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

(освітньо-кваліфікаційний рівень)

на тему: **Розробка проекту комп'ютерної мережі компанії «IT ware»**

Виконав: студент VI курсу, групи КІб-602

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

_____Денис ЗІНКЕВИЧ
(підпис) (ім'я та прізвище)

Керівник _____ Ігор ТХІР
(підпис) (ім'я та прізвище)

Рецензент _____
(підпис) (ім'я та прізвище)

Тернопіль – 2023

Відокремлений структурний підрозділ
«Тернопільський фаховий коледж
Тернопільського національного технічного університету імені Івана Пулюя»

Відділення телекомунікацій та електронних систем
Циклова комісія комп'ютерної інженерії
Освітньо-кваліфікаційний рівень бакалавр
Спеціальність 123 «Комп'ютерна інженерія»
(шифр і назва)

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"01" травня 2023 року

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

Зінкевич Денис Васильович
(прізвище, ім'я, по батькові студента)

1. Тема роботи: **Розробка проекту комп'ютерної мережі компанії «IT ware»**

керівник роботи: **Тхір Ігор Любомирович**
(прізвище, ім'я, по батькові)

затверджені наказом вищого навчального закладу від 1.05.2023р. № 4/9-173

2. Строк подання студентом кваліфікаційної роботи 21.06.2023р.

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)

АНОТАЦІЯ

ВСТУП

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

4.8 Складання кошторису витрат та визначення собівартості НДР

4.9 Розрахунок ціни НДР

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Вимоги до організації робочих місць користувачів ПК

ВИСНОВКИ

ПЕРЕЛІК ПОСИЛАНЬ

Висновки: навести результати роботи по кожному розділу зокрема і загальний висновок по кваліфікаційній роботі

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 кваліфікаційної роботи бакалавра

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Оксана РЕДЬКВА викладач		
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	02.05	
2	Збір і узагальнення інформації по роботі	15.05	
3	Написання першого розділу	24.05	
4	Розробка технічного та робочого проекту	29.05	
5	Написання спеціального розділу	2.06	
6	Розрахунок економічної частини	5.06	
7	Написання розділу охорони праці	7.06	
8	Виконання графічної частини	12.06	
9	Оформлення проекту	16.06	
10	Проходження нормоконтролю	19.06	
11	Попередній захист роботи	21.06	
12	Захист роботи		

7. Дата видачі завдання 2.05.2023р.

Студент _____ Денис ЗІНКЕВИЧ
(підпис) (ім'я та прізвище)

Керівник кваліфікаційної роботи _____ Ігор ТХІР
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Зінкевич Д.В. Розробка проекту комп'ютерної мережі компанії «IT ware» : кваліфікаційна робота на здобуття освітнього ступеня бакалавр, за спеціальністю 123 Комп'ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2023. 85с.

Кваліфікаційна робота описує головні етапи створення компютерної мережі. В роботі приводиться структура підприємства, опис та вибір топології та технології мережі, проводиться підбір та налаштування обладнання мережі.

Проводиться обґрунтування вибору програмного забезпечення та способи його налаштування. В роботі розроблено модель мережі.

Описано методику розрахунку вартості робіт та описані питання з техніки безпеки та охорони праці.

Ключові слова: компютерна мережа, топологія, технологія, сервер, вита пара.

ANNOTATION

Zinkevich D.V. Development of a computer network project of the "IT ware" company: qualifying work for obtaining a bachelor's degree, specialty 123 Computer Engineering. Separate Structural Subdivision "Ternopil Professional College of Ternopil Ivan Puluj National Technical University", 2023. 85p.

The qualification work describes the main stages of creating a computer network. The work presents the structure of the enterprise, description and selection of network topology and technology, selection and configuration of network equipment.

The justification of the choice of the software and the methods of its adjustment are carried out.

A network model is developed in the paper. The methodology for calculating the cost of works is described, as well as issues related to safety and occupational health and safety.

Key words: computer network, topology, technology, server, twisted pair.

ЗМІСТ

ВСТУП

Локальна мережа це є сукупність компютерів та периферійних пристроїв, з'єднаних між собою в межах певної площі. З різних типів мереж локальні мережі можна виділити за приватною власністю, високою швидкістю та низьким рівнем помилок.

Локальна мережа відрізняється від інших типів комп'ютерних мереж тим, що пристрої, підключені до локальної мережі, знаходяться в одній будівлі, тобто будинку чи офісі. Ці комп'ютери, принтери, сканери та інші пристрої підключаються до маршрутизатора за допомогою кабелю Ethernet або через бездротовий маршрутизатор і точку доступу Wi-Fi. Найпростіший тип мережі - це підключення комп'ютерів та принтерів в якомусь офісі. Загалом, локальна мережа - один із засобів передачі даних.

Переваги локальних мсреж:

- спільне використання ресурсів;
- централізоване управління обладнанням і даними;
- легке підключення обладнання від різних постачальників.

При використанні локальної мережі багаторазово прискорюється доступ до інформації, що знаходиться на одному з комп'ютерів мережі. Особливо відчутно це при роботі з великими файлами. Більше не потрібно кілька разів ходити від одного комп'ютера до іншого з флеш-накопичувачами.

За допомогою локальної мережі можна поєднувати комп'ютери будь-яких типів і з будь-якими операційними системами.

Міжнародний комітет, що спеціалізується на стандартизації в галузі локальних комп'ютерних мереж, дає наступне визначення цим системам: "Локальні комп'ютерні мережі відрізняються від інших видів мереж тим, що вони звичайно обмежені невеликим географічним районом, таким, як група поруч розташованих будівель, і, в залежності від каналів зв'язку здійснюють передачу

даних в діапазонах швидкостей від помірних до високих з низьким рівнем помилок .” Значення параметрів району, загальна протяжність, кількість вузлів, швидкість передачі і топологія локальної обчислювальної мережі можуть бути різними, але комітет IEEE802 обмежує використання в локальних мережах кабелів довжиною до кількох кілометрів, підтримки декількох сотень станцій різноманітної топології при швидкості передачі інформації порядку 1-2 і більше Мбіт/с”.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Темою дипломного проекту є розробка проекту комп’ютерної мережі для компанії «IT ware» .

Область застосування розробки - автоматизація робочого процесу компанії шляхом структуризації інформаційних потоків та систем зберігання даних.

Дана мережа повинна слугувати для задоволення потреб підприємства в :

- об’єднанні ПК, що входять до різних структурних одиниць.
- спільному використанні одного швидкісного підключення до мережі Інтернет.
- використання служб локальної мережі та мережі Інтернет.
- обміні інформацією.

1.1.2 Призначення розробки

Дана комп’ютерна мережа призначена для організації ефективної роботи всіх працівників компанії «IT ware». Вимоги що ставляться перед мережею:

- спільне ефективне використання таких комп’ютерних ресурсів, такі як жорсткі диски та принтери з метою зниження витрат на закупівлю обладнання;
- використовувати спільного програмного забезпечення в мережі замість того, щоб купувати ліцензійне програмне забезпечення для кожного клієнта;

- ефективний спосіб збереження даних користувачів мережі на одному централізованому мережевому ресурсі;
- централізований спосіб керування доступом до спільних ресурсів з метою підвищення корпоративної безпеки;
- ефективний спосіб передачі даних та повідомлення між учасниками локальної мережі;
- спільне використання єдиного інтернет-з'єднання для всіх користувачів локальної мережі.

1.2.3 Вимоги до апаратного та програмного забезпечення

Система проектується і будується відповідно до міжнародного стандарту ISO / IEC 11801 редакції 2002 року, відповідає категорії 5е.

СКС будується на пасивних компонентах СКС (кабельно-провідникова продукція, інформаційні розетки, патчпанелі і патчкорди).

Робоче місце складається з одного порта RJ-45 категорії 5е для підключення кінцевого пристрою.

Розміщення робочих місць відповідно до наявного плану-схеми.

Кожен кабель промаркований на обох кінцях. Маркування, що здійснюється на монтажних панелях, забезпечує однозначну і унікальну ідентифікацію місця розташування протилежного кінця кабелю.

Мережа яку проектуємо чітко поділена на робочі групи, швидкість мережі буде 100/1000 Мбіт/с.

Апаратне забезпечення мережі має бути загальновживане, 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.

В даному випадку операційні системи, які використовуються на підприємстві, це сімейство Windows.

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

1.2.4 Стадії та етапи розробки

При організації мережі всі роботи можна поділити на наступні етапи:

- Збір інформації
- Створення і затвердження проектів
- Фізична реалізація мережі
- Експлуатація та моніторинг мережі

При зборі інформації необхідно визначитись в питаннях:

- Який тип організації і чи планується її зростання.
- Яке програмне забезпечення буде використано в мережі.
- Визначити тип мережі, топологію, провідники та інше обладнання.
- Визначити кількість і потребу магістралей вертикального та горизонтального кабелювання.
- Тип підключення до глобальної мережі та підібрати маршрутизатор.

1.1.5 Вимоги до документації

В результаті проектування потрібно створити наступну документацію:

- Логічна топологія
- Фізична топологія

Після виконання вищевказаних робіт можна приступити до монтажу системи.

Після запуску організації, ці документи є основними експлуатаційними документами IT інфраструктури.

1.1.6 Техніко-економічні показники

Для розробки проекту локальної комп'ютерної мережі та введення його в експлуатацію необхідно передбачити витрати на:

- збір та узагальнення інформації про наявний комп ютерний парк організації;
- розробку проектної документації на мережу,
- підбір, закупівля та встановлення активного та пасивного мережевого обладнання;
- закупівлю та налаштування програмного забезпечення серверів та робочих станцій;
- тестування мережі.

Загальна кількість нормо-годин на всі процеси від проектування до впровадження, конфігурування та тестування мережі не повинно перевищувати 100 годин.

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.

Для перевірки готовності працездатності мережі повинні передбачатися такі заходи:

- перевірка маркування та цілісності всіх кабельних з'єднань;
- перевірка коректності налаштування драйверів мережевих карт, мережевих сервісів, IP-адрес та шлюзів;

- перевірка коректності доступу та збереження інформації у спільному мережевому сховищі;
- перевірка коректності налаштування доступу до глобальної мережі.

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.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис задачі та характеристика підприємства

Метою кваліфікаційної роботи є створення комп'ютерної мережі, яка повинна об'єднати всі ПК, забезпечити можливість обміну інформацією та зберігання даних, забезпечити всім робочим станціям спільний доступ до мережевих ресурсів та Інтернет.

Дана організація займається проектуванням та експлуатацією систем водопостачання та меліорації. Має свій невеликий магазин, де реалізує деяку запірну та керуючу арматуру.

Відділи компанії, які потрібно підключити до її локальної комп'ютерної мережі, розміщені в одній будівлі у межах першого поверху.

У приміщенні висота від підлоги до перекриття - 3,2 метра, стіни в приміщенні комбіновані — піноблоки та керамогранітна цегла.

Розведення кабелю необхідно виконати прихованим способом. Біля комутаційної шафи необхідно організувати прихований канал для підведення кабелів до шафи за допомогою пластикового короба 100х100 або іншого розміру. Комутаційну шафу встановлюємо в окремому приміщенні.

До особливостей проектування мережі слід віднести потребу поділу всього адресного простору мережі на окремі підмережі з метою підвищення безпеки експлуатації та зменшення обчислювального навантаження на комутаційні пристрої локальної мережі.

Поділ на підмережі слід здійснити на основі організаційних підроздшв компанії. До таких підрозділів належать:

- адміністрація
- працівники
- інформаційні табло

Персональні комп’ютери будуть розміщуватись у таких кабінетах:

- фінансовий відділ,
- керівник філії,
- інженери, проектанти,
- склад.

Варто зазначити, що в мережі прсутні телевізори, які виступають як інформаційні табло.

2.2 Розробка та обґрунтування логічної та фізичної схем мережі [7,8]

Під топологією (компонуванням, конфігурацією, структурою) комп’ютерної мережі звичайно розуміється фізичне розташування комп’ютерів мережі й спосіб з’єднання їх лініями зв’язку. Важливо відзначити, що поняття топології ставиться, насамперед, до локальних мереж, у яких структуру зв’язків можна легко простежити. У глобальних мережах структура зв’язків звичайно схована від користувачів, вона не надто важлива, тому що кожний сеанс зв’язку може виконуватися по своєму власному шляху.

Топологія визначає вимоги до устаткування, тип використовуваного кабелю, можливі й найбільш зручні методи керування обміном, надійність роботи, можливості розширення мережі.

Існує три основних топології мережі:

- шина (bus), при якій всі комп’ютери паралельно підключаються до однієї лінії зв’язку й інформація від кожного комп’ютера одночасно передається всім іншим комп’ютерам (див. рис. 2.1);
- зірка (star), при якій до одного центрального комп’ютера приєднуються інші периферійні комп’ютери, причому кожний з них використовує свою окрему лінію зв’язку (див. рис 2.2);

– кільце (ring), при якій кожний комп’ютер передає інформацію завжди тільки одному комп’ютеру, наступному в ланцюжку, а одержує інформацію тільки від попереднього комп’ютера в ланцюжку, і цей ланцюжок замкнутий в «кільце» (див. рис. 2.3).

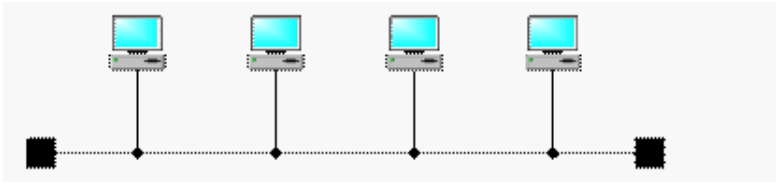

Рисунок 2.1 - Топологія типу “шина”

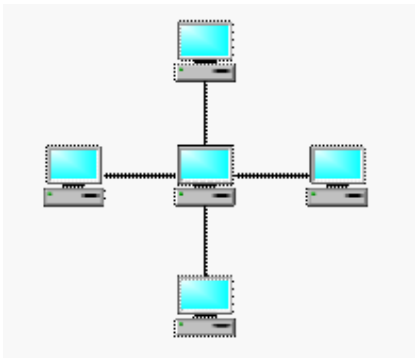

Рисунок 2.2 - Топологія типу “зірка”

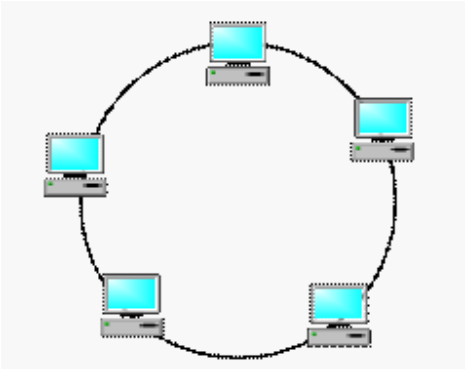

Рисунок 2.3 - Топологія типу “кільце”

На практиці нерідко використовують і комбінації базових топологій, але більшість мереж орієнтовані саме на ці три. Розглянемо тепер коротко особливості перерахованих мережних топологій.

Топологія «шина» (або, як її ще називають, «загальна шина») самою своєю структурою припускає ідентичність мережного устаткування комп'ютерів, а також рівноправність всіх абонентів.

При такому з'єднанні комп'ютери можуть передавати пакети тільки по черзі, тому що лінія зв'язку єдина. У іншому випадку передана інформація буде спотворюватися в результаті накладення (конфлікту, колізії). Таким чином, у шині реалізується режим напівдуплексного (half duplex) обміну (в обох напрямках, але по черзі, не одночасно).

У топології «шина» відсутній центральний елемент, через який передається вся інформація, що збільшує її надійність (адже при відмові будь-якого центра перестає функціонувати вся керована цим центром система).

Додавання нових абонентів у шину досить просте й звичайно можливе навіть під час роботи мережі. У більшості випадків при використанні шини потрібна мінімальна кількість сполучного кабелю в порівнянні з іншими топологіями. Правда, треба врахувати, що до кожного комп'ютера (крім двох крайніх) підходить два кабелі, що не завжди зручно.

Оскільки розв'язання можливих конфліктів у цьому випадку лягає на мережне устаткування кожного окремого абонента, апаратура мережного адаптера при топології «шина» виходить складнішою, ніж при інших топологіях. Однак через широке поширення мереж з топологією «шина» (Ethernet, Arcnet) вартість мережного устаткування виходить не занадто високою.

Шині не страшні відмови окремих комп'ютерів, тому що всі інші комп'ютери мережі можуть нормально продовжувати обмін. Може здатися, що шині не страшний і обрив кабелю, оскільки в цьому випадку ми одержимо дві цілком працездатні шини. Однак через особливості поширення електричних си-

гналів по довгих лініях зв’язку необхідно передбачати включення на кінцях шини спеціальних пристроїв – термінаторів. Без включення термінаторів сигнал відбивається від кінця лінії й спотворюється так, що зв’язок по мережі стає неможливим. Так що при розриві або ушкодженні кабелю порушується узгодження лінії зв’язку, і припиняється обмін навіть між тими комп’ютерами, які залишилися з’єднаними між собою. Коротке замикання в будь-якій точці кабелю шини виводить із ладу всю мережу. Будь-яку відмову мережного устаткування в шині дуже важко локалізувати, тому що всі адаптери включені паралельно, і зрозуміти, який з них вийшов з ладу, не просто.

При проходженні по лінії зв’язку мережі з топологією «шина» інформаційні сигнали послабляються й ніяк не відновлюються, що накладає жорсткі обмеження на сумарну довжину ліній зв’язку, крім того, кожний абонент може одержувати з мережі сигнали різного рівня залежно від відстані до передавального абонента. Це висуває додаткові вимоги до прийомних вузлів мережного устаткування. Для збільшення довжини мережі з топологією «шина» часто використовують кілька сегментів (кожний з яких являє собою шину), з’єднаних між собою за допомогою спеціальних відновлювачів сигналів - репітерів.

Однак таке нарощування довжини мережі не може тривати нескінченно, тому що існують ще й обмеження, пов’язані з кінцевою швидкістю поширення сигналів по лініях зв’язку.

Топологія «Зірка» - це топологія з явно виділеним центром, до якого підключаються всі інші абоненти. Весь обмін інформацією йде винятково через центральний комп’ютер, на який у такий спосіб лягає дуже велике навантаження. Зрозуміло, що мережне устаткування центрального абонента повинне бути істотно більше складним, чим устаткування периферійних абонентів. Про рівноправність абонентів у цьому випадку говорити не доводиться. Як правило, саме центральний комп’ютер є самим потужним, і саме на нього покладають всі функції по керуванню обміном. Ніякі конфлікти в мережі з топологією «зі-

рка» у принципі неможливі, тому що керування повністю централізоване, конфліктувати нема чому.

Якщо говорити про стійкість зірки до відмов комп'ютерів, то вихід з ладу периферійного комп'ютера ніяк не відбивається на функціонуванні частини мережі, що залишилася, зате будь-яка відмова центрального комп'ютера робить мережу повністю непрацездатною. Тому повинні прийматися спеціальні заходи щодо підвищення надійності центрального комп'ютера і його мережної апаратури. Обрив будь-якого кабелю або коротке замикання в ньому при топології «зірка» порушує обмін тільки з одним комп'ютером, а всі інші комп'ютери можуть нормально продовжувати роботу. На відміну від шини, у зірці на кожній лінії зв'язку перебувають тільки два абоненти: центральний і один з периферійних. Найчастіше для їхнього з'єднання використовується дві лінії зв'язку, кожна з яких передає інформацію тільки в одному напрямку. Таким чином, на кожній лінії зв'язку є тільки один приймач і один передавач. Все це істотно спрощує мережне встаткування в порівнянні із шиною й рятує від необхідності застосування додаткових зовнішніх термінаторів. Проблема загасання сигналів у лінії зв'язку також вирішується в «зірці» простіше, ніж в «шині», адже кожний приймач завжди одержує сигнал одного рівня.

Зірка, показана на рисунку, називається активною, або справжньою зіркою. Існує також топологія, що називається пасивною зіркою, що тільки зовні схожа на зірку. У цей час вона поширена набагато більше, ніж активна зірка. Досить сказати, що вона використовується в самій популярній на сьогоднішній день мережі Ethernet.

У центрі мережі з даною топологією міститься не комп'ютер, а комутатор, що виконує ту ж функцію, що й репітер. Він відновлює сигнали, що надходять, й пересилає їх в інші лінії зв'язку. Хоча схема прокладки кабелів подібна справжній або активній зірці, фактично ми маємо справу із шинною топологією, тому що інформація від кожного комп'ютера одночасно передається до всіх інших комп'ютерів, а центрального абонента не існує. Природно,

пасивна зірка виходить дорожчою звичайної шини, тому що в цьому випадку обов'язково потрібно ще й комутатор. Однак вона надає цілий ряд додаткових можливостей, пов'язаних з перевагами зірки. Саме тому останнім часом пасивна зірка усе більше витісняє справжню зірку, що вважається малоперспективною топологією.

Можна виділити також проміжний тип топології між активною й пасивною зіркою. У цьому випадку концентратор не тільки ретранслює сигнали, але й робить керування обміном, однак сам в обміні не бере участь.

Велика перевага зірки (як активної, так і пасивної) полягає в тому, що всі точки підключення зібрані в одному місці. Це дозволяє легко контролювати роботу мережі, локалізувати несправності мережі шляхом простого відключення від центра тих або інших абонентів (що неможливо, наприклад, у випадку шини), а також обмежувати доступ сторонніх осіб до життєво важливого обладнання. Загальним недоліком для всіх топологій типу «зірка» є значно більша, ніж при інших топологіях, витрата кабелю. Наприклад, якщо комп'ютери розташовані в одну лінію, те при виборі топології «зірка» знадобиться в кілька разів більше кабелю, чим при топології «шина». Це може істотно вплинути на вартість всієї мережі в цілому.

Топологія «Кільце» – це топологія, у якій кожний комп'ютер з'єднаний лініями зв'язку тільки із двома іншими: від одного він тільки одержує інформацію, а іншому тільки передає. На кожній лінії зв'язку, як і у випадку зірки, працює тільки один передавач і один приймач. Це дозволяє відмовитися від застосування зовнішніх термінаторів. Важлива особливість кільця полягає в тому, що кожний комп'ютер ретранслює (відновлює) сигнал, тобто виступає в ролі репітера, тому загасання сигналу у всьому кільці не має ніякого значення, важливо тільки загасання між сусідніми комп'ютерами кільця. Чітко виділеного центра в цьому випадку немає, всі комп'ютери можуть бути однаковими. Однак досить часто в кільці виділяється спеціальний абонент, що управляє обміном або контролює обмін. Зрозуміло, що наявність такого керуючого

абонента знижує надійність мережі, тому що вихід його з ладу відразу ж паралізує весь обмін.

Строго говорячи, комп'ютери в кільці не є повністю рівноправними (у відмінність, наприклад, від шинної топології). Одні з них обов'язково одержують інформацію від комп'ютера, що веде передачу в цей момент, раніше, а інші – пізніше. Саме на цій особливості топології й будуються методи керування обміном по мережі, спеціально розраховані на «кільце». У цих методах право на наступну передачу (або, як ще говорять, на захоплення мережі) переходить послідовно до наступного по колу комп'ютера.

Підключення нових абонентів в «кільце» звичайно зовсім безболісно, хоча й вимагає обов'язкової зупинки роботи всієї мережі на час підключення. Як і у випадку топології «шина», максимальна кількість абонентів у кільці може бути досить велика (до тисячі й більше). Кільцева топологія звичайно є самою стійкою до перевантажень, вона забезпечує впевнену роботу із самими великими потоками переданої по мережі інформації, тому що в ній, як правило, немає конфліктів (на відміну від шини), а також відсутній центральний абонент (на відміну від зірки).

Оскільки сигнал у кільці проходить через всі комп'ютери мережі, вихід з ладу хоча б одного з них (або ж його мережного встаткування) порушує роботу всієї мережі в цілому. Точно так само будь-який обрив або коротке замикання в кожному з кабелів кільця робить роботу всієї мережі неможливою. Кільце найбільш уразливе до ушкоджень кабелю, тому в цій топології звичайно передбачають прокладку двох (або більше) паралельних ліній зв'язку, одна з яких перебуває в резерві.

У той же час велика перевага кільця полягає в тому, що ретрансляція сигналів кожним абонентом дозволяє істотно збільшити розміри всієї мережі в цілому (часом до декількох десятків кілометрів). Кільце щодо цього істотно перевершує будь-які інші топології.

Недоліком кільця (у порівнянні із зіркою) можна вважати те, що до кожного комп’ютера мережі необхідно підвести два кабелі.

Іноді топологія «кільце» виконується на основі двох кільцевих ліній зв’язку, що передають інформацію в протилежних напрямках. Мета подібного рішення – збільшення (в ідеалі удвічі) швидкості передачі інформації. До того ж при ушкодженні одного з кабелів мережа може працювати з іншим кабелем (правда, гранична швидкість зменшиться).

Крім трьох розглянутих основних, базових топологій нерідко застосовується також мережна топологія «дерево» (tree), яку можна розглядати як комбінацію декількох зірок. Як і у випадку зірки, дерево може бути активним і пасивним. При активному дереві в центрах об’єднання декількох ліній зв’язку перебувають центральні комп’ютери, а при пасивному - комутатори.

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.

Коли говоримо про топологію мережі, то маємо на увазі чотири зовсім різних поняття, що ставляться до різних рівнів мережної архітектури:

- Фізична топологія (тобто схема розташування комп’ютерів і прокладки кабелів). У цьому змісті, наприклад, пасивна зірка нічим не відрізняється від активної зірки, тому її нерідко називають просто «зіркою».
- Логічна топологія (тобто структура зв’язків, характер поширення сигналів по мережі). Це, напевно, найбільш правильне визначення топології.

– Топологія керування обміном (тобто принцип і послідовність передачі права на захват мережі між окремими комп’ютерами).
– Інформаційна топологія (тобто напрямок потоків інформації, переданої по мережі).

Різновиди Ethernet Ethernet - архітектура мереж, що грунтується на логічній топології шини, з розподіленим середовищем передавання, методом доступу до середовища передавання CSMA/CD, описана стандартом IEEE802.3.

За фізичною реалізацією розрізняють: - 10Base5 - Thick ("товстий") Ethernet; - 10Base2 - Thin ("тонкий") Ethernet; - 10BaseT - Twisted-pair Ethernet (Ethernet на витій парі); - 10Broad36 - мережа на широкосмуговому 75-Омному коаксіальному кабелі; - 10BaseF - кілька варіантів мережі на оптоволоконному кабелі; - 100BaseT - стандарти Fast Ethernet на витій парі (100 BaseT4, 100 BaseTX).

Перший елемент в умовному позначенні архітектури - швидкість передавання в Мбіт/с; другий елемент позначає спосіб передавання: Base - пряме немодульоване передавання, Broad - використання широкосмугового кабелю з частотним ущільненням каналів; третій елемент - середовище передавання (T - вита пара, F - оптоволокно) або довжина сегмента кабелю в сотнях метрів (сучасні мережні адаптери дають змогу збільшувати довжину сегмента.

В рамках стандарту Ethernet створені специфікації 10BaseT, що використовує дві неекрановані виті пари UTP (Unshielded Twisted Pare) 3,4 або 5 категорій, та 100BaseT4, що грунтується на чотирьох витих парах UTP 5 категорії або екранованій витій парі STP (Shielded Twisted Pare). Для зв'язку між вузлами мережі необхідними є дві виті пари провідників: одна - для передавання, інша - для приймання інформації. Звичайно, замість двох кабелів по одній парі витих провідників у кожній використовують один кабель з чотирма парами провідників. Окрім економії та технічних переваг, це створює можливість переходу на більш швидкісні мережні архітектури без заміни самого кабелю.

Найбільш вразливе місце Ethernet на витій парі - кабельний центр, вихід з ладу якого паралізує всі вузли мережі, з'єднані з ним витими парами. Слід відмітити основні характеристики та переваги витої пари: - фізична топологія - зірка; - максимальна довжина променя - 100 м; - до кожного вузла під'єднується лише один кабель; - пошкодження кабелю виводить з ладу лише один мережний вузол; - несанкціоноване прослуховування пакетів у мережі ускладнюється.

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.

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

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

Кабельна система локальної мережі побудована на основі неекранованої витої пари категорії 5e (див.рис. 2.4).

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.

Враховуючи розміри підприємства, кількість робочих місць, вибираємо тип мережі Ethernet 1000Base T. Для цього типу мережі вибираємо топологію типу розширена зірка, . Проте враховуючи присутність безпровідної точки доступу в мережі тип топології буде гібридна.

Рисунок 2.4 - Неекранована вита пара категорії 5е

2.3 Підбір обладнання для проектованої мережі

Дана мережа побудована, як було сказано вище, за топологіями — розширена зірка та комірчата. Отримана топологія - комбінована.

Для реалізації розробки, аналізуючи план приміщень, ми побудуємо мережу на одному комутаторі рівня 2L+. Кількість розеток підприємста, котрі необхідно об’єднати - менше 48 шт, отже нам буде достатньо одного 48 портового комутатора, тим більше, що такі комутатори мають ще 2-4 порти для магістрального об’єднання комутаторів. Даний комутатор має вміти працювати з Vlan-ами для сегментації мережі.

Самі віртуальні мережі будуть створені іншим комутатором (маршрутизатором) і він же буде маршрутизувати трафік між ними а також надавати доступ до мережі інтернет.

До головного комутатора під’єднаємо лінки на точки доступу, включивши їх в окремий Vlan в цілях безпеки мережі.

Для телевізорів мережі теж передбачимо окремий Vlan.

Все описане відображено в таблиці 2.1

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

Вузол мережі	Робоча група/ номер Vlan		Номер порта головного комутатора	Адреса підмережі/Маска
1	2		3	4
A_1—A_29, A_33—A_35	office	100	1-29, 33-35	10.10.10.0/24
A_30—A_32	buch	200	30-32	10.10.20.0/24
tv_1—tv_4	tv	300	38-41	10.10.30.0/24
wifi_1—wifi_4	wifi	400	42-45	10.10.40.0/24
S_1, S_2	office	100	47,48	10.10.10.0/24

Для забезпечення потреб мережі вибір головного комутатора проведемо за даними інтерент магазину ROZETKA, засобами фільтра оберемо три комутатори. Порівняльна характеристика яких наведена у таблиці 2.2.

Таблиця 2.2 – Порівняльна характеристика 48 портових комутаторів

Параметри	TP-Link TL-SG3452P	HP Aruba Instant On 1930 JL685A	Cisco CBS250-48P-4G-EU
1	2	3	4
Тип комутатора	L3		
Можливість віддаленого управління	керований	керований	керований

Продовження таблиці 2.2

1	2	3	4
Порти	48xGbE, 4xSFP+, Мідні 1 Гбіт/с	48xGbE, 4xSFP+, Мідні 1 Гбіт/с	48xGbE, 4xSFP+, Мідні 1 Гбіт/с
Підтримка PoE	Так Від 250 - 500 Вт	ні	Так Від 250 - 500 Вт
Ціна	31 500 грн.	28 200 грн.	41 600 грн

Виходячи з таблиці 2.2, враховуючи співвідношення ціни до технічних характеристик пристрою для мережі вибрано комутатор TP-Link TL-SG3452P , зовнішній вигляд якого зображено на рисунку 2.4 а докладні характеристики в таблиці 2.3. Він по ціні дорожчий, але термін гарантії та наявність POE портів я вважаю перевагою.

Рисунок 2.4– Зовнішній вигляд комутатора TP-Link TL-SG3452P

Таблиця 2.3 - Докладні характеристики комутатора

параметр	Значення
1	2
Тип:	керований L3
Комутаційна матриця:	104 Гбіт/с

Продовження таблиці 2.3

1	2
Швидкість пересилання пакетів:	77.4 Mpps
Таблиця MAC-адрес:	16 тис. адрес
Кількість портів Gigabit Ethernet:	48 шт.
Кількість портів SFP+:	4 шт.
Кількість портів з підтримкою PoE:	48 шт.
Стандарт PoE:	802.3af/at
Порти управління:	1 × RJ-45,1 × USB
Особливості:	можливість встановлення у стійку
Тип охолодження:	активне, 3 вентилятори
Діапазон робочих температур:	0...40 °C
Живлення:	AC 100...240 В

Аналогічно оберемо маршрутизатор. Для вибору виставимо фільтр по ціні до 50 тисяч грн, можливість працювати з Vlan, та кількість портів не більше 8, згідно з таблицею 2.1. Технічні характеристики маршрутизаторів наведені в таблиці 2.4.

Таблиця 2.4 – Порівняльна характеристика маршрутизаторів

	Mikrotik CCR2004-16G-2S+PC	Cisco RV016-G5	Cisco RV260P
1	2	3	4

Управління	керований	керований	керований

Продовження таблиці 2.4

1	2	3	4
Управління	керований	керований	керований
Порти	2 x SFP, 16 x Gigabit	16 x Fast Ethernet	8 x RJ-45 10/100/1000 Мбит/с LAN 1 x RJ-45/SFP Combo 10/100/1000 Мбит/с WAN
Гарантія	24 місяців	24 місяців	24 місяців
Ціна	16 700 грн	22 617 грн	15 500 грн

Виходячи з таблиці 2.4, враховуючи співвідношення ціни до технічних характеристик пристрою для мережі обрано комутатор Mikrotik CCR2004-16G-2S+PC, зовнішній вигляд якого зображено на рисунку 2.5.

Рисунок 2.5 – Зовнішній вигляд Mikrotik CCR2004-16G-2S+PC

- Пристрій до 300% швидше за попередні маршрутизатори. Вбудований комутатор. Керований.
- Призначення - Промисловий

- Інтерфейси - 16 портів Gigabit Ethernet, 1 порт USB 3.0 /type A, 1 порт serial RJ45, 2 x 10G SFP+ порту
- Роз'єм живлення: 2 xDC jack
- Пам'ять - Об'єм оперативної пам'яті: 4 ГБ, Об'єм флеш-пам'яті: 128 МБ NAND
- Процесор - Annapurna Alpine AL32400
- Кількість ядер процесора - 4
- Номінальна частота процесора, ГГц - 1.7
- Операційна система - MikroTik RouterOS /(v7 only)
- живлення - Зовнішній БП
- Габарити - 44 x 272 x 195 мм, 1U

У мережі використовується безпровідна точка доступу, ми зупинили наш вибір на моделі Mikrotik cAP XL ac (RbcAPGi-5acD2nD-XL). Тут порівняння ми навіть не робимо, ми просто підбираємо по потрібних параметрах. Порівняння не робимо, оскільки головний маршрутизатор цієї ж фірми, і він має здатність створювати єдину безпровідну мережу, котра побудована з кількох точок доступу. Зовнішній вигляд точки показано на рисунку 2.6.

Рисунок 2.6 – Зовнішній вигляд безпровідної точки доступуMikrotik cAP XL ac (RbcAPGi-5acD2nD-XL)

Докладні технічні характеристики обраної точки:

Діапазон робочих частот	2.4/5 GHz
Бездротовий стандарт	2.4 GHz - 802.11b/g/n, 5 GHz - 802.11ac
Процесор	IPQ-4019
Номінальна частота процесора	710 MHz
Кількість ядер процесора	4
Об'єм оперативної пам'яті	128 MB
Розмір сховища даних	16 MB
Тип сховища даних	FLASH
Мережевий інтерфейс	(2) 10/100/1000 Ethernet порту
Посилення антени	2.4 GHz – 6 dBi/5 GHz – 5.5 dBi
Кількість каналів	2.4 GHz - 2/5 GHz -2
Діаграма спрямованості антени	360°
Операційна система	RouterOS
Рівень ліцензії	4
Джерело живлення	24V 1.2A адаптер; PoE in 802.3af/at
Роз'єм живлення	1 (PoE-IN)
Підтримувані формати вхідної напруги	17-57 V PoE out, Passive PoE до 57V
Максимальне енергоспоживання, Вт	24
Діапазон температур, °C	-40 до +70
Розміри, мм	191 x 42
Вага, г	650

У комп’ютерній мережі передбачено використання комп’ютерів в якості двох серверів. Дані компютери ми оберемо аналогічно. Критеріями вибору серверів будуть: процесор Intel I3, з 8+ Gb памяті, та двома ссд на 240 Гб для системи. Технічна характеристика обраного ПК наведена у таблиці 2.5.

Таблиця 2.5 – Характеристики сервера ARTLINE Business R15 v14

Параметр	Значення
1	2
Тип процесора	Чотириядерний Intel Core i3-10100 (3.6 — 4.3 ГГц)
Об'єм оперативної пам'яті	16 ГБ
Тип пам'яті	DDR4 2400
Тип відеокарти і об’єм відеопам'яті	Інтегрована, Intel HD Graphics
Чіпсет материнської плати	PRIME H570M-PLUS
Об'єм HDD	2 SSD 256
Оптичний привід	-
Форм-фактор	2U Rackmount
Гарантія	36 місяців
Ціна	23 000 грн

Сервер ARTLINE Business R15v14 побудований на базі материнської плати Asus Prime H570-PLUS. Плата підтримує процесори Intel 10 та 11 покоління. З особливостей: оптимізована система живлення, повноцінне охолодження та утиліта Fan Xpert 2+, технологія OptiMem для стабільної роботи модулів пам'яті, сучасні інтерфейси: PCIe 4.0, два слоти M.2, 1G Ethernet (контролер Intel), USB 3.2 Gen2 Type-C та внутрішній роз'єм Thunderbolt 4.

До серверів добавимо по два гдд на 4 Тб для інформації підприємства. Всі вінчестера об'єднаємо в RAID масив дзеркало, ціна ПК зросте на 8 000 грн.

Отже, ми обрали таке обладнання:

маршрутизатор — 1 шт — 16 700 грн - Mikrotik CCR2004-16G-2S+PC

комутатор головний - 1 шт — 31 500 грн - TP-Link TL-SG3452P

точка доступу — 4 шт — 3 500 грн - Mikrotik cAP XL ac (RbcAPGi-5acD2nD-XL)

сервер — 2 шт — 31 000 грн- ARTLINE Business R15v14+

2.4 Особливості монтажу мережі [14]

Щоб кабель передавав дані без втрат, сигнал був якісним, а швидкість залишалася на належному рівні важливо правильно вибрати та прокласти кручену пару.

Вибір кручений пари

Насамперед, слід визначитися, де монтуватиметься кабель: у приміщенні або на вулиці. Внутрішні моделі оснащуються щільними оболонками з полівінілхлориду, часто вогнетривкими. Така ізоляція добре захищає провідники від перегинів, пилу та вологи. Однак вона не стійка до ультрафіолету та морозів, сильних механічних навантажень. Тому для вуличної прокладки варто вибирати спеціальну зовнішню кручену пару. Оболонка такого кабелю виготовляється із щільного поліетилену. Він забезпечує стійкість до перепадів температури, прямим сонячним променям та механічним ушкодженням.

Примітка: зовнішні кабелі зазвичай менш гнучкі, ніж внутрішні. Це важливо врахувати під час проведення монтажних робіт.

Окрім способу прокладання, при виборі варто орієнтуватися на матеріал провідників. їх роблять із сталі, алюмінію та міді.

Також часто зустрічаються біметалічні варіанти - алюмінієві з мідним покриттям. Найкраще - мідний варіант. Він забезпечує якісніший сигнал, та до перегинів стійкіший.

Також важливо врахувати технічні характеристики, такі як категорію, кількість пар та екранування.

Категорія свідчить про максимальну швидкість передачі.

Що стосується типу екранування, то все залежить від умов монтажу. Якщо провід планується прокладати поруч із джерелами електромагнітного випромінювання (трансформаторами, електронікою), треба брати екранований кабель. Найпоширеніші - це FTP, із загальним для всіх пар екраном у вигляді фольги, і STP - з екраном у вигляді металевого обплетення. Але й інші варіанти. Екран захищає від радіочастотних перешкод.

Особливості монтажу крученого кабелю

Прокладання дроту у приміщенні. Ідеальний варіант - монтувати кабель усередині стіни, підлоги чи стелі. У цьому випадку його укладають у перекриттях, розміщуючи в гофрованих трубах або металорукавах. Головний плюс - провід добре захищений від зовнішніх впливів. Ще одна перевага — після ремонту кабелів не видно. У стіну, підлогу чи стелю можна укласти кабель, тільки якщо в приміщенні ще не зроблено ремонт.

У відремонтованому приміщенні можна прокласти кабель у спеціальному коробі. Найчастіше - пластиковому. Він може кріпитися на стіну замість плінтуса і на стелю. Фіксуються короби просто: на клей або шурупи. Перевага такого способу - легкий монтаж. Є варіанти, розраховані на різну кількість кабелів, що відрізняються діаметром. У такого способу прокладання є плюси:

- простота обслуговування та легкість розширення мережі: щоб відремонтувати провід, прокласти нову лінію, треба просто зняти кришку кабель- каналу;
- додатковий захист: короб береже провід від перегинів, вологи та илу.

При прокладанні кабелю в каналі паралельно з електропроводкою варто поставити перегородку, яка розділить мережеву та силову частини. Це захистить від електромагнітного випромінювання.

Ще один метод внутрішнього монтажу - прокласти кабель по периметру приміщення та закріпити скобами. Недоліки способу - відсутність додаткового захисту дроту і порушення естетичності. Плюси - простота та невисока вартість прокладки.

При монтажі слід дотримуватися радіуса вигину, який виробник зазвичай вказує в характеристиках дроту. В іншому випадку ви ризикуєте поламати провідники.Зазначимо, що найкраще підключати комп'ютери та мережеві пристрої за допомогою спеціальних сполучних шнурів на основі крученої пари — литих патч-кордів. Це кабель, який обтиснутий конекторами з обох кінців. Однак якщо відстань між комутованими девайсами велика, довжини патчкорду може не вистачити.

З особливостей прокладки кабелю в даній мережі слід наголосити таке:

- всі робочі місця обладнанні розетками RJ45, котрі розміщені на стіні приміщення на висоті 30 см від підлоги (це показано на листі — фізична топологія), Розетки А1-А8 виконані в підлогових лючках, і йдуть в підлзі в гофротрубі до серверної. Точне місце визначається проектом для меблювання приміщення.
- до розетки кабель монтується в стіні в штробах з підйомом понад стелею Армстронг, там він зібраний пучками та йде до ІТ відділу де він спускається в коробі 100х100 мм до комутаційної шафи та закінчується “забитим” в пач-панель,
- аналогічно проведені розетки для телевізорів, лише вонии знаходяться на відповідній сті на висоті 1600 мм над підлогою,
- розетки точок доступу також проведені аналогічно, але вони знаходяться понад стелею Армстронг у вказаних місцях по схемі, котра зображена на листі — Фізична топологія. Там понад стелею варто забезпечити надлишок кабелю, скрученого в міні бухти, довжиною 3-5 метрів, для можливості радіопланування.

2.5 Тестування мережі [10]

Тестування комп'ютерної мережі є завершальним етапом монтажу комп'ютерної мережі, а також необхідною умовою її прийняття в експлуатацію.

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

Що таке тестування комп'ютерної мережі?

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

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

- детальне вивчення роботи мережі
- оцінка якості сигналів, що передаються
- виявлення «прихованих» дефектів
- визначення «вузьких місць» продуктивності серверів
- оцінка захищеності мережі від вторгнення внутрішніх та зовнішніх порушників
- внесення необхідних доповнень та коректив
- завершальне регулювання налаштувань обладнання
- усунення несправностей у роботі

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

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

Несправності фізичного рівня можуть виникнути у мережному пристрої, середовищі передачі або в місці їх контакту. Вони найпростіше піддаються виявленню, оскільки мають постійний характер (природно, досі їх усунення). Локалізувати несправність можна зокрема за допомогою найпростіших тестерів для локальних мереж. Такі тестери перевіряють роботу каналу в один бік (від тестера до концентратора або мережної плати комп'ютера). Якщо дефект має місце в середовищі передачі, його можна виявити за допомогою кабельного тестера. Плаваючі помилки, зумовлені поганим контактом у з'єднувачах, діагностувати дещо складніше. Але навіть такі несправності можна виявити за допомогою кабельного тестера – достатньо бути уважним. До речі, хоч як це банально звучить, але хочеться нагадати, що найкращий спосіб профілактики утворення дефектів у середовищі передачі - використання якісних матеріалів та виконання професійного монтажу.

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

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

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

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

Незважаючи на всі переваги, портативні мережеві тестери мають один недолік - вони не можуть перехоплювати і декодувати пакети. І якщо такі можливості необхідні, наприклад, для більш глибокого вивчення проблем функціонування мережних додатків, тоді вам варто звернути увагу на аналізатори протоколів. Фактично вони є комп'ютером з одним або кількома мережевими

інтерфейсами, зі спеціалізованим програмним забезпеченням. Деякі з цих аналізаторів можуть розуміти дві сотні (!) різних протоколів. Кожен як мінімум здатний перехоплювати пакети та фільтрувати їх відповідно до заданих параметрів. Використовуючи відповідні фільтри, ви можете отримати масу різної інформації, що іноді виявляється просто незамінною. Надалі збережена інформація може бути оброблена для складання узагальненого зведення про пакети та отримання детального резюме про протоколи, що використовуються в них. Крім того, всі аналізатори фіксують час проходження пакета та показують мережеві та фізичні адреси його відправника та одержувача.

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

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

2.6 Захист комп’ютерної мережі

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 конфіденційність.

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.

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. При роботі над пунктом використано [17]

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Налаштування маршрутизатора

Налаштування виконується через програму WinBox. (див.рис. 3.1)

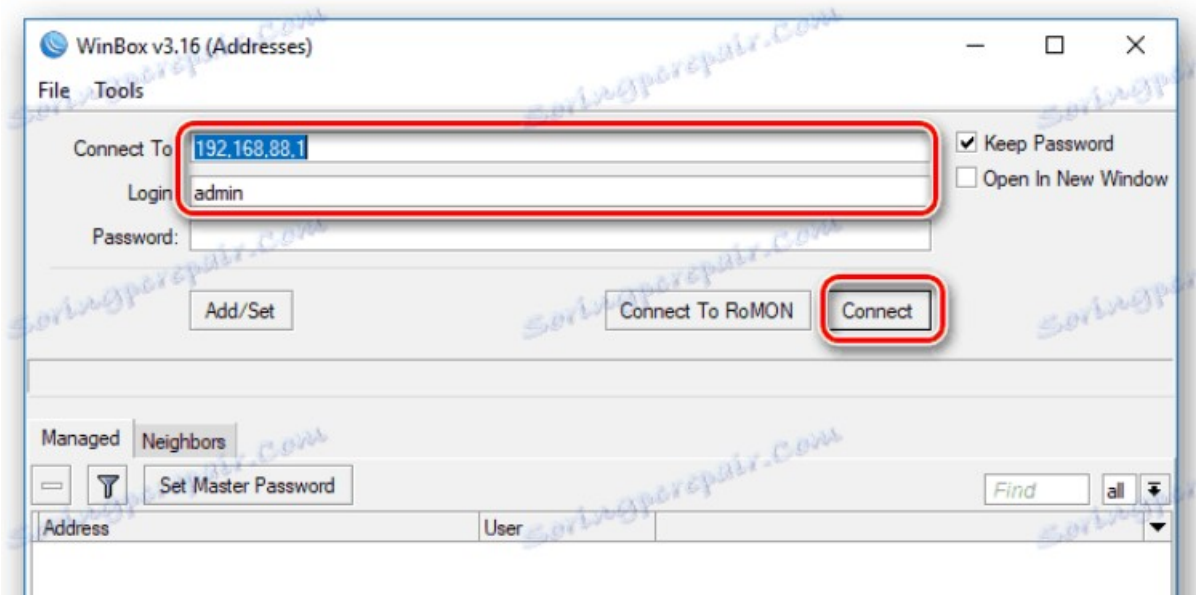

Рисунок 3.1 - Загальний вигляд вікна програми WinBox

Підключаємось до роутера, скидаємо конфігурацію на порожню (blank).

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

Підключаємося до роутера за MAC-адресою.

Створюємо VLAN.

Створюємо інтерфейс VLAN100, VLAN200, VLAN300, VLAN400, .

/interface vlan add name=VLAN100 vlan-id=100 interface=ether5

/interface vlan add name=VLAN200 vlan-id=200 interface=ether5

/interface vlan add name=VLAN300 vlan-id=300 interface=ether5

/interface vlan add name=VLAN400 vlan-id=400 interface=ether5

IP-адреси для інтерфейсів.

/ip address add interface=VLAN100 address=10.10.10.1/24 network= 10.10.10.0

/ip address add interface=VLAN200 address=10.10.20.1/24 network= 10.10.20.0

/ip address add interface=VLAN300 address=10.10.30.1/24 network= 10.10.30.0

/ip address add interface=VLAN400 address=10.10.40.1/24 network= 10.10.40.0

DHCP-сервер для VLAN.

/ip dhcp-server network add address=10.10.10.0/28 gateway=10.10.10.1 dns-server=10.10.10.1

/ip pool add name=VLAN100-POOL ranges=10.10.10 .2- 10.10.10.200

/ip dhcp-server add address-pool=VLAN100-POOL disabled=no interface=VLAN100 name=DHCP-VLAN100

/ip dhcp-server network add address=10.10.20.0/28 gateway=10.10.20.1 dns-server=10.10.20.1

/ip pool add name=VLAN200-POOL ranges=10.10.20 .2- 10.10.20.200

/ip dhcp-server add address-pool=VLAN200-POOL disabled=no interface=VLAN200 name=DHCP-VLAN200

/ip dhcp-server network add address=10.10.30.0/28 gateway=10.10.30.1 dns-server=10.10.30.1

/ip pool add name=VLAN300-POOL ranges=10.10.30 .2- 10.10.30.200

/ip dhcp-server add address-pool=VLAN300-POOL disabled=no interface=VLAN300 name=DHCP-VLAN300

/ip dhcp-server network add address=10.10.40.0/28 gateway=10.10.40.1 dns-server=10.10.40.1

/ip pool add name=VLAN400-POOL ranges=10.10.40 .2- 10.10.40.200

/ip dhcp-server add address-pool=VLAN400-POOL disabled=no interface=VLAN400 name=DHCP-VLAN400

Налаштування VLAN завершено.

Далі слід виконати базові налаштування локальної мережі, Інтернету, безпеки тощо.

Створення мосту (bridge).

/interface bridge add name=bridge1

Додавання портів у міст.

/interface bridge port add bridge=bridge1 interface= VLAN100 hw=yes

/interface bridge port add bridge=bridge1 interface= VLAN200 hw=yes

/interface bridge port add bridge=bridge1 interface= VLAN300 hw=yes

/interface bridge port add bridge=bridge1 interface= VLAN400 hw=yes

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

Призначення IP-адреса для мосту локальної мережі.

/ip address add interface=bridge1 address=192.168.1.1/24

Отримання зовнішньої IP-адреси.

DHCP Client.

/ip dhcp-client add interface=ether1 disabled=no

DNS.

/ip dns set servers=192.168.1.1 allow-remote-requests=yes

Створення правила NAT для доступу в Інтернет.

/ip firewall nat add action=masquerade chain=srcnat out-interface=ether1

Правила фільтрації в Firewall.

1.Правило дозволяє вхідні пакети від встановлених та пов'язаних (з раніше дозволеними) з'єднань.

/ip firewall filter add action=accept chain=input connection-state=established,related comment="RULE 1 accept established,related"

2.Правило відкидає невірні пакети вхідного трафіку.

/ip firewall filter add action=drop chain=input connection-state=invalid comment=" RULE 2 drop invalid"

3.Правило дозволяє трафік ICMP протоколу. Використовується для Ping, Traceroute.

/ip firewall filter add action=accept chain=input protocol=icmp comment=" RULE 3 accept ICMP"

4.Правило відкидає весь трафік, що йде від інтерфейсів локальної мережі.

/ip firewall filter add action=drop chain=input in-interface=!bridge1 comment=" RULE 4 drop all not coming from LAN"

Правила транзитного трафіку.

5.Правило дозволяє проходить трафік для пакетів у з'єднаннях established, related, untracked

/ip firewall filter add action=accept chain=forward connection-state=established,related,untracked comment=" RULE 5 accept established,related, untracked"

6.Правило відкидає невірні пакети трафіку, що проходить.

/ip firewall filter add action=drop chain=forward connection-state=invalid comment=" RULE 6 drop invalid"

7. Правило відкидає прохідний трафік із зовнішньої мережі, що не відноситься до NAT.

/ip firewall filter add action=drop chain=forward connection-nat-state=!dstnat connection-state=new in-interface=ether1 comment=" UA 7 drop all from WAN not DSTNATed"

У нижньому рядку потрібно розмістити правило, що забороняє все інше по входу роутера.

/ip firewall filter add action=drop chain=input in-interface=ether1 comment="F

Інтерфейс доступу.

/ip service set telnet disabled=yes

/ip service set ftp disabled=yes

/ip service set www disabled=yes

/ip service set ssh disabled=yes

/ip service set api disabled=yes

/ip service set api-ssl disabled=yes

Налаштування дати та часу.

/system ntp client set enabled=yes primary-ntp=88.147.254.230 secondary-ntp=88.147.254.232

Ідентифікатор роутера.

/system identity set name=SW2

Резервна копія конфігурації.

/system backup save name=config1

В мережі використовуються точки доступу цього самого виробника, для їх роботи потрібно налаштувати програмний контролер, котрий буде керувати безпровідною мережею.

Настроювання CAPsMAN на роутері MikroTik

Основне завдання, яке виконує контролер CAPsMAN , це управління всіма пристроями MikroTik . На його базі створюється єдиний центр управління трафіком та моніторинг роботи WiFi мережі. Між точками доступу створюються суміжні зони покриття таким чином, щоб при переході з однієї зони до іншої з'єднання WiFi мало можливість швидкого перемикання. Подібне швидке перемикання дозволяє залишатися онлайн без необхідності ручного перемикання.

Обладнання MikroTik суттєво відрізняється від своїх конкурентів наявністю у прошивці менеджера управління WiFi мережами

Увімкнути контролер CAPsMAN

Налаштування знаходиться в CAPsMAN→CAP Interface→Manager (див. рис 3.2)

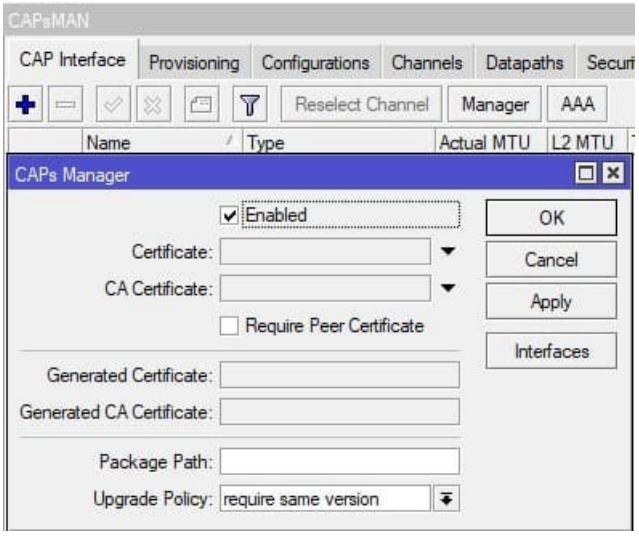

Рисунок 3.2 - Ввімкнення контролера CAPsMAN у WinBox

Далі послідовно робимо наступне:

Визначення частотних каналів CAPsMAN

/caps-man channel

add band=2ghz-b/g/n control-channel-width=20mhz extension-channel=XX \

frequency=2412,2437,2462 name=2G

add band=5ghz-a/n/ac control-channel-width=20mhz extension-channel=XXXX name=\ 5G

Налаштування CAPsMAN Datapath

/caps-man datapath

add client-to-client-forwarding=yes local-forwarding=yes name=Datapath

Налаштування пароля CAPsMAN

/caps-man security

add authentication-types=wpa2-psk encryption=aes-ccm group-encryption=aes-ccm \

group-key-update=20m name=IT_Ware passphrase=11223344

Загальна конфігурація CAPsMAN

/caps-man configuration

add channel=2G country=no_country_set datapath=Datapath installation=any \

mode=ap name=2G rx-chains=0,1,2,3 security=Security ssid=Home tx-chains=\

0,1,2,3

add channel=5G country=no_country_set datapath=Datapath installation=any \

mode=ap name=5G rx-chains=0,1,2,3 security=Security ssid=Home tx-chains=\

0,1,2,3

/caps-man manager set enabled=yes upgrade-policy=require-same-version

CAPsMAN Provisioning, поширення конфігурації на точки доступу

/caps-man provisioning

add action=create-dynamic-enabled hw-supported-modes=ac master-configuration=\

5G name-format=prefix-identity name-prefix=5G

add action=create-dynamic-enabled hw-supported-modes=gn master-configuration=\

2G name-format=prefix-identity name-prefix=2G

3.2 Налаштування точки доступу [11]

Для початку необхідно підключити точки до портів головного комутатора SW1 згідно листа “логічна топологія”. Далі необхідно за допомогою програму WinBox підключитися до точки та послідовно внести в неї наступну конфігураці (це робиться в меню термінал):

Створення Bridge на точці доступу

/interface bridge

add admin-mac=02:F1:41:46:46:E2 auto-mac=no name=Bridge-LAN

Додавання портів до Bridge для точки доступу

Підключити точку доступу до CAPsMAN

/interface wireless

managed by CAPsMAN

channel: 2462/20-eC/gn(28dBm), SSID: Home, CAPsMAN forwarding

set [find default-name=wlan1] ssid=MikroTik station-roaming=enabled

managed by CAPsMAN

channel: 5200/20-eCee/ac(14dBm), SSID: Home, CAPsMAN forwarding

set [find default-name=wlan2] ssid=MikroTik station-roaming=enabled

/interface wireless security-profiles

set [find default=yes] supplicant-identity=MikroTik

/user group

set full policy="local,telnet,ssh,ftp,reboot,read,write,policy,test,winbox,pas\

sword,web,sniff,sensitive,api,romon,dude,tikapp"

```
/interface bridge port
add bridge=Bridge-LAN interface=ether1
add bridge=Bridge-LAN interface=ether2
/interface wireless cap
set bridge=Bridge-LAN discovery-interfaces=Bridge-LAN enabled=yes interfaces=\
wlan1,wlan2
/ip dhcp-client
add disabled=no interface=Bridge-LAN
```

Присвоїти ідентифікатор для точки доступу

```
/system identity
set name=AP_1
/system scheduler
add name=Auto-Upgrade-Firmware on-event="if ([/system routerboard get current-\
firmware] != [/system routerboard get upgrade-firmware]) do={\r\
\n/system routerboard upgrade\r\
\n:delay 15s\r\
\n/system reboot\r\
\n}" policy=\
ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon \
start-time=startup
/tool ??romon
set enabled=yes
```

Правило MikroTik CAPsMAN для безшовного роумінгу

```
add action=reject allow-signal-out-of-range=10s disabled=no interface=all \
signal-range=-120..-85 ssid-regexp=""
```

3.3 Налаштування головного комутатора

Налаштування головного комутаторами

Для налаштування головного комутатора необхідно запустити будь-який браузер, і в адресному вікні набрати IP адресу комутатора- 192.168.0.1. сам комутатор повинен бути підключений в мережу.

Далі буде стандартна процедура авторизиції, в результаті якої ми попадаємо в головне вікно WEB інтерфейсу, котре показане на рисунку 3.3.

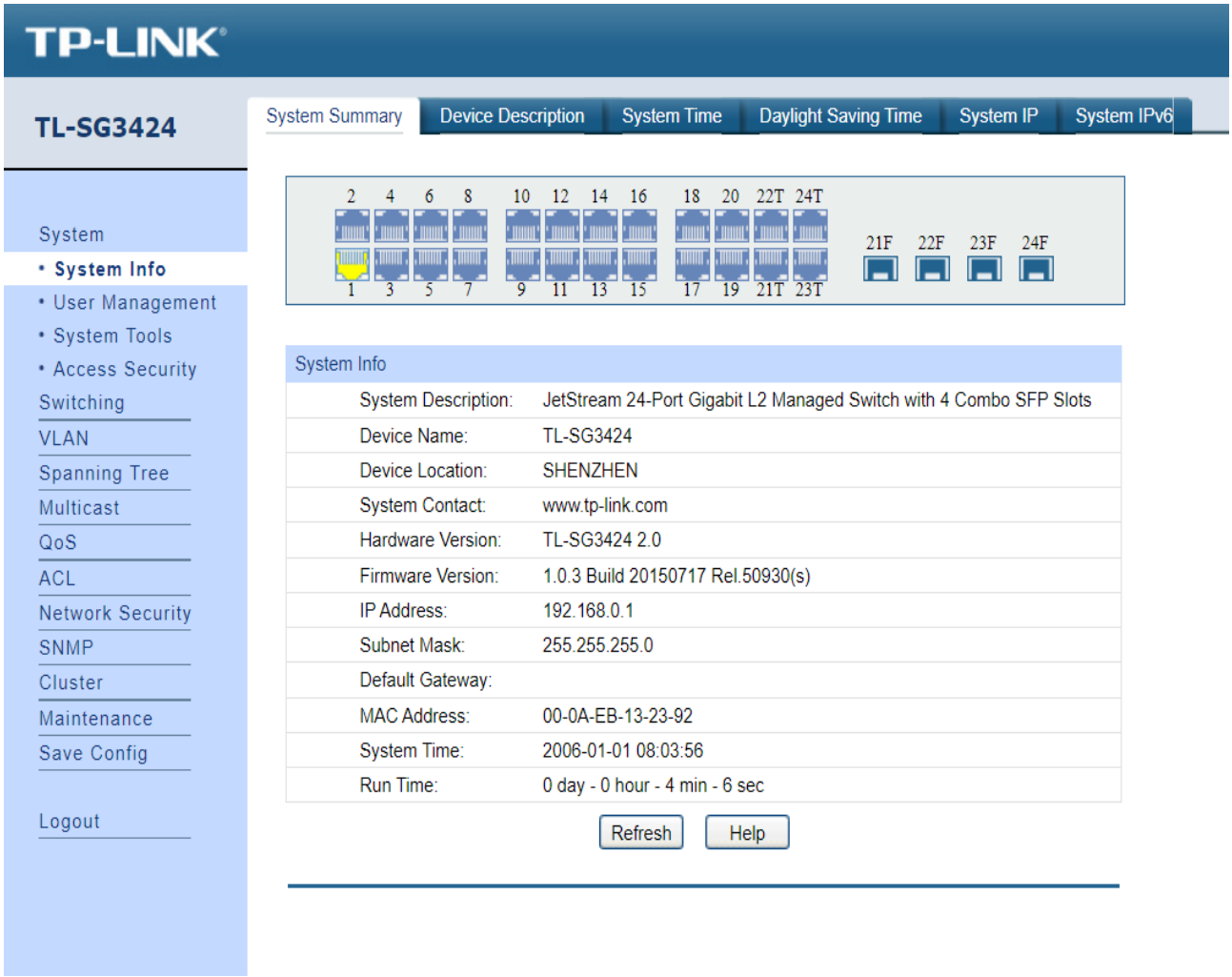

Рисунок 3.3 - Головне вікно WEB інтерфейсу комутатора

Для роботи проектованої мережі нам необхідно на комутаторі створити необхідні Vlan-и та привязати їх до певних портів. Для прикладу на рисунку 3.4 показано створення Vlan100 та привязка її до портів 1-4,7.

Згідно з таблицею 2.1 — ми створимо Vlan100 і прив'яжемо до портів 1-29, 33-35, 47,48. Аналогічно створимо Vlan 200 (порти 30-32), Vlan300 (порти 38-41), Vlan400 (порти42-45).

Далі нам необхідно вказати, тип порту -Access чи Trunk (див.рис. 3.5). Це робиться в меню PortConfig, де ми просто конкретному порту вказуємо його тип, це показано на рисунку . У нас всі порти Access, лише 49 порт буде Trunk, оскільки він служить для зв'язку з маршрутизатором.

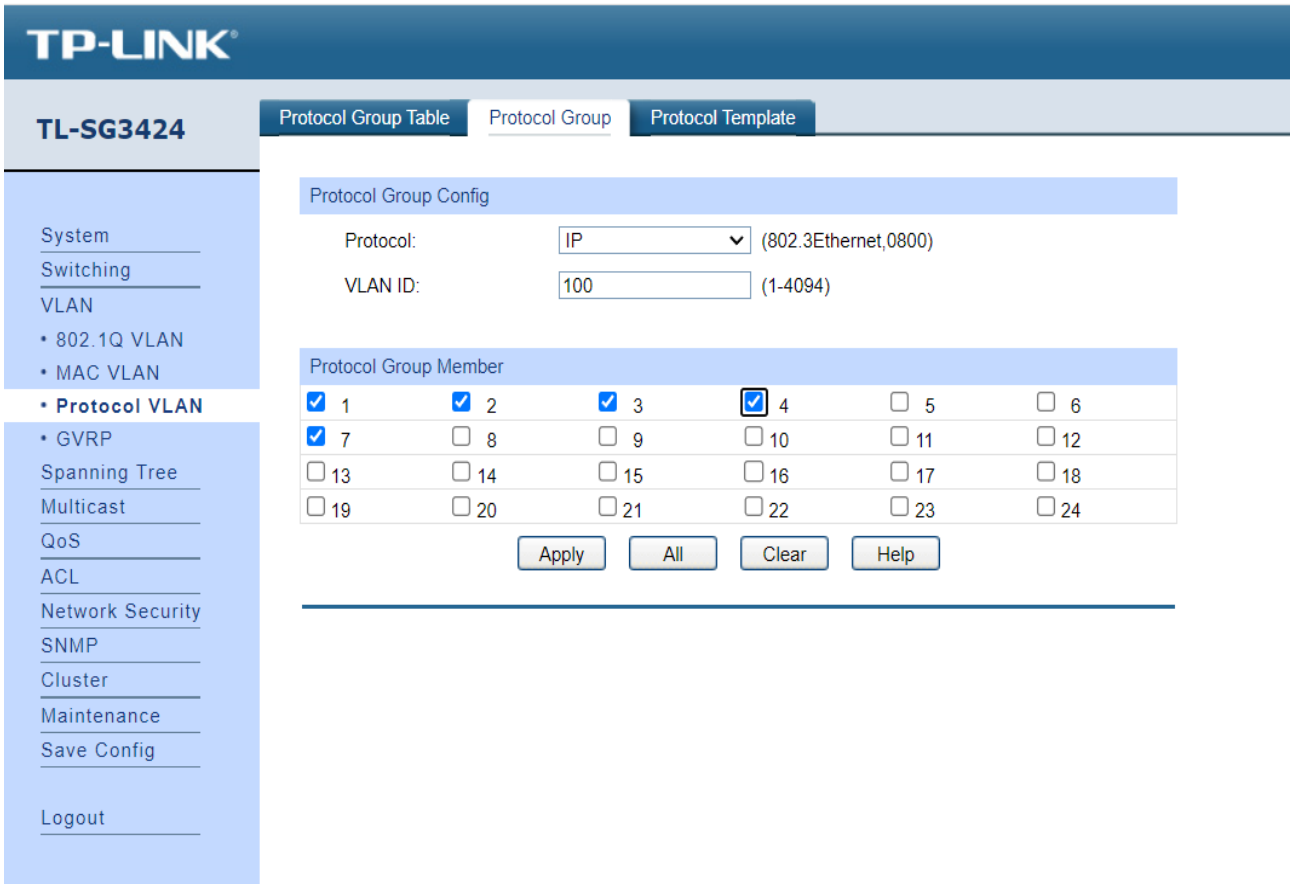

Рисунок 3.4 - Створення необхідних Vlan та привязка її до певного порту

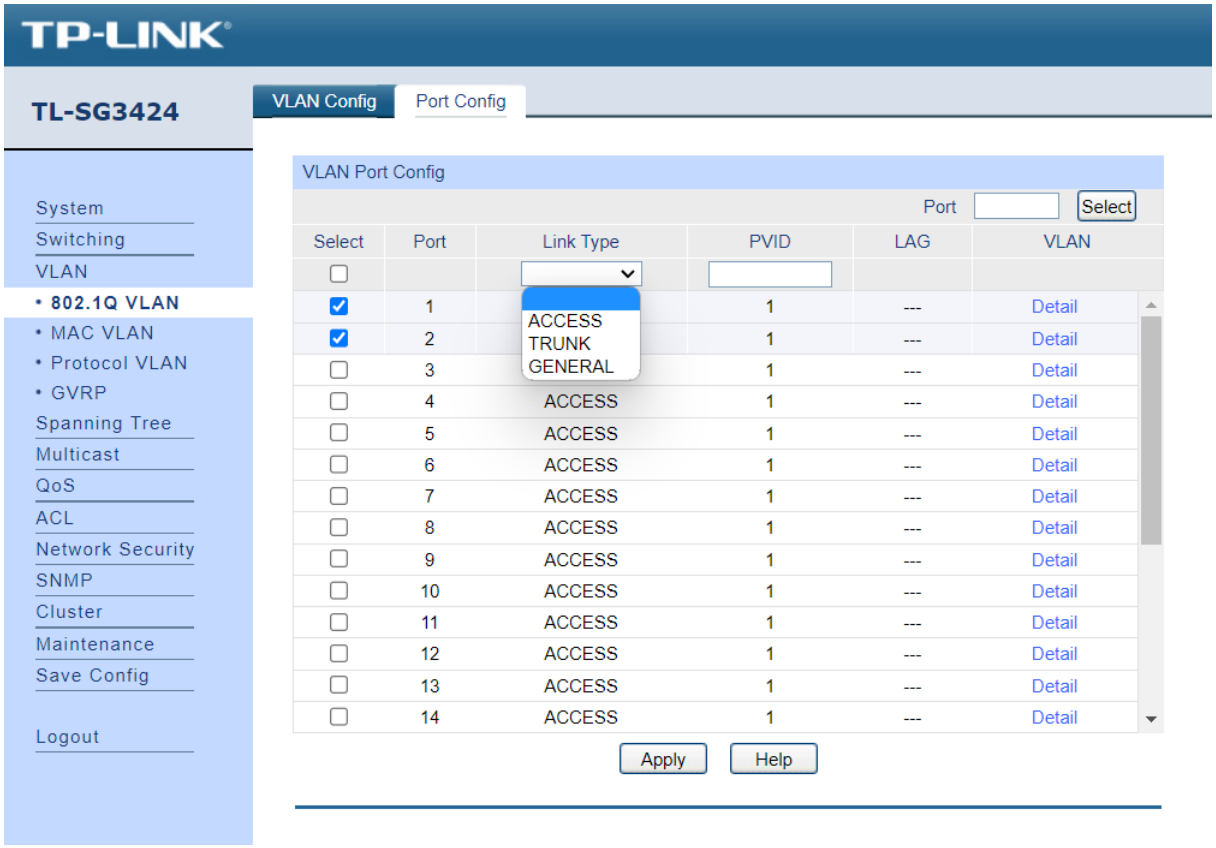

Рисунок 3.5 - Вказування типу роботи порта

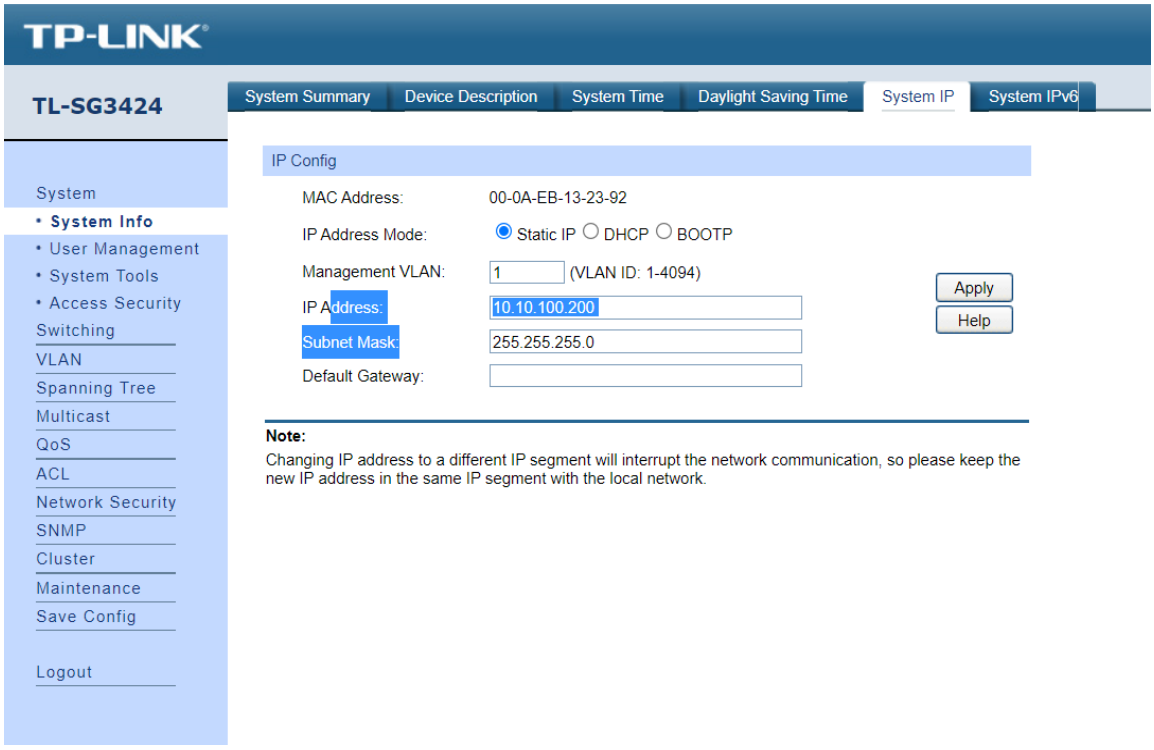

Рисунок 3.6 - Зміна IP адреси комутатора

Меню SystemIP дозволяє змінити IP адресу комутатора. Нам її необхідно змінити на 10.10.100.200.(див.рис. 3.6)

3.4 FreeNAS встановлення та налаштування [12,13]

FreeNAS – це операційна система для мережного зберігання даних. Вона заснована на FreeBSD та підтримує CIFS , NFS , iSCSI , FTP , RSYN , а також RAID . Це веб-інструмент з відкритим вихідним кодом та один із найвідоміших інструментів централізованого керування зберіганням даних.

Підтримує файлові системи ZFS . Знімки ZFS можна використовувати для створення віддаленого резервного копіювання. Також додаткові знімки однієї і тієї ж файлової системи можуть бути створені інкрементально. У разі збою локального диска, будь-який знімок ZFS може бути відправлений на нову файлову систему ZFS для відновлення даних.

Безпека даних

RAID-Z є частиною RAID у файловій системі ZFS . Файлова система ZFS забезпечує цілісність даних протягом усього. Кожна файлова система перевіряється контрольними сумами згори до низу.

Шифрування даних

FreeNAS має унікальну функцію шифрування даних у файловій системі ZFS , яка недоступна в інших проектах Open Source NAS. А також доступне шифрування даних на весь том. Зашифрований том доступний для читання тільки тим користувачам FreeNAS , які мають майстер-ключ для цього тому. За бажанням користувач може використовувати парольну фразу для додаткового рівня безпеки.

Можливо вам буде цікаво: Як у Linux форматувати флешку у exFAT

Спільне використання файлів у FreeNAS

Ви можете обмінюватись даними з FreeNAS як професіонал. Він підтримує всі основні операційні системи з методами обміну даними SMB , CIFS (MS

Windows), NFS (Unix/Linux), AFP (Apple), а також FTP або iSCSI . Крім того, він підтримує VMware VAAI , MS ODX , кластеризацію на базі MS Server 2008 та 2012 R2 .

Управління на основі веб-інтерфейсу

Будь-який аспект FreeNAS може керуватися за допомогою Web-інтерфейсу. За допомогою веб-панелі адміністратора можна керувати всім, включаючи створення томів, налаштування прав користувачів або оновлення програмного забезпечення. У FreeNAS також доступний ssh .

Плагіни

Для розширення можливостей FreeNAS доступно безліч модулів, що під-ключаються, і плагінів сторонніх виробників. Вони дозволяють користувачеві використовувати різні програми відповідно до його потреб.

Ось деякі з доступних плагінів:

Bacula – для резервного копіювання на основі мережі.

Couchpotato – автоматичний завантажувач торентів.

Crashplan – резервне копіювання даних на віддалений сервер або комп'ютери.

Owncloud - управління персональною хмарою.

Вимоги до встановлення FreeNAS

- Апаратне забезпечення на базі процесора x64 біт
- 4 ГБ ОЗУ
- Мінімум 1 ТБ сховища

Можливо вам буде цікаво: Увімкнути SSH на Fedora

Встановлення FreeNAS на сервер чи ПК

Завантажте FreeNAS за цим посиланням . Запишіть образ ISO на DVD або зробіть завантажувальний usb-накопичувач .

Далі увімкніть комп'ютер або сервер і запустіть процес інсталяції. Як на зображенні виберіть 1 і натисніть Enter.

Початок встановлення FreeNAS

Далі потрібно вибрати пристрій зберігання, після чого натисніть OK .

Вибір пристрою зберігання

Тепер натисніть ' Yes ', щоб підтвердити процес встановлення.

Продовжити встановлення FreeNAS

Далі потрібно ввести кілька разів пароль адміністратора та натиснути OK.

Встановлення пароля адміністратора

Після завершення процесу встановлення система попросить перезавантажитись. Натисніть OK і вийміть завантажувальну флешку.

Завершення встановлення

При завантаженні FreeNAS вам потрібно вибрати Звичайне завантаження (Normal Bootup).

Завантаження FreeNAS

Після завершення завантаження з'явиться меню, яке включає всі інструменти керування. Зверніть увагу на вказану ip-адресу, яку ми будемо використовувати для керування FreeNAS .

Налаштування FreeNAS

Відкрийте веб-переглядач і перейдіть за адресою http://IP-address/ .

Увійдіть у систему під ім'ям користувача ' root ' та паролем, який був заданий у процесі установки.

Далі з'явиться майстер керування FreeNAS , в ньому доступні різні опції для керування, наприклад резервним копіюванням.

Web інтерфейс FreeNAS

Можливо вам буде цікаво: Як увімкнути автоматичне оновлення Ubuntu 20.04

Використовуючи консоль управління FreeNAS , ви можете легко встановлювати та налаштовувати системи зберігання даних.

Базове налаштування

Подальше налаштування та керування буде здійснюватися виключно через веб-інтерфейс за адресою http://ip-адреса-NAS/, яку ми задали на попередньому етапі. Логін за замовчуванням admin, а пароль - freenas.

Після входу йдемо в розділ System → General Setup (див. рис 3.7), де змінюємо мову інтерфейсу, виставляємо часовий пояс і вмикаємо за бажанням синхронізацію з NTP-сервером. Натискаємо Save та оновлюємо сторінку у браузері.

Потім міняємо про всяк випадок пароль для входу в веб-інтерфейс і після збереження заново заходимо в програму (див.рис. 3.8). До речі, не забувайте після зміни будь-яких налаштувань натискати кнопки «Зберегти», «Застосувати зміни» тощо.

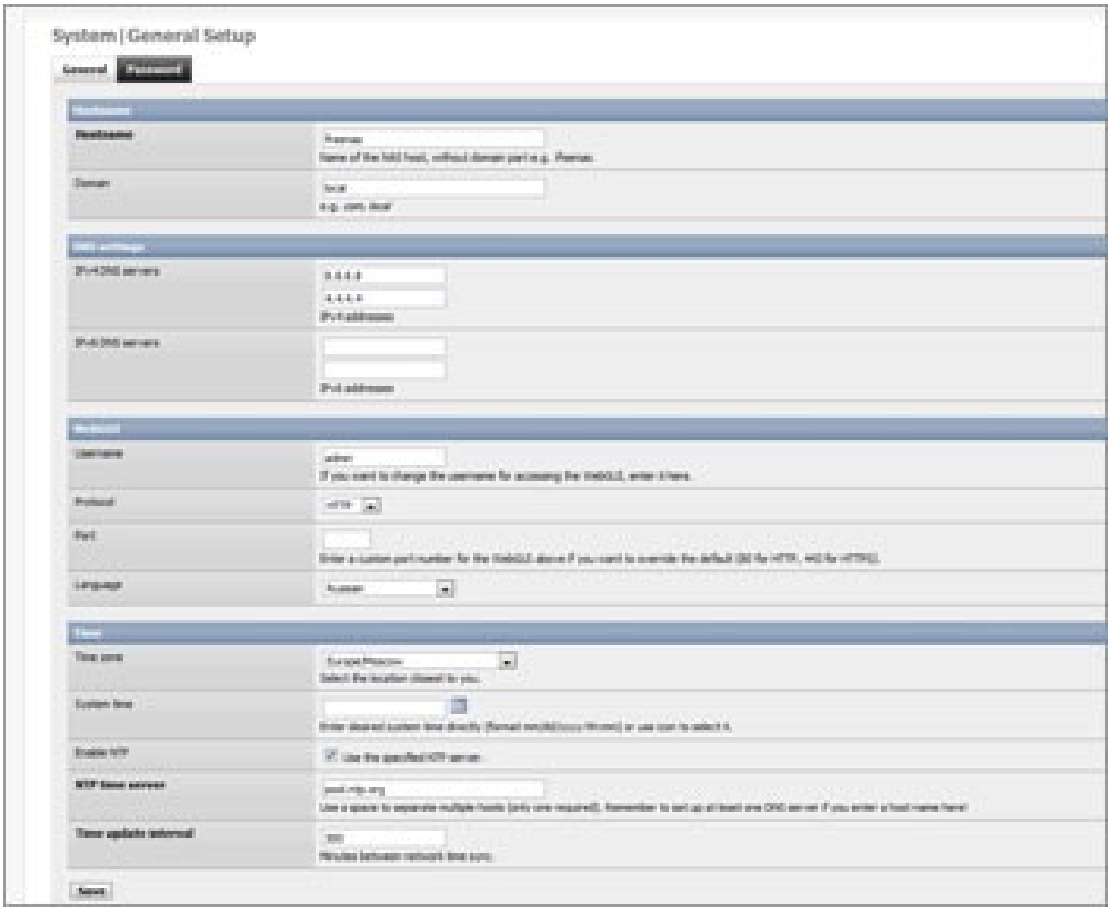

Рисунок 3.7 - Вигляд вікна System → General Setup

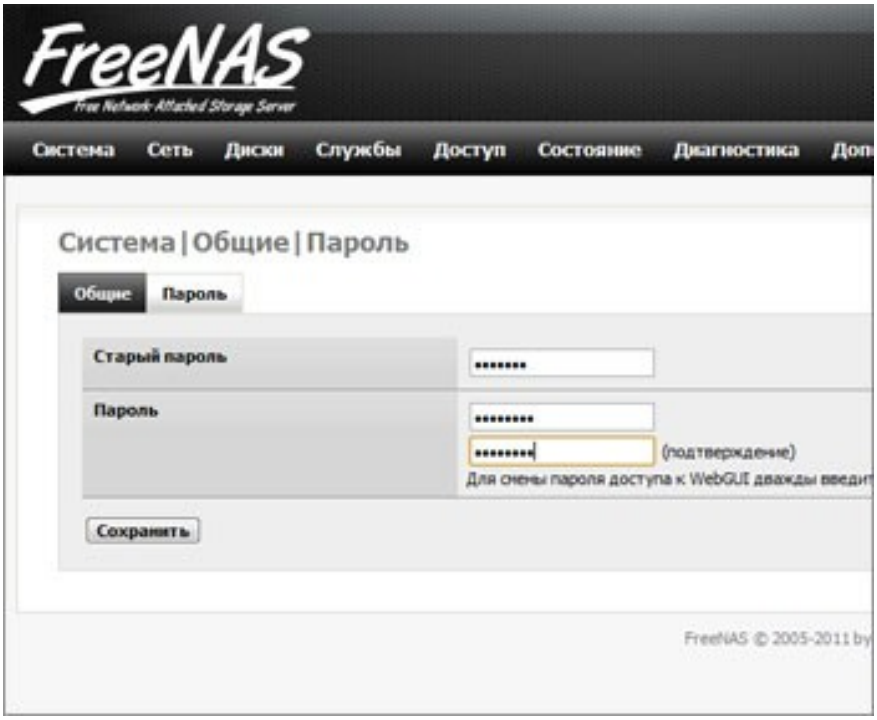

Рисунок 3.8 - Вигляд вікна входу в програму

Якщо ви дозволили створення swap-розділу, його треба підключити. Для цього йдемо в секцію «Діагностика» → «Інформація» → «Розділи» та уважно вивчаємо інформацію про розбивку диска. У нашому прикладі диск розбитий на три розділи різного об'єму – для ОС, даних та підкачування. Зорієнтуватися, який, де можна за обсягом. Нам потрібно зорієнтуватися та дізнатися шлях до розділу підкачування. Ім'я диска у прикладі /dev/ad0 (воно видно зверху), за розміром (256 Мбайт) підходить третій розділ. Таким чином шлях до нього буде /dev/ad0s3. Взагалі ж, ті, хто уважніше, мали помітити, що під час встановлення нам було показано цей шлях відразу після форматування диска. Тепер переходимо в "Система" → "Додатково" → "Файл підкачки", вибираємо в типі пристрій і вказуємо шлях. Тиснемо «Зберегти».

Настав час розібратися з логікою роботи з накопичувачами. Для початку нам треба додати диски до системи. Йдемо в «Диски» → «Управління» та клацаємо на список. Вибираємо у списку наш диск. Якщо у вас їх у системі кілька, то постарайтеся нічого не наплутати та вибрати потрібний. Увімкніть SMART і виберіть ФС. У нашому прикладі був лише один диск, на який ми ставили ОС.

(див. рис. 3.9)У такому разі потрібно вибрати UFS with Soft Updates. Якщо ви додаєте інший, вже відформатований диск з даними, потрібно вказати відповідний тип файлової системи. Натискаємо "Додати".

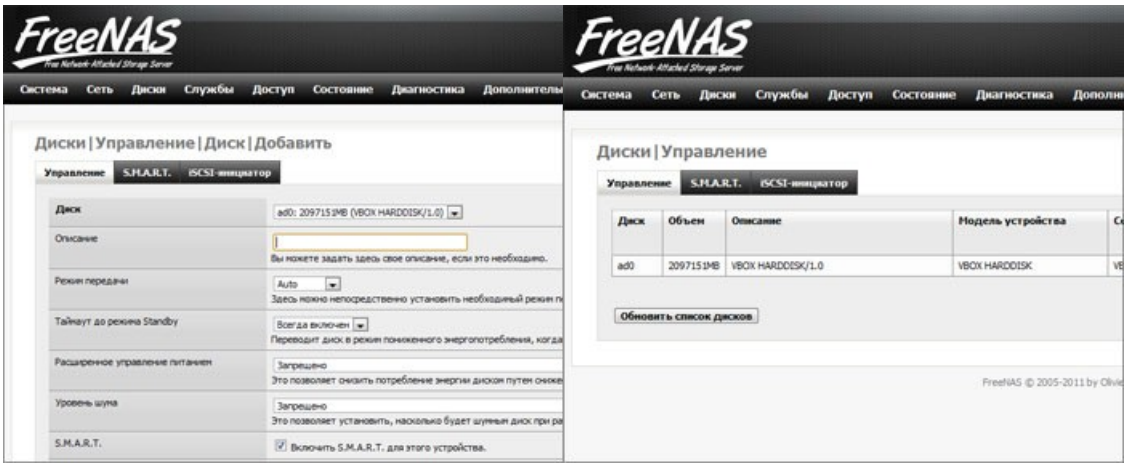

Рисунок 3.9 - Добавляння диску до мережевого сховища

Якщо у вас є ще не відформатовані диски, перейдіть в розділ «Диски» → «Форматування», виберіть потрібний диск (знову ж таки, не переплутайте нічого) і відформатуйте його. Вкрай рекомендується використовувати UFS, але це необов'язково. Тепер усі накопичувачі можна монтувати. Ідемо в «Диски» → «Точка монтування», тиснемо на плюсик, вибираємо як тип диск, потім власне накопичувач, вказуємо номер розділу (див. вище, у нашому випадку був 2) і тип ФС, а також вбиваємо ім'я точки монтування, яке для кожного диска має бути унікальним. Натискаємо «Додати» та «Застосувати зміни». Все, на цьому базова установка FreeNAS завершена.

Налаштування доступу (див. рис. 3.10)

Щоб відкрити доступ до мережі NAS, потрібно включити хоча б службу CIFS/SMB (NetBIOS). У налаштуваннях треба буде змінити за бажанням ім'я робочої групи, ім'я NAS у мережі, виставити кодування, включити сервер часу та дозволити AIO. Інші параметри можна залишити за замовчуванням та натиснути «Зберегти та перезапустити». Потім необхідно додати хоча б один мережевий ресурс, вказавши ім'я та коментар, а також шлях до нього. Спочатку всі

наші точки монтування знаходяться в каталозі /mnt, тому шлях до кореня накопичувача буде виглядати як /mnt/точка_монтування/ (у нашому прикладі це буде /mnt/data/). Краще, звичайно, створити в корені диска кілька папок і вже їх додавати до мережевих ресурсів, але це справа смаку. Якщо у вас кілька дисків, то не забудьте розшарити їх аналогічним чином.

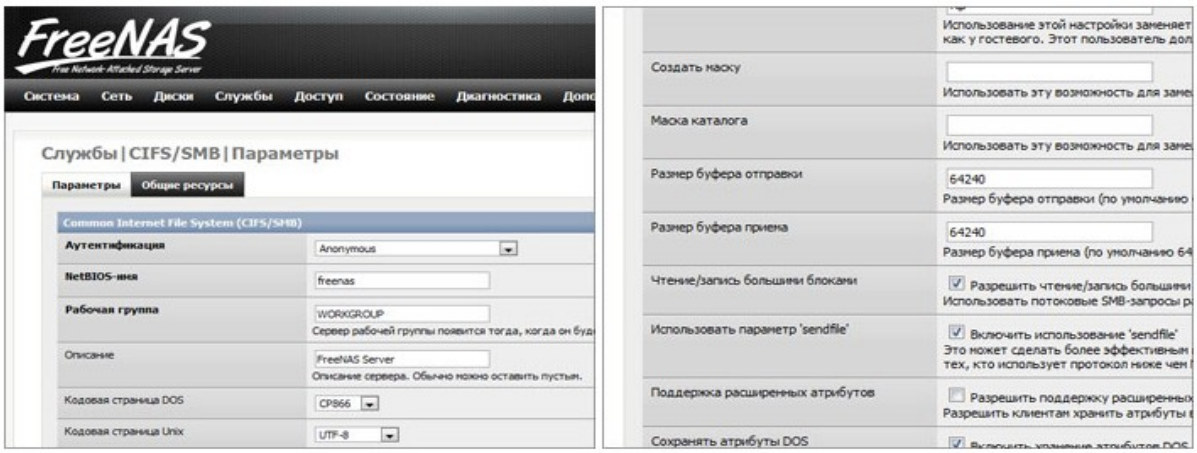

Рисунок 3.10 - Налаштування доступу до мережевого ресурсу

Для керування файлами та папками прямо з веб-інтерфейсу використовуйте файловий менеджер із розділу «Додатково». Логін та пароль для нього такий самий, як і у користувачів у FreeNAS.(див.рис. 3.11)

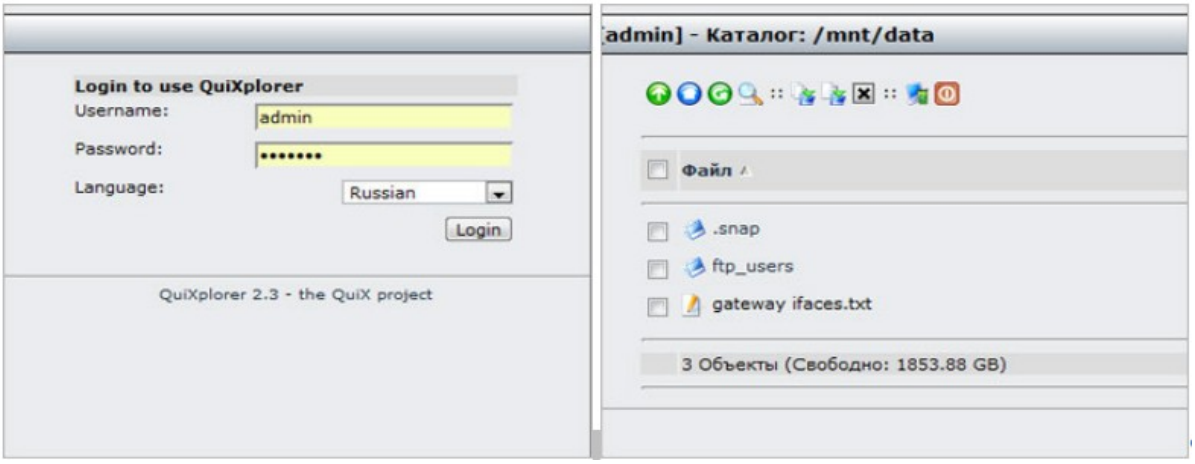

Рисунок 3.11 - Вигляд вікна керування файлами та папками веб-інтерфейсу

SMB-ресурси ми будемо використовувати в локальній мережі, а для доступу ззовні краще включити FTP-сервер. Звичайно, на роутері треба буде прокинути 21-й TCP-порт, а також включити DDNS-службу (така є і у складі FreeNAS, якщо що). У параметрах служби FTP треба дозволити вхід лише авторизованих користувачів та не забути зберегти налаштування.

Керування користувачами знаходиться у розділі «Доступ» → «Користувачі». Для доступу користувача до FTP-сервера треба вказати як основну групу ftp (див. рис. 3.12). А домашній каталог розмістити на диску з даними, заздалегідь створивши його. Якщо відзначити галочкою пункт «Надати доступ до порталу користувача», то при авторизації у веб-інтерфейсі FreeNAS можна буде використовувати не лише обліковий запис адміністратора, але й реквізити даного користувача. Правда, покерувати NAS йому не вдасться - тільки змінити свій пароль та запустити файловий менеджер, який працюватиме тільки в межах домашньої директорії користувача.

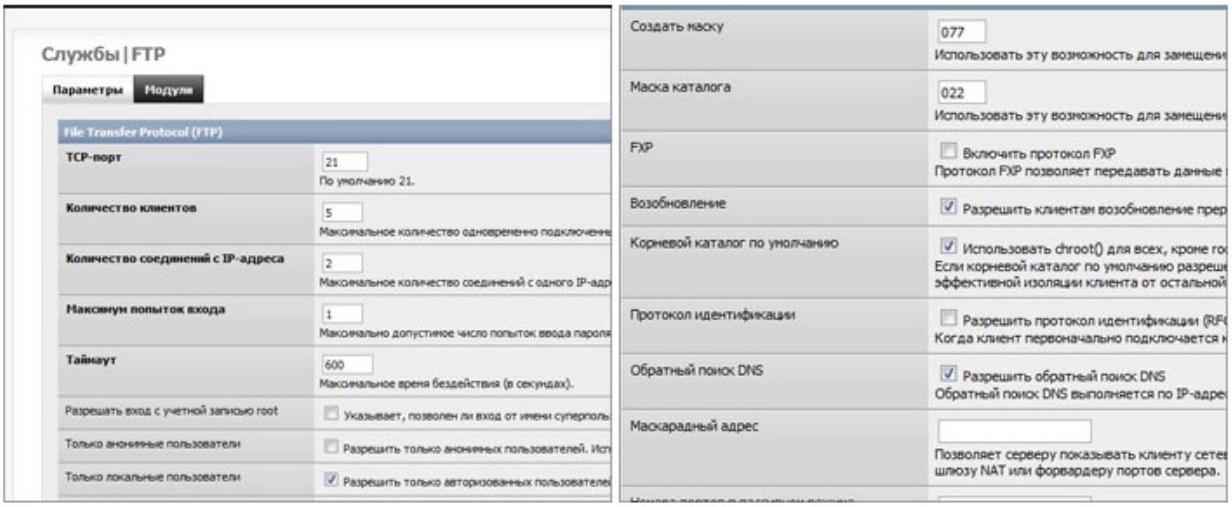

Рисунок 3.12 - Вигляд вікна налаштування доступу користувача до FTP

3.5 Інструкція з використання тестових наборів та тестових програм

Для діагностики мережі використовуються команди PING і TRACERT.

Команда ping - команда командного рядка, яка використовується для перевірки здатності даного комп'ютера “достукатися” вказаного цільового комп'ютера. Команда ping зазвичай використовується як простий спосіб перевірити, чи може комп'ютер здійснювати зв'язок через мережу з іншим комп'ютером або мережевим пристроєм.

Команда ping працює, відправляючи Інтернет-протокол керування повідомленнями (ICMP) Echo Request повідомлення на цільовий комп'ютер і очікування відповіді.

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.

Команда ping доступна в командному рядку в операційних системах Windows 10, Windows 8, Windows 7, Windows Vista та Windows XP. Команда ping також доступна в старих версіях Windows, таких як Windows 98 та 95.

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. Приклад застосування команди зображено на рисунку 3.13

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

Має наступний синтаксис :

tracert [ключі] ім’я вузла

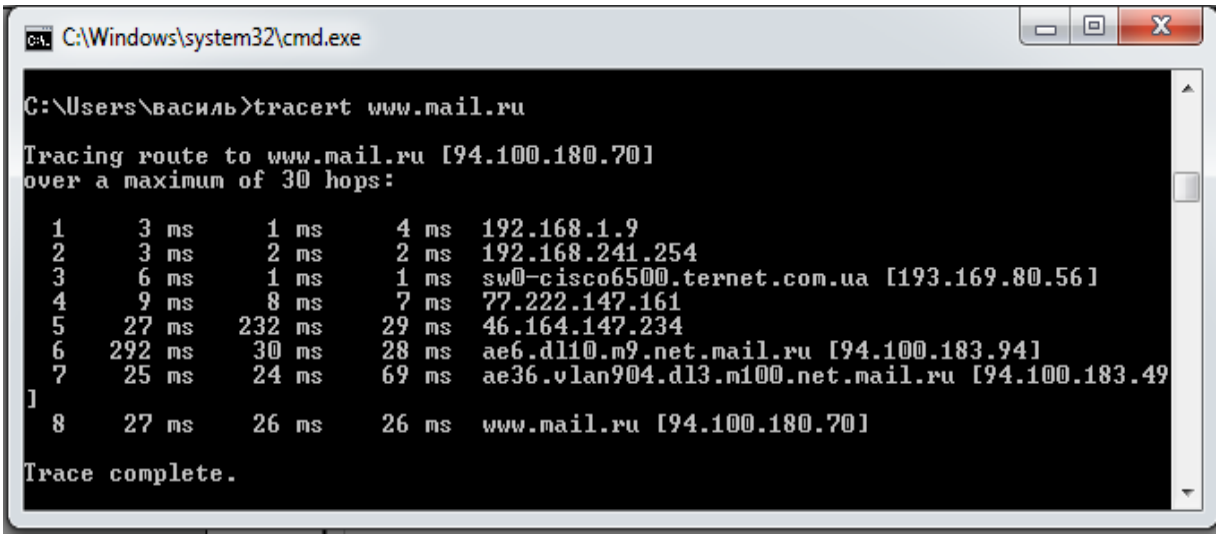

Рисунок 3.13 – Застосування команди TRACERT

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.

Команда ifconfig в Unix та подібних системах використовується для налаштування та виведення параметрів мережевого інтерфейсу для мережі за допомогою TCP/IP. її можна використовувати, щоб призначити адресу мережевому інтерфейсу, налаштувати або переглянути інформацію про його конфігурацію.

Утиліта вважається застарілою, але все одно зустрічається в багатьох інструкціях для налаштування мережі. Ifconfig зручна: з простим синтаксисом і зрозумілим виведенням інформації.

Команда IPCONFIG виводить інформацію про всі мережеві карти, встановлені в системі і зв’язках PPP.

В базову інформацію входять:

- IP-адреса;
- маска підмережі;
- шлюз по замовчуванню;
- сервери DNS;
- домен NT.

Якщо застосувати в даній команді ключ /all, то буде виведений список апаратних MAC-адрес пристроїв і інформацію по DHCP.

3.7 Моделювання мережі

Cisco Packet Tracer розроблений компанією Cisco і рекомендується використовувати при вивченні телекомунікаційних мереж та мережевого обладнання, а також для проведення уроків з лабораторних робіт у вищих закладах.

Основні можливості Packet Tracer: (за матеріалами [16])

- Дружній графічний інтерфейс (GUI), що сприяє кращому розумінню організації мережі, принципів роботи пристрою;
- Можливість змоделювати логічну топологію: робочий простір для створення мережі будь-якого розміру на CCNA-рівні складності;
- моделювання у режимі real-time (реального часу);
- режим симуляції;
- Багатомовність інтерфейсу програми: що дозволяє вивчати програму своєю рідною мовою.
- удосконалене зображення мережного обладнання зі здатністю додавати/видаляти різні компоненти;
- наявність Activity Wizard дозволяє мережевим інженерам, студентам та викладачам створювати шаблони мереж та використовувати їх надалі.
- проектування фізичної топології: доступна взаємодія з фізичними пристроями, використовуючи такі поняття як місто, будинок, стійка тощо;

Широке коло можливостей даного продукту дозволяє мережевим інженерам: конфігурувати, налагоджувати та будувати обчислювальну мережу. Також даний продукт незамінний у процесі, оскільки дає наочне відображення роботи мережі, що підвищує освоєння матеріалу учнями.

Емулятор мережі дозволяє мережевим інженерам проектувати мережі будь-якої складності, створюючи та відправляючи різні пакети даних, зберігати та коментувати свою роботу. Фахівці можуть вивчати та використовувати такі

мережеві пристрої, як комутатори другого та третього рівнів, робочі станції, визначати типи зв'язків між ними та з'єднувати їх.

На заключному етапі після того, як мережа спроектована, фахівець може приступати до конфігурування вибраних пристроїв за допомогою термінального доступу або командного рядка (див.рис 3.14).

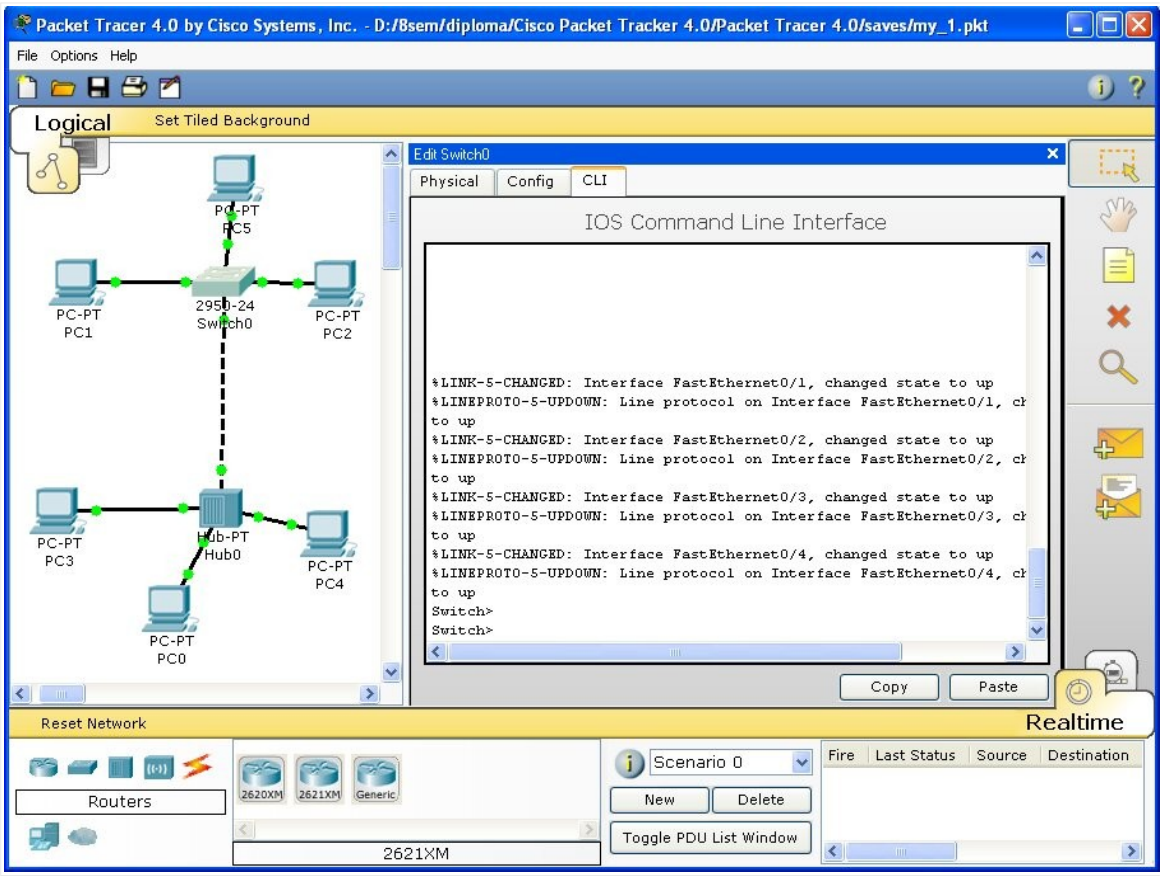

Рисунок 3.14 – Cisco Packet Tracer

Однією з найважливіших особливостей даного симулятора є у ньому «Режиму симуляції» (див.рис 3.15). У цьому режимі всі пакети, що пересилаються всередині мережі, відображаються у графічному вигляді.

Ця можливість дозволяє мережевим фахівцям наочно продемонструвати, за яким інтерфейсом зараз переміщається пакет, який протокол використовується і т.д.

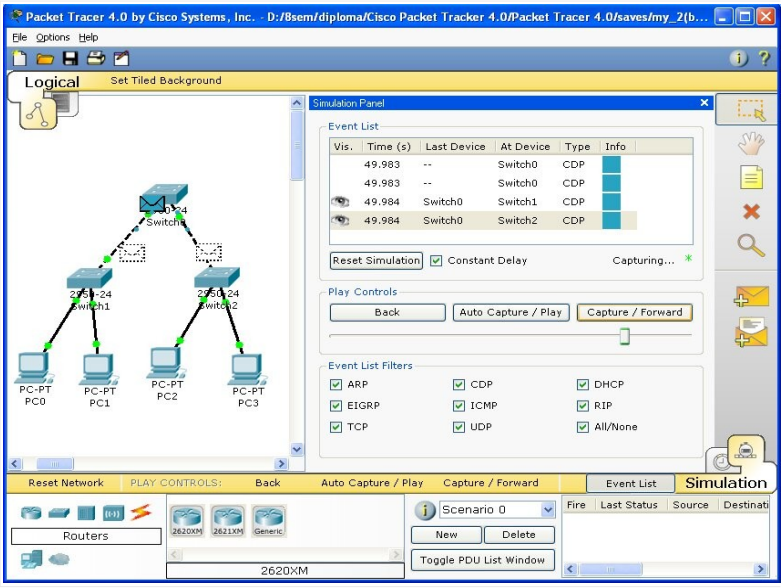

Рисунок 3.15 – Режим «Симуляції» у Cisco Packet Tracer

Однак, це не всі переваги Packet Tracer: в «Режимі симуляції» мережеві інженери можуть не тільки відстежувати протоколи, що використовуються, але й бачити, на якому з семи рівнів моделі OSI даний протокол задіяний (див.рис 3.16).

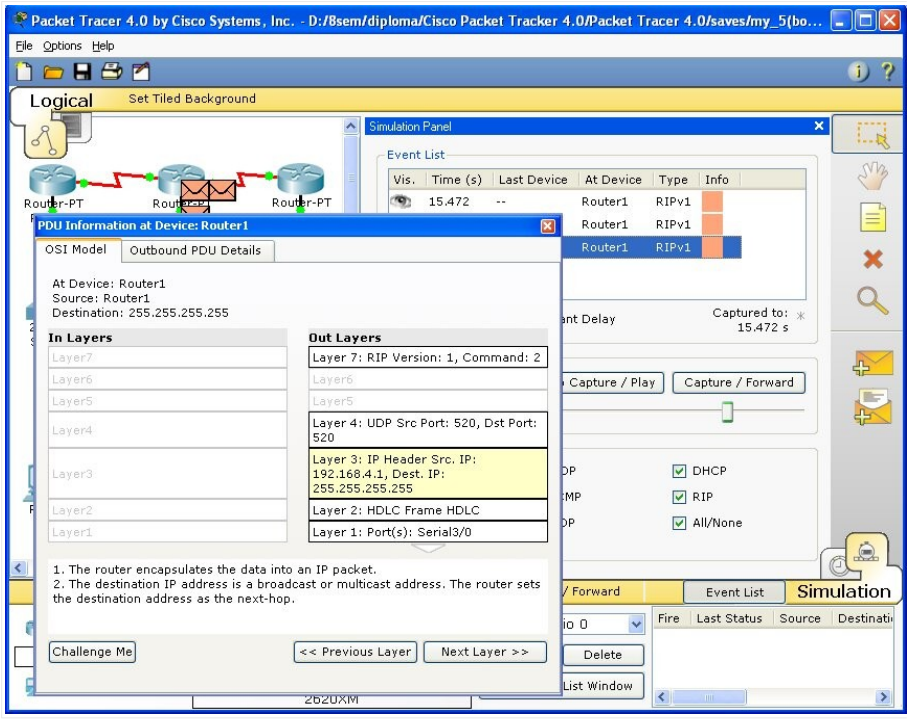

Рисунок 3.16 - Аналіз семирівневої моделі OSI у Cisco Packet Tracer

Така простота і наочність, що здається на перший погляд, робить практичні заняття надзвичайно корисними, поєднуючи в них як отримання, так і закріплення отриманого матеріалу.Packet Tracer здатний моделювати велику кількість пристроїв різного призначення, а також багато різних типів зв'язків, що дозволяє проектувати мережі будь-якого розміру на високому рівні складності.

Інтерфейс Cisco Packet Tracer

Інтерфейс програми Cisco Packet Tracer представлений рисунку 3.17

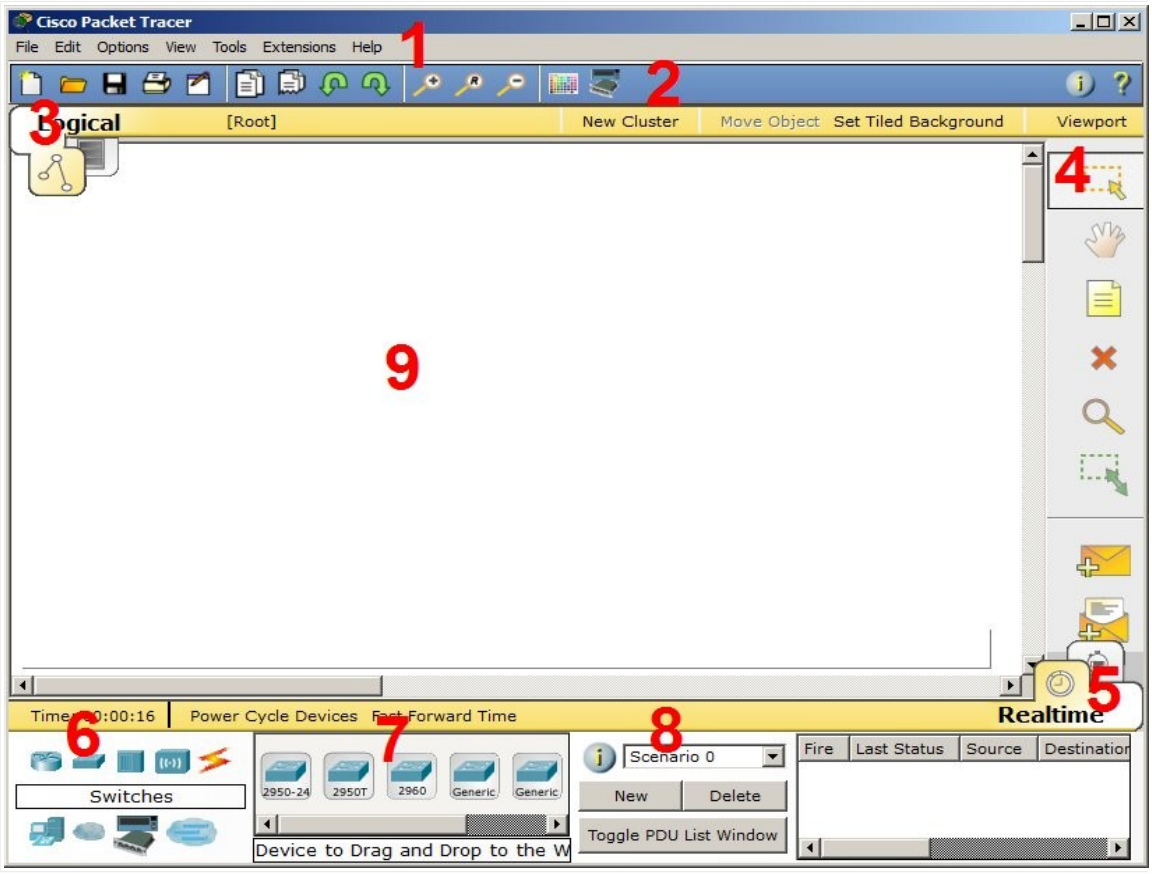

Рисунок 3.17 – Інтерфейс програми Cisco Packet Tracer

На рисунку 3.17 зображено:

1. Головне меню програми;
2. Панель інструментів – дублює деякі пункти меню;
3. Перемикач між логічною та фізичною організацією;

4. Ще одна панель інструментів містить інструменти виділення, видалення, переміщення, масштабування об'єктів, а так само формування довільних пакетів;
5. Перемикач між реальним режимом (Real-Time) та режимом симуляції;
6. Панель з групами кінцевих пристроїв та ліній зв'язку;
7. Самі кінцеві пристрої тут містяться всілякі комутатори, вузли, точки доступу, провідники.
8. Панель створення сценаріїв користувача;
9. Робочий простір;

Більшу частину даного вікна займає робоча область, в якій можна розміщувати різні мережеві пристрої, з'єднувати їх різними способами і як наслідок отримувати різні мережеві топології.

Зверху, над робочою областю, розташована головна панель програми та її меню. Меню дозволяє виконувати збереження, завантаження мережевих топологій, налаштування симуляції та багато інших цікавих функцій. Головна панель містить найчастіше використовувані функції меню.

Праворуч від робочої області, розташована бічна панель, що містить ряд кнопок, що відповідають за переміщення полотна робочої області, видалення об'єктів і т.д.

Знизу під робочою областю розташована панель обладнання.(див.рис. 3.18)

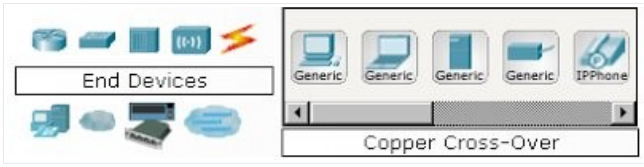

Рисунок 3.18 - Панель обладнання Packet Tracer

Дана панель містить у своїй лівій частині типи доступних пристроїв, а праворуч доступні моделі. При виконанні різних лабораторних робіт, цю

панель доведеться використовувати набагато частіше, ніж усі інші. Тому розглянемо її докладніше.

При наведенні на кожний із пристроїв, у прямокутнику, що знаходиться в центрі між ними, буде відображатися його тип. Типи пристроїв, які найчастіше використовуються в лабораторних роботах Packet Tracer, представлені на рисунку 3.19

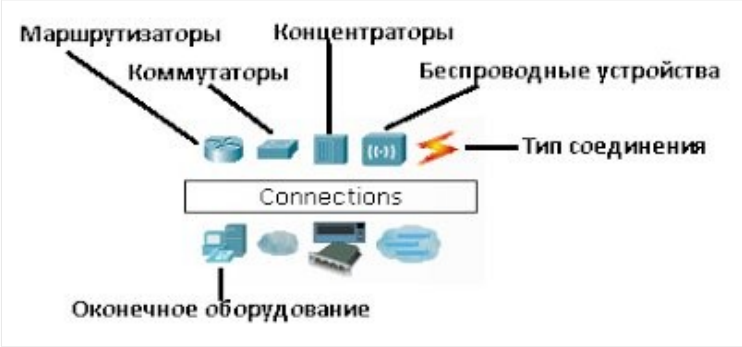

Рисунок 3.19 - Основні типи пристроїв

Розглядати конкретні моделі пристроїв кожного типу не має великого сенсу. На окремий розгляд заслуговують типи зєднань. Перерахуємо найчастіше використовувані їх (розгляд типів підключень йде зліва направо, відповідно до наведеному рисунку 3.20).

Рисунок 3.20 - Типи з'єднань пристроїв у Packet Tracer

- Автоматичний тип – при цьому типі з'єднання PacketTracer автоматично вибирає найкращі тип з'єднання для вибраних пристроїв
- Консоль – консольні з'єднання
- Мідь Пряме – з'єднання мідним кабелем типу кручена пара , обидва кінці кабелю обтиснуті в однаковій розкладці. Підійде для таких

з'єднань: комутатор - комутатор, комутатор - маршрутизатор, комутатор - комп'ютер та ін.

– Мідь кросовер – з'єднання мідним кабелем типу кручена пара , кінці кабелю обтиснуті як кросовер. Підійде для з'єднання двох комп'ютерів.
– Оптика – з'єднання за допомогою оптичного кабелю , необхідно для з'єднання пристроїв, що мають оптичні інтерфейси.
– Телефонний кабель – звичайний телефонний кабель, який може знадобитися для підключення телефонних апаратів.
– Коаксіальний кабель – підключення пристроїв за допомогою коаксіального кабелю .

Використовуючи даний продукт, ми створили модель мережі, котра показана на рисунку 3.21

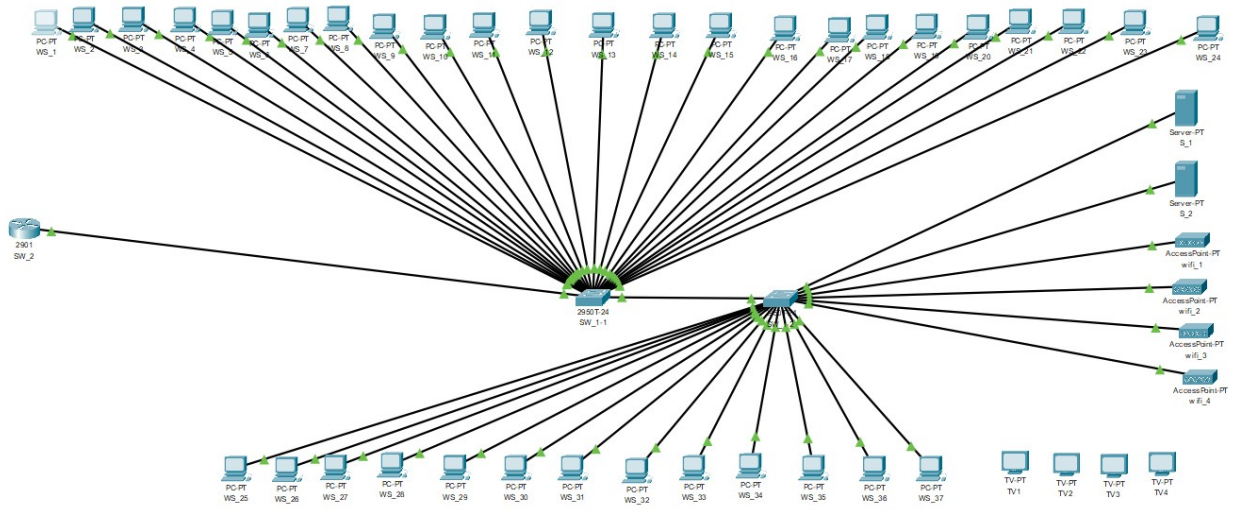

Рисунок 3.21 – Отримана модель мережі

4. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини дипломного проекту є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проекту локальної комп'ютерної мережі коипанії «IT ware» і прийняття рішення про її подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки.

Для розрахунку вартості НДР необхідно виконати наступні етапи:

описати технологічний процес розробки із зазначенням трудомісткості кожної операції;

визначити суму витрат на оплату праці основного і допоміжного персоналу, включаючи відрахування на соціальні заходи;

визначити суму матеріальних затрат;

обчислити витрати на електроенергію для науково-виробничих цілей;

розрахувати транспортні витрати;

нарахувати суму амортизаційних відрахувань;

визначити суму накладних витрат;

скласти кошторис та визначити собівартість НДР;

розрахувати ціну НДР;

визначити економічну ефективність та термін окупності продукту.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

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

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

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1.	Підготовка	Інженер	7
2	Розробка проекту мережі	Інженер	26
3	Монтаж пасивного обладнання	Лаборант	22
4	Налаштування активного комутаційного обладнання	Технік	10
5	Встановлення та на лаштування програмного забезпечення	Технік	10
6	Тестування мережі	Технік	4
Р а з о м		–	79

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

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

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

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

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

Основна заробітна плата розраховується за формулою:

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

де $Тс$ – тарифна ставка, грн.;

$Кг$ – кількість відпрацьованих годин.

$$З_{осн.}=75*33+60*22+70*24=4155{,}00 \text{ грн.}$$

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

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

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

$$З_{дод.}= 4155{,}00 *0{,}14=581{,}70 \text{ грн.}$$

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

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

$$В_{о.п.} = 4155{,}00 +581{,}70=4736{,}70 \text{ грн.}$$

Крім того, слід визначити відрахування на заробітну плату:

єдиний соціальний внесок – 22 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{з.п.}=ФОП \cdot 0{,}376, \quad (4.4)$$

де $ФОП$ – фонд оплати праці, грн.

$$В_{з.с.} = 4736{,}70*0{,}376=1781{,}00 \text{ грн.}$$

Проведені розрахунки зведемо у наступну таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Дод. заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на опл. пр., грн. 6=3+4+5
		Тарифна ставка, грн.	К-сть від-працьов. год.	Факт. нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1	Інженер	75	33	2475,00	346,50	-	-
2	Технік	70	24	1680,00	235,20	-	-
3	Лаборант	60	22	1320,00	184,80	-	-
	Разом	-	-	4155,00	581,70	1781,00	4736,70

4.3 Розрахунок матеріальних витрат

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

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

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

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

$$З_{м.в.} = 95737{,}00 \text{ грн.}$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	2	3	4	5	6
1	Кабель UTP Cat5e	м	750	15,00	11250,00
2	Роз'єми RJ-45	шт	200	14,00	2800,00
3	Розетки RJ-45	шт	45	45,00	2025,00
4	Короб пластиковий 40*25*2м	шт	64	48	3072,00
5	Дюбель	шт	300	0,30	90,00
6	Комутатор керований TP-Link TL-SG3452P	шт	1	31500,00	31500,00
7	Точка доступу Mikrotik cAP XL ac (RbcAPGi-5acD2nD-XL)	шт	4	3500,00	14000,00
8	Сервер ARTLINE Business R15v14+	шт	2	31000,00	31000,00
	Р а з о м				95737,00

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

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

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Для розробки проекту даної локальної комп'ютерної мережі викори-

стовується один ПК, потужність якого W = 6,5 кВт і який працює 27 годин.

$$З_е=0,50*27*6,5=87,75 \text{ грн.}$$

4.5 Визначення транспортних затрат

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

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

де $Т_В$ – транспортні витрати.

$$Т_В=95737,00*0,08=7658,96 \text{ грн}$$

4.6 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному вигляді необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

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

Для визначення амортизаційних відрахувань застосовуємо формулу:

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

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

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

$Н_А$ – норма амортизації, %.

Для проектування даної комп'ютерної мережі використовується один комп'ютер (вартість якого становить 28675,00 грн.), який працює 27 годин.

Тоді:

A= 28675,00*0,04*27/150=258,08 грн.

4.7 Обчислення накладних витрат

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

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

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

де $H_В$ – накладні витрати.

$H_В$=4736,70*0,3=1421,01 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	4736,70	4,24
Відрахування на соціальні заходи	581,70	1,59
Матеріальні витрати	95737,00	85,72
Витрати на електроенергію	87,75	0,08
Транспортні витрати	7658,96	6,86
Амортизаційні відрахування	258,08	0,23
Накладні витрати	1421,01	1,27
Собівартість	111680,49	100,00

Собівартість (СВ) НДР розрахуємо за формулою:

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

$C_в$=111680,49 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_В \cdot (1 + Р_{рен}) \cdot К + В_{н.і.}}{К} \cdot (1 + ПДВ), \quad (4.12)$$

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

$К$ – кількість замовлень, од.;

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

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

$Ц$=111680,49*(1+0,26)*(1+0,2)= 174221,57 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:

$$П = Ц - С_в \quad (4.13)$$

$$П = 174221,57 - 111680,49 = 62541,08 \text{ грн.}$$

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

$$Е_р = П / С_в, \quad (4.14)$$

де П – прибуток; $С_в$ – собівартість.

$$Е_р = 62541,08 / 174221,57 = 0,56$$

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

$$Т_р = 1 / Е_р \qquad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку

$$Т_р=1/0,56=1,79.$$

Всі дані розрахунків внесемо в зведену таблицю 4.5 техніко-економічних показників.

Таблиця 4.5 - Економічні показники НДР

№ п/п	Показник	Значення
1	2	3
1.	Собівартість, грн.	111680,49
2.	Плановий прибуток, грн.	62541,08
3.	Ціна, грн.	174221,57
4.	Термін окупності, рік	1,79

В результаті аналізу економічних показників, розрахованих та зведених у таблицю 4.5, можна прийти до висновку, що при терміні окупності – 1,79 року проводити роботи по впровадженню даної мережі є доцільним та економічно вигідним.

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Вимоги до організації робочих місць користувачів ПК

При розміщенні робочих місць з персональними комп'ютерами відстань між робочими столами з відеомоніторами (у напрямі тилу поверхні одного відеомонітора і екрану іншого відеомонітора) повинно бути не менше 2,0 м, а відстань між бічними поверхнями відеомоніторів - не менше 1,2 м.

Робочі місця з персональними комп'ютерами в приміщеннях з джерелами шкідливих виробничих факторів розміщуються в ізольованих кабінах з організованим повітрообміном.

При виконанні творчої роботи, що вимагає значного розумового напруження або високої концентрації уваги, робочі місця з персональними комп'ютерами рекомендується ізолювати один від одного перегородками висотою 1,5-2,0 м.

Екран відеомонітора повинен знаходитися від очей користувача на відстані 600-700 мм, але не ближче 500 мм з урахуванням розмірів алфавітно-цифрових знаків і символів.

Конструкція робочого столу повинна забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання з урахуванням його кількості і конструктивних особливостей, характеру виконуваної роботи. При цьому допускається використання робочих столів різних конструкцій, що відповідають сучасним вимогам ергономіки. Поверхня робочого столу повинна мати коефіцієнт відбиття 0,5-0,7.

Висота робочої поверхні столу для дорослих користувачів повинна регулюватися в межах 680-800 мм; при відсутності такої можливості висота робочої поверхні столу повинна складати 725 мм.

Модульними розмірами робочої поверхні столу для ПК, на підставі яких повинні розраховуватися конструктивні розміри, слід вважати: ширину - 800,

1000, 1200 і 1400 мм, глибину - 800 і 1000 мм при нерегульованої його висоті, рівній 725 мм.

Робочий стіл повинен мати простір для ніг висотою не менше 600 мм, шириною - не менше 500 мм, глибиною на рівні колін - не менше 450 мм, на рівні витягнутої ноги - не менше 650 мм.

Конструкція робочого стільця (крісла) повинна забезпечувати підтримку раціональної робочої пози під час роботи на персональному комп'ютері, дозволяти змінювати позу з метою зниження статичного напруження м'язів шейноплечевой області і спини для попередження розвитку втоми.

Тип робочого стільця (крісла) слід вибирати з урахуванням зростання користувача, характеру та тривалості роботи з ПК. Робочий стілець (крісло) повинен бути підйомно-поворотним, регульованим по висоті і кутам нахилу сидіння і спинки, а також відстані спинки від переднього краю сидіння, при цьому регулювання кожного параметра повинні бути незалежною, легко здійснюваної мати надійну фіксацію.

Поверхня сидіння, спинки та інших елементів стільця (крісла) повинна бути напівм'якої, з нековзним, слабо електризується і повітропроникним покриттям, що забезпечує легке очищення від забруднень.

5.2 Пожежна безпека на підприємстві [15]

Пожежна безпека забезпечується організаційними, технічними заходами.

До організаційних заходів належать:

- розробка правил, інструкцій, інструктажів з протипожежної безпеки;
- організація навчання та інструктування працівників;
- здійснення контролю за дотриманням протипожежного режиму;
- організація добровільних пожежних дружин;

– щоденна перевірка протипожежного стану приміщень після закінчення роботи;
– організація перевірки належного стану пожежної техніки та інвентарю.

До технічних заходів належать:

– дотримання пожежних норм, вимог та правил при влаштуванні будівель, споруд, складів;
– підтримання у справному стані систем опалення, вентиляції, обладнання;
– улаштування автоматичної пожежної сигналізації, систем автоматичного гасіння пожеж та пожежного водопостачання;
– заборона використання обладнання, пристроїв, приміщень та інструментів, що не відповідають вимогам протипожежної безпеки;
– правильна організація праці на робочих місцях з використанням пожежонебезпечних інструментів, приладів, технологічних установок.

Протипожежний інструктаж та навчання

З метою запобігання виникненню пожеж, їх поширенню та для боротьби з ними робітники, інженерно-технічні працівники проходять інструктажі й навчання за спеціальними програмами.

Види протипожежних інструктажів:

– вступний;
– первинний;
– повторний;
– позаплановий.

Вступний інструктаж проходять усі робітники, які приймаються на роботу. Його проводить спеціальна особа, відповідальна за протипожежну безпеку підприємства, організації.

При проведенні цього інструктажу працівників знайомлять з основними вимогами Закону України «Про пожежну безпеку», з установленим на підприємстві протипожежним режимом, з найбільше пожежонебезпечними ділянками, де забороняється палити, використовувати відкритий вогонь, з практичними діями у разі виникнення пожежі, з можливими причинами виникнення пожеж і вибухів та заходами щодо їх запобігання.

Первинний протипожежний інструктаж новоприйнятий робітник проходить на робочому місці перед початком роботи, а також при переміщенні з одного цеху до іншого, на іншу посаду, спеціальність або виробничу операцію.

Під час первинного інструктажу:

- знайомлять з пожежною безпекою цеху, ділянки, з правилами та інструкціями з пожежної безпеки;
- показують запасні виходи, оповіщувачі пожежної сигналізації, вогнегасники, засоби пожежогасіння;
- перевіряють практичні дії особи, яка інструктується на випадок пожежі.

Повторний інструктаж проводять безпосередньо в цеху двічі на рік у термін, встановлений керівником підприємства, згідно з програмою первинного інструктажу на робочому місці.

Позаплановий протипожежний інструктаж проводиться при зміні пожежної безпеки технологічного процесу, використанні нових пожежонебезпечних матеріалів, при самозайманні, загорянні та пожежах.

Навчання правил пожежної безпеки проводиться на виробництві, один раз на рік.

Особи, яких приймають на роботу, пов’язаною з підвищеною пожежною небезпекою, проходять спеціальне навчання (пожежно технічний мінімум).

На рисунку 5.1 приведено план приміщення організації та позначені на ньому знаки пожежної безпеки.

Рисунок 5.1 — Знаки пожежної безпеки на підприємстві

ВИСНОВКИ

В ході виконання кваліфікаційної роботи спроектовано комп’ютерну мережу компанії «IT ware». 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.

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

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

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

ПЕРЕЛІК ПОСИЛАНЬ

1. Буров Є. “Комп’ютерні мережі”. – Львів.: СП ”БаК”, 1999.- 468 с., іл.
2. Райський Ю.С., Олексюк В.П., Балик А.В. Адміністрування комп'ютерних мереж і систем: Навч. пос. — Тернопіль: Навчальна книга - Богдан. 2010.— 196 с.
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. Усатенко, Каченюк, Терехова. Выполнение электрических схем по ЕСКД: Справочник. – М.: Издательство стандартов, 1989. – 325с.
5. Тхір І.Л., Юзьків А.В., Калушка В.П. Посібник користувача ПК. ─ Тернопіль: Технічний коледж ТДТУ, 2005. : іл.
6. Чирва Ю.О., Баб'як О.С. Безпека життєдіяльності Навчальний псібник.- К.: Атаса, 2001.-304 с.
7. Комп’ютерні мережі URL: https://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6 (дата звернення:4.04.2023).
8. Побудова та адміністрування INTRANET-мереж URL:https://ami.lnu.edu.ua/wp-content/uploads/2018/01/Intranet1.pdf (дата звернення:4.05.2023).
9. Побудова та адміністрування INTRANET-мереж URL: https://trigada.ucoz.com/publ/prokladka_vitoj_pary/1-1-0-229 (дата звернення:14.05.2023).
10. Тестування та діагностика локальних мереж. URL:https://skomplekt.com/tools/134446.html/ (дата звернення:24.05.2023).

11. Як налаштувати точку доступу UbiQuiti UniFi AP URL: https://ntools.com.ua/information/faq/kak-nastroit-tochku-dostupa-ubiquiti-unifi-ap (дата звернення:18.05.2023).
12. FreeNAS встановлення та налаштування URL:https://setiwik.ru/freenas-ustanovka-i-nastroyka/ (дата звернення:12.04.2023).
13. Домашнее файлохранилище на базе FreeNAS URL: https://3dnews.ru/619273 (дата звернення:14.04.2023).
14. Монтаж кабеля витої пари URL: https://e-server.com.ua/sovety/123-pravilnyj-montazh-kabelya-vitoj-pary (дата звернення:23.05.2023).
15. ОСНОВИ ПОЖЕЖНОЇ БЕЗПЕКИ URL: https://sites.google.com/view/mamchur-natalia/ОСНОВИ ПОЖЕЖНОЇ БЕЗПЕКИ (дата звернення:19.05.2023).
16. Основи роботи з Cisco Packet Tracer URL: https://pc.ru/articles/osnovy-raboty-s-cisco-packet-tracer (дата звернення:26.05.2023).