НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ

імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки
(повне найменування інституту, назва факультету)

Кафедра програмованої електроніки, електротехніки і телекомунікацій
(повна назва кафедри)

«Допущений до захисту»
Завідувач кафедри _____ В. М. Рябенький
д.т.н., професор
« 16 » грудня 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти «магістр»

на тему: Розробка середовища для тестування мережевої інфраструктури.

Виконав: студент 6 курсу, групи 6321М
спеціальності 171
«Електроніка»
шифр і назва спеціальності)

ОПП «Електронні системи»

Трешнюк О. І.
(прізвище та ініціали студента)

Керівник Дьяконов О. С.
(прізвище та ініціали)

Рецензент Черно О. О.
(прізвище та ініціали)

м. Миколаїв – 2024 року

Національний університет кораблебудування імені адмірала Макарова

ННІ	автоматики та електротехніки
Кафедра	програмованої електроніки, електротехніки і телекомунікацій
Рівень вищої освіти	другий (магістерський)
Спеціальність	171 «Електроніка»
ОПП	Електронні системи

ЗАТВЕРДЖУЮ
Завідувач кафедри _____ В. М. Рябенький
д.т.н., професор
« 16 » жовтня 2024 р.

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ АТЕСТАЦІЙНУ РОБОТУ СТУДЕНТУ

Трешнюку Олегу Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка середовища для тестування мережевої інфраструктури.

керівник роботи Дьяконов Олексій Сергійович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу
від «__» травня 2024 року № ___-уч.

2. Строк подання студентом роботи

3. Вихідні дані до роботи протокол LoRaWAN, гіпервізор ProxMox, програмне та апаратне забезпечення Mikrotk, програмне та апаратне забезпечення SuperMicro

4. Мета дослідження Розробка імітаційного середовища для моделювання мережевої інфраструктури.

5. Зміст розрахунково-пояснювальної записки
(перелік питань, які потрібно розробити) 1. Сучасні тенденції розвитку апаратного забезпечення. 2. Огляд програмного забезпечення. 3. Впровадження мережевої інфраструктури. 4. Охорона праці.

6. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Презентація у PowerPoint

7. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Тубальцев А.М.		

8. Дата видачі завдання « 16 » жовтня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз сучасних тенденцій розвитку	02.10.2024	Вик.
	мережевого обладнання		
2	Аналіз сучасних тенденцій розвитку	20.10.2024	Вик.
	серверного обладнання		
3	Вивчення основних характеристик технології	10.11.2024	Вик
	Wi-Fi та протаколу LoRaWAN		
4	Розробка середовища для мережевої	21.11.2024	Вик.
	інфраструктури		
5	Охорона праці	03.12.2024	Вик.
6	Оформлення дипломної роботи, підготовка	05.12.2024	Вик.
	графічного матеріалу		

Студент _____ О. І. Трешнюк
(підпис) (прізвище та ініціали)

Керівник роботи _____ О. С. Дьяконов
(підпис) (прізвище та ініціали)

Анотація

У роботі виконано розробку середовища для тестування мережевої інфраструктури, у тому числі локальної мережі між підрозділами ГУ ДСНС у Миколаївській області. Розглянуто отримання інформації з датчиків за допомогою протоколу LoRaWAN та технологія Wi-Fi з використанням CAPsMAN. Основними перевагами запропонованого середовища для тестування мережевої інфраструктури є масшабування, зручність керування, вартість та можливість зміни програмного коду під різні задачі.

Ключові слова: LoRaWAN, Wi-Fi, гіпервізор, RouterOS.

Abstract

The work includes the development of an environment for testing the network infrastructure, including the local network between the units of the State Emergency Service of Ukraine in the Mykolaiv region. Obtaining information from sensors using the LoRaWAN protocol and Wi-Fi technology using CAPsMAN are considered. The main advantages of the proposed environment for testing network infrastructure are scalability, ease of management, cost, and the ability to change the software code for different tasks.

Keywords: LoRaWAN, Wi-Fi, hypervisor, RouterOS.

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень та термінів.. 5
Вступ 6
Розділ 1. Сучасні тенденції розвитку апаратного забезпечення 8
1.1. Мережеві пристрої: комутатори, маршрутизатори, точки доступу 8
1.2. Сервери для розміщення тестових додатків і служб 16
1.3. Забезпечення безперебійним живленням 19
Розділ 2. Огляд програмного забезпечення..... 25
2.1. Операційні системи для серверів і систем зберігання даних 25
2.2. Мережеве програмне забезпечення 31
2.3. Програмне забезпечення систем безперебійного живлення..... 35
Розділ 3. Впровадження мережевої інфраструктури 44
3.1. Створення локальної мережі. 44
3.2. Сегментація мережі, VLAN, VPN. 48
3.3. Підключення датчиків за допомогою протоколу LoRaWAN 55
3.4. Системи моніторингу стану мережі. 60
Розділ 4. ОХОРОНА ПРАЦІ 69
4.1. Основні положення щодо охорони праці в Україні 69
4.2. Вимоги до інженерної інфраструктури технологічних приміщень 70
4.3. Основи електробезпеки 71
Висновки..... 73
Список використаних джерел..... 74
Додаток А Приклад прийнятого пакету LoRaWAN 76

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

KVM (Kernel-based Virtual Machine) – технологія віртуалізації

LoRaWAN (Long Range Wide Area Network) – Глобальна мережа великого радіусу дії

VPS (Virtual Private Server) – віртуальний приватний сервер

IoT (Internet of Things) – Інтернет речей

VPN (Virtual Private Network) – віртуальна приватна мережа

DNS (Domain Name System) – система доменних імен

IP (Internet Protocol) – інтернет протокол

LAN (Local Area Network) – локальна обчислювальна мережа

WAN (Wide Area Network) – глобальна мережа

VLAN (Virtual Local Area Network) – віртуальна локальна мережа

QoS (Quality of Service) – набір механізмів, що дозволяють забезпечити певні гарантії якості для передачі даних в мережі

ОС – операційна система

LTE (Long-Term Evolution) – стандарт мобільного зв'язку четвертого покоління

VoIP (Voice over Internet Protocol) – технологія передачі голосових повідомлень через мережу Інтернет.

L2TP (Layer 2 Tunneling Protocol) – тунельний протокол другого рівня

ПЗ – Програмне забезпечення

ДБЖ – джерело безперебійного живлення

ВСТУП

Розвиток мережевих технологій призвів до появи складних інфраструктур, що включають комутатори, маршрутизатори, сервери, а також бездротові технології, такі як Wi-Fi та LoRaWAN. Ефективне функціонування таких мереж залежить від правильної конфігурації та взаємодії всіх компонентів.

Ця робота присвячена розробці середовища для тестування мережевої інфраструктури, яке дозволить інтегрувати різноманітне обладнання та протоколи, моделювати різні топології мереж та оцінювати їх продуктивність.

В якості основи для розробки локальної мережі було обрано апаратне забезпечення для мережевої інфраструктури Mikrotik, для отримання даних з датчиків використовувались сучасний протокол LoRaWAN.

					171.6321М.КР.ПЗ.Р1		
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*			
Розробник		Трешнюк О. І.			Сучасні тенденції розвитку апаратного забезпечення	*Літ.*	*Арк.* 7 / *Аркушів*
Консультант							
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова	
Керівник		Дьяконов О. С.					
Зав. каф.		Рябенький В. М.					

РОЗДІЛ 1. СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ

1.1. Мережеві пристрої: комутатори, маршрутизатори, точки доступу

Для створення мережевої інфраструктури розглянемо основні компоненти апаратного забезпечення. До таких компонентів входять: мережа (маршрутизатори, комутатори, точки доступу та супутникові термінали), сервери для розміщення тестових додатків і служб, безперебійні джерела живлення.

Мережеві пристрої – це невід'ємна частина сучасних інформаційних систем, яка забезпечує з'єднання між різними комп'ютерами, серверами та іншими пристроями для обміну даними. Вони відіграють ключову роль у сучасному світі, забезпечуючи з'єднання між пристроями та системами. Розуміння принципів їх роботи допоможе ефективніше використовувати мережу та вирішувати потенційні проблеми.

Маршрутизатор – це ключовий пристрій у будь-якій комп'ютерній мережі, який керує рухом даних між різними мережами.

До основних складових маршрутизаторів належать IP-адреси, таблиці маршрутизації та пакети даних. Кожен пристрій у мережі має унікальну IP-адресу, яку маршрутизатор використовує для визначення, куди відправити пакет даних. Всередині маршрутизатора зберігається таблиця маршрутів, яка містить інформацію про те, як досягти інших мереж. Дані розбиваються на невеликі пакети, кожен з яких містить інформацію про відправника та одержувача. Маршрутизатор аналізує ці пакети і направляє їх найкоротшим шляхом.

Маршрутизатори необхідні для з'єднання різних мереж, оптимізації трафіку та забезпечення безпеки. Маршрутизатори дозволяють об'єднувати локальні мережі (LAN), глобальні мережі (WAN) та інші типи мереж. Маршрутизатор вибирає найефективніший шлях для передачі даних, що дозволяє зменшити затримки і підвищити швидкість роботи мережі. Багато

маршрутизаторів мають вбудовані функції безпеки, такі як брандмауер, який захищає мережу від несанкціонованого доступу.

Основні характеристики маршрутизаторів включають швидкість, кількість портів та функціональність. Швидкість визначає, з якою швидкістю маршрутизатор може обробляти дані. Кількість портів визначає кількість фізичних портів для підключення пристроїв. Додаткові функції, такі як QoS (якість обслуговування), VPN, батьківський контроль тощо, розширюють можливості маршрутизатора.

У якості основного маршрутизатора для побудови нашої мережі розглянемо Mikrotik CCR1036-8G-2S+ (рис. 1.1).

Рисунок 1.1 – Mikrotik CCR1036-8G-2S+

Перевагами цього маршрутизатору є невисока вартість та вбудована ліцензія на пристрій, що значно економить кошти в порівняння з маршрутизаторами компанії Cisco, підтримка декількох операційних систем (RouterOS та SWoS), процесор на 36 ядер частотою 1.2 GHz, COM-порт в форматі RJ-45 для сервісного обслуговування пристрою, USB-порт, слот для MicroCD, сенсорний екран для відображення інформації про стан завантаження процесору та мережі, два SFP+-порта для підключення оптичних SFP-модулей 10G, 1.25G та вісім 10/100/1000 Ethernet ports.

Комутатор – це центральний пристрій у комп'ютерних мережах, який з'єднує декілька пристроїв в єдину мережу та забезпечує передачу даних між ними. Він є фундаментальним елементом будь-якої сучасної комп'ютерної мережі. Його основна функція полягає в з'єднанні множини мережевих

пристроїв (комп'ютерів, серверів, периферії) в єдине ціле та забезпеченні ефективного обміну даними між ними.

Роль комутатора в мережі полягає в об'єднанні пристроїв, підвищенні пропускної здатності, збільшенні надійності та забезпеченні безпеки. Він створює єдине логічне середовище, в якому різноманітні пристрої можуть взаємодіяти, незважаючи на свою фізичну розподіленість. За рахунок сегментації мережі та використання механізмів переадресації, комутатори значно збільшують ефективність передачі даних, мінімізуючи колізії та затримки. Розбиваючи мережу на менші сегменти, комутатори підвищують її стійкість до збоїв. Пошкодження одного сегмента не призводить до повного відключення всієї мережі. Крім того, комутатори підтримують різноманітні механізми безпеки, такі як VLAN, які дозволяють ізолювати різні сегменти мережі та обмежити доступ до ресурсів.

Існує два основних типи комутаторів: некеровані та керовані. Некеровані комутатори – це прості у використанні пристрої, які не потребують складних налаштувань. Зазвичай застосовуються в невеликих мережах з обмеженими вимогами. Керовані комутатори надають широкий спектр можливостей для налаштування та керування мережею. Підтримують такі функції, як VLAN, QoS, агрегацію портів та інші.

Основними характеристиками комутаторів є пропускна здатність, кількість портів, тип портів та рівень. Кількість портів визначає максимальну кількість пристроїв, які можна підключити до комутатора. Порти бувають мідні (для витої пари) та оптичні (для волоконно-оптичних кабелів). Комутатори поділяються на рівні 2 (дата лінк) та рівень 3 (маршрутизатори). Комутатори рівня 2 працюють на рівні канального доступу, а комутатори рівня 3 можуть виконувати маршрутизацію між різними мережами.

При виборі комутатора необхідно враховувати розмір мережі та кількість підключених пристроїв, вимоги до пропускної здатності, необхідність підтримки додаткових функцій (VLAN, QoS тощо) та бюджет.

Комутатор є ключовим компонентом будь-якої сучасної мережі. Вибір правильного комутатора дозволяє забезпечити високу продуктивність, надійність та безпеку мережі.

Для з’єднання кінцевих пристроїв на об’єктах з великою кількістю користувачів використовуємо комутатор CRS354-48G-4S+2Q+RM (рис. 1.2).

Рисунок 1.2 – Mikrotik CRS354-48G-4S+2Q+RM

Цей комутатор має можливість підключення одразу до 48 пристроїв за допомогою 10/100/1000 Ethernet ports та масштабувати мережу на швидкості 40G за допомогою портів QSFP+ або 10G за допомогою SFP+.

У разі використання великої кількості IP-телефонів, точок доступу та камер відеонагляду доцільно використовувати комутатори з функцією PoE живлення. PoE (Power over Ethernet) – це технологія, яка дозволяє передавати як дані, так і електричну енергію по одному Ethernet-кабелю. Це особливо корисно для живлення мережевих пристроїв, точок доступу Wi-Fi, IP-камер, VoIP-телефонів, які можуть бути встановлені в місцях, де немає зручного доступу до електромережі, у разі підключення комутаторів до джерел безперебійного живлення точки доступу Wi-Fi, IP-камери, VoIP-телефони будуть працювати незважаючи на переключення та вимкнення світла. У якості PoE комутатора від Mikrotik будемо використовувати CRS354-48P-4S+2Q+RM.

При невеликій кількості пристроїв доцільно розглядати комутатори з кількістю 0/100/1000 Ethernet ports до 2 - Mikrotik CRS326-24G-2S+RM.

Рисунок 1.3 – Mikrotik CRS326-24G-2S+RM

Для об’єднання комутаторів між собою на великі відстані потрібно використовувати оптичну мережу.

Оптична мережа – це один із типів комп'ютерної мережі, яка для передачі даних по оптичних волокнах використовує світло. На відміну від мідних мереж, оптичні мережі забезпечують значно більшу пропускну здатність, менші втрати сигналу та більшу стійкість до електромагнітних перешкод.

Переваги оптичних мереж полягають у високій пропускній здатності, можливості передачі даних на великі відстані без помітних втрат якості та імунітеті до перешкод. Оптичні волокна можуть передавати дані на швидкостях, які незрівнянні з мідними кабелями. Оптичні сигнали можуть передаватися на значні відстані без помітних втрат якості. Оптичні волокна не схильні до електромагнітних перешкод, що необхідно для використання в промислових умовах або там, де є багато електронного обладнання. Крім того, оптичні сигнали важче підслухати, що забезпечує більш високий рівень безпеки.

Для з’єднання комутаторів за стандартом для високошвидкісних оптичних з'єднань SFP+ можна використати модулі NGOPTICS NG-SFP+2733-20D, NG-SFP+3327-20D та комутатор Mikrotik CRS326-24S+2Q+RM. Ці компоненти дозволять створити високопродуктивну оптичну мережу з необхідною пропускною здатністю та відстанню передачі даних.

Рисунок 1.4 – Mikrotik CRS326-24S+2Q+RM

Точки доступу – це пристрої, які дозволяють бездротовим пристроям, таким як смартфони, планшети, ноутбуки та інші, підключатися до мережі Інтернет або локальної мережі. Вони є невід'ємною частиною сучасних бездротових мереж і забезпечують швидкий доступ до мережі інтернет.

Серед широкого асортименту продуктів MikroTik особливе місце займають точки доступу для Інтернету речей (IoT). Ці пристрої призначені для створення бездротових мереж, які об'єднують різноманітні IoT-пристрої, такі як датчики та інші інтелектуальні пристрої.

IoT точка доступа MikroTik – це спеціалізований пристрій, розроблений для побудови мереж Інтернету речей (IoT). Він поєднує в собі можливості Wi-Fi точки доступу та шлюзу LoRaWAN, що робить його універсальним інструментом для різних IoT-проектів (рис. 1.5).

Рисунок 1.5 – MikroTik wAP LR8 kit (RBwAPR-2nD&R11e-LR8)

LoRaWAN – це низькоенергоспоживчий протокол дальнього радіусу дії, спеціально розроблений для IoT. Він дозволяє створювати масштабні мережі з великою кількістю пристроїв, що працюють від батарей, і забезпечує надійний зв'язок у важкодоступних місцях. MikroTik wAP LR8 kit універсальний, простий для встановлення та налаштування, має високу надійність та масштабованість, використовується для моніторинг стану обладнання, контроль виробничих процесів.

MikroTik LtAP mini LTE kit - це компактний та потужний пристрій, призначений для створення бездротових мереж з використанням технологій Wi-Fi та LTE. Це ідеальне рішення для забезпечення інтернет-зв'язку в різних умовах, особливо там, де немає стаціонарного інтернет-з'єднання (рис. 1.6).

Рисунок 1.6 – MikroTik LtAP mini LTE kit (RB912R-2nD-LTm&R11e-LTE)

Переваги пристрою:

- Wi-Fi: Підтримка стандарту 802.11b/g/n на частоті 2.4 ГГц для бездротового підключення пристроїв.
- LTE: Вбудований 4G LTE-модем для підключення до Інтернету через мобільну мережу.
- GPS: Модуль GPS для визначення географічних координат.
- Компактний корпус: легко монтується на стіну або іншу поверхню.

- Вологозахищений корпус: Захист від впливу зовнішніх факторів, таких як дощ та пил.

MikroTik cAP ax – це високопродуктивна Wi-Fi точка доступу, призначена як для внутрішнього, так і для зовнішнього використання. Точка доступу ідеально підходить для створення мереж типу mesh, що забезпечує безшовне бездротове підключення між різними пристроями та локаціями (рис. 1.7).

Рисунок 1.7 – MikroTik cAP ax (cAPGi-5HaxD2HaxD)

Ключові особливості cAP ax:

- Швидкісний Wi-Fi: Підтримує стандарт 802.11ax Wi-Fi для більш високих швидкостей і більшої пропускної здатності.
- Двохдіапазонний Wi-Fi: Працює як на частоті 2.4 ГГц, так і 5 ГГц для оптимальної продуктивності.
- Можливість створення мереж mesh: Легко створює мережі mesh з кількох пристроїв cAP ax для розширеного покриття.
- Міцний корпус: Вологозахищений корпус, придатний для зовнішньої установки.

- Потужне обладнання: Обладнаний високопродуктивним процесором та великою кількістю оперативної пам'яті.
- Гнучка конфігурація: Налаштовувані параметри через зручний інтерфейс RouterOS.
- Розширені функції безпеки: Підтримує шифрування WPA3 для підвищення безпеки.

Продукти MikroTik відрізняються високою продуктивністю, гнучкістю налаштування та доступною ціною. Їхнє обладнання використовується для створення як невеликих домашніх мереж, так і великих організацій. Власна операційна система RouterOS, яка встановлена на все обладнання MikroTik забезпечує широкий спектр функцій, включаючи маршрутизацію, брандмауер, VPN, QoS та багато іншого. RouterOS дозволяє налаштувати комутатори, маршрутизатори, точки доступу LoraWan, Wi-Fi, LTE модеми в єдине середовище під будь-які потреби користувача.

1.2. Сервери для розміщення тестових додатків і служб

Вибір сервера – це відповідальне завдання, яке вимагає ретельного аналізу потреб вашого бізнесу. Кожна з компаній – Cisco, Dell та Supermicro – пропонує широкий асортимент серверного обладнання, що відрізняється за характеристиками, ціною та призначенням. Давайте розглянемо основні відмінності та переваги кожного виробника.

Cisco – це компанія, яка традиційно спеціалізується на мережевих технологіях. Їхні сервери часто інтегруються з іншими мережевими компонентами Cisco, забезпечуючи високу сумісність та ефективність. Компанія пропонує широкий спектр програмного забезпечення для управління серверами та мережами, що спрощує адміністрування. Однак, обладнання Cisco зазвичай дорожче за аналоги інших виробників. Тому Cisco є оптимальним вибором для великих організацій, які потребують складних мережевих рішень та високого рівня безпеки.

Рисунок 1.8 – Сервер Cisco UCS C220 M5 Rack Server At-a-Glance

Dell має широкий асортимент серверів, які підходять під різні завдання – від невеликих підприємств до великих дата-центрів. Сервери Dell відомі своєю надійністю та довгим терміном служби. Компанія пропонує широкий діапазон цін, що дозволяє підібрати оптимальне рішення під бюджет. Крім того, Dell має розвинену мережу сервісних центрів та надає якісну технічну підтримку. Це робить сервери Dell універсальним рішенням для багатьох компаній.

Рисунок 1.9 – Сервер Dell EMC PowerEdge R6625

Сервери ***Supermicro*** відрізняються високою модульністю, що дозволяє конфігурувати систему під конкретні завдання. Як правило, сервери Supermicro мають більш привабливу ціну порівняно з аналогами інших виробників. Багато моделей Supermicro оптимізовані для низького споживання енергії. Компанія спеціалізується на створенні високопродуктивних серверів для обчислювальних задач, таких як машинне навчання та аналіз даних. Це робить сервери Supermicro популярним

вибором для компаній, які шукають гнучкі, енергоефективні та високопродуктивні рішення.

Рисунок 1.10 – Сервер SuperMicro 6016T-NTRF (4 LFF)

Таблиця 1.1 – Порівняння характеристик серверів

Характеристика	**Cisco**	**Dell**	**Supermicro**
Спеціалізація	Мережеві технології	Універсальні рішення	Високопродуктивні сервери
Ціна	Висока	Середня	Низька
Гнучкість конфігурації	Висока	Середня	Висока
Програмне забезпечення	Широкий спектр власних рішень	Багатостороннє програмне забезпечення	Відкриті платформи
Типовий користувач	Великі корпорації	Різноманітні компанії	Компанії, що потребують високої продуктивності

Вибір конкретного виробника сервера залежить від ваших потреб. Для інтеграції з існуючою мережею Cisco та високим рівнем безпеки оптимальним вибором є сервера Cisco. Якщо вам потрібен надійний і універсальний сервер за розумною ціною, зверніть увагу на Dell. А якщо вам потрібен високопродуктивний сервер для обчислювальних задач та гнучка конфігурація, Supermicro – це відмінний варіант.

При виборі сервера важливо враховувати такі фактори: бюджет, завдання, які буде виконувати сервер, масштабованість системи в майбутньому та необхідний рівень технічної підтримки.

Виходячи з використання відкритих платформ та вартості продукції, для розробки середовища для тестування мережевої інфраструктури будемо

використовувати сервера SuperMicro. Цей вибір обумовлений високою модульністю серверів SuperMicro, що дозволяє конфігурувати систему під конкретні завдання, а також їхньою привабливою ціною та енергоефективністю.

1.3. Забезпечення безперебійним живленням

Безперебійне живлення є критично важливим для багатьох пристроїв та систем, особливо в умовах нестабільної електромережі. Воно дозволяє уникнути втрати даних, пошкодження обладнання та забезпечує безперервну роботу важливих систем. Безперебійне живлення захищає обладнання від різких перепадів напруги, коротких замикань та відключень електроенергії. Воно також дозволяє зберегти незбережені дані та уникнути їх втрати. Для багатьох систем, таких як сервери, системи безпеки, медичне обладнання, безперервна робота є критично важливою.

Існує кілька способів забезпечити безперебійне живлення. Найпоширенішим є використання ДБЖ. Онлайн ДБЖ забезпечують найвищий рівень захисту, постійно перетворюючи змінний струм у постійний і назад. Лінійно-інтерактивні ДБЖ більш економічні, але менш захищені від перепадів напруги. Резервні ДБЖ найпростіші та найдешевші, але забезпечують лише захист від повного відключення електроенергії.

Крім ДБЖ, для забезпечення безперебійного живлення можна використовувати акумулятори, генератори та сонячні батареї. Акумулятори можуть використовуватися як самостійне джерело живлення або в поєднанні з ДБЖ. Генератори виробляють електроенергію за рахунок спалювання палива і зазвичай використовуються для забезпечення резервного живлення великих об'єктів. Сонячні батареї – це екологічно чисте джерело енергії, яке може забезпечити як основне, так і резервне живлення.

Одним із інноваційних рішень для зберігання енергії є Tesla Powerwall 2.0. Ця система працює в комплексі з сонячними панелями, дозволяючи

накопичувати надлишкову електроенергію і використовувати її в пікові години споживання або під час відключень електроенергії.

Рисунок 1.11 – Tesla Powerwall 2.0

Tesla Powerwall 2.0 – це сучасна система зберігання енергії. Вона дозволяє накопичувати надлишкову електроенергію, вироблену вдень сонячними панелями, і використовувати її вночі або під час відключень електроенергії. Це дозволяє заощадити на оплаті електроенергії та зробити споживання енергії більш незалежним від зовнішніх факторів.

Виготовлений з високоякісних матеріалів, Tesla Powerwall 2.0 забезпечує довгий термін служби. За допомогою мобільного додатку користувач може відстежувати споживання енергії, керувати роботою системи та налаштовувати її під свої потреби.

Забезпечення безперебійного живлення є важливим аспектом для багатьох пристроїв та систем. Вибір оптимального рішення залежить від конкретних потреб та бюджету. Сучасні системи зберігання енергії, такі як

Tesla Powerwall 2.0, відкривають нові можливості для ефективного використання енергії та забезпечення автономності. Вони підходять для заживлення приватних будинків та офісів, мають можливість заряджатися як від центрального енергопостачання, так і від генератора чи сонячних панелей.

APC Smart-UPS 5000 - це потужний і надійний пристрій безперебійного живлення (ПБЖ), який забезпечує захист вашого обладнання від різноманітних проблем з електромережею. Він застосовується для захисту серверів, мережевого обладнання та іншої критично важливої електроніки (рис. 1.12).

Рисунок 1.12 – APC Smart-UPS 5000

Основні функції та характеристики APC Smart-UPS 5000 включають захист від перепадів напруги, перенапруги та шумів в мережі. ПБЖ постійно моніторить якість вхідної напруги і автоматично коригує її, забезпечуючи стабільну роботу підключеного обладнання. Вбудовані фільтри слугують для захисту обладнання від шкідливих перенапруг, які можуть виникнути внаслідок грозових розрядів або інших електромагнітних перешкод. У разі відключення електроенергії ПБЖ автоматично перемикається на живлення від батарей, забезпечуючи безперебійну роботу підключеного обладнання. Час автономної роботи залежить від моделі і ємності батарей, але зазвичай достатній для безпечного завершення роботи і збереження даних.

Більшість моделей Smart-UPS мають вбудований мікропроцесор, який забезпечує інтелектуальне управління, моніторинг стану батарей і надає

інформацію про роботу ПБЖ. Деякі моделі підтримують мережеве управління, що дозволяє віддалено контролювати і конфігурувати ПБЖ.

APC Smart-UPS 5000 широко використовується для захисту серверів, мережевого обладнання та медичного обладнання. Він забезпечує безперебійну роботу цих систем, запобігає втраті даних і гарантує безпеку критично важливих процесів.

Компанія APC є одним з лідерів на ринку ПБЖ, а моделі Smart-UPS відомі своєю високою надійністю і довгим терміном служби. ПБЖ Smart-UPS мають широкий спектр функцій, що дозволяють адаптувати їх під різні потреби. Вони мають інтуїтивно зрозумілий інтерфейс і легко налаштовуються. Компанія APC надає всебічну підтримку своїм продуктам, включаючи технічну документацію, драйвери і програмне забезпечення.

Висновки

Для створення середовища моделювання мережевої інфраструктури були обрані комутатори, маршрутизатори, IoT точки доступу компанії MikroTik. Для розгортання програмного забезпеченні найбільш підходящим є використання серверів SuperMicro.

					171.6321М.КР.ПЗ.Р2		
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*			
Розробник		Трешнюк О. І.			Огляд програмного забезпечення	*Літ.*	*Арк.* 24 / *Аркушів*
Консультант							
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова	
Керівник		Дьяконов О. С.					
Зав. каф.		Рябенький В. М.					

РОЗДІЛ 2. ОГЛЯД ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1. Операційні системи для серверів і систем зберігання даних

Розвиток сучасних мережевих інфраструктур вимагає надійних і ефективних інструментів для тестування. Програмне забезпечення для тестування мереж дозволяє симулювати різні сценарії, виявляти вузькі місця, оцінювати продуктивність та безпеку мережі.

Розглянемо основні категорії такого програмного забезпечення та їх функціональні можливості:

- Створення віртуальних мереж.
- Моделювання різних топологій і сценаріїв.
- Конфігурування мережевого обладнання.
- Налаштування маршрутизаторів, комутаторів, брандмауерів та іншого обладнання.
- Вимірювання продуктивності.
- Визначення пропускної здатності, затримки, втрат пакетів.

Вибір правильного програмного забезпечення для тестування мережевої інфраструктури є важливим кроком для гарантування надійності та ефективності мережі. Використання інструментів дозволяє виявляти проблеми на ранніх етапах, оптимізувати роботу мережі та забезпечити її безпеку.

Для функціонування середовища для тестування мережевої інфраструктури розглянемо можливість розміщення програмного забезпечення на VPS за допомогою Гіпервізору.

Гіпервізор дозволяє запускати кілька операційних систем одночасно на одному фізичному сервері. Використання гіпервізорів для створення віртуальних машин на одному фізичному сервері приносить багато переваг для тестування мережевої інфраструктури.

По-перше, це суттєво економить ресурси. Замість того, щоб купувати кілька фізичних комп'ютерів для різних тестових завдань, можна

використовувати один потужний сервер і розподіляти його ресурси між декількома VPS.

По-друге, гіпервізори забезпечують високу гнучкість. Створення, видалення та клонування віртуальних машин здійснюється за лічені хвилини.

По-третє, кожна VPS ізольована від інших, що забезпечує високий рівень безпеки та стабільності. Це особливо важливо при тестуванні нового програмного забезпечення, коли можуть виникати непередбачені ситуації.

Крім того, гіпервізори дозволяють створювати ізольовані середовища для тестування нового програмного забезпечення. Це дозволяє перевірити його роботу в різних умовах без ризику пошкодити основну систему.

Нарешті, гіпервізори дозволяють легко створювати резервні копії віртуальних машин. Це дозволяє відновити VPS в разі виникнення проблем зі збоями програмного забезпечення або апаратні несправності.

Існує багато різних гіпервізорів, кожен з яких має свої особливості та переваги. Ось деякі з найпопулярніших:

- *VMware vSphere*: Це один з найпотужніших і функціональних гіпервізорів на ринку. Він широко використовується у великих підприємствах для створення складних віртуальних інфраструктур.
- *Microsoft Hyper-V*: Вбудований в операційну систему Windows Server, що робить його доступним у використанні для користувачів Windows.
- *Oracle VirtualBox*: Безкоштовний і відкритий гіпервізор, який ідеально підходить для домашнього використання, навчання та невеликих проектів.
- *Proxmox VE*: Відкритий гіпервізор, вбудований в ядро Linux, який надає широкий спектр функцій керування VPS.

Proxmox Virtual Environment (Proxmox VE) – це універсальна платформа віртулізації з відкритим кодом, що заснована на Debian Linux. Вона поєднує в собі віртуальні машини (KVM) та контейнери (LXC). Це

означає, що можуj одночасно запускати як традиційні операційні системи (Windows, Linux), так і легкі контейнери для сучасних мікросервісів.

Proxmox Virtual Environment універсальний, гнучкий та доступний. Один з ключових факторів – це єдиний інтуїтивно зрозумілий веб-інтерфейс для керування віртуальними машинами та контейнерами в одному місці. Це значно спрощує адміністрування та знижує поріг входу для нових користувачів.

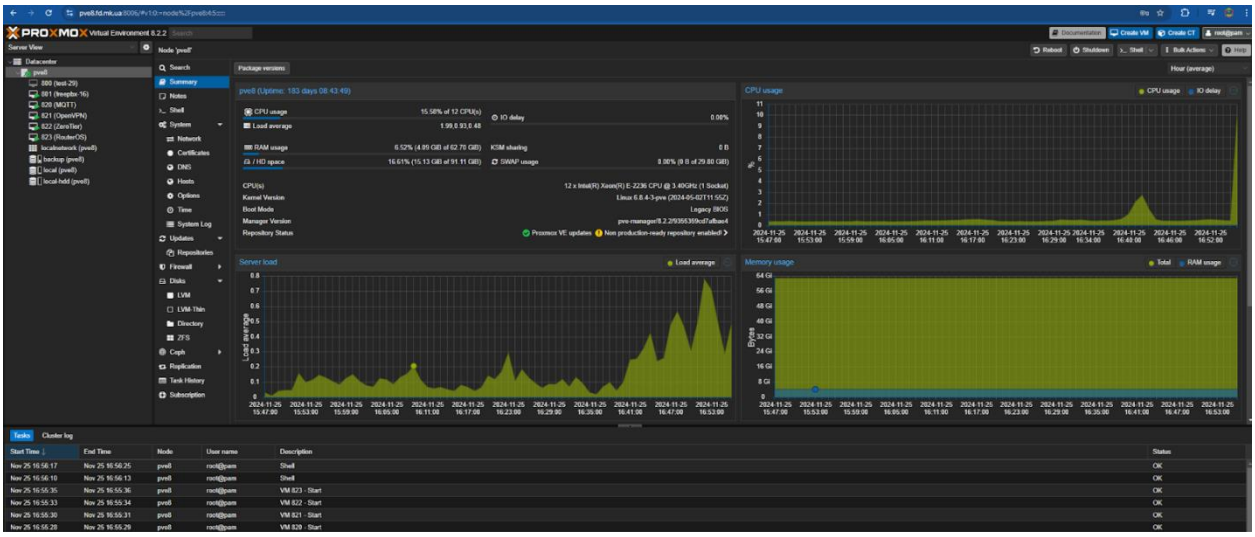


Рисунок 2.1 – Інтерфейс ProxMox Virtual Environment 8.2.2

Крім того, Proxmox відрізняється високою гнучкістю. Він підтримує різноманітні типи зберігання даних, мережеві технології і може працювати в кластерах, що забезпечує високу доступність. Це дозволяє адаптувати платформу до вимог різних середовищ і масштабувати її відповідно до зростаючих потреб.

Автоматизація – ще одна сильна сторона Proxmox. Вбудовані інструменти дозволяють автоматизувати рутинні завдання, такі як створення резервних копій, міграцію VPS та масштабування інфраструктури. Це значно зменшує ручну роботу адміністратора і підвищує ефективність.

Важливою перевагою Proxmox є те, що він є відкритим і безкоштовним. Користувачі мають повний доступ до коду і можуть його

модифікувати під свої потреби. Крім того, велика спільнота розробників і користувачів забезпечує активну розробку і підтримку платформи.

І нарешті, Proxmox відрізняється високою продуктивністю. Він ефективно використовує ресурси сервера і забезпечує стабільну роботу VPS та контейнерів.

Для чого використовується Proxmox?

Proxmox знаходить широке застосування в різних сферах:

- Контейнеризація: Розгортання легких і ізольованих контейнерів для сучасних мікросервісів забезпечує високу щільність розміщення додатків та швидку масштабованість.
- Приватні хмари: Створення власної хмарної інфраструктури дозволяє підвищити гнучкість і масштабованість IT-систем.
- Віртуалізація серверів: Створення і управління VPS для різних операційних систем дозволяє консолідувати серверні ресурси і оптимізувати їх використання.
- Тестування і розробка: Створення ізольованих середовищ для розробки і тестування програмного забезпечення дозволяє швидко і безпечно проводити експерименти.
- Лабораторії: Використання в навчальних закладах для навчання студентів технологіям віртуалізації та контейнеризації.

Завдяки своїй універсальності і гнучкості Proxmox може бути використаний як для невеликих домашніх лабораторій, так і для центрів обробки даних.

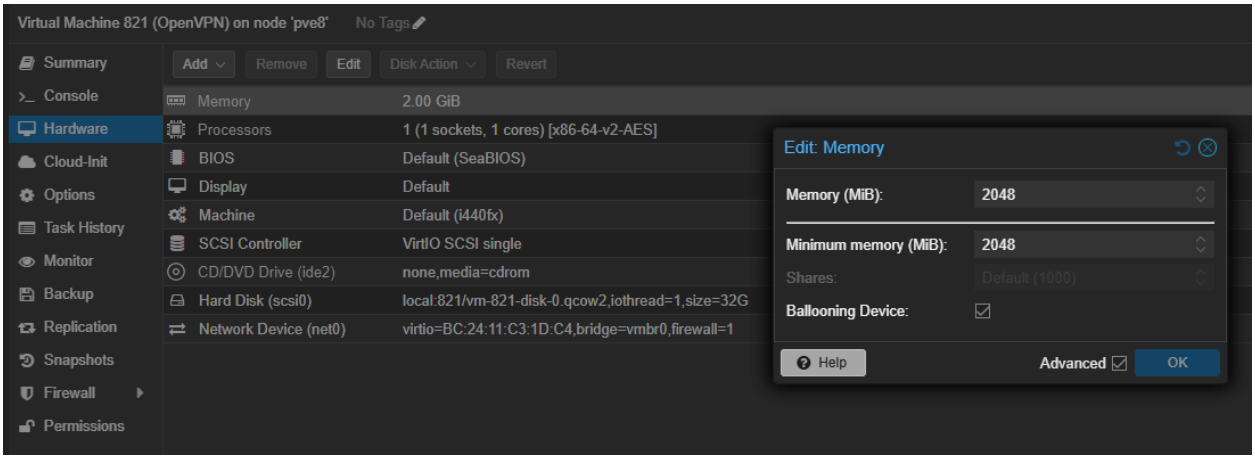


Рисунок 2.2 – Інтерфейс гнучкого налаштування параметрів VPS

Proxmox Backup Server - це спеціалізоване рішення для резервного копіювання та відновлення даних, розроблене спеціально для роботи з віртуальними середовищами Proxmox VE. Це потужний інструмент, який дозволяє забезпечити надійний захист ваших даних, VPS та контейнерів.

Proxmox Backup Server пропонує інтуїтивно зрозумілий веб-інтерфейс, який дозволяє легко налаштувати і керувати процесом резервного копіювання. Крім того, платформа підтримує різноманітні стратегії резервного копіювання, включаючи повне, інкрементальне та диференціальне резервування, дозволяючи оптимізувати використання дискового простору та час резервування.

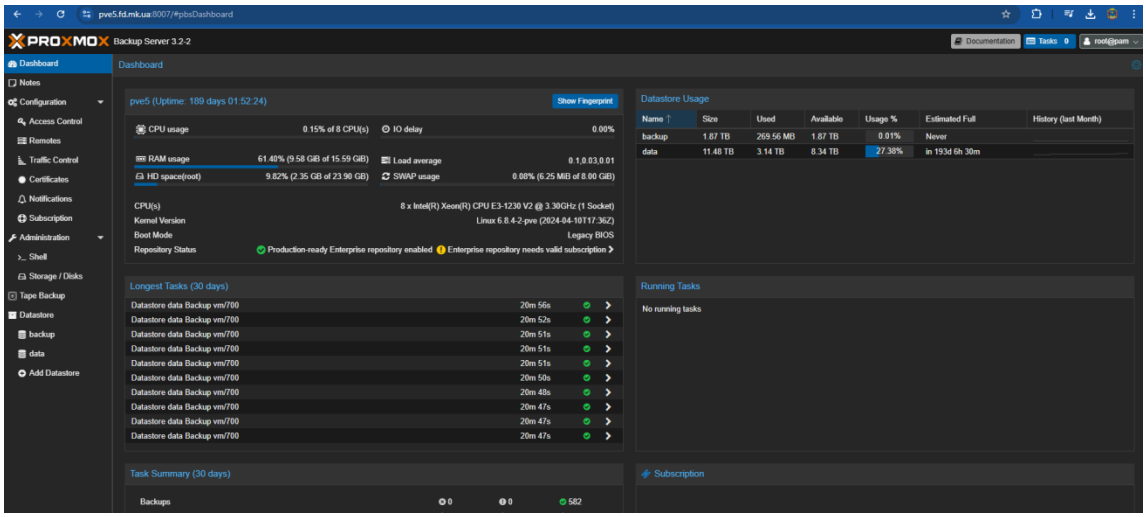


Рисунок 2.3 – Інтерфейс ProxMox Backup Server 3.2-2

Важливою перевагою є можливість відновлення на рівні об'єкта, тобто ви можете відновити не тільки всю віртуальну машину, а й окремі файли або директорії. Платформа підтримує зберігання резервних копій на локальних дисках, мережевих сховищах або в хмарних сервісах, що забезпечує гнучкість у виборі місця зберігання.

Завдяки можливості планування та автоматизації, резервне копіювання відбувається регулярно і без втручання адміністратора.

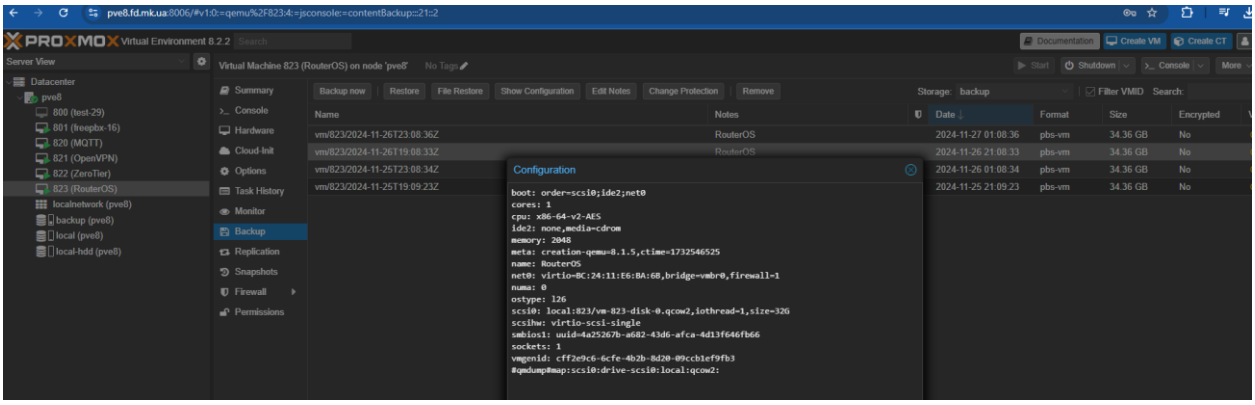


Рисунок 2.4 – Інтерфейс інформації про резервну копію VPS у PVE

Переваги використання Proxmox Backup Server:

- Надійний захист даних: Запобігає втраті даних внаслідок збоїв, природних катаклізмів або кібератак.
- Швидке відновлення: Дозволяє відновити втрачені дані або повністю відновити систему.
- Економія дискового простору: Дедуплікація даних значно зменшує необхідний обсяг дискового простору.
- Підвищення продуктивності: Оптимізовані алгоритми забезпечують мінімальний вплив на продуктивність системи.
- Легкість у використанні: Інтуїтивний веб-інтерфейс та автоматизація роблять роботу з Proxmox Backup Server доступною навіть для неспеціалістів.

Отже, Proxmox Backup Server є незамінним інструментом для забезпечення надійного резервного копіювання вашої віртуальної

інфраструктури, що працює на платформі Proxmox VE. Він пропонує широкий спектр функцій, високу продуктивність та легкість у використанні.

2.2. Мережеве програмне забезпечення

Мережеве програмне забезпечення: протоколи маршрутизації, управління мережею

Мережеве програмне забезпечення відіграє ключову роль у інформаційних системах, забезпечуючи ефективну передачу даних та безпеку мереж. До основних категорій мережевого програмного забезпечення належать: протоколи маршрутизації, системи управління мережею та системи виявлення вторгнень.

Протоколи маршрутизації визначають правила передачі даних між мережами. Вони відповідають за вибір оптимального шляху для пакетів даних, забезпечуючи надійну та ефективну доставку інформації.

Системи управління мережею дозволяють адміністраторам конфігурувати, моніторити та керувати мережевими пристроями та сервісами. Вони надають інструменти для налаштування мережевих параметрів, діагностики проблем та оптимізації продуктивності мережі.

Системи виявлення вторгнень призначені для виявлення несанкціонованого доступу до мережі або системи. Вони аналізують мережевий трафік та систему на наявність ознак атак, таких як сканування портів, спроби проникнення та інші загрози.

RouterOS та ***SWoS*** є прикладами операційних систем, які широко використовуються в мережевому обладнанні. RouterOS, розроблена компанією MikroTik, є популярною операційною системою для маршрутизаторів, що забезпечує широкий спектр функціональних можливостей, включаючи маршрутизацію, брандмауер, VPN та інші сервіси. SWoS (Software-Defined WAN Operating System) є програмно-визначеною

операційною системою для мереж WAN, що дозволяє централізовано керувати великими мережами і забезпечувати високу гнучкість конфігурації.

Обидві операційні системи, RouterOS та SWoS, надають потужні інструменти для управління мережами та забезпечення їх безпеки.

RouterOS – це спеціалізована операційна система, створена на основі Linux, яка призначена для роботи на маршрутизаторах. Вона була розроблена латвійською компанією MikroTik і стала популярною завдяки своїй гнучкості, широким можливостям та відносно невисокій вартості.

Вбудований фаєрвол дозволяє ефективно контролювати вхідний та вихідний трафік, фільтрувати пакети за різними критеріями, створювати правила NAT (Network Address Translation) та забезпечувати високий рівень безпеки мережі.

RouterOS підтримує різноманітні протоколи VPN , такі як PPTP, L2TP, IPsec, що забезпечує створення безпечних тунелів для передачі даних.

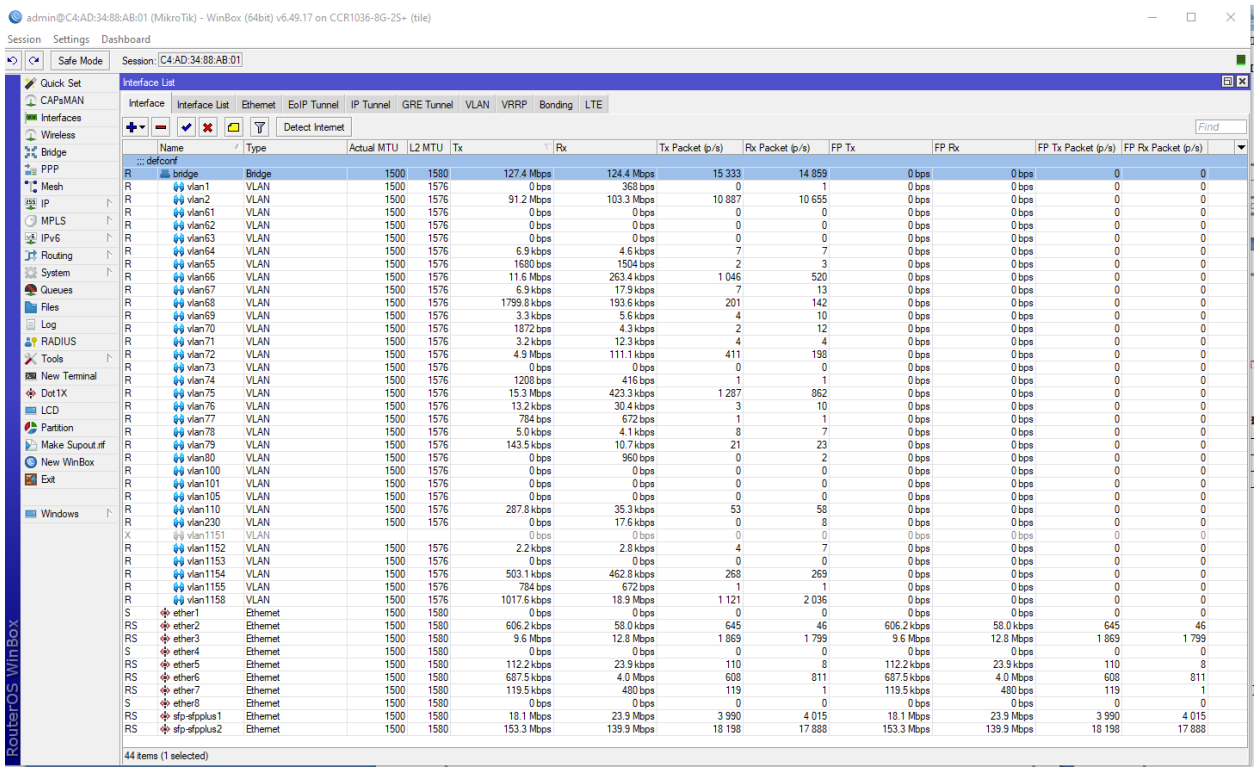


Рисунок 2.5 – Інтерфейс Winbox RourOS від Mikrotik

Багато моделей маршрутизаторів MikroTik підтримують бездротові стандарти Wi-Fi, що дозволяє створювати бездротові мережі та керувати ними за допомогою RouterOS. Функція QoS (Quality of Service) дозволяє пріоритезувати певний тип трафіку (наприклад, VoIP або відео), забезпечуючи його більш плавну роботу.

RouterOS може працювати як динамічний DNS-сервер, що дозволяє присвоювати динамічним IP-адресам статичні доменні імена. Мова скриптів RouterOS дозволяє автоматизувати багато завдань і створювати складні конфігурації.

RouterOS знайшла широке застосування серед системних адміністраторів для налаштування складних мереж, створення VPN-тунелів та оптимізації трафіку. Провайдери інтернет-послуг використовують RouterOS для побудови мереж доступу, управління трафіком та надання VPN-сервісів. Компанії обирають RouterOS для створення безпечних і надійних корпоративних мереж. Навіть ентузіасти використовують RouterOS для експериментів з мережевими технологіями.

RouterOS відрізняється високою гнучкістю, що дозволяє адаптувати систему під будь-які потреби. Вона відома своєю стабільністю і надійністю. І, що важливо, вартість ліцензій RouterOS є відносно невисокою.

Незважаючи на всі переваги, RouterOS має і деякі недоліки. Для новачків інтерфейс і можливості системи можуть здатися занадто складними. Крім того, код RouterOS не є відкритою, що обмежує можливості її модифікації.

SwOS (Switch Operating System) – це ОС, спеціально розроблена компанією MikroTik для управління її комутаторами. На відміну від RouterOS, яка орієнтована на маршрутизацію, SwOS фокусується на функціоналі, характерному для мережевих комутаторів.

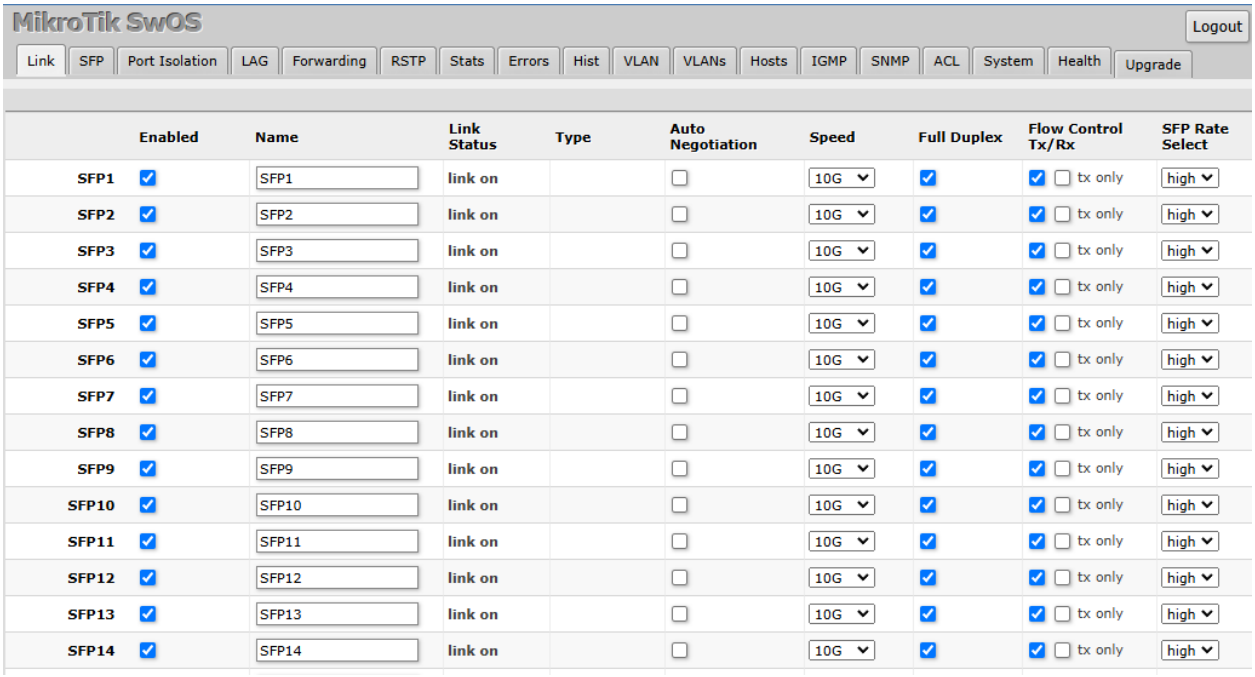


Рисунок 2.6 – Інтерфейс SWoS від Mikrotik

SwOS дозволяє конфігурувати різні аспекти роботи портів, такі як швидкість, дуплекс, VLAN, дзеркалювання трафіку та багато іншого. Підтримує створення віртуальних локальних мереж (VLAN), що дозволяє сегментувати мережу та підвищити її безпеку. Забезпечує управління якістю обслуговування (QoS), дозволяючи пріоритезувати певний тип трафіку. Також дозволяє фільтрувати мережевий трафік на основі MAC-адреси. Для запобігання циклів в мережі SwOS підтримує протокол Spanning Tree Protocol, а для агрегації декількох фізичних портів в один логічний – протокол Link Aggregation Control Protocol.

RouterOS – це універсальна операційна система для маршрутизації, тоді як SwOS спеціалізується на функціоналі комутаторів. SwOS має більш спрощений інтерфейс, оскільки його функціонал менш широкий, ніж у RouterOS. SwOS орієнтований на протоколи рівня 2 (Ethernet), тоді як RouterOS підтримує також протоколи рівня 3 (IP).

SwOS знайшла широке застосування серед системних адміністраторів для управління комутаторами в мережі, провайдерів інтернет-послуг для побудови мереж доступу та компаній для створення локальних мереж.

SwOS відрізняється простотою використання завдяки більш інтуїтивно зрозумілому інтерфейсу, ніж у RouterOS. Система відома своєю високою стабільністю. Також SwOS легко інтегрується з RouterOS, що дозволяє створювати комплексні мережеві рішення.

2.3. Програмне забезпечення систем безперебійного живлення

Програмне забезпечення для систем безперебійного живлення (UPS) – це незамінний інструмент для моніторингу, управління та контролю роботи ДБЖ. Воно забезпечує ефективне використання ДБЖ, захищає підключене обладнання від перебоїв в електромережі та допомагає уникнути втрати даних.

UPS Network Management Card 2 - це спеціалізована плата, яка встановлюється в деякі моделі систем безперебійного живлення для розширення їх функціональності та забезпечення віддаленого моніторингу. Ця карта перетворює ваш ДБЖ на інтегровану частину вашої IT-інфраструктури, надаючи вам повний контроль над його роботою.

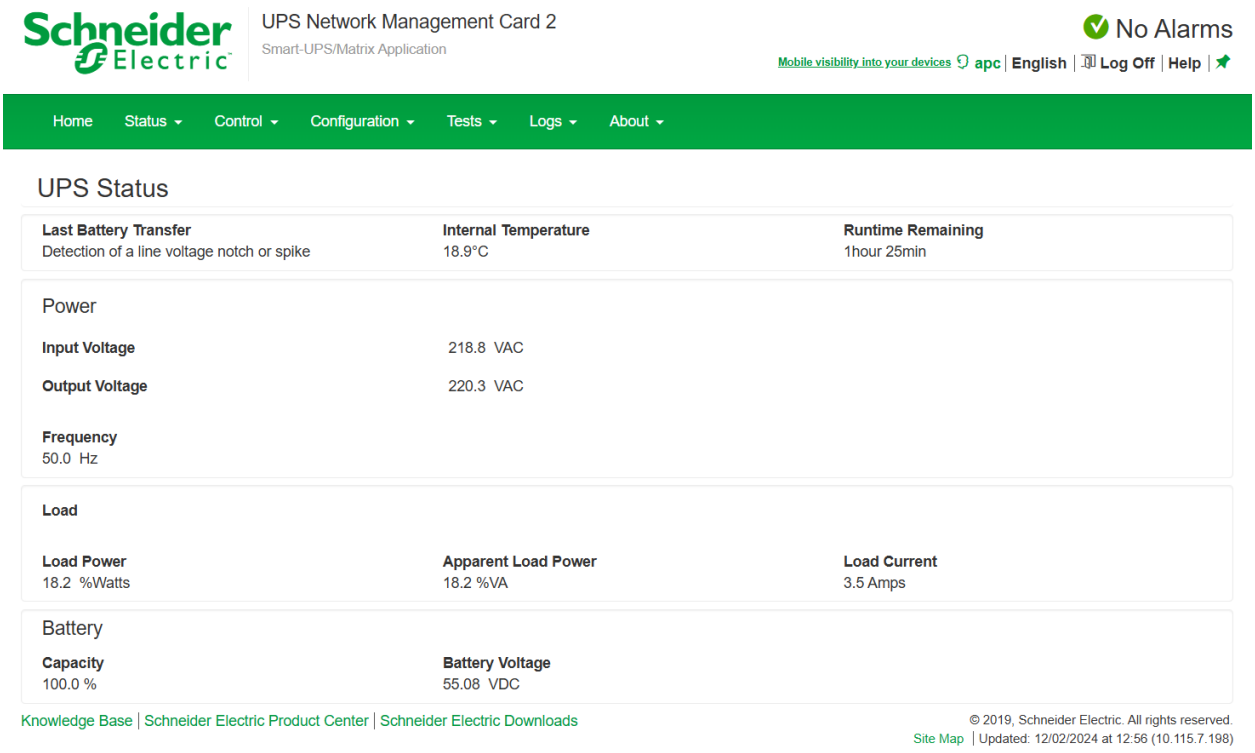


Рисунок 2.7 – Інтерфейс UPS Network Management Card 2 для Smart-UPS

Smart-UPS 5000 - це високопродуктивне мережеве джерело безперебійного живлення, розроблене для захисту критично важливого обладнання від перебоїв в електромережі та перенапруг. Воно є популярним вибором для бізнесу та дата-центрів завдяки своїм надійним функціям та довговічності.

Smart-UPS 5000 забезпечує чисту, безперервну електроенергію для чутливого електронного обладнання завдяки чистій синусоїдальній вихідній напрузі. Крім того, воно дозволяє збільшити час автономної роботи шляхом додавання додаткових батарейних модулів. Мережеве управління забезпечує віддалений моніторинг та керування через мережеві інтерфейси, що значно спрощує процес управління. Автоматичне регулювання напруги (AVR) коригує низькі та високі значення напруги без розряджання батареї, забезпечуючи стабільну роботу підключеного обладнання. Холодний пуск дозволяє забезпечити живлення підключеного обладнання навіть за відсутності мережевої напруги, а функція заміни батарей без зупинки дозволяє замінювати батареї без відключення ДБЖ. Розширене управління батареями максимізує термін служби та продуктивність батарей.

Smart-UPS 5000 знайшов широке застосування в різних сферах. У дата-центрах він захищає сервери, системи зберігання даних та мережеве обладнання. У телекомунікаціях забезпечує безпеку мережевої інфраструктури, маршрутизаторів та комутаторів. В охороні здоров'я захищає медичне обладнання та дані пацієнтів. У фінансових установах захищає критично важливі системи та запобігає втраті даних.

При виборі відповідної моделі Smart-UPS 5000 слід враховувати кілька факторів. Номінальна потужність (ВА) визначає, яке обладнання може бути підключено до ДБЖ. Час автономної роботи вказує, як довго ДБЖ зможе забезпечувати живлення при відключенні електроенергії. Вхідна та вихідна напруга повинні відповідати параметрам вашої електромережі та

підключеного обладнання. Можливості мережевого управління дозволяють віддалено контролювати та моніторити роботу ДБЖ.

Ретельно зваживши всі ці фактори, використаємо модель Smart-UPS 5000 для захисту критично важливого обладнання та забезпечення безперебійної роботи серверного обладнання.

WinPower View – це мобільний додаток, розроблений для зручного та ефективного віддаленого моніторингу системам безперебійного живлення. Завдяки цьому додатку ви можете легко контролювати робочий стан ваших ДБЖ, своєчасно отримувати сповіщення про збої та спрощувати процес технічного обслуговування.

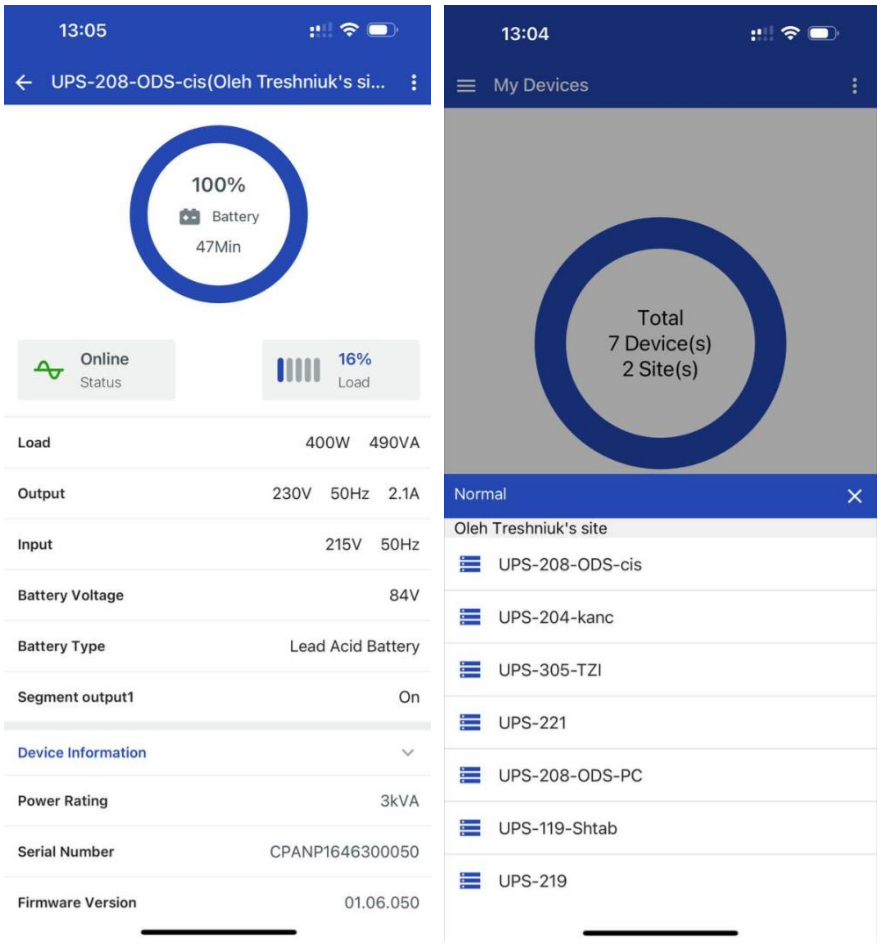


Рисунок 2.8 – Інтерфейс WinPower View

Додаток надсилає своєчасні сповіщення про будь-які збої або відхилення від нормальної роботи ДБЖ. Ви також можете налаштувати

регулярні тести самоперевірки акумуляторів, щоб переконатися в їхній працездатності та своєчасно виявити потенційні проблеми.

WinPower View спрощує процес технічного обслуговування ДБЖ, дозволяючи легко відстежувати історію подій.

Інтуїтивно зрозумілий інтерфейс дозволяє легко освоїти додаток навіть недосвідченим користувачам. Своєчасне виявлення та усунення проблем дозволяє уникнути несподіваних збоїв в роботі обладнання. А завдяки мобільності, ви можете контролювати ДБЖ з будь-якого пристрою з доступом до інтернету.

WinPower View буде корисний як системним адміністраторам для ефективного управління великою кількістю ДБЖ в мережі, так і керівникам підприємств для контролю стану критично важливого обладнання. Навіть власники малого бізнесу зможуть захистити своє обладнання від перепадів напруги та забезпечити безперебійну роботу.

WinPower View є незамінним помічником для моніторингу телекомунікаційних шаф обладнаних джерелом безперебійного живлення Power Walker 3000 Model Name RT 3K дозволяючи відслідковувати стан обладнання.

Програмне забезпечення **Tesla Powerwall 2.0** дозволяє ефективно керувати накопиченою енергією, відстежувати її використання та налаштовувати систему під свої потреби.

Ви можете відстежувати рівень заряду батареї, споживання енергії в домі, генерацію сонячної енергії та інші важливі параметри в будь-який час. Програмне забезпечення дозволяє вам вибирати різні режими роботи Powerwall, такі як резервне копіювання, самоспоживання, піковий зсув та інші. Воно також аналізує ваші звички споживання енергії та пропонує оптимальні стратегії для максимального використання сонячної енергії.

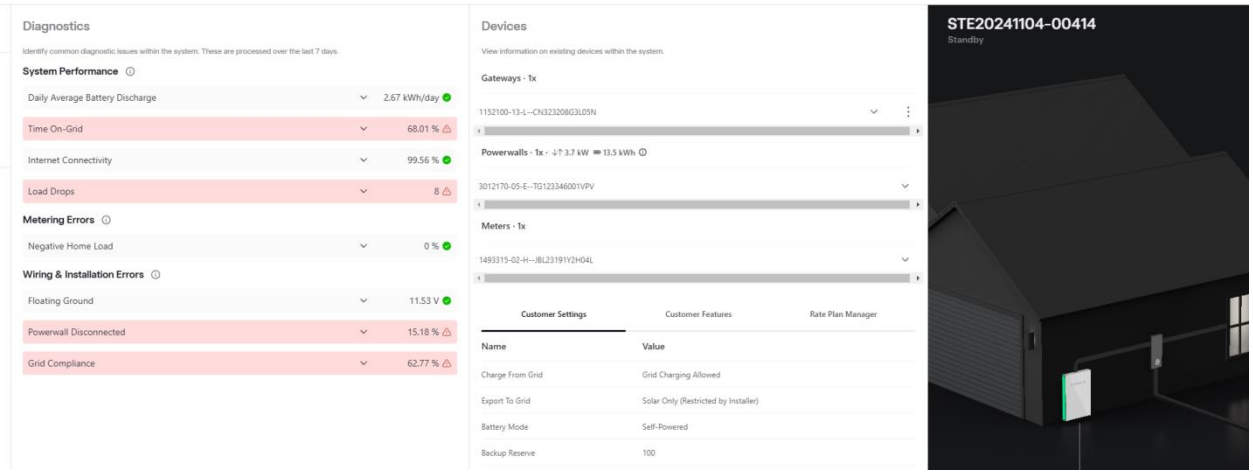


Рисунок 2.9 – Інтерфейс https://powerhub.energy.tesla.com/

Powerwall може інтегруватися з іншими системами "розумного дому", такими як термостати, освітлення та системи безпеки, що дозволяє автоматизувати процеси та підвищити енергоефективність. Tesla регулярно випускає оновлення ПЗ, які додають нові функції та покращують продуктивність системи.

Ви можете керувати Powerwall 2.0 за допомогою мобільного додатка Tesla, веб-інтерфейсу або навіть голосових команд через сумісні з Tesla пристрої.

Інтуїтивно зрозумілий інтерфейс дозволяє легко освоїти систему навіть недосвідченим користувачам. Широкі можливості налаштування дозволяють адаптувати систему під будь-які потреби. Завдяки програмному забезпеченню Tesla Powerwall 2.0, ви можете легко перейти на використання відновлюваних джерел енергії та досягти енергетичної незалежності.

Програмне забезпечення для UPS - це потужний інструмент, який розширює функціональність звичайного джерела безперебійного живлення. Воно перетворює простий пристрій на розумну систему, яка не тільки захищає ваше обладнання від перепадів напруги, але й дозволяє ефективно керувати ним та отримувати детальну інформацію про його роботу.

Програмне забезпечення для систем безперебійного живлення (UPS) відкриває широкі можливості для ефективного управління та моніторингу

цих систем. Воно дозволяє відстежувати різноманітні параметри UPS, такі як рівень заряду батарей, напругу, частоту та температуру.

Програмне забезпечення також надає гнучкі можливості керування режимами роботи UPS. Ви можете налаштувати автоматичне перемикання між різними режимами роботи (нормальний, резервний, байпас) за розкладом або за певними умовами. Це дозволяє оптимізувати роботу UPS та забезпечити максимальну надійність електропостачання.

Однією з важливих функцій програмного забезпечення є своєчасне інформування користувача про зміни стану UPS. Ви можете налаштувати отримання сповіщень про різні події, такі як низький рівень заряду батарей, перевантаження, відключення електроенергії тощо. Сповіщення можуть надсилатися різними способами: звуковими сигналами, повідомленнями на екран, електронною поштою.

Для забезпечення безперебійної роботи підключеного обладнання, програмне забезпечення для UPS може автоматично зберігати дані та коректно завершувати роботу програм у разі відключення електроенергії. Це дозволяє уникнути втрати важливої інформації та пошкодження обладнання.

Сучасні рішення для управління UPS підтримують інтеграцію з іншими системами. Це дозволяє створити єдину інформаційну систему, що включає в себе UPS, системи моніторингу, системи керування будівлями та інше обладнання. Така інтеграція забезпечує комплексне управління інфраструктурою та підвищує ефективність.

ПЗ для UPS дозволяє аналізувати дані про роботу системи для виявлення трендів, прогнозування можливих проблем та оптимізації роботи. Це допомагає своєчасно виявляти та усувати потенційні неполадки, підвищуючи надійність системи.

Багато сучасних рішень для управління UPS підтримують автоматизацію рутинних операцій. Наприклад, програмне забезпечення може автоматично виконувати щоденну перевірку стану батарей,

перезавантажувати систему при виявленні помилок або виконувати інші дії за розкладом.

Висновки

Проведений огляд програмного забезпечення дозволив нам детально ознайомитися з широким спектром доступних рішень та їх можливостями. Аналіз показав, що сучасний програмний ринок пропонує різноманітні інструменти, які відповідають потребам як малих підприємств, так і великих корпорацій.

Особливу увагу привернули рішення, що базуються на хмарних технологіях, які забезпечують високу масштабованість та доступність. Вони дозволяють компаніям швидко адаптуватися до змін ринку та знижують витрати на інфраструктуру.

Крім того, помітна тенденція до інтеграції штучного інтелекту та машинного навчання в програмні продукти. Це відкриває нові можливості для автоматизації процесів, аналізу даних та прийняття рішень.

Однак, разом з перевагами, існують і певні виклики. Одним з них є постійна еволюція технологій, що вимагає від компаній регулярного оновлення програмного забезпечення та перенавчання персоналу. Крім того, важливою проблемою залишається забезпечення кібербезпеки, оскільки зростає кількість кібератак.

Підсумовуючи, можна сказати, що сучасний програмний ринок пропонує широкий вибір рішень, які дозволяють автоматизувати бізнес-процеси, підвищити ефективність роботи та отримати конкурентні переваги. Однак, для успішного використання програмного забезпечення необхідно ретельно аналізувати потреби бізнесу, вибирати оптимальні рішення та забезпечувати їх безпеку.

					171.6321М.КР.ПЗ.РЗ		
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*			
Розробник		Трешнюк О. І.			Впровадження мережевої інфраструктури.	*Літ.*	*Арк.* 43 / *Аркушів*
Консультант							
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова	
Керівник		Дьяконов О. С.					
Зав. каф.		Рябенький В. М.					

РОЗДІЛ 3. ВПРОВАДЖЕННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

3.1. Створення локальної мережі.

Локальна мережа – це об'єднання кількох комп'ютерів та інших пристроїв (принтери, сканери тощо) в єдину систему для обміну даними. LAN може бути дротовою (за допомогою Ethernet-кабелів) або бездротовою (Wi-Fi).

Локальна мережа значно спрощує роботу та обмін інформацією в межах одного приміщення або будівлі. Вона дозволяє обмінюватися файлами, документами та мультимедійним контентом між різними пристроями. Завдяки локальній мережі можна організувати спільний доступ до периферії, що значно підвищує зручність використання. Крім того, локальна мережа дозволяє створити єдину точку доступу до Інтернету для всіх пристроїв, а також організувати власні сервери для зберігання даних, веб-сервісів та баз даних.

Процес створення локальної мережі включає кілька етапів:

1. Підключення: Комп'ютери підключаються до мережі бездротово через Wi-Fi або за допомогою Ethernet-кабелів.
2. Налаштування: Кожному пристрою присвоюється унікальна IP-адреса, маска підмережі, вказується шлюз та DNS-сервери.
3. Створення робочої групи: Всі комп'ютери об'єднуються в одну робочу групу.
4. Налаштування спільного доступу: Визначаються папки та пристрої, якими будуть користуватися всі в мережі.
5. Перевірка підключення: Перевіряється, чи всі пристрої бачать один одного в мережі.

Виходячи з великої кількості мережевих пристроїв, таких як сервери зберігання даних, сервери баз даних, Wi-Fi мережі та підключення підрозділів проведемо модернізацію локальної мережі. Перехід з традиційних мідних мереж Ethernet на оптичні волоконні мережі є

стратегічним рішенням для багатьох організацій. Оптичні мережі пропонують ряд переваг, які роблять їх більш привабливими для сучасних вимог до швидкості передачі даних, надійності та масштабованості:

- Вища пропускна здатність: Оптичні волокна здатні передавати дані на значно більших швидкостях, ніж мідні кабелі, що дозволяє ефективно обробляти великі обсяги даних.
- Менші втрати сигналу: Оптичні сигнали менше схильні до перешкод та затухання, що забезпечує більш стабільну та надійну передачу даних на великі відстані.
- Більша безпека: Оптичні кабелі важче прослуховувати, що підвищує рівень безпеки переданих даних.
- Імунітет до електромагнітних перешкод: Оптичні волокна не схильні до впливу електромагнітних полів, що робить їх ідеальним рішенням для промислових середовищ та місць з високим рівнем електромагнітних перешкод.
- Довговічність: Оптичні волокна мають тривалий термін служби і не схильні до корозії.

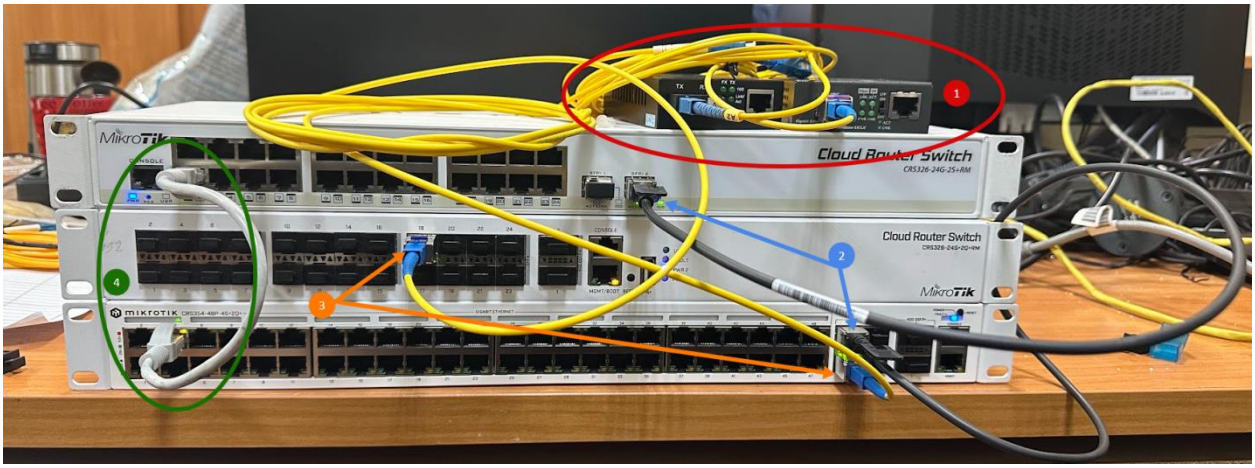


Рисунок 3.1 – Типи підключення комутаторів

Розглянемо основні способи підключення комутаторів:

Оптичні медіаконвертери (1 на рис 3.1) – це мережеві пристрої, які виконую важливу функцію перетворення електричних сигналів, що передаються по мідному кабелю, в оптичні сигнали, які можуть передаватися по волоконно-оптичному кабелю, і навпаки. Завдяки цій здатності медіаконвертери дозволяють об'єднувати в єдину мережу різні типи кабелів, розширюючи можливості та відстані передачі даних.

DAC (Direct Attach Copper) кабель, або кабель прямого підключення (2 на рис 3.1), є високошвидкісним мідним кабелем, який використовується для з'єднання мережевого обладнання на коротких відстанях. Він є альтернативою оптичним модулям і знайшов широке застосування в дата-центрах.

SFP+ (Enhanced Small Form-factor Pluggable) (3 на рис 3.1) – це компактні, гарячозамінні модулі, які використовуються для передачі даних в телекомунікаційних системах. Вони забезпечують високу швидкість передачі даних (до 10 Гбіт/с) і можуть працювати як з мідними, так і з оптичними кабелями. SFP+ модулі встановлюються в спеціальні слоти на мережевому обладнанні (комутаторах, маршрутизаторах тощо).

Кабель Ethernet (4 на рис 3.1) – кабель, по якому передаються дані в комп'ютерних мережах. Він являє собою пару або кілька пар мідних проводів, скручених певним чином для зменшення електромагнітних перешкод. Ethernet-кабелі широко використовуються для з'єднання комп'ютерів, мережевих пристроїв в локальних мережах.

Таблиця 3.1 – Порівняння основних типів підключення

Тип підключення	**Швидкість**	**Вартість**	**Відстань**	**Простота підключення**
медіаконвертер	10 Мбіт/с 100 Мбіт/с 1 Гбіт/с 10 Гбіт/с	Дорогий	Обмежується швидкістю кабелю Ethernet	Потребує додаткового активного обладнання
DAC	10 Гбіт/с 40 Гбіт/с 100 Гбіт/с	Дешевий	3-7 м 3-5 м 1-2 м	Простота у використанні, просто кабель
SFP+	1 Гбіт/с 10 Гбіт/с 100 Гбіт/с	Дорогий	Декілька десятків кілометрів по одномодовому волокну	Необхідно модулі SFP+ відповідного типу
Кабель Ethernet	10 Мбіт/с 100 Мбіт/с 1 Гбіт/с 10 Гбіт/с	Дешевий	До 100 м До 100 м До 100 м До 100 м	Застарілий тип підключення.

Виходячи з вартості підключення та швидкостей передачі даних, для з’єднання комутаторів в телекомунікаційній шафі будемо використовувати кабель прямого підключення, а для підключення комутаторів на великій відстані оптоволоконну мережу з SFP+ модулями.

Мережеве обладнання розмістимо в телекомунікаційній шафі, кінцеві користувачі підключимо за допомогою патч-панелі для централізованого підключення та організації мережевих кабелів. Вона слугує своєрідним "розподільчим щитом" для мережі, дозволяючи легко підключати,

відключати та перепідключати різні пристрої, проводи сховаємо у оргонайзер.

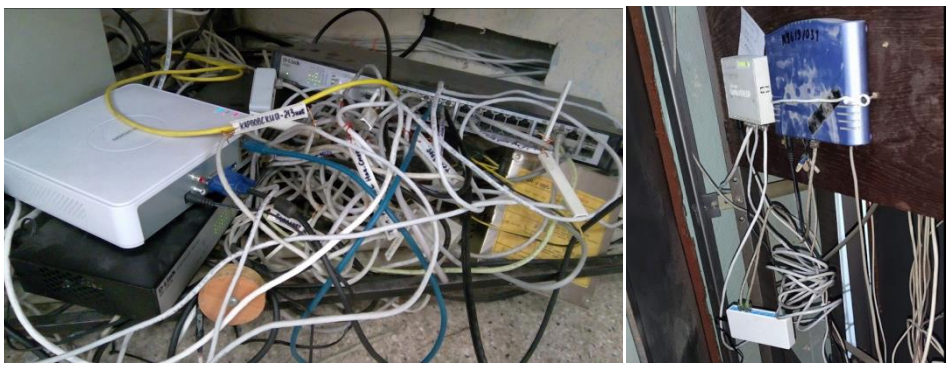


Рисунок 3.2 – Телекомунікаційне обладнання до оновлення

Рисунок 3.3 – Телекомунікаційна шафа після оновлення

3.2. Сегментація мережі, VLAN, VPN.

Сегментація мережі – це процес поділу великої комп'ютерної мережі на менші, ізольовані підмережі, або сегменти. Це дозволяє покращити продуктивність, безпеку та керованість мережі.

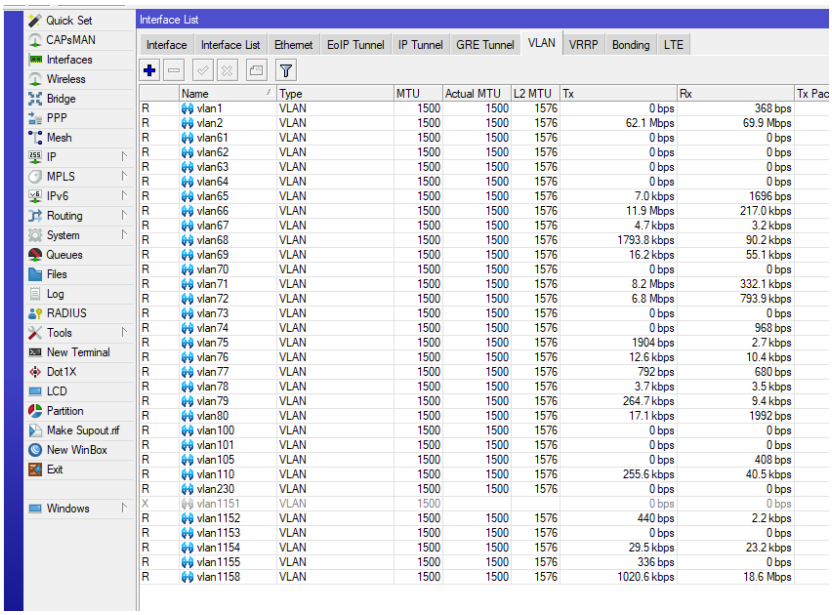
Сегментація мережі – це важливий процес, який дозволяє покращити роботу мережі в багатьох аспектах. По-перше, вона значно підвищує продуктивність мережі, зменшуючи навантаження на обладнання та кількість зіткнень пакетів даних. По-друге, сегментація є ефективним засобом

підвищення безпеки мережі, оскільки дозволяє ізолювати різні її частини та впроваджувати для кожної з них індивідуальні політики безпеки. Крім того, сегментація спрощує управління мережею, роблячи її більш зрозумілою та керованою.

Існує два основних способи сегментації мережі: фізична та логічна. Фізична сегментація передбачає використання спеціального мережевого обладнання, такого як комутатори, для розділення мережі на окремі сегменти. Логічна сегментація, у свою чергу, дозволяє створювати віртуальні мережі на одному фізичному сегменті за допомогою технології VLAN.

Сегментація мережі має безліч переваг. Вона дозволяє збільшити пропускну здатність мережі, підвищити її надійність і безпеку, а також спростити управління. Кожен сегмент мережі працює незалежно від інших, що зменшує ризик того, що проблема в одному сегменті призведе до збою всієї мережі. Крім того, сегментація дозволяє впроваджувати різні політики безпеки для різних сегментів, що підвищує загальний рівень безпеки мережі.

Для сегментації мережі Головного управління використаємо VLAN за допомогою правил в операційній системі RouterOS у Mikrotik CCR1036-8G-2S+



	Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx	Tx Pac
R	vlan1	VLAN	1500	1500	1576	0 bps	368 bps	
R	vlan2	VLAN	1500	1500	1576	62.1 Mbps	69.9 Mbps	
R	vlan61	VLAN	1500	1500	1576	0 bps	0 bps	
R	vlan62	VLAN	1500	1500	1576	0 bps	0 bps	
R	vlan63	VLAN	1500	1500	1576	0 bps	0 bps	
R	vlan64	VLAN	1500	1500	1576	0 bps	0 bps	
R	vlan65	VLAN	1500	1500	1576	7.0 kbps	1696 bps	
R	vlan66	VLAN	1500	1500	1576	11.9 Mbps	217.0 kbps	
R	vlan67	VLAN	1500	1500	1576	4.7 kbps	3.2 kbps	
R	vlan68	VLAN	1500	1500	1576	1793.8 kbps	90.2 kbps	
R	vlan69	VLAN	1500	1500	1576	16.2 kbps	55.1 kbps	
R	vlan70	VLAN	1500	1500	1576	0 bps	0 bps	
R	vlan71	VLAN	1500	1500	1576	8.2 Mbps	332.1 kbps	
R	vlan72	VLAN	1500	1500	1576	6.8 Mbps	793.9 kbps	
R	vlan73	VLAN	1500	1500	1576	0 bps	0 bps	
R	vlan74	VLAN	1500	1500	1576	0 bps	968 bps	
R	vlan75	VLAN	1500	1500	1576	1904 bps	2.7 kbps	
R	vlan76	VLAN	1500	1500	1576	12.6 kbps	10.4 kbps	
R	vlan77	VLAN	1500	1500	1576	792 bps	680 bps	
R	vlan78	VLAN	1500	1500	1576	3.7 kbps	3.5 kbps	
R	vlan79	VLAN	1500	1500	1576	264.7 kbps	9.4 kbps	
R	vlan80	VLAN	1500	1500	1576	17.1 kbps	1992 bps	
R	vlan100	VLAN	1500	1500	1576	0 bps	0 bps	
R	vlan101	VLAN	1500	1500	1576	0 bps	0 bps	
R	vlan105	VLAN	1500	1500	1576	0 bps	408 bps	
R	vlan110	VLAN	1500	1500	1576	255.6 kbps	40.5 kbps	
R	vlan230	VLAN	1500	1500	1576	0 bps	0 bps	
X	vlan1151	VLAN	1500			0 bps	0 bps	
R	vlan1152	VLAN	1500	1500	1576	440 bps	2.2 kbps	
R	vlan1153	VLAN	1500	1500	1576	0 bps	0 bps	
R	vlan1154	VLAN	1500	1500	1576	29.5 kbps	23.2 kbps	
R	vlan1155	VLAN	1500	1500	1576	336 bps	0 bps	
R	vlan1158	VLAN	1500	1500	1576	1020.6 kbps	18.6 Mbps	

Рисунок 3.4 – Сегментація мережі за допомогою VLAN

Мережу розділимо на відповідні сегменти, такі як серверне обладнання, обладнання для відеоспостереження, VoIP-телефонія, Wi-Fi мережа та відповідні структурні відділи.

Wi-Fi мережу створимо за допомогою технології **Mikrotik CAPsMAN (Controller Access Point System Manager),** яка дозволяє контролювати та керувати всіма бездротовими точками доступу MikroTik з одного місця. Це означає, що ви можете налаштувати всі параметри мережі, такі як SSID, паролі, радіочастоти, потужність сигналу тощо, для всіх точок доступу одночасно.

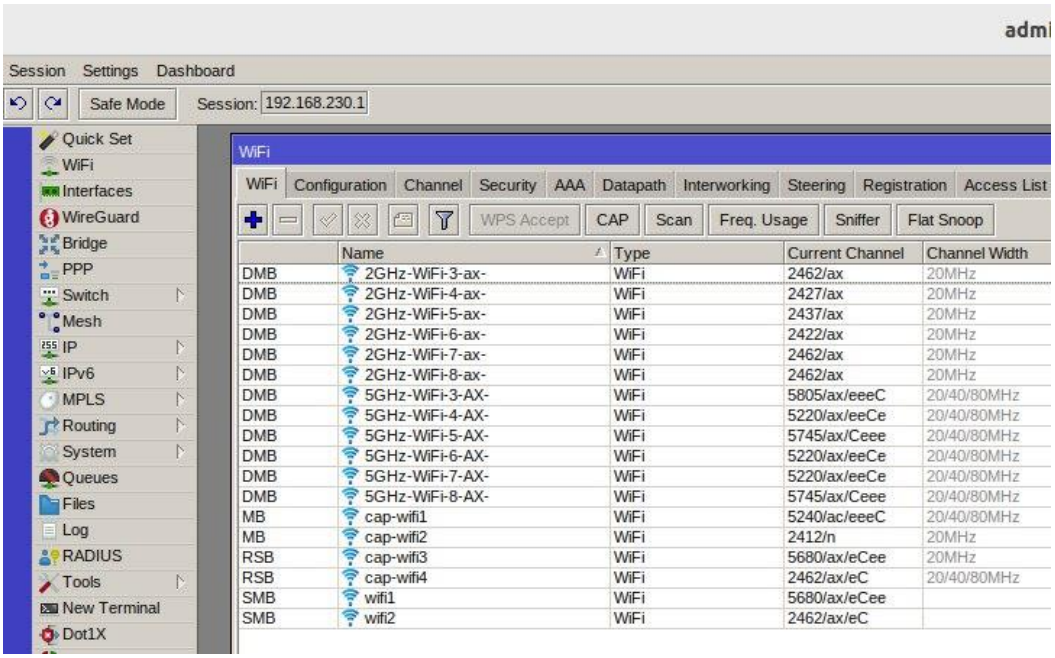
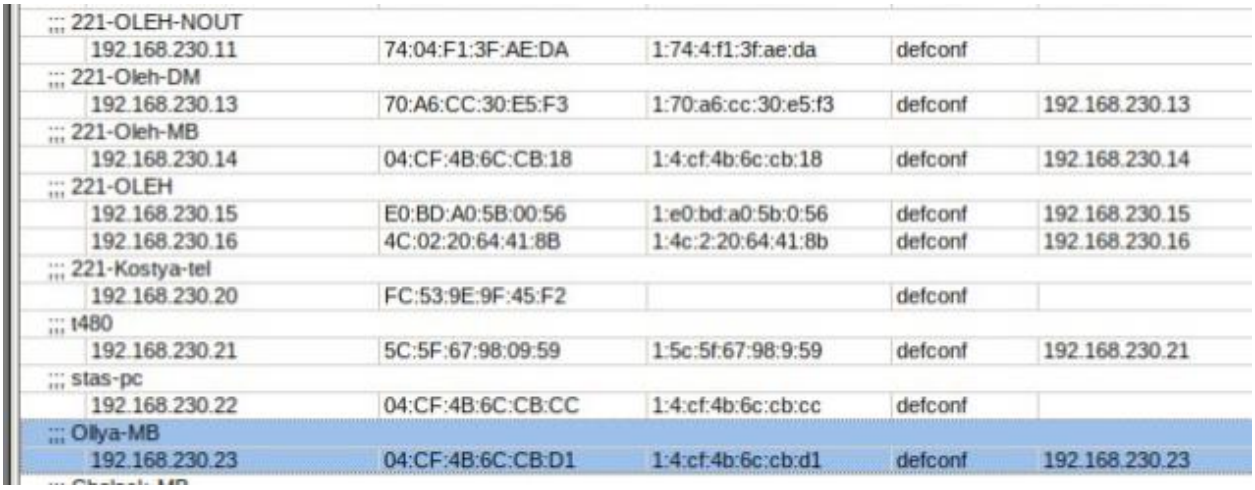


Рисунок 3.5 – Підключені 8 Wi-Fi точок доступу Mikrotik cAP ax

Для уникнення зашумленості мережі використаємо різні канали Wi-Fi як це вказано рис. 3.5. Вони поділяють частотний діапазон на менші частини, дозволяючи пристроям працювати більш ефективно та не заважати передачі даних між пристроями які підключені до різних точок доступу в межах їх бачення.

Так як це мережа організації, обмежимо доступ до інших сегментів мережі за допомогою VLAN та правил FireWall, а нових користувачів будемо

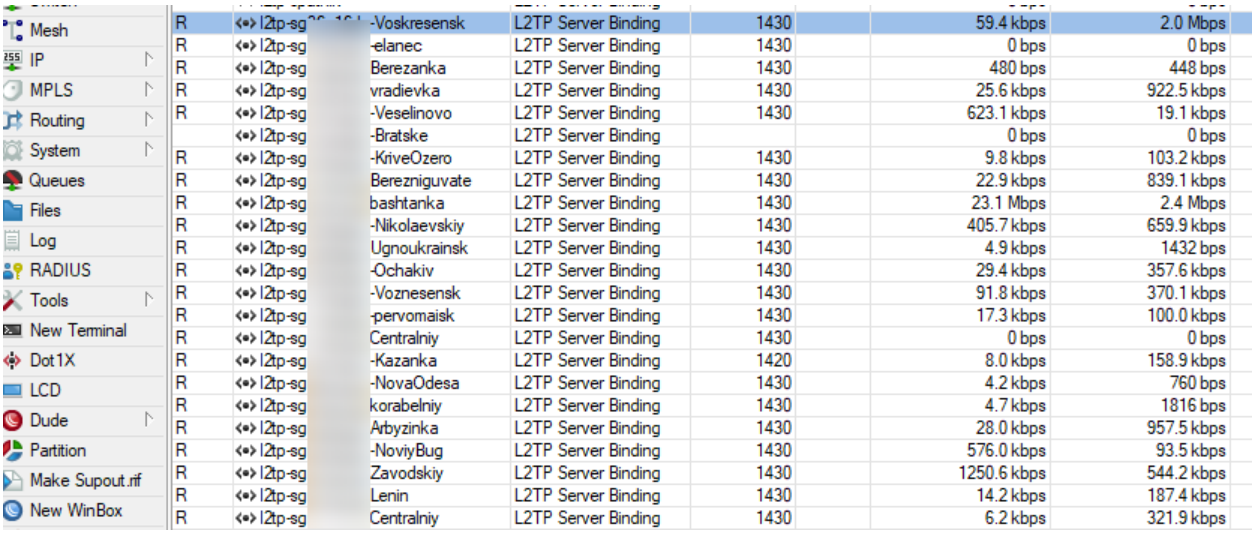
підключати після ознайомлення з політиками організації. Приклад авторизованих пристроїв можно побачити на рис. 3.6.



;;; 221-OLEH-NOUT				
192.168.230.11	74:04:F1:3F:AE:DA	1:74:4:f1:3f:ae:da	defconf	
;;; 221-Oleh-DM				
192.168.230.13	70:A6:CC:30:E5:F3	1:70:a6:cc:30:e5:f3	defconf	192.168.230.13
;;; 221-Oleh-MB				
192.168.230.14	04:CF:4B:6C:CB:18	1:4:cf:4b:6c:cb:18	defconf	192.168.230.14
;;; 221-OLEH				
192.168.230.15	E0:BD:A0:5B:00:56	1:e0:bd:a0:5b:0:56	defconf	192.168.230.15
192.168.230.16	4C:02:20:64:41:8B	1:4c:2:20:64:41:8b	defconf	192.168.230.16
;;; 221-Kostya-tel				
192.168.230.20	FC:53:9E:9F:45:F2		defconf	
;;; t480				
192.168.230.21	5C:5F:67:98:09:59	1:5c:5f:67:98:9:59	defconf	192.168.230.21
;;; stas-pc				
192.168.230.22	04:CF:4B:6C:CB:CC	1:4:cf:4b:6c:cb:cc	defconf	
;;; Olya-MB				
192.168.230.23	04:CF:4B:6C:CB:D1	1:4:cf:4b:6c:cb:d1	defconf	192.168.230.23

Рисунок 3.6 – Авторизовані пристрої на DHCP-сервері Mikrotik.

Підрозділи Головного управління підключимо до середовища для тестування мережевої інфраструктури за допомогою протоколу тунелювання другого рівня L2TP, який використовується для створення віртуальних приватних мереж (VPN). Іншими словами, L2TP дозволяє створити безпечне з'єднання між двома або більше мережами через Інтернет, ніби вони знаходяться фізично поруч.



R	l2tp-sg	-Voskresensk	L2TP Server Binding	1430	59.4 kbps	2.0 Mbps
R	l2tp-sg	-elanec	L2TP Server Binding	1430	0 bps	0 bps
R	l2tp-sg	Berezanka	L2TP Server Binding	1430	480 bps	448 bps
R	l2tp-sg	vradievka	L2TP Server Binding	1430	25.6 kbps	922.5 kbps
R	l2tp-sg	-Veselinovo	L2TP Server Binding	1430	623.1 kbps	19.1 kbps
	l2tp-sg	-Bratske	L2TP Server Binding		0 bps	0 bps
R	l2tp-sg	-KriveOzero	L2TP Server Binding	1430	9.8 kbps	103.2 kbps
R	l2tp-sg	Berezniguvate	L2TP Server Binding	1430	22.9 kbps	839.1 kbps
R	l2tp-sg	bashtanka	L2TP Server Binding	1430	23.1 Mbps	2.4 Mbps
R	l2tp-sg	-Nikolaevskiy	L2TP Server Binding	1430	405.7 kbps	659.9 kbps
R	l2tp-sg	Ugnoukrainsk	L2TP Server Binding	1430	4.9 kbps	1432 bps
R	l2tp-sg	-Ochakiv	L2TP Server Binding	1430	29.4 kbps	357.6 kbps
R	l2tp-sg	-Voznesensk	L2TP Server Binding	1430	91.8 kbps	370.1 kbps
R	l2tp-sg	-pervomaisk	L2TP Server Binding	1430	17.3 kbps	100.0 kbps
R	l2tp-sg	Centralniy	L2TP Server Binding	1430	0 bps	0 bps
R	l2tp-sg	-Kazanka	L2TP Server Binding	1420	8.0 kbps	158.9 kbps
R	l2tp-sg	-NovaOdesa	L2TP Server Binding	1430	4.2 kbps	760 bps
R	l2tp-sg	korabelniy	L2TP Server Binding	1430	4.7 kbps	1816 bps
R	l2tp-sg	Arbyzinka	L2TP Server Binding	1430	28.0 kbps	957.5 kbps
R	l2tp-sg	-NoviyBug	L2TP Server Binding	1430	576.0 kbps	93.5 kbps
R	l2tp-sg	Zavodskiy	L2TP Server Binding	1430	1250.6 kbps	544.2 kbps
R	l2tp-sg	Lenin	L2TP Server Binding	1430	14.2 kbps	187.4 kbps
R	l2tp-sg	Centralniy	L2TP Server Binding	1430	6.2 kbps	321.9 kbps

Рисунок 3.7 – Активні сесії серверу L2TP Mikrotik.

Сегментацію мережі підрозділів також здійснимо за допомогою підмереж IP, де кожному підрозділу задамо свій діапазон з маскою 255.255.255.0 як вказано на рис. 3.8.

i	AS	10.	01.0/24	l2tp-s	-Centralniy reachable	1
i	AS	10.	02.0/24	l2tp-s	-Centralniy reachable	1
i	AS	10.	03.0/24	l2tp-s	-Zavodskiy reachable	1
i	AS	10.	04.0/24	l2tp-s	-Lenin reachable	1
i	AS	10.	05.0/24	l2tp-s	-korabelniy reachable	1
i	AS	10.	06.0/24	l2tp-s	-Arbyzinka reachable	1
i	AS	10.	07.0/24	l2tp-s	-bashtanka reachable	1
i	AS	10.	08.0/24	l2tp-s	-Berezanka reachable	1
i	AS	10.	09.0/24	l2tp-s	-Berezniguvate reachable	1
i	AS	10.	10.0/24	l2tp-s	o-Bratske reachable	1
i	AS	10.	11.0/24	l2tp-s	o-Veselinovo reachable	1
i	AS	10.	12.0/24	l2tp-s	o-Voznesensk reachable	1
i	AS	10.	13.0/24	l2tp-s	-vradievka reachable	1
i	AS	10.	14.0/24	l2tp-1	reachable	1
i	AS	10.	15.0/24	l2tp-s	o-elanec reachable	1
i	AS	10.	16.0/24	l2tp-s	o-Voskresensk reachable	1
i	AS	10.	17.0/24	l2tp-s	o-Kazanka reachable	1
i	AS	10.	18.0/24	l2tp-s	o-KriveOzero reachable	1
i	AS	10.	19.0/24	l2tp-s	o-Nikolaevskiy reachable	1
i	AS	10.	20.0/24	l2tp-s	o-NoviyBug reachable	1
i	AS	10.	21.0/24	l2tp-s	o-NovaOdesa reachable	1
i	AS	10.	22.0/24	l2tp-s	o-Ochakiv reachable	1
i	AS	10.	23.0/24	l2tp-s	o-pervomaisk reachable	1
i	AS	10.	24.0/24	l2tp-2	urivka reachable	1
i	AS	10.	25.0/25	l2tp-s	-Ugnoukrainsk reachable	1

Рисунок 3.7 – Сегментація мережі підрозділів.

Для підключення мобільних пунктів управління використаємо аналогічну схему підключення за допомогою MikroTik LtAP mini LTE kit та мобільного зв’язку LTE або терміналів StarLink підключених до комутаторів Mikrotik.

Рисунок 3.8 – Мобільні пункти управління,
що задіяні на Миколаївщині

Для безпеки передачі інформації всі дані будемо шифрувати за допомогою IPsec – набору протоколів, призначених для забезпечення безпеки передачі даних по мережі Інтернет. Він працює на рівні мережі, додаючи до ваших даних додаткові шари захисту. Він забезпечує аутентифікацію, перевіряючи, хто саме відправляє дані, щоб запобігти підробці. Крім того, IPsec шифрує дані, роблячи їх незрозумілими для сторонніх осіб, забезпечуючи конфіденційність. Також він перевіряє, чи не були дані змінені під час передачі, гарантуючи їх цілісність. І, нарешті, IPsec захищає від повторної передачі, запобігаючи повторному використанню застарілих пакетів даних.

IPsec використовується для об'єднання віддалених офісів в єдину мережу та захисту конфіденційних даних, що передаються по Інтернету. Переваги IPsec полягають у високому рівні безпеки, гнучкості, сумісності з різним мережевим обладнанням та операційними системами, а також у масштабованості. IPsec працює в двох основних режимах: транспортному, де шифрується тільки дані, та тунельному, де шифрується весь IP-пакет.

На структурній схемі мережевої інфраструктури (рис 3.9) зображено локальну мережу між Головним управлінням, підрозділами та мобільними пунктами управління за допомогою обладнання Mikrotik з використанням провайдерів зв’язку, LTE та супутникових терміналів за допомогою l2tp. Завдяки чому ми маємо об'єднану мережу VoIP-телефонії, систему відео спостереження та доступ до локальних ресурсів з будь-якого місця дислокації.

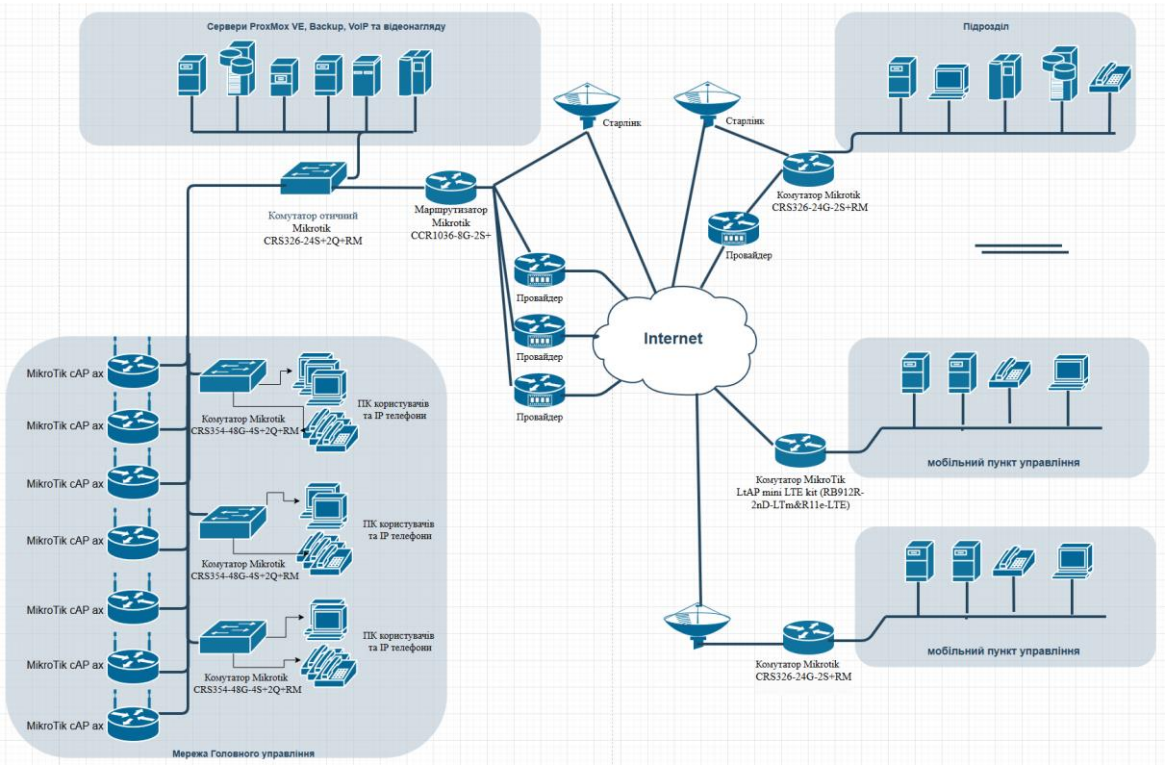


Рисунок 3.9 – Структурна схема мережевої інфраструктури

Для резервування мережевих каналів використаємо другий порт Mikrotik в який підключимо супутниковий термінал StarLink, для автоматичного переключення задамо пріорітет (рис. 3.10) більший за основного провайдера, таким чином, у разі відсутності активного з'єднання PPPoE від провайдера автоматично буде назначатись наступний за пріорітетом маршрут.

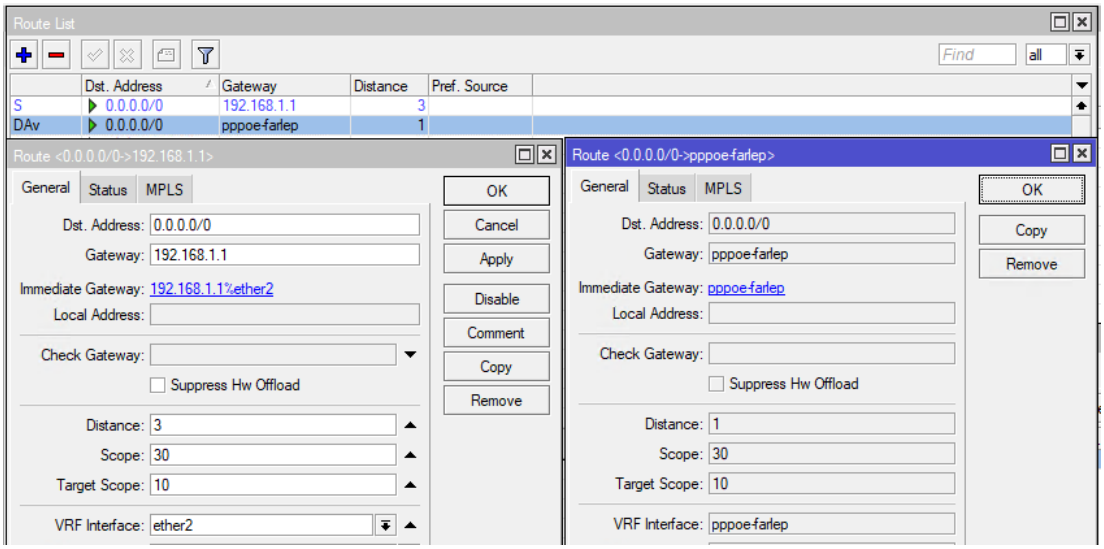


Рисунок 3.10 – Вкладка Route List

3.3. Підключення датчиків за допомогою протоколу LoRaWAN

LoRaWAN – це бездротовий мережевий протокол для побудови мереж Інтернету речей на великі відстані. Ця технологія ідеально підходить для пристроїв, які потребують тривалої роботи від батареї та передачі невеликих обсягів даних.

Одна з ключових особливостей LoRaWAN – це велика дальність дії сигналу. Він може поширюватися на відстань до кількох кілометрів, що дозволяє покривати великі території. Крім того, технологія LoRaWAN відрізняється низьким енергоспоживанням, завдяки чому пристрої можуть працювати роками від батареї. Ще одна важлива характеристика – проникна здатність сигналу, який добре проходить через стіни та інші перешкоди. Мережі LoRaWAN також легко масштабуються, дозволяючи підключати велику кількість пристроїв.

Завдяки своїм характеристикам, LoRaWAN знаходить широке застосування в різних сферах, зокрема в Інтернеті речей. Його використовують для створення розумних міст, де датчики збирають дані про освітлення, паркування, якість повітря тощо. У сільському господарстві LoRaWAN застосовується для моніторингу вологості ґрунту, температури та рівня води. В логістиці ця технологія використовується для відстеження вантажів та управління запасами. Також LoRaWAN знаходить застосування в енергетиці для збору даних з розумних лічильників та моніторингу стану мереж. Крім того, LoRaWAN активно використовується в індустріальному Інтернеті речей для моніторингу виробничих процесів та контролю якості продукції. І, звичайно ж, LoRaWAN знайшов своє місце в розумних будинках, де він використовується для автоматизації систем опалення, освітлення та безпеки.

Мережа LoRaWAN складається з кількох основних елементів. Це кінцеві пристрої – датчики, та інші пристрої, які збирають або передають дані. Шлюзи приймають сигнали від кінцевих пристроїв і передають їх на

сервер, який є централізованим елементом мережі. Сервер керує мережею, зберігає дані та забезпечує безпеку.

Одними з головних переваг LoRaWAN є низька вартість впровадження, гнучкість, довготривала робота пристроїв та легка масштабованість. Ці фактори роблять LoRaWAN перспективною технологією для розвитку Інтернету речей.

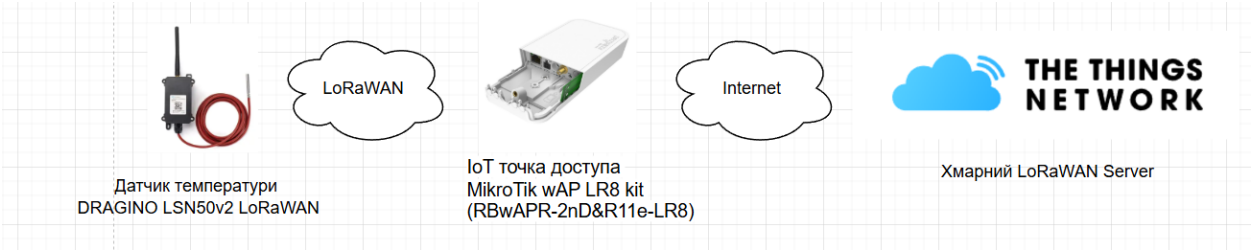


Рисунок 3.11 – схема підключення датчику до серверу

Конфігурація LoRa-шлюзу Mikrotik показана на рис. 3.12.

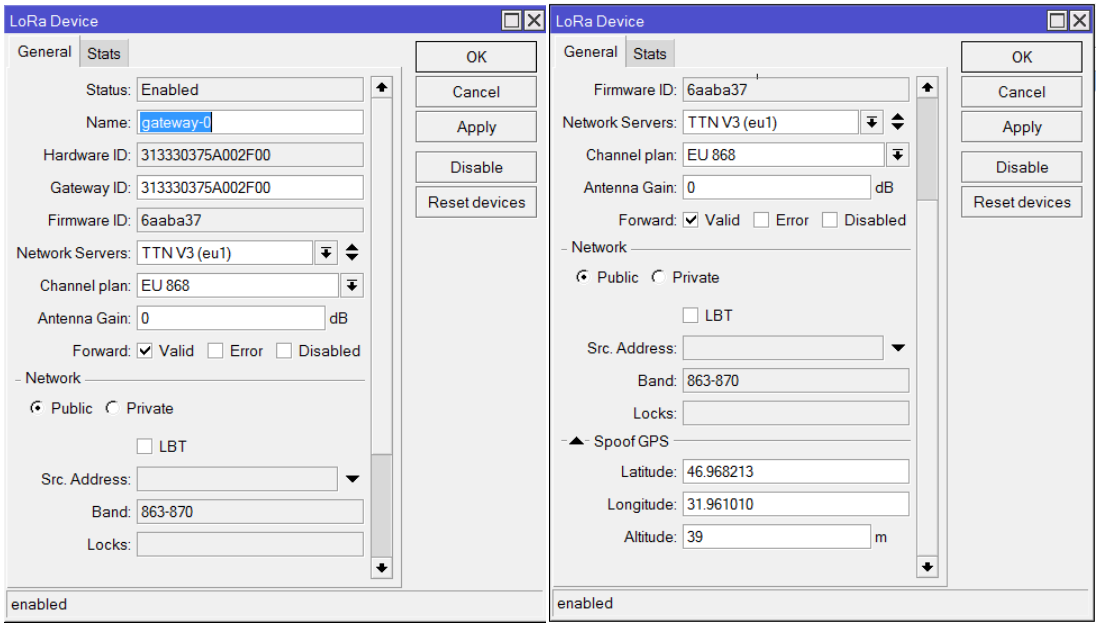
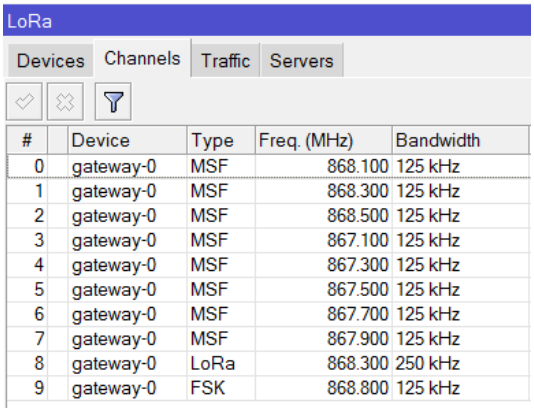


Рисунок 3.12 – Конфігурація LoRa-шлюзу Mikrotik

Канали з частотами, які використовуються для устаткування, зображено на рис. 3.13.

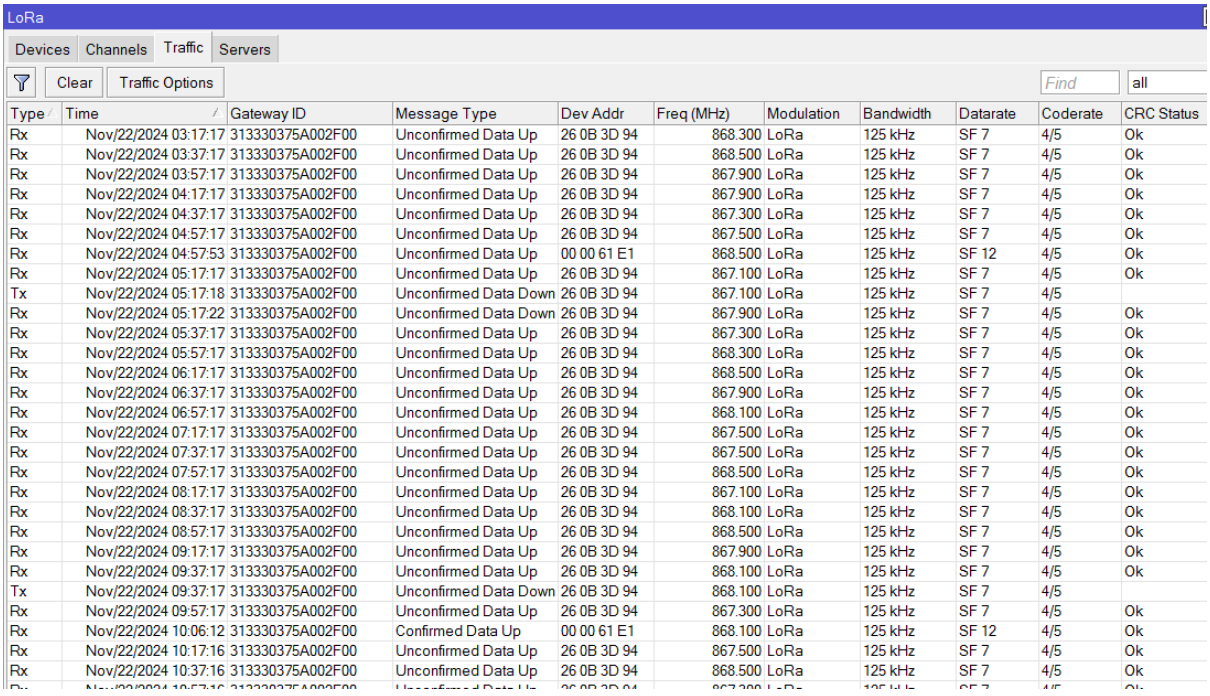


#	Device	Type	Freq. (MHz)	Bandwidth
0	gateway-0	MSF	868.100	125 kHz
1	gateway-0	MSF	868.300	125 kHz
2	gateway-0	MSF	868.500	125 kHz
3	gateway-0	MSF	867.100	125 kHz
4	gateway-0	MSF	867.300	125 kHz
5	gateway-0	MSF	867.500	125 kHz
6	gateway-0	MSF	867.700	125 kHz
7	gateway-0	MSF	867.900	125 kHz
8	gateway-0	LoRa	868.300	250 kHz
9	gateway-0	FSK	868.800	125 kHz

Рисунок 3.13 – Частотний план LoRa-шлюзу Mikrotik

Після проведення попередніх налаштувань та подачі живлення на датчик температури та вологості DRAGINO LSN50v2 у вкладці «Traffic» на Mikrotik можна спостерігати статистику за переданими та прийнятими пакетами LoRa (рис. 3.14).

По кожному пакету доступна повна інформація (рис. 3.14). З наведених прикладів видно, що адреса датчика температури та вологості в мережі LoRaWAN, що задана у шістнадцятковому форматі: 26 0B 3D 94.



Type	Time	Gateway ID	Message Type	Dev Addr	Freq (MHz)	Modulation	Bandwidth	Datarate	Coderate	CRC Status
Rx	Nov/22/2024 03:17:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	868.300	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 03:37:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	868.500	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 03:57:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.900	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 04:17:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.900	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 04:37:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.300	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 04:57:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.500	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 04:57:53	313330375A002F00	Unconfirmed Data Up	00 00 61 E1	868.500	LoRa	125 kHz	SF 12	4/5	Ok
Rx	Nov/22/2024 05:17:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.100	LoRa	125 kHz	SF 7	4/5	Ok
Tx	Nov/22/2024 05:17:18	313330375A002F00	Unconfirmed Data Down	26 0B 3D 94	867.100	LoRa	125 kHz	SF 7	4/5	
Rx	Nov/22/2024 05:17:22	313330375A002F00	Unconfirmed Data Down	26 0B 3D 94	867.900	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 05:37:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.300	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 05:57:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	868.300	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 06:17:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	868.500	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 06:37:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.900	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 06:57:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	868.100	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 07:17:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.500	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 07:37:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.500	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 07:57:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	868.500	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 08:17:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.100	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 08:37:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	868.100	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 08:57:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	868.500	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 09:17:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.900	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 09:37:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	868.100	LoRa	125 kHz	SF 7	4/5	Ok
Tx	Nov/22/2024 09:37:17	313330375A002F00	Unconfirmed Data Down	26 0B 3D 94	868.100	LoRa	125 kHz	SF 7	4/5	
Rx	Nov/22/2024 09:57:17	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.300	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 10:06:12	313330375A002F00	Confirmed Data Up	00 00 61 E1	868.100	LoRa	125 kHz	SF 12	4/5	Ok
Rx	Nov/22/2024 10:17:16	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	867.500	LoRa	125 kHz	SF 7	4/5	Ok
Rx	Nov/22/2024 10:37:16	313330375A002F00	Unconfirmed Data Up	26 0B 3D 94	868.500	LoRa	125 kHz	SF 7	4/5	Ok

Рисунок 3.14 – Інформація про Traffic

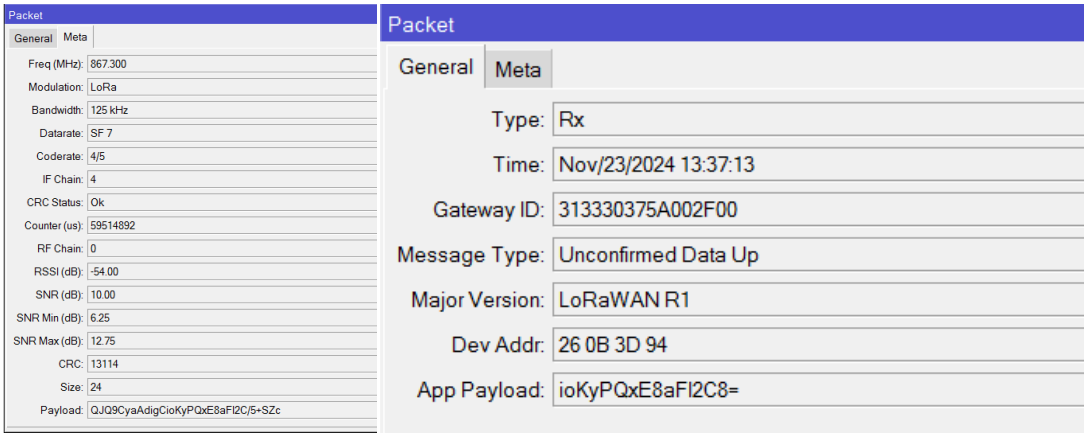


Рисунок 3.15 – Інформація про пакет

Перевіримо коректність роботи LoRaWAN за допомогою серверу The Things Network. Для цього створимо акант та авторизуємось на сервері.

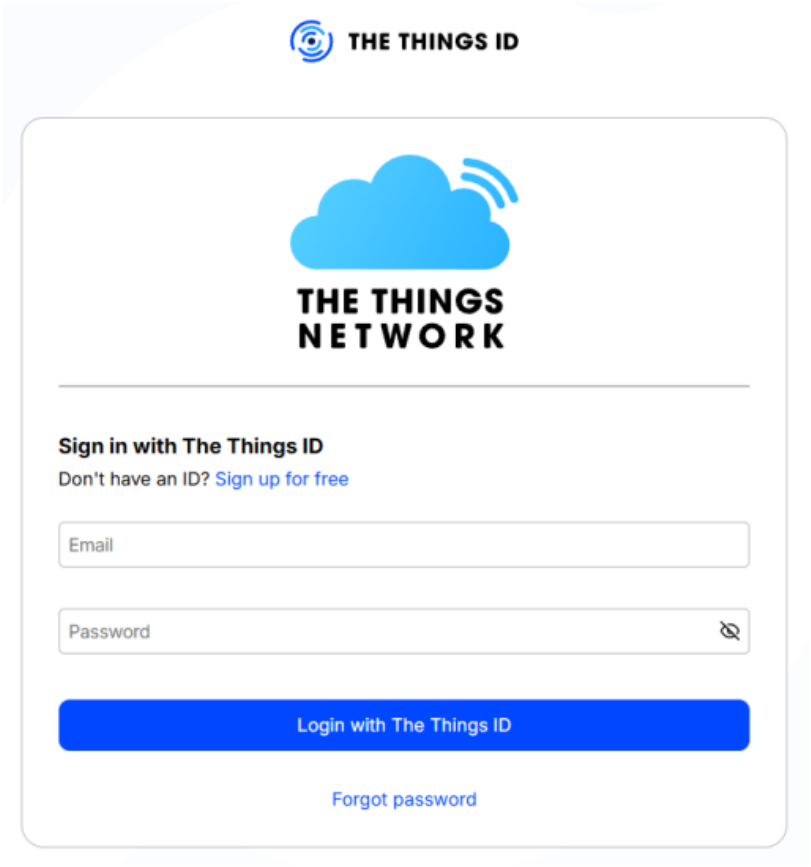


Рисунок 3.16 – Сторінка авторизації на сервері

На сервері The Things Network міститься загальна інформація про доданий шлюз LoRaWAN (рис. 3.17).

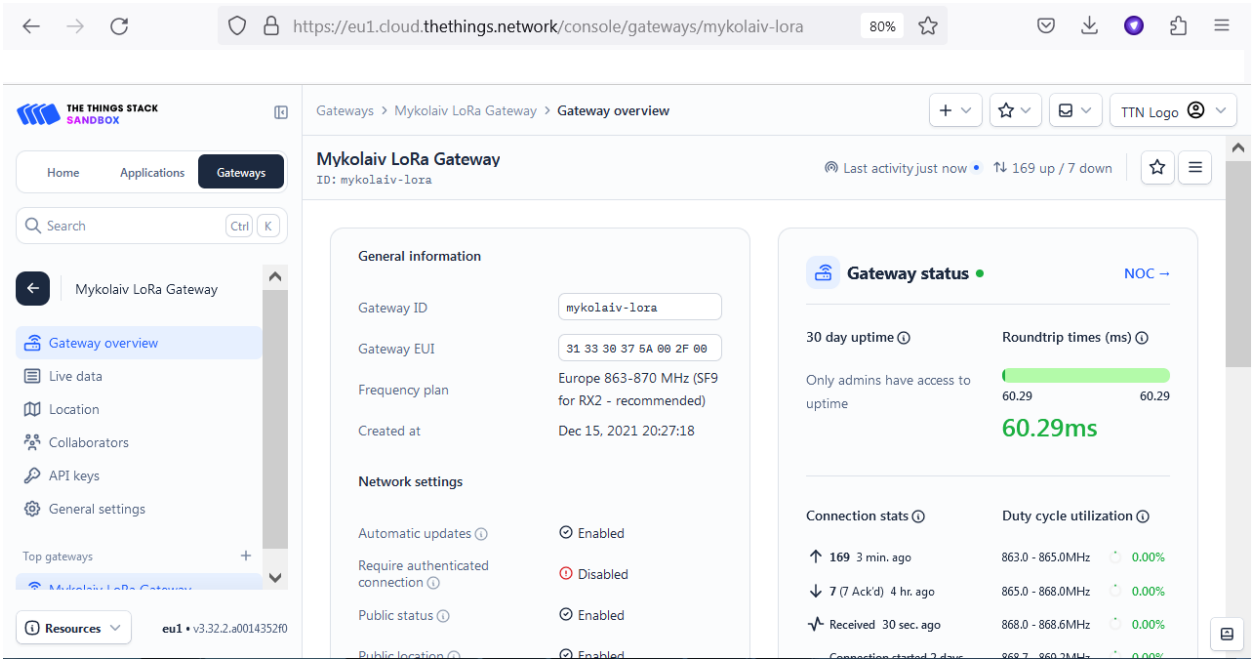


Рисунок 3.17 – Інформація про шлюз о LoRaWAN

Для обробки даних у вкладці «Application» було додано пристрій на основі готового шаблону LSN50V2. Лог отриманих даних з датчику DRAGINO LSN50v2 наведено на рис. 3.18.

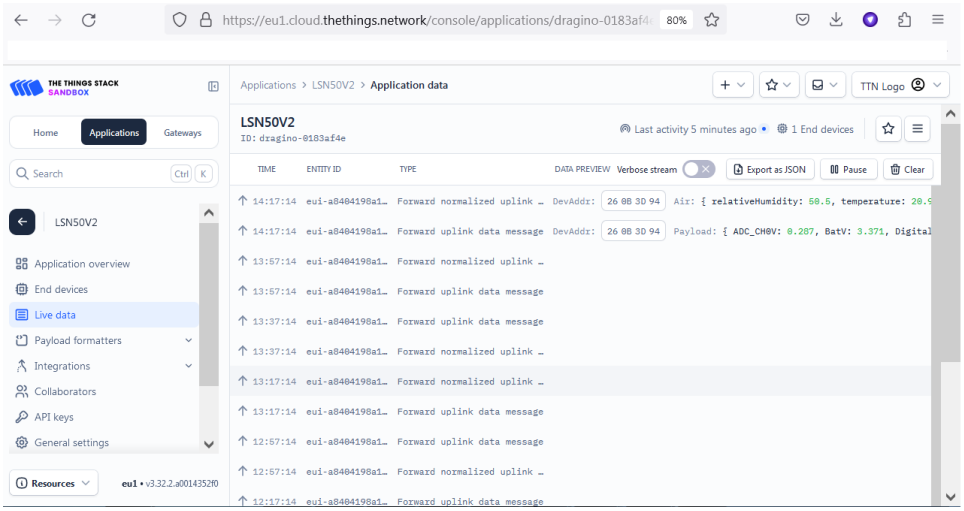


Рисунок 3.18 – Лог декодованих пакетів

Лог декодованих пакетів LoRaWAN – це запис усіх даних, які були успішно прийняті та розшифровані шлюзом LoRaWAN та передані на сервер.

Це детальний журнал, який містить інформацію про кожен окремий пакет даних, що надходить від пристроїв, підключених до мережі LoRaWAN.

Лог декодованих пакетів є незамінним інструментом для моніторингу роботи мережі, аналізу даних, виявлення та усунення неполадок, розробки та тестування додатків, а також забезпечення безпеки мережі. Він дозволяє відстежувати активність пристроїв, виявляти аномалії, отримувати цінну інформацію про роботу підключених пристроїв, швидко виявляти причини проблем зі зв'язком та вживати необхідних заходів.

Типовий лог містить інформацію про час прийняття пакету, ID шлюзу, DevEUI пристрою, ключ сеансу, порядковий номер пакету, дані пакету, силу прийнятого сигналу (RSSI), співвідношення сигнал/шум (SNR), маршрут пакету та коди помилок.

Для роботи з логом можна використовувати різні інструменти: текстові редактори для ручного перегляду, табличні процесори для сортування та візуалізації, ПЗ для аналізу даних LoRaWAN та інструменти командного рядка для обробки логу за допомогою скриптів.

Лог декодованих пакетів LoRaWAN є цінним джерелом інформації для розуміння роботи мережі та діагностики проблем. Ретельний аналіз логу дозволяє оптимізувати роботу мережі, підвищити її надійність та безпеку. Деталі логу DRAGINO LSN50v2 у додатках.

3.4. Системи моніторингу стану мережі.

Для моніторингу мережі будемо використовувати **Cacti** та **Nagios** – це дві системи моніторингу мереж та систем, кожна з яких має свої сильні сторони та підходить для різних завдань

Cacti – це відкрита платформа для моніторингу різноманітних IT-систем. Вона дозволяє збирати, аналізувати та візуалізувати дані про роботу мереж, серверів, баз даних та інших компонентів IT-інфраструктури.

Cacti збирає статистичні дані з різних джерел (сервери, мережеве обладнання, датчики тощо) за допомогою різних протоколів і відображає їх у вигляді зручних графіків, таблиць та діаграм. Це дозволяє легко відстежувати тенденції, виявляти аномалії та оцінювати загальний стан системи. Система підтримує створення кастомних дашбордів, які об'єднують найважливішу інформацію в одному місці. Крім того, Cacti може надсилати сповіщення про критичні ситуації та автоматизувати багато рутинних задач. Завдяки модульній архітектурі, Cacti легко адаптувати до конкретних потреб користувача за допомогою плагінів.

Популярність Cacti обумовлена кількома факторами: відкритим кодом, гнучкістю, великим співтовариством користувачів та простотою використання. Безкоштовне використання та можливість модифікації роблять Cacti доступним для широкого кола користувачів. Гнучка архітектура дозволяє адаптувати систему до різних середовищ. Активна спільнота користувачів постійно розробляє нові можливості та вирішує проблеми. Інтуїтивно зрозумілий інтерфейс та велика кількість готових шаблонів спрощують роботу з системою.

Cacti широко використовується для моніторингу мереж, серверів, баз даних, віртуальних машин та систем зберігання даних. За допомогою Cacti можна відстежувати пропускну здатність мережі, завантаження процесора, використання пам'яті, стан дисків та багато іншого. На рис. 3.18 вказані актуальні графіки навантаження мережі основного маршрутизатору Mikrotik CCR1036-8G-2S+.

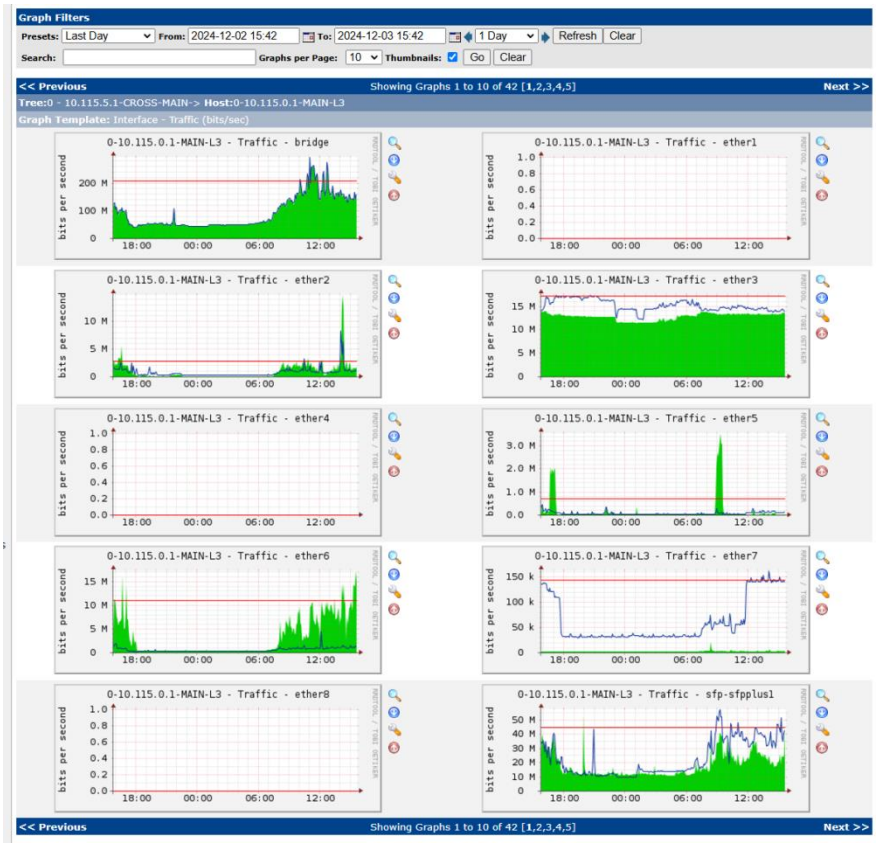


Рисунок 3.19 – Графіки навантаження мережі

Використання Cacti дозволяє проактивно вирішувати проблеми та знижувати витрати на обслуговування IT-інфраструктури. Своєчасне виявлення та усунення проблем дозволяє уникнути серйозних збоїв і забезпечити безперебійну роботу системи. На рис. 3.19 вказано версію використання SNMP, час роботи маршрутизатора, а також контактні дані пристрою. **SNMP (Simple Network Management Protocol)** – це стандартний інтернет-протокол для керування мережевими пристроями. Він дозволяє збирати інформацію про стан мережі, конфігурувати пристрої та виявляти проблеми.

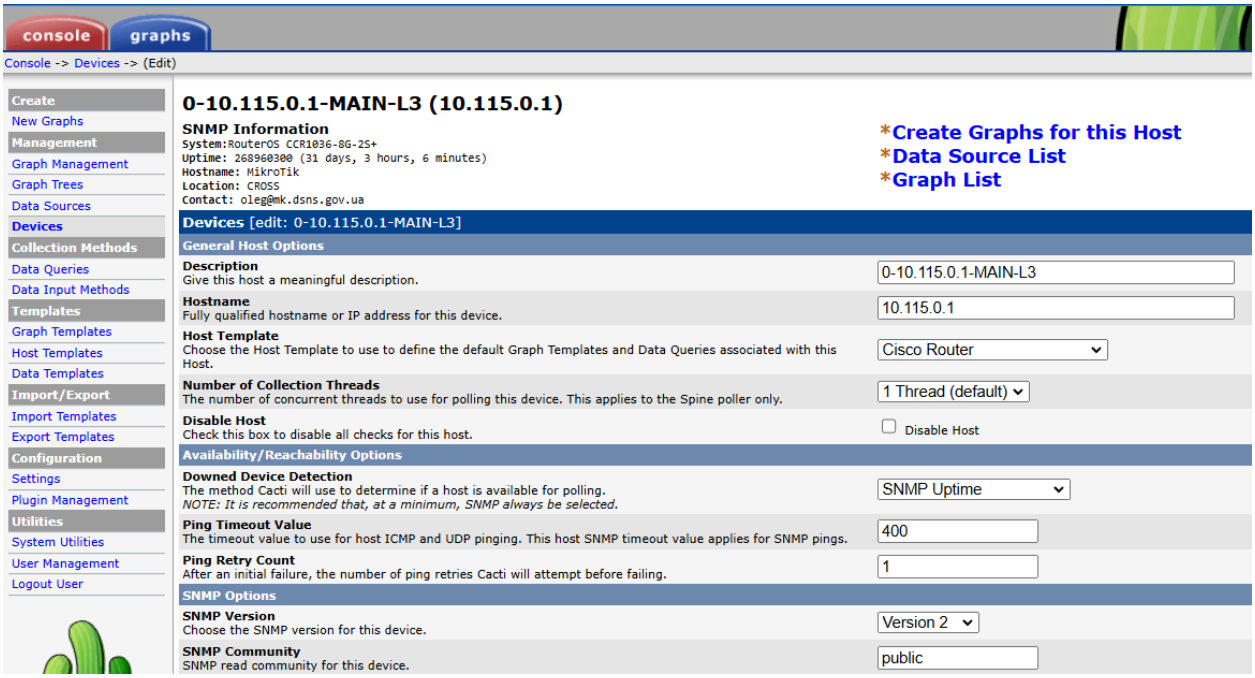


Рисунок 3.20 – Інформація про комутатор Mikrotik CCR1036-8G-2S+

Для активації SNMP на Mikrotik необхідно відкрити вкладку налаштування SNMP, додати дані про сервер та перелік IP, з яких можна отримати інформацію про обладнання (рис 3.21).

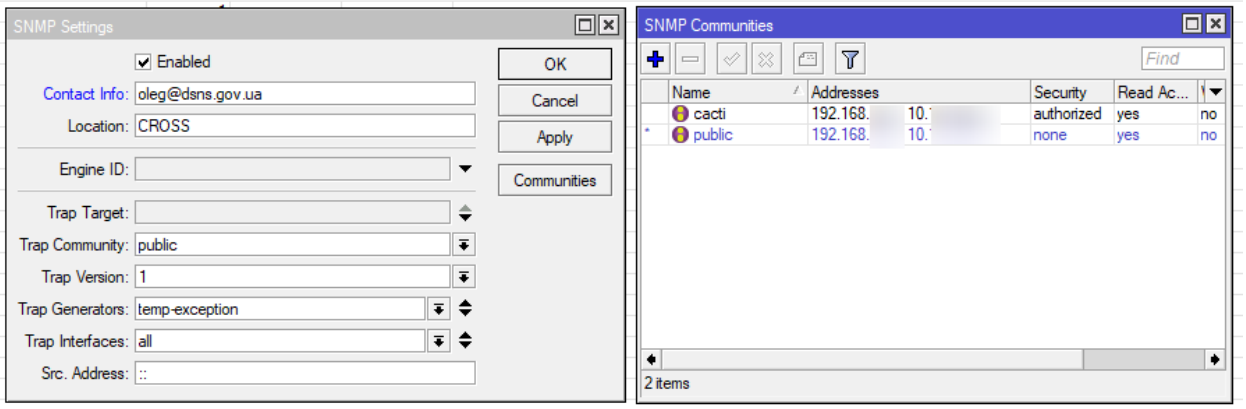


Рисунок 3.21 – Вкладка налаштування SNMP Mikrotik

Cacti є незамінним інструментом для системних адміністраторів і фахівців з IT-безпеки. Cacti дозволяє ефективно моніторити різноманітні IT-системи, забезпечуючи їх надійну та безперебійну роботу.

Nagios - це інструмент, призначений для моніторингу стану комп'ютерних систем і мереж. Він дозволяє відстежувати роботу серверів,

служб, мережевих протоколів та інших компонентів IT-інфраструктури. Завдяки Nagios можна своєчасно виявляти будь-які проблеми та оперативно реагувати на них, що дозволяє забезпечити безперебійну роботу систем.

Для додавання нових пристроїв створимо конфігураційні файли які містять запити SNMP від необхідних пристроїв.

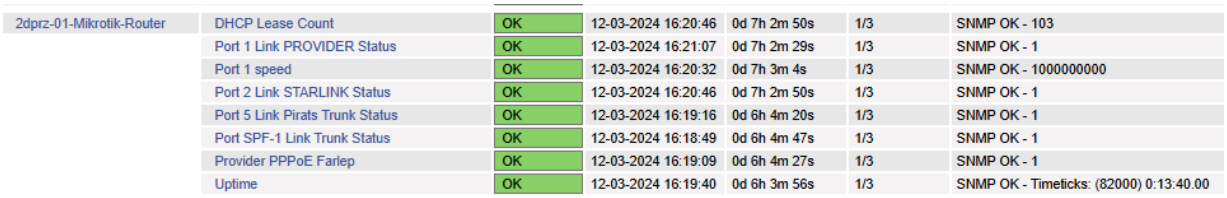
```
define host {
 use linux-server
 host_name 2dprz-01-Mikrotik-2-Router
 alias 2dprz-01-Mikrotik-2 Router
 notes 2dprz-01-Mikrotik-2 Router
 address 10.115.101.2
 }


define service {
 use generic-service
 host_name 2dprz-01-Mikrotik-2-Router
 service_description Uptime
 check_command check_snmp! -C public -o 1.3.6.1.2.1.1.3.0 -P 1
}
```

Рисунок 3.22 – Конфігурація Nagios для моніторингу Mikrotik

Nagios працює таким чином: адміністратор налаштовує систему, вказуючи які саме компоненти необхідно моніторити. Потім Nagios періодично перевіряє стан кожного з цих компонентів. На основі отриманих даних система оцінює, чи все працює коректно. У випадку виявлення будь-яких відхилень від норми Nagios надсилає сповіщення адміністратору.

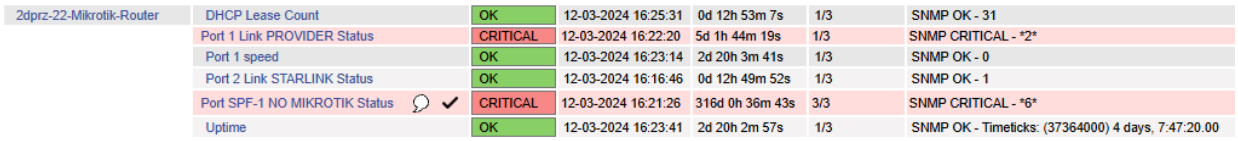
Популярність Nagios обумовлена кількома факторами: гнучкістю налаштувань, можливістю розширення функціональності за допомогою плагінів, великою спільнотою користувачів та наявністю безкоштовної версії з відкритим кодом. На рисунку 3.23 вказано актуальний стан мережі в підрозділі, зазначено статус роботи основного провайдеру та резервного каналу зв’язку через Старлінк, швидкість порту провайдера, а також час роботи обладнання.



2dprz-01-Mikrotik-Router	DHCP Lease Count	OK	12-03-2024 16:20:46	0d 7h 2m 50s	1/3	SNMP OK - 103
	Port 1 Link PROVIDER Status	OK	12-03-2024 16:21:07	0d 7h 2m 29s	1/3	SNMP OK - 1
	Port 1 speed	OK	12-03-2024 16:20:32	0d 7h 3m 4s	1/3	SNMP OK - 1000000000
	Port 2 Link STARLINK Status	OK	12-03-2024 16:20:46	0d 7h 2m 50s	1/3	SNMP OK - 1
	Port 5 Link Pirats Trunk Status	OK	12-03-2024 16:19:16	0d 6h 4m 20s	1/3	SNMP OK - 1
	Port SPF-1 Link Trunk Status	OK	12-03-2024 16:18:49	0d 6h 4m 47s	1/3	SNMP OK - 1
	Provider PPPoE Farlep	OK	12-03-2024 16:19:09	0d 6h 4m 27s	1/3	SNMP OK - 1
	Uptime	OK	12-03-2024 16:19:40	0d 6h 3m 56s	1/3	SNMP OK - Timeticks: (82000) 0:13:40.00

Рисунок 3.23 – Стан мережі Mikrotik у Nagios

Головні переваги використання Nagios: проактивне вирішення проблем, підвищення доступності систем, оптимізація використання ресурсів та зниження загальних витрат на обслуговування IT-інфраструктури. На рисунку 3.24 показано проблемні питання, такі як відсутній зв'язок до провайдеру (порт 1), а також відсутній зв'язок з іншим комутатором у частині (Порт SFP).



2dprz-22-Mikrotik-Router	DHCP Lease Count	OK	12-03-2024 16:25:31	0d 12h 53m 7s	1/3	SNMP OK - 31
	Port 1 Link PROVIDER Status	CRITICAL	12-03-2024 16:22:20	5d 1h 44m 19s	1/3	SNMP CRITICAL - *2*
	Port 1 speed	OK	12-03-2024 16:23:14	2d 20h 3m 41s	1/3	SNMP OK - 0
	Port 2 Link STARLINK Status	OK	12-03-2024 16:16:46	0d 12h 49m 52s	1/3	SNMP OK - 1
	Port SPF-1 NO MIKROTIK Status	CRITICAL	12-03-2024 16:21:26	316d 0h 36m 43s	3/3	SNMP CRITICAL - *6*
	Uptime	OK	12-03-2024 16:23:41	2d 20h 2m 57s	1/3	SNMP OK - Timeticks: (37364000) 4 days, 7:47:20.00

Рисунок 3.24 – Стан мережі Mikrotik у Nagios з проблемою

Таким чином, Nagios є незамінним інструментом для системних адміністраторів, які прагнуть забезпечити безперебійну роботу своїх систем та підвищити їхню надійність.

Повідомлення від систем моніторінгу для зручності можна надсилати на мобільні додатки та дивитись через веб-браузер за допомогою сервісу Slack. **Slack** – це популярний хмарний сервіс для командної роботи та спілкування. Його можна розглядати як сучасний робочий простір, де команди можуть обмінюватися повідомленнями, файлами, організовувати проекти та інтегрувати різні інструменти. Приклад повідомлення про проблему в мережі зображено на рисунку 3.25.

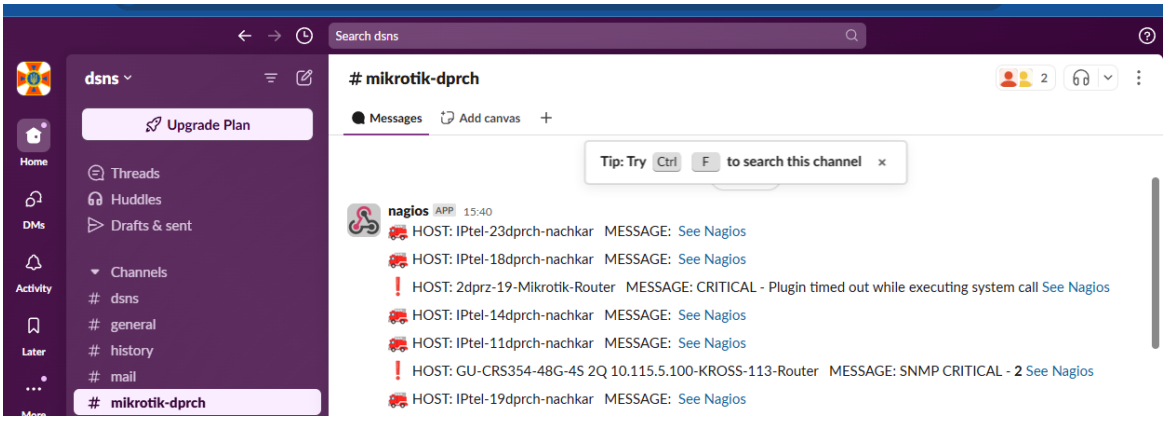


Рисунок 3.25 – Інформація про стан мережі за допомогою Slack

Висновки

Впровадження мережевої інфраструктури є складним процесом, який вимагає комплексного підходу. Оптимальне поєднання технологій VLAN і VPN дозволяє створити гнучку, масштабовану та надійну мережеву інфраструктуру, яка відповідає сучасним вимогам організації.

Проект з впровадження мережевої інфраструктури продемонстрував успішне поєднання традиційних мережевих технологій (локальні мережі, VLAN, VPN) з сучасними рішеннями в галузі Інтернету речей (IoT). Використання протоколу LoRaWAN для підключення датчиків відкриває нові можливості для автоматизації та моніторингу різних процесів. В результаті впровадження проекту було створено інтелектуальну мережу, яка дозволяє збирати та аналізувати дані з датчиків, оптимізувати ресурси та підвищити ефективність процесів.

Впровадження мережевої інфраструктури включало в себе декілька ключових етапів: проектування топології мережі, вибір обладнання, конфігурацію мережевих пристроїв, налаштування VLAN і VPN, а також інтеграцію датчиків LoRaWAN. Завдяки використанню сучасних технологій та дотриманню стандартів безпеки, вдалося створити стабільну та надійну мережу, яка забезпечує високу швидкість передачі даних і захист інформації.

					171.6321М.КР.ПЗ.Р4		
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*			
Розробник		Трешнюк О. І.			Охорона праці	*Літ.*	*Арк.* 68 / *Аркушів*
Консультант		Тубальцев А. М.					
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова	
Керівник		Дьяконов О. С.					
Зав. каф.		Рябенький В. М.					

РОЗДІЛ 4. ОХОРОНА ПРАЦІ

4.1. Основні положення щодо охорони праці в Україні

Охорона праці в Україні – це сукупність заходів, спрямованих на забезпечення безпечних і здорових умов праці, збереження життя та здоров'я працівників. Ця система охоплює правові, соціальні, економічні, організаційно-технічні, санітарно-гігієнічні та лікувально-профілактичні заходи.

Основним законодавчим актом, що регулює відносини в галузі охорони праці, є Закон України "Про охорону праці". Цей закон визначає права та обов'язки роботодавців і працівників, встановлює вимоги до умов праці, а також передбачає відповідальність за порушення законодавства про охорону праці.

Законодавство про охорону праці складається з Кодексу законів про працю України (322-08), Закону України "Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності" (1105-14) та прийнятих відповідно до них нормативно-правових актів.

Ключовим принципом охорони праці є пріоритет життя і здоров'я працівників. Роботодавець зобов'язаний створити на кожному робочому місці умови, які відповідають вимогам безпеки та гігієни праці. Це передбачає проведення інструктажів з охорони праці, забезпечення працівників засобами індивідуального захисту, регулярний медичний огляд, а також створення безпечних умов роботи з обладнанням.

Державна політика в галузі охорони праці спрямована на постійне вдосконалення системи захисту працівників. Важливу роль відіграють також профспілки, які представляють інтереси працівників і контролюють дотримання вимог законодавства про охорону праці.

Незважаючи на досягнуті результати, проблема охорони праці в Україні залишається актуальною. Високий рівень виробничого травматизму

та професійних захворювань свідчить про необхідність подальшого вдосконалення системи охорони праці.

4.2. Вимоги до інженерної інфраструктури технологічних приміщень

Відповідно до Наказу ДСНС 10.10.2022 № 573 Про організацію роботи відомчої цифрової електронної комунікаційної мережі ДСНС затверджені вимоги до інженерної інфраструктури технологічних приміщень (серверних) для розміщення серверного та електронного комунікаційного обладнання відомчої цифрової електронної комунікаційної мережі ДСНС:

Проходи попереду та позаду обладнання повинні забезпечувати вільний доступ і складати щонайменше 80 сантиметрів.

Площа серверного приміщення має складати від 20 м кв.

Перебування в серверному приміщенні людей на постійній основі (використання приміщення як робочого кабінету) заборонено.

Траси звичайного і пожежного водопостачання, опалення та каналізації мають бути винесені за межі серверної і не перебувати безпосередньо над нею на верхніх поверхах.

Через серверну не мають проходити будь-які транзитні електронні комунікації та кабелі електропостачання.

Приміщення серверної згідно з ДБН В.2.5-56:2014 "Системи протипожежного захисту" (далі - ДБН В.2.5-56) обов’язково підлягають обладнанню системою пожежної сигналізації, тип застосовуваного обладнання системи та місця установки датчиків визначається на етапах технічного проєктування відповідно до вимог ДБН В.2.5 56, ДСТУ CEN/TS 54-14:2021 "Системи пожежної сигналізації та оповіщування. Частина 14. Настанови щодо побудови, проектування, монтування, пусконалагоджування, введення в експлуатацію, експлуатування та технічного обслуговування". Приміщення серверних, які не підлягають обладнанню згідно з ДБН В.2.5-56 автоматичними системами газового

пожежогасіння, оснащуються первинними засобами пожежогасіння (пересувними або переносними газовимивогнегасниками).

Система електропостачання серверної за своїм функціональним призначення відноситься до електроприймачів критичної (особливої) групи з неперервним режимом роботи та за ступенем надійності електропостачання належить до електроприймачів першої категорії згідно з ДБН В.2.5-23:2010 "Інженерне обладнання будинків і споруд. Проектування електрообладнання об`єктів цивільного призначення" (далі - ДБН В.2.5-23).

4.3. Основи електробезпеки

Електробезпека – це сукупність заходів, спрямованих на захист людини від ураження електричним струмом. Електричний струм, проходячи через людський організм, може призвести до різних видів травм, від легких опіків до смерті. Тому знання основ електробезпеки є життєво необхідним для кожної людини.

Одним із найважливіших аспектів електробезпеки є розуміння видів ураження електричним струмом. Їх можна поділити на дві основні групи: місцеві та загальні. Місцеві ураження проявляються у вигляді опіків, електричних знаків, металізації шкіри та інших пошкоджень тканин в місці контакту з провідником під напругою. Загальні ураження впливають на весь організм, порушуючи роботу серцево-судинної та нервової систем. Вони можуть призвести до втрати свідомості, судом, паралічу дихання і навіть смерті.

Важливим фактором, що впливає на тяжкість ураження електричним струмом, є сила струму, тривалість його проходження через тіло людини, шлях струму, а також індивідуальні особливості організму. Чим більша сила струму і чим довше він протікає через тіло, тим важчими будуть наслідки. Шлях струму також відіграє важливу роль. Найнебезпечнішими вважаються шляхи, що проходять через серце і головний мозок.

Для основ електробезпеки використовують нормативний документ ДСТУ 12.1.009-76 "Система стандартів безпеки праці. Електробезпека. Терміни і визначення" який встановлює єдині для всієї території України терміни та визначення в галузі електробезпеки. Він є невід'ємною частиною системи забезпечення безпеки праці та використовується в науковій, технічній і виробничій діяльності.

Для запобігання ураження електричним струмом необхідно дотримуватися простих правил електробезпеки. Це включає в себе використання тільки справних електроприладів, дотримання правил експлуатації електроустановок, проведення регулярних оглядів електропроводки, а також захист від ураження електричним струмом за допомогою заземлення, занулення та інших захисних засобів.

Знання основ електробезпеки та дотримання правил безпечної експлуатації електроустановок дозволяє уникнути багатьох нещасних випадків і зберегти здоров’я.

ВИСНОВКИ

У кваліфікаційній роботі з Розробки середовища для тестування мережевої інфраструктури проаналізовано сучасні тенденції розвитку апаратного забезпечення та зроблений огляд програмного забезпечення для функціонування мережі. Зокрема, було досліджено новітні мережеві комутатори, маршрутизатори, а також системи віртуалізації. Паралельно з цим було проведено ретельний огляд програмного забезпечення, необхідного для ефективного функціонування мережі. Особливу увагу було приділено операційним системам, системам управління мережею, а також мережевим інструментам для тестування датчиків які працюють за протоколом LoRaWAN. На основі проведеного аналізу було розроблена мережева інфраструктура, яка дозволяє об'єднати Головне управління, підрозділи та пересувні пункти управління в єдину локальну мережу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Телекомунікаційні системи передачі : навч. посібник / І. П. Лісовий, В. М. Рябенький, О. С. Дьяконов. – Миколаїв : НУК, 2016. – 212 с.

2. Автоматика та електротехніка: Матеріали Всеукраїнської науковотехнічної конференції студентів, аспірантів та молодих вчених [Електронний ресурс]. − Миколаїв: НУК, 2024. – 113 с.

3. Рябенький В.М. Схемотехніка: пристрої цифрової електроніки: підручник у 2 т. / В.М. Рябенький, В.Я. Жуйков, Ю.С. Ямненко, О.В. Борисов. Київ : НТУУ «КПІ» Вид-во «Політехніка», 2015. Т.1. 400 с

4. Редька І.В. Принципи опису систем цифрової обробки сигналів на структурно-функціональному рівні / І.В.

5. Редька, О.І. Трешнюк, О.О. Ушкаренко // Автоматика та електротехніка: Матеріали Всеукраїнської науковотехнічної конференції студентів, аспірантів та молодих вчених. Миколаїв: НУК, 2023. С. 57-59.

6. Mikrotik CCR1036-8G-2S+ — [електронний ресурс].URL: https://mikrotik.com/product/CCR1036-8G-2Splus

7. Mikrotik CRS326-24S+2Q+RM — [електронний ресурс].URL: https://mikrotik.com/product/crs326_24s_2q_rm

8. Mikrotik CRS354-48G-4S+2Q+RM — [електронний ресурс].URL: https://mikrotik.com/product/crs354_48g_4splus2qplusrm

9. Mikrotik CRS354-48P-4S+2Q+RM — [електронний ресурс].URL: https://mikrotik.com/product/crs354_48p_4s_2q_rm

10. Mikrotik CRS326-24G-2S+RM — [електронний ресурс].URL: https://mikrotik.com/product/CRS326-24G-2SplusRM

11. IoT точка доступа MikroTik wAP LR8 kit (RBwAPR-2nD&R11e-LR8) — [електронний ресурс].URL: https://mikrotik.com/product/wap_lr8_kit

12. Точка доступа MikroTik LtAP mini LTE kit (RB912R-2nD-LTm&R11e-LTE) — [електронний ресурс].URL: https://mikrotik.com/product/ltap_mini_lte_kit

13. Wi-Fi Mikrotik cAP ax (cAPGi-5HaxD2HaxD) — [електронний ресурс].URL: https://mikrotik.com/product/cap_ax

14. DRAGINO LSN50v2 LoRaWAN — [електронний ресурс].URL: https://manuals.plus/uk/dragino/lsn50v2-lorawan-temperature-sensor-manual#battery_how_to_replace

15. Proxmox Virtual Environment — [електронний ресурс].URL: https://www.proxmox.com/en/proxmox-virtual-environment/overview

16. Proxmox Backup Server — [електронний ресурс].URL: https://www.proxmox.com/en/proxmox-backup-server/overview

17. Cacti — The Complete RRDTool-based Graphing Solution — [електронний ресурс].URL: https://www.cacti.net/info/cacti

18. Nagios Core Services Platform — [електронний ресурс].URL: https://www.nagios.org/faq/

ДОДАТОК А

Приклад прийнятого пакету LoRaWAN


```
{
 "name": "gs.status.receive",
 "time": "2024-11-23T12:20:48.764958995Z",
 "identifiers": [
  {
   "gateway_ids": {
    "gateway_id": "mykolaiv-lora",
    "eui": "313330375A002F00"
   }
  }
 ],
 "data": {
  "@type": "type.googleapis.com/ttn.lorawan.v3.GatewayStatus",
  "time": "2024-11-23T12:20:47Z",
  "versions": {
   "ttn-lw-gateway-server": "3.32.2-rc1-SNAPSHOT-a0014352f0"
  },
  "antenna_locations": [
   {
    "latitude": 46.968213,
    "longitude": 31.96101,
    "altitude": 39,
    "source": "SOURCE_GPS"
   }
  ],
  "ip": [
   "5.1.11.186"
```

```
    ],
    "metrics": {
      "rxfw": 0,
      "ackr": 0,
      "txin": 0,
      "txok": 0,
      "rxin": 0,
      "rxok": 0
    }
  },
  "correlation_ids": [
    "gs:status:01JDCFFCZW3N54GWXG58QN3G5G"
  ],
  "origin": "ip-10-100-5-31.eu-west-1.compute.internal",
  "context": {
    "tenant-id": "CgN0dG4="
  },
  "visibility": {
    "rights": [
      "RIGHT_GATEWAY_STATUS_READ"
    ]
  },
  "unique_id": "01JDCFFCZWQG1W92NVZA2KNT7C"
}
```

Приклад декодованого пакету

Forward uplink data message:


```
{
  "name": "as.up.data.forward",
  "time": "2024-11-23T12:17:14.747060758Z",
  "identifiers": [
    {
      "device_ids": {
        "device_id": "eui-a8404198a183af4e",
        "application_ids": {
          "application_id": "dragino-0183af4e"
        },
        "dev_eui": "A8404198A183AF4E",
        "join_eui": "A000000000000101",
        "dev_addr": "260B3D94"
      }
    }
  ],
  "data": {
    "@type": "type.googleapis.com/ttn.lorawan.v3.ApplicationUp",
    "end_device_ids": {
      "device_id": "eui-a8404198a183af4e",
      "application_ids": {
        "application_id": "dragino-0183af4e"
      },
      "dev_eui": "A8404198A183AF4E",
      "join_eui": "A000000000000101",
      "dev_addr": "260B3D94"
    },
```

```
"correlation_ids": [
  "gs:uplink:01JDCF8VS6R4G55WV4M02SH7J2"
],
"received_at": "2024-11-23T12:17:14.743863616Z",
"uplink_message": {
  "session_key_id": "AX4kmLM3Rads2m8BfNVxdQ==",
  "f_port": 2,
  "f_cnt": 75896,
  "frm_payload": "DSsAAAEfAADRAfk=",
  "decoded_payload": {
    "ADC_CH0V": 0.287,
    "BatV": 3.371,
    "Digital_IStatus": "L",
    "Door_status": "OPEN",
    "EXTI_Trigger": "FALSE",
    "Hum_SHT": 50.5,
    "TempC1": 0,
    "TempC_SHT": 20.9,
    "Work_mode": "IIC"
  },
  "normalized_payload": [
    {
      "action": {
        "contactState": "open"
      },
      "air": {
        "relativeHumidity": 50.5,
        "temperature": 20.9
      },
```

```
      "battery": 3.371
    }
  ],
  "rx_metadata": [
    {
      "gateway_ids": {
        "gateway_id": "mykolaiv-lora",
        "eui": "313330375A002F00"
      },
      "time": "2024-11-23T12:17:13.490170Z",
      "timestamp": 2459452755,
      "rssi": -57,
      "channel_rssi": -57,
      "snr": 7.5,
      "location": {
        "latitude": 46.96821322,
        "longitude": 31.96101031,
        "altitude": 38,
        "source": "SOURCE_REGISTRY"
      },
      "uplink_token":
"ChsKGQoNbXlrb2xhaXYtbG9yYRIIMTMwN1oALwAQ04rhlAkaDAjKj4e6Bh
DmzcT8ASC4mLuWytUl",
      "channel_index": 2,
      "received_at": "2024-11-23T12:17:14.529606374Z"
    }
  ],
  "settings": {
    "data_rate": {
```

```
      "lora": {
        "bandwidth": 125000,
        "spreading_factor": 7,
        "coding_rate": "4/5"
      }
    },
    "frequency": "868500000",
    "timestamp": 2459452755,
    "time": "2024-11-23T12:17:13.490170Z"
  },
  "received_at": "2024-11-23T12:17:14.535649944Z",
  "consumed_airtime": "0.061696s",
  "packet_error_rate": 0.04761905,
  "locations": {
    "user": {
      "latitude": 46.96797315846318,
      "longitude": 31.960990726947788,
      "altitude": 30,
      "source": "SOURCE_REGISTRY"
    }
  },
  "version_ids": {
    "brand_id": "dragino",
    "model_id": "lsn50-v2",
    "hardware_version": "_unknown_hw_version_",
    "firmware_version": "1.7.2",
    "band_id": "EU_863_870"
  },
  "network_ids": {
```

```
        "net_id": "000013",
        "ns_id": "EC656E0000000181",
        "tenant_id": "ttn",
        "cluster_id": "eu1",
        "cluster_address": "eu1.cloud.thethings.network"
      }
    }
  },
  "correlation_ids": [
    "gs:uplink:01JDCF8VS6R4G55WV4M02SH7J2"
  ],
  "origin": "ip-10-100-15-109.eu-west-1.compute.internal",
  "context": {
    "tenant-id": "CgN0dG4="
  },
  "visibility": {
    "rights": [
      "RIGHT_APPLICATION_TRAFFIC_READ"
    ]
  },
  "unique_id": "01JDCF8VZVG42RYPJ6RHT70W7Z"
}
```


Forward normalized uplink data message:


```
{
  "name": "as.up.normalized.forward",
  "time": "2024-11-23T12:17:14.747331652Z",
  "identifiers": [
```

```
  {
    "device_ids": {
      "device_id": "eui-a8404198a183af4e",
      "application_ids": {
        "application_id": "dragino-0183af4e"
      },
      "dev_eui": "A8404198A183AF4E",
      "join_eui": "A000000000000101",
      "dev_addr": "260B3D94"
    }
  }
],
"data": {
  "@type": "type.googleapis.com/ttn.lorawan.v3.ApplicationUp",
  "end_device_ids": {
    "device_id": "eui-a8404198a183af4e",
    "application_ids": {
      "application_id": "dragino-0183af4e"
    },
    "dev_eui": "A8404198A183AF4E",
    "join_eui": "A000000000000101",
    "dev_addr": "260B3D94"
  },
  "correlation_ids": [
    "gs:uplink:01JDCF8VS6R4G55WV4M02SH7J2"
  ],
  "received_at": "2024-11-23T12:17:14.743863616Z",
  "uplink_normalized": {
    "session_key_id": "AX4kmLM3Rads2m8BfNVxdQ==",
```

```
"f_port": 2,
"f_cnt": 75896,
"frm_payload": "DSsAAAEfAADRAfk=",
"normalized_payload": {
  "action": {
    "contactState": "open"
  },
  "air": {
    "relativeHumidity": 50.5,
    "temperature": 20.9
  },
  "battery": 3.371
},
"rx_metadata": [
  {
    "gateway_ids": {
      "gateway_id": "mykolaiv-lora",
      "eui": "313330375A002F00"
    },
    "time": "2024-11-23T12:17:13.490170Z",
    "timestamp": 2459452755,
    "rssi": -57,
    "channel_rssi": -57,
    "snr": 7.5,
    "location": {
      "latitude": 46.96821322,
      "longitude": 31.96101031,
      "altitude": 38,
      "source": "SOURCE_REGISTRY"
```

```
      },
      "uplink_token":
"ChsKGQoNbXlrb2xhaXYtbG9yYRIIMTMwN1oALwAQ04rhlAkaDAjKj4e6Bh
DmzcT8ASC4mLuWytUl",
      "channel_index": 2,
      "received_at": "2024-11-23T12:17:14.529606374Z"
    }
  ],
  "settings": {
    "data_rate": {
      "lora": {
        "bandwidth": 125000,
        "spreading_factor": 7,
        "coding_rate": "4/5"
      }
    },
    "frequency": "868500000",
    "timestamp": 2459452755,
    "time": "2024-11-23T12:17:13.490170Z"
  },
  "received_at": "2024-11-23T12:17:14.535649944Z",
  "consumed_airtime": "0.061696s",
  "network_ids": {
    "net_id": "000013",
    "ns_id": "EC656E0000000181",
    "tenant_id": "ttn",
    "cluster_id": "eu1",
    "cluster_address": "eu1.cloud.thethings.network"
  }
```

```
    }
  },
  "correlation_ids": [
    "gs:uplink:01JDCF8VS6R4G55WV4M02SH7J2"
  ],
  "origin": "ip-10-100-15-109.eu-west-1.compute.internal",
  "context": {
    "tenant-id": "CgN0dG4="
  },
  "visibility": {
    "rights": [
      "RIGHT_APPLICATION_TRAFFIC_READ"
    ]
  },
  "unique_id": "01JDCF8VZV3S4TZZ6WY8P3HJFY"
}
```