Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Яковлєва Ярослава Юрійовича
(ПІБ)
академічної групи 123-20-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему "Комп'ютерна система компанії "Dnipro-M" з детальним опрацюванням побудови та налаштування корпоративної мережі"
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Цвіркун Л.І.			
спеціальної частини	проф. Цвіркун Л.І.			
розділів:				
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л. В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри

інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В
(підпис) (прізвище, ініціали)

"__" _____ _____

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Яковлєва Я. Ю. **академічної групи** 123-20-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

за освітньо-професійною програмою 123 «Комп'ютерна інженерія»
(офіційна назва)

на тему "Комп'ютерна система компанії "Dnipro-M" з детальним опрацюванням побудови та налаштування корпоративної мережі"

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.06.2024
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	16.06.2024
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	25.06.2024
Розробка компонента системи	Виконується детальна розробка компонента системи	26.06.2024

Завдання видано _____ проф. Цвіркун Л.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі _____

Дата подання до екзаменаційної комісії _____

Прийнято до виконання _____ Яковлєв Я. Ю.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 106 с., 39 рис., 13 табл., 2 дод., 20 джерел.

КОМП’ЮТЕРНА СИСТЕМА, КОМЕРЦІЙНІ ПРОДАЖІ, ІНТЕРНЕТ РЕЧЕЙ, МАРШРУТИЗАТОР, КОМУТАТОР, CISCO, NAT, VPN, DHCP, VLAN

Об’єкт розробки – комп’ютерна система “Dnipro-M” з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета роботи − створення комп’ютерної системи компанії “Dnipro-M”.

Здійснено розробку комп’ютерної системи з можливістю технічної та програмної модернізації, орієнтованої на застосування у комерційному підприємстві компанії "Dnipro-M", у сферу діяльності якої входить дистрибуція будівельних інструментів та обслуговування й консультація клієнтів. Розроблена система дозволяє:

– забезпечити надійне з'єднання та інформаційну звітність між підрозділами компанії;

– підвищити ефективність управління, обліку та аналізу даних;

– забезпечити віддалений доступ до інформаційних ресурсів компанії;

– підвищити рівень безпеки та продуктивність праці у компанії.

Розроблена комп'ютерна мережа виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Робота системи перевірена за допомогою емуляції моделі комп’ютерної мережі із застосуванням програмного середовища Cisco Packet Tracer.

Результати перевірки у вигляді таблиць та рисунків описані і наводяться у пояснювальній записці та додатках.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПК – Персональний комп’ютер.

LAN – Local Area Network.

DHCP – Dynamic Host Configuration Protocol.

VLAN – Virtual Local Area Network.

NAT – Network Address Translation.

VPN – Virtual Private Network.

IoT – Internet of Things.

ВСТУП

У сучасному світі сфера комерційних продажів є максимально залежною від ефективності використання інформаційних технологій, зокрема комп'ютерних мереж. Застосування комп'ютерних систем у цій галузі, що охоплює великих гравців ринку продажів, є критичною необхідністю для забезпечення оперативності, надійності та безпеки бізнес-процесів. Успішне функціонування торгових компаній вимагає безперебійного обміну інформацією між різними підрозділами, швидкого реагування на запити клієнтів, а також ефективного управління логістичними процесами.

Комп'ютерні мережі дозволяють забезпечити централізоване управління організаціями, що значно підвищує продуктивність праці й ефективність роботи підприємства. Вони надають можливість інтегрувати системи управління обліку продажів, CRM-системи для взаємодії з клієнтами, а також системи електронного документообігу. Це, в свою чергу, сприяє підвищенню якості обслуговування клієнтів, скороченню часу обробки замовлень та зниженню операційних витрат.

У галузі комерційних продажів комп'ютерні мережі є основою для розвитку електронної інтернет-дистрибуції, яка з кожним роком набирає все більшу популярність. Використання комп'ютерних мереж дозволяє забезпечити високий рівень захисту даних, що є надзвичайно важливим в умовах зростаючих кіберзагроз.

Таким чином, застосування комп'ютерних систем у сфері комерційних продажів є ключовим фактором успішного ведення бізнесу, що забезпечує підвищення конкурентоспроможності, покращення якості обслуговування клієнтів та оптимізацію внутрішніх процесів підприємства.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп’ютерної системи

У сучасному світі, де будівництво та ремонтна діяльність займають важливе місце в економіці, комерційні компанії, що спеціалізуються на реалізації та обслуговуванні будівельних інструментів, мають ключове значення у цій сфері. Вони забезпечують ринок інструментами і обладнанням, необхідним для будівництва, ремонту та реставрації будівель та споруд.

Ця галузь вимагає від компаній бути конкурентоспроможними та оперативно відповідати на потреби ринку. Компанії-реалізатори будівельного обладнання повинні працювати над розробкою нових технічних рішень та вдосконаленням існуючих продуктів для задоволення потреб споживачів. Вони також повинні забезпечують послуги технічної підтримки та сервісу, щоб гарантувати ефективне використання своїх продуктів клієнтами.

У сучасному світі, де технології відіграють вирішальну роль у бізнес-процесах, комп'ютерні системи стають невід'ємною складовою успішної діяльності будь-якої комерційної компанії. Вони допомагають у керуванні та веденні обліку складів та матеріалів, організації продажів та обслуговуванні клієнтів, управління замовленнями та логістикою, а також для забезпечення комунікації та співпраці між відділами та філіями.

Використання сучасних інформаційних технологій дозволяє підприємствам в цій галузі бути більш ефективними, швидкими та конкурентоспроможними на ринку. Вони можуть вчасно реагувати на зміни в попиті та підтримувати високий рівень обслуговування своїх клієнтів. Таким чином, комп'ютерні системи стають невід'ємною частиною успішної діяльності компаній, що займаються реалізацією та сервісним обслуговуванням будівельних інструментів, і відіграють важливу роль у їхньому розвитку та зростанні.

1.2 Характеристика і структура об’єкта впровадження

Компанія “Dnipro-M” — українська організація, що спеціалізується на різноманітних аспектах будівельного сектору. Зокрема, вона займається дистриб'юцією та наданням сервісних послуг з обслуговування будівельних інструментів. Ця сфера діяльності включає в себе велику кількість процесів, які вимагають ефективного управління та організації.

Впровадження комп'ютерної системи дозволяє автоматизувати багато процесів управління, обліку та аналізу даних. Це включає системи обліку обладнання та інструментів, керування замовленнями, контроль якості продукції та ведення обліку фінансових операцій.

Крім того, для компанії “Dnipro-M” важливо мати доступ до інформаційних ресурсів з будь-якого місця, тому існування мережевих систем та систем віддаленого доступу є ключовим аспектом впровадження комп'ютерних технологій. Це дозволяє працівникам компанії ефективно спілкуватися, обмінюватися інформацією та працювати над спільними завданнями навіть у віддалених місцях.

Спеціалізована служба підтримки компанії “Dnipro-M” надає консультації клієнтам щодо використання та налаштування придбаних продуктів, допомагає у вирішенні технічних питань та надає інформацію про гарантійне обслуговування. Компанія забезпечує сервісні послуги, які включають у себе ремонт та технічне обслуговування будівельних інструментів. Професійна техніка компанії “Dnipro-M” підлягають ретельній перевірці, ремонту та обслуговуванню для забезпечення їхньої надійності та продовження терміну експлуатації.

1.2.1 Організаційна структура підприємства

У компанії “Dnipro-M” реалізований лінійний тип організаційної структури, тобто, це така структура, між елементами якої існують лише одноканальні взаємодії, кожен підлеглий має лише одного лінійного

керівника, який виконує всі адміністративні та інші функції у відповідному підрозділі.

Організація підприємства складається із структурних підрозділів, кожний з яких відповідає за виконання відповідних функцій. Усі відділи підприємства підпорядковуються генеральному директорові. Кожен відділ має свою внутрішню структуру, що складається з керівників, фахівців та адміністративного персоналу, які спільно працюють над досягненням поставлених цілей та завдань.

Генеральному директорові безпосередньо підзвітні директори відповідних відділів: виконавчий, комерційний, фінансовий, IT-відділ та відділ служби підтримки. Генеральний директор, як керівник компанії, відіграє ключову роль у розвитку та успіху підприємства. Він відповідає за загальне керівництво та стратегічне планування діяльності компанії.

Виконавчий відділ відповідає за координацію діяльності всіх відділів компанії та виконання стратегічних завдань, визначених вищим керівництвом.

Комерційний відділ відповідає за управління продажами та маркетингом, а також за логістичні процеси та постачання. Кожен з цих аспектів відділу спеціалізується на певних функціях компанії та забезпечує взаємодію зі своїми клієнтами та партнерами. Для розподілення обов’язків та полегшення управління, відділ було поділено за функціоналом на три окремі підрозділи:

– підрозділ продажів: відповідає за активний пошук нових клієнтів, укладання угод тощо;

– підрозділ маркетингу: займається розробкою та впровадженням маркетингових стратегій та акцій, а також рекламою продукції;

– підрозділ логістики: відповідає за планування та організацію поставок, зберігання і транспортування товарів компанії через фірм-посередників.

Фінансовий відділ відповідає за ведення обліку фінансової діяльності компанії, складання економічних звітностей, управління та планування бюджету.

IT-відділ забезпечує розробку, налагодження та підтримку інформаційних систем та сервісних технологій компанії. Відповідає за безперебійну роботу комп'ютерної інфраструктури, мережі та програмного забезпечення.

Останнім відділом компанії є служба підтримки. Вона забезпечує технічну підтримку клієнтів щодо використання продукції компанії, вирішення їхніх запитів та проблем. Надає консультації щодо використання товарів та послуг.

Ця організаційна структура дозволяє досягти гнучкості та адаптивності компанії “Dnipro-M” до змін на ринку та в умовах конкуренції. Це дозволяє підприємству ефективно виконувати свої функції, забезпечувати високий рівень обслуговування та задовольняти потреби своїх клієнтів.

Схему організаційної структури компанії зображено на рисунку 1.1.

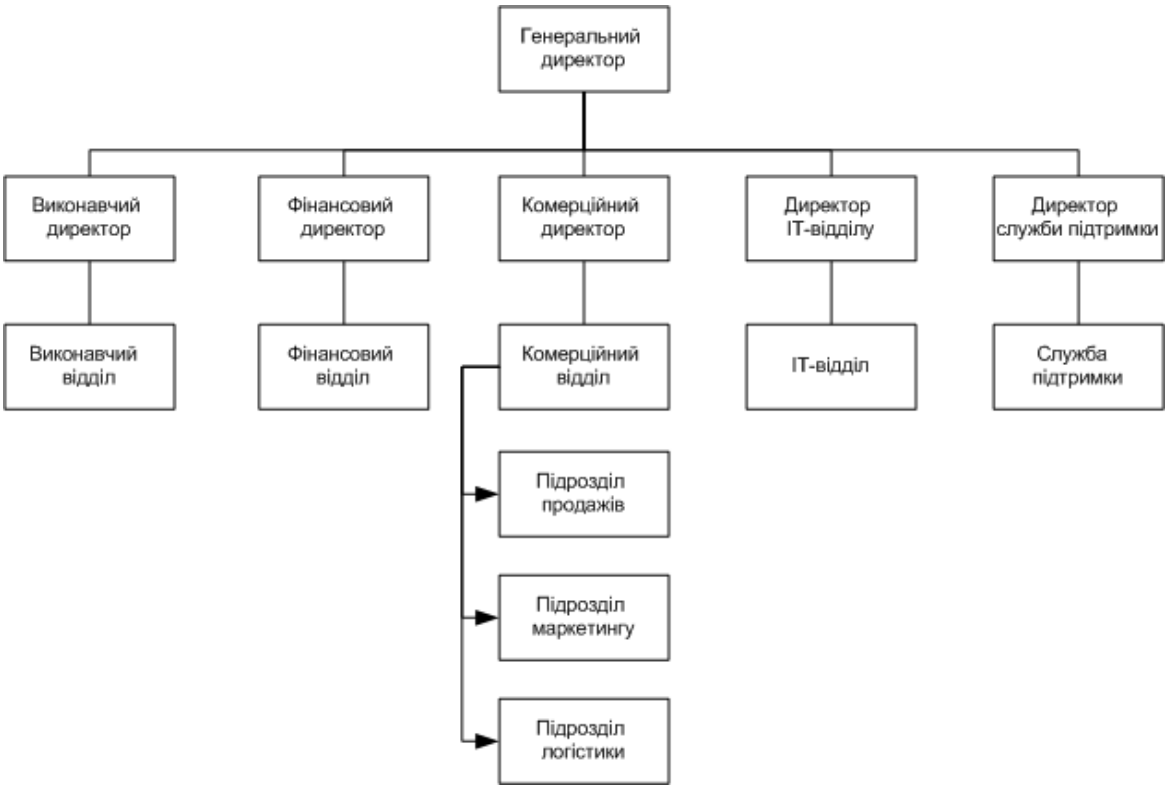

Рисунок 1.1 − Схема організаційної структури підприємства

1.2.2 Розміщення структурних підрозділів підприємства

Топологічно компанія “Dnipro-M” складається з двох геопозицій, що є двома віддаленими один від одного офісами компанії – головний офіс, що вміщує виконавчий, комерційний, IT- та фінансовий відділи, та офіс служби підтримки.

Головний офіс знаходиться на двох поверхах будівлі, що розташована за адресою вулиця Князя Ярослава Мудрого, 40, Дніпро, Дніпропетровська область, 49000.

Офіс служби підтримки знаходиться на першому поверху будівлі за адресою вулиця Салтівська, 3, Дніпро, Дніпропетровська область, 49026.

Відстань між будівлями становить 5000 метрів.

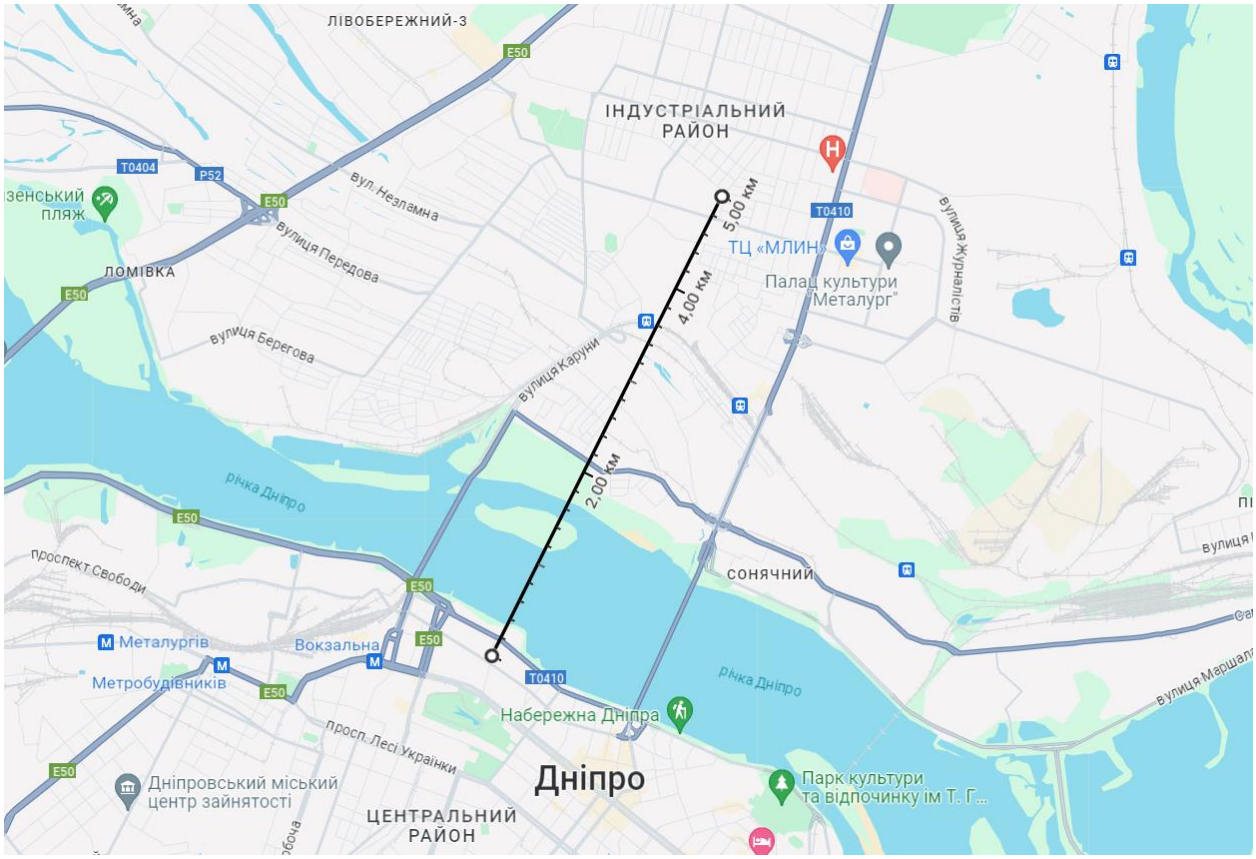

Рисунок 1.2 – Топографічна схема розміщення головного офісу та відділу служби підтримки

Як зазначалося вище головний офіс займає два поверхи багатоповерхової будівлі. На першому поверсі знаходяться фінансовий (Ф) та

виконавчий (В1, В2) відділ, а також ІТ-відділ (ІТ). Виконавчий відділ займає два приміщення, фінансовий та ІТ – по одному. Також під мережеве обладнання та сервери виділено окреме приміщення – серверна кімната, у ній знаходяться всі маршрутизатори, а також комутатори та сервери пов’язані з вищезазначеними відділами, деякі компоненти IoT. Схема першого поверху головного офісу з умовними позначеннями на рисунку нижче.

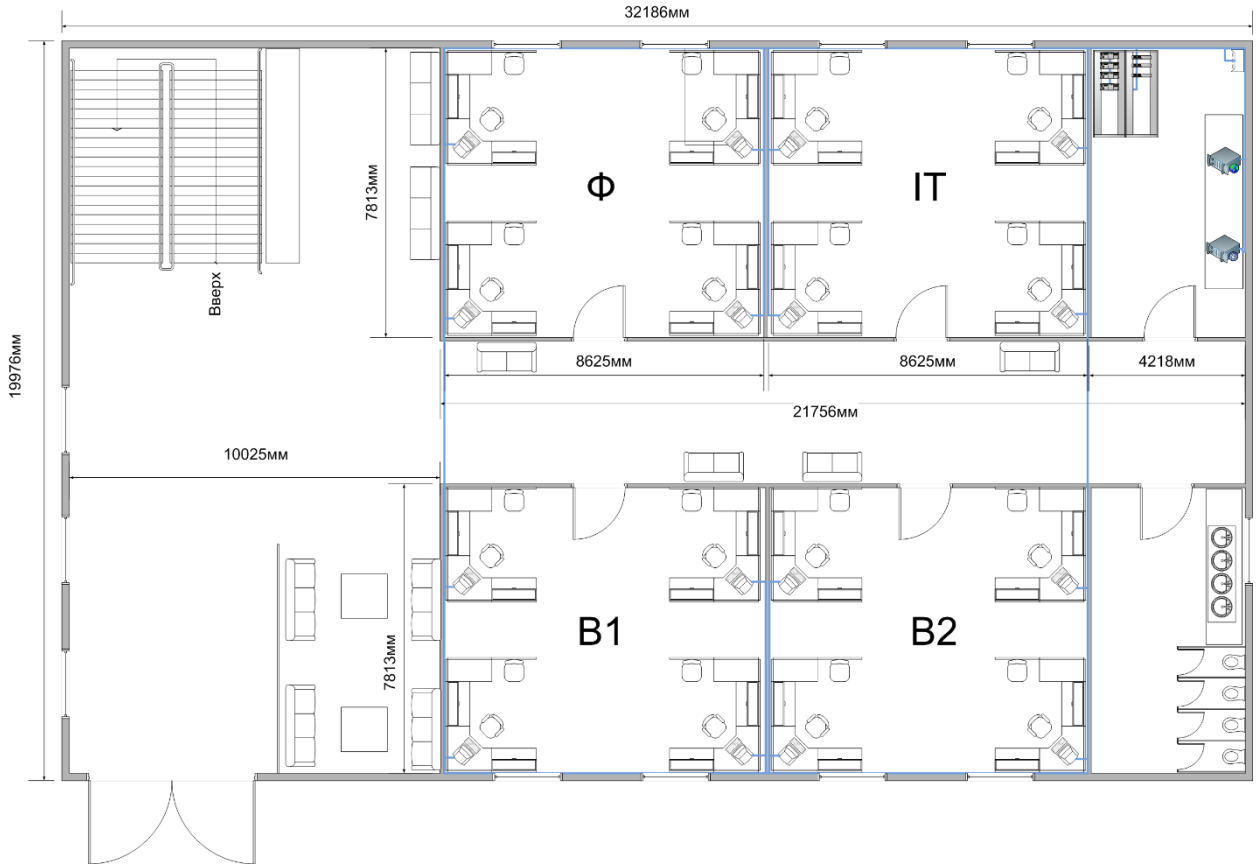

Рисунок 1.3 – Структурна схема розміщення відділів на першому поверсі головного офісу компанії “Dnipro-M”

Другий поверх головного офісу відведений повністю під комерційний відділ. На другому поверсі розміщено кімнату зустрічей і три офісні приміщення. Так як комерційний відділ поділений на три підрозділи, логічно розмістити кожен з них у окремі приміщення. Таким чином офісні приміщення другого поверху поділені між підрозділами продажів (КП), маркетингу (КМ) та логістики (КЛ). Крім того, на другому поверсі також розміщена серверна кімната, у якій знаходяться комутатори комерційного

відділу та відповідний сервер, а також компоненти IoT. Схема другого поверху головного офісу з умовними позначеннями на рисунку нижче.

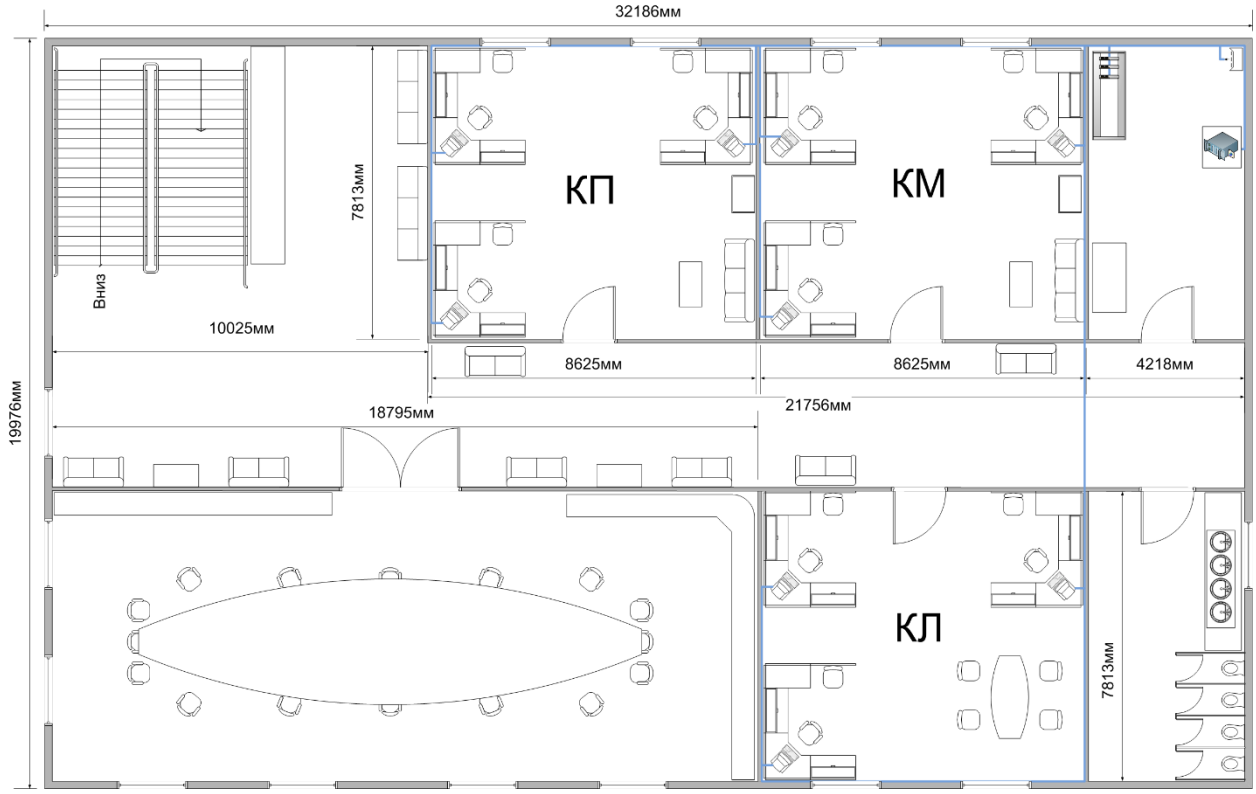

Рисунок 1.4 – Структурна схема розміщення відділів на другому поверсі головного офісу компанії “Dnipro-M”

Віддалений офіс служби підтримки являє собою виділену площу на першому поверсі будівлі. На цій площі знаходяться два офісні приміщення відведені під потреби відповідного відділу компанії “Dnipro-M”. В одному із приміщень, окрім робочих місць персоналу, також знаходиться мережеве обладнання для підтримки мережевої інфраструктури відділу та з’єднання з головним офісом. Схема приміщень офісу служби підтримки представлена на рисунку нижче.

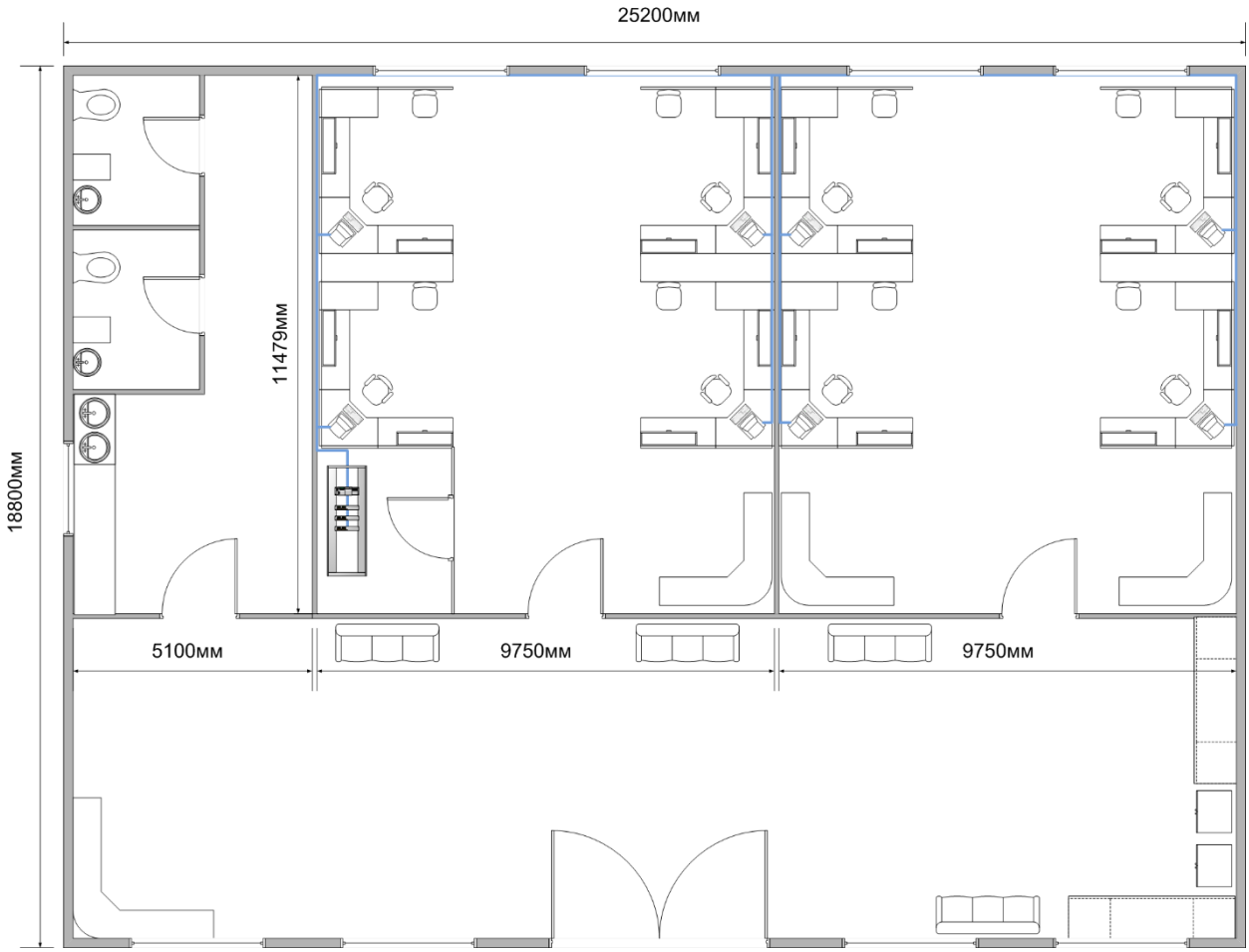

Рисунок 1.5 – Структурна схема офісу відділу служби підтримки компанії “Dnipro-M”

1.3 Стислі відомості про технологію керування (обчислення) для об’єкта впровадження

Технологія керування комп'ютерною мережею в компанії “Dnipro-M” включає в себе ряд стратегій, методів та інструментів, спрямованих на забезпечення ефективного функціонування, безпеки та надійності мережевої інфраструктури. Основні принципи керування в мережі “Dnipro-M” орієнтовані на оптимізацію ресурсів, забезпечення високої продуктивності та забезпечення відповідності стандартам безпеки та конфіденційності даних.

На мережевому та канальному рівнях використовуються різноманітні протоколи маршрутизації та комутації даних, такі як EIGRP, VLANs, Ethernet та інші, які дозволяють ефективно керувати трафіком та забезпечувати

балансування навантаження. Керування мережевими пристроями, такими як комутатори та маршрутизатори, здійснюється за допомогою системи ліній віртуальних терміналів, що надають захищений доступ до інструментів моніторингу, налаштування та діагностики пристроїв.

Важливою складовою технології керування є забезпечення безпеки мережі. Для цього використовуються засоби автентифікації та авторизації, налаштування мережевих екранів та списків контролю доступу, захищені шифровані з'єднання та інші заходи захисту. Регулярний аудит безпеки та оновлення програмного забезпечення також входять в стратегію керування мережею.

Для забезпечення високої доступності мережевих сервісів використовуються технології резервування та балансування навантаження, такі як резервні маршрути, мережеві з'єднання з дублюванням та інше.

Управління мережею в компанії “Dnipro-M” забезпечується командою кваліфікованих спеціалістів ІТ-відділу, які постійно вдосконалюють свої навички та вивчають нові технології для забезпечення оптимального функціонування мережевої інфраструктури.

1.4 Принципи та технічні способи інформаційного забезпечення об’єкта впровадження

Інформаційне забезпечення комп'ютерної мережі компанії “Dnipro-M” базується на низці принципів та технічних способів, спрямованих на забезпечення доступності, цілісності та конфіденційності даних, а також ефективного використання інформаційних ресурсів.

Один з основних принципів інформаційного забезпечення є цілісність, він полягає в тому що гарантує, що дані залишаються недоторканими та не змінюються без потреби. Для досягнення цього принципу можуть бути використані механізми контролю доступу та аудиту системних подій.

Ще одним ключовим принципом є забезпечення конфіденційності даних, тобто забезпечення того, щоб лише авторизовані користувачі мали

доступ до чутливої інформації. Для цього можуть бути використані різноманітні технології, включаючи механізми автентифікації та авторизації, шифрування даних та каналів зв’язку.

Один з ключових принципів, що не менш важливий, ніж цілісність і конфіденційність, – це забезпечення доступності інформації. Він полягає у тому, що користувачі мають доступ до необхідних ресурсів інформації у відповідний час та місце. Для забезпечення доступності можуть бути використані механізми резервування даних, моніторингу та управління пропускною здатністю мережі, а також використання резервного обладнання, резервних ліній зв’язку та мережевих маршрутів.

Ще один принцип, який важливо враховувати, є забезпечення ефективності та оптимальної роботи мережі. Це може охоплювати розробку та впровадження ефективних алгоритмів маршрутизації та комутації, використання технологій кешування, а також постійне моніторинг та вдосконалення мережевих процесів для забезпечення оптимальної продуктивності.

Іншим важливим аспектом є забезпечення можливості розширення та масштабування мережі відповідно до потреб компанії. Це відбувається шляхом створення гнучкої мережевої інфраструктури, яка може легко адаптуватися до зростання обсягів даних та змін у бізнес-потребах.

1.5 Аналіз процесу керування і визначення якісних задач та кількісних вимог, що подаються до проектованого виробу

Для досягнення успіху в ефективному впроваджені комп’ютерної системи у компанії “Dnipro-M”, необхідно докладно проаналізувати поточні процеси керування та визначити якісні та кількісні параметри, що впливають на їх ефективність.

Однією з основних якісних задач є забезпечення точності та надійності мережевого обчислень та керування. Вирішення цієї задачі передбачає вибір оптимального обладнання та його точне й правильне налаштування. Це

допоможе ефективно керувати різними аспектами бізнес-процесів та операцій що проводяться у мережі, ураховуючи велику кількість факторів та обмежень, що маються у компанії. Важливо забезпечити високу доступність мережі, щоб уникнути небажаних зупинок у роботі компанії.

Крім того, важливою якісною задачею є забезпечення безпеки та захисту інформації. Оскільки бізнес-процеси та комерційні операції містять конфіденційну та критичну інформацію, комп'ютерна система повинна мати вбудовані заходи безпеки, які запобігають несанкціонованому доступу та зберігають цінні дані в безпеці.

З точки зору кількісних показників, одним з важливих параметрів є продуктивність системи, що передбачає швидкість передачі даних, пропускну здатність та завантаженість мережі. Ефективне налаштування обладнання та системи в цілому, повинно забезпечувати швидку реакцію на зміни умов обчислення та запити операторів, а також дозволяти ефективному обміну даними між різними відділами та підрозділами компанії.

Отже, аналізуючи процеси керування, були визначені вимоги до проектованої комп'ютерної мережі, що включають потребу високої продуктивності, надійності, безпечності та безвідмовності. Також слід зазначити важливу вимогу до масштабованості системи – здатність мережі розширюватись або зменшуватись в залежності від потреб користувачів та обсягу трафіку даних, при цьому зберігаючи високий рівень продуктивності, надійності та ефективності. Це також включає часткове або повне забезпечення сумісності з існуючими або розроблюваними програмними та апаратними засобами.

1.6 Аналітичний огляд існуючих способів обробки та передачі інформації

Аналіз існуючих способів обробки та передачі інформації допоможе створити дієву стратегію для впровадження комп'ютерної мережі компанії "Dnipro-M". Це включає розгляд та вивчення різноманітних технологій та

протоколів, що використовуються для забезпечення ефективної комунікації та обміну даними між різними пристроями та вузлами мережі.

Перш за все, важливо зазначити, що для ефективного впровадження розроблюваної мережі “Dnipro-M”, слід базуватися на мережеву ієрархічну структуру Cisco. Ця структура використовується для розподілу мережевих функцій та відокремлення рівнів мережі для полегшення управління та підтримки. У мережевій ієрархічній структурі Cisco виділяються такі рівні:

– ядро (Core). Цей рівень відповідає за передачу даних високої швидкості між різними локальними мережами або між різними сегментами мережі. В компанії “Dnipro-M” на цьому рівні повинні бути розміщені маршрутизатори з високою пропускною здатністю, які забезпечують швидке маршрутизування та перенаправлення трафіку;

– дистрибуційний (Distribution) або рівень доступу (Access). Ці рівні забезпечують комутацію та фільтрацію трафіку між різними сегментами мережі. Часто їх об’єднують у один рівень. Вони відповідають за забезпечення доступу до мережевих ресурсів та розподілу навантаження. На цих шарах можуть бути розміщені комутатори рівнів L2 та L3, а також розподільчі маршрутизатори та точки доступу з підтримкою різних протоколів та методів комутації даних, включаючи віртуалізацію, агрегацію та управління широкомовного домену;

– рівень хостів (Host). Цей рівень забезпечує підключення кінцевих пристроїв (комп'ютерів, серверів та інших високопродуктивних систем) до мережі. На цьому рівні використовуються з’єднання з комутаторами, точками доступу тощо, які забезпечують розподілення трафіку між пристроями та впорядкування його.[3]

Окрім мережевої ієрархічної структури Cisco, слід також розглянути стандартизовані та уніфіковані технології та протоколи для передачі та обробки інформації, так як мережа повинна відповідати принципам доступності, масштабованості та мати можливість обмінюватися

інформацією з іншими диверсифікованими мережами та мережею Інтернет. До таких відносяться:

– Ethernet. Одна з основних технологій мережевого зв'язку, яка використовується для з'єднання різних пристроїв у локальні мережі. Найпопулярніший протокол кабельних комп'ютерних мереж, що працює на фізичному та канальному рівні;

– стек протоколів TCP/IP. Основні протоколи мережевого зв'язку в Інтернеті, який використовується для передачі даних між різними пристроями. Фактично це систематизований набір, що поділяється на чотири рівні: прикладний, транспортний, міжмережевий та рівень доступу до середовища передачі;[4]

– Wi-Fi. Технологія бездротової передачі інформації, яка дозволяє підключати пристрої до мережі без використання кабелів. Бездротова передача даних за технологією Wi-Fi буде основою для майбутньої реалізації IoT-системи клімат контролю приміщень та систем безпеки.

1.7 Завдання і мета роботи

Метою роботи є організація корпоративної комп'ютерної мережі з детальним опрацюванням побудови, налаштування та безпеки компанії “Dnipro-M”.

Для вирішення поставленої мети в роботі слід виконати наступні завдання:

– виконати аналіз об’єкта;

– сформулювати технічні вимоги для розробки комп’ютерної системи;

– підібрати оптимальну архітектуру мережі відповідно до потреб компанії;

– розробити специфікацію апаратних засобів та структурованої кабельної мережі;

– провести аналіз мережевого трафіку;

– розробити модель комп’ютерної мережі та виконати конфігурацію мережевого обладнання ;

– реалізувати IoT-системи клімат-контролю та безпеки;

– провести тестування моделі мережі та IoT-компонента.

1.8 Визначення можливих напрямків рішення поставлених задач

Для вирішення поставлених завдань щодо розробки комп’ютерної мережі компанії “Dnipro-M”, з реалізацією побудови та налаштування корпоративної мережі й безпеки можуть бути використані наступні рішення:

1. Вибір мережевої архітектури. Для комп’ютерної мережі компанії буде обрано розподілену архітектуру з гібридним підходом. В розподіленій архітектурі передбачається розподіл мережевих ресурсів між взаємопов’язаними вузлами. При розробці архітектури слід базуватися на мережеву ієрархічну структуру Cisco – розділення мережі на ядро, елементи доступу та безпосередньо хости-вузли.

2. Вибір обладнання, яке відповідає потребам компанії щодо продуктивності, безпеки та масштабованості. Необхідно провести оцінку потреб у мережевому обладнанні, такому як комутатори, маршрутизатори, мережеві екрани та сервери.

3. Вибір типів з’єднання та кабельної системи. Для з'єднання між офісами буде використано мережу Інтернет. Це забезпечить можливість передачі даних між віддаленими локаціями без потреби встановлення приватних ліній зв'язку. Використання одного з місцевих провайдерів Інтернет забезпечить доступність та надійність зв'язку. Для підключення пристроїв усередині будівель компанії буде використовуватися вита пара. Вита пара є стандартом для Ethernet-мереж і є надійним та ефективним засобом передачі даних. Вона забезпечить достатню швидкість передачі даних та стійкість до електромагнітних перешкод, що особливо важливо для забезпечення надійності мережі.

4. Вибір технологій, стандартів і протоколів. Використання протоколу динамічної маршрутизації EIGRP дозволить ефективно керувати маршрутами в мережі “Dnipro-M”, забезпечуючи швидке виявлення та адаптацію до змін в мережевому середовищі. Використання VLAN дозволить логічно розділити підмережу комерційного відділу на окремі функціональні сегменти з метою підвищення керування трафіком та безпеки. Запровадження агрегації каналів (EtherChannel) у віддаленому офісі дозволить об'єднати кілька фізичних з'єднань між комутаторами в одне логічне з'єднання, що підвищить пропускну здатність та надійність мережі. Запровадження NAT та VPN дозволить приховати внутрішні IP-адреси в мережі від зовнішнього Інтернету та забезпечить необхідний рівень безпеки і захисту від зовнішніх атак, та дозволить об’єднати віддалені комп’ютерні системи офісів у одну.

5. Захист і безпека. Необхідно провести розробку стратегій та заходів для забезпечення безпеки мережі, включаючи використання мережевих екранів, списків контролю доступ, шифрування каналів зв’язку, розробки політики паролів, автентифікації та авторизації, та мережевого моніторингу.

6. Використання веб-сервісів та хмарних технологій. Слід розглянути впровадження інтернет-сервісів та хмарних послуг для забезпечення резервного копіювання даних, зберігання та обробки інформації, а також для забезпечення віддаленого доступу до ресурсів мережі. Це повинно включати налаштування WEB- (HTTP)-, DNS- та TFTP-серверів.

7. Реалізація IoT-системи клімат-контролю та безпеки. У головному офіс компанії повинна функціонувати IoT-підмережа, розподілена по поверхам будівлі, що повинна забезпечувати контроль за температурою та вологістю приміщень, система доступу та безпеки до критичних точок мережі – серверні кімнати, а також протипожежна безпека.

8. Резервне забезпечення та безвідмовність мережі. Необхідно включити розробку стратегій та заходів для забезпечення надійності та доступності мережі, що включає створення резервних ліній зв'язку.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до комп'ютерної системи

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонування системи

2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії

Комп'ютерна система (КС) компанії "Dnipro-M" (далі Система) призначена для підтримки прийняття рішень, забезпечення звітності у процесі керування комерційною діяльністю (продажі, технічне обслуговування, клієнтська консультація).

Система компанії поділяється на локальні мережі (LAN) згідно до загальної архітектури, наведеному в додатку А:

– відділ служби підтримки, LAN1. Розроблювана мережа відділу повинна проводити забезпечення зв'язку для: віддаленого офісу відділу служби підтримки з головним офісом компанії, сервісної підтримки віддалених користувачів та клієнтів, розв'язання технічних питань і проблем, що виникли у покупців та клієнтів. Необхідно забезпечити зв'язок для 12 вузла – робочих станцій (персональний комп'ютерів) операторів (робітників відділу);

– фінансовий відділ, LAN2. Мережа цього відділу повинна проводити забезпечення зв'язку у структурних одиницях компанії для проведення фінансової діяльності та обробки фінансових даних. Мережа повинна бути з високою безпекою та доступністю для забезпечення безперебійної роботи фінансових систем компанії "Dnipro-M". Необхідно забезпечити зв'язок для 10 вузлів;

– виконавчий відділ, LAN3. Мережа цього відділу відповідає за забезпечення зв'язку структурних одиниць компанії для організаційного управління, прийняття та видачі стратегічних рішень і задач компанії. Мережа

повинна забезпечувати високу швидкість передачі даних та конфіденційність для обробки важливої інформації. Необхідно забезпечити зв’язок для 12 вузлів;

– комерційний відділ, LAN4. Відділ логічно поділений на 3 підрозділи: продажів, маркетингу та логістику. Мережа відділу відповідає за забезпечення з’єднання структурних одиниць компанії для можливості введення комерційної діяльності. До мережі входить файловий TFTP-сервер, для збереження конфігурацій та документацій відділу та системи компанії загалом. Виходячи із поділу відділу на підрозділи, вимагається впровадити ділення мережі комерційного відділу на три віртуальні підмережі зі своїм унікальним функціоналом. Необхідно забезпечити зв’язок для 10 вузлів;

– IT-відділ, LAN5. Мережа IT-відділу відповідає за забезпечення IT-інфраструктури та підтримки мережевої систем компанії, надає доступ до комп’ютерної системи для системних адміністраторів та операторів. До неї мережі IT-відділу також входять сервери HTTP, для надання з’єднання з веб-сторінками та інтерфейсами, та DNS, для перекладу доменних імен в IP-адреси. Необхідно забезпечити зв’язок для 3 вузлів.

У Системі є IoT-мережа клімат-контролю та безпеки. Вона представлена 2 підсистемами контролю температури та вологості на основі мікроконтролерів (кожна функціонує на окремому поверсі головного офісу), 2 системи безпеки да доступу для серверних кімнат (за їхньою кількістю), протипожежна сигналізація.

Мережа повинна мати розподілену архітектуру з гібридним підходом. В розподіленій архітектурі передбачається розподіл мережевих ресурсів між взаємопов’язаними вузлами. Архітектура повинна базуватися на мережеву ієрархічну структуру Cisco – розділення мережі на ядро, елементи доступу та безпосередньо хости-вузли.

2.1.1.1.2 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами системи

Основу мережевої інфраструктури повинен складати стек протоколів TCP/IP. Усі підмережі компанії повинні використовувати протокол IP для адресації та маршрутизації, та TCP/UDP для забезпечення доставки пакетів та роботи серверів.

Для локальних мереж використовується технологія Ethernet, яка повинна бути застосована для кабельних з’єднань та забезпечувати достатні швидкості передачі. У критичній ділянці мережі офісу служби підтримки (LAN1), застосовується технологія агрегація каналів EthernetChannel для об'єднання декілька фізичних портів в один логічний канал та протоколу LACP для конфігурації логічних портів.

У підмережі LAN4, яка обслуговує комерційний відділ компанії, слід створити три віртуальні підмережі (VLAN), для логічного розділення фізичної мережі: VLAN24 для підрозділу продажів, VLAN34 для маркетингу та VLAN44 для логістики.

Маршрутизація в мережі компанії повинна здійснюватися за допомогою динамічного протоколу EIGRP.

Для забезпечення зв'язку мережі компанії з Інтернетом через провайдера необхідно використовувати трансляцію адрес NAT – перетворення приватних IP-адрес внутрішніх ресурсів у публічні.

Для забезпечення закритого та шифрованого каналу зв’язку між віддаленим та головним офісами необхідно впровадити сервіс віртуальних приватних мереж (VPN) поверх Інтернет.

Компоненти IoT-системи клімат-контролю та безпеки повинні використовувати бездротовий зв’язок за технологією Wi-Fi. З’єднання повинно забезпечуватися точкою доступа, або шлюзом IoT.

2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної системи із суміжними системами

Система повинна використовувати стек протоколів TCP/IP та Ethernet, та відповідні до них фізичні та логічні порти, для базової взаємодії з суміжними віддаленими комп'ютерними мережами, які функціонують на тих же рівнях моделі OSI та стандартів IEEE, та Інтернет, а також підтримувати протоколи HTTP/S, DNS та TFTP для обміну даними з системами, що існують поверх вищезазначених мереж, що включають веб-інтерфейси та клієнт-орієнтовані додатки на віддалених хостах.

Обмін даними повинен відбуватися у форматах, які розуміють усі взаємодіючі системи. Основними форматами даних будуть XML та JSON.

Система повинна інтегруватися з додатками та веб-інтерфейсами за допомогою API-інтерфейсів (Application Programming Interface), веб-служб тощо.

2.1.1.1.4 Вимоги до режимів функціонування системи

Система компанії "Dnipro-M" повинна задовольняти наступні вимоги до режимів функціонування мережі:

– стандартний режим роботи. Система має забезпечувати неперервність роботи протягом усього часу експлуатації, повинна бути доступною для користувачів у будь-який час, за винятком запланованих перерв на технічне обслуговування чи невеликі періоди відновлення після аварійних ситуацій;

– обслуговування обладнання. Адміністратори Системи проводять заплановані роботи з обслуговування обладнання: оновлення програмного забезпечення, заміна та конфігурація компонентів. Заплановані перерви на ремонт та обслуговування Системи повинні мати мінімальний вплив на доступність послуг для користувачів: необхідне застосування резервних каналів, маршрутів та компонентів Системи, на час простою основного обладнання;

– аварійне відновлення. Режим виникає під час аварійних ситуацій або відмов в роботі мережі. Адміністратори проводять якнайшвидше відновлення роботи Системи і сервісів після аварії. Застосовуються резервні канали зв’язку та резервні копії даних.

2.1.1.1.5 Вимоги до діагностування системи

Спеціалісти ІТ-відділу повинні забезпечувати постійний моніторинг системи, для виявлення та аналізу потенційних проблем. Система діагностування (правила) повинна забезпечувати наступні функції:

– спеціалісти ІТ-відділу повинні забезпечувати постійний моніторинг стану мережевої інфраструктури, включаючи активність мережевих пристроїв (комутаторів, маршрутизаторів), використання каналів зв'язку, рівень загрузки ліній передачі даних та інші параметри, що впливають на продуктивність мережі;

– спеціалісти ІТ-відділу повинні виявляти потенційні проблеми та відхилення в роботі мережі, такі як перевантаження каналів, відмови мережевих пристроїв, збої в роботі програмного забезпечення тощо. Крім того, необхідне забезпечення можливості аналізу цих проблем з метою швидкого виявлення та усунення причин їх виникнення;

– при діагностуванні повинно здійснюватися логування всіх подій та відхилень у роботі мережі, забезпечуючи збереження історії подій для подальшого аналізу та вирішення проблем;

– для діагностування повинна надаватися можливість віддаленого доступу та керування для операторів та адміністраторів, щоб вони могли в режимі реального часу відстежувати стан мережі, виконувати діагностику та вирішувати проблеми, навіть якщо вони перебувають за межами корпоративного офісу.

2.1.1.1.6 Перспективи розвитку системи

Планується поступове розширення комп'ютерної мережі компанії “Dnipro-M” з метою підтримки зростаючих потреб передачі інформації, обчислення та забезпечення належного функціонування. Основним напрямком розвитку є збільшення кількості фізичних з’єднань та розширення адресного простору відділів.

У мережі LAN1 планується розширення кількості хостів до 21.

У майбутньому в мережі LAN2 планується досягти кількості вузлів 72.

У мережі LAN3 потрібно урахувати розширення до 48 вузлів.

Для мережі LAN4 необхідно збільшити кількість хостів з 10 до 49.

Для мережі LAN5 необхідно урахувати збільшення вузлів до 125.

Планується, що дане розширення мережевого покриття буде виконане у відповідності до стандартів та вимог.

При виборі активного й пасивного мережевого обладнання, їхньої кількості, розробці та впровадження комп’ютерної системи необхідно врахувати ці вимоги розширення та масштабування.

2.1.1.2 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему

2.1.1.2.1 Вимоги до чисельності персоналу (користувачів) системи

Основні вимоги до чисельності операторів та користувачів комп’ютеризованих робочих місць кожного відділу та підрозділу корпоративної комп’ютерної мережі компанії “Dnipro-M”:

– служба підтримки, віддалений офіс, LAN1. Кількість користувачів мережі становить 12. Необхідно врахувати розширення відділу до 21 користувача;

– фінансовий відділ, головний офіс, LAN2. Кількість користувачів мережі становить 10. Врахувати розширення до 72;

– виконавчий відділ, головний офіс, LAN3. Кількість користувачів мережі становить 12. Врахувати розширення до 48;

– комерційний відділ, головний офіс, LAN4:

а) підрозділ продажів, VLAN 24. Кількість користувачів підмережі становить 3. Врахувати розширення до 16;

б) підрозділ маркетингу, VLAN 34. Кількість користувачів підмережі становить 3. Врахувати розширення до 16;

в) підрозділ логістики, VLAN 44. Кількість користувачів підмережі становить 4. Врахувати розширення до 17;

– IT-відділ, головний офіс, LAN5. Кількість користувачів мережі становить 3. Врахувати розширення можливих підключень до 125.

2.1.1.2.2 Вимоги до кваліфікації персоналу, порядку його підготовки і контролю знань і навичок

Основні вимоги кваліфікації персоналу та порядку його підготовки і контролю знань і навичок в компанії “Dnipro-M” діляться на два рівні: рівень користувача-оператора мережі компанії, з базовими навичками роботи з ПК та відповідним програмним забезпеченням, та рівень IT-спеціалістів.

Рівню IT-спеціалістів компанії “Dnipro-M” повинні відповідати компетенції та навички працівників IT-відділу. Системні адміністратори та мережеві інженери цього відділу повинні мати вищу технічну освіту в галузі інформаційних технологій та досвід роботи з розподіленими комп’ютерними мережами.

2.1.1.3 Показники призначення

Вимогами до показників призначення комп'ютерної мережі компанії “Dnipro-M” є необхідні параметри, які визначають, наскільки система відповідає своїм цілям. Основна ціль комп'ютерної мережі полягає у забезпеченні зручного, простого та надійного доступу користувачів-

операторів до загальних ресурсів мережі та спільного використання цих ресурсів з надійним захистом від несанкціонованого доступу, зберігаючи конфіденційність та цілісність даних..

Комп’ютерна мережа повинна функціонувати стабільно та без перебоїв 99,9% часу на рік, запобігаючи випадкам відмов у роботі. Важливо, щоб вона автоматично, або за втручанням операторів, відновлювалася після можливих збоїв.

Користувачі повинні мати швидкий доступ до даних та ресурсів мережі, щоб забезпечити ефективну роботу. Середній час відповіді на запити користувачів повинен бути менше 50 мс; Пропускна здатність з’єднання з вузлами операторів не повинна бути менше ніж 100 Мбіт/с, на магістральних з’єднаннях – не менше 1 Гбіт/с.

Показник сумісності комп’ютерної мережі відповідає за забезпечення взаємодії з існуючими технологіями та здатності інтегруватися з майбутніми технічними рішеннями без перешкод. Це включає використання стандартів IEEE, OSI тощо.

Показник легкості адміністрування та зручності користування передбачає комфортний доступ до адміністративних інструментів та інформаційних ресурсів мережі, а також відповідає за здатність своєчасно та відповідно реагувати на потреби користувачів мережі. Необхідне застосування у Системі «юзер-френдлі» та інтуїтивно зрозумілих користувацьких інтерфейсів (API, додатків).

2.1.1.4 Вимоги безпеки

Забезпечення безпеки під час монтажу, налагодження, експлуатації, обслуговування та ремонту технічних засобів комп’ютерної мережі “Dnipro-M” має відповідати чинним нормативним актам з охорони праці та стандартів[5].

Усі роботи з мережею повинні виконуватися кваліфікованим персоналом, який пройшов відповідне навчання з питань безпеки при роботі

з електрообладнанням і має дозвіл на роботу з заживленими технічними засобами.

Повинні бути дотримані наступні правила при монтажу активного та заживленого обладнання:

– усе обладнання повинно мати належне заземлення;

– необхідне використання захисних вимикачів для запобігання електричним ударам;

– монтаж і налагодження обладнання мають виконуватися за допомогою інструментів з ізоляцією.

Також необхідне дотримання вимог для мінімізації електромагнітних пробоїв – усі кабелі та проводки повинні бути екранованими;

2.1.1.5 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи

2.1.1.5.1 Умови і регламент (режим) експлуатації, що повинні забезпечувати використання технічних засобів (ТЗ) системи з заданими технічними показниками

Корпоративна комп'ютерна мережа компанії "Dnipro-M" повинна працювати цілодобово та безперервно, окрім аварійних випадків та перерв на технічне обслуговування і діагностування. Експлуатація системи має здійснюватися в умовах, які відповідають чинному законодавству, нормативам і стандартам.

Приміщення, де встановлено обладнання комп'ютерної системи "Dnipro-M", має відповідати наступним вимогам:

– забезпечення достатнього рівня освітленості, на рівні 500 Лк/м^2;

– відсутність агресивних середовищ, а також контроль за рівнем пилу, який не повинен перевищувати 0,75 мг/м^3;

– електрична складова електромагнітного поля не повинна перевищувати 0,3 Н/м у діапазоні частот від 0,15 до 300,00 МГц.

Кліматичні умови зони експлуатації повинні відповідати нормам[6]:

– температура навколишнього повітря повинна бути в межах від +10°C до +25°C;

– відносна вологість повітря має знаходитись в межах 40% до 80% при температурі повітря +10°C для запобігання конденсації;

– атмосферний тиск в межах від 84 кПа до 107 кПа.

Необхідно дотримуватися вимог щодо пожежної безпеки у приміщеннях, де розташована та функціонує система, згідно стандартів[7].

Необхідно дотримуватися вимог щодо електробезпеки у комп'ютерній системі згідно держстандарту[5].

2.1.1.5.2 Вимоги до параметрів мереж енергопостачання (живлення та заземлення)

Комп'ютерна мережа компанії "Dnipro-M" та відповідне до неї обладнання має бути забезпечена стійким та надійним електропостачанням з урахуванням вимог до живлення та заземлення, встановлених відповідними нормативними документами. Для заземлення компонентів мережі необхідне застосування системи типу TN-S, яка забезпечує найвищий рівень електробезпеки людей і обладнання.

Комп'ютерна система та відповідне обладнання повинні працювати в умовах стабільного живлення, що відповідає вимогам стандартів[8] , а саме:

– напруга живлення в мережі повинна бути в межах 230 В зі стабільністю не менше ±10%;

– номінальна частота напруги електропостачання має бути 50 Гц з можливим відхиленням у ± 1 % (тобто 49,5 Гц...50,5 Гц) протягом 99,5 % часу за рік.

Комп'ютерна система та відповідне обладнання, що включає розетки, мережеве та операторське обладнання, комутаційні шафи та стійки, повинні

бути належно заземленим. Необхідне дотримання вимог до елементів уземлення згідно стандартів[5]. Загальні вимоги до заземлення:

– опір заземлюючого контуру має мати до 4 Ом (для мереж загального призначення);

– елементи заземлення повинні забезпечувати надійний відвод струмів короткого замикання та інших електричних ризиків.

Забезпечення стабільної напруги є важливою складовою для запобігання пошкодження електронного обладнання компанії. У системі офісів необхідне встановлення стабілізаторів напруги на кожному важливому вузлі електроживлення системи для компенсації можливих перепадів напруги. Обладнання стабілізації повинно забезпечувати низьку відсоткову похибки стабілізації.

2.1.1.5.3 Вимоги до складу, розміщенню й умовам збереження комплекту запасних виробів і приладів

Комплект запасних виробів і приладів комп’ютерної мережі “Dnipro-M” повинен містити достатню кількість запасних компонентів для забезпечення безперебійної роботи мережі в разі виникнення непередбачуваних та аварійних ситуацій. Склад запасних виробів повинен включати наступні найменування:

– мережеве обладнання: маршрутизатори, комутатори, точки доступу тощо, у кількості до 2 одиниць кожного виробу;

– електронно-обчислювальне обладнання робочих місць: компоненти, що включають ЦПУ, ОЗУ, диски та накопичувачі, материнські плати, кабелі-з’єднувачі тощо, для персональних комп’ютерів та робочих станцій працівників у кількості до 5 одиниць, та для серверів у кількості до 2 одиниць;

– пасивні компоненти мережі: мережеві кабелі (патч-корд) виду вита пара UTP (перехресний та прямий) не менше 30 метрів; мережеві розетки та коннектори RJ-45 у кількості 50 одиниць кожна.

Комплект запасних виробів і приладів повинен знаходитися в спеціально відведених приміщеннях на стелажах та полицях з мінімальним контактом з підлогою, для забезпечення захисту від вологості, пилу, температурних коливань та інших негативних чинників. Приміщення для зберігання запасів, відповідно до вимог, повинно бути обладнане системами вентиляції та кондиціонування повітря, що забезпечують температуру в межах від +10°C до +25°C та вологість повітря не більше 80%.

2.1.1.5.4 Вимоги до регламенту обслуговування

Регламент обслуговування комп'ютерної мережі “Dnipro-M” визначає процедури та умови, які необхідно дотримуватися функціонування системи. Повинні виконуватися наступні процедури обслуговування:

– планове (регулярне) технічне обслуговування. Обслуговування мережі повинно проводитися регулярно відповідно до встановленого графіку – кожного місяця (30 календарних днів). Технічне обслуговування включає перевірку стану обладнання та конфігурацій, виявлення і усунення несправностей та пошкоджень, а також профілактичні заходи для запобігання можливих проблем;

– ремонт та відновлення. Необхідне впровадження процедур та залучення відповідних осіб для екстреного обслуговування, швидкого виявлення та усунення несправностей у випадку виникнення аварійних ситуацій або критичних відмов в роботі мережі та програм. Процедура передбачає якомога швидше відновлення роботи мережі після виникнення аварійних ситуацій шляхом відновлення роботи активного обладнання або запуску резервних механізмів та компонентів. Граничний час на відновлення – не більше 4 годин після виникнення аварії;

– оновлення та модернізація. Необхідне впровадження процедур своєчасного оновлення програмного забезпечення, апаратного забезпечення та мережевих технологій, що повинні відповідати до вимог сучасних та

майбутніх стандартів безпеки, ефективності, сумісності та інтегрованості. Частота оновлення повинна становити від 6 до 12 місяців для програмного забезпечення та до 5 років для апаратного, залежно від вимог до продуктивності мережі;

– документування та звітність. Необхідне забезпечення систематичного ведення документації щодо проведених робіт з обслуговування, ремонтів та замін обладнання. Передбачено формування звітів про стан мережі, виявлені проблеми та заходи, що були прийняті для їх вирішення. Також повинні складатися журнали обліку та інвентаризації, в яких фіксуються наявність, стан та дії над обладнанням, включаючи встановлення нових компонентів, заміну, видалення чи перенесення.

2.1.1.6 Вимоги до захисту інформації від несанкціонованого доступу

Для забезпечення високого рівня захисту інформації від несанкціонованого доступу у Системі компанії “Dnipro-M” необхідно впровадити правила, політики та технічні рішення щодо інформаційної безпеки:

– критичні вузли мережі, сервери та активне обладнання повинні бути розміщені у захищеному приміщенні (серверна кімната) з обмеженим доступом. Вхід до серверної повинен здійснюватися за допомогою електронних RFID-карток, виданим окремим операторам мережі та адміністраторам;

– паролі повинні мати мінімум 8 символів, містити великі та малі літери латинського алфавіту, цифри та спеціальні символи. Паролі повинні змінюватися кожні 6 місяців для стандартних вузлів мережі, та 90 днів – для критичних вузлів. Заборонено зберігати паролі у відкритому вигляді або на паперових носіях;

– політика контролю доступу повинна включати автентифікацію, авторизацію та облік дій користувачів (AAA). У Системі необхідне

запровадження клієнт-серверної системи AAA RADIUS, з налаштуваннями локальної бази даних доступу автентифікованих клієнтів за визначеним паролем;

– необхідне встановлення та налаштування файрволів та списків контролю доступу (ACL) для обмеження доступу до локального блоку IP 10.24.112.0/21 для адресації у віддалених мережах та Інтернет;

– для шифрування з'єднань по лініях віртуальних терміналів необхідне використання протоколу SSH, та IPsec для VPN-з'єднань.

2.1.1.7 Вимоги до патентної чистоти

У Системі компанії “Dnipro-M” мають дотримуватися правила та зобов’язання щодо патентних прав та інтелектуальної власності згідно діючого законодавства встановленого на території України.

2.1.1.8 Додаткові вимоги

2.1.1.8.1 Вимоги до кабель-каналів, інформаційним та електричним розеткам

Вимоги до кабель-каналів:

– кабель-канали повинні бути достатньої ширини та глибини для зручного прокладання мережевих та електричних кабелів. Розмір визначається на етапі прокладання;

– кабель-канали повинні мати захисні властивості від впливу зовнішнього середовища, такого як пил, волога, температурні коливання тощо. Рекомендований клас захисту – IP44;

– необхідно передбачити розділення кабель-каналів для окремого прокладання мережних кабелів та електроживлення.

Вимоги до інформаційних розеток:

– інформаційні розетки повинні відповідати стандартам TIA/EIA-568-B для організації мережі Ethernet (RJ-45) та бути здатними підтримувати необхідні швидкості передачі даних – на рівні 100 Мбіт/с;

– кожна робоча станція, вузол, пристрій або активний елемент мережі повинні мати мінімум 1 інформаційну розетку;

– розташування інформаційних розеток повинно бути зручним для експлуатації, забезпечувати легкий доступ до них, а також продукувати мінімізацію довжини мережевих кабелів;

Вимоги до електричних розеток:

– кількість електричних розеток повинна бути на рівні до 3 на одне робоче місце для забезпечення живлення пристроїв;

– розташування електричних розеток повинно бути зручним для підключення пристроїв та мінімізації довжини електричних кабелів.

2.1.1.8.2 Вимоги до комунікаційного обладнання і його розташування

Комунікаційне обладнання повинно бути розміщене в спеціально відведених, обладнаних та захищений від несанкціонованого доступу технічних приміщеннях – серверних кімнатах. Доступ до приміщень повинні мати лише адміністратори мережі, обслуговуючий персонал технічних засобів та вище керівництво. Вхід забезпечується за допомогою систем електронних RFID-карток.

Приміщення повинні мати належну вентиляцію, систему кондиціювання, та забезпечувати захист від пилу, вологи та інших негативних факторів, визначених у розділі 2.1.1.5.1.

Необхідне використання стандартних 19-дюймових шаф для монтажу комунікаційного обладнання. Шафи повинні мати достатню міцність та стійкість для утримання обладнання та забезпечення його безпеки. Обладнання повинно бути розташоване таким чином, щоб забезпечити

належну вентиляцію, висоту розташування від підлоги та доступність для обслуговування – відстань між компонентами 20-30 см. Також необхідно продумати організацію кабельних з'єднань та патч-панелей для зручного монтажу мережевих проводок. Корпус комутаційної шафи має бути заземленим згідно вимог.

Кабельні траси повинні бути відведені від вузлів мережі до місць розташування комунікаційного обладнання шляхом використання кабельних каналів. Траси повинні бути відповідно марковані та організовані для полегшення обслуговування.

2.1.1.8.3 Вимоги до однорідності

Для забезпечення однорідності по типу сигнальних кабелів, вони повинні мати однакову конструкцію та параметри. Всі кабелі мережі повинні відповідати одному стандарту та категорії, рекомендується використання кабелів категорії Cat.5/5e-6 для реалізації мережі Ethernet. При використанні кабелів Cat.6, потрібно запровадити у мережу зворотну сумісність зі старшими стандартами Cat.5/5e, для сумісності та однорідності системи з іншими компонентами.

Всі роз'єми, використані для підключення кабелів до обладнання та на мережевих платформах, повинні бути стандартизовані та відповідати вимогам RJ45, для реалізації мережевих з’єднань Ethernet.

2.1.1.8.4 Вимоги до резервування

У комп’ютерній мережі компанії “Dnipro-M” мають бути застосовані наступні принципи резервування:

– резервування каналів зв'язку. Необхідно впровадити додаткові канали зв'язку між маршрутизаторами рівня ядра головного офісу;

– резервне копіювання даних. Для забезпечення відновлення інформації в разі її втрати або пошкодження, слід використовувати серверно-

орієнтованих систем резервного копіювання для збереження даних. Конфігураційні файли активного мережевого обладнання повинні мати резервну копію на TFTP-сервері. Згідно регламенту обслуговування, копії конфігураційних файлів повинні перевірятися та оновлюватися (за потреби) кожні 30 днів;

– резервне обладнання. У Системі повинні бути у наявності комплекти запасних комутаторів, маршрутизаторів, точок доступу, які, за допомогою адміністраторів мережі, повинні приймати на себе роботу у випадку відмови основного обладнання.

2.1.2 Вимоги до налаштувань та функцій, виконуваних системою

Мережа компанії повинна функціонувати на рівні локальних підмереж, згідно кількості та функціоналу відділів. Для розробки корпоративної мережі повинен бути застосований блок приватних IP-адрес – 10.24.112.0/21. При розподілені адрес для підмереж необхідно врахувати критерії найкращої суммарізації та мінімальної витрати адрес, кількості кінцевих вузлів, мережевого активного обладнання, інформаційних систем, а також враховувати потреби для масштабування та майбутнього розширення. Таким чином, мережа, на структурно-функціональному рівні, повинна бути поділена на наступні відділи-підмережі компанії, згідно розрахункам за методом маски змінної довжини (VLSM):

– служба підтримки, віддалений офіс, LAN1. Адресація: 10.24.113.192/27;

– фінансовий відділ, головний офіс, LAN2. Адресація: 10.24.112.128/25;

– виконавчий відділ, головний офіс, LAN3. Адресація: 10.24.113.128/26;

– комерційний відділ, головний офіс, LAN4. Адресація: 10.24.113.0/25;

– IT-відділ, головний офіс, LAN5. Адресація: 10.24.112.0/25.

Для функціонування зв’язку на рівні ядра, необхідно прокласти між маршрутизаторами основні та резервні канальні лінії, для адресації яких слід застосувати адреси із блоку 10.0.14.0/24.

Для функціонування IoT-підсистеми клімат-контролю та безпеки, необхідно провести налаштування шлюза-IoT та систем керування. Це включає налаштування локальної бездротової мережі Wi-Fi: назва мережі «DniproM_IoT»; безпека мережі – WPA2-PSK з шифруванням AES. Для адресації IoT компонентів та приладів використовувати блок 10.24.114.0/24. Розробити програми та скрипти керування компонентами IoT, та реалізувати їх у вигляді коду для мікроконтролерів й правил-умов (Conditions) для «розумних пристроїв» на веб-орієнтованому додатку IoT.

Повинно бути впроваджено функціонування агрегації каналів між комутаторами віддаленого офісу служби підтримки для підвищення пропускної здатності та забезпечення резервування.

Для розділення мережі комерційного відділу на логічно-функціональні сегменти, необхідно застосувати технологію віртуальних мереж – VLAN. Це дозволить створити для кожного підрозділу свої віртуальні інтерфейси й адресацію та полегшить управління. Поділ LAN4 на VLAN:

– підрозділ продажів, VLAN24. Адресація: 10.24.113.0/27;

– підрозділ маркетингу, VLAN34. Адресація: 10.24.113.32/27;

– підрозділ логістики, VLAN44. Адресація: 10.24.113.64/27.

У корпоративній мережі компанії повинні функціонувати правила та політики призначення IP-адрес для вузлів та пристроїв у LAN:

– перші можливі для використання адреси повинні бути призначені інтерфейсам і підінтерфейсам маршрутизаторів;

– другі з можливих адрес повинні бути призначені комутаторам;

– серверам повинні бути призначені IP-адреса за правилом: IP-адрес дорівнює першому можливому адресу у мережі+9+14;

– всі інші адреси призначені для кінцевих вузлів.

Необхідно щоб у кожному відділі та підрозділі функціонувало автоматичне призначення IP адрес вузлам мережі. Для цього на маршрутизаторах, які забезпечують відповідні мережі, потрібне налаштування DHCP-сервера, пул яких повинен бути розподілений згідно правил та мережевих адрес зазначених вище.

Для функціонування зв'язку між мережами головного офісу необхідно впровадити маршрутизацію EIGRP у системі. При налаштуванні протокола, необхідно вказати номер автономної системи-процесу 100, оголосити всі адреси мереж та віртуальних мереж. Окремо, необхідно налаштувати на крайньому маршрутизаторі (що з'єднаний з обладнанням провайдера) маршрут (шлюз) за умовчанням 0.0.0.0/0 і розповсюдити його через оновлення маршрутів. Для всіх інших з'єднань використовувати статичну маршрутизацію.

Для з'єднання кінцевих вузлів з Інтернетом, а також для можливості впровадження інтернет-сервісів на основі локального обладнання компанії, необхідно впровадити трансляцію адрес NAT. Для NAT, провайдер надав 3 блоки зовнішніх адрес: 209.165.202.0/30 та 64.100.13.0/30 – використовуються для адресації портів крайніх маршрутизаторів компанії та провайдера; 209.165.200.0/26 – для динамічного (для звичайних вузлів) та статичного (для серверів) NAT.

HTTP-сервер повинен надавати функції веб-інтерфейсу для взаємодії з ресурсами компанії. DNS-сервер надає функції перетворення доменних імен на адреси, що забезпечує просту взаємодію з веб-сервером. TFTP-сервер застосовується для забезпечення функціонування простої бази даних резервування компанії з віддаленим доступом.

Мережа повинна мати налаштовані механізми захисту від несанкціонованого доступу за допомогою списків контролю доступу (ACL, файрволів) на крайніх маршрутизаторах. На всіх активних комунікаційних приладах необхідне впровадження систем авторизації та автентифікації AAA RADIUS за паролем для прямого та віддаленого доступу. Віддалене з'єднання

по лініям віртуальних терміналів необхідно забезпечити шифруванням SSH. Для забезпечення функціонування захищеного зв’язку між головним офісом та віддаленим, поверх Інтернет повинена функціонувати мережа VPN за протоколом IPsec.

2.1.3 Вимоги до видів забезпечення

2.1.3.1 Вимоги до лінгвістичного забезпечення системи

Основна мова взаємодії користувача з інтерфейсами вузлів, серверів та іншого обчислювального обладнання комп'ютерної мережі “Dnipro-M” повинна бути українською. Також повинна бути забезпечена можливість легкого переключення на англійську мову для зручності іншомовних користувачів.

Код скриптів керування актуаторами та датчиками, під’єднаними до мікроконтролерів у системі IoT, повинні бути реалізовані мовою Python.

2.1.3.2 Вимоги до технічного забезпечення системи

Вимоги до комп’ютерів на робочих місцях:

– процесор: мінімум рівень моделі Intel Core i5 або аналог AMD з частотою 2.5 ГГц та 4 ядра та інтегрованим графічним чіпом рівня Intel UHD Graphics 630 або вище;

– оперативна пам'ять: мінімум 8 ГБ ОЗУ DDR4;

– жорсткий диск: HHD, SSD ємністю мінімум 256 ГБ;

– мережева карта: Gigabit Ethernet;

– операційна система: Windows 10 Pro або новіше / Ubuntu 18.04 LTS або новіше.

Вимоги до серверів:

– процесор: Intel Xeon або аналог AMD з мінімальною кількістю 16 ядер;

– оперативна пам'ять: мінімум 64 ГБ ОЗУ DDR4;

– жорсткий диск: RAID 1 конфігурація з SSD, ємністю мінімум 1 ТБ;

– мережева карта: Gigabit Ethernet;

– операційна система: Windows Server 2019, Linux серверні дистрибутиви або інші аналогічні системи.

Вимоги до комутаторів:

– підтримка протоколів VLAN, STP, RSTP, SNMP;

– підтримка технології агрегації каналів EtherChannel;

– мінімум 24 порти FastEthernet та 2 порти GigabitEthernet;

– пропускна здатність мінімум 1 мільйон пакетів на секунду.

Вимоги до маршрутизаторів:

– пропускна здатність мінімум 1 Гбіт/с;

– мінімум 4 Serial-порти та мінімум 2 порти GigabitEthernet;

– підтримка протоколів маршрутизації EIGRP, OSPF, RIP;

– підтримка протоколів NAT, DHCP, VLAN;

– розширені налаштування безпеки з ACL і підтримкою шифрування SSH.

Вимоги до шлюзу-IoT:

– підтримка Wi-Fi з максимальною кількістю до 32 одночасних підключень;

– мінімум 4 порти Ethernet для можливості дротового підключення IoT-пристроїв;

– підтримка протоколу безпеки WPA, WPA2/-PSK тощо.

2.2 Розробка апаратної частини комп’ютерної системи

2.2.1 Розробка структурної схеми комплексу технічних засобів та специфікації апаратних засобів комп’ютерної системи

Як зазначалося у попередніх пунктах роботи, комп’ютерна мережа компанії “Dnipro-M” повинна бути впроваджена у топологічно віддалених локаціях – компанія складається з головного офісу та віддаленого, у свою чергу головний офіс займає два поверхи орендованої будівлі, віддалений –

один поверх. Відділ служби підтримки займає віддалений офіс, всі інші відділи – головний. З'єднання офісів до Інтернет забезпечується через місцевого провайдера.

Загальна архітектура комп'ютерної мережі компанії "Dnipro-M" представлена у додатку А.

Згідно технічних вимог до комп'ютерної системи, мережа повинна бути поділена на 5 підмереж, згідно кількості відділів компанії. Відділ комерції, повинен додатково поділений на 3 віртуальні підмережі, згідно кількості підрозділів. У системі, на канальному рівні та за типами з'єднань, повинна бути запроваджено Ethernet-мережа. Між маршрутизаторами рівня ядра використовуються Serial-кабелі. Маршрутизатори та комутатори поєднуються між собою за допомогою прямого кабеля, так само як і комп'ютери до комутаторів. Для з'єднання комутаторів один з одним використовується крос-кабель.

За технічними вимогами до функцій, забезпечення та системи в цілому, а також загальною архітектурою (додаток А), необхідно провести наступне розподілення апаратних засобів між структурами компанії та її підмережами, враховуючи перспективи розвитку, розширення та майбутнього масштабування:

– кількість маршрутизаторів у головному офісі – 4, кількість маршрутизаторів у віддаленому офісі – 1;

– служба підтримки, LAN1. Кількість вузлів – 21. Кількість комутаторів: 3;

– фінансовий відділ, LAN2. Кількість вузлів – 72. Кількість комутаторів: 3;

– виконавчий відділ, LAN3. Кількість вузлів – 48. Кількість комутаторів: 2;

– комерційний відділ, LAN4. Кількість комутаторів – 3. Розміщення TFTP-серверу. Розподіл віртуальних підмереж:

а) підрозділ продажів, VLAN 24. Кількість вузлів – 16;

б) підрозділ маркетингу, VLAN 34. Кількість вузлів – 16;

в) підрозділ логістики, VLAN 44. Кількість вузлів – 17;

– IT-відділ, LAN5. Кількість вузлів – 125. Кількість комутаторів: 6. Розміщення HTTP-, DNS-серверів.

IoT-система та всі її компоненти повинні бути забезпечені бездротовим зв'язком Wi-Fi, для цього слід використати бездротовий шлюз-IoT, який обслуговується мережею IT-відділу. Для розширення покриття мережі Wi-Fi слід застосувати бездротову точку доступу, під'єднану до шлюзу Ethernet-кабелем. Підсистеми клімат-контролю представлена мікроконтролерами (з підтримкою Wi-Fi), що оперують настінними нагрівачами, кондиціонерами та зволожувачами, дані збираються за допомогою датчиків вологості та температури, інформація по зміннам виводиться на LCD-монітор та два контрольних діоди (нагрів та охолодження). Кожен поверх головного офісу має окрему систему клімат-контролю з одним набором вищезазначених елементів. У Системі є контроль доступу та безпеки до серверних кімнат: RFID-зчитувачі, веб-камери, датчики руху, смарт-двері. Вікна у робочих кабінетах є «розумними», з віддаленим керуванням. У будівлі головного офісу є комплект датчиків вогню, які при пожежі вмикають сигналізацію.

Згідно результатів аналізу об'єкта впровадження та всіх вищезазначених вимог була розроблена структурна схема комплексу технічних засобів комп'ютерної мережі компанії "Dnipro-M", що показано на рисунку 2.1, умовні позначки до схеми – рисунок 2.2.

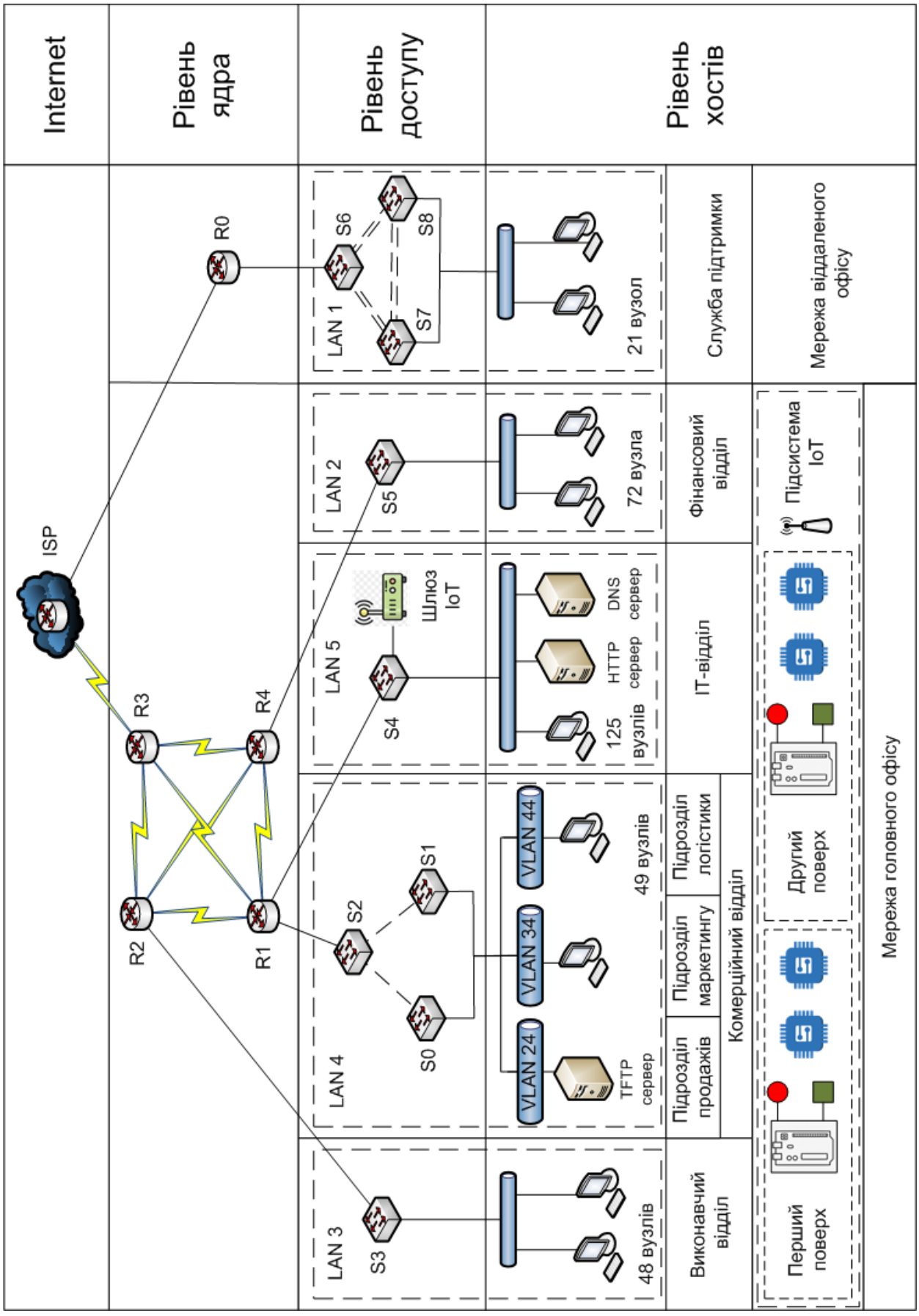

Рисунок 2.1 – Структурна схема комплексу технічних засобів комп’ютерної мережі компанії “Dnipro-M”

Рисунок 2.2 – Умовні позначення до структурної схеми комплексу технічних засобів

Усе мережеве активне обладнання, а також обчислювальні станції, були підібрані згідно результатів аналізу об’єкта впровадження та вимог до технічного забезпечення системи.

Таблиця 2.1 – Специфікація обладнання, використаного при побудові корпоративної мережі компанії “Dnipro-M”

Позиція	Найменування і технічна характеристика	Тим, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1	Маршрутизатор Cisco серії 2900. 3× integrated 10/100/1000 Ethernet ports (RJ-45 only), 1× service module slot, 1× ISM slot, 2× onboard DSP slots, 4× EHWIC slots, 256MB CF default, 512MB DRAM default.	Cisco 2911/K9	од.	5	За структурною схемою: Router Детальні характеристики[9]

Продовження таблиці 2.1.

2	Комутатор Cisco серії Catalyst 2960. 24× Ethernet 10/100 ports, 2× 10/100/1000 TX uplinks, Throughput: 6.5 Mpps, Backplane Capacity: 16 Gbps, DRAM: 16 MB.	Cisco WS-C2960-24TT-L	од.	17	За структурною схемою: Switch Детальні характеристики[10]
3	Стійковий сервер. Процесори: два Intel Xeon Silver 4216 Processor 2.10-3.20 GHz 16-Core, ОЗУ: 8×8 ГБ DDR4-2666, Жорсткий диск: RAID конфігурація SSD 1 ТБ, Мережева карта: GigabitEthernet, ОС: Windows Server 2019.	Cisco UCS C220 M5	од.	3	За структурною схемою: HTTP-, DNS-, TFTP-сервер Детальні характеристики[11]
4	Комп'ютер настільний. Процесор: Intel 6-Core i5-10400 2.9-4.3GHz з Intel UHD Graphics 630, ОЗУ: 8 ГБ DDR4-2666, Жорсткий диск: 240 ГБ SSD, Мережева карта: GigabitEthernet, ОС: Windows 10.	-	од.	315	За структурною схемою: ПК
5	Шлюз-IoT DLC-100. Wi-Fi: 802.11 B/A/G/N/AC 4× Ethernet 100 ports 1× Ethernet 10/100/1000 port	Cisco DLC-100	од.	1	За структурною схемою: Шлюз-IoT

Закінчення таблиці 2.1.

6	Точка доступу CISCO 3702i Wi-Fi: 802.11 B/A/G/N/AC 1× Ethernet 10/100/1000 port	CISCO AIR-CAP3702I-E-K9	од.	1	За структурною схемою: Точка доступу
7	Arduino UNO R4 WiFi	ABX00087	од.	2	За схемою: Мікроконтролер
8	Електронагрівач повітряного опалення, 90 кВт	C-EVN-90-50-90	од.	2	За структурною схемою: Актуатор
9	Кондиціонер зовнішній, 80 кВт	Hitecsa RMXCA	од.	2	
10	Зволожувач повітря, 3 кВт, 30 л/г	Celsis HD-30	од.	2	
11	LED червоний	-	од.	2	
12	LED синій	-	од.	2	
13	LCD-дисплей 128x64	LCD 12864	од.	2	
14	Датчик температури	TMP36	од.	2	За структурною схемою: Датчик
15	Датчик вологості	DHT22	од.	2	
16	Смарт-вікно	QHW QH-YS-220V-3L	од.	7	За структурною схемою: Смарт-девайс IoT
17	Смарт-замок дверей	TTLOCK ONIX WiFi	од.	2	
18	RFID-зчитувач	TF1-EM-W-WIFI	од.	2	
19	Датчик руху (лазерний)	SAFERHOMEE HB-T001Q8	од.	2	
20	Веб-камера 1920x1080, 15 к/с	TP-LINK Tapo C500	од.	4	
21	Датчики вогню	AJAX FireProtect 2	од.	4	
22	Сигналізація	Atis Kit GSM+WiFi 130T	к.	1	

Розгляд структурованої кабельної мережі проведемо на прикладі офісу віддаленої мережі відділу служби підтримки компанії “Dnipro-M”. План розміщення вузлів комп'ютерної системи та спроектовану схему розкладки кабельних мереж представлено на рисунку 2.2.

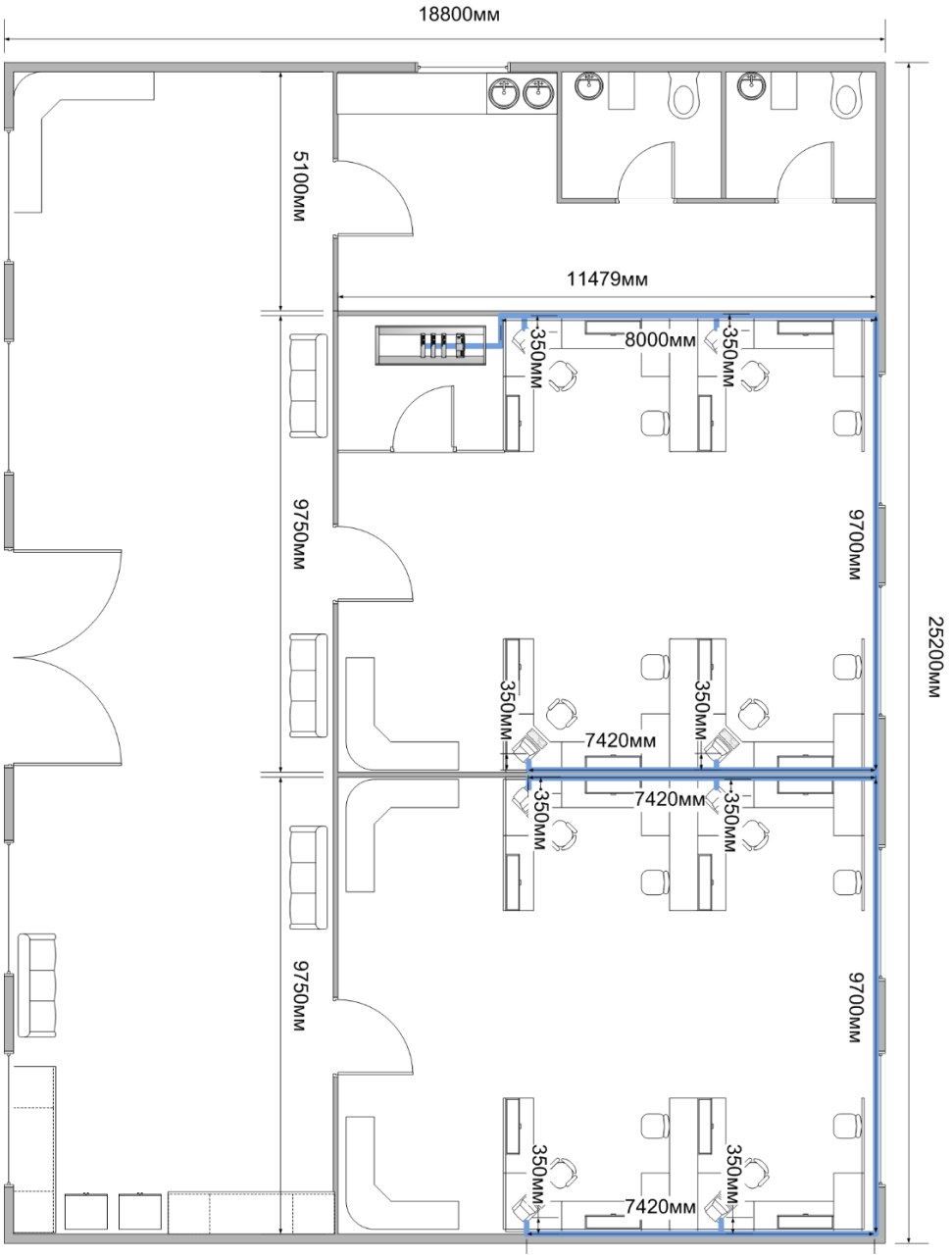

Рисунок 2.2 – Схема розміщення кабельних мереж служби підтримки компанії “Dnipro-M”

Специфікація структурованої кабельної мережі наведена в таблиці 2.2.

Таблиця 2.2 – Специфікація структурованої кабельної мережі

Позиція	Найменування і технічна характеристика	Тим, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1	Кабельний канал 40×16 мм	MK Ega Mini, YT3/D1	м	45	Відповідно проекту, для прокладання витої пари
2	Комп'ютерна розетка RJ45 Cat.5 UTP	Schneider Electric, EPH4300123	од.	21	Відповідно проекту
3	Кабель кручена пара UTP Cat.5E	FinMark 4P 24AWG PE-MR	м	60	Відповідно проекту
4	Кабельний канал 12×12мм	ТМ 220 65663	м	60	Відповідно проекту, для прокладання електропроводки
5	Електрична розетка із заземленням, 16А, 250В	ДКС 76482В	од.	25	Відповідно проекту
6	Провід мідний ПВС 2х2,5 мм²	GalKat GAL0254	м	80	Відповідно проекту

2.2.2 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Найбільша підмережа корпоративної комп'ютерної мережі компанії "Dnipro-M" – це LAN5, кількість персональних комп'ютерів в ній – 125.

За вимогами, середня інтенсивність трафіку складає μ = 167 кадрів/с , а середня довжина повідомлення відповідає стандартним 1500 байт, для кадру Ethernet.

Пропускна здатність лінії, в яку маршрутизується трафік – 1000 Мбіт/с.

Для того, щоб уникнути перенавантаження маршрутизатора, швидкість находження пакетів до нього повинна буде менше швидкості їх відправлення. Розрахуємо максимальний розмір навантаження пакетів:

$$\mu_{\text{вих}} = \frac{1000000000}{1500 * 8} = 83333 \ \frac{\text{пакетів}}{\text{с}}$$

Розрахунок максимальної кількості пристроїв, які можуть бути під'єднані (обслуговуватися) до маршрутизатора:

$$N = \frac{83333 \text{ пакетів/с}}{167 \text{ кадрів/с}} = 499 \text{ пристроїв}$$

Така максимальна кількість повністю задовольняє умови мережі IT-відділу, що складається з 125 комп'ютерів.

Визначимо інтенсивність вихідного трафіку:

$$\lambda = 125 * 167 \frac{\text{кадрів}}{\text{с}} = 20875 \frac{\text{кадрів}}{\text{с}}$$

Визначимо коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu_{\text{вих}}} = \frac{20875}{83333} = 0.25$$

Визначимо коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho} = \frac{0.25}{1-0.25} = 0.33$$

Визначимо середню затримку кадру у черзі:

$$T = \frac{1}{\mu_{\text{вих}} - \lambda} = \frac{1}{83333 - 20875} = 16 \text{ мкс}$$

Визначимо середню довжину черги:

$$L_{\text{черг}} = \frac{\rho^2}{1-\rho} = \frac{0.25^2}{1-0.25} = 0.083$$

Визначимо середній час перебування пакета в черзі:

$$\text{T}_{\text{очік}} = \frac{L_{\text{черг}}}{\lambda} = \frac{0.083}{20875} = 4 \text{ мкс}$$

Пропускну здатність заповненої мережі на канальному рівні знаходимо наступним чином:

$$\text{b} = \lambda * 8 * \ 1500 = 20875 * 8 * 1500 = 250500000 \frac{\text{біт}}{\text{с}} = 250.5 \frac{\text{Мбіт}}{\text{с}}$$

Такі результати затримки, заповненості каналу та пропускної здатності повністю задовольняють встановлені вимоги.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

Відповідно до завдання та поставлених вимог, для проектування корпоративної мережі компанії “Dnipro-M” було надано адресний простір, необхідна кількість підмережі та розподілення кількості вузлів між ними, згідно таблиці 3.1.

Таблиця 3.1 - Блок IP-адрес та кількість вузлів у сегментах мережі

Блок адрес	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
10.24.112.0 /21	21	72	48	49	125

За таблицею та згідно вимог, кількість підмереж розроблюваної Системи повинна складати 5, загальна кількість вузлів у всіх сегментах – 315.

Враховуючи критерії найкращої сумарізації та мінімальної витрати адресного простору, найкращим методом розподілу та розрахунку адресації корпоративної мережі є використання маски змінної довжини – VLSM (Variable Length Subnet Masks). На відміну від методу фіксованої маски, VLSM дозволяє адаптувати підмережі виділеного адресного простору відповідно до конкретної кількості необхідних з’єднань до хостів, що забезпечує більш ефективне використання IP-адрес.

Так як, маска мережі – це двійкове число, яке містить першими одиниці в тих розрядах, які відповідають за визначення адреси мережі, та нулі в розрядах, що відповідають за адреси вузлів, для знаходження маски мережі визначеного розміру необхідно провести бінарне віднімання маски одиничної адреси (255.255.255.255, префікс /32) від значення, що відповідає формулі:

$$h \geq log_2(N+2), \tag{3.1}$$

де h – кількість бітів, що визначає кількість нулів у масці;

$N+2$ – кількість вузлів у мережі, з урахуванням широкомовної та адреси мережі.

Спрощений варіант для визначення префіксу маски m, при використанні 32-бітних адрес:

$$m = 32 - h \tag{3.2}$$

Для запобігання сценарію переповнення адресного простору розподілених підмереж за змінною маскою, необхідно провести резервацію кількості можливих з'єднань у підмережах. Число резервації має бути більшим за суму вузлів (ПК та сервери), принаймні на 10 одиниць, а також враховувати кількість активного мережевого обладнання, яке обслуговує відповідну підмережу.

Для розрахунку за VLSM, пам'ятаючи про адресу та розмір початкового блоку, необхідно розташувати всі сегменти в порядку спадання – таким чином, першою мережею для розподілу виступить LAN5, IT-відділ. Задана за вимогами кількість вузлів вже включає резервацію. Згідно розрахунків за формулою (3.1), кількість бітів маски для адресації вузлів становить 7. Це число відповідає числу бітів які необхідно відсікти від молодших байтів (октетів) загального блоку адреси, та заповнити для визначення діапазону підмережі (що включає широкомовну та адресу підмережі). Діапазон адрес для LAN5 таким чином становить:

10.24.112.0|0000000| - 10.24.112.0|1111111| , або:

10.24.112.0 - 10.24.112.127.

Визначена маска за префіксом /25, розрахованим за формулою (4.2), становить 255.255.255.128. Для визначення наступного номеру адреси, перший невідсічений молодший біт необхідно інкрементувати, тобто номер наступної підмережі становить:

10.24.112.10000000, або 10.24.112.128.

Наступною за розміром підмережа є LAN2, з кількістю вузлів 72. Враховуючи резервацію, за формулою (4.1), кількість бітів адресації вузлів становить 7. Це відповідає масці 255.255.255.128 та префіксу /25. Заповнюючи біти попередньої визначеної адреси отримаємо діапазон: 10.24.112.128 - 10.24.112.255. Адреса наступного доступного блоку починається з 10.24.113.0.

Для розрахунку наступної мережі – LAN4, кількість вузлів 49, при резервації необхідно врахувати, що ця мережа повинна бути додатково поділена на віртуальні підмережі, згідно трьох підрозділів відділу комерції, у якому функціонує LAN4, та додаткової віртуальної мережі для обслуговування пристроїв. Це збільшує потребу у додатковому просторів у 8 адрес до загальної суми резервації. Таким чином кількість «нульових» бітів маски повинно становити 7. Маска для LAN4 – 255.255.255.128, префікс – /25. Діапазон: 10.24.113.0 - 10.24.113.127. Інкрементуємо невідсічений біт та отримуємо адресу наступної мережі – 10.24.113.128.

Мережа LAN3, з необхідним забезпеченням з'єднання для 48 вузлів, за розрахунками згідно формули (3.1) та урахуванням резервації, необхідно відсікти 6 біт від маски з префіксом /32. Отримана маска становить 255.255.255.192, префікс – /26. Діапазон адрес у підмережі LAN3: 10.24.113.128 - 10.24.113.191. Адреса наступної мережі – 10.24.113.192.

Маска останньої, найменшої мережі – LAN1, що повинна обслуговувати 21 вузол, згідно розрахунків використовуючи формули (3.1), (3.2) та правил резервації, становить 255.255.255.224, префікс – /27, бітів адресації вузлів у масці – 5. Діапазон адрес: 10.24.113.192 -10.24.113.223.[12]–[13]

Результати розрахунку адресації комп'ютерної мережі "Dnipro-M" згідно виділеного блоку адрес 10.24.112.0 /21 та методу VLSM, представлені у таблиці 3.2.

Таблиця 3.2 – Схема адресації підмереж “Dnipro-M”

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
LAN1	21	10.24.113.192	255.255.255.224	10.24.113.193	10.24.113.222
LAN2	72	10.24.112.128	255.255.255.128	10.24.112.129	10.24.112.254
LAN3	48	10.24.113.128	255.255.255.192	10.24.113.129	10.24.113.190
LAN4	49	10.24.113.0	255.255.255.128	10.24.113.1	10.24.113.126
LAN5	125	10.24.112.0	255.255.255.128	10.24.112.1	10.24.112.126

Розрахунок мереж, що будуть використані для адресації каналів між маршрутизаторами компанії та між обладнанням провайдера-Інтернет (ISP), буде проводитись за маскою фіксованої довжини. Так як ці мережі повинні забезпечувати адресацію для типу підключення «point-to-point», який у випадку розроблюваної мережі представлений з’єднанням за двома інтерфейсами між маршрутизаторами, найкращою маскою за критерієм мінімальної витрати є 255.255.255.252, префікс /30. Кожний з 4 маршрутизаторів ядра головного офісу за вимогами має бути забезпечений резервними каналами, таким чином кожний маршрутизатор матиме по 3 з’єднанням з іншими. Для адресації каналів між маршрутизаторами ядра головного офісу необхідно використати блок 10.0.14.0/24. Маршрутизатор провайдера надає послуги з’єднання з Інтернет для головного і віддаленого офісів компанії. Для каналу між головним офісом і провайдером слід використати мережу 209.165.202.0/30, між віддаленим офісом і ISP – 64.100.13.0/30. Кінцеві розрахунки для канальних мереж представлені у таблиці 3.3.

Таблиця 3.3 – Схема адресації каналів між маршрутизаторами мережі

Назва мережі	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
CON_1	10.0.14.0	255.255.255.252	10.0.14.1	10.0.14.2
CON_2	10.0.14.4	255.255.255.252	10.0.14.5	10.0.14.6
CON_3	10.0.14.8	255.255.255.252	10.0.14.9	10.0.14.10
CON_4	10.0.14.12	255.255.255.252	10.0.14.13	10.0.14.14
CON_5	10.0.14.16	255.255.255.252	10.0.14.17	10.0.14.18
CON_6	10.0.14.20	255.255.255.252	10.0.14.21	10.0.14.22
ISP_MO	209.165.202.0	255.255.255.252	209.165.202.1	209.165.202.2
ISP_SO	64.100.13.0	255.255.255.252	64.100.13.1	64.100.13.2

3.2 Розрахунок схеми адресації пристроїв

Розрахунок схем адресації локальних та канальних підмереж дозволяє приступити до розподілення IP-адрес між мережевими пристроями, що функціонують у комп'ютерній системі компанії "Dnipro-M". При призначені адрес до пристроїв та інтерфейсів, необхідно притримуватися наступних правил:

– перші можливі для використання IP-адреси призначати інтерфейсам і підінтерфейсам маршрутизаторів у LAN;

– перші можливі для використання адреси повинні бути призначені інтерфейсам і підінтерфейсам маршрутизаторів;

– другі з можливих адрес повинні бути призначені комутаторам;

– серверам повинні бути призначені IP-адреса за правилом: IP-адрес дорівнює першому можливому адресу у мережі+9+14;

– всі інші адреси призначені для кінцевих вузлів.

Згідно вищезазначених правил, були розроблені таблиці схем адресації маршрутизаторів, комутаторів та серверів.

Таблиця 3.4 – Схема адресації інтерфейсів маршрутизаторів

Пристрій	Інтерфейс	IP-адреса	Маска	VLAN	Інтерфейс підключеного пристрою
Yakovlev_Router_1	Gig0/0	10.24.113.193	255.255.255.224	-	Gig0/1
	Gig0/1	64.100.13.2	255.255.255.252	-	Gig0/1
Yakovlev_Router_2	Se0/2/0	10.0.14.9	255.255.255.252	-	Se0/2/0
	Se0/2/1	10.0.14.14	255.255.255.252	-	Se0/2/1
	Se0/3/0	10.0.14.18	255.255.255.252	-	Se0/3/0
	Se0/3/1	209.165.202.1	255.255.255.252	-	Se0/3/1
Yakovlev_Router_3	Se0/2/0	10.0.14.10	255.255.255.252	-	Se0/2/0
	Se0/2/1	10.0.14.6	255.255.255.252	-	Se0/2/1
	Se0/3/0	10.0.14.22	255.255.255.252	-	Se0/3/0
	Gig0/0	10.24.112.129	255.255.255.128	-	Gig0/1
Yakovlev_Router_4	Se0/2/0	10.0.14.2	255.255.255.252	-	Se0/2/0
	Se0/2/1	10.0.14.5	255.255.255.252	-	Se0/2/1
	Se0/3/0	10.0.14.17	255.255.255.252	-	Se0/3/0
	Gig0/0.24	10.24.113.1	255.255.255.224	24	Gig0/1 (Trunk)
	Gig0/0.34	10.24.113.33	255.255.255.224	34	Gig0/1 (Trunk)
	Gig0/0.44	10.24.113.65	255.255.255.224	44	Gig0/1 (Trunk)
	Gig0/0.99	10.24.113.97	255.255.255.240	99	Gig0/1 (Trunk)
	Gig0/1	10.24.112.1	255.255.255.128	-	Gig0/1
Yakovlev_Router_5	Se0/2/0	10.0.14.1	255.255.255.252	-	Se0/2/0
	Se0/2/1	10.0.14.13	255.255.255.252	-	Se0/2/1
	Se0/3/0	10.0.14.21	255.255.255.252	-	Se0/3/0
	Gig0/0	10.24.113.129	255.255.255.192	-	Gig0/1
Yakovlev_Router_ISP	Gig0/0	209.165.201.1	255.255.255.240	-	Fa0
	Gig0/1	64.100.13.1	255.255.255.252	-	Gig0/1
	Se0/3/1	209.165.202.2	255.255.255.252	-	Se0/3/1

Таблиця 3.5 – Схема адресації інтерфейсів комутаторів

Пристрій	Інтерфейс (VLAN)	IP-адреса	Маска	Шлюз
Yakovlev_LAN1_Switch1	SVI 1	10.24.113.194	255.255.255.224	10.24.113.193
Yakovlev_LAN1_Switch2	SVI 1	10.24.113.195	255.255.255.224	10.24.113.193
Yakovlev_LAN1_Switch3	SVI 1	10.24.113.196	255.255.255.224	10.24.113.193
Yakovlev_LAN2_Switch1	SVI 1	10.24.112.130	255.255.255.128	10.24.112.129
Yakovlev_LAN2_Switch2	SVI 1	10.24.112.131	255.255.255.128	10.24.112.129
Yakovlev_LAN2_Switch3	SVI 1	10.24.112.132	255.255.255.128	10.24.112.129
Yakovlev_LAN3_Switch1	SVI 1	10.24.113.130	255.255.255.192	10.24.113.129
Yakovlev_LAN3_Switch2	SVI 1	10.24.113.131	255.255.255.192	10.24.113.129
Yakovlev_LAN4_Switch1	SVI 99	10.24.113.98	255.255.255.240	10.24.113.97
Yakovlev_LAN4_Switch2	SVI 99	10.24.113.99	255.255.255.240	10.24.113.97
Yakovlev_LAN4_Switch3	SVI 99	10.24.113.100	255.255.255.240	10.24.113.97
Yakovlev_LAN5_Switch1	SVI 1	10.24.112.2	255.255.255.128	10.24.112.1
Yakovlev_LAN5_Switch2	SVI 1	10.24.112.3	255.255.255.128	10.24.112.1
Yakovlev_LAN5_Switch3	SVI 1	10.24.112.4	255.255.255.128	10.24.112.1
Yakovlev_LAN5_Switch4	SVI 1	10.24.112.5	255.255.255.128	10.24.112.1
Yakovlev_LAN5_Switch5	SVI 1	10.24.112.6	255.255.255.128	10.24.112.1
Yakovlev_LAN5_Switch6	SVI 1	10.24.112.7	255.255.255.128	10.24.112.1

Таблиця 3.6 – Схема адресації інтерфейсів серверів

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Сервер-HTTP	Fa0	10.24.112.24	255.255.255.128	10.24.112.1	-	Fa0/3
Сервер-DNS	Fa0	10.24.112.25	255.255.255.128	10.24.112.1	-	Fa0/4
Сервер-TFTP	Fa0	10.24.113.24	255.255.255.224	10.24.113.1	24	Fa0/5

3.3 Налаштування моделі комп’ютерної системи

За технічними вимогами до комп’ютерної системи компанії “Dnipro-M”, а також за схемами адресації канальних та локальних підмереж, схемами адресації пристроїв, було створено емуляцію розроблюваної комп’ютерної мережі за допомогою засобів та можливостей програмного забезпечення Cisco Packet Tracer. Результат створення емуляції комп’ютерно системи компанії “Dnipro-M” зображений на рисунку 3.1.

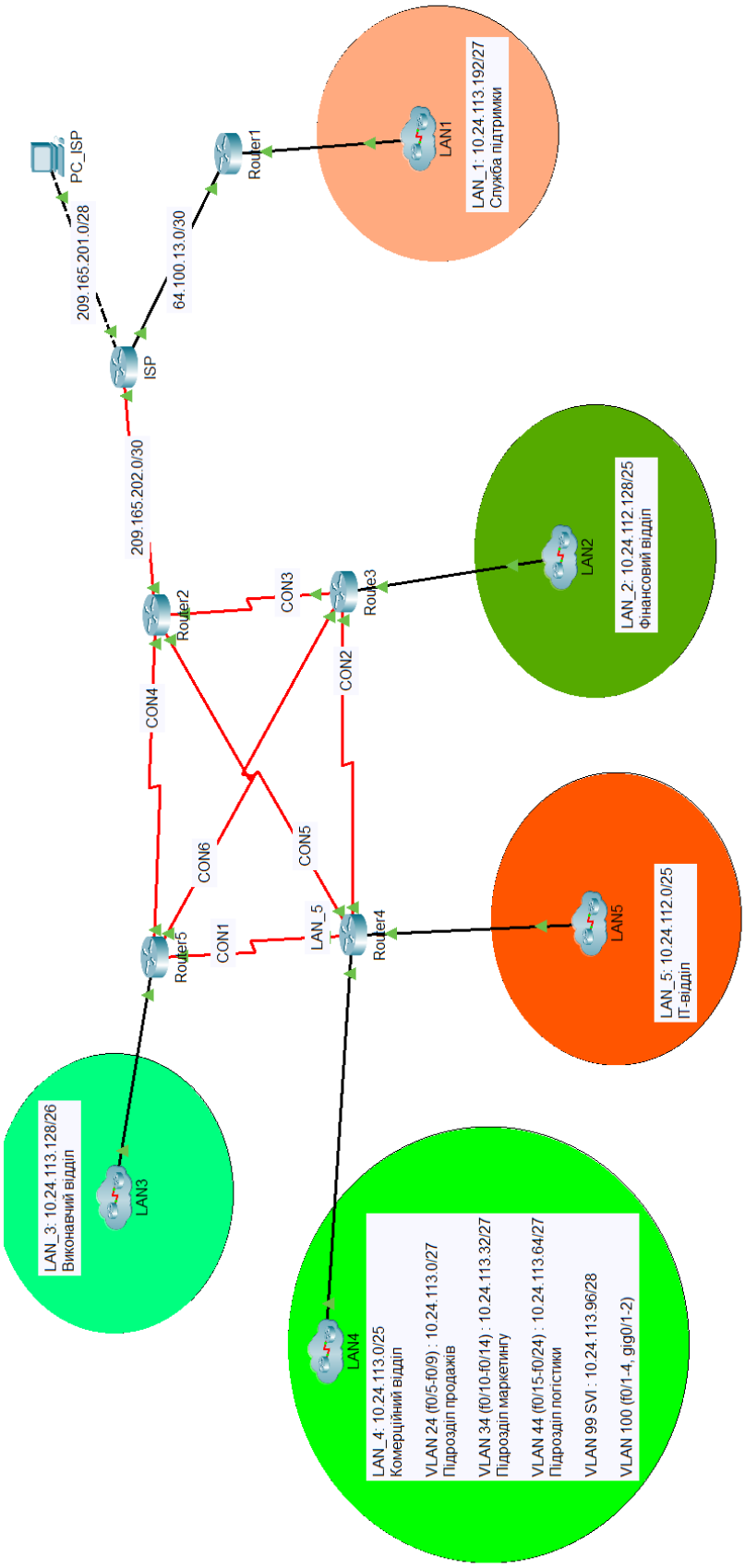

Рисунок 3.1 – Логічна топологія комп’ютерної мережі компанії “Dnipro-M”

3.4 Налаштування роботи комп’ютерної мережі

3.4.1 Базове налаштування конфігурації пристроїв

Для виконання базового налаштування пристроїв, що використовують Cisco IOS, відповідно до вимог щодо безпеки, доступу та ідентифікації, треба скористатися командами описаними нижче. Налаштування проводилось на прикладі граничного (з’єднаний з ISP) маршрутизатора головного офісу.

Доступ до привілейованого режиму та режиму конфігурації відбувається за командами:

```
Router>en
Router#conf t
```

Назва пристрою задається наступною командою:

```
Router(config)#hostname Yakovlev_Router_2.
```

Налаштування на пристроях паролю cisco до консолі і vty, оберемо доступ до 16 ліній віртуальних терміналів:

```
Yakovlev_Router_2(config)#line console 0
Yakovlev_Router_2(config-line)#password cisco
Yakovlev_Router_2(config-line)#login
Yakovlev_Router_2(config-line)#line vty 0 15
Yakovlev_Router_2(config-line)#password  cisco
```

Налаштування паролю class до привілейованого режиму:

```
Yakovlev_Router_2(config-line)#login
Yakovlev_Router_2(config-line)#enable secret class
```

Для забезпечення більшої інформаційної безпеки, паролі що зберігаються у відкритому вигляді зашифруємо:

```
Yakovlev_Router_2(config)#service password-encryption
```

Встановлення банеру MOTD, що буде відображатися при вході до консолі:

```
Yakovlev_Router_2(config)#banner motd #
@ Property of the company Dnipro-M @
Authorized Access Only! #
```

Налаштування використання протоколу ssh на усіх лініях vty:

Yakovlev_Router_2(config)#line vty 0 15

Yakovlev_Router_2(config-line)#transport input ssh

Yakovlev_Router_2(config-line)#login local

Призначення на пристроях локального привілейованого користувача 123201_Yakovlev, з паролем admincisco:

Yakovlev_Router_2(config)#username 123201_Yakovlev privilege 15 secret admincisco

Налаштування домену пристрою:

Yakovlev_Router_2(config)#ip domain-name Yakovlev_Router_2

Для шифрування даних необхідно створити ключ RSA завдовжки 1024 біт [14]:

Yakovlev_Router_2(config)#crypto key generate rsa

The name for the keys will be: Yakovlev_Router_2.Yakovlev_Router_2

How many bits in the modulus [512]: 1024

Для налаштування DCE-інтерфейсів маршрутизаторів спочатку необхідно визначити тип Serial-інтерфейса командою «show controllers **номер_інтерфейса**».

```
Yakovlev_Router_2#show controllers serial 0/3/0
Interface Serial0/3/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 128000
idb at 0x81081AC4, driver data structure at 0x81084AC0
```

Рисунок 3.2 – Визначення типу Serial-інтерфейсу

Задамо на визначених DCE-інтерфейсах маршрутизаторів тактову частоту 128000:

Yakovlev_Router_2(config)#interface Serial0/3/0

Yakovlev_Router_2(config-if)#clock rate 128000

Згідно вимог до розроблюваної мережі, з метою збільшення пропускної здатності і надійності каналів в віддаленій мережі LAN_1 відділу служби

підтримки, на 3 комутаторах цього сегменту необхідно виконати об'єднання фізичних ліній. Для виконання цієї умови скористаємось технологією агрегації EtherChannel, що дозволить об'єднати кілька фізичних каналів Ethernet в один логічний.

Налаштування логічних каналів EtherChannel проведено на прикладі комутатора Yakovlev_LAN1_Switch1. Для конфігурації першого логічного каналу використано порти FastEthernet 21 та 22, для другого – 23 та 24, протокол конфігурації каналів – LACP (Link Aggregation Control Protocol). Команди налаштування одного з логічних каналів [15]:

```
Yakovlev_LAN1_Switch1(config)#interface range fa0/21-22
Yakovlev_LAN1_Switch1(config-if-range)#channel-group 1 mode active
Yakovlev_LAN1_Switch1(config)#interface port-channel 1
Yakovlev_LAN1_Switch1(config-if)#switchport mode trunk
Yakovlev_LAN1_Switch1(config-if)#switchport trunk allowed vlan all
```

3.4.2 Налаштування маршрутизаторів

Маршрутизатори є невід’ємними мережевими компонентами, що забезпечують передачу даних між різними сегментами розподіленої мережі та відповідає за їхнє об’єднання в логічному інформаційному просторі. Об’єднання мереж відбувається з рахунок процесу маршрутизації – знаходження найоптимальнішого шляху передачі пакетів між пристроями. Розрізняють статичну та динамічну маршрутизацію. Налаштування статичної маршрутизація відбувається за рахунок ручного введення адміністраторами маршрутів між мережами, з можливим урахуванням метрики – «ціни» маршруту. Найчастіше такі маршрути використовуються для налаштування шлюзу за замовчуванням та для сталих ділянок мережі.

Динамічна маршрутизація натомість дозволяю автоматизувати процес визначення та оновлення маршрутів. Динамічна маршрутизація підтримується відповідними протоколами. Згідно вимог до мережі, у головному офісі компанії “Dnipro-M” повинен функціонувати протокол динамічної

маршрутизації, що підтримує множинні шляхи, має малий час збіжності і реагування та створює мінімальний службовий трафік. За цими вимогами було обрано протокол EIGRP. Деякі з переваг EIGRP:

– дуже низьке використання мережевих ресурсів під час роботи; у стабільній мережі передаються лише пакети привітання;

– коли відбувається зміна топології, поширюються лише зміни таблиці маршрутизації, а не вся таблиця маршрутизації, що зменшує мережеве навантаження;

– швидкий час конвергенції при змінах у топології мережі;

– для визначення адміністративної відстані, використовується алгоритм розсіяного оновлення (DUAL), що дозволяє оптимізувати пошук найкоротшого шляху.

Згідно схем адресації, описаних у таблицях 3.2 та 3.3, проведемо налаштування маршрутизації у мережі компанії “Dnipro-M”. Налаштування проводилось на прикладі граничного маршрутизатора головного офісу Yakovlev_Router_2. У налаштуваннях необхідно вказати маршрутизатору використовувати протокол маршрутизації EIGRP з ідентифікатором процесу 100 – номер цього процесу необхідно буде використовувати на всіх маршрутизаторах, так як він вказує на єдиний простір розрахунку маршрутів. Проведено оголошення безпосередньо підключених мереж маршрутизатора:

```
Yakovlev_Router_2(config)#router eigrp 100
Yakovlev_Router_2(config-router)#network 10.0.14.8 0.0.0.3
Yakovlev_Router_2(config-router)#network 10.0.14.12 0.0.0.3
Yakovlev_Router_2(config-router)#network 10.0.14.16 0.0.0.3
```

Проведено налаштування маршруту за умовчанням, згідно вимоги до маршрутизатора з прямим підключенням до інтернет-провайдера (ISP), і розповсюджено його через оновлення маршрутизації:

```
Yakovlev_Router_2(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.2
Yakovlev_Router_2(config)#router eigrp 100
```

Yakovlev_Router_2(config-router)#redistribute static

Провайдер, у свою чергу, додав до своїх таблиць статичні маршрути до головного та віддаленого офісу компанії “Dnipro-M”, а також до мереж, що використовуються для NAT.

На граничному маршрутизаторі необхідно налаштувати ручне підсумовування. Для цього необхідно вимкнути автоматичну суму маршрутів та вказати сумарний об’єднаний блок для адрес згідно таблиць 3.2 та 3.3 – це буде адреса 10.0.0.0/8, з ідентифікатором EIGRP на вихідному інтерфейсі (шлюзі):

Yakovlev_Router_2(config)#router eigrp 100

Yakovlev_Router_2(config-router)#no auto-summary

Yakovlev_Router_2(config)#interface Serial0/3/1

Yakovlev_Router_2(config-if)#ip summary-address eigrp 100 10.0.0.0 255.0.0.0

Для налаштування необхідних значень метрик на інтерфейсах маршрутизаторів, задано однакову пропускну спроможність на serial-інтерфейсах, рівну 128 Кб/с:

Yakovlev_Router_2(config)#interface Serial0/3/0

Yakovlev_Router_2(config-if)#bandwidth 128

На маршрутизаторах, які обслуговують локальні мережі відділів компанії “Dnipro-M”, необхідно відключити поширення оновлень маршрутизації на інтерфейси в локальні мережі, а також налаштувати автоматичне призначення IP-адрес вузлам в підмережах – провести конфігурацію сервісу DHCP на роутері. Конфігурація нижче проводилась на маршрутизаторі Yakovlev_Router_4, що обслуговує підмережу LAN5 та підмережу LAN4, яка поділена на віртуальні підмережі (налаштування VLAN розглянуто у відповідному пункті). [16]

Відключення поширення маршрутизації на інтерфейси локальних мереж:

Yakovlev_Router_4(config)#router eigrp 100

Yakovlev_Router_4(config-router)#passive-interface GigabitEthernet0/1

Налаштування DHCP для підмережі LAN5, адреси серверів HTTP та DNS виключені з пулу, проведено резервацію для 10 перших адрес:

```
Yakovlev_Router_4(config)#ip dhcp excluded-address 10.24.112.1 10.24.112.10
Yakovlev_Router_4(config)#ip dhcp excluded-address 10.24.112.24
Yakovlev_Router_4(config)#ip dhcp excluded-address 10.24.112.25
Yakovlev_Router_4(config)#ip dhcp pool poollan5
Yakovlev_Router_4(dhcp-config)#network 10.24.112.0 255.255.255.128
Yakovlev_Router_4(dhcp-config)#default-router 10.24.112.1
Yakovlev_Router_4(dhcp-config)#dns-server 10.24.112.25
```

За вимогами до інформаційної безпеки, необхідно впровадити підтримку служби AAA на всі маршрутизатори. Для реалізації цієї задачі потрібно налаштувати RADIUS-сервер, з відповідним протоколом, що використовується для автентифікації, авторизації та обліку користувачів у комп'ютерних мережах. У ролі надавача послуг сервісу RADIUS було обрано сервер-TFTP. Налаштування сервера представлено на рисунку 3.1.

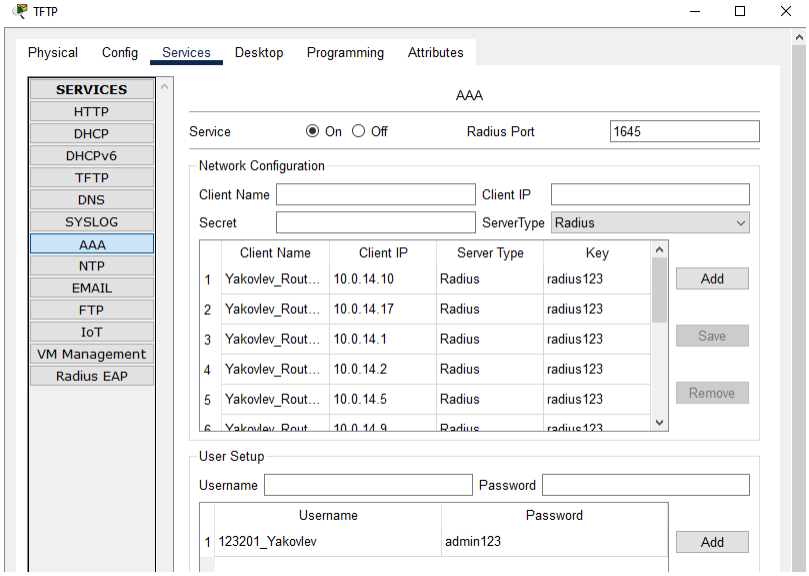

Рисунок 3.3 – Налаштування сервісу AAA-RADIUS

Налаштування маршрутизаторів на підтримку служби AAA-RADIUS, за прикладом конфігурації Yakovlev_Router_4, представлені нижче. Включення служби AAA та конфігурація з'єднання з RADIUS-сервером:

```
Yakovlev_Router_4(config)#aaa new-model
Yakovlev_Router_4(config)#radius-server host 10.24.113.24 auth-port 1645 key radius123
```

Налаштування аутентифікації на основі протоколу RADIUS для доступу до консолі:

```
Yakovlev_Router_4(config)#aaa authentication login console group radius local
Yakovlev_Router_4(config)#line console 0
Yakovlev_Router_4(config-line)#login authentication console
```

Налаштування локальної бази даних AAA для доступу до віртуальних терміналів VTY:

```
Yakovlev_Router_4(config)#aaa authentication login default local
Yakovlev_Router_4(config)#username Yakovlev_Router_4 password admin123
Yakovlev_Router_4(config)#line vty 0 15
Yakovlev_Router_4(config-line)#login authentication default
```

3.4.3 Налаштування роботи Інтернет

Згідно вимог до розроблюваної мережі компанії “Dnipro-M”, головний і відділений офіси компанії повинні мати встановленого одного місцевого провайдера послуг доступу до Інтернет – ISP. За таблицею 3.3, для фізичного з’єднання граничних маршрутизаторів провайдер надав дві мережі «point-to-point»:

– 209.165.202.0/30 – для з’єднання головного офісу і мережі ISP;

– 64.100.13.0/30 – для з’єднання віддаленого офісу і мережі ISP.

Адреси інтерфейсів граничних маршрутизаторів відповідних мереж, згідно таблиці 3.4, попередньо вже були налаштовані як шлюзи за замовчуванням.

Також провайдер надав 2 пули «білих» IP-адрес для впровадження статичного та динамічного NAT у підмережах компанії “Dnipro-M”, що

дозволить доступ до мережі Інтернет і функціонування необхідних серверних рішень:

– 209.165.200.0/27 – для головного офісу;

– 209.165.200.32/27 – для віддаленого офісу.

У головному офісі для налаштування динамічного NAT необхідно використати діапазон 209.165.200.5 – 209.165.200.30. Для статичного NAT використовуються нерозподілений діапазон із пулу, його необхідно застосувати для трансляції адрес серверів компанії.

Таблиця 3.7 – Розподіл глобальних адрес між серверами компанії

Сервер	Глобальна адреса	Локальна адреса
HTTP	209.165.200.4	10.24.112.24
DNS	209.165.200.3	10.24.112.25
TFTP	209.165.200.2	10.24.113.24

Приклад налаштування NAT проводився на граничному маршрутизаторі головного офісу Yakovlev_Router_2. Для впровадження NAT необхідно налаштувати список контролю доступу (ACL), у якому потрібно визначити правила доступу для мереж компанії – встановлено заборону на взаємодію підмереж головного офісу і віддаленого; адресі, визначеній ручним підсумовуванням на шлюзовому порті, дозволено доступ до будь-якої мережі. Команди консолі для конфігурації:

Yakovlev_Router_2(config)#ip access-list extended NAT14

Yakovlev_Router_2(config-ext-nacl)#deny ip 10.24.112.0 0.0.0.127 10.24.113.192 0.0.0.31

Yakovlev_Router_2(config-ext-nacl)#deny ip 10.24.112.128 0.0.0.127 10.24.113.192 0.0.0.31

Yakovlev_Router_2(config-ext-nacl)#deny ip 10.24.113.0 0.0.0.127 10.24.113.192 0.0.0.31

Yakovlev_Router_2(config-ext-nacl)#deny ip 10.24.113.128 0.0.0.63 10.24.113.192 0.0.0.31

Yakovlev_Router_2(config-ext-nacl)#deny ip 10.0.14.0 0.0.0.255 10.24.113.192 0.0.0.31

Yakovlev_Router_2(config-ext-nacl)#permit ip 10.0.0.0 0.255.255.255 any

Створення пулу для динамічної трансляції адрес, за вимогами назва пулу повинна бути «Internet»:

Yakovlev_Router_2(config)#ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224

Для функціонування динамічного NAT необхідно провести прив'язку розробленого списку контролю доступу для трансляції та відповідного пулу «білих» IP-адрес:

Yakovlev_Router_2(config)#ip nat inside source list NAT14 pool Internet

Згідно таблиці 3.7, проведено налаштування статичної трансляції адрес для HTTP-, DNS- та TFTP-серверів:

Yakovlev_Router_2(config)#ip nat inside source static 10.24.112.24 209.165.200.4

Yakovlev_Router_2(config)#ip nat inside source static 10.24.112.25 209.165.200.3

Yakovlev_Router_2(config)#ip nat inside source static 10.24.113.24 209.165.200.2

Для нормального функціонування трансляції адрес потрібно визначити інтерфейси які є внутрішніми (inside) для NAT, а які – є зовнішніми (outside). Всі пакети, які надходять на inside-інтерфейс у внутрішній мережі, будуть транслюватися на зовнішні при виході через outside-інтерфейс. Всі пакети, які надходять на outside-інтерфейс із зовнішньої мережі у внутрішню, будуть транслюватися у локальні адреси. Команди конфігурації інтерфейсів [17]:

Yakovlev_Router_2(config)#interface Serial0/3/0

Yakovlev_Router_2(config-if)#ip nat inside

Yakovlev_Router_2(config)#interface Serial0/3/1

Yakovlev_Router_2(config-if)#ip nat outside

Після впровадження NAT, потрібно налаштувати доступ до сервера HTTP за доменом «http://123.dnipro.ua». Для цього необхідно провести

налаштування прив’язки доменного ім’я до адреси веб-сервера – 209.165.200.4, на DNS-сервері. На самому HTTP-сервері була створена веб-сторінка з відомостями про тему та завдання на кваліфікаційну роботу.

Відділи головного і віддаленого офісу, після налаштування параметрів трансляції адрес, мають доступ до Інтернет. Вони використовують єдиний адресний простір для підмереж, але все ще є віддаленими та розділеними, не існує можливості прямого налаштування маршрутизації між мережами головного та віддаленого офісів. Для вирішення цієї проблеми, необхідно імплементувати «тунелювання трафіку» за технологією VPN.

VPN забезпечуватиме з’єднання між локальними мережами, яке функціонуватиме поверх мережевої інфраструктури Інтернет. Принцип роботи VPN-мереж полягає у створені шифрованого мережевого тунелю – пакети меншого рівня OSI/TCP/IP інкапсулюються у пакети вищого рівня. Так як, інкапсуляція локального трафіку проходить на трансльовані пакети за NAT, це дозволить передавати дані між віддаленими LAN-відділами компанії поверх маршрутизованих пакетів за «білими» IP-адресами. Шифрування вкладених даних забезпечить достатній рівень інформаційної безпеки та конфіденційності.

Згідно вимог, необхідно налаштувати віртуальну приватну мережу site-to-site VPN з використанням протоколу IPsec. Конфігурація проводилась на прикладі Yakovlev_Router_1, що розміщений у віддаленому офісі служби підтримки. Так як, потрібно забезпечити зв’язок між віддаленими відділами компанії “Dnipro-M”, треба створити новий список контролю доступу, який на відміну від «NAT»-списку, повинен дозволяти трафік між локальними підмережами:

Yakovlev_Router_1(config)#ip access-list extended VPN

Yakovlev_Router_1(config-ext-nacl)#permit ip 10.24.113.192 0.0.0.31 10.24.112.0 0.0.0.127

Yakovlev_Router_1(config-ext-nacl)#permit ip 10.24.113.192 0.0.0.31 10.24.112.128 0.0.0.127

Yakovlev_Router_1(config-ext-nacl)#permit ip 10.24.113.192 0.0.0.31 10.24.113.0 0.0.0.127

Yakovlev_Router_1(config-ext-nacl)#permit ip 10.24.113.192 0.0.0.31 10.24.113.128 0.0.0.63

Yakovlev_Router_1(config-ext-nacl)#permit ip 10.24.113.192 0.0.0.31 10.0.14.0 0.0.0.255

Активізація ліцензії шифрування з'єднання IPsec VPN, після якої необхідно перезапустити роутер:

Yakovlev_Router_1(config)#license boot module c2900 technology-package securityk9

Переконавшись в активації модулю безпеки, можна налаштувати політику ISAKMP, для створення та управління ключами IPSec-тунелів, задамо пріоритет політиці 10. Алгоритмом шифрування обрано AES (Advanced Encryption Standard), достатньо потужний та поширений. Метод автентифікації – pre-share, тобто використання взаємного заздалегідь визначеного ключа. Обмін ключами відбувається за протоколом Діффі-Геллмана – параметр ISAKMP group 2. Ключом для з'єднання з головним офісом компанії обрано слово «cisco». Команди:

Yakovlev_Router_1(config)#crypto isakmp policy 10

Yakovlev_Router_1(config-isakmp)#encr aes

Yakovlev_Router_1(config-isakmp)#authentication pre-share

Yakovlev_Router_1(config-isakmp)#group 2

Yakovlev_Router_1(config-isakmp)#crypto isakmp key cisco address 209.165.202.1

Визначення набору трансформацій для IPsec-тунелю – використання AES для шифрування даних; алгоритм HMAC-SHA – для перевірки цілісності даних:

Yakovlev_Router_1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

Налаштування криптографічної карти необхідно для визначення параметрів безпеки та IPsec-тунелю. Потрібно визначити IP-адресу віддаленого з'єднання (peer), набір трансформацій та відповідність адрес перетворення згідно визначеного списку контролю доступу для VPN [18]:

```
Yakovlev_Router_1(config)#crypto map MAP 10 ipsec-isakmp
Yakovlev_Router_1(config-crypto-map)#description VPN connection to Yakovlev_Router_2
Yakovlev_Router_1(config-crypto-map)#set peer 209.165.202.1
Yakovlev_Router_1(config-crypto-map)#set transform-set VPN-SET
Yakovlev_Router_1(config-crypto-map)#match address VPN
```

Призначаємо криптографічну карту до вихідного (з'єднаного з ISP) інтерфейса маршрутизатора віддаленого офісу служби підтримки:

```
Yakovlev_Router_1(config)#interface GigabitEthernet0/1
Yakovlev_Router_1(config-if)#crypto map MAP
```

3.4.4 Захист інформації в комп'ютерній системі. Налаштування віртуалізації VLAN

Захист інформації від несанкціонованого доступу вимагає комплексного підходу до технічних рішень. У попередніх пунктах було описано налаштування автентифікації та авторизації користувачів для доступу до обладнання, налаштовано захищений шифрований канал зв'язку між віддаленими офісами, а також застосовані елементи простого фаєрвол (ACL). Іншим підходом до захисту інформаційних ресурсів є віртуалізація мережевого простору компанії "Dnipro-M" – використання мереж VLAN.

VLAN – це група кінцевих вузлів у комутованій мережі, яка логічно сегментована за функціоналом, та є незалежною від фізичного розташування. VLAN мають ті самі атрибути, що й фізичні локальні мережі, але групування кінцевих вузлів, можливо навіть якщо вони фізично не розташовані в одному сегменті LAN. Будь-який порт комутатора може належати до однієї з існуючих VLAN, і одноадресні, широкомовні та багатоадресні пакети пересилаються та

передаються лише вузлам у цій VLAN. Кожна VLAN вважається такою, якщо пакети надіслані до вузлів, які не належать до цієї VLAN, повинні пересилатися через маршрутизатор.

Згідно вимог до мережі, простір комерційного відділу повинен бути поділений на 3 віртуальні підмережі згідно трьох підрозділів: продажів, маркетингу та логістики. Крім того, необхідно налаштувати віртуальну підмережу для управління мережевим обладнання відділу. Для керування транковими порта (магістральні лінії), які служать для передачі трафіку декількох VLAN через один канал, необхідно призначити Native VLAN з номером 100. Розподіл портів доступу між VLAN представлений у таблиці 3.7

Таблиця 3.8 – Розподіл мереж VLAN

Номер VLAN	Ім’я VLAN	Примітка	Розподіл портів доступу
1	Default	Не використовується	-
24	Sales	Підрозділ продажів	Fa0/5-9
34	Marketing	Підрозділ маркетингу	Fa0/10-14
44	Logistic	Підрозділ логістики	Fa0/15-24
99	Management	Управління обладнанням відділу комерції	SVI99
100	Native	Налаштування транкових (магістральних) каналів	Fa0/1-4, Gig0/1-2

Для розрахунку адресації мереж VLAN скористаємось методом VLSM та поділимо адресний простір відділу комерції, LAN4, згідно таблиці 3.2, за формулами та правилами (3.1), (3.2). Заповнимо відповідну таблицю адресації.

Таблиця 3.9 – Схема адресації мереж VLAN

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону адрес	Кінцеве значення діапазону адрес
VLAN24	17	10.24.113.0	255.255.255.224	10.24.1.1	10.24.1.30
VLAN34	16	10.24.113.32	255.255.255.224	10.24.1.33	10.24.1.62
VLAN44	16	10.24.113.64	255.255.255.224	10.24.1.65	10.24.1.94
VLAN99	4	10.24.113.96	255.255.255.240	10.24.1.97	10.24.1.110

Налаштування проводились на маршрутизаторі Yakovlev_Router_4, що обслуговує відділ комерції. Для функціонування VLAN, необхідно створити 4 підінтерфейса, згідно адрес розподілених віртуальних підмереж та за стандартом інкапсуляції IEEE 802.1Q. Приклад створення підінтерфейсів для VLAN24 та VLAN99:

```
Yakovlev_Router_4(config)#interface GigabitEthernet0/0.24
Yakovlev_Router_4(config-subif)#encapsulation dot1Q 24
Yakovlev_Router_4(config-subif)#ip address 10.24.113.1 255.255.255.224
Yakovlev_Router_4(config)#interface GigabitEthernet0/0.99
Yakovlev_Router_4(config-subif)#encapsulation dot1Q 99
Yakovlev_Router_4(config-subif)#ip address 10.24.113.97 255.255.255.240
```

Далі необхідно налаштувати функціонування сервера DHCP для мереж VLAN на роутері. Потрібно створити пули DHCP з назвами «poolvlan» та відповідним номером, виключити з пулу перші 10 адрес та адреси серверів і для кожного вказати адресу DNS-сервера і шлюз за умовчанням. Приклад налаштування пулу для VLAN24:

```
Yakovlev_Router_4(config)#ip dhcp excluded-address 10.24.113.1 10.24.113.10
Yakovlev_Router_4(config)#ip dhcp excluded-address 10.24.113.24
Yakovlev_Router_4(config)#ip dhcp pool poolvlan24
```

Yakovlev_Router_4(dhcp-config)#network 10.24.113.0 255.255.255.224

Yakovlev_Router_4(dhcp-config)#default-router 10.24.113.1

Yakovlev_Router_4(dhcp-config)#dns-server 10.24.112.25

Налаштування комутатора для розподілу VLAN, проводилось на прикладі Yakovlev_LAN4_Switch1. Приклад створення та призначення імені для віртуальних підмереж підрозділу продажів та Native, згідно таблиці 3.8, на комутаторі:

Yakovlev_LAN4_Switch1(config)#vlan 24

Yakovlev_LAN4_Switch1(config-vlan)#name Sales

Yakovlev_LAN4_Switch1(config)#vlan 100

Yakovlev_LAN4_Switch1(config-vlan)#name Native

Згідно таблиці 3.8, проведено налаштування розподілу портів доступу комутатора за VLAN, на прикладах віртуальних підмереж підрозділів продажів та логістики:

Yakovlev_LAN4_Switch1(config)#interface range FastEthernet0/10-14

Yakovlev_LAN4_Switch1(config-if-range)#switchport mode access

Yakovlev_LAN4_Switch1(config-if-range)#switchport access vlan 34

Yakovlev_LAN4_Switch1(config)#interface range FastEthernet0/15-24

Yakovlev_LAN4_Switch1(config-if-range)#switchport mode access

Yakovlev_LAN4_Switch1(config-if-range)#switchport access vlan 44

Порти, які необхідно налаштувати на транковий режим, повинні допускати пересилання пакетів визначених вище віртуальних підмереж та були призначенні до відповідної магістральної VLAN [19]:

Yakovlev_LAN4_Switch1(config)#interface range FastEthernet0/1-4, GigabitEthernet0/1-2

Yakovlev_LAN4_Switch1(config-if-range)#switchport mode trunk

Yakovlev_LAN4_Switch1(config-if-range)#switchport trunk native vlan 100

Yakovlev_LAN4_Switch1(config-if-range)#switchport trunk allowed vlan 24, 34, 44, 99, 100

Згідно вимог до мережі та таблиці розподілу інтерфейсів для серверів 3.6, на портах комутаторів, підключених до серверів, необхідно налаштувати функцію безпеки згідно правил:

– тільки двом унікальним пристроям був дозволений доступ до порту;

– MAC-адрес пристрою розпізнавався динамічно і додавався в поточну конфігурацію;

– під час порушенні системи безпеки з’являлося повідомлення, а порт залишався включеним.

Проведено налаштування безпеки портів, на прикладі комутатора Yakovlev_LAN4_Switch3 та під’єднаного TFTP-сервера до нього, згідно вищезазначених правил:

```
Yakovlev_LAN4_Switch3(config)#interface FastEthernet0/5
Yakovlev_LAN4_Switch3(config-if)#switchport port-security
Yakovlev_LAN4_Switch3(config-if)#switchport port-security maximum 2
Yakovlev_LAN4_Switch3(config-if)#switchport port-security violation restrict
Yakovlev_LAN4_Switch3(config-if)#switchport port-security mac-address sticky
```

3.5 Перевірка роботи комп’ютерної системи

Для перевірки базового налаштування та налаштування служби AAA, спробуємо з’єднатися до віртуального терміналу Yakovlev_Router_4 з ПК однієї із підмереж за протоколом SSH.

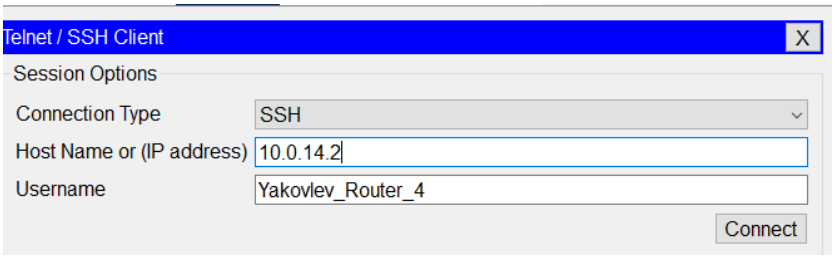

Рисунок 3.4 – Відкриття сесії SSH до Yakovlev_Router_4

Доступ до віртуальної лінії маршрутизатора Yakovlev_Router_4 відбувається лише за локальною базою даних облікових записів AAA та

визначеним паролем «admin123». Доступ до привілейованого режиму лише за паролем «class». Виконавши команду «show run», можна побачити що ім'я пристрою змінено, всі паролі зашифровані, назначений банер MOTD тощо.

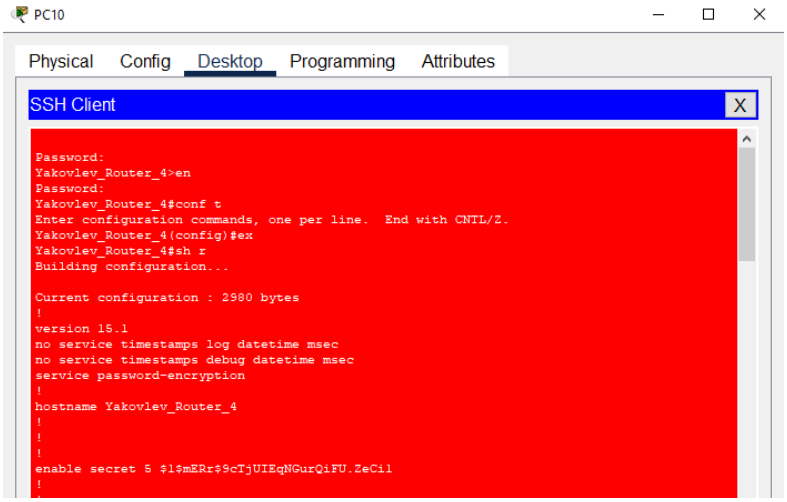

Рисунок 3.5 – Перегляд активної конфігурації для перевірки базових налаштувань

Для перевірки EtherChannel в LAN1, виконаємо команду «show etherchannel port-channel» на комутаторі Yakovlev_LAN1_Switch1.

```
Group: 1
----------
               Port-channels in the group:
               ---------------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 00d:02h:52m:28s
Logical slot/port   = 2/1       Number of ports = 2
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/22   Active             0
  0     00     Fa0/21   Active             0
Time since last port bundled:    00d:02h:52m:28s    Fa0/21
```

Рисунок 3.6 – Активна група агрегованого каналу на комутаторі LAN1

Перевірка маршрутизації за протоколом EIGRP проводиться виконання команди «show ip route» на одному із маршрутизаторів мережі головного офісу, нехай це буде граничний маршрутизатор Yakovlev_Router_2, який також має статичний маршрут шлюзу за замовчуванням. Пропінгуємо

комп’ютери різних LAN для перевірки фактичної передачі даних між вузлами різних підмереж .

```
Yakovlev_Router_2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 16 subnets, 6 masks
D       10.0.14.0/30 [90/21024000] via 10.0.14.13, 02:55:48, Serial0/2/1
                     [90/21024000] via 10.0.14.17, 02:55:47, Serial0/3/0
D       10.0.14.4/30 [90/21024000] via 10.0.14.17, 02:55:48, Serial0/3/0
                     [90/21024000] via 10.0.14.10, 02:55:46, Serial0/2/0
C       10.0.14.8/30 is directly connected, Serial0/2/0
L       10.0.14.9/32 is directly connected, Serial0/2/0
C       10.0.14.12/30 is directly connected, Serial0/2/1
L       10.0.14.14/32 is directly connected, Serial0/2/1
C       10.0.14.16/30 is directly connected, Serial0/3/0
L       10.0.14.18/32 is directly connected, Serial0/3/0
D       10.0.14.20/30 [90/21024000] via 10.0.14.13, 02:55:48, Serial0/2/1
                      [90/21024000] via 10.0.14.10, 02:55:46, Serial0/2/0
D       10.24.112.0/25 [90/20512256] via 10.0.14.17, 02:55:48, Serial0/3/0
D       10.24.112.128/25 [90/20512256] via 10.0.14.10, 02:55:46, Serial0/2/0
D       10.24.113.0/27 [90/20514560] via 10.0.14.17, 02:55:48, Serial0/3/0
D       10.24.113.32/27 [90/20514560] via 10.0.14.17, 02:55:48, Serial0/3/0
D       10.24.113.64/27 [90/20514560] via 10.0.14.17, 02:55:48, Serial0/3/0
D       10.24.113.96/28 [90/20514560] via 10.0.14.17, 02:55:48, Serial0/3/0
D       10.24.113.128/26 [90/20512256] via 10.0.14.13, 02:55:48, Serial0/2/1
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/30 is directly connected, Serial0/3/1
L       209.165.202.1/32 is directly connected, Serial0/3/1
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Рисунок 3.7 – Таблиця маршрутизації граничного роутера Yakovlev_Router_2

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:63FF:FE41:8E9D
   IPv6 Address.....: ::
   IPv4 Address.....: 10.24.112.140
   Subnet Mask.....: 255.255.255.128
   Default Gateway.....: ::
                                 10.24.112.129

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

C:\>ping 10.24.113.140

Pinging 10.24.113.140 with 32 bytes of data:

Request timed out.
Reply from 10.24.113.140: bytes=32 time=13ms TTL=126
Reply from 10.24.113.140: bytes=32 time=2ms TTL=126
Reply from 10.24.113.140: bytes=32 time=13ms TTL=126

Ping statistics for 10.24.113.140:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 13ms, Average = 9ms
```

Рисунок 3.8 – Виконання команди «ping» між комп’ютерами підмереж LAN2 та LAN3

Для перевірки справності роботи DHCP-сервісів, необхідно у налаштуваннях вузлів-ПК обрати відповідний пункт та дочекатися призначення IP-адреси від роутера.

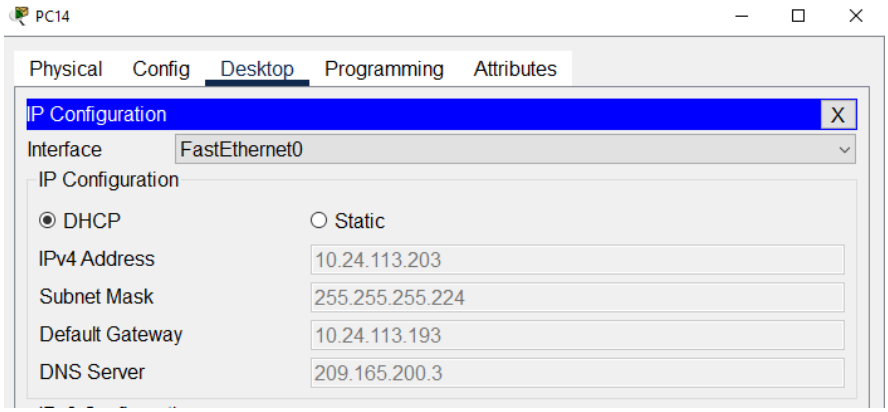

Рисунок 3.9 – Успішне призначення адреси за DHCP

Для перевірки налаштування NAT та сервісів HTTP та DNS, необхідно спробувати зайти на веб-сторінку компанії із віддаленого вузла провайдера. Після успішного входу необхідно продивитись таблиці трансляцій адрес.

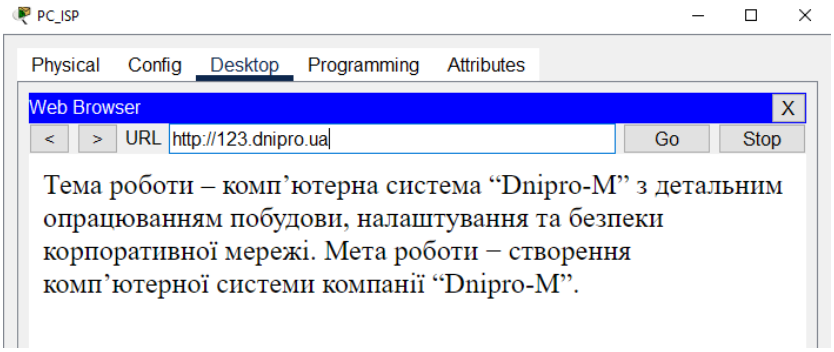

Рисунок 3.10 – Успішне встановлення з'єднання з вузлами у Інтернет за допомогою NAT

```
Yakovlev_Router_2#show ip nat tr
Pro  Inside global     Inside local       Outside local      Outside global
udp 209.165.200.3:53   10.24.112.25:53    209.165.201.5:1025 209.165.201.5:1025
---  209.165.200.2     10.24.113.24       ---                ---
---  209.165.200.3     10.24.112.25       ---                ---
---  209.165.200.4     10.24.112.24       ---                ---
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1024 209.165.200.5:1024
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1025 209.165.200.5:1025
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1026 209.165.200.5:1026
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1027 209.165.200.5:1027
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1028 209.165.200.5:1028
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1029 209.165.200.5:1029
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1030 209.165.200.5:1030
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1031 209.165.200.5:1031
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1032 209.165.200.5:1032
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1033 209.165.200.5:1033
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1034 209.165.200.5:1034
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1035 209.165.200.5:1035
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1036 209.165.200.5:1036
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1037 209.165.200.5:1037
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1038 209.165.200.5:1038
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1039 209.165.200.5:1039
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1040 209.165.200.5:1040
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1041 209.165.200.5:1041
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1042 209.165.200.5:1042
tcp 209.165.200.3:3100010.24.112.25:31000 209.165.200.5:1043 209.165.200.5:1043
```

Рисунок 3.11 – Таблиця трансляцій адрес зі статичними записами та записами динамічного NAT

Перевірка встановлення та функціонування VPN-мережі між віддаленим та головним офісами компанії “Dnipro-M” поверх Інтернет, відбувається шляхом пінгування локальних адрес цих офісів, які не маршрутизуються провайдером. На граничних маршрутизаторах, для перевірки VPN-тунелю необхідно використати команду «show crypto ipsec sa».

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.24.112.139

Pinging 10.24.112.139 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.24.112.139: bytes=32 time=2ms TTL=125
Reply from 10.24.112.139: bytes=32 time=2ms TTL=125

Ping statistics for 10.24.112.139:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2D0:58FF:FE0C:9444
   IPv6 Address.....: ::
   IPv4 Address.....: 10.24.113.204
   Subnet Mask.....: 255.255.255.224
   Default Gateway.....: ::
                                 10.24.113.193
```

Рисунок 3.12 – Виконання команди пінг між вузлами віддаленого та головного офісів

```
local  ident (addr/mask/prot/port): (10.24.112.128/255.255.255.128/0/0)
remote  ident (addr/mask/prot/port): (10.24.113.192/255.255.255.224/0/0)
current_peer 64.100.13.2 port 500
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

  local crypto endpt.: 209.165.202.1, remote crypto endpt.:64.100.13.2
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/1
  current outbound spi: 0xC28E7AF9(3264117497)

  inbound esp sas:
   spi: 0x97F16326(2549179174)
     transform: esp-aes esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 2004, flow_id: FPGA:1, crypto map: MAP
     sa timing: remaining key lifetime (k/sec): (4525504/3464)
     IV size: 16 bytes
     replay detection support: N
     Status: ACTIVE
```

Рисунок 3.13 – Перевірка шифрованого VPN-тунелю між офісами

Роботу віртуальних підмереж можна перевірити командою «show vlan brief» на одному із комутаторів розділеною віртуалізацією підмережі. Фактично для перевірки правильності налаштування VLAN, а також для перевірки пулів DHCP для віртуальних підмереж, продивимось призначену адресу за DHCP трьох вузлів, які під'єднані до різних за тегуванням розподільчих портів комутаторів.

```
Yakovlev_LAN4_Switch3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Gig0/1
                                                Gig0/2
24   Sales                            active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9
34   Marketing                        active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14
44   Logistic                         active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
99   Management                       active
100  Native                           active
```

Рисунок 3.14 – Розподіл портів доступу комутатора між VLAN

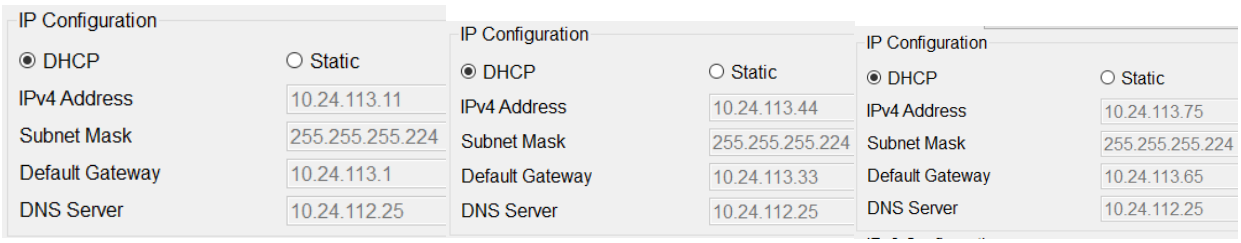

Рисунок 3.15 – Призначенні адреси вузлів, що з'єднані до одного комутатора, відповідають схемі адресації VLAN

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Технічні рішення реалізації IoT-компонента системи

Інтернет речей (IoT) – це концепція мереж, за допомогою яких фізичні об'єкти, від пристроїв побутового використання до великих промислових систем, з'єднані мережевим обладнанням, що дозволяє збирати та обмінюватися даними. Основна ідея полягає в тому, що пристрої IoT можуть бути "розумними" та автономними, тобто здатними збирати інформацію, аналізувати її та реагувати на зміни в реальному часі без прямої людської участі. Основні компоненти IoT:

– датчики: це електронні пристрої, які відстежують певні параметри та перетворюють їх у сигнали, якими можуть оперувати інші компоненти IoT;

– з’єднання: необхідне забезпечення безперебійної комунікації між пристроями, найчастіше це бездротові технології;

– обробка даних: це процес збору, аналізу та обробки інформації, яку надсилають датчики; зазвичай використовуються хмарні та туманні обчислення;

– додатки: програмне забезпечення, яке використовує оброблені дані для маніпуляції виконавчими пристроями IoT та відображення станів системи.[2]

У рамках розробки IoT-компонента комп’ютерної мережі компанії “Dnipro-M” була спроєктована система, що забезпечую клімат-контроль та безпеку на двох поверхах головного офісу. Розроблена систем ділиться на два концептуальних рішення:

– туманні (Edge) обчислення. Контроль температури та вологості відбувається двома мікроконтролерами (розподіленими між поверхами), які керують виконавчими керованими пристроями: електронагрівачі, кондиціонери та зволожувачі повітря; дані збирають від датчиків температури та вологості. Для кожного поверху головного офісу комплект наборів датчиків

та актуаторів є індивідуальним. Такий тип обчислення дозволяє зменшити час відгуку системи та полегшити навантаження на сервери, а сама система клімат-контролю забезпечить достатній рівень комфорту праці та ефективного енергоспоживання;

– хмарні обчислення. На IoT-сервер компанії “Dnipro-M” покладається контроль за: системами безпеки серверних кімнат, що включають правила контролю доступу за RFID-картками, а також відеоспостереження за порушниками цих правил; реалізація протипожежної сигналізації; контроль за "розумними"-вікнами та іншими смарт-девайсами.

Зв'язок та управління між компонентами IoT-системи здійснюється через бездротову мережу Wi-Fi. Для забезпечення бездротового покриття використовується шлюз-IoT DLC100 та точка доступу, що розширює зону мережі Wi-Fi.

Управління та контроль за IoT-системою здійснюється через веб-інтерфейс «IoT-Monitor». Підсистема клімат-контролю керується скриптом розробленим під архітектуру мікроконтролера.

4.2 Налаштування з’єднання IoT-компоненті та сервісів

Для збору та обробки даних IoT-системи, а також для реалізації хмарних обчислень Інтернету речей у комп’ютерній системі компанії “Dnipro-M”, необхідно налаштувати відповідний веб-орієнтований сервіс. Було прийнято рішення використати обчислювальні можливості DNS-сервера, як найменш навантаженої обчислювальної машини, у порівняні з іншими серверами. На сервері необхідно увімкнути функцію «IoT», а адміністратору мережі “Dnipro-M” налаштувати обліковий запис «admin» з паролем «admin». У налаштуваннях DNS-сервісу потрібно додати запис-прив’язку домену «iot.123.dnipro.ua» до адреси 209.165.200.3, таким чином спрощено доступ IoT-сервісу.

Налаштування бездротової мережі необхідно починати з конфігурації бездротового маршрутизатора (шлюзу). Так як мережа IoT та її компоненти обслуговуються IT-відділом, згідно вимог, маршрутизатор повинен мати адресу інтерфейсу «Internet», що належить до простору LAN5 – виділено адресу із пулу резервації – 10.25.112.10. За вимогами до налаштувань IoT-системи, для її адресації необхідно використати блок 10.24.114.1/24. Розроблено таблицю 4.1 основних параметрів налаштувань шлюзу-IoT, згідно технічних вимог до розроблюваної мережі. Параметри безпеки бездротової мережі повторені на точці доступа, яка з'єднана зі шлюзом Ethernet-кабелем за першим інтерфейсом для локальної мережі.

Таблиця 4.1 – Налаштування бездротового маршрутизатора

Параметр	Значення
Назва пристрою	DniproM_IoT
IP-адреса локальної мережі шлюзу-IoT	10.24.114.1/24
IP-адреса порту «Internet»	10.24.112.10/25
Шлюз за замовчуванням	10.24.112.1/25
SSID бездротової мережі	Yakovlev_IoT
Метод автентифікації та шифрування	WPA2-PSK/AES
Ключ автентифікації (пароль) для підключення до мережі	yakovlev123

Згідно таблиці, проведено налаштування шлюзу DniproM_IoT, результати на рисунках 4.1.

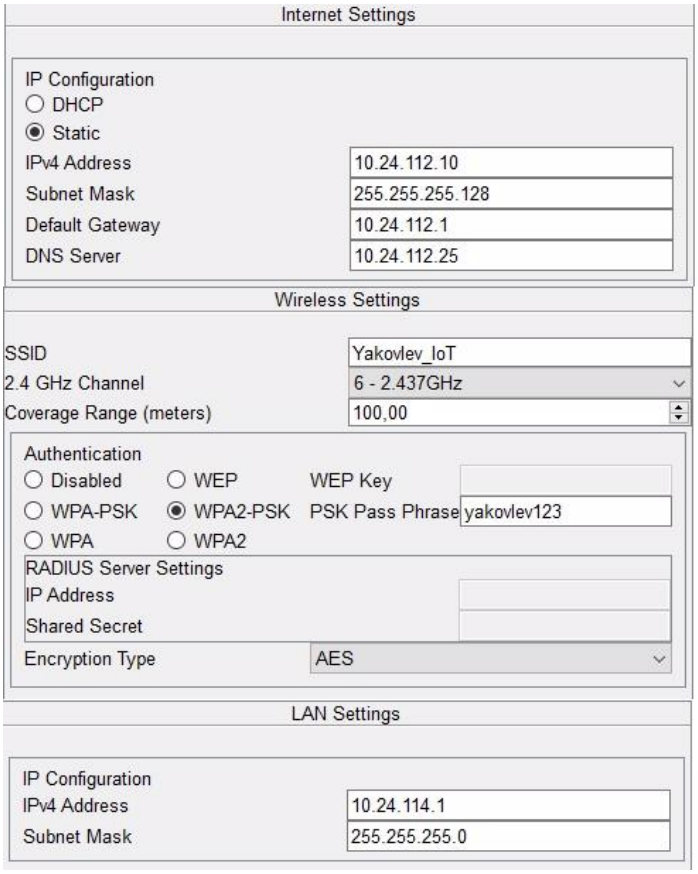

Рисунок 4.1 – Налаштування шлюзу DniproM_IoT

Для можливості об’єднання набору «розумних» IoT-пристроїв та компонентів у одну об’єднану мережу, необхідно переконатися у тому що вони підтримують можливість передачі даних за Wi-Fi. До плат мікроконтролерів та розумних пристроїв необхідно додати модуль бездротового зв’язку PT-IOT-NM-1W. Крім того, було прийнято рішення застосувати кабельне Ethernet-з’єднання для відеоспостереження за серверними кімнатами – переконатися у наявності Ethernet-інтерфейсу на веб-камерах та провести підключення до вільних слотів шлюзу-IoT. При фізичному підключенню модулів та кабелів до IoT-пристроїв потрібно дотримуватись вимог до техніки безпеки, визначеними технічними вимогами до поводження з електрообладнанням.

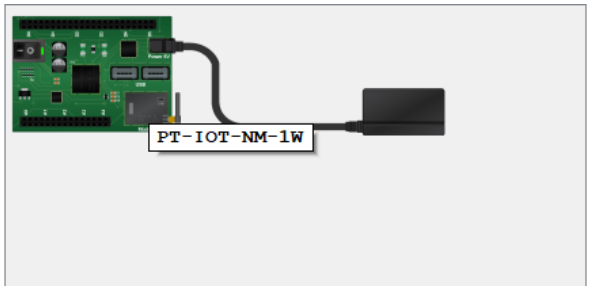

Рисунок 4.2 – Приєднанання модулю бездротового зв’язку

У вікні налаштувань інтерфейсу бездротового модуля IoT-пристроїв необхідно встановити параметри бездротової мережі згідно таблиці 4.1.

У мережевих конфігураціях IoT-пристроїв та плат мікроконтролерів потрібно налаштувати отримання IP-адреси за протоколом DHCP. Надати назви пристроям згідно їх функціоналу та розміщення. Далі обрати сервер реєстрації пристроїв та збереження даних IoT. Для даної моделі мережі обрано параметр Remote Server, задано адресу серверу IoT та параметри автентифікації до відповідного веб-сервісу: адреса – 209.165.200.3, обліковий запис – логін «admin», пароль «admin». Приклад на рисунку 4.3.

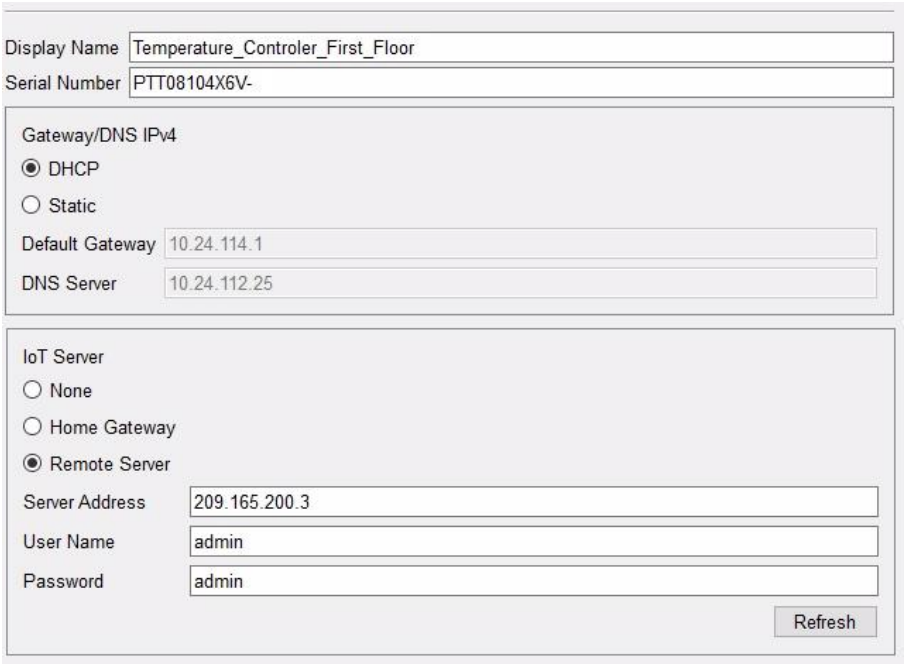

Рисунок 4.3 – Приклад конфігурації IoT-пристрою

IoT-компоненти туманних обчислень, а саме сенсори та актуатори, було об’єднано з платою мікроконтролера (MCU), застосовуючи кабель IoT Custom Cable. Схему підключення пристроїв та розподіл портів вводу/виводу наведено у таблиці 4.2. Дана схема розподілу застосовується на підсистемах клімат-контролю обох поверхів для обох плат.

Таблиця 4.2 – Схема підключення компонентів MCU

Пристрій	Вхід	Тип входу	Напрям
Temperature_Sensor	A0	Аналоговий	IN(Вхід)
Humiture_Sensor	A1	Аналоговий	IN(Вхід)
LCD_Temperature (LCD-екран)	D0	Дискретний	OUT(Вихід)
Heat (електрообігрівач)	D1	Дискретний	OUT(Вихід)
Cooler (кондиціонер)	D2	Дискретний	OUT(Вихід)
Heat_LED	D3	Дискретний	OUT(Вихід)
Cooler_LED	D4	Дискретний	OUT(Вихід)
Humidifier (зволожувач)	D5	Дискретний	OUT(Вихід)

Загальна схема логічної топології IoT-пристроїв у розроблюваному компоненті представлена на рисунку 4.4.

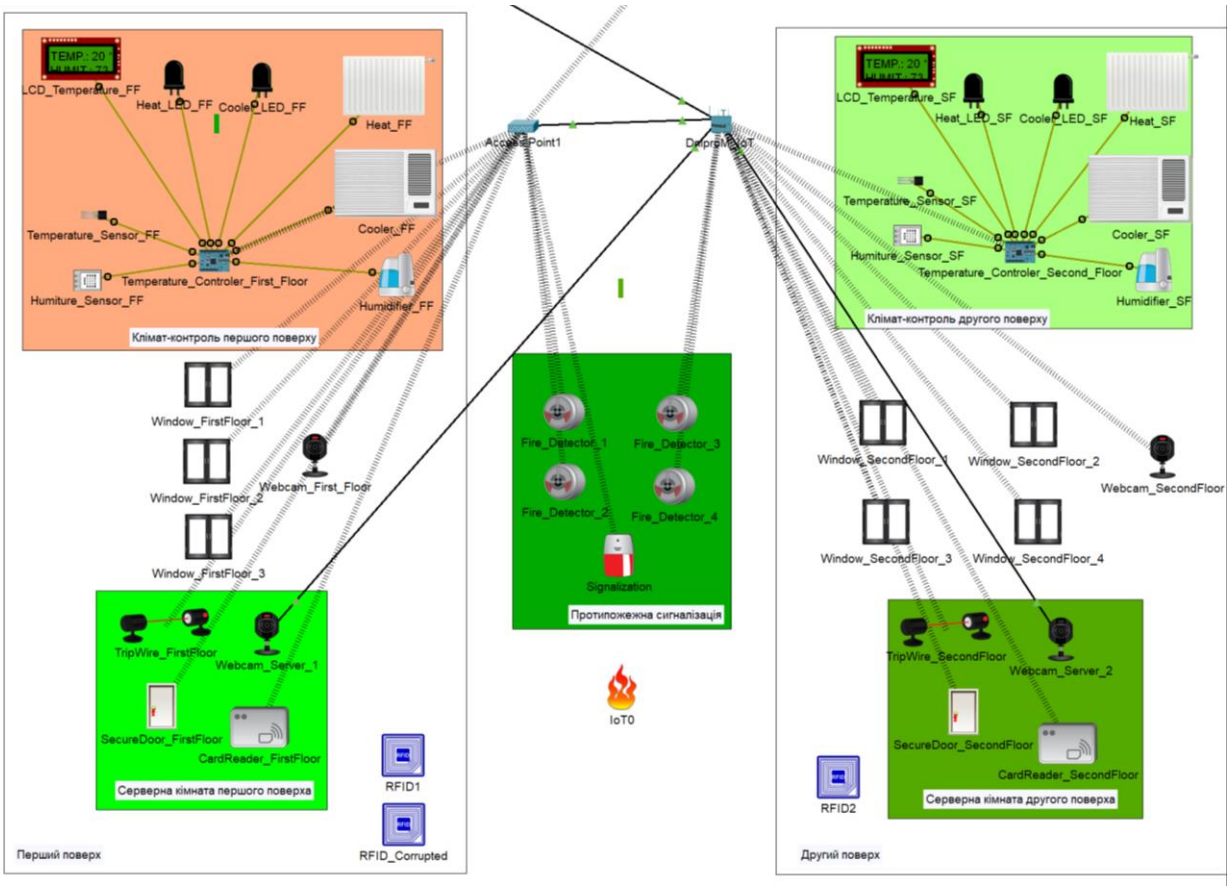

Рисунок 4.4 – Мережева топологія IoT-системи

4.3 Налаштування та перевірка підсистеми клімат-контролю

Туманні обчислення клімат-контролю забезпечуються платами мікроконтролерів (MCU), які виконують управління виконавчими пристроями за параметрами датчиків, забезпечуючи локальну обробку даних та прийняття рішень на місці.

Так як, вже було проведена фізична компоновка систем, для наступних налаштувань IoT-підсистеми клімат-контролю необхідно, за технічними вимогами, запрограмувати плати за допомогою мови Python та необхідних пакетів і бібліотек до неї для неперервного читання значень датчиків і запису на виконавчі елементи, керовані умовною логікою.

За вимогами керівництва компанії та побажань працівників, потрібно підтримувати температуру у кабінетах головного офісу на рівні від 20 до 25 градусів по Цельсію та відносної вологості 60.

Згідно таких вимог, було підібрані оптимізовані параметри та розроблено алгоритм задач, які повинна виконувати програма: за температури нижче 15°C буде вмикатися лише опалення, у діапазоні від 20 до 25°C всі виконавчі прилади будуть вимкненими, вище 25°C – вмикається лише кондиціонер; якщо вологість нижче 60 – вмикається зволожувач, у протилежному випадку – вимикається; інформація по станам кондиціонерів та обігрівачів (вимкнено/увімкнено) відображається на щитку контрольної плати за допомогою синього та червоного світлодіодів відповідно; цифрові показники датчиків виводити на LCD-екран, розміщеному та щитку; показники датчиків та стани актуаторів виводити на веб-інтерфейс IoT-сервісу.

Через віртуальний програматор плат мікроконтролерів, було записано у пам’ять та запущено на виконання код скрипта Python, який визначатиме поведінку IoT-компонентів згідно описаного текстового алгоритму. Текст програми представлений у додатку Б.

При розробці коду було використано бібліотеку веб-API IoEClient, що надає можливість надсилати дані до сервера. Під час програмування для віддаленого моніторингу та керування використано функції бібліотеки:

– IoEClient.setup(api) налаштовує API для віддаленого моніторингу та керування з сервера IoT. Аргументом функції виступають JSON-записи(states), що описують порядок виведення графічних елементів на сторінці керування IoT. Були реалізовані 5 записів, що описують: цифрові значення температури та вологості, стани обігрівача, кондиціонера та зволожувача.

– IoEClient.reportStates(states) повідомляє про стани пристрою серверу IoT. Аргумент – це рядок, який представляє всі стани цього пристрою. Кількість станів має відповідати кількості записів-states у функції IoEClient.setup().

У коді для зчитування температури та вологості на датчиках застосовано функцію analogRead() – перетворює вхідну напругу аналогового входу у

діапазоні 0-5 В у цілі значення діапазону від 0 до 1023 відповідно. Для взаємодії з актуаторами використано digitalWrite(), що надсилає значення увімкнено/вимкнено на цифровий вихід. Для виведення інформації на LCD-дисплей використано customWrite(), аргументом виступає рядковий тип даних.

Перевірка підсистеми клімат-контролю проводилась у середовищі та засобами Cisco Packet Tracer, з урахуванням можливості налаштування параметрів емуляції стану атмосферних показників. Результати перевірки представлені на рисунках 4.5–4.7.

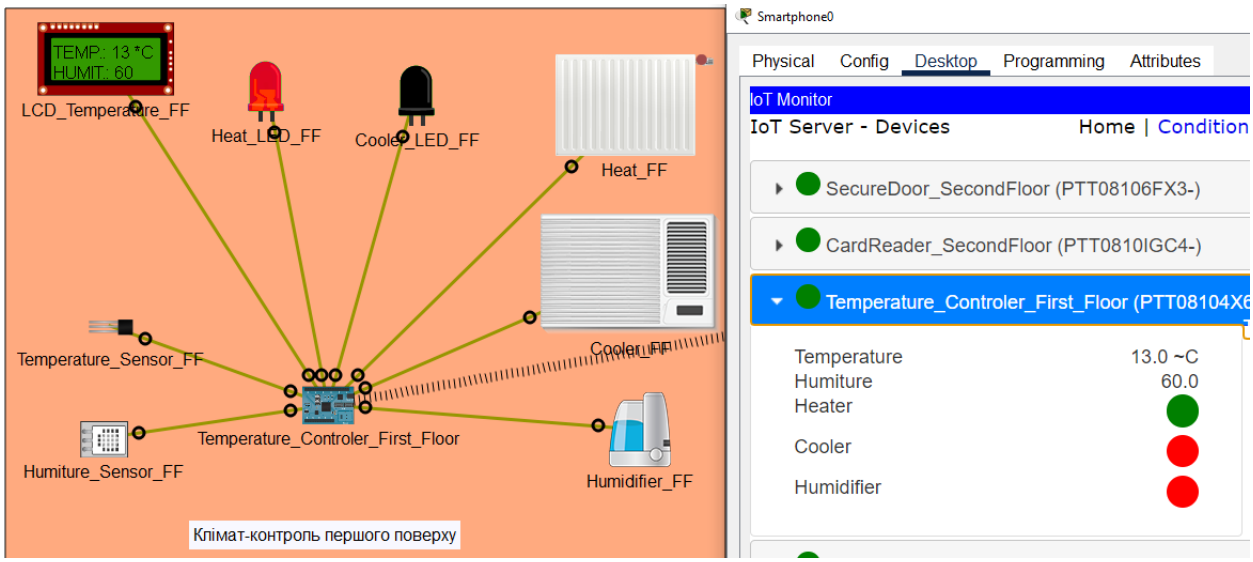

Рисунок 4.5 – Стан клімат-контролю при температурі 13°C та вологості 60

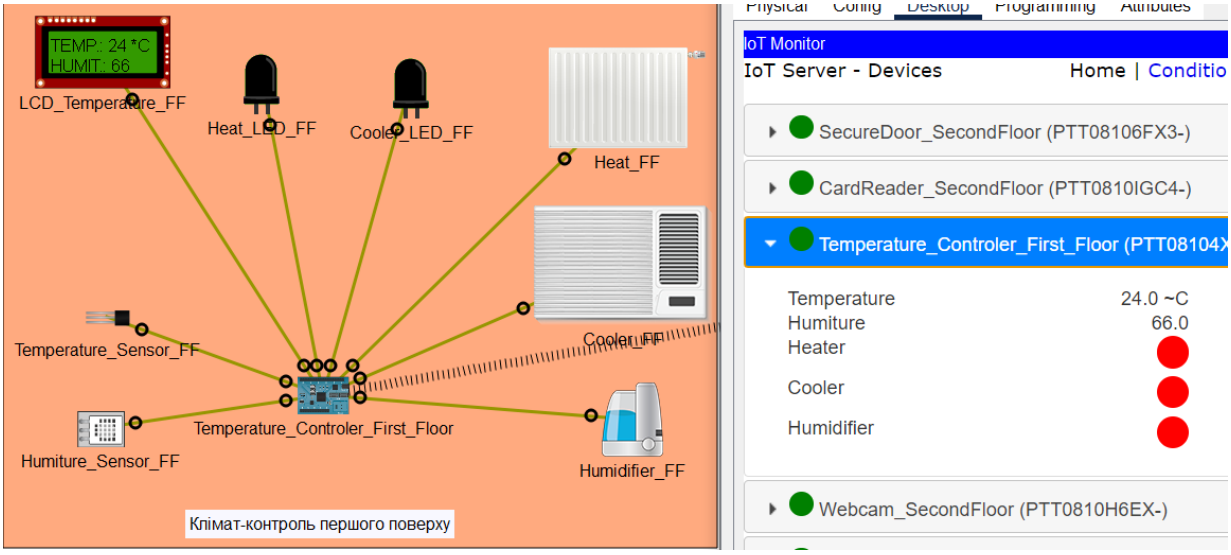

Рисунок 4.6 – Стан клімат-контролю при температурі 24°C та вологості 66

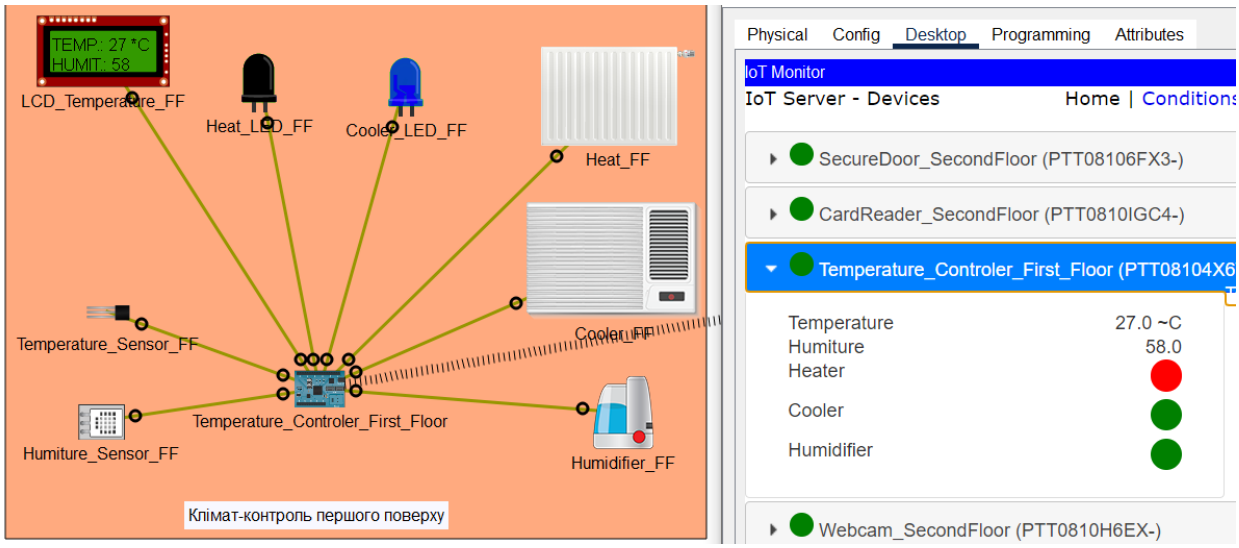

Рисунок 4.7 – Стан клімат-контролю при температурі 27°C та вологості 58

4.4 Налаштування та перевірка систем безпеки й «розумних»-пристроїв

Реалізація IoT-систем безпеки у компанії “Dnipro-M” та контролю за смарт-девайсами включає в себе взаємодію з хмарним сервісом для передачі та збереження даних, проведення їхнього аналізу та виконання визначених сценаріїв керування.

Налаштування хмарної програмної частини IoT-компонента виконується на IoT-сервері, доступ до якого можна отримати через будь-який авторизований пристрій. Для налаштування сценаріїв управління необхідно скористатися веб-браузером, або програмою «IoT-Monitor», та увійти до сторінки керування за доменом відповідного сервера й пройти автентифікацію за визначеним адміністратором мережі обліковим записом.

На головній сторінці веб-сервісу відобразився перелік підключених IoT-пристроїв, для кожного з яких є можливість віддаленого керування і спостереження станів.

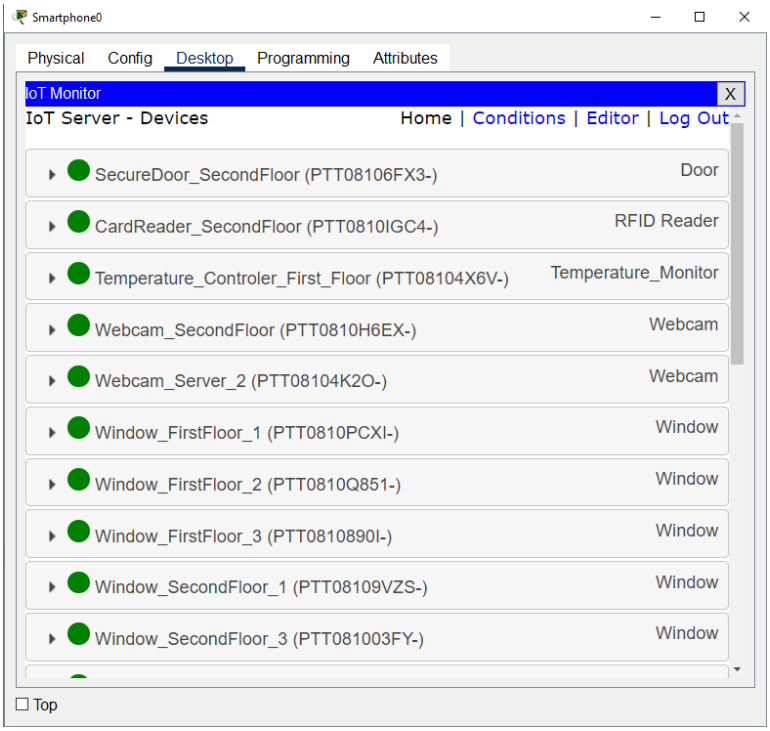

Рисунок 4.8 – Головна сторінка огляду та керування Smart Devices IoT-сервера

Сценарії функціонування систем безпеки та контролю за пристроями Інтернету речей компанії “Dnipro-M” задаються на вкладці Conditions. Для відтворення сценарію необхідно створити правила-умови, за якими будуть працювати пристрої IoT. Щоб додати сценарій необхідно натиснути Add, далі вказати назву правила, задати умови в полі «If» та дії в полі «Then set», які буду відбуватися у разі виконання зазначених умов.

Було додано сценарії ідентифікації за зчитувачами-RFID. Згідно нього, доступ до приміщення серверних кімнат має лише персонал з картами за ідентифікаторами 1001 та 1002, при інших умовах – відмова доступу. Ідентифікатор 0 відповідає стану очікування RFID-зчитувача. При успішній автентифікації за RFID – двері серверної відмикаються, при стані очікування чи відмови – серверна зачинена.

First_Server_Door_Unlock	CardReader_FirstFloor Status is Valid	Set SecureDoor_FirstFloor Lock to Unlock
First_Server_Door_Lock	Match any: • CardReader_FirstFloor Status is Invalid • CardReader_FirstFloor Status is Waiting	Set SecureDoor_FirstFloor Lock to Lock
First_CardReader_Valid	Match any: • CardReader_FirstFloor Card ID = 1001 • CardReader_FirstFloor Card ID = 1002	Set CardReader_FirstFloor Status to Valid
First_CardReader_Invalid	Match all: • CardReader_FirstFloor Card ID != 0 • CardReader_FirstFloor Card ID != 1001 • CardReader_FirstFloor Card ID != 1002	Set CardReader_FirstFloor Status to Invalid

Рисунок 4.9 – Сценарії реалізації доступу до серверної за RFID

Персоналу було надано відповідні RFID-картки, проте одна з них виявилась пошкоджена та наділена невідповідним ідентифікатором. На рисунку нижче представлена ситуація використання нормальної та «зіпсованої» карт доступу.

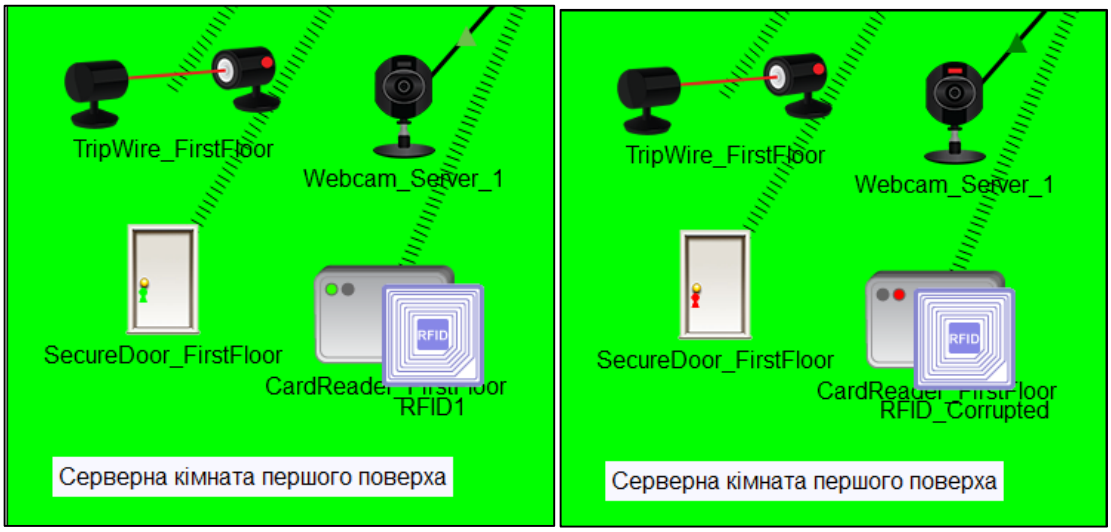

Рисунок 4.10 – Доступ до серверної кімнати за різними RFID

При неавторизованому доступі та компрометації правил доступу до серверної потрібно вмикати відеоспостереження за потенційним порушником. Для цього було налаштовано сценарії, що спрацьовують при активації датчиків руху та невідповідності авторизованому стану RFID-зчитувача.

First_Server_Save	Match all: • TripWire_FirstFloor On is true • CardReader_FirstFloor Status is Valid	Set Webcam_Server_1 On to false
First_Server_NotSave	Match any: • Match all: ◦ TripWire_FirstFloor On is true ◦ CardReader_FirstFloor Status is Invalid • Match all: ◦ TripWire_FirstFloor On is true ◦ CardReader_FirstFloor Status is Waiting	Set Webcam_Server_1 On to true

Рисунок 4.11 – Сценарії відеоспостереження за порушенням правил доступу до серверної

Ситуація несанкціонованого входу до серверної кімнати представлена на рисунку 4.12.

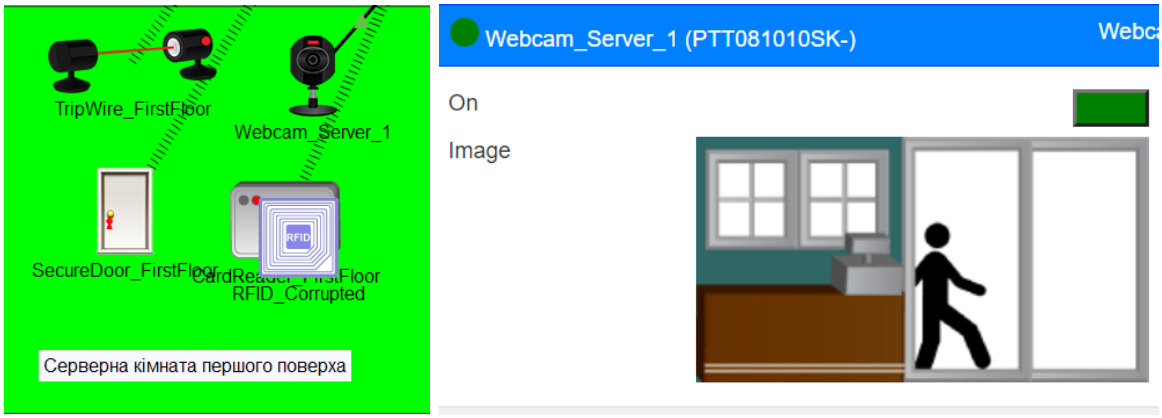

Рисунок 4.12 – Відеоспостереження за порушником правил доступу до серверної кімнати

Система протипожежної безпеки забезпечується 4 датчиками вогню, розміщеними у місцях найбільш потенційних місць загоряння. Для відповідності стандартам безпеки, необхідно одразу евакуювати персонал за першим сигналом протипожежної сигналізації. Сигналізація повинна спрацьовувати за фіксацією вогню хоча б одним датчиком із блоку. Налаштування сценарію на рисунку 4.13.

Fire_Alarm	Match any: • Fire_Detector_1 Fire Detected is true • Fire_Detector_2 Fire Detected is true • Fire_Detector_3 Fire Detected is true • Fire_Detector_4 Fire Detected is true	Set Signalization On to true
Fire_Save	Match all: • Fire_Detector_1 Fire Detected is false • Fire_Detector_2 Fire Detected is false • Fire_Detector_3 Fire Detected is false • Fire_Detector_4 Fire Detected is false	Set Signalization On to false

Рисунок 4.13 – Сценарії протипожежної безпеки

У на одному із вузлів у головному офісі сталася несправність у системі електроживлення, що призвело до невеликої пожежі. Ситуація спрацювання протипожежної безпеки на рисунку нижче.

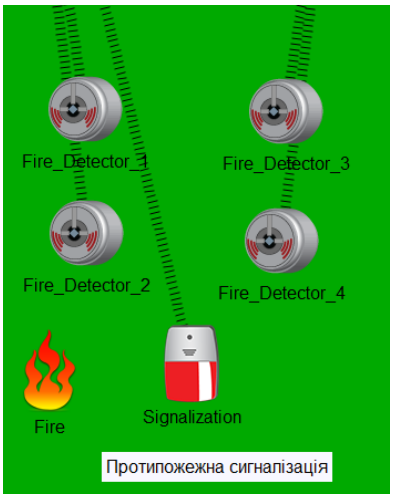

Рисунок 4.14 – Спрацювання протипожежної сигналізації

Останніми сценаріями для «розумних»-пристроїв є комбінована система, що використовує розрахунки «туманних» обчислень для хмарного керування IoT-вікнами. Згідно прохань персоналу, вікна першого поверху повинні закриватися при 15°C та відкриватися при 25°C. На другому поверсі головного офісу необхідно налаштувати відкриття вікон при 24°C та закриття при 18°C. Налаштовані сценарії та їхнє виконання хмарними ресурсами представлені на рисунку 4.15 і рисунках 4.16 та 4.17 відповідно.

FirstFloor_Windows_Open	Temperature_Controler_First_Floor Temperature > 25.0 ~C	Set Window_FirstFloor_1 On to true Set Window_FirstFloor_2 On to true Set Window_FirstFloor_3 On to true
FirstFloor_Windows_Close	Temperature_Controler_First_Floor Temperature < 15.0 ~C	Set Window_FirstFloor_1 On to false Set Window_FirstFloor_2 On to false Set Window_FirstFloor_3 On to false
SecondFloor_Windows_Open	Temperature_Controler_Second_Floor Temperature > 24.0 ~C	Set Window_SecondFloor_1 On to true Set Window_SecondFloor_2 On to true Set Window_SecondFloor_3 On to true Set Window_SecondFloor_4 On to true
SecondFloor_Windows_Close	Temperature_Controler_Second_Floor Temperature < 18.0 ~C	Set Window_SecondFloor_1 On to false Set Window_SecondFloor_2 On to false Set Window_SecondFloor_3 On to false Set Window_SecondFloor_4 On to false

Рисунок 4.15 – Сценарії керування вікнами за різних температур

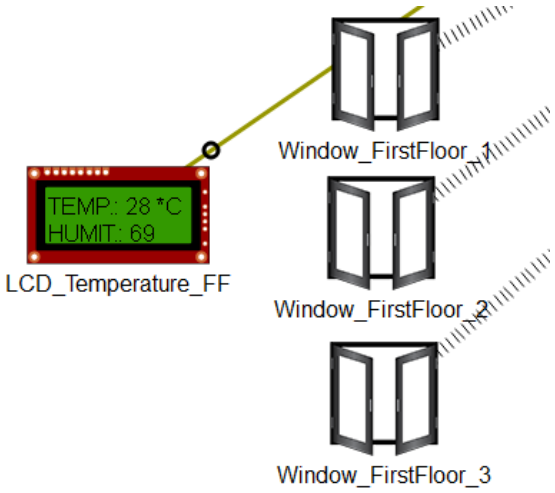

Рисунок 4.16 – Вікна першого поверха відкриті при температурі 28°C

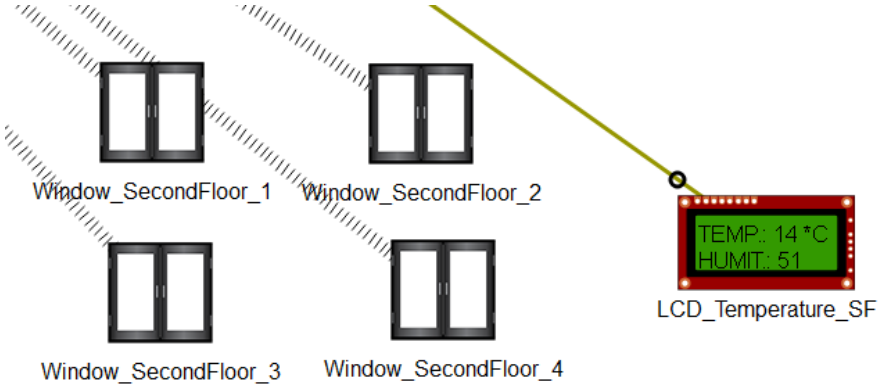

Рисунок 4.17 – Вікна другого поверху закриті при температурі 14°C

ВИСНОВКИ

Метою кваліфікаційної роботи була розробка та впровадження комп'ютерної системи компанії “Dnipro-M”. Це українська організація, що спеціалізується на різноманітних аспектах будівельного сектору. Зокрема, вона займається реалізацією обладнання та наданням сервісних послуг клієнтам. Аналізуючи об’єкт впровадження, було виявлено, що компанія “Dnipro-M” має розгалужену організаційно-топографічну структуру, що поєднує, розділений на відділи головний офіс та віддалений підрозділ служби підтримки. Необхідно було забезпечити організацію комп’ютерною системою, призначеною для підтримки прийняття рішень, забезпечення звітності у процесі ведення комерційної діяльності.

На основі проведеного аналізу було сформульовано технічне завдання до розробки комп'ютерної системи, що включає різноманітні вимоги до функціоналу мережі, ефективності обміну даними, безпеки та безвідмовності компонентів, сумісності із існуючими рішеннями тощо. На основі потреб та вимог компанії була обрана оптимальна архітектура схема мережі, яка включає в себе реалізацію комплексу технічних засобів комп’ютерної системи. Було аналіз мережевого трафіку, а також розрахунки адресації мереж та обладнання. Згідно поставлених задач та проведених розрахунків, було створено емуляцію комп’ютерної системи “Dnipro-M” у програмі Cisco Packet Trace. Розробка моделі комп’ютерної системи включала: налаштування корпоративної мережі та відповідного обладнання; імплементація IoT-компонента клімат-контролю та безпеки; тестування функціональних компонентів та мережі в цілому на відповідність вимог перед нею.

Розроблена система є гнучкою і може бути легко адаптована до зміни умов та нових вимог, що забезпечує її довгострокову ефективність та надійність. Поставлені перед проектом цілі були досягнуті в повному обсязі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. What is a LAN? Local Area Network. Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html (дата звернення: 30.05.2024).

2. Інтернет речей (IoT) – що це таке і як працює, суть, технології і приклади. Termin.in.ua. URL: https://termin.in.ua/internet-rechey-iot/ (дата звернення: 30.05.2024).

3. Ієрархічна модель мережі – RCI-Consulting. [Електронний ресурс] – Режим доступу: https://rci-c.com/technology/yerarkhycheskaia-model-sety/ (дата звернення: 30.04.2024).

4. Cisco Internetworking Basics. Cisco: Software, Network, and Cybersecurity Solutions - Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/linked/tcpip.htm (дата звернення: 30.05.2024).

5. ДСТУ Б В.2.5-82:2016 Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом – К.: УкрНДНЦ, 2016. – 109 с.

6. Постанова № 42 від 01.12.99 «Про санітарні норми мікроклімату виробничих приміщень» ДСН 3.3.6.042-99 / Міністерство охорони здоров'я України.

7. ДСТУ 8828:2019 Пожежна безпека. Загальні положення – К.: УкрНДНЦ, 2020. – 84 с.

8. ДСТУ EN 50160:2023 Характеристики напруги електропостачання в електричних мережах загальної призначеності – К.: УкрНДНЦ, 2023. – 54 с.

9. Cisco 2900 Series Integrated Services Routers Data Sheet. Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html (дата звернення: 30.05.2024).

10. Cisco Catalyst 2960 Series Switches. Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/series.html (дата звернення: 30.05.2024).

11. Cisco UCS C220 M5 Rack Server Data Sheet. Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/datasheet-c78-739281.html (дата звернення: 30.05.2024).

12. NEPSweb main page. [Електронний ресурс] – Режим доступу: https://nepsweb.co.uk/docs/subnetting.pdf (дата звернення: 21.06.2024).

13. Awati R. What is Variable Length Subnet Mask (VLSM)?. Networking. [Електронний ресурс] – Режим доступу: https://www.techtarget.com/searchnetworking/definition/variable-length-subnet-mask (дата звернення: 21.06.2024).

14. Basic Configuration Using the CLI. Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/security/ips/4-0/installation/guide/hwchap4.html (дата звернення: 21.06.2024).

15. Cisco - Configuring EtherChannel. Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/etherchannel.html (дата звернення: 21.06.2024).

16. IP Routing: EIGRP Configuration Guide. Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-mt/ire-15-mt-book/ire-enhanced-igrp.html (дата звернення: 21.06.2024).

17. Configure Network Address Translation. Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html (дата звернення: 21.06.2024).

18. Cisco IOS VPN Configuration Guide. Cisco. [Електронний ресурс] – Режим доступу:

https://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html (дата звернення: 21.06.2024).

19. Configuring VLANs. Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/layer2/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide_Release_5-x_chapter4.html (дата звернення: 21.06.2024).

20. КОМП’ЮТЕРНІ МЕРЕЖІ Частина 1 НАВЧАЛЬНИЙ ПОСІБНИК [Електронний ресурс]: навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології», спеціалізації «Інженерія програмного забезпечення інформаційно управляючих систем» та «Інформаційне забезпечення робототехнічних систем»/ Б. Ю. Жураковський, І.О. Зенів; КПІ ім.Ігоря Сікорського. – 336 с.

Додаток А

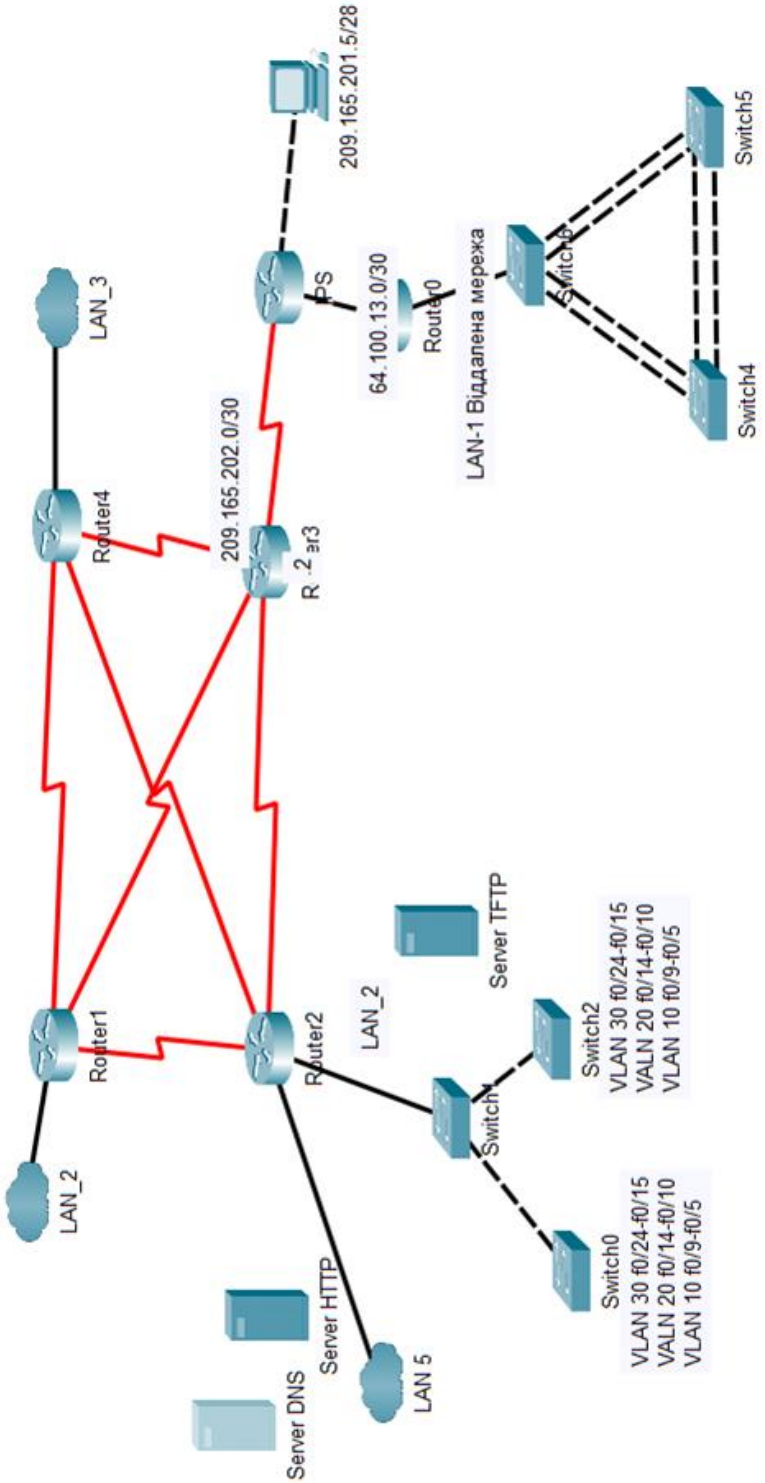

Рисунок ДА.1 – Загальна архітектура комп’ютерної системи компанії “Dnipro-M”

Додаток Б

Текст програм налаштування комп’ютерної системи компанії “Dnipro-M”

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАНЬ МЕРЕЖІ ТА ІОТ-КОМПОНЕНТА КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми
804.02070743.24014-01 12 01
Листів 20

2024

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування конфігурації маршрутизаторів та комутаторів корпоративної мережі комп’ютерної системи, а також скрипт для програмування мікроконтролера IoT-компонента.

Ця програма призначена для забезпечення базових налаштувань роутерів та комутаторів, доступу до командного рядка та ліній vty, налаштування інтерфейсів обладнання, протоколів DHCP, EIGRP, AAA, NAT, розгортання мережі VPN, застосування VLAN.

Код скрипту написаний мовою Python, призначений для контролю за температурою та вологістю у приміщеннях де розгорнута комп’ютерна мережа, відлагоджений у програмному середовищі Cisco Packet Tracer, призначений для застосування на мікроконтролері серії Arduino UNO R4 WiFi.

ЗМІСТ

1. Конфігурація Yakovlev_Router_2

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Yakovlev_Router_2
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
no ip cef
no ipv6 cef
!
username 123201_Yakovlev privilege 15 secret 5 $1$mERr$MKp6WULHmjLdYVBw6rbD11
!
license udi pid CISCO2911/K9 sn FTX152449UY-
license boot module c2900 technology-package securityk9
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp key cisco address 64.100.13.2
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map MAP 10 ipsec-isakmp
```

```
 description VPN connection to R5
 set peer 64.100.13.2
 set transform-set VPN-SET
 match address VPN
!
ip domain-name Yakovlev_Router_2
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/2/0
 bandwidth 128
 ip address 10.0.14.9 255.255.255.252
```

```
 ip nat inside
!
interface Serial0/2/1
 bandwidth 128
 ip address 10.0.14.14 255.255.255.252
 ip nat inside
 clock rate 128000
!
interface Serial0/3/0
 bandwidth 128
 ip address 10.0.14.18 255.255.255.252
 ip nat inside
 clock rate 128000
!
interface Serial0/3/1
 ip address 209.165.202.1 255.255.255.252
 ip nat outside
 ip summary-address eigrp 100 10.0.0.0 255.0.0.0 5
 crypto map MAP
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 100
 redistribute static
 network 10.0.14.8 0.0.0.3
 network 10.0.14.12 0.0.0.3
 network 10.0.14.16 0.0.0.3
!
```

```
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT pool Internet
ip nat inside source static 10.24.112.24 209.165.200.4
ip nat inside source static 10.24.112.25 209.165.200.3
ip nat inside source static 10.24.113.24 209.165.200.2
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.2
!
ip flow-export version 9
!
ip access-list extended VPN
 permit ip 10.24.112.0 0.0.0.127 10.24.113.192 0.0.0.31
 permit ip 10.24.112.128 0.0.0.127 10.24.113.192 0.0.0.31
 permit ip 10.24.113.0 0.0.0.127 10.24.113.192 0.0.0.31
 permit ip 10.24.113.128 0.0.0.63 10.24.113.192 0.0.0.31
 permit ip 10.0.14.0 0.0.0.255 10.24.113.192 0.0.0.31
ip access-list extended NAT
 deny ip 10.24.112.0 0.0.0.127 10.24.113.192 0.0.0.31
 deny ip 10.24.112.128 0.0.0.127 10.24.113.192 0.0.0.31
 deny ip 10.24.113.0 0.0.0.127 10.24.113.192 0.0.0.31
 deny ip 10.24.113.128 0.0.0.63 10.24.113.192 0.0.0.31
 deny ip 10.0.14.0 0.0.0.255 10.24.113.192 0.0.0.31
 permit ip 10.0.0.0 0.255.255.255 any
ip access-list extended PRIVATE_ACL
 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any
 permit ip any any
!
banner motd #
```

```
@ Property of the company Dnipro-M @
Authorized Access Only! #
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
!
end
```

2. Конфігурація Yakovlev_Router_4

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Yakovlev_Router_4
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
```

```
!
ip dhcp excluded-address 10.24.113.1 10.24.113.10
ip dhcp excluded-address 10.24.113.33 10.24.113.42
ip dhcp excluded-address 10.24.113.65 10.24.113.74
ip dhcp excluded-address 10.24.113.24
ip dhcp excluded-address 10.24.112.1 10.24.112.10
ip dhcp excluded-address 10.24.112.24
ip dhcp excluded-address 10.24.112.25
!
ip dhcp pool poolvlan24
 network 10.24.113.0 255.255.255.224
 default-router 10.24.113.1
 dns-server 10.24.112.25
ip dhcp pool poolvlan34
 network 10.24.113.32 255.255.255.224
 default-router 10.24.113.33
 dns-server 10.24.112.25
ip dhcp pool poolvlan44
 network 10.24.113.64 255.255.255.224
 default-router 10.24.113.65
 dns-server 10.24.112.25
ip dhcp pool poollan5
 network 10.24.112.0 255.255.255.128
 default-router 10.24.112.1
 dns-server 10.24.112.25
!
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
```

```
!
no ip cef
no ipv6 cef
!
username 123201_Yakovlev privilege 15 secret 5
$1$mERr$MKp6WULHmjLdYVBw6rbD11
username Yakovlev_Router_4 password 7 082048430017544541
!
license udi pid CISCO2911/K9 sn FTX1524EU86-
!
ip domain-name Yakovlev_Router_4
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.24
 encapsulation dot1Q 24
 ip address 10.24.113.1 255.255.255.224
!
interface GigabitEthernet0/0.34
 encapsulation dot1Q 34
 ip address 10.24.113.33 255.255.255.224
!
interface GigabitEthernet0/0.44
 encapsulation dot1Q 44
 ip address 10.24.113.65 255.255.255.224
```

```
!
interface GigabitEthernet0/0.99
 encapsulation dot1Q 99
 ip address 10.24.113.97 255.255.255.240
!
interface GigabitEthernet0/1
 ip address 10.24.112.1 255.255.255.128
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/2/0
 ip address 10.0.14.2 255.255.255.252
 clock rate 128000
!
interface Serial0/2/1
 ip address 10.0.14.5 255.255.255.252
!
interface Serial0/3/0
 ip address 10.0.14.17 255.255.255.252
!
interface Serial0/3/1
 no ip address
 clock rate 128000
 shutdown
```

```
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 100
 passive-interface GigabitEthernet0/1
 network 10.24.113.0 0.0.0.127
 network 10.0.14.0 0.0.0.3
 network 10.0.14.4 0.0.0.3
 network 10.0.14.16 0.0.0.3
 network 10.24.112.0 0.0.0.127
!
ip classless
!
ip flow-export version 9
!
banner motd #
@ Property of the company Dnipro-M @
Authorized Access Only! #
!
line con 0
 password 7 0822455D0A16
 login authentication console
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 login authentication default
```

```
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login authentication default
 transport input ssh
!
end
```

3. Конфігурація Yakovlev_LAN4_Switch1

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Yakovlev_LAN4_Switch1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
ip domain-name Yakovlev_LAN4_Switch1
!
username 123201_Yakovlev secret 5 $1$mERr$MKp6WULHmjLdYVBw6rbD11
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 24,34,44,99-100
 switchport mode trunk
```

```
!
interface FastEthernet0/2
 switchport trunk native vlan 100
 switchport trunk allowed vlan 24,34,44,99-100
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 100
 switchport trunk allowed vlan 24,34,44,99-100
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 100
 switchport trunk allowed vlan 24,34,44,99-100
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 24
```

```
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 44
 switchport mode access
!
```

```
interface FastEthernet0/16
 switchport access vlan 44
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 44
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 44
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 44
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 44
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 44
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 44
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 44
```

```
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 44
 switchport mode access
!
interface GigabitEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 24,34,44,99-100
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk native vlan 100
 switchport trunk allowed vlan 24,34,44,99-100
 switchport mode trunk
!
interface Vlan1
 no ip address
!
interface Vlan99
 ip address 10.24.113.98 255.255.255.240
!
ip default-gateway 10.24.113.97
!
banner motd #
@ Property of the company Dnipro-M @
Authorized Access Only! #
!
line con 0
 password 7 0822455D0A16
```

```
 login
!
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
!
End
```

4. Python-скрипт DniproMIoT.py

```
from gpio import *
from time import *
from ioeclient import *
IoEClient.setup({
        "type": "Temperature_Monitor",
        "states":[
        {
                "name": "Temperature",
                "type": "number",
                "unit": "~C",
                "decimalDigits":1
        },
        {"name": "Humiture",
                "type": "number",
                "unit": "",
                "decimalDigits":1},
```

```
        {"name": "Heater",
                "type": "bool"},
        {"name": "Cooler",
                "type": "bool"},
        {"name": "Humidifier",
                "type": "bool"}
]});
def main():
        pinMode(0, OUT)
        pinMode(1, OUT)
        pinMode(2, OUT)
        pinMode(3, OUT)
        pinMode(4, OUT)
        pinMode(5, OUT)
        HeatState = 0
        CoolerState = 0
        HumitState = 0
        while True:
                Temp = analogRead(A0)*200/1023 -100
                Humit = analogRead(A1)*100/1023
                customWrite(0,"TEMP.: " + str(Temp) + " *C\n"+
                                        "HUMIT.: " + str(Humit))
                if (Temp < 15):
                        digitalWrite(1, HIGH)
                        digitalWrite(3, HIGH)
                        digitalWrite(2, LOW)
                        digitalWrite(4, LOW)
                        HeatState = 1
                        CoolerState = 0
                if (Temp > 20 and Temp < 25):
```

```
                digitalWrite(1, LOW)
                digitalWrite(3, LOW)
                digitalWrite(2, LOW)
                digitalWrite(4, LOW)
                HeatState = 0
                CoolerState = 0
            if (Temp > 25):
                digitalWrite(2, HIGH)
                digitalWrite(4, HIGH)
                digitalWrite(1, LOW)
                digitalWrite(3, LOW)
                HeatState = 0
                CoolerState = 1
            if (Humit < 60):
                customWrite(5,1)
                HumitState = 1
            else:
                customWrite(5,0)
                HumitState = 0
            IoEClient.reportStates([Temp, Humit, HeatState, CoolerState,
HumitState])
if __name__ == "__main__":
    main()
```