Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

БАКАЛАВРСЬКА ДИПЛОМНА РОБОТА

на тему:

Комп'ютерна мережа Шамраївського цукрового заводу

ПОЯСНЮВАЛЬНА ЗАПИСКА

Виконав: студент 4 курсу, групи 2КІ-18Б
Спеціальності 123 — комп'ютерна інженерія
Котельніков А.П.
Керівник к.т.н., проф. каф. ОТ:
Захарченко С.М.
Рецензент к.т.н., доц. каф. МБІС:
Карпінець В.В.

Допущено до захисту
д.т.н., проф. Азаров О.Д.
" 22 " червня 2022 р.

Вінниця ВНТУ – 2022 року

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра обчислювальної техніки

Освітньо-кваліфікаційний рівень бакалавр

Спеціальність 123 — «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри

обчислювальної техніки

проф. Азарову О.Д.

«08» 02 2022 р.

З А В Д А Н Н Я

НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Котельнікову Андрію Павловичу

1 Тема проекту «Комп'ютерна мережа Шамраївського цукрового заводу», керівник роботи к.т.н., проф. каф. ОТ Захарченко С.М. затверджена наказом вищого навчального закладу від «24» березня 2022 року № 66 Строк подання студентом проекту 22.06. 2022 р.

2 Вихідні дані до проекту: призначення — проектування комп'ютерних мереж; основні підтримувані функції — передача пакетів між робочими станціями; використовувані сторонні ресурси — фото з відеокамер іншого заводу.

3 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): вступ, аналіз предметної області, розробка комп'ютерної мережі

4 Перелік необхідного матеріалу: технічне завдання, комп'ютерна схема.

5 Консультанти розділів роботи приведений в таблиці 1

Таблиця 1 — Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
Спеціальна частина	Захарченко С.М, професор кафедри ОТ		

6 Дата видачі завдання «24» березня 2022 р.

7 Календарний план виконання БДР приведений в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів виконання комплексної бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Постановка задачі роботи	07.03.22	вик.
2	Аналіз предметної області	08.03-19.03.22	вик.
3	Аналіз сучасних підходів до побудови мереж на основі інтернет речей	21.03-30.03.22	вик.
4	Аналіз поняття компютерні мережі	04.04-21.04.22	вик.
5	Аналіз принципів роботи компютерних мереж	22.04-24.04.22	вик.
6	Проектування компютерної мережі	25.04-06.05.22	вик.
7	Розробка компютерної мережі	09.05-13.05.22	вик.
8	Розробка функціоналу компютерної мережі	15.05-21.05.22	вик.
9	Підготовка матеріалів та опис розробки інформаційної системи	22.05-25.05.22	вик.
10	Аналіз виконання роботи, висновки, додатки	26.05-31.05.22	вик.
11	Перевірка якості виконання бакалаврського проекту та усунення недоліків	02.06 -10.06.22	вик.

Студент _____ Котельніков А.П.

Керівник роботи _____ Захарченко С.М

АНОТАЦІЯ

Котельніков А.П. проектування комп’ютерної мережі для Шамраївського цукрового заводу. Бакалаврська кваліфікаційна робота зі спеціальності 123 — Комп’ютерна Інженерія, Вінниця: ВНТУ, 2022. Пояснювальна записка містить 89 сторінок, 18 рисунків та 19 посилань.

В даній бакалаврській дипломній роботі була розроблена мережа цукрового заводу. На основі здійсненого аналізу предметної області було проаналізовано сучасні підходи до побудови інформаційних систем в мережі та наведено декілька аналогів. Відповідно до поставленої задачі було розроблено проект, з використанням DHCP, SSH та NAT. Таким чином було отримано зручну та швидкодіючу систему що спрощує управління підприємством та надає змогу екстреного віддаленого керування устаткуванням.

Ключові слова: інтернет речі, проект мережі, віддалене управління, взаємодія устаткування з мережею, Cisco packet tracer.

ANNOTATION

Kotelnikov A.P. designing a computer network for Shamraiv Sugar Plant. Bachelor's thesis in the specialty 123 — Computer Engineering, Vinnytsia: VNTU, 2022. The explanatory note contains 89 pages, 18 figures and 19 references.

In this bachelor's thesis, a network of a sugar factory was developed. Based on the analysis of the subject area, modern approaches to the construction of information systems in the network were analyzed and several analogues were presented. In accordance with the task, a project was developed using DHCP, SSH and NAT. Thus, a convenient and fast system was obtained, which simplifies the management of the enterprise and allows emergency remote control of equipment.

Keywords: Internet of Things, network design, remote control, hardware-to-network interaction, Cisco packet tracer.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

OSPF — Open Shortest Path First

LAN — Local Area Network

WAN — Wide Area Network

IEEE — Institute of Electrical and Electronics Engineers

UTP — Unshielded Twisted Pair

WWW — World Wide Web

FTP — File Transfer Protocol

IRC — Internet Relay Chat

DHCP — Dynamic Host Configuration Protocol

NAT — Network Address Translation

ACL — Access Control List

WEP —Wired Equivalent Privacy

WPA — Wi-Fi Protected Access

ЗМІСТ

					08-23.БДР.024.00.000 ПЗ		
Змн.	*Арк.*	*№ докум.*	*Підпис*	*Дата*			
Розробив		Котельніков А.П.			Комп'ютерна мережа Шамраївського цукрового заводу. Пояснювальна записка	*Літ.*	*Аркуш* 7 / *Аркушів* 89
Керівник		Захарченко С.М.					
Опонент		Карпінець В.В.				ВНТУ, гр. 2КІ-18б	
Н.контр.		Швець С. І.					
Затвердж.		Азаров О.Д					

ВСТУП

Комп’ютерні мережі є важливою частиною будь-якого бізнесу. Поява комп’ютерних мереж зумовлена практичною потребою в обміні даними. Без мереж багато щоденних завдань можуть бути важкими та незручними. Наприклад, для того, щоб група співробітників могла працювати з документами, вони повинні були роздрукувати інформацію або скопіювати її на інші носії.

Важливою перевагою мереж є спільне використання пристроїв та їх ресурсів: принтерів, модемів, комп’ютерів та інших пристроїв. Мережі надають доступ до кожного жорсткого диска, розділяючи дисковий простір на всіх комп’ютерах для спільного використання. Сумісна робота кількох комп’ютерів неможлива без мережі.

З розвитком технологій і потреб агропромисловим комплексам необхідно інтегрувати нові мережеві технології та модернізувати мережі, або оновити існуючі мережі. Сільське господарство ідеально підходить для інформаційних технологій та комп’ютерних мереж. Використання технологій сприяє підвищенню продуктивності та розвитку аграрного сектору. Правильне використання інформаційних технологій сприяє розвитку сільського господарства та виведенню його на новий рівень. Ферми часто оснащені обладнанням, не характерним для традиційних комп’ютерних мереж, таким як В. різні датчики температури і вологості, вагові процесори або сканери штрих-кодів. Такі пристрої можуть вимагати певних умов для підключення до мережі та додаткових налаштувань для роботи.

Актуальність теми полягає у тому, що на сьогоднішній день у більшості сільськогосподарських підприємств не реалізуються всі можливості комп’ютерної мережі. Прокладання мережі здатно збільшити виробничі потужності та скоротити документообіг.

Об’єктом дослідження використання мережі для промислового заводу з використанням технологій інтернет речей.

Предмет дослідження амраївський цукровий завод, його устаткування та проектування мережі на території підприємства.

Метою дослідження є підвищення продуктивності товариства з обмеженою відповідальністю «Шамраївський цукровий завод» шляхом створення та функціонування корпоративної комп’ютерної мережі.

Для досягнення мети проекту потрібно виконати такі **задачі**:

— провести аналіз сучасних технологій впровадження комп'ютерних мереж, особливо на сільськогосподарських підприємствах;

— розробити логічну структуру комп’ютерної мережі підприємства ТОВ «Шамраївський цукровий завод»;

— обґрунтувати вибір активного обладнання для реалізації мережі;

— провести конфігурацію активних пристроїв;

— провести моделювання та тестування мережі за допомогою симулятора Cisco Packet Tracer.

Методи дослідження дипломної роботи: використовувалася та досліджувалася компютерна мережа на основі технології інтернет речей і наведенні висновки про її роботу за допомогою Cisco Pacet Tracer.

Практична цінність розробленої мережі полягає в:

— поглибленні рівню захисту зв’язку між підрозділами використувуючи сучасні технології;

— своєчасному та оперативному забезпеченні інформаційними даними відповідних користувачів та системи управління підприємства;

— підвищенні конкурентоспроможністі компанії, в ринкових умовах господарювання.

1 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ СПЕЦІАЛІЗОВАНИХ МЕРЕЖ

1.1 Моделі мережі TCP / IP і OSI

Проектування будь-якої мережі передбачає використання базової моделі. Модель взаємодії відкритих систем (OSI) — модель, яка розділяє етапи мережі на сім відповідних рівнів, кожен з яких виконує певну функцію. Важливо також взаємодію однакових рівнів приймача і передавача, що забезпечує передачу інформації між учасниками. Кожен нижчий рівень у моделі надає конкретні послуги передачі інформації на вищий рівень. [2]. В таблиці 1.1 показані всі рівні моделі OSI.

Таблиця 1.1 — Рівні моделі OSI

№ рівня	Рівень	Англійська назва рівня	Основні задачі	Основні елементи
7	Прикладний	A — Application	Форми взаємодії прикладних процесів	Програми які відображають інформацію з представницького рівня
6	Представницький	P — Presentation	Перетворення данних	POP3, FTP, TFTP, SMTP, HTTP, NTP, SNMP та інші
5	Сеансовий	S — Session	Організація та проведення діалогу	DNS, UDP та інші
4	Транспортний	T — Transport	Налагодження наскрізних сполучень	TCP, UDP та інші
3	Мережевий	N — Network	Прокладання сполучень між системами	IP та інші
2	Канальний	DL — Data link	Передавання між суміжними системами	Ethernet, FDDI, FR та інші
1	Фізичний	PL — Physical link	Спряження з фізичними середовищами передавння	Біти інформації та типи модуляції

Фізичний рівень відповідає за транспортування інформації між вузлами мережі за допомогою певного носія (кабель, трансляція тощо). Фізичний рівень відповідає за передачу інформації від початку до кінця каналу, характеристики сигналу, швидкість передачі даних, відстань передачі інформації, типи фізичних з'єднань та інші характеристики. Протоколи фізичного рівня: RS-232, RS-485, RJ-11, RJ-45, IEEE 802.15, 802.11.

Канальний рівень забезпечує певний ступінь надійності передачі інформації по фізичному каналу. Канальний рівень також відповідає за фізичну адресацію та топологію мережі. Він також повідомляє про перебої в мережі та доставку інформації. Протоколи канального рівня: Ethernet для локальних мереж, протокол «точка-точка» (PPP), HDLC та ADCCP для з'єднань «точка-точка».

Мережевий рівень забезпечує ідентифікацію кінцевих одержувачів інформації. Забезпечує підключення користувача та вибір маршруту. Протоколи, які відповідають цьому рівню, визначають найкращий спосіб надсилання інформації в Інтернеті. Протоколи мережевого рівня — це такі протоколи, як IPv4, IPv6, ICMP, IGMP.

Транспортний рівень відповідає за транспортування даних по мережі. Рівень трафіку контролює порядок надсилання повідомлень. На цьому рівні існують механізми створення, підтримки та видалення віртуальних каналів. Протоколи рівня передачі TCP і UDP регулюють цілісність передачі даних. TCP вимагає попереднього підключення і гарантує повну цілісність, повторні запити у разі втрати даних і запобігає клонування при отриманні двох копій пакета. UDP працює без встановлення підключення, підтвердження і не гарантує доставку. UDP використовується для трафіку в режимі реального часу. Використовується для серверів, які надсилають невеликі відповіді великій кількості клієнтів.

Сеансовий рівень синхронізує взаємодію між об’єктами представницького рівня та контролює обмін інформацією між ними. Він також

забезпечує спосіб надсилання інформації, створення сповіщень про сеанси та інших рівнів шаблону нижче. Сеансовий рівень відповідає за встановлення та зупинку сеансів між завданнями програми. Регіональний інформаційний протокол (ZIP) і протокол управління сеансами (SCP) є прикладами такого рівня впровадження.

Представницький ріваень обробляє інформацію з прикладного рівня. Тобто він обробляє інформацію та представляє її у правильному форматі для подальшого використання.

Прикладний рівень визначає кількість ресурсів для майбутнього підключення, визначає та встановлює наявність комунікаційного партнера. Прикладний рівень синхронізує спільні процеси прикладного рівня і гарантує, що користувач отримує інформацію, отриману в бажаній йому формі. Протоколи прикладного рівня: HTTP, Gopher, Telnet, DNS, DHCP, SMTP, SNMP, CMIP, FTP, TFTP, SSH [2].

Модель TCP/IP являє собою стек протоколів, подібних до моделі OSI, розділених на чотири, а не на сім шарів. Протоколи TCP/IP прикладного рівня визначають взаємодію процесів додатків і форм представлення інформації різних комп'ютерів мережі. На основі взаємодії прикладне програмне забезпечення поділяється на клієнтське та серверне програмне забезпечення. Протоколи прикладного рівня включають FTP і TFTP, TELNET.

Протоколами рівня передачі TCP/IP є протокол керування передачею TCP та протокол користувальницьких дейтаграм UDP. Принципи їх роботи досить різні. UDP не вимагає відповідного з'єднання для відправки дейтаграм, і це не гарантує цілісність передачі. TCP, з іншого боку, гарантує повну передачу сегментів і вимагає зв'язку між комп'ютерними модулями. Протоколи на цьому рівні взаємодіють з різними архітектурними мережами.

Мережевий протокол IP є найважливішим проривом у технології TCP/IP на рівні мережі. Протокол адреси ARP; Протокол зворотної адреси RARP (Reverse ARP); Допоміжним протоколом є Internet Control Message Protocol

(ICMP), який надсилає сповіщення про помилки маршрутизації, які виникають під час надсилання до вузлів мережі. Функція протоколу IP полягає в маршрутизації пакетів між мережами. Щоб вирішити цю проблему, IP-протокол налаштовує IP-адресу мереж і вузлів, відображає розклад маршрутизації пакетів, виконує фрагменти, якщо необхідно, і дефрагментує мережеві пакети. Мережевий рівень також включає в себе набір протоколів динамічної маршрутизації RIP, OSPF, які динамічно генерують маршрути таблиці маршрутизації за допомогою різних алгоритмів.

Рівень доступу відповідає за порівняння IP-адрес із фізичними мережевими адресами (MAC-адресами) та інкапсулювання IP-дейтаграм у кадри для передачі фізичного каналу та пересилання кадрів. Протокол ARP працює на цьому рівні, вказуючи адресу від IP до MAC. Прозорість — це властивість мережі, яка приховує від користувача деталі вашого внутрішнього пристрою, що полегшує роботу в Інтернеті [3].

1.2 IP-адреса

Основними ідентифікаторами пристроїв у сучасних мережах є IP-адреси. IP-адреса — це ідентифікатор, який доступний на кожному пристрої, підключеному до Інтернету. IP-адреси призначаються провайдерами. У більшості випадків більшості комп’ютерів призначається однакова IP-адреса, тому більшість комп’ютерів мають однакову IP-адресу .

Адреси зазвичай використовуються для визначення місця підключення комп’ютера до Інтернету. Коли для рекламної кампанії встановлюється націлювання на місцеположення, IP-адреси допомагають системі Google Ads визначити, які користувачі застосовують комп’ютери в цільовому регіоні. [4].

Існує два формати IP-адрес:

— існує модель xxx IPv4, де x будь-яке число від 0 до 255, яке називається октетами, адреса IPv4 має містити чотири октети, розділені двокрапкою;

— модель IPv6 має модель y: y: y: y: y: y: y: y, де y це сегмент, який може мати значення від 0000 до FFFF (числа від 0 до 9 і A до F), враховуючи облік листів), адреса IPv6 складається з 8 сегментів, розділених двокрапкою (не крапкою).

IP-адреси також поділяються на приватні та публічні. В Інтернеті використовуються публічні адреси. Публічна IP-адреса — це IP-адреса, яка використовується для доступу до Інтернету. На відміну від індивідуальних адрес, загальнодоступні (глобальні) IP-адреси перенаправляються в Інтернет. Маючи публічну IP-адресу на своєму пристрої, ви можете організувати віддалений доступ до свого комп'ютера та камер відеоспостереження та отримати доступ до них з будь-якої точки Всесвітньої мережі. Навіть якщо у вас є загальнодоступна IP-адреса, ви можете налаштувати будь-який з ваших домашніх серверів для публікації її в Інтернеті: веб (HTTP), VPN (PPTP / IPSec / OpenVPN), медіа (аудіо / відео), FTP, мережа NAS диск, ігровий сервер тощо. Особисті адреси не маршрутизуються в Інтернет і не можуть надсилати трафік з Інтернету, вони працюють лише в межах локальної мережі [5].

Приватні адреси включають IP-адреси в таких підмережах:

— 10.0.0.0 до 10.255.255.255 з маскою 255.0.0.0 або / 8;

— 172.16.0.0 до 172.31.255.255 маска 255.240.0.0 або / 12;

— від 192.168.0.0 до 192.168.255.255 з маскою 255.255.0.0 або / 16;

— 100.64.0.0 до 100.127.255.255 маска підмережі 255.192.0.0 або / 10.

Це збережені IP-адреси. Якщо ви використовуєте лише приватні адреси, ви не зможете отримати доступ до Інтернету. Окремі IP-адреси в одній локальній мережі мають бути унікальними, і якщо ця політика порушується, мережа не працюватиме належним чином. У цьому випадку підключення до Інтернету здійснюється через NAT (трансляція мережевої адреси замінює окремі IP-адреси загальнодоступними). Такі адреси призначені для використання в закритих локальних мережах, розповсюдження таких адрес ніким не контролюється.

1.3 Технологія Ethernet

Основною технологією реалізації локальних мереж є технологія Ethernet. Ethernet — це технологія передачі пакетів, переважно для локальних комп’ютерних мереж. Ethernet став найбільш широко використовуваною технологією в середині 1990-х років, замінивши старі технології, такі як Arcnet, FDDI і Token Ring. Стандарти Ethernet визначають кабельні з'єднання фізичного рівня та електричні сигнали, формат кадру та протоколи контролю доступу. Ethernet в основному характеризується стандартами IEEE групи 802.3, характеристиками яких є: топологія — шина; Середовище передачі — коаксіальний кабель; Швидкість передачі — 10 Мбіт/с; максимальна довжина лінії — 5 км; максимальна кількість передплатників — до 1024; Довжина сегмента мережі — до 500 м; кількість абонентів в одному сегменті — до 100; спосіб доступу — CSMA / CD; вузькосмугова передача, тобто без модуляції (одноканальна).

Технологія Ethernet сьогодні є найпопулярнішою у світі, на неї припадає понад 90% ринку. Оскільки характеристики мережі, налаштування та протоколи були оприлюднені, виробники по всьому світу почали випускати повністю сумісні пристрої Ethernet. Вита пара використовується як носій передачі даних. Існує також стандарт використання волоконно-оптичних кабелів. Були внесені відповідні зміни до документування змін до стандарту IEEE 802.3. У 1995 році був представлений інший стандарт Ethernet 100 Мбіт/с (так званий Fast Ethernet, стандарт IEEE 802.3u), який використовує виту пару або волоконно-оптичні кабелі в якості середовища передачі. Версія 1000 Мбіт/с (Gigabit Ethernet, стандарт IEEE 802.3z) з'явилася в 1997 році. Існують основні топології Ethernet: шина (послідовне підключення комп’ютерів через Т-роз’єми (Т-роз’єми)), зірочка та розширена зірка (підключення комп’ютерів через комутаційні пристрої) [7]. Фото кабелю Ethernet показано на рисунку 1.1.

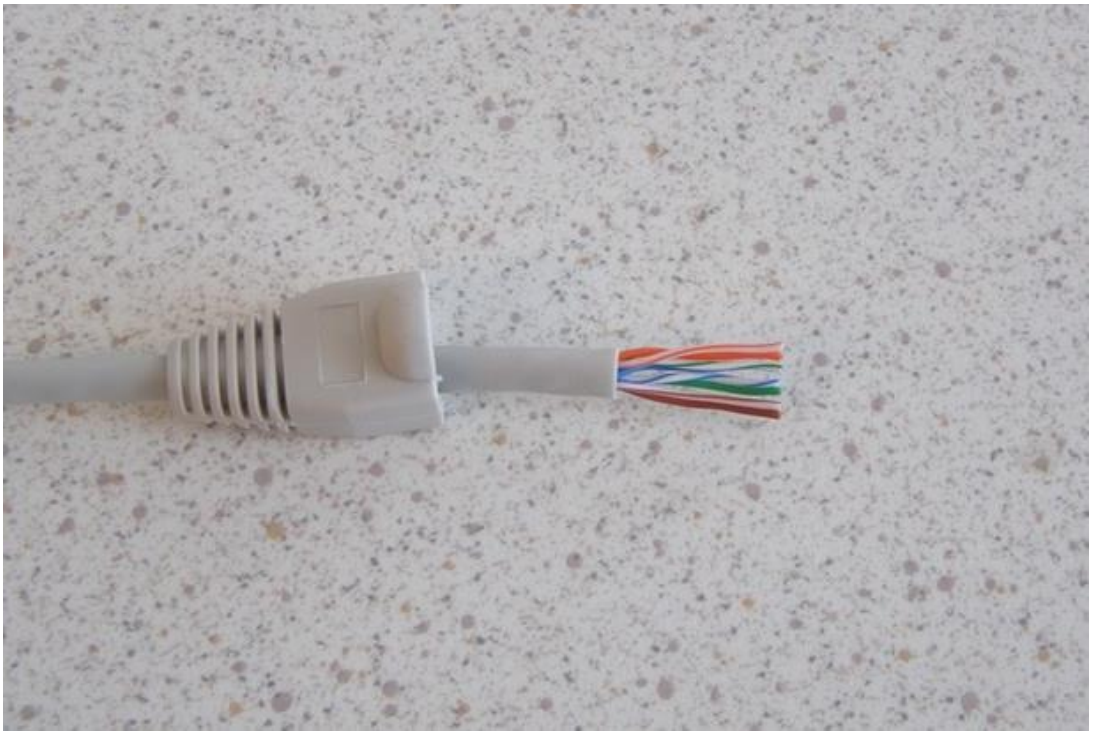

Рисунок 1.1 — Фото витої пари без ізоляції та стиснення

Модифікації Ethernet:

— підтримує стандарти Ethernet 10 Мбіт/с: 10BASE5 (товстий коаксіальний кабель); 10BASE2 (тонкий коаксіальний кабель); 10BASE-T (кручена пара); 10BASE-FL (волоконно-оптичний кабель);

— підтримує стандарти Fast Ethernet (100 Мбіт/с): 100BASE-T4 (Quadruple Twisted Pair); 100BASE-TX (подвійна вита пара); 100BASE-FX (волоконно-оптичний кабель);

— Gigabit Ethernet (1 Гбіт/с);

— 10 Gigabit Ethernet (10 Gbps);

— 40/100 Gigabit Ethernet (40/100 Gbps).

Мережа Ethernet не відрізняється за основними характеристиками або алгоритмами, багато в чому програє своїм аналогам. Але він настільки популярний завдяки потужній підтримці, найвищій стандартизації та величезному технічному оснащенню.

1.4 Технологія Wi-Fi

Основною технологією впровадження бездротових локальних мереж є IEEE 802.11 або Wi-Fi. Технологія Wi-Fi є бездротовим аналогом такого стандарту, як Ethernet. Wi-Fi має власний бездротовий стандарт, який поєднує в собі кілька протоколів і офіційно називається IEEE 802.11. Більшість офісних комп'ютерних мереж засновані на цій технології. Найпопулярнішим і широко використовуваним протоколом сьогодні є IEEE 802.11b. Він регулює роботу бездротових мереж в діапазоні частот від 2,4 до 2,48 ГГц і пропонує максимальну швидкість 11 Мбіт/с. Максимальна відстань передачі сигналу в цьому випадку становить близько 100 метрів, але на відкритому повітрі вона збільшується до 300-400 м.

Існує також стандарт 802.11a, який працює на частоті 5 ГГц і досягає швидкості до 54 Мбіт/с. Ще один 802.11g, який використовує 2,4 ГГц і може працювати зі швидкістю 54 Мбіт/с. Однак вони не користуються великим попитом через свої недоліки, наприклад, малий радіус дії, набагато складніші алгоритми, високе енергоспоживання. Крім того, зараз розробляється стандарт 802.11n, який може забезпечити швидкість близько 320 Мбіт/с [8].

Дозволяє взаємодіяти з Wi-Fi серверами, оскільки його аналоги з базами даних і програмними додатками дозволяють виходити в Інтернет. Комп'ютер, який зчитується, не повинен бути фізично підключений до мережі. Досить розмістити його в радіусі 300 м від так званої точки доступу — Wi-Fi пристрою, який виконує приблизно ті ж функції, що і звичайна офісна АТС. У цьому випадку інформація передається радіохвилями в діапазоні частот 2,4-2,48 ГГц.

Технологія Wi-Fi вирішує наступні важливі завдання:

— спрощує зв'язок з ноутбуком;

— впровадження локальної обчислювальної мережі у випадках, коли прокладка кабелю фізично неможлива або потребує обмежених чи надмірних коштів.

1.5 Технологія NAT

Обмежена кількість публічних IPv4-адрес вимагає збереження адресного простору за допомогою технології трансляції адрес. NAT — це технологія, яка дозволяє змінювати IP-адресу заголовка пакета, який проходить через маршрутизатор. Він має кілька назв: мережевий маскарад, IP-маскарад і трансляція локальної адреси.

Найпростіший тип трансляції мережевих адрес (NAT) обробляє трансляцію IP-адрес «точка-точка». Основним типом такого розподілу є RFC 2663. Він замінює лише контрольну суму IP-заголовків та IP-адрес. Ці типи трансляції слід використовувати при підключенні до мереж, адреси яких не збігаються.

Багато типів технології NAT можуть об’єднати кілька окремих хостів в один хост із загальною IP-адресою. У звичайній конфігурації локальна мережа використовує одну із зазначених «приватних» IP-адрес підмережі. Маршрутизатор в такій мережі матиме свою адресу. Маршрутизатор також підключається до Інтернету через «загальнодоступну» адресу, призначену провайдером. Оскільки трафік локальної мережі доступний в Інтернеті, адреса відправника в пакетах негайно передається з приватної адреси на публічну. Для кожного активного з’єднання маршрутизатор відстежує основні дані (включаючи адресу та порт призначення). Коли відповідь надсилається, дані, використані під час з’єднання, зберігаються на вихідному етапі та використовуються для визначення окремої адреси підмережі, до якої надсилається відповідь.

Метою цієї технології є вирішення проблеми виснаження адресного простору. Навіть великі мережі можна підключити до Інтернету за допомогою однієї IP-адреси.

Усі пакетні дейтаграми в IP-мережах мають дві IP-адреси відправлення та отримання. Передача адреси порту (PAT) — це реалізація Cisco Rapt, яка дозволяє переглядати кілька окремих IP-адрес як одну публічну адресу. Кожна адреса пов'язана з відповідним номером порту, що дозволяє їм відображатися як одна адреса. Ця технологія використовує унікальні номери портів, щоб вимкнути маршрут передачі даних. Ці числа, у свою чергу, є 16-значними цілими числами. Теоретично близько 65 536 внутрішніх адрес можна перевести в одну загальну зовнішню адресу. Насправді це значення становить близько 4000 портів, що можна порівняти з однією IP-адресою. PAT завжди зберігає вихідний порт. Якщо цей порт не порожній, його буде замінено номером першого доступного порту з початку відповідної групи — 0-511, 512-1023 або 1024-65535. У цьому випадку, якщо портів недостатньо, але доступно кілька зовнішніх IP-адрес, перейдіть до наступного і спробуйте призначити вихідний порт. Процес триває до тих пір, поки дані не будуть доступні.

Cisco виконує порівняння адрес і портів, включаючи трансляцію адрес порту з даними пакетного тунелю IPv4 через внутрішню мережу IPv6. Ця альтернатива CarrierGrade NAT і DS-Lite є неофіційною і підтримує трансляції IP-адрес/портів, тобто підтримує налаштування NAT. Це усуває проблеми з підключенням і підтримкою. Це також робить механізм переходу розгортання IPv6 дуже зручним [9].

1.6 Інтернет речей

Особливістю використання комп'ютерних мереж в агропромисловому комплексі є підключення до мережі великої кількості «розумних» пристроїв. Інтернет речей — це система, яка з'єднує комп'ютерні мережі та пов'язані промислові системи. Такі промислові установки можуть бути оснащені

вбудованими датчиками та програмним забезпеченням для збору та обміну даними з можливістю дистанційного керування та керування в автоматизованому режимі без участі людини. Елементи Усі фізичні об'єкти, які беруть участь в Інтернеті, повинні мати власні ідентифікатори, які повинні бути унікальними, незалежно від того, чи мають вони доступ до Інтернету. Існує багато систем, які дозволяють виявляти об'єкти в автоматизованому режимі. Одним з них є радіочастотний знак, прикріплений до кожного об’єкта, радіочастотний знак, прикріплений до кожного об’єкта [10].

Пристрої для введення IoT спочатку оснащуються інтерфейсами, датчиками та іншими приводами. Це дозволяє керівництву збирати інформацію, яка дозволяє отримати об’єктивні та точні дані про стан виробництва. Залишається лише організувати доставку інформації до відповідних підрозділів підприємства, що значно покращить роботу та допоможе максимально швидко та продуктивно приймати рішення. Ця інформація допомагає запобігти незапланованим простоям, відмовам і поломкам обладнання, а також своєчасному технічному обслуговуванню, таким чином підвищуючи продуктивність і спрощуючи діяльність компанії.

Такі пристрої підключаються до комп’ютерів або спілкуються з сервером даних. Підключення здійснюється через Ethernet, RS-232 або звичайний Micro-USB, а також у вигляді радіотехнологій, таких як Wi-Fi, Bluetooth, GSM. Ви можете дистанційно керувати та контролювати з будь-якого комп’ютера чи смартфона, вам потрібно підключитися до сервера, який керує пристроєм IoT, або спеціального програмного забезпечення, яке дозволяє підключатися безпосередньо до комп’ютера чи пристрою.

Велика кількість такої відокремленої та неструктурованої інформації ускладнює її фільтрацію та подання у бажаному для користувача вигляді. Існують певні аналітичні платформи, які збирають, аналізують та фільтрують дані в режимі реального часу.

Індустріальні технології Інтернету речей сприяють створенню та розвитку компаній нового рівня. З впровадженням таких технологій підприємства покажуть значно кращі результати продуктивності, а робочий процес стане більш гнучким, ефективним та економічним. Найпоширеніші пристрої: смартфони, планшети, датчики вже давно користуються великою популярністю і довели це в реальному виробництві. Сучасні дротові мережі з підтримкою датчиків і IP були розширені та доповнені бездротовими мережами. Бездротові мережі розширюють використання таких систем збору та обробки інформації. Наступним етапом розвитку таких технологій стане зближення та вдосконалення оперативно-інформаційної взаємодії.

З часом виробничі компанії, які автономно регулюють усі виробничі процеси та бізнес-процеси, необхідні для виробництва, стануть відкритими системами, що з’єднують різних учасників ринку. Процесами в системах керують хмарні сервіси, а не персонал, і кінцевою метою всіх цих перетворень є обслуговування клієнта, а не продукту [11].

Після впровадження IoT ефективність компанії зросте в кілька разів. Термін окупності таких проектів не перевищує кількох місяців. Для таких проектів існує багато живих масштабних проектів, одним з яких є обладнання для бритви Philips. Завод працює в безосвітленому приміщенні і налічує всього дев'ять співробітників. Щоб досягти цього, компанії довелося встановити у виробництво 128 роботів [10].

Harley Davidson — ще один приклад успішного впровадження Інтернету речей. Повільне реагування на запити та запити клієнтів стало основною проблемою в умовах високої конкуренції. Для вирішення цієї проблеми у 2009-2011 роках було модернізовано весь виробничий процес та перебудовано всі заводи. Це призвело до об’єднання всіх заводів в одну складальну ділянку, що дозволило покупцям вибрати з близько 1300 настроюваних версій попередніх 5 мотоциклів.У виробництві використовуються датчики, керовані спеціалізованою системою класу MES. Радіочастотні мітки на кожній деталі

та на машині ідентифікують продукт і вказують на його життєвий цикл. Платформа обробки даних діяла як інтегрована шина, яка зберігає дані від інформаційних систем і датчиків. Ця інформація дозволила зробити більш гнучке управління та повну автоматизацію виробничого процесу [10].

Модернізація виробництва привела до наступних результатів:

— виробничий цикл скоротився з 21 дня до 6 днів;

— повністю підготовлений і налаштований мотоцикл зійшов з конвеєра за 89 секунд;

— вартість акцій компанії зросла в 7 разів.

Також відбувається інтеграція Інтернету речей в агропромислові комплекси. Але крім датчиків, що входять до складу засобів обробки та передачі даних, використовують актуатори — пристрої, що перетворюють цифрові електричні сигнали з інформаційних мереж в дію. Наприклад, автоматичні системи контролю вологості в приміщенні. Комбінування приводів з датчиками є поширеним явищем.

Прикладами використання Інтернету речей в аграрному секторі є вагові процесори, системи контролю та управління доступом, сканери штрих-кодів.

Системи контролю та управління доступом є важливою частиною роботи такого типу підприємств, оскільки такі системи дозволяють вести облік робочого часу та підтримувати базу відвідувачів. При розробці системи контролю доступу необхідні джерела живлення. Вирішити першу проблему з центральним живленням можна кількома способами, цей спосіб популярний, оскільки його легше організувати, але якщо блок живлення працює погано — вся система. Ви можете використовувати кілька панелей для різних областей. Також є PoE (живлення через Ethernet). Зараз багато пристроїв мають підтримку PoE. Щоб під’єднати прилад до електромережі та зарядити його для належної роботи, потрібен лише кабель категорії 5.

Мережа ACS — контролери ACS, підключені через центральний сервер. Це оптимальний варіант для великих компаній, оскільки вони можуть управляти десятками дверей.

Системи моніторингу мережі слід використовувати в таких випадках:

— коли потрібна інформація про події або коли потрібен моніторинг у режимі реального часу;

— коли необхідно вести облік робочого часу та контролювати роботу працівників;

— чи здійснюється підключення, наприклад, із системами відеоспостереження чи пожежної сигналізації.

У таких системах ви можете контролювати події в зоні з місця, централізовано керувати правами користувачів і підтримувати базу даних з одного місця. Якщо неможливо встановити дротове з'єднання між об'єктами, можна використовувати технології бездротового з'єднання, такі як Bluetooth, Wi-Fi, ZigBee та GSM в діапазоні 2,45 ГГц.

Автономні системи значно дешевші за мережеві, прості у використанні, не вимагають сотень метрів кабелю, використання пристроїв, які спілкуються з сервером, самим сервером. облік робочого часу, надання та узагальнення інформації про події, дистанційне керування.

Вагові процесори дозволяють автоматизувати процес введення записів продукції та зберігати інформацію про вимірювання ваги в певному хронологічному порядку. Незважаючи на відмінності, всі моделі таких пристроїв підключаються до мережі однаково. Спочатку налаштовується апаратне підключення, яке можна здійснити через порти RS-232 або RS-485, а іноді може знадобитися встановити карти розширення PCI для COM-портів. Після підключення обладнання необхідно встановити необхідні драйвера для правильної роботи. Багато сучасних моделей складських ваг можна підключити до мережі через Ethernet. Це ще більше розширює можливості

користувачів і дозволяє інтегрувати вимірювальні прилади із загальною корпоративною системою обліку.

Сканери штрих-кодів полегшують співробітникам зберігання та читання інформації про продукт. Залежно від виду навчання вони поділяються на лазерні та фотосканери. Різниця між ними полягає в надійності використання, так як фотосканери, які трохи пошкоджені штрих-кодом, можуть не працювати належним чином. Сканери штрих-кодів поділяються на три типи залежно від способу підключення до комп'ютера: «пошкодження клавіатури», використання послідовного COM-порту та використання порту USB, що емулює інтерфейс RS232.

Але потужні технології, такі як Інтернет речей, мають і свої недоліки. Через популярність та новизну ринку виникла проблема невідповідності різним стандартам. Щоб вирішити цю проблему, компанії намагаються вибрати найкращі стандарти або розробити давно встановлені стандарти для загального використання. Одним із таких стандартів є OneM2M, якого вже дотримуються 230 компаній, серед яких Amazon, Cisco, Huawei, Intel, NEC, Qualcomm, Samsung та інші.

Друге питання технології — інформаційна безпека. Багато пристроїв не шифрують бездротовий трафік, системи безпеки досить прості, неможливо встановити паролі достатньої складності. Ці фактори дозволяють зловмисникам змінювати налаштування пристрою, вимикати їх або контролювати їх роботу, не повідомляючи їх власників.

1.7 Автоматизація налаштування інформації про адресу кінцевої точки.

DHCP — це протокол прикладного рівня, який автоматично розподіляє та призначає мережеві ідентифікатори (IP-адреси) мережевим комп'ютерам. Протокол працює за моделлю клієнт-сервер.

Сервер може працювати в кількох режимах, наприклад:

— динамічне виділення діапазону IP-адрес при розподілі адміністратором, в данному режимі оренда адреси не є довгостроковою і після її закінчення адреса може використовуватися іншим клієнтом;

— діапазон автоматичного розподілу також встановлюється адміністратором, але різниця в тому, що сервер веде запис минулих дій та намагається надати ту саму адресу для наступних дій;

— статичне призначення, коли DHCP-сервер призначає IP-адресу на основі таблиці MAC-адрес, заповненої вручну адміністратором мережі, якщо MAC-адреса комп’ютера не вказана в таблиці, йому не призначається мережева адреса.

Для отримання необхідних даних комп’ютер повинен зв’язатися з сервером DHCP. Для цього він надсилає пакет під назвою DHCPDISCOVER. Цей пакет розподіляється і містить апаратну адресу відправника, завданням якого є пошук сервера. Доступні сервери DHCP обробляють запит і відповідають на пакет DHCPOFFER. Цей пакет містить можливу IP-адресу та "час найму". Клієнт вибирає один із прийнятих DHCPOFFER. Потім він надсилає пакет із запитаним ім’ям сервера у відповідь на DHCPREQUEST. Щоб узгодити процес, сервер надсилає пакет підтвердження DHCPACK, який містить адресу та час оренди, який позначений як зайнятий і не може бути прийнятий жодним іншим клієнтом DHCP.

2 ПРОЕКТУВАННЯ МЕРЕЖІ

2.1 Огляд структури підприємства

Завдяки тому, що це підприємство є агропромисловим комплексом, воно займає значну площу близько 6 га. Підприємство поділено на багато промислових підприємств, але об’єкти, які потребують доступу до мережі, розташовані лише на відносно невеликій частині території. Але не всі вони входять до корпоративної мережі, бо не мають обладнання. Частиною мережі є такі розділи:

— 2 вагові дивізії;

— три операторські;

— адміністративна будівля;

— система контролю температури.

Структурна схема підприємства представлена на рисунку 2.1.

Рисунок 2.1 — Структурна схема підприємства

Кожна одиниця ваги складається з комп’ютера та одного або кількох вагових процесорів. Перший і другий ваги мають комп’ютер і два вагових процесори, а третій — комп’ютер і процесор. Операторська обладнана тільки

комп'ютерами, по одному в кожній операторській. На території є система контролю температури, яка контролює погоду та вологість.

Адміністративна будівля компанії являє собою двоповерхову будівлю, в якій проживає багато співробітників, розділених на корпоративні офіси. Компанія поділена на 8 робочих підрозділів:

— інженерна кафедра;

— магістерська кафедра;

— відділ охорони;

— вага;

— кафедра менеджменту та бухгалтерського обліку;

— лабораторне відділення;

— департамент операторів.

Схема першого поверху на рисунку 2.2.

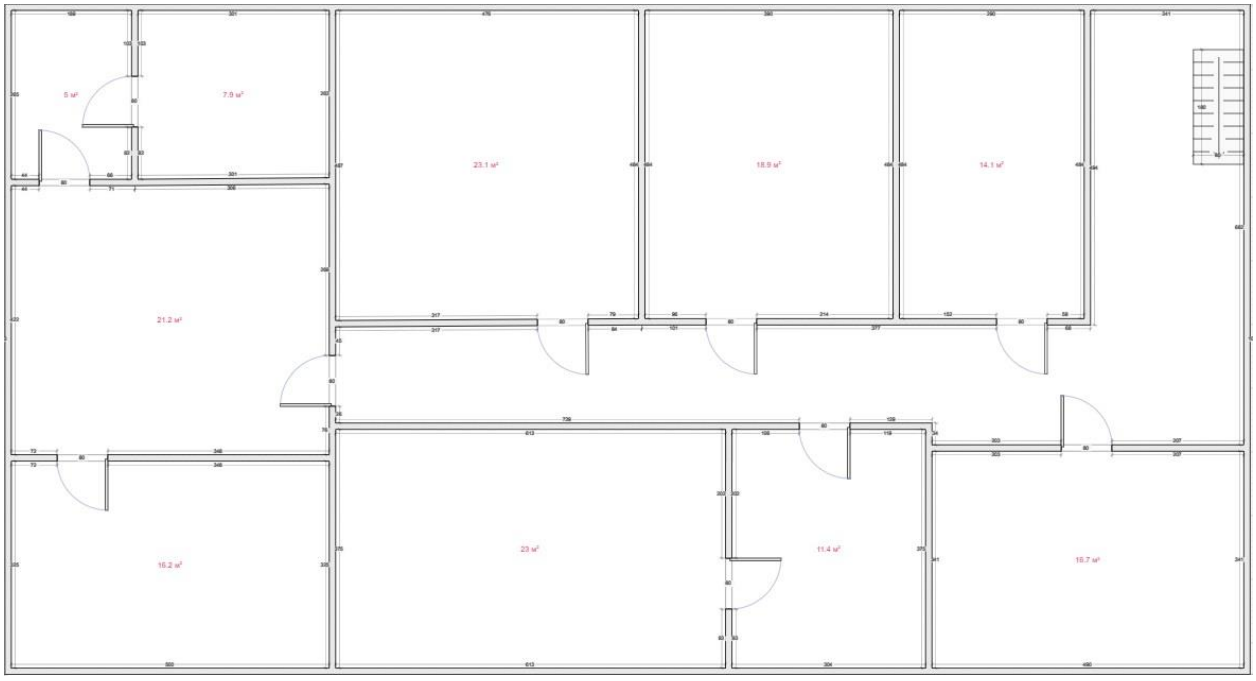

Рисунок 2.2 — Схема підприємства

Відповідність призначення шаф цифрам на схемі показано в таблиці 2.1.

Таблиця 2.1 — Відповідність номерів посад у схемі їх призначення

Номер кабінету на схемі	Призначення кабінету
1	Серверна
2	Коридор
3	Кабінет головного інженера
4	Кабінет інженерної служби
5	Лабораторія
6	Кабінет керівника
7	Приймальний кабінет
8	Бухгалтерія
9	Кабінет майстрів
10	Кабінет охорони
11	Навчальний клас

Кількість пристроїв у кожній шафі показано в таблиці 2.2.

Таблиця 2.2 — Кількість пристроїв у кожному офісі на першому поверсі

Кабінет	Пристрої
Коридор	Точка доступу Wi-Fi
Кабінет головного інженера	1 ПК, мережевий принтер
Кабінет інженерної служби	3 ПК, мережевий принтер
Кабінет старшого майстра	1 ПК
Вагова	1 ПК, 2 вагопроцесори
Прохідна	1 ПК, система контролю і управління доступом
Кабінет охорони	2 ПК та мережевий принтер
Навчальний клас	ПК моноблок

Якщо додати кількість пристроїв, які потрібно підключити до мережі на першому поверсі, то отримаємо 9 комп’ютерів, 3 мережеві принтери, 2 вагових процесора та систему контролю та управління доступом. Схема другого поверху будівлі наведена на рисунку 2.3.

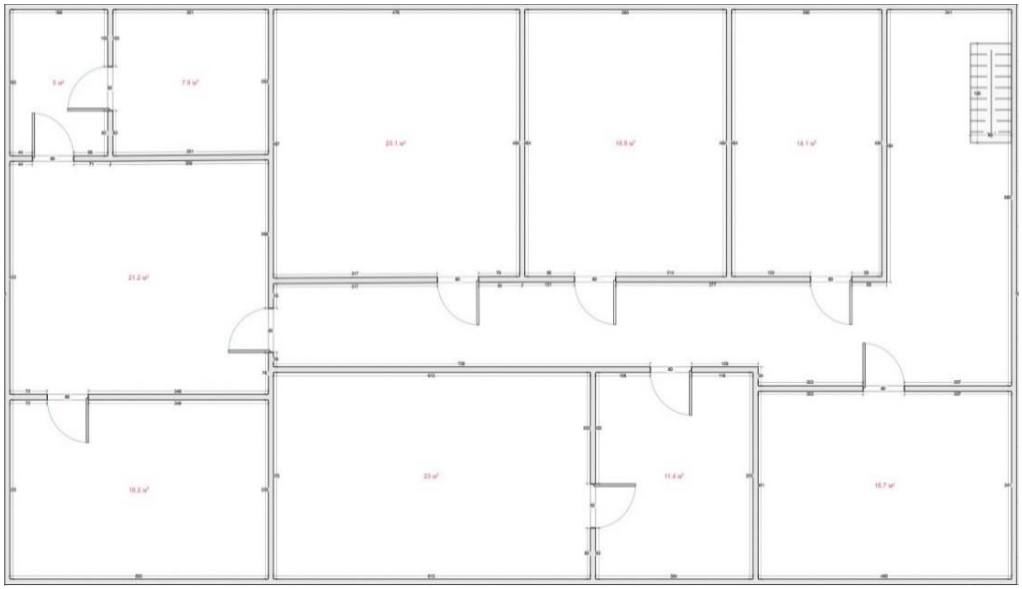

Рисунок 2.3 — Схема підприємства

Відповідність призначення шаф цифрам на схемі показано в таблиці 2.3.

Таблиця 2.3. — Відповідність номерів посад у схемі їх призначення

Номер кабінету на схемі	Призначення кабінету
1	Лабораторія
2	Переговорна
3	Кабінет керівника лабораторій
4	Коридор
5	Лабораторія
6	Кабінет керівника
7	Приймальний кабінет
8	Бухгалтерія

Кількість пристроїв у кожній шафі показано в таблиці 2.4.

Таблиця 2.4 — Кількість приладів у кожному кабінеті на другому поверсі

Кабінет	Пристрої
Лабораторія	1 ПК, 2 сканери штрих-кодів
Переговорна	Гостьова точка доступу
Кабінет керівника лабораторій	2 ПК, мережевий принтер
Лабораторія	1 ПК, 2 сканери штрих-кодів
Кабінет керівника	1 ПК
Приймальний кабінет	1 ПК
Бухгалтерія	2 ПК та мережевий принтер

Якщо додати кількість пристроїв, які потрібно підключити до мережі на першому поверсі, ви отримаєте 8 комп’ютерів, 2 мережеві принтери, 4 сканери штрих-кодів і бездротову гостьову точку доступу.

2.2 Розподіл адресного простору мережі

Компанія має три вагові відділення, дві операційні та одну офісну будівлю. Кожен з цих елементів повинен належати до окремої підмережі. Адреса 10.0.0.0 використовується для виділення адресного простору в підмережі. У таблиці 2.5. вказує, яка IP-адреса призначена певній частині мережі.

Таблиця 2.5 — Розподіл IP-адрес між бізнес-об'єктами

IP-адреса	Маска підмережі	Назва об’єкту підприємства
10.0.1.0	255.255.255.0	Адмінбудинок
10.0.2.0	255.255.255.0	Вагові
10.0.3.0	255.255.255.0	Операторські
10.0.4.0	255.255.255.0	Система контролю температури

В адміністративній будівлі компанії багато офісів та пристроїв, які необхідно підключити до мережі. Технологія VLAN повинна

використовуватися для зменшення перевантаженості мережі та безпеки мережі. VLAN — це налаштована мережа, що складається з однієї або кількох локальних мереж. Ця технологія дозволяє об’єднати групу пристроїв, доступних у кількох мережах, в одну логічну мережу. Результатом є віртуальна локальна мережа, якою керують як фізична локальна мережа. Повний тип VLAN визначається як віртуальна локальна мережа. Технологія VLAN має наступні переваги:

— вирішує проблеми мовлення;

— зменшено розмір розподілених доменів;

— дозволяє додати додатковий рівень безпеки;

— це спрощує і спрощує роботу пристрою;

— можливість логічно групувати пристрої за функціями, а не за місцем розташування;

— дозволяє створювати групи логічно підключених пристроїв, які діють так, ніби вони знаходяться у власній мережі;

— можливість логічно сегментувати мережі на основі розділів, груп проектів або функцій;

— VLAN допомагає географічно об’єднати вашу мережу для підтримки бізнесу, що розвивається;

— висока продуктивність і низька затримка;

— VLAN забезпечують хорошу продуктивність;

— користувачі можуть працювати з конфіденційною інформацією, яка не повинна бути видимою для інших користувачів;

— таким чином ви можете легко сегментувати мережу;

— це допомагає підвищити безпеку мережі;

— можливість спільного використання хостів VLAN;

— вам не потрібні додаткові пристрої та кабелі, щоб заощадити;

— зміна IP-підмережі користувача має оперативні переваги, оскільки виконується програмно;

— це зменшує кількість пристроїв для заданої топології мережі;

— VLAN спрощує керування фізичними пристроями.

Кабінети в компанії, об'єднані загальним робочим процесом, можуть бути об'єднані в тип підгрупи, який відокремлений від інших груп. Ви можете призначити кожну з цих груп до окремої VLAN. Це запобігає небажаному трансляційному трафіку та додатково захищає корпоративні дані.

Навчальні кабінети можна розділити на 5 секцій, а саме: лабораторний відділ, який складається з двох лабораторій та кабінету завідувача лабораторією, інженерний відділ, що складається з кабінетів інженерних служб та кабінету головного інженера, магістерський відділ, що складається з майстрів і майстрів. магістрантів, відділ охорони, до складу якого входить адміністративно-бухгалтерський відділ, що складається з вхідної кімнати та кабінету охорони, кабінету директора, приймальні, конференц-залу та бухгалтерії. Також необхідно виділити вимірювальну та серверну кімнату для подальшого захисту даних компанії. Є 8 розділів на 8 VLAN. У таблиці 2.6 показано номери VLAN, призначені відповідним розділам.

Таблиця 2.6 — Призначення розділів номерам VLAN

Номер VLAN	Назва відділу адмінбудинку
101	Відділ інженерів
102	Відділ майстрів
103	Відділ охорони
104	Ваговий кабінет
105	Відділ керівництва та бухгалтерії
106	Відділ лабораторій
107	Серверна

Щоб максимально використовувати адресний простір, вам потрібно використовувати маски змінної довжини для призначення IP-адреси VLAN. Необхідно враховувати можливе розширення мережі та встановлення нових пристроїв, тому мінімальна кількість хостів для підмережі становить 16 хостів. Для цього скористайтеся маскою 255.255.255.240, яка складається з 28

префіксів. У таблиці 2.7 наведено адреси внутрішніх мереж та маски, які використовуються у внутрішніх мережах адміністративної будівлі.

Таблиця 2.7 — Адреси підмереж та маски , що використовуватимуться у під мережах адмінбудинку

номер (VLAN)	Адреса підмережі	Маска підмережі	Перша доступна адреса	Остання доступна адреса	Широкомовна адреса
VLAN 101	10.0.1.0	255.255.255.240	10.0.1.1	10.0.1.14	10.0.2.15
VLAN 102	10.0.1.16	255.255.255.240	10.0.1.17	10.0.1.30	10.0.2.31
VLAN 103	10.0.1.32	255.255.255.240	10.0.1.33	10.0.1.46	10.0.2.47
VLAN 104	10.0.1.48	255.255.255.240	10.0.1.49	10.0.1.62	10.0.2.63
VLAN 105	10.0.1.64	255.255.255.240	10.0.1.65	10.0.1.78	10.0.2.79
VLAN 106	10.0.1.80	255.255.255.240	10.0.1.81	10.0.1.94	10.0.2.95
VLAN 107	10.0.1.96	255.255.255.240	10.0.1.97	10.0.1.110	10.0.2.111

Для подальшої фільтрації трафіку для підмереж, які не знаходяться в адміністративній будівлі, слід також призначити окремі мережі VLAN. Тобто всі оператори мають бути призначені для однієї VLAN, а ваги мають бути призначені для окремої VLAN. Оператор посилається на VLAN 108, а вага відноситься до VLAN 109.

2.3 Розробка логічної топології мережі

Логічна топологія — це розташування мережевих пристроїв і вузлів, які складають логічну або фізичну структуру. Існують різні типи мережевих топологій, які використовуються для організації вузла мережі для формування структури мережі. Буквальне значення топології — це структура мережі та

взаємопов'язаних вузлів. Існує два типи топологій: логічна та фізична. Логічна топологія має справу з мережевими протоколами, які використовуються для керування потоком даних у мережі. Це тип топології мережі, що використовується для визначення архітектури мережі, яка використовується для передачі даних між вузлами мережі. Вузли мережі включають роз’єми та вузли, які можна використовувати для побудови мережі. Логічна топологія допомагає визначити правильний канал для передачі даних і підтримує мережу. Логічна топологія використовується для створення способу передачі сигналів по мережі. Він використовує мережеві протоколи, які визначають спосіб надсилання пакетів. Його можна використовувати для проектування мережевої структури. Його також можна розглядати як мережеву схему і допомагає реалізувати фізичну мережу у фізичній топології. Схема має всі вузли та комутатори, задіяні в мережі, і спосіб передачі даних по мережі. Він використовується для визначення високого рівня відтворення мережі.

Якщо розглядати мережу компанії, то кожен оператор має своє приміщення та окрему внутрішню мережу вагової. Вони підключаються до адміністративної будівлі через єдиний центральний маршрутизатор, який відповідає за маршрутизацію між мережами та забезпечує доступ до Інтернету. Через це мережа не потребує протоколу динамічної маршрутизації, оскільки всі мережі підключаються безпосередньо до цього маршрутизатора. Мережні IP-адреси розповсюджуються через DHCP-сервер, розташований в адміністративній будівлі компанії. В адміністративній будівлі вузли першого та другого поверхів розділені окремими вимикачами. Потім вони підключаються до комутатора, який веде до центрального маршрутизатора.

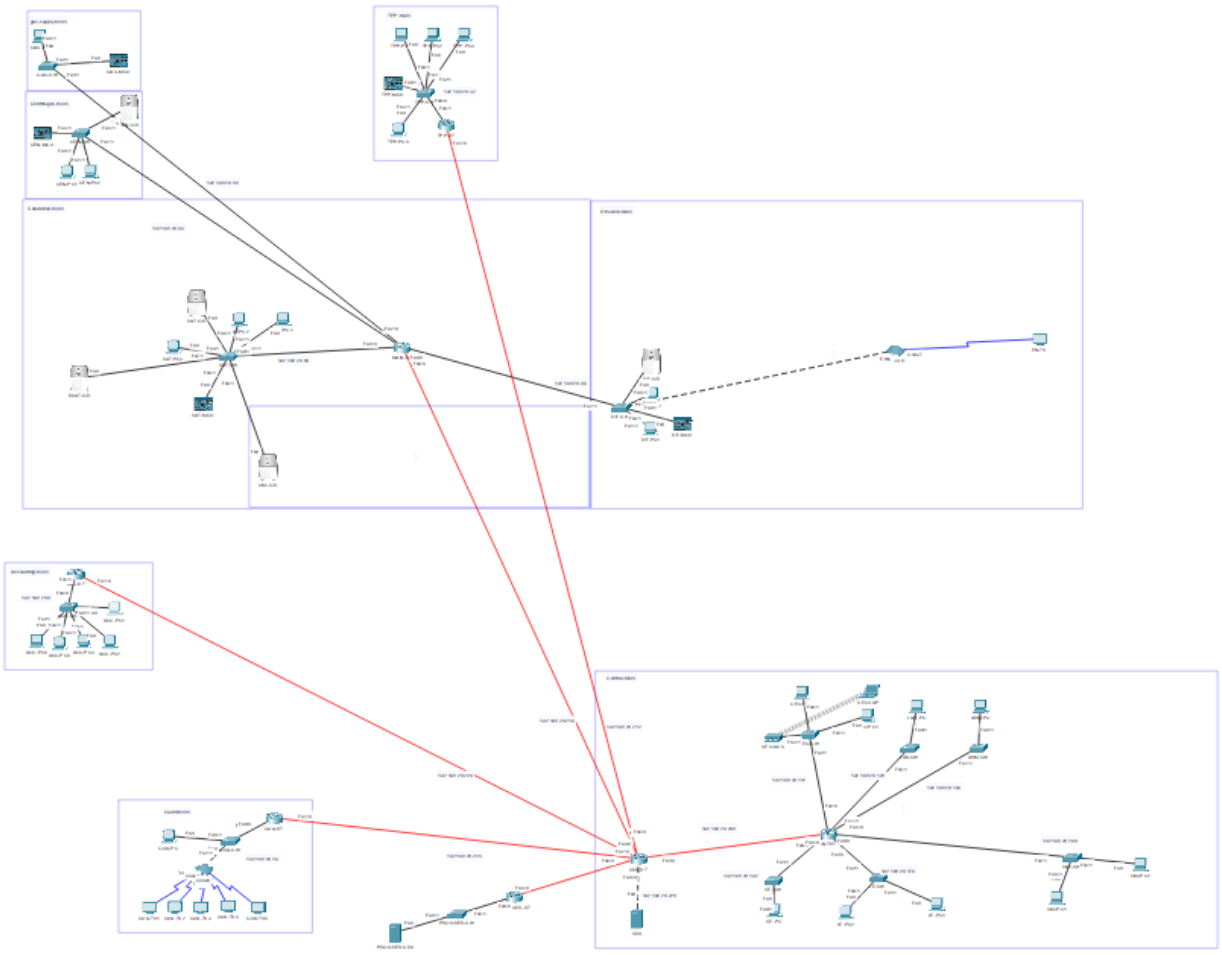

Рисунок 2.3 — Відображається логічна топологія мережі.

2.4 Вибір активних мережевих пристроїв для реалізації комп'ютерної мережі

За порівняльними характеристиками були відібрані три компанії-виробники мережевого обладнання: CISCO, MIKROTIK і Hewlett-Packard. CISCO SYSTEMS INC. є провідною мережею у світі. Сьогодні рішення Cisco є основою для постачальників послуг, малого та середнього бізнесу та корпоративних споживачів, включаючи корпорації, державні установи, комунальні підприємства та навчальні заклади. Крім того, 85% інтернет-трафіку проходить через системи Cisco.

Продукти MikroTik — це мережеві пристрої. MikroTik проектує, впроваджує та встановлює дротові та бездротові маршрутизатори, підключені пристрої та операційні системи. Для реалізації проекту African WiFi та створення мережевої інфраструктури в Малі були обрані маршрутизатори та операційні системи MikroTik виробництва MicroTik завдяки таким перевагам, як низька вартість, гнучкість, популярність та простота використання інтерфейсу.

Hewlett-Packard була американською транснаціональною компанією з інформаційних технологій, яка розробляла та поставляла широкий спектр обладнання, широко відомого як HP. Компоненти, програмне забезпечення та супутні послуги для споживачів, малих і середніх підприємств (МСП) і великих підприємств, включаючи державні, медичні та освітні споживачі. Зараз це потужний виробник мережевих технологій.

2.4.1 Маршрутизатори

Маршрутизатор — це мережевий пристрій, який передає пакети даних між комп’ютерними мережами. Маршрутизатори виконують функції транспортування трафіку в Інтернеті. Дані, надіслані через Інтернет, наприклад В., можуть бути у формі веб-сайту або пакетів даних електронною поштою. Пакет зазвичай пересилається з одного маршрутизатора на інший через мережу, яка є магістральною (наприклад, Інтернет), доки не досягне місця призначення.

Маршрутизатор підключений до двох або більше мереж передачі даних різних IP-мереж. Коли пакет даних надходить на одну з доріжок, маршрутизатор зчитує інформацію про мережеву адресу в заголовку пакета, щоб визначити останній пункт призначення. Потім він надсилає пакет до наступного рядка шляху, використовуючи інформацію в розкладі маршрутизації або політиці маршрутизації. Корпоративні маршрутизатори з'єднують великі корпоративні мережі або мережі Інтернет-провайдера з

високопродуктивними основними маршрутизаторами, які передають дані з високою швидкістю через волоконно-оптичні мережі Інтернету.

Ми розглянемо три моделі роутерів від різних виробників:

— Cisco ISR 1100 (C1111-8P);

— HP FlexNetwork MSR958 (JH300A);

— MICROTIC RB4011IGS + RM.

Cisco ISR 1100 — це високопродуктивний маршрутизатор зі фіксованою конфігурацією. Пристрій забезпечує безпечний широкосмуговий доступ. Призначений для інтеграції у великі корпоративні мережі для офісів і підприємств. Маршрутизатор допомагає підвищити продуктивність співробітників і загальну продуктивність мережі, обмежуючи перегляд Інтернету відповідними категоріями сайтів і усуваючи небажаний мережевий трафік. Кожен бізнес постійно піддається небезпеці Інтернету. За допомогою цього пристрою користувачі автоматично захищені від шкідливих або зламаних веб-сайтів, незалежно від категорії веб-сайту.

Термінали та програми можна визначати та обробляти відповідно до визначених користувачем політик для підвищення продуктивності та оптимального використання мережі. Має компактний корпус і економічний в плані живлення. Висока продуктивність пристрою дозволяє використовувати широкосмугове підключення і одночасно запускати різні мережеві послуги. Пристрій має багаторівневу систему безпеки з вбудованим брандмауером, швидкісним шифруванням і багатьма іншими функціями. Маршрутизатор працює за технологією PoE і може бути встановлений на стіні або стелі. Особливості включають багатоядерний процесор і IPsec VPN. Характеристики пристрою наведені в таблиці 2.8.

Маршрутизатор HP FlexNetwork MSR958 забезпечує високу маршрутизацію продуктів для невеликих відділень. Завдяки вбудованим і неліцензійним можливостям маршрутизації, комутації, безпеки та голосу,

Таблиця 2.8 — Характеристики Cisco ISR 1100

Оперативна пам’ять	4гб
Flash	4гб
Інтерфейс для консолі	USB 3.0
Інтерфейси DSL	Dying gasp ITU G.993.2 (VDSL2) and supported profiles: 8a, 8b, 8c, 8d, 12a, 12b, and 17a VDSL2 Vectoring ADSL Annex A and Annex B ITU G. 992.1 (ADSL), G.992.3 (ADSL2), and G.992.5 (ADSL2+) ADSL Annex M G.992.3 (ADSL2) and G.992.5 (ADSL2+
Живлення PoE	4 x PoE або 2 x PoE+ (потрібне опціональне джерело живлення "ISR-1100-POE4" на 125 Вт)
Види живлення	Від 100 В до 240 В
Максимальна споживана потужність	До 12,5 Вт
Робоча температура	Від 0 °C до 40 °C
Габарити,	42 мм x 323 мм x 230 мм
Мережеві порти	WAN: 1 x GE, 1 x SFP combo LAN: 8 x GE
Вага	2500г
Частота	від 50 Гц до 60 Гц.
Максимальна вихідна потужність	До 66 Вт (за замовчуванням)
Кількість LAN-інтерфейсів (RJ-45)	8
Робоча висота над рівнем моря	3000м
Вологість при роботі	від 5% до 90%
Ціна	35 000грн

пристрій допомагає прискорити надання послуг і спростити керування корпоративною мережею.Пристрій є гнучким у розгортанні завдяки автоматичному розподілу ресурсів і підтримці різних способів підключення до глобальної мережі.

Завдяки Comware v7 і підтримці волоконно-оптичних з’єднань ця модель форм-фактора з фіксованим портом пропонує високу продуктивність і розширені функції. Програмне забезпечення HPE Intelligent Management Center (IMC)* спрощує керування. Управління спрощується за рахунок автоматизованого розгортання (ZTD) і автоматичного виявлення VPN (ADVPN). Маршрутизатор підтримує технологію NAT і має вбудований брандмауер, підтримку VPN і функції сервера DHCP. DES, 3DES і AES підтримують шифрування 128/192/256, а також автентифікацію MD5 і SHA-1. Характеристики пристрою наведені в таблиці 2.9.

Таблиця 2.9 — Характеристики HP FlexNetwork MSR958

Оперативна пам’ять	1гб
Flash	256мб
Процесор	Marvell A370
Інтерфейс для консолі	USB 2.0
Інтерфейси	SF/RJ-45 (комбінований роз’єм), RJ-45 (WAN), 8xRJ-45 (LAN)
Живлення PoE	є
Види живлення	Від 100 В до 240 В
Максимальна споживана потужність	До 20 Вт (максимум)
Робоча температура	Від 0 °C до 45 °C
Габарити	330мм x 44,2мм x 230 мм
Вага	2000 г
Кількість LAN-інтерфейсів (RJ-45)	8
Робоча висота над рівнем моря	1500м
Вологість при роботі	від 5% до 90%
Ціна	25 433грн

Mikrotik RB4011iGS + RM оснащений чотирьохядерним процесором Cortex-A15, Annapurna Labs, Amazon. Пристрій оснащений 1 ГБ оперативної

пам’яті, що дозволяє легко виконувати всі завдання, покладені на RouterOS. Десятий порт RB4011 може мати вихід PoE. І всі ці функції розміщені в компактному, професійно виготовленому, міцному металевому корпусі з темно-чорним покриттям. Пристрої серії RB4011 — це дуже потужні маршрутизатори з десятигігабітним портом Ethernet, десятигігабітним інтерфейсом, який забезпечує додаткове підключення за рахунок прискорення обладнання SFP + і IPsec за високу вартість. Характеристики приладу наведені в таблиці 2.10.

Таблиця 2.10 — Характеристики Mikrotik RB4011iGS+RM

Оперативна пам’ять	1гб
Flash	512мб
Процесор	Cortex A15 CPU
Інтерфейс для консолі	USB 2.0
Інтерфейси	SF/RJ-45 (комбінований роз’єм), RJ-45 (WAN), 8xRJ-45 (LAN)
Живлення PoE	є
Види живлення	Від 100 до 240 В
Максимальна споживана потужність	До 19 Вт (максимум)
Робоча температура	Від мінус 40°C до 70 °C
Габарити	228 мм x 30 мм x 228 мм
Вага	1500 г
Кількість LAN-інтерфейсів (RJ-45)	10
Робоча висота над рівнем моря	1500м
Вологість при роботі	до 70%
Ціна	5449грн

2.4.2 Комутатори

CISCO SF220-24-K9-EU — 24-портовий роз'єм Fast Ethernet з 2 комбінованими портами Mini-GBIC, 24-портовий роз'єм SF220-24 10/100

Smart Plus. Роз’єм Cisco SB SF220-24 є хорошим вибором для підприємств, яким потрібна висока продуктивність, безпека та контроль. Він забезпечує рівень можливостей, необхідних для зростаючої компанії/мережі. Перемикач легко встановити і використовується як нетехнічними користувачами, так і IT-фахівцями. На додаток до інтуїтивно зрозумілого веб-інтерфейсу та утиліти Cisco FindIT, пристрій пропонує такі параметри керування, як простий протокол керування мережею (SNMP) та інтерфейс командного рядка (CLI). SF220-24 був протестований компанією Cisco, щоб забезпечити високу доступність і продуктивність, на які очікують користувачі. Продукт скорочує час передачі файлів, зберігає важливі бізнес-додатки та дозволяє вашим співробітникам швидше реагувати на запити клієнтів і клієнтів. Завдяки розширеним можливостям QoS він також забезпечує управління трафіком високої пропускної здатності та гнучкість пріоритетів, що дозволяє легко інтегрувати всі бізнес-з’єднання та з’єднання в єдину конвергентну інфраструктуру. Характеристики пристрою наведені в таблиці 2.11.

Таблиця 2.11 — Специфікації CISCO SF220-24-K9-EU

Кількість портів	24 x Ethernet 10/100/1000 Мбит/сек 4 x uplink/SFP 10/100/1000 Мбит/сек
Пропускна спроможність	8.8 Гбіт/с
Порти	SFP, Fast Ethernet, Gigabit Ethernet
PoE	немає
Flash-пам'ять	32 Мб
Робоча температура	від 0˚ до 50˚ C
Діапазон вологості (робота)	від 10% до 95% без конденсату
Живлення	Від 100 В до 240 В
Вага	3640г
Розміри	440 мм x 44 мм x 250 мм
QoS	підтримується
Швидкість передачі пакетів	6.55 Мп / с
Ціна	4699грн

Гігабітний Ethernet-роз’єм HPE 1620 24G L2 (JG913A). Це роз’єм рівня 2, яким керує HP. Його можна закріпити на спеціальній полиці для вимикачів. Оснащений 24 гігабітними портами, швидкість яких досягає 48 Гбіт/с в матриці комутації. Він також оснащений таблицею MAC-адрес на 8192 записів і двома типами внутрішньої пам'яті — 128 МБ RAM і 32 МБ Flash. Елементи керування включають консольний порт, WEB-інтерфейс та підтримку технологій Telnet і SNMP. Крім того, порти підтримують технологію автоматичного визначення типу кабелю MDI / MDI (X). Він визначає, чи використовується звичайний кабель або перехресний кабель. Характеристики пристрою наведені в таблиці 2.12.

Таблиця 2.12 — Властивості L2 Gigabit Ethernet HPE 1620 24G (JG913A)

Кількість портів	24 x Ethernet 10/100/1000 Мбіт/сек
Комутаційна спроможність	48 Гбіт/с
PoE	немає
Flash-пам'ять	32 Мб
Стекування	є (віртуальне)
Робоча температура	від 0˚ до 40˚ С
Діапазон вологості (робота)	від 10% до 95% без конденсату
Живлення	від 100 В до 240 В
Частота змінної напруги на вході	50/60 Гц
Вага	2200г
Розміри	440 мм x 44 мм x 173 мм
QoS	підтримується
Проопускна спроможність	35.7 Мп / с
Ціна	7622 грн

CSS326-24G-2S + RM — перша модель керованих роз'ємів MikroTik відкриває нову лінійку Cloud Smart Switch (CSS). Основною відмінністю цієї лінійки від серії CRS є відсутність RouterOS, а перемикач керується SwOS. Це,

звичайно, обмежує використання пристрою, але дозволяє значно знизити вартість і забезпечити високу продуктивність. Передня частина пристрою має всі 26 доступних інтерфейсів, включаючи 24 порти RJ45 Ethernet 1000/100/10 і 2 порти SFP + (модуль) для підключення волоконно-оптичних кабелів. Коммутатор має форм-фактор 1U і підтримує технологію PoE. Висхідний / низхідний канал реалізується через два порти SFP +, які підтримують модулі GBIC 1.25 і 10G. При необхідності їх можна об'єднати для отримання єдиного каналу 20 Гбіт/с. Характеристики пристрою наведені в таблиці 2.13.

Таблиця 2.13 — Характеристики CSS326-24G-2S + RM

Кількість портів	24 × 10/100/1000 Мбіт/с Ethernet з Auto-MDI/X 2 × SFP cage Gigabit Ethernet
PoE	підтримується
Flash	2 МБ
Робоча температура	від 0˚ С до 60˚ С
Діапазон вологості (робота)	від 10% до 95% без конденсату
Живлення	160 В
Потужність живлення	24 В
Частота змінної напруги на вході	50/60 Гц
Вага	1900г
Розміри	200 мм x 44 мм x 143 мм
QoS	підтримується
Ціна	3800 грн

Перемикач HP 1620-8G JG912A Цей пристрій виготовлено компанією HP. Це керований комутатор другого рівня для управління мережею малого офісу. Він оснащений 8-ма портами LAN за технологією GE (Gigabit Ethernet), тобто кожен порт забезпечує провідну швидкість до 1000 Мбіт/с. Завдяки технології комутаційної матриці загальна внутрішня швидкість передачі даних

досягає 18 Гбіт/с. Він також має 4 гігабітні порти, які підтримують технологію PoE +, що дозволяє заряджати комутатор за допомогою кабелю витої пари та підключати різні IP-пристрої. Всі порти підтримують технологію Auto-MDI / MDI (X), яка визначає, який тип кабелю використовується в порту — перехресний або звичайний. Існує WEB-інтерфейс, до якого можна отримати доступ через браузер через http / https для керування мережею та комутачем. Характеристики пристрою наведені в таблиці 2.14.

Таблиця 2.14 — Характеристики С HP 1620-8G Switch JG912A

Кількість портів	8 × 10/100/1000 Мбіт/с Ethernet з Auto-MDI/X
PoE	підтримується
Flash	32 МБ
Робоча температура	від 0˚ С до 40˚ С
Діапазон вологості (робота)	від 10% до 95% без конденсату
Живлення	від 100 В до 240 В
Потужність живлення	7 В
Частота змінної напруги на вході	50/60 Гц
Вага	1000г
Розміри	265 мм х 44 мм х 162 мм
QoS	підтримується
Ціна	3138 грн

MikroTik CRS112-8G-4S-IN — це контрольований роз'єм 3 рівня з 8 гігабітним мережевим портом і 4 портами SFP для оптики. Перемикач також можна використовувати як маршрутизатор, оскільки він має повну операційну систему RouterOS Level 5. OS RouterOS може обмежувати швидкість роботи користувачів, блокувати торренти та соціальні мережі, організовувати віддалений доступ до офісу через VPN, PPPoE, брандмауер, проксі тощо. дозволяє налаштувати. Коммутатор підтримує живлення PoE через перший порт LAN. Для цього необхідно придбати гігабітний PoE-інжектор. Купувати MikroTik CRS112-8G-4S-IN вигідно, оскільки він має низьку ціну і поєднує в собі комутатор і роутер. Його оптичні порти SFP забезпечують високу

швидкість передачі даних і захист від блискавки при прокладці волоконно-оптичних кабелів на вулиці. Купувати MikroTik CRS112-8G-4S-IN вигідно, оскільки він має низьку ціну і поєднує в собі комутатор і роутер. Його оптичні порти SFP забезпечують високу швидкість передачі даних та захист від блискавки при прокладці волоконно-оптичних кабелів на вулиці.Пристрій призначений для використання всередині приміщень при температурах від — 30°C до +60°C. Характеристики пристрою наведені в таблиці 2.15.

Таблиця 2.15 — Характеристики MikroTik CRS112-8G-4S-IN

Кількість портів	8 × 10/100/1000 Mbit/s Ethernet with Auto-MDI/X 4 × SFP cage Gigabit Ethernet (Mini-GBIC; SFP модуль не поставляется) 1 × serial port RJ45
PoE	підтримується
Flash	16 МБ
Робоча температура	від 0˚ С до 60˚ С
Діапазон вологості (робота)	від 10% до 95% без конденсату
Живлення	від 100 В до 240 В
Потужність живлення	7 В
Частота змінної напруги на вході	50/60 Гц
Вага	950г
Розміри	200 мм х 44 мм х 143 мм
QoS	підтримується
Ціна	3586 грн

Якщо вам потрібне просте високошвидкісне з’єднання для комп’ютерів і серверів, чи комплексне рішення для передачі даних, роз’єм Cisco SB SG250 може задовольнити потреби вашого бізнесу.

Швидке з’єднання з комп’ютером: продукт швидко та безпечно з’єднує співробітників, які працюють у невеликих офісах, один з одним, з усіма принтерами, серверами та іншими пристроями, які вони використовують. Висока продуктивність і надійне з’єднання прискорюють передачу файлів і обробку даних, покращують доступність мережі та забезпечують продуктивність співробітників. Гнучкий бездротовий зв’язок: комутатор працює з бездротовими рішеннями сторонніх виробників, щоб розширити

можливості вашої мережі. Продукт із можливостями безпеки, VLAN та QoS є чудовою основою для підключення бездротових мереж бізнес-класу. Легко налаштовувати та керувати. Cisco SB SG250 розроблено для того, щоб бути простим у розгортанні та використанні малими підприємствами або їх партнерами з обслуговування. Технологія Cisco Smartports надає розширені можливості та практичні вказівки шляхом автоматичного налаштування портів із певними рівнями безпеки, якості та доступності на основі найкращих методів роботи мережі Cisco та попередньо налаштованих типів підключених пристроїв, а також надання доступу до базової інформації про апаратне забезпечення та оновлень мікропрограми. Характеристики пристрою наведені в таблиці 2.16.

Таблиця 2.16 — Характеристики Cisco SB SG250

Кількість портів	8 × 10/100/1000 Mbit/s Ethernet with Auto-MDI/X
PoE	підтримується
Flash	256 МБ
Робоча температура	від 0˚ С до 60˚ С
Діапазон вологості (робота)	від 10% до 95% без конденсату
Живлення	від 120 В до 230 В
Потужність живлення	7 В
Частота змінної напруги на вході	50/60 Гц
Вага	1200г
Розміри	260 мм x 44 мм x 170 мм
QoS	підтримується
Ціна	3468 грн

2.4.3 Пристрої IoT

Мережа повинна мати систему контролю температури, сканери та вагові процесори. Якщо ви розглядаєте системи контролю температури, вибір падає на систему контролю температури та вологості в реальному часі від Huato TCP / IP (RJ45). Ця модель задовольняє всі потреби компанії, зокрема, датчики вологості та температури та можливість підключення до мережі, а також дистанційне керування та управління.

Ця функція — інтерфейс RJ-45, який усуває будь-які обмеження на відстань, оскільки ці типи пристроїв підключаються до мережі в основному за допомогою бездротових технологій, таких як Wi-Fi або GSM. Ви можете передавати дані на комп’ютер або на повноцінний сервер. За допомогою спеціального програмного забезпечення (To Monitor) можна налаштувати, зберігати та аналізувати записи та датчики в режимі реального часу. За допомогою ToCLient ви можете здійснювати моніторинг із мережевого комп’ютера. Під час встановлення обмежень система може звукові та світлові сигнали (сигнал A05 Ethernet), SMS (якщо доступний GSM (SMS) модем HE2508) та повідомлення електронною поштою. У разі збою в мережі рекордер має близько 43 000 копій внутрішньої пам'яті для копіювання. Більш детальний набір характеристик наведено в таблиці 2.17.

Таблиця 2.17 — характеристики системи контролю температури та вологості Huato

Тип сенсора	Зовнішні сенсори температури і вологості з 5 м кабелем
Діапазон вимірювань	40～85℃ / 0～100%RH
Точність вимірювання температури	±0.5℃
Точність вимірювань вологості	±5%RH
Дозвіл	Температура: 0.1 ℃ / Вологість: 0.1% RH
Обсяг запису	43,000
Діапазон частот	GSM 850 / 900 / 1800 / 1900 МГц
Акумулятор	Блок живлення 9 В / адаптер постійного струму 12 В
Інтерфейс	RJ45, завантаження даних на ПК через Ethernet
Дисплей	РК
Розмір Ркдисплея	97 мм* 78 мм (3.81 *1.37 дюйма) 52мм *31мм
Габарити	135 мм*124 мм*35 мм (5.31*4.88*1.37 дюйма)
Вага	380 г
Комплектація	блок живлення 9 В, монтажний гвинт, керівництво користувача, програмне забезпечення (LogPro)
Ціна приладу	450 USD
Ціна ліцензії для ПО (ToMonitor) на 1 прилад	30 USD
Метрологічна повірка на 1 прилад	850 грн
HE2508 GSM (SMS) —модем	320 USD

З необхідним програмним забезпеченням та метрологічним тестуванням, але без GSM-модему, в нашому випадку це не потрібно, тому вартість близько 13 810 грн. При виборі вагових процесорів було обрано три моделі, сумісні з ESIT Smart2, IE-04-A і Rinstrum R320.

Esit SMART-2 — це багатофункціональний контролер ваги, який виконує вимірювання та ваги, передає масові дані на комп'ютер і широко використовується для вирішення проблем обмеження маси. Пристрій може передавати дані на інші пристрої. Підключення здійснюється через поточний контурний інтерфейс, що дозволяє розмістити датчики подалі від блоку керування. Цей тип інтерфейсу є найбільш шумостійким. Точність вимірювань, висока швидкість ваги та віброфільтруючий пристрій роблять його одним із найкращих та найпопулярніших в Україні. Детальні характеристики пристрою наведені в таблиці 2.18.

Таблиця 2.18 — Властивості Esit SMART-2

Клас точності середній	ГОСТ 29329-92
Потужність керуючого каналу	250VAC, 220VDC / 2A
Тип керуючого каналу	релейний
Макс. кількість датчиків що підключаються	4 по 350 Ом /8 по 700 Ом
Тип перетворення в АЦП	сигма-дельта
Інтерфейс	аналоговий вихід 4..20 мА/0..5В, 2 реле, RS-232, RS-485, Wi-Fi
Тип індикатора	рідкокристалічний
Живлення	6-24В/2Вт
Функція усереднення та стабілізація маси	є
Температурний діапазон роботи	від мінус 10°С до 40 °С
Відносна вологість	від 10% до 90%
Виробник	ESIT
Габаритні розміри	118 мм х 117 мм х 46 мм
Маса (нетто)	200 г
Ступінь пило та вологозахисту	IP66
Ціна	7350 грн

Контролер обліку води Rinstrum R320 призначений для використання в автомобільних, залізничних вагах і системах з простою системою дозування (на виході 2 цифрових контрольних сигналу). Ви можете підключатися до ПК та принтерів через RS232, а також оновлювати програмне забезпечення дисплея та кнопки дистанційного керування ПК через вбудований інфрачервоний порт зв'язку (з'єднання з ПК за допомогою оптичного кабелю). Кількість одночасно підключених датчиків — до 16. Лінійне калібрування виконується за 10 точками з можливістю корекції лінійних точок. Детальні характеристики пристрою наведені в таблиці 2.19.

Таблиця 2.19 — Властивості R320 Rinstrum

Макс. кількість датчиків що підключаються	4 по 350 Ом /8 по 700 Ом
Точність перетворення	A/D 8388608
Інтерфейс	RS 232
Тип індикатора	рідкокристалічний
Функція усереднення та стабілізація маси	є
ступінь пило і вологозахисту	IP65
Температурний діапазон роботи від	від мінус 10°C до 50°C
Відносна вологість	від 10% до 90%
Виробник	Rinstrum
Ціна	12 864 грн

IE-04-A — цей індикатор використовується в різних типах платформних вантажних ваг. Його можна використовувати з невеликими односенсорними платформами, а також платформами з 4 і 8 датчиками. Кількість одночасно підключених датчиків 4x350 Ом і не більше 8700 Ом. Індикатор A12E можна підключати до 4-х і 6-провідних ланцюгів. У комплект входить вбудований акумулятор, комп'ютерний інтерфейс через RS232, функція HOLD. Детальні характеристики пристрою наведені в таблиці 2.20.

Таблиця 2.20 — Властивості IE-04-A

Макс. кількість датчиків що підключаються	4 по 350 Ом /8 по 700 Ом
Точність перетворення	A/D 130000
Швидкість перетворення	A/D 10
Вхідний діапазон сигналу	10-15
Інтерфейс	RS 232
Функція усереднення та стабілізація маси	є
Ступінь пило і вологозахисту	IP53
Температурний діапазон роботи від	0 °C до +40 °C
Габаритні розміри (ШхДхВ)	196x170x85 мм
Маса (нетто)	1,1 кг
Відносна вологість	від 10% до 90%
Ціна	2 160 грн

З усіх перерахованих вище вагових процесорів Esit SMART-2 є найкращим варіантом завдяки гнучкому підключенню, оптимальній ціні та надійності. За розмірами і умовами експлуатації не поступається аналогам. Також ця модель має найвищий захист від вологи та пилу серед розглянутих пристроїв.

При виборі сканерів штрих-кодів було обрано три моделі Zebra Motorola / Symbol LS2208, SunLux XL-6200A та Zebra Motorola / Symbol LI2208.

Motorola Symbol LS 2208 RS 232 пропонує чудову продуктивність, надійність і високі ергономічні властивості, створюючи умови, що підвищують продуктивність у будь-якій галузі. Цей сканер штрих-коду є чудовим рішенням завдяки своєму невеликому розміру та високій надійності.

Запатентований механізм сканування Motorola — це полімер, що лито під тиском, із вбудованим захистом від ударів, що забезпечує тривалий термін служби. Детальні характеристики пристрою наведені в таблиці 2.21.

Лазерний сканер штрих-кодів SunLux XL-6200A — це доступний пристрій для декодування штрих-кодів з низькою щільністю. Перевагою цього сканера є наявність підставки і можливість роботи в автоматичному режимі.

Таблиця 2.21 — Властивості IE-04-A

Інтерфейс	RS-232
Система зчитування	лазерна
Тип	ручний
Швидкість сканування	100 сканувань / с
Відстань сканування	280 мм
Глибина поля сканування	0 мм – 430 мм
Кут сканування	30˚
Напруга живлення	5 В ± 10%
Температура зберігання	від мінус 40 °С до 70 °С
Допустима висота падіння	1.5 м
Вага	146 г
Ціна	2 085грн

SunLux XL-6200A відноситься до класу пристроїв початкового рівня. Зазвичай такі пристрої купують у роздрібних продавців, на складах або в логістичних центрах з низькою швидкістю сканування штрих-кодів. Детальні характеристики пристрою наведені в таблиці 2.22.

Таблиця 2.22 — властивості SunLux XL-6200A

Інтерфейс	RS-232
Система зчитування	лазерна
Тип	ручний
Швидкість сканування	100 скянувань / с
Відстань сканування	350 мм
Глибина поля сканування	0 мм – 430 мм
Кут сканування	65˚
Напруга живлення	5 В ± 10%
Температура зберігання	від мінус 20 °С до + 60 °С
Допустима висота падіння	1 м
Вага	238 г
Ціна	1 734грн

Сканер штрих-кодів Zebra Motorola / Symbol LI2208, функцією якого є технологія сканування img. Лінійні сканери img можуть зчитувати штрих-коди на екранах мобільних телефонів, КПК, ноутбуків, планшетів та інших електронних носіїв. Запатентована одна друкована плата часто підвищує надійність пристрою, видаляючи несправні роз'єми та стрічкові кабелі. Ви можете опустити прилад і використовувати його в запиленому та вологому середовищі, не турбуючись про проблеми. Детальні характеристики пристрою наведені в таблиці 2.23.

Таблиця 2.23 — Технічні характеристики Zebra Motorola / Символ LI2208

Інтерфейс	RS-232
Система зчитування	лазерна
Тип	ручний
Швидкість сканування	547 сканувань / с
Відстань сканування	762 мм
Глибина поля сканування	0 мм – 430 мм
Кут сканування	35˚
Напруга живлення	5 В ± 10%
Температура зберігання	від мінус 40 °С до + 70 °С
Стійкість до зовнішніх подразників	витримує 100 падінь з висоти 1.5 м, 2000 падінь з висоти 0.5 м або падіння з висоти 1.8 м на бетонну поверхню
Вага	140 г
Ціна	2 406грн

Виходячи з порівняльних характеристик сканерів, модель Zebra Motorola / Symbol LI2208 була обрана за високу швидкість сканування та максимальну відстань склеювання, можливість сканування з різних електричних носіїв та

відмінну ударостійкість. Хоча за такими характеристиками він є найдорожчим серед розглянутих сканерів, ця різниця незначна і цілком узгоджена.

2.4.4 Вибір обладнення та підрахування потенційних витрат

Після короткого огляду компаній, які виробляють мережеві технології та їх продукти, ми можемо визначити плюси і мінуси кожної компанії. Всі три компанії рівні в різноманітності пристроїв, вибір пристроїв досить великий і відповідає всім цілям і потребам. За різноманітністю технологій CISCO об’єктивно є лідером у цьому плані, оскільки компанія впровадила багато сучасних мережевих технологій. Однак ця перевага не важлива, оскільки пристрої інших компаній підтримують практично всі необхідні технології для проектування потрібної нам мережі. З точки зору репутації, CISCO має найкращі рейтинги та оперативні огляди, але як MIKROTIK, так і HP мають хорошу репутацію. Технологія CISCO також займає перше місце з точки зору надійності, що свідчить про найдовший гарантійний термін. Виробники мають практично однакову стійкість до різних погодних умов. Ціна MIKROTIK іноді в кілька разів нижча за аналоги. Оскільки різниця між усіма факторами, окрім ціни, не дуже важлива і велика, то оптимальним варіантом буде вибирати прилади MIKROTIK в залежності від їх доступної ціни. Бажано використовувати обладнання одного виробника, щоб уникнути проблем з гібридною мережею.

Для корпоративної мережі потрібні 2 маршрутизатори, 2 комутатори із середньою кількістю портів і 6 комутаторів з невеликою кількістю портів. Мінімальна кількість портів на комутаторі має становити 8 портів, щоб масштабувати мережу в міру розширення технологічного обладнання. Пристроям IoT потрібні 6 вагових процесорів, 4 сканери штрих-кодів і система контролю температури. Тобто для реалізації мережі необхідно придбати 2 маршрутизатора MIKROTIK RB4011IGS + RM, 2 комутатори CSS326-24G-2S + RM, 6 комутаторів MikroTik CRS112-8G-4S-IN, 4 сканери Zebra Motorola /

Symbol LI2208. 6 вагових процесорів Esit SMART-2 і контроль температури Huato. Інформація про вартість наведена в таблиці 2.24.

Таблиця 2.24 — Інформація про вартість

Тип пристрою	Модель	Ціна за один екземпляр	Кількість	Загальна сума
Маршрутизатор	Mikrotik RB4011iGS+RM	5449 грн	2	10898 грн
Комутатор	CSS326-24G-2S	3800 грн	2	7600 грн
Комутатор	CRS112-8G-4S-IN	3586 грн	7	25102 грн
Сканер штрих кодів	Zebra Motorola/Symbol LI2208	2406 грн	4	9624 грн
Система котролю температури та вологості	Huato	13810 грн	1	13810 грн
Вагопроцесор	Esit SMART-2	7350 грн	6	44100 грн

Якщо додати усі суми, то отримаємо загальну суму витрат на обладнення без кабельної структури. Загалом виходить 111134 грн.

3 КОНФІГУРАЦІЯ МЕРЕЖИ ТА ТЕСТУВАННЯ

3.1 Налаштування віддаленого доступу

Для зручного встановлення мережевих пристроїв необхідно налаштувати віддалений доступ до них. Є два протоколи, які реалізують цю функцію, Telnet і SSH. Налаштовуємо Telnet на комутарах, а SSH потрібно налаштувати на роутері. Різниця між протоколами у використанні портів для підключення Telnet становить 23 і SSH 22 і використовує безпеку. SSH використовує методи шифрування з відкритим ключем. SSH також надсилає всі дані в зашифрованому вигляді, а Telnet надсилає дані у вигляді простого тексту.

Щоб почати інсталяцію, давайте створимо нову VLAN з номерами 111 для віддаленого доступу, який може виконувати лише адміністратор мережі. VLAN 111 має адресу 10.0.5.0. Далі вам потрібно створити VLAN 111 на всіх проміжних мережевих пристроях, призначити IP-адреси інтерфейсам VLAN і налаштувати маршрутизацію для VLAN 111. Налаштування маршрутизації VLAN описано у відповідному розділі нижче. Щоб налаштувати віддалений доступ, спочатку потрібно встановити паролі бажаного режиму. Є дві команди для додавання пароля та додавання пароля, перша зберігає пароль у звичайному режимі, друга шифрує його. Наступним кроком є створення віртуального інтерфейсу, який дозволить отримати доступ до пристрою віддалено. У режимі конфігурації віртуального інтерфейсу, щоб ввести та підключити пароль, необхідно встановити пароль і завершити конфігурацію за допомогою команди входу, яка відповідає на автентифікацію. Початкове налаштування комутатора наведено у лістингу 3.1.

Лістинг 3.1 — Налаштування на комутаторі протоколу telnet

```
Switch(config)#vlan 111
Switch(config-vlan)# name VLAN111
Switch(config)#interface vlan 111
```

Switch(config-if)#ip address 10.0.5.2 255.255.255.240

Switch(config)#enable secret 1234

Switch(config)#line vty 0 4

Switch(config-line)#user admin

Switch(config-line)#password 1234

Switch(config-line)#exit

Щоб переконатися, що він працює належним чином, налаштуйте віддалене підключення від комп’ютера адміністратора до налаштованого комутатора. Результати випробувань наведені на рисунку 3.1.

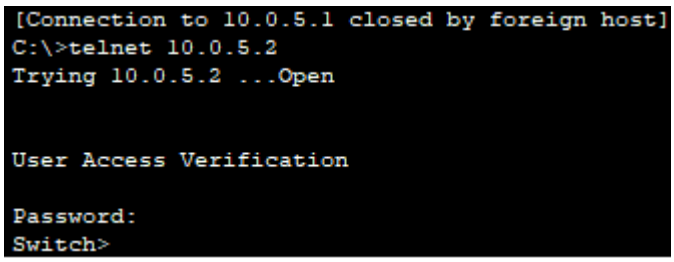

Рисунок 3.1 — Результати тестування протоколу Telnet

Оскільки підключення було успішним, конфігурація правильна. Інші роз'єми повинні бути налаштовані таким же чином. Щоб налаштувати SSH на маршрутизаторі, вам потрібно перейменувати його в консолі за допомогою команди host name. Потім, як і в telnet, потрібно створити віртуальний інтерфейс і встановити відповідні налаштування пароля. Вам також потрібно зареєструвати команду ssh для введення передачі, щоб вказати середовище доступу SSH у цьому режимі. Потім введіть ім’я домену та створіть ключ RSA. Вам потрібно створити ім’я користувача та встановити пароль для бажаного режиму, що робиться за допомогою імені користувача [ім’я] пароля [пароль]. Весь перелік команд для конфігурації SSH наведений у лістингу 3.2.

Лістинг 3.2 — Налаштування на комутаторі протоколу telnet

Router(config)#hostname CenterRouter

```
CenterRouter(config)#line vty 0 4
CenterRouter(config-line)#password 1234
CenterRouter(config-line)#transport input ssh
CenterRouter(config-line)#login
CenterRouter(config-line)#logging synchronous
CenterRouter(config)#username admin secret 1234
CenterRouter(config)#ip domain-name ROUTER
CenterRouter(config-line)#crypto key generate rsa
```

Щоб переконатися, що він працює належним чином, налаштуйте віддалене підключення від комп'ютера адміністратора до налаштованого маршрутизатора. Результати випробувань наведені на рисунку 3.2.

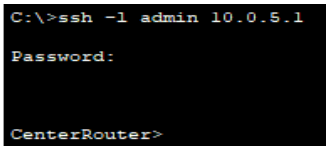

Рисунок 3.2 — Результат віддаленого підключення до роутера

Оскільки підключення було успішним, конфігурація правильна.

3.2 Налаштування VLAN і DHCP

Щоб пристрої працювали онлайн, вони повинні надати IP-адреси. Існує два способи налаштувати IP-адреси: вручну налаштувати адреси для кожного пристрою або використовувати DHCP. Перевага першого варіанту — безпека мережі, перевага другого — зручність та економія часу при великій кількості пристроїв із значно меншою інформаційною безпекою.

В якості DHCP-сервера можуть виступати різні пристрої. Наприклад, маршрутизатор, комутатор третього рівня або виділений сервер. У нашому випадку через відсутність роз'ємів третього рівня можна використовувати тільки роутер або сервер. Найкращий варіант — використовувати

корпоративний сервер. Оскільки сервер має бути в мережі VLAN107, спочатку потрібно налаштувати VLAN. Щоб налаштувати VLAN, ви повинні спочатку створити її на комутаторі в режимі конфігурації за допомогою команди vlan, а потім потрібного номера VLAN. Щоб підключити пристрій до VLAN, потрібно встановити режим доступу та призначити його потрібній мережі VLAN в інтерфейсі комутатора пристрою, підключеного до комутатора. Приклад створення VLAN і призначення режиму доступу до інтерфейсу показано в лістингу 3.3.

Лістинг 3.3 — приклад створення VLAN та присвоєння режиму доступу інтерфейсу на комутаторі Switch1

```
Switch(config)#vlan 101
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 101
Switch(config-if)#exit
Router(config)#interface fastEthernet 0/0.1
Router(config-subif)#
```

Для зручності та економії часу можна використовувати команду діапазон інтерфейсу, яка вимагає від вас вказати діапазон інтерфейсів, які потрібно налаштувати. Однак створення VLAN недостатньо для налаштування протоколу DHCP, оскільки DHCP-сервер не може отримувати пакети DHCPDISCOVER від клієнтів в окремій мережі VLAN у мережі та через обмеження домену розповсюдження.

Наступним кроком є налаштування маршрутизації між VLAN, щоб дозволити серверу DHCP спілкуватися з клієнтами. Інтерфейси маршрутизації трафіку з кількох VLAN слід скоротити. Для цього відкрийте інтерфейс за допомогою команди інтерфейсу та зареєструйте команду магістралі режиму

перемикання. Лістинг 3.4 показує приклад переведення інтерфейсу списку в режим транкингу.

Лістинг 3.4 — Переведення інтерфейсу у режим транкінгу на комутаторі Switch1:

```
Switch(config)#interface fastEthernet 0/16
Switch(config-if)#switchport mode trunk
```

Потім маршрутизатор повинен налаштувати маршрутизацію між VLAN. Для цього потрібно налаштувати маршрутизатор і створити віртуальні внутрішні інтерфейси для кожної з VLAN, до яких необхідно підключити магістральне з'єднання і вказати IP-адресу. Приклад конфігурації маршрутизації VLAN показаний у лістингу 3.5.

Лістинг 3.5 — Приклад конфігурування підінтерфейсу маршрутизатора

```
Router(config-subif)#enc
Router(config-subif)#encapsulation d
Router(config-subif)#encapsulation dot1Q 101
Router(config-subif)#ip a
Router(config-subif)#ip ad
Router(config-subif)#ip address 10.0.1.1 255.255.255.240
Router(config-subif)#no sh
Router(config-subif)#no shutdown
```

Обмін пакетами здійснюється відповідно до наведених вище конфігурацій VLAN, але вони повинні мати IP-адреси. Отже, наступним кроком є налаштування протоколу DHCP та сервера DHCP. Спочатку потрібно призначити IP-адресу серверу DHCP. Оскільки широкомовні запити для сервера DHCP не перевищують маршрутизатор на маршрутизаторі, ви повинні вказати адресу сервера, який виконує команду ip helper-address. Вам потрібно

налаштувати діапазони дозволених адрес DHCP на сервері та вказати шлюзи для кожного з них.

Останній крок — увімкнути режим динамічної адреси на пристроях, якщо він не встановлений за замовчуванням, і зачекати, поки всі клієнти отримають свої адреси. На рисунку 3.3 показано, що пристрої мають IP-адреси, а це означає, що протокол DHCP встановлений і працює належним чином.

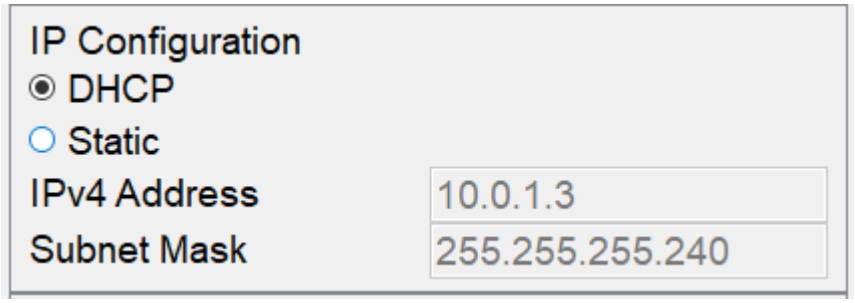

Рисунок 3.3 — Результат роботи протоколу DHCP

Також перевіряємо правильність роботи командою ping. На рисунку 3.4 показаний результат команди ping з комп’ютера. VLAN101 на комп’ютер у локальній мережі VLAN102.

```
C:\>ping 10.0.1.19

Pinging 10.0.1.19 with 32 bytes of data:

Request timed out.
Reply from 10.0.1.19: bytes=32 time<1ms TTL=127
Reply from 10.0.1.19: bytes=32 time=2ms TTL=127
Reply from 10.0.1.19: bytes=32 time=2ms TTL=127

Ping statistics for 10.0.1.19:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

Рисунок 3.4 — Результат команди ping від комп'ютера VLAN101 до комп'ютера в підмережі VLAN102

3.3 Налаштування ACL

Список доступу (ACL) — це набір правил, визначених для управління мережевим трафіком і зниження мережевих атак. ACL використовуються для фільтрації трафіку на основі набору правил, визначених для вхідного або вихідного типу з мережі.

Особливості ACL:

— набір певних правил зіставляється послідовно, тобто зіставлення починається з першого рядка, потім 2-й, потім 3-й і так далі;

— пакети зіставляються тільки до тих пір, поки не будуть відповідати правилу, після того, як правило знайдено, подальше порівняння не виконується, і це правило буде виконано.

— в кінці кожного ACL є неявна відмова, тобто якщо ні одна умова або правило не збігаються, пакет буде відкинутий.

— після того, як список доступу створений, його слід застосувати до вхідного або вихідного інтерфейсу:

— вхідні ACL — коли список доступу застосовується до вхідних пакетів на інтерфейсі, пакети спочатку обробляються відповідно до списку доступу, а потім перенаправляються на вихідний інтерфейс.

— вихідні ACL — коли список доступу застосовується до вихідних пакетів на інтерфейсі, пакет спочатку маршрутизируется, а потім обробляється на вихідному інтерфейсі.

Є два основних типи списків доступу, а саме:

— стандартний список доступу, список доступу який створюється лише за допомогою оригінальної IP-адреси, такі списки ACL дозволяють або забороняють використання всього набору протоколів, також вони не розрізняють IP-трафік, такий як TCP, UDP, Https і т.д., використовуючи номера 1-99 або 1300-1999, маршрутизатор розпізнає його як стандартний ACL і вказану адресу як вихідну IP-адресу;

— розширений список доступу, список ACL в якому використовуються як вихідна, так і цільова IP-адреса, у цьому типі ACL ми також можемо вказати, який IP-трафік повинен бути дозволений або заборонений, він використовує діапазони 100-199 і 2000-2699.

Переваги ACL:

— підвищення продуктивності мережі;

— забезпечте безпеку, оскільки адміністратор може налаштувати список входу за потребою та запобігти потраплянню небажаних пакетів у мережу;

— забезпечте контроль трафіку, оскільки він може дозволяти або забороняти залежно від потреб мережі.

Для того щоб розділити відділи, які не зв’язані на пряму з виробничим процесом від повністю задіяних у робочому процесі, використаємо стандартні ACL. Створюються ACL за допомогою стандартної команди списку доступу IP та імені ACL. Для цього необхідно створити два ACL, перший з яких обмежує потік трафіку до лабораторій, відділів контролю та безпеки в інших областях. Другий ACL, з іншого боку, забороняє доступ до лабораторій, адміністрування та безпеки. Щоб відхилити сегмент мережі в ACL, ви повинні ввести команду відмови і пам’ятати, що ACL забороняє все, що заборонено. Щоб уникнути проблем, ви не повинні приймати весь інший трафік з будь-якими командами дозволу. Після створення ACL його необхідно застосувати до інтерфейсу маршрутизатора і вказати напрямок фільтрації трафіку. Повна конфігурація ACL показана в лістингу 3.6.

Лістинг 3.6 — Повна конфігурація ACL

```
Router(config)#ip access-list standard DIVIDE
Router(config-std-nacl)#deny 10.0.1.32 0.0.0.15
Router(config-std-nacl)#deny 10.0.1.64 0.0.0.15
Router(config-std-nacl)#deny 10.0.1.80 0.0.0.15
Router(config-std-nacl)# permit any
```

```
Router(config)#interface fastEthernet 0/0.1
Router(config-subif)#ip access-group DIVIDE out
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#ip access-group DIVIDE out
Router(config)#interface fastEthernet 0/0.4
Router(config-subif)#ip access-group DIVIDE out
Router(config)#interface fastEthernet 3/0.9
Router(config-subif)#ip access-group DIVIDE out
Router(config)#interface fastEthernet 4/0.9
Router(config-subif)#ip access-group DIVIDE out
Router(config)#interface fastEthernet 2/0.8
Router(config-subif)#ip access-group DIVIDE out
Router(config)#interface fastEthernet 5/0.8
Router(config-subif)#ip access-group DIVIDE out
Router(config)#interface fastEthernet 6/0.8
Router(config-subif)#ip access-group DIVIDE out
Router(config)#ip access-list standard DIRLAB
Router(config-std-nacl)#deny 10.0.1.0 0.0.0.15
Router(config-std-nacl)#deny 10.0.1.16 0.0.0.15
Router(config-std-nacl)#deny 10.0.1.48 0.0.0.15
Router(config-std-nacl)#deny 10.0.2.0 0.0.0.255
Router(config-std-nacl)#deny 10.0.3.0 0.0.0.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#interface fastEthernet 0/0.3
Router(config-subif)#ip access-group DIRLAB out
Router(config-subif)#exit
```

3.4 Налаштування NAT

Для доступу до Інтернету вам потрібна публічна IP-адреса, але ми можемо використовувати приватні IP-адреси в корпоративній мережі. Ідея NAT полягає в тому, щоб дозволити кільком пристроям отримати доступ до Інтернету через одну публічну адресу. Для цього вам потрібно перенести приватну IP-адресу на публічну IP-адресу. Трансляція мережевих адрес (NAT) — це процес перетворення однієї або кількох локальних IP-адрес в одну або кілька глобальних IP-адрес і навпаки, щоб дозволити локальним хостам отримати доступ до Інтернету. Він також перекладає номери портів, тобто приховує номер порту хоста з іншим номером порту в пакеті, надісланому до місця призначення. Потім він створює відповідні записи для IP-адреси та номера порту в таблиці NAT. NAT зазвичай працює на маршрутизаторі або брандмауері.

NAT налаштовується на граничному маршрутизаторі, тобто маршрутизатор має локальний (внутрішній) мережевий інтерфейс та глобальний (зовнішній) мережевий інтерфейс. Коли пакет проходить через локальну мережу, NAT перетворює цю локальну (приватну) IP-адресу в глобальну (загальнодоступну) IP-адресу. Коли пакет потрапляє в локальну мережу, глобальна (загальнодоступна) IP-адреса перетворюється на локальну (приватну) IP-адресу. Коли адреси NAT вичерпані, тобто коли в налаштованому пулі немає іншої адреси, пакети не приймаються, а пакет недоступності хоста ICMP надсилається до призначення. Коли NAT виконує лише трансляцію IP-адрес, IP-адреси пакетів, які надходять до NAT, маскуються загальнодоступною IP-адресою мережі та надсилаються до місця призначення. Місце призначення надсилає відповіді на загальнодоступну IP-адресу маршрутизатора. Тому при отриманні відповіді для NAT невідомо, яка відповідь якому хосту належить. Тому, щоб уникнути цієї проблеми, NAT маскує вихідний номер порту і записує його в таблицю NAT.

Внутрішні та зовнішні адреси NAT — щоб чітко зрозуміти NAT, необхідно розрізняти типи адрес, задіяних у технології:

— внутрішня локальна IP-адреса, призначена хосту в локальній мережі не є IP-адресою призначеною вашим провайдером, вона внутрішній хост видимий з підмережі;

— внутрішня глобальна адреса, IP-адреса яка зовні представляє одну або кілька внутрішніх локальних IP-адрес, вона є внутрішнім хостом, видимим із зовнішньої мережі;

— зовнішня локальна адреса, фактична IP-адреса хоста в локальній мережі після перетворення;

— зовнішня глобальна адреса, зовнішній хост видимий із зовнішньої мережі, вона є IP-адресою зовнішнього хоста до перетворення.

NAT ділиться на кілька типів, але в цій мережі нам знадобляться лише два:

— статичний NAT дозволяє порівняння незареєстрованої (приватної) IP-адреси з офіційно зареєстрованою (публічною) IP-адресою, тобто порівняння окремого значення між локальною та глобальною адресою;

— PAT також відомий як overload NAT, процес за допомогою якого кілька локальних (приватних) IP-адрес можуть бути перетворені в одну зареєстровану IP-адресу, для розрізнення трафіку використовуються номери портів, такий тип NAT є найпоширенішим, оскільки дозволяє тисячам користувачів підключатися до інтернету за допомогою єдиної справжньої глобальної IP-адреси.

Переваги NAT:

— NAT зберігає офіційно зареєстровані IP-адреси;

— це забезпечує конфіденційність, приховуючи IP-адресу пристрою, який надсилає та отримує трафік;

— видаляє нумерацію адрес під час розробки мережі.

Недоліки NAT

— трансляція затримує перехід;

— деякі програми не працюють, коли NAT увімкнено;

— ускладнює протоколи тунелювання, такі як ipsec;

— крім того, маршрутизатор, який є пристроєм мережевого рівня, не повинен перешкоджати номерам портів.

Для покращення реалізації безпечного зв’язку корпоративної мережі із зовнішньою мережою необхідно налаштувати NAT. Першим кроком має бути призначення IP-адрес. Зовнішньою IP-адресою корпоративної мережі буде адреса 213.234.10.2 із префіксом 30, яка видана за умовою провайдером. Далі на маршрутизаторі необхідно налаштувати дефолт маршрут у якості наступного хопа слід вказати адресу інтерфейсу маршрутизатора провайдера. Після цього необхідно зайти на інтерфейси та вказати їм тип для NAT. Є два типи внутрішні (inside) та зовнішні (outside). Наступним кроком необхідно створити стандартний access-list, що дозволить адреси, які повинні бути переведені. Використовується команда access-list [номер_ACL] permit source [wildcard_маска]. PAT вмикається, використовуючи допис Overload. Вводимо команду ip nat inside source list [номер_ACL] interface[назва_інтерфейсу] overload. Команди, що прописані на маршрутизаторі наведені у лістингу 3.7.

Лістинг 3.7 — Команди конфігурування маршрутизатора

```
Router(config)#interface FastEthernet9/0
Router(config-if)#ip address 213.234.10.2 255.255.255.252
Router(config)#ip route 0.0.0.0 0.0.0.0 213.234.10.1
Router(config)#ip access-list standart FOR-NAT
Router(config-std-nacl)#permit 10.0.0.0 0.0.255.255
Router(config)#ip nat inside source list FOR-NAT interface fastEthernet 7/0 overload
```

Щоб перевірити правильність налаштування з комп'ютера корпоративної мережі виконаємо ping і вкажемо IP-адресу умовного серверу провайдера. Результат команди ping на рисунку 3.5.

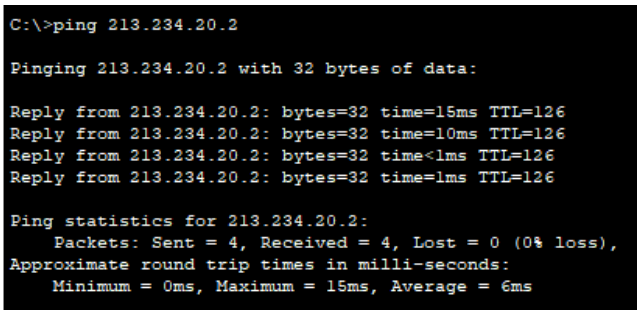

Рисунок 3.5 — Результат команди ping

Статичний NAT використаємо для того щоб надати доступ до локального сервера із зовнішньої мережі. За допомогою команди ip nat inside source static tcp 10.0.1.98 80 213.234.10.2 80, де 10.0.1.98 — адреса локального сервера, а 80 — tcp порт до якого прив'язана адреса сервера. Перевіримо правильність роботи шляхом вводу зовнішньої IP-адреси мережі у веб-браузері пристрою, що знаходиться у зовнішній мережі. Оскільки з'явилась сторінка входу у аккаунт керування пристроями IOT то усе налаштовано правильно. Результат перевірки зображений на рисунку 3.6.

Рисунок 3.6 — Результат перевірки правильності налаштування статичного NAT.

3.5 Налаштування IOT

У корпоративній мережі є декілька типів пристроїв Інтернету речей:

— система контролю температури;

— сканери штрих-кодів;

— вагопроцесори.

У середовищі packet tracer вагопроцесори та їхні аналоги відстутні, замість сканерів штрих-кодів будуть використовутись RFID Reader,тому що сканери штрих-кодів у середовищі також відстутні.

Системи контролю температури можна підключити до мережі кількома шляхами за допогою безпровідних технологій до домашнього роутера або до сервера. Оскільки,корпоративна мережа містить сласний сервер виконаємо підключення до нього. Для цього потрібно створити новий сегмент мережі та віднести його до нового VLAN. Конфігурацію IP-адреси та шлюзу отримаємо за допомогою DHCP. Наступним кроком на сервері потрібно створити середовище керування пристроями IOT. На пристрої необхідно обрати серверний тип підключення ввести адресу серверу та пароль і логін від аккаунту. Якщо все налаштовано вірно, то пристрій почне показувати значення температури повітря і керувати пристроєм або моніторити його показники можна буде через браузер будь-якого пристрою у мережі. Для перевірки зайдемо у веб-браузер та ввійдемо у аккаунт керування пристроями IOT. На рисунку 3.7. показано роботу системи контролю температури.

Рисунок 3.7 — Демонстрація роботи системи контролю температури.

На рисунку 3.8. показано можливість керування системою контролю температури на сервері.

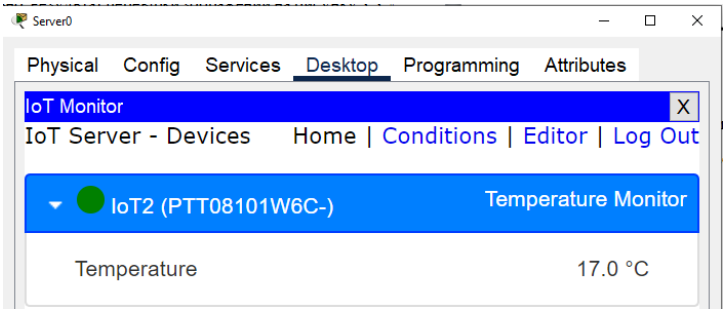

Рисунок 3.8 — Демонстрація можливості керування системою контролю температури на сервері.

RFID Reader можна підключити до мережі кількома шляхами за допогою безпровідних технологій до домашнього роутера або до сервера. Оскільки,корпоративна мережа містить сласний сервер виконаємо підключення до нього. . Якщо все налаштовано вірно, то пристрій з’явиться у наборі для керування пристроями IOT на сервері. Але для коректної роботи потрібно налаштувати роботу станів правильності Card-ID на пристроях, реалізувати це можна на сервері у вкладці conditions. Вкладка conditions зображена на рисунку 3.9.

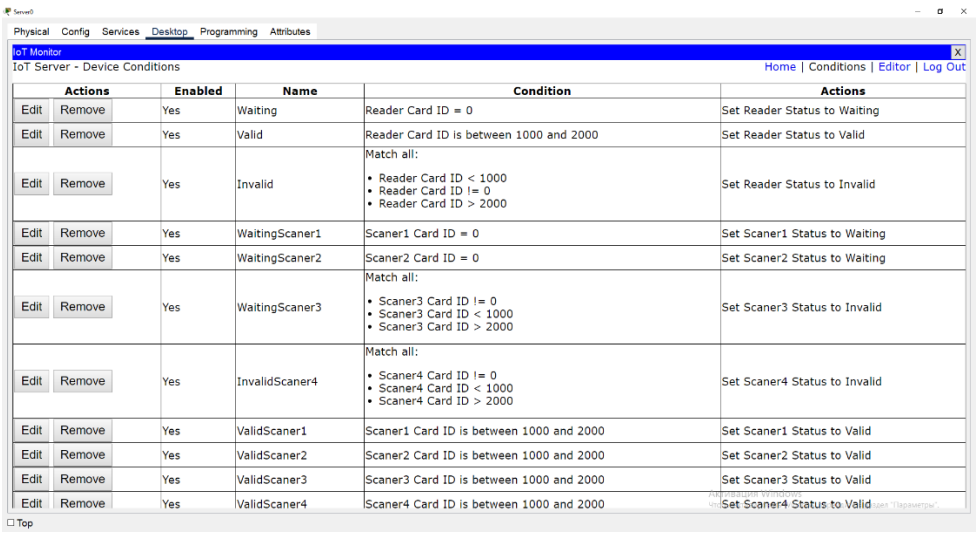

Рисунок 3.9 — Вкладка conditions на сервері.

ID карта представляє собою звичайне число, тому слід вказати діапазони чисел ID при скануванні яких пристрій буде давати позитивний сигнал. За умовою це числа від 1000 до 2000. Конфігурація діапазону зображена на рисунку 3.10.

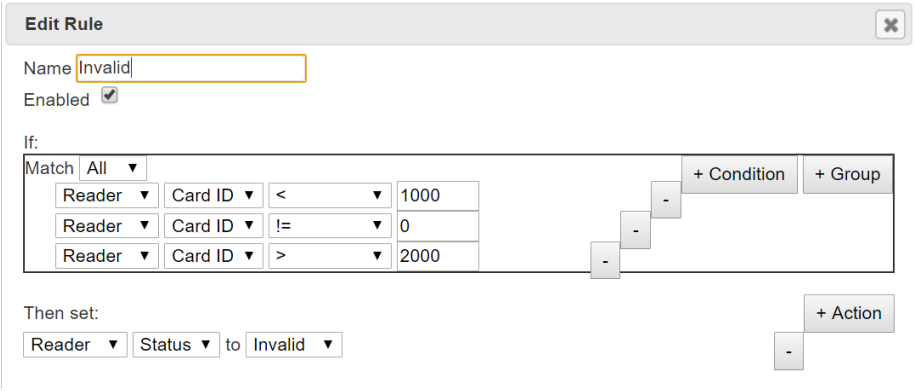

Рисунок 3.10 — Конфігурація діапазону допустимих Card-ID.

Після налаштування діапазону можна перевірити працездатність пристрою за допомогою карт. Працездатність RFID Reader Зображено на рисунку 3.11.

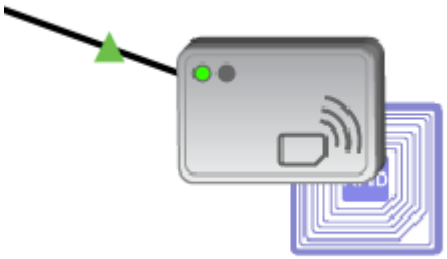

Рисунок 3.11 — Працездатність RFID Reader.

3.6 Налаштування VPN

Останнім часом стає все поширенішою тенденція працівників, що працюють віддалено. Для таких випадків необхідно подумати про додаткову

безпеку віддалених підключень у локальну мережу із зовнішньої мережі. Це можливо реалізувати за допомогою технології IPsec, яка здійснює шифрування трафіку, створює віртуальний тунель між користувачами та містить протоколи для захищеного обміну ключами. Налаштування IPsec ділиться надва етапи. Перший це узгодження політики ISAKMP, а другий це налаштування самого IPsec. Для налаштування політики ISAKMP необхідно у режим налаштування цієї політики за допомогою команди crypto isakmp policy 110. У цьому режимі слід налаштувати метод шифрування, алгоритм для хешування, ключ для перевірки достовірності , групу Діффі-Геллмана та час життя ключа під час сеансу. Варто відзначити, що політика ISAKMP визначається глобально. Це означає, що якщо у нас є п'ять різних віддалених майданчиків і налаштовано п'ять різних політик ISAKMP 1 (по одній для кожного віддаленого маршрутизатора), то, коли наш маршрутизатор намагається узгодити VPN-тунель з кожної майданчиком, він відправить всі п'ять політик і буде використовувати перший збіг, який прийнято обома сторонами.

Наступним кроком необхідно визначити Pre-Shared ключ для аутентифікації з нашим партнером за допомогою наступної команди crypto isakmp key [key] address [address]. Повний список команд для конфігурації ISAKMP політики наведено у лістингу 3.8.

Лістинг 3.8 — Повний список команд для конфігурації ISAKMP політики.

```
R(config)#  crypto isakmp policy 110
R(config-isakmp)# encr 3des
R(config-isakmp)# hash md5
R(config-isakmp)# authentication pre-share
R(config-isakmp)# group 2
R(config-isakmp)# lifetime 86400
R(config)# crypto isakmp key cisco address 192.168.1.1
```

Наступним етапом є налаштування IPsec. Цей процес ділиться на 4 частини:

— створення розширеного ACL;

— створення IPSec Transform;

— створення криптографічної карти (Crypto Map);

— примінити криптографічну карту на інтерфейсі.

ACL потрібен для того щоб вказати, який трафік потрібно пропускати через VPN-тунель. Після ACL необхідно налаштувати набір для шифрування трафіку. Останнім кроком конфігурації є створення криптографічної карти, саме цей етап об’днує налаштування ISAKMP та IPSec. Залишається тільки присвоїти карту потрібному інтерфейсу. Повний список команд для конфігурації IPsec політики наведено у лістингу 3.9.

Лістинг 3.9 — Повний список команд для конфігурації ISAKMP політики.

```
R(config)# ip access-list extended VPN-TRAFFIC
R(config-ext-nacl)# permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
R(config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac
R(config)# crypto map CMAP 10 ipsec-isakmp
R(config-crypto-map)# set peer 192.168.1.1
R(config-crypto-map)# set transform-set TS
R(config-crypto-map)# match address VPN-TRAFFIC
R(config)# interface gigabitEthernet0/1
R(config- if)# crypto map CMAP
```

ВИСНОВКИ

Проаналізовано сучасний стан технологій спеціалізованих комп'ютерних мереж. Розглянуто основні принципи та технології для побудови комп'ютерних мереж. У результаті було доведено, що впровадження пристроїв Інтеренету речей у виробництво збільшує продуктивність та налагодженість роботи.

Розроблено логічну структуру комп'ютерної мережі підприємства ТОВ «Шамраївський цукровий завод». Реалізовано сучасні рішення по покращенню роботи мережі та функціонування мережевих пристроїв

Обгрунтовано вибір мережевого обладнання та пристроїв IOT різних виробників. Критеріями огляду були технічні характеристики, стійкість до зовнішніх подразників та ціна. Після огляду було обрано моделі, що задовольняють потреби мережі та обраховано загальну суму на мережеве обладнання.

Провесдено конфігурування активних пристроїв. Здійснено огляд території підприємства на основі отриманої інформації, був здійснений розподіл підприємства на робочі підрозділи. Розглянуто стан робочого процесу підприємства та на основі цих потреб обрано набір протоколів, які необхідно інтегрувати в мережу.

У середовищі Cisco Packet Tracer створено логічну топологію мережі підприємства, інтегровано мережеві технології, а саме VLAN, NAT, DHCP, ACL, telnet, SSH та IOT. Результатом стала повністю розроблена модель мережі підприємства із можливістю віддаленого доступу та керування пристроями IOT, такими як система контролю температури та вологості, RFID-зчитувачі. Також можливість віддаленого безпечного під'єднання із зовнішньої мережі у корпоративну, через VPN-тунель.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Комп’ютерні мережі [Електронний ресурс] — режим доступу до ресурсу: http://www.kievoit.ippo.kubg.edu.ua/kievoit/2013/21/21.html

2. Модель OSI [Електронний ресурс] — режим доступу до ресурсу: http://petroonline.ho.ua/OSI.html

3. TCP/IP [Електронний ресурс] — режим доступу до ресурсу: https://uk.wikipedia.org/wiki/TCP/IP

4. IP-адреса [Електронний ресурс] — режим доступу до ресурсу: https://support.google.com/google-ads/answer/6322?hl=uk

5. У чому відмінність "білої" і "сірої" IP-адреси? [Електронний ресурс] — режим доступу до ресурсу: https://dynamic-design.com.ua/novosti/uk/vnesnij-u-comu-vidminnist-quotbilogoquot-i-quotsirogoquot-ip-adresi/

6. Що таке MAC-адреса? [Електронний ресурс] — режим доступу до ресурсу: https://2ip.ua/ua/blog/mac-address

7. Технологія ethernet [Електронний ресурс] — режим доступу до ресурсу: http://elartu.tntu.edu.ua/bitstream/123456789/9483/2/Conf_2011v1_Hliva_M-Tekhnolohiia_Ethernet_93.pdf

8. Технологія Wi-Fi [Електронний ресурс] — режим доступу до ресурсу: http://www.npblog.com.ua/index.php/hi-tech/tehnologija-wi-fi.html

9. NAT — це що таке ? Налаштування NAT[Електронний ресурс] — режим доступу до ресурсу: https://uk.carolchannings.net/kompyutery/58853-nat-eto-chto-takoe-nastroyka-nat.html

10. Промисловий Інтернет Речей [Електронний ресурс] — режим доступу до ресурсу: https://www.it.ua/knowledge-base/technology-innovation/promyshlennyj-internet-veschej

11. Інтернет речей (Internet of Things, IoT) [Електронний ресурс] — режим доступу до ресурсу: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot

12. Сайт «Valtek»: Системи контролю та управління доступом [Електронний ресурс] — режим доступу до ресурсу: https://valtek.com.ua/ua/system-integration/security-control-system/access-control/access-control-review

13. Сайт «HI-NEWS»: Видисканерів штрих кодів .[Електронний ресурс] режим доступу до ресурсу: https://hi-news.pp.ua/kompyuteri/52-yak-pdklyuchiti-skaner-shtrih-kodu-dlya-kompyutera-vidi-skanerv-shtrih-kodv-programi-dlya-shtrih-kodv.html.

14. DHCP [Електронний ресурс] — режим доступу до ресурсу: https://uk.wikipedia.org/wiki/DHCP

15. Computer Networks (5th Edition): Andrew S. Tanenbaum, David J. Wetherall, 2010, 960 p.

16. Яке обладнання потрібне для створення локальної мережі [Електроний ресурс] — режим доступу до ресурсу: https://polarize.ru/uk/video/setevoe-oborudovanie-predpriyatiya-kakoe-oborudovanie-neobhodimo/

17. Мережеві технолігії [Електроний ресурс] — режим доступу до ресурсу: https://www.ourboox.com/books/мережеві-технології/

18. Класифікація компютерних мереж [Електроний ресурс] — режим доступу до ресурсу: https://mozok.click/736-klasifkacya-kompyuternih-merezh.html\

19. Computer networks (6th Edition): I. Ross, Keith W. 2012, 875 p.

ДОДАТОК А

Технічне завдання

Міністерство освіти і науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп’ютерної інженерії

Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ

проф., д.т.н.. Азаров О.Д..

"____" _____2022 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання бакалаврської дипломної роботи

“ Комп'ютерна мережа Шамраївського цукрового заводу ”

08-23.БДР.024.00.000 ТЗ

Науковий керівник: професор к.т.н.

_____ Захарченко С.М.

Студент групи 2КІ-18б

_____ Котельніков А.П.

м. Вінниця — 2022

1 Підстава для використання бакалаврської кваліфікаційної роботи (БДР)

1.1 Актуальність розробки полягає у необхідності вирішення проблеми пошуку вільних місць на парковках, шляхом розробки веб-додатку, головною ціллю якого є використовування автоматизованої паркувальної системи, що у свою чергу спрощує пошук та дозволяє бронювати вільні місця.

1.2 Наказ про затвердження теми бакалаврської дипломної роботи.

2 Мета і призначення БДР

2.1 Мета проекту — розробка зручного у використанні веб-додатку інформаційного обслуговування автопаркінгу призначеного для загального користування.

2.2 Призначення розробки — виконання бакалаврського дипломного проекту із подальшим впровадженням та розвитком продукту.

3 Вихідні дані для виконання БДР

3.1 Проведення аналізу сучасних підходів до побудови інформаційних систем паркінгу.

3.2 Розгляд принципів роботи автоматизованих паркувальних систем.

3.2 Розробка інтерфейсу та функціоналу веб-додатку.

4 Вимоги до виконання БДР

Головна вимога — розробити зручний інтерфейс до веб-додатку, використовуючи усі здобуті навчики та знання.

5 Етапи БДР та очікувані результати

Етапи роботи та очікувані результати приведено в таблиці А.1.

6 Матеріали, що подаються до захисту БДР

До захисту подаються: пояснювальна записка БДР, ілюстративні матеріали, протокол попереднього захисту БДР на кафедрі, відгук наукового керівника, анотації до БДР українською та іноземною мовами, довідка про відповідність оформлення БДР діючим вимогам.

Таблиця А.1 — Етапи БДР

№ з/п	Назва етапів виконання комплексної бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Постановка задачі роботи	07.03.22	Аналітичний огляд літературних джерел, розділ 1
2	Аналіз предметної області	08.03-19.03.22	розділ 1
3	Аналіз сучасних підходів до побудови мереж на основі інтернет речей	21.03-30.03.22	розділ 1
4	Аналіз поняття компютерні мережі	04.04-21.04.22	розділ 2
5	Аналіз принципів роботи компютерних мереж	22.04-24.04.22	розділ 2
6	Проектування компютерної мережі	25.04-06.05.22	розділ 3
7	Розробка компютерної мережі	09.05-13.05.22	розділ 3
8	Розробка функціоналу компютерної мережі	15.05-21.05.22	розділ 3
9	Підготовка матеріалів та опис розробки інформаційної системи	22.05-25.05.22	Тези доповідей
10	Аналіз виконання роботи, висновки, додатки	26.05-31.05.22	Пояснювальна записка
11	Перевірка якості виконання бакалаврського проекту та усунення недоліків	02.06 -10.06.22	Пояснювальна записка, графічний матеріал і презентація

7 Порядок контролю виконання та захисту БДР

Виконання етапів графічної та розрахункової документації БДР контролюється науковим керівником згідно зі встановленими термінами.

Захист БДР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора.

8 Вимоги до оформлювання та порядок виконання БДР

При оформлюванні БДР використовуються:

— ДСТУ 3008 : 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302 : 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— ГОСТ 2.104-2006 «Єдина система конструкторської документації. Основні написи»;

— документами на які посилаються у вище вказаних.

ДОДАТОК Б

Налаштування роутера CNT-RT

```
CNT-RT#sh run
Building configuration...
Current configuration : 1317 bytes
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname CNT-RT

no ip cef
no ipv6 cef

interface FastEthernet0/0
 ip address 192.168.20.206 255.255.255.240
 duplex auto
 speed auto

interface FastEthernet1/0
 ip address 192.168.20.190 255.255.255.240
 duplex auto
 speed auto

interface FastEthernet2/0
 ip address 192.168.20.126 255.255.255.240
 duplex auto
```

```
 speed auto
interface FastEthernet3/0
 ip address 192.168.20.142 255.255.255.240
 duplex auto
 speed auto

interface FastEthernet4/0
 ip address 192.168.20.158 255.255.255.240
 duplex auto
 speed auto

interface FastEthernet5/0
 ip address 192.168.20.174 255.255.255.240
 duplex auto
 speed auto

interface FastEthernet6/0
 ip address 192.168.20.210 255.255.255.252

router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 192.168.20.208 0.0.0.3 area 0
 network 192.168.20.192 0.0.0.15 area 0
 network 192.168.20.176 0.0.0.15 area 0
 network 192.168.20.160 0.0.0.15 area 0
 network 192.168.20.144 0.0.0.15 area 0
 network 192.168.20.128 0.0.0.15 area 0
 network 192.168.20.112 0.0.0.15 area 0
```

```
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
 login
end
```

ДОДАТОК В

Налаштування комутатора GAS-SW

```
GAS-SW#sh run
Building configuration...

Current configuration : 584 bytes

version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname GAS-SW
spanning-tree mode pvst
spanning-tree extend system-id

interface FastEthernet0/1
switchport access vlan 10
switchport mode access

interface FastEthernet1/1
switchport mode trunk

interface FastEthernet2/1
switchport access vlan 20

interface Vlan1
no ip address
```

```
shutdown

interface Vlan10
no ip address

interface Vlan20
no ip address

line con 0

line vty 0 4
login
line vty 5 15
login
end
```

ДОДАТОК Г

Інформація про мережі компютера CEO-PC1

C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:

Link-local IPv6 Address.....: FE80::290:2BFF:FE43:9498

IPv6 Address.....: ::

IPv4 Address.....: 192.168.20.113

Subnet Mask.....: 255.255.255.240

Default Gateway.....: :: 192.168.20.126

Bluetooth Connection:

Connection-specific DNS Suffix..:

Link-local IPv6 Address.....: ::

IPv6 Address.....: ::

IPv4 Address.....: 0.0.0.0

Subnet Mask.....: 0.0.0.0

Default Gateway.....: :: 0.0.0.0

ДОДАТОК Д

Інформація про приєднану мережу сервера SRV

C:\>

ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:

Link-local IPv6 Address.....: FE80::260:3EFF:FEE1:C95C

IPv6 Address.....: ::

IPv4 Address.....: 192.168.20.229

Subnet Mask.....: 255.255.255.252

Default Gateway.....: ::192.168.20.230

FastEthernet1 Connection:

Connection-specific DNS Suffix..:

Link-local IPv6 Address.....: FE80::230:A3FF:FED9:E828

IPv6 Address.....: ::

IPv4 Address.....: 0.0.0.0

Subnet Mask.....: 0.0.0.0

Default Gateway.....: ::0.0.0.0

ДОДАТОК Е

Логічна схема підприємства

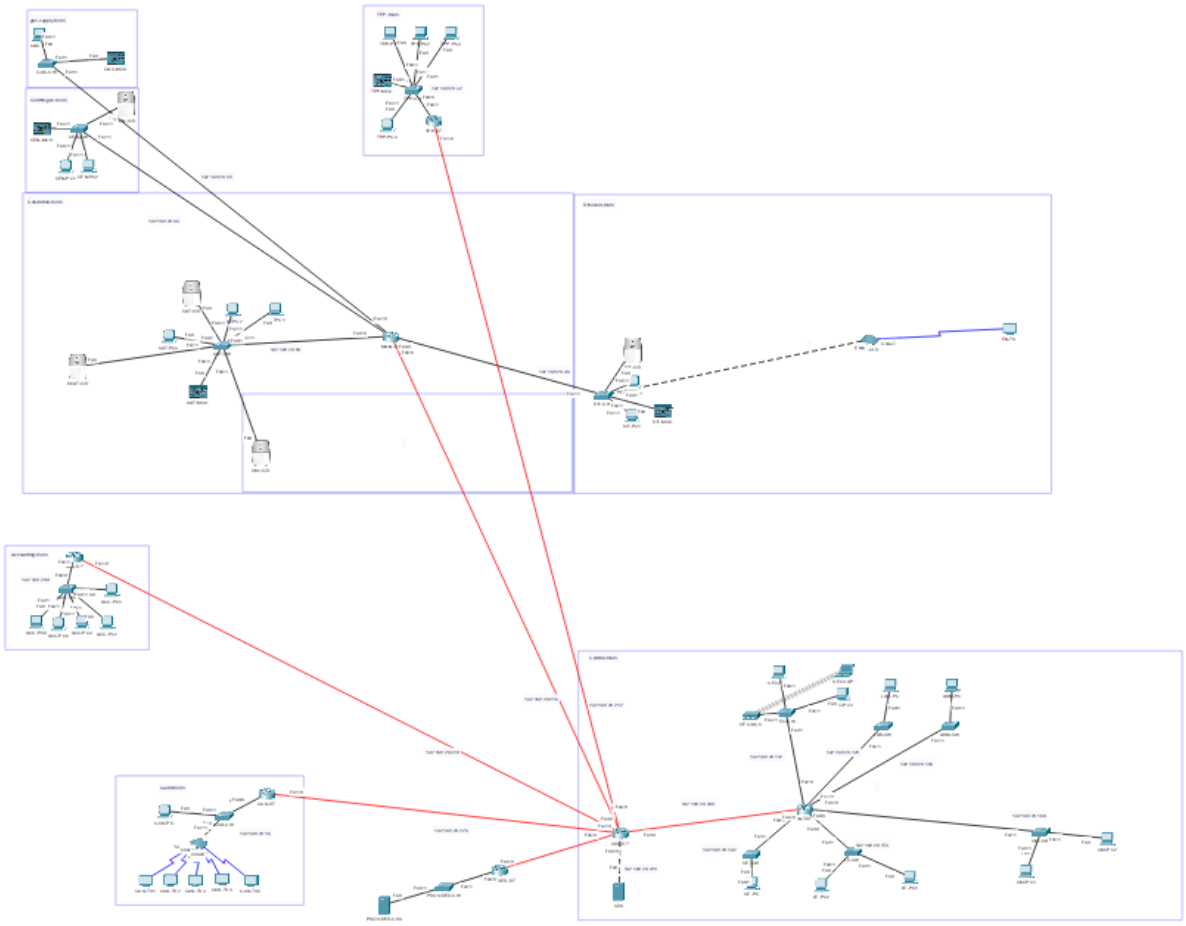

Рисунок Е.1 — Логічна схема підприємства

ДОДАТОК Ж

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Комп'ютерна мережа Шамраївського цукрового заводу

Тип роботи: бакалаврська дипломна робота
(БДР, МКР)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет)

Показники звіту подібності
Unicheck

Оригінальність 95,9% Схожість 4,1%

Аналіз звіту подібності (відмітити потрібне):

- ✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.
- □ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.
- □ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Захарченко С.М.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Котельніков А.П.

Керівник роботи _____ Захарченко С.М.