Міністерство освіти і науки України

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

Відділення телекомунікацій та електронних систем
(назва відділення)

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра
(освітній ступінь)

на тему: Модернізація проєкту комп'ютерної мережі компанії «MarKOM»

Виконав: студент VI курсу, групи КІб-602

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

_____ Ігор РЕПУШКО
(ім'я та прізвище)

Керівник Андрій ЛЯПАНДРА
(ім'я та прізвище)

Рецензент _____
(ім'я та прізвище)

Тернопіль – 2024

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

Відділення телекомунікацій та електронних систем
Циклова комісія комп'ютерної інженерії
Освітній ступінь бакалавр
Освітньо-професійна програма: Комп'ютерна інженерія
Спеціальність: 123 Комп'ютерна інженерія
Галузь знань: 12 Інформаційні технології

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"08" травня 2024 року

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

Репушко Ігор Іванович
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Модернізація проекту комп'ютерної мережі компанії «MarKOM»

керівник роботи Ляпандра Андрій Степанович
(прізвище, ім'я, по батькові)

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університетут імені Івана Пулюя» від 07.05.2024 р №4/9-224.

2. Строк подання студентом роботи: 21 червня 2024 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проектування, стандарти побудови СКС, документація на мережеве обладнання і сервери

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

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
   - План приміщень
   - Логічна топологія
   - Фізична топологія
   - Таблиця IP-адрес
   - Таблиця техніко-економічних показників
   - Модель мережі

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Оксана РЕДЬКВА заст. директора з НВР		
Охорона праці, техніка безпеки та екологічні вимоги	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	08.05	
2	Збір і узагальнення інформації	20.05	
3	Написання першого розділу	24.05	
4	Розробка технічного та робочого проекту	28.05	
5	Написання спеціального розділу	3.06	
6	Розрахунок економічної частини	5.06	
7	Написання розділу охорони праці	7.06	
8	Виконання графічної частини	10.06	
9	Оформлення проекту	14.06	
10	Погодження нормоконтролю	17.06	
11	Попередній захист роботи	21.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 08 травня 2024 року

Студент _____ Ігор РЕПУШКО
(підпис) (ім'я та прізвище)

Керівник роботи _____ Андрій ЛЯПАНДРА
(підпис) (ім'я та прізвище)

ЗМІСТ

АНОТАЦІЯ.....6
ВСТУП.....8
1 ЗАГАЛЬНИЙ РОЗДІЛ.....9
1.1 Технічне завдання.....9
1.1.1 Найменування та область застосування.....9
1.1.2 Призначеннння розробки.....9
1.1.3 Вимоги до апаратного та програмного забезпечення.....10
1.1.4 Вимоги до документації.....10
1.1.5 Техніко-економічні показники.....11
1.1.6 Стадії та етапи розробки.....11
1.1.7 Порядок контролю та прийому.....12
1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі.....13
2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ.....15
2.1 Розробка та обґрунтування логічної та фізичної схем мережі 15
2.2 Обґрунтування вибору комунікаційного обладнання.....19
2.4 Тестування мережі 23
2.5 Захист комп'ютерної мережі.....24
3 СПЕЦІАЛЬНИЙ РОЗДІЛ.....28
3.1 Налаштування комутатора Cisco CBS350-24P-4G-EU.....28
3.2 Налаштування точки доступу.....30
3.3 Налаштування MikroTik RB4011iGS+RM.....35
3.4 Встановлення та налаштування TrueNAS.....50
3.5 Інструкція з використання тестових наборів та тестових програм.....56
3.6 Основи моделювання в CISCO PACKET TRACER.....58

4 ЕКОНОМІЧНИЙ РОЗДІЛ.....64
4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР.....64
4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи65
4.3 Розрахунок матеріальних витрат.....67
4.4 Розрахунок витрат на електроенергію.....68
4.5 Визначення транспортних затрат.....68
4.6 Розрахунок суми амортизаційних відрахувань.....68
4.7 Обчислення накладних витрат.....69
4.8 Складання кошторису витрат та визначення собівартості НДР.....70
4.9 Розрахунок ціни НДР.....71
4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень.....71
5. ОХОРОНА ПРАЦІ ТЕХНІКИ БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ73
5.1 Система засобів і заходів безпечної експлуатації електроустаткування73
5.2 Розрахунок захисного заземлення.....78
ВИСНОВКИ.....88
ПЕРЕЛІК ПОСИЛАНЬ.....89

АНОТАЦІЯ

Тема кваліфікаційної роботи бакалавра - Модернізація проєкту комп'ютерної мережі компанії «MarKOM». Мета роботи — внести зміни в існуючу розробку комп'ютерної мережі підприємства, оскільки за час навчання були осягнуті нові знання, які б хотілося застосувати на практиці.

А саме в даній роботі описано заміну вхідного маршрутизатора з ПК на пристрій, встановлення нової точки доступу.

В роботі приводиться опис організації, технології передачі даних, інформаційних процесів, адміністративного управління, також надається опис мережевих вузлів, обґрунтування вибору програмного забезпечення та способи налаштування.

Приведено також налаштування маршрутизатора, використання двох каналів інтернету, та створення нового файлового сервера.

В роботі проведено аналіз обладнання котре використовується для побудови комп'ютерних мереж, проведено огляд та вибір топологій та технологій.

Описано методику розрахунку вартості робіт та описано техніку безпеки при монтажі та налагодженні мережі.

Робота написана на базі власного дипломного проекту.

ABSTRACT

The topic of the bachelor's qualification work - Modernization of the computer network project of the "MarKOM" company. The purpose of the work is to make changes to the existing development of the company's computer network, since new knowledge was acquired during the course of study, which one would like to apply in practice.

Namely, this paper describes the replacement of the incoming router from the PC to the device, the installation of a new access point.

The work provides a description of the organization, data transmission technology, information processes, administrative management, a description of network nodes, justification of the choice of software and methods of adjustment is also provided.

It also includes setting up a router, using two Internet channels, and creating a new file server.

The paper analyzes the equipment used to build computer networks, reviews and selects topologies and technologies.

The method of calculating the cost of works is described, and the safety technique during installation and adjustment of the network is described.

The work is written on the basis of one's own diploma project.

ВСТУП

Перші ЕОМ були призначені лише для швидкої обробки числових даних. Згодом обчислювальна техніка стала широко використовуватися в наукових дослідженнях, виробництві, освіті, побуті тощо. У користувачів віддалених один від одного комп'ютерів з'явилася потреба у швидкому обміні даними. Для цього було запропоновано об'єднати комп'ютери в єдину систему і таким чином передавати дані від одного комп'ютера до іншого. Так були створені комп'ютерні мережі.

Комп'ютерна мережа – це сукупність комп'ютерів і різних пристроїв, що забезпечують інформаційний обмін між комп'ютерами в мережі без використання яких-небудь проміжних носіїв інформації. Головною метою об'єднання комп'ютерів у мережу є надання користувачам можливості доступу до різних інформаційних ресурсів (наприклад, документам, програмам, баз даних і т.д.), розподіленим по цих комп'ютерів, і їх спільного використання. Мережі надають користувачам можливість не тільки швидкого обміну інформацією, але і спільної роботи на принтерах і інших периферійних пристроях, і навіть одночасної обробки документів.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Темою дипломного проекту Розробка проекту комп'ютерної мережі компанії «MarKOM».

Фірма ставить вимоги до мережі, котрі схожі з більшістю інших організацій, а саме::

Об'єднання ПК, що входять до різних відділів, налаштування підмереж для них.

Спільне використання одного швидкісного підключення до мережі Інтернет.

Використання в своїй роботі спільних ресурсів мережі та мережі Інтернет.

Максимально дешевий засіб обміну інформацією.

1.1.2 Призначеннння розробки

Дана комп'ютерна мережа призначена для організації ефективної роботи всіх працівників компанії «MarKOM». Мережа повинна забезпечити швидкий доступ до файлів, службової інформації та інших ресурсів загального використання, в тому числі друку необхідних документів, та забезпечити можливість якісної роботи працівників, забезпечити вихід в Інтернет.

Дана мережа повинна мати доступ до Internet., котрий забезпечено програмним маршрутизатором на базі вільної ОС.

Варто зауважити, що компанія «MarKOM» достатньо велика компанія. І описувати в даному дипломному проекті я буду лише частину мережі в якій розміщуються робочі місця працівників, та деякі адміністративні приміщення.

Швидкість мережі має бути 1000 Мбс.

1.1.3 Вимоги до апаратного та програмного забезпечення

Апаратні та програмні засоби комп'ютерної мережі повинні задовільняти ряду вимог.

Мережа повинна буде чітко поділена на робочі групи, швидкість мережі 1000 Мбіт/с.

Апаратне забезпечення мережі має бути загальновживане, недороге, підтримувати вказану швидкість передачі даних, мати можливість швидкої заміни, ремонту, мати можливість адміністрування.

Програмне забезпечення мережі – це сукупність мережевих операційних систем, що встановленні на комп'ютерах працівників підприємства.

Безпровідна точка доступу має підтримувати протоколи wpa-psk, wpa2-psk і відповідати стандарту 802.11n.

Комутатори робочих груп мають бути не керовані, головний комутатор — керований, окремих виділених серверів в мережі не передбачено, окрім бухгалтерського ПЗ, котрий буде розміщено в бухгалтерії.

1.1.4 Вимоги до документації

В результаті проектування потрібно створити наступну документацію:

- Інженерний журнал
- Логічна топологія
- Фізична топологія
- Матриця проблем та їх вирішення
- Помічені виходи кабелю
- Помічені траси кабелю
- Описи виходів і трас кабелю

– Резюме пристроїв MAC та IP-адрес

Після виконання вищевказаних робіт можна приступити до монтажу системи.

1.1.5 Техніко-економічні показники

Необхідно передбачити можливість збільшення кількості робочих станцій в мережі.

Забезпечити гнучкість системи до модернізації та змін в технічних особливостях.

Для розробки проекту комп'ютерної мережі передбачається затратити не більше 150 людино-годин.

Собівартість виконаних робіт не повинна перевищувати 300 000 гривень.

1.1.6 Стадії та етапи розробки

При організації мережі всі роботи можна поділити на наступні етапи:

– Збір інформації.
– Створення і затвердження проекту,
– Фізична реалізація мережі,
– Експлуатація та моніторинг мережі.

При зборі інформації необхідно визначитись в необхідних питаннях:

– Який тип організації і чи планується її зростання,
– Чи є існуючі комп'ютерні мережі,
– Побажання керівництва,
– Яке програмне забезпечення буде використано в мережі,

– Побажання користувачів.

– Визначити тип мережі, топологію, провідники та інше обладнання першого рівня,

– Визначити необхідну кількість повторювачів, концентраторів для робочих груп,

– Визначити кількість і потребу магістралей (вертикальне кабелювання та горизонтальне кабелювання),

– Кількість і потреба головного і проміжних комунікаційних вузлів,

– Визначити необхідність встановлення мостів і комутаторів або заміни іншого обладнання на них,

– Визначити необхідність встановлення маршрутизаторів,

– Тип підключення до глобальної мережі,

– Наявність спеціального обладнання для підключення до глобальної мережі.,

– Необхідний захист і процедури керування.

Все вищеописане необхідно використовувати і врахувати на етапі створення проекту, при цьому можна використовувати стандарт СКС (структурована кабельна система), які розробляються спеціалізованими фірмами.

1.1.7 Порядок контролю та прийому

При прийомці мережі необхідно виконати перевірку функціонування усіх мережевих вузлів.

Кабелі мають бути промаркованими.

Перевірка функціонування мережі виконується за допомогою прикладних утиліт або пакетів, здатних замінити дані утиліти.

Здача в експлуатацію мережі – досить важливий етап, який певною мірою визначає якісне функціонування мережі протягом всього терміну експлуатації.

Підрядник, який закінчив всі передбачені договором підряду роботи з інсталяції мережі, направляє замовнику письмове повідомлення про це разом з комплектом документів, список яких попередньо погоджено.

Замовник, який одержав повідомлення підрядника про завершення робіт та комплект документів, повинен приступити до комплексної перевірки функціональних характеристик мережі та прийняття її в експлуатацію спеціально створеною приймальною комісією.

Термін призначення комісії повинен становити не більше п'яти днів з моменту отримання письмового повідомлення підрядника про завершення робіт. В процесі здачі в експлуатацію мережі підписується відповідний акт.

1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі

Метою дипломного проекту є створення комп’ютерної мережі компанії «MarKOM», яка повинна об’єднати всі ПК працівників, забезпечити можливість обміну інформацією та зберігання даних, забезпечити всім робочим станціям спільний доступ до мережевих ресурсів та Інтернет.

Компанія здійснює продаж сучасних водно-дисперсійних лакофарбних матеріалів. Вся діяльність підприємства направлена на вихід вітчизняного виробництва акрилових обробних матеріалів на рівень провідних світових виробників.

Персональні комп’ютери будуть розміщуватись у таких приміщеннях:

– Серверна, в якій буде розміщено все комутуюче обладнання,

– Директор, буде мати один ПК, та один принтер,

– Каса, буде мати один ПК, та один принтер,

– Конференц зал, у ньому буде розміщено чотири ПК а також точка доступу,

– Відділ менеджерів, в якому буде розміщено чотири ПК,

– Відділ кадрів, в якому буде розміщено чотири ПК.

– Бухгалтерія, буде мати три робочі пк, сервер бухгалтерії та мережевий принтер.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Розробка та обґрунтування логічної та фізичної схем мережі [3,21,22,23]

Даний пункт ми скоротили, подавши лише основні тези, необхідні для роботи.

Технологія Ethernet – проста, надійна, дешева та ефективна, має високу швидкість передавання даних і завдяки цьому стала найпоширенішою. В деяких розробках починають інтегрувати в материнську плату адептери Ethernet.

Властивості мережі залежать від використовуваного типу кабеля Швидкість мережі 100 Мбіт/с. Стандарт Gigabit Ethernet затверджено у 1998 р. Може використовуватися волоконнооптичний кабель та скручена пара. Довжина сегмента для багатомодового кабеля – 500 м, для одномодового – 2000 м. Залежно від місця застосувань окремо визначені специфікації для коаксіальних кабелів та скрученої пари.

В архітектурі мереж 1000BaseT використовується топологія «зірка» на базі високоякісного кабелю «вита пара» категорії 5, в якому задіяні всі вісім жил, причому кожна з чотирьох пар провідників використовується як для прийому, так і для передачі інформації.

Технологія Wi-Fi – це можливість, не розгортаючи кабельної системи, дістати доступ до будь-яких сервісів Internet, де б не знаходився користувач, він завжди можете бути в мережі.

Технологія Wi-Fi – це безпровідний аналог стандарту Ethernet, на основі якого сьогодні побудована велика частина офісних комп’ютерних мереж. Він був зареєстрований в 1999 році.

Топологія комп'ютерної мережі відображає структуру зв'язків між її основними функціональними елементами. В залежності від компонентів, що розглядаються, розрізняють фізичну і логічну структури локальних ме-

реж. Доповнюючи одна одну, фізична та логічна структури дають найповніше уявлення про комп'ютерну мережу.

Топологія мережі визначає не тільки фізичне розташування комп’ютерів, але, що набагато важливіше, характер зв’язків між ними, особливості поширення сигналів по мережі. Саме характер зв’язків визначає ступінь відмовостійкості мережі, необхідну складність мережної апаратури, найбільш підходящий метод керування обміном, можливі типи середовищ передачі (каналів зв’язку), припустимий розмір мережі (довжина ліній зв’язку й кількість абонентів), необхідність електричного узгодження й багато чого іншого.

Враховуючи невеликі розміри підприємства, невелику кількість робочих місць, вибираємо тип мережі Ethernet 1000Base T.

Для цього типу мережі вибираємо топологію типу розширена зірка, в якій максимальна віддаленість станції до концентратора – до 100м.

Проте враховуючи присутність безпровідної точки доступу в мережі тип топології буде гібридний.

Вибір кабельної підсистеми диктується типом мережі й обраною топологією. Необхідні для стандарту фізичні характеристики кабелю закладаються при його виготовленні, про що і свідчать нанесені на кабель маркування.

Кабельна система локальної мережі побудована на основі неекранованої витої пари категорії 5е (див.рис.2.1).

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 в 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.

Проектована мережа буде поділена на сегменти, IP адреси яких, назви приміщень та груп, VLANи зведено в таблицю 2.1 та таблицю 2.2.

Таблиця 2.1 – Логічна адресація в мережі

Позначення вузлів	Робоча група/ Кількість вузлів		Назва кабінету	Номер VLAN	Адреса підмережі/ Маска
1	2	3	4	5	6
WS_1-WS_2	ADM	2	управління	10	192.168.10.0/24
WS_3-WS_5, S_1	buch	4	бухгалтерія	20	192.168.20.0/24
WS_6--WS_9	buch	4	Робота з персоналом	20	192.168.20.0/24
WS_10--WS_13	manager	4	менеджери	30	192.168.30.0/24
WS_14--WS_17	konf	4	Конференц зал	40	192.168.40.0/24
WS_18, S_2	ADMIN	1	адміністратор	100	192.168.100.0/24

Таблиця 2.2 - Таблиця конфігурування VLAN

№ п/п	Познач. вузла	Номер порту	Тип порту	Назва ме-реж. пр-ю	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
2	SW_4	15	Trunk	SW_1	8	Trunk	10

Продовження таблиці 2.2

1	2	3	4	5	6	7	8
3	SW_4	16	Trunk	SW_2	8	Trunk	20
4	SW_4	17	Trunk	SW_3	8	Trunk	20
5	SW_4	18	Trunk	SW_5	8	Trunk	30
6	SW_4	19	Trunk	SW_6	8	Trunk	30
7	SW_4	21	Trunk	WS_18		Access	10
8	SW_4	22	Trunk	AP_1		Access	10
9	SW_4	23	Trunk	S_2		Access	10
10	WS_1--WS_2			SW_1	1-6	Access	10
11	WS_3--WS_5			SW_2	1-6	Access	20
12	WS_6--WS_9			SW_3	1-6	Access	20
13	WS_10--WS_13			SW_5	1-6	Access	30
14	WS_14--WS_17			SW_6	1-6	Access	30

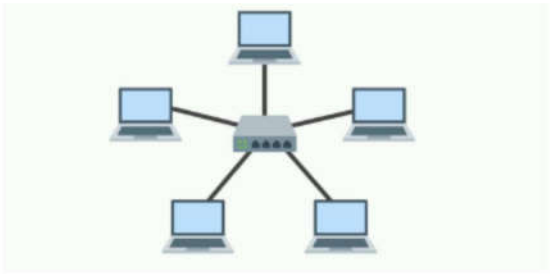


Рисунок 2.1 — Позначення зіркової топології (зверху), неекранована вита пара категорії 5е (знизу)

2.2 Обґрунтування вибору комунікаційного обладнання

Оскільки дана робота є модернізацією існуючої мережі, ми не будемо проводити вибір комутаторів робочих груп. Вони залишаються старими, а саме Linksys LGS108, зовнішній вигляд якого зображено на рисунку 2.2.

Також ми не обираємо головний комутатор, оскільки він якісний , сучасний, продуктивний, та може задовільнити всі потреби організації. В нас обрано і функціонує Cisco CBS350-24P-4G-EU, зовнішній вигляд якого зображено на рисунку 2.3.

Рисунок 2.2 – Зовнішній вигляд комутатора Linksys LGS108

Рисунок 2.3 – Зовнішній вигляд комутатора Cisco CBS350-24P-4G-EU

У мережі використовується безпровідна точка доступу. Вона була нами обрана раніше. Її марка Ubiquiti UniFi AP Long Range, зовнішній вигляд якої зображено на рисунку 2.4 Вимоги замовників мережі — було добавити ще одну точку доступу в загальному коридорі, біля кабінету бухгалтерії, оскільки є потреба використовувати мобільні застосунки для оплати послуг за допомогою мобільних терміналів, а також для зручності клієнтів.

Рисунок 2.4 – Зовнішній вигляд безпровідної точки доступу Ubiquiti UniFi AP Long Range

Була думка замінити її на іншу, але розглянувши її технічні характеристики , котрі приведені в таблиці 2.3, вирішили докупити таку саму. Правда є певний нюанс - такі точки для налаштування та своєї роботи потребують спеціального контролера, він може бути апаратним, як окремий пристрій, так і програмним, встановленим на якомусь ПК. Його потреба є тоді, коли мережа велика, і точок доступу є багато, тоді він спрощує керування та налаштування ними. В нашому випадку, ми налаштуємо точку один раз з допомогою мобільного телефону, та більше в нас не буде потреби щось змінювати, тому залишаємо таку модель точки доступу.

В мережі був присутній NAS сервер. Модель Synology DS718+. Його ми залишаємо для резервного копіювання бухгалтерії.

Виходячи з побажань замовників, ми в якості нового файлового сервера використаємо комп’ютер, що використовувався для доступу в інтернет, старий шлюз. Його продуктивності достатньо для виконання таких функцій. Його ми лише оновимо двома жорсткими дисками на 4 ТБ, щоб зробити відмовостійкий дзеркальний масив.

Таблиця 2.3 — Технічні характеристики точки доступу Ubiquiti UniFi AP Long Range

Порти:	(1) 10/100/1000 Ethernet Port
Антени:	(1) Dual-Band Antenna, Tri-Polarity, 3 dBi
Wi-Fi стандарти:	802.11 a/b/g/n/ac
Спосіб живлення	802.3af/A PoE & 24V PoE
Джерело живлення:	24V, 0.5A Gigabit PoE Adapter у комплекті
Максимальна потужність передачі 2.4 GHz 5 GHz:	 24 дБм 22 дБм
Бездротова безпека:	WEP, WPA-PSK, WPA-Enterprise (WPA/ WPA2, TKIP/AES)
VLAN:	802.1Q
Паралельних клієнтів:	200+

В якості нового шлюза ми будемо використовувати пристрій Mikrotik, який завдяки своїй гнучкості, може використовуватися з різною метою. Окрім функцій шлюза та фаєрвола мережі ми його налаштуємо на використання двох каналів провайдера інтернет.

Рисунок 2.5 – Зовнішній вигляд безпровідної точки доступу MikroTik RB4011iGS+RM

Отже оберемо шлюз. Вимога — невисока ціна, але достатня продуктивність для обслуговування 150 користувачів, а також наявність модуля для підключення оптичного каналу.

Всім вимогам відповідає MikroTik RB4011iGS+RM, технічні характеристики якого подані в таблиці 2.4, а сам він показаний на рисунку 2.5

Таблиця 2.4 — Розширені технічні характкеристики MikroTik RB4011iGS+RM

Швидкість LAN портів	1 Гбіт/с
Особливості	Підтримка PoE
	Підтримка VPN
Призначення роутера	Серверний
Конструкція антен	Немає антени
WAN-порт	Ethernet
Країна-виробник	Латвія
Інтерфейси	10 x 10/100/1000 Ethernet, 1 x SFP+
Підтримка протоколів	L2TP
	DHCP
	NAT
Wi-Fi підключення	Немає
Габарити і вага	228 x 120 x 50 мм 850 г
Країна реєстрації бренду	Латвія
Гарантія	12 місяців
вартість	8300 грн

Зведемо в таблицю 2.5 обране нами нове комутаційне обладнання.

Таблиця 2.5 - Зведена таблиця нового телекомунікаційного обладнання

Назва елемента	Модель	Ціна, грн.	Од. вим.	К-ть
Жорсткий диск	4 Тб	4300	шт	2
маршрутизатор	MikroTik RB4011iGS+RM	8300	шт	1
Точка доступу	Ubiquiti UniFi AP Long Range	3700,00	шт	1

2.4 Тестування мережі [25]

Тестувати комп’ютерні мережі можна за допомогою різних методів та тестів. Одним з поширених варіантів є тест на проникнення, що являє собою метод оцінювання захищеності комп'ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї (які не мають авторизованих засобів доступу до системи) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу). Цей процес включає активний аналіз системи з виявлення будь-якої потенційної вразливості, що може виникати внаслідок неправильної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, чи оперативне відставання в процедурних чи технічних контрзаходах. Цей аналіз проводиться з позиції потенційного нападника і може включати активне використання вразливостей.

Проблеми безпеки, що були виявлені в ході тесту на проникнення, представляються власнику системи. Ефективний тест на проникнення поєднає цю інформацію з точною оцінкою потенційного впливу на організацію і

окреслить межі технічних і процедурних контрзаходів для зменшення ризиків.

Тест на проникнення є корисним з кількох причин:

- визначення можливості певного набору атак;
- виявлення вразливостей вищого ризику, які є результатом комбінації вразливостей меншого ризику, що використовуються в певній послідовності;
- виявлення вразливостей, які може бути важко або неможливо знайти за допомогою автоматизованої мережі або застосування програмного забезпечення із сканування вразливостей;
- оцінювання величини потенційного впливу успішних атак на бізнес;
- тестування здатності захисників мережі успішно виявляти і реагувати на атаки;
- надання доказів на підтримку збільшення інвестицій у персонал і технології безпеки.

2.5 Захист комп'ютерної мережі [26]

Безпека мережі — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу. Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів. Мережева безпека включає в себе дозвіл на доступ до даних в мережі, який надається адміністратором мережі. Користувачі вибирають або їм призначаються ID і пароль або інші перевірки автентичності інформації, що дозволяє їм здійснити доступ до інформації і

програм у рамках своїх повноважень. Мережева безпека охоплює різні комп'ютерні мережі, як державні, так і приватні, які використовуються в повсякденних робочих місцях для здійснення угод і зв'язків між підприємствами, державними установами та приватними особами. Мережі можуть бути приватними, такими як всередині компанії або відкритими, для публічного доступу. Мережева безпека бере участь в організаціях, підприємствах та інших типів закладів. Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю.

Мережева безпека починається з аутентифікації, що зазвичай включає в себе ім'я користувача і пароль. Коли для цього потрібно тільки одна деталь аутентифікації (ім'я користувача), то це називають однофакторною аутентифікацією. При двофакторній аутентифікації, користувач ще повинен використати маркер безпеки або 'ключ', кредитну картку або мобільний телефон, при трьохфакторній аутентифікації, користувач повинен застосувати відбитки пальців або пройти сканування сітківки ока.

Після перевірки дійсності, брандмауер забезпечує доступ до послуг користувачам мережі. Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень (IPS).

Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб зберегти конфіденційніст.

Система безпеки мережі не ґрунтується на одному методі, а використовує комплекс засобів захисту. Навіть якщо частина обладнання виходить з ладу, решта продовжує захищати дані Вашої компанії від можливих атак.

Встановлення рівнів безпеки мережі надає Вам можливість доступу до цінної ділової інформації з будь-якого місця, де є доступ до мережі Інтернет, а також захищає її від загроз.

Система безпеки мережі:

– Захищає від внутрішніх та зовнішніх мережних атак. Небезпека, що загрожує підприємству, може мати як внутрішнє, так і зовнішнє походження. Ефективна система безпеки стежить за активністю в мережі, сигналізує про аномалії та реагує відповідним чином.
– Забезпечує конфіденційність обміну інформацією з будь-якого місця та в будь-який час. Працівники можуть увійти до мережі, працюючи вдома або в дорозі, та бути впевненими у захисті передачі інформації.
– Контролює доступ до інформації, ідентифікуючи користувачів та їхні системи. Ви маєте можливість встановлювати власні правила доступу до даних. Доступ може надаватися залежно від ідентифікаційної інформації користувача, робочих функцій, а також за іншими важливими критеріями.
– Забезпечує надійність системи. Технології безпеки дозволяють системі запобігти як вже відомим атакам, так і новим небезпечним вторгненням. Працівники, замовники та ділові партнери можуть бути впевненими у надійному захисті їхньої інформації.

Засоби захисту комп’ютерних мереж:

Брандмауери. Централізовані брандмауери та брандмауери окремих комп’ютерів можуть запобігати проникненню зловмисного мережного трафіку до мережі, яка підтримує діяльність компанії.

Антивірусні засоби. Більш захищена мережа може виявляти загрози, що створюють віруси, хробаки та інше зловмисне програмне забезпечення, і боротися з ним попереджувальними методами, перш ніж вони зможуть заподіяти шкоду.

Знаряддя, які відстежують стан мережі, грають важливу роль під час визначення мережних загроз.

Захищений віддалений доступ і обмін даними. Безпечний доступ для всіх типів клієнтів із використанням різноманітних механізмів доступу

грає важливу роль для забезпечення доступу користувачів до потрібних даних, незалежно від їх місцезнаходження та використовуваних пристроїв.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Налаштування комутатора Cisco CBS350-24P-4G-EU

Переходимо в привілейований режим. За замовчуванням пароль відсутній, тому потрібно просто натиснути на «Enter».

Активовуємо режим глобальної конфігурації.

Switch>enable

Password:

Switch#

Змінюємо ім’я комутатора (стандартне - Switch):

Switch# configure terminal

Switch(config)# hostname Cisco (задається нове ім'я - Cisco)

Cisco(config)#

Установка IP-адреси для порту управління комутатором

Cisco(config)# interface fa0/0

Cisco(config-if)# no shutdown

Cisco(config-if)# ip address 192.168.100.25 255.255.255.0

Cisco(config-if)# exit

Cisco(config)#

Установка пароля привілейованого режиму

Cisco(config)# enable secret pass1234 (пароль 111111111)

Cisco(config)#username admin secret 1111111111

Cisco(config)# exit

Cisco#

Cisco(config)# line vty 0 2 (переходимо в режим конфігурування термінальних ліній)

Cisco(config)#login local

Cisco(config-line)# transport input ssh (підключення лише по ssh)

Cisco(config-line)# exec timeout 20 0 (автовідключення сесії ssh через 20 хвилин)

Cisco(config—line)# end

Створюємо Vlan для кожного з відділів і присвоюємо їм порядкові номери і назви.

Cisco(config)#vlan 10 name ADM

Cisco(config)#vlan 20 name buch

Cisco(config)#vlan 30 name manager

Cisco(config)#vlan 40 name konf

Cisco(config)#vlan 100 name ADMIN

Співвідносимо порти комутатора створеним мереж Vlan.

Cisco(config)#interface range gi 0/1 — 2

switchport access vlan 10

description ADM

Cisco(config)#interface range gi 0/3 — 4

switchport access vlan 20

description buch

Cisco(config)#interface range gi 0/5 — 6

switchport access vlan 30

description manager

Cisco(config)#interface range gi 0/7 —8

switchport access vlan 40

description konf

Cisco(config)#interface range gi 0/9 — 24

switchport access vlan 100

description ADMIN

Для взаємодії між мережами слід створити віртуальні інтерфейси 3 -го рівня для кожного Vlan.

Cisco (config) #

inter vlan 10

ip address 192.168.10.245 255.255.255.0

no shut

inter vlan 20

ip address 192.168.20.245 255.255.255.0

no shut

inter vlan 30

ip address 192.168.30.245 255.255.255.0

no shut

inter vlan 40

ip address 192.168.40.245 255.255.255.0

no shut

inter vlan 100

ip address 192.168.100.245 255.255.255.0

no shut

inter vlan 30

ip address 192.168.10.1 255.255.255.0

no shut

Cisco(config) # ip routing

Cisco#write

Cisco(config—line)# end

Cisco# copy running-config startup-config.

3.2 Налаштування точки доступу

В компютерні мережі буде використано безпровідний сегмент.

Він потрібен для того, щоб можна було користуватися мобільними пристроями.

Одне з найбільш доступних і простих рішень на ринку безшовного WiFi можна реалізувати на базі обладнання і ПЗ Ubiquiti серії Unifi.

Розглянемо базовий сценарій розгортання безшовної бездротової мережі.

Качаємо свіжу версію контролера з сайту Ubiquiti - https:// www.ubnt.com/ download/unifi - і запустимо установку (див. рис. 3.1).

Процес мінімалістичний, не можна навіть вибрати каталог для установки контролера (до слова, він встановлюється в каталог% USERPROFILE% \ Ubiquiti UniFi).

Після завершення установки, тиснемо Finish.

У вікні налаштування тиснемо запустити браузер для управління мережею (див. рис. 3.1):

Рисунок 3.1 — Вікно налаштування браузера для налаштування мережі

При першому запуску контролер вибираємо країну і часовий пояс. (див. рис. 3.2) При необхідності в цьому ж діалоговому вікні можна запустити відновлення контролера з резервної копії (див. Зелена стрілка на скріншоті). Тиснемо Далі:

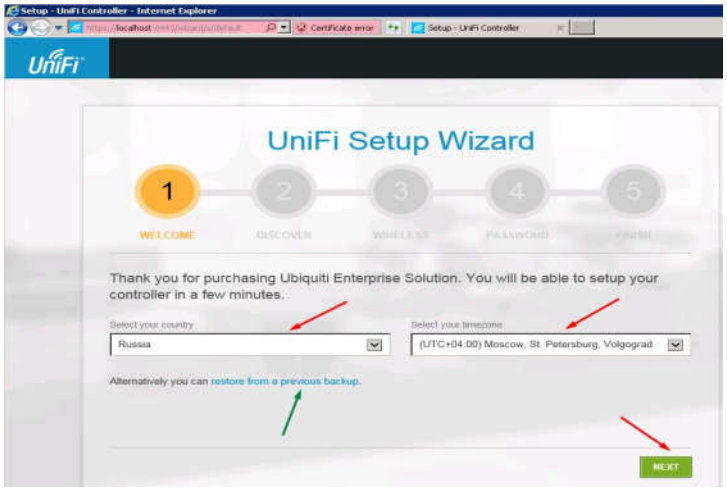


Рисунок 3.2 - Вибір країни в майстрі, чи відновлення системи.

Контролер відразу ж виявить доступні точки доступу (див. рис. 3.3), підключені до мережі (якщо точки доступу приєднані до іншого контролера, то в цьому списку вони не з'являться). Відзначаємо потрібні нам точки доступу галочками і тиснемо Далі:

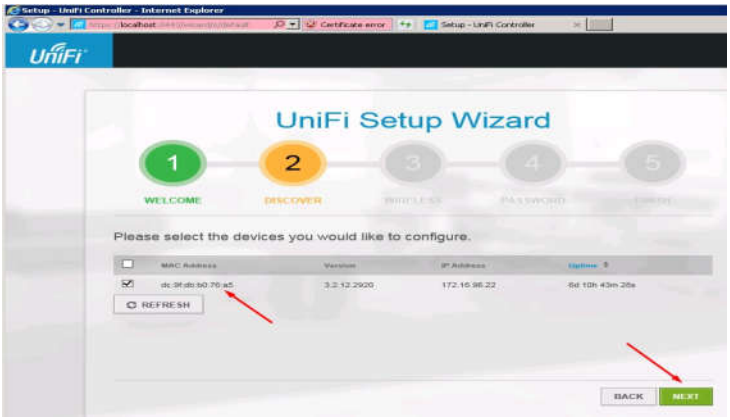


Рисунок 3.3 - Виявлена точка доступу до безпровідної мережі

На наступному кроці можна налаштувати першу WiFi мережу. Вводимо її SSID і ключ доступу. При необхідності можна відразу налаштувати гостьовий доступ (див. рис. 3.4). Тиснемо Далі:

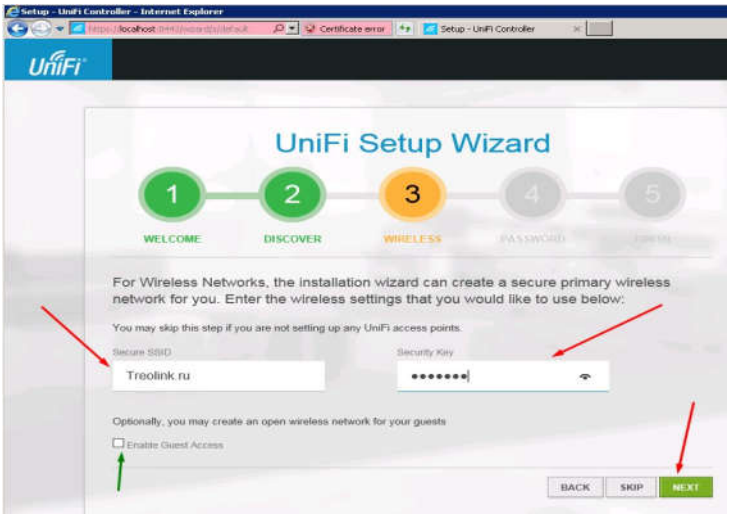


Рисунок 3.4 - Створення безпровідної мережі та ключа доступу до неї

Тепер створюємо акаунт адміністратора: вводимо назву облікового запису та пароль двічі. Далі (див. рис. 3.5):

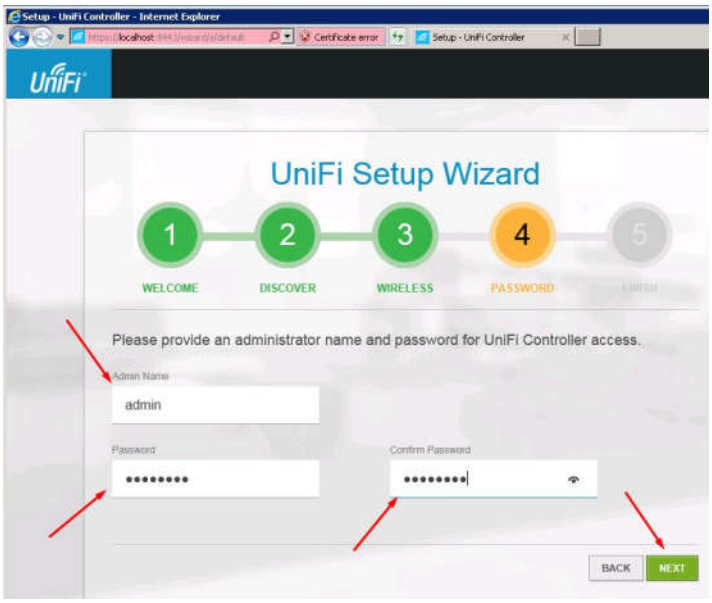


Рисунок 3.5 - Створення акаунта адміністратора

Завершуємо роботу майстра натисканням Finish :

Приєднання нових точок доступу до Ubiquiti Unifi контролер

Після завершення роботи майстра настройки, входимо в контролер під раніше створеним обліковим записом адміністратора:

І потрапляємо в панель управління контролером (див. рис.3.6):

Доприєднуєм точку доступу до контролера.

Потрібна нам точка доступу знаходиться під управлінням іншого контролера. Встановимо над нею контроль: увійдемо в меню Пристрої, клікнемо по ній, в який з'явився справа вікні властивостей натиснемо Додаткові параметри: (див. рис 3.7)

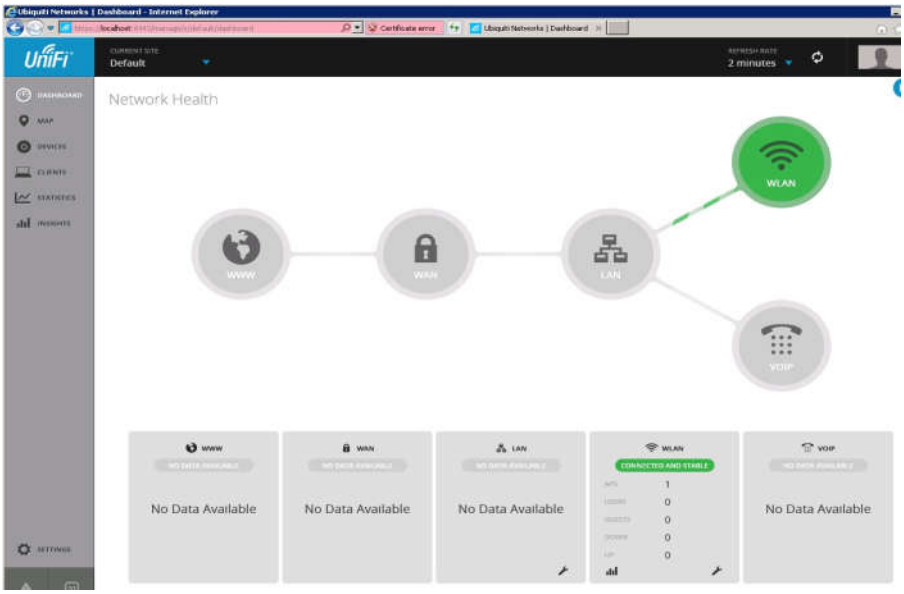


Рисунок 3.6 - Приєднання точки доступу до контролера

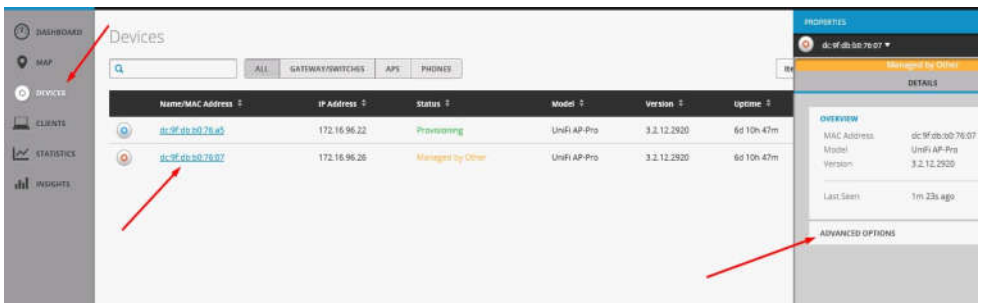


Рисунок 3.7 - Вибір додаткової точки

Введемо її логін і пароль (за замовчуванням - UBNT / UBNT) і натиснемо Прийняти: Через півхвилини точка доступу приєднається до нашого контролера (див. рис. 3.8):

Нові точки доступу, підключені до мережі, підключаються аналогічним чином, тільки для них не потрібно вводити логіни і паролі - досить просто вибрати Прийняти. Тепер між точками доступу вже працює роумінг клієнтів. WiFi-мережа вже працює, клієнти можуть переходити із зони покриття однієї точки доступу в зону покриття іншої, при цьому не втрачаючи з'єднання.

Рисунок 3.8- Приєднана нова точка доступу

3.3 Налаштування MikroTik RB4011iGS+RM

Підключення роутера MikroTik до комп'ютера

Попередньо варто відзначити, що у роутера MikroTik як порт WAN може виступати будь-який порт. Однак у заводській прошивці, як WAN порту виступає ether1 , на якому активний dhcp client . Цю особливість заводської прошивки варто враховувати при підключенні до роутера MikroTik , т.к. конфігурація визначена так, що всі вхідні з'єднання на ether1 будуть недоступні. З цього випливає те, що при первинному налаштуванні роутера MikroTik патч корд потрібно підключити в будь-який порт крім ether1 .

- Включити роутер MikroTik до електромережі;
- На порт ether1 – підключити інтернет-провайдера (WAN);
- На будь-який порт із ether2-ether5 підключити комп'ютер. Ці порти вважаються локальними (LAN).

Вхід у налаштування MikroTik RouterOS

Для налаштування роутера MikroTik найкраще скористатися утилітою Winbox , яка спеціально розроблена для керування обладнанням MikroTik .

Winbox виявить пристрій незалежно від призначеної адреси. Найчастіше це 192.168.88.1 , але й зустрічаються варіанти, коли ip адреса = «0.0.0.0». У цьому випадку підключення відбувається за адресою MAC пристрою. Крім цього Winbox відображається всі знайдені пристрої MikroTik в мережі, а також додаткову інформацію (версія прошивки, UpTime):

Запустити утилітуWinboxдля налаштування MikroTik ;

Серед списку пристроїв вибрати потрібний роутер MikroTik та натиснути кнопку Connect ;

Обліковий запис (пароль) за замовчуванням:

- користувач = "admin"
- пароль = «» (порожній)

Оскільки ручне налаштування передбачає повне налаштування роутера MikroTik з нуля, при першому підключенні необхідно повністю видалити заводське налаштування. Після натискання кнопки Remove Configuration роутер буде перезавантажено, а його налаштування видалено.

/system reset -configuration no - defaults =yes skip - backup =yes

Встановити пароль на роутер MikroTik

Першою важливою справою настроювання нового роутера MikroTik це оновлення пароля адміністратора. Випадки були різні, це пункт просто потрібно виконати.

Налаштування знаходиться в System→Users

- Натиснути + та додати новий обліковий запис адміністратора;

– Заповнити параметри: Name, Group, Password ;
– Відкрити обліковий запис admin та деактивувати кнопкою Disable

Додавання нового користувача з повними правами:

/user add name="admin-2" password="PASSWORD" group=full

деактивація старого користувача:

/user set [find name="admin"] disable="yes"

Оновлення прошивки у MikroTik RouterOS

Однією з важливих завдань при введенні в експлуатацію нового пристрою MikroTik : маршрутизатора (роутера), комутатора (світка) або точки доступу WiFi це оновлення прошивки. Найчастіше це мало рекомендований характер, але нещодавній інцидент з “ back door ” у категорії l ong-term вказав на те, що актуальність прошивки у пристроях MikroTik має критичний характер.

Налаштування знаходиться в System→Packages

– Натиснути кнопку Check For Updates ;
– Вибрати Channel = long term;
– Завантажити та встановити прошивку на MikroTik кнопкою Download&Install.

Дії в кнопці Download&Install зроблять завантаження обраної редакції прошивки та автоматичне перезавантаження роутера MikroTik . Установка буде здійснена в момент завантаження. Не вимикайте роутер MikroTik до повного перезавантаження та забезпечте стабільне живлення електромережі під час оновлення прошивки.

Налаштування локальної мережі MikroTik LAN

В основі роботи локальної мережі (LAN) на роутері MikroTik знаходиться Bridge – програмне об'єднання портів у свитч. До складу Bridge може входити будь-яка послідовність портів роутера MikroTik , а якщо туди додати всі порти – роутер стане точкою доступу WiFi або комутатором.

Варто враховувати, що таке об'єднання керується CPU . Цей факт важливий при значних навантаженнях на CPU .

Налаштування LAN на роутері MikroTik складається з наступних ключових етапів:

Об'єднання всіх локальних портів в Bridge ;

Налаштування локальної IP- адреси для роутера MikroTik ;

Налаштування сервера DHCP .

Налаштування MikroTik Bridge

Налаштування знаходиться в основному меню Bridge→Bridge

- Натиснути + та додати новий Bridge;
- Присвоїти Name для вибраного Bridge ;
- Натиснути кнопку Apply та скопіювати значення MAC Address у Admin MAC Address

/interface bridge add admin-mac=74:4D:28:68:FE:3C auto-mac=no name=bridge1

Додавання портів MikroTik до Bridge

Налаштування знаходиться в основному меню Bridge→Ports

- Натиснути + та додати новий Port ;
- Вибрати відповідні значення у параметрах: Interface, Bridge ;
- Повторіть аналогічні дії для всіх інтерфейсів, які визначені як LAN .

/interface bridge port add bridge=bridge1 hw=yes interface=ether2

/interface bridge port add bridge=bridge1 hw=yes interface=ether3

/interface bridge port add bridge=bridge1 hw=yes interface=ether4

/interface bridge port add bridge=bridge1 hw=yes interface=ether5

/interface bridge port add bridge=bridge1 interface=wlan1

/interface bridge port add bridge=bridge1 interface=wlan2

Створити Interface List LAN

Угруповання інтерфейсів у напрямку, що допомагає описувати налаштування більш загальними правилами. Це досить зручно, коли два і більше інтерфейсу є LAN або WAN і для них потрібно застосувати однакові правила Firewall , NAT .

Назва Interfaces List можна задавати довільне, воно не впливає і не перетинається ні з яким налаштуванням. Зазвичай:

LAN – локальна мережа;

WAN – інтернет-інтерфейс.

Налаштування знаходиться в Interfaces→Interfaces List→List

- Натиснути + та додати новий Interfaces List ;
- Заповнити Name = LAN .

Додати Bridge до Interface List LAN

Налаштування знаходиться в Interfaces→Interfaces List

- Натиснути + та додати новий Interfaces List Member ;
- Вибрати List = LAN та Interface = bridge1 .

Таким чином Interfaces List був доданий bridge1 і якщо в якихось налаштування роутера MikroTik вказати Interfaces List = LAN , то будуть використовувати всі інтерфейси, які до нього додані. В даному випадку це bridge1 .

Призначення локальної IP-адреси

Після додавання портів в Bridge потрібно призначити статичну IP адресу і правильніше за все це вказати як інтерфейс створений bridge1 . З цього моменту будь-яке налаштування адресації або маршрутизації в роутері MikroTik буде здійснюватися через bridge1 .

Налаштування знаходиться в IP→Addresses

- Натиснути + та додати нову IP адресу;
- Заповнити параметри: Address, Interface .

При заповненні IP -адреси важливо вказати маску підмережі. Ця часта помилка може призвести до відсутності відгуку від роутера MikroTik . При цьому значення Network заповниться автоматично.

Встановлення IP- адреси на вибраний інтерфейс

/ip address add address=192.168.0.1/24 interface=bridge1 network=192.168.0.0

Налаштування DCHP сервера в MikroTik

DHCP сервер займається видачею IP адрес всім пристроям, які відправляють відповідний запит. Це незамінна опція при налаштуванні WiFi на роутері MikroTik , але також полегшує обслуговування локальної мережі в цьому питанні.

Налаштування складатиметься з 3-х пунктів:

Визначення діапазону призначених IP адрес

Налаштування знаходиться в IP→Pool

- Натиснути + і додати новий IP Pool ;
- Заповнити параметри: Name, Addresses .

Діапазон Addresses містить IP адреси для всіх клієнтів роутера MikroTik і часто набуває значення або як показано на зображенні або 192.168.0.100-192.168.0.254 . Це дасть можливість вказувати статичні IP-адреси для: сервера, принтера, відеореєстратора, IP камери і т.д.

/ip pool add name=pool-1 ranges=192.168.0.2-192.168.0.254

Завдання мережних налаштувань для клієнта

Налаштування знаходиться в IP→DHCP Server→Networks

- Натиснути + та додати нову DHCP мережу;
- Заповнити параметри: Address, Gateway, Netmask, DNS Server .

Netmask = 24 - це еквівалент звичному значенню 255.255.255.0 ;

Gateway - шлюз за замовчуванням (роутер MikroTik);

DNS Servers – DNS сервер, який буде видано клієнту. В даному випадку це також роутер MikroTik .

/ip dhcp-server network add address=192.168.0.0/24 dns-server=192.168.0.1 gateway=192.168.0.1 netmask=24

Загальні налаштування сервера MikroTik DCHP

Налаштування знаходиться в IP→DHCP Server→DHCP

- Натиснути + та додати новий DHCP сервер;
- Заповнити параметри: Interface, Address Pool, Lease Time .

Lease Time – час оренди IP- адреси. За замовчуванням час оренди IP адреси становить або 10 або 30 хвилин, це може влити на роботу

смартфонів (Android та Iphone), які в режимі сну можуть повторно не надіслатизапит DHCP . Така ситуація може спровокувати відключення пристрою від WiFi і виправити лише при повторному підключенні;

Add ARP For Leases — додає MAC адресу пристрою до таблиці ARP , якому було видано IP адресу. Можна використовувати як блокування статичних IP . Без присутності відповідного MAC у таблиці ARP пакети з пристрою не будуть оброблятися.

/ip dhcp-server add address-pool=pool-1 disabled=no interface=bridge1 lease-time=8h name=DHCP-Server

Налаштування MikroTik DNS

У рамках цієї інструкції з налаштування роутера MikroTik буде розглянута конфігурація, коли сам роутер виступає як сервер DNS . Це має кілька переваг:

DNS записи кешуються на локальний роутер MikroTik , доступ якого в рази швидше ніж до DNS серверу провайдера;

Якщо до роутера підключено 2 провайдери, не виникатиме конфліктів щодо доступу до DNS серверів 1-го або 2-го провайдера. DNS сервер один - роутер MikroTik .

Налаштування знаходиться в IP→DNS

Для такої конфігурації сервера DNS потрібно:

- Задати зовнішні DNS сервери у параметрі Servers . Це може бути DNS сервера Google : 8.8.8.8 та 8.8.4.4 або Cloudflare : 1.1.1.1 та 1.0.0.1;
- Активувати параметр Allow Remote Requests . Це дозволить зовнішнім запитам звертатися до роутера MikroTik як до сервера DNS ;
- Звернути увагу на Cache Size . У великих мережах (від 100 вузлів) його варто збільшити у 2 чи 3 рази. За промовчанням його значення = 2048Кб.

DNS сервера Google

/ip dns

set allow-remote-requests=yes servers=8.8.8.8,8.8.4.4

АБО

DNS сервера Cloudflare

/ip dns set allow-remote-requests=yes servers=1.1.1.1,1.0.0.1

Використання загальнодоступних серверів DNS досить популярна опція в ситуаціях, коли провайдер блокує якісь сайти по DNS . У цьому випадку Google та Cloudflare DNS є лідерами в аналогічних рішеннях, надаючи безвідмовний доступ до своїх серверів DNS .

Настроювання Інтернету на роутері MikroTik

Для налаштування інтернету на роутері MikroTik потрібно зробити дві дії:

- визначити тип підключення на певному порту (куди вставлено провайдер);
- активувати функцію NAT (masquerade).

Налаштування DHCP client у MikroTik

Це найпоширеніший тип підключення інтернету на роутерах MikroTik . На вказаний порт(ether1) будуть надходити налаштування від інтернет-провайдера. DHCP клієнт не тільки полегшує налаштування інтернету, але й служить індикатором, коли послуга відсутня на лінії (не працює інтернет), але також дозволяється додати скрипт, який буде виконуватися при зміні значення Status.

Налаштування MikroTik NAT

NAT це механізм, який дозволяє перетворювати IP- адреси для транзитних пакетів. Саме NAT є основним налаштуванням, яке звичайний пристрій MikroTik перетворює на роутер.

Налаштування знаходиться в IP→Firewall→NAT

- Натиснути + і додати нове правило NAT ;
- Встановити Chain = srcnat ;
- Out Interface List = WAN ;
- Action = Masquerade .

Masquerade це основне правило NAT для роботи інтернету на роутері MikroTik .

правило для роботи інтернету

/ip firewall nat add action=masquerade chain=srcnat ipsec-policy=out,none out-interface-list=WAN

Якщо в інтернет з'єднання виділена IP адреса, то рекомендується встановити:

- Action = src-nat ;
- To Addresses = Зовнішня IP-адреса.

Налаштування Mikrotik FireWall

Firewall у роутері MikroTik є одним із найважливіших компонентів. Неправильно налаштований Firewall може призвести до обмеженого доступу до роутера MikroTik , а його відсутність ставить під загрозу всю мережеву інфраструктуру.

Firewall в обладнанні MikroTik працює за принципом зверху донизу. Оброблюваний пакет порівнюється з кожним правилом (Firewall Rule) і якщо не підпадає під умови правила, то досягає кінця Firewall і обробляється принципом "що не заборонено, то дозволено". У цій схемі важливо враховувати, що якщо Firewall на роутері MikroTik не міститиме правил заборони (Action = drop), такий роутер буде відкритий (уразливий) з інтернету.

Налаштування знаходиться в IP→Firewall

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

/ip firewall filter add action=accept chain=forward connection-state=established,related

/ip firewall filter add action=accept chain=forward in-interface-list=LAN

/ip firewall filter add action=accept chain=input in-interface-list=LAN

/ip firewall filter add action=accept chain=input protocol=icmp in-interface-list=WAN

/ip firewall filter add action=drop chain=input in-interface-list=WAN

/ip firewall filter add action=drop chain=forward connection-nat-state=!dstnat in-interface-list=WAN

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

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

Налаштування MikroTik VPN сервера L2TP

VPN сервер є популярним засобом для віддаленого підключення одного ПК(або 100 ПК) до центрального вузла. Реалізація такого сервісу є маса, але на MikroTik працює швидко та без інцидентів через недоступність. У прикладі наведено випадок L2TP як захищеного засобу передачі трафіку.

Для VPN клієнтів краще створити окрему підмережу, це додасть більше можливостей обмеження доступу між VPN клієнтами і локальною мережею, а також у самій маршрутизації.

Додавання нової підмережі

Налаштування знаходиться IP→Pool

/ip pool add name=LAN-Ip-Pool ranges=192.168.10.100-192.168.10.150

Налаштування VPN сервера L2TP (на сервері)

Налаштування знаходиться PPP→Profile

Попередньо потрібно задати параметри мережі для VPN клієнтів

/ppp profile

add change-tcp-mss=yes dns-server=192.168.10.1 local-address=\

192.168.10.1 name=l2tp remote-address=pool-1 use-encryption=yes

Активація сервера VPN L2TP

Налаштування знаходиться PPP→Interface→L2TP Server

/interface l2tp-server server

set authentication=mschap2 default-profile=l2tp enabled=yes \

ipsec-secret=mikrotik-config.ukr use-ipsec=required

Use-ipsec=required змусить vpn клієнта обов'язково використовувати IpSec;

Use-ipsec=yes (за замовчуванням) проставляє вибір vpn клієнту використання IpSec, тобто. може не використовуватись.

Створення облікового запису для клієнта VPN

Цей обліковий запис буде використовувати VPN клієнт для віддаленого підключення до VPN серверу.

Налаштування знаходиться PPP→Interface→Secrets

/ppp secret

add name=user1 password=user1 profile=l2tp

Дозвіл FireWall для підключення VPN клієнтів

Налаштування знаходиться IP→Firewall

/ip firewall filter

add action=accept chain=input comment="Port Access" dst-port=500,1701,4500 \

in-interface=WAN-ether1 protocol=udp

Налаштування інтернету для VPN клієнтів L2TP у MikroTik

Це питання буде винесено за межі цієї статті, т.к. відноситься до додаткових сервісів для VPN клієнтів. Таких сервісів може бути безліч і всі вони мають індивідуальний характер (для тих, хто шукає: потрібно налаштувати і дозволити DNS запити і Masquerade).

Розширені налаштування Mikrotik RouterOS: два зовнішні канали від одного провайдера Ця стаття написана як відповідь на запитання наших відвідувачів. До статей про підключення двох зовнішніх каналів зв'язку та їх балансування ми отримали чимало коментарів на сайті та питань до менеджерів. Зокрема, багато хто цікавився можливістю налаштування та балансування двох каналів, від одного провайдера. І щоб заповнити цю прогалину, нижче ми розповімо про основні нюанси, пов'язані з цим завданням. Головною проблемою, яка викликає питання у більшості користувачів, є -

однаковий Gateway на двох каналах, тому, прописуючи в маршрутизації два або більше рази один і той же шлюз, у результаті, ви не отримуєте балансування, тому що маршрутизатор пов'язує його з першим фізичним, що попався. інтерфейс, на якому він доступний. Такий варіант хороший, коли другий канал буде резервним. Маршрутизатор легко вибере перший з доступних, і направить трафік через нього. Але він не годиться для одночасного використання двох каналів відразу.

У нас є маршрутизатор Mikrotik, і 2 незалежні зовнішні канали, від провайдера, підключені до фізичних інтерфейсів ether1 і ether5. Інтерфейси ether2-ether4 відведені під локальну мережу. Підключаємося до маршрутизатора за допомогою фірмової утиліти Winbox і насамперед налаштовуємо підключення до провайдера. Так як вибраний нами постачальник послуг, використовує протокол динамічного налаштування вузла, або попросту кажучи DHCP, то ми налаштовуємо DHCP Client в розділі меню IP (див.рис.3.9).

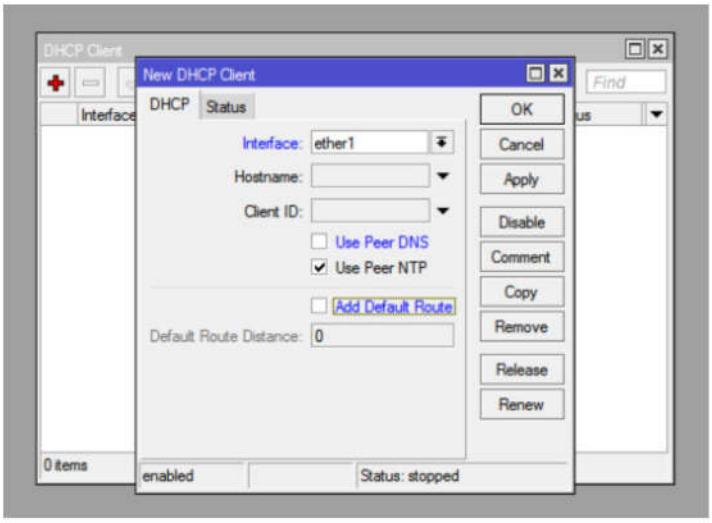


Рисунок 3.9 — Вікно налаштування інтерфейсу DHCP Client

За допомогою кнопки "+", додаємо нового клієнта, і у вікні, Interface - вибираємо перший інтерфейс, до якого підключений один з

кабелів провайдера. Галочки Use Peer DNS та Add Default Route - прибираємо.

Зберігаємо запис кнопкою OK, і повторюємо цю процедуру, для другого інтерфейсу. У результаті, у нас має бути два записи, де ми побачимо видані нам IP адреси (див.рис.3.10).

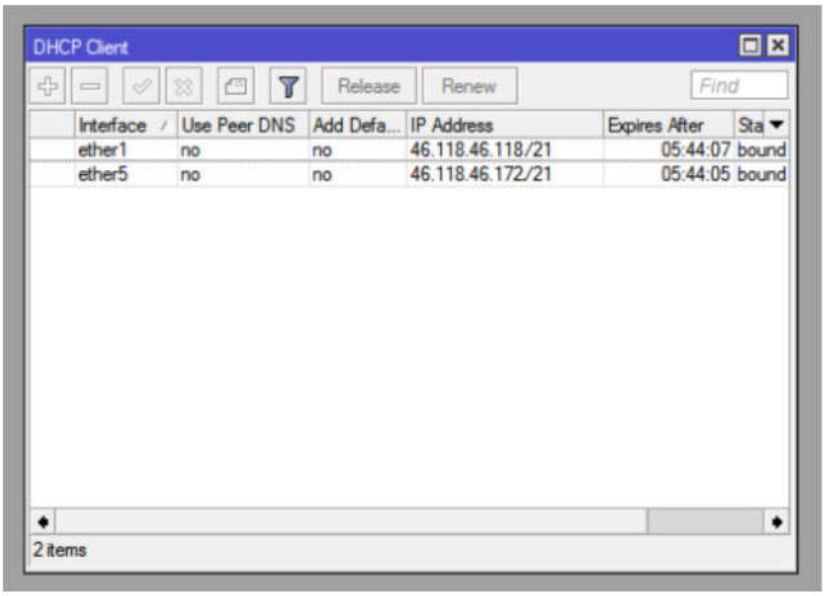


Рисунок 3.10 — Вікно з виданими нам IP адресами

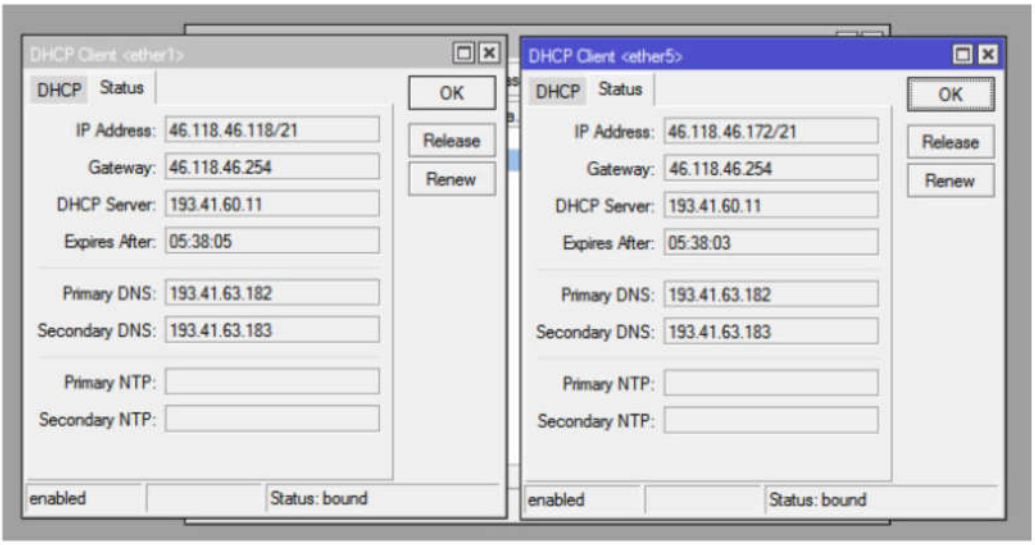


Рисунок 3.11 — Вікно з інформацією про налаштовувані інтерфейси

Тепер, нам потрібно подивитися дані на цих інтерфейсах (див.рис.3.11), і отримати інформацію про їх шлюзи, і DNS сервери, для подальшого налаштування. Для цього відкриваємо властивість кожного запису і переходимо на вкладку Status.

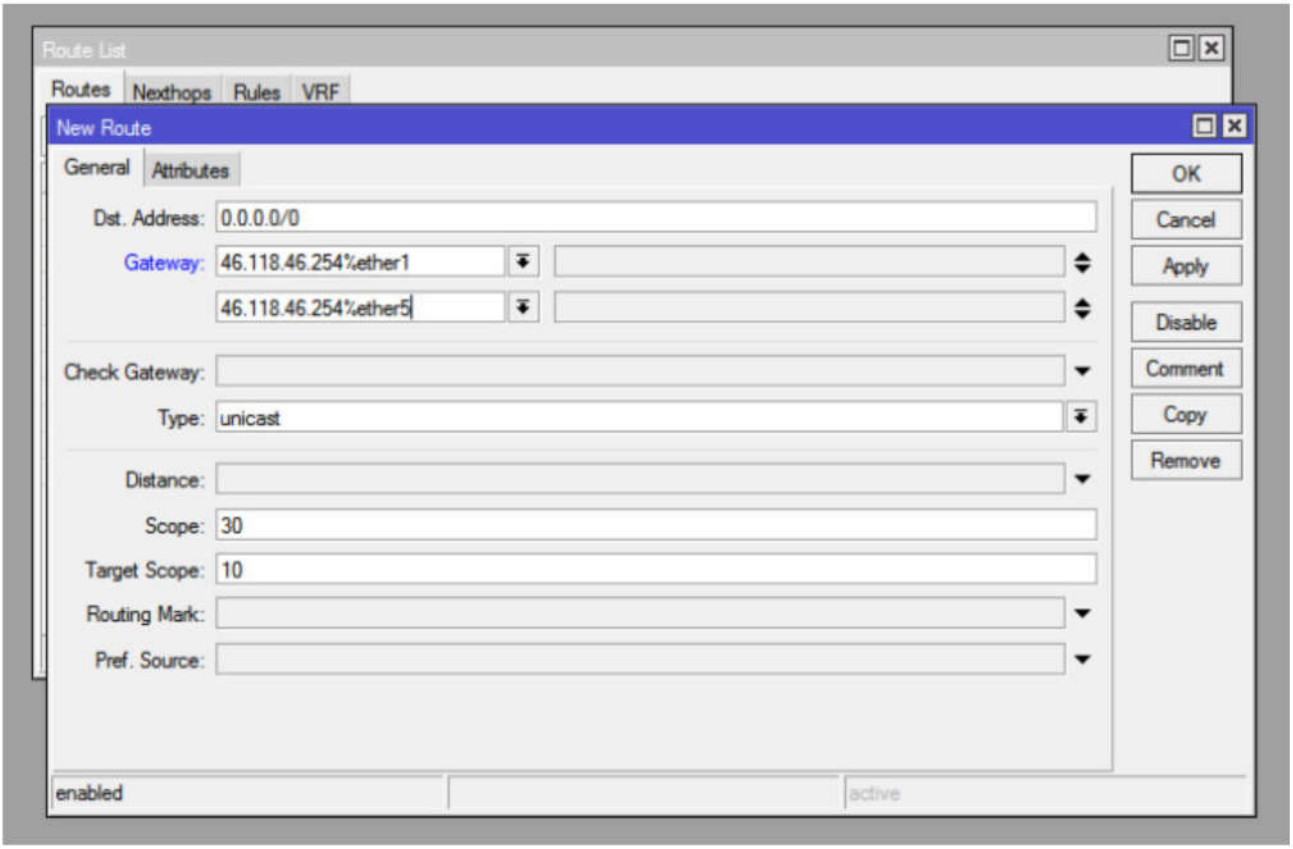


Рисунок 3.12 — Вікно налаштування маршрутизації

Тут ми бачимо, що Gateway та DNS сервери, і там і там однакові. Запам'ятовуємо чи записуємо ці дані. Переходимо до налаштування маршрутизації (див.рис.3.12). Відкриваємо розділ меню IP - Routes та створюємо нове правило, за допомогою кнопки “+”. Тут як Dst.Address - 0.0.0.0/0, а для шлюзів Gateway використовуємо комбінацію виду xx.xx.xx.xx%ether1. Як можна зрозуміти, ми вказуємо IP адресу шлюзу провайдера та фізичний інтерфейс, через який має йти до нього маршрут.

Якщо у вас канали з різною пропускною спроможністю, то ви повинні в пропорційному порядку, створити потрібну кількість Gateway, для кожного фізичного інтерфейсу.

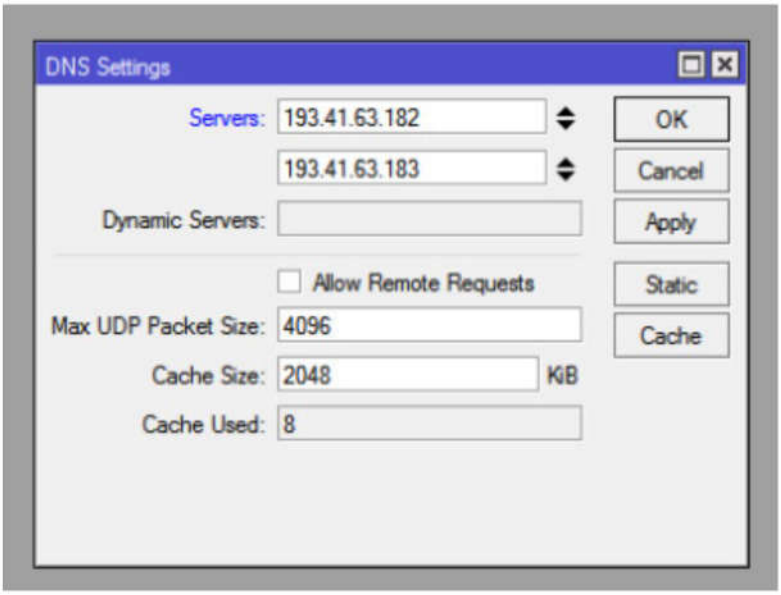


Рисунок 3.13 — Вікно налаштування DNS

Далі нам потрібно налаштувати DNS.

Для цього, переходимо в розділ меню IP - DNS, де в полях Servers, вказуємо DNS сервера провайдера, або можна використовувати публічні сервери доменних імен, на зразок 8.8.8.8 і 8.8.4.4. (див.рис.3.13)

Все, що нам залишилося зробити, це дозволити доступ з локальної мережі, в Інтернет.

Для цього ми повинні налаштувати NAT. У розділі меню IP - Firewall ми переходимо на вкладку NAT і додаємо нове правило за допомогою кнопки “+”.

На вкладці General, вибираємо Chain - scrnat, а як Out.Interface - ether1.

На вкладці Action, для параметра Action, ставимо — masquerade.

Зберігаємо правило, і створюємо таке саме, тільки для другого інтерфейсу. Наприклад, у нас це ether5, як ми обговорювали на самому

початку. Далі, відповідно до своїх потреб, ми налаштовуємо вже локальну мережу, Firewall та все необхідне. При цьому через якийсь час на тій же вкладці NAT, де ми створювали правила, можна подивитися результат нашої роботи та правильність балансування.

3.4 Встановлення та налаштування TrueNAS

Системні вимоги для операційної системи TrueNAS:

- 64-розрядний процесор Intel або AMD;
- 8 Гб оперативної пам’яті;
- окремий SSD або HDD як мінімум на 16 Гб для встановлення та роботи самої TrueNAS;
- жорсткі диски безпосередньо для самого сховища.

Для сховища бажано як мінімум 2 HDD, щоб забезпечити відмовостійкий RAID 1. І бажано, щоб диски були однакового об’єму, ще краще – щоб всі однієї моделі.

Підключати до NAS можна будь-який об’єм дисків. Але не забуваємо, що в режимі BIOS Legacy видимість кожного з дисків обмежена його максимальним розміром 2,2 Тб. Щоб цього обмеження не було, в BIOS повинен бути активним режим UEFI.

Дистрибутив TrueNAS поставляється в звичайному образі установки ISO. Скачати цей образ можна на офіційному сайті операційної системи.

Далі ISO-образ необхідно записати на завантажувальну флешку. При створенні завантажувальної флешки з TrueNAS не забуваємо про режим BIOS – Legacy або UEFI. Флешка повинна бути адаптована до режиму BIOS.

Встановлення TrueNAS

Підключаємо до NAS тимчасово монітор і клавіатуру. Запускаємо пристрій з флешки установки TrueNAS. Процес установки примітивний,

працює тільки клавіатура. Вибирати пункти меню та різні варіанти необхідно стрілками навігації. Підтверджувати вибір, тобто тиснути «Ok» – клавішею Enter.

На початковому етапі тиснемо Enter, щоб запустити перший пункт меню «Boot TrueNAS Installer», тобто установку операційної системи.

Вибираємо перший пункт «Install/Upgrade». тиснемо Enter.

Перед нами виникне перелік жорстких дисків пристрою. Вибираємо той окремий, на який потрібно встановити TrueNAS. Відмічаємо його клавішею пробілу. тиснемо Enter.

Далі йде попередження про стирання даних на обраному диску. Вибираємо «Yes».

На етапі створення облікового запису адміністратора NAS необхідно задати пароль. Ім’я нам дається дефолтне – стандартне для UNIX-систем root. Воно незмінне. Вводимо пароль, підтверджуємо його, тиснемо Enter.

Обираємо режим BIOS, під який буде підлаштована TrueNAS. «Boot via UEFI» – це UEFI, а «Boot via BI0S» – це Legacy. UEFI краще.

Етап створення файлу підкачки розміром 16 Гб. тиснемо «Create swap».

Далі TrueNAS встановиться. тиснемо Enter.

Необхідно перезапустити пристрій. Обираємо пункт «Reboot System». тиснемо Enter.

Виймаємо завантажувальну флешку. Після того, як TrueNAS повністю завантажиться, побачимо внутрішню локальну IP-адресу пристрою NAS. За допомогою цієї адреси будемо віддалено підключатися для управління пристроєм.

Вище можна звернути увагу на пункти мережевих налаштувань пристрою. Але вони будуть потрібні в поодиноких випадках, якщо NAS не буде видний в мережі. У більшості ж випадків, коли локальна мережа забез-

печується роутером, всі необхідні мережеві налаштування NAS отримає за замовчуванням.

Все, після цього монітор та клавіатура NAS не потрібні. Ми переходимо до комп'ютеру для віддаленого управління сховищем.

Налаштування TrueNAS

Далі на комп'ютері необхідно налаштувати TrueNAS, а, відповідно, налаштувати сховище NAS. Віддалене управління ним здійснюється через веб-інтерфейс. І нам для цієї задачі потрібен лише браузер. В адресній стрічці браузеру вводимо IP-адресу NAS. тиснемо Enter.

З'явиться форма віддаленого підключення до TrueNAS. Авторизуємося – вводимо логін root і той пароль, що ми задавали при створенні облікового запису адміністратора NAS. тиснемо «Увійти».

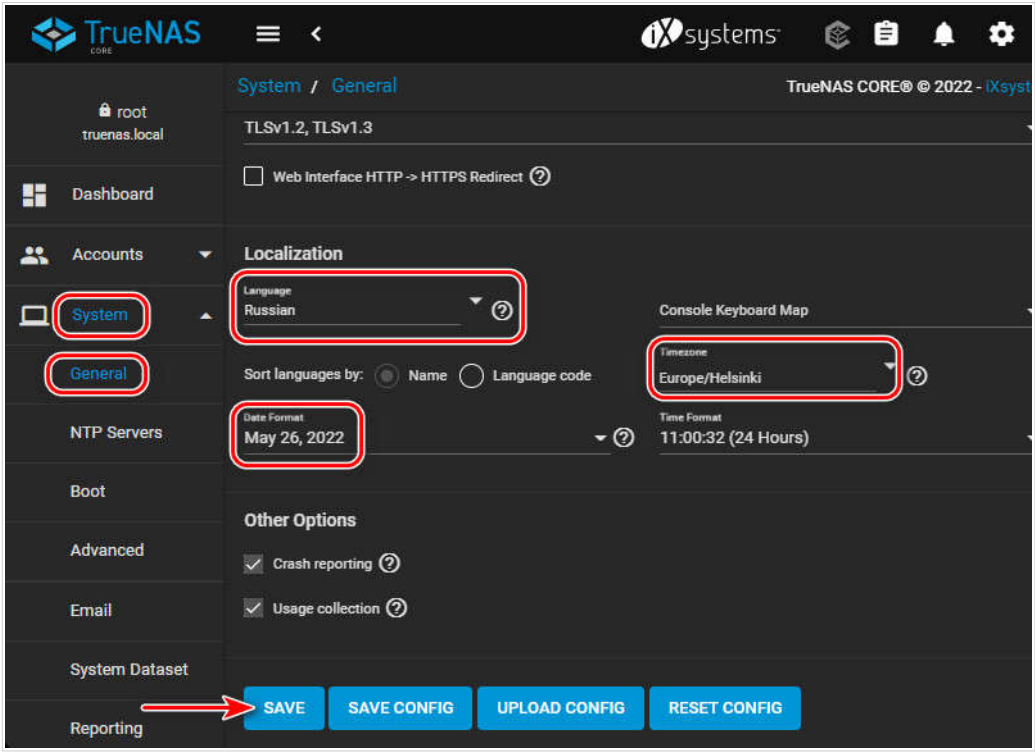


Рисунок 3.14 — Вікно налаштування локалізації

Локалізація. Побачимо, власне, операційну систему TrueNAS. Вона буде на англійській мові. І першим кроком вирішимо питання з локалі-

зацією. TrueNAS передбачає українську мову в налаштуваннях локалізації, проте, на жаль, фактично така локалізація не здійснена. Можемо залишити англійську, або обрати іншу зрозумілу мову (див.рис. 3.14).

В розділі «System → General» обираємо мову. Можемо обрати також формат дати і часовий пояс.

Створення сховища

Другим кроком створимо сховище NAS з дисків, що назначені для нього. В розділі «Сховище → Пули» тиснемо «Добавити»(див.рис. 3.15).

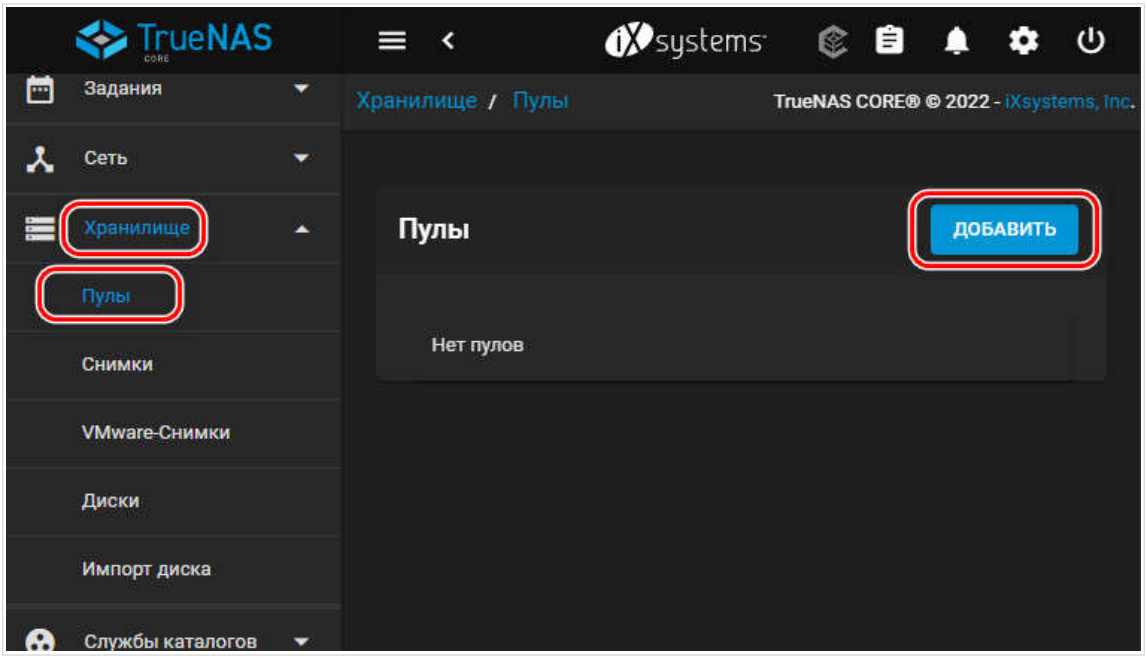


Рисунок 3.15 — Вікно створення пулу дисків

Створимо пул дисків. Пункт створення пулу встановлений за замовчуванням. тиснемо «Створити пул».

Даємо назву пулу. Ставимо галочку опції «Show disks with non-unique serial numbers». В блоці відображення дисків зліва «Доступні диски» відмічаємо галочками диски, які ми становимо в пул. В нашому випадку це 2 однакових диски, на базі яких ми створимо програмний відмовостійкий RAID 1.(див.рис. 3.16) Далі тиснемо стрілочку вправо.

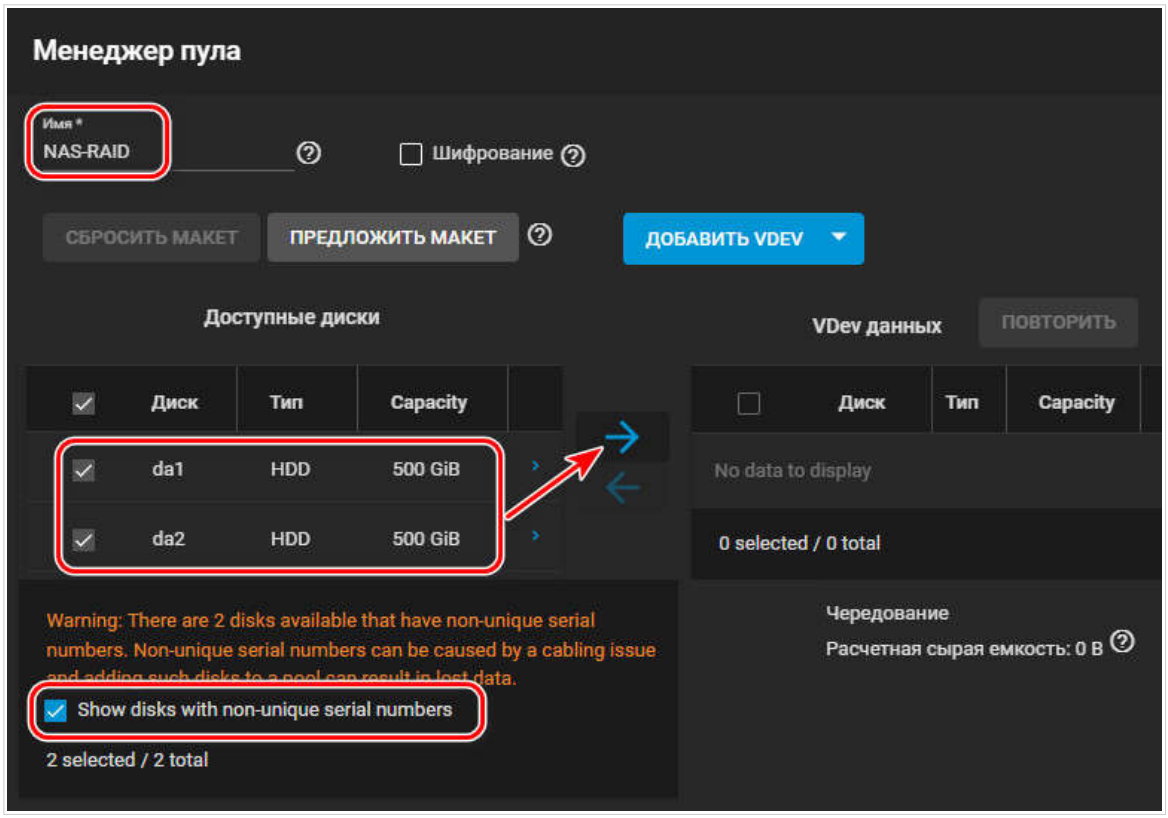


Рисунок 3.16 — Вікно вибору дисків для пулу

Вона перемістить диски в блок справа «VDev даних», тобто в пул. Тут ми знову ставимо галочки на дисках. І нижче з випадаючого списку обираємо для них тип сховища, тобто дисковий масив.

TrueNAS пропонує такі варіанти:

– Чергування (Stripe) – це RAID 0, масив без відмовостійкості, з подвоєною швидкістю обробки даних;
– Дзеркало (Mirror) – це RAID 1, базовий відмовостійкий масив з клонуванням даних на другому диску;
– RAID-Z – притаманний файловій системі ZFS відмовостійкий масив, удосконалений аналог RAID 5;
– RAID-Z2 – притаманний файловій системі ZFS відмовостійкий масив, удосконалений аналог RAID 6.

Додавання загальної папки NAS

Тепер організуємо загальні ресурси NAS – загальну папку, яка буде доступна на комп'ютерних та мобільних пристроях локальної мережі. В кінці таблиці пулу є меню, тиснемо його. Вибираємо «Добавити набір даних».

Даємо папці назву. Тип ресурсу вказуємо «SMB». тиснемо «Відправити».

Створення користувача NAS

У нас є обліковий запис адміністратора NAS для керування пристроєм root. Але потрібен ще обліковий запис користувача NAS – той за допомогою якого ми будемо підключатись до загальної папки (чи інших ресурсів у подальшому). Заходимо у розділ «Облікові записи – Користувачі». тиснемо «Добавити».

Вносимо ім'я користувача, пароль та підтверджуємо його.

Нижче можемо на майбутнє встановити допоміжні групи для цього користувача. Наприклад, ftp. Ставимо галочку облікового запису Microsoft, це потрібно для Windows. тиснемо «Відправити».

Такі облікові записи потрібно створити для кожного користувача NAS. Щоб кожен міг індивідуально зі свого комп'ютеру чи іншого пристрою користуватись ресурсами сховища.

Загальний доступ до NAS

І останній крок в рамках базового налаштування TrueNAS – це відкриття загального доступу до загальної папки для Windows за допомогою служби Samba (SMB). Це програмне забезпечення для взаємодії Windows та Unix-систем, адже TrueNAS базується на останній. В розділі «Загальний доступ → Ресурси Windows (SMB)» тиснемо «Добавити».

Розкриваємо шлях до нашої загальної папки, клікаємо її. тиснемо «Відправити».

Система запросить включення служби SMB. тиснемо «Включити службу».

І ця папка з’явиться в числі ресурсів Samba. Налаштуємо контроль доступу ACL для цієї папки. В її меню тиснемо «Edit Filesystem ACL».

Для користувача-адміністратора NAS root даємо всі права для всіх груп (права на читання та запис даних). тиснемо «Select an acl preset».

Далі вказуємо параметр ACL «Open». тиснемо «Продовжити».

На цьому все.

Підключення NAS в Windows

Щоб працювати з NAS в середовищі Windows, сховище потрібно підключити. Вводимо в адресну строку провідника IP-адресу NAS через подвійний слеш.

Авторизуємось з використанням облікового запису користувача NAS. Можемо встановити галочку запам’ятовування авторизації. тиснемо «Ок».

Після цього NAS і його загальні ресурси будуть доступні нам в блоці провідника «Мережа».

А ще можемо кожну папку NAS підключити як окремий диск зі своєю буквою. На об’єкті «Цей ПК» тиснемо контекстне меню. Вибираємо «Підключити мережевий диск». Але у Windows 11 спочатку потрібно вибрати «Показати додаткові параметри».

Вибираємо букву диску для NAS. За допомогою кнопки огляду вказуємо шлях до папки. тиснемо «Готово».

Після цього папка буде доступна в провіднику як окремий диск і як мережеве розташування.

3.5 Інструкція з використання тестових наборів та тестових програм

Для діагностики мережі використовуються команди PING і TRACERT.

Якщо є підозра, що відсутній зв’язок з деяким вузлом мережі, то команда PING (Packet Internet Groper)– перша, до якої необхідно звернутись. З допомогою цієї команди, можна перевірити правильність встановлення TCP/IP-з’єднання на локальному (віддаленому) комп’ютері.

Основна функція цієї утиліти – перевірка наявності фізичного зв’язку між двома системами в мережі. Для обміну пакетами з віддаленою системою, використовується протокол ICMP. Віддалена система відсилає пакети назад, і таким чином, коло замикається. Команда PING видає інформацію про те, скільки часу виконувалась ця операція, а також повідомляє про помилки, якщо пакети не повернулись.

Синтаксис команди в операційних системах сімейства Windows має наступний вигляд:

ping [ключі] адреса (ім’я) вузла

Ключі:

- t – продовжує відправку запитів , доки робота не буде перервана командою Ctrl-C;
- a – дозволяє використовувати імена вузлів замість IP-адрес;
- n число – вказує кількість exo запитів для відправки ;
- l довжина – вказує довжину exo – запитів;
- f – забороняє фрагментування пакету, визначає, чи пристрій змінював розмір пакету;
- i час – встановлює час життя пакету (Time to Live -TTL) відправляємих пакетів;
- v тип – встановлює тип обслуговування (TOS)
- r число – відображає шляхи для заданого числа переприйомів;
- s число – відмічає час для вказаного числа переприйомів;
- j список вузлів – маршрутизація пакетів через вказані вузли. Послідовні вузли можуть бути розділені шлюзами;

– k список вузлів - маршрутизація пакетів через вказані вузли. Послідовні вузли не можуть бути розділені шлюзами.
– w час – встановлює час очікування відповіді в мілісекундах.

Команда TRACERT також використовує протокол ICMP для визначення всіх пристроїв, через які проходить пакет на шляху до вузла призначення.

За допомогою цієї команди, можна отримати досить обширну інформацію про те, як функціонує мережа.

Має наступний синтаксис :

tracert [ключі] ім’я вузла

Ключі :

– d – використовувати імена вузлів замість IP адрес;
– h максимальне число переприйомів – максимально допустиме число переприйомів для досягнення мети;
– j список вузлів - маршрутизація пакетів через вказані вузли. Послідовні вузли можуть бути розділені шлюзами. Вільний вибір шляху серед систем у вказаному списку;
– w час – встановлення часу очікування в мілісекундах.

Існує також команда IPCONFIG, яка використовується для отримання інформації про настройку TCP/IP сервера або робочої станції Windows NT.

3.6 Основи моделювання в CISCO PACKET TRACER

Cisco Packet Tracer - це багатофункціональна програма моделювання мереж, яка дозволяє експериментувати з поведінкою мережі і оцінювати можливі сценарії.

На рисунку 3.17 показане головне вікно програми.

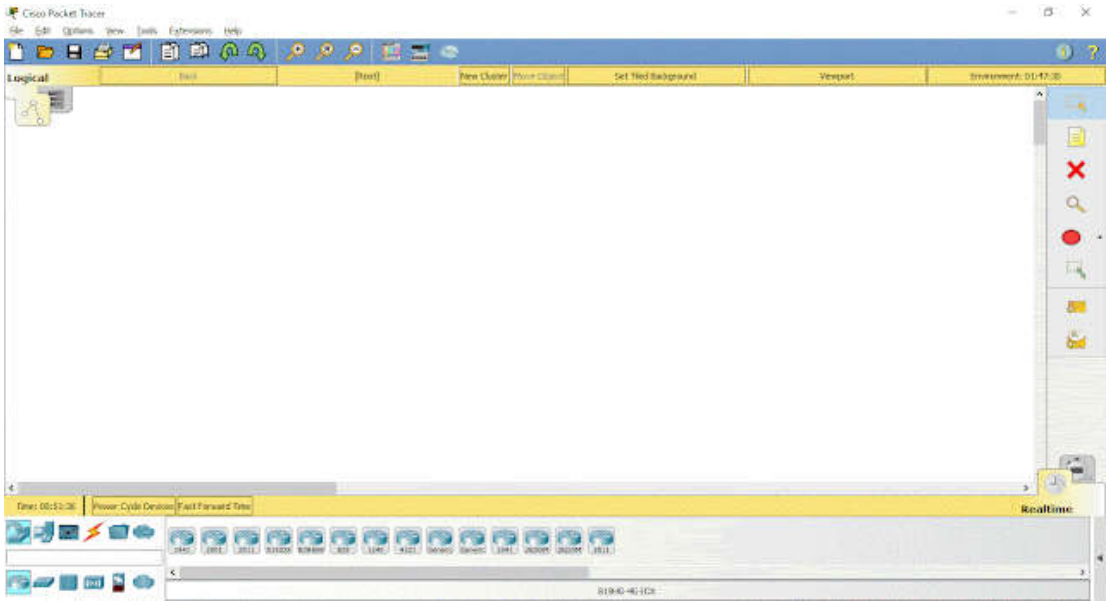


Рисунок 3.17 — Головне вікно програми Cisco Packet Tracer

У верхній частині знаходиться головне меню. Воно містить такі кнопки: File, Edit, Options, View, Tools, Extensions, Help.

Під головним меню розташовується панель з найпотрібнішими і найбільш часто вживаними елементами головного меню.

Цими елементами є: створити файл, відкрити файл, зберегти, надрукувати, майстер активності, копіювати, вставити, скасувати попередню дію, виконати попередню дію, збільшити зображення, відновити зображення, зменшити зображення, панель малювання, діалог пристроїв. Також в правому кутку видно знак ! та ?, що означають «Показати інформацію про мережу» та «Відкрити довідку в браузері відповідно».Категорія File містить стандартні пункти, такі як: створити новий файл, відкрити файл, зберегти файл, надрукувати файл, вийти. Категорія Edit містить пункти: копіювати, вставити, скасувати попередню дію, виконати попередню дію.

Категорія Options містить пункти: налаштування користувача, користувацький профіль, налаштування алгоритмів, показати журнал логів. Категорія View містить пункти: збільшення розміру схеми, відображення панелей. В категорії Tools містяться пункти: панель малювання, діалог при-

строїв. Категорія Extensions включає пункти: майстер активності, мультикористувач, IPC, скриптинг (конфігурування скриптів та інтерфейсів), очистка терміналу, агент мультикоритувача локальної мережі, агент мультикоритувача глобальної мережі, UPnP мультикористувач.

Вкладка Help містить довідку, туторіали, можна відіслати звіт про помилку та переглянути інформацію про програму.

Ще нижче розташовується перемикач між логічною та фізичною організацією мережі (див. рис. 3.18)

Рисунок 3.18 — Перемикання між логічною та фізичною організацією мережі в Cisco Packet Tracer

При зміні на фізичну організацію мережі, порожній бланк замінюється на фізичну карту, на яку можна додавати міста, будівлі, шафи, встановлювати фон. Натомість у логічній організації можна додавати кластери. Тобто фізичній організації мережі ми створюємо зовнішню структуру нашої мережі(місто->будинок->офіс). А в логічній ми всі ланки нашої структури організовуємо відповідно до заданої задачі.

В обох вкладках ми можемо змінювати характеристику(сила вітру, погодні умови, радіація і т.д) навколишнього середовища при натисканні кнопки Environment. Зміни певних значень в цьому вікні будуть позначатись на характеристиках мережі.

Знизу зліва міститься панель з присторями (див.рис. 3.19). На ній містяться різновиди хабів, свічів, роутерів, бездротових девайсів, з'єднань, кінцевих пристороїв, безпеки, емуляція глобальної мережі, з'єднання мультиюзера, кастомні пристрої.

Додавати елементи на робочу схему можна простим перетягуванням з панелі пристроїв. Двічі натиснувши на назву пристрою можна її змінити.

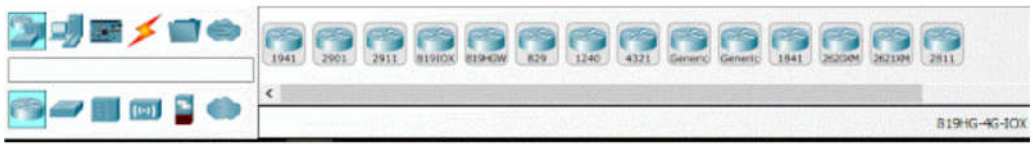


Рисунок 3.19 — Головне вікно пристроїв в Cisco Packet Tracer

Один раз натиснувши на пристрій отримаємо фізичне зображення пристрою. Тут ми можемо додавати різні модулі до комп’ютера.

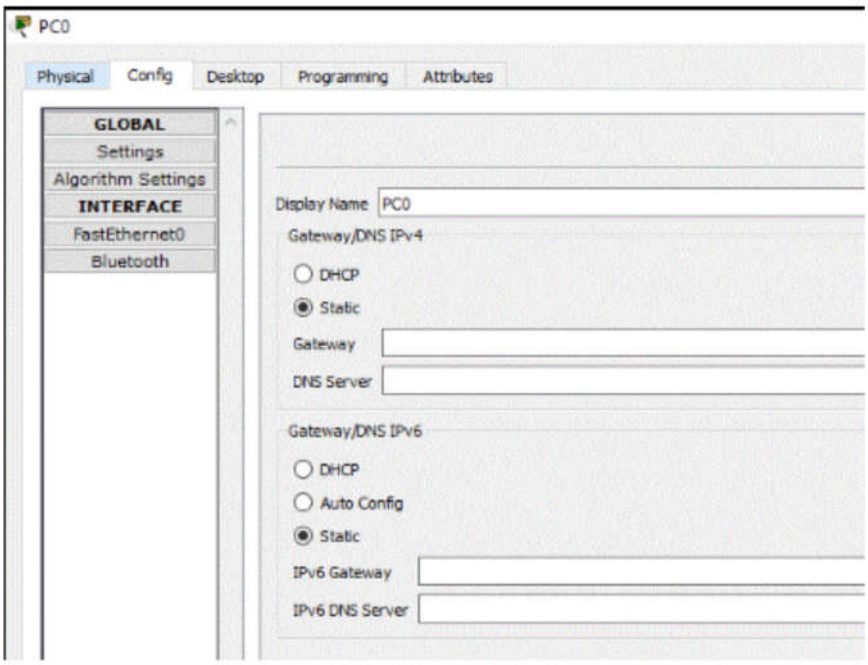


Рисунок 3.20 — Вікно налаштування параметрів в Cisco Packet Tracer

На вкладці Config (див.рис. 3.20) ми можемо налаштувати глобальні налаштування комп’ютера чи налаштувати кожен модуль окремо.

Вкладка Desktop представляє собою уявний робочий стіл з якого ми можемо керувати обраним комп’ютером. Ми можемо налаштувати IP конфігурації, зайти в термінал, виконати певні команди в командному рядку, зайти до веб-браузеру, щоб перевірити під’єднання обраного комп’ютеру до мережі Інтернет.

З правої сторони знаходиться панель інструментів. На ній містяться кнопки: виділення елементів, додавання нотатки, видалення елементу, інспектування, малювання полігону, зміна розміру фігури і формування довільних пакетів.

Знизу міститься перемикач між реальним режимом і режимом моделювання. У режимі моделювання всі пакети, що пересилаються всередині мережі, відображаються в графічному вигляді. Ця можливість дозволяє мережевим спеціалістам наочно демонструвати, по якому інтерфейсу в даний момент рухається пакет, який протокол використовується тощо.

Побудова мережі починається з визначення кількості кінцевих користувачів і їх розташуванні.

Потім настає час їх під’єднати в мережу. Це можна виконати за допомогою вкладки Connnections (див.рис. 3.21).

Рисунок 3.21 — Типи зєднань в Cisco Packet Tracer

1. автоматичний тип - при даному типі з'єднання PacketTracer автоматично вибирає найбільш бажаний тип з'єднання для вибраних пристроїв

2. консоль - консольні з'єднання

3. мідь пряме з'єднання - через мідний кабель типу вита пара, обидва кінці кабеля обтягуються в однаковій розкладці. Підійде для наступних сполучень: комутатор - комутатор, комутатор - маршрутизатор, комутатор - комп'ютер та ін.

4. мідь кроссовер - з'єднання через мідний кабель типу вита пара, кінці кабелю обтягуються як кросовер. Підійде для з'єднання двох комп'ютерів.

5. оптика - з'єднання за допомогою оптичного кабелю, необхідне для об'єднання пристроїв, що мають оптичні інтерфейси.

6. телефонний кабель - звичайний телефонний кабель, може знадобитись для підключення телефонних апаратів.

7. коаксіальний кабель - з'єднання пристроїв за допомогою коаксіального кабелю.

Так виглядає підключена мережа (див.рис. 3.22).

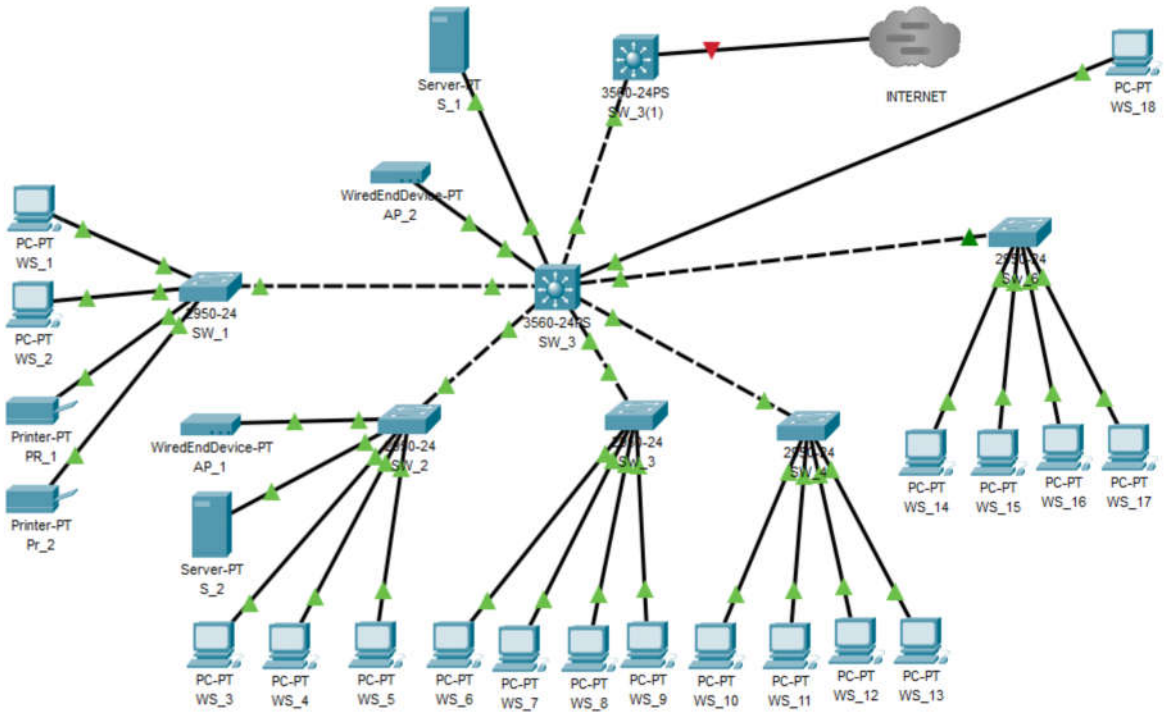


Рисунок 3.22 — Вигляд спроектованої моделі мережі

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини дипломного проекту є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності модернізації комп'ютерної мережі для компанії «MarKOM» шляхом заміни частини обладнання і прийняття рішення про її подальше впровадження в роботу.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

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

Таблиця 4.1 - Середній час виконання НДР та стадій технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Підготовка	Інженер	2
2	Розробка проекту мережі	Інженер	2
4	Налаштування активного комутаційного обладнання	Технік	8
6	Тестування мережі	Технік	1
Р а з о м			13

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.

Основна заробітна плата розраховується за формулою:

$$Зосн.=Тс* Кг, \quad (4.1)$$

де Тс – тарифна ставка, грн.;

Кг – кількість відпрацьованих годин.

Зосн.=150*4+130*9 = 1770,00 грн.

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

$$Здод.= Зосн.* Кдопл., \quad (4.2)$$

де Кдопл. – коефіцієнт додаткових виплат працівникам.

Здод.= 1770,00 *0,15=265,50 грн.

Звідси загальні витрати на оплату праці (Во.п.) визначаються за формулою:

$$Во.п.= Зосн.+ Здод., \quad (4.3)$$

Во.п. = 1770,00 + 265,50 =2035,50 грн.

Крім того, слід визначити відрахування на заробітну плату:
Отже, сума відрахувань на соціальні заходи буде становити:

$$Вз.п.=ФОП * 0,22, \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

Вз.с. = 2035,50 *0,22=765,35 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 відпрацьов. год.	Факт. нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1	Інженер	150	4	600,00	90,00	-	-
2	Технік	130	9	1170,00	175,50	-	-
	Разом	-	-	3624,00	265,50	765,35	2800,85

4.3 Розрахунок матеріальних витрат

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

$$МВі= qi * pi , \quad (4.5)$$

де qi – кількість витраченого матеріалу і-го виду;

pi – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$Зм.в.= МВі \quad (4.6)$$

Зм.в.= 20600,00 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	Жорсткий диск 4Тб	шт	2	4300,00	8600
2	Маршрутизатор MikroTik RB4011iGS+RM	шт	1	8300,00	8300,00
3	Точка доступу Ubiquiti UniFi AP Long Range	шт	1	3700,00	3700,00
	Р а з о м				20600,00

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$Зе=W* T* S, \quad (4.7)$$

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 2 години.

Зе=0,50*2*7,00=7,00 грн.

4.5 Визначення транспортних затрат

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

$$Тв=Зм.в.* 0,09 … 0,1, \quad (4.8)$$

де ТВ – транспортні витрати.

ТВ=20600,00*0,8=1648,00 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.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

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

Для визначення амортизаційних відрахувань застосовуємо формулу:

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

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

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

НА – норма амортизації, %.

Для проектування даної комп'ютерної мережі використовується один комп'ютер (вартість якого становить 19000,00 грн.), який працює 2 годин.

Тоді:

А= 19000,00*0,04*2/150=10,13 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.

$$Нв = Во.п. * 0,2 \ldots 0,6, \quad (4.10)$$

де Нв – накладні витрати.

НВ=2800,85 *0,5=1400,42 грн.

4.8 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 4.4.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до заг. суми
1	2	3
Витрати на оплату праці	2800,85	10,29
Відрахування на соціальні заходи	765,35	2,81
Матеріальні витрати	20600,00	75,65
Витрати на електроенергію	7,00	0,03
Транспортні витрати	1648,00	6,05
Амортизаційні відрахування	10,13	0,04
Накладні витрати	1400,424	0,04
Собівартість	27231,75	100,00

Собівартість (СВ) НДР розрахуємо за формулою:

$$Св= Во.п.+ Вс.з.+ Зм.в.+ Зе + Тв +А+ Нв \quad (4.11)$$

Св=27231,75 грн.

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 Ррен. – рівень рентабельності;

К – кількість замовлень, од.;

Ві.н. – вартість носія інформації, грн.;

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

Ц=27231,75*(1+0,3)*(1+0,2)= 40520,84 грн.

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва - категорія, яка характеризує результативність виробництва. Вона свідчить не лише про приріст обсягів виробництва, а й про те, якими витратами ресурсів досягається цей приріст, тобто свідчить про якість економічного зростання.

Прибуток розраховується за формулою:

$$П = Ц - Св \quad (4.13)$$

П = 40520,84 - 27231,75 = 13289,09 грн.

Економічна ефективність (Ер) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою 4.14.

$$Ер = П / Св, \quad (4.14)$$

де П – прибуток;

Св – собівартість.

Ер = 13289,09 / 27231,75 = 0,48

Поряд із економічною ефективністю розраховують (формула 4.15) термін окупності капітальних вкладень (Тр):

$$Тр = 1 / Ер \quad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку

Тр=1/0,48=2,04

Таблиця 4.5 - Економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	27231,75
2.	Плановий прибуток, грн.	13289,09
3.	Ціна, грн.	40520,84
4.	Термін окупності, рік	2,04

Враховуючи основі економічні показники, зведені у таблицю 4.5, можна зробити висновок, що при терміні окупності – 2,04 року проводити роботи по модернізації даної мережі є доцільним та економічно вигідним.

5. ОХОРОНА ПРАЦІ ТЕХНІКИ БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Система засобів і заходів безпечної експлуатації електроустаткування

Згідно з ПУЕ в електроустановках використовують такі системи заходів:

- захисне заземлення;
- занулення;
- ізоляція струмопровідних частин;
- захисне вимикання;
- малі напруги;
- недоступність до неізольованих провідників та ін..

Ці засоби захисту не є універсальними , тому для створення безпечних умов праці необхідно застосовувати не один, а кілька засобів одночасно.

Захисне заземлення – це зумисне електричне з’єднання з землею металевих не струмопровідних частин, які можуть опинитись під напругою внаслідок пошкодження електричної ізоляції

Захисне заземлення – це захист людини від ураження струмом, якщо вона доторкнулася до металевих конструкцій електрообладнання, яке опинилося під напругою.

Захисна функція полягає в тому, що сила струму, що буде проходити по тілу людини буде безпечної величини тому, що опір заземлення дуже малий порівняно з опором людини.

Отже, для виконання захисної ролі заземлюючі пристрої повинні мати дуже малий опір. Відповідно до ПУЕ допустимий опір заземлюючих пристроїв має бути не більший за 4 Ом.

Захисне заземлення обов'язково влаштовують у електроустановках при напрузі:

– 380В і більше при змінному струмі;

– 440В і більше при постійному струмі;

– 42В перемінного і 110В постійного струму в зовнішніх установках, особливо небезпечних та в умовах з підвищеною небезпекою;

– незалежно від значення напруги у всіх вибухонебезпечних приміщеннях.

Залежно від розміщення заземлювачів відносно електрообладнання заземлюючі пристрої бувають виносні і контурні, природні і штучні.

Для штучних заземлювачів використовують сталеві труби Ф від 3 до 5см з товщиною стінок 3-5мм і довжиною від 2,5 до 3м; сталеві стержні Ф 10-12мм і довжиною до 10м; кутикову сталь 40х40мм довжиною від 2,5 до 5м і т. ін..

На кожний заземлюючий пристрій складається паспорт, який включає схему заземлення, технічні дані, результати перевірки стану, характер проведених ремонтних робіт і т. ін..

Технічний стан визначається шляхом зовнішнього огляду видимої частини та вимірюванням опору, який не повинен перевищувати допустиме значення. Планове вимірювання опору виконують перед початком його експлуатації, а потім один раз на рік та після кожного капітального ремонту. Наземну частину оглядають один раз на шість місяців, а у вологих і особливо небезпечних умовах – один раз на три місяці.

Небезпеку ураження струмом можна ліквідувати шляхом швидкого відключення пошкодженої електроустановки. Для цього влаштовують занулення.

Занулення – це зумисне з'єднання металевих частин електроустановки, які зазвичай не перебувають під напругою з нульовим захисним провідником.

Це є основний засіб захисту людей від ураження струмом в установках напругою до 1000В. Захист полягає у тому, що при пробиванні ізоляції виникає коротке замикання, яке швидко вимикає пошкоджене електрообладнання від електричної мережі.

Головною умовою безпеки при експлуатації електроустановок є надійна ізоляція струмопровідних частин шаром діалектрика, який забезпечує їх надійність.

Опір ізоляції згідно з ПУЕ нормується і має досягати не менше 0,5МОм.

Матеріал ізоляції має відповідати умовам оточуючого середовища, бути стійким до агресивного середовища, вологи, нагрівання та механічного впливу, старіння і т. ін..

Стан ізоляції електричних установок відповідно до ПУЕ визначають шляхом періодичних оглядів та вимірюванням електричного опору.

Для забезпечення безпеки неізольованих провідників їх підвищують на відповідній відстані від землі, будівель, доріг:

- 6,5м над проїжджою частиною дороги;
- 3,5м над проходами;
- 2,5м над робочою поверхнею.

Безпека працюючих при експлуатації електроустаткування забезпечується також шляхом застосування стаціонарного огородження, блокування та сигналізації.

Для зменшення імовірності ураження струмом використовують малі напруги, номінальне значення яких не перевищує 42В. Напруга 42В використовується у приміщеннях I і II категорії небезпеки для живлення ручного інструменту, переносних ламп і ін..

Напруга 12В використовується для живлення ручних переносних ламп в особливо небезпечних умовах (кабельні колодязі, оглядові ями і т. ін.).

Заземлення і занулення не завжди гарантує безпеку людей від ураження струмом. Для захисту використовують захисне відключення.

Захисне відключення – це швидкодіючий захист, який забезпечує автоматичне відключення електроустановки при виникненні в ній небезпеки ураження людини струмом. Цей вид захисту спрацьовує за 0,1 – 0,05с, а занулення 0,2с і більше.

При такому нетривалому проходженні струму через тіло людини безпечним є навіть струм 500 – 650мА.

Захисне вимикання може застосовуватись як основний вид захисту, або разом з заземленням і зануленням.

Захисне вимикання окремо чи сукупно з іншими засобами захисту виконує такі функції:

– захист при замиканні на землю або корпус обладнання;
– захист при появі небезпечних струмів витікання;
– захист при переході вищої напруги на сторону нижчої;
– автоматичний контроль кола захисного заземлення і занулення.

Для захисту персоналу, що обслуговує електроустановки, використовують спеціальні захисні засоби. Ці засоби умовно поділяються на ізолюючі, огороджуючи і запобігаючи. Ізолюючі в свою чергу поділяються на основні і допоміжні.

До них належать в електроустановках напругою:

– до 1000В – штанги, діалектричні рукавиці, електровимірювальні кліщи, монтажний інструмент, а також покажчики напруги;

– понад 1000В – ізолюючі штанги, електровимірювальні кліщи, покажчики напруги, а також засоби для виконання ремонтних робіт під напругою вище 1000В;

Додаткові ізолюючі засоби не придатні витримувати робочу напругу, їх призначення полягає у тому, щоб посилити захисну дію основних ізолюючих засобів, з якими вони разом використовуються.

До додаткових ізолюючих захисних засобів в електроустановках відносяться:

– до 1000В – діелектричні галоші, килимки, ізолюючі підставки;

– понад 1000В – діелектричні рукавиці, боти, килимки, ізолюючі підставки

До захисних засобів відносяться також : захисні окуляри, захисні каски, монтерські пояси, кігті, а також екрануючі пристрої і т. ін.. Всі засоби мають зберігатися в умовах, що забезпечують їх справність.

Для обслуговування електроустановок і мереж допускаються особи, не молодше 18 років, що пройшли медичний огляд та отримали кваліфікаційну групу з техніки безпеки. Для установок понад 1000В – IV групу, а для установок до 1000В III кваліфікаційну групу.

Завдання для самостійної роботи

– Характеристика вимог безпеки до технологічного обладнання та виробничих процесів.

– Механізація і автоматизація технологічних процесівяке один з основних шляхів забезпечення безпеки.

– Дистанційне управління і візуальне спостереження за технологічними процесами в умовах сучасних форм господарювання.

– Поліпшення умов праці шляхом впровадження засобів малої автоматизації.

– Організація оптимальних форм і розмірів робочої зони.

– Безпека виробничих процесів залежно від контрольно-вимірювальних засобів і пристроїв технологічного процесу.

– Блокуючі пристрої і засоби сигналізації у відповідних робочих процесах.

– Вимоги щодо розташування та обслуговування технологічного обладнання.

– Безпека і ефективність умов праці залежно від організації робочих місць.

– Раціональна організація і планування робочих місць залежно від антропометричних даних людини.

– Вимоги безпеки при експлуатації посудин, що працюють під тиском.

– Основні причини надзвичайних ситуацій при експлуатуванні котельних апаратів.

– Вимоги безпеки при експлуатації компресорних установок.

– Безпека праці при експлуатації трубопроводів пари та гарячої води.

– Вимоги безпеки до влаштування трубопроводів і їх гідравлічного випробовування.

– Безпека праці при здійсненні газополум’яної обробки металів з використанням ацетилену, кисню, метану і інших газів.

– Технічне використання низьких температур та безпека праці при експлуатації кріогенної техніки.

– Безпека праці при організації вантажно-розвантажувальних робіт.

– Класифікація вантажів та загальні вимоги безпеки до їх перевезення.

– Транспортні шляхи на території підприємства та безпека при експлуатації внутрішньозаводського та внутрішньоцехового транспорту.

– Безпечна експлуатація внутрішньозаводських рейкових транспортних засобів та транспортних засобів безперервної дії.

5.2 Розрахунок захисного заземлення

Захисне заземлення — це навмисне електричне з'єднання із землею або з її еквівалентом металевих нормально неструмопровідних частин, які можуть опинитися під напругою. Призначення захисного заземлення полягає в тому, щоб у випадку появи напруги на металевих конструкти-

вних частинах електроустаткування (наприклад, внаслідок замикання на корпус при пошкодженні ізоляції) забезпечити захист людини від ураження електричним струмом при її доторканні до таких частин.

Відповідно до Держстандарту 12.1.030-81 захисне заземлення повинне забезпечити захист людей від вradення електричним струмом при дотику до металевих неструмопровідних частин, які можуть виявитися під напругою. Заземленням називається навмисне з'єднання електроустановок із заземлюючим пристроєм. Заземлювачем називається провідник, що перебуває в зіткненні із землею або її еквівалентом. Заземлюючим провідником називається провідник, що з'єднує заземлені частини із заземлювачем.

Сукупність з'єднуючих провідників і заземлювачів називається заземлюючим пристроєм.

Мета розрахунку захисного заземлення– визначення кількості електродів заземлювача і заземлюючих провідників, їхніх розмірів і схеми розміщення в землі, при яких опір заземлюючого пристрою розтікання струму або напруга дотику при замиканні фази на заземлені частини електроустановок не перевищують допустимих значень.

Вихідними даними для розрахунку заземлюючого пристрою є: величина опору заземлюючого пристрою, що нормується правилами, питомий опір ґрунту, що визначається вимірюваннями, розміри і умови розміщення в ґрунті одиничних заземлювачів.

Вихідні дані для розрахунку:

Захищувальний об'єкт — комп'ютерна мережа котра включає персональні комп'ютери та мережеве обладнання.

Захищувальний об'єкт — стаціонарний,

Напруга мережі — 220 В,

Виконання заземлення - з глухозаземленою нейтраллю,

Тип заземлення — стальні прутки, вертикально забиті в грунт, габаритні розміри lb=3м, d=0,04м, δт=4 мм,

Відношення відстані між трубами та їх довжини Lb/lb=1,

Розміри горизонтального заземлювача, стальної полоси Lг=Lз.с — згідно розрахунку, ширина полоси bc=3 мм,

Глибина закладання вертикальних заземлювачів hb= 0m, горизонтальних hг=0м,

Розташування прутків приймемо за чотирикутним контуром,

Грунт — чорнозем, склад — однорідний, вологість — нормальна, агресивність - нормальна.

Розв'язок:

1. Згідно з ПУЕ приміщення відноситься до П-2, Вибухонебезпека В-1, ступінь ураження електричним струмом — без підвищеної небезпеки.

2. Опір розтікання струму в заземлюючому пристрої RД<4 Ом,

3. Питомий опір грунту вибираємо з таблиці 5.1 та таблиці 5.2 ρ=30 Ом.м,

4. Коефіцієнт сезонності вертикальних заземлювачів Кс.п=1,5, коефіцієнт сезонності горизонтальних заземлювачів Кс.в=3,5,

5. Визначаємо питомий опір грунту для вертикальних заземлювачів

$$\rho_{РОЗР.В} = \rho_{табл} \quad К_{с.в} \qquad (5.1)$$

$$\rho_{РОЗР.В} = 30 \quad 1{,}5 = 45 \text{ (Ом .м)}$$

6. Визначаємо питомий опір грунту для горизонтальних заземлювачів

$$\rho_{РОЗР.Г} = \rho_{табл} \quad К_{с.г} \qquad (5.2)$$

$$\rho_{РОЗР.Г} = 30 \quad 3{,}5 = 105 \text{ (Ом .м)}$$

7. Визначаємо відстань від поверхні землі до середини вертикального заземлювача

$$t = hb+0,5\ lb \quad (5.3)$$

t = 0+0,5 3=1,5 (м)

8. Визначаємо опір розтіканню струму вибираємо з таблиці 5.3 та таблиці 5.4 в одному вертикальному заземлювачі

$$R_B=\frac{\rho_{РОЗР.В.}}{2\pi l_B} ln\left(\frac{4\cdot l_B}{d}\right) \quad (5.4)$$

$$R_B=\frac{45}{2\cdot 3,14\cdot 3} ln\left(\frac{4\cdot 3}{0,04}\right)=13(Ом)$$

9. Визначаємо теоретичну кількість вертикальних заземлювачів без врахування коефіцієнта використання ηвв=1

$$nтв=RB/(RД\quad ηвв) \quad (5.5)$$

nтв=13/(4 1)=3 (шт)

10. Визначаємо коефіцієнт використання вертикальних заземлювачів ηвв при слідуючих вихідних даних: число заземлювачів — 3, відношення Lb/lb=1. Приймемо ηвв =0,73 (таблиця 5.6 та таблиця 5.5)

11. Визначаємо nн.в — необхідну кількість вертикальних заземлювачів з врахуванням ηвв

$$nнв=RB/(RД\quad ηвв) \quad (5.6)$$

nнв=13/(4 0,73)=5 (шт)

12. Визначаємо Rрозр.в - розрахунковий опір, Ом, розтіканню струму у вертикальних заземлювачах

$$R_{розр.в}=R_B/(n_{Н.В}\ \eta_{вв}) \quad (5.7)$$

Rрозр.в=13/(5 0,73)=3,56 (Ом)

13. Визначаємо відстань між вертикальними заземлювачами виходячи з співвідношення Lb/lb=1,

$$L_b=1\ l_b \quad (5.8)$$

Lb=1 3=3 (м)

14. Визначаємо довжину з'єднувальної стрічки — горизонтального заземлювача

$$L_{з.с}=1{,}05\ L_b\ (n_{нв}-1) \quad (5.9)$$

Lз.с=1,05 3 (5-1)=12.6 (м)

15. Визначаємо опір розтіканню струму в горизонтальному заземлювачі

$$R_{Г.З.К.}=\frac{\rho_{РОЗР.Г.}}{2\pi L_{З.К.}}\ln\frac{2L_{З.К.}}{b_K} \quad (5.10)$$

$$R_{Г.З.К.}=\frac{105}{2\cdot 3{,}14\cdot 12{,}6}\ln\frac{4\cdot 12{,}6}{0{,}03}=9{,}8\ (Ом)$$

16. Визначаємо коефіцієнт використання горизонтального заземлювача виходячи з умови що Lb/lb=1, та nнв=5 шт. За таблицею 7.6 [7]С.263 приймаємо ηвг = 0,19.

17. Визначаємо розрахунковий опір розтіканню струму в горизонтальному заземлювачі при числі електродів nг=1

$$Rрозр.г=Rгзс/(nг \quad ηвг) \tag{5.11}$$

Rрозр.г=9,8/(1 0,19)=52 (Ом)

18. Визначаємо розрахунковий теоретичний опір розтіканню струму у вертикальному та горизонтальному заземлювальних пристроях

$$R_{РОЗР.В.Г.}=\frac{1}{\frac{1}{R_{РОЗР.В.}}+\frac{1}{R_{РОЗР.Г.}}} \tag{5.12}$$

$$R_{РОЗР.В.Г.}=\frac{1}{\frac{1}{3,56}+\frac{1}{52}}=3,31\ (Ом)$$

19. Вибираємо матеріал з'єднувальних провідників. В нашому випадку це буде неекранований мідний провідник з площею поперечного січення 4 мм

20. Вибираємо матеріал магістральної шини. В нашому випадку це буде сталева шина товщиною 4 мм з площею поперечного січення 100 мм2.

Схема розрахованого заземлення показана на рисунку 5.1

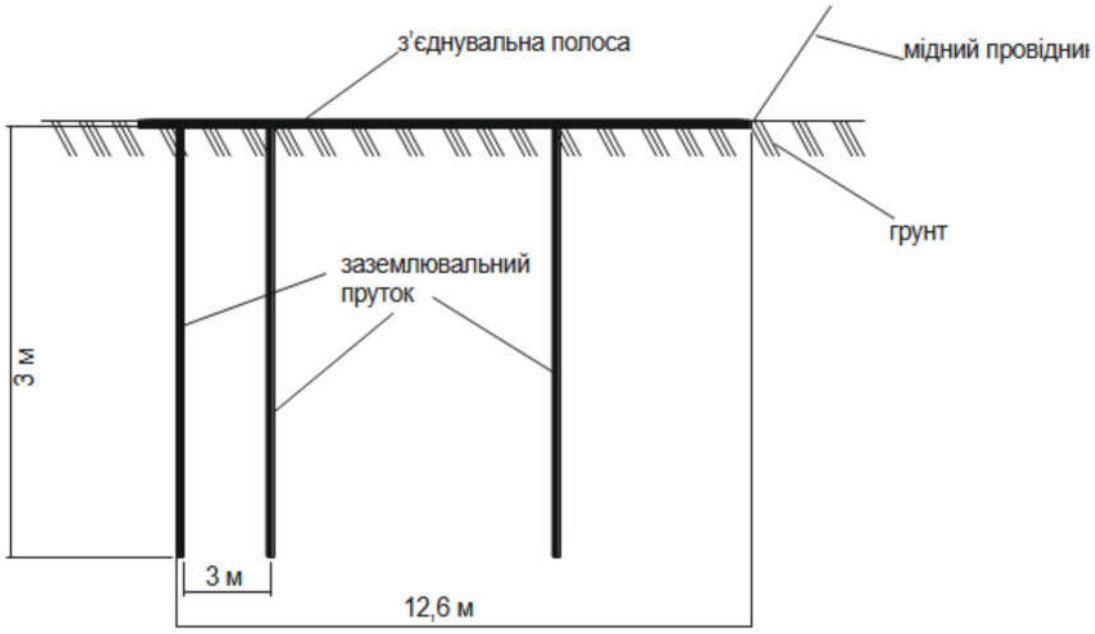


Рисунок 5.1 — Схема призначення розмірів, для розрахунку захисного заземлення

Таблиця 5.1 - Приблизні значення питомих електричних опорів різних грунтів та води, Ом • м

Грунт, вода	Можливі межі коливань, р	При вологості 10-20% до маси грунту	Рекомендоване значення для приблизних розрахунків
1	2	3	4
Глина	8-70	40	40
Суглинок	40 150	100	100
Чорнозем	9-530	200	200
Торф	10-30	20	20

Продовження таблиці 5.1

1	2	3	4
Садова земля	30 60	40	40
Супісок	150 400	300	300
Пісок	400-700	700	700
Кам’янистий	500 800		
Скелястий	Ю'-ІО		
Вода:			
морська	0.2 1.0		1.0
річкова	10-100		80
водоймищ	40-50		50
струмкова	10-60		60
грунтова	20-70		50

Таблиця 5.2 - Коефіцієнт сезонності вимірюванні її опору

Кліматична юна	Вологість землі при вимірюванні		
	підвищена	Нормальна	Мала
1	2	3	4
К с.в. для електрода довжиною Lb = 3 м			
1	1.9	1,7	1.5
II	1,7	1,5	1,3
III	1.5	1,3	1.2
IV	1.3	1,1	1.0
К с.в. для електрода довжиною Lb = 5 м			

Продовження таблиці 5.2

1	2		3
1	1.5	1-4	1.3
II	1.4	1,3	1.2
III	1.3	1,2	1.1
IV	1.2	1,1	1.0

Таблиця 5.3 - Значення коефіцієнта використання вертикальних заземлювачів hВ, розташованих у ряду

Відношення відстані між електродами до їх довжини (ї ї	Кількість заземлювачів п									
	2	3	4	5	6	7	8	9	10	11
1	2	3	4	5	6	7	8	9	10	11
1	0.86	0.81	0.77	0.74	0.72	0.70	0,67	0.65	0.62	0.60
2	0.95	0.92	0.89	0,86	0.84	0.82	0.79	0.77	0.75	0.73
3	0.97	0.94	0.92	0.90	0.88	0.87	0.85	0.83	0.82	0.81

Таблиця 5.4 - Значення коефіцієнта використання вертикальних заземлювачів hВ, розташованих по контуру

Відношення відстані між електродами до їх довжини	Кількість заземлювачів п							
	4	8	12	16	20	40	60	100
1	2	3	4	5	6	7	8	9

Продовження таблиці 5.4

1	2	3	4	5	6	7	8	9
1	0.66	0,56	0,50	0,47	0.44	0,41	0,39	0,36
2	0.76	0,68	0,65	0,63	0,61	0,58	0,55	0,52
3	0.84	0,77	0,73	0,70	0,68	0,66	0.64	0,62

Таблиця 5.5- Значення коефіцієнта використання горизонтального стрі- чкового електрода hr, що з'єднує вертикальні заземлювачі, розташовані у ряд

all	Кількість заземлювачів її									
	*>	3	4	5	6	7	8	9	10	11
1	2	3	4	5	6	7	8	9	10	11
1	0.84	0.76	0.71	0.67	0,64	0.62	0.60	0.58	0,56	0,55
2	0.90	0.85	0.81	0.79	0,77	0.75	0.74	0.73	0,72	0.71
3	0.93	0.90	0.87	0,85	0,83	0.82	0.81	0.80	0.79	0.78

Таблиця 5.6 - Значення коефіцієнта використання горизонтального стрічкового електрода h, що з'єднує вертикальні заземлювачі, розташовані по контуру

all	Кількість заземлювачів п									
	4	6	8	10	12	16	20	40	60	100
1	2	3	4	5	6	7	8	9	10	11
1	0.45	0.40	0.36	0,34	0.32	0.30	0.27	0,22	0.20	0.19
2	0.55	0.48	0.43	0.40	0.38	0.35	0.32	0,29	0.27	0.23
3	0.70	0.64	0.60	0.56	0.54	0.50	0.45	0,39	0.36	0.33

ВИСНОВКИ

В ході проектування модернізовано комп’ютерну мережу організації “MarKOM”. 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.

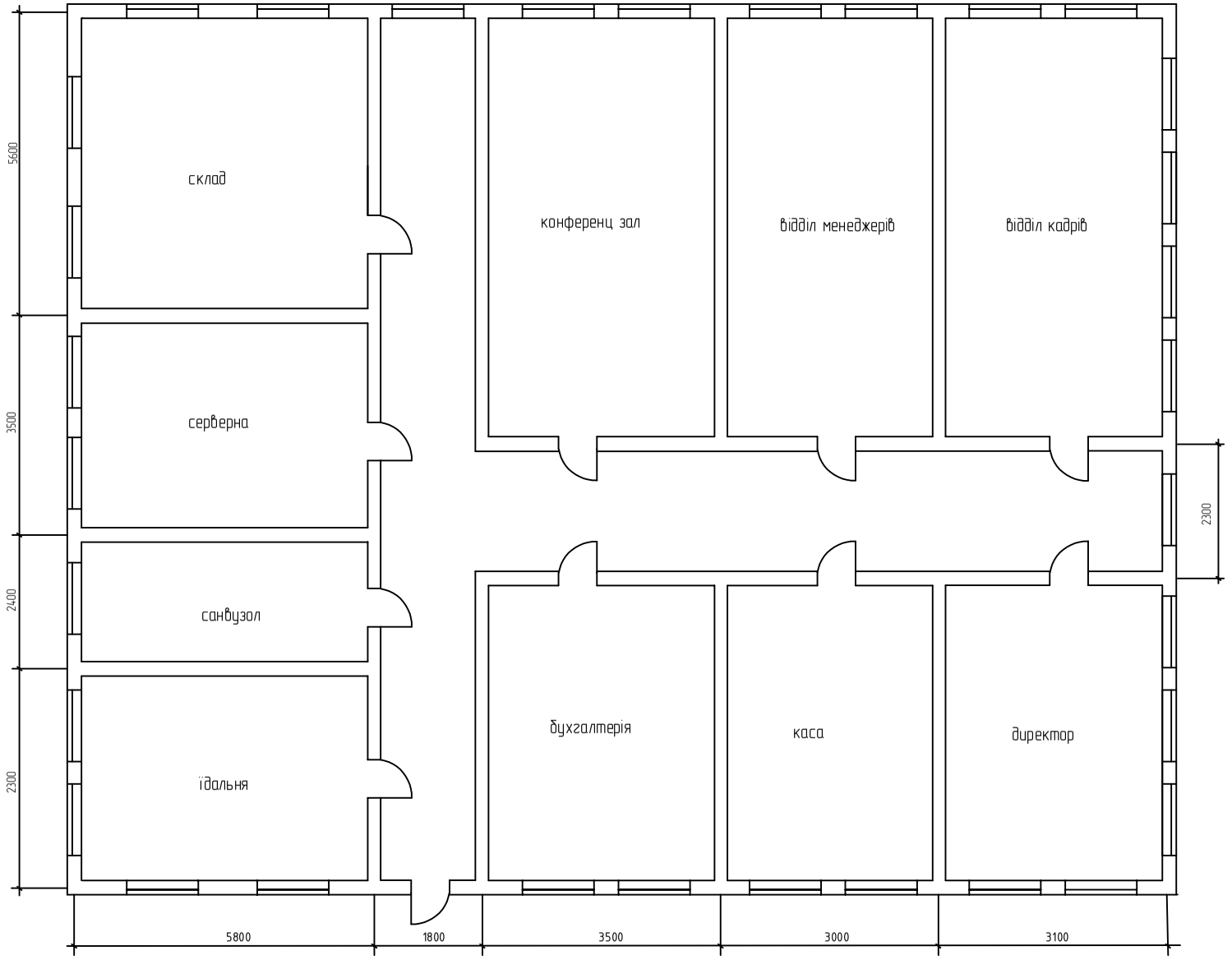
В економічному розділі розраховано собівартість модернізації мережі, її економічну ефективність, термін окупності та інші показники.

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

ПЕРЕЛІК ПОСИЛАНЬ

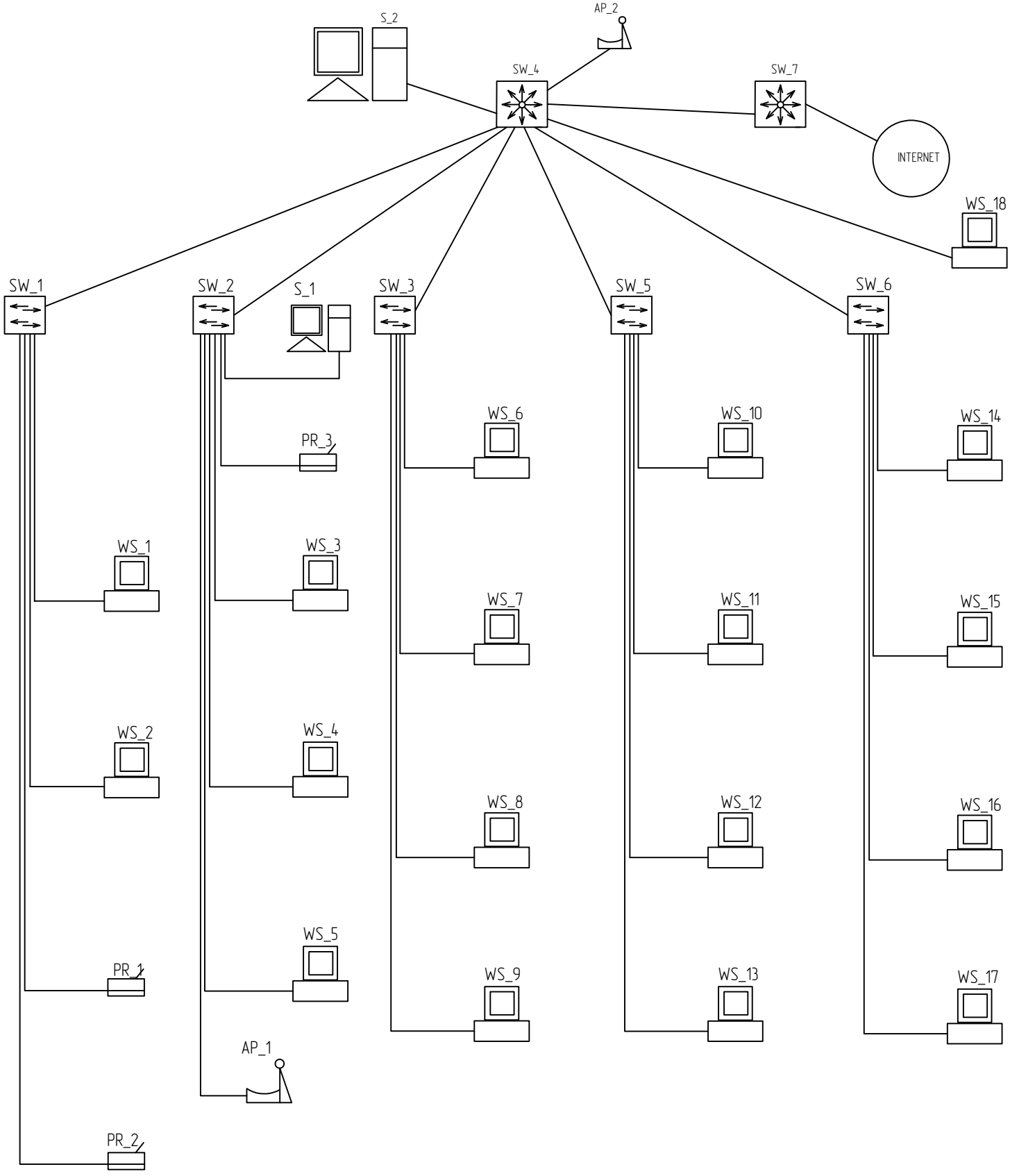
1. Антонов В.М. Сучасні комп'ютерні мережі. Підручник — К.: "МК-Прес", 2005. — 480 с.
2. Буров Є. Комп'ютерні мережі, 2-е видання. - БаК, 2004. – 584 с.: іл.
3. Городецька, О. С. Г70 Комп’ютерні мережі : навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. Вінниця : ВНТУ, 2017. 129 с.
4. Додонов О. Г., Ланде Д. В., Путятін В. Г. Інформаційні потоки в глобальних комп’ютерних мережах. — К.: Наук, думка, 2009. — 295 с
5. Іртегов Д.В. Введення в мережні технології, К., 2014.
6. Шорошев В. В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп’ютерних систем. Монографія. - К.: ДУПСТ, 2011. - с.257.
7. Business Products [Електронний ресурс] – URL: http:// www.trendnet.com/products/business/category/switches (дата звернення 11.04.2024)
8. Комутатори [Електронний ресурс] – URL: http://hotline.ua/computer/ kommutatory/(дата звернення 12.04.2024)
9. Охорона праці – Москальова В.М. [Електронний ресурс] –URL: http://studentbooks.com.ua/content/view/1327/76/(дата звернення 13.04.2024)
10. URL:http://uadoc.zavantaq.com/text/18809/index-10.html (дата звернення 22.04.2024)
11. URL:https://doc.player.net/63547955-A-o-azarova-n-v-lisak-kom p-yuterni merezhi-ta-telekomunikaciyi.html (дата звернення 25.04.2024.)
12. https://studopedya.ru/2-18781.html(дата звернення 28.04.2024)
13. URL:https://uk.wikipedia.org/wiki/ТесТ на проникнення (дата звернення 11.05.2024)

14. URL:https://lektsii.org/5-26558.html (дата звернення 19.05.2024)
15. Розширені налаштування Mikrotik RouterOS URL:https://lanmarket.ua/ua/stats/rukovodstvo-dlya-nachinayushchikh-po-nastroyke-routera-mikrotik-ot-nachala-do-kontsa/(дата звернення 15.05.2024)
16. Розширені налаштування Mikrotik RouterOS: два зовнішні канали від одного провайдера URL:https://lanmarket.ua/ua/stats/rasshirennye-nastroyki-Mikrotik-RouterOS%3A-dva-vneshnih-kanala-ot-odnogo-provaydera-/(дата звернення 16.05.2024)
17. Знайомство з CISCO PACKET TRACER. URL: https://nickshevtsov.blogspot.com/2017/10/cisco-packet-tracer.html (дата звернення:28.05.2024).



								2024.КВР.123.602.21.00.00 ПП	
Зм.	Арк.	№Докум.	Підпис	Дат.	Модернізація проекту комп'ютерної мережі компанії "МагКОМ" План Приміщень		Літ.	Маса	Масшт.
Розроб.		Рецушко І.І.							1:100
Керів.		Лаврінйов А.С.					Аркуш 1	Аркушів 1	
Н.контр.		Пришмак В.А.					ВСП ТФК ТНТУ, КІ 602, м.Тернопіль		
Рецензія									
затв.									

								2024.КВР.123.602.21.00.00 ФТ	
Зм.	Арк.	№Докум.	Підпис	Дат.					
Розроб.		Рецушко І.І.			Модернізація проекту комп'ютерної мережі компанії "МагКОМ" Фізична топологія		Літ.	Маса	Масшт.
Керів.		Лапчійор А.С.							1:100
Нконтр.		Пришмак В.А.					Аркуш 1	Аркушів 1	
Рецензія							ВСП ТФК ТНТУ, КІ 602, м.Тернопіль		
затв.									



						2024.КВР.123.602.21.00.00 /ЛТ	
Зм.	Арк.	№Докум.	Підпис	Дат.	Модернізація проєкту комп'ютерної мережі компанії "МагКОМ" Логічна топологія	Літ.	Маса	Масшт.
Розроб.		Репушко І.І.						1:100
Керів.		Лавандра А.І.				Н		
Н.контр.		Пришмак В.А.				Аркуш 1	Аркушів 1	
Рецензія						ВСП ТФК ТНТУ, КІ 602, м.Тернопіль		
затв.								

ТАБЛИЦЯ IP-АДРЕСАЦІЇ В МЕРЕЖІ			
№ П.П	НАЗВА	IP-АДРЕСА\Маска	РОБОЧА ГРУПА\Vlan
1	WS_1	192.168.10.0\24	ADM\10
2	WS_2		
3	WS_3	192.168.20.0\24	buch\20
4	WS_4		
5	S_1		
6	WS_5		
7	WS_6	192.168.20.0\24	buch\20
8	WS_7		
9	WS_8		
10	WS_9		
11	WS_10	192.168.30.0\24	manager\30
12	WS_11		
13	WS_12		
14	WS_13		
15	WS_13		
16	WS_14	192.168.40.0\24	CONF\40
17	WS_15		
18	WS_16		
19	WS_17		
20	WS_18	192.168.100.1\24	admin\100
21	S2	192.168.100.1\24	admin\100
22	AP_1	192.168.20.1\24	buch\20
23	AP_2	192.168.100.1\24	admin\100
24	SW_4	192.168.100.1\24	admin\100
25	SW_7	192.168.100.1\24	admin\100
26		призначається провайдером	

							2024.КВР.123.602.21.00.00 ТА	
Зм.	Арк.	№Докум.	Підпис	Дат.	Модернізація проекту комп'ютерної мережі компанії "МагКОМ" Таблиця IP адресації		Літ.	Маса	Масшт.
Розроб.		Репушко І.І.					Н		
Керів.		Лапандра А.І.					Аркуш 1	Аркушів 1	
Н.контр.		Пришмак В.А.					ВСП ТФК ТНТУ, КІ 602, м.Тернопіль		
Рецензія									
затв.									

ТАБЛИЦЯ ТЕХНІКО-ЕКОНОМІЧНИХ ПОКАЗНИКІВ							
№ п\п	параметр	одиниці виміру	значення	№ п\п	параметр	одиниці виміру	значення
1	технологія мережі	–	ethernet 1000	8	тип доступу до інтернет	–	вита пара
2	топологія мережі	–	гібридна	9	марка маршрутизатора доступу в інтернет	–	MikroTik RB4011iGS+RM
3	середовище передачі	–	Вита пара кат. 5E	10	термін окупності	рік	2,04
4	кількість вузлів мережі	шт	25	11	плановий прибуток	грн	13289,09
5	марка головного комутатора	–	Cisco CBS350-24P-4G-EU	12	собівартість	грн	27231,75
6	марка 8-ми портового комутатора	–	Linksys LGS108	13	ціна	грн	40520,84
7	марка точки доступу	–	Ubiquiti UniFi AP Long Range	14			