Форма № Н-9.02

Міністерство освіти і науки України

Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»
(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян
(назва відділення)

Циклова комісія комп'ютерної інженерії
(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра
(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі компанії "NOWA-T"**

Виконав: студент IV курсу, групи КІ-412

Спеціальності 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

_____ Назарій ВАСИЛЮК
(ім'я та прізвище)

Керівник Роксолана БОЛЮБАШ
(ім'я та прізвище)

Рецензент _____
(ім'я та прізвище)

Тернопіль – 2025

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ТЕРНОПІЛЬСЬКИЙ ФАХОВИЙ КОЛЕДЖ
ТЕРНОПІЛЬСЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
імені ІВАНА ПУЛЮЯ»

Відділення **інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян**
Циклова комісія **комп'ютерної інженерії**
Освітньо-професійний ступінь **фаховий молодший бакалавр**
Освітньо-професійна програма: **Обслуговування комп'ютерних систем і мереж**
Спеціальність: **123 Комп'ютерна інженерія**
Галузь знань: **12 Інформаційні технології**

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"31" березня 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Василюку Назарію Олександровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі компанії "NOWA-T"**

керівник роботи Болюбаш Роксолана Юріївна
(прізвище, ім'я, по батькові)

Затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя» від 28.03.2025р № 4/9-166а.

2. Строк подання студентом роботи: 13 червня 2025 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проєктування, стандарти ANSI/EIA/TIA 568 - "Commercial Building Telecommunications Wiring Standart" і ANSI/EIA/TIA 569 - "Commercial Building Standart for Telecommunications Pathwais and Spaces

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Загальний розділ. Розробка технічного та робочого проєкту. Спеціальний розділ. Економічний розділ. Охорона праці та безпека життєдіяльності.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
- план приміщень;
- фізична топологія мережі;
- логічна топологія;
- таблиця IP-адрес;
- таблиця техніко-економічних показників.

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Богдана МАРТИНЮК викладач		
Охорона праці та безпека життєдіяльності	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	01.04	
2	Збір і узагальнення інформації	05.05	
3	Написання першого розділу	16.05	
4	Розробка технічного та робочого проекту	23.05	
5	Написання спеціального розділу	30.05	
6	Розрахунок економічної частини	2.06	
7	Написання розділу охорони праці	4.06	
8	Виконання графічної частини	9.06	
9	Оформлення проєкту	11.06	
10	Погодження нормоконтролю	12.06	
11	Попередній захист роботи	13.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 01 квітня 2025 року

Студент _____ Назарій ВАСИЛЮК
(підпис) (ім'я та прізвище)

Керівник роботи _____ Роксолана БОЛЮБАШ
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Проєктування комп’ютерної мережі для підприємства “NOWA-T”».

Мета роботи полягає у створенні проєкту локальної комп’ютерної мережі, яка відповідатиме сучасним вимогам до швидкості обміну даними, забезпечуватиме спільний доступ до інформаційних ресурсів та підтримуватиме підключення до глобальної мережі Інтернет.

У кваліфікайній роботі надається структурований опис діяльності організації, особливостей процесів передавання даних, аналізуються інформаційні потоки, детально розглядаються етапи налаштування мережевого та комутаційного обладнання, а також виконується обґрунтування вибору програмного забезпечення та методики його конфігурації.

Окрему увагу приділено порівняльному аналізу апаратних засобів, які можуть бути використані для побудови мережевої інфраструктури. Проведено вибір оптимальних мережевих топологій і технологій з урахуванням специфіки підприємства.

Додатково описано розрахунок вартості проєкту, а також викладено рекомендації з дотримання техніки безпеки під час виконання монтажних робіт.

ABSTRACT

The topic of the qualification work: “Design of a computer network for the enterprise “NOWA-T””.

The purpose of the work is to create a project of a local computer network that will meet modern requirements for the speed of data exchange, provide shared access to information resources and support connection to the global Internet.

The qualification work provides a structured description of the organization’s activities, the features of data transfer processes, analyzes information flows, examines in detail the stages of configuring network and switching equipment, and justifies the choice of software and its configuration methods.

Special attention is paid to the comparative analysis of hardware that can be used to build a network infrastructure.

The optimal network topologies and technologies are selected taking into account the specifics of the enterprise.

Additionally, the calculation of the project cost is described, and recommendations for observing safety precautions during installation work are set out.

ЗМІСТ

					2025.КВР.123.412.01.00.00 ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Василюк Н О			"Розробка проєкту комп'ютерної мережі компанії "NOWA-T"» Пояснювальна записка	Літ.	Арк. 4 / Аркушів
Перевір.		Болюбаш Р Ю					
Реценз.						ВСП ТФК ТНТУ КІ-412	
Н. Контр.							
Затверд.							

ВСТУП

Інтелектуальні можливості сучасних комп'ютерів демонструють вражаючий рівень розвитку цифрових технологій. Основними характеристиками, що визначають потенціал комп'ютера, є здатність обробляти великі обсяги інформації та ефективно її аналізувати. Системи штучного інтелекту можуть за лічені секунди опрацьовувати мільйони варіантів сценаріїв розвитку подій і на цій основі приймати оптимальні рішення.

Сучасні нейронні мережі вже здатні генерувати зображення, музичні твори, поезію. Проте їхня креативність базується виключно на аналізі раніше створених людиною зразків. Машинне навчання дає змогу системі відтворювати нові продукти, спираючись на статистичні закономірності у вже наявних даних. Однак створення інноваційних, по-справжньому проривних ідей залишається, принаймні наразі, прерогативою людини.

Таким чином, комп'ютери демонструють надзвичайну функціональність і здатні суттєво оптимізувати повсякденну діяльність людини. Однак їх здатність до аналізу обмежується лише вже наявною інформацією — системи не володіють абстрактним мисленням у людському розумінні.

Сьогодні комп'ютери стали незамінним інструментом у житті сучасної людини. Завдяки розвитку інтернету та цифрових технологій комп'ютери перетворилися на універсальний засіб комунікації. Географічна відстань більше не є перешкодою для спілкування чи виконання професійних обов'язків. Пошук інформації значно спростився — відповідь на будь-яке запитання можна знайти за лічені секунди. Сфера онлайн-торгівлі стрімко розвивається, а розважальні сервіси стали доступні безпосередньо з дому.

Роль комп'ютера виходить далеко за межі побутових завдань. Він впливає на всі ключові напрями розвитку суспільства: від промисловості до медицини. Сучасна наука неможлива без комп'ютерних технологій — вони забезпечують

високу точність і швидкість проведення досліджень у різних галузях: біології, хімії, соціології тощо.

Комп’ютер є універсальним носієм інформації, що сприяє реалізації творчого та інтелектуального потенціалу користувача. Паралельно трансформується ринок праці: змінюється структура професій та механізми обігу інтелектуальної власності. Взаємодія між людиною і комп’ютером стає дедалі глибшою. Серед звичних інструментів — голосові помічники, які можуть розпізнавати мовлення, інтерпретувати його зміст та виконувати команди користувача.

Інтеграція комп’ютерів у мережі вже не просто технічна можливість, а нагальна потреба сучасного інформаційного суспільства. Комп’ютерна мережа — це система, що об’єднує просторово рознесені обчислювальні пристрої, між якими здійснюється обмін даними через різноманітні засоби передавання інформації. За матеріалами мережі інтернет

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Темою даного кваліфікаційної роботи є розробка локальної комп’ютерної мережі для підприємства “NOWA-T”.

Основна мета — створення ефективної, масштабованої та безпечної інфраструктури, що забезпечить стабільну взаємодію між усіма підрозділами компанії.

Мережа повинна відповідати таким вимогам:

– забезпечення об’єднання персональних комп’ютерів, які розташовані в різних структурних підрозділах підприємства, у єдиний інформаційний простір;
– організація централізованого високошвидкісного доступу до мережі Інтернет для всіх користувачів;
– забезпечення підтримки служб внутрішньої локальної мережі, а також стабільного доступу до зовнішніх інтернет-ресурсів;
– створення ефективного й економічного каналу обміну даними між користувачами, що мінімізує витрати на документообіг.

Додатково, проект передбачає врахування можливості масштабування мережі в майбутньому, інтеграцію з безпровідними технологіями, резервування ключових елементів інфраструктури та реалізацію базових механізмів захисту інформації.

Це дозволить підвищити надійність роботи мережі та забезпечити її відповідність сучасним вимогам до корпоративних IT-систем.

1.1.2 Призначення розробки

Проєктована комп’ютерна мережа має на меті забезпечення ефективного функціонування всіх працівників підприємства.

Організація спеціалізується на наданні широкого спектра рекламних послуг, що потребує надійного інформаційного середовища для обміну даними та колективної роботи.

До основних вимог, що висуваються до мережевої інфраструктури, належать:

– забезпечення спільного використання апаратних ресурсів, зокрема мережевих принтерів, що дозволяє оптимізувати витрати на обладнання та його обслуговування;
– надання доступу до єдиного ліцензійного програмного забезпечення з будь-якої точки мережі, що спрощує його адміністрування та оновлення;
– централізоване зберігання користувацьких даних із можливістю організації резервного копіювання та підвищення надійності доступу до інформації;
– впровадження механізмів централізованого управління доступом до ресурсів, що підвищує рівень контролю та безпеки;
– реалізація технічних засобів для посилення корпоративної інформаційної безпеки, включаючи автентифікацію користувачів та обмеження доступу;
– організація спільного високошвидкісного інтернет-доступу з можливістю розподілу пропускної здатності між користувачами.

Описані вимоги спрямовані на створення інфраструктури, що дозволить не лише підвищити продуктивність роботи персоналу, але й забезпечити гнучкість, масштабованість і захищеність інформаційної системи підприємства.

1.2.3 Вимоги до апаратного та програмного забезпечення

Проєктована мережа реалізується відповідно до вимог міжнародного стандарту ISO/IEC 11801 (редакція 2002 року), що регламентує побудову структурованих кабельних систем (СКС) категорії 5е. Такий підхід забезпечує необхідну пропускну здатність і надійність мережевої інфраструктури на рівні сучасних вимог підприємств малого та середнього бізнесу.

СКС базується на використанні пасивних компонентів: кабельно-провідникової продукції категорії 5е, інформаційних розеток, патч-панелей та патчкордів. Усі компоненти сертифіковані відповідно до міжнародних стандартів і забезпечують стабільну роботу мережі.

Робоче місце користувача обладнується одним портом RJ-45 категорії 5е, призначеним для підключення кінцевого пристрою. Розташування точок доступу до мережі розробляється згідно з планом розміщення приміщень, з урахуванням ергономіки та зручності обслуговування.

Усі сегменти кабельної системи піддаються маркуванню з обох боків, що дозволяє точно ідентифікувати кожен кабель на монтажних панелях і визначити місце його закінчення, спрощуючи подальше обслуговування, діагностику та модернізацію мережі.

Мережа логічно поділена на робочі групи з підтримкою швидкості передавання даних 100/1000 Мбіт/с. Такий поділ дозволяє оптимізувати трафік і забезпечити надійний зв’язок між різними підрозділами підприємства.

Вибір активного мережевого обладнання ґрунтується на вимогах до підтримки відповідної швидкості, можливості адміністрування, забезпечення легкого ремонту або заміни, а також сумісності з іншими компонентами мережі. Усе апаратне забезпечення має бути поширеним і перевіреним у практичному застосуванні.

Програмне забезпечення, що забезпечує функціонування мережі, представлено операційними системами сімейства Windows, які встановлюються на робочі станції співробітників. Це дозволяє уніфікувати середовище експлуатації та спростити технічне обслуговування.

Для покриття бездротового доступу в мережу застосовується точка доступу, що підтримує сучасні протоколи безпеки WPA-PSK і WPA2-PSK, а також відповідає стандарту IEEE 802.11n. Це дозволяє забезпечити захищене підключення мобільних пристроїв і підвищити гнучкість у використанні мережевих ресурсів.

1.2.4 Стадії та етапи розробки

На початковому етапі збору інформації необхідно провести детальний аналіз параметрів організації, її поточної структури та потенціалу зростання. Визначення типу організації дозволяє правильно спланувати масштаб мережі та її подальшу модернізацію.

Комплексне опрацювання цих питань на етапі проектування дозволяє мінімізувати ризики під час реалізації мережі та забезпечити її стабільну та ефективну роботу в майбутньому.

Серед ключових завдань цього етапу:

– Визначення передбачуваного зростання організації з метою формування резервів масштабованості мережі.
– Вибір програмного забезпечення, що буде використовуватися на клієнтських та серверних пристроях мережі.
– Розробка логічної структури мережі, вибір її типу та топології, а також підбір типу кабельної системи, активного та пасивного обладнання.

– Розрахунок необхідної кількості вертикальних (магістральних) та горизонтальних сегментів кабельної системи відповідно до архітектури будівлі.
– Визначення типу підключення до глобальної мережі Інтернет, з подальшим вибором відповідного маршрутизатора, що забезпечить необхідну пропускну здатність і функціональність.

1.1.5 Вимоги до документації

У результаті етапу проектування мережевої інфраструктури необхідно сформувати комплект основної технічної документації, що включає:

– Логічну топологію мережі, яка описує структуру взаємозв'язків між пристроями на логічному рівні, відображаючи маршрути обміну даними між вузлами;
– Фізичну топологію, яка містить точне розташування обладнання, кабельних трас та точок підключення відповідно до реального планування приміщень.

Після завершення підготовчого етапу та затвердження проєктної документації можна переходити до безпосереднього монтажу кабельної інфраструктури та встановлення активного обладнання.

У подальшому, після введення мережі в експлуатацію, зазначені документи виконують роль основних експлуатаційних матеріалів для відділу IT.

Вони необхідні для обслуговування мережі, проведення оновлень, усунення несправностей та модифікацій мережевої структури.

Правильно оформлена документація суттєво полегшує адміністрування системи та забезпечує її стійкість і надійність у довгостроковій перспективі.

1.1.6 Техніко-економічні показники

Спроєктована комп’ютерна мережа повинна відповідати таким ключовим вимогам:

– Сучасність і економічна доцільність: рішення повинно базуватись на актуальних технологіях із мінімальними витратами на обладнання та впровадження, при цьому забезпечуючи належний рівень продуктивності та надійності.
– Висока швидкість передавання даних: мережа має підтримувати швидкість обміну інформацією в діапазоні 100/1000 Мбіт/с, що забезпечить комфортну роботу користувачів у локальному середовищі та дозволить ефективно взаємодіяти з загальнодоступними сервісами.
– Можливість масштабування: топологія та обране обладнання повинні передбачати потенціал для подальшого розширення мережі — як у кількості робочих місць, так і в обсязі переданих даних, без потреби повної реконструкції інфраструктури.
– Доступ до глобальної мережі Інтернет: система повинна забезпечувати надійний, захищений та безперебійний вихід в Інтернет для всіх користувачів з можливістю гнучкого керування трафіком та політиками безпеки.

1.1.7 Порядок контролю та прийому

Під час приймання до експлуатації побудованої мережі необхідно провести повну перевірку працездатності всіх мережевих вузлів. Усі кабелі повинні мати чітке маркування відповідно до встановлених вимог.

Перевірка мережі здійснюється із застосуванням спеціалізованих програмних утиліт або відповідних програмних комплексів, які дозволяють здійснити діагностику параметрів мережі. Здача мережі в експлуатацію є ключовим

етапом реалізації проєкту, оскільки від її якості значною мірою залежить подальша стабільна робота системи.

Після завершення усіх передбачених договором робіт підрядник надсилає замовнику письмове повідомлення про готовність об'єкта, до якого додається повний пакет технічної документації, попередньо погоджений сторонами. Замовник, отримавши відповідне повідомлення, зобов’язаний ініціювати проведення комплексного тестування системи шляхом створення спеціалізованої приймальної комісії, яка здійснює оцінку функціональних характеристик побудованої мережі та формалізує рішення щодо прийняття її в експлуатацію.

Усі подальші зміни в конфігурації мережі, зокрема розширення кількості робочих місць або збільшення штату користувачів, мають оформлюватися окремими Заявками з подальшим внесенням змін до Технічного завдання у формі Додатків. Розміщення структурованих кабельних систем (СКС) на робочих місцях повинно суворо відповідати плану-схемі, викладеній у фізичній топології проєкту. Приймальна комісія має бути призначена не пізніше ніж через п’ять днів після надходження повідомлення про завершення робіт. Результатом процедури здачі є підписання акту приймання системи в експлуатацію.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис задачі та характеристика підприємства

Метою роботи є розробка та впровадження локальної обчислювальної мережі, яка забезпечить інтеграцію усіх персональних комп'ютерів підприємства в єдину інформаційну систему. Основними функціональними завданнями мережі є організація ефективного обміну даними між робочими станціями, централізоване збереження інформації та забезпечення доступу користувачів до внутрішніх і зовнішніх (Інтернет) ресурсів. Реалізація проєкту має сприяти підвищенню продуктивності роботи співробітників завдяки злагодженому функціонуванню інформаційної інфраструктури.

Технічні характеристики приміщення, де реалізується проєкт, передбачають висоту стель 3,5 метра, а стіни виконані з гіпсокартону та оштукатурені, що необхідно врахувати при монтажі мережі. Кабельна інфраструктура повинна бути організована прихованим способом для забезпечення естетики та безпеки експлуатації. У зоні встановлення комутаційної шафи передбачено облаштування прихованого кабельного каналу з використанням пластикового кабельного короба розміром 100×100 мм або еквівалентного за параметрами. Саму комутаційну шафу планується розмістити в окремому технічному приміщенні, що дозволить підвищити рівень організації мережевої інфраструктури та забезпечити зручність технічного обслуговування.

Компанія "NOWA-T" спеціалізується на наданні комплексу рекламних послуг, які включають як класичну друковану рекламу, так і цифрові інструменти просування. Це передбачає необхідність наявності стабільного й швидкісного доступу до Інтернету, високої пропускної здатності внутрішньої мережі та підтримки мережевих сервісів, які використовуються у процесах дизайну, обробки графіки, передачі великого обсягу даних та віддаленої комуніка-

ції із клієнтами. Мережа повинна відповідати сучасним стандартам, бути масштабованою і гнучкою для подальшого розвитку компанії.

2.2 Розробка та обґрунтування логічної та фізичної схем мережі

Однією з ключових характеристик, що визначає особливості побудови комп'ютерних мереж, є їхня топологія. Під топологією мережі розуміють спосіб фізичного або логічного з'єднання мережевих вузлів між собою. До таких вузлів відносяться комп'ютери, мережеві комутатори (свічі), концентратори, маршрутизатори, точки доступу та інші активні і пасивні елементи інфраструктури.

Топологія визначає, яким чином дані передаються між пристроями, як відбувається маршрутизація трафіку, а також впливає на продуктивність, відмовостійкість і масштабованість мережі. Фактично вона є схемою фізичних зв'язків між мережевими елементами, які забезпечують взаємодію та передачу даних у межах всієї системи. У практиці проектування мережі обрана топологія значною мірою зумовлює технічні рішення, витрати на реалізацію, а також подальше обслуговування та модернізацію мережевої інфраструктури.

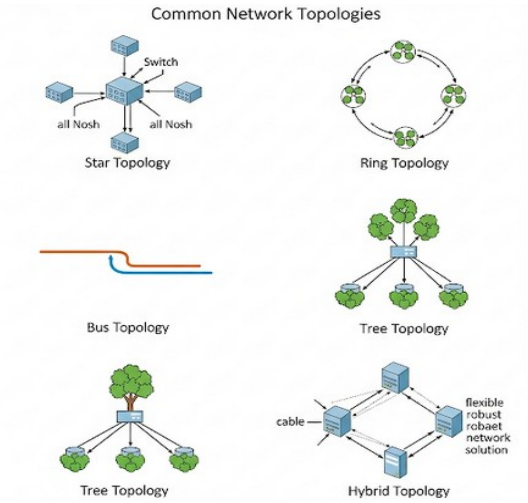


Рисунок 2.1 - Типи топологій

Мережеві характеристики значною мірою залежать від типу обраної топології, оскільки вона визначає основні принципи організації фізичних та логічних з'єднань між вузлами системи. Зокрема, від вибору певної топології залежать такі ключові аспекти, як кількість і тип необхідного мережевого обладнання, функціональні можливості використовуваних пристроїв, гнучкість та масштабованість інфраструктури, а також способи організації адміністрування і керування мережею.

Найпоширенішими базовими топологіями є: комірчата (mesh), кільцева (ring), зіркоподібна (star), шинна (bus) та деревоподібна (tree). Кожна з них має свої переваги та недоліки, які враховуються при проектуванні мережі для конкретних умов експлуатації. У практиці побудови корпоративних мереж досить часто використовуються також комбіновані або гібридні топології, що поєднують риси декількох базових структур для досягнення оптимального балансу між вартістю, надійністю та продуктивністю мережі (див. рис. 2.1).

Шинна топологія передбачає використання спільного каналу передачі даних — коаксіального кабелю, до якого підключаються всі вузли мережі. Для коректної роботи системи на кінцях кабелю встановлюються термінатори, які запобігають відбиттю сигналу. Однією з основних проблем цього типу топології є загальна доступність переданої інформації — будь-який підключений вузол має змогу перехопити пакети, що проходять через шину. Крім того, уразливим місцем є сам кабель: у разі його пошкодження припиняє роботу вся мережа.

Кільцева топологія забезпечує з'єднання кожного комп'ютера з двома сусідніми, утворюючи замкнуте коло. Інформація передається по колу послідовно через кожен вузол, поки не досягне адресата. Незважаючи на простоту реалізації, кільце також має недоліки, аналогічні шині: вразливість до пошкоджень лінії зв'язку та відсутність конфіденційності переданих даних. При цьому вихід з ладу одного вузла або кабельної ділянки може порушити функціонування всієї мережі.

Зіркоподібна топологія характеризується наявністю центрального пристрою (хабу або комутатора), до якого під’єднуються всі інші вузли. Вона забезпечує централізоване керування і високу живучість — у разі виходу з ладу одного з кабелів чи вузлів це не впливає на роботу інших елементів мережі. Проте несправність центрального комутатора призводить до повного припинення функціонування мережі. Завдяки відсутності прямого з'єднання між вузлами знижується ризик перехоплення даних та підвищується безпека.

Комірчаста топологія, або повнозв'язна, забезпечує високу відмовостійкість, оскільки кожен вузол має декілька з’єднань з іншими. Це дозволяє підтримувати працездатність мережі навіть у разі кількох обривів кабелів. Разом з тим така структура вимагає значних витрат на кабельну інфраструктуру та складного адміністрування, що обмежує її використання у великих корпоративних мережах.

Топологія типу "решітка" (грид) застосовується переважно в обчислювальних системах високої продуктивності, таких як суперкомп’ютери. Вузли розташовуються у вигляді регулярної багатовимірної решітки, що дозволяє ефективно масштабувати архітектуру. Наприклад, одновимірна решітка — це звичайний ланцюг, що за замиканням перетворюється у кільце, тоді як дво- або тривимірна решітка дозволяє збільшити кількість з'єднань і забезпечити паралельну обробку даних на великій кількості вузлів. Така структура дозволяє досягати високої продуктивності, проте вимагає точного проєктування та спеціалізованого апаратного забезпечення.

Розглянуті раніше типи топологій є базовими конструктивними моделями побудови локальних мереж. Проте у реальних умовах побудова обчислювальної мережі визначається конкретними завданнями, які вона має вирішувати, а також особливостями циркуляції інформаційних потоків між її вузлами. Тому практична реалізація мережі зазвичай являє собою комбінування базових топологій, утворюючи складні синтезовані схеми, що відповідають конкретним технічним, функціональним та економічним вимогам.

Сучасні комп’ютерні мережі характеризуються низкою ключових властивостей, які визначають їхню якість і функціональність. Однією з таких властивостей є продуктивність, яка включає:

– Час реакції, тобто проміжок часу між моментом ініціації запиту до мережевого ресурсу та отриманням відповіді;
– Пропускну здатність, що відображає кількість інформації, яку мережа може передати за одиницю часу;
– Затримку передачі, яка описує часовий інтервал між надходженням пакета на вхід мережевого пристрою і його появою на виході.

Ще однією важливою характеристикою є надійність, яка включає:

– Коефіцієнт готовності – питому частку часу, коли система доступна для використання;
– Захищеність – здатність мережі забезпечувати цілісність і конфіденційність інформації, захищаючи її від несанкціонованого доступу;
– Відмовостійкість – можливість стабільної роботи мережі у разі виходу з ладу окремих її компонентів.

Розширюваність мережі визначає можливість інтеграції нових компонентів – додаткових користувачів, вузлів, програмного забезпечення тощо – без необхідності масштабної перебудови всієї інфраструктури. Тісно пов’язане з цим поняття масштабованості означає, що мережа здатна зростати як у кількості вузлів, так і в територіальному охопленні без помітного зниження продуктивності.

Важливою властивістю є також прозорість, що означає спрощення взаємодії користувача з мережею за рахунок приховування технічних деталей її функціонування. Завдяки цьому користувач може зосередитися на виконанні своїх завдань, не занурюючись у внутрішню логіку мережевих процесів.

Керованість мережі передбачає централізований моніторинг і адміністрування її елементів, включаючи виявлення збоїв, усунення неполадок, аналіз ефективності та планування подальшого розвитку.

Сумісність означає здатність мережі функціонувати з різними апаратними платформами та програмним забезпеченням, що особливо важливо для гетерогенних інформаційних систем.

З огляду на масштаби підприємства та кількість робочих місць, для реалізації мережевої інфраструктури доцільно обрати технологію Ethernet 1000Base-T, яка забезпечує передачу даних зі швидкістю до 1 Гбіт/с по витій парі категорії 5e або вищої. В якості топології обрано розширену зірку, що забезпечує централізоване управління і високу відмовостійкість. У зв'язку з наявністю бездротової точки доступу, остаточна схема мережі набуває гібридного характеру, поєднуючи елементи дротового і бездротового з'єднання.

Вибір кабельної підсистеми визначається як типом обраної мережі, так і специфікою топології. Фізичні параметри кабелю, необхідні для підтримки відповідного стандарту передачі даних, задаються на етапі виробництва і позначаються відповідним маркуванням, яке містить інформацію про категорію, тип ізоляції, екранування тощо. Це дозволяє забезпечити стабільність роботи мережі відповідно до обраної конфігурації.

У результаті, сьогодні практично всі мережі проектуються на базі UTP і волоконно-оптичних кабелів, коаксіальний кабель застосовують лише у виняткових випадках і те, як правило, при організації низькосшвидкісних стеків у монтажних шафах.

Серед всіх можливих середовищ передачі даних мережа Ethernet 1000Base T передбачає використання кабелю кручена пара категорії 5, 5e, 6та 7.

Розрізняють такі види крученої пари:

- неекранована вита пара (UTP — Unshielded twisted pair)
- екранована вита пара (STP — Shielded twisted pair)
- фольгована вита пара (FTP — Foiled twisted pair)
- фольгована екранована вита пара (SFTP — Shielded Foiled twisted pair)

Кабельна система локальної мережі побудована на основі неекранованої витої пари категорії 5е (див. рис. 2.2). Даний тип кабелю, як і будь-який інший має свої характеристики, правила монтажу та експлуатації. Недотримання цих вимог призведе до передчасного зносу кабельної системи.Використовуваний кабель є дешевий та простий для прокладання. Як концентратори можна використати багато різних пристроїв. Мережа на скрученій парі проста обслуговуванні, експлуатації та діагностуванні пошкоджень.

Кабелі горизонтальної системи повинні використовуватися разом з комутаційним устаткуванням і патч-кордами (або перемичками) тієї ж або більш високої категорії робочих характеристик.

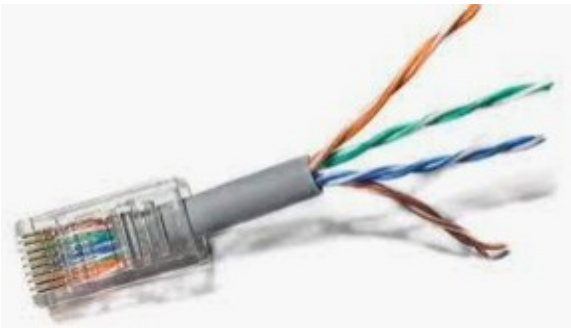


Рисунок 2.2 - Неекранована вита пара категорії 5е

У структурі локальної мережі використано пять некерованих комутаторів, кожен з яких має 16 портів. Якщо подивится на логічну схему мережі, ми побачимо, що ці комутатори будуть мати надлишкові порти, але оскільки ціна на ринку вісьми портових та шістнадцятипортових комутаторів різниться не багато, то з метою уніфікації мережі ми візьмемо і використаєио лише 16 портові. Ці комутатори слугують для підключення робочих місць мережі. Всі вони з'єднані лінками з центральним керованим комутатором, який виконує функцію основного вузла комутації та забезпечує централізоване управління трафіком.

Завдяки такій архітектурі можливо організувати декілька логічно ізольованих робочих груп, які функціонують автономно одна від одної. Це досягається шляхом конфігурації на керованому комутаторі віртуальних локальних мереж (VLAN). Частину його портів призначено для окремих VLAN, що дозволяє забезпечити ізоляцію трафіку між різними групами користувачів, підвищуючи рівень безпеки та керованість мережевої інфраструктури. Для кожного VLAN передбачено доступ до глобальної мережі Інтернет через маршрутизатор, однак без можливості взаємодії між окремими сегментами VLAN — це дозволяє обмежити міжмережевий трафік і зменшити ризики внутрішніх загроз. Окрім цього, до центрального комутатора підключено точку бездротового доступу, яка також виділена в окремий VLAN.

Такий підхід дозволяє логічно відокремити бездротовий сегмент від основної кабельної мережі з метою підвищення загального рівня інформаційної безпеки.

Уся описана вище структура та розподіл портів між VLAN детально представлена в таблиці 2.1.

Таблиця 2.1 – Логічна адресація в мережі та відповідні Vlan-и на портах головного комутатора

Вузол мережі	Робоча група/ номер Vlan		Назва кабінету	Номер порта головного комутатора	Адреса підмережі/Маска
1	2	3	4	5	6
WS_1—WS_4	office	3	дизайнери	1	192.168.3.0/24

Продовження таблиці 2.1

1	2	3	4	5	6
WS_5—WS_7	it	3	Відділ підтримки	2	192.168.3.0/24
WS_8-WS_19	office	3	дизайнери	3	192.168.3.0/24
WS_20—WS_25	office	8	Керівництво та економісти	3	192.168.8.0/24
WS_26—WS_32	office	3	Маркетологи, поліграфія	7	192.168.3.0/24
S_1, S_2	office	3	Відділ IT	9,10	192.168.3.0/24
Ap_1	wifi	9	серверна	11,12	192.168.9.0/24

2.3 Обґрунтування вибору комунікаційного обладнання

У проєктованій комп'ютерній мережі передбачається використання комутаторів із шістнадцятьма портами для забезпечення підключення кінцевих пристроїв.

З метою задоволення потреб підприємства "NOWA-T" було здійснено підбір відповідного мережевого обладнання на основі пропозицій, представлених в інтернет-магазині ROZETKA.

За допомогою фільтрації товарів у ціновому діапазоні від 4000 до 7000 гривень було відібрано три моделі комутаторів, технічні характеристики яких зведено в таблиці 2.2 для зручного порівняння.

Аналізуючи дані таблиці, з урахуванням балансу між вартістю та функціональними можливостями пристроїв, для реалізації мережевої інфраструктури було обрано комутатор TP-LINK TL-SG1016PE. Незважаючи на дещо вищу вартість у порівнянні з іншими моделями, дана модель має ряд переваг, серед

яких особливо варто відзначити наявність підтримки технології PoE (Power over Ethernet), що дозволяє передавати живлення по мережевому кабелю, а також розширений гарантійний термін від виробника. Ці характеристики суттєво підвищують експлуатаційну цінність пристрою в умовах корпоративного використання.

Зовнішній вигляд обраного комутатора представлено на рисунку 2.3, що дозволяє оцінити конструктивні особливості та форму виконання пристрою.

Таблиця 2.2 – Комутатори робочих груп на 16 портів

Характеристика	TP-LINK TL-SG1016PE	D-Link DGS-1100-16V2	Zyxel GS1900-16
1	2	3	4
Кількість портів	16 x Gigabit Ethernet RJ45	16 x Gigabit Ethernet RJ45	16 x Gigabit Ethernet RJ45
Підтримка PoE	Так (8 портів PoE+, 802.3at/af)	Ні	Ні
Загальний PoE бюджет	150 Вт	N/A	N/A
Комутаційна ємність	32 Гбіт/с	32 Гбіт/с	32 Гбіт/с
Швидкість пересилання пакетів	23.8 Mpps	23.8 Mpps	23.8 Mpps
Jumbo Frame	10 КБ	9 КБ	9 КБ
Орієнтовна ціна	6000 грн	4700 грн	3500 грн

Рисунок 2.3 –Вигляд комутатора TP-LINK TL-SG1016PE спереду

Аналогічним чином здійснено підбір центрального комутатора, який відіграє ключову роль у структурі мережі, виконуючи функції комутації між усіма робочими групами та керування віртуальними локальними мережами (VLAN).

Для пошуку відповідного обладнання в інтернет-магазині було застосовано фільтри:

- максимальна вартість до 50 000 грн,
- підтримка VLAN,
- кількість портів не менше 12

На основі встановлених критеріїв сформовано перелік доступних моделей, порівняльні технічні характеристики яких подано в таблиці 2.3.

Таблиця 2.3 – Порівняльна характеристика керованих комутаторів

Характеристика	Cisco Business CBS250-16T-2G	TP-Link JetStream TL-SG2218	D-Link DGS-1210-18
1	2	3	4
Тип комутатора	Smart Managed	L2 Managed	Smart Managed
Кількість Gigabit RJ45 портів	16	16	16

Продовження таблиці 2.3

1	2	3	4
Кількість SFP/ SFP+ портів	2 x Gigabit SFP	2 x Gigabit SFP	2 x Gigabit SFP
PoE підтримка	Ні	Ні	Ні
Комутаційна ємність	36 Гбіт/с	36 Гбіт/с	36 Гбіт/с
Швидкість пере-силання пакетів	26.78 Mpps	26.78 Mpps	26.8 Mpps
Jumbo Frame	9 КБ	9 КБ	10 КБ
Routing (Марш-рутизація)	Статична IPv4/ IPv6	Статична IPv4/IPv6	Статична IPv4
VLAN підтримка	4096 активних VLANs (802.1Q), Voice/Surveillance VLAN	4K VLANs (802.1Q), GVRP, QinQ	256 статичних VLANs (802.1Q), Auto Voice/ Surveillance VLAN
Управління	Веб-інтерфейс, CLI, SNMP	Веб-інтерфейс, CLI, SNMP, Omada SDN	Веб-інтерфейс, D-Link Network Assistant
Приблизна вартість	9500 грн.	8500 грн.	8000 грн.

На основі даних таблиці 2.3, а також з урахуванням співвідношення ціни та технічних параметрів, для використання в якості центрального комутатора мере-

жі було обрано модель Cisco Business CBS250-16T-2G. Цей пристрій відповідає всім заданим вимогам — підтримує VLAN, має необхідну кількість портів, відзначається високою надійністю та функціональністю, що робить його оптимальним вибором для побудови керованої та масштабованої мережі.

Рисунок 2.4 – Зовнішній вигляд Cisco Business CBS250-16T-2G

У мережі передбачено використання бездротової точки доступу для забезпечення з’єднання мобільних пристроїв.

З метою вибору оптимального варіанту було проаналізовано три моделі точок доступу.

Порівняльна характеристика цих моделей представлена у таблиці 2.4, що дозволяє здійснити обґрунтований вибір з урахуванням технічних параметрів та вартості обладнання.

Таблиця 2.4 – Порівняльна характеристика точок доступу

Характеристика	Ubiquiti UniFi AP Long Range (UAP-LR)	TP-Link Omada EAP610	Zyxel NWA110AX
1	2	3	4
Стандарт Wi-Fi	802.11n (Wi-Fi 4)	802.11ax (Wi-Fi 6)	802.11ax (Wi-Fi 6)

Продовження таблиці 2.4

1	2	3	4
Діапазони частот	2.4 ГГц (однодіапазонна)	2.4 ГГц та 5 ГГц (дводіапазонна)	2.4 ГГц та 5 ГГц (дводіапазонна)
Швидкість Wi-Fi (макс.)	300 Mbps (2.4 GHz)	574 Mbps (2.4 GHz) + 1201 Mbps (5 GHz) = 1775 Mbps	575 Mbps (2.4 GHz) + 1200 Mbps (5 GHz) = 1775 Mbps
MIMO	2x2 MIMO (2.4 GHz)	2x2 MIMO (2.4 GHz) + 2x2 MIMO (5 GHz)	2x2 MIMO (2.4 GHz) + 2x2 MIMO (5 GHz)
Ethernet порти	1 x Gigabit Ethernet	1 x Gigabit Ethernet	1 x Gigabit Ethernet
Живлення	Passive PoE (24V)	802.3at/af PoE (Active PoE)	802.3at/af PoE (Active PoE)
Управління	UniFi Network Controller (локальний/хмарний)	Omada SDN Controller (апаратний/програмний/хмарний)	Zyxel Nebula Cloud (хмарний) / Standalone
Вартість	4-5 тисяч грн	4900 грн	Близько 5000 грн

На підставі аналізу даних, наведених у таблиці 2.4, з урахуванням оптимального співвідношення вартості та функціональних можливостей, для реалізації бездротового сегмента мережі було обрано точку доступу TP-Link Omada EAP610.

Цей пристрій забезпечує вирізняється якісним апаратним виконанням і надійною роботою в умовах постійного навантаження.

Рисунок 2.5 – Зовнішній вигляд безпровідної точки доступуTP-Link Omada EAP610

У комп’ютерній мережі підприємства “NOWA-T” заплановано використання персональних комп’ютерів у ролі двох серверів, а також одного вузла, який виконуватиме функцію шлюза для підключення до мережі Інтернет. Вибір відповідного обладнання здійснюється за аналогічним принципом, що й попередньо описані компоненти мережі, із врахуванням необхідних технічних характеристик.

Для забезпечення надійної та стабільної роботи серверної частини обрані комп’ютери на базі процесора Intel Core i3–5-го покоління, з обсягом оперативної пам’яті не менше 8 ГБ, а також оснащені двома твердотільними накопичувачами (SSD) по 240 ГБ кожен — один для операційної системи, інший для резервного збереження службової інформації або логів.

У таблиці 2.5 наведено детальну технічну характеристику обраної моделі ПК ARTLINE Business B29 (B29v75), який задовольняє вказаним вимогам щодо апаратного забезпечення та є доцільним вибором для реалізації серверної інфраструктури в межах локальної мережі.

Таблиця 2.5 – Характеристики ПК ARTLINE Business B29 (B29v75)

Характеристика	Значення
Код моделі	B29v75
Виробник ПК	ARTLINE
Серія ПК	Business B29
Процесор	Intel® Core™ i5-13400
Кількість ядер процесора	10 ядер (6P + 4E)
Кількість потоків	16 потоків
Базова тактова частота	2.5 GHz
Максимальна тактова частота (Turbo Boost)	4.6 GHz
Інтегрована графіка	Intel HD (Intel UHD Graphics 730)
Оперативна пам'ять (RAM)	64 GB DDR4-3200 A-brand
Накопичувач 1 (системний SSD)	480GB M.2 NVMe SSD
Накопичувач 2 (HDD)	1 TB (Тип: BOX)
Чіпсет материнської плати	Intel® H610
Модель материнської плати	PRIME H610M-K D4 (Asus)
Блок живлення	400W
Операційна система	No OS (без ОС)
Гарантія	38 місяців

ARTLINE Business B29 (B29v75) / ARTLINE / Intel® Core™ i5 / Intel (6p+4e)-Core i5-13400 2.5-4.6GHz / Intel HD / 64GB DDR4-3200 A-brand / 480GB

M.2 NVMe SSD / 1TB / BOX / Intel® H610 / PRIME H610M-K D4 / LogicPower S605 U3 / 400W / No OS / Black / 12міс. / B29v75

ARTLINE Business B29 (B29v75) – ідеальне рішення для ефективної організації роботи в офісі. Гарантія на цей продукт становить цілих 38 місяців, що говорить про високий рівень надійності та довговічності цього пристрою. Цей системний блок виконаний у класичному чорному кольорі, що підкреслює його строгий та професійний вигляд.

Серцем цього комп'ютера є процесор Intel Core i5-13400 із 10 ядрами, що працюють на частоті від 2.5 до 4.6 ГГц. Ця потужна "мозкова" частина забезпечує неймовірно високу продуктивність і дозволяє легко справлятися з найвибагливішими завданнями. Процесор охолоджується за допомогою BOX системи, що гарантує надійне охолодження та стійку роботу за будь-яких умов.

Великий обсяг оперативної пам'яті – це одна з основних переваг комп'ютера. 64 ГБ DDR4-3200 A-brand дозволяють багатозадачністю без уповільнень та перебоїв. Ви можете одночасно працювати з безліччю програм, обробляти великі обсяги даних і навіть займатися відеомонтажем – все відбуватиметься на найвищому рівні.

Зберігайте свої файли, документи та програми на швидкому та ємному накопичувачі об'ємом 480 ГБ M.2 NVMe SSD. Це гарантує миттєвий доступ до інформації та швидке завантаження операційної системи. Додатково вам доступний об'ємний HDD накопичувач на 1 ТБ для довгострокового зберігання даних.

Материнська плата PRIME H610M-K D4, заснована на чіпсеті Intel H610, забезпечує стабільну роботу всієї системи. Інтегрована відеокарта Intel HD дозволяє переглядати мультимедійний контент та обробляти графіку. Все це поміщено в елегантний корпус LogicPower S605 U3, який, крім своєї стильної зовнішності, також сприяє ефективному охолодженню.

Отже, ми обрали таке обладнання:

- комутатори не керовані — 5 шт — 6000 грн - TP-LINK TL-SG1016PE
- комутатор керований - 1 шт — 9 500 грн - Cisco Business CBS250-16T-2G
- точка доступу — 1 шт — 4800 грн - TP-Link Omada EAP610
- сервер — 1 шт — 33 000 грн- ARTLINE Business B29 (B29v75)
- сервер — 2 шт — 25 000 грн- ARTLINE Business B29 (B29v75)

2.4 Особливості монтажу мережі

Особливості монтажу та правила поводження з неекранованою крученою парою UTP 5e

Монтаж неекранованої витої пари категорії 5e досить простий, але має свої нюанси, які слід враховувати для забезпечення надійної роботи мережі. Залежно від умов прокладки, існують два основні типи зовнішньої ізоляції кабелю.

Якщо кабель прокладається всередині приміщення, для зовнішньої оболонки зазвичай використовується полівінілхлорид (ПВХ). Цей матеріал має високу стійкість до лугів, розчинників, мінеральних олій та багатьох видів кислот, що робить його довговічним в умовах стандартного офісного або житлового середовища. Також він не підтримує горіння, що є додатковою перевагою з точки зору пожежної безпеки. Однак, ПВХ має низьку морозостійкість і чутливий до ультрафіолетового випромінювання, тому його не рекомендується використовувати для прокладки на відкритому повітрі або в умовах сильних температурних коливань.

Для зовнішньої прокладки, тобто коли кабель знаходиться поза приміщенням, необхідно застосовувати ізоляцію з поліетилену (ПЕ). Поліетиленова оболонка більш стійка до впливу морозу та ультрафіолету, має високу механічну міцність та ударостійкість. При прокладанні на великі відстані, особливо якщо кабель натягують між віддаленими опорами, поліетиленову оболонку додатково

посилюють сталевим тросом або сталевою жилою, щоб уникнути провисання та пошкоджень.

Матеріал провідників відіграє ключову роль в роботі кабелю. Стандартом для крученої пари є мідні провідники, які забезпечують високу провідність і довговічність. Для зниження вартості виробники іноді використовують біметалеві провідники — ССА (обміднений алюміній). Такий кабель може працювати без проблем на коротких відстанях, але при довгих лініях виникають підвищені втрати сигналу через більший опір, а також скорочується термін служби кабелю.

При прокладці витої пари поряд із силовими кабелями існують чіткі норми по мінімальним відстаням, які необхідно дотримуватися. Відстань залежить від типу крученої пари (екранована чи ні), потужності силового кабелю та інших параметрів. Хоча в невеликих приміщеннях спільне розміщення силових і мережевих кабелів може не викликати проблем із якістю сигналу, для стабільності зв'язку все ж рекомендується розводити їх на відстань не менше 30–50 см.

Ще один важливий момент — неекрановану виту пару слід уникати прокладки поруч із джерелами сильних електромагнітних завад, такими як понижуючі трансформатори, люмінесцентні світильники із пускорегулюючою апаратурою тощо. Якщо все ж потрібно перетинати силові та мережеві кабелі, це треба робити виключно під прямим, перпендикулярним кутом, щоб мінімізувати взаємні перешкоди.

Прокладку кабелю слід виконувати цілими шматками, без сполук по трасі, щоб уникнути втрат сигналу та механічних пошкоджень. Важливо заздалегідь продумати оптимальний маршрут з мінімальною довжиною траси. На поворотах кабель не повинен згинатися під прямим кутом — мінімальний радіус вигину має бути не меншим за чотири діаметри кабелю, щоб не пошкодити внутрішні жили і не погіршити характеристики сигналу.

Для підключення витої пари до комп'ютерів або мережевого обладнання існують два основні варіанти: встановлення розетки RJ-45 або виведення кабелю

зі стіни з подальшим обтиском коннектором. Перший варіант вважається більш практичним і зручним, оскільки при пошкодженні відкритої частини кабелю достатньо замінити тільки сегмент від стіни до розетки. Якщо ж кабель одразу підключений коннектором, при поломці доведеться встановлювати додаткові з'єднувачі або повністю замінювати кабель, що часто ускладнює ремонт, особливо у завершеному інтер'єрі.

2.5 Тестування мережі

Тестування комп'ютерної мережі є завершальним етапом монтажу комп'ютерної мережі, а також необхідною умовою її прийняття в експлуатацію. Тестування дає можливість переконатися у якості роботи системи та нормальному функціонуванні всіх мережних додатків, а також гарантувати відповідність мережі існуючим нормативним документам. Об'єктивне тестування комп'ютерної мережі дозволяє усунути як дрібні, і серйозні недоліки у її роботі, заощадити на подальшому обслуговуванні комп'ютерних мереж хорошу суму.

Що таке тестування комп'ютерної мережі?

Отже, від якості тестування комп'ютерної мережі безпосередньо залежить її надійність та довговічність, тому до цього питання слід підходити вдумливо та докладно. Навпаки, якщо з тестуванням комп'ютерної мережі поспішити або зовсім пустити справу на самоплив, під загрозою опиниться вся інформаційна база підприємства.

Тестування комп'ютерних мереж реалізується як за допомогою спеціального тестового обладнання, так і з використанням комп'ютерного обладнання та програмного забезпечення. Процедура тестування включає наступні опорні пункти:

- детальне вивчення роботи мережі
- оцінка якості сигналів, що передаються

– виявлення «прихованих» дефектів
– визначення «вузьких місць» продуктивності серверів
– оцінка захищеності мережі від вторгнення внутрішніх та зовнішніх порушників
– внесення необхідних доповнень та коректив
– завершальне регулювання налаштувань обладнання
– усунення несправностей у роботі

Після завершення тестування пасивного та активного обладнання комп'ютерної мережі на неї складається документація " - процедура, покликана допомогти майбутнім користувачам мережі експлуатувати її вільно, раціонально і з максимально високими для роботи підприємства результатами.

Проблеми, що виникають у локальних мережах, можна умовно розділити на три основні групи: несправності на фізичному рівні, перевантаження в мережі і помилки в роботі мережевих протоколів. Несправності фізичного рівня обумовлені виходом з ладу будь-яких електричних або електронних мережевих пристроїв та компонентів. Перевантаження в мережі виникають, якщо той чи інший мережевий пристрій не справляється з обробкою запитів, що до нього надходять. Помилки в роботі мережних протоколів призводять до того, що мережні пристрої не можуть взаємодіяти один з одним через некоректне функціонування мережних драйверів або неможливість обробки мережею пакетів якогось протоколу (або декількох протоколів одночасно).

Несправності фізичного рівня можуть виникнути у мережному пристрої, середовищі передачі або в місці їх контакту. Вони найпростіше піддаються виявленню, оскільки мають постійний характер (природно, досі їх усунення). Локалізувати несправність можна зокрема за допомогою найпростіших тестерів для локальних мереж. Такі тестери перевіряють роботу каналу в один бік (від тестера до концентратора або мережної плати комп'ютера). Якщо дефект має місце в середовищі передачі, його можна виявити за допомогою кабельного

тестера. Плаваючі помилки, зумовлені поганим контактом у з'єднувачах, діагностувати дещо складніше. Але навіть такі несправності можна виявити за допомогою кабельного тестера – достатньо бути уважним. До речі, хоч як це банально звучить, але хочеться нагадати, що найкращий спосіб профілактики утворення дефектів у середовищі передачі - використання якісних матеріалів та виконання професійного монтажу.

Зовсім інша справа - помилки внаслідок навантаження мережі та некоректної роботи мережевих протоколів. Такі помилки найважчі у виявленні, оскільки найчастіше носять нерегулярний характер. Вони й більш підступні, оскільки можуть паралізувати роботу організації у невідповідний момент. Їх інструментальна діагностика виконується за допомогою досить дорогих приладів - мережевих тестерів та аналізаторів протоколів.

Мережеві тестери займають проміжне положення між кабельними тестерами та аналізаторами протоколів. Вони є незамінними для пошуку несправностей у мережах. Виробники випускають широку гаму таких приладів, що відрізняються набором контрольованих параметрів та сервісних функцій, здатністю працювати в тих чи інших мережах (наприклад, Ethernet та/або Token Ring), конструктивним виконанням та ціною. Ці прилади дозволяють вимірювати безліч різних параметрів, наприклад пікову та усереднену завантаженість, частку широкомовного трафіку, збої у роботі протоколів верхніх рівнів. У мережах Ethernet деякі з них здатні підраховувати кількість конфліктів (колізій), ідентифікувати адреси DLC-пакетів (з помилками CRC, коротких та довгих), відрізняти фрагменти від пакетів з помилками CRC та коротких пакетів.

Надзвичайно зручною та корисною є здатність деяких мережевих тестерів зберігати результати тестування для подальшої обробки. Зазвичай результати завантажуються потім у комп'ютер і обробляються відповідними програмами отримання аналітичної інформації (наприклад, піку максимального навантаження у мережі, кількості і типів помилок). Для отримання повної картини функціонування мережі дані можуть бути відсортовані за протоколами та помилками.

Деякі сучасні моделі мережевих тестерів можуть працювати як сервери Web, тому вони дозволяють як інтерфейс користувача використовувати звичайний браузер. Але найцікавішими пристроями є прилади, що поєднують функції портативного мережевого та кабельного тестера. Хоча їхня вартість і висока, вони поєднують у собі найкращі якості обох пристроїв і надзвичайно зручні в експлуатації.

Незважаючи на всі переваги, портативні мережеві тестери мають один недолік - вони не можуть перехоплювати і декодувати пакети. І якщо такі можливості необхідні, наприклад, для більш глибокого вивчення проблем функціонування мережних додатків, тоді вам варто звернути увагу на аналізатори протоколів. Фактично вони є комп'ютером з одним або кількома мережевими інтерфейсами, зі спеціалізованим програмним забезпеченням. Деякі з цих аналізаторів можуть розуміти дві сотні (!) різних протоколів. Кожен як мінімум здатний перехоплювати пакети та фільтрувати їх відповідно до заданих параметрів. Використовуючи відповідні фільтри, ви можете отримати масу різної інформації, що іноді виявляється просто незамінною. Надалі збережена інформація може бути оброблена для складання узагальненого зведення про пакети та отримання детального резюме про протоколи, що використовуються в них. Крім того, всі аналізатори фіксують час проходження пакета та показують мережеві та фізичні адреси його відправника та одержувача.

Аналізатори протоколів здатні навіть збирати дані роботи того чи іншого зазначеного користувачем рівня, причому вся необхідна інформація виявляється відразу перед очима користувача. Але щоб користуватися такими пристроями, адміністратор повинен мати високу кваліфікацію і досить добре розумітися на мережевих протоколах. В іншому випадку він або буде просто не в змозі впоратися з великим обсягом інформації (навіть фільтри не завжди допомагають), або може неправильно інтерпретувати дані аналізатора. Спроби ж внести виправлення на основі невірних висновків загрожують серйозною небезпекою виходу з ладу сегмента мережі. Тому аналізатори протоколів найчастіше викори-

стовуються як експертні системи і лише у тих випадках, коли всі інші засоби вичерпані.

Зазначимо, що портативні мережеві тестери хоча і вимагають певної кваліфікації, але в цілому простіше в освоєнні. Сьогодні, при мінімальній вазі та габаритах, вони мають потужність, достатню для діагностики більшості проблем у ЛОМ, особливо за підтримки функцій кабельного тестера.

За матеріалами https://skomplekt.com/tools/134446.html/

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Налаштування головного комутатора

1. Початкове підключення та доступ до веб-інтерфейсу

Перед початком конфігурації переконайтеся, що комутатор фізично підключений.

Знаходження IP-адреси комутатора:

Варіант 1 (рекомендований): Утиліта Cisco Business Discovery (CBD): Завантажте та встановіть Cisco Business Discovery Utility (раніше FindIT Network Discovery Utility) з офіційного сайту Cisco. Запустіть її – вона автоматично знайде комутатор у вашій мережі та покаже його IP-адресу.

Варіант 2: IP-адреса за замовчуванням: Якщо комутатор не отримав IP через DHCP, він використовуватиме IP-адресу за замовчуванням: 192.168.1.254. Переконайтеся, що ваш комп'ютер знаходиться в тій же підмережі (наприклад, 192.168.1.10 з маскою 255.255.255.0).

Доступ до веб-інтерфейсу (див. рис. 3.1):

Відкрийте веб-браузер (Chrome, Firefox, Edge).

Введіть IP-адресу комутатора в адресний рядок (наприклад, https://192.168.1.254). Використовуйте https для безпечного з'єднання.

Облікові дані за замовчуванням:

Ім'я користувача (Username): cisco або admin

Пароль (Password): cisco або admin

Зміна паролю за замовчуванням (див. рис. 3.2)

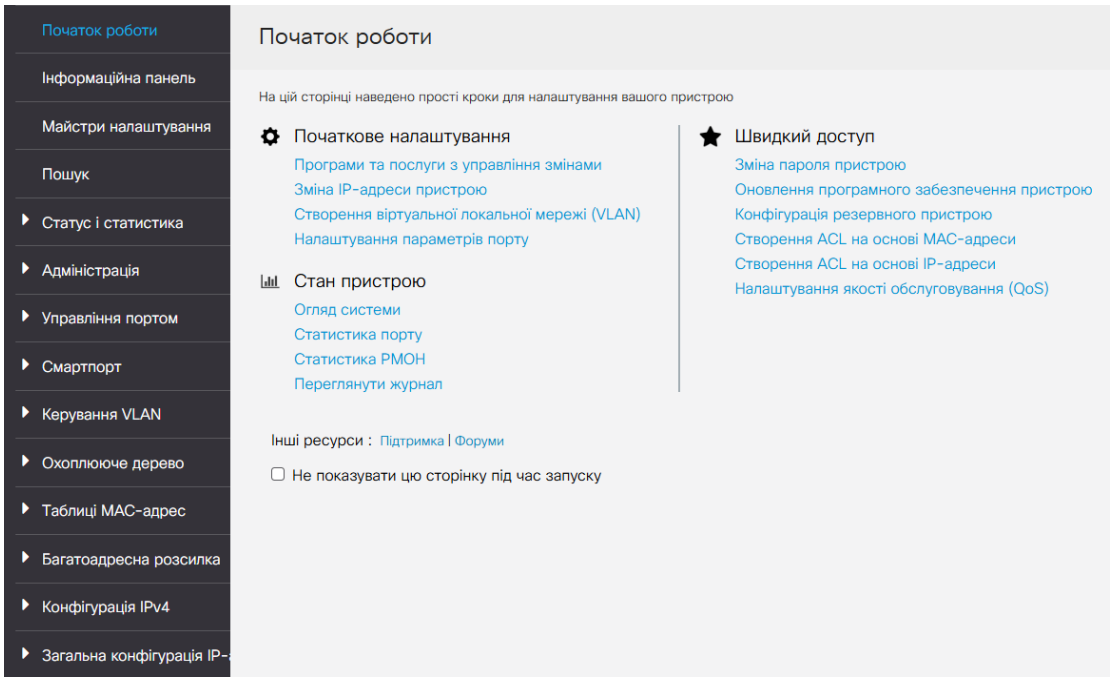


Рисунок 3.1 – Початкове меню інтерфейсу пристрою

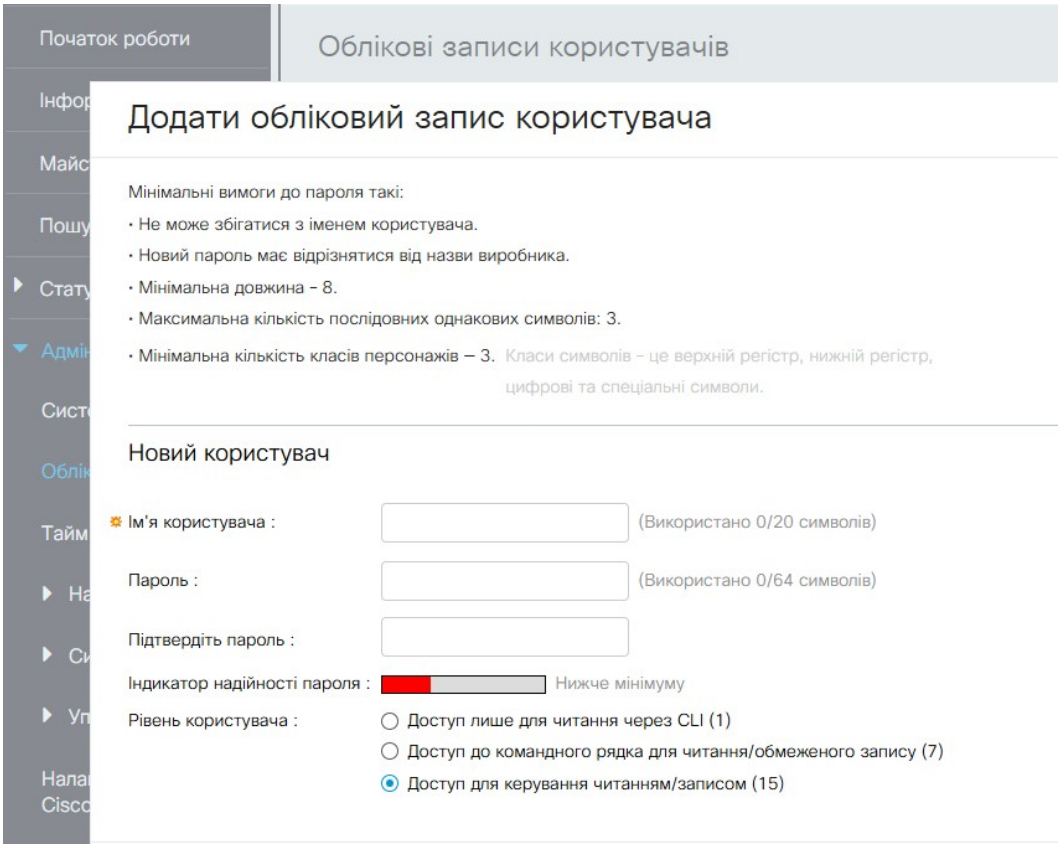


Рисунок 3.2 – Вікно створення нового користувача чи зміни паролю

2. Базові налаштування системи

Після входу до веб-інтерфейсу виконайте ці кроки:

Зміна IP-адреси управління (див. рис. 3.3):

Перейдіть до Administration > Interface Settings > IPv4 Interface.

Змініть тип IP-адреси з DHCP на Static.

Введіть бажану IP-адресу, маску підмережі та IP-адресу шлюзу за замовчуванням (Default Gateway).

Натисніть Apply (Застосувати). Після цього вам, можливо, доведеться знову підключитися до комутатора за новою IP-адресою.

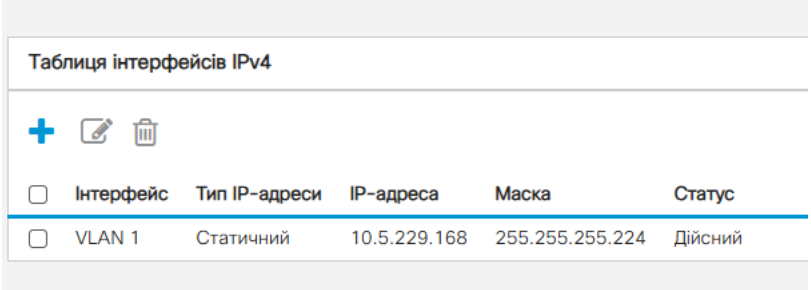


Рисунок 3.3 – Вікно зміни IP адреси пристрою

Налаштування системного часу (NTP):

Перейдіть до Administration > Time Settings > SNTP Client.

Увімкніть SNTP Client.

Додайте IP-адреси або доменні імена серверів NTP (наприклад, pool.ntp.org або внутрішні NTP-сервери).

Налаштуйте часовий пояс (Time Zone) (див. рис. 3.4).

Натисніть Apply. Правильний час важливий для журналів подій та сертифікатів.

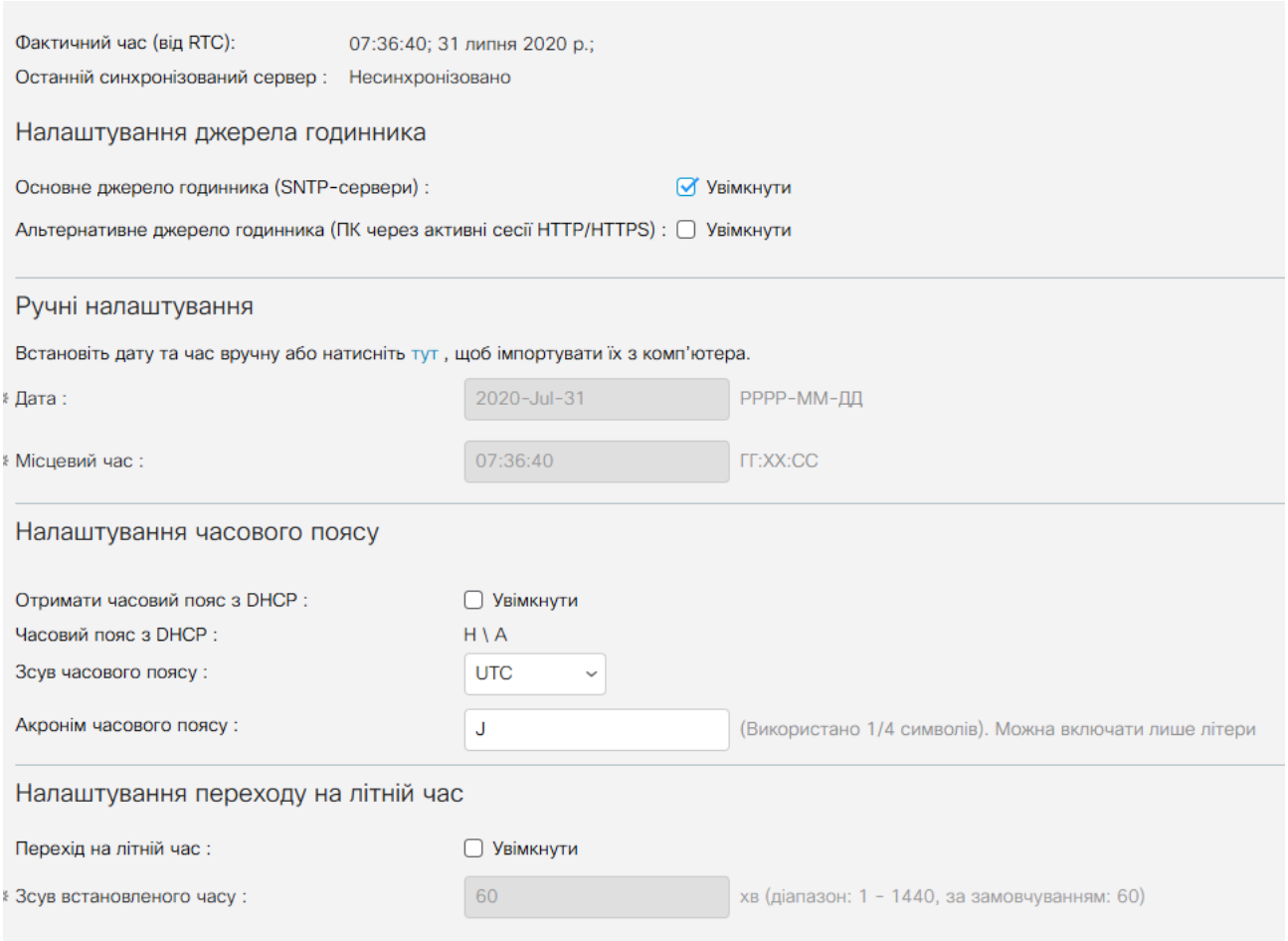


Рисунок 3.4 – Початкове вікно встановлення системного часу

Оновлення прошивки (Firmware Update):

Настійно рекомендується оновити прошивку до останньої стабільної версії. Це забезпечує виправлення помилок, підвищення безпеки та додавання нового функціоналу.

Завантажте останню прошивку для CBS250-16T-2G з офіційного сайту Cisco (потрібен Cisco.com акаунт).

Перейдіть до Administration > File Management > Firmware Upgrade.

Виберіть HTTP/HTTPS/TFTP/SCP (найпростіше використовувати HTTP/HTTPS з комп'ютера) або USB (якщо є USB-порт і підтримується).

Завантажте файл прошивки на комутатор (див. рис. 3.5).

Після завантаження, активуйте нову прошивку та перезавантажте комутатор. НЕ вимикайте живлення під час оновлення!

Збереження конфігурації:

ОБОВ'ЯЗКОВО! Усі зміни, які ви вносите, є тимчасовими, доки ви не збережете їх.

Натисніть значок Save (зазвичай дискета) у верхньому правому куті або перейдіть до Administration > File Management > Copy/Save Configuration.

Виберіть Running Configuration до Startup Configuration і натисніть Apply.

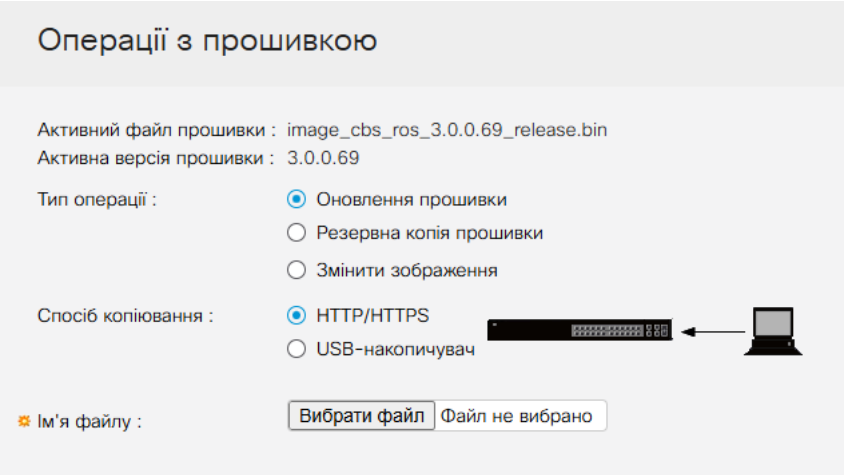


Рисунок 3.5 – Вікно оновлення прошивки

3. Основні мережеві конфігурації

3.1. Віртуальні локальні мережі (VLAN)

VLAN дозволяють логічно розділити вашу мережу на окремі сегменти, підвищуючи безпеку та ефективність (див. рис. 3.6).

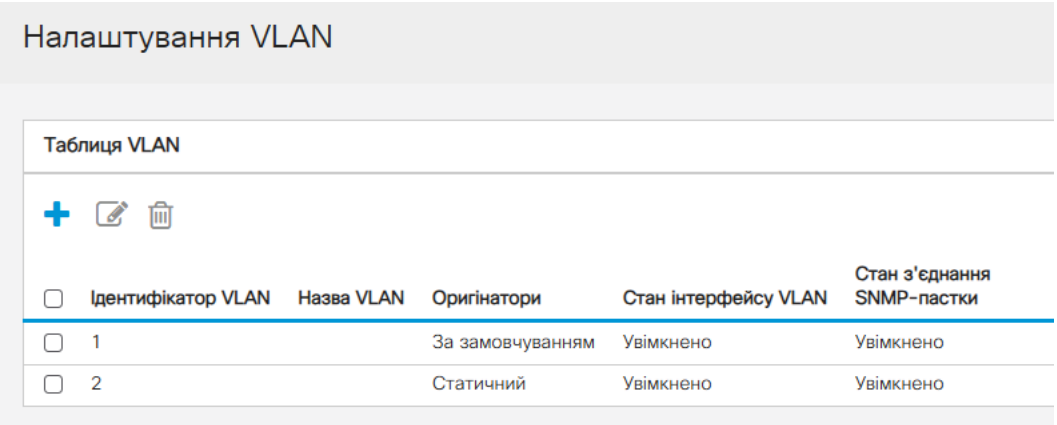


Рисунок 3.6 – Початкове вікно роботи з VLAN

Створення VLAN:

Перейдіть до VLAN Management > Create VLAN (див. рис. 3.7).

Натисніть Add та введіть VLAN ID (наприклад, 10, 20) та VLAN Name (наприклад, "Users", "Servers").

Натисніть Apply.

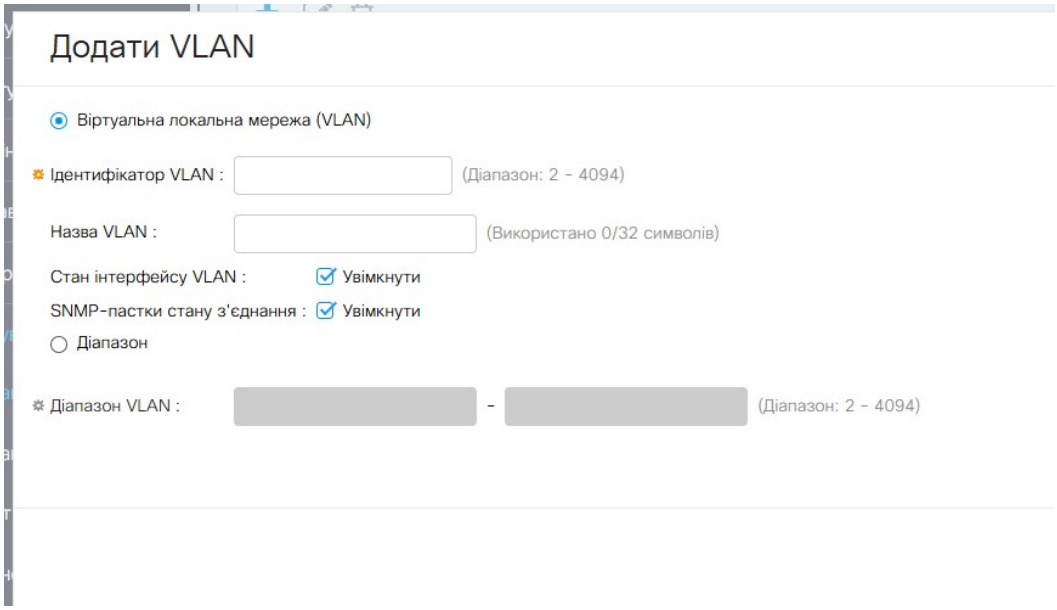


Рисунок 3.7 – Вікно створення VLAN

Призначення портів до VLAN:

Перейдіть до VLAN Management > Port to VLAN.

Виберіть VLAN ID, до якої хочете призначити порти.

Access Port (порт доступу): Для кінцевих пристроїв (комп'ютер, принтер, IP-телефон). Порт належить лише одній VLAN (див. рис. 3.8).

Виберіть порт(и) та встановіть VLAN Membership як Access.

Встановіть PVID (Port VLAN ID) на цю ж VLAN ID.

Натисніть Apply.

Trunk Port (магістральний порт): Для з'єднання з іншими комутаторами або маршрутизаторами, які передають трафік декількох VLANs.

Виберіть порт(и) та встановіть VLAN Membership як Trunk.

Виберіть, які VLANs дозволені на цьому транк-порті (Permitted VLANs).

Встановіть Native VLAN ID (непозначений трафік на цьому порту, зазвичай VLAN 1, але можна змінити).

Натисніть Apply.

3.2. Агрегація каналів (Link Aggregation - LAG/LACP)

Об'єднує декілька фізичних портів в один логічний канал для збільшення пропускної здатності та відмовостійкості.

Перейдіть до Port Management > Link Aggregation > LAG Management.

Натисніть Add.

Виберіть LAG ID (наприклад, LAG1).

Виберіть LAG Type як LACP (рекомендовано для сумісності) або Static.

Додайте бажані порти до групи (Members).

Натисніть Apply. На іншому кінці (іншому комутаторі або сервері) також потрібно налаштувати LAG на відповідних портах.

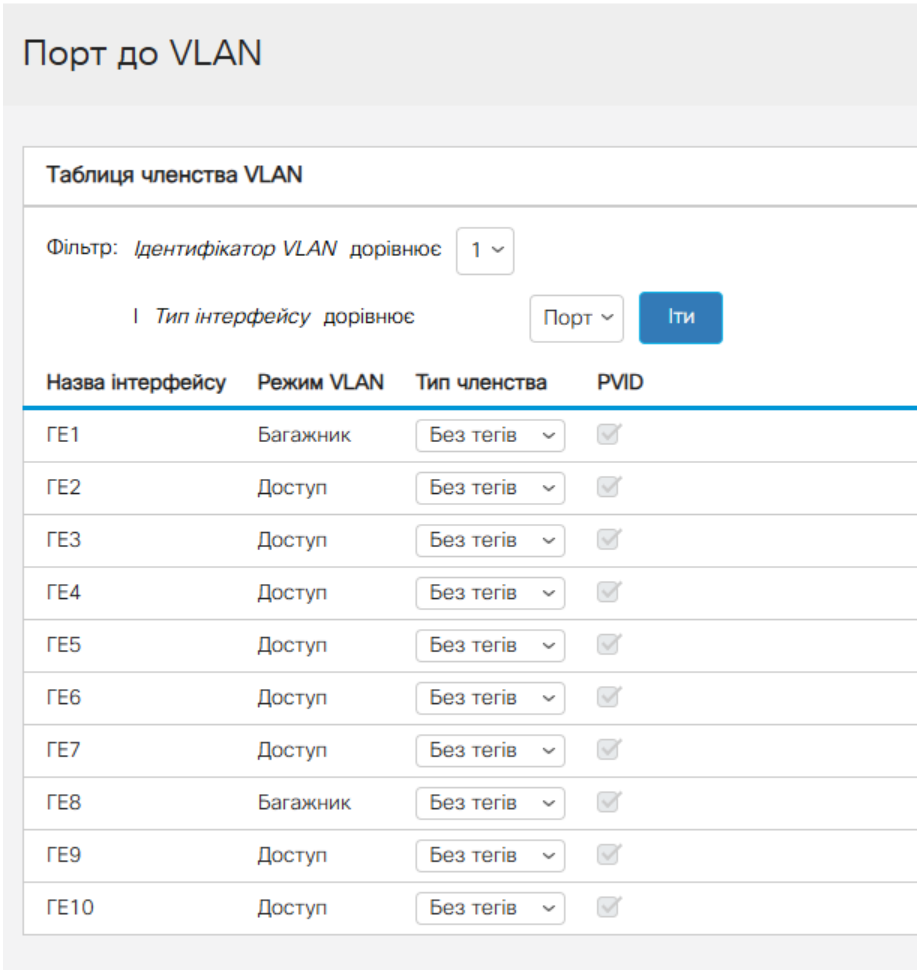


Рисунок 3.8 – Присвоєння порту VLAN ID

3.3. Якість обслуговування (Quality of Service - QoS)

Дозволяє пріоритезувати критичний трафік (наприклад, VoIP, відео) над менш чутливим до затримок трафіком.

Перейдіть до QoS > QoS Basic Settings.

Увімкніть QoS Mode і виберіть метод класифікації трафіку (наприклад, 802.1p або DSCP).

Перейдіть до QoS > CoS/802.1p Settings або QoS > DSCP to Queue Settings для налаштування мапінгу пріоритетів до черг.

Ви можете налаштувати Bandwidth Control на окремих портах (QoS > Bandwidth Control) для обмеження або гарантування пропускної здатності.

3.4. Безпека портів (Port Security)

Обмежує кількість MAC-адрес, які можуть підключатися до певного порту, запобігаючи несанкціонованим пристроям.

Перейдіть до Security > Port Security.

Виберіть порт(и) (див. рис. 3.9).

Увімкніть Port Security.

Встановіть Max Allowed MAC Addresses (наприклад, 1, якщо це порт для одного комп'ютера).

Виберіть Action при порушенні (наприклад, Discard - відкидати пакети, Shutdown - вимкнути порт).

Натисніть Apply.

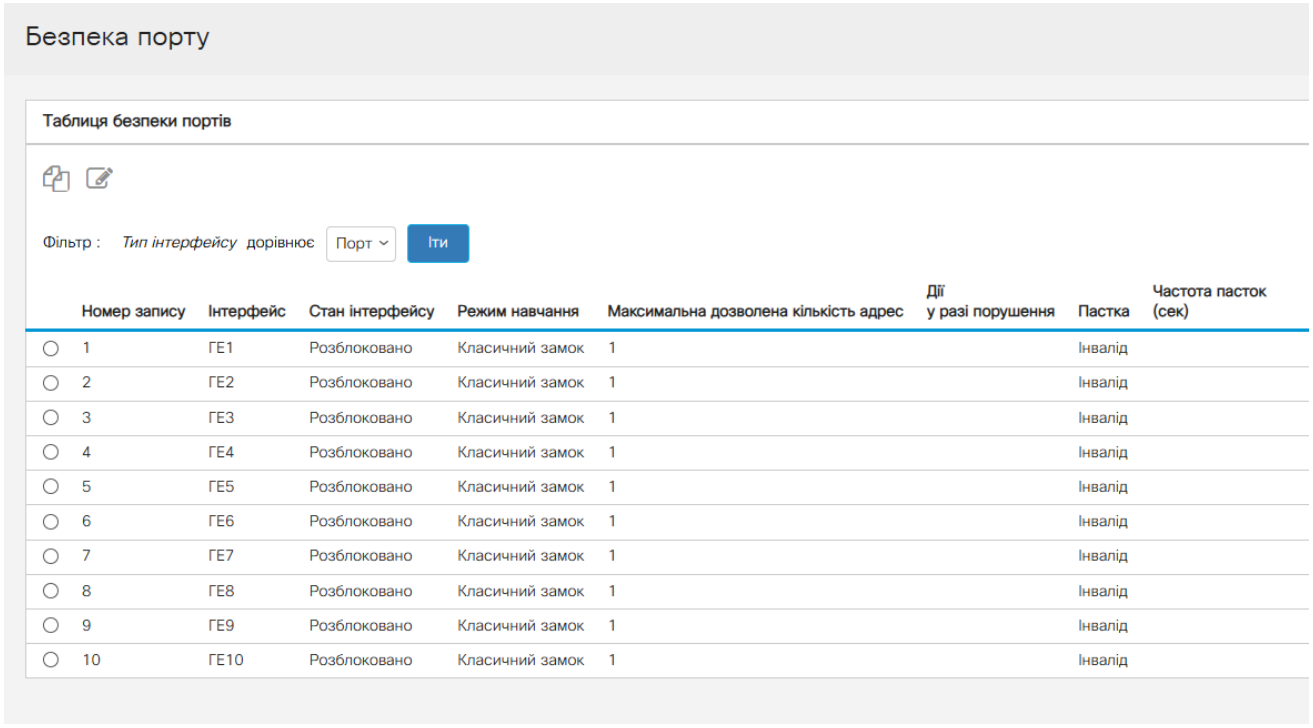


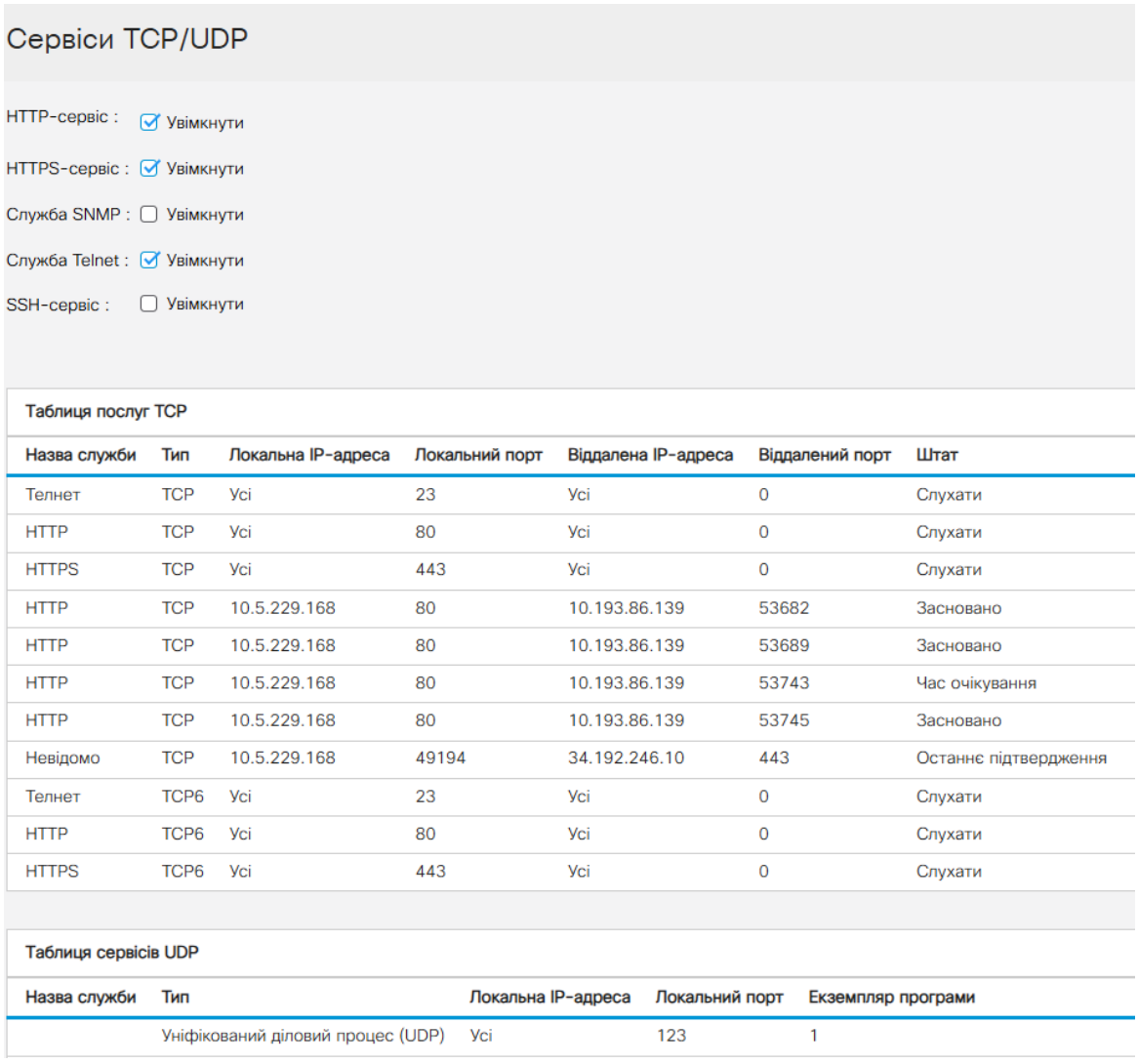
Рисунок 3.9 – Налаштування Port Security

4. Моніторинг та усунення несправностей

Системний журнал (Log):

Перейдіть до Administration > Log > RAM Log. Переглядайте логи для виявлення проблем або несанкціонованих дій.

Налаштуйте Remote Log (Syslog) (Administration > Log > Remote Log Servers) для відправки логів на зовнішній syslog-сервер.



Сервіси TCP/UDP

HTTP-сервіс : Увімкнути

HTTPS-сервіс : Увімкнути

Служба SNMP : Увімкнути

Служба Telnet : Увімкнути

SSH-сервіс : Увімкнути

Таблиця послуг TCP

Назва служби	Тип	Локальна IP-адреса	Локальний порт	Віддалена IP-адреса	Віддалений порт	Штат
Телнет	TCP	Усі	23	Усі	0	Слухати
HTTP	TCP	Усі	80	Усі	0	Слухати
HTTPS	TCP	Усі	443	Усі	0	Слухати
HTTP	TCP	10.5.229.168	80	10.193.86.139	53682	Засновано
HTTP	TCP	10.5.229.168	80	10.193.86.139	53689	Засновано
HTTP	TCP	10.5.229.168	80	10.193.86.139	53743	Час очікування
HTTP	TCP	10.5.229.168	80	10.193.86.139	53745	Засновано
Невідомо	TCP	10.5.229.168	49194	34.192.246.10	443	Останнє підтвердження
Телнет	TCP6	Усі	23	Усі	0	Слухати
HTTP	TCP6	Усі	80	Усі	0	Слухати
HTTPS	TCP6	Усі	443	Усі	0	Слухати

Таблиця сервісів UDP

Назва служби	Тип	Локальна IP-адреса	Локальний порт	Екземпляр програми
	Уніфікований діловий процес (UDP)	Усі	123	1

Рисунок 3.10 – Створення Static Routing

Статус портів:

Перейдіть до Port Management > Port Settings або Port Management > Port Status. Переглядайте статус, швидкість, помилки на портах.

Статистика трафіку:

Port Management > Port Statistics. Дозволяє бачити обсяги трафіку та помилки на кожному порту.

5. Додаткові можливості.

Static Routing (див. рис. 3.10)(Статична маршрутизація): Комутатор CBS250 підтримує базову статичну маршрутизацію. Налаштовується в розділі IP Configuration > Static Routes.

Access Control Lists (ACL): Розширені правила фільтрації трафіку за різними критеріями. Налаштовується в розділі Security > ACL.

SNMP: Протокол для моніторингу мережевих пристроїв з централізованої системи управління. Налаштовується в Administration > SNMP.

Cisco Business Dashboard: Для управління кількома комутаторами Cisco Business з єдиного інтерфейсу. Рекомендується для великих розгортань.

6. Важливі нагадування

Задайте час перезавантаження пристрою (див. рис. 3.11)

Завжди зберігайте конфігурацію! Після будь-яких змін натискайте кнопку "Save" (дискета) у веб-інтерфейсі.

Регулярно робіть резервні копії конфігурації: Експортуйте файл конфігурації (Administration > File Management > Copy/Save Configuration), щоб можна було відновити налаштування в разі потреби (див. рис. 3.12).

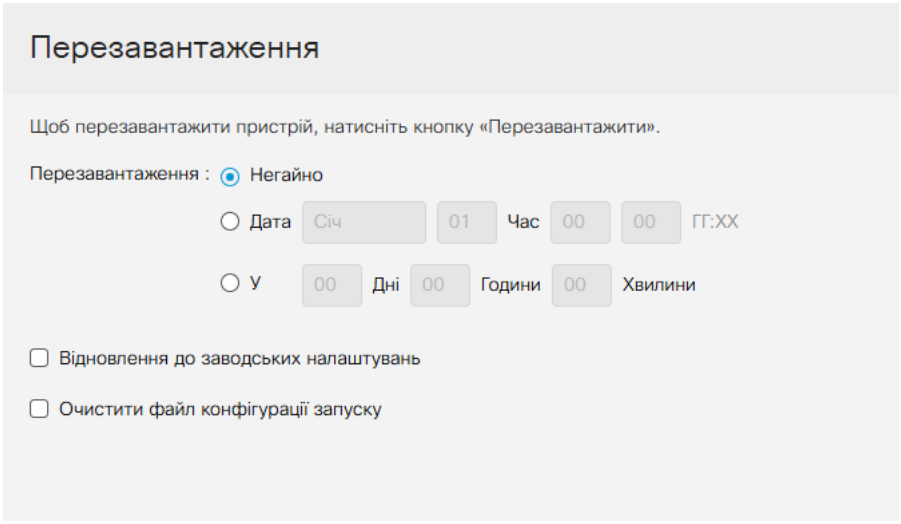


Рисунок 3.11 – Задання часу перевантаження пристрою

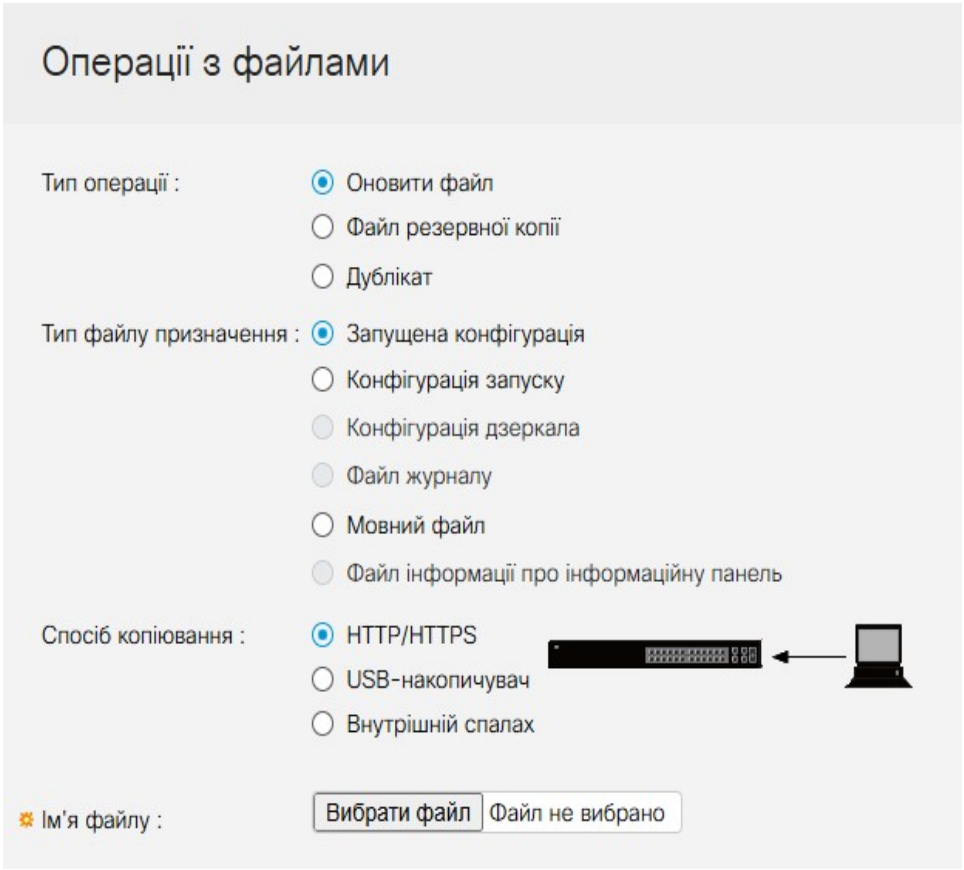


Рисунок 3.12 – Створення резервної копії прошивки

Звертайтеся до офіційної документації Cisco: Для детальної інформації та розширених налаштувань завжди використовуйте повне керівництво користувача для вашої моделі CBS250, доступне на сайті Cisco.

3.2 Інструкція встановлення серверної операційної системи Debian

Завантаження з інсталяційного диска починається з меню, в якому перераховано кілька варіантів встановлення (див. рис. 3.13).

Далі для встановлення серверної ОС Debian 10 виконати такі операції:

1. Вибрати процес встановлення ОС.

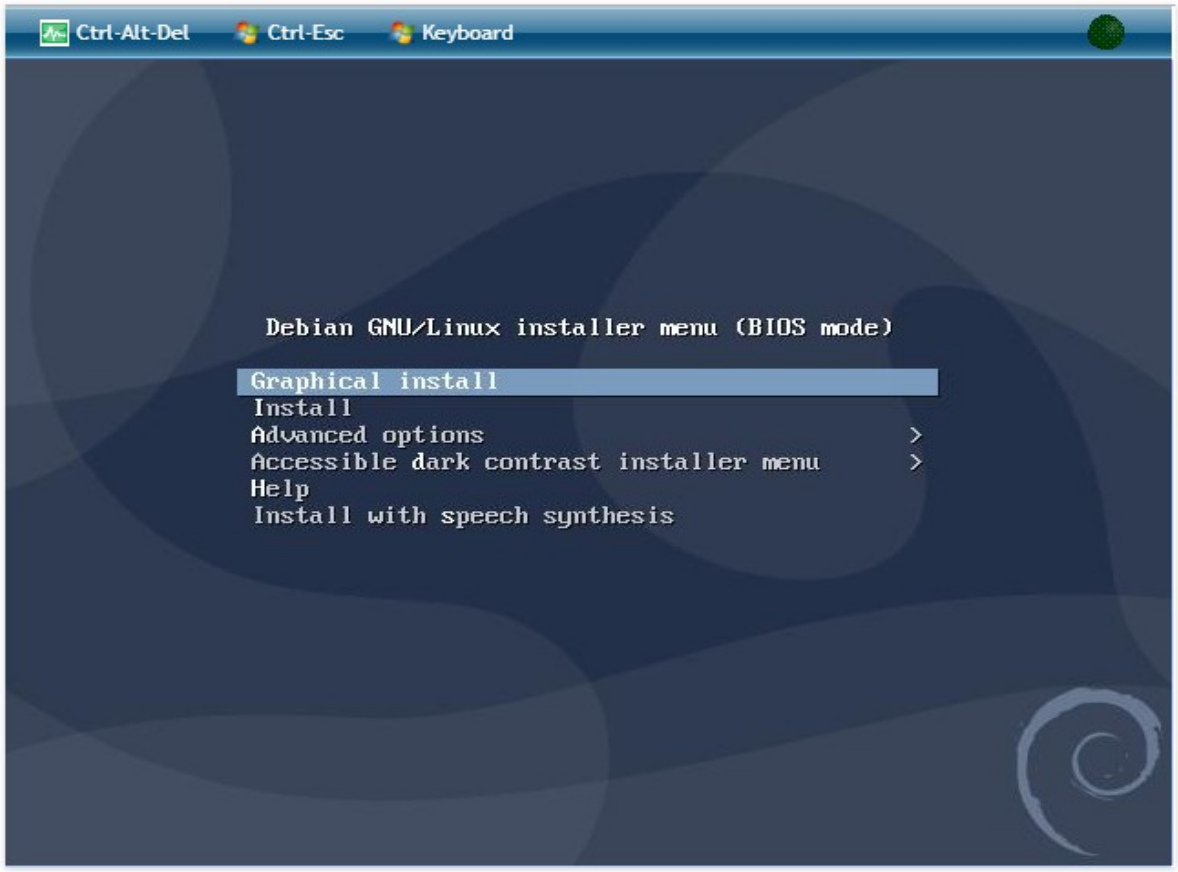


Рисунок 3.13 – Початкове меню інсталятора Debian 10

2. Вибрати мову менеджера інсталяції (див. рис. 3.14).

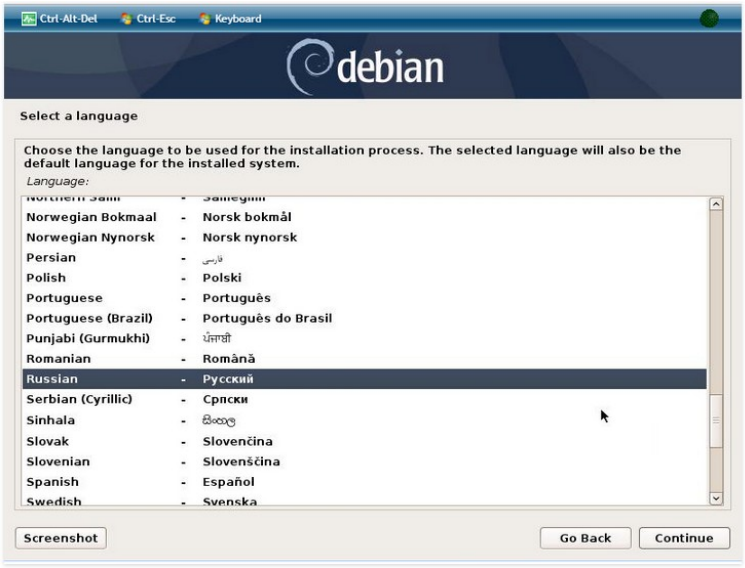


Рисунок 3.14 – Вибір мови менеджера встановлення

3. Вибрати місцезнаходження сервера, від чого залежить часовий пояс і час на сервері (див. рис. 3.15).

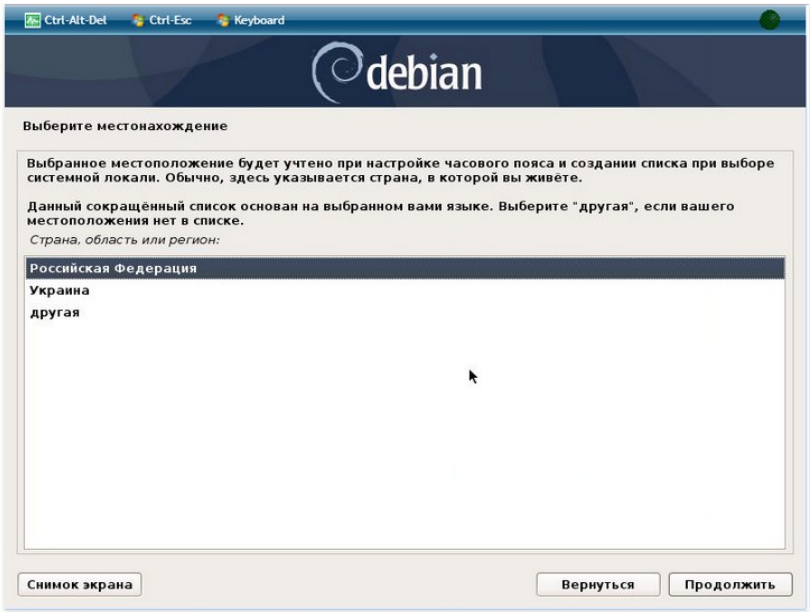


Рисунок 3.15 – Вибір місця знаходження сервера

4. Вибрати розкладку клавіатури (див. рис. 3.16). Краще вибрати «англійську» - буде зручніше використовувати ОС, далі можна буде добавити і українську розкладку, далі називаємо сервер (див. рис. 3.17).

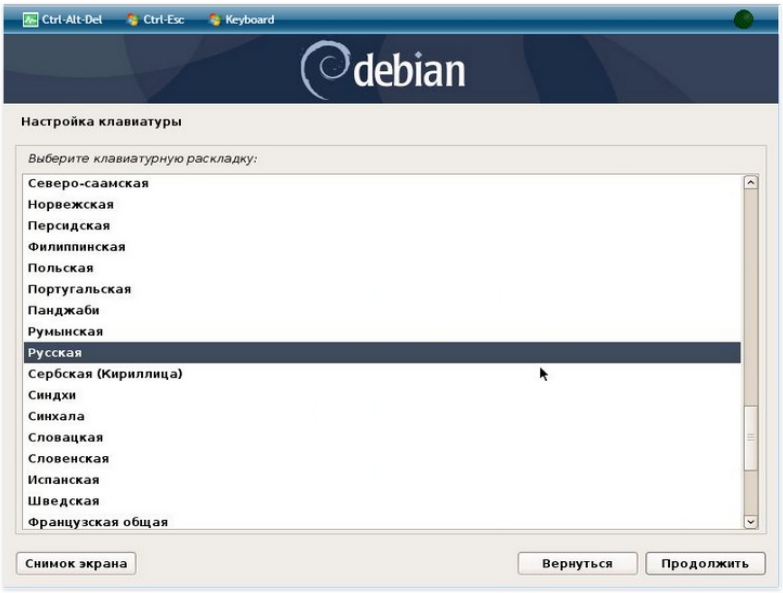


Рисунок 3.16 – Вибір розкладки клавіатури

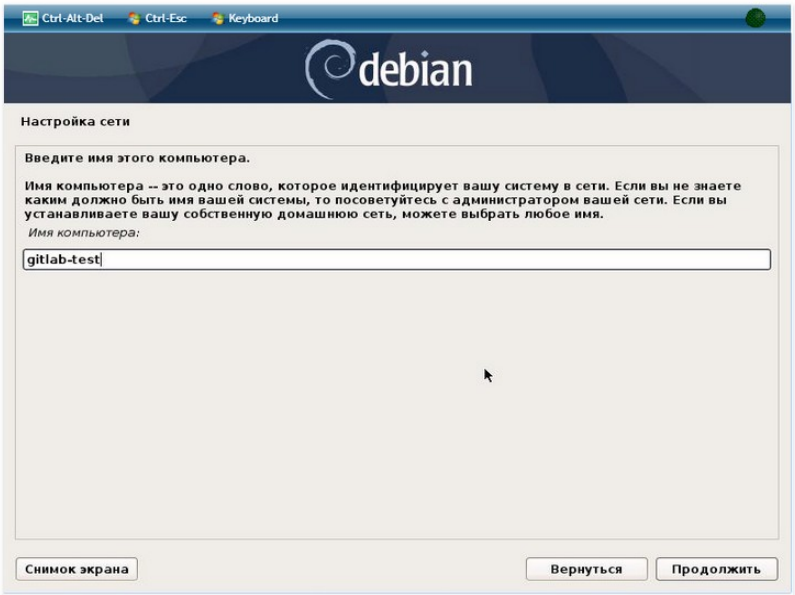


Рисунок 3.17 – Вибір назви сервера Debian

5. Ввести ім’я сервера в мережі (див. Рис. 3.18).

Рисунок 3.18 – Введення назви сервера в мережі

6. Ввести доменне ім’я мережі, якщо таке існує (див. рис. 3.19).

Рисунок 3.19 – Введення доменного імені мережі

7. Задати і підтвердити пароль користувача root (див. Рис. 3.20 — 3.21).

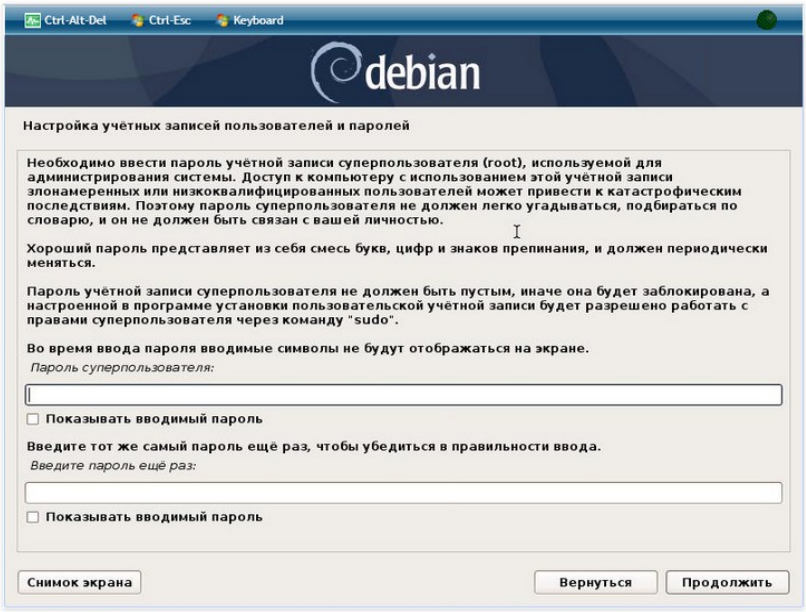


Рисунок 3.20 – Введення паролю суперкористувача root

Рисунок 3.21 – Підтвердження паролю суперкористувача root

8. Ввести повне ім’я користувача, який створюється системою для виконання неадміністративних задач (див. рис. 3.22).

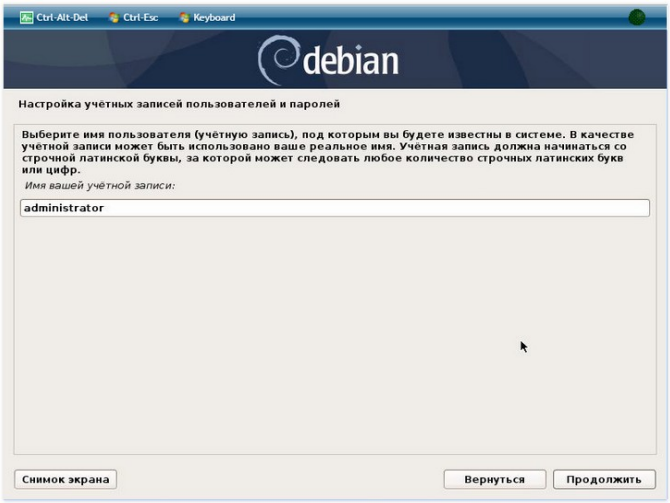


Рисунок 3.22 – Введення повного імені користувача без адміністративних прав

9. Ввести логін і пароль користувача, який створюється системою для виконання неадміністративних задач (див. рис. 3.23-3.24).

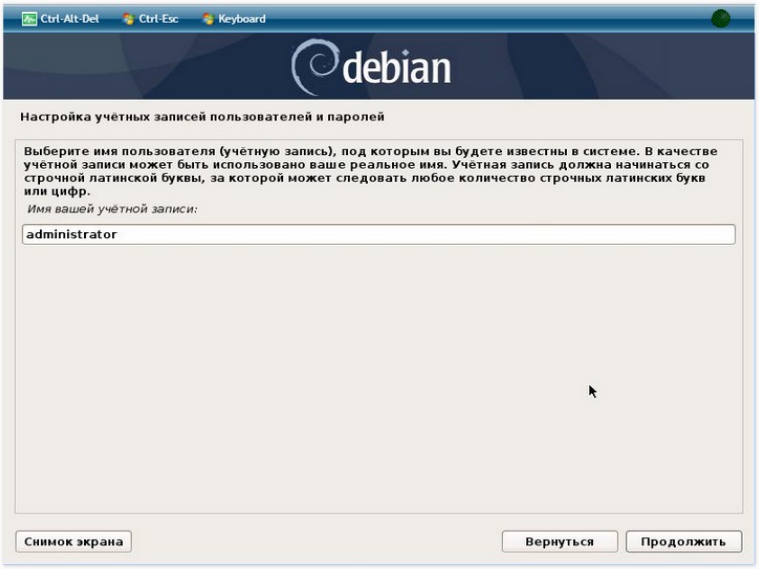


Рисунок 3.23 – Введення логіну користувача без адміністративних прав

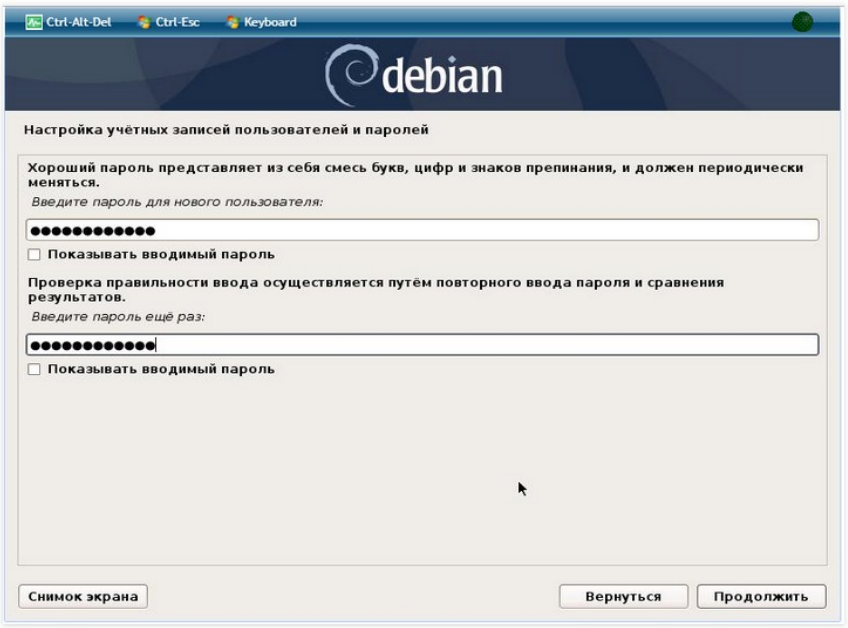


Рисунок 3.24– Введення паролю

10. Вибрати метод розбивки дискового простору (див. рис. 3.25).

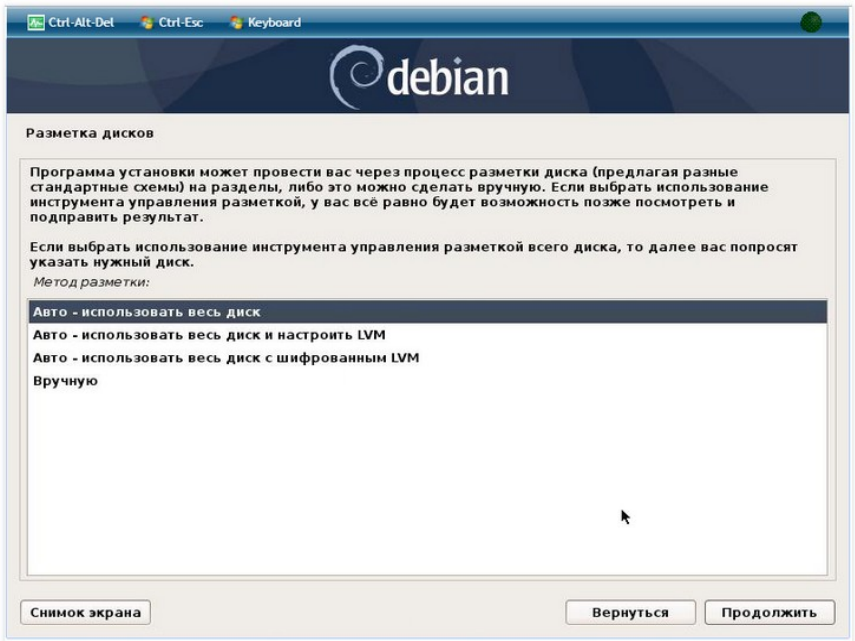


Рисунок 3.25 – Вибір методу використання дискового простору

11. Вибрати цільовий диск для розбивки і використання ОС (див. рис. 3.26).

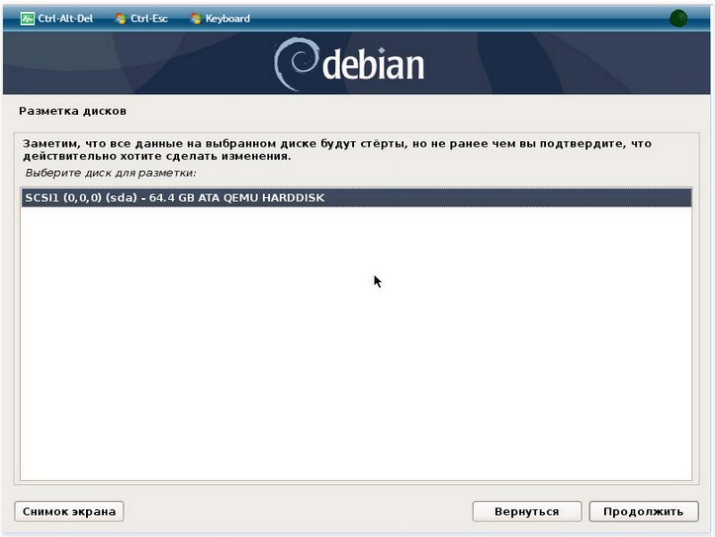


Рисунок 3.26 – Вибір диску для розбиття на розділи

12. Вибрати принцип розбивки дискового простору (див. рис. 3.27).

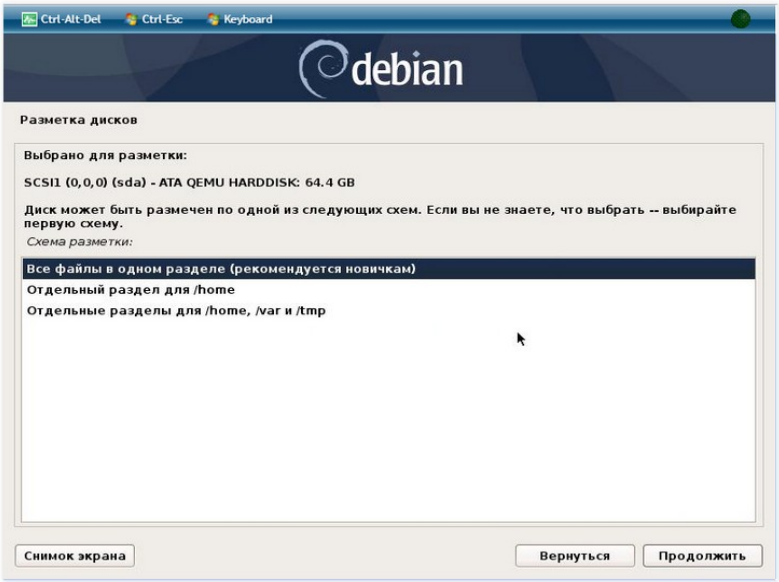


Рисунок 3.27 – Вибір принципу розбиття дискового простору

13. Завершити процес підготовки до розбиття дискового простору (див. рис. 3.28).

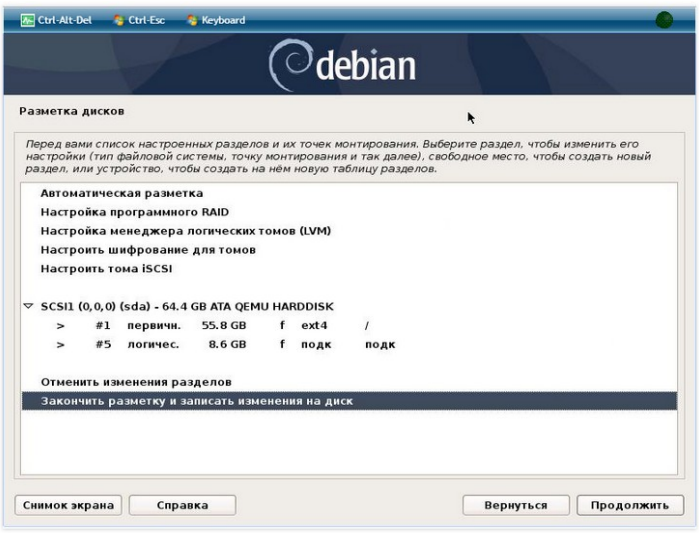


Рисунок 3.28 – Завершення розбиття дискового простору

14. Підтвердити розбиття дискового простору (див. рис. 3.29), після чого зміни будуть внесені на диск і процес встановлення ОС перейде до активної фази – копіювання системних файлів на диск і встановлення базової системи.

Рисунок 3.29 – Підтвердження розбивки дискового простору

15. Вибрати країну, репозиторій якої буде використано для завантаження програмних пакетів (див. рис. 3.30).

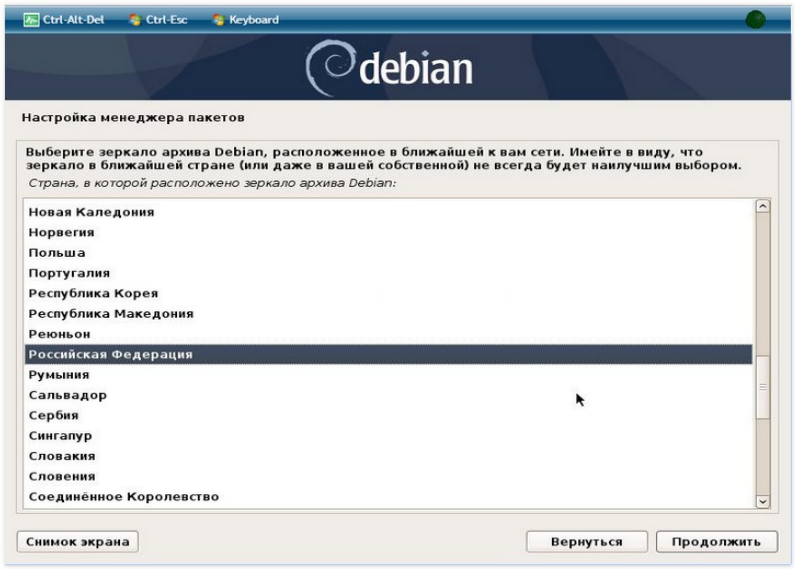


Рисунок 3.30 – Вибір країни, репозиторії якої будуть використовуватись

16. Вибрати репозиторій пакунків (див. рис. 3.31).

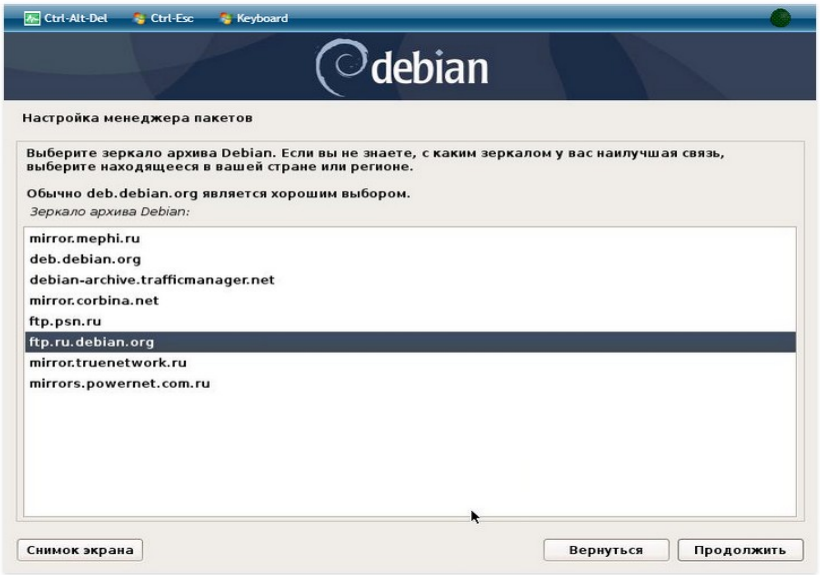


Рисунок 3.31 – Вибір репозиторія пакунків програм

17. Вказати мережеву адресу проксі-сервера, якщо в мережі такий присутній (див. рис. 3.32).

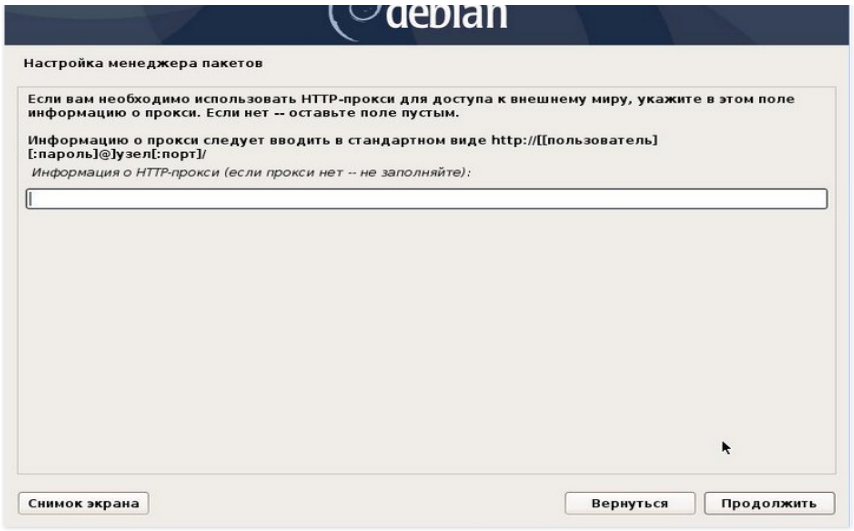


Рисунок 3.32 – Введення адреси проксі-сервера мережі

18. Вибрати додаткове програмне забезпечення відповідно до ролі сервера мережі (див. рис. 3.33).

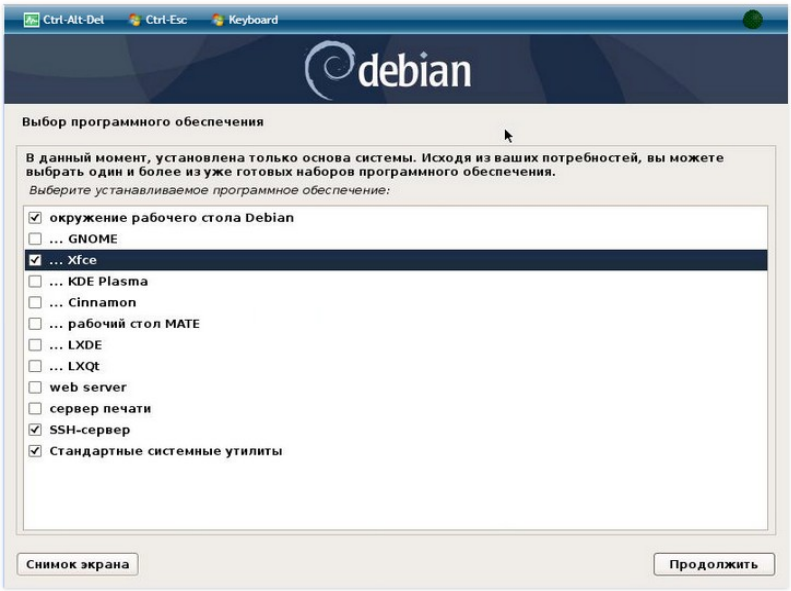


Рисунок 3.33 – Вибір програмного забезпечення сервера

19. Встановити завантажувач ОС GRUB (див. рис. 3.34).

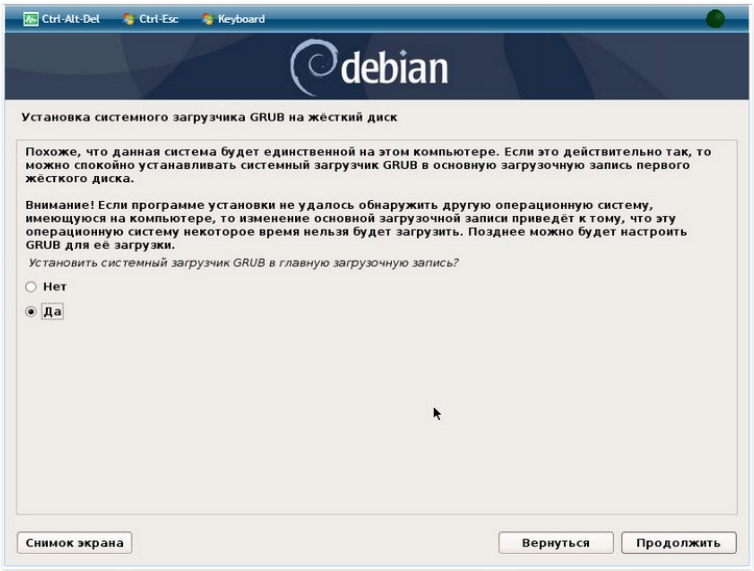


Рисунок 3.34 – Вікно встановлення завантажувача ОС GRUB

20. Завершити інсталяцію натиснувши кнопку Продовжити (див. рис. 3.35).

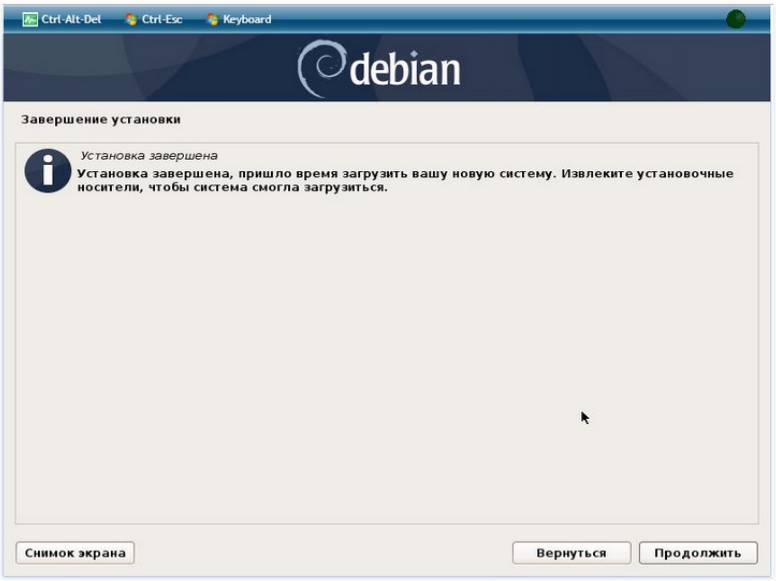


Рисунок 3.35 – Вікно завершення інсталяції

3.3 Налаштування брандмауера

У цьому розділі я детально розповім про основні правила роботи з iptables — потужним інструментом для налаштування фаєрволу в Linux-системах. Важливо розуміти, що налаштування iptables потрібно виконувати дуже обережно, адже помилка може призвести до того, що комп'ютер або сервер стане недоступним через мережу, особливо якщо ви працюєте з хмарними хостингами.

Перш ніж почати, хочу пояснити невелике, але важливе розмежування в термінології. Сам фаєрвол, що працює в ядрі Linux, називається Netfilter. Natfilter — це набір модулів ядра, який керує фільтрацією пакетів. Iptables — це утиліта командного рядка, яка використовується для управління правилами цього фаєрволу. На жаль, часто помилково вважають, що «iptables» — це назва самого фаєрволу, але це не так.

За допомогою Netfilter через iptables можна виконувати такі основні завдання:

– Визначати, який вхідний мережевий трафік можна пропускати або забороняти, налаштовуючи правила для певних портів, протоколів (IPv4, IPv6, TCP, UDP), IP-адрес, MAC-адрес або цілих підмереж.
– Аналогічно, управляти вихідним трафіком, контролюючи, які з'єднання може встановлювати система.

Далі розглянемо основні команди iptables, які допоможуть вам керувати фаєрволом:

– Щоб переглянути всі поточні правила, використовуйте команду:

iptables -L -n

Тут ви побачите «ланцюжки» (chains), які називаються INPUT (для вхідного трафіку), OUTPUT (для вихідного трафіку) і FORWARD (для пакетів, що пересилаються між інтерфейсами).

Якщо потрібно швидко видалити всі наявні правила, скористайтесь командою:

iptables -F

Вона очищує всі правила в усіх ланцюжках.

– Для зміни політики за замовчуванням, наприклад, щоб заборонити весь вхідний трафік або навпаки дозволити, використовуйте:

iptables -P INPUT DROP

або

iptables -P INPUT ACCEPT

Тут `-P` означає «policy» — політику обробки пакетів, якщо жодне правило не спрацювало.

– Для заборони доступу з конкретної IP-адреси чи підмережі виконайте:

iptables -A INPUT -s 123.45.67.89 -j DROP

або

iptables -A INPUT -s 123.45.0.0/16 -j DROP

Ця команда додає (-A — append) правило, яке відкидає (DROP) пакети з вказаних джерел.

Цікаво, що можна використовувати і доменні імена, наприклад:

iptables -A INPUT -s example.ru -j DROP

Однак для роботи з доменами потрібно переконатися, що у вашій системі правильно налаштований DNS.

Заборонити вихідні з’єднання на певну IP-адресу можна командою:

iptables -A OUTPUT -d 123.45.67.89 -j DROP

У правилах можна застосовувати заперечення, наприклад, заборонити всі IP-адреси, крім однієї:

iptables -A INPUT ! -s 123.45.67.89 -j DROP

Для видалення певного правила за номером у ланцюжку виконайте:

iptables -D INPUT 1

Тут 1 — це порядковий номер правила, який можна дізнатися з виводу iptables -L -n --line-numbers.

Або видалити конкретне правило за умовою, наприклад:

iptables -D INPUT -s 123.45.67.89 -j DROP

Крім того, у правилах можна вказувати протоколи через опцію `-p`. Підтримуються всі протоколи, такі як ICMP, TCP, UDP, або їх числові ідентифікатори. Порти можна вказати через `--sport` (порт відправника) або `--dport` (порт призначення). Наприклад:

iptables -A INPUT -p tcp --sport 80 -j ACCEPT

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Іноді важливо вставити правило не в кінець, а на початок ланцюжка. Для цього використовується команда з опцією -I, наприклад:

iptables -I INPUT 3 ...

Це вставить правило на позицію номер 3.

Щоб зберегти налаштування фаєрволу в файл і не втратити їх після перезавантаження системи, виконайте:

iptables-save > /etc/iptables.rules

А для відновлення правил:

iptables-restore < /etc/iptables.rules

І наостанок — важливий крок, щоб при кожному завантаженні системи ваші правила застосовувалися автоматично. Для цього створіть скрипт /etc/network/if-pre-up.d/iptables з таким вмістом:

```
#!/bin/sh
iptables-restore < /etc/iptables.rules
exit 0
```

Не забудьте зробити його виконуваним:

```
chmod +x /etc/network/if-pre-up.d/iptables
```

3.4 Інструкція з налаштування проксі-сервера Squid

Механізми управління доступом в Squid дозволяють гнучко реалізовувати політику доступу до інтернет-ресурсів, грунтуючись на тимчасових інтервалах, інформації про кешування, доступу до певних сайтів і т.д. Управління доступом в Squid грунтується на двох різних компонентах: ACL-елементах і списках доступу (access list). Список доступу фактично дозволяє або забороняє доступ до сервісу.

Деякі найважливіші типи ACL-елементів перераховані нижче

src: Джерело, тобто IP-адреса клієнта;

dst: Приймач, тобто IP-адреса серверу;

srcdomain: Джерело, тобто доменне ім'я клієнта;

dstdomain: Приймач, тобто доменне ім'я серверу;

time: Час дня і день тижня;

url_regex: Регулярний вираз для перевірки відповідності URL;

urlpath_regex: Регулярний вираз для перевірки відповідності URL-шляху разом з назвою протоколу і ім'ям хоста;

proxy auth: Перевірка автентичності користувача за допомогою зовнішнього процесу;

maxconn: Максимальна кількість з'єднань на одну клієнтську IP-адресу.

Щоб застосувати, треба визначити набір ACL і застосувати до них правила. Формат ACL-виразів:

aci acl_element_name type_of_acl_element values_to_acl

Зауваження:

acl_element_name може бути любим ім'ям, призначеним користувачем ACL елементу.

Два ACL не можуть мати одинакових імені;

Будь-який ACL складається із списку значень. При перевірці на відповідність декільком значенням використовується АБО-логика. Іншими словами, ACL елемент відповідає, коли знайдена відповідність хоча б для одного із значень.

Не всі ACL елементи можуть використовуватися із списками доступу всіх типів.

Різні ACL елементи, розташовані на різних рядках, групуються squid'ом в єдиний список;

Доступні декілька різних типів списків доступу. Ті які ми збираємося використовувати приведені нижче:

http access: Дозволяє HTTP-клієнтам здійснювати доступ на HTTP-порт. Це основний список управління доступом.

no_cache: Визначає кешування відповідей на запити.

Зауваження:

Правила перевіряються в тому порядку, в якому вони записані; перевірка уривається, як тільки знайдена відповідність одному з правил;

Список доступу може складатися з декількох правил;

Якщо не була знайдена відповідність жодному з правил, то виконується дія за умовчанням, протилежне останньому правилу в списку. Дію за умовчанням краще указувати явно;

Над всіма елементами в списку доступу виконується операція І (AND), а декілька виразів http_acess об'єднуються операцією АБО (OR);

http_access Action statement 1 AND statement2 AND statement OR http_access Action statement3;

Правила завжди читаються від низу до верху.

Управління доступом до Інтернет

Різноманітні механізми і правила управління доступом пропонують дуже хороший і гнучкий шлях контролю клієнтського доступу до Інтернет. Приклади настройок, що часто використовуються, приведені нижче; у жодному випадку не можна обмежуватися тільки цими настройками.

1. Дозволити доступ до Інтернет вибраним машинам

aci allowed_clients src 192.168.0.10 192.168.0.20 192.168.0.30

http_access allow allowed_clients

http_access deny !allowed clients

Тут дозволений доступ до Інтернет машинам з IP-адресами 192.168.0.10, 192.168.0.20 і 192.168.0.30, а всім іншим (в списку їх немає) - заборонений.

Обмежити доступ певним часом:

aci allowed_clients src 192.168.0.1/255.255.255.0

aci regular_days time MTWHF 10:00-16:00

http_access allow allowed_clients regular_days

http_access deny allowed_clients

Тут доступ надається всім машинам мережі 192.168.0.1 протягом часу з понеділка по п'ятницю з 10:00 ранку до 4:00 дня.

Доступ в різний час для різних клієнтів

aci host1 src 192.168.0.10

aci host2 src 192.168.0.20

aci host3 src 192.168.0.30

acl morning time 10:00-13:00

acl lunch time 13:30-14:30

acl evening time 15:00-18:00

http_access allow host1 morning

http_access allow host1 evening

http_access allow host2 lunch

http_access allow host3 evening

http_access deny all

Вищенаведені правила дозволяють доступ комп'ютеру hostl ранком (з 10:00 до 13:00) і увечері (з 15:00 до 18:00), а комп'ютерам host2 і host3 після обіду (з 13:30 до 14:30) і увечері відповідно (з 15:00 до 18:00).

Всі елементи запису доступу об'єднуються операцією І (AND) і виконуються таким чином:

http_access Action statement1 AND statement2 AND statement OR.

Множинні оголошення http_access об’єднуються операцією АБО (OR), а елементи доступу в них об'єднуються операцією І. У зв'язку з цим рядок http_access allow host1 morning evening ніколи не спрацює, оскільки виразів morning AND evening ніколи не буде істинним (ранок і вечір ніколи не перетинаються), і, отже, ніяких дій не буде.

Блокування сайтів

Squid може запобігти доступу до певних сайтів або сайтів, адреса яких містить певне слово. Це може бути реалізовано таким чином:

aci allowed_clients src 192.168.0.1/255.255.255.0

aci banned_sites url_regex abc.com *()(*.com

http_access deny banned_sites

http_access allow allowed_clients

Аналогічним чином можна заборонити доступ до сайтів, адреса яких містить визначене слів, наприклад dummy і fake

aci allowed_clients src 192.168.0.1/255.255.255.0

aci banned_sites url_regex dummy fake

http_access deny banned_sites

http_access allow allowed_machines

acl allowed_clients src 192.168.0.1/255.255.255.0

acl banned_sites url_regex "/etc/banned.list"

http_access deny banned_sites

http_access allow allowed_clients

Оптимізація

Squid може обмежувати максимальну кількість з'єднань за допомогою елемента maxconn. Для використовування цієї можливості, повинна бути включена підтримка client db.

acl mynetwork 192.168.0.1/255.255.255.0

acl numconn maxconn 5

http_access deny mynetwork numconn

Зауваження: ACL maxconn використовує порівняння "менше-чим". ACL спрацьовує, якщо кількість з'єднань більше заданого значення. Тому maxconn і не указується в списку http_access.

Кешування

Відповіді на запити кешуються і це добре для статичних сторінок. Немає ніякої потреби кешувати cgi-сторінки або сервлети. Цьому можна запобігти використовуванням ACL-елемента no_cache.

acl cache_preventl url_regex cgi-bin /?

acl cache_prevent2 url_regex Servlet

no_cache_deny cache_preventl

no_cache_deny cache_prevent2

Створення власних повідомлень про помилки

Можна створити свої власні повідомлення про помилки доступу за допомогою опції deny_info. Всі повідомлення про помилки Squid за умовчанням зберігаються в каталозі /etc/squid/errors. Каталог з файлами повідомлень про помилки може бути змінений за допомогою error_directory. Можна навіть змінити самі повідомлення.

acl allowed_clients src 192.168.0.1/255.255.255.0

acl banned_sites url_regex abc.com *()(*.com

http_access deny banned_sites

deny_info ERRBANNEDSITE banned_sites

http_access allow allowed_clients

У вищенаведеному прикладі спеціальне повідомлення відображається як тільки користувач намагається дістати доступ до сайту, що містить в назві заборонене слово. Файл з ім'ям ERRBANNEDSITE повинен знаходиться у вище-

наведеному каталозі помилок. Повідомлення про помилку повинне бути в HTML-форматі.

Всі розглянуті приклади, демонструють лише невелику частину реальних можливостей ACL. Пояснення призначення ACL-елементів і елементів доступу, необхідне для більш серйозного їх використовування можна знайти в FAQ на домашній сторінці Squid.

3.5 Налаштування точки доступу

TP-Link Omada EAP610 — це високопродуктивна дводіапазонна точка доступу стандарту Wi-Fi 6, яка ідеально підходить для сучасних офісів, готелів, магазинів та інших комерційних приміщень. Вона є частиною екосистеми TP-Link Omada SDN (Software Defined Networking), що дозволяє централізовано керувати великою кількістю пристроїв.

1. Перед початком: Що вам знадобиться

TP-Link Omada EAP610: Сама точка доступу.

Кабель Ethernet: Для підключення до мережі та живлення (PoE).

PoE-інжектор або PoE-комутатор: EAP610 підтримує стандарти 802.3at (PoE+) та 802.3af (PoE) для живлення через Ethernet-кабель. Переконайтеся, що ваш PoE-інжектор або порт комутатора надає достатню потужність.

Комп'ютер: Для початкового налаштування або запуску програмного контролера Omada.

Omada SDN Controller (для централізованого управління):

Апаратний контролер: TP-Link Omada OC200 або OC300 (рекомендовано для простоти та надійності).

Програмний контролер: Програмне забезпечення, що встановлюється на ПК (Windows, Linux, Mac) або віртуальну машину.

Хмарний контролер: Якщо ви використовуєте хмарний сервіс Omada.

2. Метод 1: Автономний режим (Standalone Mode) через веб-інтерфейс

Цей метод підходить, якщо у вас лише одна точка доступу EAP610 і вам не потрібні функції централізованого управління (наприклад, безшовний роумінг, гостьові портали, моніторинг кількох AP).

Фізичне підключення:

Підключіть кабель Ethernet від PoE-інжектора/комутатора до порту Ethernet на EAP610.

Підключіть інший кінець кабелю Ethernet від PoE-інжектора/комутатора до вашої локальної мережі (до маршрутизатора або комутатора).

Зачекайте, поки EAP610 завантажиться (індикатор Status має світитися зеленим).

Знаходження IP-адреси EAP610:

За замовчуванням EAP610 отримує IP-адресу через DHCP. Перевірте список підключених пристроїв на вашому маршрутизаторі, щоб знайти IP-адресу EAP610.

Якщо DHCP не працює, EAP610 може використовувати резервну IP-адресу за замовчуванням: 192.168.0.254. Переконайтеся, що ваш комп'ютер знаходиться в тій же підмережі (наприклад, 192.168.0.10).

Доступ до веб-інтерфейсу:

Відкрийте веб-браузер і введіть IP-адресу EAP610 (наприклад, http://192.168.0.254).

Введіть облікові дані за замовчуванням:

Ім'я користувача (Username): admin

Пароль (Password): admin

Негайно змініть пароль за замовчуванням на більш надійний, коли з'явиться відповідний запит.

Базові налаштування Wi-Fi:

Перейдіть до розділу Wireless Settings або Wireless (назва може відрізнятися в залежності від прошивки) (див.рис. 3.36).

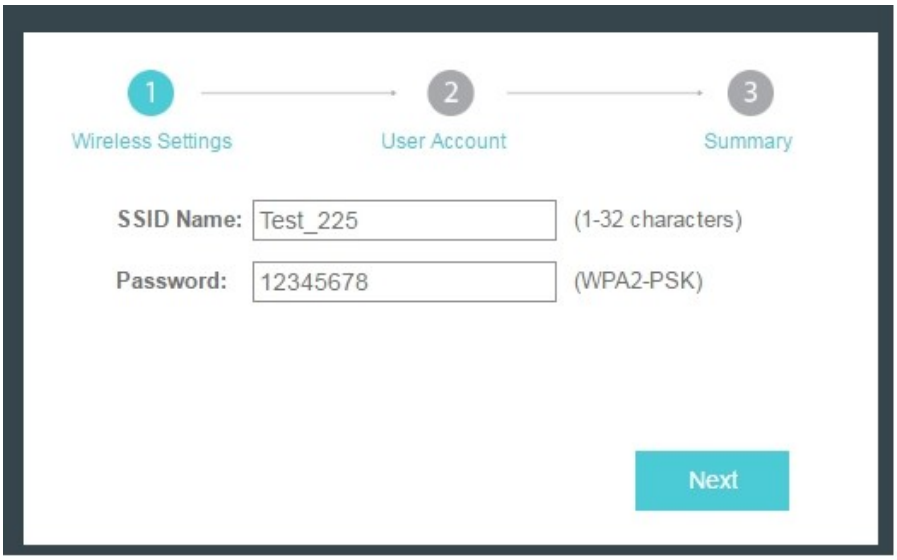


Рисунок 3.36 - Створення мережі через контролер

Створіть SSID (ім'я Wi-Fi мережі):

Введіть бажане ім'я мережі (наприклад, "MyOfficeWi-Fi").

Виберіть Security (наприклад, WPA2-PSK або WPA2/WPA3-PSK).

Введіть Password (ключ доступу до Wi-Fi).

Увімкніть мережу для діапазонів 2.4 ГГц та 5 ГГц.

Налаштуйте параметри радіо (Radio Settings): Зазвичай краще залишити канал (Channel) та потужність (Power) в режимі "Auto" для початку, але для оптимізації можна вручну вибрати найменш завантажені канали.

Натисніть Save або Apply.

Збереження конфігурації: Переконайтеся, що ви зберегли всі зміни, щоб вони залишалися після перезавантаження.

Обмеження автономного режиму: EAP610 у цьому режимі працює як звичайна точка доступу. Ви не отримаєте переваг централізованого управління, роумінгу між кількома AP, розширених гостьових функцій тощо. Для повного використання можливостей Omada EAP610 рекомендується Метод 2.

3. Метод 2: Централізоване управління через Omada SDN Controller (Рекомендовано)

Це найбільш ефективний спосіб управління EAP610, особливо якщо у вас кілька точок доступу Omada або ви плануєте розширювати мережу.

3.1. Налаштування Omada SDN Controller (коротко)

Якщо у вас ще немає контролера Omada, його потрібно налаштувати:

Апаратний контролер (OC200/OC300): Підключіть його до мережі, увімкніть живлення. Зайдіть до його веб-інтерфейсу за замовчуванням (знайдіть IP через DHCP) і виконайте початкове налаштування майстром.

Програмний контролер: Завантажте та встановіть програмне забезпечення Omada SDN Controller з веб-сайту TP-Link на ваш комп'ютер/сервер. Запустіть його та виконайте початкове налаштування.

Хмарний контролер: Увійдіть до свого облікового запису TP-Link Cloud та створіть нове середовище Omada.

Після налаштування контролера, переконайтеся, що він запущений та доступний у вашій мережі.

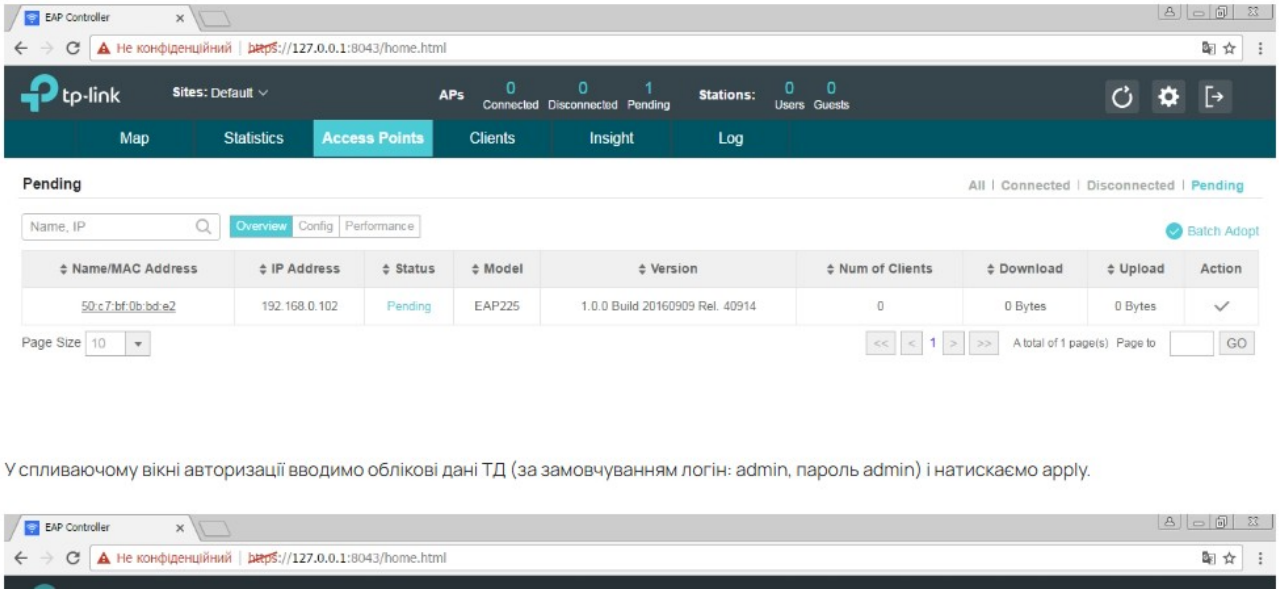
3.2. Прийняття (Adoption) EAP610 контролером

Скидання EAP610 до заводських налаштувань (якщо потрібно): Якщо EAP610 раніше працювала в автономному режимі або була підключена до іншо-

го контролера, скиньте її, утримуючи кнопку Reset (зазвичай на задній панелі) протягом 5-10 секунд, доки індикатор Status не почне блимати.

Підключення EAP610 до мережі: Підключіть EAP610 до тієї ж локальної мережі (або до мережі, яка може маршрутизуватись до контролера), де знаходиться ваш Omada SDN Controller.

Запуск контролера: Відкрийте веб-інтерфейс вашого Omada SDN Controller(див.рис. 3.37).



У спливаючому вікні авторизації вводимо облікові дані ТД (за замовчуванням логін: admin, пароль admin) і натискаємо apply.

Рисунок 3.37 - Підключена точка доступу у WEB інтерфейсі

Знаходження та прийняття AP:

У контролері перейдіть до розділу Devices (Пристрої).

Ваша EAP610 повинна з'явитися у списку зі статусом Pending (Очікує прийняття).

Натисніть кнопку Adopt (Прийняти) навпроти EAP610.

Контролер автоматично завантажить необхідну прошивку на EAP610 (якщо потрібно) та налаштує її. Цей процес може зайняти кілька хвилин, і AP кілька разів перезавантажиться.

Після успішного прийняття статус EAP610 зміниться на Connected (Підключено)(див.рис. 3.38).

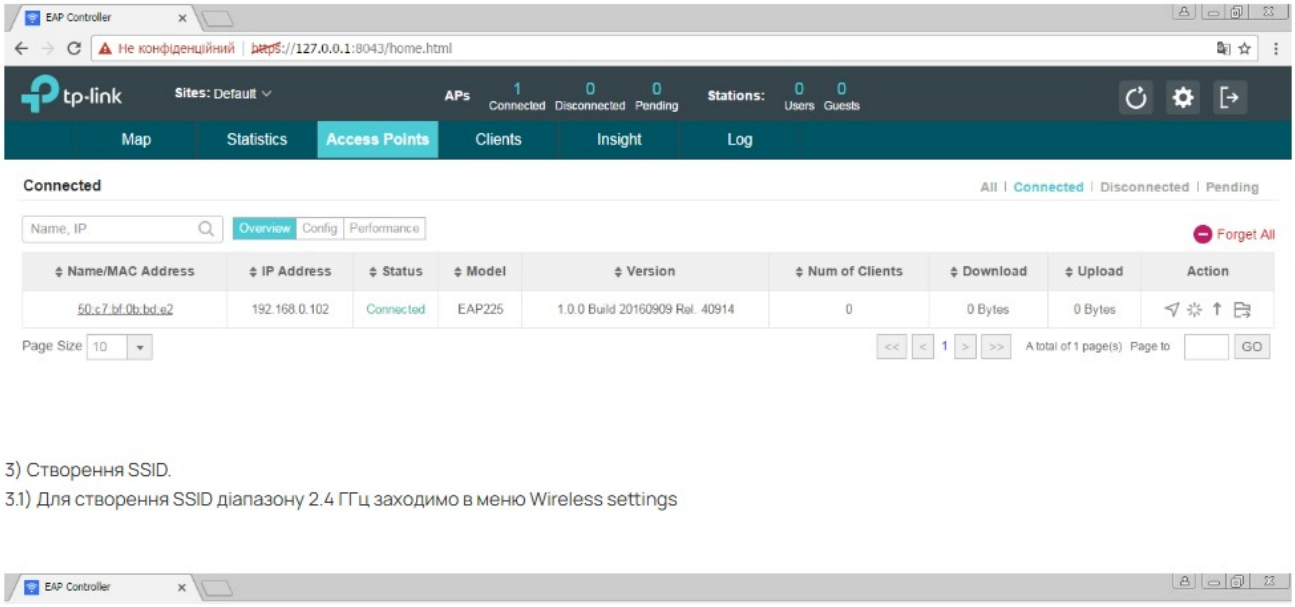


Рисунок 3.38 - Індикація підключеної точки доступу

3.3. Налаштування бездротової мережі через Omada SDN Controller

Після прийняття EAP610, усі налаштування Wi-Fi та мережі виконуються централізовано через контролер.

Створення Wi-Fi мереж (SSID) (див.рис. 3.39):

У контролері перейдіть до Settings (Налаштування) > Wireless Networks (Бездротові мережі).

Натисніть Create New Wireless Network (Створити нову бездротову мережу).

Введіть Name/SSID (назву мережі), виберіть Security Type (наприклад, WPA2-PSK або WPA2/WPA3 Personal), введіть Password.

Виберіть Enabled для діапазонів 2.4 GHz та 5 GHz.

VLAN ID (за потреби): Якщо ви використовуєте VLAN, вкажіть відповідний VLAN ID для цієї мережі.

Натисніть Apply або Save.

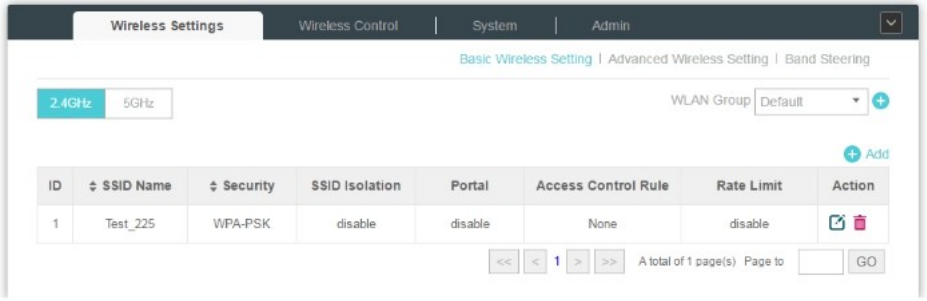


Рисунок 3.39 - Створення радіодіапазону

Примітка: Ви можете створити кілька SSID для різних цілей (наприклад, основна мережа, гостьова мережа).

Налаштування гостьової мережі (Guest Network) (див.рис. 3.40):

Якщо вам потрібен гостьовий портал з авторизацією, перейдіть до Settings > Guest Network.

Увімкніть Guest Network, налаштуйте Authentication (наприклад, Simple Password, Voucher, Hotspot).

Налаштуйте Splash Page (сторінку авторизації) за вашим бажанням.

Оптимізація радіопараметрів (Radio Settings):

Перейдіть до Settings > RF Management.

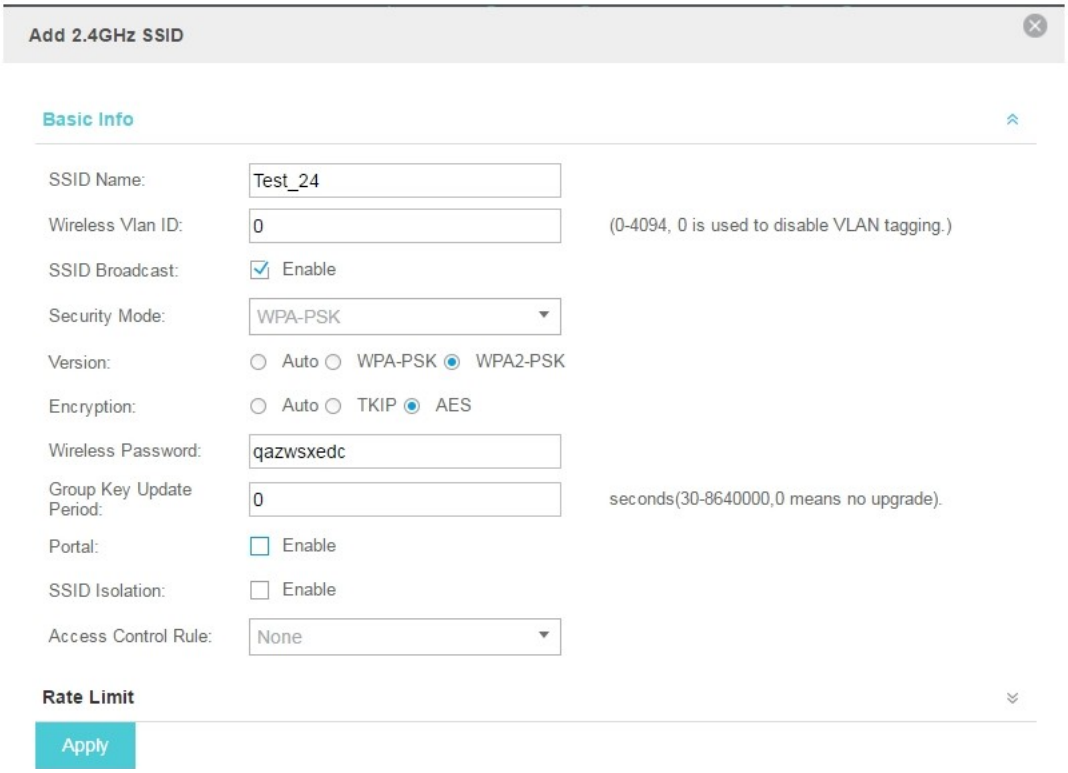


Рисунок 3.40 - Вікно вказування параметрів безпровідної мережі

Тут ви можете оптимізувати канали Wi-Fi та потужність передачі для кожної точки доступу, щоб мінімізувати перешкоди та забезпечити найкраще покриття. Зазвичай, контролер автоматично оптимізує це, але досвідчені користувачі можуть налаштувати вручну.

Для 2.4 ГГц використовуйте канали 1, 6, 11 (не перекриваються). Для 5 ГГц доступно більше каналів.

Встановіть потужність передачі на "Medium" або "Low" для щільних розгортань, щоб покращити роумінг.

Інші функції (у контролері):

Fast Roaming (802.11r/k/v): Налаштуйте для безшовного переміщення клієнтів між AP.

Band Steering: Автоматично перенаправляє клієнтів на діапазон 5 ГГц, якщо він підтримується, для кращої продуктивності.

Mesh (бездротовий Uplink): Якщо вам потрібно підключити деякі AP бездротовим способом, налаштуйте Mesh у контролері.

Моніторинг: Контролер надає детальну статистику по трафіку, клієнтах, стану AP та іншім параметрам мережі.

Оновлення прошивки AP: Завжди оновлюйте прошивку через контролер, він автоматично керує цим процесом.

4. Важливі поради та найкращі практики

Завжди використовуйте контролер для Omada AP: Це розкриває весь потенціал системи Omada SDN, дозволяючи централізовано управляти всіма вашими пристроями.

Регулярно оновлюйте прошивку: Як контролера, так і точок доступу, щоб отримувати нові функції, виправлення помилок та покращення безпеки.

Плануйте розташування AP: Для оптимального покриття розташуйте точки доступу так, щоб забезпечити перекриття сигналів та мінімізувати "мертві зони".

Використовуйте надійні паролі: Для Wi-Fi мереж та доступу до контролера.

3.6 FreeNAS встановлення та налаштування

FreeNAS — високофункціональна операційна система для організації мережевого зберігання даних

FreeNAS є повноцінною операційною системою, спеціально розробленою для побудови рішень типу NAS (Network Attached Storage) — мережевих сховищ даних, які забезпечують централізований доступ до файлів у локальній або глобальній мережі. В основі FreeNAS лежить стабільна і потужна UNIX-подібна

система FreeBSD, яка гарантує надійність, гнучкість та високу продуктивність. Операційна система підтримує численні протоколи обміну даними, зокрема CIFS/SMB (сумісні з Windows), NFS (переважно використовується в Unix/Linux), iSCSI (мережевий інтерфейс блочного рівня), FTP, RSYNC та масиви RAID, що забезпечує сумісність з широким спектром клієнтських пристроїв і сценаріїв використання.

FreeNAS має відкритий вихідний код, що дозволяє користувачам гнучко налаштовувати систему під власні потреби, а також отримувати оновлення й доповнення від великої спільноти розробників. Крім того, система надає веб-орієнтований інтерфейс керування, який дозволяє адміністратору виконувати всі основні дії без потреби в знанні командного рядка. Це робить FreeNAS одним із найзручніших і водночас потужних рішень для створення NAS-серверів як у домашньому середовищі, так і в малому або середньому бізнесі.

Основні характеристики FreeNAS

1. Реплікація та резервне копіювання на основі ZFS

Однією з ключових особливостей FreeNAS є підтримка сучасної файлової системи ZFS (Zettabyte File System), яка забезпечує високу ступінь захисту даних, масштабованість і ефективне управління дисковим простором. Зокрема, у ZFS реалізовано механізм знімків (snapshots), які дозволяють фіксувати стан файлової системи на певний момент часу. Ці знімки можуть використовуватися для організації віддаленого резервного копіювання, включно з інкрементальним копіюванням — тобто передаванням лише змінених даних, що значно зменшує навантаження на мережу та економить місце.

У разі втрати даних або пошкодження локального носія, адміністратор може відновити дані за допомогою одного з раніше створених знімків, передавши його на іншу файлову систему ZFS. Такий підхід робить систему надзвичайно стійкою до збоїв і сприяє безперебійному збереженню критично важливої інформації.

2. Забезпечення цілісності даних та RAID-Z

FreeNAS підтримує вдосконалену реалізацію RAID — так звану RAID-Z, яка є частиною файлової системи ZFS. На відміну від класичних масивів, RAID-Z забезпечує автоматичне виявлення та виправлення помилок шляхом використання контрольних сум. Усі операції запису та зчитування даних супроводжуються перевіркою їхньої цілісності, що дозволяє уникнути «тихих» пошкоджень (silent data corruption), які можуть залишитися непоміченими в інших файлових системах. Такий підхід гарантує, що кожен файл, незалежно від його розміру або структури, зберігається без спотворень і з максимально можливою точністю.

3. Розширене шифрування даних

Система FreeNAS реалізує вбудовану підтримку апаратного й програмного шифрування даних на рівні томів файлової системи ZFS. Це дозволяє створювати повністю зашифровані розділи, доступ до яких може бути отриманий лише за наявності майстер-ключа, що генерується при створенні тому. Для додаткового рівня безпеки також можна використовувати парольну фразу, яка значно ускладнює несанкціонований доступ до інформації, навіть у разі фізичного доступу до диска. Така система шифрування особливо корисна для зберігання конфіденційних документів або критичних бізнес-даних.

Можливості обміну файлами в мережі

FreeNAS надає користувачеві широкі можливості щодо організації спільного доступу до файлів у гетерогенному середовищі, що складається з різних операційних систем. Серед підтримуваних протоколів:

- SMB/CIFS — для Windows-систем;
- NFS — для Unix/Linux;
- AFP — для Apple/macOS;
- FTP та iSCSI — для специфічних сценаріїв збереження і передачі даних.

Крім того, FreeNAS підтримує сучасні технології віртуалізації та інтеграції, зокрема VMware VAAI, Microsoft ODX, а також кластеризацію на базі Windows Server 2008/2012 R2, що дозволяє ефективно інтегрувати NAS у складні корпоративні IT-інфраструктури.

Адміністрування через веб-інтерфейс

Користувацький веб-інтерфейс FreeNAS є інтуїтивно зрозумілим і водночас функціонально насиченим. Через нього адміністратор може виконувати всі ключові операції: створення томів, налаштування файлових дозволів, керування користувачами, моніторинг стану системи, встановлення оновлень та керування мережею. Для досвідчених користувачів також доступний доступ через SSH, який дає змогу виконувати команди безпосередньо з термінала. Завдяки цьому FreeNAS підходить як для новачків, так і для професіоналів.

Система плагінів: розширення можливостей

FreeNAS підтримує численні плагіни, що дозволяють інтегрувати сторонні програми та сервіси для розширення функціональності. Завдяки цій модульності користувач може налаштувати NAS-сервер як мультимедійний центр, систему резервного копіювання, приватну хмару тощо. Серед найпопулярніших плагінів:

- Bacula — система резервного копіювання з мережею підтримки клієнтів;
- CouchPotato — автоматичне завантаження торрент-файлів;
- CrashPlan — резервне копіювання даних у хмару або на інші пристрої;
- OwnCloud — створення приватного хмарного сховища для синхронізації та спільного доступу до файлів.

Системні вимоги до встановлення FreeNAS

Щоб забезпечити стабільну й ефективну роботу FreeNAS, необхідно мати наступну конфігурацію апаратного забезпечення:

- Процесор із підтримкою 64-бітної архітектури (x64);

– Мінімум 4 ГБ оперативної пам’яті (рекомендується більше для активного використання ZFS);
– Накопичувач обсягом щонайменше 1 ТБ для основного сховища даних.

Покрокове встановлення FreeNAS

Інсталяція FreeNAS є відносно простою. Для цього необхідно:

1. Завантажити актуальний ISO-образ операційної системи з офіційного сайту розробника.

2. Записати образ на DVD-диск або створити завантажувальний USB-накопичувач за допомогою відповідного інструмента (наприклад, Rufus).

3. Увімкнути сервер або комп’ютер і завантажитися з підготовленого носія.

4. У меню встановлення обрати перший пункт (пункт «1») та натиснути клавішу Enter для запуску процесу інсталяції.

Початок інсталяції FreeNAS

Після запуску завантажувального середовища FreeNAS із USB-носія або DVD-диска, система автоматично перейде до початкового меню встановлення. Наступним кроком користувач повинен обрати фізичний пристрій, на який буде інстальовано операційну систему. Це має бути окремий накопичувач (рекомендується SSD або USB-накопичувач мінімум на 8 ГБ). Після вибору необхідного пристрою підтверджуємо дію натисканням кнопки OK.

Підтвердження встановлення

Далі система покаже повідомлення-попередження про те, що всі дані на обраному диску буде знищено. Для підтвердження наміру інсталювати FreeNAS потрібно вибрати Yes. Це критичний крок, який розпочне безпосереднє копіювання системних файлів і розгортання середовища FreeNAS.

Встановлення пароля адміністратора

У наступному вікні інсталятора необхідно кілька разів ввести пароль адміністратора системи (користувача root). Це обліковий запис із повними правами доступу до налаштувань і керування NAS-сервером. Після введення пароля підтверджуємо дію, натиснувши OK.

Завершення інсталяції та перезавантаження

Після завершення встановлення система повідомить про успішне завершення процесу та запропонує перезавантаження. Натисніть OK, після чого обов’язково вийміть завантажувальний USB-носій або DVD-диск, щоб уникнути повторного запуску інсталятора при наступному завантаженні.

Початкове завантаження FreeNAS

Після перезавантаження на екрані з’явиться меню вибору режиму запуску. Виберіть пункт Normal Bootup — стандартне завантаження FreeNAS. Після завершення ініціалізації системи відобразиться службове консольне меню, яке містить набір інструментів для базового локального керування сервером. У цьому меню буде вказана IP-адреса, яку система отримала від DHCP-сервера (якщо він увімкнений у мережі). Ця адреса знадобиться для доступу до веб-інтерфейсу адміністрування.

Початкове налаштування через веб-інтерфейс

Відкрийте будь-який сучасний веб-браузер і перейдіть за вказаною IP-адресою у форматі: http://IP-адреса/

На екрані з’явиться форма для входу в систему. Введіть логін root та пароль, який був заданий під час інсталяції.

Після входу в систему відкриється майстер початкового налаштування (Wizard). Він дозволяє крок за кроком налаштувати основні параметри системи — обсяг томів зберігання, протоколи доступу до файлів, резервне копіювання тощо.

Зміна базових параметрів системи (див.рис. 3.41)

Після запуску веб-інтерфейсу рекомендується одразу налаштувати загальні системні параметри. Для цього перейдіть у розділ System → General Setup. У цьому меню можна:

– змінити мову інтерфейсу на українську або іншу з доступних;
– вказати поточний часовий пояс для коректного журналювання;
– за потреби активувати синхронізацію з NTP-сервером для точного часу.

Після внесення змін натисніть Save, а також оновіть сторінку у браузері.

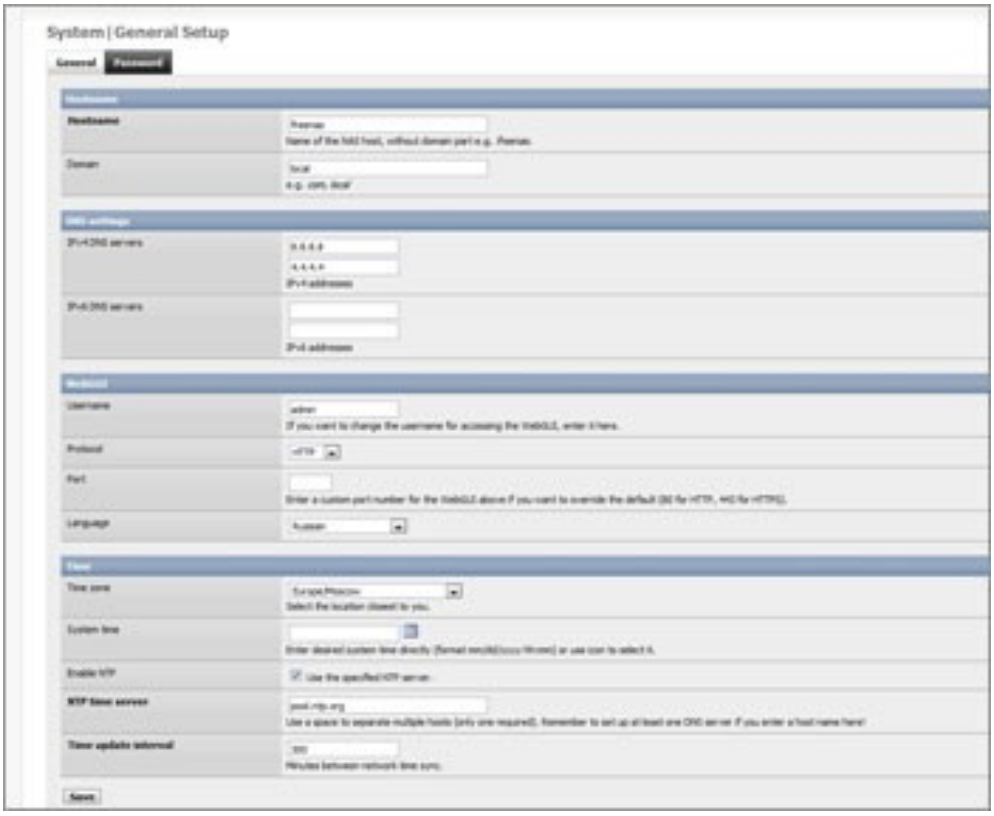


Рисунок 3.41 - Розділ System → General Setup інтерфейсу FreeNAS

Зміна пароля адміністратора веб-інтерфейсу

Із міркувань безпеки рекомендується одразу змінити пароль за замовчуванням для доступу до веб-інтерфейсу. Для цього перейдіть до відповідного розділу

налаштувань, змініть пароль і натисніть Зберегти. Система попросить вас повторно ввійти вже з новим паролем (див.рис. 3.42).

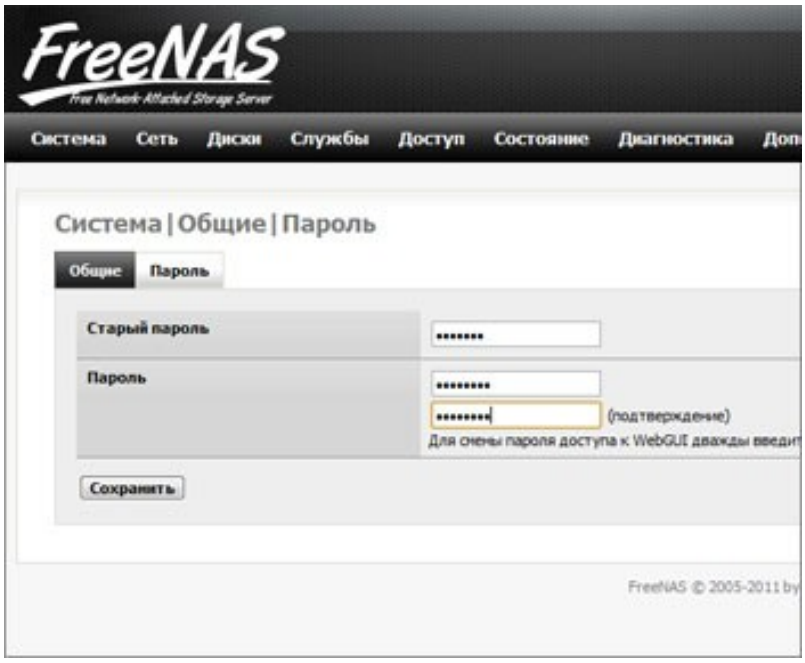


Рисунок 3.42 — Вікно зміни паролю адміністратора

Подальше керування

Усі подальші дії з адміністрування системи — створення пулів даних, налаштування спільного доступу, запуск плагінів тощо — виконуються виключно через веб-інтерфейс FreeNAS за тією ж IP-адресою. Стандартні облікові дані:

- логін: admin
- пароль: freenas (якщо не змінювались під час майстра налаштування)

Якщо під час встановлення системи FreeNAS було дозволено створення swap-розділу, наступним кроком є його ручне підключення до системи для забезпечення стабільної роботи при нестачі оперативної пам’яті. Для цього необхідно виконати низку дій через веб-інтерфейс керування системою.

Крок 1: Визначення розділу підкачування

Спочатку необхідно з’ясувати, на якому саме фізичному розділі диска розташовано файл підкачки. Для цього в головному меню перейдіть до розділу «Діагностика» → «Інформація» → «Розділи».

У цьому вікні буде відображена детальна інформація про всі виявлені розділи дисків, включно з їхнім іменуванням, обсягом, типом та призначенням. Зазвичай диск, на який інстальовано FreeNAS, розбитий на кілька частин:

- перший розділ — для самої операційної системи;
- другий — для користувацьких даних;
- третій — для swap (розділу підкачування).

Орієнтуватися можна за розміром: у типовому прикладі розмір розділу підкачки становить 256 Мбайт. Якщо ім’я диска, наприклад, /dev/ad0, то третій розділ цього диска буде мати ім’я /dev/ad0s3.

Примітка: уважні користувачі могли помітити, що шлях до розділу підкачки система вже показувала під час завершального етапу інсталяції, одразу після форматування диска.

Крок 2: Підключення файлу підкачки

Після того як шлях до розділу підкачки ідентифіковано, переходимо до його безпосереднього підключення в системі. Для цього:

1. Відкрийте меню «Система» → «Додатково» → «Файл підкачки».

2. У полі «Тип» оберіть «Пристрій» (Device).

3. У полі «Шлях» (Path) вручну введіть ідентифікатор розділу, наприклад:
/dev/ad0s3

4. Натисніть кнопку «Зберегти» (Save) для підтвердження змін.

Після цього FreeNAS автоматично почне використовувати визначений swap-розділ як додаткове джерело пам’яті в разі нестачі фізичної оперативної

пам’яті (RAM), що позитивно впливає на стабільність системи при високих навантаженнях.

Налаштування роботи з накопичувачами у FreeNAS

Після успішного встановлення FreeNAS та первинного налаштування системи настає момент для конфігурації накопичувачів. Це є ключовим етапом, адже правильне підключення та форматування дисків забезпечує стабільне зберігання й доступ до даних.

Крок 1: Додавання нового диска до системи

Щоб додати один або кілька накопичувачів до FreeNAS, виконайте такі дії:

У головному меню перейдіть до розділу «Диски» → «Управління».

У вікні управління натисніть на кнопку відкриття списку дисків (див. рис. 3.43). Перед вами з’явиться перелік усіх доступних фізичних пристроїв зберігання, підключених до системи.

Увага: Якщо у вашій системі кілька накопичувачів, будьте особливо уважними під час вибору, щоб не переплутати диски та не втратити важливі дані. Звертайте увагу на назви, розміри та інші характеристики, що допоможуть ідентифікувати потрібний пристрій.

Виберіть потрібний диск зі списку.

Крок 2: Активація SMART-моніторингу

Перед додаванням диска до системи рекомендується ввімкнути функцію SMART (Self-Monitoring, Analysis and Reporting Technology). Це дозволить системі регулярно відстежувати стан накопичувача, аналізувати його здоров’я та заздалегідь попереджати про потенційні збої або вихід з ладу.

– Поставте галочку навпроти пункту «Enable SMART» або подібного варіанту у вікні налаштувань диска.

Крок 3: Вибір файлової системи

На цьому етапі потрібно визначитися з файловою системою, яку буде використовувати накопичувач. Залежно від того, новий диск чи вже форматований раніше, вибір може відрізнятися (див рис.3.43 та див.рис. 3.44)

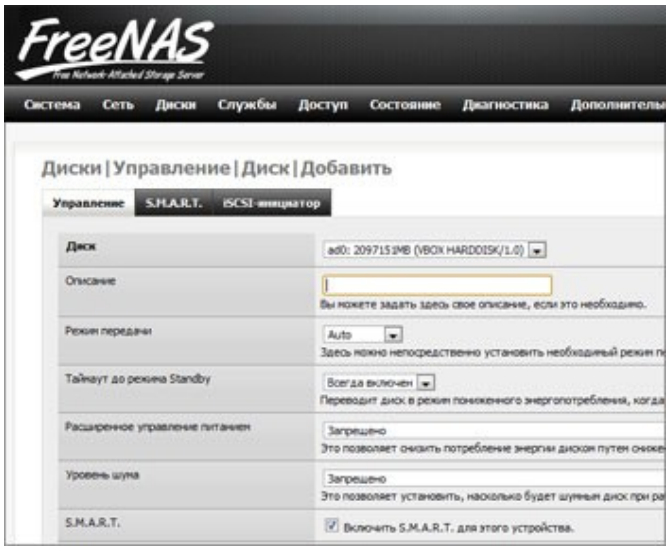


Рисунок 3.43 - Вікно вибору диску

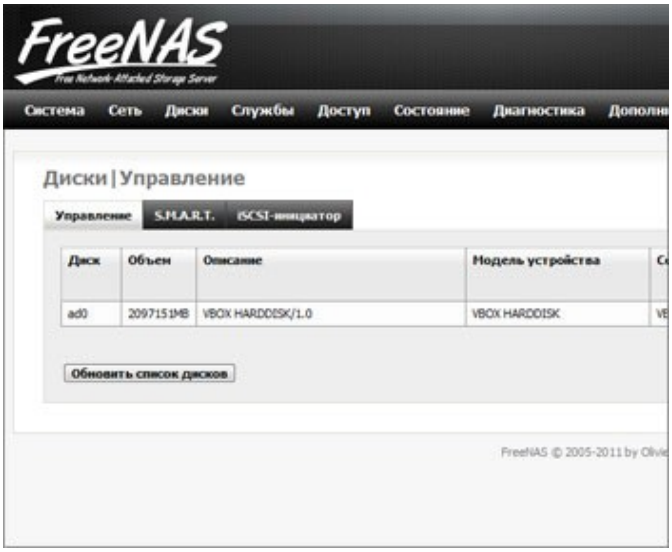


Рисунок 3.44 — Вказування параметрів диску

– Якщо ви додаєте чистий диск, на який буде записуватись нова інформація, оберіть файлову систему UFS with Soft Updates — вона є надійною та добре інтегрується з FreeNAS.
– Якщо ж ви додаєте вже існуючий диск з важливими даними, обов'язково вкажіть той тип файлової системи, в якому цей диск був попередньо відформатований (наприклад, ZFS, UFS, FAT, NTFS тощо), щоб уникнути втрати інформації (див. рис. 3.44).

Примітка: Якщо вибрати неправильну файлову систему, система може не розпізнати структуру даних або навіть запропонувати переформатування, що призведе до втрати інформації.

Крок 4: Додавання диска

Після вибору всіх параметрів — SMART, файлової системи та самого накопичувача — натисніть кнопку «Додати» (Add). Обраний диск буде приєднано до системи, і ви зможете почати роботу з ним у межах FreeNAS.

Форматування та монтування накопичувачів у FreeNAS

Після додавання нових накопичувачів до системи FreeNAS, наступним кроком є їх форматування та монтування, що забезпечить коректну роботу файлової системи та доступ до збережених даних.

Крок 1: Форматування накопичувачів

Якщо у вас є диски, які ще не були відформатовані, необхідно виконати їх попередню підготовку до використання:

Перейдіть у меню «Диски» → «Форматування».

У списку виберіть потрібний диск. Будьте уважні, аби не переплутати пристрої, особливо якщо у системі підключено декілька дисків — неправильний вибір може призвести до втрати даних.

Виберіть тип файлової системи для форматування. Рекомендується використовувати файлову систему UFS (Unix File System), яка є стабільною та сумісною

з FreeNAS. Втім, вибір не є обов'язковим — можливо застосування інших файлових систем за необхідності.

Примітка: Форматування повністю очищує диск. Переконайтеся, що на обраному накопичувачі немає потрібних даних.

Крок 2: Створення точок монтування

Після форматування всі накопичувачі необхідно змонтувати, щоб операційна система могла з ними працювати:

Перейдіть у меню «Диски» → «Точка монтування».

Натисніть кнопку «+», щоб створити нову точку монтування.

У формі вибору:

– Вкажіть тип джерела – диск (або розділ).
– Оберіть сам диск, який щойно відформатували.
– Введіть номер розділу (як правило, це 1, якщо диск не поділений на декілька).
– Вкажіть тип файлової системи, відповідно до вибраного при форматуванні.
– Присвойте унікальне ім’я точки монтування, наприклад, data, media, backup тощо.

Після внесення усіх параметрів натисніть «Додати», а потім — «Застосувати зміни».

На цьому етапі базове налаштування дисків завершено. Тепер можна перейти до конфігурації мережевого доступу до NAS.

Налаштування доступу до мережевого сховища

Щоб мати змогу обмінюватися файлами в локальній мережі через FreeNAS, необхідно налаштувати відповідні служби, а також створити загальні ресурси.

Крок 1: Увімкнення CIFS/SMB (NetBIOS) (див.рис. 3.45)

Для забезпечення доступу з Windows-сумісних пристроїв активуйте протокол CIFS/SMB:

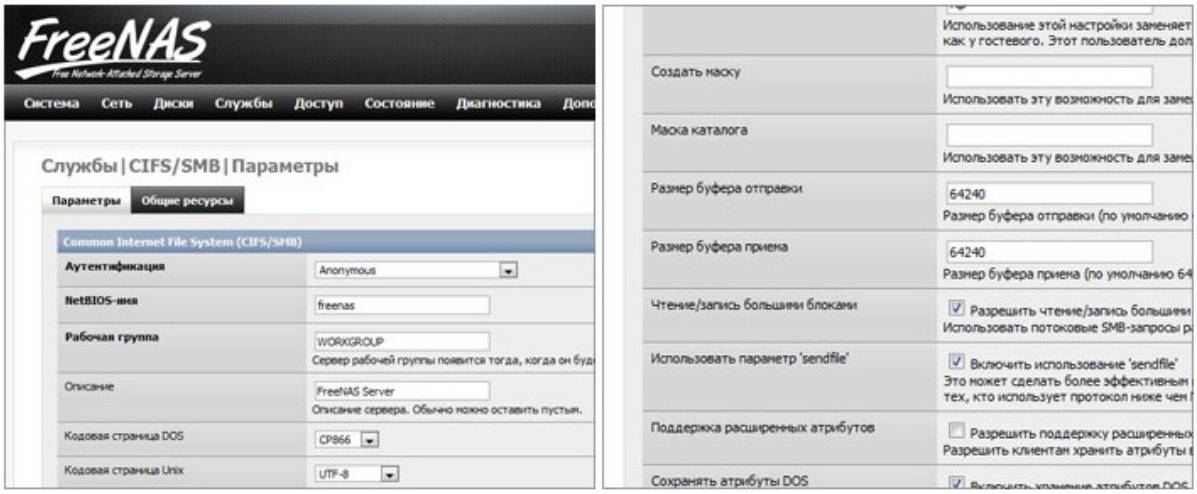


Рисунок 3.45 — Включення служби CIFS/SMB (NetBIOS)

Перейдіть у відповідний розділ служб та увімкніть CIFS/SMB (NetBIOS) (див. рис. 3.45).

У налаштуваннях CIFS виконайте такі дії:

– За потреби змініть ім’я робочої групи, щоб воно відповідало локальній мережі.
– Встановіть ім’я пристрою NAS, яке буде відображатись у мережі.
– Виберіть відповідне кодування символів (наприклад, UTF-8).
– Увімкніть сервер часу (NTP) для синхронізації годинника.
– Активуйте опцію AIO (Asynchronous I/O) для покращеної продуктивності.

Інші параметри, як правило, можна залишити за замовчуванням. Після завершення конфігурації натисніть «Зберегти та перезапустити», щоб застосувати зміни.

Крок 2: Створення мережевих ресурсів (шарів) (див.рис. 3.46)

Для надання доступу до конкретних каталогів слід створити мережеві ресурси (так звані "шари"):

Перейдіть до розділу керування CIFS-ресурсами (див. рис. 3.46).

Створіть новий ресурс, вказавши:

– Ім’я ресурсу – це буде відображуване ім’я шару у мережі.
– Коментар – за бажанням, для зручності ідентифікації.
– Шлях до каталогу – усі точки монтування знаходяться у каталозі /mnt/, тому типовий шлях виглядає як /mnt/ім’я_точки_монтування/ (наприклад, /mnt/data/).

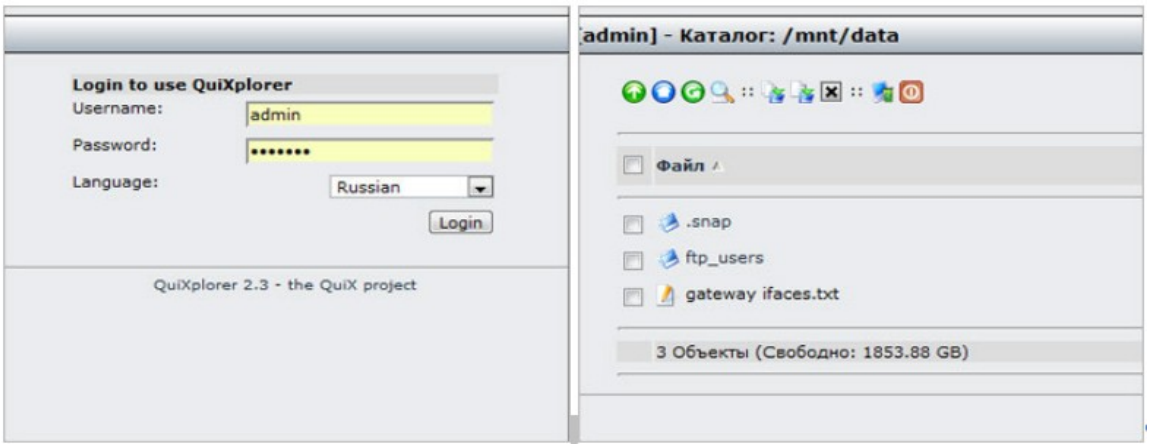


Рисунок 3.46 — Додавання мережевого ресурсу

Порада: Рекомендується створити в межах точки монтування окремі папки для різних типів даних (наприклад, /mnt/data/photos, /mnt/data/backups), а вже ці підкаталоги розшарювати, що дозволяє краще структурувати ресурси.

Якщо у вас є кілька накопичувачів або розділів, не забудьте повторити процес створення мережевих ресурсів для кожного з них.

На цьому етапі FreeNAS повністю готовий до роботи як повноцінне мережеве сховище. Доступ до даних можливий з будь-якого пристрою в локальній мережі, за умови належного налаштування прав і доступу.

Для керування файлами та папками прямо з веб-інтерфейсу використовуйте файловий менеджер із розділу «Додатково». Логін та пароль для нього такий самий, як і у користувачів у FreeNAS.

3.7 Інструкція з використання тестових наборів та тестових програм

Для діагностики функціонування комп'ютерної мережі часто використовуються утиліти PING та TRACERT, які входять до стандартного набору засобів більшості операційних систем, зокрема Windows. Ці інструменти дозволяють перевірити зв'язність між вузлами, виявити проблеми маршрутизації та оцінити час затримки при передаванні пакетів.

У разі виникнення підозри на відсутність зв'язку з певним вузлом мережі першою командою, до якої слід звернутись, є PING (Packet Internet Groper). Цей інструмент дозволяє перевірити коректність встановлення з'єднання за протоколом TCP/IP як на локальному, так і на віддаленому комп'ютері. Основна функція утиліти полягає у визначенні наявності фізичного та логічного з'єднання між двома мережевими пристроями.

Команда PING працює на основі протоколу ICMP (Internet Control Message Protocol). Вона надсилає ехо-запити до віддаленого вузла, який, у разі наявності з'єднання, повертає відповідні ехо-відповіді. Таким чином перевіряється двосторонній зв'язок. У процесі виконання команда виводить статистику, включаючи час затримки відповіді, кількість успішно отриманих відповідей і втрату пакетів, що дозволяє оцінити якість з'єднання.

Синтаксис команди у середовищі Windows виглядає наступним чином:

ping [ключі] адреса_вузла

Найпоширеніші ключі:

– t – безперервна відправка запитів до примусового завершення (Ctrl+C);
– a – дозвіл IP-адреси у DNS-ім’я вузла;
– n число – кількість запитів, які буде надіслано;
– l довжина – визначення розміру ICMP-пакетів у байтах;
– f – заборона фрагментації пакета;
– i TTL – встановлення часу життя пакету (Time To Live);
– v тип – визначення типу обслуговування (TOS);
– r число – відображення маршрутів до вказаного числа переходів;
– s число – фіксація часу проходження для заданої кількості переходів;
– j список_вузлів – вказання маршруту через певні вузли (вільна маршрутизація);
– k список_вузлів – сувора маршрутизація через зазначені вузли без проміжних шлюзів;
– w час – встановлення тайм-ауту очікування відповіді у мілісекундах.

Інша важлива утиліта – TRACERT (Trace Route), яка також використовує ICMP-протоколи і призначена для відображення маршруту, що проходить пакет до вузла призначення. Вона дозволяє побачити всі проміжні пристрої (роутери), через які дані проходять у мережі, надаючи інформацію про кожен стрибок.

Синтаксис команди:

tracert [ключі] ім’я_вузла

Серед ключових параметрів:

– d – не виконувати DNS-резолюцію IP-адрес у доменні імена;
– h число – обмеження максимальної кількості переходів (TTL);
– j список_вузлів – вказання маршруту через певні вузли з можливістю вибору шляху;
– w час – вказівка часу очікування відповіді у мілісекундах.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проекту локальної комп'ютерної мережі компанії "NOWA-T" і прийняття рішення про її подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки.

Для розрахунку вартості НДР необхідно виконати наступні етапи:

- описати технологічний процес розробки із зазначенням трудомісткості кожної операції;
- визначити суму витрат на оплату праці основного і допоміжного персоналу, включаючи відрахування на соціальні заходи;
- визначити суму матеріальних затрат;
- обчислити витрати на електроенергію для науково-виробничих цілей;
- розрахувати транспортні витрати;
- нарахувати суму амортизаційних відрахувань;
- визначити суму накладних витрат;
- скласти кошторис та визначити собівартість НДР;
- розрахувати ціну НДР;
- визначити економічну ефективність та термін окупності продукту.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР доцільно дані витрат часу по окремих операціях технологічного процесу звести у таблицю 4.1.

Таблиця 4.1 - Середній час виконання НДР та стадії (операції) технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Підготовка	Інженер	6
2	Розробка проекту мережі	Інженер	20
3	Монтаж пасивного обладнання	Лаборант	20
4	Налаштування активного комутаційного обладнання	Технік	10
5	Встановлення та на лаштування програмного забезпечення	Технік	10
6	Тестування мережі	Технік	2
Р а з о м		–	68

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до

якої включають витрати на оплату праці, не пов'язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

Основна заробітна плата розраховується за формулою:

$$З_{осн.}=Т_с \cdot К_г, \quad (4.1)$$

де $Тс$ – тарифна ставка, грн.;

$Кг$ – кількість відпрацьованих годин.

$$З_{осн.}=100*26+80*22+60*40=6760,00 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.}= З_{осн.} \cdot К_{допл.}, \quad (4.2)$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам.

$$З_{дод.}= 6760,00 *0,14=946,40 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.}= З_{осн.}+ З_{дод.}, \quad (4.3)$$

$$В_{о.п.} = 6760,00 + 946,40 = 7706,40 \text{ грн.}$$

Крім того, слід визначити відрахування на заробітну плату:

– єдиний соціальний внесок – 22 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{з.п.}=ФОП \cdot 0,22, \quad (4.4)$$

де $ФОП$ – фонд оплати праці, грн.

$$В_{з.с.} =7706,40*0,22=1695,32 \text{ грн.}$$

Проведені розрахунки зведемо у наступну таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Дод. заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на опл. пр., грн. 6=3+4+5
		Тарифна ставка, грн.	К-сть від-працьов. год.	Факт. нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1	Інженер	100	26	2600,00	364,00	-	-
2	Технік	80	22	1760,00	246,4	-	-
3	Лаборант	60	40	2400,00	336,00	-	-
	Разом	-	-	6760,00	946,40	1695,32	9401,72

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{Bi} = q_i \cdot p_i \,, \tag{4.5}$$

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \Sigma M_{Bi} \tag{4.6}$$

$$З_{м.в.} = 118930{,}00 \text{ грн.}$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	Кабель UTP Cat5e	м	750	18,0	13500
2	Роз'єми RJ-45	шт	200	2,00	400
3	Розетки RJ-45	шт	50	55,00	2750
4	Короб пластиковий 40*25*2м	шт	64	51,00	3264
5	Дюбель	шт	300	0,72	216
6	Комутатори не керовані TP-TP-LINK TL-SG1016PE	шт	5	6000,00	30000
7	Комутатор керований Cisco Business CBS250-16T-2G	шт	1	4800,00	4800
8	Точка доступу TP-Link Omada EAP610	шт	1	6000,00	6000
9	Сервер ARTLINE Business B29 (B29v75)	шт	1	33000,00	33000
	Сервер ARTLINE Business B29 (B29v75)	шт	1	25000,00	25000
	Р а з о м				118930

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S, \quad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Для розробки проекту даної локальної комп'ютерної мережі використовується один ПК, потужність якого W = 0,5 кВт і який працює 34 годин.

$$З_е=0,50*34*7=119.00 \text{ грн.}$$

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8–10 % від загальної суми матеріальних затрат.

$$Т_в=З_{м.в.} \cdot 0,08 \dots 0,1, \quad (4.8)$$

де $Т_В$ – транспортні витрати.

$$Т_В=118930,00*0,08=9514,40 \text{ грн}$$

4.6 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення.

Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Мінімально допустимі строки їх корисного використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$А=\frac{Б_В \cdot Н_А}{100\%}, \quad (4.9)$$

де $А$ – амортизаційні відрахування за звітний період, грн.;

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

H_A – норма амортизації, %.

Для проектування даної комп'ютерної мережі використовується один комп'ютер (вартість якого становить 25000,00), який працює 34 годин.

Тоді:

$$A = 25000*0,04*34/150=283,33 \text{ грн.}$$

4.7 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20–60 % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0,2 \ldots 0,6, \quad (4.10)$$

де H_B – накладні витрати.

$$H_B = 7706,4*0,3=2311,92 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 4.4.

Собівартість (СВ) НДР розрахуємо за формулою:

$$C_в = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_е + Т_в + A + H_в \quad (4.11)$$

$$C_в = 145306,93 \text{ грн.}$$

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до заг. суми
Витрати на оплату праці	7706,4	5,48
Відрахування на соціальні заходи	1695,32	1,21
Матеріальні витрати	118930	84,61
Витрати на електроенергію	119	0,08
Транспортні витрати	9514,4	6,77
Амортизаційні відрахування	283,33	0,2
Накладні витрати	2311,92	1,64
Собівартість	140560,37	100

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_B \cdot (1 + P_{рен}) \cdot K + B_{н.і.}}{K} \cdot (1 + ПДВ), \quad (4.12)$$

де $P_{рен.}$ – рівень рентабельності;

K – кількість замовлень, од.;

$B_{і.н.}$ – вартість носія інформації, грн.;

$ПДВ$ – ставка податку на додану вартість, (20 %).

$Ц$=140560,37*(1+0,26)*(1+0,2)= 212527,28 грн.

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Для визначення ефективності продукту розраховують чисту теперішню вартість (ЧТВ) і термін окупності ($T_{ОК}$).

$$ЧТВ = -K_В + \sum_{i=1}^{t} \frac{Г_П}{(1+i)^t}, \quad (4.13)$$

де $K_В$ – затрати на проект;

$Г_n$ – грошовий потік за t–ий рік;

t – відповідний рік проекту;

i - величина дисконтної ставки (10…15%).

$ЧТВ = -140560,37 + 121366,9/(1+0,1) + 121366,9/(1+0,1)^2 = 70076,42$ (грн.)

Якщо ЧТВ ≥ 0, то проект може бути рекомендований до впровадження.

Термін окупності визначається за формулою:

$$T_{ОК} = T_{ПВ} + \frac{H_В}{Г_{ПР}}, \quad (4.14)$$

де $T_{ПВ}$ – період до повного відшкодування витрат, років;

$H_В$ – невідшкодовані витрати на початок року, грн.;

$Г_{ПР}$ – грошовий потік на початок року, грн.

$$T_{ОК} = 1 + 30226,81/121366,91,15 = 1,2$$

Таблиця 4.5 - Економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	140560,37
2.	Плановий прибуток, грн.	71966,91
3.	Ціна, грн.	212527,28
4.	Чиста теперішня вартість, грн	70076,42
5.	Термін окупності, рік	1,2

В результаті аналізу економічних показників, зведених у таблицю 4.5, можна проводити роботи по впровадженню даної мережі.

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Небезпека утворення статичної електрики

Статична електрика - це заряди електрики, що накопичуються на виробничому обладнанні, речах побуту, на тілі чи одязі людини внаслідок контактного або індуктивного впливу. Сила струму даного виду електрики, як правило, дуже мала, але потенціал напруги може бути досить великим. Внаслідок цього статична напруга може стати небезпечною для життя людини, як на виробництві, так і в побуті.

У виробничих умовах накопичення зарядів статичної електрики відбувається під час: наливання електризуючи рідин (етилового ефіру, бензину, етилового і метилового спирту, бензолу) в незаземлені резервуари, цистерни та інші ємкості; протікання рідин пго трубах, ізольованих від землі або по гумових шлангах (із збільшенняи швидкості витікання рідини величина заряду і його потужність збільшується); очищеннч тканин, забруднених діелектричними рідинами та подібних процесів; перемішування речовин у змішувачах.

Фізіологічна дія статистичної електрики залежить від звільненої під час розгляду енергії і може відчуватися як слабкий, помірний, сильний укол або поштовх. трудовий виробничий травматизм протипожежний

Ці уколи й поштовхи безпечні, тому що сила стуму статистичної електрики дуже мала. Але такий вплив може призвести до тяжких нещасних випадків внаслідок рефлекторного руху поблизу незахищених рухомих частин устаткування або падіння з висоти.

Як захиститися від статичної електрики?

По суті, усе різноманіття методів захисту від електростатики зводиться до вибору з двох шляхів: або необхідно створити умови для того, щоб не пов'язані електрони розсіювалися самі по собі, не провокуючи перехід зі стрекотом, або

попередити саме виникнення ефекту, не даючи накопичитися заряду. Найпростішим способом позбутися від будь-яких можливих електроударів статикою є банальне заземлення електроприладів. Передбачається, що корпуси пристроїв, хоча й не перебувають під напругою безпосередньо, можуть поступово накопичувати заряд. Якщо ми забезпечимо стік цього заряду у землю через окремий кабель, то дотики до корпусу перестануть становити загрозу для здоров'я.

У побутових приладах заземлення зазвичай виконується за допомогою третьої жовто-зеленої жили у живильному шнурі. Вона з'єднується з відповідним контактом у розетці та по дроту веде до захисного заземлення та на вулиці. У автомобілях та багатьох пересувних механізмах заземлення ще більш очевидне: до кузова або корпусу кріпиться смужка зі струмопровідного матеріалу або ланцюжок, який при їзді торкається асфальту та забезпечує стік статичного заряду у землю.

Ще один широко відомий спосіб позбутися від зайвих електронів на предметах полягає у тому, щоб збільшити електропровідність діелектричних матеріалів. Зробивши це, Ви отримаєте можливість відводити зайвий заряд на інші об'єкти, знижуючи сумарний потенціал. Потрібний ефект досягається із застосуванням різних спреїв та аерозолів, які наносяться на предмети. Окрім того, на великі прилади та пристрої можна наклеювати спеціальні плівки, які збирають заряд на себе. Принцип дії й у тих, і у інших однаковий: просто у другому випадку плівка наклеюється відразу, а у першому вона стає результатом висихання складу на поверхні об'єкту.

Схожий ефект дає й банальне зволоження повітря: якщо у будинку висока вологість, предмети меблів та інші поверхні набувають дуже тонкої плівки-нальоту, яка забезпечує підвищену електричну провідність. Ще краще іонізувати повітря у приміщенні: іонізатор відразу генерує необхідну кількість позитивно та негативно заряджених частинок та викидає їх потоком за допомогою вентилятора. Завдяки гарному поширенню, кожен іон швидко «знаходить своє місце», притягаючись до мікрочасток протилежної полярності та нейтралізуючи заряд.

У промисловості, де будь-яка іскра може представляти серйозну небезпеку, застосовують інші підходи. Наприклад, розробляють нові принципи здійснення виробничого процесу, які повністю виключають або мінімізують ймовірність накопичення заряду на поверхні верстатів та агрегатів, готують мікроклімат відповідним чином, використовують антистатичні речовини при обробці обладнання та спецодягу персоналу. За рахунок того, що світильники та допоміжні засоби виробництва знаходяться поза зоною можливого торкання людиною, знижується ймовірність контакту між різнозарядженими тілами та виникнення іскри. На високонебезпечних виробництвах співробітники проходять через так звану клітку Фарадея – це великий бокс, стінки якого сформовані з металевої сітки з маленькими клітинками. Конструкція переймає на себе будь-який розряд та відводить його у землю окремими кабелем.

5.2 Організація навчання з охорони праці в компанії

Згідно з Законом України “Про охорону праці”. Державний комітет України по нагляду за охороною праці наказом від 04.04.94 р. затвердив “Типове положення про навчання, інструктаж і перевірку знань працівників з питань охорони праці”. Відповідно до цього документу всі працівники при прийомі на роботу, в процесі роботи проходять на підприємстві інструктаж з питань охорони праці, надання першої медичної допомоги потерпілим від нещасних випадків, з правил поведінки при аваріях. Навчання працівників правилам безпеки праці запроваджується в усіх підприємствах, установах, незалежно від характеру і ступеня небезпеки виробництва. Форми такого навчання: інструктажі, технічні мінімуми, так зване курсове навчання, спеціальне навчання, навчання перевірки знань посадових осіб, підвищення кваліфікації, навчання студентів та учнів навчальних закладів.

Інструктаж з охорони праці проводиться в усіх підприємствах, установах і організаціях, незалежно від характеру їх виробничої діяльності, освіти, кваліфі-

кації, стажу, досвіду з даного фаху або посади працівників. Керівництво (організація) за своєчасне і правильне проведення інструктажів покладає відповідальність на власника (керівника) підприємства, установи, організації, а у підрозділах – на керівника підрозділу. За характером та інтервалами інструктажі бувають: ввідними і на робочому місці – первинними, позаплановими і цільовими.

Організація навчання працюючих в охороні праці на всіх підприємствах і в організаціях здійснюється відповідно до ДСТУ 12.0.004-79 “ССБП. Організація навчання працюючих в безпеці праці. Загальні положення” і галузевих методичних вказівок. Ці документи визначають порядок і види навчання робочих, інженерно-технічних працівників і службовців безпеці праці.

Ввідний Інструктаж проводять з усіма, хто влаштовується на роботу, а також відряджається, хто вчиться та студентами, що прибули на виробниче навчання або практику. Його проводить інженер з охорони праці або особа, на яку покладені ці обов’язки. Ввідний інструктаж має проводитися в кабінеті з охорони праці або спеціально обладнаному приміщенні з використанням сучасних технічних засобів навчання і пропаганди, а також наочних знарядь (плакатів, натурних експонатів, макетів, кінофільмів, діапозитивів і моделей). Інструктаж проводять відповідно до інструкції, розробленої з урахуванням вимог ССБП, особливостей даного виробництва, затвердженої керівником підприємства та комітетом профспілки.

Ввідний інструктаж проводить інженер з охорони праці або особа, на яку покладені Його обов’язки, з усіма особами, що приймаються на роботу, а також з тими, що прибули у відрядження, студентами, учнями, направленими на виробничу практику. Метою ввідного Інструктажу є роз’яснення значення виробничої трудової дисципліни, ознайомлення з характером майбутньої роботи, загальними умовами, з вимогами безпеки: ознайомлення з основними положеннями законодавства про працю, правилами внутрішнього трудового розпорядку, основними правилами електробезпеки. Порядком складання актів про нещасний випадок, порядком надання першої допомоги потерпілому: загальними вимогами

до організації та утримання робочих місць; вимогами особистої гігієни, виробничої санітарії, призначення використання засобів Індивідуального захисту, санспецодягу та спецвзуття, з основними вимогами пожежної безпеки.

Про запровадження ввідного Інструктажу роблять запис у спеціальному журналі реєстру інструктажів з питань охорони праці, а також у документі про прийом працівника на роботу. Журнал має бути прошнурований, пронумерований і скріплений печаткою. Зберігається він у інженера з охорони праці.

Інструктаж проводиться з одним або з групою робітників у кабінеті охорони праці або в спеціально обладнаному приміщенні з використанням сучасних технічних засобів навчання, наочних посібників.

Про проведення ввідного інструктажу і перевірку знань того, хто навчається, роблять запис у журналі реєстрації ввідного інструктажу і в особистій картці з обов'язковими підписами Інструктора й інструктуючого.

Повторний інструктаж на робочому місці повинні проходити всі працівники, незалежно від кваліфікації, освіти та стажу роботи: на роботах з підвищеною небезпекою праці – раз у квартал, на Інших роботах – раз на півріччя. Його проводять індивідуально або з групою працівників одного фаху, бригади – за інструкціями для даної професії, посади.

Позаплановий інструктаж проводять при зміні правил, норм, Інструкцій, технологічного процесу або обладнання, внаслідок чого змінюються умови безпеки праці, при порушенні працівником правил та інструкцій з охорони праці, застосування неправильних способів праці, які можуть призвести до травми або аварії, при нещасному випадку, при перервах у роботі: для робіт, до яких ставляться підвищені додаткові вимоги безпеки праці – понад ЗО календарних діб. для решти робіт – 60 і більше діб. Цей Інструктаж проводять згідно з розпорядженням установ, які здійснюють державний нагляд за охороною праці індивідуально або з групою працівників однієї професії.

5.3 Контроль параметрів шуму та вібрації в компанії “NOWA-T”

Для вимірювання шуму використовують шумоміри з відповідними фільтрами і частотними аналізаторами (див.рис. 5.1)., які дозволяють виміряти рівні звукового тиску шуму в октавних смугах, а також за шкалою „А” визначити рівень звуку. Звичайний шумомір складається з мікрофона, підсилювача, фільтрів (корегуючих, октавних) та показуючого приладу.

Порядок контролю шуму регламентовано ДСН 3.3.6.037-99. Вимірювання шуму проводиться на постійних робочих місцях у приміщеннях, на території підприємств, у промислових спорудах та машинах (у кабінах, на пультах управління і т.п.). Результати вимірювань повинні характеризувати шумовий вплив за час робочої зміни (робочого дня).

При проведенні вимірювань мікрофон слід розташовувати на висоті 1,5 м над рівнем підлоги чи робочого майданчика (якщо робота виконується стоячи) чи на висоті і відстані 15 см від вуха людини, на яку діє шум (якщо робота виконується сидячи чи лежачи). Мікрофон повинен бути зорієнтований у напрямку максимального рівня шуму та віддалений не менш ніж на 0,5 м від оператора, який проводить вимірювання.

Рисунок 5.1 - Прибор для контролю шуму – шумомір ШІ-01

Тривалість вимірювання переривчастого шуму повинна відповідати часу повного робочого циклу з урахуванням сумарної тривалості перерв з рівнем фонового шуму. Для шуму, що коливається у часі, допускається загальна тривалість вимірювання 30 хвилин безперервно або вимірювання складається з трьох десятихвилинних циклів. Для імпульсного шуму тривалість вимірювання становить 30 хвилин.

Для вимірювання вібрацій широко використовуються електричні вібровимірювальні прилади, принцип дії котрих базується на перетворенні кінематичних параметрів коливного руху в електричні величини, які вимірюються та реєструються за допомогою електричних приладів (див.рис. 5.2).

Октава-101ВМ ВВМ-201

Рисунок 5.2 - Віброметри

Основні елементи цих приладів - первинні вимірювальні перетворювачі, в якості яких використовують ємнісні, індукційні, п'єзоелектричні перетворювачі, які сприймають коливні зміщення, швидкість та прискорення.

Найчастіше використовуються п'єзоелектричні перетворювачі віброприскорення — акселерометри (див.рис. 5.3).

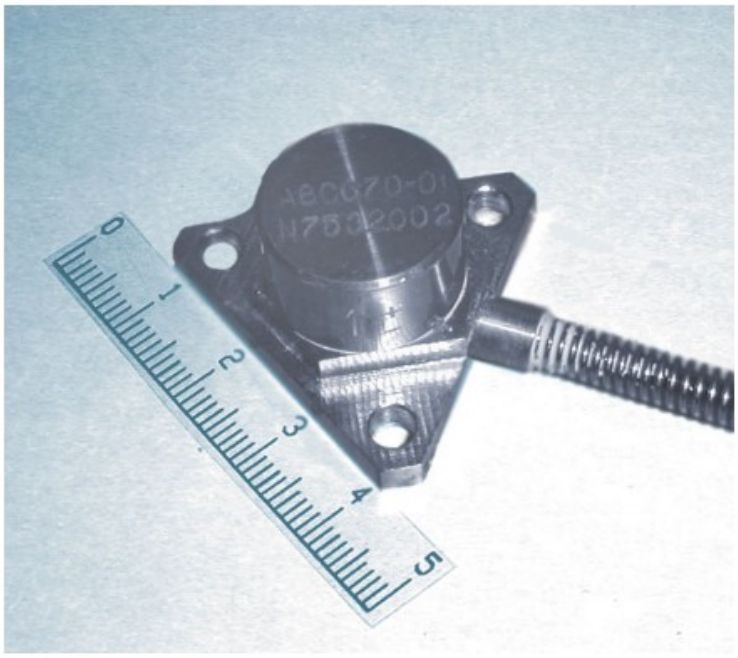


Рисунок 5.3 - Акселерометр АВС 070-01

Вібровимірювальними приладами з давачами можна вимірювати вібрації в багатьох точках. Їх перевага - дистанційність вимірювання параметрів вібрації, проста будова, відсутність інерційності.

Кількість вимірювань параметрів вібрації повинна бути не менше трьох для кожної октавної смуги частот. Вимірювальними параметрами вібрації є пікові аби середньоквадратичні значення віброзміщення, віброшвидкості або віброприскорення в октавних або 1/3-октавних смугах частот.

ВИСНОВКИ

В ході роботи над кваліфікаційною роботою спроектовано комп'ютерну мережу компанії "NOWA-T"

Зроблено аналітичний огляд літератури та існуючих рішень, та на його основі спроектовано логічну та фізичну топологію мережі. Вибрано пасивне та активне комутаційне обладнання, сервер, точку доступу та програмне забезпечення.

Кваліфікаційна робота містить повністю завершену логічну і фізичну топології мережі, таблицю IP-адресації та техніко-економічних показників які подано в графічній частині.

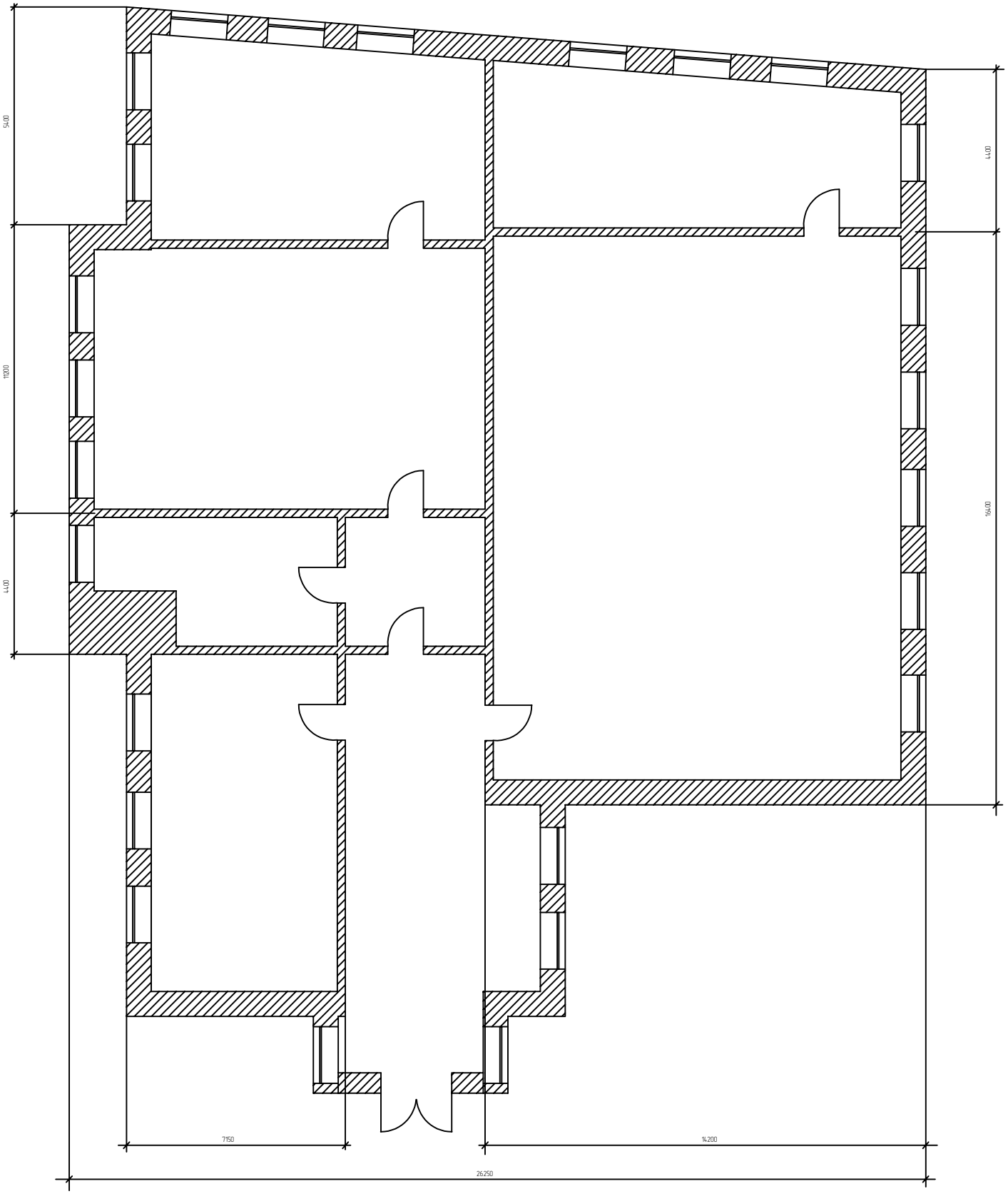
В економічному розділі розраховано собівартість мережі, її економічну ефективність, термін окупності та інші показники.

Останній розділ кваліфікаційної роботи описує питання охорони праці, та техніки безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

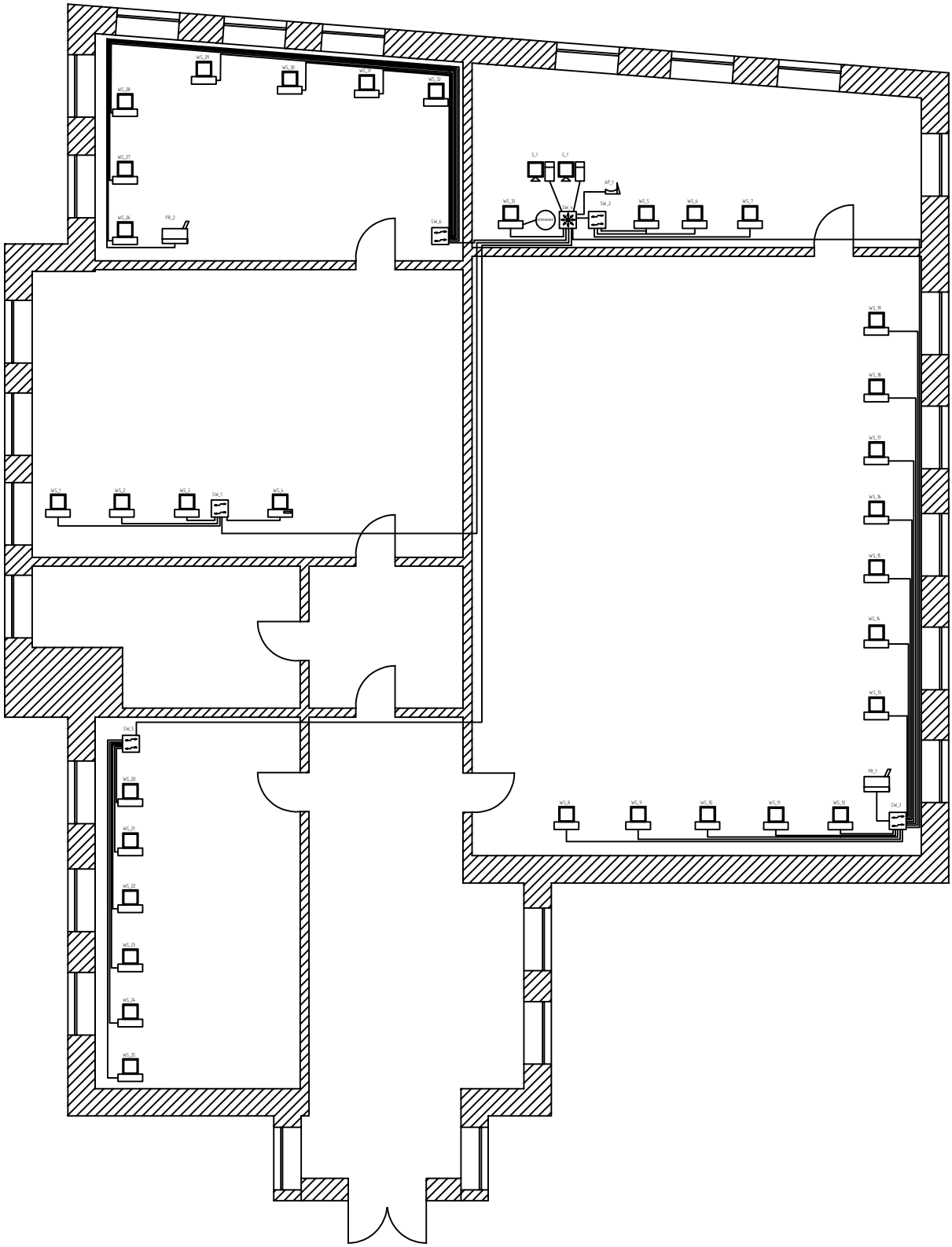
1. Антонов В.М. Сучасні комп'ютерні мережі. Підручник — К.: "МК-Прес", 2005. — 480 с.
2. Буров Є. Комп'ютерні мережі, 2-е видання. - БаК, 2004. – 584 с.: іл.
3. Додонов О. Г., Ланде Д. В., Путятін В. Г. Інформаційні потоки в глобальних комп’ютерних мережах. — К.: Наук, думка, 2009. — 295 с
4. Іртегов Д.В. Введення в мережні технології, К., 2014.
5. Шорошев В. В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп’ютерних систем. Монографія. - К.: ДУПСТ, 2011. - с.257.
6. Журавська І. М. Проектування та монтаж локальних комп’ютерних мереж : [навчальний посібник] / І. М. Журавська. – Миколаїв : Видавництво ЧДУ ім. Петра Могили, 2016. – 396 с.
7. Business Products. URL:: http://www.trendnet.com/ products/business/ category/switches. (дата звернення: 18.04.2025.)
8. Комутатори URL: http://hotline.ua/ computer/kommutatory/ (дата звернення: 11.05.2024.)Москальова В.М. Охорона праці URL: http://studentbooks.com.ua/content/view/1327/76/ (дата звернення: 11.04.2025.)
9. Діагностика локальних мереж URL: http://ukrefs.com.Ua/print:paqe.1.170653-Diaqnostika-lokal-nyh-seteiy.html (дата звернення: 18.04.2025.)

2025.КВР.123.412.01.00.00 ПП

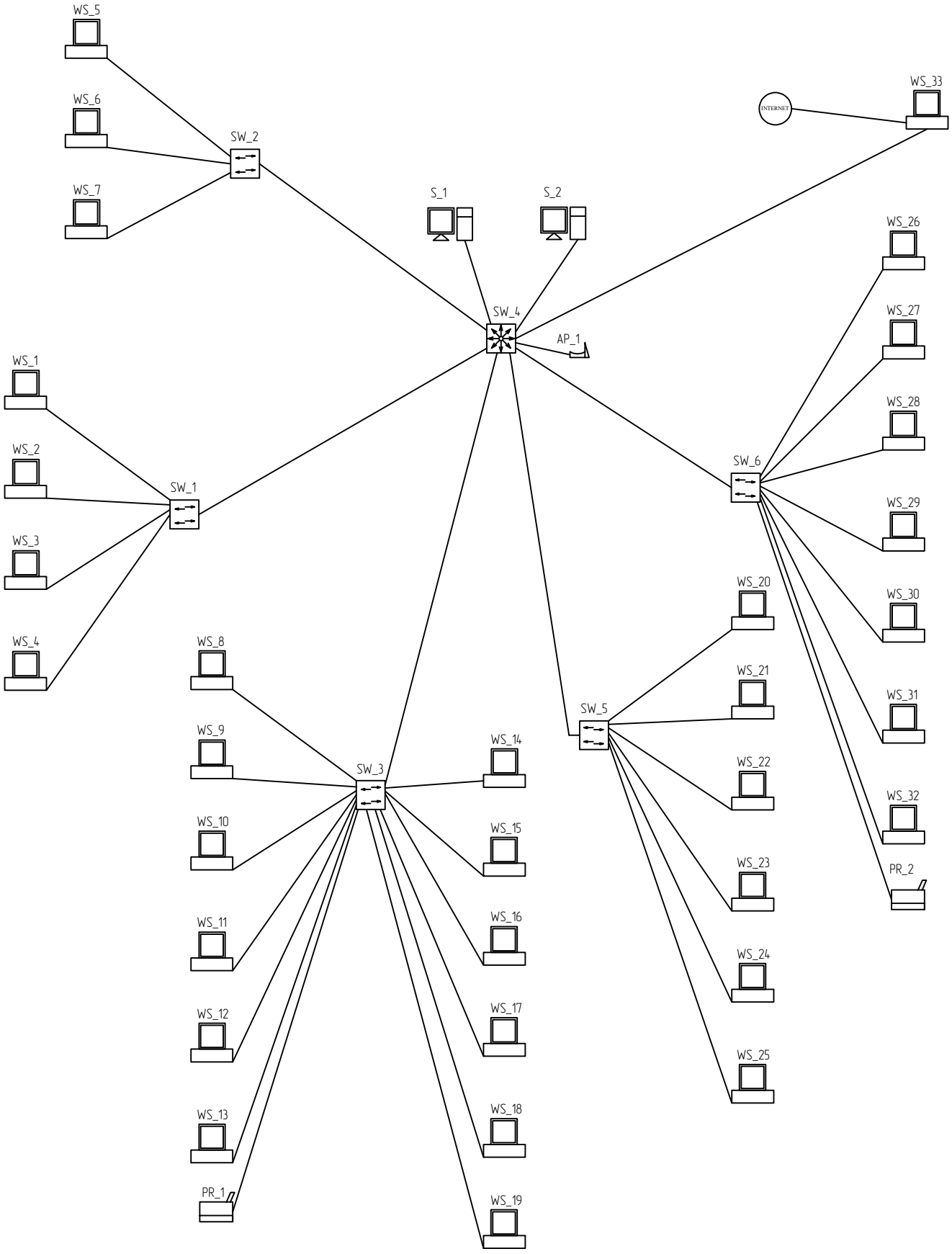


					2025.КВР.123.412.01.00.00 ПП	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії "NOWA-T" План приміщень	Літ. / Маса / Масшт.
Розроб.		Василюк Н.О.				- / 1:100
Керів.		Голобаш Р.Ю.				
Н.контр.		Язьків А.В.				Аркуш 1 / Аркушів 1
Рецензія						
Затв.						ВСП ТФК ТНТУ КІ-412, м.Тернопіль

2025.КВР.123.412.01.00.00 ФТ



						2025.КВР.123.412.01.00.00 ФТ		
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії "NOWA-T" Фізична топологія	Літ.	Маса	Масшт.
Розроб.		Василюк Н. О.					-	
Керів.		Болобаш Р. Ю.				Аркуш 1	Аркушів 1	
Т.контр.		Язьків А. В.				ВСП ТФК ТНТУ КІ-412, м.Тернопіль		
Реценз.								
Затв.								



						2025.КВР.123.412.01.00.00 ЛТ	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проєкту комп'ютерної мережі компанії "NOWA-T" Логічна топологія	Літ.	Маса	Масшт.
Розроб.		Василюк Н. О.					-	
Керів.		Болюбаш Р. Ю.				Аркуш 1	Аркушів 1	
Н.контр.		Язьків А. В.				ВСП ТФК ТНТУ КІ-412, м.Тернопіль		
Рецензія								
Затв.								

ТАБЛИЦЯ IP-АДРЕСАЦІЇ В МЕРЕЖІ

№ п.п	НАЗВА	IP-АДРЕСА	МАСКА	РОБОЧА ГРУПА
1	WS_1	192.168.3.10	255.255.255.0	OFFICE
2	WS_2	192.168.3.11	255.255.255.0	OFFICE
3	WS_3	192.168.3.12	255.255.255.0	OFFICE
4	WS_4	192.168.3.13	255.255.255.0	OFFICE
5	WS_5	192.168.3.14	255.255.255.0	it
6	WS_6	192.168.3.15	255.255.255.0	it
7	WS_7	192.168.3.16	255.255.255.0	it
8	WS_8	192.168.3.17	255.255.255.0	OFFICE
9	WS_9	192.168.3.18	255.255.255.0	OFFICE
10	WS_10	192.168.3.19	255.255.255.0	OFFICE
11	WS_11	192.168.3.20	255.255.255.0	OFFICE
12	WS_12	192.168.3.21	255.255.255.0	OFFICE
13	WS_13	192.168.3.22	255.255.255.0	OFFICE
13	WS_14	192.168.3.23	255.255.255.0	OFFICE
15	WS_15	192.168.3.24	255.255.255.0	OFFICE
16	WS_16	192.168.3.25	255.255.255.0	OFFICE
17	WS_17	192.168.3.26	255.255.255.0	OFFICE
18	WS_18	192.168.3.27	255.255.255.0	OFFICE
19	WS_19	192.168.3.28	255.255.255.0	OFFICE
20	WS_20	192.168.8.10	255.255.255.0	ECON
21	WS_21	192.168.8.11	255.255.255.0	ECON
22	WS_22	192.168.8.12	255.255.255.0	ECON
23	WS_23	192.168.8.13	255.255.255.0	ECON
24	WS_24	192.168.8.14	255.255.255.0	ECON
25	WS_25	192.168.8.15	255.255.255.0	ECON
26	WS_26	192.168.3.29	255.255.255.0	OFFICE
27	WS_27	192.168.3.30	255.255.255.0	OFFICE
28	WS_28	192.168.3.31	255.255.255.0	OFFICE
29	WS_29	192.168.3.32	255.255.255.0	OFFICE
30	WS_30	192.168.3.33	255.255.255.0	OFFICE
31	WS_31	192.168.3.34	255.255.255.0	OFFICE
32	WS_32	192.168.3.35	255.255.255.0	OFFICE
33	SW_4	192.168.3.200	255.255.255.0	OFFICE
34	AP_1	192.168.9.1	255.255.255.0	WIFI
35	PR_1	192.168.3.100	255.255.255.0	OFFICE
36	PR_2	192.168.8.100	255.255.255.0	ECON
37	S_1	192.168.3.205	255.255.255.0	OFFICE
38	S_2	192.168.3.206	255.255.255.0	OFFICE
39	S_3	192.168.3.207	255.255.255.0	OFFICE
40	WS_33	призначено провайдером		
		192.168.3.254	255.255.255.0	OFFICE

Зм.	Арк.		Підпис	Дат.
Розроб.		Василюк Н.О.		
Керів.		Болобаш Р.Ю.		
Н.контр.		Язьків А.В.		
Рецензія				
Затв.				

2025.КВР.123.412.01.00.01 ТБ

Розробка проекту комп'ютерної мережі компанії "NOWA-T"

Таблиця IP-адресації

Літ.	Маса	Масшт.
К		-

Аркуш 1 | Аркушів 1

ВСП ТФК ТНТУ КІ-412, м.Тернопіль

ТАБЛИЦЯ ТЕХНІКО-ЕКОНОМІЧНИХ ПОКАЗНИКІВ

№ п\п	параметр	одиниці вимірювання	значення	№ п\п	параметр	одиниці вимірювання	значення
1	технологія мережі	–	ethernet 100\1000	9	марка серверів, 3 шт	–	ARTLINE Business B29 (B29v75)
2	топологія мережі	–	гібридна	10	операційна система proxyсервера	–	Debian 10
3	середовище передачі	–	Вита пара кат. 5E	11	тип доступу до Internet	–	реальна IP, вита пара
4	кількість серверів	шт	3	12	термін окупності	рік	1,2
5	кількість вузлів мережі	шт	37	13	плановий прибуток	грн	71966,91
6	марка головного комутатора	–	Cisco Business CBS250-16T-2G	14	собівартість	грн	140560,37
7	марка 16-ти портового комутатора	–	TP-LINK TL-SG1016PE	15	ціна	грн	212527,28
8	марка точки доступу	–	TP-Link Omada EAP610	16			

						2025.КВР.123.412.01.00.02 ТБ	
Зм.	Арк.	№докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії "NOWA-T" Таблиця техніко-економічних показників	Літ.	Маса	Масшт.
Розроб.		Василюк Н.О.					-	
Керів.		Болобаш Р.Ю.				Аркуш 1	Аркушів 1	
Н.контр.		Юзьків А.В.				ВСП ТФК ТНТУ КІ-412, м.Тернопіль		
Затв.								