

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

Інститут електроенергетики  
(інститут)

Факультет інформаційних технологій  
(факультет)

Кафедра інформаційних технологій та комп'ютерної інженерії  
(повна назва)

**ПОЯСНЮВАЛЬНА ЗАПИСКА**

кваліфікаційної роботи ступеня бакалавра  
(бакалавра, спеціаліста, магістра)

студента Шарапова Єгора Вікторовича  
(ПІБ)

академічної групи 123-21ск-1  
(шифр)

спеціальності 123 Комп'ютерна інженерія  
(код і назва спеціальності)

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

на тему «IoT система індивідуального зберігання інвентарю підприємства «Yellow Box»  
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Сергєєва К.Л.			
розділів:				
розробка апаратної частини	доц. Бешта Д.О.			
розробка корпоративної мережі	ас. Панферова Я.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)

«\_\_\_» \_\_\_\_\_ 202 року

**ЗАВДАННЯ  
на кваліфікаційну роботу  
ступеня бакалавр**

студента Шарапов Є.В.

(прізвище та ініціали)

академічної групи

123-21ск-1

(шифр)

спеціальності

123 «Комп'ютерна інженерія»

за освітньо-професійною програмою

123 «Комп'ютерна інженерія»

(офіційна назва)

на тему «ІоТ система індивідуального зберігання інвентарю  
підприємства «Yellow Vox»

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

<b>Розділ</b>	<b>Зміст</b>	<b>Термін виконання</b>
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати завдання, конкретизувати предмет та мету роботи	01.04.2024
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	30.04.2024
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	20.05.2024
Розробка компонента системи	Виконується детальна розробка компонента системи	04.06.2024

**Завдання видано**

\_\_\_\_\_ (підпис керівника)

доц. Сергєєва К.Л.

(прізвище, ініціали)

**Дата видачі**

\_\_\_\_\_

**Дата подання до екзаменаційної комісії**

\_\_\_\_\_

**Прийнято до виконання**

\_\_\_\_\_ (підпис студента)

Шарапов Є.В.

(прізвище, ініціали)

## РЕФЕРАТ

Пояснювальна записка: 74 с., 18 рис., 6 табл., 9 джерел, 2 додатки.

КОМПОНЕНТ, МЕРЕЖА, ПРОТОКОЛ, ШЛЮЗ, ТУМАННІ  
ОБЧИСЛЕННЯ, ІОТ

Об'єкт: ІоТ система індивідуального зберігання інвентарю підприємства «Yellow Box».

Мета: впровадження ІоТ-рішення в конфігурації та специфікації, що враховує специфіку підприємства «Yellow Box» яке надає послуги оренди приміщень індивідуального зберігання речей.

Розроблена ІоТ-система виконана з можливістю масштабування та оновлення програмного забезпечення, орієнтована як складова частина корпоративної мережі підприємства «Yellow Box», орієнтована на виконання функцій енергозбереження, відеонагляду, безпеки задимлення, збору та аналітики даних за допомогою хмарних сервісів.

Розробка корпоративної мережі підприємства «Yellow Box» та ІоТ-системи була здійснена у рамках кваліфікаційної роботи бакалавра.

Розроблена модель ІоТ-системи налаштована та перевірена в симуляторах Packet Tracer та TincerCAD.

Розроблена модель мережі реалізована та протестована в симуляторі мереж Cisco Packet Tracer.

## ЗМІСТ

	Стр.
Перелік умовних позначень, символів, одиниць, скорочень і термінів.....	7
Вступ.....	8
1 Стан питання і постановка задачі.....	10
1.1 Стисла характеристика галузі та умов застосування КС.....	10
1.2 Характеристика і структура об'єкта впровадження.....	12
1.3 Організаційна структура підприємства Yellow Vox.....	15
1.4 Принципи, технічні способи та математичні методи інформаційного забезпечення об'єкта впровадження.....	17
1.5 Аналітичний огляд існуючих способів обробки та передачі інформації.....	22
1.6 Завдання і мета роботи.....	23
1.7 Визначення можливих напрямків рішення поставлених завдань.....	24
2 Розробка апаратної частини комп'ютерної системи.....	26
2.1 Технічні вимоги до Системи.....	26
2.2.1 Вимоги до системи в цілому.....	26
2.2.1.1 Вимоги до структури і функціонування Системи.....	26
2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації Системи.....	26
2.1.1.1.2 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами Системи.....	27
2.1.1.1.3 Вимоги до діагностування Системи.....	28
2.1.1.1.4 Перспективи розвитку, модернізації Системи.....	29
2.1.1.2 Вимоги до показників призначення.....	29
2.1.1.3 Вимоги до експлуатації.....	30
2.1.1.3.1 Умови і режим експлуатації, що повинні забезпечувати використання технічних засобів Системи з заданими технічними показниками.....	30
2.1.1.3.2 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи.....	31

2.1.1.3.3	Вимоги до складу, розміщенню й умовам збереження комплекту запасних виробів і приладів.....	32
2.1.1.3.4	Вимоги до регламенту обслуговування.....	32
2.1.2	Вимоги до налаштувань, які виконуються у Системі.....	32
2.1.3	Вимоги до видів забезпечення Системи.....	33
2.1.3.1	Вимоги до інформаційного забезпечення.....	33
2.1.3.2	Вимоги до лінгвістичного забезпечення.....	34
2.1.3.3	Вимоги до технічного забезпечення.....	34
2.1.3.4	Вимоги до організаційного забезпечення.....	34
2.2	Розробка апаратної частини IoT системи.....	35
2.2.1	Розробка загальної структури комп'ютерної системи.....	35
2.2.2	Розробка структури комплексу технічних засобів IoT системи.....	36
2.2.3	Розробка специфікації апаратних засобів IoT системи.....	40
2.2.4	Розробка переліку вхідних та вихідних сигналів.....	45
2.2.5	Розробка принципової схеми.....	46
2.2.6	Розрахунок інтенсивності вихідного трафіку найбільшої LAN Yellow Vox.....	47
3	Проектування корпоративної мережі та перевірка роботи комп'ютерної системи підприємства.....	49
3.1	Розрахунок схеми адресації корпоративної мережі «Yellow Vox».....	49
3.2	Розробка топологічної схеми корпоративної мережі.....	52
3.3	Проектування комп'ютерної мережі та розрахунок її налаштувань.....	54
3.3.1	Базове налаштування конфігурації пристроїв.....	54
3.3.2	Налаштування маршрутизаторів корпоративної мережі.....	55
3.3.3	Налаштування роботи Інтернет.....	58
3.3.4	Захист інформації в комп'ютерній системі від несанкціонованого доступу.....	60
3.3.4	Перевірка роботи моделі комп'ютерної системи.....	63
4	Розробка компонента системи.....	64
4.1	Об'єкт та тип впроваджуваного компонента системи.....	66
4.2	Налаштування IoT-системи.....	67
4.3	Моделювання IoT-системи.....	72

Висновки.....	75
Перелік посилань.....	76
Додаток А           Текст програми налаштування мережі.....	78
Додаток Б           Текст програми налаштування компонента IoT.....	90

## **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ**

ПК – персональний комп'ютер;

КМ – корпоративна мережа;

КС – комп'ютерна система;

IoT – Internet of Things;

VLAN – віртуальна локальна мережа;

DHCP – протокол динамічної настройки вузла;

LAN – локальна мережа;

WAN – глобальна мережа;

VLSM – метод мережевих масок змінної довжини;

AAA – Authentication, Authorization, Accounting.

## ВСТУП

У сфері IoT-систем в напрямі індивідуального зберігання речей станом на зараз спостерігаються кілька світових тенденцій.

Розширення функціональності. Системи зберігання все більше поєднуються з IoT технологіями для забезпечення додаткових функцій, таких як моніторинг стану, віддалене керування і сповіщення про стан або витрату ресурсів.

Збільшення безпеки. Використання IoT у системах зберігання дозволяє покращити безпеку шляхом впровадження систем відстеження, відеоспостереження та автоматичних сповіщень про будь-які незвичайні події.

Оптимізація витрат ресурсів. Системи IoT можуть забезпечувати аналітику щодо використання ресурсів (наприклад, електроенергії, води тощо), щоб допомогти компаніям ефективніше управляти їхнім споживанням.

Розвиток хмарних технологій. Збільшення доступності хмарних технологій сприяє зберіганню та обробці великих обсягів даних з пристроїв IoT, що дозволяє використовувати їх для аналізу, прогнозування та оптимізації.

Збільшення уваги до приватності та кібербезпеки. З огляду на збільшену кількість підключених пристроїв, увага до захисту приватності та захисту від кібератак стає дедалі важливішою, і компанії з надання послуг зберігання повинні враховувати ці аспекти у своїх послугах.

Застосування IoT-систем з функціями відеоспостереження, доступу, керування освітленням та кліматом є актуальним напрямом для компаній, що надають послуги оренди приміщень індивідуального зберігання речей.

1. Підвищення безпеки. Відеоспостереження допомагає виявляти будь-які незвичайні або підозрілі дії в об'єкті зберігання, що може допомогти у запобіганні



крадіжок та втрат. Крім того, віддалений доступ до відеоспостереження дозволяє власникам відстежувати ситуацію в реальному часі.

2. Зручне керування ресурсами. Інтегровані системи керування освітленням та кліматом дозволяють оптимізувати витрати енергії та забезпечувати комфортні умови для зберігання речей. Наприклад, автоматичне вимкнення світла або регулювання температури відповідно до потреб користувачів може зменшити споживання енергії і витрати на обслуговування.

3. Покращення досвіду користувача. Забезпечення доступу до онлайн-платформ або додатків для віддаленого керування і моніторингу може підвищити задоволення клієнтів і зробити процес оренди приміщень більш зручним і ефективним.

4. Конкурентні переваги. Використання сучасних IoT технологій може стати конкурентною перевагою для компаній, що надають послуги оренди приміщень, допомагаючи їм привернути нових клієнтів та зберегти існуючих.

Таким чином, впровадження технологій IoT може бути важливим кроком для оптимізації операцій і поліпшення обслуговування в сфері оренди приміщень індивідуального зберігання речей.

Отже, мета даної кваліфікаційної роботи – впровадження IoT-рішення в конфігурації та специфікації, що враховує специфіку підприємства «Yellow Box» яке надає послуги оренди приміщень індивідуального зберігання речей.

## 1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

### 1.1 Стисла характеристика галузі та умов застосування КС

Сфера діяльності компанії Yellow Box пов'язана з наданням індивідуальних боксів для збереження майна поза межами місця проживання. Використання орендованих складів для вивільнення простору в житлових приміщеннях є розповсюдженою практикою у Європі. Індивідуальні бокси також застосовуються в якості: точок продажу, приміщення Інтернет магазину, бізнесових складів, місце тимчасового зберігання речей (ремонт в житловому приміщенні).



Рисунок 1.1 – Міні-склад YellowBox

Актуальність бізнесу компанії Yellow Box та зацікавленість клієнтів полягає у наступному.

1. Безпека. Клієнти, які шукають місце для зберігання своїх особистих речей, цінують безпеку. Індивідуальні бокси Yellow Box оснащені передовими системами безпеки, включаючи відеоспостереження, контроль доступу, протипожежна безпека та відеоспостереження та інші заходи, що дозволяють клієнтам відчувати себе захищеними.

2. Зручність. Індивідуальні бокси Yellow Box доступні для оренди в різних розмірах і розташуваннях, що дозволяє клієнтам обирати оптимальний варіант

для своїх потреб. Крім того, зручне розташування боксів може забезпечувати легкий доступ для клієнтів.

3. Приватність. Багато людей шукають місце для зберігання особистих речей, де вони можуть бути впевнені у збереженні приватності. Індивідуальні бокси Yellow Vox можуть надавати цю приватність, дозволяючи клієнтам зберігати свої речі в безпечному та конфіденційному середовищі.

4. Заощадження часу і простору. Для багатьох клієнтів, особливо тих, хто має обмежений простір вдома або на роботі, може бути важливо мати доступне місце для зберігання речей, які не використовуються щодня. Yellow Vox надає можливість зберігати ці речі в безпечному місці поза дому, що дозволяє клієнтам звільнити простір у своїх основних приміщеннях.

5. Гнучкість та доступність. Компанія Yellow Vox надає гнучкі тарифні плани і умови оренди, що відповідають різним потребам клієнтів. Крім того, доступність боксів у різних локаціях може забезпечити зручний доступ для широкого кола клієнтів.

Для зручності клієнтів, компанії з оренди індивідуальних боксів розташовують свої будівлі на околиці міст. Будівля оснащуються вантажними ліфтами для зручного переміщення. Клієнтам пропонуються можливості з вибору площі боксу, оренди стелажів для речей, широкі можливості доступу до боксів. В боксах забезпечується температура у приміщенні від +5 до +25°C.

Діяльність компанії Yellow Vox з наданням індивідуальних боксів також пов'язана з деякими обмеженнями. Надаються можливості зберігання наступних категорій речей: офісна техніка та меблі, архівні документи, товари інтернет-магазинів, знімальний інвентар і декорації, запчастини, екіпірування для спорту і туризму, одяг та взуття на продаж, Продукція бізнесу. Заборонено зберігання наступних категорій речей: продукти харчування, тварини, рослини, зброя та деталі зброї, вибухонебезпечні предмети, токсичні речовини.

## 1.2 Характеристика і структура об'єкта впровадження

IoT-систему в складі комп'ютерної системи буде впроваджено для компанії Yellow Box. Будівля компанії Yellow Box, що надає індивідуальні бокси для зберігання речей, знаходиться за адресою м. Київ, вул. Віскозна, 17а (Дніпровський район).

Будівля представляє собою п'яти поверхову будову з габаритними розмірами 34\*16м<sup>2</sup> та висотою поверху 2,72 метри. Знання габаритів будівлі допомагає забезпечити ефективну та надійну мережу, яка відповідає потребам користувачів та вимогам бізнесу.

Знання габаритних розмірів будівлі має важливе значення при проектуванні мережі з різних причин:

1. Ефективне розташування обладнання: Розмір будівлі визначає доступний простір для розташування різного обладнання, такого як сервери, комутатори, маршрутизатори та інше мережеве обладнання. Знання габаритів допомагає планувати оптимальне розташування цього обладнання для максимальної продуктивності та зручності обслуговування.

2. Розгалуження мережі: Розміри будівлі впливають на топологію мережі, так як вони визначають довжину кабелів, необхідних для підключення різних пристроїв. Знання габаритів дозволяє планувати оптимальну розмітку мережних кабелів та точок доступу.

3. Зонування і сегментація мережі: Габарити будівлі впливають на потребу у зонуванні та сегментації мережі. Великі будівлі можуть вимагати розділення мережі на різні сегменти або зони для забезпечення оптимальної пропускної здатності та безпеки.

4. Безпека мережі: Габарити будівлі впливають на проектування безпеки мережі, включаючи розташування точок доступу, вогнепроникність стін, розміщення відеоспостереження та інші аспекти фізичної безпеки.

5. Масштабність мережі: Розміри будівлі важливі для масштабування мережі. При проектуванні мережі потрібно враховувати можливі зміни у розмірах будівлі та вимоги щодо розширення мережі в майбутньому.

План розташування приміщень першого поверху будівлі наведений на рисунку 1.1. Тут зазначені також під які служби та відділи виділені приміщення. Всі організаційні підрозділи, що забезпечують діяльність компанії, розташовані на першому поверсі, в той час як інші поверхи будівлі виділені під складські приміщення.

План розташування приміщень на поверху будівлі є важливим етапом для побудови мережі, оскільки він визначає локації, де будуть розміщені різноманітні пристрої та з'єднання мережі.

Важливо врахувати потреби користувачів та вимоги мережі при плануванні призначення приміщень.

Це допоможе забезпечити ефективну та надійну мережу, яка відповідає потребам організації.

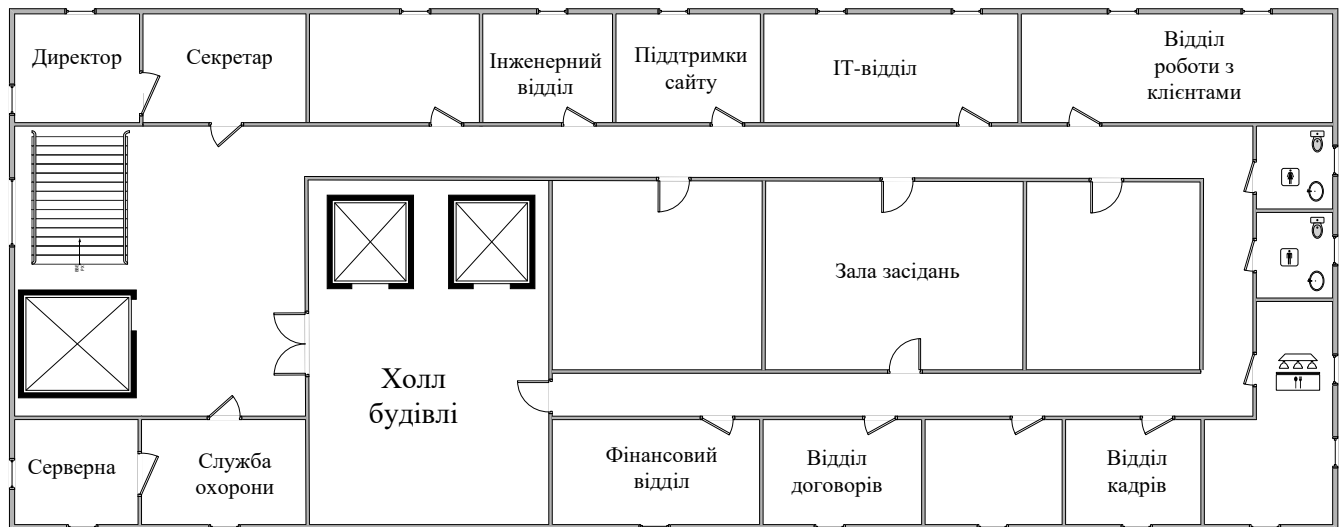


Рисунок 1.2 – Топологічна схема першого поверху (адміністративний)

При побудові фізичної топології корпоративної мережі компанії Yellow Vox важливим є розміщення мережних портів та точок доступу. Приміщення компанії розподілені відповідно до групування їх за функціоналом підрозділів.

Для офісного проверху Yellow Vox визначене розташування серверної кімнати. В ній заплановане розміщення серверів, комутаторів, маршрутизаторів та іншого мережного обладнання. Також враховані вимоги щодо електропостачання, вентиляції та безпеки для цієї області.

З огляду на план приміщення та специфіки компанії Yellow Vox, заплановані точки доступу до Wi-Fi. Визначені місця розташування точок доступу до Wi-Fi для забезпечення покриття всього приміщення бездротовим зв'язком.

Другий поверх також забезпечується покриттям Wi-Fi з огляду на особливості застосованого обладнання.

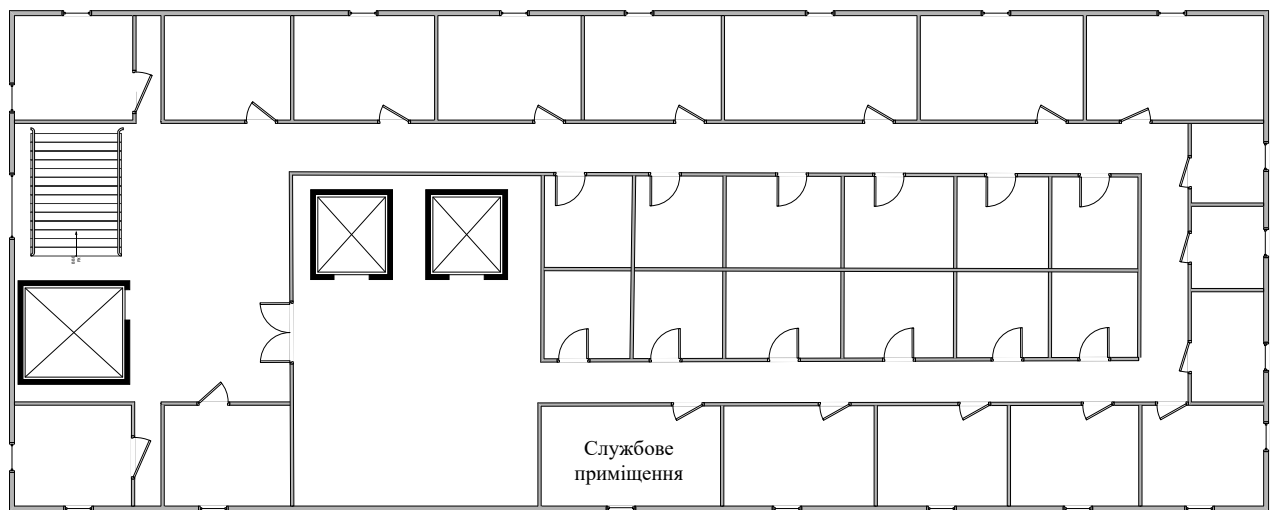


Рисунок 1.3 – Топологічна схема другого поверху (боксы зберігання)

План будівлі компанії Yellow Vox, призначення приміщень за функціоналом структурних підрозділів та групування підрозділів за підпорядкуванням надають підстави до побудови топології комп'ютерної мережі підприємства.

### 1.3 Організаційна структура підприємства Yellow Vox

Організаційна структура компанії Yellow Vox з надання послуг зберігання наведена на рисунку 1.4. Організаційна структура компанії Yellow Vox побудована виходячи з підпорядкування підрозділів та їх повноваження, відповідальність керівників підрозділів в компанії. За типом в даній компанії застосовано функціональну організаційну структуру, в якій співробітники об'єднані за спеціалізаціями.

Професійні фахівці, які забезпечують роботу компанії Yellow Vox з послуг індивідуального зберігання речей, включають в себе такі позиції:

1. Консультанти з обслуговування клієнтів: Вони надають інформацію клієнтам про доступні послуги, вирішують їх запитання та допомагають у виборі оптимального варіанту зберігання.

2. Менеджери зі зберігання: Вони керують щоденною діяльністю складів, відповідають за організацію та безпеку приміщень для зберігання речей, а також за планування і моніторинг інвентаризації.

3. Спеціалісти з безпеки: Вони відповідають за забезпечення безпеки приміщень та речей, розробляють та впроваджують системи контролю доступу та відеоспостереження.

4. Технічний персонал: Інженери та техніки, які відповідають за технічне обслуговування і ремонт обладнання для зберігання речей, такого як розумні шафи, контейнери або системи камерних сховищ.

5. Менеджери з розвитку бізнесу і маркетингу: Вони відповідають за розвиток нових ринків, просування послуг компанії та залучення нових клієнтів через рекламу та маркетингові кампанії.

6. Фахівці з обробки замовлень: Це люди, які відповідають за обробку замовлень клієнтів, прийом та видачу речей, а також за підтримання бази даних клієнтів.

7. Фінансові аналітики і бухгалтери: Вони відповідають за фінансовий облік та аналіз ефективності бізнесу, розробку бюджетів та фінансові стратегії.

Ці співробітники разом забезпечують ефективне та безпечне функціонування компанії з послуг індивідуального зберігання речей.

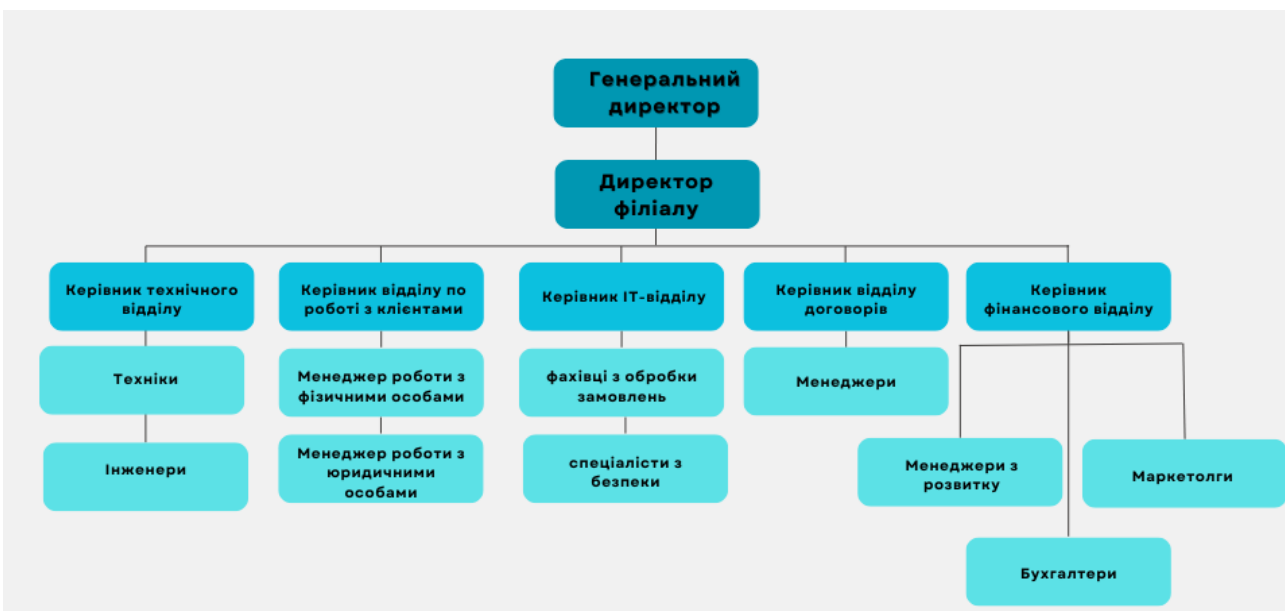


Рисунок 1.4 – Організаційна структура компанії Yellow Vox

Функціональна організаційна схема компанії Yellow Vox, яка надає послуги зберігання, має наступні підрозділи.

Управління (директорат). Включає в себе вище розташований менеджмент компанії, такий як директор, керівники відділів та інші відповідальні посадові особи. Цей відділ відповідає за стратегічне планування, прийняття стратегічних рішень та координацію всіх інших відділів.

Відділ клієнтського обслуговування. Відповідає за комунікацію з клієнтами, прийом та обробку їх запитів, надання консультацій щодо послуг зберігання та вирішення будь-яких питань чи проблем, які можуть виникнути. Цей підрозділ у зв'язку зі специфікою обов'язків поділений на менеджерів по роботі з фізичними та юридичними особами.



Технічний відділ. Відповідає за технічне обслуговування та ремонт обладнання для зберігання речей, такого як системи безпеки, механізми для переміщення товарів, системи контролю вологості та температури тощо.

Відділ ІТ. Відповідає за розробку та підтримку програмного забезпечення, що використовується для управління системами зберігання, включаючи програми для керування бронюванням боксів, моніторингу безпеки, обліку клієнтів тощо. Також налаштування та підтримку мережевої інфраструктури, включаючи Wi-Fi мережі, сервери для зберігання даних, системи резервного копіювання. Відділ ІТ обслуговує сайт компанії, прийом заявок на оренду боксів зберігання, надає технічну підтримку для співробітників компанії та клієнтів, які користуються системами зберігання.

Відділ ІТ підтримує забезпечення безпеки складських приміщень та товарів клієнтів, підтримку систем безпеки, відеоспостереження, контролю доступу тощо.

Фінансовий відділ. Відповідає за фінансовий облік, складання бюджетів, контроль над витратами та прибутками, розрахунок тарифів для клієнтів та інші фінансові аспекти діяльності компанії. Також присутній підрозділ з маркетингу, що відповідає за рекламу та маркетинг компанії, просування послуг зберігання, залучення нових клієнтів та збереження існуючих.

#### **1.4 Принципи, технічні способи та математичні методи інформаційного забезпечення об'єкта впровадження**

Останнім часом підприємства, що займаються індивідуальним зберіганням речей, все активніше використовують можливості сучасних технічних та інформаційних технологій у своїй діяльності. Серед найбільш актуальних поєднання систем зберігання з IoT технологіями для забезпечення додаткових функцій, таких як моніторинг стану, віддалене керування і сповіщення про стан або витрату ресурсів, покращення безпеки шляхом впровадження систем

відстеження, відеоспостереження та автоматичних сповіщень про будь-які незвичайні події.

Для підприємства Yellow Box проект архітектури корпоративної мережі на даний час розроблений та активне мережне обладнання обране під нього.

При впровадженні IoT-системи важливо обирати технології, які відповідають потребам конкретного проекту. В проектах IoT можуть бути застосовані наступні ключові технології.

Сенсори та датчики. Такі пристрої вимірюють фізичні або хімічні величини і перетворюють їх на електричні сигнали, які можна аналізувати. Це можуть бути датчики температури, вологості, руху, світла, рівня води тощо. Датчики руху або інфрачервоні датчики присутності можуть використовуватися для виявлення присутності людей в приміщенні. Ці дані можуть бути використані для активації систем освітлення та інших IoT пристроїв. За допомогою розумних систем освітлення, які підключені до мережі IoT, можна автоматично регулювати яскравість та час роботи освітлення в приміщенні в залежності від присутності людей та освітленості навколишнього середовища. Камери відеоспостереження з підключенням до мережі IoT можуть використовуватися для моніторингу приміщення та виявлення присутності людей. Вони також можуть використовуватися для забезпечення безпеки та відстеження будь-яких незвичайних подій. Розумні термостати або системи HVAC (системи опалення, вентиляції та кондиціонування повітря), підключені до мережі IoT, можуть регулювати температуру в приміщенні в залежності від потреб та умов.

Мережеві протоколи. Для обміну даними між пристроями використовуються різні мережеві протоколи, такі як Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRaWAN тощо. Вибір протоколу залежить від вимог проекту щодо дальності зв'язку, енергоефективності, пропускної здатності, кошторису тощо.

Хмарні платформи. Дані, зібрані з IoT пристроїв, можуть бути відправлені до хмарної платформи для зберігання, обробки та аналізу. Це дозволяє віддалено керувати пристроями, моніторити їх стан, вивчати тенденції та забезпечувати безпеку даних.

Аналітика даних та штучний інтелект. Зібрані дані можуть бути оброблені та проаналізовані за допомогою алгоритмів штучного інтелекту та машинного навчання. Так можна прогнозувати події.

Блокчейн. У деяких випадках технологія блокчейн може застосовуватися для забезпечення безпеки, цілісності та недійсності даних, що передаються між IoT пристроями.

Розумні пристрої та системи. Це можуть бути розумні домашні пристрої, які забезпечують автоматизацію та зручність для користувачів. Наприклад, розумні термостати, розумні розетки, розумні системи безпеки тощо.

Для підключення пристроїв IoT на складах використовуються різні технології залежно від конкретних вимог та умов. Основними є наступні технології.

Технологія Wi-Fi. Wi-Fi є однією з найпоширеніших технологій для підключення IoT пристроїв на складах. Вона забезпечує високу швидкість передачі даних та зручне встановлення. Проте потребує енергоефективності для деяких пристроїв, щоб уникнути перевитрати енергії.

Технологія Bluetooth. Bluetooth може бути використаний для підключення пристроїв IoT на невеликих відстанях від контрольного пристрою або мобільного телефону. Він ідеально підходить для моніторингу та управління пристроями в обмежених просторових умовах.

Технологія RFID (Radio-Frequency Identification). RFID використовується для бездротового відстеження та ідентифікації товарів та пакунків на складі. Ця

технологія дозволяє швидко і ефективно відстежувати рух товарів без необхідності відкривати або сканувати кожен пакунок окремо.

Технологія Zigbee. Zigbee є низькопотужною бездротовою мережею, яка ідеально підходить для великих складів з багатьма пристроями, які вимагають довгого терміну служби від батареї. Вона забезпечує надійний зв'язок на великій відстані та вимагає мінімального споживання енергії.

Технологія LoRaWAN. LoRaWAN – це інша низькопотужна бездротова технологія, яка підходить для використання на великих відстанях та в умовах обмеженого доступу до інфраструктури. Вона ідеально підходить для відстеження вантажів та моніторингу умов середовища на відкритих складах.

Технологія NB-IoT (Narrowband IoT). NB-IoT – це стандарт мережі, який дозволяє підключати мільйони пристроїв IoT до мобільної мережі. Він забезпечує низьке споживання енергії та довгий дальній зв'язок, що робить його ідеальним для використання на складах.

З огляду на наступні умови для приміщення, потреб та спроможностей компанії Yellow Vox в якості провідної технології реалізації IoT-системи обрана технологія WiFi. Компанія Yellow Vox пропонує невеликі бокси зберігання речей, тобто будівля невелика. Простінки в будівлі виконані з матеріалів, що не спричиняють перешкод розповсюдження радіосигналів. Топологічно будівля компанії розташована в межах міста, тобто обмеження доступу до енергоживлення відсутнє.

NB-IoT може бути вигідним в тих випадках, коли доступ до мобільного зв'язку є дешевшим або більш доступним, ніж побудова власної мережі, але в компанії реалізована власна корпоративна мережа з підтримкою технології WiFi.

Технологія WiFi є однією з найпоширеніших технологій бездротового зв'язку і широко використовується для домашніх та корпоративних мереж, IoT систем. Вона забезпечує високу швидкість передачі даних і зручність

встановлення та використання, що робить її привабливим вибором для багатьох застосувань.

Технологія WiFi також має свої обмеження. Ось деякі з них.

1. Дальність зв'язку. WiFi мережі мають обмежений радіус дії, зазвичай від декількох до кількох сотень метрів. Це означає, що вони не підходять для передачі даних на великі відстані, такі як деякі інші технології, наприклад, LoRaWAN або NB-IoT.

2. Пропускна здатність. Висока пропускна здатність WiFi може призводити до перенасичення мережі, особливо у великих місцях, де багато пристроїв конкурують за доступ до мережі. Це може призводити до зниження швидкості передачі даних та переривань у зв'язку.

3. Енергоспоживання. WiFi пристрої, особливо ті, які активно використовуються для передачі даних, можуть споживати більше енергії порівняно з іншими бездротовими технологіями. Це може бути недоцільним для деяких IoT пристроїв, особливо тих, які працюють в умовах обмеженого живлення або потребують довгого терміну служби від батареї.

4. Безпека. WiFi мережі можуть бути вразливими до різних видів кібератак, таких як перехоплення даних або вторгнення в мережеву інфраструктуру. Неправильно налаштовані мережі можуть стати джерелом загрози для конфіденційності та безпеки даних.

5. Частотні перешкоди. WiFi мережі працюють на різних частотах (наприклад, 2,4 ГГц або 5 ГГц), які можуть бути зайняті іншими пристроями або викликати перешкоди від інших джерел безпроводного сигналу, таких як мікрохвильові печі або Bluetooth пристрої.

## 1.5 Аналітичний огляд існуючих способів обробки та передачі інформації

Сьогодні на ринку IoT-систем розумного дому існує багато компаній, які пропонують як готові системи, так і окремі компоненти. Це дозволяє споживачам легко знаходити і замовляти готові набори для управління побутовими пристроями від різних виробників. Деякі з них включають такі відомі бренди, як Samsung SmartThings, Google Nest, Amazon Echo (Alexa), Apple HomeKit, Xiaomi Mi Home, Philips Hue, TP-Link Kasa, і TP-Link Deco. Кожен з цих виробників пропонує свої власні набори IoT з різноманітними функціями та можливостями.

Розглянемо набір сенсорів від компанії Xiaomi Mi, які є частиною їх екосистеми розумного дому, яка пропонує різноманітні сенсорні пристрої для контролю різних аспектів оточення. До складу входять: Ось деякі переваги та недоліки цього набору: концентратор, два датчики руху, два датчики вікон, два датчики дверей і бездротова кнопка-вимикач.



Рисунок 1.5 – Набір сенсорів від компанії Xiaomi Mi

Переваги набору. Ціна – продукти Xiaomi Mi зазвичай відомі своєю доступністю і відмінним співвідношенням ціни та якості. Різноманітність – набір сенсорів Xiaomi Mi включає в себе різні типи сенсорів, такі як сенсори руху,

дверей/вікон, температурні сенсори тощо, що дозволяє користувачам створювати різноманітні сценарії автоматизації. Інтеграція з іншими пристроями - продукти Xiaomi Mi можуть бути легко інтегровані з іншими пристроями розумного дому, що базуються на популярних стандартах зв'язку, таких як Zigbee або Wi-Fi.

Недоліки. Специфічність - продукти Xiaomi Mi можуть бути менш сумісні з пристроями інших виробників, що використовують інші протоколи зв'язку або мають обмежену інтеграцію. Обмежена географічна доступність - деякі продукти Xiaomi Mi можуть бути доступні лише в обмежених регіонах, що обмежує їх доступність для споживачів з інших країн.

Однак готові набори для керування розумним складом мають високу вартість, тому більш доцільно застосувати мікроконтролер і виконати налаштування з'єднання та налаштування пристроїв, що підтверджує актуальність роботи. Для управління системою, яка має об'єднувати автоматизоване керування і зручний доступ користувача через різні пристрої, такі як комп'ютер, ноутбук, телефон і планшет необхідно застосування хмарної платформи.

## **1.6 Завдання і мета роботи**

Метою роботи є впровадження IoT-рішення в конфігурації та специфікації, що враховує специфіку підприємства «Yellow Vox» яке забезпечить ефективне та автоматизоване управління приміщеннями для зберігання речей. Головною метою є забезпечення комфорту та безпеки для користувачів, а також оптимізація витрат енергії та ресурсів. Наступні цілі необхідно реалізувати для впровадження роботи.

Визначити технічні вимоги реалізації системи.

Обрати архітектуру мережі.

Розробити специфікацію обладнання.

Виконати розрахунок мережі та налаштування обладнання.

Реалізувати систему, яка в реальному часі визначає присутність людей в приміщенні за допомогою датчиків руху або інфрачервоних сенсорів.

Забезпечити автоматичне регулювання освітлення в приміщенні в залежності від присутності людей та освітленості навколишнього середовища для забезпечення комфортних умов та енергоефективності.

Розробити систему відеоспостереження, яка забезпечить нагляд за приміщенням та допоможе у виявленні незвичайних подій або порушень безпеки.

Реалізувати систему керування температурою в приміщенні для забезпечення оптимальних умов для зберігання речей та комфорту користувачів.

Максимізувати енергоефективність системи шляхом інтелектуального керування освітленням та температурою в приміщенні з урахуванням режиму роботи та присутності людей.

## **1.7 Визначення можливих напрямків рішення поставлених задач**

У зв'язку з новим проектом для підприємства Yellow Box, є можливість вибрати найбільш підходящий напрямок для вирішення поставлених завдань. Існуючі підмережі підприємства відповідають його організаційній структурі. На поточному етапі топологія мережі компанії Yellow Box виглядає так, як показано на рисунку 1.6.



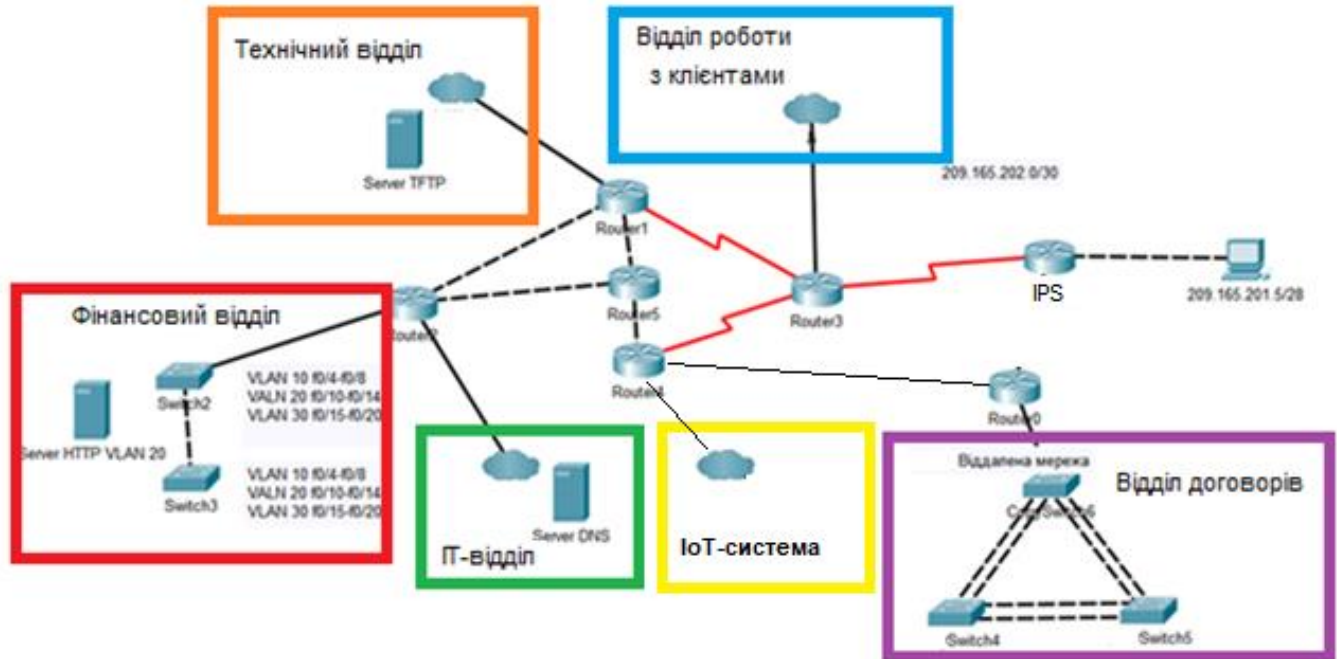


Рисунок 1.6 – Топологія мережі підприємства Yellow Vox

Чотири підмережі розташовані у офісі, а також мережа LAN\_5 для віддалених користувачів. Для комунікації використовуються маршрутизатори і комутатори від компанії Cisco. Зв'язок обладнання виконується за допомогою оптоволоконного кабелю.

Для вирішення поставлених завдань до існуючої мережі додається мережа розумних пристроїв LAN\_6, з обладнанням тієї ж фірми, що і для основної мережі. Використання оптоволоконного кабелю обумовлене його меншою вартістю, більшою довжиною сегментів та вищою швидкістю у порівнянні з мідним кабелем.

У підмережі відділу ІТ LAN\_2 буде встановлено сервер, на якому будуть зберігатися дані, зібрані з розумних датчиків ІоТ-системи. В мережі компанії Yellow Vox будуть здійснені налаштування для обмеження доступу до підмережі розумних пристроїв. Для роботи котеджів доступ до редагування і перегляду повинні мати тільки адміністратори.

## **2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ**

### **2.1. Технічні вимоги до 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 та ступені централізації Системи**

Комп'ютерна система (далі Система) підприємства Yellow Vox повинна складатись з шести підмереж. П'ять підмереж утворені для структурних підрозділів підприємства, такі як: відділ клієнтського обслуговування, технічний відділ, відділ ІТ, фінансовий відділ, відділ договорів. Розподіл виконаний згідно із загальною архітектурою мережі підприємства, що надана замовником (розділ ПЗ 1.5). Шоста підмережа виділена під IoT-систему.

В складі мережі підприємства Yellow Vox повинні бути налаштовані сервери HTTP, DNS, IoT та TFTP, та забезпечено справне функціонування. Сервери розподілені наступним чином: сервери HTTP в підмережі фін. відділу, DNS – в відділі роботи з клієнтами, TFTP та IoT мають бути розташовані у ІТ-відділі.

Система Інтернету речей підприємства Yellow Vox має бути реалізована на базі спеціального серверу із сервісом IoT та виділеного спеціалізованого маршрутизатору для зв'язку з усіма «розумними» пристроями цього компоненту Системи.

Система Інтернету речей підприємства Yellow Vox має бути впроваджена в наступних локаціях: коридори другого поверху та приміщення серверної кімнати на першому поверху.

Для серверної кімнати необхідно забезпечити: контроль присутності всередині та зовні кімнати; керування освітленням; контроль CO<sub>2</sub> із звуковим сповіщенням про небезпеку; відеоспостереження зовні кімнати.

Для коридорів другого поверху необхідно забезпечити: контроль присутності всередині та зовні боксу; керування освітленням відповідно до наявності людини; контроль температури та вологості всередині боксу зберігання; контроль CO<sub>2</sub> із звуковим сповіщенням про небезпеку; відеоспостереження коридорів.

#### **2.1.1.1.2. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами Системи**

Задля забезпечення користувачів мережі підприємства Yellow Box можливістю обміну даними інфраструктура компанії повинна включати використання комбінації провідних та бездротових технологій, таких як Ethernet, Wi-Fi, Bluetooth.

Для забезпечення зв'язку користувачів в підмережах корпоративної мережі підприємства Yellow Box необхідно:

- забезпечити розподіл IP-адрес з вихідної мережі 172.24.208.0/21;
- забезпечити розмір підмереж відповідно до вимог підприємства, а саме: відділ клієнтського обслуговування (68), технічний відділ (37), відділ ІТ(68), фінансовий відділ(219), відділ договорів (29), система ІоТ (76);
- забезпечити динамічну адресацію кінцевих мережних пристроїв в підмережах;
- забезпечити динамічну маршрутизацію в мережах WAN за протоколом EIGRP;
- забезпечити можливість віддаленого доступу до активних мережних пристроїв;

– забезпечити можливість віддаленого доступу до серверів підприємства Yellow Box із забезпеченням їх статичними адресами;

– забезпечити можливість працівникам підприємства Yellow Box вихід до мережі Internet, використовуючи технології NAT та PAT (внутрішні IP-адреси пристроїв КС змінювати на зовнішні з діапазону 209.165.200.5 - 209.165.200.30).

В підмережі фінансового відділу застосувати технологію VLAN для поділу її на три віртуальні підмережі: відділ менеджерів, відділ маркетингових, відділ бухгалтерів.

В підмережі IT-відділу об'єднати хости за технологією агрегації каналів EtherChannel.

Кабельні системи КС підприємства Yellow Box виконати за технологією Ethernet. Для системи Інтернету речей забезпечити можливість застосування технології бездротового зв'язку WiFi.

Обмін інформацією між компонентами Системи повинен відбуватись відповідно до стандартних протоколів передачі даних на рівні програмного забезпечення.

#### **2.1.1.1.3. Вимоги до діагностування Системи**

Для виявлення проблем у Системі та їх типу адміністратор системи повинен мати можливість переглядати поточні налаштування мережевих та інших пристроїв. На активних мережних пристроях повинні бути налаштовані лінії VTU з протоколом доступу SSH. Якщо виявлено проблеми мережевого характеру, рекомендується використання діагностичних інструментів (утиліти) такі як ping або tracert, для перевірки доступності мережевих пристроїв та виявлення проблем у мережевому зв'язку, а також систем моніторингу мережі для виявлення аномалій у трафіку та виявлення можливих проблем у мережевому з'єднанні.

#### **2.1.1.1.4. Перспективи розвитку, модернізації Системи**

Розподіл виділеної провайдером IP-адреси 172.24.208.0/21 для організації сегментації мережі з огляду до майбутніх викликів, інновацій та покращення продуктивності.

Для модернізації Системи необхідно передбачити наступні напрями: збільшення кількості активних мережевих вузлів (рекомендовано закладати можливість додавання нових мережевих вузлів для поліпшення покриття та надійності мережі); впровадження мережевої аналітики (використання мережевих аналітичних інструментів для збору та аналізу даних про трафік, дає змогу виявляти аномалії, оптимізувати роботу мережі та виявляти проблеми); підвищення масштабованості мережі (закласти можливості для підвищення масштабованості мережі для відповіді на зростаючі потреби бізнесу та користувачів – не менш як 20 вузлів в кожній підмережі).

#### **2.1.1.2 Вимоги до показників призначення**

IoT система індивідуального зберігання інвентарю підприємства «Yellow Box» повинна забезпечувати наступні показники призначення:

- контроль присутності всередині та зовні боксу;
- керування освітленням відповідно до наявності людини;
- контроль температури та вологості всередині боксу зберігання;
- контроль CO<sub>2</sub> із звуковим сповіщенням про небезпеку;
- відеоспостереження коридорів;
- зберігання даних на сервері IoT;
- керування «розумними» речами відповідно до алгоритму.

До складу мережі повинно входити шість підмереж з визначеною кількістю кінцевих мережних пристроїв: відділ клієнтського обслуговування (68 вузлів), технічний відділ (37 вузлів), відділ IT(68 вузлів), фінансовий відділ(219 вузлів), відділ договорів (29 вузлів), система IoT (76 вузлів).

Інтенсивність трафіку в мережі  $\mu = 176$  (кадрів/с).

Використовувати вихідний блок адрес 172.24.208.0/21.

Статична зовнішня адреса HTTP-сервера у підмережі фінансового відділу 209.165.220.10.

Середня довжина повідомлень в мережі підприємства складає 690 байт.

Затримка передачі пакету в найбільшій мережі не більше  $\leq 6$  мс.

### **2.1.1.3 Вимоги до експлуатації**

#### **2.1.1.3.1 Умови і режим експлуатації, що повинні забезпечувати використання технічних засобів Системи з заданими технічними показниками**

Технічні засоби IoT повинні функціонувати в діапазоні температур від  $-20^{\circ}\text{C}$  до  $+50^{\circ}\text{C}$ .

Відносна вологість повітря у приміщеннях зберігання не повинна перевищувати 90% без конденсації.

Обладнання повинно мати ступінь захисту не менше IP65.

Технічні засоби повинні живитися від стабільного джерела постійного струму з напругою 12-24 В, або через адаптер від стандартної електричної мережі 220 В.

Система повинна бути обладнана резервним джерелом живлення для забезпечення безперебійної роботи при перебоях у мережі. Для безперервної передачі даних IoT пристрої повинні бути підключені до мережі через Wi-Fi, Ethernet або мобільний зв'язок (GSM/4G).

Використання резервних каналів зв'язку забезпечує високу надійність передачі даних. Система повинна включати засоби автентифікації і шифрування даних для захисту інформації від несанкціонованого доступу, що забезпечує конфіденційність і безпеку даних користувачів.

Обладнання має бути оснащено засобами для дистанційного моніторингу і діагностики стану пристроїв, що дозволяє своєчасно виявляти і усувати несправності, знижуючи ризик простоїв.

Технічні засоби повинні підтримувати можливість віддаленого оновлення програмного забезпечення для впровадження нових функцій і виправлення виявлених помилок.

Система повинна працювати в цілодобовому режимі, забезпечуючи постійний доступ користувачів до інвентарю, а обслуговування і технічні роботи повинні проводитися в години мінімального навантаження для зниження впливу на користувачів.

#### **2.1.1.3.2 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи**

Кількість обслуговуючого персоналу визначається відповідно до поточних потреб компанії, забезпечуючи ефективне управління та обслуговування всіх «Yellow Box» об'єктів. Персонал повинен мати необхідну кваліфікацію в сфері логістики, безпеки та управління майном, а також володіти навичками роботи з клієнтами. Обслуговуючий персонал повинен володіти знаннями з використання системи управління «Yellow Box» об'єктами, включаючи програмне забезпечення для моніторингу та контролю доступу.

Режими роботи персоналу мають бути організовані таким чином, щоб забезпечити безперебійну роботу компанії та задовольнити потреби клієнтів у доступі до своїх боксів у будь-який час. Це передбачає чергування персоналу, щоб забезпечити цілодобову підтримку та реагування на запити клієнтів. Окрім цього, персонал повинен регулярно проходити тренінги та навчання для підвищення кваліфікації та ознайомлення з новими технологіями та методами в сфері зберігання майна.

### **2.1.1.3.3 Вимоги до складу, розміщенню й умовам збереження комплекту запасних виробів і приладів**

Мають бути у наявності компоненти для швидкої заміни та ремонту основних частин Системи, такі як сенсори, контролери, мережеві адаптери, джерела живлення, резервні акумулятори, корпуси для захисту електроніки, кабелі та конектори.

Запасні частини повинні зберігатися в спеціально відведеному приміщенні або зоні з чітким маркуванням та інвентарним обліком.

Умови зберігання мають відповідати вимогам щодо температури від  $-10^{\circ}\text{C}$  до  $+30^{\circ}\text{C}$  та вологості не більше 75%, приміщення повинно бути захищене від прямих сонячних променів, пилу і вологи, а також обладнане системою вентиляції.

Приміщення повинно бути оснащено системами безпеки, такими як сигналізація, відеоспостереження і контроль доступу.

Необхідно проводити регулярний контроль і облік запасних частин через інвентаризації та ведення журналу обліку.

### **2.1.1.3.4 Вимоги до регламенту обслуговування**

Інструкції з експлуатації повинні встановлювати види, частоту та регламент обслуговування технічних засобів, причому це повинно проводитися не рідше одного разу на рік.

## **2.1.2 Вимоги до налаштувань, які виконуються у Системі**

Налаштування доступу – забезпечення контролю за доступом до системи та інвентарю через автентифікацію користувачів та встановлення прав доступу на основі ролей.



Моніторинг стану – налаштування системи моніторингу для постійного спостереження за станом інвентарю, включаючи виявлення несправностей та вчасну реакцію на них.

Зберігання даних – налаштування системи зберігання даних для збереження інформації про стан інвентарю, історію його використання та інші важливі дані.

Керування інвентарем – налаштування функціоналу керування інвентарем, включаючи можливість віддаленого керування, реєстрацію змін та аудит дій користувачів.

Взаємодія з іншими системами – налаштування інтеграції з іншими системами, такими як системи управління запасами або системи безпеки, для обміну даними та координації роботи.

Захист даних – налаштування засобів захисту даних, включаючи шифрування та забезпечення конфіденційності та цілісності інформації.

Автоматизація процесів – налаштування автоматичних процесів, таких як автоматичне оновлення програмного забезпечення або виконання регулярних перевірок стану інвентарю.

### **2.1.3 Вимоги до видів забезпечення Системи**

#### **2.1.3.1 Вимоги до інформаційного забезпечення**

Має бути забезпечене точного та надійного збереження даних про стан інвентарю, моніторинг і аналіз цього статусу, підтримку журналювання та аудиту для відстеження змін, інтеграцію з іншими системами управління запасами, захист конфіденційності та цілісності даних, а також автоматизацію процесів збереження та обробки даних для підвищення ефективності та зручності користування системою.

### **2.1.3.2 Вимоги до лінгвістичного забезпечення**

Інтерфейс Системи має бути легко зрозумілий для користувачів, з можливістю вибору мови, підтримки міжнародних стандартів у виведенні інформації та взаємодії з користувачами, а також якісний переклад та інтерпретацію даних для різних мовних груп користувачів.

### **2.1.3.3 Вимоги до технічного забезпечення**

Система індивідуального зберігання інвентарю має включати наявність надійних сенсорів та пристроїв зберігання даних, швидкість та стабільність мережевого зв'язку, можливість віддаленого керування та моніторингу, високий рівень захисту даних та конфіденційності, сумісність з іншими пристроями та системами, а також енергоефективність та довгий термін служби обладнання.

### **2.1.3.4 Вимоги до організаційного забезпечення**

Обслуговуючий персонал повинен мати відповідну кваліфікацію, та регулярно проходити тренінги з експлуатації та обслуговування Системи.

Необхідно організувати цілодобову службу технічної підтримки для вирішення технічних проблем або запитів користувачів.

Система повинна бути обладнана засобами моніторингу для постійного спостереження за станом обладнання та його продуктивністю.

Важливо впровадити процедури безпеки, включаючи автентифікацію та шифрування даних, щоб захистити систему від несанкціонованого доступу. Дотримуватися регламенту обслуговування, який включає регулярні перевірки та технічне обслуговування, є обов'язковим.

Необхідно вести актуальну документацію, яка містить інструкції з експлуатації, технічні описи та журнали обслуговування.

## **2.2 Розробка апаратної частини IoT системи**

### **2.2.1 Розробка загальної структури комп'ютерної системи**

Відповідно до ієрархічної моделі побудови архітектури мережі від компанії Cisco, відомої як Cisco Hierarchical Network Design Model, можна розділити функції мережі на логічні рівні, що полегшує розробку, управління та розширення мережі. Кожен рівень відповідає за свої конкретні завдання і може бути легко масштабований або модифікований відповідно до потреб бізнесу.

Виходячи з цього принципу комплекс технічних засобів КС підприємства «Yellow Box» розділені на три рівні.

Перший рівень (Core Layer) склали маршрутизатори в кількості п'яти. Маршрутизатори Rout\_YB\_0 – Rout\_YB\_4, призначені для сегментації мережі на підмережі. Маршрутизатор Rout\_YB\_5 виконує роль резервного.

Другий рівень (Distribution Layer) представлений комутаторами в кількості семи. Комутатори підмереж Технічного відділу, Відділу роботи з клієнтами, Відділу роботи з договорами виконують об'єднання хостів в локальну мережу. Два комутатори підмережі фінансового відділу за технологією VLAN розділяють її на ще три підмережі: менеджери, маркетологи, бухгалтери. Три комутатори підмережі IT-відділу об'єднують хости за технологією агрегації каналів EtherChannel.

Третій рівень (Access Layer) представлений персональними комп'ютерами співробітників компанії «Yellow Box», мережними принтерами в підмережах Відділу роботи з клієнтами та Відділу роботи з договорами, сервери компанії та «розумними речами» IoT системи.

Підмережі в компанії з'єднуються за допомогою кабелів Serial, Gigabit та Fast Ethernet, які з'єднують комутатори та маршрутизатори у локальних мережах підприємства «Yellow Box».

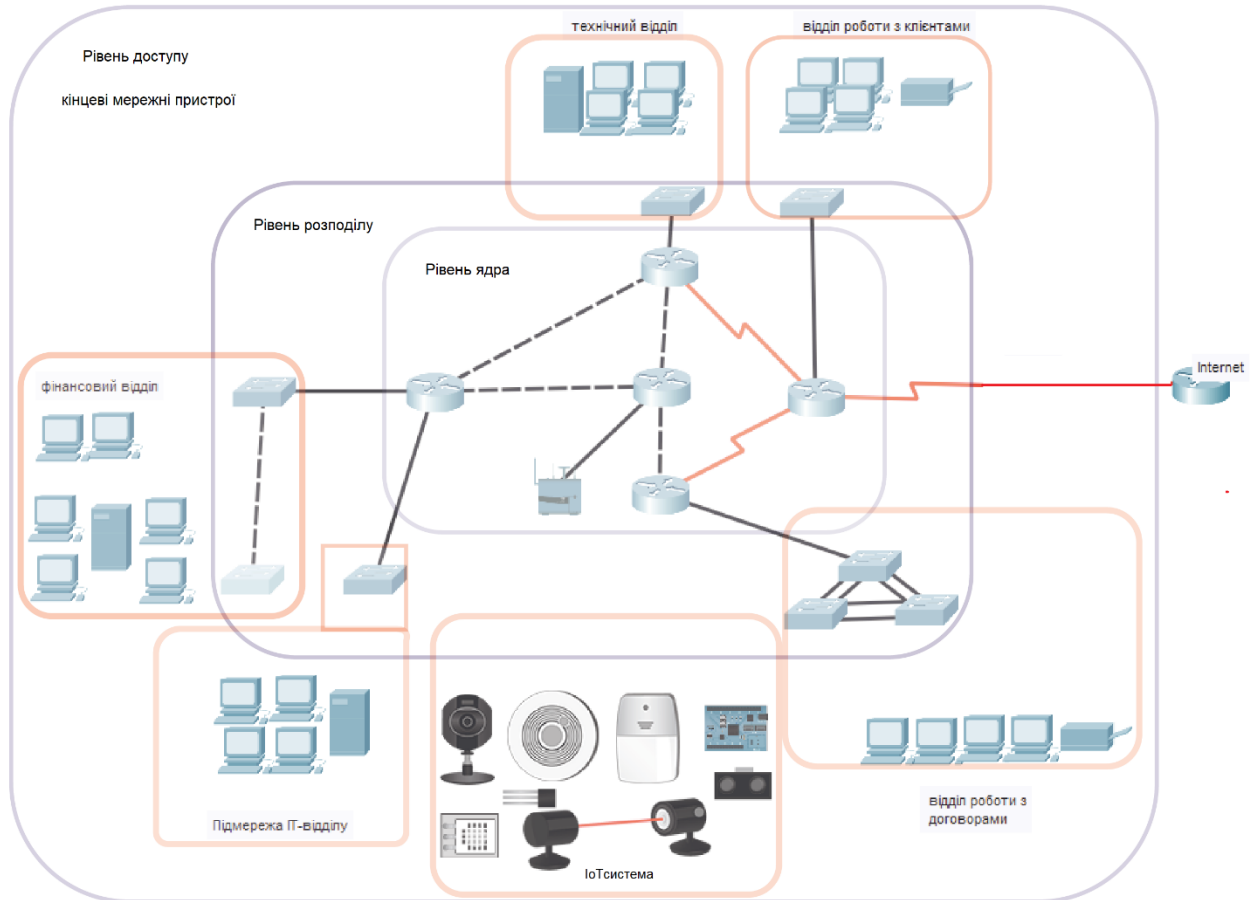


Рисунок 2.1 – Структурна схема комплексу технічних засобів

### 2.2.2 Розробка структури комплексу технічних засобів IoT системи

Структурна схема комплексу технічних засобів IoT системи підприємства «Yellow Box» складається з рівнів відповідно до архітектури IoT.

Дотримання архітектури IoT яка виділяє п'ять рівнів (Things, Getway, Network, Cloud, Application), що взаємодіють між собою, утворюючи повноцінну архітектуру IoT, дозволяє збирати, обробляти та використовувати дані з різноманітних пристроїв для досягнення визначених цілей та завдань.

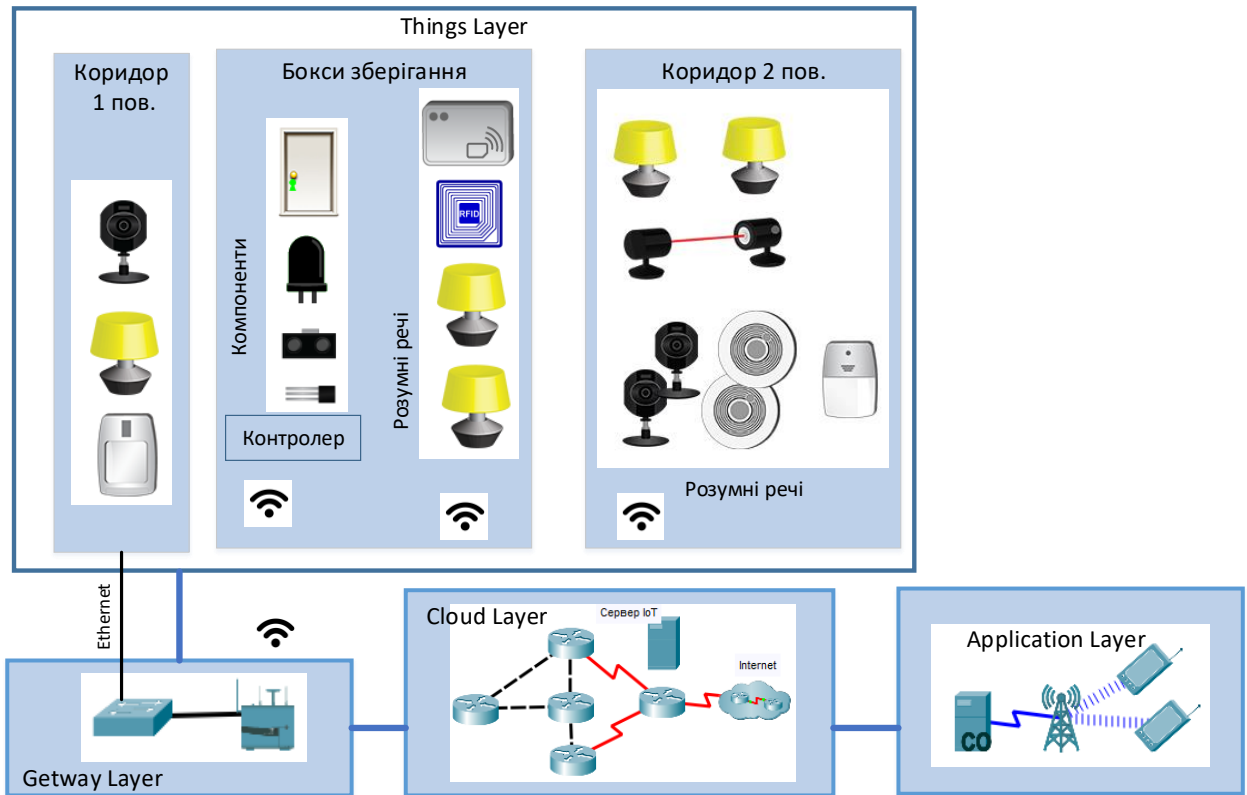


Рисунок 2.2 – Структурна схема комплексу технічних засобів IoT системи

Пристрої (Things). На цьому рівні знаходяться фізичні пристрої, такі як сенсори, контролери, розумні пристрої та інші пристрої IoT, які здатні до збору даних або керувати навколишнім середовищем.

В боксах зберігання розташовані як компоненти так і «розумні» речі. В боксах розташовані наступні компоненти: датчик температури для контролю температури в межах  $+12^{\circ}\text{C}$  до  $27^{\circ}\text{C}$  відповідно до вимог, датчик перетину для контролю присутності в приміщенні, діоди візуального сповіщення невідповідності температури, замок електромеханічний з доступом за RFID. Компоненти передають дані та керуються контролером, який аналізує дані та передає на сервер IoT. «Розумні» речі в зоні бокса: лампи освітлення та RFID-приймач за технологією WiFi мають доступ до шлюза системи IoT – маршрутизатора типу «Home gateway» з підтримкою технологій WiFi та Ethernet.

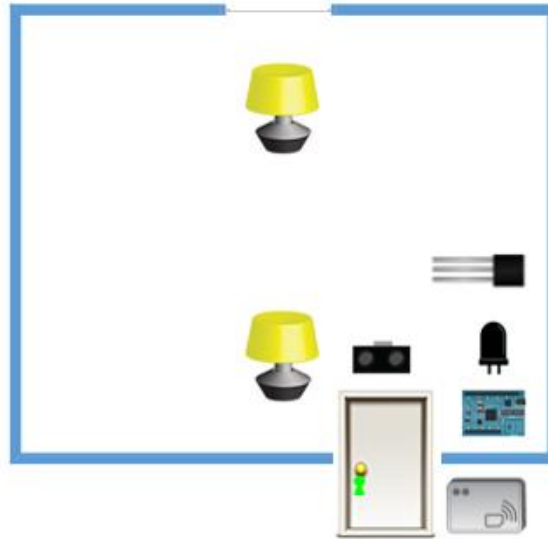


Рисунок 2.3 – План розміщення пристроїв IoT системи в боксі

В коридорі другого поверху будівлі встановлені наступні пристрої IoT. Датчики перетину за сигналами яких контролюється присутність людей та виконуються вмикання камер спостереження та освітлення. Специфічною особливістю приміщень під склади індивідуального зберігання речей невеликих об'ємів є довгі коридори та нечасте відвідування комір орендаторами. Тому освітлення вмикається за наявністю в коридорі людей. Розташування датчиків перетину, камер та освітлення наведено на рисунку 2.3.

Також для виявлення небезпеки виникнення задимленості або пожеж в коридорах встановлені датчики виявлення диму та сирена для звукового сповіщення про загрозу.

На першому поверсі знаходиться серверна. Для контролю доступу до неї встановлені наступні Smart пристрої IoT з підтримкою технології WiFi. Інфрачервоний датчик виявлення руху за сигналом якого вмикаються web-камера та освітлення. Отримані дані передаються до серверу IoT. Так як відстань між місцем встановлення роутера Home Gateway DLC-100 виходить за межі зони

покриття WiFi в серверній встановлена додаткова бездротова точка доступу для підключення пристроїв даної зони до роутера.

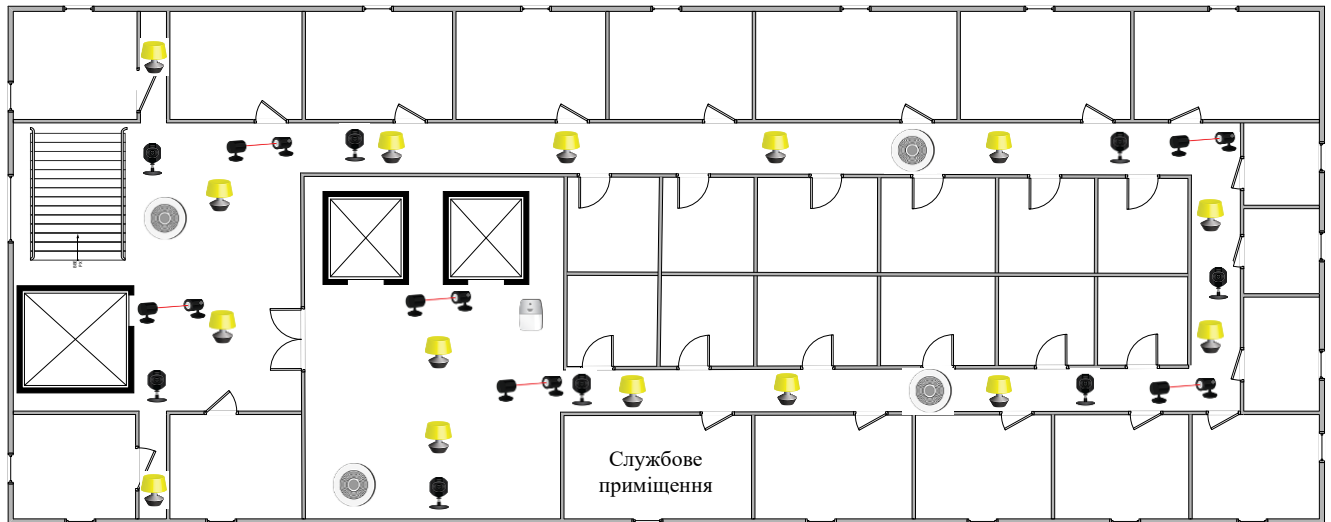


Рисунок 2.4 – План розміщення пристроїв IoT системи поверх 2

Рівень шлюзів і мереж (Cloud) в системі IoT виконує ключову функцію у забезпеченні комунікації та обміну даними між пристроями IoT та центральними системами, дозволяючи збирати та аналізувати дані для прийняття рішень. Цей рівень також забезпечує гнучкість та масштабованість системи IoT, дозволяючи легко інтегрувати нові пристрої та розширювати функціональність мережі.

Шлюзами в системі IoT підприємства «Yellow Vox» є контролери, роутер Home Gateway DLC-100 та бездротова точка доступу. Шлюзи – це пристрої, які виступають посередниками між пристроями IoT, що працюють у різних мережах або протоколах зв'язку, і центральними системами. Вони здійснюють конвертацію та агрегацію даних, а також можуть виконувати функції локального аналізу даних перед їх відправкою до хмари.

На рівні мереж в системі IoT Yellow Vox використані мережні технології, такі як Wi-Fi та Ethernet. Ці мережі забезпечують зв'язок між пристроями IoT та шлюзами.

Рівень хмарних сервісів (Cloud Services) в системі IoT підприємства «Yellow Box» представлений віддаленим сервером IoT, що за логічною топологією мережі знаходиться в підмережі IT-відділу. Сервером здійснюється зберігання, обробка та аналіз даних, зібраних від пристроїв IoT. Включає в себе рішення для обробки великих обсягів даних та аналітики для винесення розумних рішень.

Рівень додатків (Applications) в системі IoT підприємства «Yellow Box» представлений наявністю функціоналу для отримання даних спостереження з баксів зберігання речей на смартфон користувача. Цей рівень представляє собою ПЗ з яким взаємодіє користувач.

### **2.2.3 Розробка специфікації апаратних засобів IoT системи**

У процесі розробки системи Інтернету речей для компанії індивідуального зберігання речей "Yellow Box" для приватних орендарів, критичним кроком є відбір апаратних засобів і елементної бази. Цей важливий відбір вплине на взаємодію пристроїв між собою та збір, обробку та передачу даних. Далі буде докладно розглянуто обрані пристрої та компоненти, що забезпечують виконання функціоналу системи IoT.

У якості хабу системи Інтернету речей буде використано рішення від компанії Cisco DLC-100.

Cisco DLC-100 – це концентратор і маршрутизатор для пристроїв Інтернету речей, який також виконує функції сервера для збору, обробки та передачі інформації між IoT-пристроями. Крім того, він забезпечує веб-інтерфейс, що дозволяє користувачам здійснювати моніторинг та керування різноманітними розумними пристроями. Домашні пристрої можуть підключатися до домашнього шлюзу через бездротовий або дротовий зв'язок. Технічні характеристики цього пристрою наведені в таблиці 2.1.



Таблиця 2.1 – Технічна характеристика Cisco DLC-100

Назва	Параметр
ЦП	RK3568 ARM® чотирьох ядерний 64-бітний процесор, ARM G52 2EE, OpenCL 2.0, Vulkan 1.1
ОЗП	4GB двоканальна 64Bit LPDDR4
eMMC	До 128 ГБ
ОС	Debian10
Діапазон покриття	250 метрів
Порти	1 x USB 3.0, 1x Internet, 4 x Gigabit Ethernet,
Бездротовий протокол	Wi-Fi

В якості датчику руху було обрано рішення від компанії Intervision IoT-PIR.

Датчики на основі технології PIR (піроелектричний) виявляють рухомі об'єкти, які мають інфрачервоне випромінювання.

Таблиця 2.2 – Технічна характеристика Intervision IoT-PIR

Назва	Параметр
Тип	бездротовий
Дальність детектування руху	12 метрів
Горизонтальний / вертикальний кут детектування руху	110°/ 90°
Максимальна відстань до хаба	100м
Джерело живлення	DC12V/3A
Тип елемента живлення	3V CR123A
Бездротовий протокол	Wi-Fi

Для реалізації відеонагляду обрана камера Cruiser 2 (IPC-GS7EP-5M0WE). Відеокамера Cruiser 2 Wi-Fi Imou підходить для реалізації IoT системи нагляду з огляду на технічні вимоги.

Таблиця 2.3 – Технічна характеристика InterVision WFX-AI4

Назва	Параметр
Тип	бездротова
Тип матриці	1/2.7" Aptina AR0522 CMOS sensor. 5 Мп
ІЧ-підсвітка	30 метрів
Аудіоінтерфейси	вбудований мікрофон і динамік
Максимальна відстань до хаба	100м
Живлення	DC 12В 1А
Регулювання за осями	0~340° Поворот; 0~90° Наклон
Бездротовий протокол	Wi-Fi

Для реалізації розумного освітлення обрана Wi-fi LED лампа Yeelight YLDP007.

Таблиця 2.4 – Технічна характеристика YLDP007

Назва	Параметр
Тип	бездротова
Цоколь	E27
Максимальна потужність	8W
Максимальна відстань до хаба	100м
Живлення	220 В
Бездротовий протокол	Wi-Fi

Для реалізації доступу в приміщення обраний бездротовий Smart замок ZKTeco GL300W Wi-Fi.

Таблиця 2.4 – Технічна характеристика ZKTeco GL300W

Назва	Параметр
Тип	електроригельний
Стан без живлення	закритий (NC)
Живлення	4 батареї AA
Максимальна відстань до хаба	100м
Спосіб відкриття	кодом, картою, брелоком
Бездротовий протокол	Wi-Fi
Пам'ять RFID карт	100

Для реалізації контролю задимленості в коридорах обраний бездротовий Smart Earykong (JY-GZ-01AQ).

Таблиця 2.4 – Технічна характеристика Earykong

Назва	Параметр
Тип детектування	дим
Тип підключення	бездротовий
Живлення	2 батареї ААА
Максимальна відстань до хаба	100м
Бездротовий стандарт	Wi-Fi

Для реалізації туманих обчислень та рівня доступу до мережі (Gateway) в системі IoT боксів зберігання компанії «Yellow Box» обрані наступні компоненти.

Базою для побудови системи є контролер Arduino Nano IoT. Дана модель об'єднує модуль зв'язку Wi-Fi і функціональні можливості мікропроцесора в одному чіпі. Перевагами Arduino Nano IoT є мікропроцесор ESP32 з частотою 240 МГц, наявність 14 цифрових та 8 аналогових I/O, вбудований модуль Wi-Fi, об'єм пам'яті SRAM 32КБ / Flash 2КБ.

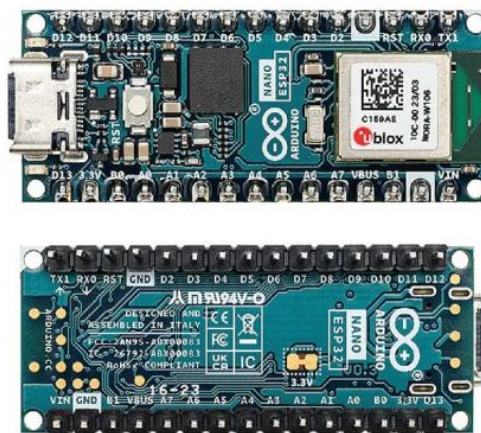


Рисунок 2.5 – Плата Arduino Nano IoT



Підключення модуля реле до Ардуіно використане для керування за допомогою мікроконтролера потужним навантаженням зі змінним струмом. Реле – це електромеханічний пристрій, що використовується для замикання і розмикання електричного кола за допомогою електромагніту. Коли на електромагнітну котушку подається керуюча напруга, в ній створюється електромагнітне поле, яке притягує металеву пластину і замикає контакти потужного навантаження. Таким чином, за допомогою SRD-05VDC здійснюється керування освітленням у приміщеннях боксів для зберігання речей.

#### 2.2.4 Розробка переліку вхідних та вихідних сигналів

У таблиці 2.6 наведено опис сигналів, які є вхідними для IoT-системи.

У таблиці 2.7 наведено опис керованих компонентів, для яких IoT-система виробляє вихідні сигнали.

Таблиця 2.6 – Вхідні сигнали

№	Найменування інформації	Ідентифікатор	Отрим.	Функція	Вид	Тип сигналу
1	Датчик температури LM35DZ	DT	A0	Контр.	Аналог.	5В
2	Датчик виявлення руху HC-SR501	PIR1	D9	Контр.	Дискр.	3,3 В
3	Датчик виявлення руху HC-SR501	PIR2	D10	Контр.	Дискр.	3,3 В

Таблиця 2.7 – Вихідні сигнали

№	Найменування інформації	Ідентифікатор	Отрим.	Функція	Вид	Тип сигналу
1	Реле (вмикання/вимикання) SRD-05VDC-SL-C	PIR1	D11	Кер.	Дискр.	5В
2	Реле (вмикання/вимикання) SRD-05VDC-SL-C	PIR2	D12	Кер.	Дискр.	5В
3	Світлодіод Led	LED	D13	Кер.	Дискр.	2,8 В

### 2.2.5 Розробка принципової схеми

Принципова схема підсистеми для боксів зберігання речей з урахуванням вимог та забезпечення функціоналу наведена на рис. 2.6.

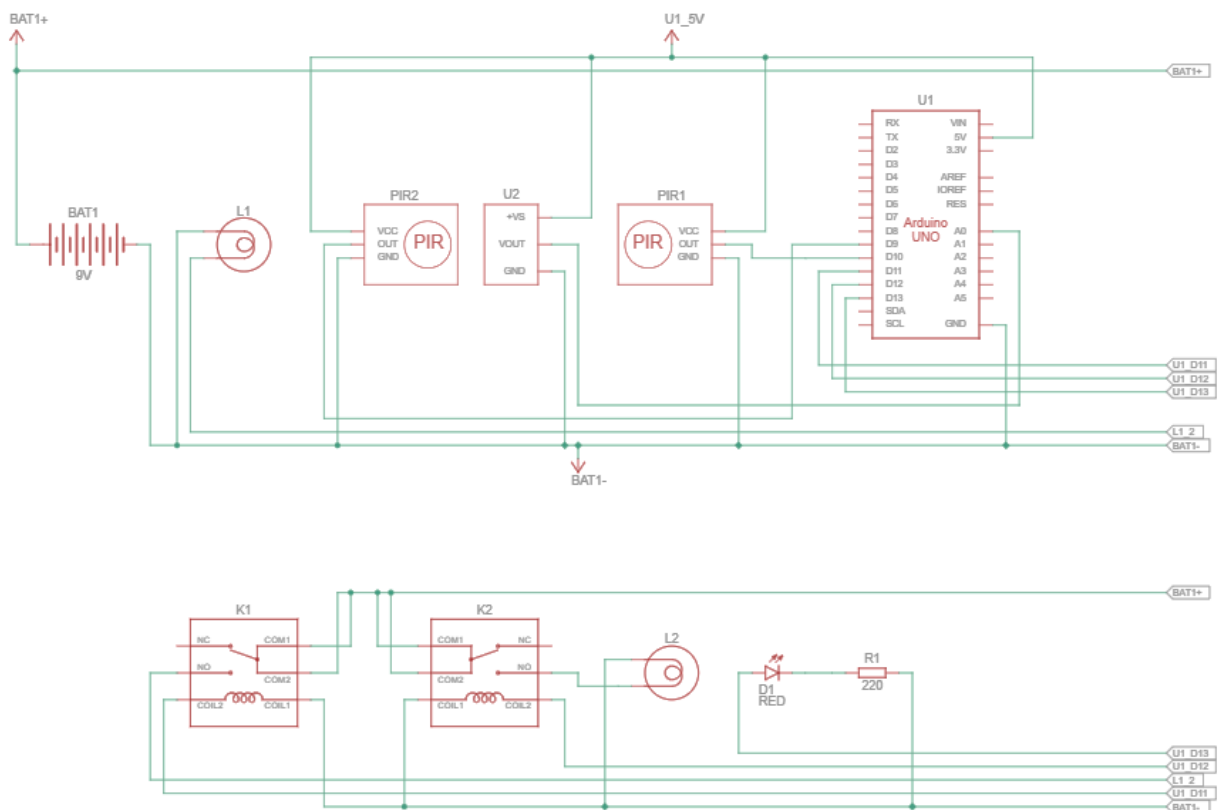


Рисунок 2.6 – Схема принципова

## 2.2.6 Розрахунок інтенсивності вихідного трафіку найбільшої LAN Yellow Box

В підмережі «Відділ внутрішній» встановлений комутатор Cisco 2960-24TC-L та маршрутизатор 2901/K9, що об'єднують кінцеві мережні пристрої. Використовується лінія з пропускною здатністю 1000 Мбіт/с. Середня інтенсивність трафіку LAN Yellow Box  $\mu=176$  (кадрів/с) та середня довжина повідомлення – 650 байт. Загальна кількість хостів  $N = 90$ .

Пропускна здатність:

$$Pr.p = \mu * l * N * 8 = 176 * 650 * 90 * 8 = 60,4 \text{ (Мбіт/с), де}$$

Загальне навантаження на комутатор:

$$\mu_{\text{вих}} = 1000 \text{ 000 000} / (650 * 8) = 43333 \text{ пакетів/с}$$

Максимум приєднання:

$$N = 43333 / 176 = 301 \text{ джерел.}$$

Інтенсивність вихідного трафіку:

$$\lambda = N * \mu = 90 * 176 = 12900 \text{ (пакетів/с)}$$

Коефіцієнт затримки на рівні розподілу:

$$\rho = \frac{\lambda}{\mu_{\text{вих}}} = \frac{12900}{43333} = 0,32$$

Коефіцієнт зайнятості комутатора:

$$r = \frac{\rho}{1 - \rho} = \frac{0,12}{1 - 0,12} = 0,02$$

Середня затримка кадру:

$$T = \frac{1}{(\mu - \lambda)} = \frac{1}{43333 - 12600} = 2,9 * 10^{-6} \text{ с}$$

Середня довжина черги:

$$\mathcal{L}_{\text{чер}} = \frac{\rho^2}{1 - \rho} = \frac{0,12^2}{1 - 0,12} = 0,001$$

Середній час перебування пакета в черзі:

$$T_{\text{оч}} = \frac{L_{\text{чер}}}{\lambda} = \frac{0,001}{12900} = 0,79 \text{ мкс}$$

Це значення менше необхідного значення 6 мс, що задовольняє вимогам.

Пропускна здатність каналу:

$$\lambda = \frac{\text{пропускна здатність}}{\text{довжина кадру}} = \frac{b}{l}$$

$$b = \lambda * l = 12590 * 650 * 8 = 60278000 \text{ біт/с} = 60,3 \text{ Мбіт/с}$$

Що відповідає пропускній здатності вихідного каналу в 1000 Мбіт/с.



### 3 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

#### 3.1 Розрахунок схеми адресації корпоративної мережі «Yellow Box»

Для побудови КС підприємства «Yellow Box», відповідно до технічних вимог, при розрахунках IP-адресації мережі використаний адресний простір 172.24.208.0/21. Адреса мережі WAN каналів 10.0.9.0/24.

Розподіл вихідної IP-адреси мережі на підмережі виконаний із застосуванням таких технологій як CIDR і VLSM.

Кількість вузлів в підмережах зазначена в п. 2.2.1.3.

Кількість віртуальних мереж 3.

Таблиця 3.1 – Схема адресації мережі компанії Yellow Box

Назва підмережі	Розмір	Адреса	Десяткова маска	Діапазон доступних адрес
LAN5 Відділ фінансовий	219	172.24.208.0	255.255.255.0	172.24.208.1 - 172.24.208.254
LAN6 Система IoT	70	172.24.209.0	255.255.255.128	172.24.209.1 - 172.24.209.126
LAN2 Відділ клієнтського обслуговування	68	172.24.209.128	255.255.255.128	172.24.209.129 - 172.24.209.254
LAN3 відділ IT	68	172.24.210.0	255.255.255.128	172.24.210.1 - 172.24.210.126
LAN4 Технічний відділ	37	172.24.210.128	255.255.255.192	172.24.210.129 - 172.24.210.190
LAN1 Відділ договорів	29	172.24.210.192	255.255.255.224	172.24.210.193 - 172.24.210.222
VLAN39	30	172.24.208.0	255.255.255.224	172.24.208.1 - 172.24.208.30

Продовження таблиці 3.1

VLAN49	30	172.24.208.32	255.255.255.224	172.24.208.33 - 172.24.208.62
VLAN59	30	172.24.208.64	255.255.255.224	172.24.208.65 - 172.24.208.94
VLAN99	10	172.24.208.96	255.255.255.240	172.24.208.97 - 172.24.208.110
WAN1	2	10.0.9.0	255.255.255.252	10.0.9.1 - 10.0.9.2
WAN2	2	10.0.9.4	255.255.255.252	10.0.9.5 - 10.0.9.6
WAN3	2	10.0.9.8	255.255.255.252	10.0.9.9 - 10.0.9.10
WAN4	2	10.0.9.12	255.255.255.252	10.0.9.13 - 10.0.9.14
WAN5	2	10.0.9.16	255.255.255.252	10.0.9.17 - 10.0.9.18
WAN IPS	2	209.165. 202.0	255.255.255.224	209.165.202.1- 209.165.202.2
WAN Remout	2	64.100.13.0	255.255.255.252	64.100.13.1- 64.100.13.2
LAN IPS	2	209.165.200.0	255.255.255.0	209.165.200.1 - 209.165.200.254

В таблиці 3.2 представлена схема IP-адресації пристроїв мережі КС підприємства «Yellow Box».

Таблиця 3.2 – Схема адресації пристроїв мережі

Ім'я пристрою	Інтер- фейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключе ного пристрою
LAN2 Відділ клієнтського обслуговування						
Sharapov_R3	S0/2/0	10.0.9.16	/30	-	-	S0/2/0
	S0/1/0	10.0.9.20	/30	-	-	S0/1/0
	G0/0	172.20.209.129	/25	-	-	G0/0
	S0/2/0	209.165.202.1	/30	-	-	S0/0/0
Sharapov_Sw2	Vlan1	172.20.209.130	/25	172.20.209.129	-	G0/1
PC1 - PC8	NIC	172.24.209.246 - 172.24.209.254	/25	172.20.209.129	-	Fa0/1- Fa0/8
Printer1	NIC	172.24.209.139	/25	172.20.209.129	-	Fa0/10
LAN3 відділ IT						
Sharapov_R2	G0/1	172.24.210.1	/25	-	-	G0/1

## Продовження таблиці 3.2

Sharapov_Sw3	Vlan1	172.24.210.2	/25	172.24.210.1		G0/2
PC1- PC9	NIC	172.24.210.126- 172.24.210.117	/25	172.24.210.1	-	F0/0-F0/9
Server_DNS	NIC	172.24.210.10	/25	172.24.210.1	-	Fa0/24
Server HTTP	NIC	10.22.186.9	/24	10.22.186.1	-	Fa0/24
<b>LAN4 Технічний відділ</b>						
Sharapov_R1	G0/1	172.24.210.129	/26	-	-	G0/1
Sharapov_Sw4	Vlan1	172.24.210.130	/26	172.24.210.129	-	G0/1
PC1- PC8	NIC	172.24.210.190- 172.24.210.182	/26	172.24.210.129	-	F0/0-F0/8
Server_TFTP	NIC	172.24.210.139	/26	172.24.210.129	-	Fa0/24
<b>LAN1 Відділ договорів</b>						
Sharapov_R4	G0/0	172.24.210.193	/30	-	-	G0/0
Sharapov_S1	Vlan1	172.24.210.194	/25	172.24.210.193	-	G0/1
Sharapov_S2	Vlan1	172.24.210.195	/25	172.24.210.193	-	G0/1
Sharapov_S3	Vlan1	172.24.210.196	/25	172.24.210.193	-	G0/1
PC1- PC9	NIC	172.24.210.222- 172.24.210.216	/25	172.24.210.193	-	F0/0-F0/9
Printer2	NIC	172.24.210.198	/25	172.24.210.193	-	Fa0/10
DLC100	Internet	172.24.209.1	/24	-	-	G0/2
IoT1 - IoT14	Wireless	192.168.25.100- 192.168.25.114	/24	192.168.25.1	-	Wireless
AccessPoint	Port0	172.24.210.203	/24	172.24.210.193	-	Fa0/19
<b>LAN5 Відділ фінансовий</b>						
Sharapov_R2	G0/1	-	-	-	-	-
	G0/1.39	172.24.208.1	/27	-	18	G0/1
	G0/1.49	172.24.208.33	/27	-	28	G0/1
	G0/1.59	172.24.208.65	/27	-	38	G0/1
	G0/1.99	172.24.208.97	/27	-	99	G0/1
	S0/0/0	10.0.9.1	/30	-	-	S0/0/0
	S0/1/0	10.0.9.5	/30	-	-	S0/1/0
PC39.1-PC39.4	NIC	172.24.208.30- 172.24.208.26	/27	172.24.208.1	39	Fa0/4- Fa0/8
PC49.1-PC49.5	NIC	172.24.208.62- 172.24.208.58	/27	172.24.208.33	49	Fa0/10- Fa0/14
PC59.1-PC59.5	NIC	172.24.208.94- 172.24.208.90	/27	172.24.208.65	59	Fa0/15- Fa0/20
Server TFTP	NIC	172.24.208.43	/27	172.24.208.33	49	Fa0/24
Sharapov_Sw2.1	G0/1	172.24.208.98	/27	172.24.208.97	99	G0/1
Sharapov_Sw2.2	G0/2	172.24.208.99	/27	172.24.208.97	99	G0/2
<b>IPS</b>						
Rout_IPS	F4/0	209.165.202.2	/27	-	-	F4/0
HC	F1/0	209.165.200.1	/24	-	-	G0/1
Server_IPS	NIC	209.165.200.10	/24	209.165.200.1	-	G0/0
Server_IoT	NIC	209.165.200.11	/24	209.165.200.1	-	G0/2

### 3.2 Розробка топологічної схеми корпоративної мережі

Результати розрахунків схема IP-адресації та технічні вимоги до КС фірми «Yellow Vox» дозволи побудувати схему логічної топології мережі. Загальна логічна схема наведена на рисунку 3.2.

На рисунку 3.1 наведена логічна топологія підмережі IoT.

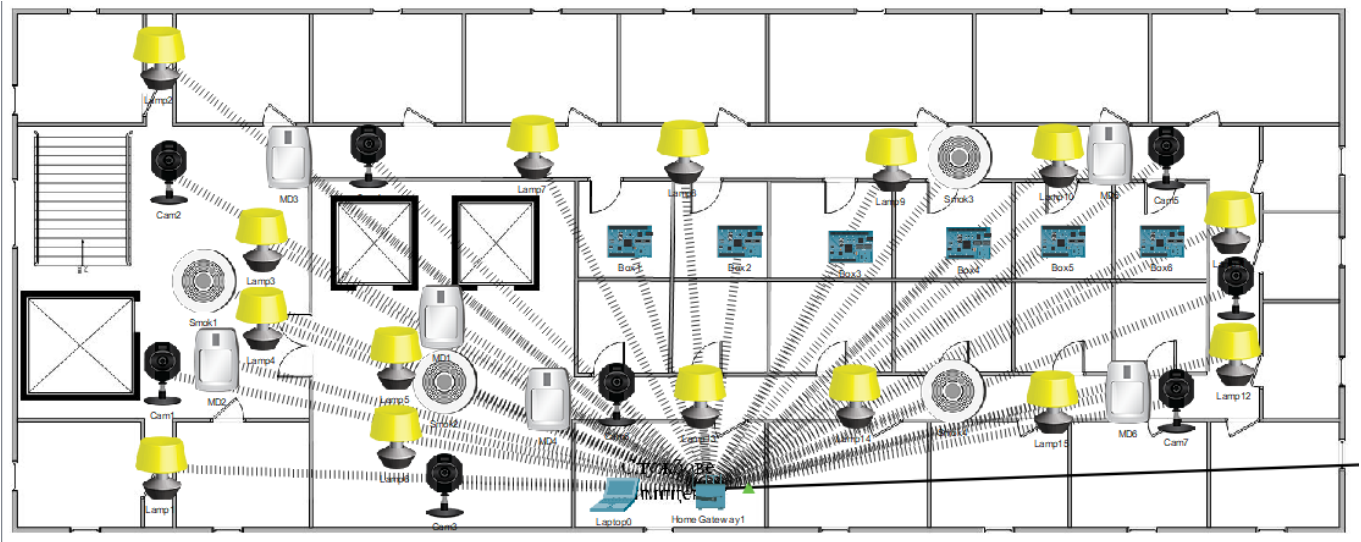


Рисунок 3.1 – Схема логічної топології підмережі IoT

«Розумні» пристрої підмережі IoT мають бездротове з'єднання за технологією WiFi з роутером DC-100, який має зону покриття 250 метрів. Такої зони покриття достатньо для будівлі з боксами зберігання компанії «Yellow Vox» з довжиною в 240 м.

До одного Wi-fi роутера можна підключити велику кількість різних клієнтських пристроїв, тобто підключення пристроїв одночасно. Для прикладу DC-100 підтримує 2007 клієнтів.

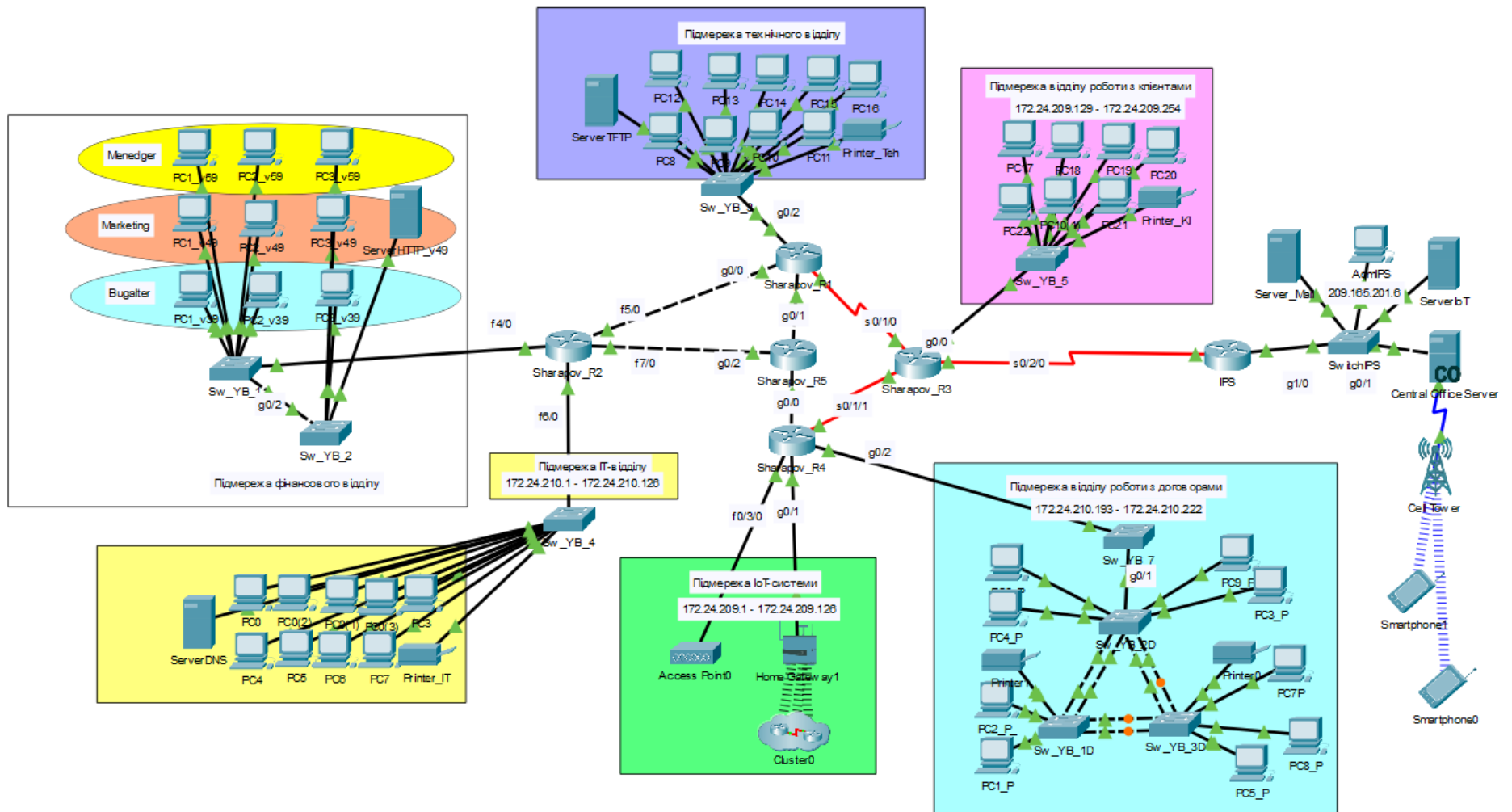


Рисунок 3.2 – Схема логічної топології КС

### 3.3 Проектування комп'ютерної мережі та розрахунок її налаштувань

#### 3.3.1 Базове налаштування конфігурації пристроїв

Відповідно до технічних вимог було виконано базове налаштування активних мережних пристроїв комп'ютерної системи компанії «Yellow Box» виконане за технічними вимогами (п. 2.1.4.2.2).

Приклад команд налаштування на Sharapov\_R2.

```

Router(config)#no ip domain-lookup
Router(config)#hostname Sharapov_R2
Sharapov_R2(config)#service password-encryption
Sharapov_R2(config)#enable secret class
Sharapov_R2(config)#line console 0
Sharapov_R2(config-line)#password cisco
Sharapov_R2(config-line)#login
Sharapov_R2(config-line)#exit
Sharapov_R2(config)#banner motd #123-21ck Sharapov. There is
protection#
Sharapov_R2(config)#username 12321ck_Sharapov password admincisco;
Sharapov_R2(config)#ip domain-name Sharapov_R2
Sharapov_R2(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Sharapov_R2(config)#line vty 0 4
Sharapov_R2(config-line)#login local
Sharapov_R2(config-line)#transport input ssh
Sharapov_R2(config)#interface f5/0
Sharapov_R2 (config-if)# ip address ck 10.0.9.1 255.255.255.252
Sharapov_R2(config-if)#no shutdown

```

### 3.3.2 Налаштування маршрутизаторів корпоративної мережі

У комп'ютерній системі компанії «Yellow Vox», згідно з технічними вимогами, застосовано протокол динамічної маршрутизації EIGRP, який є дистанційно-векторним протоколом, з номером автономної системи 20. Під час налаштування маршрутизації на маршрутизаторах «Yellow Vox», для serial-інтерфейсів встановлено пропускну здатність 128 Кбіт/с, вартість метрики 7500 та швидкість каналу 128000 біт/с. Ці налаштування забезпечують оптимальну продуктивність і надійність мережі, відповідаючи вимогам компанії до мережевої інфраструктури.

```
Sharapov_R4(config)#interface s0/1/0
```

```
Sharapov_R4(config-if)#bandwidth 128
```

```
Sharapov_R4(config-if)# clock rate 128000
```

Приклад налаштування маршрутизації на Sharapov\_R3:

Включити протокол EIGRP на маршрутизаторі:

```
Sharapov_R3(config)#router eigrp 20
```

```
Sharapov_R3(config-router)# )#eigrp router-id 13.13.13.13
```

Об'явлені мереж, що підключені до маршрутизатора:

```
Sharapov_R3(config-router)#network 172.24.209.128 0.0.0.63
```

```
Sharapov_R3(config-router)#network 10.0.9.12. 0.0.0.3
```

```
Sharapov_R3(config-router)#network 10.0.9.16. 0.0.0.3
```

```
Sharapov_R3(config-router)#network 209.165.202.0 0.0.0.252
```

Задано інтерфейси, на які не надсилаються оновлення таблиці маршрутизації:

```
Sharapov_R3(config-router) #passive-interface G0/1
```

Маршрут за замовчуванням на Sharapov\_R3:

```
ip route 0.0.0.0 0.0.0.0 209.165.202.1
```

Розповсюдження через оновлення даних протоколу EIGRP:

```
Sharapov_Rout_2(config-router)#redistribute static
```

Файл конфігурації роутера зберігається в енерго-незалежну пам'ять.

```
Sharapov_R3#copy running-config startup-config
```

Перевірити таблицю маршрутизації роутера можна командою:

```
Sharapov_R3#show ip route
```

Перевірку таблиці маршрутизації роутера Sharapov\_R3 наведено на рисунку 3.3. Таблиці маршрутизації інших роутерів КС наведено в додатку А.

```
Sharapov_R3#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 209.165.202.1 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
D    10.0.9.0/30 [90/20514560] via 10.0.9.17, 01:50:14, Serial0/1/0
D    10.0.9.4/30 [90/20514816] via 10.0.9.22, 01:50:16, Serial0/1/1
     [90/20514816] via 10.0.9.17, 01:50:14, Serial0/1/0
D    10.0.9.8/30 [90/20512256] via 10.0.9.17, 01:50:14, Serial0/1/0
D    10.0.9.12/30 [90/20512256] via 10.0.9.22, 01:50:16, Serial0/1/1
C    10.0.9.16/30 is directly connected, Serial0/1/0
L    10.0.9.18/32 is directly connected, Serial0/1/0
C    10.0.9.20/30 is directly connected, Serial0/1/1
L    10.0.9.21/32 is directly connected, Serial0/1/1
172.24.0.0/16 is variably subnetted, 6 subnets, 6 masks
D    172.24.0.0/16 [90/20517120] via 10.0.9.17, 01:50:14, Serial0/1/0
S    172.24.208.0/21 is directly connected, Serial0/2/0
C    172.24.209.128/25 is directly connected, GigabitEthernet0/0
L    172.24.209.129/32 is directly connected, GigabitEthernet0/0
D    172.24.210.128/26 [90/20514560] via 10.0.9.17, 01:50:14, Serial0/1/0
D    172.24.210.192/27 [90/20512256] via 10.0.9.22, 01:50:16, Serial0/1/1
D    209.165.200.0/24 [90/20514560] via 10.0.9.22, 01:50:16, Serial0/1/1
209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.202.0/27 is directly connected, Serial0/2/0
L    209.165.202.2/32 is directly connected, Serial0/2/0
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Рисунок 3.3 – Таблиця маршрутизації на Sharapov\_R3

В мережі компанії «Yellow Box» налаштований DHCP-сервіс на роутерах, для надання налаштувань TCP/IP для хостів в підмережах.

Налаштування пулу DHCP приведемо на прикладу LAN1 « Відділ IT»:

```
Sharapov_Rout_4(config)#ip dhcp pool poolLAN_IT
```

```
Sharapov_Rout_4(dhcp-config)#network 172.24.209.0 255.255.255.128
```

```
Sharapov_Rout_4(dhcp-config)#default-router 172.24.209.1
```

```
Sharapov_Rout_4(dhcp-config)#dns-server 172.24.210.10
```

В мережі компанії «Yellow Box» налаштований сервіс AAA (Authentication Authorization and Accounting). AAA – система аутентифікації,



авторизації і обліку подій, вбудована в операційну систему Cisco IOS, служить для надання користувачам безпечного віддаленого доступу до мережного обладнання Cisco.

```
Sharapov_R4(config)#aaa new-model //запуск служби AAA
```

*Sharapov\_R2(config)#aaa authentication login default local //*  
налаштування методу аутентифікації за замовчуванням з використання локальної бази користувачів

*Sharapov\_R4(config)#aaa authentication login Login group radius local //*  
налаштування методу аутентифікації Login з використанням серверу RADIUS, а якщо він недоступний, то з використанням локальної бази користувачів

```
Sharapov_R4(config)#line console 0
```

*Sharapov \_R4(config-line)#login authentication Login //* застосування методу аутентифікації Login на консольній лінії

```
Sharapov _R4(config)#line vty 0 4
```

*Sharapov \_R4(config-line)#login authentication default //* застосування методу аутентифікації за замовчуванням на vty-лінії

Налаштування RADIUS-сервер:

```
Sharapov _R4(config)#radius-server host 172.24.210.10 auth-port 1645
```

```
Sharapov _R4(config)#radius-server key radius12321
```

```
123-21sk Sharapov. Login for authorized users only

User Access Verification

Username: Sharapov_R1
Password:
Sharapov_R1>en
Sharapov_R1>enable
Password:
Sharapov_R1#sh
Sharapov_R1#show r
Sharapov_R1#show running-config
Building configuration...
```

Рисунок 3.4 – Аутентифікація на маршрутизаторі за допомогою служби AAA та сервера RADIUS

AAA

Service  On  Off Radius Port

---

Network Configuration

Client Name  Client IP

Secret  ServerType

	Client Name	Client IP	Server Type	Key	
1	Sharapov_R1	172.24.210.129	Radius	Sharapov123	<input type="button" value="Add"/>
2	Sharapov_R2	172.24.208.1	Radius	Sharapov123	<input type="button" value="Save"/>
3	Sharapov_R3	172.24.210.1	Radius	Sharapov123	
4	Sharapov_R4	172.24.210.193	Radius	Sharapov123	

---

User Setup

Username  Password

	Username	Password	
1	Sharapov_R1	Sharapov123	<input type="button" value="Add"/>
2	Sharapov_R2	Sharapov123	<input type="button" value="Save"/>
3	Sharapov_R3	Sharapov123	
4	Sharapov_R4	Sharapov123	

Рисунок 3.5 – Аутентифікація на сервері RADIUS 172.24.210.138

### 3.3.3 Налаштування роботи Інтернет

NAT на прикордонному маршрутизаторі налаштовано згідно з вимогами:

- пул адрес: з 209.165.202.1 по 209.165.202.30;
- 192.168.133.9/24 – адреса Server HTTP;
- номер списку доступу: 20;
- ім'я пулу: Internet.

Приклад налаштування NAT на Sharapov\_R3:

Список контролю доступу, що дозволяє всі адреси внутрішньої мережі:

```
Sharapov_R3(config)# access-list 3 permit 172.24.208.1 0.0.7.255
```

Пул для динамічного виділення інтернет адрес:

```
Sharapov_R3(config)#ip nat pool Internet 209.165.202.5 209.165.202.30
netmask 255.255.255.185
```

Підміна адреси внутрішньої мережі на інтернет адреси згідно з списком контролю доступу:

```
Sharapov_R3(config)#ip nat inside source list 20 pool Internet
```

Адреса статичного NAT для серверу HTTP:

```
Sharapov_R3(config)#ip nat inside source static 172.24.210.10
209.165.200.5
```

Призначення інтерфейсу в якості вихідного для трафіку з мережі приватних адрес:

```
Sharapov_R3(config)#interface S0/2/0
```

```
Sharapov_R3(config-if)#ip nat outside
```

Призначення інтерфейсу в якості вхідного для трафіку з мережі приватних адрес:

```
Sharapov_R3(config-if)#interface Serial0/1/0
```

```
Sharapov_R3(config-if)#ip nat inside
```

```
Sharapov_R3(config-if)#interface Serial0/1/1
```

```
Sharapov_R3(config-if)#ip nat inside
```

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.202.11:1	172.24.208.45:1	209.165.201.5:1	209.165.201.5:1
icmp	209.165.202.10:1	172.24.208.78:1	209.165.201.5:1	209.165.201.5:1
icmp	209.165.202.10:2	172.24.208.78:2	209.165.201.5:2	209.165.201.5:2
icmp	209.165.202.10:3	172.24.208.78:3	209.165.201.5:3	209.165.201.5:3
icmp	209.165.202.7:1	172.24.209.140:1	209.165.201.5:1	209.165.201.5:1
icmp	209.165.202.6:3	172.24.210.138:3	209.165.201.5:3	209.165.201.5:3
icmp	209.165.202.6:4	172.24.210.138:4	209.165.201.5:4	209.165.201.5:4
icmp	209.165.202.9:1	172.24.210.17:1	209.165.201.5:1	209.165.201.5:1
icmp	209.165.202.8:1	172.24.210.206:1	209.165.201.5:1	209.165.201.5:1
---	209.165.202.3	172.24.208.42	---	---

Рисунок 3.6 – Таблиця перетворювань NAT на Sharapov\_R3

### 3.3.4 Захист інформації в комп'ютерній системі від несанкціонованого доступу

Д підмережі «Фінансовий підрозділ» були створені 3 підмережі VLAN та дві відповідно протоколу.

Таблиця 3.4 – Назви VLAN для підмережі

Номер VLAN	Ім'я VLAN	Примітка
1	Default	Не використовується
39	Marketing department	Відділ маркетингу
49	Management department	Відділ менеджменту
59	Accounting department	Відділ бухгалтерії
99	Management	Управління пристроями
100	Native	Власна

Port Status Summary Table for Sw_YB_1				
Device Name: Sw_YB_1				
Custom Device Model: 2960 IOS15				
Hostname: Sw_YB_1				
Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Down	1	--	000A.41DD.6101
FastEthernet0/2	Down	1	--	000A.41DD.6102
FastEthernet0/3	Down	1	--	000A.41DD.6103
FastEthernet0/4	Up	39	--	000A.41DD.6104
FastEthernet0/5	Up	39	--	000A.41DD.6105
FastEthernet0/6	Down	39	--	000A.41DD.6106
FastEthernet0/7	Down	39	--	000A.41DD.6107
FastEthernet0/8	Down	39	--	000A.41DD.6108
FastEthernet0/9	Down	1	--	000A.41DD.6109
FastEthernet0/10	Up	49	--	000A.41DD.610A
FastEthernet0/11	Up	49	--	000A.41DD.610B
FastEthernet0/12	Down	49	--	000A.41DD.610C
FastEthernet0/13	Down	49	--	000A.41DD.610D
FastEthernet0/14	Down	49	--	000A.41DD.610E
FastEthernet0/15	Up	59	--	000A.41DD.610F
FastEthernet0/16	Up	59	--	000A.41DD.6110
FastEthernet0/17	Down	59	--	000A.41DD.6111
FastEthernet0/18	Down	59	--	000A.41DD.6112
FastEthernet0/19	Down	59	--	000A.41DD.6113
FastEthernet0/20	Down	59	--	000A.41DD.6114
FastEthernet0/21	Down	1	--	000A.41DD.6115
FastEthernet0/22	Down	1	--	000A.41DD.6116
FastEthernet0/23	Down	1	--	000A.41DD.6117
FastEthernet0/24	Down	1	--	000A.41DD.6118
GigabitEthernet0/1	Up	--	--	000A.41DD.6119
GigabitEthernet0/2	Up	--	--	000A.41DD.611A
Vlan1	Down	1	<not set>	000A.417D.33ED
Vlan99	Up	99	172.24.208.98/28	000A.417D.3301

Рисунок 3.7 – Налаштування VLAN на Sw\_YB1

Port Status Summary Table for Sw\_YB\_2

---

Device Name: Sw\_YB\_2  
 Custom Device Model: 2960 IOS15  
 Hostname: Sw\_YB\_2

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Down	1	--	0002.168B.8801
FastEthernet0/2	Down	1	--	0002.168B.8802
FastEthernet0/3	Down	1	--	0002.168B.8803
FastEthernet0/4	Up	39	--	0002.168B.8804
FastEthernet0/5	Down	39	--	0002.168B.8805
FastEthernet0/6	Down	39	--	0002.168B.8806
FastEthernet0/7	Down	39	--	0002.168B.8807
FastEthernet0/8	Down	39	--	0002.168B.8808
FastEthernet0/9	Down	1	--	0002.168B.8809
FastEthernet0/10	Up	49	--	0002.168B.880A
FastEthernet0/11	Up	49	--	0002.168B.880B
FastEthernet0/12	Down	49	--	0002.168B.880C
FastEthernet0/13	Down	49	--	0002.168B.880D
FastEthernet0/14	Down	49	--	0002.168B.880E
FastEthernet0/15	Up	59	--	0002.168B.880F
FastEthernet0/16	Down	59	--	0002.168B.8810
FastEthernet0/17	Down	59	--	0002.168B.8811
FastEthernet0/18	Down	59	--	0002.168B.8812
FastEthernet0/19	Down	59	--	0002.168B.8813
FastEthernet0/20	Down	59	--	0002.168B.8814
FastEthernet0/21	Down	1	--	0002.168B.8815
FastEthernet0/22	Down	1	--	0002.168B.8816
FastEthernet0/23	Down	1	--	0002.168B.8817
FastEthernet0/24	Down	1	--	0002.168B.8818
GigabitEthernet0/1	Down	1	--	0002.168B.8819
GigabitEthernet0/2	Up	--	--	0002.168B.881A
Vlan1	Down	1	<not set>	00E0.A393.AAEB
Vlan99	Up	99	172.24.208.99/27	00E0.A393.AA01

Рисунок 3.8 – Налаштування VLAN на Sw\_YB1

На рисунках наведено розподіл портів комутаторів за віртуальним мережами VLAN, які було створено за технічними вимогами.

Для здійснення передачі трафіку між VLAN необхідно налаштувати порт F4/0 маршрутизатора Sharapov\_R2 на підтримку технології інкапсуляції 802.1Q.

```
Sharapov_R2(config)#interface a4/0
```

```
Sharapov_R2(config-if)#no shutdown
```

Налаштування підінтерфейсу для маршрутизації трафіку між VLAN.

*Sharapov\_R2(config)#interface f4/0.1*

Тегування пакетів для данного підінтерфейсу.

*Sharapov\_R2(config-subif)#encapsulation dot1Q 39 //*

*Sharapov\_R2(config-subif)#ip address 172.24.208.0 255.255.255.224*

Port Status Summary Table for Sharapov_R2					
Device Name: Sharapov_R2					
Device Model: Router-PT					
Hostname: Sharapov_R2					
Port	Link	IP Address	IPv6 Address	MAC Address	
FastEthernet4/0	Up	<not set>	<not set>	0004.9A8B.A33D	
FastEthernet4/0.39	Up	172.24.208.1/27	<not set>	0004.9A8B.A33D	
FastEthernet4/0.49	Up	172.24.208.33/27	<not set>	0004.9A8B.A33D	
FastEthernet4/0.59	Up	172.24.208.65/27	<not set>	0004.9A8B.A33D	
FastEthernet4/0.99	Up	172.24.208.97/28	<not set>	0004.9A8B.A33D	
FastEthernet5/0	Up	10.0.9.1/30	<not set>	0090.2165.6738	
FastEthernet6/0	Up	172.24.210.1/25	<not set>	0009.7C4C.A0E1	
FastEthernet7/0	Up	10.0.9.5/30	<not set>	0040.0BB4.993E	
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Sharapov_R2					

Рисунок 3.9 – Перевірка налаштування 802. 1Q на Sharapov\_R2

### 3.3.5 Перевірка роботи моделі комп'ютерної системи

Виконання команди Ping між хостами з підмереж LAN4 «Технічне обслуговування» та LAN2 «Робота з клієнтами».

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.24.209.140

Pinging 172.24.209.140 with 32 bytes of data:

Reply from 172.24.209.140: bytes=32 time=33ms TTL=126
Reply from 172.24.209.140: bytes=32 time=1ms TTL=126
Reply from 172.24.209.140: bytes=32 time=1ms TTL=126
Reply from 172.24.209.140: bytes=32 time=23ms TTL=126

Ping statistics for 172.24.209.140:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 33ms, Average = 14ms
C:\>|

```

Рисунок 3.10 – Результат команди «ping» між підмережами КС «Yellow Vox»

Для перевірки працездатність мережі також перевіряється, налаштування до активних мережних пристроїв, перевірку зв'язку між вузлами з різних VLAN, автоматичне призначення адрес при використанні протоколу DHCP.

Для перевірки безпечного віддаленого доступу за SSH зробимо підключення з командного рядка PC з підмережі LAN4 «Технічне обслуговування» до маршрутизатора Sharapov\_R1 від користувача Sharapov\_12321ск з паролем admincisco.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l Sharapov 172.24.210.129

Password:
Sharapov_R1>enable
Password:
Sharapov_R1#show run
Building configuration...

Current configuration : 2546 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sharapov_R1
!
!
!
enable secret 5 $l$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
ip dhcp excluded-address 172.24.210.129 172.24.210.139
!
ip dhcp pool POOL_Teh
network 172.24.210.128 255.255.255.192

```

Рисунок 3.11– Перевірка підключення до маршрутизатора Sharapov\_R1 за допомогою протоколу SSH

Діагностична команда налаштувань DHCP.



```

Sharapov_R4#show ip dhcp binding
IP address      Client-ID/
                Hardware address
209.165.200.6   00D0.9714.EB01   --   Automatic
172.24.210.200 00D0.BC71.E977   --   Automatic
172.24.210.206 0090.0C95.7324   --   Automatic
172.24.210.204 0060.706A.2A9E   --   Automatic
172.24.210.209 0002.4A61.316D   --   Automatic
172.24.210.205 000A.F34A.9800   --   Automatic
172.24.210.207 0060.706C.A5D0   --   Automatic
172.24.210.208 00E0.F7E2.81A5   --   Automatic
172.24.210.203 0001.C75D.E56C   --   Automatic
172.24.210.202 000D.BD1A.6039   --   Automatic
172.24.210.201 0040.0B67.6972   --   Automatic
172.24.210.210 0001.64D8.BA87   --   Automatic
Sharapov_R4#

```

Рисунок 3.12 – Таблиця призначення IP-адрес вузлам за протоколом DHCP

Перевіримо доступність мережі Інтернет на пограничний роутер Sharapov\_R3.


Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	AdmIPS	Sharapov_R3	ICMP		0.000	N	0	(edit)
	Successful	AdmIPS	Sharapov_R1	ICMP		0.000	N	1	(edit)
	Successful	AdmIPS	Sharapov_R5	ICMP		0.000	N	2	(edit)
	Successful	AdmIPS	Sharapov_R2	ICMP		0.000	N	3	(edit)

Рисунок 3.13 – Перевірка Internet

## 4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

### 4.1 Об'єкт та тип впроваджуваного компоненту системи

Система IoT компанії «Yellow Box» побудована із застосуванням технологій туманних та хмарних обчислень. Загалом система забезпечує ефективне керування ресурсами, підвищення рівня безпеки та комфорту, а також оптимізацію енергоспоживання в будівлі.

Розумні речі, встановлені в коридорах, призначені для керування освітленням по наявності людей (розумні лампи та датчики виявлення присутності типу PIR), для відеонагляду по наявності людей та контролю задимленості (розумні датчики чадного диму та розумні сирени). Дані з цих пристроїв надсилаються до віддаленого серверу IoT, що підтримує хмарну платформу для збору, аналітики та керування.

Таким чином виконується функція моніторингу та аналітики в реальному часі. Завдяки використанню хмарних обчислень дані з сенсорів можуть аналізуватися в режимі реального часу для оперативного прийняття рішень.

Завдяки доступу до хмарної платформи система IoT буде підтримувати автоматичне оновлення програмного забезпечення та конфігурацію пристроїв, що забезпечує їхню безперебійну роботу та актуальність.

Доступ до хмарної платформи також забезпечує високу безпеку даних, завдяки використанню сучасних методів шифрування та аутентифікації, які забезпечують захист даних від несанкціонованого доступу.

Веб-інтерфейс для користувача дозволить адміністраторам системи та кінцевим користувачам переглядати дані, отримані з сенсорів, та керувати налаштуваннями системи.

Для моделювання роботи розумних речей використовується програмне середовище Cisco Packet Tracer. Це програмне забезпечення дозволяє моделювати та візуалізувати мережі й пристрої IoT. Завдяки зручному функціоналу, можна швидко та ефективно провести моделювання, що

допоможе виявити й усунути можливі неполадки на ранньому етапі, запобігаючи додатковим витратам під час реалізації. Також Packet Tracer надає можливість моделювання роботи з IoT сервером. Веб-інтерфейс серверу дозволяє створювати сценарії автоматизованого керування розумними речами [6].

Туманні обчислення для локальної обробки. Для зниження затримки та зменшення навантаження на мережу частина обробки даних буде виконуватися на рівні туманних обчислень, близько до джерела даних. Компоненти системи IoT працюють з контролером, який має інтерфейс Wi-Fi. Керування виконує контролер, а дані для аналітики надсилаються до віддаленого серверу IoT [7].

#### **4.2 Налаштування IoT-системи**

Застосовуючи можливості середовища моделювання мереж і розумних пристроїв Packet Tracer виконаний проект, що реалізує систему IoT компанії «Yellow Box», що є інтегрованою частиною корпоративної мережі компанії.

Мережа системи IoT має адресний простір IP 172.24.209.0/25. Дані розумних речей передаються на віддалений сервер з IP адресою 209.165.201.6/28.

Важливим етапом є налаштування зв'язку розумних пристроїв з шлюзом та віддаленим IoT сервером.

З боку шлюза IoT (маршрутизатор DCL100) виконані налаштування: ім'я мережі SSID (SharapovYB), метод автентифікації (WPA\_PSK) та пароль (Yellow28), IP-налаштування на інтерфейсі Internet.

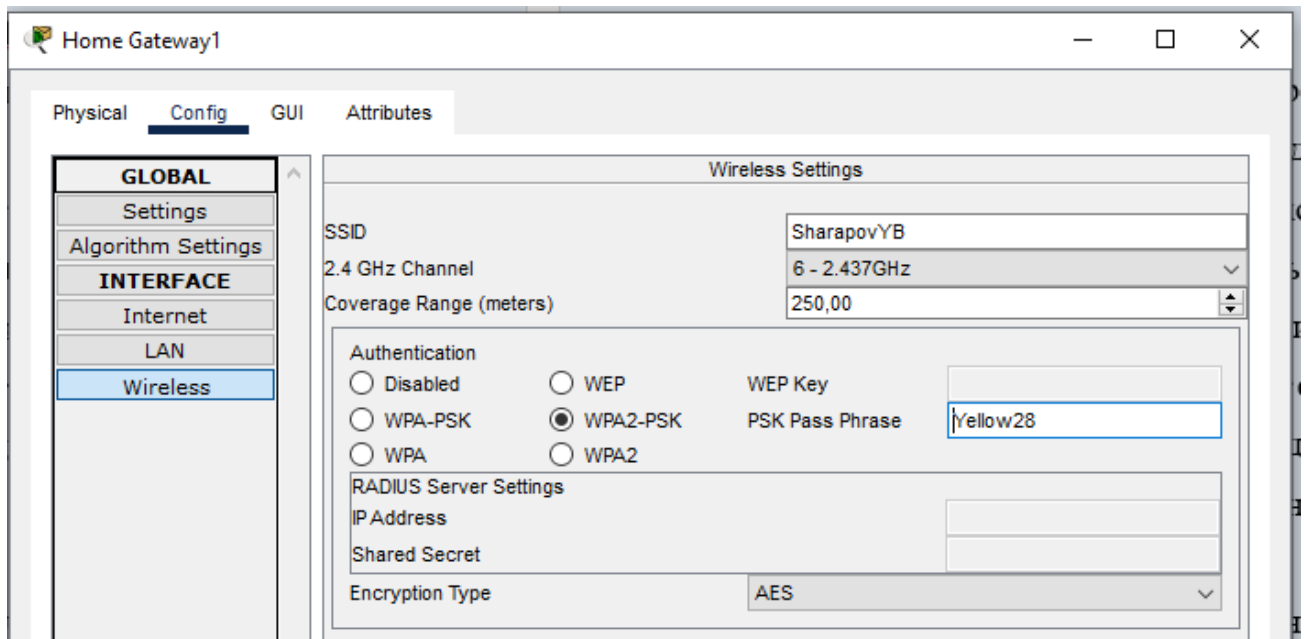


Рисунок 4.1 – Налаштування шлюза IoT

З боку розумної речі виконані налаштування: ім'я мережі SSID (SharapovYB), метод автентифікації (WPA\_PSK) та пароль (Yellow28), IP-налаштування за протоколом DHCP від шлюза IoT та зазначено IP-адресу віддаленого серверу для розумних речей компанії «Yellow Box» та параметри акаунту для під'єднання.

 The image shows a configuration window for an IoT Server. It contains the following fields and options:
 

- IoT Server selection:
  - None
  - Home Gateway
  - Remote Server
- Server Address: 209.165.201.6
- User Name: Sharapov
- Password: admin
- Refresh button

Рисунок 4.2 – Налаштування зв'язку з IoT сервером на пристрої IoT

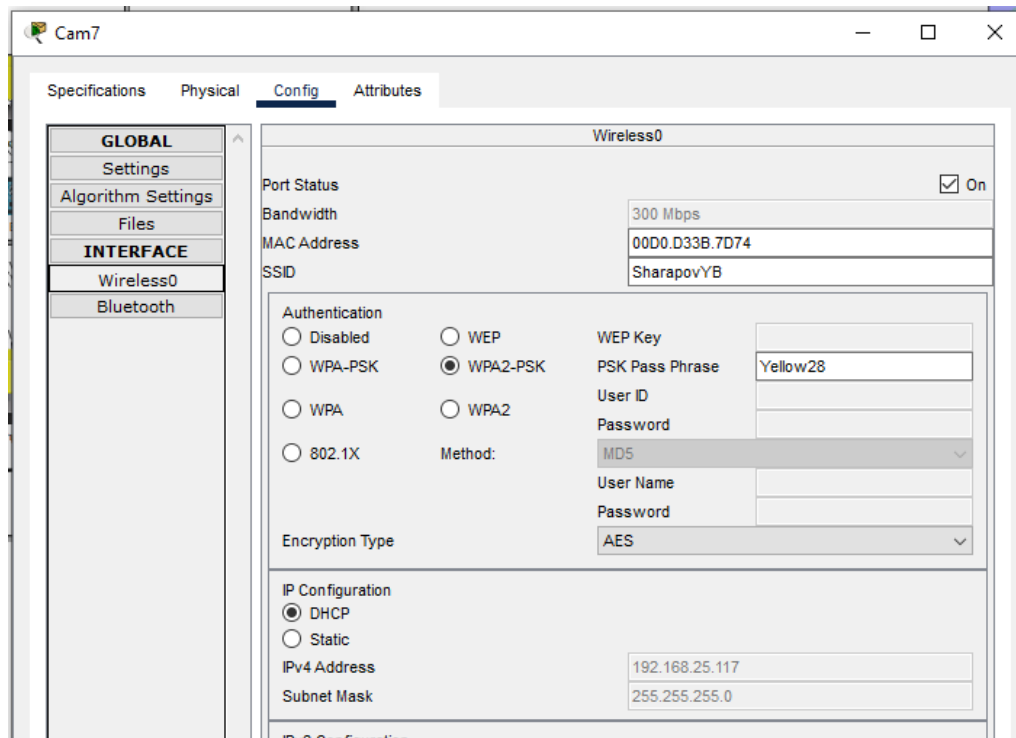


Рисунок 4.3 – Налаштування розумної речі

За допомогою Web-інтерфейсу IoT серверу створено сценарій автоматизованого керування IoT пристроями системи.

Умовно пристрої IoT системи компанії «Yellow Box» на поверху з боксами зберігання поділені на групи за доцільністю. Наприклад, група1 це зона ліфтів, де необхідно за ознакою наявності руху вмикати освітлення та камеру відеоспостереження.

Розподіл на такі зони допомагають раціонально керувати освітленням тільки в тих зонах, де виявлений рух.

Дитчики диму відстежують рівень CO<sub>2</sub> та за умови перевищення зазначеного рівня вмикають сирени попередження.

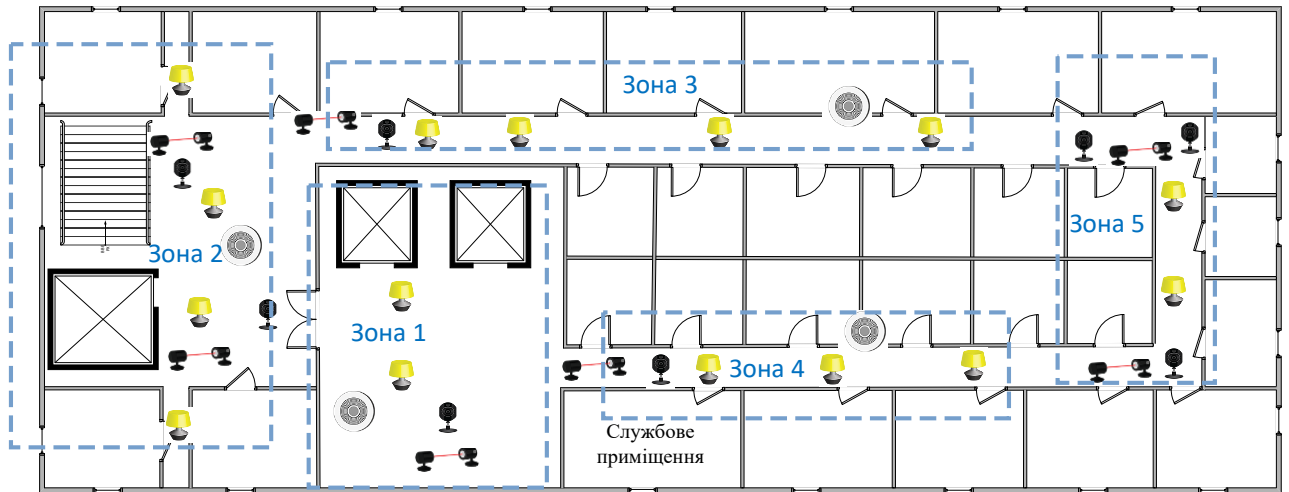


Рисунок 4.4 – Зонування простору поверху

Доступ до віддаленого серверу IoT здійснюється за параметрами аккаунта, який створений в сервісі IoT,

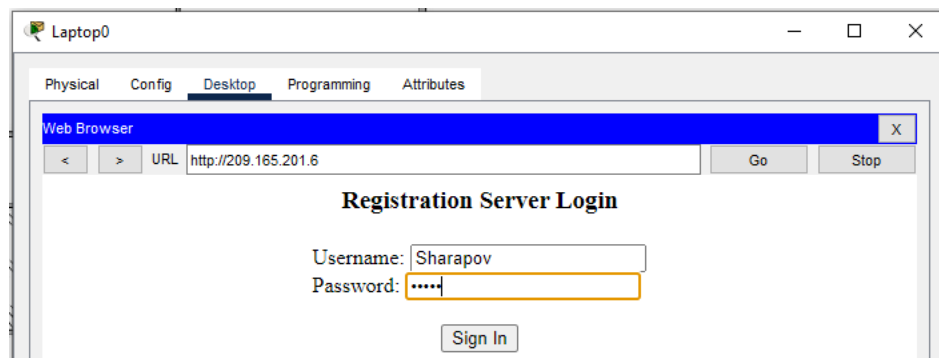


Рисунок 4.5 – Доступ до віддаленого серверу з мережі IoT

Сценарій керування IoT системою для компанії «Yellow Vox», виглядає, як наведено на рисунку 4.5, де також наведений результат роботи системи IoT варіанту, коли в зоні 2 є людина і зафіксоване перевищення рівня чадного газу.

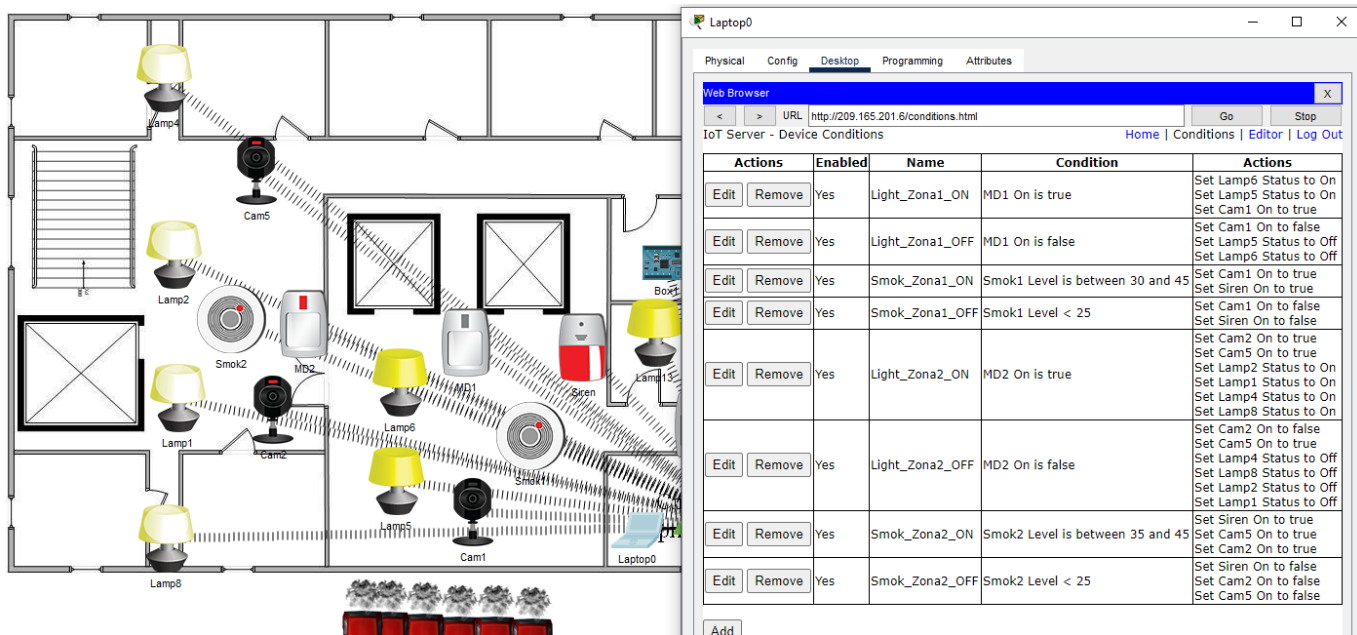


Рисунок 4.6 – Правила керування освітленням

Кожен контролер в боксах має доступ до шлюза системи IoT за технологією WiFi і передають дані компонентів до хмарної платформи на віддаленому сервері.

Виконання функціоналу контролером забезпечується його програмуванням мовою Python із застосуванням IoT API для роботи з портами I/O та IoE Client на сервері.

На рисунку 4.6 наведений сценарій спрацювання системи в випадку наявності людей в боксі (по сигналам від датчиків присутності PIR вмикається освітлення відповідної зони) та вимірювання температури з передачею показників до хмарної платформи на віддаленому сервері IoT та сигналізацією діюдом про невідповідність температурних показників нормі.

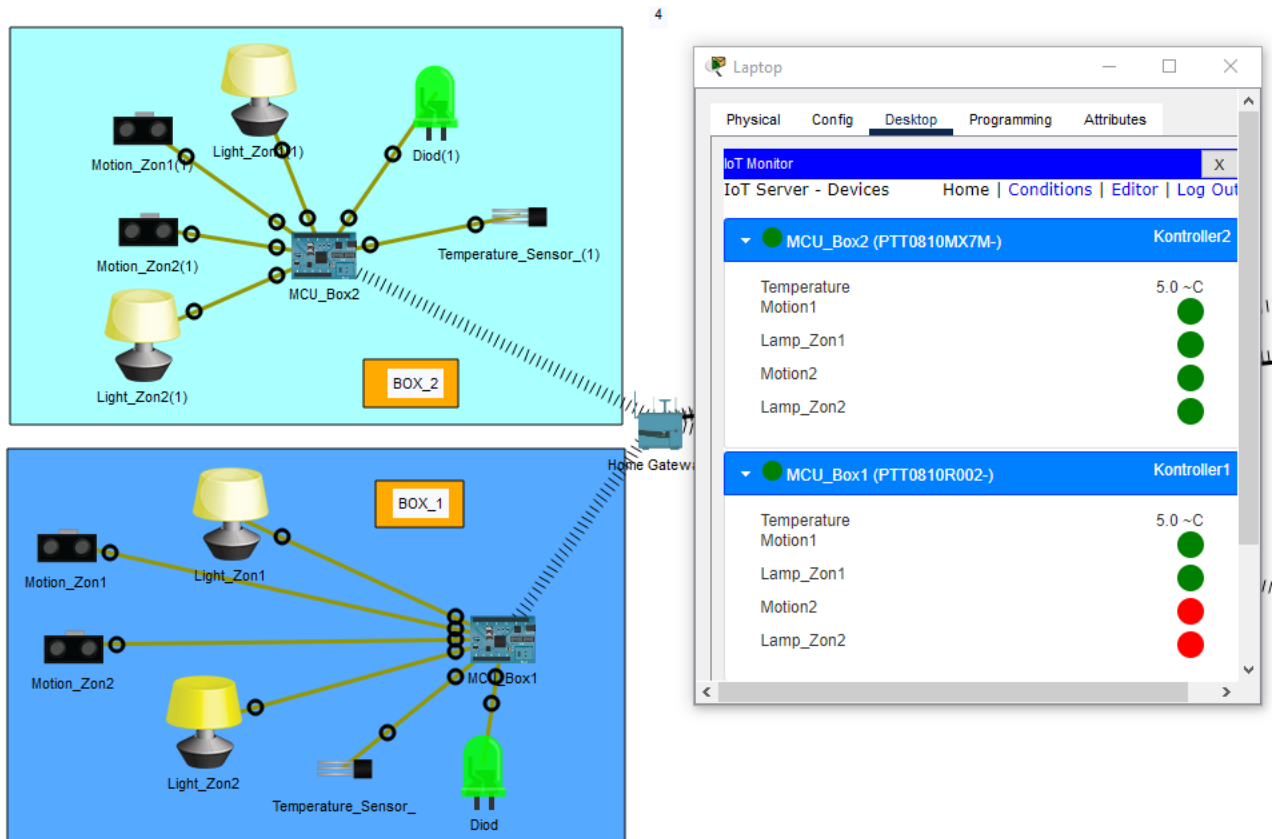


Рисунок 4.7 – Перевірка роботи компонентів системи IoT компанії «Yellow Box»

### 4.3 Моделювання IoT-системи

Пристрій розумного боксу створений з використанням Arduino Nano IoT, який оснащений чіпом ESP32. Цей чіп поєднує в собі модуль зв'язку Wi-Fi і функції мікропроцесора.

Для роботи з мікроконтролером Arduino Nano IoT на базі ESP32 можна використовувати програмне середовище ESP-IDF та писати код мовою програмування C. Альтернативно, можна використовувати середовище Arduino з мовою програмування C++. Існують й інші програми для реалізації системи, але середовище Arduino надає переваги, такі як ефективне використання пам'яті, широкий вибір бібліотек та велика спільнота розробників, що полегшує пошук інформації для розробки. Це середовище використовує компілятор gcc, який можна застосовувати окремо від інтегрованого середовища розробки (IDE) із системою збірки make.



Іншим варіантом є використання PlatformIO, яке забезпечує взаємодію між багатьма IDE та вбудованими апаратними платформами, а також надає незалежні від платформи функції, такі як налагодження, тестування та аналіз коду. Arduino також підтримує оновлення OTA, за умови наявності достатнього місця у флеш-пам'яті для одночасного зберігання нової та старої версій прошивки [9].

Програмне забезпечення написано в середовищі розробки Arduino з використанням ESP32 Arduino IDE. Це середовище забезпечує API для підключення до мережі Wi-Fi, спілкування через TCP і UDP, створення серверів HTTP і DNS, використання флеш-пам'яті та роботи з периферійними пристроями I2C.

Для візуалізації та створення макетної схеми можна використовувати програмне забезпечення TinkerCAD. Це програмне забезпечення з відкритим кодом, яке робить електроніку простішою та доступнішою, дозволяючи віртуально моделювати електричні схеми, створювати та налагоджувати програмний код для контролеру.

На рисунку 4.7 наведений результат моделювання системи в TinkerCAD.

Таблиця 4.1 – Зведена таблиця підключення компонентів

Пристрій	Вхід	Тип входу	Напряв
Давач температури	A0	Аналоговий	IN (вхід)
Діод	D13	Дискретний (цифровий)	OUT(вихід)
Давач руху 1	D9	Дискретний (цифровий)	IN (вихід)
Реле лампи 1	D12	Дискретний (цифровий)	OUT(вихід)
Давач руху 1	D10	Дискретний (цифровий)	IN (вихід)
Реле лампи 1	D11	Дискретний (цифровий)	OUT(вихід)

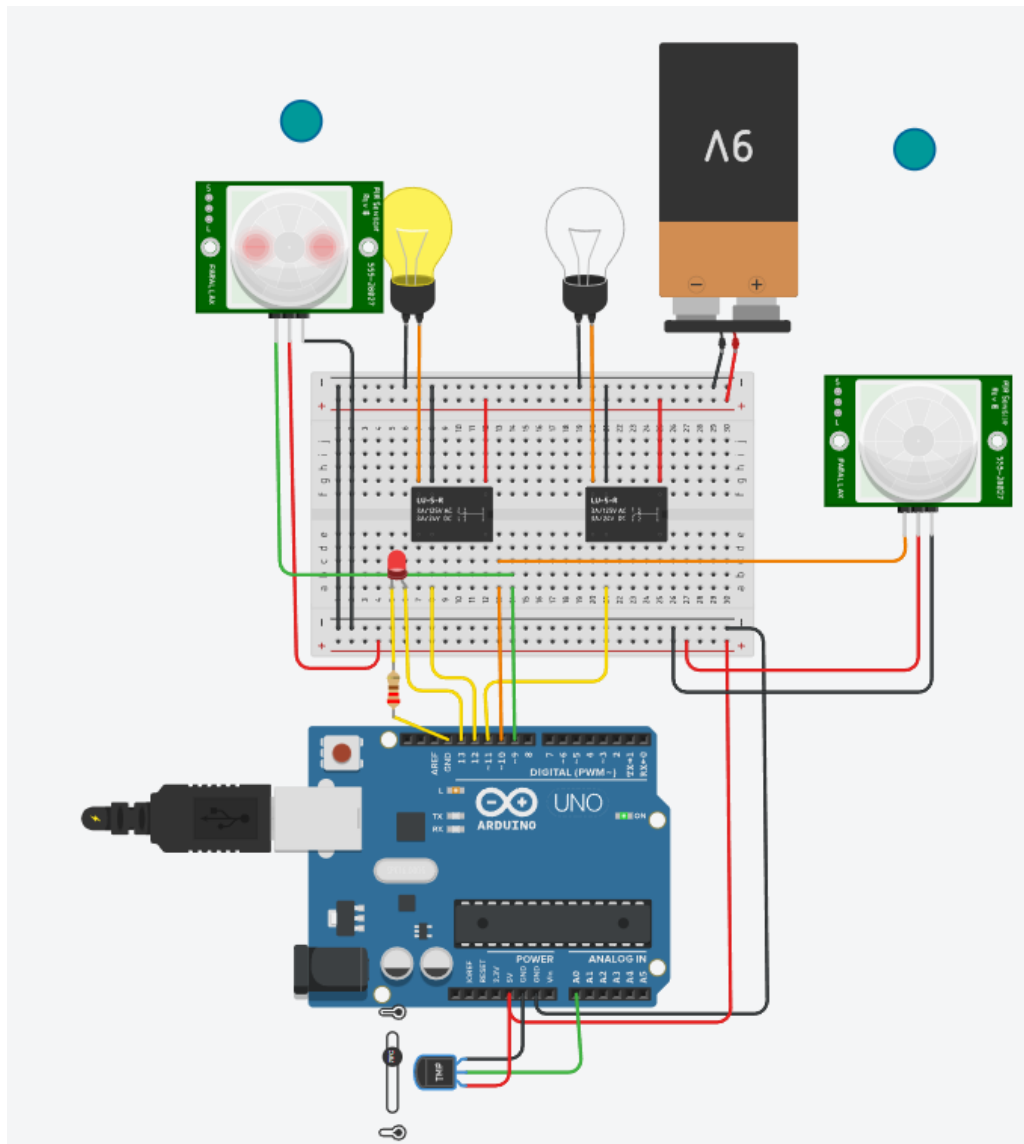


Рисунок 4.8 – Модель в TinkerCAD

У цьому проєкті мікроконтролер (MCU) запрограмовано мовою C++ для безперервного зчитування значень датчиків і запису на виконавчі елементи, керовані умовною логікою. Крім того, програмне забезпечення мікроконтролера забезпечує високу швидкість і точність обробки даних, дозволяючи ефективно реагувати на зміну умов та забезпечуючи надійне функціонування всієї системи. У діалоговому вікні TinkerCAD на вкладці «Код» виконане програмування системи на C++. Текст програми наведений в додатку 2.

## ВИСНОВКИ

У кваліфікаційній роботі було проаналізовано умови та вимоги підприємства «Yellow Box», на основі яких спроектовано IoT-систему індивідуального зберігання інвентарю та корпоративну мережу зі змішаною топологією. Під час проектування IoT-системи було виконано специфікацію обладнання для її реалізації, а також вибрано обладнання для бездротової мережі, програмне забезпечення та хмарну платформу. Корпоративну мережу, складовою частиною якої є IoT-система, розраховано за IPv4; було обрано технології передачі даних та кабельні системи.

Відповідно до архітектури мережі, функціонального призначення вузлів та технології передачі даних, було вибрано активне обладнання компанії Cisco та виконано його налаштування. У рамках кваліфікаційної роботи розроблено проект та створено модель IoT-системи, яка була змодельована в пакеті TinkerCAD та протестована в симуляторі Packet Tracer.

Таким чином, завдання кваліфікаційної роботи – впровадження IoT-рішення в конфігурації та специфікації, що враховує особливості підприємства «Yellow Box», яке забезпечить ефективне та автоматизоване управління приміщеннями для зберігання речей, успішно виконане.

## ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2022. – 65 с.
2. Комп'ютерна академія Cisco [Електронний ресурс] – Режим доступу: <https://www.netacad.com> (дата звернення 19.05.2023р.)
3. Точки доступу WI-FI [Електронний ресурс] – Режим доступу: <https://ntools.com.ua/uk/information/faq/skolko-k-odnoj-wi-fi-tochke-dostupa-mozhno-podkljuchit-ustrojstv>
4. Комп'ютерні мережі. Книга 1 : [навч. посіб.] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. – Львів : «Магнолія 2006», 2019. – 256 с.
5. Комп'ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панфьорова; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч.2. – 39 с.
6. Б.Ю. Жураковський, І.О. Зенів. Технології інтернету речей: навч. посібник / за ред. М.М. Ткача - Міністерство освіти і науки України, Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.
7. Лунтовський А.О. / Основи проектування безпроводових комп'ютерних мереж: навч. посібник / А.О. Лунтовський, І.В. Мельник. – К.: Освіта України. 2011. – 352 с.
8. Hasan M., Anik M. H., Chowdhury S., Chowdhury S. A., Bilash T. I., Islam S. Low-cost Appliance Switching Circuit for Discarding Technical Issues of Microcontroller Controlled Smart Home. International Journal of Sensors and Sensor Networks. 2019. Pp. 16-22.

9. Ramon Nastase. Cisco CCNA CommandGuide: AnIntroductoryGuidefor CCNA 17 &ComputerNetworkingBeginners.– Independentlypublished, 2018. – 74 p. ISBN-10: 1731124279, ISBN-13: 978-1731124272

10. Gota, D. I., Puscasiu, A., Fanca, A., Miclea, L., & Valean, H. Smart home automation system using Arduino microcontrollers. IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR). 2020. Pp. 1-7.

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

**ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ  
НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ**

Текст програми  
804.02070743.20020-01 12 01

Листів 11

**2024**

## АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування компонентів корпоративної мережі комп'ютерної системи. Програма призначена для забезпечення налаштування IP, DHCP, VLSM, EtherCanel, AAA, інтерфейсів, протоколу маршрутизації, NAT, консольних і vty ліній та створення мереж VPN, домену и ssh комп'ютерної системи.

**ЗМІСТ**

		Стор.
1.	Налаштування роутера Sharapov_R2	4
2.	Налаштування роутера Sharapov_R3	6
3.	Налаштування роутера Sharapov_R4	9
4.	Налаштування комутатора Sw_YB_1	11



## 1. Налаштування роутера Sharapov\_R2

```

!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sharapov_R2
enable secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded-address 172.24.208.1 172.24.208.10
ip dhcp excluded-address 172.24.208.33 172.24.208.43
ip dhcp excluded-address 172.24.208.65 172.24.208.75
ip dhcp excluded-address 172.24.210.1 172.24.210.10
!
ip dhcp pool POOL_VLAN39
network 172.24.208.0 255.255.255.224
default-router 172.24.208.1
dns-server 172.24.210.10
ip dhcp pool POOL_VLAN49
network 172.24.208.32 255.255.255.224
!
!
default-router 172.24.208.33
dns-server 172.24.210.10
ip dhcp pool POOL_VLAN59
network 172.24.208.64 255.255.255.224
default-router 172.24.208.65
dns-server 172.24.210.10
ip dhcp pool POOL_IT
network 172.24.210.0 255.255.255.128
default-router 172.24.210.1
dns-server 172.24.210.10
!
!
username Sharapov password 7 0822455D0A16
!
no ip domain-lookup
ip domain-name Sharapov_R2
!
!
interface FastEthernet4/0
no ip address
duplex auto
speed auto
!
interface FastEthernet4/0.39
encapsulation dot1Q 39

```

```

ip address 172.24.208.1
255.255.255.224
!
interface FastEthernet4/0.49
encapsulation dot1Q 49
ip address 172.24.208.33
255.255.255.224
!
interface FastEthernet4/0.59
encapsulation dot1Q 59
ip address 172.24.208.65
255.255.255.224
!
interface FastEthernet4/0.99
encapsulation dot1Q 99
ip address 172.24.208.97
255.255.255.240
!
interface FastEthernet5/0
description des WAN1
ip address 10.0.9.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet6/0
description to IT
ip address 172.24.210.1
255.255.255.128

```

```

duplex auto
speed auto
!
interface FastEthernet7/0
description WAN2
ip address 10.0.9.5 255.255.255.252
duplex auto
speed auto
!
router eigrp 20
redistribute static
passive-interface FastEthernet4/0.39
passive-interface FastEthernet4/0.49
passive-interface FastEthernet4/0.59
passive-interface FastEthernet4/0.99
network 10.0.9.0 0.0.0.3
network 10.0.9.4 0.0.0.3
network 172.24.210.0 0.0.0.127
network 172.24.208.0 0.0.0.31
network 172.24.208.32 0.0.0.31
network 172.24.208.64 0.0.0.31
network 172.24.208.96 0.0.0.15
auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!

```

```

ip flow-export version 9
!
banner motd #123-21ck Sharapov.
There is protection#
!
!
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

      1.   Налаштування   роутера
Sharapov_R3
!
version 15.1

no service timestamps log datetime
msec
no service timestamps debug datetime
msec
service password-encryption
!
hostname Sharapov_R3
!
enable secret 5
$1$mERr$hX5rVt7rPNoS4wqbXKX7
m0
!
ip dhcp excluded-address
172.24.209.129 172.24.209.139
!
ip dhcp pool POOL_Kiient
  network 172.24.209.128
255.255.255.128
  default-router 172.24.209.129
  dns-server 172.24.210.10
!
!
username Sharapov password 7
0822455D0A16
!
license udi pid CISCO2911/K9 sn
FTX1524ZW69-
!
no ip domain-lookup

```

```

ip domain-name Sharapov_R3
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
  description TO Klient
  ip address 172.24.209.129
  255.255.255.128
  ip nat inside
  duplex auto
  speed auto
!
interface Serial0/1/0
  description WAN5
  bandwidth 128
  ip address 10.0.9.18 255.255.255.252
  ip nat inside
  clock rate 128000
!
interface Serial0/1/1
  description to WAN6
  bandwidth 128
  ip address 10.0.9.21 255.255.255.252
  ip nat inside
  clock rate 128000
!
interface Serial0/2/0
  description to ISP
  bandwidth 128
  ip address 209.165.202.2
  255.255.255.224
  ip nat outside
!
  switchport mode access
  router eigrp 20
  redistribute static
  passive-interface GigabitEthernet0/0
  network 10.0.9.20 0.0.0.3
  network 10.0.9.16 0.0.0.3
  network 172.24.209.128 0.0.0.127
!
  ip nat pool Internet 209.165.202.5
  209.165.202.30 netmask
  255.255.255.224
  ip nat inside source list 2 pool Internet
  ip nat inside source static
  172.24.208.42 209.165.202.3
  ip classless
  ip route 0.0.0.0 0.0.0.0 209.165.202.1
  ip route 172.24.208.0 255.255.248.0
  Serial0/2/0
!
  ip flow-export version 9
!
  access-list 2 permit 172.24.208.0
  0.0.7.255

```

```

!
no cdp run
!
banner motd #123-21sk Sharapov.
Login for authorized users 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

```

### 3. Налаштування роутера Sharapov\_R4

```

!
version 15.1
no service timestamps log datetime
msec
no service timestamps debug datetime
msec

```

```

service password-encryption
!
hostname Sharapov_R4
!
enable secret 5
$1$mERr$hX5rVt7rPNoS4wqbXKX7
m0
!
ip dhcp excluded-address
209.165.200.1 209.165.200.5
ip dhcp excluded-address
172.24.210.193 172.24.210.199
!
ip dhcp pool POOL_SHome
network 209.165.200.0 255.255.255.0
default-router 209.165.200.1
dns-server 10.22.226.139
ip dhcp pool POOL_Dog
network 172.24.210.192
255.255.255.224
default-router 172.24.210.193
dns-server 172.24.210.10
!
username Sharapov password 7
0822455D0A16
license udi pid CISCO2911/K9 sn
FTX1524681F-
!
no ip domain-lookup

```

```
ip domain-name Sharapov_R4
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
description TO R5
ip address 10.0.9.14 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
description TO SmartHome
ip address 209.165.200.1
255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/2
description TO Dogovor
ip address 172.24.210.193
255.255.255.224
duplex auto
speed auto
!
interface Serial0/1/1
description to R3
bandwidth 128

ip address 10.0.9.22 255.255.255.252
!
router eigrp 20
redistribute static
passive-interface GigabitEthernet0/2
network 10.0.9.0 0.0.0.3
network 10.0.9.20 0.0.0.3
network 172.24.210.192 0.0.0.31
network 172.24.209.0 0.0.0.127
network 10.0.9.12 0.0.0.3
network 209.165.200.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!
ip flow-export version 9
!
no cdp run
!
banner motd #123-21sk Sharapov.
Login for authorized users 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. Налаштування комутатора
Sw_YB_1
!
version 15.0
no service timestamps log datetime
msec
no service timestamps debug datetime
msec
service password-encryption
!
hostname Sw_YB_2
!
enable secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7
m0
!
ip domain-name Sharapov_Sw_YB_2
!
username Sharapov privilege 1
password 7 0822455D0A16
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
switchport access vlan 39
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 39
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 39
switchport mode access

```

```
!  
interface FastEthernet0/7  
  switchport access vlan 39  
  switchport mode access  
!  
interface FastEthernet0/8  
  switchport access vlan 39  
  switchport mode access  
!  
interface FastEthernet0/9  
  shutdown  
!  
interface FastEthernet0/10  
  switchport access vlan 49  
  switchport mode access  
!  
interface FastEthernet0/11  
  switchport access vlan 49  
  switchport mode access  
  switchport port-security  
  switchport port-security maximum 2  
  switchport port-security mac-address  
  sticky  
  switchport port-security violation  
  restrict  
!  
interface FastEthernet0/12  
  switchport access vlan 49  
  switchport mode access  
!  
interface FastEthernet0/13  
  switchport access vlan 49  
  switchport mode access  
!  
interface FastEthernet0/14  
  switchport access vlan 49  
  switchport mode access  
!  
interface FastEthernet0/15  
  switchport access vlan 59  
  switchport mode access  
!  
interface FastEthernet0/16  
  switchport access vlan 59  
  switchport mode access  
!  
interface FastEthernet0/17  
  switchport access vlan 59  
  switchport mode access  
!  
interface FastEthernet0/18  
  switchport access vlan 59  
  switchport mode access  
!
```



```
interface FastEthernet0/19
  switchport access vlan 59
  switchport mode access
!
interface FastEthernet0/20
  switchport access vlan 59
  switchport mode access
!
interface FastEthernet0/21
  shutdown
!
interface FastEthernet0/22
  shutdown
!
interface FastEthernet0/23
  shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
  switchport trunk native vlan 100
  switchport trunk allowed vlan
39,49,59,99-100
  switchport mode trunk
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan99
  description LAN Vnutr_99
  ip address 172.24.208.99
255.255.255.224
!
ip default-gateway 172.24.208.97
!
banner motd #123-21ck Sharapov.
There is protection#
!
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
```

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

**ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ  
НАЛАШТУВАННЯ ІОТ СИСТЕМИ**

Текст програми  
804.02070743.20020-01 12 01

Листів 3

**2024**

## АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування IoT-системи та моделювання в Packet Tracer. Програмний код створений мовою Python для контролерів.

**ЗМІСТ**

		Стор.
1.	Лістинг коду для моделювання в Packet Tracer	3

```

from gpio import *
from time import *
from ioecclient import *
import math

MoushenSensor1 = 0 # Датчик наявності під'єднаний до цифрового виводу
0
Lamp1 = 3; # лампа під'єднана до цифрового виводу 1
MoushenSensor2 = 2 # Датчик наявності під'єднаний до цифрового виводу
2
Lamp2 = 1; # лампа під'єднана до цифрового виводу 3
Diod = 4; # Diod під'єднаний до цифрового виводу 0

pinMode(MoushenSensor1, IN) # встановлений режим роботи порта як "вхід"
pinMode(Diod, OUT) #встановлений режим роботи порта як "вихід"
pinMode(MoushenSensor2, IN)
pinMode(Lamp1, OUT)
pinMode(Lamp2, OUT)

IoEClient.setup({
    "type": "Kontroller1",
    "states": [
        {
            "name": "Temperature",
            "type": "number",
            "unit": "~C",
            "imperialUnit": "~F",
            "toImperialConversion": "Temperature*1.8+32",
            "toMetricConversion": "(Temperature-32)/1.8",
            "decimalDigits":1
        },
        {
            "name": "Motion1",
            "type": "bool"
        },
        {
            "name": "Lamp_Zon1",
            "type": "bool"
        },
    ]
})

```

```

{
    "name": "Motion2",
    "type": "bool"
  },

  {
    "name": "Lamp_Zon2",
    "type": "bool"
  } ]
});

```

def detectTemperature(): # функція запису набору символів (str) на зазначений порт

```

value=((analogRead(A0)*200/1023-100))

```

```

if (value < 10):

```

```

    digitalWrite(Diod, HIGH)

```

```

else:

```

```

    digitalWrite(Diod, LOW)

```

```

def main():

```

```

    while True:

```

```

        Temperature=analogRead(A0)* 200 / (1023) -100

```

```

        add_event_detect(A0, detectTemperature)

```

```

        MD1 = digitalRead(MoushenSensor1)

```

```

        if (MD1 == HIGH):

```

```

            customWrite(Lamp1, 1)

```

```

            delay(500)

```

```

            Motion1=1

```

```

            Lamp_Zon1=1

```

```

        else:

```

```

            customWrite(Lamp1, 0)

```

```

            Motion1=0

```

```

            Lamp_Zon1=0

```

```

        MD2 = digitalRead(MoushenSensor2)

```

```

        if (MD2 == HIGH):

```

```

            customWrite(Lamp2, 1)

```

```
        delay(500)
        Motion2=1
        Lamp_Zon2=1
    else:
        customWrite(Lamp2, 0)
        Motion2=0
        Lamp_Zon2=0

    IoEClient.reportStates([ Temperature, Motion1, Lamp_Zon1,
Motion2, Lamp_Zon2])

if __name__ == "__main__":
    main()
```