's technical support service data was performed, proving the significance of temporary power outages in the total number of customer inquiries. The expert assessment method was used to determine the technology that best meets the requirements of the modern fixed Internet services market.

The fourth section provides an example of the practical implementation of the selected technology in existing communication networks. A theoretical review was conducted, and modern practices for implementing passive optical network (PON) technology were studied. An optical budget calculation was also made, and a list of necessary equipment for network construction in the chosen location was compiled.

Keywords: NETWORK EMULATOR, ROUTER, SWITCH, ACCESS SERVER, BGP, OSPF, DHCP, PPPOE, RADIUS, NAT, DIAGNOSTICS, VIRTUALIZATION, KVM, LXC, WEB SERVER, STATISTICAL ANALYSIS, EXPERT ASSESSMENT METHOD, PON, OPTICAL BUDGET.

ЗМІСТ

ВСТУП

Галузь інформаційних технологій є однією з перших за швидкістю розвитку у сучасному світі. Вона знаходиться у постійному русі, здійснюючи перетворення у всіх аспектах життя суспільства. Для виконання завдань шаблоного аналізу все частіше застосовуються нейронні мережі, для спрощення сприйняття специфичних масивів інформації широко використовуються мовленнєві моделі, а у побуті пересічної людини з'являється все більше підключених до глобальної мережі смарт-пристроїв.

Інформаційні технології стають життєвою необхідністю для бізнесу. Українські компанії все частіше використовують різноманітні програмні рішення для автоматизації бізнес-процесів, управління клієнтською базою та аналізу даних. Наприклад, у сфері електронної комерції активно розвиваються нові сервіси та платформи, які полегшують процеси продажу та підтримки клієнтів. Хмарні сервіси дозволяють зберігати дані в онлайні та мати до них доступ з будь-якого пристрою з Інтернетом. Це забезпечує більшу гнучкість та ефективність у роботі.

Україна також активно розвивається у сфері штучного інтелекту (AI) та машинного навчання (ML). Деякі українські компанії вже успішно впроваджують технології штучного інтелекту для різних завдань, починаючи від аналізу даних і закінчуючи автоматизацією процесів у виробництві.

Також важливою складовою розвитку інформаційних технологій в Україні є освіта. Українські університети активно розвивають програми підготовки IT-спеціалістів, а також організовують різноманітні курси та тренінги з сучасних технологій для широкої громадськості.

Інформаційні технології в Україні мають великий потенціал для подальшого розвитку. За умови правильної стратегії розвитку, активної підтримки держави та підготовки кваліфікованих кадрів, ця галузь може стати одним із ключових драйверів економічного зростання країни.

Видатки на енергетичне забезпечення IT-інфраструктури зростають пропорційно до розширення галузі, саме тому в останні роки дуже велика увага приділяються питанням оптимізації енергоспоживання. Окрім видатків на енергоживлення, через зростання ролі IT у майже всіх сферах життя людини, включаючи не тільки побут, але й бізнес та промисловість, зростають потенційні фінансові втрати через перебої у енергопостачанні. Тому говорячи про енергоефективність, ми обов'язково також маємо на увазі певну автономність для забезпечення безперервного режиму роботи.

Телекомунікація є зв'язуючою ланкою між усіма системами сучасного життя, тому забезпечення безперервності у наданні послуг зв'язку є ключовим

завданням для фахівців галузі.

Актуальність. Регулярні перерви в електропостачанні через збройну агресію російської федерації проти громадян України різко підкреслюють проблему зв'язку в країні. Ця проблема широко висвітлюється у засобах масової інформації, зокрема у інтернет виданні “Українська правда”[1].

Кожен раз, коли вимикається світло, користувачі активно переключаються на використання мережі стільникового зв'язку для передачі даних, що призводить до значного навантаження на вежі мобільних операторів.

Сучасні мобільні мережі розраховані на те, що більшість користувачів використовує провідний стаціонарний інтернет. Однак через раптовий наплив абонентів, мобільні мережі не в змозі задовольнити підвищену потребу. Через це кожного разу під час блекаутів інтернет-мережа мобильних операторів, що є резервною для фіксованого зв’язку, також стає практично недоступною через перевантаження.

Оскільки мобільні оператори та інтернет-провайдери залежать від електроенергії, значні перебої у постачанні електрики залишають українців без зв'язку.

У жовтні 2023 року у зв'язку зі збільшенням споживання електроенергії в регіоні велика частина електричної мережі була тимчасово відключена, що викликало серйозні перебої в роботі мобільного зв'язку. Це підкреслило необхідність розробки стратегій та механізмів для забезпечення неперервного функціонування зв'язку навіть у складних умовах.

Влада також активно впроваджуються заходи для забезпечення неперервності зв'язку в умовах кризи. Наприклад, 26 листопада 2022 року президент Володимир Зеленський ввів у дію рішення РНБО "Про забезпечення електронними комунікаційними послугами в умовах воєнного стану" [2].

Зараз українські оператори зв'язку активно працюють над підвищенням стійкості мережі та вровадженням нових технологій, які дозволять забезпечити неперервний доступ до зв'язку навіть у найскладніших умовах.

Широко застосовуються різні підходи до оптимізації усіх сегментів мереж операторів для покращення енергонезалежності: активно застосовуються підходи віртуалізації для винесення серверної частини поза межі мережі живлення оператора, йдуть процеси оновлення модельного ряду обладнання на більш енергоефективне та йде пошук технологій, що значним чином можуть підвищити відмовостійкість мереж в умовах нестабільного енергопостачання.

Мета дослідження: у дослідженні мають бути вирішені дві важливі задачі, кожна з яких має велике значення для подальшого розвитку та функціонування інформаційних технологій в сучасному світі. Перше завдання полягає в визначенні значущості фактору непередбачуваного знеструмлення обладнання оператора зв'язку на загальну роботу мережі оператора. Це важливо, оскільки доступ до інтернету в сучасному світі стає необхідністю для багатьох аспектів життя, від роботи до розваг, та його надійність є ключовим аспектом задоволення потреб користувачів. Друге завдання передбачає використання методу експертних оцінок для визначення оптимальної технології, яка

відповідатиме нагальним потребам бізнесу і матиме необхідний запас за ключовими параметрами для успішної комерційної експлуатації протягом наступних 10-15 років, з мінімальними витратами на модернізацію. Це означає, що ми маємо вибрати технологічні рішення, які не лише відповідають поточним потребам бізнесу, а й будуть забезпечувати його конкурентоспроможність у майбутньому і дозволять ефективно працювати на протязі тривалого часу.

Об'єктом дослідження є комутаційна мережа оператора зв'язку, статистика звернень абонентів щодо відсутності зв'язку.

Предметом дослідження є енергонезалежний режим роботи обладнання оператора зв'язку, вплив різних факторів на виникнення перебоїв у роботі мережі, шляхи оптимізації мережі для досягнення цілі збільшення часу автономної роботи.

Методи досліджень. Для вирішення першого завдання ми проаналізували за допомогою кореляційного аналізу дані кількості звернень до технічної підтримки оператора зв'язку за 40 днів. Це допомогло нам зрозуміти, які фактори впливають на отримання послуг абонентом у потрібний для нього час.

Друге завдання передбачає використання методу експертних оцінок. Для його вирішення ми залучили експертів з галузі індустрії зв'язку, з розумінням тенденцій ринку та прогнозуванням його розвитку. На основі отриманих даних ми змогли визначити, яка технологія є найбільш вигідною для бізнесу в майбутньому і може забезпечити йому конкурентну перевагу.

Апробацію теми було проведено під час CXXXIII Міжнародної науково-практичної інтернет - конференції «Розвиток науки та техніки України під час воєнного стану», 3 листопада 2023 року[3], а також XVI Всеукраїнської науково-практичної WEB конференції аспірантів, студентів та молодих вчених «Комп'ютерні інтелектуальні системи та мережі» (КІСМ-2024). [4]

Наукові положення. Пошук методів зменьшення споживної потужності мережевою інфраструктурою обумовлений факторами: зростання вартості електроенергії, зростаючими вимогами до автономності. У роботі магістра роглянуті наступні шляхи для збільшення атовномності систем: використання технології серверної віртуалізації, впровадження технології пасивних оптичних мереж PON замість класичної технології FTTB. В ході наукового дослідження за допомогою методу експертної оцінки обгрунтували припущення щодо доцільності використання технології PON виходячи з основного критерію «енергостоживання».

Практичне значення. Дослідження має великий потенціал для вдосконалення інфраструктури зв'язку та забезпечення стабільності та ефективності її роботи в майбутньому. Аналіз впливу непередбачуваних відключень та вибір оптимальної технології для впровадження може допомогти операторам зв'язку підвищити якість своїх послуг і забезпечити задоволення потреб клієнтів протягом тривалого часу.

1. МЕРЕЖІ ОПЕРАТОРА ДРОТОВОГО ЗВ’ЯЗКУ

Об'єктом дослідження у магістерській роботі є мережа оператора зв'язку, тому далі наведений теоретичний матеріал щодо програмних налаштувань кожного з елементів мережі, вимоги до розробленої мережі та пояснення щодо доцільності використання певних технічних рішень.

Корпоративна інформаційна система базується на обчислювальній інфраструктурі, що включає різні компоненти: кабельну мережу, мережеве обладнання, комп'ютери та периферійні пристрої, сховища даних, а також системне програмне забезпечення (операційні системи, бази даних). Вона також використовує спеціальні програми для моніторингу і керування мережею, а в деяких випадках і прикладні програми. В управлінні такою мережею зазвичай застосовується централізована система контролю. Основними активними елементами мережі є: маршрутизатори, комутатори і різні сервери. Маршрутизатор зберігає таблицю маршрутизації, яка може бути статичною або динамічною, залежно від потреб мережі; комутатори забезпечують зв’язок між різними елементами мережі.

При побудові мережі з невеликою кількістю маршрутизаторів (до трьох) найчастіше використовуються статичні маршрути. У випадках складніших і більших мереж варто застосовувати динамічну маршрутизацію. Доступ до основної частини мережі забезпечується через комутатори, які організовують локальні підмережі. Однією з ключових технологій для розгортання сучасних корпоративних мереж є Ethernet [5], але виходячи з вимоги енергонезалежності та автономності, в Україні стрімко розвивається зв’язок за технологією пасивних оптичних мереж.

1.1. Розробка структури мережі оператора

Будь яке проектування починається зі складання та аналізу вимог до системи. В залежності від пріоритету зазначених замовником вимог, проектуальник обирає технічні рішення, що найкращим чином реалізують поставлені завдання. У магістерській роботі розглядається стаціонарна оптоволокона мережа оператору, що надасть змогу користувачам мати доступ до мережі Інтернет у період довготривалих відключень електроживлення.

Вимоги до проектованої мережі

1) Проектована мережа повинна забезпечувати послугами широкосмугового доступу до мережі Інтернет населення, бізнес об'єкти та державні установи з можливістю надання фіксованої IP-адреси та мати

2) автономність з боку оператора до 72 х годин з моменту пропадання енергопостачання у кросовій оператора зв’язку.
3) Оператор повинен мати власну автономну систему з пулом на 1024 фіксованих адрес.
4) Згідно з вимогами потенційного замовника мережа повинна забезпечити якісне покриття для 4000 абонентів.
5) Враховуючи аналітику актуальної статистики використання ємності каналу, необхідно виділяти 1.7 Мбіт/с на кожного абонента. Виходячи з попередньої вимоги, вхідний канал повинен мати ємність не менше ніж 6.8Гбіт/с.
6) Мережа повинна мати резервування основного каналу з ємністю не меньше 30% від ємності основного каналу.
7) Оскільки операторські мережі перебувають у цілодобовій роботі для забезпечення безперервного надання послуг зв'язку, вимоги щодо обладнання є вищими, ніж до пристроїв домашнього та початкового корпоративного класу. Надійність пристроїв характеризується показником середнього наробітку між відмовами MTBF (англ. Mean time between failures - середній час між відмовами, середній наробіток на відмову).
   MTBF у проектованій мережі повинен бути не менше ніж 100000 годин для мережевих пристроїв.
8) Абонентський логічний канал зв’язку повинен мати шифрування.
9) Ядро мережі повинно мати можливість масштабування для потенційного збільшення кількості абонентів від 2 х разів.
10) Мережа оператора повинна включати офіційний сайт для інформування абонентів щодо своєї діяльності.
11) Бажано дотримуватись використання технічних рішень з низького та середнього цінового сегменту для зменшення витрат на старт бізнесу у новій локації.

Для проектування мережі, виходячи з перелічених вище вимог, обираємо для використання на рівні ядра та вузлової комутації обладнання компанії Mikrotik, що має значні переваги у вартості та функціональності, порівняно з іншими брендами, що пропонують власні рішення для побудови корпоративних мереж.

Обладнання компанії Mikrotik відоме своєю високою функціональністю та надійністю, що робить його популярним вибором серед мережевих адміністраторів і підприємств різного масштабу. При порівняно невисокій вартості, роутери, комутатори та інше мережеве обладнання Mikrotik пропонують широкий спектр функцій, які зазвичай доступні лише в продукції преміум-сегменту. Гнучкість налаштувань – ще одна важлива перевага Mikrotik. За допомогою операційної системи RouterOS, користувачі отримують доступ до великої кількості інструментів для налаштування маршрутизації, безпеки, фільтрації трафіку та управління пропускною здатністю. Це дозволяє

підлаштувати мережу під будь-які потреби, починаючи від домашнього використання і закінчуючи масштабними корпоративними мережами.

Продуктивність і стабільність є важливими характеристиками обладнання Mikrotik. Навіть за високих навантажень роутери та комутатори забезпечують стабільну роботу мережі без збоїв, що особливо важливо для бізнесу, де будь-який простій може призвести до значних збитків.

Ще однією суттєвою перевагою є постійні оновлення програмного забезпечення. Mikrotik регулярно випускає нові версії RouterOS, що додають нові можливості та підвищують безпеку обладнання.

Таким чином, обладнання Mikrotik пропонує відмінну функціональність, гнучкість і стабільність за доступною ціною, що робить його ідеальним вибором для різних типів користувачів.

Для рівня доступу, що має бути виконаний за технологією пасивних оптичних мереж, обираємо оптичні термінали компанії BDCOM.

Оптичні термінали компанії BDCOM пропонують широкий спектр переваг, які роблять їх популярним вибором для побудови високошвидкісних мереж. Однією з головних переваг є висока продуктивність. Обладнання BDCOM підтримує сучасні технології передачі даних, що дозволяє забезпечувати стабільні з'єднання з великою пропускною здатністю. Це особливо важливо для підприємств, які потребують безперебійної передачі великих обсягів даних. Також варто відзначити енергоефективність обладнання BDCOM, що є ключовою вимогою проектованої системи. Використання передових технологій дозволяє значно знизити енергоспоживання терміналів, що не лише зменшує витрати на електроенергію, а й сприяє збереженню ресурсів і зменшенню впливу на довкілля.

Надійність оптичних терміналів BDCOM – ще один важливий аспект. Компанія відома своїми високими стандартами якості, що гарантує стабільну роботу навіть в умовах підвищеного навантаження. Це забезпечує безперервну роботу мережі без простоїв, що критично важливо для бізнесу та інтернет-провайдерів.

Гнучкість у налаштуваннях та підтримка різних протоколів робить ці термінали універсальними. Вони легко інтегруються в існуючі мережеві інфраструктури, що полегшує їхнє впровадження та модернізацію мережі.

Доступність і масштабованість продукції BDCOM дозволяє підприємствам будь-якого розміру використовувати оптичні термінали для ефективного розвитку своєї мережевої інфраструктури, зберігаючи при цьому високу якість послуг.

NAS (network access server, мережевый сервер доступу) сервери та сервер з віртуальними машинами виконані на апаратній частині HP Z400, та керуються операційними системи Router OS, та Proxmos на базі ОС Debian.

Склад проектованої мережі.

Проектована система з урахуванням вимог: вартості, масштабування, MTBF, складається з:

- маршрутизатору: CCR2004-1G-12S+2XS;
- коммутатора: CRS326-24S+2Q+RM;
- двох серверів NAS-серверів HP Z400 під керуванням операційної системи Mikrotik RouterOS;
- віртуального серверу HP Z400 з сервісами оператора;
- двох OLT-терміналів: BDCOM GP3600-16;
- системи резервного енергозабезпечення;

Вимога енергозабезпечення протягом 72 х годин з моменту відключення основного джерела електричного струму виконується за наступним сценарієм: у разі відключення першого джерела живлення система живиться за допомогою онлайн джерела безперервного енергозабезпечення від акумуляторних блоків протягом 5ти годин. За цей час представники оператора, що були оповіщені про позаштатну ситуацію, готують до роботи інверторний генератор, що забезпечуватиме живлення подальше живлення системи після вичерпання ємності батарей джерела безперервного енергозабезпечення.

Потужність системи є сумою максимальних споживчих потужностей усіх її елементів. Перелік потужностей обладнання та їх сума наведені у таблиці 1.1.

Таблиця 1.1 - споживча потужність мережевого обладнання системи

№ З/п	Найменування обладнання	Кількість, шт.	Середня потужність на од., Вт.
1	Маршрутизатор CCR2004-1G-12S+2XS [6]	1	49
2	Комутатор CRS326-24S+2Q+RM [7]	1	69
3	Сервер HP Z400 [8]	3	102
4	Оптичний-термінал BDCOM GP3600-16 [9]	2	70
Разом:			564

Для реалізації системи первинного резервування електроживлення використовуємо обладнання компані APC. Обладнання компанії APC є надійним рішенням для резервування енергопостачання серверів, пропонуючи безліч переваг, які роблять його важливим елементом будь-якої IT-інфраструктури. Однією з основних переваг є безперебійна робота серверів під час відключення електроенергії. Завдяки використанню джерел безперебійного живлення (UPS) від APC, сервери продовжують працювати протягом критичного часу, що дозволяє уникнути втрати даних та запобігти пошкодженню обладнання.

Висока надійність обладнання APC забезпечує захист серверів від перепадів напруги, перевантажень і інших проблем з енергопостачанням, що можуть спричинити несправності в системах. Це особливо важливо для бізнесу, де будь-яка зупинка роботи серверів може призвести до фінансових втрат.

Додаткова суттєва перевага — масштабованість. Обладнання APC легко інтегрується в існуючу інфраструктуру і може бути налаштоване відповідно до потреб бізнесу. Це дозволяє з легкістю збільшувати потужність і кількість пристроїв для забезпечення резервного живлення у міру зростання IT-інфраструктури. Окрім цього, інтелектуальні системи моніторингу забезпечують постійний контроль за станом енергопостачання та роботи UPS. Це дозволяє оперативно реагувати на проблеми та вчасно обслуговувати обладнання.

Система резервного енергозабезпечення складається з:

- одного джерела безперервного енергозабезпечення: APC Smart-UPS X;
- 2х додаткових блоків акумуляторів: APC Smart-UPS X-Series External Battery Pack;
- інвертерного генератору: Hyundai HHY 1050Si.

Вибір складу обладнання первинного резервування обумовлений вимогами та розрахованій у таблиці 1.1 середній споживчій потіжності. Завдяки інтерактивному графіку [10] зробили висновок, що ємності обраного обладнання APC вистачить для реалізації запропонованого вище сценарію забезпечення резервування енергоживлення обладнання оператора.

Планована архітектура мережі передбачає, що головний маршрутизатор оператору буде встановлювати BGP-сесії з основним та резервним постачальником послуг. До нього підключаються сервери доступу, віртуальний сервер та комутатор агрегації. На віртуальному сервері розміщені контейнери/віртуальні машини з білінгом, сервером авторизації, DNS-сервером, веб-сервером. Сервери доступу виконують функції: надання доступу до глобальної мережі за результатом авторизації за даними білінгу, NAT для абонентів з “сірими адресами”, надання доступу до глобальної мережі абонентам з активованою послугою статичної IP-адреси, призначення адрес локальної мережі за протоколом DHCP. До комутатору агрегації підключаються усі маршртизатори та оптичні термінали. Для побудови схеми мережі та перевірки налаштувань визначилися з використанням мережевого симулятору.

Мережеві симулятори є невід'ємним інструментом сучасного системного адміністратора та використовуються для моделювання та тестування комп'ютерних мереж без необхідності фізичного обладнання. Вони дозволяють відтворити реальні мережеві топології, що складаються з маршрутизаторів, комутаторів, серверів та інших пристроїв, для перевірки їхньої роботи в різних умовах. Симулятори широко використовуються для навчання, тестування нових конфігурацій, діагностики можливих проблем у мережах, а також для

підготовки до сертифікаційних іспитів у галузі мережевих технологій. Ключовою перевагою використання симуляторів є відсутність необхідності у фізичному обладнанні. Наприклад, замість того, щоб купувати дорогі маршрутизатори або комутатори, користувачі можуть налаштувати їх віртуальні версії за допомогою програмного забезпечення. Це суттєво знижує витрати на навчання та експерименти з мережами. Тобто вони дозволяють експериментувати з різними конфігураціями без ризику пошкодити реальну мережу. Це дає можливість вивчати роботу мереж у різних сценаріях, таких як налаштування безпеки, тестування якості обслуговування або налаштування протоколів маршрутизації. У разі виникнення помилок або збоїв можна легко внести корективи і повторити тестування.

У нашому випадку симулятор використовувався для оптимізації і планування мереж. Симулятор дозволив протестувати продуктивність мережі до її впровадження, допомагаючи прийняти обґрунтовані рішення щодо масштабування, маршрутизації та розподілу ресурсів.

Для побудови структурної схеми мережі та налаштування її елементів використали мережевий симулятор GNS3. Це потужний інструмент для моделювання комп'ютерних мереж, що дозволяє створювати складні мережеві топології без фізичного обладнання. Він підтримує емуляцію різних пристроїв, включаючи маршрутизатори, комутатори та брандмауери, що робить його ідеальним для навчання та тестування мережевих конфігурацій. Схему проектованої мережі представлено на рисунку 1.2.

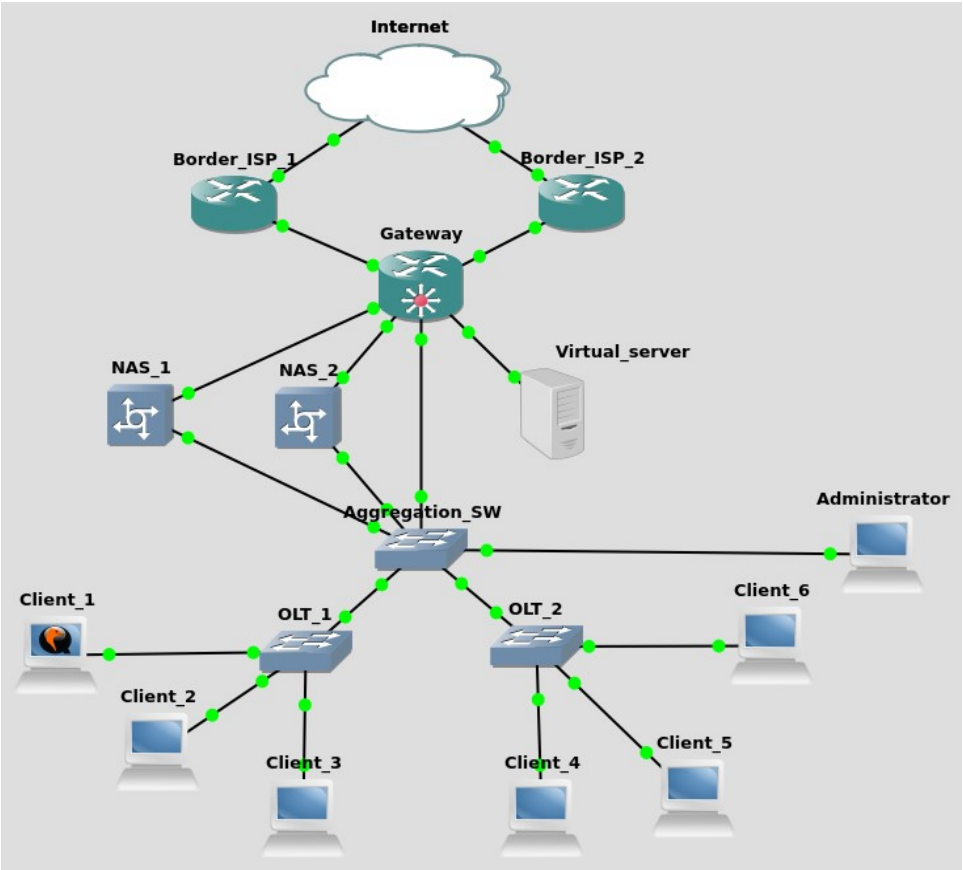

Рисунок 1.2 - схема мережі оператора зв’язку

Адресні простори та ідентифікатори мережі

У проектованій мережі використали наступні адресні простори, номери автономних систем та ідентифікатори віртуальних мереж:

- номер автономної системи проектованої мережі: 65432;
- номер автономної системи основного постачальника вхідного каналу: 64534;
- мережа для встановлення BGP-сессії з основним постачальником: 100.90.80.0/30;
- номер автономної системи резервного постачальника вхідного каналу: 64758;
- мережа для встановлення BGP-сессії резервного постачальника: 100.80.60.0/30;
- мережа адрес, що будуть розглянуті у якості фиксованих зовнішніх IP-адрес, що маршрутизається обраною автономною системою 65432: 100.100.92.0/22;
- підмережі для наданная абонентом послуг зі статичної IP-адреси: 100.100.94.0/24, 100.100.95.0/24;
- підмережа адрес зовнішніх сервісів опреатора: 100.100.92.0/27, vlan 1200;
- підмережа адрес loopback інтерфейсів серверів доступу: 100.100.92.32/28;
- резервована підмережа для потенційних додаткових сервісів: 100.100.92.48/28;
- підмережа адрес для потенційних клієнтів з гарантованим каналом, з типом підключення Static IP, трафік яких не йде повз сервери доступу: 100.100.92.64/26;
- підмережі NAT для серверів доступу по 62 адреси:100.100.92.128/26, 100.100.92.192/26, vlan 1203;
- підмережі для локального адресного простору (DHCP) першого та другого серверу доступу: 10.10.0.0/20; 10.10.96.0/20;
- підмережі для пулів PPPoE-серверів: 10.11.0.0/20; 10.11.96.0/20;
- підмережі для пулів абонентів з несплаченою послугою: 10.12.0.0/20; 10.12.96.0/20;
- підмережа локальних адрес серверів/мережевого обладнання оператору:10.9.8.0/22 vlan 1204;
- підмережа адрес для адміністративної мережі:10.9.16.0/24, vlan 1205;
- номери віртуальних мереж (VLAN) клієнтів:1000-1031;
- номери службових віртуальних мереж (VLAN): 1200-1205.

Повний лістинг налаштувань шлюзу GATEWAY, серверу доступу NAS_1 та комутатору агрегації Aggregation_SW наданий відповідно у додатках: додаток А, додаток Б, додаток В.

1.2. Динамічна маршрутизація у локальній мережі та балансування вхідних каналів. OSPF, BGP.

Маршрутизація є ключовим елементом для ефективного функціонування сучасних комп'ютерних мереж. Її основне завдання — забезпечити передачу даних між різними пристроями та вузлами, які можуть бути розташовані у локальних або глобальних мережах. Маршрутизація виконує важливі функції, що роблять її незамінною для роботи мереж. Маршрутизація дозволяє пакетам даних знайти найоптимальніший шлях від джерела до призначення. Пакети проходять через різні маршрутизатори, що з'єднують мережеві сегменти, забезпечуючи безперервний потік інформації навіть через складні мережі.

Маршрутизатори аналізують доступні шляхи і вибирають ті, які забезпечують найменші затримки або найкращу пропускну здатність. Це дозволяє уникати перевантажень у мережі і підтримувати високий рівень продуктивності. У випадку відмови одного з маршрутизаторів або сегментів мережі, маршрутизація дозволяє пакетам автоматично обирати альтернативний маршрут. Це забезпечує безперебійність зв'язку і знижує ризики простоїв.У великих мережах маршрутизація допомагає з'єднувати різні сегменти, наприклад, локальні мережі (LAN) з глобальними (WAN), забезпечуючи взаємодію між різними частинами інфраструктури.

Маршрутизатори можуть застосовувати механізми фільтрації трафіку та контролю доступу для захисту мереж від несанкціонованих доступів або шкідливих даних.

У складних мережах, де є кілька можливих шляхів для передачі даних між точками, маршрути обираються на основі наявної інформації про топологію мережі. Цей вибір залежить від різних критеріїв, таких як затримка трафіку, пропускна здатність або кількість пройдених маршрутизаторів (хопів). Маршрутизатори використовують таблиці маршрутизації для зберігання інформації про маршрути. Коли пакет потрапляє до маршрутизатора, той порівнює адресу призначення з наявними записами в таблиці та визначає наступний вузол для відправки пакета. Для автоматизації цього процесу маршрутизатори використовують маршрутизуючі протоколи (routing protocols), такі як OSPF або BGP. Ці протоколи дозволяють обмінюватися інформацією про топологію мережі та оновлювати таблиці маршрутизації в реальному часі, що забезпечує точний вибір найкращих маршрутів [11, с-7].

Згідно із вимогами мережа оператора зв’язку має резервування вхідних каналів. З’єднання з основним та резервним постачальником послуг виконане за допомогою протоколу BGP. Резервування також реалізоване за допомогою цього протоколу.

Протокол BGP (Border Gateway Protocol) працює на основі так званих “автономних систем” (AS – Autonomous System). Кожна автономна система представляє собою групу мережевих пристроїв, які належать до певної організації або провайдера. Усередині автономної системи для обміну маршрутною інформацією між маршрутизаторами використовується Internal BGP (внутрішній BGP, IBGP). Це дозволяє маршрутизаторам ділитися

інформацією про доступні маршрути, забезпечуючи ефективну передачу даних всередині мережі [11, с-43].

Коли виникає необхідність обміну маршрутною інформацією між різними автономними системами, застосовується External BGP (зовнішній BGP, EBGP). Зовнішній BGP дозволяє автономним системам взаємодіяти одна з одною, забезпечуючи глобальний обмін маршрутами між різними провайдерами та організаціями. Це надзвичайно важливо для Інтернету, оскільки дозволяє окремим мережам зв'язуватися між собою, формуючи єдину глобальну мережу.

Одна з особливостей протоколу BGP полягає в тому, що “відносини між сусідніми маршрутизаторами” (пірінг або "сусідство") необхідно налаштовувати вручну. Це означає, що адміністраторам мережі потрібно конфігурувати зв'язки між маршрутизаторами для обміну маршрутами за допомогою BGP. У порівнянні з іншими динамічними протоколами маршрутизації, такими як OSPF чи EIGRP, де сусідство часто встановлюється автоматично, BGP вимагає чіткого налаштування та координації між двома сторонами. Коли організація потребує налаштування BGP для зв'язку з провайдером Інтернет-послуг (ISP), необхідна тісна взаємодія між обома сторонами. Це включає налаштування пірінгових сесій, обмін маршрутною інформацією і забезпечення правильного управління маршрутами для уникнення конфліктів або затримок у мережі.

Завдяки своїй гнучкості та масштабованості, BGP став ключовим протоколом для забезпечення стабільності та надійності роботи Інтернету на глобальному рівні.

Вхідні параметри для налаштування головного шлюзу (Gateway):

- номер автономної системи проектованої мережі: 65432;
- номер автономної системи основного постачальника вхідного каналу: 64534;
- мережа для встановлення BGP-сессії з основним постачальником: 100.90.80.0/30;
- номер автономної системи резервного постачальника вхідного каналу: 64758;
- мережа для встановлення BGP-сессії резервного постачальника: 100.80.60.0/30.

Налаштування маршрутизатору Gateway виконали у наступному порядку:

- зміна стандартного паролю (лістинг 1.3);
- перейменування інтерфейсів (лістинг 1.4);
- додавання адрес на визначені інтерфейси (лістинг 1.5);
- налаштування шаблону для використання у BGP сесіях (лістинг 1.6);
- налаштування вихідного та вхідного фільтрів BGP (лістинг 1.7)
- встановлення BGP-сесій (лістинг 1.8).

Згідно визначеного порядку налаштування приведений лістинг команд:

```
password old-password=123456 new-password=123456 confirm-new-рфііцщкв=123456
```

Лістинг 1.3

```
/interface ethernet
set [ find default-name=ether1 ] disable-running-check=no name=ether1_external_1
set [ find default-name=ether2 ] disable-running-check=no name=ether2_external_2
```

Лістинг 1.4

```
/ip address
add address=100.90.80.2/30 interface=ether1_external_1 network=100.90.80.0
add address=100.80.60.2/30 interface=ether2_external_2 network=100.80.60.0
```

Лістинг 1.5

```
/routing bgp template
set default as=65432 disabled=no output.redistribute=connected router-id=100.92.0.3 routing-table=main
```

Лістинг 1.6

```
/routing filter rule
add chain=bgp_out_1 disabled=no rule="if (dst == 100.100.92.0/22) { accept; }"
add chain=bgp_in_1 disabled=no rule="if (dst == 0.0.0.0/0) { set distance +200; set bgp-local-pref 200;
accept; }"
add chain=bgp_in_2 disabled=no rule="if (dst == 0.0.0.0/0) { set distance +210; set bgp-local-pref 199;
accept
```

Лістинг 1.7

```
/routing bgp connection
add as=65432 disabled=no input.filter=bgp_in_1 local.role=ebgp name=bgp_peer_1 output.filter-
chain=bgp_out_1 remote.address=100.90.80.1/32 .as=64534 router-id=100.100.92.3 routing-table=main
templates=default
add as=65432 disabled=no input.filter=bgp_in_2 local.role=ebgp name=bgp_peer_2 output.filter-
chain=bgp_out_1 remote.address=100.80.60.1/32 .as=64758 router-id=100.100.92.3 routing-table=main
templates=default
```

Лістинг 1.8

За допомогою атрибутів “bgp-local-pref ” та “distance” задаємо порядок використання першого та другого з’єднання з операторами вищого рівня, що забезпечує балансування каналів. Налаштування додаткового фільтру на віддачу тільки зовнішньої мережі запобігає передачі локальних маршрутів у мережі постачальників.

На рисунку 1.9 зображений статус встановлення сесій з надавачами послуг та основні параметри з'єднання.

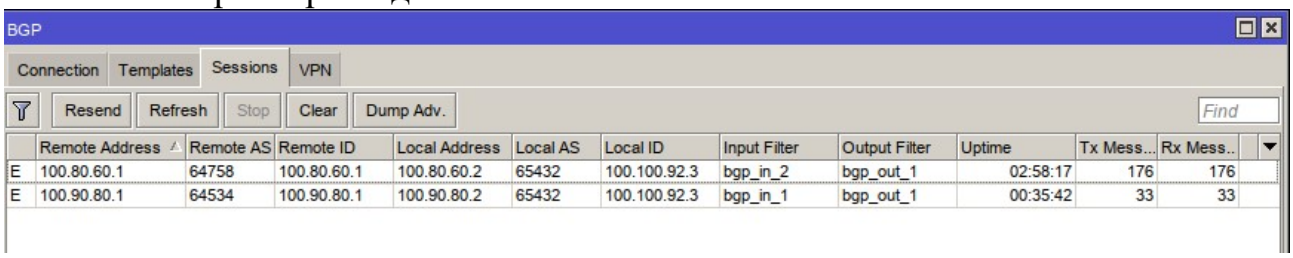

Рисунок 1.9 - вікно статусу встановлення BGP-сесій

Для обміну інформації щодо наявних локальних підмереж між пристроями використали протокол OSPF.

OSPF (Open Shortest Path First) — це протокол маршрутизації, що ґрунтується на алгоритмі найкоротшого шляху та використовує відкриті стандарти для обміну маршрутною інформацією між маршрутизаторами. Він

відноситься до протоколів маршрутизації за станом каналів (link-state), що робить його надійним і ефективним рішенням для великих та складних мереж. OSPF підтримує ієрархічну структуру, що дозволяє розбивати великі мережі на зони, де кожна зона під'єднана до головної зони — зони нуль або зони магістралі (backbone area). Така структура знижує кількість службового трафіку, що передається по мережі, і підвищує продуктивність. Це важливо для забезпечення швидкої конвергенції мережі та зменшення впливу на мережу у разі збою або зміни топології.

Однією з головних переваг OSPF є його здатність до швидкої конвергенції, тобто до швидкого оновлення маршрутів при зміні стану мережі. Завдяки алгоритму Дейкстри (SPF), OSPF швидко обчислює найкоротший шлях до призначення для кожного маршрутизатора на основі зібраної інформації про стан каналів. Кожен OSPF-маршрутизатор обмінюється інформацією про свої канали з сусідами через спеціальні повідомлення, відомі як LSA (Link State Advertisements). Ці повідомлення розповсюджуються мережею методом лавинної розсилки, забезпечуючи всі маршрутизатори в зоні однаковою інформацією про топологію мережі. Така архітектура гарантує, що кожен маршрутизатор володіє актуальними даними для побудови найефективніших маршрутів. OSPF також підтримує граничні маршрутизатори зон (Area Border Routers, ABR), які з'єднують різні зони та обробляють інформацію про топологію для кожної з них окремо. Це дозволяє локалізувати зміни топології в межах однієї зони, не впливаючи на інші, що зменшує навантаження на всю мережу.

Додатковою важливою особливістю OSPF є підтримка автентифікації. Це підвищує безпеку мережі, оскільки маршрутизатори можуть перевіряти автентичність отриманої інформації перед її використанням. OSPF широко використовується в корпоративних мережах і мережах провайдерів завдяки своїй гнучкості, ефективності та масштабованості. Він забезпечує надійну маршрутизацію навіть у складних і великих інфраструктурах, роблячи його одним із найпопулярніших протоколів динамічної маршрутизації у світі. [11, с-35].

У спроектований у магістерській роботі мережі маємо 3 маршрутизатори: Gateway, NAS_1, NAS_2. між собою вони обмінюються маршрутною інформацією за допомогою OSPF. Маршрутизатор Gateway знаходиться тільки у
у зоні backbone, але сервери доступу NAS_1, NAS_2 окрім backbone мають так звані “тупікові зони” з адресами локальних підмереж, якими керує безпосередньо сервер.

Налаштовуємо OSPF за наступною послідовністю:

- додавання адрес на визначені інтерфейси
- створення фільтри зі вказанням обов'язкових адрес для передачі підмереж зі статичними IP-адресами;
- створення інстанцію;
- створення зон;

- створення шаблонів з вказанням мереж та інтерфейсів.

Налаштування динамічної маршрутизації на Gateway, NAS_1, NAS_2 з використанням протоколу OSPF наведені у лістингах 1.11, 1.12, 1.13 відповідно.

```
/routing filter rule
add chain=ospf_out comment=clients_stst_ip_networks disabled=no rule="if (dst in 100.100.94.0/24)
{accept}if (dst in 100.100.95.0/24) {accept}"
```

Лістинг 1.10

```
/routing ospf instance
add disabled=no name=10.9.8.1 originate-default=alway
/routing ospf area
add disabled=no instance=10.9.8.1 name=backbone
/routing ospf interface-template
add area=backbone disabled=no interfaces=ext_services networks=100.100.92.0/27
```

Лістинг 1.11

```
/routing ospf instance
add disabled=no name=NAS_1 out-filter-chain=ospf_out router-id=100.100.92.1
/routing ospf area
add disabled=no instance=NAS_1 name=backbone
add area-id=10.10.0.0 disabled=no instance=NAS_1 name=local_dhcp type=stub
add area-id=10.11.0.0 disabled=no instance=NAS_1 name=local_pppoe type=stub
add area-id=10.12.0.0 disabled=no instance=NAS_1 name=local_debtor type=stub
add area-id=100.100.94.0 default-cost=1 disabled=no instance=NAS_1 name=stat_ip_ppooe no-summaries
nssa-translator=candidate type=stub
/routing ospf area range
add area=backbone disabled=no prefix=100.100.92.0/27
add area=local_dhcp disabled=no prefix=10.10.0.0/20
add area=local_pppoe disabled=no prefix=10.11.0.0/20
add area=local_debtor disabled=no prefix=10.12.0.0/20
/routing ospf interface-template
add area=backbone disabled=no interfaces=ext_services networks=100.100.92.0/27
add area=local_dhcp disabled=no networks=10.10.0.0/20 passive
add area=local_pppoe disabled=no networks=10.11.0.0/20 passive
add area=local_debtor disabled=no networks=10.12.0.0/20 passive
add area=stat_ip_ppooe disabled=no interfaces=local_loop networks=100.100.92.33/32 passive
```

Лістинг 1.12

```
/routing ospf instance
add disabled=no name=NAS_2 out-filter-chain=ospf_out router-id=100.100.92.2
/routing ospf area
add disabled=no instance=NAS_2 name=backbone
add area-id=10.10.96.0 disabled=no instance=NAS_2 name=local_dhcp type=stub
add area-id=10.11.96.0 disabled=no instance=NAS_2 name=local_pppoe type=stub
add area-id=10.12.96.0 disabled=no instance=NAS_2 name=local_debtor type=stub
add area-id=100.100.94.0 default-cost=1 disabled=no instance=NAS_2 name=stat_ip_ppooe no-summaries
nssa-translator=candidate type=stub
/routing ospf area range
add area=backbone disabled=no prefix=100.100.92.0/27
add area=local_dhcp disabled=no prefix=10.10.96.0/20
add area=local_pppoe disabled=no prefix=10.11.96.0/20
add area=local_debtor disabled=no prefix=10.12.96.0/20
/routing ospf interface-template
add area=backbone disabled=no interfaces=ext_services networks=100.100.92.0/27
```

```
add area=local_dhcp disabled=no networks=10.10.96.0/20 passive
add area=local_pppoe disabled=no networks=10.11.96.0/20 passive
add area=local_debtor disabled=no networks=10.12.96.0/20 passive
add area=stat_ip_ppooe disabled=no interfaces=local_loop networks=100.100.92.34/32 passive
```

Лістинг 1.13

Зазначимо, що на маршрутизаторі Gateway (лістинг 1.10) налаштовано редистрибуцію маршруту за замовчуванням для уникнення необхідності додавати додатковий маршрут на серверах доступу; а у шаблонах зі stub-зонами вказано, що інтерфейси у цій зоні є пасивними, тобто з ними не ведеться обмін маршрутною інформацією за цим протоколом.

Результат правильності виконаних налаштувань показаний на рисунку 1.14, де ми бачимо таблицу марштутизації Gateway з отриманими як за протоколом BGP маршрутами за замовчуванням, так і отриманими за протоколом OSPF маршрутами з локальними підмережами від серверів доступу NAS_1 та NAS_2.

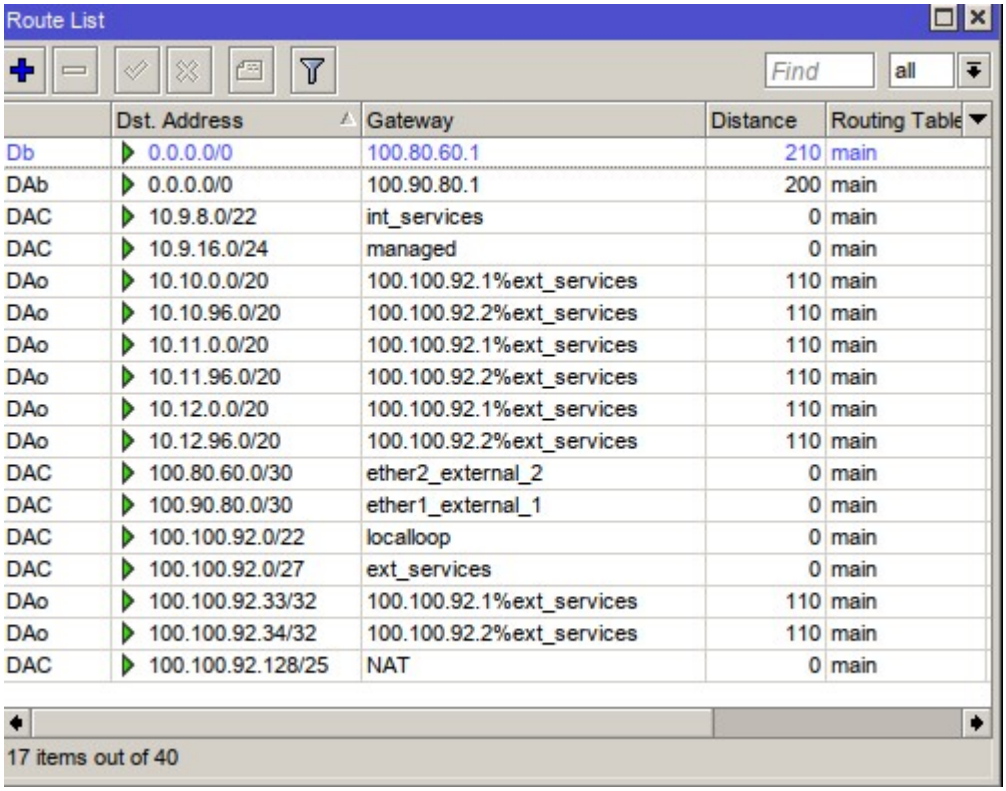

Рисунок 1.14 - таблиця маршрутизації Gateway

Також на рисунку 1.15 зображена таблиця маршрутизації серверу доступу NAS_2 з отриманим від Gateway маршрутом за замовчуванням, локальними підмережами та підмережею зовнішніх адрес NAS_1.

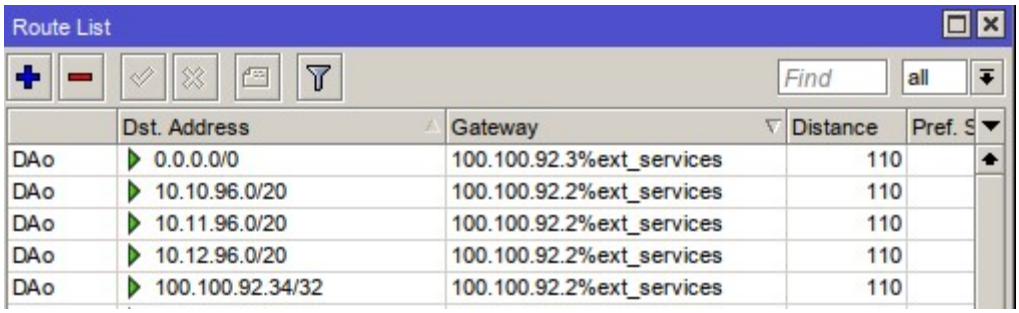

Рисунок 1.15 - таблиця маршрутизації NAS_2

Аналогічну таблицу маємо на сервері доступу NAS_1. На рисунку 1.16 зображені отримані мрашути від Gateway та NAS_2.

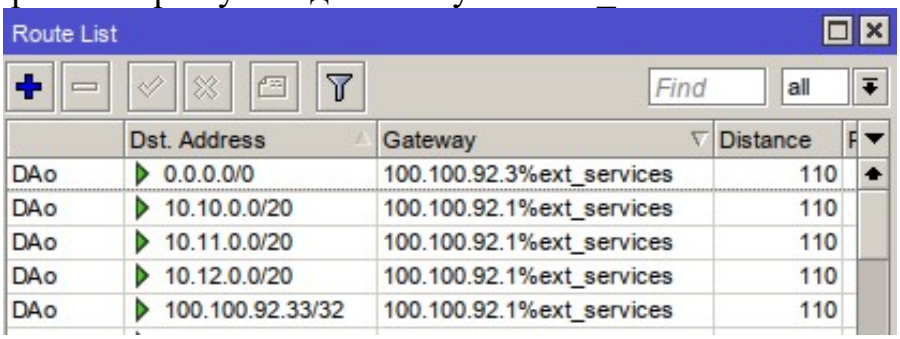

Рисунок 1.16 - таблиця маршрутизації NAS_1

1.3. Локальний сегмент мережі оператора зв'язку. VLAN, DHCP, PPPoE, NAT.

Локальна мережа оператора є сукупністю встановленого або орендованого обладнання/каналів зв'язку та логічних зв'язків між ними. У магістерській роботі розглянуто мережу для забезпечення послугами доступу до Інтернет до 4096 абонентів. Локальна мережа фізично складається з обладнання вказаного у таблиці 1.1 та логічно розділена на підмережі не тільки адресними просторами, та й з використання технології VLAN.

Віртуальна локальна мережа (VLAN) — це технологія, яка дозволяє розділити фізичну мережу на кілька логічних сегментів, що функціонують незалежно один від одного. VLAN створює групи вузлів мережі, ізольованих на канальному рівні, що означає, що кадри всередині однієї VLAN не можуть бути передані до іншої VLAN на основі MAC-адреси. Це ізоляція поширюється на будь-які кадри, включаючи одиничні, групові або широкомовні.

В межах однієї VLAN кадри передаються за стандартною технологією канального рівня, що забезпечує нормальне функціонування комунікацій між вузлами всередині цього логічного сегмента. При цьому, фізична структура мережі може відрізнятися, оскільки вузли з однієї VLAN можуть бути під'єднані до різних комутаторів. Завдяки цьому VLAN дозволяє відокремити логічну структуру мережі від її фізичної конфігурації, що робить мережу більш гнучкою та зручною для управління. Однією з функцій VLAN є обмеження широкомовного трафіку. Усі широкомовні кадри та кадри, для яких комутатор

не може знайти MAC-адресу отримувача, залишаються в межах однієї VLAN. Це значно знижує навантаження на мережу, оскільки мінімізується кількість широкомовних штормів, які можуть негативно впливати на продуктивність мережі. Додатково у технології VLAN є можливість гнучкого розподілу користувачів на ізольовані групи. Кожен користувач або пристрій в мережі може бути включений до своєї VLAN, забезпечуючи їхню ізоляцію на канальному рівні. Це підвищує рівень безпеки, оскільки обмежується розповсюдження кадрів другого рівня (MAC-кадрів) лише в межах однієї VLAN. Для зв'язку між різними VLAN необхідне обладнання комутації третього рівня, що дозволяє реалізувати політику взаємодії між різними сегментами мережі.

Окрім безпеки та ізоляції, VLAN дозволяє оптимізувати керування трафіком у мережі. Кадри другого рівня можуть бути спрямовані за необхідними шляхами, що допомагає контролювати потоки трафіку в різних сегментах мережі, покращуючи її загальну продуктивність і надійність. Таким чином, використання VLAN є ефективним інструментом для побудови гнучкої, безпечної та продуктивної мережевої інфраструктури [12].

Технологія VLAN використана як для розділення службових мереж з зовнішніми адресами, так й для відокремлення абонентських підмереж. Рівень доступу згідно таблиці 1.1 представлений двома оптичними терміналами, що мають по 16 портів кожних. Для кожного фізичного порту виділили по 1 VLAN, тому кількість абонентський підмереж та вланів дорівнює 32. Абонентські влани створені на серверах доступу, на комутаторі агрегації та безпосередньо на оптичних терміналах. У даному розділі розглядаємо створення та налаштування абонентських мереж на серверах доступу та на комутаторі агрегації. Налаштування оптичних терміналах розглянуто у розділі 1.6. Оскільки на усіх перелічених вузлах встановлене обладнання одного вендора, лістинг створення вланів буде схожим. Нижче для прикладу наведений частковий лістинг 1.17 з командами для створення абонентських вланів на інтерфейсі серверу доступу NAS_1, що відповідає за локальну абонентську мережу.

```
/interface vlan
add interface=ether2_internal name=local_00 vlan-id=1000
add interface=ether2_internal name=local_01 vlan-id=1001
……
add interface=ether2_internal name=local_30 vlan-id=1030
add interface=ether2_internal name=local_31 vlan-id=1031
```

Лістинг 1.17

Для абонентських мереж використані влан з ідентифікатором від 1000 до 1031. Назва влану частково співпадає з ідентифікатором для зручності експлуатації.

Коефіцієнт розділення кожного порту є 1:128, але для зручності використовуємо абонентські підмережі по 256 хостів, тобто мережі з маскою /24.

Адреси абонентським пристроям будуть виділятися автоматично з використанням протоколу DHCP. DHCP дозволяє автоматизувати процес призначення IP-адрес та інших параметрів мережі (наприклад, маски підмережі, шлюзу за замовчуванням) кожному вузлу. Клієнти мережі отримують IP-адреси на певний термін, який називається лізингом . Цей підхід дозволяє ефективно керувати обмеженим ресурсом IP-адрес у великих мережах і зменшити потребу в ручному налаштуванні.

DHCP може працювати в кількох режимах:

1). Динамічний розподіл . У цьому режимі DHCP-сервер виділяє IP-адреси з попередньо налаштованого діапазону на певний період часу. Коли термін дії оренди закінчується, клієнт має або продовжити лізинг, або звільнити IP-адресу, яка повертається до пулу доступних адрес.

2). Автоматичне виділення . У цьому випадку DHCP-сервер намагається призначити вузлу ту IP-адресу, яку він використовував раніше, якщо вона ще доступна. Це забезпечує стабільність налаштувань для клієнтів, які часто підключаються до тієї самої мережі.

3). Статичний розподіл . Адміністратор може зафіксувати IP-адресу для певного пристрою на основі його MAC-адреси . Це дозволяє уникнути випадкового зміщення важливих пристроїв, таких як сервери або принтери, до нових IP-адрес під час роботи мережі.

Процес отримання IP-адреси через DHCP починається з того, що клієнт, який не має IP-адреси, відправляє спеціальне широкомовне повідомлення — DHCP DISCOVER . У ньому він використовує свою MAC-адресу, а як IP-адресу джерела вказує 0.0.0.0, оскільки власної IP-адреси ще не має. Це повідомлення пересилається всім пристроям у мережі і повинно досягти DHCP-сервера.

Після отримання запиту DHCP-сервер перевіряє наявність вільних IP-адрес у своєму пулі та відправляє клієнту відповідь у вигляді повідомлення DHCP OFFER , яке містить запропоновану IP-адресу, тривалість оренди та додаткові параметри (маску підмережі, шлюз). Якщо в мережі є кілька DHCP-серверів, клієнт може отримати кілька пропозицій. Наступним етапом клієнт вибирає одну з отриманих пропозицій і надсилає широкомовний DHCP REQUEST , щоб підтвердити вибір IP-адреси. У цьому повідомленні зазначено, яку саме адресу клієнт вибрав та який сервер її запропонував. На завершальному етапі DHCP-сервер підтверджує запит за допомогою повідомлення DHCP ACK , яке містить остаточні дані для налаштування мережевого інтерфейсу клієнта. Після отримання цього підтвердження клієнт використовує надану IP-адресу до закінчення терміну дії оренди або до наступного перезапуску.

Завдяки DHCP мережеві адміністратори можуть ефективно керувати адресним простором, а клієнти можуть автоматично отримувати всі необхідні налаштування для роботи в мережі без втручання користувачів [13].

Налаштування DHCP-серверів на обладнанні під керуванням Mikrotik Router OS виконують за наступним порядком:

- створення пулів з адресами для видачі (з резервуванням для можливих службових цілей перших 10 адрес у кожному пулі);
- додавання адреси на інтерфейс шлюзу, з якого буде відбуватися видача адрес хостам;
- додавання серверу з вказанням інтерфейсу, пулу для видачі адрес та додатковими параметрами за необхідності, наприклад часом оренди адреси, або назву налаштування;
- додавання шаблону для кожної підмережі, де вказується адреса шлюз та адреси додаткових сервісів, наприклад: DNS, NTP та інші.

У лістингу 1.18 наведений перелік команд для налаштування DHCP-серверів для серверу доступу NAS_1 для першої та останньої абонентської мережі за наведеним вище порядком.

```
/ip pool
add name=pool_local_00 ranges=10.10.0.10-10.10.0.254
add name=pool_local_31 ranges=10.10.31.10-10.10.31.254
/ip address
add address=10.10.0.1/24 interface=local_00 network=10.10.0.0
add address=10.10.31.1/24 interface=local_31 network=10.10.31.0
/ip dhcp-server
add add-arp=yes address-pool=pool_local_00 interface=local_00 lease-time=2m name=DHCP_vlan_1000
add add-arp=yes address-pool=pool_local_31 interface=local_31 lease-time=2m name=DHCP_vlan_1031
/ip dhcp-server network
add address=10.10.0.0/24 dns-server=100.100.92.4 gateway=10.10.0.1
add address=10.10.31.0/24 dns-server=100.100.92.4 gateway=10.10.31.1
```

Лістинг 1.18

Сервер доступу NAS_2 є резервним для видачі адрес хостам, тому при додаванні серверів до абонентських вланів додаємо параметр *delay-threshold=20s*, що дозволить надавати адреси від резервного серверу тільки у випадку відсутності відповіді від основного DHCP- серверу протягом 20 секунд.

Доступ до локальної мережі є вільним. Для доступу до мережі інтернет використовується підключення PPPoE з авторизацією за логіном та паролем.

PPPoE (Point-to-Point Protocol over Ethernet) — це технологія, яка дозволяє встановлювати з'єднання між кінцевим користувачем та інтернет-провайдером через Ethernet-мережі. Вона поєднує в собі функції протоколу PPP, який використовується для передачі даних через телефонні лінії, і стандарту Ethernet, що забезпечує передачу даних у локальних мережах. PPPoE широко використовується для підключення до Інтернету через DSL, кабельні модеми та інші види широкосмугових з'єднань. Оскільки PPPoE використовує аутентифікацію через логін і пароль, інтернет-провайдери можуть контролювати доступ до своїх ресурсів, надавати різні тарифи та моніторити трафік кожного користувача окремо. Такий підхід робить PPPoE зручним для

комерційного використання, зокрема для тарифікації та обліку споживаного інтернет-трафіку.

Процес встановлення з'єднання через PPPoE починається з ініціації з'єднання клієнтом, який надсилає запит на сервер провайдера. Сервер відповідає, надаючи IP-адресу, налаштування DNS та інші мережеві параметри. Після цього між клієнтом і сервером встановлюється сесія, через яку передаються дані. PPPoE забезпечує капсуляцію трафіку, що дозволяє передавати пакети через Ethernet, гарантуючи при цьому конфіденційність і безпеку даних, роблячи його ефективним рішенням для підключення до Інтернету через широкосмугові мережі, забезпечуючи одночасно гнучкість і контроль за користувачами [14].

За аналогією до DHCP-сервером, створюється PPPoE-сервер для кожної з абонентських підмереж та призначається до відповідного інтерфейсу маршрутизатору. У нашому випадку цими інтерфейсами є VLAN.

Налаштування PPPoE-серверів на обладнанні під керуванням Mikrotik RouterOS виконують за наступним порядком:

- створення пулу за адресами для клієнтів;
- створення шаблону для використання PPPoE-серверами з вказанням додаткових параметрів, наприклад адресу серверу чи використання шифрування або компресії;
- створення безпосередньо PPPoE-серверів з вказанням додадкових параметрів, наприклад: ім’я служби.
- підключення Radius-серверу (серверу авторизації) замість використання локальних даних для авторизації.

У лістингу 1.19 наведений перелік команд для налаштування PPPoE-серверів для серверу доступу NAS_1 для першої та останньої абонентської мережі за наведеним вище порядком.

```
/ip pool
add name=pool_pppoe ranges=10.11.0.1-10.11.15.254
/ppp profile
add change-tcp-mss=yes dns-server=100.100.92.4 local-address=100.100.92.33 name=PPPoE_prifile only-one=yes remote-address=pool_pppoe use-encryption=yes use-ipv6=no
/interface pppoe-server server
add authentication=pap,chap default-profile=PPPoE_prifile disabled=no interface=local_00 one-session-per-host=yes service-name=operator
add authentication=pap,chap default-profile=PPPoE_prifile disabled=no interface=local_31 one-session-per-host=yes service-name=operator
/ppp aaa
set accounting=no use-radius=yes
```

Лістинг 1.19

Для надання авторизованим клієнтам доступу до мережі інтернет через зовнішні адреси серверів доступу використовується механізм NAT та PAT.

Трансляція IP-адрес за допомогою NAT (Network Address Translation), визначена в RFC 3022, дозволяє вузлам у приватній мережі, які не мають

глобально унікальних зареєстрованих IP-адрес, взаємодіяти з іншими вузлами через Інтернет. Використання NAT дозволяє замінювати приватні IP-адреси на публічні, зареєстровані IP-адреси в кожному пакеті, що проходить через маршрутизатор або інший пристрій, який підтримує цю технологію.

NAT функціонує як посередник між приватною мережею і глобальною мережею, наприклад, Інтернетом. Приватні адреси, які використовуються всередині локальної мережі, не є унікальними в глобальному масштабі і не можуть безпосередньо використовуватися для зв'язку з інтернет-серверами. Проте завдяки NAT, ці приватні IP-адреси можуть бути замінені на публічні адреси під час виходу на зовнішні мережі, забезпечуючи тим самим доступ до Інтернету для пристроїв, які використовують приватні адреси. Основна функція NAT полягає в тому, щоб замінювати приватні IP-адреси на зареєстровані публічні IP-адреси в полі відправника кожного IP-пакета. Цей процес називається трансляцією мережевих адрес. Маршрутизатор NAT також веде таблицю відповідностей між приватними і публічними IP-адресами, що дозволяє контролювати і маршрутизувати зворотний трафік до правильних пристроїв у локальній мережі.

Типи IP-адрес у NAT:

1) внутрішні (приватні) IP-адреси: використовуються в межах локальних мереж і не призначені для глобального використання. Вони належать до таких діапазонів:
    a) 10.0.0.0 - 10.255.255.255 (10.0.0.0/8) – одна мережа класу A.
    b) 172.16.0.0 - 172.31.255.255 (172.16.0.0/12) – група з 16 суміжних мереж класу B.
    c) 192.168.0.0 - 192.168.255.255 (192.168.0.0/16) – група з 256 мереж класу C.
2) зовнішні (публічні) IP-адреси: це зареєстровані глобально унікальні IP-адреси, які надаються інтернет-провайдерами для забезпечення зв'язку між локальними мережами і глобальними мережами, такими як Інтернет.

NAT дозволяє використовувати одну публічну IP-адресу для кількох пристроїв у локальній мережі. Це досягається за рахунок динамічної трансляції адрес і є вигідним рішенням для мереж середнього розміру, які потребують доступу до Інтернету через єдину IP-адресу.

PAT (Port Address Translation) є різновидом NAT, який додатково використовує порти для мультиплексування кількох приватних IP-адрес на одну публічну IP-адресу. У PAT кожному з'єднанню з Інтернетом призначається унікальний порт разом із публічною IP-адресою. Ця технологія забезпечує можливість одночасного використання одного публічного IP для великої кількості пристроїв у локальній мережі. PAT працює наступним чином: коли пристрій у локальній мережі надсилає запит до Інтернету, NAT змінює IP-адресу відправника на публічну IP-адресу маршрутизатора і додає унікальний порт для кожного з'єднання. То ж, коли відповідь повертається з Інтернету,

маршрутизатор за допомогою таблиці трансляції може визначити, до якого внутрішнього пристрою і порту направити відповідь.

PAT має низку переваг порівняно з NAT:

- ефективне використання IP-адрес. Один публічний IP може використовуватися сотнями пристроїв, що знижує потребу в додаткових IP-адресах;
- гнучкість. Оскільки кожне з'єднання використовує унікальний порт, кілька пристроїв можуть використовувати одну і ту ж IP-адресу без конфліктів.

Зазначимо, що NAT і PAT є важливими технологіями для організації доступу до Інтернету, які забезпечують економію IP-адрес, підвищують безпеку і надають гнучкість для зростання та розвитку локальних мереж. Оскільки діапазон IPv4 обмежений, NAT і PAT дозволяють значно зменшити кількість публічних IP-адрес, необхідних для великої кількості пристроїв у локальних мережах. Крім того, приватні IP-адреси не видимі в Інтернеті, що забезпечує додатковий рівень захисту внутрішньої мережі. Також технології NAT і PAT дозволяють легко масштабувати мережі, додаючи нові пристрої без необхідності отримання нових публічних IP-адрес.

У Mikrotik RouterOS реалізовано два варіанти організації PAT. Це srcnat та masquerade. На відміну від класичного srcnat, при налаштуванні masquerade адміністратор не вказує конкретну зовнішню адресу, натомість маршрутизатор автоматично використовує налаштовані зовнішні адреси. Це вдале рішення для швидкого налаштування невеликої мережі з одним або кількома зовнішніми адресами, але оператори зв’язку з десятками адрес на зовнішніх інтерфейсах використовують більш класичний підхід для балансування підключенні з локальної мережі до глобальної мережі.

RouterOS завдяки опції per-connection-classifier маршрутизатор може рівномірно розподіляти встановленні підключення на підставі адреси джерела між налаштованими зовнішніми адресами для NAT. У магістерській роботі кожному з двох серверів виділено по 62 зовнішні адреси.

У лістингу 1.20 наведено приклад налаштування нату для NAS_1 з обома варіантами: для адрес з пулів клієнтів з несплаченою послугою адреси виду 10.12.0.0/20 (masquerade) та для активних користувачів з пулу 10.11.0.0.20 з розділенням підключень 1:62 на кожну с зовнішніх адрес. Також додатково вказано, що не потрібно використовувати механізм NAT для звернень до ресурсів, що знаходяться у локальній мережі оператора. Адреси підмереж оператора заздалегідь додані в лист *operators_addresses*. Команди для додавання до адрес-листу з переліком підмереж надано у лістингу 1.21

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ext_services src-address=10.12.0.0/20
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-list=!operators_addresses per-
connection-classifier=src-address:62/0 src-address=10.11.0.0/20 to-addresses=100.100.92.130
……
```

```
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-list=!operators_addresses per-connection-classifier=src-address:62/60 src-address=10.11.0.0/20 to-addresses=100.100.92.190
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-list=!operators_addresses per-connection-classifier=src-address:62/61 src-address=10.11.0.0/20 to-addresses=100.100.92.191
```

Лістинг 1.20

```
/ip firewall address-list
add address=100.100.92.0/22 list=operators_addresses
add address=10.10.0.0/20 list=operators_addresses
add address=10.11.0.0/20 list=operators_addresses
add address=10.12.0.0/20 list=operators_addresses
add address=10.12.96.0/20 list=operators_addresses
add address=10.11.96.0/20 list=operators_addresses
add address=10.10.96.0/20 list=operators_addresses
```

Лістинг 1.21

1.4. Шейпінг трафіку абонентів

С точки зору Інтернет як послуги, існує декілька підходів до тарифоутворення. Вартість тарифу в основному залежить від двох факторів: складу пакету послуг та швидкості доступу до глобальної мережі. У магістерській роботі розглянули приклад обмеження трафіку абонентів в залежності від обраного тарифного плану, використовуючи можливості шейперу трафіку операційної системи Mikrotik RouterOS.

Шейпер трафіку на обладнанні компанії Mikrotik — це потужний інструмент для управління мережевим трафіком, який дозволяє контролювати швидкість передачі даних через мережу, забезпечуючи ефективний розподіл пропускної здатності. Ця функція є надзвичайно корисною для адміністраторів мереж, оскільки вона дозволяє уникати перевантажень, підтримувати якість обслуговування (QoS) і забезпечувати стабільну роботу критичних сервісів. Шейпер трафіку є механізмом обмеження швидкості передачі даних для конкретних типів трафіку, мережевих пристроїв або інтерфейсів. Він працює шляхом обмеження пропускної здатності, забезпечуючи дотримання встановлених лімітів для вхідного або вихідного трафіку. На обладнанні Mikrotik цей інструмент дозволяє точно налаштувати передачу даних, зокрема розділити трафік на класи та забезпечити пріоритетність для певних видів трафіку [16].

У системі RouterOS від Mikrotik шейпер трафіку реалізується за допомогою кількох інструментів, серед яких найпоширеніший — це Queue. Він дозволяє задавати обмеження швидкості для окремих користувачів або груп пристроїв, а також налаштовувати пріоритетність обробки трафіку. Шейпер може бути налаштований на рівні інтерфейсу або IP-адрес, що дозволяє обмежувати швидкість як для всієї мережі, так і для окремих підключень. Наприклад, можна встановити максимальну швидкість завантаження і вивантаження для конкретного користувача, що дозволить рівномірно розподілити ресурси мережі.

Шейпер може застосовуватись для обмеження пропускної здатності. Адміністратор може точно встановити, яку максимальну швидкість можуть

використовувати окремі користувачі, пристрої або сегменти мережі. Це допомагає уникнути ситуацій, коли один користувач займає всю доступну пропускну здатність, залишаючи інших без достатнього ресурсу. Також Mikrotik RouterOS дозволяє задавати пріоритети для різних типів трафіку, що дозволяє критичним службам, таким як VoIP або відеоконференції, отримувати більше ресурсів, ніж, наприклад, трафіку для завантаження файлів.

Адміністратор може налаштувати гарантовану мінімальну швидкість для певних користувачів або служб, що забезпечує стабільність їх роботи незалежно від загального навантаження на мережу. Дуже зручними також і вбудовані інструменти для моніторингу використання пропускної здатності і аналізу трафіку в реальному часі. Це дозволяє адміністратору точно бачити, як використовується пропускна здатність і вносити корективи за необхідності.

Існує дві основні технології для шейпінгу трафіку на обладнанні Mikrotik - *Simple Queues* та *Queue Tree*, які дозволяють ефективно контролювати пропускну здатність мережі. Хоча обидва підходи мають схожі цілі, вони відрізняються за принципом роботи та можливостями, що робить їх придатними для різних сценаріїв використання.

Simple Queues — це більш простий і швидкий спосіб обмеження пропускної здатності для окремих пристроїв або IP-адрес. Ця технологія дозволяє створювати обмеження на вхідний і вихідний трафік для конкретних користувачів або сегментів мережі. Simple Queues є ідеальним рішенням для малих і середніх мереж, де необхідно легко керувати пропускною здатністю без складних налаштувань. Основною перевагою Simple Queues є простота налаштування і зручність у використанні. Адміністратору потрібно вказати лише IP-адресу або інтерфейс, швидкість завантаження та вивантаження, що робить цей метод популярним серед користувачів, які шукають просте рішення для обмеження трафіку.

Queue Tree — це більш гнучка та потужна технологія, яка дозволяє налаштовувати пріоритезацію трафіку на більш детальному рівні. Queue Tree використовується для побудови складних черг, що можуть керувати трафіком у кількох напрямах одночасно, даючи можливість задавати пріоритети для різних типів трафіку (наприклад, VoIP, HTTP, FTP) або створювати ієрархічні черги. Головною перевагою Queue Tree є здатність працювати з великою кількістю правил і пріоритетів. Це робить її ідеальною для великих корпоративних мереж, де важливо точно розподілити ресурси між різними типами трафіку і забезпечити стабільну роботу критичних служб.

В залежності від поставлених завдань, кожен з наведених вище методів має свої переваги. Найзначнішою перевагою Simple Queues є більш економне використання обчислювальної потужності ЦП серверу доступу, але Queue Tree дозволяє значно гнучкіше налаштовувати шейпер для досягнення найкращої якості сервісу та використання вхідного каналу оператора.

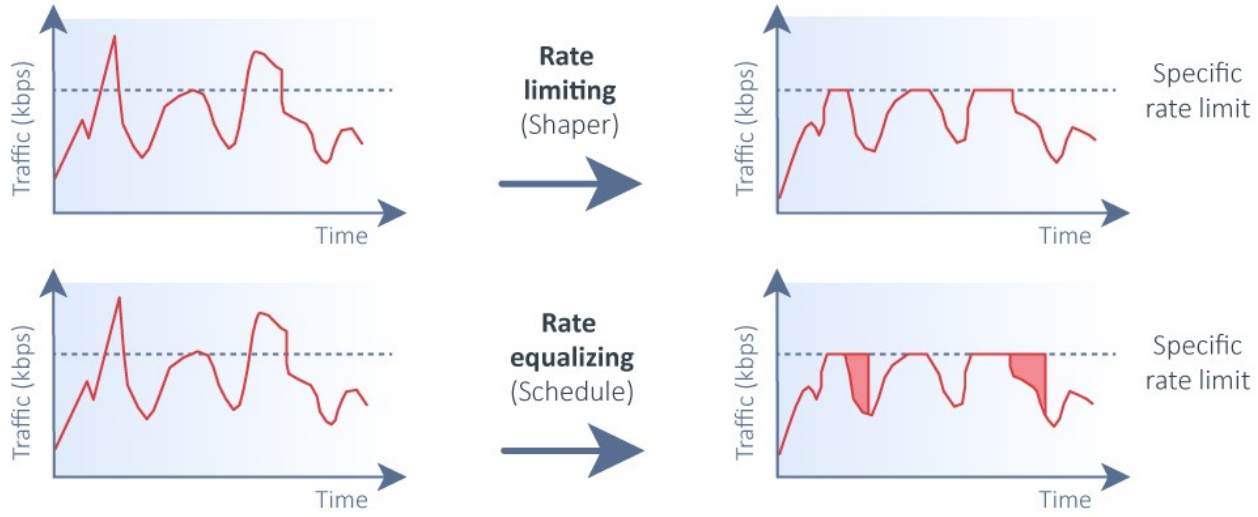

Рисунок 1.22 - порівняння Simple Queues та Queue Tree

У магістерській роботі було використано технологію Queue Tree. Для прикладу було реалізовано 3 сценарії роботи з шейпером:

- абонент має несплачений рахунок за послуги, тому швидкість доступу до глобальної мережі знижено до 1 Мбіт/с;
- абонент отримує послугу на швидкості до 50 мБіт/с, але застосовано технологію Burst Limit, що дозволяє на завданий адміністратором час збільшити абонентові швидкість до 100 Мбіт/с.;
- абонент отримує послугу на швидкості до 200 мБіт/с, але на завданий проміжок часу швидкість збільшено до 500 Мбіт/с. Крім того, правило шейпінгу для максимального тарифу активно тільки у завданих адміністратором рамках прайм-тайму з 19:00 до 23:00 щодня.

Авторизація для доступу до глобальної мережі відбувається за наступним сценарієм:

- абонентський пристрій відправляє запит на з'єднання до PPPoE-серверу, налаштованого на сервері доступу;
- PPPoE-сервер отримує запит з даними авторизації та звертається до серверу авторизації;
- сервер авторизації віддає отримані дані до біллінгу, що надає наявну в нього інформацію згідно із запитом;
- отримавши відповідь від білінгу, сервер авторизації формує відповідь, у якій відхиляє запит або надає дозвіл на авторизацію та передає додаткові атрибути;
- в залежності від відповіді серверу авторизації, сервер доступу відхиляє запит на з'єднання або дозволяє, застосовуючи отримані атрибути.

У магістерській роботі атрибутами, що відповідають за тарифний план є *Mikrotik-Address-List*, що приймає значення: *"50M"*, *"200M"* та *Framed-Pool* зі значенням *"pool_debtor"*. Атрибутів може бути декілька, в залежності від

додаткових послуг. Наприклад, у магістерській роботі реалізовано можливість закріпити за абонентом певну статичну IP-адресу. Для цього використано атрибут *Framed-Ip-Address*. В залежності від адрес-листу або адреси з пулу, що має авторизований абонент, які він отримує виходячи з відповіді біллнгу/обраного тарифного плану, відповідним чином маркуються пакети на завантаження та віддачу трафіку. Налаштування маркування згідно з описаними сценаріями пакетів наведені у лістингу 1.23.

```
/ip firewall mangle
add action=mark-packet chain=forward dst-address-list=50M new-packet-mark=50M_in_mark
passthrough=no
add action=mark-packet chain=forward new-packet-mark=50M_out_mark passthrough=no src-address-
list=50M
add action=mark-packet chain=forward dst-address-list=200M new-packet-mark=200M_in_mark
passthrough=no time=19h-23h,sun,mon,tue,wed,thu,fri,sat
add action=mark-packet chain=forward new-packet-mark=200M_out_mark passthrough=no src-address-
list=200M time=19h-23h,sun,mon,tue,wed,thu,fri,sat
add action=mark-packet chain=forward dst-address-list=pool_debtor new-packet-
mark=pool_debtor_in_mark passthrough=no
add action=mark-packet chain=forward new-packet-mark=pool_debtor_out_mark passthrough=no src-
address-list=pool_debtor
```

Лістинг 1.23

В залежності від маркування пакету, технологія *Queue Tree* застосовує до нього визначений тип черги. В лістингу 1.24 наведені команди створення типів черг, у лістингу 1.25 наведені компади створення черг *Queue Tree*.

```
/queue type
add kind=pcq name=50M_in pcq-burst-rate=100M pcq-burst-threshold=50M pcq-burst-time=10m10s pcq-
classifier=dst-address pcq-rate=52M
add kind=pcq name=50M_out pcq-burst-rate=100M pcq-burst-threshold=50M pcq-burst-time=10m10s pcq-
classifier=src-address pcq-rate=52M
add kind=pcq name=200M_out pcq-burst-rate=500M pcq-burst-threshold=200M pcq-burst-time=10m10s
pcq-classifier=src-address pcq-rate=210M
add kind=pcq name=200M_in pcq-burst-rate=500M pcq-burst-threshold=200M pcq-burst-time=10m10s
pcq-classifier=dst-address pcq-rate=210M
add kind=pcq name=debtor_in pcq-classifier=dst-address pcq-rate=1M
add kind=pcq name=debtor_out pcq-classifier=src-address pcq-rate=1M
```

Лістинг 1.24

```
/queue tree
add name=Common_in parent=global queue=default
add name=Common_out parent=global queue=default
add name=50M_in packet-mark=50M_in_mark parent=Common_in queue=50M_in
add name=50M_out packet-mark=50M_out_mark parent=Common_out queue=50M_out
add name=200M_in packet-mark=200M_in_mark parent=Common_in queue=200M_in
add name=200M_out packet-mark=200M_out_mark parent=Common_out queue=200M_out
add name=debtor_in packet-mark=pool_debtor_in_mark parent=Common_in queue=debtor_in
add name=debtor_out packet-mark=pool_debtor_out_mark parent=Common_out queue=debtor_out
```

Лістинг 1.25

Для коректної роботи шейперу з прив'язкою до часу/дня тижня необхідно заздалегідь налаштувати автоматичну синхронізацію часу з обраним сервером часу. Також за потреби можна дозволити використовувати безпосередньо маршрутизатор у якості власного мережевого серверу часу. Перелік команд для налаштування NTP-клієнту та серверу наведено в лістингу 1.26

```
/system ntp client
set enabled=yes
/system ntp server
set enabled=yes
/system ntp client servers
add address=time.google.com
add address=clock.nyc.he.net
```

Лістинг 1.26

У разі вірного налаштування всіх необхідних параметрів у вікні Winbox, що э спеціальним програмним забезпеченням для налаштування Mikrotik RouterOS, можемо побачити активні та неактивні правила маркування в залежності від налаштувань часу роботи правил.

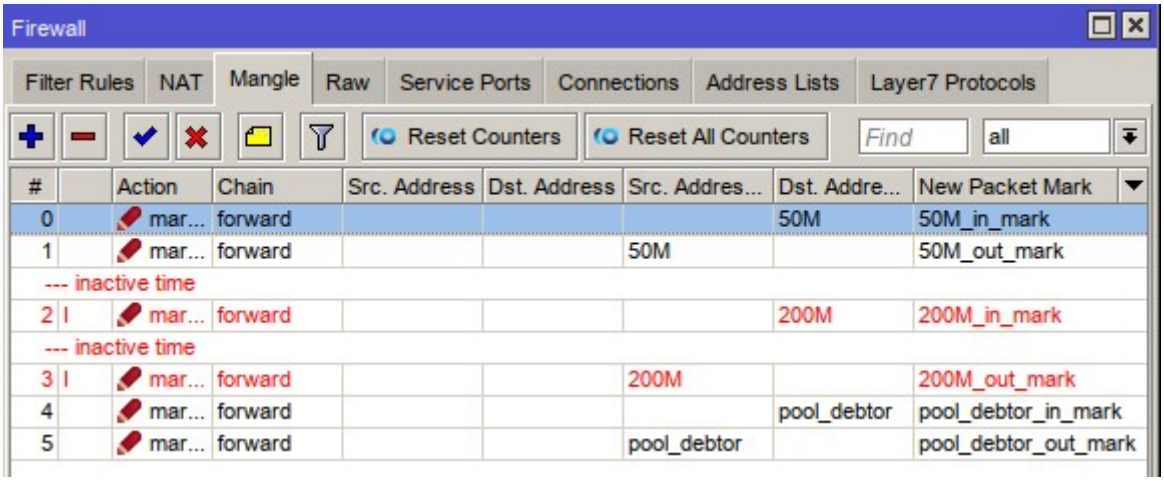

Рисунок 1.27 - перелік активних та неактивних правил маркування трафіку

1.5. Файрвол, як інструмент захисту від зовнішніх атак та елемент забезпечення стабільності роботи попередженні внутрішніх загроз

Питання інформаційної безпеки посягає ледь не найвищу сходинку у рейтингу важливості у сучасних інформаційних систем. Забезпечення інформаційної безпеки є комплексним питання, що має у своєму складі як адміністративну (організаційну) складову, так і технічних компонент. Найважливішою складовою технічного забезпечення безпеки інформаційної системи є налаштування файрволу (брандмауэру). Системи захисту можуть бути реалізовані апаратним або програмним рішенням, також застосовуються комбіновані підходи, особливо у сферах з підвищеними вимогами до захисту інформації, наприклад: фінансові, державні установи, середній та великий

бізнес. За суттю файрвол э ключовим елементом будь-якої інформаційної системи, який забезпечує захист від несанкціонованого доступу, шкідливих атак та витоку даних. Він функціонує як бар'єр між внутрішньою мережею та зовнішніми джерелами, такими як Інтернет, контролюючи потік вхідного і вихідного трафіку на основі встановлених правил. Основна мета брандмауера це забезпечити безпеку мережі та захистити інформацію, яка в ній передається, від зовнішніх загроз. Відомо, що відкритість мережі для зовнішніх підключень створює ризики зловмисних атак, таких як віруси, трояни, DDoS-атаки та спроби вторгнень. Без ефективної системи захисту ці загрози можуть призвести до втрати даних, порушення роботи систем або фінансових втрат.

Firewall (брандмауер) є першим рівнем оборони проти таких загроз, фільтруючи трафік на основі заздалегідь визначених правил. Він дозволяє лише дозволений трафік та блокує будь-який інший, що не відповідає критеріям безпеки. Завдяки цьому брандмауер захищає мережеву інфраструктуру від несанкціонованого доступу, допомагаючи забезпечити конфіденційність, цілісність та доступність даних [17].

Існує кілька типів брандмауерів, які можуть бути застосовані залежно від потреб і складності інформаційної системи:

- пакетні фільтри - один із найпростіших і найпоширеніших видів брандмауера, який працює на основі аналізу заголовків IP-пакетів. Пакетний фільтр дозволяє або блокує пакети на основі IP-адреси відправника, адреси отримувача, порту та протоколу.
- Більш складні брандмауери використовують проксі-сервери для посередництва між внутрішньою та зовнішньою мережею. Вони можуть аналізувати трафік на більш високому рівні, зокрема на рівні додатків, і забезпечувати більш детальне фільтрування.
- Станові брандмауери (stateful firewalls). Цей тип брандмауера відстежує стан кожного з'єднання і дозволяє трафіку проходити лише в тому випадку, якщо він відповідає встановленим правилам для поточних сесій. Це підвищує ефективність фільтрації, оскільки аналізується не лише кожен окремий пакет, але й уся сесія передачі даних.

У Mikrotik RouterOS брандмауер реалізовано через iptables, що дозволяє створювати та керувати правилами для фільтрації трафіку. Брандмауер RouterOS пропонує кілька інструментів і підходів для забезпечення захисту мережі: брандмауер, стейтфул-фільтрація, NAT, захист від DoS-атак.

Брандмауер Mikrotik дозволяє фільтрувати трафік на основі IP-адрес, портів, протоколів та інших параметрів. Адміністратор може створювати правила для входу, виходу та пересилання пакетів, обмежуючи доступ до мережі лише дозволеним користувачам. У RouterOS підтримується стейтфул-фільтрація, що дозволяє контролювати стан з'єднань. Це означає, що система може запам'ятовувати активні сесії та автоматично дозволяти пов'язаний трафік, якщо це дозволено правилами брандмауера. Також Mikrotik підтримує

трансляцію мережевих адрес (NAT), що дозволяє приватним мережам взаємодіяти із зовнішніми мережами, такими як Інтернет, використовуючи одну або кілька публічних IP-адрес. Це не лише допомагає керувати трафіком, але й додає додатковий рівень безпеки, приховуючи внутрішню мережу.

Як і будь-який сучасний корпоративний маршрутизатор, RouterOS має інструменти для виявлення та блокування атак типу відмова в обслуговуванні (DoS). Це робиться за допомогою аналізу аномальних зразків трафіку і автоматичного блокування підозрілих IP-адрес, які намагаються перевантажити мережу.

Зазвичай застосовується декілька підходів до налаштування брандмауера в Mikrotik RouterOS:

- Простий фільтр трафіку. Це базовий спосіб створення правил, що дозволяють або блокують певні пакети на основі IP-адрес, портів або протоколів. Адміністратор може налаштувати правила для вхідного, вихідного або пересилюваного трафіку. Наприклад, можна заблокувати доступ до певних IP-адрес або портів для захисту від небажаних з'єднань.
- Швидкі фільтри та чорні списки. RouterOS дозволяє створювати чорні списки для автоматичного блокування небажаних IP-адрес або пристроїв. Це особливо корисно для запобігання доступу до мережі з боку підозрілих джерел.
- Налаштування захисту для NAT. NAT дозволяє використовувати публічні IP-адреси для внутрішньої мережі, приховуючи її від зовнішнього світу. Важливо правильно налаштувати NAT разом із брандмауером, щоб гарантувати, що лише дозволений трафік може потрапляти у внутрішню мережу.
- Додаткові правила безпеки. Mikrotik також дозволяє налаштовувати додаткові рівні захисту, такі як обмеження за кількістю з'єднань, або використання вбудованого Intrusion Detection System (IDS) для виявлення можливих вторгнень у мережу.

Отже, брандмауери забезпечують фільтрацію трафіку, контролюючи потоки даних до і з мережі. Завдяки функції станної та безстанної фільтрації брандмауери ефективно запобігають несанкціонованому доступу. Налаштування правильних правил фільтрації дозволяє уникати взломів, які можуть призвести до втрати, зміни або знищення конфіденційної інформації. Окрім цього, брандмауери допомагають контролювати вихідний трафік, що забезпечує відповідність безпековим політикам організації.

Файрвол у Mikrotik RouterOS має дуже широкі можливості з фільтрації трафіку, реалізовані за допомогою функцій [18]:

- stateless packet inspection
- stateful packet inspection
- Layer-7 protocol detection
- peer-to-peer protocols filtering
- traffic classification by:

- source MAC address
- IP addresses (network or list) and address types (broadcast, local, multicast, unicast)
- port or port range
- IP protocols
- protocol options (ICMP type and code fields, TCP flags, IP options and MSS)
- interface the packet arrived from or left through
- internal flow and connection marks
- DSCP byte
- packet content
- rate at which packets arrive and sequence numbers
- packet size
- packet arrival time

Завдяки популярності RouterOS серед мережевих адміністраторів, у мережі можна знайти багато прикладів налаштування тих чи інших засобів захисту в залежності від потреб та ресурсних можливостей маршрутизаторів. У магістерській роботі реалізований захист маршрутизаторів з використанням механізмів: tarpit, port or port range, rate at which packets arrive and sequence numbers. Фільтруються ланцюги *input* та *forward*. Попередньо необхідно налаштувати переліки адрес *address-list* та переліки інтерфейсів *interface-list*, що використовуватимуться у фільтрації (лістінг 1.28) - створимо перелік з адресами адміністративної мережі, перелік з всіма адресами мережі, перелік з адресами абонентів зі статичними адресами, перелік адрес з дозволом OSPF; перелік зовнішніх інтерфейсів.

Фільтрація відбувається за наступним планом:

- пропускати встановлені та пов’язані з’єднання (лістінг 1.29), а також пакети OSPF з визначених для них адрес та дозволяти ping;
- використовуючи механізм port or port range, блокувати на 24 години адреси, що намагаються несанкціоновано потрапити ззовні на маршрутизатор, використовуючи порти 22,23,3389 та порти SIP-телефоії (лістінг 1.30);
- застосовуючи механізм *tarpit*, захищати мережу від DDOS атак (лістінг 1.31);
- застосовуючи механізм *rate at which packets arrive and sequence numbers* блокувати адреси, що потенційно атакують зовнішні ресурси з локальної мережі, за винятком зовнішніх “білих” адрес абонентів бізнесу, що потенційно можуть використовувати послугу для налаштування особистих сервісів, що дійсно можуть генерувати велику кількість трафіку. Крім того, завдяки статичній адресі можуть буту однозначно ідентифіковані у разі порушення законодавчих норм (лістінг 1.32).
- блокувати вхідний трафік з будь-яких адрес, крім довіреного переліку (лістінг 1.33);

- у ланцюзі *forward* блокувати нові вхідні з’єднання, що не були ініційовані з локальної мережі, крім абонентів з статичною зовнішньою адресою (лістінг 1.34).
- блокувати трафік, що йде з абонентських мереж до службової мережі (лістінг 1.35).
- у ланцюгах *input* та *forward* блокувати трафік, що RoiterOS вважає некоректним (лістінг 1.36).

Tarpit — це спеціальний механізм обробки трафіку в RouterOS, який використовується для захисту від спроб несанкціонованого доступу або атак, таких як сканування портів чи brute force. Основна ідея tarpit полягає в тому, щоб затримувати встановлення з'єднань із потенційно шкідливими хостами, замість того, щоб просто блокувати їх. Коли використовується механізм tarpit, маршрутизатор Mikrotik приймає запит на встановлення з'єднання, але не дозволяє його завершити. Це призводить до того, що зловмисний хост залишається «застряглим», очікуючи на відповідь, тим самим витрачаючи ресурси та час. Це ефективний спосіб нейтралізації шкідливих атак, оскільки атакувальний пристрій змушений тримати відкритим з'єднання на тривалий час, що уповільнює його подальші спроби атаки або сканування мережі.

Основні особливості механізму tarpit:

- Затримка з'єднання, тобто замість блокування атак, tarpit утримує з'єднання активним, не дозволяючи його завершити, що сповільнює роботу атакувального пристрою;
- захист від сканування портів та brute force-атак дозволяє мінімізувати негативні наслідки від таких атак, утримуючи ресурси зловмисників;
- *tarpit* забезпечує ефективну обробку шкідливого трафіку без значних витрат ресурсів на боці захищеної мережі.

```
/interface list
add name=WAN
/interface list member
add interface=ext_NAT list=WAN
add interface=ext_services list=WAN
/ip firewall address-list
add address=10.9.16.0/24 list=allow_admin
add address=100.100.92.0/27 list=OSPF_in
add address=100.100.92.0/22 list=operators_addresses
add address=10.10.0.0/20 list=operators_addresses
add address=10.11.0.0/20 list=operators_addresses
add address=10.12.0.0/20 list=operators_addresses
add address=10.12.96.0/20 list=operators_addresses
add address=10.11.96.0/20 list=operators_addresses
add address=10.10.96.0/20 list=operators_addresses
add address=10.9.8.0/22 list=allow_admin
add address=10.9.16.0/24 list=allow_admin
add address=100.100.94.0/24 list=stat_ip_clients
add address=100.100.95.0/24 list=stat_ip_clients
```

Лістинг 1.28

```
/ip firewall filter
add action=accept chain=input comment="established, releated" connection-state=established,related
```

```
add action=accept chain=forward connection-state=established,related comment="established, releated"
add action=accept chain=input comment="allow ping" protocol=icmp
add action=accept address-list=OSPF_in chain=input comment=allow_ospf in-interface=ext_services
protocol=ospf
```

Лістинг 1.29

```
/ip firewall filter
add action=add-src-to-address-list address-list=bad_guy address-list-timeout=1d chain=input
comment="ptrap_for_a_bad_guy" disabled=yes in-interface-list=WAN protocol=tcp psd=21,3s,3,1 src-
address-list=!allow_admin
add action=add-src-to-address-list address-list=bad_guy address-list-timeout=1d chain=input
comment="ptrap_for_a_bad_guy" disabled=yes dst-port=22,23,3389 in-interface-list=WAN protocol=tcp
src-address-list=!allow_admin
add action=add-src-to-address-list address-list=bad_guy address-list-timeout=1d chain=input
comment="ptrap_for_a_bad_guy" disabled=yes dst-port=5060,5061,5062,9060,4695 in-interface-list=WAN
protocol=udp src-address-list=!allow_admin
/ip firewall raw
add action=drop chain=prerouting in-interface-list=WAN src-address-list=bad_guy
```

Лістинг 1.30

```
/ip firewall filter
add action=drop chain=forward comment="drop input !allow_admin" dst-address-list=allow_admin src-
address-list=operators_addresses
add action=add-src-to-address-list address-list=blocked-addr address-list-timeout=1d chain=input
comment="DDOS protect" connection-limit=50,32 protocol=tcp
```

Лістинг 1.31

```
/ip firewall filter
add action=drop chain=forward comment="DDOS forward protection" connection-state=new dst-address-
list=ddosed src-address-list=ddoser
add action=jump chain=forward comment="DDOS forward protection" connection-state=new jump-
target=detect-ddos
add action=return chain=detect-ddos comment="DDOS forward allow stat_ip" src-address-
list=stat_ip_clients
add action=return chain=detect-ddos comment="DDOS forward allow operators tooperators" dst-address-
list=operators_addresses src-address-list=operators_addresses
add action=return chain=detect-ddos comment="DDOS forward protection" dst-limit=500,500,src-and-dst-
addresses/10s
add action=return chain=detect-ddos comment="DDOS forward protection" limit=400,5:packet protocol=tcp
tcp-flags=syn
add action=add-dst-to-address-list address-list=ddosed address-list-timeout=1d chain=detect-ddos
comment="DDOS forward protection"
add action=add-src-to-address-list address-list=ddoser address-list-timeout=1d chain=detect-ddos
comment="DDOS forward protection"
```

Лістинг 1.32

```
/ip firewall filter
add action=drop chain=input disabled=yes src-address-list=!allow_admin
```

Лістинг 1.33

```
/ip firewall filter
add action=drop chain=forward connection-nat-state=!dstnat connection-state=new dst-address-
list=stat_ip_clients
```

Лістинг 1.34

```
/ip firewall filter
add action=drop chain=input connection-state=invalid
add action=drop chain=forward connection-state=invalid
```

Лістинг 1.35

```
/ip firewall filter
```

```
add action=drop chain=forward comment=drop_abon_to_stuff_network dst-address-list=allow_admin src-address-list=operators_addresses
```

Лістинг 1.36

1.6. Застосування технології пасивних оптичних мережу у структурі об’єкту дослудження.

Технологія пасивних оптичним мереж в останні роки знайшла застосування не тільки у класичних для неї сегментах ринку послуг у населених пунктах з низькою щільністю розміщення абонентів, таких як сільська місцевість, приватний сектор, а й у багатоповерхових будинках - класична зона впровадження технології FTTB (*fiber to the building*). У магістерській роботі, спираючись на обгрунтування поступового переходу з BTTB до PON (*passive optical networks*) [4], розглянута мережа оператора, у який у якості сегменту “останньої милі” використані два оптичні термінали BDCOM GP3600-16.

BDCOM GP3600-16 — це сучасний оптичний лінійний термінал (OLT), призначений для побудови гнучких і масштабованих мереж FTTH на основі технології GPON (Gigabit Passive Optical Network). Завдяки високій продуктивності та надійності, цей пристрій дозволяє операторам зв'язку забезпечувати високошвидкісні інтернет-послуги з мінімальними витратами.

Рисунок 1.37 - оптичний термінал BDCOM GP3600-16

Основні технічні характеристики BDCOM GP3600-16 [9]:

- кількість портів PON: 16 GPON-портів, що дозволяють підключати до 256 оптичних абонентських терміналів (ONT) на один порт, використовуючи сплітери;
- 4 порти SFP+ для підключення до ядра мережі або аплінку зі швидкістю 10 Гбіт/с, що гарантує високу пропускну здатність;
- максимальна загальна пропускна здатність системи досягає 205 Гбіт/с, що дозволяє обробляти великий обсяг трафіку без затримок;
- великий розмір буферної пам'яті, що забезпечує ефективне управління трафіком та зниження ризику втрат пакетів при високих навантаженнях;
- підтримка мультикаст-трансляцію для IPTV-послуг, що робить його ідеальним для інтернет-провайдерів, які пропонують мультимедійні сервіси;

- інтерфейси віддаленого керування: SNMP, CLI та веб-інтерфейс для зручного адміністрування та моніторингу пристрою.

Налаштування оптичного терміналу проводиться за наступним сценарієм:
- перехід до режиму конфігурування встановлення паролю адміністратору (лістинг 1.38);
- налаштування IP-адреси пристрою та маршруту за замовчуванням (лістинг 1.39);
- конфігурування uplink-портів (лістинг 1.40);
- конфігурування листів доступу з дозволом тільки для адрес службової мережі обладнання та адрес мережі адміністратору (лістинг 1.41);
- налаштування SNMP для потреб моніторингу пристрою (лістинг 1.42);
- налаштування NTP для встановлення загальносистемного часу на пристрої (лістинг 1.43);
- конфігурування профайлів для абонентських терміналів (ONU) (лістинг 1.44));
- конфігурування пікової швидкості у 500 Мбіт/с для абонентських терміналів та встановлення MTU (лістинг 1.45);
- налаштування автоматичної реєстрації ONU (лістинг 1.46)
- додавання профайлів до інтерфейси оптичного терміналу (лістинг 1.47);
- активація технології DHCP Snooping для фільтрації DHCP з довірених джерел (лістинг 1.48);
- активація фільтру та збереження налаштувань (лістинг 1.49).

Нижче наведені лістини налаштувань згідно з переліком для оптичного терміналу, позначеного на рисунку 1.2 як OLT_1. Налаштування другого терміналу є ідентичними, окрім IP-адреси пристрою.

```
enable
config
aaa authentication login default local
aaa authentication enable default none
aaa authorization exec default local
username root password 0 123456
enable password 0 123456
service password-encryption
```

Лістинг 1.38

```
interface vlan 1204
description management
ip address 10.9.8.6 255.255.255.0
no ip directed-broadcast
exit
ip route default 10.9.8.1
```

Лістинг 1.39

```
interface gigaEthernet 0/4
description UPLINK
no shutdown
switchport trunk vlan-allowed 1204,1205,1000-1031
```

```
switchport trunk vlan-untagged none
switchport mode dot1q-tunnel-uplink
dhcp snooping trust
exit
```

Лістинг 1.40

```
ip access-list standard MANAGEMENT
permit 10.9.8.0 255.255.252.0
permit 10.9.16.0 255.255.255.0
exit
ip telnet access-class MANAGEMENT
ip telnet attack-defense
ip http server
```

Лістинг 1.41

```
snmp-server community 0 public RO MANAGEMENT
snmp-server contact Plinskyi_Volodymyr
snmp-server location Kryvyi_Rih
```

Лістинг 1.42

```
time-zone Kyiv 2 0
ntp query-interval 3600
ntp server 10.9.8.1
```

Лістинг 1.43

```
gpon profile onu-flow-mapping vlan1000
 gpon-profile entry 1 uni type eth-uni all
 gpon-profile entry 1 vlan 1000
 gpon-profile entry 1 virtual-port 1

gpon profile onu-vlan vlan1000
 gpon-profile vlan mode trunk
 gpon-profile vlan pvid 1000 0
 gpon-profile vlan trunk vlan-allowed 1000
……
gpon profile onu-flow-mapping vlan1031
 gpon-profile entry 1 uni type eth-uni all
 gpon-profile entry 1 vlan 1031
 gpon-profile entry 1 virtual-port 1

gpon profile onu-vlan vlan1031
 gpon-profile vlan mode trunk
 gpon-profile vlan pvid 1031 0
 gpon-profile vlan trunk vlan-allowed 1031
```

Лістинг 1.44

```
gpon profile onu-rate-limit ratelimit-default id 1
 gpon-profile pir 500000 cir 5000
gpon profile onu-uni MTU
gpon-profile max-frame-size 1550
```

Лістинг 1.45

```
gpon onu-config-template vlan1000
cmd-sequence 001 gpon onu tcont-virtual-port-bind-profile tvbind-default
cmd-sequence 002 gpon onu flow-mapping-profile vlan1000
cmd-sequence 003 gpon onu uni 1 vlan-profile vlan1000
cmd-sequence 004 gpon onu uni 1 uni-profile MTU
……
gpon onu-config-template vlan1031
cmd-sequence 001 gpon onu tcont-virtual-port-bind-profile tvbind-default
cmd-sequence 002 gpon onu flow-mapping-profile vlan1031
```

```
cmd-sequence 003 gpon onu uni 1 vlan-profile vlan1031
cmd-sequence 004 gpon onu uni 1 uni-profile MTU
```

Лістинг 1.46

```
interface GPON0/1
description users
gpon pre-config-template vlan1000 bind-onuid 1-128
gpon bind-onutype onutype-default-hgu precedence 127
gpon bind-onutype onutype-default precedence 128
filter dhcp
switchport trunk vlan-allowed 1000
switchport trunk vlan-untagged none
switchport mode trunk
storm-control broadcast threshold 1000
storm-control multicast threshold 1000
switchport protected 1
no shutdown
……..
interface GPON0/31
description users
gpon pre-config-template vlan1031 bind-onuid 1-128
gpon bind-onutype onutype-default-hgu precedence 127
gpon bind-onutype onutype-default precedence 128
filter dhcp
switchport trunk vlan-allowed 1031
switchport trunk vlan-untagged none
switchport mode trunk
storm-control broadcast threshold 1000
storm-control multicast threshold 1000
switchport protected 1
no shutdown
```

Лістинг 1.47

```
ip dhcp enable
ip dhcp-relay snooping
ip dhcp-relay snooping vlan  1000
……..
ip dhcp-relay snooping vlan  1031
ip dhcp-relay snooping rapid-refresh-bind
show ip dhcp-relay snooping binding all
```

Лістинг 1.48

```
filter enable
write all
```

Лістинг 1.49

У мережах оператору також може застосовуватись механізм ручної реєстрації абонентських терміналів. Це дозволяє запобігти використанню сторонніх неузгоджених з оператором пристроїв, що потенційно можуть вносити несправності у роботу мережі. Також адміністратор може у ручному режимі дозволяти проходження трафіку необхідних вланів на абонентському терміналі у режимі trunk, так само, як вручну змінювати застосований до терміналу профайл у разі необхідності. Окрім можливостей консольного доступу, OLT-термінали мають більш комфортний для оператора веб-інтерфейс. Зручною особливістю технології пасивних оптичних мереж з точки

зору мережевого адміністратора є можливість віддалено перезавантажити абонентський термінал, а також відстежувати рівень сигналу до клієнта, або температуру терміналу (рисунок 1.50).

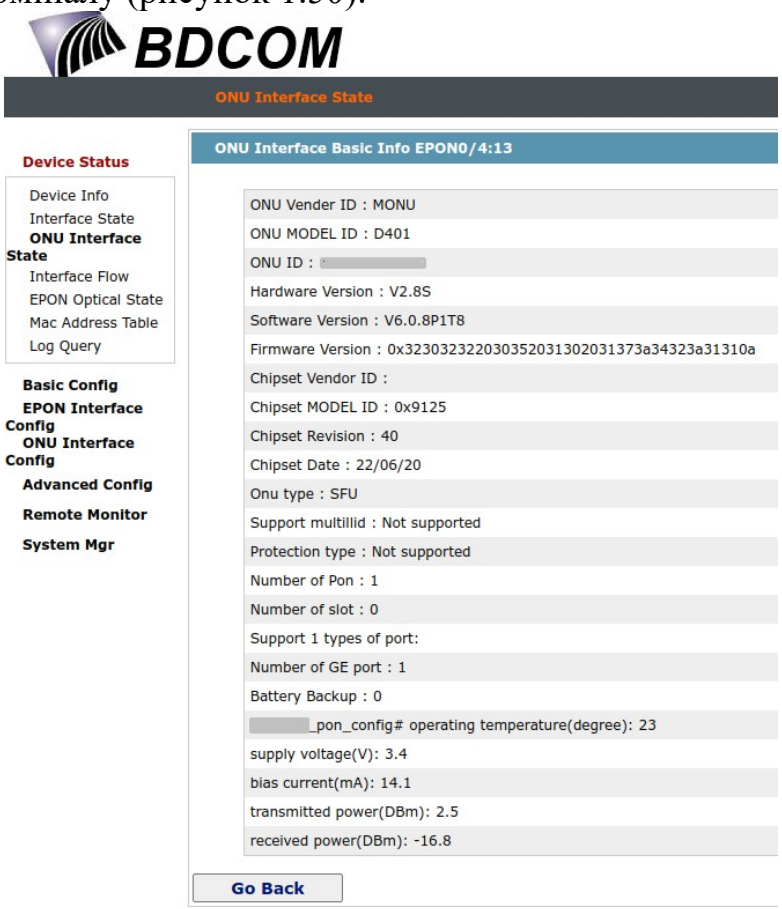

Рисунок 1.50 - сторінка статистики абонентського терміналу на веб-інтерфейсі оптичного терміналу BDCOM

1.7. Визначення працездатності системи з використанням базових утиліт діагностики: ping, traceroute.

Мережева діагностика є невід'ємною частиною підтримки та налагодження комп'ютерних мереж. Для швидкої перевірки з'єднання, виявлення проблем з маршрутизацією або визначення затримки в мережі, найчастіше використовуються утиліти ping і traceroute. Ці інструменти базуються на простих, але ефективних механізмах передачі даних та дозволяють мережевим адміністраторам вчасно виявляти та усувати проблеми в роботі мережі.

У магістерській роботі сценарій користування послугою доступу до мережі Інтернет передбачає отримання комп’ютером абонента локальної IP-адреси за допомогою DHCP без доступу до глобальної мережі. Для доступу до Інтернет необхідне PPPoE з’єднання та авторизація. В залежності від відповіді абонент може отримувати доступ з “сірою” IP-адресою, зі статичною “Білою” IP-адресою, отримати доступ до мережі з параметрами боржника за абонплатою, або не отримати у разі невірних даних авторизації. Для тестування склали чек-

лист (таблиця 1.51), за допомогою якого відслідкували співпадіння очікуваного результату з фактичним.

Таблиця 1.51 - чек-лист перевірки виконання сценарію доступу до глобальної мережі.

№ З/п	Опис перевірки	Очікуваний результат	Відповідність отриманого результату до очікуваного
1	Перевірка працездатності DHCP-серверу оператора	Клієнтський пристрій отримує від обладнання оператора адресу, з визначеного пулу.	Відповідає (рисунок 1.53)
2	Перевірка роботи серверу авторизації оператора шляхом спроби авторизації з не валідними даними	Помилка авторизації з кодом 691.	Відповідає (рисунок 1.54)
3	Перевірка роботи серверу доступу шляхом отримання доступу до послуги з “сірою” IP-адресою	IP-адреса абонента з пулу адрес для NAT Успішне виконання команди ping та трасування до вузла 1.1.1.1	Відповідає (рисунок 1.55)
4	Перевірка роботи серверу доступу шляхом отримання доступу до послуги з “білою” IP-адресою	IP-адреса абонента з пулу статичних адрес. Успішне виконання команди ping та трасування до вузла 1.1.1.1	Відповідає (рисунок 1.56) (рисунок 1.57)
5	Перевірка роботи серверу доступу шляхом отримання доступу до послуги з пулу для боржників	IP-адреса абонента з пулу боржників. Успішне виконання команди ping та трасування до вузла 1.1.1.1	Відповідає (рисунок 1.58)
6	Перевірка роботи налаштування резервування каналів оператором	Трасування йде через вузол резервного оператора 10.80.60.1 замість основного 10.90.80.1	Відповідає (рисунок 1.59)

У магістерській роботі у якості серверу авторизації використаний фірмовий *Mikrotik User Manager*, що дозволяє швидко налаштувати

повноцінний сервер авторизації, завдаючи не тільки облікові дані, ай додаткові параметри до них та переглядати журнал авторизації.

MikroTik User Manager — це потужний пакет для управління користувачами та контролю доступу в мережах, розроблений для роботи на маршрутизаторах MikroTik. Цей інструмент виступає як Radius-сервер, який дозволяє централізовано керувати автентифікацією, авторизацією і обліком користувачів у мережі. User Manager забезпечує гнучкість налаштувань для створення обмежень на доступ до мережі, що робить його ідеальним для інтернет-провайдерів, хостелів, кафе та офісів [19].

Основні функції та можливості:

- Автентифікація через RADIUS: User Manager інтегрується з іншими пристроями MikroTik та сторонніми мережевими системами для автентифікації користувачів через стандартний протокол RADIUS. Це дозволяє створювати централізовані системи контролю доступу для різних точок доступу в межах однієї або кількох мереж.
- Створення користувачів та профілів: За допомогою User Manager адміністратори можуть створювати облікові записи користувачів з індивідуальними налаштуваннями, такими як ліміт швидкості, обсяг трафіку або час підключення. Кожен користувач може мати свій унікальний профіль доступу, що спрощує управління великими базами користувачів.
- Білінг та облік трафіку: Система підтримує моніторинг використання інтернету для кожного користувача, з можливістю виставлення рахунків на основі обсягу спожитого трафіку або часу з'єднання.
- Підтримка купонів та ваучерів: User Manager надає можливість генерації тимчасових облікових записів у вигляді ваучерів для короткочасного доступу до мережі, що корисно для публічних місць, таких як кафе чи готелі.

У лістингу 1.52 вказані налаштування пакету User Manager для діагностики працездатності спроектованої мережі.

```
/user-manager user group
add inner-auths=ttls-pap,ttls-chap,ttls-mschap1,ttls-mschap2,peap-mschap2 name=ordinary_client \
    outer-auths=pap,chap,mschap1,mschap2,eap-tls,eap-ttls,eap-peap,eap-mschap2
/user-manager user
add attributes=Mikrotik-Address-List:50M comment=client1 group=ordinary_client name=user
add attributes=Mikrotik-Address-List:50M,Framed-IP-Address:100.100.94.5 comment=client1 group=\
    ordinary_client name=user_stat
add attributes=Framed-Pool:pool_debtor comment=client1 group=ordinary_client name=debtor
/user-manager
set certificate=*0 enabled=yes require-message-auth=no
/user-manager router
add address=10.9.8.2 name=NAS_1
add address=10.9.8.3 name=NAS_2
```

Лістинг 1.52

Вхідні дані для діагностики:

1) діапазон адрес локальної мережі DHCP: 10.10.0.10-10.10.0.254, або 10.10.96.10-10.10.96.254;
2) невалідні дані авторизації: zorro/password;
3) валідні дані авторизації для користувача з сірою адресою: user/123456, 10.11.0.1-10.11.15.254, або 10.11.96.1-10.11.111.254
4) валідні дані авторизації для користувача з сірою адресою: user_stat/123456, 100.100.94.5;
5) валідні дані авторизації для боржника з сірою адресою: debtor/123456, 10.12.0.1-10.12.15.254 або 10.12.96.1-10.12.111.254;

Для діагностики використали утиліти *ping* та *tracert*. Утиліта *ping* є основним інструментом для перевірки доступності інших пристроїв у мережі. Вона працює за допомогою протоколу ICMP (Internet Control Message Protocol), який надсилає спеціальні запити (Echo Request) до вказаної IP-адреси або доменного імені, а у відповідь отримує Echo Reply. При кожному запуску ping надсилає один або більше ICMP-запитів до цільового пристрою. Якщо пристрій доступний і з'єднання є стабільним, він відповідає зворотним сигналом, що підтверджує його роботу. За допомогою цього інструменту можна перевірити наявність з'єднання з іншим пристроєм. Якщо ви отримуєте відповідь на ICMP-запит, це означає, що мережевий шлях між вашим комп'ютером і цільовим пристроєм працює належним чином, також виміряти затримку між запитом і відповіддю, яка зазвичай виводиться у мілісекундах. Це дозволяє оцінити якість з'єднання.

У разі успішної перевірки з'єднання ми бачимо кілька рядків з повідомленням про затримку, кількість надісланих і отриманих пакетів, а також середній час відгуку. Якщо з'єднання не вдалося, система виведе відповідне повідомлення про помилку.

Команда tracert дозволяє дізнатися маршрут, яким пакети проходять від вашого комп'ютера до цільового пристрою. Це надзвичайно корисний інструмент для діагностики мережевих проблем, оскільки він показує всі проміжні маршрутизатори (або "вузли"), через які проходить трафік. Traceroute працює шляхом поступового збільшення "часу життя" пакета (TTL — Time to Live), що дозволяє виявити кожен проміжний маршрутизатор на шляху до цільового сервера. Коли TTL досягає нуля, маршрутизатор надсилає зворотний сигнал, що дозволяє команді traceroute визначити його IP-адресу і час затримки на кожному етапі. Отримана інформація є корисною для виявлення проблем на маршруті. Якщо один із вузлів на шляху перестає відповідати або значно збільшує час відповіді, це може вказувати на перевантаження або несправність на конкретному маршрутизаторі. За допомогою traceroute можна побачити, які частини маршруту працюють швидко, а де є затримки. Якщо трасування не є успішним, тоді можна виявити точне місце розриву зв'язку. Якщо один із вузлів на шляху не відповідає, це дозволяє локалізувати проблему та вчасно повідомити адміністраторів відповідної мережі.

У результаті виконання *ping* та *tracert* ми бачимо список вузлів з їхніми IP-адресами і часом відгуку на кожному етапі маршруту. Мережа стабільна, але оскільки тестування відбувається у емуляторі, вузли відповідають з більшими затримками, ніж якщо б перевірка відбувалась б у реальних умовах..

Найчастіше ping і traceroute використовуються разом для більш глибокого аналізу мережевих проблем. Спочатку ping дозволяє швидко перевірити доступність пристрою та якість з'єднання, а traceroute допомагає виявити конкретні вузли, які викликають затримки або інші проблеми на шляху до цільового пристрою.

Якщо ми бачимо, що ping до певної адреси не проходить, використання traceroute може показати, де саме втрачаються пакети або виникає розрив зв'язку. Це дозволяє більш точно виявити джерело проблеми та передати цю інформацію адміністраторам мережі або інтернет-провайдеру для подальшого вирішення.

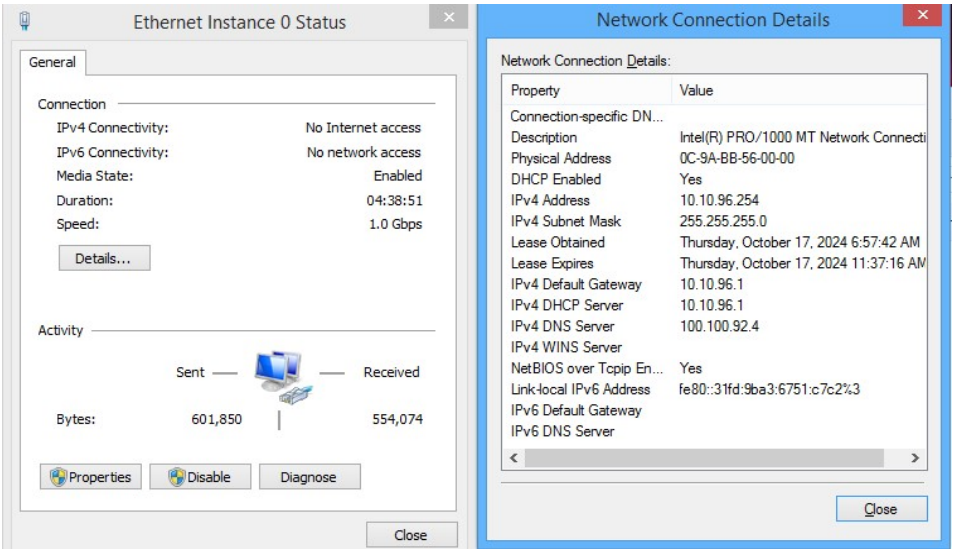

Рисунок 1.53 - результат перевірки №1 таблиці 1.51

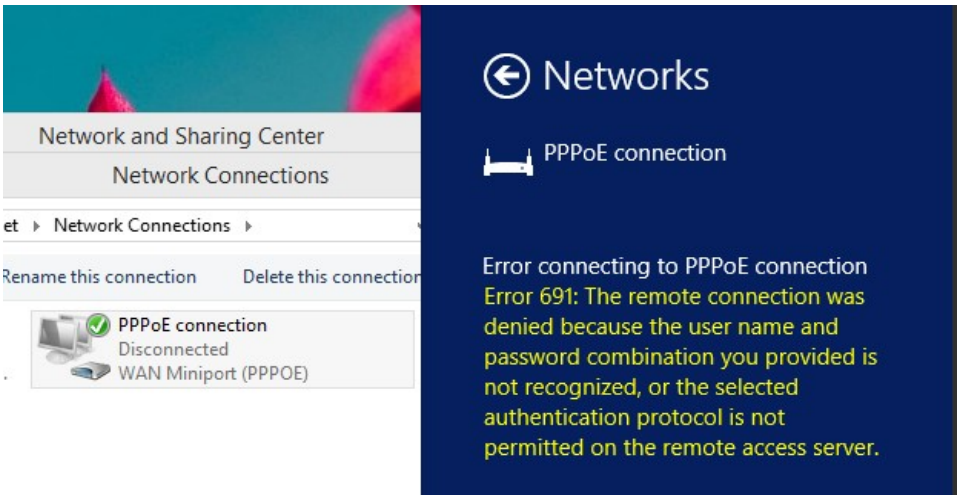

Рисунок 1.54 - результат перевірки №2 таблиці 1.51

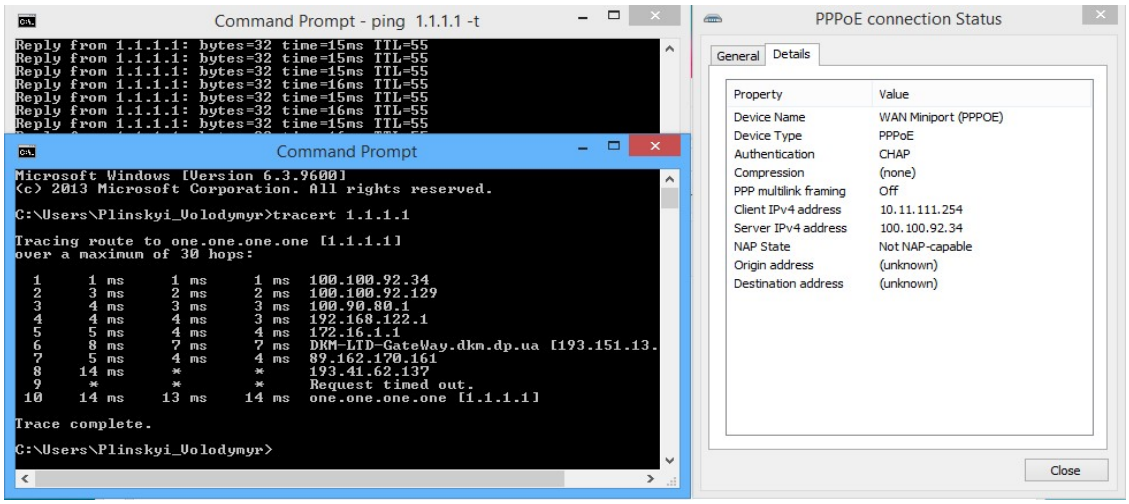

Рисунок 1.55 - результат перевірки №3 таблиці 1.51

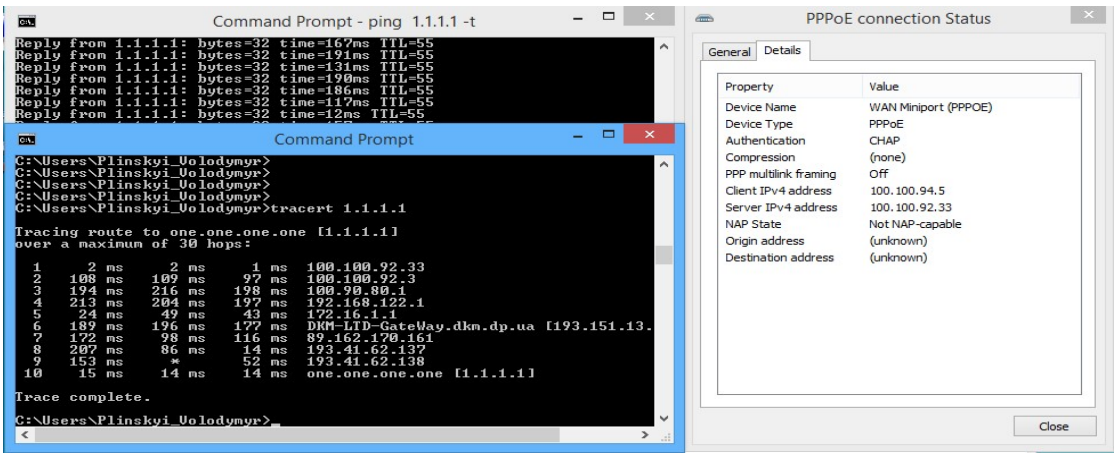

Рисунок 1.56 - результат перевірки №4 таблиці 1.51

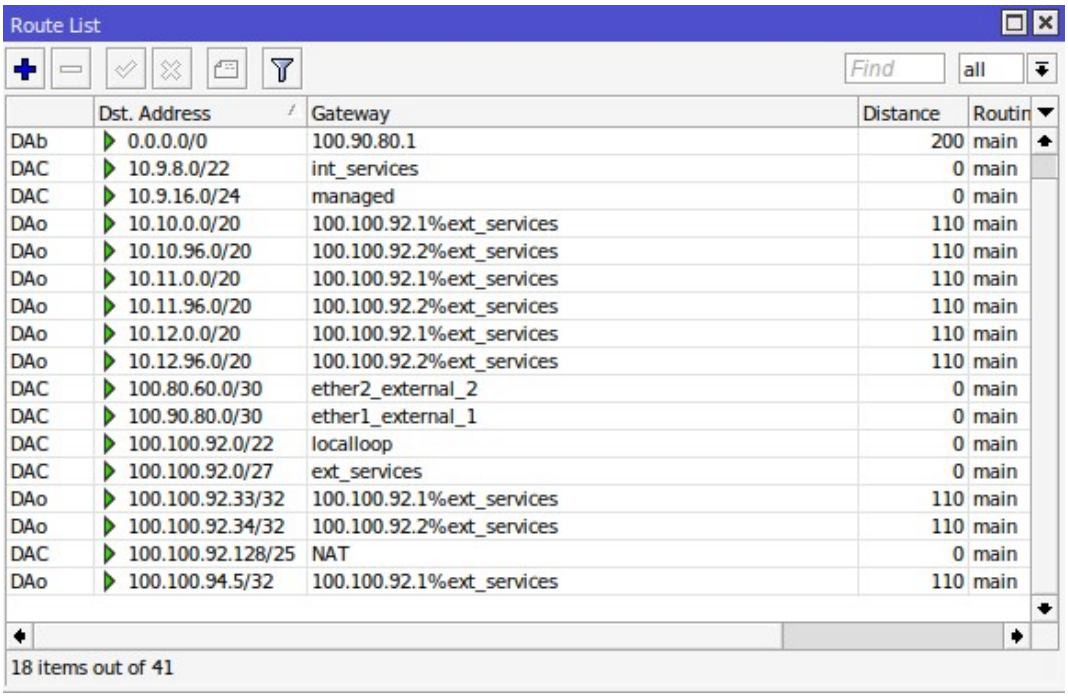

Рисунок 1.57 - результат перевірки №4 таблиці 1.51

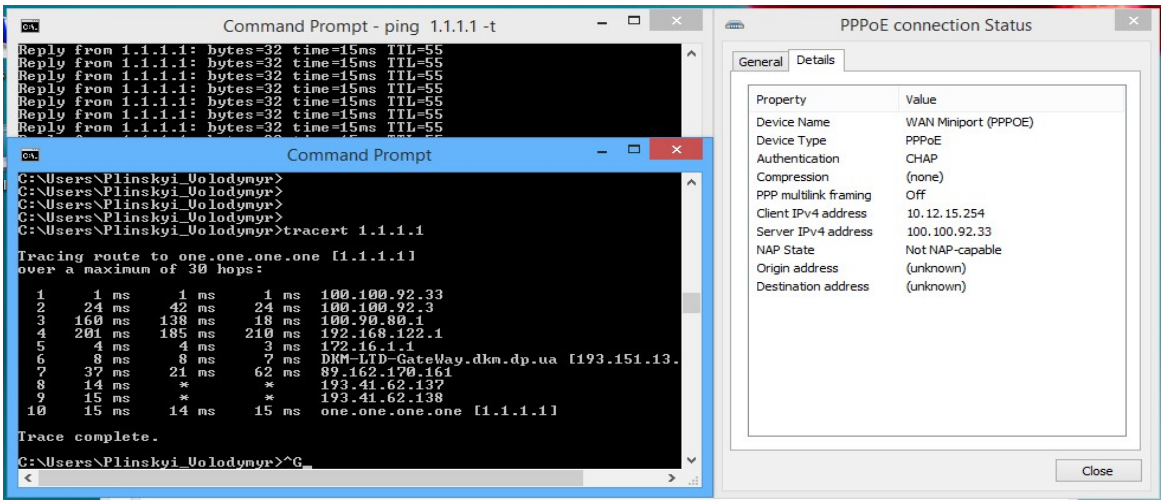

Рисунок 1.58 - результат перевірки №5 таблиці 1.51

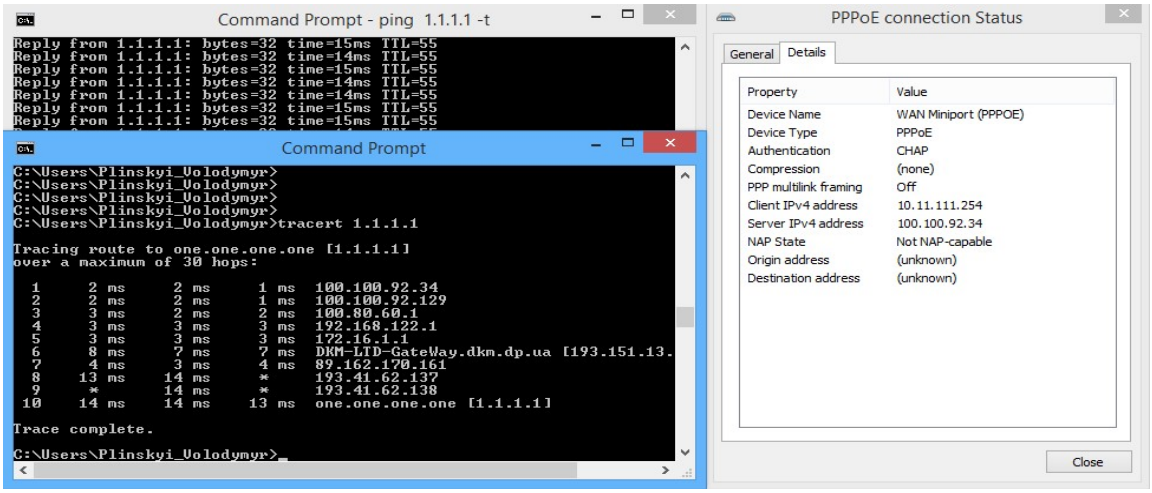

Рисунок 1.59 - результат перевірки №6 таблиці 1.51

Висновки за розділом

У даному розділі були розглянуті вимоги проектованої мережі оператора зв'язку, як об’єкта дослідження; забезпечення її автономності в контексті енергонезалежності, а також виконане налаштування основних елементів інфраструктури, таких як маршрутизатор GATEWAY, сервери доступу NAS_1 і NAS_2, та сервери DHCP. Особливу увагу було приділено налаштуванню динамічної маршрутизації та встановленню з’єднання клієнтського обладнання для забезпечення доступу абонентів мережі до Інтернету. При проектуванні мережі основним завданням було забезпечення стабільного та надійного з'єднання з Інтернетом для клієнтів, а також доступ до локальних ресурсів у межах мережі. Важливим аспектом було передбачення масштабованості мережі для можливості подальшого її розширення без втрати продуктивності.

У сучасних умовах забезпечення енергонезалежності мережі є важливим фактором. Для забезпечення автономної роботи мережі у випадку перебоїв з електропостачанням передбачено використання джерел безперебійного живлення (UPS) та резервних генераторів. Такий підхід дозволяє підтримувати

роботу ключових елементів інфраструктури (маршрутизатор, сервери, комутатори) навіть під час відсутності основного живлення. Це гарантує мінімальні перерви у роботі мережі та забезпечує безперервний доступ користувачів до Інтернету та інших сервісів.

Маршрутизатор GATEWAY був налаштований як основний шлюз мережі, через який проходить весь вхідний та вихідний трафік. Було налаштовано динамічну маршрутизацію OSPF для забезпечення правильного напрямку трафіку до різних сегментів мережі. Крім того, було забезпечено підтримку NAT (*Network Address Translation*) для розподілу зовнішньої IP-адреси між внутрішніми користувачами. Для захисту мережі від зовнішніх загроз також були налаштовані правила фільтрації трафіку за допомогою брандмауера.

Для автоматичного присвоєння IP-адрес клієнтським пристроям були налаштовані два DHCP-сервери, що працюють у режимі відмовостійкості. Це забезпечує плавний перехід на резервний сервер у випадку відмови основного, що дозволяє уникнути проблем з підключенням до мережі та Інтернету. Налаштування DHCP дозволило автоматизувати процес налаштування клієнтських пристроїв, зменшуючи кількість ручних налаштувань. Для надання клієнтам мережі доступу до Інтернету було налаштовано PPPoE-з'єднання (Point-to-Point Protocol over Ethernet). Це забезпечило безпечне з'єднання з Інтернетом через автентифікацію користувачів. У процесі налаштування були перевірені параметри з'єднання, а також забезпечено стабільне підключення для кожного користувача.

2. ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ, ЯК ШЛЯХУ ДОСЯГНЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ ТА АВТОНОМНОСТІ

Одним зі шляхів досягнення енергоефективності у мережі оператора зв'язку є впровадження технологій віртуалізації для більш ефективного використання апаратних ресурсів серверів. Завдяки сучасним технологіям є можливість розмістити декілька серверів на одній фізичній машині, що майже пропорційно зменшить сумарне споживання електроенергії, що не тільки економічно доцільно з огляду на витрати за електроенергію, а й значно підвищить час автономної роботи від існуючих джерел автономного живлення. Найпопулярнішими рішеннями в області віртуалізації є рішення від світових лідерів: VMware, Microsoft Hyper-V, Proxmox, Xen та інщі. Компанії-клієнти можуть обирати, як саме застосовувати технології віртуалізації - розмістити сервер з віртуальними машинами локально на власній технічній площадці, або користуватися хмарними сервісами, наприклад: Amazon Web Services, Microsoft Azure та ін. Кожний з варіантів має свої переваги та недоліки. Наприклад, встановлення локального серверу має переваги безпеки та повного контролю за даними, нульову щомісячну платню, а також незалежність від наявності інтернет з'єднання, натомість серед недоліків: погана масштабованість, відповідальність за енергозабезпечення та резервування даних. Хмарні сервіси є масштабованими, відмовостиікими, мають зовнішню технічну підтримку та початкові низькі витрати на початок роботи, хоча мають серед недоліків щомісячну абонплату та меншу безпеку збереження даних сама через організацію роботи за допомогою глобальної мережі.

У магістерській роботі розглянутий варіант з використанням локального серверу, реалізованого за допомогою рішення Proxmox. Proxmox Virtualization — це потужна платформа з відкритим вихідним кодом для управління віртуалізацією, яка надає широкі можливості для адміністраторів і розробників. Основні переваги використання Proxmox включають [20]:

1) Підтримка KVM і LXC: Proxmox дозволяє запускати повноцінні віртуальні машини (KVM) та легкі контейнери (LXC) на одній платформі. Це надає гнучкість у виборі між продуктивністю та ефективністю ресурсів.
2) Зручний веб-інтерфейс: Інтуїтивно зрозуміла панель управління через браузер дозволяє легко керувати всіма аспектами віртуальних середовищ — від створення машин до моніторингу ресурсів, що робить Proxmox доступним навіть для користувачів з базовими знаннями.
3) Вбудовані інструменти резервного копіювання та відновлення: Proxmox забезпечує автоматизоване резервне копіювання і відновлення

4) віртуальних машин, що підвищує безпеку даних і спрощує відновлення у випадку збоїв.
5) Кластеризація та високодоступні середовища: Proxmox підтримує створення кластерів з кількох вузлів, що дозволяє легко масштабувати ресурси та забезпечувати високу доступність для критично важливих сервісів.

6) Підтримка різних сховищ: Платформа підтримує різні типи сховищ, включаючи локальні диски, мережеві файлові системи (NFS, CIFS), та спеціалізовані системи зберігання (Ceph, ZFS).

2.1. Розгортання платформи корпоративної віртуалізації

Інсталяційних образ Proxmox можна безкоштовно та без реєстрації завантажити з офіційного сайту [20]. Процессор на сервері обов’язково має підтримувати технологію віртуалізації, а об’єм оперативної пам’яті має бути не меньше 2 ГБ; на жорсткому диску середовище займає мінімум 2 ГБ, тому для розрахунку необхідної конфігурації серверу необхідно заздалегить визначитись з рекомендованими вимогами тих віртуальних машин або контейнерів, що будуть розміщені в середовищі. Рекомендований об’єм оперативної пам'яті хост-машини має бути вищим, ніж сума виділених об’ємів ОЗУ контейнерів, аналогічні вимоги для об’єму накопичувачів. Крім того, необхідно передбачити додатковий об’єм для зберігання резервних копій та тимчасового простору для “зліпків” розділів контейнерів.

Інсталяція є досить типовою. Після завантаження з інсталяційного носія адміністратор проходить через кілька етапів попереднього налаштування системи:

1) Вибір інтерфейсу встановлення: графійний або термінальний.
2) Вибір файлової системи та додаткові налаштування граничних значень простору для системи, віртуальних машин, та розділу підкачки (рисунок 2.1).
3) Також адміністратор обирає мову системи, часову зону та розкладку клавіатури
4) Далі задається пароль root користувача та адреса електронної пошти адміністратора.
5) На наступному екрані маємо обрати базовий інтерфейс для доступу до мережі у процесі встановлення та інші мережеві налаштування, що потім можна бути змінити (рисунок 2.2).
6) По закінченню на останньому екрані перед перезавантаженням відображаються загальні відомості щодо вказаних у процесі інсталяції даних. .

Рисунок 2.1 - налаштування розмітки накопичувача

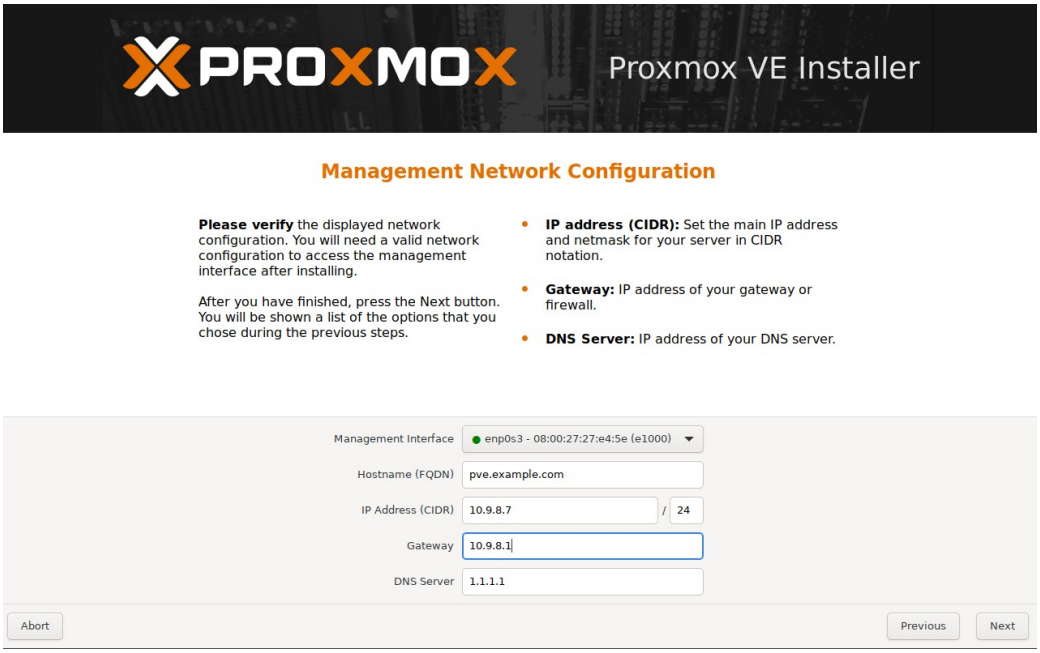

Рисунок 2.2 - налаштування мережевих параметрів

Після перезавантаження сервера на екрані відображається адреса для доступу через WEB-інтерфейс *https:10.9.8.7:8006* та классичне linux-запрошення до локальної авторизації користувача. У магістерській роботі використовували саме веб-інтерфейс для доступу та використання системою віртуалізації.

Веб-інтерфейс Proxmox надає зручні і потужні інструменти для управління віртуальними середовищами. Основні можливості веб-інтерфейсу Proxmox включають:

- Управління віртуальними машинами (KVM) та контейнерами (LXC): Через веб-інтерфейс можна легко створювати, налаштовувати, запускати,

зупиняти та видаляти віртуальні машини та контейнери. Інтуїтивно зрозуміле меню дозволяє здійснювати ці операції з кількома кліками.

- Моніторинг ресурсів: Інтерфейс надає вичерпну інформацію про стан системи в реальному часі, включаючи завантаження процесора, використання оперативної пам'яті, мережевий трафік і використання дискових ресурсів. Це дозволяє ефективно стежити за станом кожної віртуальної машини або контейнера.
- Кластеризація та управління вузлами: Можна створювати кластери з кількох вузлів Proxmox, керувати ними через один веб-інтерфейс, переміщувати віртуальні машини між вузлами та відслідковувати їх стан. Це спрощує управління великими інфраструктурами.
- Резервне копіювання та відновлення: Вбудовані інструменти резервного копіювання дозволяють планувати автоматизоване резервування віртуальних машин або контейнерів, а також виконувати відновлення у випадку збою або аварійної ситуації.
- Підтримка сховищ: Веб-інтерфейс дозволяє налаштовувати різні типи сховищ для віртуальних машин і контейнерів, зокрема локальні диски, мережеві файлові системи (NFS, CIFS), та розподілені системи зберігання (Ceph, ZFS).
- Мережеві налаштування: Proxmox дозволяє легко керувати віртуальними мережевими інтерфейсами, налаштовувати мости, віртуальні локальні мережі (VLAN) та інші параметри для віртуальних машин і контейнерів.
- Міграція віртуальних машин: Через веб-інтерфейс можна виконувати як живу, так і офлайн міграцію віртуальних машин між вузлами кластера без перерв у роботі сервісів.
- Керування правами доступу: Інтерфейс дозволяє створювати користувачів, налаштовувати їхні ролі та права доступу до різних функцій Proxmox. Це дає можливість чітко розподіляти адміністративні права в організації.
- Журнали та сповіщення: Веб-інтерфейс дозволяє переглядати системні журнали і події, а також налаштовувати сповіщення про критичні події, що забезпечує ефективний моніторинг і швидке реагування на потенційні проблеми.

Перш за все налаштували файрвол з дозволом входити (ланцюг input) тількі з підмережі адміністратора 10.9.16.0/24 та правилом відкидати усі інші з’єднання (рисунок 2.3); ввімкнули підтримку вланів на мережевому інтерфейсі (рисунок 2.4) для використання віртуальними машинами різних мереж.

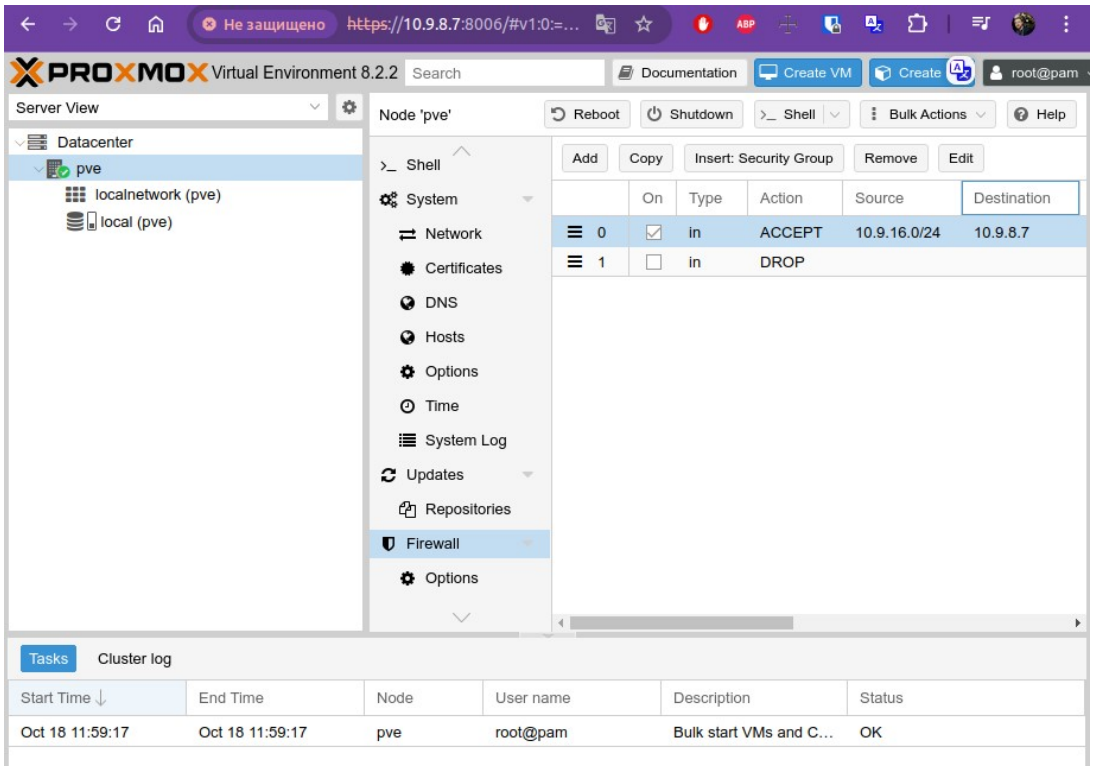

Рисунок 2.3 - додавання базових правил файрволу для захисту від небажаного доступу

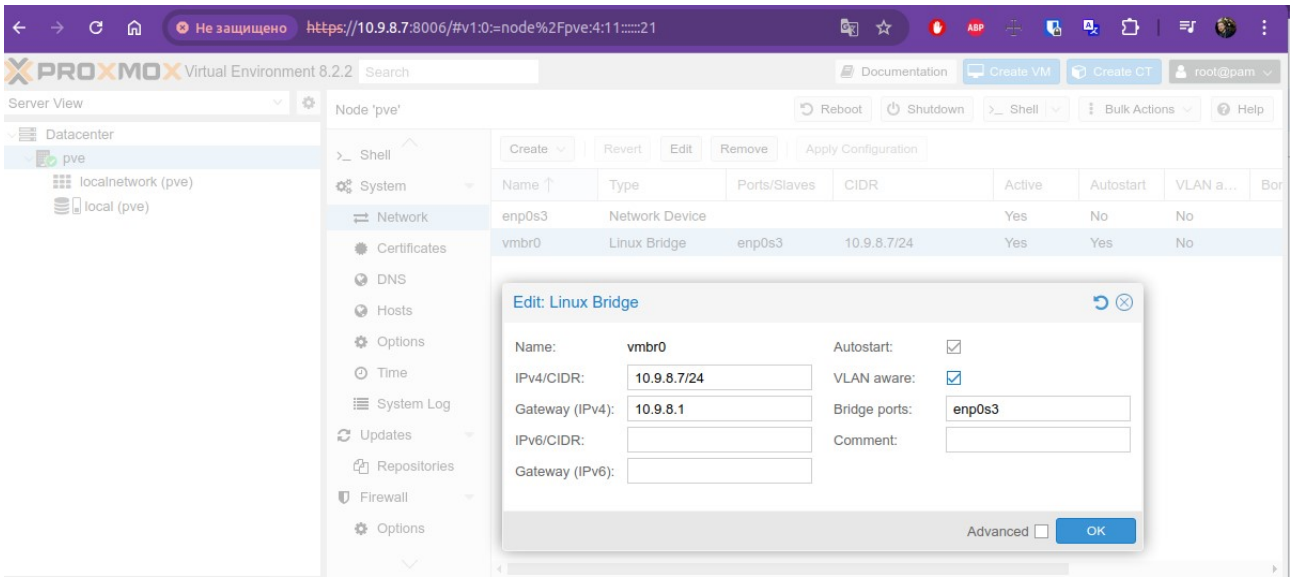

Рисунок 2.4 - активація підтримки віртуальних локальних мереж на мережевому інтерфейсі.

Система віртуалізації Proxmox підтримує два різних типи віртуалізації: KVM та LXC, які мають свої переваги та недоліки. У таблиці 2.5 наведене їх порівняння.

Таблиця 2.5 - порівняння технологій KVM та LXC

Параметри порівняння	Віртуальні машини KVM	Контейнери LXC
Архітектура	KVM є повноцінною віртуалізацією на рівні апаратного забезпечення. Це означає, що кожна віртуальна машина працює як окремий екземпляр операційної системи з власним ядром, драйверами та повним ізолюванням від хост-системи. Кожна машина KVM може запускати різні операційні системи (наприклад, Linux, Windows), оскільки вона працює як повноцінна віртуалізована версія фізичної машини.	Контейнери LXC використовують віртуалізацію на рівні операційної системи. Це означає, що всі контейнери працюють на одному ядрі Linux, і кожен контейнер ізольований, але розділяє ядро хост-системи. Контейнери LXC можуть запускати лише Linux-дистрибутиви, оскільки використовують спільне ядро з хост-системою.
Споживання ресурсів	Віртуальні машини KVM потребують більше ресурсів, оскільки вони включають повноцінну ОС і власне ядро. Це призводить до значного використання оперативної пам'яті та процесорних ресурсів. KVM забезпечує кращу ізоляцію, що корисно для безпеки, але це робить їх менш ефективними з точки зору швидкого запуску та обсягу ресурсів.	Контейнери LXC споживають набагато менше ресурсів, оскільки всі контейнери працюють на спільному ядрі та не потребують запуску повноцінної операційної системи. Завдяки цьому контейнери запускаються швидше, ніж віртуальні машини KVM, і дозволяють на одному сервері розміщувати більше інстансів, що робить їх більш ефективними у використанні ресурсів.

Продовження таблиці 2.5

Ізоляція та безпека	Кожна машина KVM повністю ізольована від інших, оскільки має свою ОС, мережеві інтерфейси та дискові ресурси. Це забезпечує високий рівень безпеки, оскільки будь-яка проблема всередині однієї віртуальної машини не впливатиме на інші або на хост. VM надає кращу ізоляцію в сенсі безпеки.	Контейнери мають нижчий рівень ізоляції порівняно з KVM, оскільки вони розділяють ядро з хостом. Хоча вони ізольовані, проблеми безпеки на рівні ядра можуть впливати на всі контейнери. Проте контейнери забезпечують досить високий рівень ізоляції для багатьох додатків, особливо якщо мова йде про розгортання мікросервісів або однотипних додатків.
Продуктивність	Через повну віртуалізацію KVM може мати певну затримку та більш високе навантаження на хост-систему. Це пов'язано з потребою емуляції апаратних компонентів, таких як CPU, пам'ять та інше. Проте віртуальні машини KVM підходять для завдань, що потребують повної ізоляції та підтримки різних ОС.	Контейнери LXC працюють практично з нативною продуктивністю, оскільки немає необхідності в емуляції апаратного забезпечення. Це забезпечує більшу швидкість виконання програм та менше навантаження на хост-систему. Вони ідеально підходять для розгортання Linux-додатків, які вимагають швидкого виконання і легкої масштабованості.
Використання	Підходить для розгортання різних операційних систем, запуску критично важливих додатків, що потребують повної ізоляції, та для використання різних дистрибутивів. Добре підходить для випадків, коли потрібні повноцінні віртуальні машини з окремими ОС і розширеними налаштуваннями.	Оптимальний варіант для мікросервісів, розподілених додатків та хостингу однотипних Linux-додатків, де потрібна ефективність і швидкість. Ідеально підходить для ситуацій, коли необхідно швидко масштабувати додатки без значного навантаження на хост.

У магістерській роботі розглядається мережа оператора, що має обов'язкові сервери обліку даних клієнтів - білінгова система, сервер домених імен - DNS-сервер та веб-сервер з офіційним сайтом компанії. Виходячи з порівняння таблиці 2.5, обираємо KVM-віртуалізацію для білінгу, та LXC для DNS-серверу та веб-серверу.

2.2. Огляд сервісів у мережі оператора зв'язку

У мережах операторів зв'язку можуть знаходитись багато сервісів, що можуть бути як внутрішніми ресурсами оператору, так і забезпечувати додаткові послуги для абонентів. Сучасні оператори зв'язку використовують білінгові системи, CRM-системи, IP-телефонію, сервери віддаленого доступу, моніторингові системи та інше для покращення якості надання послуг. У якості додаткових послуг зазвичай виступають різноманітні кешуючі сервери для контенту, поштові сервери, хостинг, веб-сервери, та інщі.

У магістерській роботі передбачено розгляд мережі оператора з обов'язковою наявністю сайту компанії, але слід розуміти практичну наявність білінгу, системи авторизації та серверу доменних імен для виконання вимоги регулятору щодо блокування небезпечних ресурсів.

Сучасні білінгові системи є комплексами, що вже включають сервер авторизації, особистий кабінет, інтегровані системи поповнення рахунку абонентів та іноді мають навіть певний функціонал CRM-систем. Як приклад розглянемо досить популярне рішення MikBill від українського розробника.

Mikbill — це сучасна система білінгу та обліку послуг для провайдерів інтернету і операторів зв'язку, що забезпечує автоматизоване управління клієнтськими обліковими записами, тарифікацією та платежами. Вона підтримує роботу з мережевими пристроями, такими як роутери Mikrotik, та дозволяє організовувати повноцінне керування доступом до мережі Інтернет. Mikbill набуває все більшої популярності серед інтернет-провайдерів завдяки своїй багатофункціональності, гнучкості та зручності у використанні.

Mikbill надає повний набір функцій для управління послугами інтернет-провайдера. Основні можливості системи включають [21]:

- Управління клієнтами: Система дозволяє створювати та обробляти клієнтські облікові записи, а також налаштовувати індивідуальні тарифи для кожного користувача. Провайдер може легко відстежувати активних користувачів, призупиняти або відновлювати доступ до послуг в залежності від стану їх рахунку.
- Автоматизація білінгу та тарифікації: Mikbill дозволяє налаштовувати гнучку систему тарифікації. Провайдери можуть створювати різні тарифні плани, які будуть автоматично застосовуватися до клієнтів, в залежності від їх підписки. Це полегшує процес виставлення рахунків і нарахування платежів.
- Платіжні системи: Система підтримує інтеграцію з багатьма популярними платіжними сервісами, такими як LiqPay, Interkassa,

WebMoney та інші. Це дає можливість клієнтам легко оплачувати послуги через різні платіжні системи, що підвищує зручність і швидкість розрахунків.

- Контроль доступу до мережі: Однією з ключових особливостей Mikbill є інтеграція з мережевими пристроями, зокрема роутерами Mikrotik. Це дозволяє провайдерам централізовано керувати доступом до інтернету через протоколи PPPoE, DHCP та Hotspot. Система автоматично регулює доступ користувачів до мережі в залежності від стану їх облікового запису.
- Моніторинг та статистика: Mikbill забезпечує детальну статистику по використанню трафіку кожним клієнтом, що дозволяє провайдерам контролювати обсяг використаних ресурсів і своєчасно реагувати на будь-які аномалії чи зловживання. Це також допомагає у створенні звітів для аналізу та оптимізації роботи мережі.
- Система сповіщень: Система підтримує налаштування автоматичних сповіщень для клієнтів, зокрема через SMS або email. Клієнти можуть отримувати повідомлення про стан їх рахунку, завершення дії підписки або необхідність поповнення балансу.

Однією з найбільших переваг Mikbill є її гнучкість та налаштовуваність. Система може легко адаптуватися до різних умов роботи провайдера, незалежно від масштабів бізнесу. Від малих локальних мереж до великих операторів, Mikbill пропонує зручні інструменти для управління, що підходять для будь-яких сценаріїв. Система автоматично синхронізується з мережевими пристроями, що значно спрощує адміністрування мережі. Провайдери можуть автоматизувати більшість операцій, що стосуються надання інтернет-послуг — від підключення користувачів до контролю за їхнім використанням ресурсів.

Mikbill також добре інтегрується з різними системами платежів і підтримує багато способів оплати. Це дозволяє клієнтам обирати найбільш зручний для них спосіб поповнення рахунку. Автоматизація процесу білінгу та обробки платежів економить час і ресурси провайдера.

Як бачимо, Mikbill є потужним інструментом для автоматизації білінгу, управління клієнтами та контролю доступу до інтернету. Завдяки своїй функціональності та інтеграції з мережевими пристроями, вона дозволяє провайдерам ефективно керувати своїми послугами і забезпечувати якісне обслуговування клієнтів. Незважаючи на деякі технічні вимоги до налаштування, її гнучкість і можливості роблять Mikbill оптимальним вибором для багатьох провайдерів, крім того, додатковою перевагою також є повна сумісність та навіть рекомендації розробника щодо використання системи у віртуальному просторі, зокрема у Proxmox.

Щодо реалізації DNS-серверу э багато рішень, що в залежності від потреб можуть реалізовуватись простіше, або складніше.

DNS-сервер (Domain Name System сервер) необхідний для перетворення доменних імен, зрозумілих людині (наприклад, www.knu.edu.ua), у IP-адреси

(наприклад, 185.104.45.41), які використовуються комп'ютерами для обміну даними в Інтернеті. Оскільки люди зазвичай використовують для доступу до вебсайтів і онлайн-ресурсів доменні імена, а комп'ютери та мережеві пристрої для обміну інформацією між собою потребують IP-адрес, DNS-сервери виконують ключову роль у забезпеченні зручного доступу до Інтернету. Коли користувач вводить доменне ім'я в браузері, DNS-сервер знаходить відповідну IP-адресу для цього домену. Це дозволяє браузеру підключитися до потрібного сервера і завантажити сайт. Також DNS-сервери зберігають кешовані записи, що дозволяє зменшити час, необхідний для пошуку IP-адреси для вже відомих доменів. Це прискорює процес відкриття вебсайтів, які користувачі відвідують часто. Без DNS-серверів користувачам довелося б запам'ятовувати складні числові IP-адреси для кожного вебсайту. DNS робить Інтернет зручнішим, дозволяючи використовувати зрозумілі доменні імена замість числових адрес.

DNS-сервери також можуть підтримувати протоколи захисту, такі як DNSSEC (Domain Name System Security Extensions), що допомагають запобігти атакам, таким як підміна DNS-запитів або перенаправлення на фальшиві вебсайти.

Як приклад більш простого рішення можна навести Pi-Hole. Pi-hole — це популярне рішення для блокування реклами та шкідливих доменів на рівні мережі, що працює як DNS-сервер. Його основна функція полягає у фільтрації небажаного контенту, зокрема реклами, трекерів і шкідливих вебсайтів, ще до того, як ці запити досягнуть користувацьких пристроїв. Крім блокування реклами, Pi-hole також здатний захищати користувачів від небезпечних сайтів і трекерів, завдяки використанню спеціальних списків заблокованих доменів, які постійно оновлюються. Pi-hole має зручний веб-інтерфейс, який дозволяє адмініструвати сервер, контролювати статистику запитів DNS, додавати або видаляти домени зі списків блокування. Його можна встановити на Raspberry Pi, Linux-сервери, Docker або навіть віртуальні машини, що робить його універсальним рішенням для будь-якої домашньої чи офісної мережі.

Завдяки своїй простоті та ефективності, Pi-hole є відмінним інструментом для покращення приватності, продуктивності та безпеки в мережі, блокуючи небажані запити на рівні DNS [22].

Більш професійним є використання bind9 для реалізації повноцінного DNS-серверу.

BIND9 (Berkeley Internet Name Domain) — це один із найпопулярніших і найбільш використовуваних DNS-серверів у світі, розроблений для обслуговування доменних імен. Він широко застосовується як для налаштування локальних мереж, так і для роботи з публічними доменами в Інтернеті. BIND9 підтримує як рекурсивні, так і авторитативні запити DNS. Це означає, що він може використовуватися як сервер для обробки локальних запитів (рекурсивний режим), так і для обслуговування публічних доменів, зберігаючи відповідні записи DNS (авторитативний режим). Однією з важливих функцій BIND9 є підтримка DNSSEC (Domain Name System Security Extensions), яка забезпечує підписування DNS-запитів і підвищує безпеку

мережі, захищаючи від таких атак, як DNS спуфінг. Широкі можливості конфігурації: BIND9 дозволяє створювати детальні конфігурації, налаштовуючи різні зони, політики кешування, переадресацію та інші параметри DNS. Це робить його гнучким рішенням для організацій будь-якого масштабу.

BIND9 активно розвивається і підтримується організацією Internet Systems Consortium (ISC). Він відомий своєю надійністю і стабільністю в роботі навіть в умовах високих навантажень.

Завдяки своїй надійності, підтримці безпеки та широким можливостям конфігурації, BIND9 є стандартом у сфері управління DNS для великих мереж і публічних інфраструктур в Інтернеті [23].

2.3. Налаштування веб-серверу у віртуальному контейнері та створення сайту компанії

Першим етапом на шляху до створення сайту компанії є створення віртуального LXC-середовища. Завдяки зручному веб-інтерфейсу процес створення не займає багато часу. У майстрі створення контейнеру необхідно вказати пароль адміністратора, вказати об’єми оперативної пам’яті, жорсткого диска та кількість ядер, що зможе використовувати контейнер. Також завдається заздалегить завантажений шаблон системи та налаштовуються мережеві інтерфейси. Proxmox підтримує багато різних linux-дистрибутивів та має можливість прямо через власний веб-інтерфейс завантажити з офіційних джерел потрібний шаблон дистрибутиву. Для майбутнього веб-серверу ми обрали Debian 12. Після успішного створення й запуску користувач може через інтерфейс хост-системи підключитися до консолі контейнеру та почати робити попередні налаштування доступу, після чого підключатися безпосередньо до контейнеру.

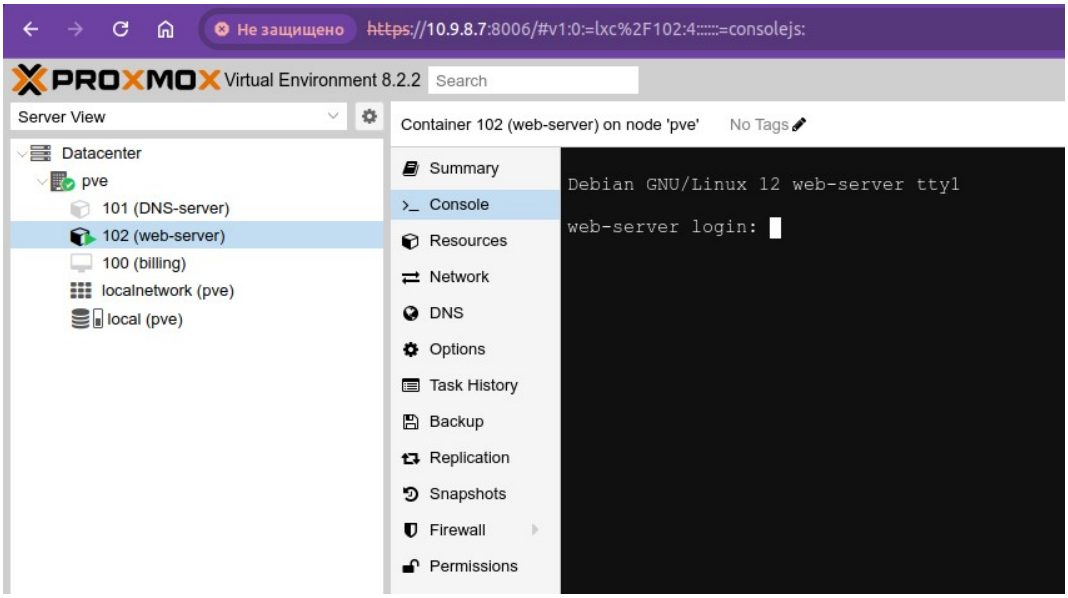

Рисунок 2.6 - інтерфейс підключення до консолі контейнеру

На даному етапі необхідно виконати стандартні дії з оновлення пакетів та встановлення додаткових системних утиліт для більш зручного моніторингу та адміністрування; встановити правильний час у системі та додати українську локаль для підтримки кирилиці у консолі.. Також відключаємо передвстановлений файрвол *nftables* та встановлюємо класичний *iptables*.

```
apt update && apt upgrade -y
timedatectl set-timezone Europe/Kiev
dpkg-reconfigure locales
systemctl stop nftables
systemctl disable nftables
apt install mc htop iotop wget sudo iptables -y
```

Лістинг 2.7

Для налаштування файрволу створили файл з таблицею правил та додали до неї правила, що дозволяють клієнтам з адміністративної підмережі підключатись до сервера без обмежень, та дозволити звернення до веб-серверу за портами 443 та 80. Усім іншим доступ заборонено. Виправлений перелік правил активували та встановили пакет для збереження налаштувань.

```
touch iptables
cat <<EOF >> iptables
*filter
:INPUT ACCEPT [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -s 127.0.0.0/8 -j ACCEPT
-A INPUT -s 10.8.16.0/24 -j ACCEPT
-A INPUT -p tcp --dport 80 -j ACCEPT
-A INPUT -p tcp --dport 443 -j ACCEPT
-A INPUT -j DROP
COMMIT
EOF
iptables-restore < iptables
apt install iptables-persistent
```

Лістинг 2.8

Після налаштування безпеки необхідно відкрити доступ до контейнеру за протоколом ssh. Для цього додали у файл налаштувань ssh строку, що дозволяє доступ з правами адміністратора та перезапустили службу.

```
echo -e "PermitRootLogin yes" >> /etc/ssh/sshd_config
systemctl restart sshd
```

Лістинг 2.9

Для реалізації безпосередньо веб-серверу обрали LiteSpeed Web Server, що є сучасним рішенням та має багато переваг, порівняно з класичним Apache.

LiteSpeed — це високопродуктивний веб-сервер, який є альтернативою більш поширеним рішенням, таким як Apache та Nginx. Він розроблений для забезпечення швидкої обробки HTTP-запитів, ефективного управління ресурсами та оптимізації продуктивності веб-додатків [24].

Основними моментами, що відображають різницю в швидкості роботи між LiteSpeed та Apache є: обробкка запитів, продуктивність при файлів, використання ресурсів та захист від DDoS-атак. LiteSpeed використовує асинхронну архітектуру обробки запитів, що дозволяє обробляти більшу кількість одночасних з'єднань без значного збільшення використання ресурсів. У той же час Apache використовує багатопоточну модель або модель з багатьма процесами (в залежності від обраного модуля MPM), що може призвести до швидкого споживання оперативної пам'яті при збільшенні кількості запитів, особливо у високонавантажених сценаріях. LiteSpeed значно швидший в обробці статичного контенту, такого як зображення, файли CSS та JavaScript. Він здатний працювати з великими обсягами таких запитів з меншим навантаженням на сервер. Apache поступається LiteSpeed у швидкості обробки статичних файлів через свою архітектуру і використання додаткових ресурсів на кожне з'єднання.

LiteSpeed має вбудований LSCache, який суттєво прискорює роботу динамічних сайтів на CMS-системах, таких як WordPress, Joomla, Magento тощо. Завдяки кешуванню динамічного контенту, LiteSpeed дозволяє швидко віддавати сторінки без потреби в кожному запиті генерувати їх заново, а Apache не має вбудованої кешуючої системи для динамічного контенту, хоча для цього можна використовувати додаткові модулі, такі як Varnish або сторонні кешуючі рішення, що часто ускладнює конфігурацію.

Також LiteSpeed краще оптимізований для використання ресурсів, особливо під час роботи з великим обсягом одночасних з'єднань. Він використовує менше оперативної пам'яті та процесорного часу, особливо у випадках високого навантаження. Для порівняння Apache при великій кількості одночасних запитів може споживати значно більше ресурсів, що може призводити до перевантаження сервера.

LiteSpeed має вбудовані функції захисту від атак типу DDoS і може швидше реагувати на такі загрози, знижуючи навантаження на сервер.

Додатковим плюсом для адміністратора є можливість розгорнути середовище, що включає веб-сервер та базу даних однією командою. У магістерській роботі запит на завантаження та приклад конфігурації виглядає таким чином:

```
wget https://raw.githubusercontent.com/litespeedtech/ols1clk/master/ols1clk.sh && bash ols1clk.sh --dbrootpassword 123456 --adminuser admin --adminpassword 123456 --prefix diplomwork --dbname diplomwork_db --dbuser diplomwork_db_user --dbpassword 123456 --email vp7587@gmail.com --wordpressplus diplomwork.example.com --wpuser admin --wppassword 123456
```

Лістинг 2.10

Переконатись, що встановлення пройшло успішно можна зайшовши на до адміністративного інтерфейсу за адресою сервера та портом 7080.

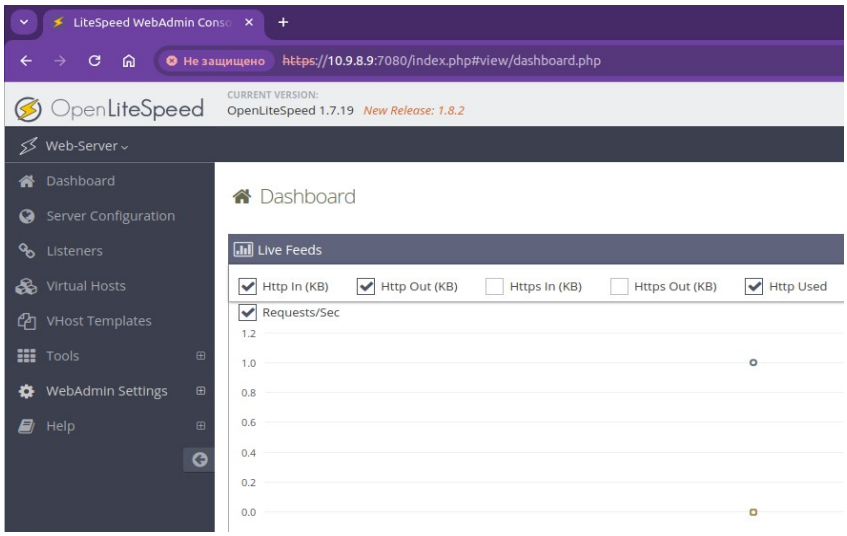

Рисунок 2.11 - адміністративна консоль LiteSpeed

Найзручнішим для швидкого запуску є використання платформи для створення сайтів. Прикладом є WordPress. WordPress — це популярна система управління контентом (CMS), яка використовується для створення і управління веб сайтами. Вона має відкритий вихідний код і базується на мові програмування PHP у поєднанні з базою даних MySQL або MariaDB. Wordpress є вже перевстановленим, тому у випадку, коли інсталяція пройшла без помилок, ми можемо потрапити на сторінку сайту за вказаним при інсталяції веб-серверу доменим ім’ям або IP-адресою та почати наповнювати сайт.

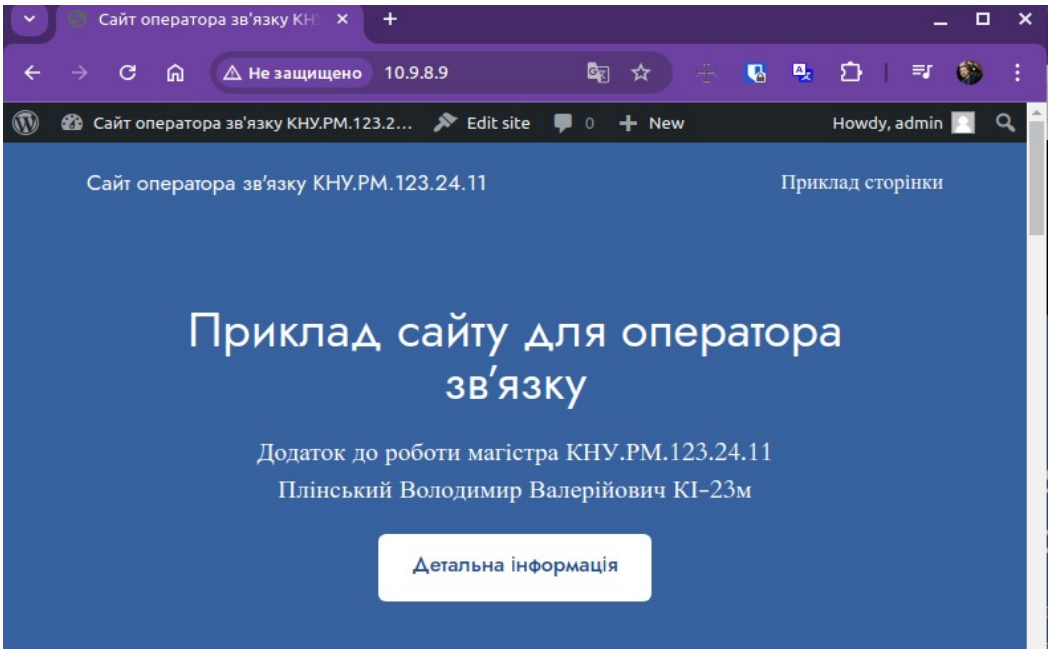

Рисунок 2.12 - приклад оформлення сайту на WordPress

Висновки за розділом

У другому розділі розглянули технологію віртуалізації, як шлях до вровадження енергоефективного режиму роботи, що також може бути одним з кроків до оптимізації енергоефективності мережі оператора. Було розглянуто практичні приклади віртуалізації на базі платформи Proxmox, зокрема створення KVM віртуальних машин та LXC контейнерів. Описали переваги та можливості обох типів віртуалізації.

Однією з ключових відмінностей між KVM та LXC контейнерами є їхня архітектура. Віртуальні машини на базі KVM забезпечують повну ізоляцію на рівні апаратного забезпечення, дозволяючи запускати різні операційні системи з незалежним ядром, що особливо корисно для ситуацій, де потрібна висока безпека та гнучкість. Це робить KVM ідеальним для розгортання критично важливих серверів, які мають виконувати завдання з високими вимогами до ресурсів і безпеки. LXC контейнери базуються на віртуалізації на рівні операційної системи, де всі контейнери розділяють ядро хост-системи. Це забезпечує легшу та швидшу роботу контейнерів, а також дозволяє ефективніше використовувати ресурси сервера. В рамках роботи був створений LXC контейнер, в якому було розгорнуто веб-сервер, що показало високий рівень продуктивності при мінімальних затратах на ресурси.

Як приклад застосування LXC контейнерів було розгорнуто веб-сервер у межах одного з контейнерів. Це продемонструвало простоту та швидкість налаштування середовища для розміщення веб-додатків. Використання LXC дозволило швидко встановити веб-сервер і налаштувати всі необхідні сервіси без надмірного навантаження на серверну інфраструктуру. Тестування показало, що такий підхід є ефективним рішенням для невеликих проектів або серверів, які не потребують повної ізоляції, але потребують високої продуктивності.

Таким чином продемонстрували, що віртуалізація надає ефективні рішення для різних типів задач, а її можливості роблять її універсальним інструментом для створення сучасних інфраструктур.

3. ДОСЛІДЖЕННЯ ФАКТОРУ НЕСТАБІЛЬНОСТІ ЕНЕРГОЗАБЕЗПЕЧЕННЯ ТА ПОШУК ОПТИМАЛЬНОЇ ТЕХНОЛОГІЇ ДЛЯ ЗМЕНШЕННЯ ВПЛИВУ НА ЯКІСТЬ НАДАННЯ ПОСЛУГИ ФІКСОВАНОГО ІНТЕРНЕТ

У дослідженні ми поставили собі на меті визначення найзначущого фактору у переході мережі до несправного стану, також необхідно зробити вибір оптимальної технології для побудови комп'ютерної мережі в одному з районів міста. Отже, при виборі оптимальної технології для побудови комп'ютерної мережі в районі міста, необхідно враховувати енергонезалежність, швидкість доступу, вартість розгортання і експлуатаційні характеристики. Кожна з розглянутих технологій має свої переваги та недоліки, і важливо зважити їх при прийнятті рішення.

Виходячи з досвіду, у більшості випадків більшість районів з багатоквартирними будинками складається з приблизно 20 будівель, а великі райони з точку зору топології та фізичного прокладання ліній зв’язку все одно зручно групувати приблизно по 15-20 будинків. Спираючись на це, порівнюємо технології широкосмугового доступу до мережі виходячи з цієї кількості будівель.

3.1. Аналіз потенційних технічних рішень для визначення оптимальної технології згідно актуальними потребами галузі

У третьому розділі порівняняли наступні технології: FTTB, xPON(GPON), Cable (DOCSIS), ADSL.

Опис порівнюваних технологій.

FTTB - FTTB означає "Fiber to the Building" або "Волокно до будівлі". Технологія FTTB передбачає прокладання оптичного волокна до будівлі (наприклад, житлового будинку або офісного приміщення), де встановлюється спеціальний обладнаний пристрій-конвертор, що перетворює оптичний сигнал у електричній. Після перетворення електричний сигнал передається на активні мережеві пристрої (комутатори), які забезпечують розподіл інтернет-сигналу між користувачами.

В Україні технологія FTTB стала застосовуватися масово з появою та розвитком мереж оптоволоконного зв'язку у великих містах протягом останніх 25 років.

Основні переваги технології FTTB:

- висока швидкість передачі даних;

- невелика вразливість до електромагнітних перешкод та втрат сигналу;
- невибагливість перевитої крученої пари до умов монтажу;
- відсутність необхідності встановлення додаткового обладнання для отримання послуг;
- відносно мала цінність кабелю для вандалів.

Однак, серед недоліків можна виділити:

- необхідність живлення обладнання на кожному будинку;
- витрати на облаштування кросового шафи на кожному будинку.

Середня швидкість доступу до мережі за технологією FTTB в Україні зазвичай залежить від обладнання інтернет-оператор та кількості підключених користувачів. Вона може сягати від 100 Мбіт/с до 1 Гбіт/с.

Прикладом активного обладнання, що широко використовується операторами зв’язку в Україні є комутатор D-Link DGS-1210-28.

Рисунок 3.1 - комутатор D-Link DGS-1210-28

Основні характеристики [25], що можуть бути розглянуті у досліджуванні:

- кількість портів: 24 порти 1000Мбіт/с, 4 SFP порти 1000Мбіт/с;
- максимальна споживана потужність: 23Вт;
- середня ціна: 7 500 грн.

xPON означає "Passive Optical Network", де "x" може бути GEPON (EPON), або GPON, залежно від використаного обладнання. Технологія xPON використовує оптичне волокно для передачі сигналу до кінцевого користувача через пасивну оптичну мережу. Сигнал з оптичного мультиплексора розділяється на кілька окремих потоків за допомогою пасивних розгалужувачів і подається до кінцевих користувачів. У кінцівки мережі розташовані оптичні термінали, які перетворюють оптичний сигнал у сигнал, придатний для використання кінцевими пристроями. В Україні технологія xPON почала активно застосовуватися для підключення до інтернет здебільшого користувачів приватного сектора з 2012 році, але з початком повномасштабного вторгнення та обстрілами російською федерацією цивільних енергетичних об'єктів України з 2022 року ця технологія почала активно впроваджуватись

для надання послуг Інтернет у багатоквартирних будинках через перевагу енергоефективності.

Основні переваги технології xPON включають:
- висока пропускна здатність і швидкість передачі даних через оптичне волокно;
- ефективне використання оптичного волокна за рахунок пасивних елементів мережі;
- несприйнятливість до електромагнітних перешкод;
- відсутність необхідності встановлення активного обладнання на кожному будинку;
- нульова цінність елементів мережевої інфраструктури для третіх осіб.

Серед недоліків можна відзначити:
- високі вимоги до монтажу абонентської лінії зв'язку;
- необхідність встановлення додаткового обладнання для отримання послуги.

Середня швидкість доступу до мережі за технологією xPON в Україні може коливатися від 100 Мбіт/с до 1 Гбіт/с в залежності від типу використовуваної технології, але потенційно у майбутньому швидкість може бути збільшена до 2,5 Гбіт/с.

Прикладом активного обладнання, що широко використовується операторами зв'язку в Україні є оптичний термінал C-DATA fd1608.

Рисунок 3.2 - оптичний термі C-DATA fd1608

Основні характеристики [26], що можуть буди розглянуті у досліджені:
- максимальна кількість підтримуваних абонентських пристроїв: 1024;
- максимальна споживана потужність: 50Вт;
- середня вартість: 45 000 грн.

DOCSIS означає "Data Over Cable Service Interface Specification".

DOCSIS - це стандарт передачі даних через кабельну мережу. Ця технологія дозволяє використовувати існуючу інфраструктуру кабельного телебачення для передачі даних в обидві сторони - від провайдера до користувача (downstream) і від користувача до провайдера (upstream).

В Україні технологія DOCSIS стала застосовуватися в основному з початку 2000-х років, коли кабельні оператори почали надавати послуги високошвидкісного інтернету на базі своїх мереж, але згодом більшість операторів зв'язку в Україні для надання послуг Інтернет перейшли на FTTB через суттєві недоліки технології DOCSIS.

Основні переваги технології DOCSIS включають:

- використання існуючої інфраструктури кабельного телебачення, що дозволяє швидко впроваджувати послуги високошвидкісного інтернету;
- доступність послуг для користувачів у великих містах і місцевостях, де є кабельні мережі.

Серед недоліків можна відзначити:

- обмежена пропускна здатність мережі в порівнянні з іншими технологіями, такими як FTTB, xPON;
- залежність від стану і якості кабельної інфраструктури;
- відносно високі витрати на підтримку та модернізацію мережі;
- необхідність встановлення додаткового обладнання для отримання послуги;
- висока цінність елементів мережевої інфраструктури для злодіїв.

Середня швидкість доступу до мережі за технологією DOCSIS в Україні зазвичай залежить від стандарту, що використовує оператор, але в основному це десятки мегібіт на секунду.

Прикладом активного обладнання, що використовується операторами зв’язку в Україні є компактна головна станція кабельних модемів Teleste DAH100.

Рисунок 3.3 - головна станція кабельних модемів Teleste DAH100

Основні характеристики [27], що можуть буди розглянуті у досліджені:

- максимальна кількість підтримуваних абонентських пристроїв: 500;
- максимальна споживана потужність: 60Вт;
- середня вартість: 170 000 грн.

ADSL означає "Asymmetric Digital Subscriber Line".

ADSL - це технологія передачі даних по телефонній лінії, яка використовується для надання доступу до Інтернету. Вона передає дані з використанням високочастотних сигналів по телефонній лінії, в той час як голосовий сигнал передається по низькочастотній смузі. Однією з головних особливостей ADSL є те, що швидкість завантаження (з Інтернету до користувача) зазвичай вища, ніж швидкість відвантаження (від користувача до Інтернету).

Початок застосування технології ADSL в Україні датується приблизно середини 2000-х років, коли кілька операторів почали надавати послуги доступу до Інтернету через телефонні лінії.

Основні переваги технології ADSL:

- відносно низькі витрати на впровадження, оскільки вона використовує існуючу інфраструктуру телефонної мережі;
- висока доступність для користувачів, оскільки телефонні лінії мають практично всюди;
- висока енергонезалежність через відсутність розгалуженого активного обладнання.

Серед недоліків можна виділити:

- обмежена швидкість відвантаження (з користувача до Інтернету);
- залежність від відстані до центрального офісу зв'язку, яка впливає на якість і швидкість з'єднання;
- обмежені можливості передачі великого обсягу даних, порівняно з іншими технологіями, такими як оптоволокно або кабельний Інтернет;
- необхідність встановлення додаткового обладнання для отримання послуги;
- висока цінність елементів мережевої інфраструктури для злодіїв.

Середня швидкість доступу до мережі за технологією ADSL в Україні може коливатися від 1 Мбіт/с до 24 Мбіт/с в залежності від вибраного тарифного плану та відстані до центрального офісу зв'язку.

Прикладом активного обладнання, що може використовуватися операторами зв’язку є модульне шассі IP DSLAM D-Link DAS-4672.

Рисунок 3.4 - модульне шассі IP DSLAM D-Link DAS-4672

Основні характеристики [28], що можуть бути розглянуті у дослідженні:

- максимальна кількість підтримуваних абонентських пристроїв: 672;
- максимальна споживана потужність: 49Вт;
- середня вартість: 52 000 грн. (без урахування модулів).

3.2. Обґрунтування значущості фактору енергоефективності / енергонезалежності через дослідження впливу знеструмлення обладнання оператора зв'язку на кількість звернень до служби технічної підтримки

Для досягнення мети перевірки значущості фактору відсутності електропостачання на доступність послуги використовувався метод кореляційно-регресійного аналізу.

Датасет для виконання завдання аналізу сформований на підставі зафіксованих звернень до служби технічної підтримки оператора зв'язку ТОВ "ДКМ" з групи будинків у зоні покриття послугою провайдером у місті Кривий Ріг. Датасет охоплює період часу з 10.03.2024 по 21.04.2024, та 3.04.2024 12.04.2024. Перші два дні місяця були навмисно виключені, щоб фактор відсутності послуги через відсутність абонплати та пов'язаних з цим порушень користувачем налаштувань власного обладнання не впливав на загальний тренд.

Розглянуто кореляцію кількості звернень щодо відсутності зв’язку в залежності від наступних факторів: вихід з ладу обладнання клієнта, пошкодження лінії зв’язку у приміщенні клієнта, пошкодження лінії зв’язку в технічних приміщеннях або кабельних каналах, перерва в наданні послуги в наслідок планових технічних робіт або виході з ладу обладнання оператора, відсутність зв'язку через знеструмлення обладнання оператора.

Зазначимо, що певні фактори остаточно були виявлені не під час звернення клієнта, а встановлені фахівцями оператора безпосередньо в приміщенні надання послуги, тому остаточна статистика була сформована в результаті співставлення даних операторів хелпдеску та виконаних тікетів спеціалістами лінійно-монтажного відділу.

Також у дослідженні береться до уваги факт, що абонент звертається до служби технічної підтримки не кожного разу, коли може не бути зв’язку, а тільки у випадках, коли така відсутність помічена та абонент потребує консультації щодо методів усунення несправності. Додатковою умовою є припущення, що протягом місяця звертаються різні абоненти та повторних звернень немає. Отже отримали функцію мети та 5 основних факторів.

Датасет представлений у таблиці з наступними даними:

Y - загальна кількість звернень;

X1 - звернення, пов’язані з виходом з ладу обладнання клієнта (“завис” маршрутизатор/компьютер або надаються консультації з налаштування абонентських пристроїв);

X2 - звернення через пошкодження лінії зв’язку у приміщенні клієнта;

X3 - звернення через пошкодження лінії зв’язку в технічних приміщеннях або кабельних каналах;

X4 - звернення через через перерву в наданні послуги внаслідок планових технічних робіт або виході з ладу обладнання оператора;

X5 - звернення через відсутність послуги, пов’язані з знеструмленням обладнання оператора;

Зазначимо, що звернення про відсутність зв'язку через знеструмлення обладнання оператора відбуваються у випадках, коли у абонента немає електропостачання у його приміщенні, але є можливість заживити взасні пристрої, або через знеструмлення проміжних комутаційних вузлів рівня останньої милі, через що до приміщення клієнта може не приходити сигнал.

Таблиця 3.5 – залежність загального обсягу звернень від причини звернення до служби технічної підтримки

Y	X1	X2	X3	X4	X5
6	6	0	0	0	0
34	20	0	1	0	13

Продовження таблиці 3.5

21	16	0	1	0	4
93	18	0	0	0	75
30	19	2	3	0	6
21	17	2	0	0	2
11	10	0	1	0	0
7	7	0	0	0	0
18	12	0	1	0	5
24	16	0	1	5	2
24	17	0	0	0	7
19	14	0	0	0	5
27	22	0	1	0	4
4	2	0	1	1	0
11	10	0	1	0	0
30	18	0	0	0	12
12	12	0	0	0	0
13	11	2	0	0	0
20	13	1	1	0	5
42	18	0	1	0	23
8	7	1	0	0	0
17	17	0	0	0	0
43	19	2	4	0	18
22	16	0	1	0	5
34	22	1	0	0	11
14	10	0	1	0	3
20	19	0	1	0	0
45	20	0	3	0	22
18	14	0	1	0	3
35	19	1	1	0	14
48	20	0	0	3	25
40	21	0	3	0	16

Виконання кореляційного аналізу.

Одне з головних завдань у будь-якому дослідженні, - це встановлення зв'язків між різними факторами, які впливають на процес, який вивчається. Щоб зрозуміти явище, потрібно дослідити не лише його зв'язки з іншими явищами, а й взаємозв'язки всіх його аспектів. Тобто, треба з'ясувати закономірності змін у взаємопов'язаних явищах та показниках, що їх описують.

У практичній роботі науковця часто потрібно вивчати залежність між різними змінними. Якщо дві характеристики, отримані для одного об'єкта, змінюються разом так, що одну можна передбачити за іншою, то кажуть, що вони корелюють між собою. У статистиці кореляція виражає ступінь такого взаємозв'язку за допомогою коефіцієнта кореляції.

Кореляційний зв'язок - це одночасні зміни двох або більше ознак (множинний кореляційний зв'язок). Він показує, що зміна однієї ознаки співвідноситься зі зміною іншої. Проте це не означає, що одна ознака спричиняє іншу. Кореляція показує лише, що їх зміни часто співпадають, але чи це причина або вона знаходиться десь інде, ми не можемо визначити.[29]

Кореляційний зв'язок може бути двох типів: позитивним і негативним.

У позитивному зв'язку, коли одна ознака зростає, інша теж зростає. Якщо одна ознака падає, то й інша також.

У негативному зв'язку, коли одна ознака зростає, інша падає, і навпаки.

Ступінь кореляції вимірюється коефіцієнтом кореляції, який позначається як "r". Він може бути від -1 до +1.

Сила зв'язку не залежить від його напрямку і визначається за числовим значенням коефіцієнта кореляції. Якщо цей коефіцієнт близький до 1 за модулем, це вказує на сильний зв'язок між ознаками.

Класифікація кореляційної за силою:

- сильна при $|r| \geq 0,7$;
- середня при $0,5 \leq |r| < 0,7$;
- помірна при $0,3 \leq |r| < 05$;
- слабка при $0,2 \leq |r| < 0,3$;
- дуже слабка при $|r| < 0,2$;

Кореляційний аналіз виконувався за допомогою математичного пакету IBM SPSS (англ. Statistical Package for the Social Sciences — «статистичний пакет для соціальних наук»).[30]

Після імпорту вхідного датасету виконали аналіз за допомогою вбудованих інструментів за наступним сценарієм: меню “Аналіз” -> “Кореляція” -> “Парні”.

Попередньо змінили назву стовпців з умовних позначень, вказаних у таблиці 3.5, на більш зрозумілі, виходячи з опису параметрів.

Майстер обробки даних даних для кореляційного аналізу зображений на рисунку 3.6.

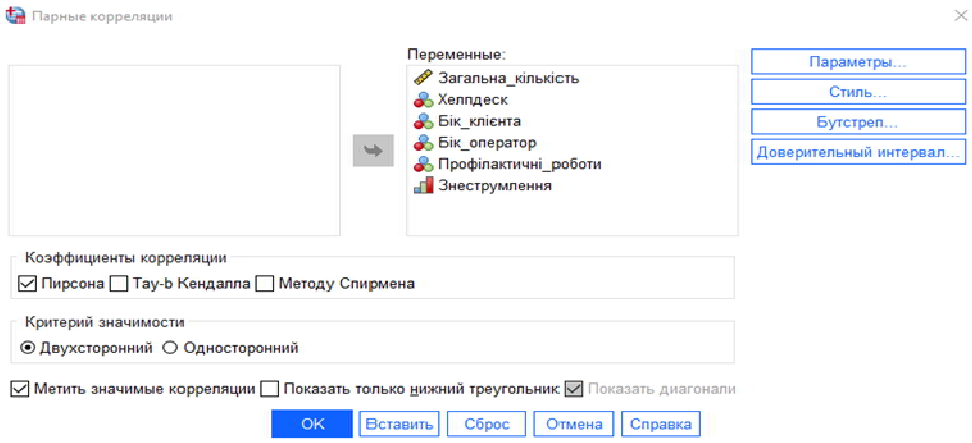

Рисунок 3.6 –майстер обробки даних даних для кореляційного аналізу

Для кореляційного аналізу використовуємо коефіцієнт Пірсона, який є мірою прямолінійного зв'язку між змінними: його значення досягають максимуму, коли точки на графіку двовимірного розсіювання лежать на одній прямій лінії.

Кореляційний аналіз показав, що найзначущім фактором у залежності кількості звернень до технічної підтримки (рисунок 3.7) є X5 - відсутність зв'язку через знеструмлення обладнання оператора. Коефіцієнт кореляції дорівнює 0,951. Другим за впливом є звернення до служби технічної підтримки, що мають більше консультативний характер та не потребують безпосереднього втручання у лінію зв’язку фахівців оператора. Коефіцієнт кореляції дорівнює 0,668.

Інші фактори мають коефіцієнт кореляції менше за 0,5, отже робимо висновок, що вони не впливають значущим шляхом на кількість звернень.

Корреляции

		Загалом	Хелпдеск	БікКлієнта	БікОператор	Профілактика	Знеструмлення
Загалом	Корреляция Пирсона	1	,668**	,018	,231	,073	,951**
	знач. (двухсторонняя)		<,001	,921	,204	,692	<,001
	N	32	32	32	32	32	32
Хелпдеск	Корреляция Пирсона	,668**	1	,109	,312	,040	,421*
	знач. (двухсторонняя)	<,001		,551	,083	,829	,017
	N	32	32	32	32	32	32
БікКлієнта	Корреляция Пирсона	,018	,109	1	,241	-,150	-,074
	знач. (двухсторонняя)	,921	,551		,183	,411	,688
	N	32	32	32	32	32	32
БікОператор	Корреляция Пирсона	,231	,312	,241	1	-,057	,087
	знач. (двухсторонняя)	,204	,083	,183		,757	,635
	N	32	32	32	32	32	32
Профілактика	Корреляция Пирсона	,073	,040	-,150	-,057	1	,014
	знач. (двухсторонняя)	,692	,829	,411	,757		,940
	N	32	32	32	32	32	32
Знеструмлення	Корреляция Пирсона	,951**	,421*	-,074	,087	,014	1
	знач. (двухсторонняя)	<,001	,017	,688	,635	,940	
	N	32	32	32	32	32	32

**. Корреляция значима на уровне 0,01 (двухсторонняя).

*. Корреляция значима на уровне 0,05 (двухсторонняя).

Рисунок 3.7 – дані кореляційного аналізу вхідного дата сету статистичного пакету SPSS

3.3. Використання методу експертної оцінки для визначення оптимальної технології широкосмугового доступу до інтернет з приоритетом на критерій енергоефективності

Експертна оцінка як метод дослідження питань вибору оптимального рішення.

Оскільки прийняття рішень стає все складнішим через збільшення кількості факторів, інформації тощо, використання математичних методів вже не так ефективне. Математичні методі все частіше поєднуються з оцінкою фахівців, що дозволяє покращити результати прогнозування або моделі, порівняно з біль класичним підходом використання тільки засобів математичного аналізу. Перевагою методу експертних оцінок є можливість прийняття рішень, коли об'єктивні методи не можуть дати достатню точність результату, а також зменшення витрат на експерименти та збір та обробку масивів статистичних даних. Недоліком методу є суб’єктивність та можлива упередженість фахівців, чия думка враховується у дослідженні. Однак статистика говорить, що помилка при застосуванні цього методу складає 5-10%, що є на одному рівні з математичним методами аналізу [31].

Існують два види експертної оцінки: індивідуальна та колективна. Індивідуальна оцінка - це висновок, який робиться одним експертом. Колективна оцінка - це результат роботи групи експертів, які використовують певні методи для прийняття рішень. Експеримент проводився з отриманням індивідуальних оцінок.

Існують різні способи проведення експертизи, такі як: обговорення, опитування, інтерв'ю, брейнштормінг, нарада, бізнес-ігри та інші. Часто використовують комбінацію різних методів для досягнення кращих результатів.

Існують також три методи проведення експертної оцінки: групове анкетування, метод сценаріїв та мозковий штурм. Експеримент використовував опитування, як засіб отримання експертної думки.

Методика підготовки та проведення експерименту включає наступні основні етапи:

1. Визначення мети експертного аналізу: чітко визначається мета та критерії, за якими результат експерименту буде оцінений.
2. Визначення мети експертного аналізу: чітко визначається мета та критерії, за якими результат експерименту буде оцінений.
3. Формування експертної групи: учасники експерименту повинні мати глибоку знання у галузі, що вивчається. У разі, якщо експерти мають різний рівень знань з фаху, їх оцінки можуть бути помножені на “ранг експертності”, що попередньо визначається для кожного з учасників.
4. Розробка процедур та анкет для проведення експертної оцінки: експерти аналізують завдання на основі свого логічного мислення та інтуїції,

спираючись на свої знання і досвід Це потребує високого рівня кваліфікації учасників.

5. Отримання результатів експертної оцінки: експерти приймають рішення та дають оцінки, які можуть бути числовими або якісними. Цей етап завершує роботу експертів. Оцінка дається за шкалою, що є інструментом оцінки явища, або характеристика об’єкта. Шкали може бути: номінальна, порядкова, інтервальна та шкала відношення.

6. Обробка даних опитування та аналіз отриманих результатів: результати обробляються з метою отримання остаточної оцінки проблеми. Кількість процедур на цьому етапі залежить від поставленого завдання. Щоб забезпечити швидкість та уникнути помилок, на цьому етапі часто використовується комп'ютерна техніка.

7. Визначення ступеня досягнення мети експертизи: отримані в результаті експерименту дані порівнюються з визначеними перед початком експерименту критеріями та надається висновок про досягнення мети експерименту, або його провал.

Під час експерименту з використанням методу експертних оцінок часто використовують інтервальну або порядкову шкалу для оцінки. Зазвичай для оцінювання об'єктів за цими шкалами використовують такі методи, як ранжування, парне порівняння та пряма оцінка.

Ранжування - це впорядкування об'єктів у послідовності зростання або зменшення певної характеристики. Цей метод дозволяє виділити найбільш важливі фактори або параметри з усіх досліджуваних. Результатом ранжування є впорядкований список.

Згідно з методикою експеримент проводився наступним чином:

- перед початком експерименту менеджментом оператора зв’язку були визначені ключові параметри, що є важливими для бізнесу з точки зору швидкості та вартості розгортання нової мережі, а також значущих експлуатаційних характеристик. Згідно з ранжуванням було визначено вагу кожного з параметрів. Були підібрані для порівняння технології, що поширені у країні та можуть бути використані для вирішення поставленої задачі розгортання сучасної комп'ютерної мережі;
- на другому етапі було відібрано 6 фахівців зі значним досвідом роботи у галузі;
- на третьому етапі за узгодженим переліком характеристик та обраних технологій було сформовано опитування;
- на четвертому етапі групі експертів з повідомили вхідні дані та запропонували пройти опитування;
- на п'ятому етапі результати було просумовано для кожного з параметрів та для отримання середнього рангу розділено на кількість опитуваних. Згідно з результатами середнього рангу технології було розташовано від кращої за певним параметром до меньш привабливої. Потім ранг було

помножено на вагу параметру. Отримані значення було просумовано для кожної з технологій та підставі отриманих значень було виконане остаточне ранжування технологій;
- отриманий результат було проаналізовано на відповідність мети проведення експерименту.

Експеримент для визначення оптимальної технології з використанням методу експертних оцінок.

Вибір технології широкосмугового доступу до Інтернету залежить від багатьох факторів, таких як розташування, бюджет, потреби в швидкості та стабільності зв'язку. Кожна з технологій має свої переваги та недоліки, і важливо враховувати їх при прийнятті рішення.

У таблиці 3.9 наведений опис параметрів, за якими відбувається порівняння технологій, параметри відсортовано у порядку важливості згідно з умовами завдання та важливістю для бізнесу.

Таблиця 3.8 – параметри для порівняння технологій широкосмугового доступу до мережі Інтернет

№ З/п	Назва параметру для порівняння	Опис параметру
1	Енергоспоживання	Енергоспоживання обладнання для забезпечення роботи інтернету абонентів у 20 ти будинках
2	Вартість активної частини	Вартість активного обладнання для забезпечення доступом до мережі абонентів 20 будинків.
3	Швидкість з'єднання	Вважаємо, що швидкість з’єднання є сумою максимальних значення прийому та передачі інформації за актуальними на 2022 рік значеннями стандарту
4	Вартість підключення нових розподільних вузлів	Вартість підключення нових технічних площадок до існуючої мережі, включаючи кабелі, кабельну арматуру, шафи для обладнання тощо.

Продовження таблиці 3.8

5	Витрати на підключення нового абонента	Вартість матеріалів та роботи для підключення нового абонента до мережі
6	Необхідність абонентського терміналу	Вартість встановлення додаткового клієнтського обладнання для отримання послуги споживачем
7	Витрати на обслуговування обладнання	Вартість амортизації / технічного обслуговування встановленого обладнання
8	Цінність лінії для злодіїв	Велика цінність матеріалу лінії зв’язку підвищує шанс пошкодження третіми особами.
9	Вплив несправності лінії абонента на сегмент мережі оператора	Зворотній вплив замикання/обриву лінії зв’язку на сегмент мережі оператора.
10	Можливість масштабування	Вартість збільшення кількості абонентів у разі вичерпання розрахованої кількості
11	Стійкість ліній зв’язку до впливу зовнішніх факторів	Стійкість лінії зв’язку механічним пошкодженням до виходу зі справного стану
12	Строк експлуатації ліній зв’язку	Строк експлуатації ліній зв’язку враховуючи деградацію оптоволокна, діелектричних елементів електричної лінії зв’язку, можливе розтяжіння кабелю та погіршення характеристик зв’язку через зміну еталенної ємності та інших параметрів лінії.

Розподіляємо "Вага" між параметрами таким чином, щоб у сумі він дорівнював 1. Найвище значення “важливості” 12 має перший параметр, найнижчий 1 має останній параметр. Сума значень “важливості” від 12 до 1 дорівнює 78. Для визначення ваги кожного балу “важливості” розділимо 1 на 78 та отримуємо 0,01282. Для визначення ваги параметру помножимо його “важливість” на вагу одного балу.

Таблиця 3.9 – розводіл ваг параметрів у залежності від ступеня важливості.

№ З/п	Назва параметру для порівняння	Важлівість	Вага
1	Енергоспоживання	12	0,15384
2	Вартість активної частини	11	0,14102
3	Швидкість з'єднання	10	0,1282
4	Вартість підключення нових розподільних вузлів	9	0,1282
5	Витрати на підключення нового абонента	8	0,11538
6	Необхідність абонентського терміналу	7	0,08974
7	Витрати на обслуговування обладнання	6	0,07692
8	Цінність лінії для злодіїв	5	0,0641
9	Вплив несправності лінії абонента на сегмент мережі оператора	4	0,05128
10	Вартість масштабування	3	0,03846
11	Стійкість ліній зв’язку до впливу зовнішніх факторів	2	0,02564
12	Строк експлуатації ліній зв’язку	1	0,01282
Сума		78	1

Для порівняння використовуємо метод ранжування, надаючи кожному з параметрів ранг від 1 до 4, вважаючи 4 за найкращій результат, а 1 за найгірший (найдорожчий або найнезручніший у розумінні витрат людино-годин).

Для визначення рангу було створене опитування [32], де експертам запропоновано поставити оцінку від 1 до 4 за кожним з параметрів кожній технології. В експерименті прийняли участь 6 експертів.

Таблиця 3.10 – середній біл технологій за параметром на підставі опитування експертів

№ З/п	Назва параметру для порівняння	Назва технології			
		FTTB	GPON	DOCSIS	ADSL
1	Енергоспоживання	2,17	3,50	2,00	2,33
2	Вартість активної частини	2,17	3,67	1,83	2,33
3	Швидкість з'єднання	3,00	4,00	1,83	1,17
4	Вартість підключення нових розподільних вузлів	1,83	2,33	3,67	2,17
5	Витрати на підключення нового абонента	1,67	1,50	2,83	2,33
6	Необхідність абонентського терміналу	3,67	2,33	1,83	2,17
7	Витрати на обслуговування обладнання	1,17	3,83	2,33	2,67
8	Цінність лінії для злодіїв	2,33	2,83	1,67	1,50
9	Вплив несправності лінії абонента на сегмент мережі оператора	2,17	3,00	2,17	2,67
10	Вартість масштабування	3,00	2,50	2,83	1,67
11	Стійкість ліній зв’язку до впливу зовнішніх факторів	2,00	3,67	1,83	2,50
12	Строк експлуатації ліній зв’язку	2,17	3,50	1,83	2,50

Бали, віддані за кожну з технологій у окремому параметрі, було підсумовано та розділено на кількість експертів, що брали участь у опитуванні. (таблиця 3.10).

На основі отриманого середнього рангу було сформоване остаточне ранжування у таблиці 3.11.

Таблиця 3.11 – ранжування технологій за параметрами на підставі експертної середньої оцінки

№ З/п	Назва параметру для порівняння	Вага	Назва технології			
			FTTB	GPON	DOCSIS	ADSL
1	Енергоспоживання	0,15384	2	4	1	3
2	Вартість активної частини	0,14102	2	4	1	3
3	Швидкість з'єднання	0,1282	3	4	2	1
4	Вартість підключення нових розподільних вузлів	0,1282	1	3	4	2
5	Витрати на підключення нового абонента	0,11538	2	1	4	3
6	Необхідність абонентського терміналу	0,08974	4	3	1	2
7	Витрати на обслуговування обладнання	0,07692	1	4	2	3
8	Цінність лінії для злодіїв	0,0641	3	4	2	1
9	Вплив несправності лінії абонента на сегмент мережі оператора	0,05128	3	4	2	1
10	Вартість масштабування	0,03846	4	2	3	1
11	Стійкість ліній зв’язку до впливу зовнішніх факторів	0,02564	2	4	1	3
12	Строк експлуатації ліній зв’язку	0,01282	2	4	1	3

Для отримання коефіцієнту для кожного з параметрів таблиці 3.11 перемножимо його вагу на його ранг.

Отримуємо суму рангів та будємо підсумковий ранжований ряд, виходячи з принципу – чим вище ранг, чим привабливішою є технологія.

Таблиця 3.12 – ранжування технологій на підставі добутку рангу та ваги параметру

№ З/п	Назва параметру для порівняння	Назва технології			
		FTTB	GPON	DOCSIS	ADSL
1	Енергоспоживання	0,30768	0,61536	0,15384	0,46152
2	Вартість активної частини	0,28204	0,56408	0,14102	0,42306
3	Швидкість з'єднання	0,3846	0,5128	0,2564	0,1282
4	Вартість підключення нових розподільних вузлів	0,11538	0,34614	0,46152	0,23076
5	Витрати на підключення нового абонента	0,20512	0,10256	0,41024	0,30768
6	Необхідність абонентського терміналу	0,35896	0,26922	0,08974	0,17948
7	Витрати на обслуговування обладнання	0,07692	0,30768	0,15384	0,23076
8	Цінність лінії для злодіїв	0,1923	0,2564	0,1282	0,0641
9	Вплив несправності лінії абонента на сегмент мережі оператора	0,15384	0,20512	0,10256	0,05128
10	Вартість масштабування	0,15384	0,07692	0,11538	0,03846
11	Стійкість ліній зв’язку до впливу зовнішніх факторів	0,05128	0,10256	0,02564	0,07692
12	Строк експлуатації ліній зв’язку	0,02564	0,05128	0,01282	0,03846

Продовження таблиці 3.12

Сума рангів	2,3076	3,41012	2,0512	2,23068
Підсумковий ранг	2	1	4	3
Загальний вигляд ранжованого ряду	GPON>FTTB>ADSL>DOCSIS			

Згідно з відсумковім загальним рангом найкращою до впровадження є технологія GPON.

За ключовим в межах дослідження параметром енергоефективності технологія GPON також є кращою.

Висновки за розділом.

У третьому розділі зробили аналіз найпоширеніших технологій доступу до Інтернету в Україні: PON (Passive Optical Network), FTTB (Fiber To The Building), ADSL (Asymmetric Digital Subscriber Line) і DOCSIS (Data Over Cable Service Interface Specification). У кожної з цих технологій є свої недоліки та переваги, і вибір між ними залежить від умов розгортання та потреб бізнесу.

Було розглянуто формування набору даних для визначення критеріїв, які впливають на кількість звернень до служби технічної підтримки оператора. Аналіз цих даних допомагає оптимізувати витрати, раціонально розподіляти робочий час між відділом хелпдеску та монтажно-лінійним відділом. Використаний програмний пакет для обробки статистичних даних SPSS виявив, що найзначущими факторами звернень були проблеми з доступом до мережі через знеструмлення обладнання оператора та запити на консультації з коефіцієнтами кореляції 0,951 та 0,668 відповідно.

Провели порівняння основних технічних характеристик кожної з порівняних технологій відповідно до важливих для бізнесу критеріїв. Для цього був застосований метод експертних оцінок. На першому етапі експерименту на було сворене опитування, у якому взяли участь 6 фахівців оператора зв’язку. Учасники опитування розподілили технології від кращої до гіршої за кожним з критеріїв порівняння. Зібрані дані були оброблені за описаною методикою роботи за методом експертних оцінок. На основі проведених досліджень було сформовано ранжований ряд, що має вигляд GPON>FTTB>ADSL>DOCSIS, з чого зроблено висновок, що найкращою для досліджених умов та параметрів є технологія GPON.

4. ПРАКТИЧНЕ ЗАСТОСУВАННЯ ОТРИМАНИХ У ХОДІ НАУКОВОГО ДОСЛІДЖЕННЯ РЕЗУЛЬТАТІВ

Технологія пасивних оптичних мереж набуває дуже швидкого поширення останніми роками. Окрім високої якості зв’язку та перешкодостійкості, основною перевагою, що за період активних обстрілів армією РФ з лютого 2022 року цивільних об'єктів енергетичної інфраструктури України набула ледь не найважливішого значення, стала енергонезалежність технології PON. Якщо спочатку встановлення таких мереж було дорогим і складним (навіть з урахуванням подальшого зростання теоретична потужність перевищувала існуючий попит у кілька разів), то сьогодні ціни на волоконну оптику та мережеві оптичні компоненти впали, а в мережах доступу використання волоконно-оптичних кабелів стало дуже перспективним.

Існує декілька видів технології PON:

- APON - ATM PON - на основі технології ATM;
- BPQN - широкосмуговий PON;
- EPON - Ethernet PON - на основі технології Ethernet;
- GPON - Gigabit PON - на основі технології Gigabit Ethernet.

Недоліком технології PON є відносна відсутність масштабованості, тому етап проектування є дуже важливим і навіть вирішальним для роботи мережі у довгостроковій перспектив. Завдання проектування також полягає в тому, щоб мережа відповідала основним вимогам потужності сигналу. Втрати на розсіювання безпосередньо пов’язані з нерівномірністю оптичного шляху, тобто коли втрати на сегментах OLT-ONTi різні. Необхідно враховувати, що оптичний бюджет системи обмежений, а необґрунтований розподіл оптичної потужності призводить до зниження масштабованості мережі. Існує додаткове розсіювання через допуски в значеннях коефіцієнта розділення сплітера [33].

Для даного користувацького устрою єдиним доступним методом вирівнювання оптичних втрат є вибір коефіцієнта поділу оптичного сплітеру. Для невеликих мереж можна вибрати симетричний спліттер або приблизно розрахувати його параметри. Неоптимальність рішення в цьому випадку компенсується великими резервами потужності, що не підходить для великих мереж. Необхідно враховувати, що оптичний бюджет системи обмежений, а необґрунтоване розподіл оптичної потужності призведе до зниження масштабованості мережі. Існує додаткове розсіювання через допуски в значеннях коефіцієнта розділення сплітера. Необхідно обчислити усі їх параметри. У цьому випадку неоптимальність рішення компенсується великим запасом потужності, який не підходить для великих мереж.

4.1. Оптичний бюджет PON-мережі

При проектуванні PON використовуємо концепцію збалансованої мережі, коли рівень потужності, прийнятий усіма абонентськими вузлами, має бути приблизно однаковим.

Оскільки розрахунок збалансованої PON мережі йде від абонентського пристрою та методом підбору обираються поділювачі, що забезпечують вирівнювання потужності сигналу між усіма пристроями мережі, перш за все необхідно визначитись із значенням рівня сигналу на абонентському терміналі.

У PON-мережах використовують топології: дерево та шина. Приклади зображені на рисунках: 4.1, 4.2. Також дуже часто в залежності від реальних умов застосовують змішану топологію.

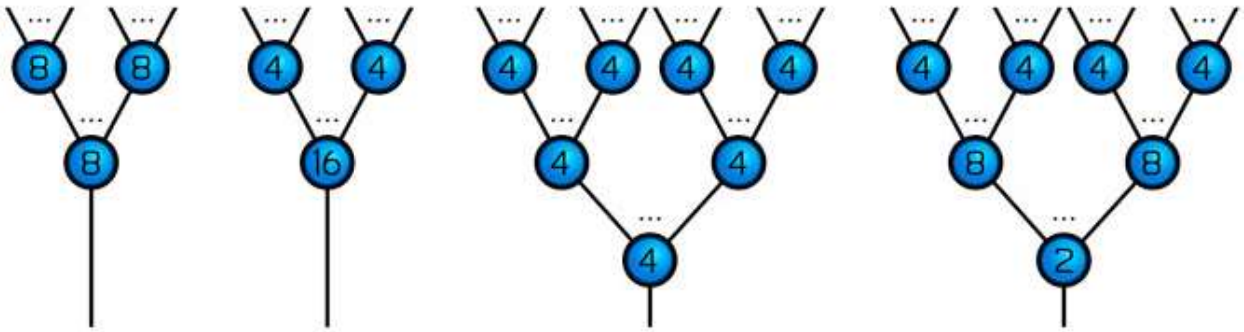

Рисунок 4.1 - приклад топології “Дерево”.

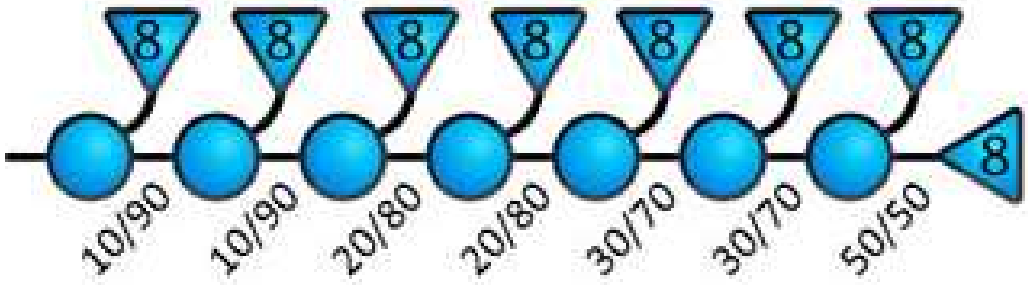

Рисунок 4.2 - приклад топології “Шина”.

Також при розрахунку велику роль грає тип підключення сплиттера. Існує кілька варіантів підключення сплітера:

1. Зварювання (всі виходи розгалужувача припаяні до волокна).

   Переваги:

   - Мінімальне завмирання сигналу;

   - Витрати робочого часу найвищі при пошуку несправностей мережі.

2. Механічний (всі виходи розгалужувача підключаються до оптоволокна за допомогою роз'ємів).

   Переваги:

   - максимальне ослаблення сигналу;

   - трудовитрати при пошуку несправностей мережі мінімальні.

3. Комбінація (частина виходу сплітера припаяна до оптоволокна, а решта підключена через роз'єм).

Переваги:

- оптимальне ослаблення сигналу;
- трудовитрати при пошуку несправностей мережі мінімальні.

Приклад комбінованого варіанту підключення сплітерів:

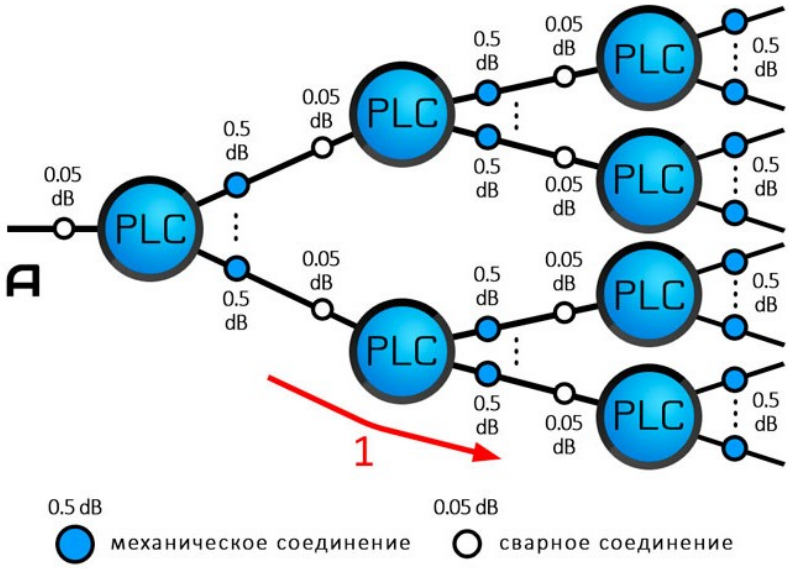

Рисунок 4.3 - приклад використання комбінованого типу з'єднання у топології "дерево".

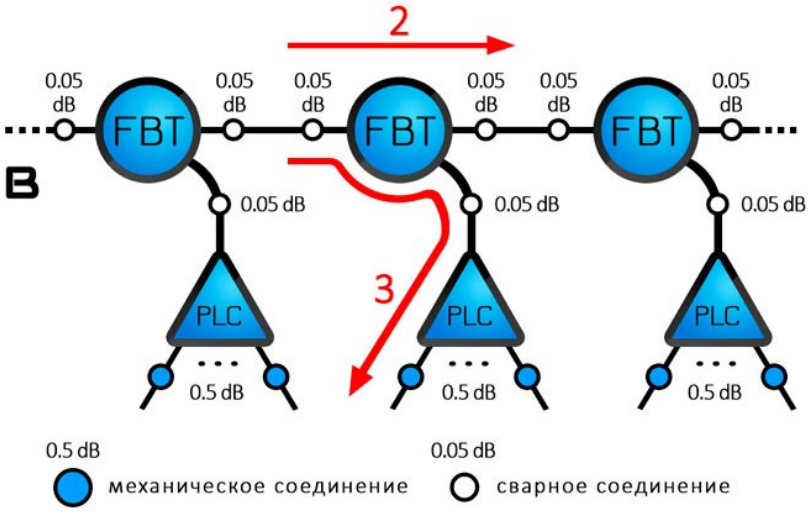

Рисунок 4.4 - приклад використання комбінованого типу з'єднання у топології "шина".

Практика показує, що провайдери найчастіше обирають комбінований варіант «включення» сплітера, так як він пропонує компроміс між ослабленням сигналу та простотою усунення несправностей у мережі [34].

Сучасні оптичні модулі мають чутливість до 30 Дб. Вважаємо, що оптична лінія, крім останньої милі, побудована шляхом зварювання оптичного волокна

та поділювачів, має згасання сигналу на місці стику не більше 0,05 дБ, а остання миля є FTTH кабелем з двома фаст-коннекторами на кінцях. Отже між операторським поділювачем та ONU-терміналом абонента є два механічних з'єднання зі згасанням Z_m не більше 0,5дБ. Вважається, що втрати на фаст-конекторі $Z_{ФК}$ не мають бути більшими за 0,35 Дб. Отже згасання останньої милі можно порахувати згідно з формулою:

$$Z_{ом} = 2 * Z_m + 2 * Z_{фк} = 2 * 0{,}5 + 2 * 0{,}35 = 2\ дБ. \quad (4.5)$$

На практиці згасання у останній милі може бути суттєвим через бажання кінцевого споживача сховати кабель у приміщенні, використовуючи короби, плінтуси та інще, не приділяючи уваги рекомендованому радіусу згинання оптоволокна. Тому при розрахунку вноситься певний запас потужності на цей експлуатаційний фактор. Отже додамо значення експлуатаційного резерва у $Z_{ер} =$ 4Дб до значення згасання останньої милі.

Тоді розрахункове згасання сигналу на вході обладнання клієнта P_K буде дорівнювати різниці чутливості модуля та додатку згасання останньої милі з експлуатаційним резервом.

$$P_K = P_{min} - (Z_{ом} + Z_{ер}) = 30 - (4 + 2) = 24\ Дб. \quad (4.6)$$

При розрахунку реального проекту оптичний бюджет втрат має бути порахований точніше для кожного кінцевого вузла мережі. Для визначення сумарного згасання всіх елементів ланцюга можна скористатися формулою, поданою нижче:

$$Z_{\sum} = \alpha * L_{\sum} + Z_З * N_З + Z_m * N_М + S_{\sum}, \text{ dB} \quad (4.7)$$

$\mathbf{Z_{\sum}}$ - сумаре згасання сигналу;

$\boldsymbol{\alpha}$ - згасання сигналу на 1км оптоволокна на довжині хвилі 1310нм;

$\mathbf{L_{\sum}}$ - сумарна довжина оптоволокна від OLT-а до кінцевого вузла;

$\mathbf{Z_З}$ - загасання сигналу на зварному з'єднанні;

$\mathbf{N_З}$ - кількість зварних з'єднань на пусті слідування сигналу від OLT-а до кінцевого вузла;

$\boldsymbol{Z_m}$ - згасання сигналу на механічному з'єднанні;

$\mathbf{N_М}$ - кількість механічних з'єднань на шляху проходження сигналу від OLT-а до кінцевого вузла;

$\mathbf{S_{\sum}}$ - сумарне згасання сигналу на каскаді сплітерів;

4.2. Розрахунок необхідної кількості елементів мережі для впровадження технології PON у обраній локації

Для вибору активного обладнання для впровадження широкосмугового доступу до Інтернет на певній локації перш за все необхідно визначитись з планованою кількістю потенційних абонентів. Виходячи з даних джерела slovoidilo.ua [35] за результатами дослідження DataReportal середній рівень проникнення послуг Інтернет в Україні на січень 2024 складає 79.2%. У цей показник входять як фіксований зв'язок, так и мобільний інтернет. Згідно з більш раннім дослідженням Factum Group Ukraine [36] кількість абонентів, що користуються виключно мобільними пристроями, складає 15%. Тобто можемо зробити висновок, до проникнення послуг саме фіксованого Інтернет складає приблизно 64.2%.

Згідно із завданням розраховуємо кількість потенційних абонентів шляхом перемноження кількості квартир у вказаній локації на коефіцієнт проникнення послуги Інтернет. Обрана локація: м.Кривий Ріг, пр. Миру, будинки: 31-41 (непарна сторона). Будинки у обраній локації складаються з 1-10 під'їздів та мають по 36 квартир у кожному, крім будинків 35, 37, що мають по 1 одному під'їзду та 72 квартири. Для спрощення підрахунку вважаємо, що вони теж мають два під'їзда по 36 квартир. Отримуємо кількість під'їздів у обраній локації 30. Перемноживши кількість під'їздів на кількість квартир, отримуємо 30*36=1080 квартири у потенційній зоні покриття. Перемножимо отримане значення на процент проникнення послуги та отримуємо 1080*64.2%=901 квартиру. Підприємство розраховує, що може зайняти 25% ринку за обраними адресами, отже 693 множимо на 25% та отримуємо 693*25%=173.

Найближчим за показником максимальної кількості абонентів є GEPON концентратор BDCOM P3310, що має максимальну ємність 256 клієнтських пристроїв. Він має 4 GEPON порти та має коефіцієнт ділення 1:64. Враховуючи обов'язкову необхідність резервування живлення, обираємо модифікацію BDCOM P3310-DC (рисунок 4.8), що передбачає живлення постійним струмом.

Також з активного обладнання необхідні оптичні трансивери (приклад на рисунку 4.9), яких знадобиться 4 шт. Одним з параметрів оптичного трансиверу є вихідна потужність оптичного сигналу, тому для обрання оптичного трансиверу необхідно спочатку розрахувати оптичним бюджет мережі. Оптимальний вибір оптичної потужності трансивера забезпечує баланс між рівнем сигналу та вірогідністю появи дрифту сигналу через занадто сильний випромінювач.

Рисунок 4.8 - GEPON концентратор BDCOM P3310.

Рисунок 4.9 - SFP GEPON трансівер FoxGate SFP-1,25G-GEPON (C++)-20SC.

Побудова схеми розміщення комутаційних боксів з прив’язкою до плану вулиці.

У попередньому пункті розрахували кількість абонентів за обраними адресами - 173 приміщеня. Також визначили, що кількість під’їздів 30, отже кількість потенційних абонентів на під’їзд складає 173/30=6. Виключенням є зазначені раніше будинки пр.Миру 35 та пр.Миру 37, де потенційна кількість абонентів є у два рази вищою, але у розрахунку це враховано. Отже у кожному під’їзді планується встановлючати PON-бокс (рисунок 4.10) з дільником сигналу 1:8, та у двох випадках 1:16. Також зазначимо, що за таким розрахунком залишається біля 25% від загальної ємності оптичного концентратору для потенційного збільшення кількості клієнтів від планованої, що має сенс з урахуванням тенденцій розвитку пасивних оптичних мереж та їх перевагами над FTTB. Таким чином технічна межа ємності проектованої мережі складає 31% клієнтів фіксованого зв’язку у обраній локації.

Рисунок 4.10 - оптичний бокс Crosver FOB-07-08R.

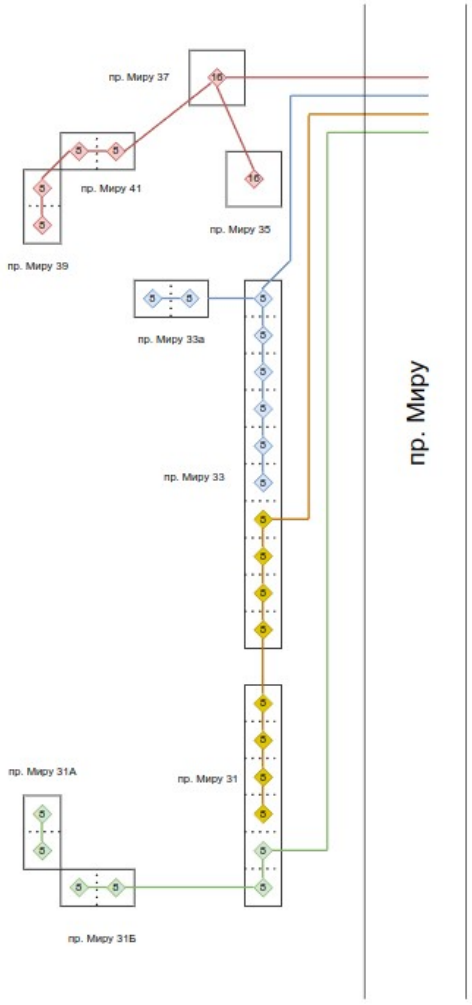

Рисунок 4.11 - схема розташування оптичних боксів відносно під'їздів кожного з будинків планованої зони покриття.

На рисунку 4.11 зображена схема розташування оптичних боксів відносно під'їздів кожного з будинків планованої зони покриття. Також зазначений коефіцієнт встановленого у боксі дільника (рисунок 4.12), колір оптоволокна

та приналежність встановленого кросового обладнання до гілки, якщо вважати гілкою лінію зв’язку від кожного з 4х оптичних випромінювачів.

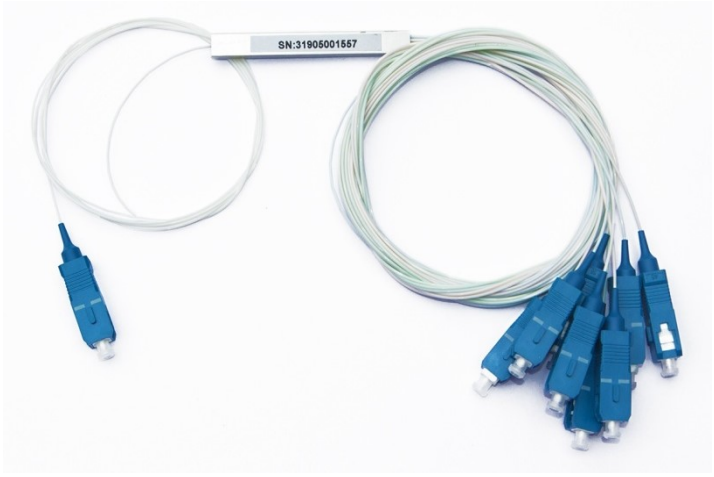

Рисунок 4.12 - Дільник оптичний Coupler PLC роз'ємами SC / UPC з кількістю виходів 8.

Розрахунок оптичного бюджету PON-мережі.

Для розрахунку оптичного бюджету кожного з 4х сегментів проектованої мережі використали формулу 4.7 та планований рівень сигналу/згасання безпосередньо у абонента згідно з розрахунком 4.6. У таблиці 4.13 наведені значення згасання сигналу на кожному з виводів обраного дільника.

Таблиця 4.13 - значення згасання сигналу у оптичних дільниках.

Планарні дільники		Зварні дільники	
Дільник	Згасання, dB	Дільник	Згасання, dB
1x2	4.3	50/50	3.17/3.19
1x3	6.2	45/55	3.73/2.71
1x4	7.4	40/60	4.01/2.34
1x6	9.5	35/65	4.56/1.93
1x8	10.7	30/70	5.39/1.56
1x12	12.5	25/75	6.29/1.42
1x16	13.9	20/80	7.11/1.06
1x24	16.0	15/85	8.16/0.76
1x32	17.2	10/90	10.08/0.49
1x64	21.5	5/95	13.70/0,32
1x128	25.5		

На рисунку 4.14 зображена схема розташування дільників у сегменті та розраховані значення падіння сигналу з урахуванням 2х зварних стиків на кожний перехід між дільниками та падіння у механічному з'єднанні на вході. Розраховані значення сигналу на кінці першого сегменту знаходяться диапазоні 20.76-21.58 dB та є кращими за бажане значення за розрахунком 4.6. Значення на кінцях дільників на різних будинках є приблизно однаковими, що свідчить про вірність підібраних дільників.

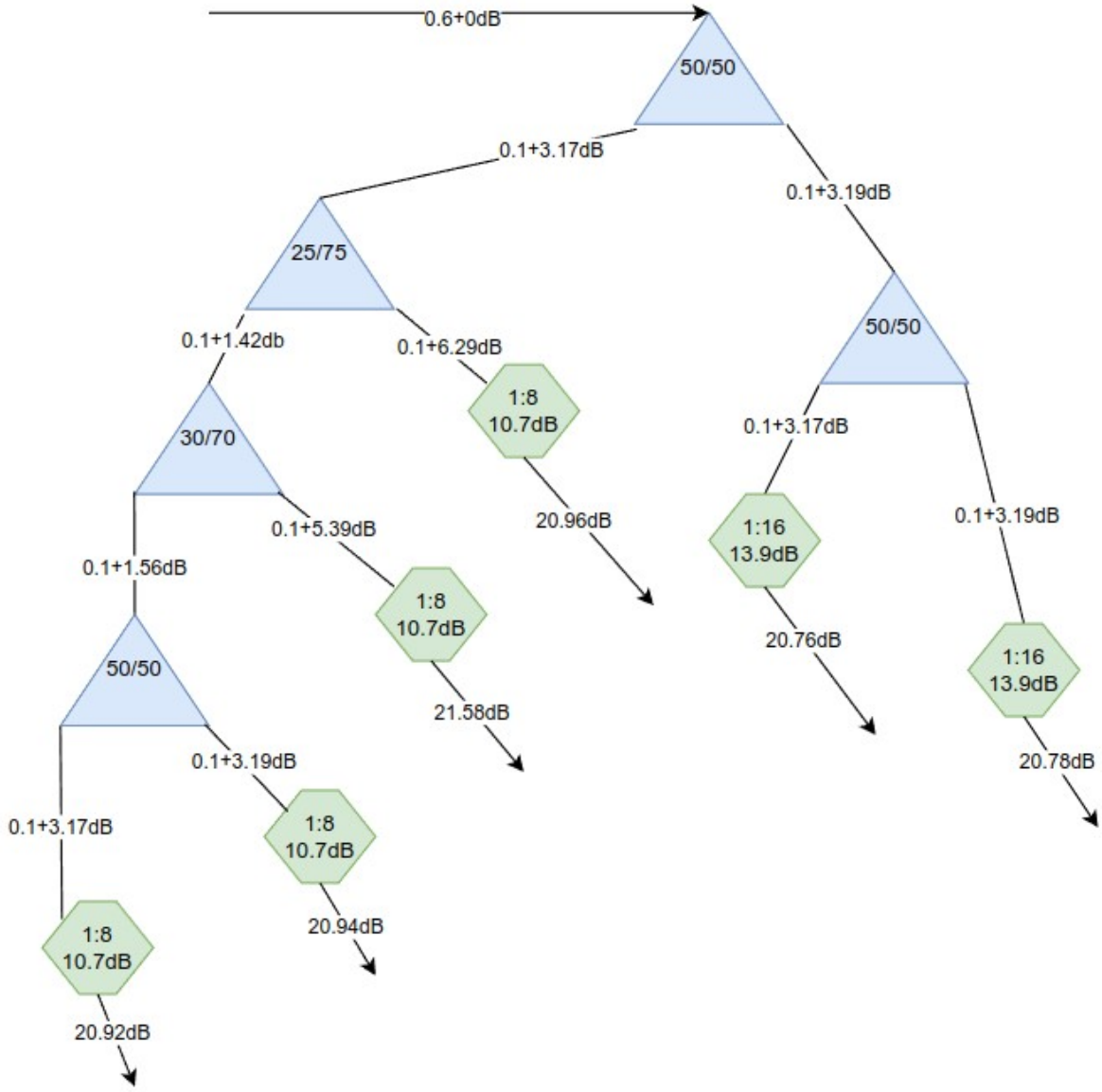

Рисунок 4.14 - схема розподілення згасання сигналу у 1му сегменті мережі.

Аналогічним чином розрахували кількість дільників та рівнів сигналів 2-4 сегментів, додаючи на вхід суму оптичних втрат на кожному з'єднанні у передуючих стиках. Розрахунок зображений на рисунках 4.15-4.17.

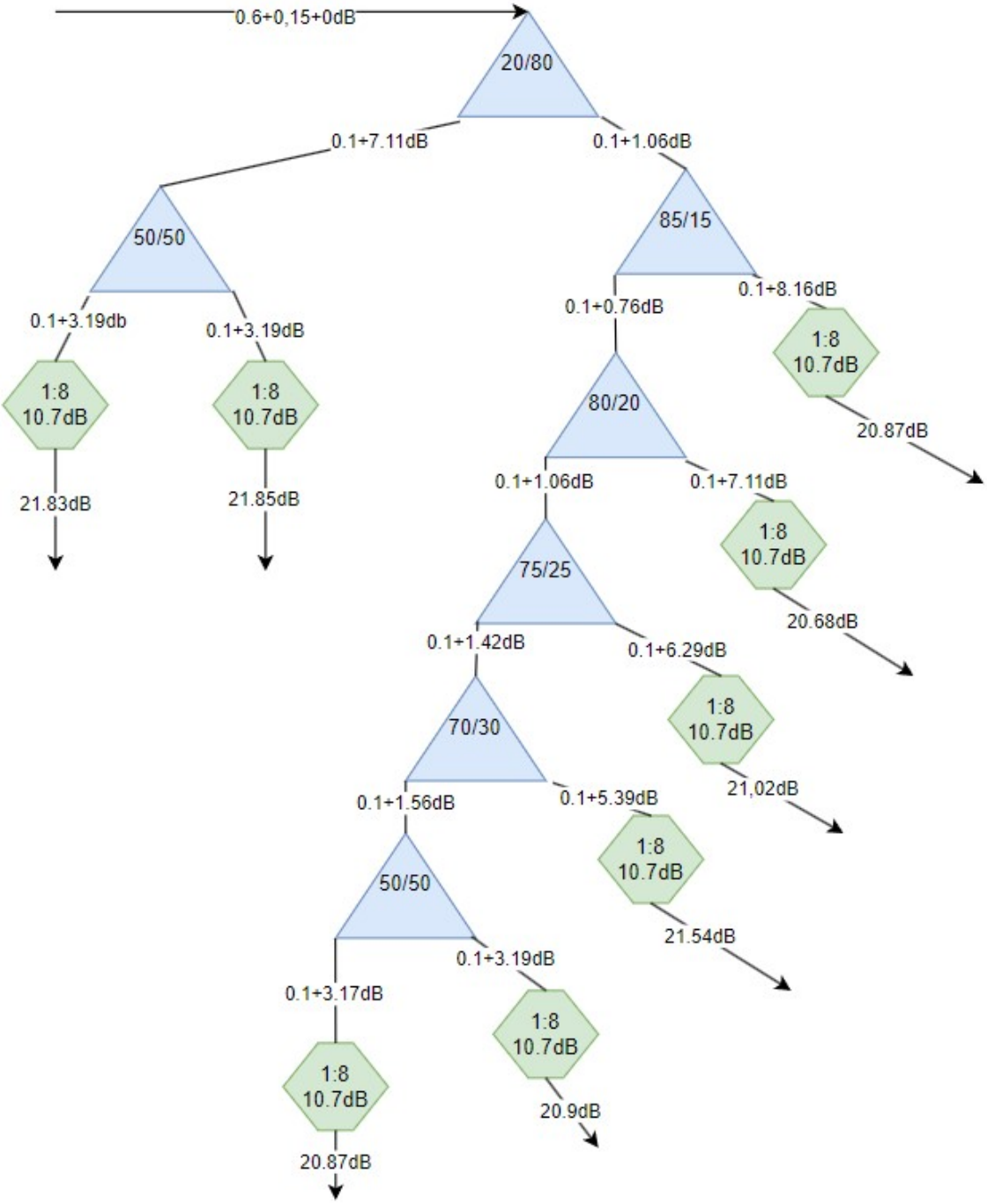

Рисунок 4.15 - схема розподілення згасання сигналу у 2му сегменті мережі.

Згідно з формулою 4.7 мали б врахувати падіння сигналу безпосередньо у оптоволокні, що складає максимально 0.3dB на 1 км кабелю, але сумарна довжина найкоротшого сегменту є меншою за 100 метрів, а найдовшого - 700 метрів, тому падінням рівня сигналу у диапазоні 0.01-0.2dB вирішили знехтувати.

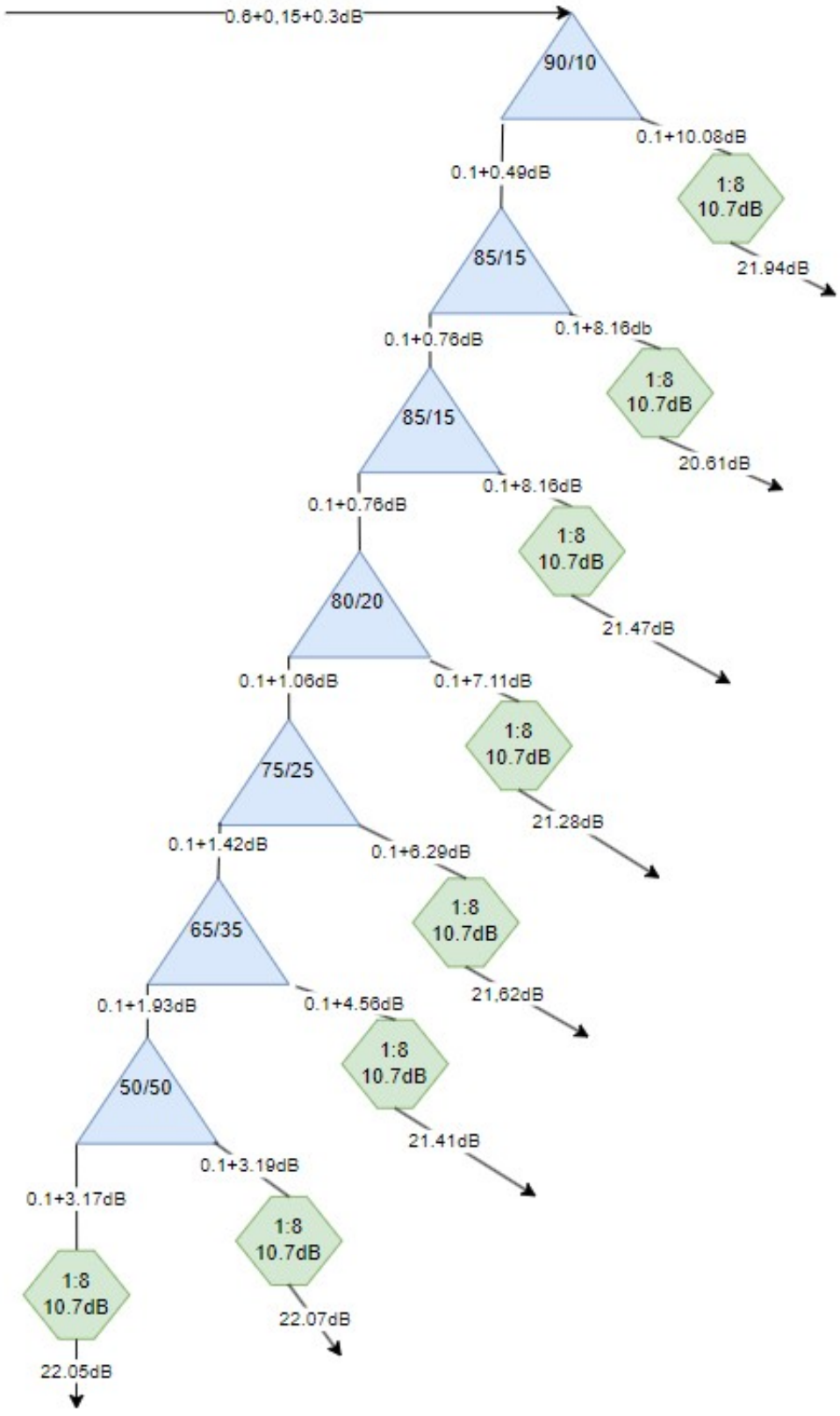

Рисунок 4.16 - схема розподілення згасання сигналу у 3му сегменті мережі.

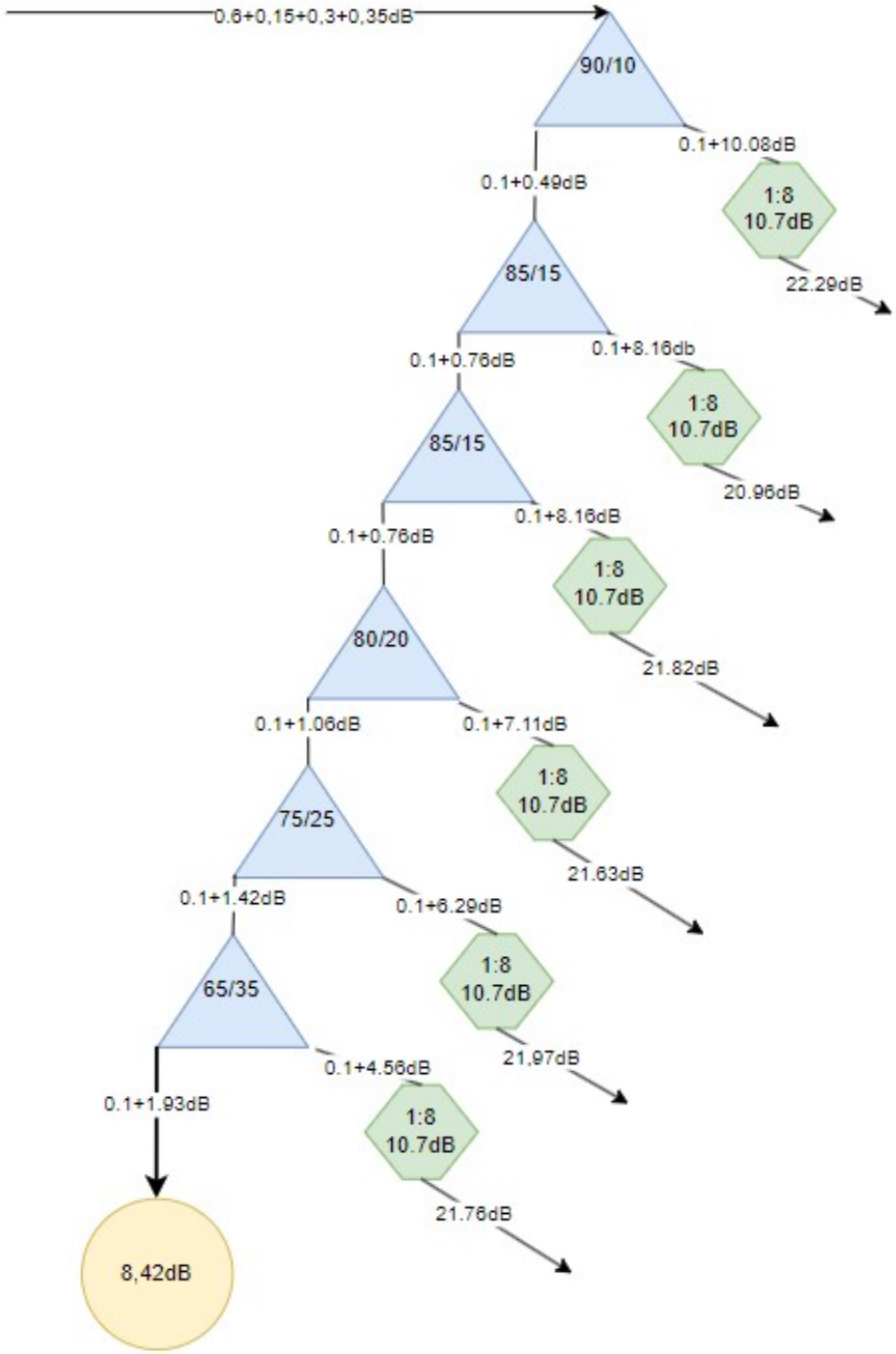

Рисунок 4.17 - схема розподілення згасання сигналу у 4му сегменті мережі.

Зазначимо, що у 4му сегменті залишається можливість добудувати лінію з ємністю до 16 клієнтів. На рисунку 4.17 у кінці лінії вказане вхідне згасання для продовження майбутньої ділянки.

Формування переліку необхідного для розгортання пасивної оптичної мережі активного та пасивного обладнання.

Грунтуючись на результатах отриманого розрахунку, обираємо оптичний трансівер. Найвище розраховане згасання по всім сегментам проектованої мережі складає 22,29 дБ, а розраховане бажане за формулою 4.6 згасання складає приблизно 24 дБ, тому рекомендовано використовувати трансивер класу В з потужністю передавача 1,5dB.

Обробивши отримані в результаті розрахунку дані по кількості елементів мережі, склали перелік необхідного обладнання та навели його у таблиці 4.18.

Таблиця 4.18 - перелік та кількість обладнання для впровадження PON-мережі.

№.З/п	Найменування	Кількість
1	GEPON концентратор BDCOM P3310	1
2	SFP GEPON трансівер A-GEAR 1G SC	4
3	Оптичний бокс Crosver FOB-07-08R.	28
4	Дільник PLC роз'ємами SC / UPC з кількістю виходів 8	26
5	Дільник PLC роз'ємами SC / UPC з кількістю виходів 16	2
6	Дільник FBT 10/90 SC / UPC	2
7	Дільник FBT 15/85 SC / UPC	5
8	Дільник FBT 20/80 SC / UPC	3
9	Дільник FBT 25/75 SC / UPC	4
10	Дільник FBT 30/70 SC / UPC	2
11	Дільник FBT 35/65 SC / UPC	2
12	Дільник FBT 50/50 SC / UPC	3
13	Прохідний адаптер SC / UPC	240

Висновки за розділом.

У четвертому розділі розглянули загальні поняття про пасивні оптичні мережі, види топологій та методику розрахунку втрат сигналу з урахуванням проміжних оптоволоконних стіків. Також розглянули основні види топологій пасивних оптичних мереж та методику розрахунку втрат сигналу з урахуванням проміжних стіків. Розрахували оптичний бюджету та обрали топологію в залежності від безпосереднього розташування розподільчих комутаційних пунктів. Виходячи з побудованого плану та розрахунку розподілення оптичних втрат, склали перелік необхідного для розгортання PON-мережі активного та пасивного обладнання.

ВИСНОВКИ

У магістерській роботі досліджена проблематика забезпечення енергоефективності операторських мереж зв’язку з оглядом технічних рішень, що можуть бути застосовані для збільшення часу автономного режиму роботи. Основні тези щодо причин, які спонукали до пошуку рішень проблеми енергозалежності було розглянуто на CXXXIII Міжнародній науково-практичної інтернет - конференції «Розвиток науки та техніки України під час воєнного стану» [3], та на Всеукраїнській науково-практичній web конференції аспірантів, студентів та молодих вчених КІСМ 2024 [4] були запропоновані конкретні шляхи вирішення цієї проблеми.

У процесі розробки проекту розглянули основні технології, що застосовуються у мережах операторів зв’язку та вже існуючі рішення, що можуть бути застосовані для досягнення мети побудови/модернізації енергоефективної мережі оператора зв’язку. З допомогою мережевого емулятору створили модель, що складається з базових вузлів мережі. Також налаштували взаємодію вузлів мережевого обладнання між собою, тим самим упевнившись, що модель відповідає нашим вимогам. На другому етапі побудови моделі навели приклад впровадження технологій віртуалізації для оптимізації використання апаратних ресурсів у випадку використання декількох сервісів у мережі. На прикладі налаштування веб-серверу продемонстрували легкість та ефективність впровадження цієї технології.

Використовуючи на побудовану модель, зробили дослідження, у якому визначили найуразливіші місця мережі, де проблема нестійкості енергозабезпечення найбільш притично може вплинути на сталість надання послуг зв’язку. Обробили статистику звернень до служби технчної підтримки діючого оператору зв’язку, та за допомогою статистичних програмних пакетів довели значущість фактору нестабільності енергопостачання у загальній кількості звернень.

Спираючись на отримані дані, використали метод експертної оцінки для визначення технічного рішення, що допоможе зменшити вплив віялових відключень на час безперервної роботи мереж зв’язку. Результатом дослідження за поставлених умов було визначено, що найефективнішою технологією для впровадження з розглянутих є технологія пасивних оптичних мереж.

Дослідження включає огляд практичного застосування обраної технології у реальному секторі. Проведений розрахунок показує економічну доцільність впровадження технології PON не тільки для побудови нових мереж, а й для модернізації діючих розподільчих пунктів.

Результати дослідження можуть бути використані при проектуванні мереж операторів зв’язку та у подальшій науковій роботі, що стане базою для пошуку додаткових шляхів оптимізації та розробки нових за структурою мереж передачі даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) “Українська правда”, “Мережі готові, але не скрізь. Чи будуть українці з інтернетом при вимкненнях світла.” від 2 жовтня 2023. URL: https://www.epravda.com.ua/publications/2023/10/2/704965/
2) Рішення РНБО України "Про забезпечення електронними комунікаційними послугами в умовах воєнного стану". URL: https://www.president.gov.ua/documents/8022022-45001
3) Збірник CXXXIII Міжнародної науково-практичної інтернет - конференції «Розвиток науки та техніки України під час воєнного стану», 3 листопада 2023 року, с 117.
4) Сенько А. О., Плінський В. В.. «Комутаційна мережа оператора зв'язку з оптимізацією енергонезалежного режиму роботи» КІСМ 2024, с33.
5) Куц В.Ю, Берест Р.Ю., “Проектування комп’ютерних мереж. Методичні вказівки до практичних занять”. К.: НТУУ «КПІ», 2012, с5.
6) Технічні характеристики маршрутизатору CCR2004-1G-12S+2XS. URL: https://mikrotik.com/product/ccr2004_1g_12s_2xs#fndtn-specifications
7) Технічні характеристики комутатору CRS326-24S+2Q+RM. URL: https://mikrotik.com/product/crs326_24s_2q_rm
8) Технічні характеристики серверу HP Z40. URL: https://www.cgchannel.com/2009/07/hp-z400-workstation-by-jason-lewis-2/2/#:~:text=At%20idle%2C%20the%20system%20drew,184%20watts%20from%20the%20wall.
9) Технічні характеристики оптичного-термінал BDCOM GP3600-16. URL: https://deps.ua/ua/katalog/concentrators-olt/46394.html
10) Інтерактивних графік часу роботи в залежності від складу комплексу резервного енергоживлення SMX3000HV. URL: https://www.se.com/ua/uk/products-runtime-graph/SMX3000HV/apc-smartups-x-%D0%BB%D1%96%D0%BD%D1%96%D0%B9%D0%BD%D0%BE%D1%96%D0%BD%D1%82%D0%B5%D1%80%D0%B0%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%B8%D0%B9-3-%D0%BA%D0%B2%D0%B0-%D1%81%D1%82%D1%96%D0%B9%D0%BA%D0%B0-%D0%B1%D0%B0%D1%88%D1%82%D0%B0-4u-208230-%D0%B2-8-%D1%80%D0%BE%D0%B7%D0%B5%D1%82%D0%BE%D0%BA-c13-2-%D1%80%D0%BE%D0%B7%D0%B5%D1%82%D0%BA%D0%B8-c19-iec-smartslot-%D0%BF%D0%BE%D0%B4%D0%BE%D0%B2%D0%B6%D0%B5%D0%BD%D0%B8%D0%B9-%D1%87%D0%B0%D1%81-%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D0%B8/

11) Купін А. І. , Чубаров В. А., Музика І. О., Кумченко Ю. О., Сенько А. О., Кузнєцов Д. І., “Проектування комп’ютерних систем та мереж”. Кривий Ріг, 2018.
12) Приходько С. І., Жученко О. С., Штомпель М. А., СколотаС. В., "Методичні вказівки до лабораторних, практичних занять і самостійної роботи з дисциплін «Телекомунікаційні та інформаційні мережі», «Телекомунікаційні та інформаційні мережі на залізничному транспорті», «Мережеві технології», «інтегральні цифрові мережі зв’язку». Харків 2018, с5.
13) Коваль Ю. В., СтавровськийА. Б., "Інформаційні мережі" Навчальний посібник. Київ, 2021, с-29.
14) Інтернет джерело. Основні характеристики протоколу PPPoE. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/pppoe
15) Киричек Г. Г., Семерюк Т.М., "Методичні вказівки до виконання лабораторних робіт з дисципліни "комп’ютерні мережі". Запоріжжя, 2014, с-4-9.
16) Документація Mikrotik RouterOS, розділ “Черги”. URL: https://help.mikrotik.com/docs/display/ROS/Queues
17) Інтернет джерело. “Що захищає мережевий екран”. URK: https://ko.paljnycia.cx.ua/articles/shho-zahishhae-mizhmerezhevij-ekran.html
18) Документація Mikrotik RouterOS, розділ “Файрволл”. URL https://help.mikrotik.com/docs/display/ROS/Firewall
19) Документація Mikrotik RouterOS пакет UserManager. URL: https://help.mikrotik.com/docs/spaces/ROS/pages/2555940/User+Manager
20) Офіційний сайт платформи корпоративної віртуалізації Proxmox. URL: https://www.proxmox.com/en/
21) Офіційний сайт білінгової системи MikBill. URL: https://mikbill.pro/
22) Офіційний сайт Pi-Hole. URL: https://pi-hole.net/
23) Официйний сайт Bind. URL: https://www.isc.org/bind/
24) Офіційний сайт LiteSpeed Web Server. URL: https://www.litespeedtech.com/
25) Технічні характеристики комутатора DGS-12-10-28. URL: https://comfy.ua/kommutator-lokal-noj-seti-switch-d-link-dgs-1210-28.html?gad_source=1&gclid=Cj0KCQjwxeyxBhC7ARIsAC7dS38IIZUmzX9vWuGVpVB6JA9FIO3gD6bX0D3B17M9D4ufdZ4C9zmg5BAaAmimEALw_wcB
26) Технічні характеристики оптичного терміналу C-DATA fd1608. URL: https://f.ua/ua/c-data/fd1604s-2ac.html?gad_source=1&gclid=Cj0KCQjwxeyxBhC7ARIsAC7dS38jYyQsKc2Gl_XHOv3EMVKCihdO52wi92i_R-lal3BD6eI-5oDGt78aAjK_EALw_wcB
27) Технічні характеристики головної станція кабельних модемів Teleste DAH100. URL: https://deps.ua/katalog/ru-golovnyie-stantsii/teleste-dah100.html
28) Технічні характеристики модульного шассі IP DSLAM D-Link DAS-4672. URL: https://elmir.ua/equipment_xdsl/modular_chassis_ip_dslam_d-link_das-4672.html#specs

29) Запорізький національний університет. Кореляційний аналіз. Лекція 7. URL: https://moodle.znu.edu.ua/pluginfile.php/425789/mod_resource/content/1/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%207.pdf
30) SPSS - пакет для статистичної обробки даних URL: https://www.ibm.com/spss
31) Шапочка М. К., Макарюк О. В. "Застосування експертних оцінок при прийнятті рішень за умов невизначеності". 2006 р, с142. URL: https://core.ac.uk/download/pdf/14035398.pdf
32) Опитування експертів для порівняння технологій доступу до мережі за різними параметрами. URL: https://forms.gle/TXAtQXdDivYWwohf6
33) Ковальчук В. К, Овчинніков К. А., Тесленко А. Ю., Методичка з проектування пасивних оптичних мереж Харьковский Національний Університет радиоэлектроники 2008р. ISSN 0485-8972 Радиотехніка. 2008. Вип. 155
34) Розрахунок оптичного бюджету втрат URL: https://ic-line.ua/wiki/7-raschjot-opticheskogo-byudzheta-poter
35) Дослідження DataReportal [Електронний ресурс] режим доступу: https://www.slovoidilo.ua/2024/04/15/infografika/suspilstvo/yak-povnomasshtabna-vijna-vidobrazylasya-kilkosti-internet-korystuvachiv-ukrayini
36) Дослідження Factum Group Ukraine [Електронний ресурс] режим доступу: https://inau.ua/sites/default/files/file/1801/iv_kvartal_2017.pdf
37) Купін А.І. , Чубаров В.А. , Музика І.О., Методичні рекомендації для підготовки випускової роботи магістрів за спец. 123 – «Комп'ютерна інженерія», 2023 р.

Додаток А

Лістинг налаштування маршрутизатору GATEWAY

```
[admin@Gateway] > export
# 2024-10-18 07:02:22 by RouterOS 7.16.1
# software id =
#
/interface bridge
add frame-types=admit-only-vlan-tagged name=bridge_local port-cost-mode=short
protocol-mode=none pvid=4093 vlan-filtering=yes
add name=localloop port-cost-mode=short protocol-mode=none
/interface ethernet
set [ find default-name=ether1 ] disable-running-check=no name=ether1_external_1
set [ find default-name=ether2 ] disable-running-check=no name=ether2_external_2
set [ find default-name=ether3 ] disable-running-check=no
name=ether3_internal_SW
set [ find default-name=ether4 ] disable-running-check=no name=ether4_BRAS_1
set [ find default-name=ether5 ] disable-running-check=no name=ether5_BRAS_2
set [ find default-name=ether6 ] disable-running-check=no
name=ether6_Virtual_server
set [ find default-name=ether7 ] disable-running-check=no
set [ find default-name=ether8 ] disable-running-check=no
set [ find default-name=ether9 ] disable-running-check=no
set [ find default-name=ether10 ] disable-running-check=no
set [ find default-name=ether11 ] disable-running-check=no
set [ find default-name=ether12 ] disable-running-check=no
set [ find default-name=ether13 ] disable-running-check=no
set [ find default-name=ether14 ] disable-running-check=no
set [ find default-name=ether15 ] disable-running-check=no
/interface vlan
add interface=bridge_local name=ext_NAT vlan-id=1203
add interface=bridge_local name=ext_services vlan-id=1200
add interface=bridge_local name=int_services vlan-id=1204
add interface=bridge_local name=managed vlan-id=1205
/disk
set slot1 media-interface=none media-sharing=no slot=slot1
set slot2 media-interface=none media-sharing=no slot=slot2
set slot3 media-interface=none media-sharing=no slot=slot3
set slot4 media-interface=none media-sharing=no slot=slot4
set slot5 media-interface=none media-sharing=no slot=slot5
set slot6 media-interface=none media-sharing=no slot=slot6
set slot7 media-interface=none media-sharing=no slot=slot7
set slot8 media-interface=none media-sharing=no slot=slot8
set slot9 media-interface=none media-sharing=no slot=slot9
```

```
set slot10 media-interface=none media-sharing=no slot=slot10
set slot11 media-interface=none media-sharing=no slot=slot11
set slot12 media-interface=none media-sharing=no slot=slot12
set slot13 media-interface=none media-sharing=no slot=slot13
set slot14 media-interface=none media-sharing=no slot=slot14
set slot15 media-interface=none media-sharing=no slot=slot15
set slot16 media-interface=none media-sharing=no slot=slot16
/interface list
add name=allow_admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=pool_managed ranges=10.9.16.10-10.9.16.254
/ip smb users
set [ find default=yes ] disabled=yes
/port
set 0 name=serial0
/routing bgp template
set default as=65432 disabled=no output.redistribute=connected router-id=100.92.0.3
routing-table=main
/routing ospf instance
add disabled=no name=10.9.8.1 originate-default=always
/routing ospf area
add disabled=no instance=10.9.8.1 name=backbone
/user-manager user group
add inner-auths=ttls-pap,ttls-chap,ttls-mschap1,ttls-mschap2,peap-mschap2
name=ordinary_client outer-auths=pap,chap,mschap1,mschap2,eap-tls,eap-ttls,eap-
peap,eap-mschap2
/user-manager user
add attributes=Mikrotik-Address-List:50M comment=client1 group=ordinary_client
name=user
add attributes=Mikrotik-Address-List:50M,Framed-IP-Address:100.100.94.5
comment=client1 group=ordinary_client name=user_stat
add attributes=Framed-Pool:pool-debtor comment=client1 group=ordinary_client
name=debtor
/interface bridge port
add bridge=bridge_local frame-types=admit-only-vlan-tagged
interface=ether3_internal_SW internal-path-cost=10 path-cost=10 pvid=4093
add bridge=bridge_local interface=ether4_BRAS_1 internal-path-cost=10 path-
cost=10 pvid=4093
add bridge=bridge_local interface=ether5_BRAS_2 internal-path-cost=10 path-
cost=10 pvid=4093
add bridge=bridge_local interface=ether6_Virtual_server internal-path-cost=10 path-
cost=10
```

```
/ip firewall connection tracking
set udp-timeout=10s
/ip neighbor discovery-settings
set discover-interface-list=allow_admin
/ip settings
set max-neighbor-entries=2048
/ipv6 settings
set max-neighbor-entries=7168
/interface bridge vlan
add bridge=bridge_local
tagged=bridge_local,ether3_internal_SW,ether4_BRAS_1,ether5_BRAS_2,ether6_V
irtual_server vlan-ids=1200
add bridge=bridge_local
tagged=bridge_local,ether3_internal_SW,ether4_BRAS_1,ether5_BRAS_2 vlan-
ids=1203
add bridge=bridge_local
tagged=bridge_local,ether3_internal_SW,ether6_Virtual_server vlan-ids=1204
add bridge=bridge_local
tagged=bridge_local,ether3_internal_SW,ether6_Virtual_server vlan-ids=1205
/interface list member
add interface=int_services list=allow_admin
add interface=managed list=allow_admin
/interface ovpn-server server
set auth=sha1,md5
/ip address
add address=100.90.80.2/30 interface=ether1_external_1 network=100.90.80.0
add address=100.100.92.3/27 interface=ext_services network=100.100.92.0
add address=10.9.8.1/22 disabled=yes interface=int_services network=10.9.8.0
add address=100.100.92.0/22 interface=localloop network=100.100.92.0
add address=10.9.16.1/24 interface=managed network=10.9.16.0
add address=100.100.92.129/25 interface=ext_NAT network=100.100.92.128
add address=100.80.60.2/30 interface=ether2_external_2 network=100.80.60.0
add address=10.9.8.5/22 interface=int_services network=10.9.8.0
/ip dns
set servers=8.8.8.8,1.1.1.1
/ip firewall address-list
add address=10.9.8.0/22 list=allow_admin
add address=10.9.16.0/24 list=allow_admin
add address=100.90.80.1 list=bgp_neighbours
add address=100.80.60.1 list=bgp_neighbours
add address=10.9.16.0/24 list=managed_network
add address=100.100.92.0/27 list=OSPF_in
add address=192.168.122.0/24 list=allow_admin
/ip firewall filter
```

```
add action=accept chain=input comment="established, releated" connection-
state=established,related
add action=accept chain=forward connection-state=established,related
add action=accept chain=input comment=allow_ping protocol=icmp
add action=accept chain=input comment="allow bgp input for peers" dst-port=179
protocol=tcp src-address-list=bgp_neighbours
add action=accept chain=input comment=allow_OSPF in-interface=ext_services
protocol=ospf src-address-list=OSPF_in
add action=add-src-to-address-list address-list=blocked-addr address-list-timeout=1d
chain=input comment="DDOS protect" connection-limit=50,32 protocol=tcp src-
address-list=!operators_addresses
add action=tarpit chain=input comment="DDOS protect" connection-limit=3,32
protocol=tcp src-address-list=blocked-addr
add action=drop chain=forward comment="DDOS forward protection" connection-
state=new dst-address-list=ddosed src-address-list=ddoser
add action=jump chain=forward comment="DDOS forward protection" connection-
state=new jump-target=detect-ddos
add action=return chain=detect-ddos comment="DDOS forward allow stat_ip" src-
address-list=stat_ip_clients
add action=return chain=detect-ddos comment="DDOS forward allow local" dst-
address-list=operators_addresses src-address-list=operators_addresses
add action=return chain=detect-ddos comment="DDOS forward protection" dst-
limit=500,500,src-and-dst-addresses/10s
add action=return chain=detect-ddos comment="DDOS forward protection"
limit=400,5:packet protocol=tcp tcp-flags=syn
add action=add-dst-to-address-list address-list=ddosed address-list-timeout=1d
chain=detect-ddos comment="DDOS forward protection"
add action=add-src-to-address-list address-list=ddoser address-list-timeout=1d
chain=detect-ddos comment="DDOS forward protection"
add action=drop chain=input disabled=yes src-address-list=!allow_admin
add action=drop chain=input connection-state=invalid
add action=drop chain=forward connection-nat-state=!dstnat connection-state=new
dst-address-list=stat_ip_clients
add action=drop chain=forward connection-state=invalid
add action=drop chain=forward comment=drop_abon_to_stuff_network dst-address-
list=allow_admin src-address-list=operators_addresses
/ip firewall nat
add action=masquerade chain=srcnat comment="masquarade managed network" src-
address-list=managed_network
/ip ipsec profile
set [ find default=yes ] dpd-interval=2m dpd-maximum-failures=5
/ip service
set telnet disabled=yes
set ftp disabled=yes
```

```
set www disabled=yes
set ssh disabled=yes
set api disabled=yes
set winbox address=10.9.8.0/22,10.9.16.0/24,192.168.122.0/24
set api-ssl disabled=yes
/ip smb shares
set [ find default=yes ] directory=/pub
/radius incoming
set accept=yes
/routing bgp connection
add as=65432 disabled=no input.filter=bgp_in_1 local.role=ebgp name=bgp_peer_1
output.filter-chain=bgp_out_1 remote.address=100.90.80.1/32 .as=64534 router-
id=100.100.92.3 routing-table=main templates=default
add as=65432 disabled=no input.filter=bgp_in_2 local.role=ebgp name=bgp_peer_2
output.filter-chain=bgp_out_1 .redistribute=connected
remote.address=100.80.60.1/32 .as=64758 router-id=100.100.92.3 routing-
table=main templates=default
/routing filter rule
add chain=bgp_out_1 disabled=no rule="if (dst == 100.100.92.0/22) { accept; }"
add chain=bgp_in_1 disabled=no rule="if (dst == 0.0.0.0/0) { set distance +200; set
bgp-local-pref 200; accept; }"
add chain=bgp_in_2 disabled=no rule="if (dst == 0.0.0.0/0) { set distance +210; set
bgp-local-pref 199; accept; }"
/routing ospf interface-template
add area=backbone disabled=no interfaces=ext_services networks=100.100.92.0/27
/system identity
set name=Gateway
/system note
set show-at-login=no
/system ntp client
set enabled=yes
/system ntp server
set enabled=yes
/system ntp client servers
add address=time.google.com
add address=clock.nyc.he.net
/tool mac-server
set allowed-interface-list=none
/tool mac-server mac-winbox
set allowed-interface-list=allow_admin
/user-manager
set certificate=*0 enabled=yes require-message-auth=no
/user-manager router
add address=10.9.8.2 name=NAS_1
```

```
add address=10.9.8.3 name=NAS_2
```

Додаток Б

Лістинг налаштування маршрутизатору NAS_1

```
[admin@NAS_1] > export
# 2024-10-18 10:10:03 by RouterOS 7.16.1
# software id =
#
/interface bridge
add name=local_loop port-cost-mode=short protocol-mode=none
/interface ethernet
set [ find default-name=ether1 ] disable-running-check=no name=ether1_external
set [ find default-name=ether2 ] disable-running-check=no name=ether2_internal
/interface vlan
add interface=ether1_external name=ext_NAT vlan-id=1203
add interface=ether1_external name=ext_services vlan-id=1200
add interface=ether2_internal name=int_services vlan-id=1204
add interface=ether2_internal name=local_00 vlan-id=1000
add interface=ether2_internal name=local_01 vlan-id=1001
add interface=ether2_internal name=local_02 vlan-id=1002
add interface=ether2_internal name=local_03 vlan-id=1003
add interface=ether2_internal name=local_04 vlan-id=1004
add interface=ether2_internal name=local_05 vlan-id=1005
add interface=ether2_internal name=local_06 vlan-id=1006
add interface=ether2_internal name=local_07 vlan-id=1007
add interface=ether2_internal name=local_08 vlan-id=1008
add interface=ether2_internal name=local_09 vlan-id=1009
add interface=ether2_internal name=local_10 vlan-id=1010
add interface=ether2_internal name=local_11 vlan-id=1011
add interface=ether2_internal name=local_12 vlan-id=1012
add interface=ether2_internal name=local_13 vlan-id=1013
add interface=ether2_internal name=local_14 vlan-id=1014
add interface=ether2_internal name=local_15 vlan-id=1015
add interface=ether2_internal name=local_16 vlan-id=1016
add interface=ether2_internal name=local_17 vlan-id=1017
add interface=ether2_internal name=local_18 vlan-id=1018
add interface=ether2_internal name=local_19 vlan-id=1019
add interface=ether2_internal name=local_20 vlan-id=1020
add interface=ether2_internal name=local_21 vlan-id=1021
add interface=ether2_internal name=local_22 vlan-id=1022
add interface=ether2_internal name=local_23 vlan-id=1023
add interface=ether2_internal name=local_24 vlan-id=1024
add interface=ether2_internal name=local_25 vlan-id=1025
add interface=ether2_internal name=local_26 vlan-id=1026
add interface=ether2_internal name=local_27 vlan-id=1027
```

```
add interface=ether2_internal name=local_28 vlan-id=1028
add interface=ether2_internal name=local_29 vlan-id=1029
add interface=ether2_internal name=local_30 vlan-id=1030
add interface=ether2_internal name=local_31 vlan-id=1031
/disk
set slot1 media-interface=none media-sharing=no slot=slot1
set slot2 media-interface=none media-sharing=no slot=slot2
set slot3 media-interface=none media-sharing=no slot=slot3
set slot4 media-interface=none media-sharing=no slot=slot4
set slot5 media-interface=none media-sharing=no slot=slot5
set slot6 media-interface=none media-sharing=no slot=slot6
set slot7 media-interface=none media-sharing=no slot=slot7
set slot8 media-interface=none media-sharing=no slot=slot8
set slot9 media-interface=none media-sharing=no slot=slot9
set slot10 media-interface=none media-sharing=no slot=slot10
set slot11 media-interface=none media-sharing=no slot=slot11
set slot12 media-interface=none media-sharing=no slot=slot12
set slot13 media-interface=none media-sharing=no slot=slot13
set slot14 media-interface=none media-sharing=no slot=slot14
/interface list
add name=allow_admin
add name=WAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=pool_pppoe ranges=10.11.0.1-10.11.15.254
add name=pool_debtor ranges=10.12.0.1-10.12.15.254
add name=pool_local_00 ranges=10.10.0.10-10.10.0.254
add name=pool_local_01 ranges=10.10.1.0-10.10.1.254
add name=pool_local_02 ranges=10.10.2.0-10.10.2.254
add name=pool_local_03 ranges=10.10.3.0-10.10.3.254
add name=pool_local_04 ranges=10.10.4.0-10.10.4.254
add name=pool_local_05 ranges=10.10.5.0-10.10.5.254
add name=pool_local_06 ranges=10.10.6.0-10.10.6.254
add name=pool_local_07 ranges=10.10.7.0-10.10.7.254
add name=pool_local_08 ranges=10.10.8.0-10.10.8.254
add name=pool_local_09 ranges=10.10.9.0-10.10.9.254
add name=pool_local_10 ranges=10.10.10.0-10.10.10.254
add name=pool_local_11 ranges=10.10.11.0-10.10.11.254
add name=pool_local_12 ranges=10.10.12.0-10.10.12.254
add name=pool_local_13 ranges=10.10.13.0-10.10.13.254
add name=pool_local_14 ranges=10.10.14.0-10.10.14.254
add name=pool_local_15 ranges=10.10.15.0-10.10.15.254
add name=pool_local_16 ranges=10.10.16.0-10.10.16.254
```

```
add name=pool_local_17 ranges=10.10.17.0-10.10.17.254
add name=pool_local_18 ranges=10.10.18.0-10.10.18.254
add name=pool_local_19 ranges=10.10.19.0-10.10.19.254
add name=pool_local_20 ranges=10.10.20.0-10.10.20.254
add name=pool_local_21 ranges=10.10.21.0-10.10.21.254
add name=pool_local_22 ranges=10.10.22.0-10.10.22.254
add name=pool_local_23 ranges=10.10.23.0-10.10.23.254
add name=pool_local_24 ranges=10.10.24.0-10.10.24.254
add name=pool_local_25 ranges=10.10.25.0-10.10.25.254
add name=pool_local_26 ranges=10.10.26.0-10.10.26.254
add name=pool_local_27 ranges=10.10.27.0-10.10.27.254
add name=pool_local_28 ranges=10.10.28.0-10.10.28.254
add name=pool_local_29 ranges=10.10.29.0-10.10.29.254
add name=pool_local_30 ranges=10.10.30.0-10.10.30.254
add name=pool_local_31 ranges=10.10.31.0-10.10.31.254
/ip smb users
set [ find default=yes ] disabled=yes
/port
set 0 name=serial0
/ppp profile
add change-tcp-mss=yes dns-server=100.100.92.4 local-address=100.100.92.33
name=PPPoE_prifile only-one=yes remote-address=pool_pppoe use-ipv6=no
/queue type
add kind=pcq name=50M_in pcq-burst-rate=100M pcq-burst-threshold=50M pcq-
burst-time=10m10s pcq-classifier=dst-address pcq-rate=52M
add kind=pcq name=50M_out pcq-burst-rate=100M pcq-burst-threshold=50M pcq-
burst-time=10m10s pcq-classifier=src-address pcq-rate=52M
add kind=pcq name=200M_out pcq-burst-rate=500M pcq-burst-threshold=200M
pcq-burst-time=10m10s pcq-classifier=src-address pcq-rate=210M
add kind=pcq name=200M_in pcq-burst-rate=500M pcq-burst-threshold=200M pcq-
burst-time=10m10s pcq-classifier=dst-address pcq-rate=210M
add kind=pcq name=debtor_in pcq-classifier=dst-address pcq-rate=1M
add kind=pcq name=debtor_out pcq-classifier=src-address pcq-rate=1M
/queue interface
set ether1_external queue=ethernet-default
set ether2_internal queue=ethernet-default
/queue tree
add name=Common_in parent=global queue=default
add name=Common_out parent=global queue=default
add name=50M_in packet-mark=50M_in_mark parent=Common_in queue=50M_in
add name=50M_out packet-mark=50M_out_mark parent=Common_out
queue=50M_out
add name=200M_in packet-mark=200M_in_mark parent=Common_in
queue=200M_in
```

```
add name=200M_out packet-mark=200M_out_mark parent=Common_out
queue=200M_out
add name=debtor_in packet-mark=pool_debtor_in_mark parent=Common_in
queue=debtor_in
add name=debtor_out packet-mark=pool_debtor_out_mark parent=Common_out
queue=debtor_out
/routing ospf instance
add disabled=no name=NAS_1 out-filter-chain=ospf_out router-id=100.100.92.1
/routing ospf area
add disabled=no instance=NAS_1 name=backbone
add area-id=10.10.0.0 disabled=no instance=NAS_1 name=local_dhcp type=stub
add area-id=10.11.0.0 disabled=no instance=NAS_1 name=local_pppoe type=stub
add area-id=10.12.0.0 disabled=no instance=NAS_1 name=local_debtor type=stub
add area-id=100.100.94.0 default-cost=1 disabled=no instance=NAS_1
name=stat_ip_ppooe no-summaries nssa-translator=candidate type=stub
/ip firewall connection tracking
set udp-timeout=10s
/ip neighbor discovery-settings
set discover-interface-list=allow_admin
/ip settings
set max-neighbor-entries=14336
/ipv6 settings
set max-neighbor-entries=7168
/interface list member
add interface=int_services list=allow_admin
add interface=ext_NAT list=WAN
add interface=ext_services list=WAN
/interface pppoe-server server
add authentication=pap,chap default-profile=PPPoE_prifile disabled=no
interface=local_00 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_01 one-session-per-
host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_02 one-session-per-
host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_03 one-session-per-
host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_04 one-session-per-
host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_05 one-session-per-
host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_06 one-session-per-
host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_07 one-session-per-
host=yes service-name=operator
```

```
add default-profile=PPPoE_prifile disabled=no interface=local_08 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_09 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_10 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_11 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_12 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_13 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_14 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_15 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_16 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_17 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_18 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_19 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_20 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_21 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_22 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_23 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_24 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_25 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_26 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_27 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_28 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_29 one-session-per-host=yes service-name=operator
```

```
add default-profile=PPPoE_prifile disabled=no interface=local_30 one-session-per-host=yes service-name=operator
add default-profile=PPPoE_prifile disabled=no interface=local_31 one-session-per-host=yes service-name=operator
/ip address
add address=10.9.8.2/22 interface=int_services network=10.9.8.0
add address=10.10.0.1/24 interface=local_00 network=10.10.0.0
add address=10.10.1.1/24 interface=local_01 network=10.10.1.0
add address=10.10.2.1/24 interface=local_02 network=10.10.2.0
add address=10.10.3.1/24 interface=local_03 network=10.10.3.0
add address=10.10.4.1/24 interface=local_04 network=10.10.4.0
add address=10.10.5.1/24 interface=local_05 network=10.10.5.0
add address=10.10.6.1/24 interface=local_06 network=10.10.6.0
add address=10.10.7.1/24 interface=local_07 network=10.10.7.0
add address=10.10.8.1/24 interface=local_08 network=10.10.8.0
add address=10.10.9.1/24 interface=local_09 network=10.10.9.0
add address=10.10.10.1/24 interface=local_10 network=10.10.10.0
add address=10.10.11.1/24 interface=local_11 network=10.10.11.0
add address=10.10.12.1/24 interface=local_12 network=10.10.12.0
add address=10.10.13.1/24 interface=local_13 network=10.10.13.0
add address=10.10.14.1/24 interface=local_14 network=10.10.14.0
add address=10.10.15.1/24 interface=local_15 network=10.10.15.0
add address=10.10.16.1/24 interface=local_16 network=10.10.16.0
add address=10.10.17.1/24 interface=local_17 network=10.10.17.0
add address=10.10.18.1/24 interface=local_18 network=10.10.18.0
add address=10.10.19.1/24 interface=local_19 network=10.10.19.0
add address=10.10.20.1/24 interface=local_20 network=10.10.20.0
add address=10.10.21.1/24 interface=local_21 network=10.10.21.0
add address=10.10.22.1/24 interface=local_22 network=10.10.22.0
add address=10.10.23.1/24 interface=local_23 network=10.10.23.0
add address=10.10.24.1/24 interface=local_24 network=10.10.24.0
add address=10.10.25.1/24 interface=local_25 network=10.10.25.0
add address=10.10.26.1/24 interface=local_26 network=10.10.26.0
add address=10.10.27.1/24 interface=local_27 network=10.10.27.0
add address=10.10.28.1/24 interface=local_28 network=10.10.28.0
add address=10.10.29.1/24 interface=local_29 network=10.10.29.0
add address=10.10.30.1/24 interface=local_30 network=10.10.30.0
add address=10.10.31.1/24 interface=local_31 network=10.10.31.0
add address=100.100.92.1/27 interface=ext_services network=100.100.92.0
add address=100.100.92.130/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.33 interface=local_loop network=100.100.92.33
add address=100.100.92.131/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.132/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.133/25 interface=ext_NAT network=100.100.92.128
```

add address=100.100.92.134/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.135/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.136/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.137/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.138/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.139/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.140/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.141/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.142/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.143/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.144/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.145/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.146/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.147/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.148/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.149/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.150/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.151/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.152/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.153/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.154/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.155/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.156/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.157/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.158/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.159/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.160/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.161/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.162/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.163/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.164/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.165/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.166/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.167/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.168/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.169/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.170/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.171/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.172/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.173/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.174/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.175/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.176/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.177/25 interface=ext_NAT network=100.100.92.128

```
add address=100.100.92.178/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.179/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.180/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.181/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.182/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.183/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.184/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.185/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.186/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.187/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.188/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.189/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.190/25 interface=ext_NAT network=100.100.92.128
add address=100.100.92.191/25 interface=ext_NAT network=100.100.92.128
add address=10.11.0.0/20 interface=local_loop network=10.11.0.0
add address=10.12.0.0/20 interface=local_loop network=10.12.0.0
/ip dhcp-server
add add-arp=yes address-pool=pool_local_00 interface=local_00 lease-time=2m
name=DHCP_vlan_1000
add add-arp=yes address-pool=pool_local_01 interface=local_01 lease-time=2m
name=DHCP_vlan_1001
add add-arp=yes address-pool=pool_local_02 interface=local_02 lease-time=2m
name=DHCP_vlan_1002
add add-arp=yes address-pool=pool_local_03 interface=local_03 lease-time=2m
name=DHCP_vlan_1003
add add-arp=yes address-pool=pool_local_04 interface=local_04 lease-time=2m
name=DHCP_vlan_1004
add add-arp=yes address-pool=pool_local_05 interface=local_05 lease-time=2m
name=DHCP_vlan_1005
add add-arp=yes address-pool=pool_local_06 interface=local_06 lease-time=2m
name=DHCP_vlan_1006
add add-arp=yes address-pool=pool_local_07 interface=local_07 lease-time=2m
name=DHCP_vlan_1007
add add-arp=yes address-pool=pool_local_08 interface=local_08 lease-time=2m
name=DHCP_vlan_1008
add add-arp=yes address-pool=pool_local_09 interface=local_09 lease-time=2m
name=DHCP_vlan_1009
add add-arp=yes address-pool=pool_local_10 interface=local_10 lease-time=2m
name=DHCP_vlan_1010
add add-arp=yes address-pool=pool_local_11 interface=local_11 lease-time=2m
name=DHCP_vlan_1011
add add-arp=yes address-pool=pool_local_12 interface=local_12 lease-time=2m
name=DHCP_vlan_1012
```

```
add add-arp=yes address-pool=pool_local_13 interface=local_13 lease-time=2m
name=DHCP_vlan_1013
add add-arp=yes address-pool=pool_local_14 interface=local_14 lease-time=2m
name=DHCP_vlan_1014
add add-arp=yes address-pool=pool_local_15 interface=local_15 lease-time=2m
name=DHCP_vlan_1015
add add-arp=yes address-pool=pool_local_16 interface=local_16 lease-time=2m
name=DHCP_vlan_1016
add add-arp=yes address-pool=pool_local_17 interface=local_17 lease-time=2m
name=DHCP_vlan_1017
add add-arp=yes address-pool=pool_local_18 interface=local_18 lease-time=2m
name=DHCP_vlan_1018
add add-arp=yes address-pool=pool_local_19 interface=local_19 lease-time=2m
name=DHCP_vlan_1019
add add-arp=yes address-pool=pool_local_20 interface=local_20 lease-time=2m
name=DHCP_vlan_1020
add add-arp=yes address-pool=pool_local_21 interface=local_21 lease-time=2m
name=DHCP_vlan_1021
add add-arp=yes address-pool=pool_local_22 interface=local_22 lease-time=2m
name=DHCP_vlan_1022
add add-arp=yes address-pool=pool_local_23 interface=local_23 lease-time=2m
name=DHCP_vlan_1023
add add-arp=yes address-pool=pool_local_24 interface=local_24 lease-time=2m
name=DHCP_vlan_1024
add add-arp=yes address-pool=pool_local_25 interface=local_25 lease-time=2m
name=DHCP_vlan_1025
add add-arp=yes address-pool=pool_local_26 interface=local_26 lease-time=2m
name=DHCP_vlan_1026
add add-arp=yes address-pool=pool_local_27 interface=local_27 lease-time=2m
name=DHCP_vlan_1027
add add-arp=yes address-pool=pool_local_28 interface=local_28 lease-time=2m
name=DHCP_vlan_1028
add add-arp=yes address-pool=pool_local_29 interface=local_29 lease-time=2m
name=DHCP_vlan_1029
add add-arp=yes address-pool=pool_local_30 interface=local_30 lease-time=2m
name=DHCP_vlan_1030
add add-arp=yes address-pool=pool_local_31 interface=local_31 lease-time=2m
name=DHCP_vlan_1031
/ip dhcp-server config
set store-leases-disk=never
/ip dhcp-server network
add address=10.10.0.0/24 dns-server=100.100.92.4 gateway=10.10.0.1
add address=10.10.1.0/24 dns-server=100.100.92.4 gateway=10.10.1.1
add address=10.10.2.0/24 dns-server=100.100.92.4 gateway=10.10.2.1
```

```
add address=10.10.3.0/24 dns-server=100.100.92.4 gateway=10.10.3.1
add address=10.10.4.0/24 dns-server=100.100.92.4 gateway=10.10.4.1
add address=10.10.5.0/24 dns-server=100.100.92.4 gateway=10.10.5.1
add address=10.10.6.0/24 dns-server=100.100.92.4 gateway=10.10.6.1
add address=10.10.7.0/24 dns-server=100.100.92.4 gateway=10.10.7.1
add address=10.10.8.0/24 dns-server=100.100.92.4 gateway=10.10.8.1
add address=10.10.9.0/24 dns-server=100.100.92.4 gateway=10.10.9.1
add address=10.10.10.0/24 dns-server=100.100.92.4 gateway=10.10.10.1
add address=10.10.11.0/24 dns-server=100.100.92.4 gateway=10.10.11.1
add address=10.10.12.0/24 dns-server=100.100.92.4 gateway=10.10.12.1
add address=10.10.13.0/24 dns-server=100.100.92.4 gateway=10.10.13.1
add address=10.10.14.0/24 dns-server=100.100.92.4 gateway=10.10.14.1
add address=10.10.15.0/24 dns-server=100.100.92.4 gateway=10.10.15.1
add address=10.10.16.0/24 dns-server=100.100.92.4 gateway=10.10.16.1
add address=10.10.17.0/24 dns-server=100.100.92.4 gateway=10.10.17.1
add address=10.10.18.0/24 dns-server=100.100.92.4 gateway=10.10.18.1
add address=10.10.19.0/24 dns-server=100.100.92.4 gateway=10.10.19.1
add address=10.10.20.0/24 dns-server=100.100.92.4 gateway=10.10.20.1
add address=10.10.21.0/24 dns-server=100.100.92.4 gateway=10.10.21.1
add address=10.10.22.0/24 dns-server=100.100.92.4 gateway=10.10.22.1
add address=10.10.23.0/24 dns-server=100.100.92.4 gateway=10.10.23.1
add address=10.10.24.0/24 dns-server=100.100.92.4 gateway=10.10.24.1
add address=10.10.25.0/24 dns-server=100.100.92.4 gateway=10.10.25.1
add address=10.10.26.0/24 dns-server=100.100.92.4 gateway=10.10.26.1
add address=10.10.27.0/24 dns-server=100.100.92.4 gateway=10.10.27.1
add address=10.10.28.0/24 dns-server=100.100.92.4 gateway=10.10.28.1
add address=10.10.29.0/24 dns-server=100.100.92.4 gateway=10.10.29.1
add address=10.10.30.0/24 dns-server=100.100.92.4 gateway=10.10.30.1
add address=10.10.31.0/24 dns-server=100.100.92.4 gateway=10.10.31.1
/ip dns
set servers=1.1.1.1,8.8.8.8
/ip firewall address-list
add address=10.9.16.0/24 list=allow_admin
add address=100.100.92.0/27 list=OSPF_in
add address=100.100.92.0/22 list=operators_addresses
add address=10.10.0.0/20 list=operators_addresses
add address=10.11.0.0/20 list=operators_addresses
add address=10.12.0.0/20 list=operators_addresses
add address=10.12.96.0/20 list=operators_addresses
add address=10.11.96.0/20 list=operators_addresses
add address=10.10.96.0/20 list=operators_addresses
add address=10.9.8.0/22 list=allow_admin
add address=192.168.122.0/24 list=allow_admin
add address=100.100.94.0/24 list=stat_ip_clients
```

```
add address=100.100.95.0/24 list=stat_ip_clients
/ip firewall filter
add action=accept chain=input comment="established, releated" connection-
state=established,related
add action=accept chain=forward connection-state=established,related
add action=accept chain=input comment="allow ping" protocol=icmp
add action=accept chain=input comment=allow_ospf in-interface=ext_services
protocol=ospf
add action=add-src-to-address-list address-list=bad_guy address-list-timeout=1d
chain=input comment=trap_for_a_bad_guy in-interface-list=WAN protocol=tcp
psd=21,3s,3,1 src-address-list=!allow_admin
add action=add-src-to-address-list address-list=bad_guy address-list-timeout=1d
chain=input comment=trap_for_a_bad_guy dst-port=22,23,3389 in-interface-
list=WAN protocol=tcp src-address-list=!allow_admin
add action=add-src-to-address-list address-list=bad_guy address-list-timeout=1d
chain=input comment=trap_for_a_bad_guy dst-port=5060,5061,5062,9060,4695 in-
interface-list=WAN protocol=udp src-address-list=!allow_admin
add action=add-src-to-address-list address-list=blocked-addr address-list-timeout=1d
chain=input comment="DDOS protect" connection-limit=50,32 protocol=tcp src-
address-list=!operators_addresses
add action=tarpit chain=input comment="DDOS protect" connection-limit=3,32
protocol=tcp src-address-list=blocked-addr
add action=drop chain=forward comment="DDOS forward protection" connection-
state=new dst-address-list=ddosed src-address-list=ddoser
add action=jump chain=forward comment="DDOS forward protection" connection-
state=new jump-target=detect-ddos
add action=return chain=detect-ddos comment="DDOS forward allow stat_ip" src-
address-list=stat_ip_clients
add action=return chain=detect-ddos comment="DDOS forward allow operators to
operators" dst-address-list=operators_addresses src-address-list=operators_addresses
add action=return chain=detect-ddos comment="DDOS forward protection" dst-
limit=500,500,src-and-dst-addresses/10s
add action=return chain=detect-ddos comment="DDOS forward protection"
limit=400,5:packet protocol=tcp tcp-flags=syn
add action=add-dst-to-address-list address-list=ddosed address-list-timeout=1d
chain=detect-ddos comment="DDOS forward protection"
add action=add-src-to-address-list address-list=ddoser address-list-timeout=1d
chain=detect-ddos comment="DDOS forward protection"
add action=drop chain=input disabled=yes src-address-list=!allow_admin
add action=drop chain=input connection-state=invalid
add action=drop chain=forward connection-nat-state=!dstnat connection-state=new
dst-address-list=stat_ip_clients
add action=drop chain=forward connection-state=invalid
```

```
add action=drop chain=forward comment=drop_abon_to_stuff_network dst-address-
list=allow_admin src-address-list=operators_addresses
/ip firewall mangle
add action=mark-packet chain=forward dst-address-list=50M new-packet-
mark=50M_in_mark passthrough=no
add action=mark-packet chain=forward new-packet-mark=50M_out_mark
passthrough=no src-address-list=50M
# inactive time
add action=mark-packet chain=forward dst-address-list=200M new-packet-
mark=200M_in_mark passthrough=no time=19h-23h,sun,mon,tue,wed,thu,fri,sat
# inactive time
add action=mark-packet chain=forward new-packet-mark=200M_out_mark
passthrough=no src-address-list=200M time=19h-23h,sun,mon,tue,wed,thu,fri,sat
add action=mark-packet chain=forward dst-address-list=pool_debtor new-packet-
mark=pool_debtor_in_mark passthrough=no
add action=mark-packet chain=forward new-packet-mark=pool_debtor_out_mark
passthrough=no src-address-list=pool_debtor
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ext_services src-
address=10.12.0.0/20
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/0 src-
address=10.11.0.0/20 to-addresses=100.100.92.130
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/1 src-
address=10.11.0.0/20 to-addresses=100.100.92.131
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/2 src-
address=10.11.0.0/20 to-addresses=100.100.92.132
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/3 src-
address=10.11.0.0/20 to-addresses=100.100.92.133
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/4 src-
address=10.11.0.0/20 to-addresses=100.100.92.134
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/5 src-
address=10.11.0.0/20 to-addresses=100.100.92.135
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/6 src-
address=10.11.0.0/20 to-addresses=100.100.92.136
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/7 src-
address=10.11.0.0/20 to-addresses=100.100.92.137
```

```
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/8 src-
address=10.11.0.0/20 to-addresses=100.100.92.138
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/9 src-
address=10.11.0.0/20 to-addresses=100.100.92.139
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/10 src-
address=10.11.0.0/20 to-addresses=100.100.92.140
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/11 src-
address=10.11.0.0/20 to-addresses=100.100.92.141
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/12 src-
address=10.11.0.0/20 to-addresses=100.100.92.142
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/13 src-
address=10.11.0.0/20 to-addresses=100.100.92.143
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/14 src-
address=10.11.0.0/20 to-addresses=100.100.92.144
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/15 src-
address=10.11.0.0/20 to-addresses=100.100.92.145
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/16 src-
address=10.11.0.0/20 to-addresses=100.100.92.146
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/17 src-
address=10.11.0.0/20 to-addresses=100.100.92.147
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/18 src-
address=10.11.0.0/20 to-addresses=100.100.92.148
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/19 src-
address=10.11.0.0/20 to-addresses=100.100.92.149
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/20 src-
address=10.11.0.0/20 to-addresses=100.100.92.150
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/21 src-
address=10.11.0.0/20 to-addresses=100.100.92.151
```

```
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/22 src-
address=10.11.0.0/20 to-addresses=100.100.92.152
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/23 src-
address=10.11.0.0/20 to-addresses=100.100.92.153
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/24 src-
address=10.11.0.0/20 to-addresses=100.100.92.154
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/25 src-
address=10.11.0.0/20 to-addresses=100.100.92.155
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/26 src-
address=10.11.0.0/20 to-addresses=100.100.92.156
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/27 src-
address=10.11.0.0/20 to-addresses=100.100.92.157
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/28 src-
address=10.11.0.0/20 to-addresses=100.100.92.158
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/29 src-
address=10.11.0.0/20 to-addresses=100.100.92.159
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/30 src-
address=10.11.0.0/20 to-addresses=100.100.92.160
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/31 src-
address=10.11.0.0/20 to-addresses=100.100.92.161
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/32 src-
address=10.11.0.0/20 to-addresses=100.100.92.162
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/33 src-
address=10.11.0.0/20 to-addresses=100.100.92.163
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/34 src-
address=10.11.0.0/20 to-addresses=100.100.92.164
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/35 src-
address=10.11.0.0/20 to-addresses=100.100.92.165
```

```
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/36 src-
address=10.11.0.0/20 to-addresses=100.100.92.166
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/37 src-
address=10.11.0.0/20 to-addresses=100.100.92.167
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/38 src-
address=10.11.0.0/20 to-addresses=100.100.92.168
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/39 src-
address=10.11.0.0/20 to-addresses=100.100.92.169
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/40 src-
address=10.11.0.0/20 to-addresses=100.100.92.170
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/41 src-
address=10.11.0.0/20 to-addresses=100.100.92.171
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/42 src-
address=10.11.0.0/20 to-addresses=100.100.92.172
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/43 src-
address=10.11.0.0/20 to-addresses=100.100.92.173
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/44 src-
address=10.11.0.0/20 to-addresses=100.100.92.174
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/45 src-
address=10.11.0.0/20 to-addresses=100.100.92.175
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/46 src-
address=10.11.0.0/20 to-addresses=100.100.92.176
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/47 src-
address=10.11.0.0/20 to-addresses=100.100.92.177
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/48 src-
address=10.11.0.0/20 to-addresses=100.100.92.178
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/49 src-
address=10.11.0.0/20 to-addresses=100.100.92.179
```

```
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/50 src-
address=10.11.0.0/20 to-addresses=100.100.92.180
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/51 src-
address=10.11.0.0/20 to-addresses=100.100.92.181
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/52 src-
address=10.11.0.0/20 to-addresses=100.100.92.182
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/53 src-
address=10.11.0.0/20 to-addresses=100.100.92.183
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/54 src-
address=10.11.0.0/20 to-addresses=100.100.92.184
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/55 src-
address=10.11.0.0/20 to-addresses=100.100.92.185
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/56 src-
address=10.11.0.0/20 to-addresses=100.100.92.186
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/57 src-
address=10.11.0.0/20 to-addresses=100.100.92.187
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/58 src-
address=10.11.0.0/20 to-addresses=100.100.92.188
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/59 src-
address=10.11.0.0/20 to-addresses=100.100.92.189
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/60 src-
address=10.11.0.0/20 to-addresses=100.100.92.190
add action=src-nat chain=srcnat comment=nat_for_pppoe_users dst-address-
list=!operators_addresses per-connection-classifier=src-address:62/61 src-
address=10.11.0.0/20 to-addresses=100.100.92.191
/ip firewall raw
add action=drop chain=prerouting in-interface-list=WAN src-address-list=bad_guy
/ip ipsec profile
set [ find default=yes ] dpd-interval=2m dpd-maximum-failures=5
/ip route
add blackhole disabled=yes distance=254 dst-address=10.0.0.0/8 gateway="" pref-
src=0.0.0.0 routing-table=main scope=30 suppress-hw-offload=no target-scope=10
```

```
add blackhole disabled=no distance=254 dst-address=172.16.0.0/12 gateway="" pref-
src=0.0.0.0 routing-table=main scope=30 suppress-hw-offload=no target-scope=10
add blackhole disabled=no distance=254 dst-address=192.168.0.0/16
gateway=0.0.0.0 pref-src=0.0.0.0 routing-table=main suppress-hw-offload=no
/ip smb shares
set [ find default=yes ] directory=/pub
/ipv6 firewall filter
add action=drop chain=input
/ppp aaa
set accounting=no use-radius=yes
/ppp secret
add disabled=yes name=client1 profile=PPPoE_prifile
/radius
add address=10.9.8.5 require-message-auth=no service=ppp timeout=3s
/routing filter rule
add chain=ospf_out comment=clients_stst_ip_networks disabled=no rule="if (dst in
100.100.94.0/24) {accept}if (dst in 100.100.95.0/24) {accept}"
/routing ospf area range
add area=backbone disabled=no prefix=100.100.92.0/27
add area=local_dhcp disabled=no prefix=10.10.0.0/20
add area=local_pppoe disabled=no prefix=10.11.0.0/20
add area=local_debtor disabled=no prefix=10.12.0.0/20
/routing ospf interface-template
add area=backbone disabled=no interfaces=ext_services networks=100.100.92.0/27
add area=local_dhcp disabled=no networks=10.10.0.0/20 passive
add area=local_pppoe disabled=no networks=10.11.0.0/20 passive
add area=local_debtor disabled=no networks=10.12.0.0/20 passive
add area=stat_ip_ppooe disabled=no interfaces=local_loop
networks=100.100.92.33/32 passive
/system clock
set time-zone-name=Europe/Kyiv
/system identity
set name=NAS_1
/system logging
add disabled=yes topics=radius,debug
/system note
set show-at-login=no
/system ntp client
set enabled=yes
/system ntp client servers
add address=10.9.8.5
/tool mac-server
set allowed-interface-list=none
/tool mac-server mac-winbox
```

```
set allowed-interface-list=allow_admin
[admin@NAS_1] >
```

Додаток В
Лістинг налаштування комутатору Aggregation_SW

```
[admin@Aggregation_sw] > export
# 2024-10-18 07:17:15 by RouterOS 7.12.1
# software id =
#
/interface bridge
add frame-types=admit-only-vlan-tagged name=local_bridge protocol-mode=none
pvid=4093 vlan-filtering=yes
/interface ethernet
set [ find default-name=ether1 ] disable-running-check=no name=ether1_NAS_1
set [ find default-name=ether2 ] disable-running-check=no name=ether2_NAS_2
set [ find default-name=ether3 ] disable-running-check=no name=ether3_Gateway
set [ find default-name=ether4 ] disable-running-check=no name=ether4_OLT_1
set [ find default-name=ether5 ] disable-running-check=no name=ether5_OLT_2
set [ find default-name=ether6 ] disable-running-check=no
set [ find default-name=ether7 ] disable-running-check=no
set [ find default-name=ether8 ] disable-running-check=no
set [ find default-name=ether9 ] disable-running-check=no
set [ find default-name=ether10 ] disable-running-check=no
set [ find default-name=ether11 ] disable-running-check=no
set [ find default-name=ether12 ] disable-running-check=no
set [ find default-name=ether13 ] disable-running-check=no
set [ find default-name=ether14 ] disable-running-check=no
set [ find default-name=ether15 ] disable-running-check=no
set [ find default-name=ether16 ] disable-running-check=no
set [ find default-name=ether17 ] disable-running-check=no
set [ find default-name=ether18 ] disable-running-check=no
set [ find default-name=ether19 ] disable-running-check=no
set [ find default-name=ether20 ] disable-running-check=no
set [ find default-name=ether21 ] disable-running-check=no
set [ find default-name=ether22 ] disable-running-check=no
set [ find default-name=ether23 ] disable-running-check=no
set [ find default-name=ether24 ] disable-running-check=no
set [ find default-name=ether25 ] disable-running-check=no
set [ find default-name=ether26 ] disable-running-check=no
set [ find default-name=ether27 ] disable-running-check=no name=ether27_admin
/interface vlan
add interface=local_bridge name=int_service vlan-id=1204
add interface=local_bridge name=local_00 vlan-id=1000
add interface=local_bridge name=local_01 vlan-id=1001
add interface=local_bridge name=local_02 vlan-id=1002
add interface=local_bridge name=local_03 vlan-id=1003
```

```
add interface=local_bridge name=local_04 vlan-id=1004
add interface=local_bridge name=local_05 vlan-id=1005
add interface=local_bridge name=local_06 vlan-id=1006
add interface=local_bridge name=local_07 vlan-id=1007
add interface=local_bridge name=local_08 vlan-id=1008
add interface=local_bridge name=local_09 vlan-id=1009
add interface=local_bridge name=local_10 vlan-id=1010
add interface=local_bridge name=local_11 vlan-id=1011
add interface=local_bridge name=local_12 vlan-id=1012
add interface=local_bridge name=local_13 vlan-id=1013
add interface=local_bridge name=local_14 vlan-id=1014
add interface=local_bridge name=local_15 vlan-id=1015
add interface=local_bridge name=local_16 vlan-id=1016
add interface=local_bridge name=local_17 vlan-id=1017
add interface=local_bridge name=local_18 vlan-id=1018
add interface=local_bridge name=local_19 vlan-id=1019
add interface=local_bridge name=local_20 vlan-id=1020
add interface=local_bridge name=local_21 vlan-id=1021
add interface=local_bridge name=local_22 vlan-id=1022
add interface=local_bridge name=local_23 vlan-id=1023
add interface=local_bridge name=local_24 vlan-id=1024
add interface=local_bridge name=local_25 vlan-id=1025
add interface=local_bridge name=local_26 vlan-id=1026
add interface=local_bridge name=local_27 vlan-id=1027
add interface=local_bridge name=local_28 vlan-id=1028
add interface=local_bridge name=local_29 vlan-id=1029
add interface=local_bridge name=local_30 vlan-id=1030
add interface=local_bridge name=local_31 vlan-id=1031
/disk
set slot1 slot=slot1 type=hardware
set slot2 slot=slot2 type=hardware
set slot3 slot=slot3 type=hardware
set slot4 slot=slot4 type=hardware
set slot5 slot=slot5 type=hardware
set slot6 slot=slot6 type=hardware
set slot7 slot=slot7 type=hardware
set slot8 slot=slot8 type=hardware
set slot9 slot=slot9 type=hardware
set slot10 slot=slot10 type=hardware
set slot11 slot=slot11 type=hardware
set slot12 slot=slot12 type=hardware
set slot13 slot=slot13 type=hardware
set slot14 slot=slot14 type=hardware
set slot15 slot=slot15 type=hardware
```

```
set slot16 slot=slot16 type=hardware
set slot17 slot=slot17 type=hardware
set slot18 slot=slot18 type=hardware
/interface list
add name=allow_admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/port
set 0 name=serial0
/interface bridge port
add bridge=local_bridge fast-leave=yes interface=ether1_NAS_1 pvid=4093
trusted=yes
add bridge=local_bridge interface=ether2_NAS_2 pvid=4093 trusted=yes
add bridge=local_bridge fast-leave=yes interface=ether3_Gateway pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether4_OLT_1 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether5_OLT_2 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether6 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether7 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether8 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether9 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether10 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether11 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether12 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether13 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether14 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether15 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether16 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether17 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether18 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether19 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether20 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether21 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether22 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether23 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether25 pvid=4093
add bridge=local_bridge fast-leave=yes interface=ether26 pvid=1204
add bridge=local_bridge fast-leave=yes interface=ether27_admin pvid=1204
/ip neighbor discovery-settings
set discover-interface-list=allow_admin
/interface bridge vlan
add bridge=local_bridge
tagged=ether1_NAS_1,ether2_NAS_2,ether3_Gateway,local_bridge
untagged=ether27_admin,ether26 vlan-ids=1204
```

```
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1000
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1001
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1002
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1003
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1004
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1005
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1006
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1007
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1008
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1009
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1010
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1011
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1012
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1013
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1014
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether4_OLT_1 vlan-
ids=1015
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1016
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1017
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1018
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1019
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1020
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1021
```

```
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1022
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1023
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1024
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1025
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1026
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1027
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1028
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1029
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1030
add bridge=local_bridge tagged=ether1_NAS_1,ether2_NAS_2,ether5_OLT_2 vlan-
ids=1031
/interface list member
add interface=int_service list=allow_admin
/ip address
add address=10.9.8.4/24 interface=int_service network=10.9.8.0
/ip dns
set servers=8.8.8.8,1.0.0.1
/ip firewall address-list
add address=10.9.8.0/22 list=allow_admin
add address=10.9.16.0/24 list=allow_admin
add address=192.168.122.0/24 list=allow_admin
/ip firewall filter
add action=accept chain=input connection-state=established,related
add action=drop chain=input src-address-list=!allow_admin
/system identity
set name=Aggregation_sw
/system note
set show-at-login=no
/tool mac-server
set allowed-interface-list=none
/tool mac-server mac-winbox
set allowed-interface-list=allow_admin
[admin@Aggregation_sw] >
```