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

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Тимченка Богдана Миколайовича
(ПІБ)
академічної групи 123-19-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

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

на тему "Комп'ютерна система юридичної фірми "Avaris" з реалізацією побудови та налаштування корпоративної мережі та підсистеми IoT безпеки"
(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
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)
"____" червня 2023 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавр

студента Тимченка Б.М. **академічної групи** 123-19-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

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

на тему "Комп'ютерна система юридичної фірми "Avaris" з реалізацією побудови та налаштування корпоративної мережі та підсистеми IoT безпеки"

затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 № 350-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	17.05.2023
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	23.05.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	26.05.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	27.05.2023

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

Дата видачі 19.12.2022

Дата подання до екзаменаційної комісії 08.06.2023

Прийнято до виконання _____ Тимченко Б.М

РЕФЕРАТ

Пояснювальна записка: 78с., 26 рис., 13 табл., 1 дод., 6 джерел.

МЕРЕЖА, СИСТЕМА, БЕЗПЕКА, ПРИСТРІЙ, ЮРИДИЧНА КОМПАНІЯ, ПРОТОКОЛ, ТОПОЛОГІЯ

Об’єкт розробки – комп’ютерна система для юридичної компанії «Avaris», з опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета роботи – розробка та налаштування корпоративної мережі для компанії «Avaris».

Виконано проєктування та розробка комп’ютерної системи з можливістю швидкої зміни та додавання функціоналу шляхом перепрограмування. Створена система орієнтована на забезпечення швидкого та надійного зв’язку між відділами компанії «Avaris» та збір статичної інформації.

Комп’ютерна система забезпечує легку масштабованість, а також програмну та технічну модернізацію системи.

Розроблена система забезпечує комунікацію між працівниками компанії, зберігання та безпеку даних у мережі.

Розроблена мережа реалізована відповідно до завдання на кваліфікаційну роботу бакалавра.

Моделювання та перевірка роботи системи виконані у програмному середовищі Cisco Packet Tracer.

Результати перевірки працездатності системи наведені у вигляді таблиць та рисунків наведено у пояснювальній записці та додатках.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КС – комп’ютерна система.

КМ – комп’ютерна мережа.

ПК – персональний комп’ютер.

DHCP – (Dynamic Host Configuration Protocol) — протокол, який дозволяє автоматично призначати адреси вузлам у мережі.

ACL – (Access Control List) – технологія, яка дозволяє обмежувати проходження вказаного типу трафіку на пристрої.

VLAN – (Virtual Local Area Network) – технологія, яка дозволяє розподіляти пристрої в мережі на робочі групи, не використовуючи додаткові маршрутизатори.

NAT – (Network Address Translation) – технологія, яка дозволяє транслювати приватні адреси у публічні при проходженні пакету через пристрій, шляхом змінення його заголовку.

OSPF – (Open Shortest Path First) – протокол динамічної маршрутизації.

VPN – (Virtual Private Network) – технологія, яка дозволяє створювати віртуальні мережі поверх мереж, які мають нижчий ступінь довіри.

ВСТУП

Сучасні технології і швидкий розвиток інформаційного суспільства вимагають від підприємств ефективної організації своєї інфраструктури та забезпечення безперебійного обміну даними в межах організації та зовнішніми партнерами. В умовах розширюваного бізнесу та глобалізації, корпоративна мережа стає ключовим фактором успіху для багатьох організацій. Вона забезпечує надійність, безпеку та ефективність комунікаційних процесів, впливаючи на управління, роботу співробітників та конкурентоспроможність підприємства.

Нові технології передачі даних, розширена реальність, інтернет речей та хмарні технології є основними світовими тенденціями, що впливають на розвиток комп'ютерних мереж. Розуміння цих тенденцій допомагає врахувати сучасні вимоги та напрямки у розробці корпоративних мереж.

У цьому контексті, дана кваліфікаційна робота присвячена розробці корпоративної мережі, яка відповідає поточним вимогам технологічного розвитку та задовольняє потреби організаційного середовища.

Актуальність даної кваліфікаційної роботи обумовлена потребою організацій у побудові ефективної та надійної корпоративної мережі. Результати дослідження можуть стати основою для вдосконалення існуючих мереж або розробки нових, забезпечуючи ефективну комунікацію, обмін даними та збереження інформації.

Подальші сфери застосування кваліфікаційної роботи можуть охоплювати різні галузі бізнесу, урядові структури, освітні заклади та інші організації, які прагнуть вдосконалити свою мережеву інфраструктуру.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умови застосування КС

Юридична галузь включає в себе правову систему, яка регулює права та обов'язки людей та організацій, а також способи їх врегулювання. Вона складається з різних підгалузей, таких як цивільне, кримінальне, адміністративне, комерційне та інші.

Юридична галузь є надзвичайно важливою, оскільки вона забезпечує порядок та стабільність в суспільстві, регулює взаємини між людьми та організаціями, захищає права та свободи громадян. Крім того, дана галузь є необхідною для забезпечення розвитку бізнесу та економіки, оскільки вона регулює відносини між підприємствами та їх клієнтами.

Основними принципами юридичної галузі є принцип законності, правової держави та правової відповідальності. Законність передбачає дотримання законів та правил, встановлених у правовій системі. Правова держава покладає на державу відповідальність за забезпечення дотримання прав та свобод громадян, а також рівності перед законом.

Юридична галузь надзвичайно різноманітна та постійно розвивається, враховуючи зміни в суспільстві та економіці. Вона включає в себе велику кількість професій, таких як юристи, адвокати, нотаріуси, судді, прокурори та інші, які забезпечують реалізацію правової системи.

Юридична галузь характеризується значним обсягом документів, що потребують зберігання та обробки, а також необхідністю обміну конфіденційною інформацією з клієнтами та партнерами.

Застосування комп'ютерних мереж може полегшити процеси зберігання, обробки та обміну інформацією, забезпечуючи швидкий та безпечний доступ до даних. Крім того, використання спеціалізованих програмних засобів може значно збільшити ефективність роботи юридичної компанії та покращити якість наданих послуг.

Останнім часом в Україні відбувається активна реформа правової системи, що передбачає зміну в законодавстві, вдосконалення процедур

судового розгляду та забезпечення більш ефективного захисту прав громадян. Також важливим напрямком розвитку юридичної галузі в Україні є використання сучасних технологій, зокрема комп'ютерних мереж та програмного забезпечення, що сприяють автоматизації процесів та підвищенню ефективності роботи юридичних компаній та інших юридичних структур.

1.2 Характеристика і структура об’єкта впровадження

1.2.1 Характеристика об’єкта впровадження

Об’єкт впровадження – офіс юридичної компанії «Avaris».

Компанія «Avaris Law Group» - це відома українська юридична компанія, яка спеціалізується на наданні комплексних юридичних послуг для бізнесу та приватних осіб.

Заснована в 2005 році, компанія має широкий діапазон клієнтів, серед яких є вітчизняні та міжнародні компанії, урядові та недержавні організації, приватні особи.

Основні напрямки діяльності компанії включають:

- Корпоративне право та бізнес-структуризація: «Avaris» надає клієнтам юридичну підтримку у формуванні, реєстрації та управлінні корпоративними структурами. Компанія також забезпечує консультації з питань корпоративного управління, ведення торговельної діяльності, реструктуризації та ліквідації компаній.[1]
- Податкове право та оподаткування: Компанія забезпечує професійну підтримку з питань податкового планування та оптимізації, контролю за податковими ризиками та співпрацю з органами державної податкової служби.[1]

- Трудове право: «Avaris» надає юридичну підтримку з питань трудового права, включаючи укладання трудових договорів,

вирішення спорів з працівниками, а також консультування з питань зайнятості, оплати праці та соціального захисту.[1]

- Міжнародне право: Компанія надає послуги з питань міжнародного права, зокрема здійснення зовнішньоекономічної діяльності, міжнародної торгівлі, знання інтелектуальної власності та забезпечення правової підтримки у міжнародних торгових операціях.[1]
- Судова та арбітражна практика: Компанія надає юридичну підтримку з питань розгляду спорів у судах та арбітражних судах. Компанія має досвід роботи з різними типами спорів, включаючи корпоративні, трудові, податкові, земельні та інші.[1]
- Нерухомість: Компанія забезпечує юридичну підтримку з питань нерухомості, включаючи консультації з питань купівлі, продажу та оренди нерухомості, забезпечення ведення реєстрації прав власності та інші.[1]
- Банківське та фінансове право: Компанія забезпечує юридичну підтримку з питань банківського та фінансового права, включаючи консультації з питань кредитування, лізингу, інвестицій та інших.[1]

«Avaris» відома своїм високим рівнем професіоналізму та дотриманням етичних стандартів у своїй роботі. Компанія керується принципом повної конфіденційності та забезпечує захист інтересів своїх клієнтів.

Компанія також активно займається благодійною діяльністю. Вона співпрацює з різними благодійними організаціями та фондами, надає безкоштовну юридичну допомогу та підтримку у судових справах. Компанія також підтримує розвиток мистецтва та культури, організовує різноманітні культурні та освітні заходи для своїх клієнтів та громадськості. Вона співпрацювала з благодійним фондом "Країна Мрій" та надала юридичну допомогу молодим талановитим людям з малозабезпечених сімей для отримання вищої освіти.

Компанія має свої офіси в Києві, Одесі, Харкові, Дніпрі, Миколаєві, Сумах, Запоріжжі та Львові, а також має можливість працювати з клієнтами з усієї України та з-за кордону, завдяки використанню сучасних технологій комунікації та онлайн-інструментів.

Загалом, компанія «Avaris» є однією з провідних юридичних компаній в Україні, яка забезпечує професійну та якісну юридичну підтримку з різних галузей права, враховуючи індивідуальні потреби кожного клієнта. Компанія активно розвивається та впроваджує нові технології, щоб забезпечити найкращі результати для своїх клієнтів.

1.2.2 Розміщення структурних підрозділів підприємства

Топологія розміщення офісу юридичної компанії «Avaris» складається з головного та віддаленого офісу.

Головний офіс розташовано за адресою Україна, 49051, Дніпропетровська обл., м. Дніпро, проспект Слобожанський, 42. Він складається з двох орендованого поверху у даній будівлі. Віддалений офіс орендує один поверх у будівлі за адресою проспект Слобожанський, 106. Відстань між головним та віддаленим офісами 2500 м. Схему георозміщення офісів зображено на рисунку 1.1.

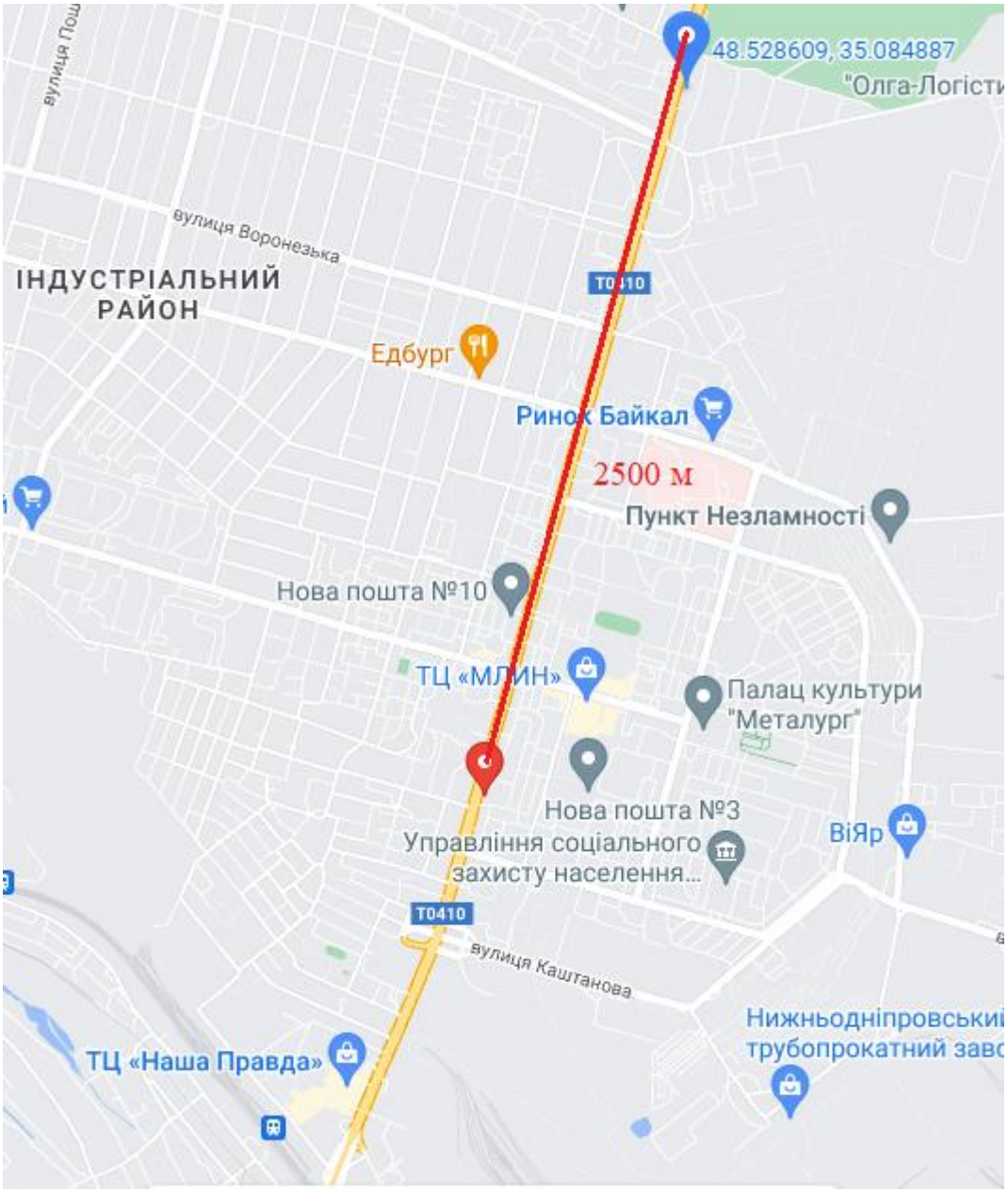

Рисунок 1.1 – Георозміщення основного та віддаленого офісів компанії «Avaris»

1.2.3 Організаційна структура підприємства

Організаційна структура компанії «Avaris» складається з наступних відділів:

- директор;
- керівники практики;
- корпоративне право;
- антимонопольне та конкурентне право;

- судова практика;
- нерухомість та будівництво;
- інтелектуальна власність;
- контрактне право;
- ліквідація та банкруцтво.

Компанія має лінійно-функціональну структуру управління. Лінійна структура управління - це один з видів організаційної структури, в якій всі підрозділи організації підпорядковані одному головному керівнику або керівництву вертикальної ланки.

Керівник кожного підрозділу напряму звітує про свою діяльність тільки вищестоящому керівництву і має право видавати доручення своїм підлеглим.

Ця структура є досить простою та прямолінійною, тому вона добре підходить для малих організацій або організацій з невеликою кількістю підрозділів. Однак вона може бути неефективною для великих організацій з багатьма різними підрозділами, оскільки це може призвести до перевантаження керівництва вертикальних ланок та повільної реакції на зміни в зовнішньому середовищі.

В компанії «Avaris» кожен керівник практики відповідає за власний підрозділ та напряму підпорядковується директору.

Схему організаційної структури підприємства наведено на рисунку 1.4.

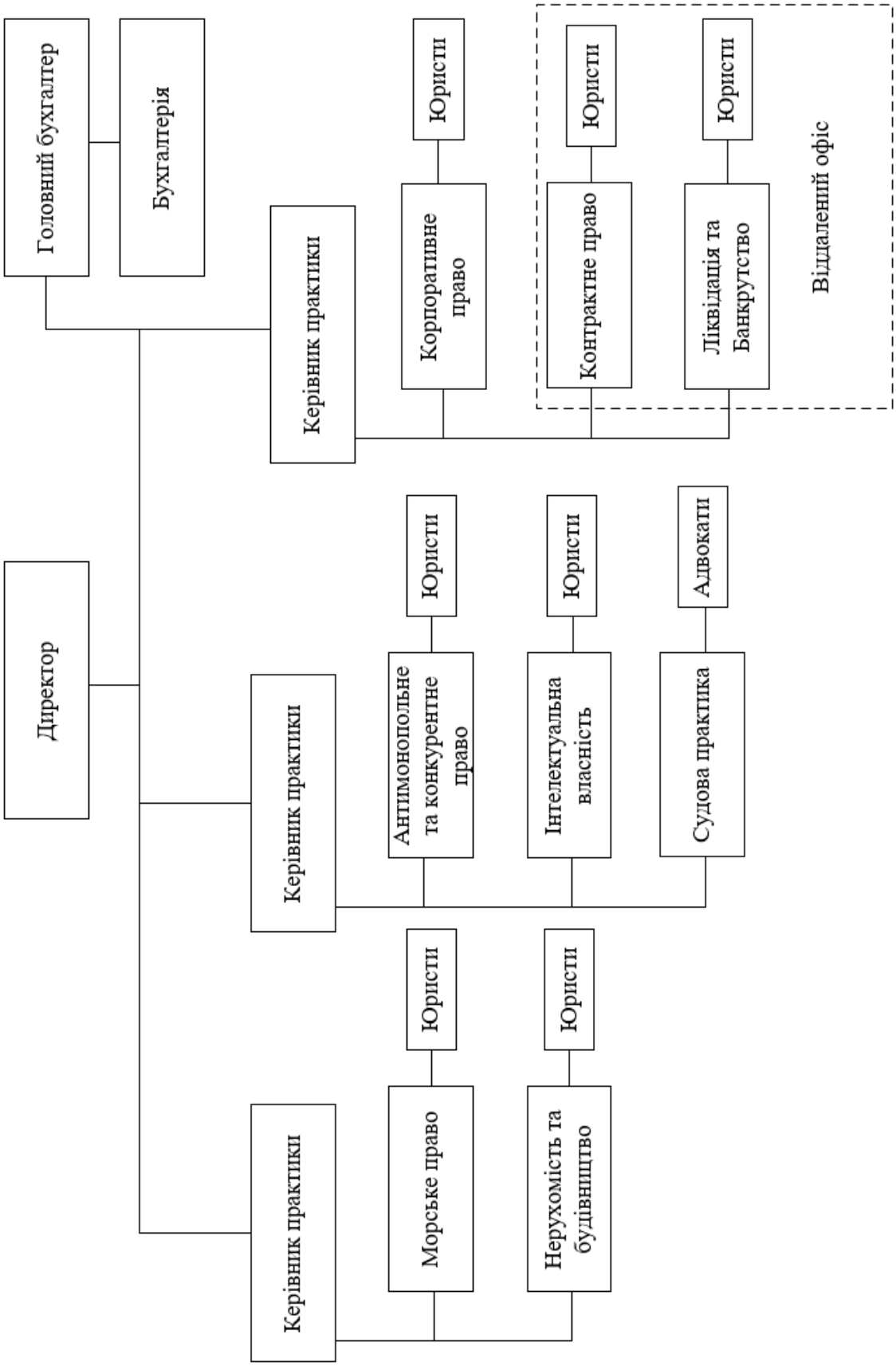

Рисунок 1.4 – Організаційна структура підприємства

1.2.4 Аналіз топологічної схеми розміщення структурних підрозділів підприємства

На рисунку 1.2 зображено структурну схему відділу бухгалтерії.

На рисунку 1.3 зображено частину структурної схеми відділу нерухомості та будівництва, який знаходиться у віддаленій мережі.

Рисунок 1.2 – Структурна схема відділу бухгалтерії

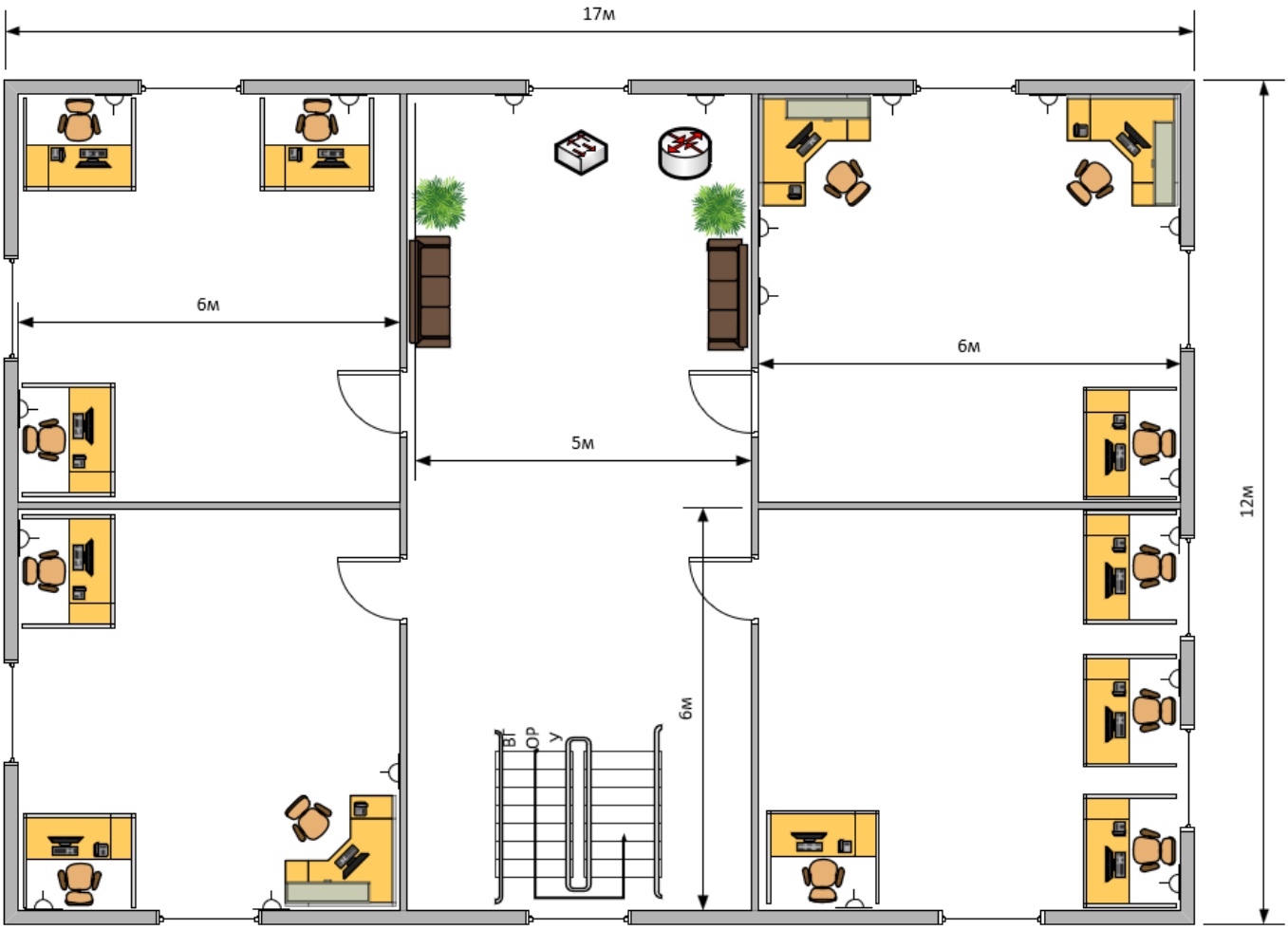

Рисунок 1.3 – Структурна схема частини відділів ліквідації бізнесу та банкрутства та контрактного права

1.3 Принципи, технічні способи та математичні методи інформаційного забезпечення об’єкта впровадження

Юридичні компанії широко використовують інформаційні технології для забезпечення ефективної та швидкої роботи. Нижче описано деякі принципи, технічні способи та математичні методи, які використовуються для інформаційного забезпечення компанії:

1. Захист конфіденційної інформації: юридична компанія повинна дотримуватись строгих правил збереження конфіденційної інформації своїх клієнтів. Для цього використовуються різноманітні криптографічні методи, такі як шифрування, хешування та цифрові підписи.

2. Електронний документообіг: електронний документообіг дозволяє юристам зберігати та обмінюватися документами в електронному форматі, що дозволяє забезпечити безпеку даних та збільшити ефективність процесу. Це зроблено за допомогою електронних поштових скриньок, веб-порталів та спеціалізованих програм для електронного документообігу.[2]
3. Використання штучного інтелекту та аналітики даних: використання методів штучного інтелекту та аналітики даних дозволяє прогнозувати тенденції та покращувати процеси прийняття рішень.
4. Резервне копіювання даних: юридична компанія повинна використовувати системи резервного копіювання даних, щоб захистити свою інформацію від випадкового видалення або пошкодження. Це здійснюється за допомогою зовнішніх дисків, хмарних сховищ та інших методів.
5. Системи управління відносинами з клієнтами (CRM): CRM системи дозволяють юридичним компанії вести облік клієнтів та їх потреб, спілкуватися з клієнтами, контролювати терміни та облікові записи, тощо.
6. Математичні методи та алгоритми: математичні методи та алгоритми допомагають вирішувати складні правові питання та забезпечують більш точний та ефективний аналіз даних. Наприклад, алгоритми машинного навчання використовуються для автоматичної класифікації документів та визначення ризиків у правових питаннях.

1.4 Аналітичний огляд існуючих способів обробки та передачі інформації

Юридичні компанії щодня стикаються зі значною кількістю інформації, яку необхідно обробляти та передавати в межах внутрішнього кола співробітників та зовнішніх клієнтів. Для забезпечення безперебійної та

ефективної роботи компанії важливо використовувати оптимальні способи обробки та передачі інформації.

Для цього використовуються системи електронного документообігу, які дозволяють зберігати, обробляти та передавати документи в електронному вигляді, що дозволяє зменшити кількість паперових документів та покращити їх доступність та зручність використання. Такі системи забезпечують безпеку та конфіденційність даних, а також дозволяють ефективно керувати документами та контролювати їх доступність. Але варто враховувати, що в разі відсутності доступу до мережі Інтернет може бути обмежена можливість використання систем електронного документообігу, що може призвести до затримок у роботі та негативно вплинути на продуктивність.[2]

Також ефективними є корпоративні портали. Вони дозволяють співробітникам та клієнтам отримувати доступ до потрібної інформації та документів в онлайн-режимі. Вони забезпечують доступ до різних видів інформації, включаючи новини, документацію, поради та інші ресурси, що допомагають підвищити ефективність роботи.

Важливим методом обробки інформації є хмарні технології. Ці технології дозволяють зберігати та обробляти інформацію в хмарних сервісах, що забезпечує доступність даних з будь-якого місця та пристрою з Інтернетом. Хмарні технології дозволяють зменшити витрати на обладнання та програмне забезпечення, а також забезпечують безпеку та захист даних. З мінусів можна виділити те, що користувачі не мають повного контролю над збереженням та обробкою їх даних, оскільки це залежить від постачальника хмарних сервісів. Також хмарні сервіси можуть збирати та використовувати дані користувачів для рекламних або інших комерційних цілей, що може бути проти вимог конфіденційності.[3]

Корисними є мобільні застосунки, які дозволяють співробітникам та клієнтам отримувати доступ до потрібної інформації та документів зі своїх мобільних пристроїв. Вони забезпечують швидкий та зручний доступ до інформації в будь-який час та з будь-якого місця.

1.5 Постановка завдання та мета роботи

Завданням кваліфікаційної роботи є розробка комп'ютерної система юридичної фірми "Avaris" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі з реалізацією IoT системи безпеки офісів компанії.

Для вирішення поставленої мети в роботі слід виконати наступні завдання:

- провести аналіз організаційної та структурної схем підприємства, його потреб та умов виконання проєкту;
- на основі зібраної інформації скласти технічні вимоги до розроблюваної системи та виконати розробку її апаратної частини; Зробити підбір необхідного обладнання та програмного забезпечення. Скласти його специфікацію;
- визначити структуру IoT компонента системи та завдання, яке дана система буде виконувати;
- визначитися з технологіями та топологією, що будуть використовуватися. Важливо вибрати технології, які найкраще відповідають потребам фірми;
- провести аналіз мережевого трафіку. Для ефективного планування мережі необхідно проаналізувати типи та обсяги мережевого трафіку, які будуть здійснюватися в офісах компанії;
- обрати спосіб управління мережею;
- створити фізичну та логічну топології КМ. Після вибору технологій та топології необхідно розробити фізичну та логічну структуру мережі, включаючи розташування мережевого обладнання, маршрутизаторів, комутаторів та інших пристроїв;
- виконати розрахунок адресації мережі компанії за методом VLSM;

- виконати конфігурування мережевого обладнання корпоративної мережі. Встановити IP-адреси, налаштувати безпеку, VLAN, DHCP, NAT та маршрутизацію;
- виконати налаштування безпеки в мережі з налаштуванням VPN та аутентифікації користувачів при доступі до пристроїв;
- розробити IoT систему безпеки офісів, яка буде обладнана розумними камерами, датчиками та сенсорами і забезпечуватиме увімкнення сирени при пожежі або несанкціонованому доступі до приміщень офісів;
- виконати тестування комп'ютерної мережі за допомогою моделювання у середовищі Cisco Packet Tracer та впровадження системи в роботу;

Результуюча мережа має бути надійною, масштабованою, гнучкою, безпечною та швидкою.

1.6 Визначення можливих напрямків рішення поставлених завдань

При виборі технології, на основі якої буде виконуватися побудова локальної мережі, є два основних варіанти: Wi-Fi та дротова Ethernet мережа. Основні переваги бездротової мережі полягають у тому, що бездротова мережа не потребує викладки кабелів, що робить процес побудови та розширення мережі менш трудомістким та швидким. Також бездротова мережа зазвичай менш коштує, оскільки не потребує придбання та установки кабелів, розгалужувачів та інших елементів дротової мережі. Але бездротова мережа значно програє Ethernet мережі у швидкості передачі даних та стабільності. Дротова мережа менш схильна до перерв у з'єднанні та впливу зовнішніх факторів, таких як перешкоди або електромагнітні інтерференції. Тому буде раціонально виконати побудову мережі для юридичної компанії на основі Ethernet.

При виборі топології мережі доречно зупинитися на топології типу зірка, так як вона зручна у керуванні та легко масштабується за необхідності.

Для забезпечення безпеки пристроїв варто встановити паролі на лінії consol та vty, на лініях vty необхідно використовувати захищений протокол ssh. На всіх пристроях мережі компанії необхідно встановити пароль до привілейованого режиму. Також необхідно впровадити в мережі технологію VPN.

У відділах корпоративного права та судової практики необхідно впровадити технологію віртуальних локальних мереж (VLAN). У відділах нерухомості та морського права потрібно впровадити технологію агрегації каналів (Ethernet Channel). У якості протоколу динамічної маршрутизації доцільно обрати протокол OSPF, так як він сумісний з більшістю обладнання. Для доступу до інтернету необхідно налаштувати технологію NAT на прикордонному маршрутизаторі, який пов’язано з провайдером.

При побудові IoT системи доцільно використати варіант побудови на основі технології IEEE 802.11 (Wi-Fi).

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до комп'ютерної системи компанії «Avaris»

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури та функціонування системи підрозділів компанії «Avaris»

Нижче наведено основні вимоги до структури та функціонування комп'ютерної системи юридичної компанії «Avaris».

Мережа повинна складатися з п'яти підмереж (LAN1-LAN5). LAN1 буде виділено для відділів нерухомості та морського права. LAN2 виділено під відділи антимонопольного та конкурентного права та інтелектуальної власності. LAN3 виділено під відділи ліквідації бізнесу та банкрутства та контрактного права. LAN4 виділено під відділ бухгалтерії. LAN 5 виділено для відділів корпоративного права та судової практики.

За вимогами від замовника підмережі повинні мати наступну кількість вузлів:

LAN1 – 100;

LAN2 – 97;

LAN3 – 95;

LAN4 – 32;

LAN5 – 41;

Також мережа повинна бути побудована за топологічною схемою, зображеною на рисунку 2.1, яка надана замовником.

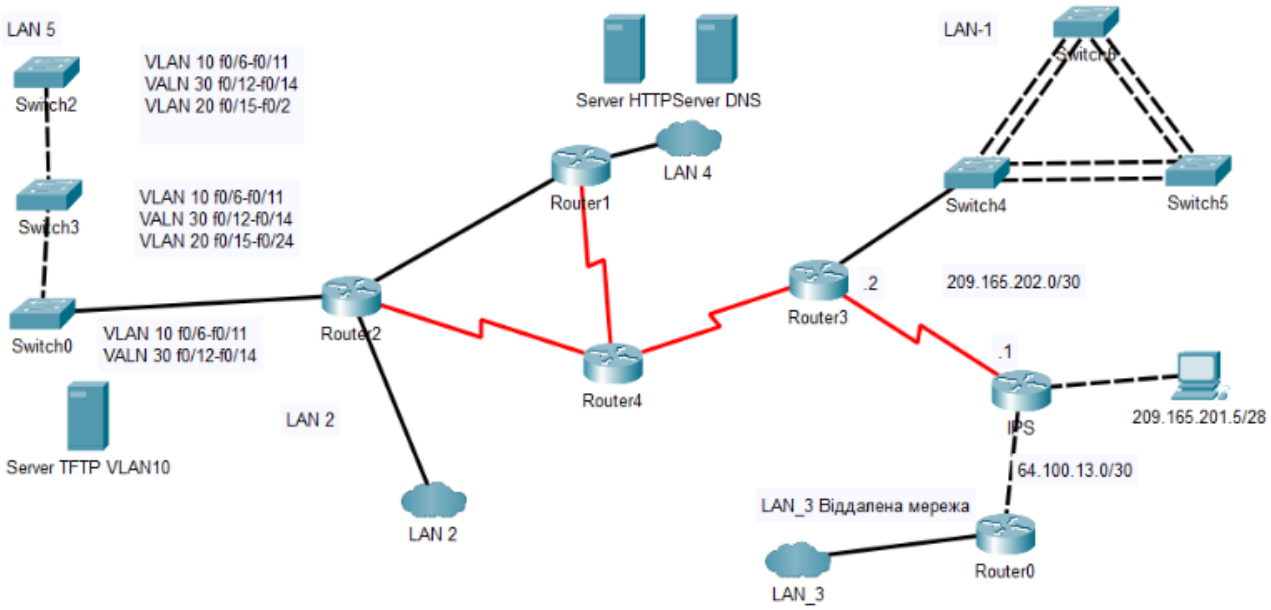

Рисунок 2.1 – Загальна архітектура мережі компанії

2.1.1.2 Вимоги до способів і засобів зв’язку між компонентами комп’ютерної системи компанії «Avaris»

Зв’язок між пристроями та комутаторами у мережі необхідно забезпечувати за допомогою інтерфейсів FastEthernet. Зв’язок комутаторів з маршрутизаторами повинен виконуватися через Gigabit інтерфейси. Маршрутизатори у мережі потрібно з’єднувати через інтерфейси Serial. Для забезпечення зв’язку між розробленими підмережами необхідно реалізувати протокол динамічної маршрутизації OSPF. Для доступу до мережі Internet необхідно реалізувати технологію динамічного NAT на пограничних маршрутизаторах головного та віддаленого офісів компанії. Щоб забезпечити захищене з’єднання між головним та віддаленим офісом необхідно виконати налаштування технології VPN на базі протоколу IPsec.

2.1.1.3 Вимоги до характеристик взаємозв'язків комп'ютерної системи компанії «Avaris» із суміжними системами, вимоги до її сумісності

Розроблена система повинна підтримувати усі стандартні протоколи обміну даними, такі як HTTP, HTTPS, FTP та інші. Усе мережеве обладнання повинно бути сумісним з такими технологіями, як VLAN, NAT, DHCP та AAA. Розроблена система повинна бути сумісною з іншими системами. Для цього система повинна мати змогу інтерпретувати формати даних, які використовуються у більшості суміжних систем, такі як JSON та XML. Під час взаємодії з іншими підсистемами повинні бути реалізовані такі методи захисту, як аутентифікація та шифрування, для забезпечення безпеки системи компанії.

2.1.1.4 Вимоги до режимів функціонування комп'ютерної системи компанії «Avaris»

Розроблена система повинна мати здатність функціонувати у разі оновлень та аварійних ситуацій (вихід із ладу частини мережевого обладнання). Для цього необхідно забезпечити додаткові з'єднання між комутаторами у відділах нерухомості та морського права. Також, усі маршрутизатори, окрім пограничного, повинні бути з'єднані між собою для забезпечення функціонування системи у разі обриву однієї з ліній зв'язку. Необхідно провести розрахунок інтенсивності трафіку у найбільшій підмережі компанії, щоб забезпечити для системи достатню швидкодію.

2.1.1.5 Вимоги до діагностування комп'ютерної системи компанії «Avaris»

Не менше, ніж раз на пів року (у разі непередбачуваних пошкоджень системи та її виходу з ладу, аналіз та ремонтні роботи проводяться поза графіком) відповідний персонал компанії (мережеві інженери) повинен проводити діагностування системи на наявність як фізичних, так і програмних

проблем. При перевірці наявності фізичних проблем персонал повинен приділити увагу таким проблемам, як:

- пошкодження каналів зв’язку (обрив кабелів системи);
- фізичне пошкодження мережевого обладнання та комп’ютерів системи;
- повний або частковий вихід з ладу мережевого та комп’ютерного обладнання.

При перевірці наявності програмних проблем з мережею персонал повинен приділити увагу таким проблемам, як:

- помилки або збої у конфігурації мережевого обладнання (маршрутизатори та комутатори);
- відсутність критичних оновлень мережевого обладнання та ПК;
- відсутність необхідних драйверів на комп’ютерах системи.

Після проведення повної діагностики системи персонал повинен виконувати журналювання кожної визначеної та виправленої помилки та несправності у мережі.

2.1.1.6 Перспективи розвитку комп’ютерної системи компанії «Avaris»

Система буде експлуатуватися компанією у довгостроковій перспективі, тому має бути виконана відповідно до усіх поставлених вимог. Необхідно забезпечити легку масштабованість мережі використанням мережевих протоколів, орієнтованих на роботу у великих мережах (OSPF). Необхідно забезпечити легку модернізацію системи шляхом додавання нових, або заміни старих мережевих пристроїв. Для цього необхідно використовувати пристрої, які матимуть додаткову кількість інтерфейсів та які підтримують усі сучасні мережеві протоколи. Адресація мережі повинна бути виконана з запасом адрес для кожної підмережі (не менше 15 адрес), це дозволить уникнути перерахунку адресації при збільшенні кількості вузлів.

2.1.1.7 Вимоги до показників призначення

Основне призначення комп’ютерної мережі полягає у забезпеченні спільного доступу до документів, правової документації, клієнтських файлів та інших ресурсів всередині компанії. Це сприяє співпраці між різними відділами та співробітниками, покращує ефективність роботи та забезпечує єдність інформації в організації. Також не менш важливим призначенням є забезпечення безпеки даних. Комп’ютерна мережа дозволяє встановлювати механізми захисту та контролю доступу до конфіденційних даних компанії. Також комп’ютерна мережа дозволяє з'єднуватися з Інтернетом та мати доступ до різних онлайн-ресурсів, поштових серверів, баз даних та хмарних сервісів. Це дає змогу здійснювати пошук інформації, використовувати онлайн-інструменти та взаємодіяти з клієнтами та іншими організаціями через Інтернет.

2.1.1.8 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню технічних засобів комп’ютерної системи компанії «Avaris»

2.1.1.8.1 Умови і регламент експлуатації, які забезпечують використання технічних засобів системи з заданими технічними показниками

Мережеве обладнання повинно працювати в діапазоні температур від 15°C до 25°C. Важливо уникати екстримально низьких або високих температур, оскільки це може призвести до нестабільної роботи або пошкодження обладнання.

Рекомендована вологість повітря для мережевого обладнання становить не більше 75% без конденсації. Висока вологість може спричинити корозію і електричні замикання, тоді як надмірна сухість може спричинити статичну електрику. Важливо також уникати потрапляння рідини на обладнання.

Необхідно забезпечити наявність порошкових вогнегасників у кількості не менше 25 одиниць для головного офісу, та не менше 10 одиниць для віддаленого офісу. Вогнегасники повинні бути розміщені біля кімнат з найбільшою кількістю мережевого обладнання.

При експлуатації, зберіганні та перевезенні обладнання необхідно дотримуватися усіх вимог, зазначених безпосередньо виробником даного обладнання.

2.1.1.8.2 Вимоги до параметрів мереж енергопостачання (живлення та заземлення)

Електроживлення в офісі повинно бути стабільним, кабелі живлення повинні бути новими, без пошкоджень ізоляції. Всі електричні точки в офісі повинні мати надійне заземлення. Розетки повинні бути типу F, напруга, яка подається на розетки, повинна бути 220В з частотою 50 герц (стандартні значення напруги та частоти в Україні).

Всі розетки, проводи та електричні прилади повинні бути без ознак пошкодження або корозії. Забороняється використання розеток, вимикачів та електричних з'єднань, які мають найменші ознаки пошкодження або не відповідають стандартам.

Усім працівникам компанії заборонено підключати до енергомережі компанії власні електричні пристрої (за виключенням телефонів та ноутбуків) та подовжувачі.

2.1.1.8.3 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи

Для впровадження та обслуговування система має бути забезпечена відповідним технічним персоналом.

Персонал повинен включати мережевих інженерів (у кількості не менше 10 працівників), до обов'язків яких входить:

- впровадження та інтеграція системи в роботу;
- детальна діагностика системи раз на пів року;
- виконання ремонту та налагодження системи у разі непередбачуваної поламки;

- проведення навчання та інструктажу для нових працівників, які займаються обслуговуванням системи.

Також необхідно забезпечити необхідну кількість системних адміністраторів (15 системних адміністраторів для головного офісу та 5 для віддаленого), до обов'язків яких входить:

- щоденне обслуговування та перевірка системи;
- виправлення проблем з комп'ютерами працівників компанії;
- забезпечення регулярного оновлення усіх вузлів компанії;
- доповідання стану роботи системи мережевим інженерам.

Усі мережеві інженери компанії повинні мати освіту не нижче ступеня магістра у галузі інформаційних технологій та досвід роботи з комп'ютерними системами не менше двох років.

Системні адміністратори повинні мати освіту не нижче ступеня бакалавра у галузі інформаційних технологій та досвід роботи з комп'ютерними системами не менше, ніж пів року.

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

Необхідно забезпечити офіси компанії додатковим мережевим та комп'ютерним обладнанням для заміни у разі непередбачуваного виходу з ладу обладнання.

Запасні вироби повинні зберігатися в безпечному та доступному місці, де вони будуть захищені від пилу, вологості, температурних змін і потенційних пошкоджень. Усі приміщення, в яких зберігається обладнання, повинні бути захищені від несанкціонованого доступу.

Перелік запасних приладів, якими повинні бути забезпечені офіси наступний:

- маршрутизатори у кількості не менше 3;
- комутатори у кількості не менше 10;

- додаткові комплектуючі ПК (блоки живлення, материнські плати та оперативна пам’ять);
- кабелі витої пари UTP не менше 30 метрів;
- конектори RJ45 у кількості не менше 50.

Усе запасне обладнання необхідно зберігати в оригінальній упаковці, в якій здійснюється постачання виробником разом з гарантійними талонами та документацією з експлуатації. Зберігання виконується згідно умов, зазначених виробником.

2.1.1.8.5 Вимоги до регламенту обслуговування комп’ютерної системи компанії «Avaris»

Необхідно запровадити регулярну перевірку та налаштування апаратного та програмного забезпечення, оновлення оперативної системи та драйверів, а також перевірку на наявність вірусів і шкідливих програм.

Необхідно впровадити план відновлення комп’ютерної системи після аварії, який описує дії, що необхідно вжити в разі виникнення критичної ситуації, такої як втрата даних або вимкнення системи. Це включає процедури відновлення даних з резервних копій, відновлення роботи мережі та відновлення доступу до системи.

Комп’ютерна система повинна бути обладнана програмним забезпеченням для моніторингу стану апаратного та програмного забезпечення, щоб виявляти можливі несправності, вирішувати проблеми з мережевим з'єднанням, виявляти загрози безпеці і забезпечувати ефективну роботу системи.

2.1.1.9 Вимоги до патентної чистоти

Компанія повинна користуватись лише легальним програмним забезпеченням, яке має правову охорону. Використання піратського або нелегального програмного забезпечення може призвести до порушення патентних прав і мати юридичні наслідки. Всі ліцензійні угоди мають бути

дотримані. Компанія має переконатися відсутності порушень патентних прав на програмне забезпечення, апаратне забезпечення та дизайн інтерфейсів, що використовується у своїй діяльності. Компанія повинна уникати використання технологій або інтелектуальної власності, яка порушує патентні права інших компаній. Це включає уникання використання патентованих алгоритмів, методів та систем без дозволу від власників патентів.

2.1.2 Додаткові вимоги

2.1.2.1 Вимоги до активного обладнання

Активне мережеве обладнання повинно бути сумісним з існуючими мережевими протоколами та стандартами, що використовуються в компанії (TCP/IP, DHCP, Ethernet). Це дозволить безперебійну інтеграцію з існуючою інфраструктурою та забезпечить сумісність з іншими пристроями.

Мережеве обладнання повинно бути масштабованим для відповіді на зростаючі потреби компанії. Це означає, що воно повинно мати можливість розширення, додавання нових портів, модулів або підключення додаткових пристроїв для підтримки збільшення обсягу даних та кількості користувачів.

Обладнання повинно мати достатню пропускну здатність для задоволення потреб компанії. Це означає, що маршрутизатори та інші пристрої повинні мати достатню швидкість передачі даних (до 1 Гбіт/с), щоб підтримувати велику кількість користувачів та обсяг даних, що пересилаються.

Виробник обладнання повинен надавати відповідну технічну підтримку, оновлення програмного забезпечення та патчі безпеки. Компанія повинна мати доступ до технічної підтримки для вирішення будь-яких проблем або неполадок, що виникають у зв'язку з мережевим обладнанням.

2.1.2.2 Вимоги до кабель-каналів, інформаційних та електричних розеток

Кабель-канали повинні бути розташовані зручно та безпечно, з урахуванням можливості заміни та обслуговування кабелів. Кабель-канали мають бути достатньо просторими (рекомендований розмір не менше, ніж 20х20 мм), щоб помістити всі необхідні кабелі та дроти, а також забезпечити мінімальне згинання кабелів для запобігання їх пошкодженню.

Інформаційні розетки повинні бути зручними для підключення обладнання та мати захисні ковпачки для запобігання пошкодженню під час з'єднання. Розетки та кабель-канали повинні мати позначення для зручності ідентифікації та обслуговування.

При встановленні нових кабель-каналів та розеток, має бути врахована можливість розширення мережі та підключення нового обладнання в майбутньому.

2.1.2.3 Вимоги до комунікаційного обладнання і його розташування

Комунікаційне обладнання повинно розміщуватись у комутаційних шафах, котрі кріпляться на стіну. Комутаційні шафи повинні мати достатній розмір і ємність для розміщення всього необхідного мережевого обладнання (не менше 10 дюймів у діагоналі).

Комутаційні шафи повинні мати належну організацію кабелювання, включаючи горизонтальні і вертикальні кабельні канали, гачки для фіксації кабелів і маркування портів для забезпечення чистоти і структурованості кабельного монтажу, полегшення підключення та усунення несправностей і забезпечення легкого доступу до кабельних з'єднань.

Комутаційні шафи повинні бути замкнутими або мати механізми безпеки, такі як замки або біометричні системи доступу, щоб запобігти несанкціонованому доступу до обладнання.

Більшість комутаторів повинні мати 24 порти типу FastEthernet. Обладнання також повинно бути розміщене з урахуванням можливості забезпечення доступу для технічного обслуговування та ремонту.

2.1.2.4 Вимоги до резервування

Нижче наведено основні вимоги до резервування даних у комп'ютерній системі компанії «Avaris»:

- резервне копіювання повинно виконуватися регулярно (один раз на тиждень);
- резервна копія повинна містити всі важливі дані, що зберігаються в системі. Вона повинна включати файли, бази даних, конфігураційні файли, програмне забезпечення та всі інші компоненти, які необхідні для відновлення системи;
- резервні копії повинні зберігатися на зовнішніх пристроях, які фізично відокремлені від основної системи;
- резервні копії повинні бути зашифровані для забезпечення конфіденційності даних;
- після створення резервної копії необхідно перевірити її цілісність, щоб переконатися, що дані були успішно збережені і можуть бути відновлені.

2.1.3 Вимоги до налаштувань та функцій, виконуваних системою

Система повинна забезпечувати доступ до необхідної інформації з будь-якого місця та в будь-який час. Мережа повинна дозволяти віддалений доступ до систем та ресурсів компанії з-за меж офісу, що дозволяє співробітникам працювати з будь-якого місця та забезпечувати продуктивність в разі відряджень або віддаленої роботи.

Система повинна забезпечувати захист інформації від несанкціонованого доступу, зловмисних програм та вірусів. Вона повинна

підтримувати шифрування даних, фільтрацію трафіку, аутентифікацію користувачів та інші заходи безпеки.

Система повинна забезпечувати комунікацію між працівниками компанії та зовнішніми контрагентами за допомогою електронної пошти, відеоконференцій та інших засобів.

Система повинна бути забезпечена резервним копіюванням даних на зовнішні носії, а також забезпечена відновленням даних у разі втрати або пошкодження.

Система повинна мати можливості централізованого управління, моніторингу та керування. Це дозволяє адміністраторам мережі віддалено керувати мережевими пристроями, відслідковувати стан мережі, виявляти і усувати проблеми та забезпечувати безпеку мережі.

Основні вимоги до підсистем компанії:

- на кожному мережевому пристрої необхідно призначити ім’я, встановити паролі до режиму EXEC та ліній console та vty. Зазначити використання протоколу SSH замість Telnet при віддаленому з’єднанні з пристроями. На кожному пристрої створити користувача та доменне ім’я;
- налаштувати адресацію усіх пристроїв мережі;
- у відділі нерухомості та морського права необхідно впровадити технологію агрегації фізичних каналів для забезпечення більшої стабільності та пропускної здатності;
- у відділі корпоративного права та судової практики необхідно виконати розбиття підмережі на VLAN за таким принципом: VLAN23 – корпоративне право, VLAN33 – судова практика, VLAN43 – керівники;
- виконати налаштування конфігурації DHCP для забезпечення динамічного призначення адрес вузлам;
- реалізувати аутентифікацію на маршрутизаторах за допомогою служби AAA з використанням протоколу Radius;

- зв’язок між усіма підсистемами необхідно забезпечити налаштуванням динамічної маршрутизації. На кожному маршрутизаторі налаштувати статичні маршрути за замовчуванням;
- на пограничних маршрутизаторах офісів виконати налаштування списків доступу ACL, динамічного NAT та VPN на базі IPsec;
- на DCE-інтерфейсах маршрутизаторів встановити частоту 128000 та пропускну здатність 128;
- виконати налаштування HTTP та DNS серверів таким чином, щоб забезпечити роботу сайту компанії за доменним ім’ям 123.dnipro.ua;
- виконати налаштування безпеки портів комутаторів, до яких під’єднано сервери, за допомогою switchport security.

Необхідно впровадити IoT систему, яка буде забезпечувати безпеку приміщень головного та віддаленого офісів та повинна виконувати наступні функції:

- увімкнення сирени та камер спостереження при спрацюванні датчика руху;
- увімкнення сирени при спрацюванні датчика вогню та відмикання дверей;
- доступ до офісних приміщень за допомогою RFID карток та зчитувача.

Пристрої, за допомогою яких виконується побудова IoT компонента системи повинні підтримувати стандарт IEEE 802.11 (Wi-Fi) та Ethernet. IoT-система повинна функціонувати у власній локальній мережі за допомогою HomeGateway та бути налаштованою за допомогою IoT-серверу, в якості якого виступає сам HomeGateway.

2.1.4 Вимоги до видів забезпечення

2.1.4.1 Вимоги до інформаційного забезпечення

1. Регулярне оновлення програмного та апаратного забезпечення. Оновлення програм та драйверів необхідне, щоб запобігти вразливостям в системі та забезпечити її стабільну роботу.
2. Резервне копіювання даних. Регулярне створення резервних копій даних на зовнішньому носії необхідне, щоб запобігти втраті важливої інформації в разі виникнення технічних проблем.
3. Захист від вірусів та зломів. Комп'ютерна мережа повинна мати антивірусне програмне забезпечення, що оновлюється регулярно. Також необхідно забезпечити відповідний рівень захисту для доступу до важливої інформації.
4. Сумісність та інтеграція: Інформаційне забезпечення повинно бути сумісним із використовуваним програмним забезпеченням та системами в юридичній компанії. Інтеграція між різними додатками та системами допомагає ефективно обмінюватися даними та спрощує робочі процеси.

2.1.4.2 Вимоги до лінгвістичного забезпечення

Взаємодія з системою повинна бути забезпечена українською та англійською мовами за замовчуванням. Система повинна підтримувати мови, які використовуються клієнтами.

Система повинна мати зрозумілий та зручний інтерфейс для користувачів, що дозволяє легко та швидко здійснювати пошук і вибір необхідної інформації.

Система повинна забезпечувати підтримку різних мовних форматів, таких як Unicode та UTF-8.

2.1.4.3 Вимоги до технічного забезпечення

Усі комп’ютери в системі повинні бути забезпечені характеристиками, не нижче наведених:

- Intel Core i5 не нижче 9 покоління;
- оперативна пам’ять типу DDR4, обсягом не менше 8 гб;
- використання дискретних відеоадаптерів не обов’язкове;
- блоки живлення не менше 500W;
- комп’ютери повинні бути забезпечені усіма стандартними портами (не менше 1 USB 3.0 та 2 USB 2.0).

Кожне робоче місце повинно бути забезпечене монітором з довжиною діагоналі 23 дюйми, мембранною клавіатурою та дротовою мишею.

Усі мережеві пристрої (маршрутизатори та комутатори), які використовуються при побудові мережі, повинні бути від фірми виробника Cisco. Маршрутизатори повинні мати не менше 2 GE інтерфейсів. Пристрої повинні бути від офіційного дилера та мати всю відповідну документацію та гарантійні талони.

2.1.4.4 Вимоги до організаційного забезпечення

Доступ до мережевого обладнання повинен мати лише спеціалізований персонал (системні адміністратори та мережеві інженери з відповідною освітою та досвідом роботи, описаними у розділі 2.1.1.7.4), який займається його обслуговуванням. У разі виникнення помилок або несправностей (таких як поламка обладнання, пошкодження кабелів, неправильне налаштування конфігурації, неправильне встановлення обладнання) персонал, котрий експлуатує систему повинен звернутися то персоналу, котрий займається обслуговуванням системи. Заборонено спроби самостійного налагодження чи ремонту мережевого обладнання неспеціалізованим персоналом.

2.1.4.5 Вимоги до методичного забезпечення

Методичне забезпечення повинно містити інструкції та рекомендації щодо використання інформаційних систем, програмного забезпечення, електронних баз даних та інших технічних засобів. Це допомагає персоналу компанії користуватися різноманітними інструментами та технологіями з високою ефективністю та безпекою. Методичне забезпечення повинно включати посилання на відповідні стандарти та нормативи, які регулюють діяльність компанії, такі як законодавчі акти, правила, положення та інші документи, які встановлюють вимоги до проведення юридичних процедур, збереження даних та інші аспекти роботи компанії. Методичне забезпечення повинно передбачати навчання та підтримку персоналу щодо використання інформаційних систем, технічних засобів та методологій роботи. Це можуть бути тренінги, семінари, консультації та інші форми навчання, які сприяють підвищенню кваліфікації та компетентності персоналу.

2.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи компанії «Avaris»

2.2.1 Обстеження об'єкту розробки

Проаналізувавши організаційну схему підприємства, його структурну схему, загальну архітектуру мережі, сформовану замовником, та складені технічні вимоги до системи, можна виконати розробку структурної схеми комплексу технічних засобів комп'ютерної системи (рисунок 2.2).

Вся мережа розділена на 5 підмереж. Зв'язок між маршрутизаторами забезпечується за допомогою інтерфейсів Serial. Комутатори з'єднуються з маршрутизаторами за допомогою інтерфейсів Gigabit Ethernet. Зв'язок між комп'ютерами та комутаторами забезпечується за допомогою інтерфейсів Fast Ethernet. Зв'язок IoT пристроїв забезпечується за допомогою Wi-Fi.

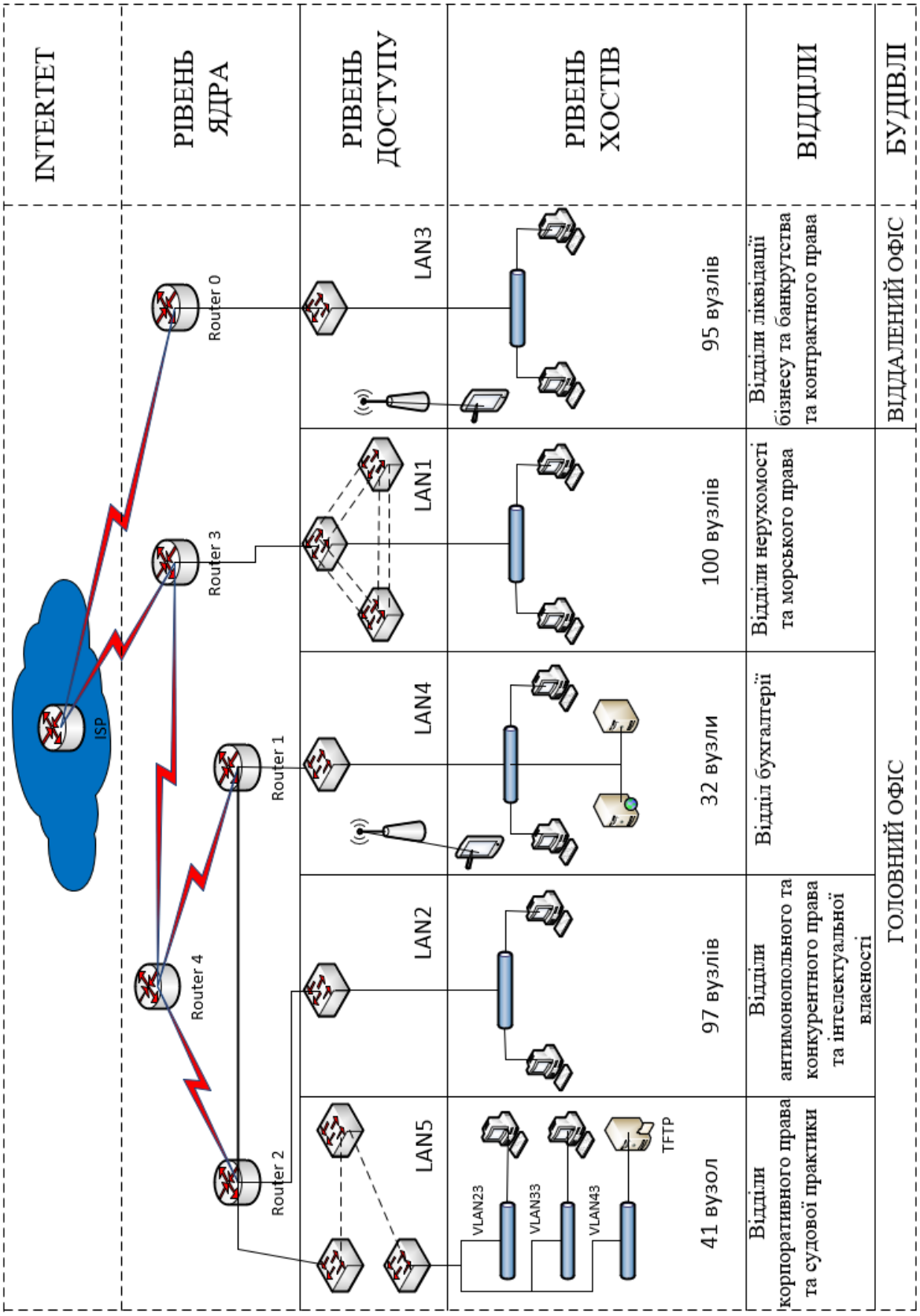

Рисунок 2.2 - Структурна схема комплексу технічних засобів комп’ютерної системи

2.3 Розробка специфікації апаратних засобів комп’ютерної системи

У якості комутаційного обладнання для побудови мережі обрано комутатори серії Cisco WS-C2960-24TT-L. Комутатори серії WS-C2960-24TT-L забезпечують високу швидкість передачі даних по мережі, що робить їх ідеальними для використання в швидкісних корпоративних мережах. Завдяки підтримці швидкості передачі даних 10/100 Мбіт/с, ці комутатори здатні ефективно обробляти великі обсяги трафіку. омутатори Cisco WS-C2960-24TT-L мають широкий набір функцій і можливостей. Вони підтримують важливі мережеві протоколи, такі як VLAN, QoS (Quality of Service), STP (Spanning Tree Protocol) і ACL (Access Control Lists), що дозволяє налаштовувати та керувати трафіком в мережі. омутатори серії WS-C2960-24TT-L мають високу надійність і відмовостійкість. Вони підтримують функції, такі як Spanning Tree Protocol (STP), які забезпечують резервування шляхів і виявлення петель у мережі, що дозволяє уникнути переривань в роботі мережі. Крім того, вони мають вбудований механізм захисту від перенавантаження портів, що допомагає запобігти втраті пакетів і забезпечує стабільну роботу мережі.

У якості маршрутизаторів для мережі обрано Cisco 2911/K9. Cisco 2911/K9 пропонує швидкісну обробку даних та широку пропускну здатність. Вони оснащені потужним процесором та пам'яттю, що дозволяє їм обробляти великі обсяги даних та забезпечувати швидку передачу інформації. Маршрутизатори серії Cisco 2911/K9 мають модульну архітектуру, яка дозволяє легко розширювати їх функціональність. Завдяки наявності слотів для додаткових модулів можна додатково розширити можливості маршрутизатора, додавши нові порти або функціональні можливості. Cisco 2911/K9 пропонує широкий спектр функцій безпеки, що дозволяє захищати мережу від різних загроз. Вони підтримують шифрування даних, віртуальні приватні мережі (VPN), файрвол та системи виявлення вторгнень (IDS/IPS). Це дозволяє забезпечити конфіденційність, цілісність та доступність даних, що передаються через мережу.

Маршрутизатори серії Cisco 2911/K9 підтримують широкий спектр мережевих протоколів, таких як IP, IPv6, MPLS та BGP. Це робить їх гнучкими і спроможними працювати в різних мережевих середовищах із різними вимогами.

У якості серверного обладнання було обрано сервери Cisco UCS C240 M4 24 SFF 2U. Cisco UCS C240 M4 24 SFF 2U оснащені потужними процесорами і розширюваною оперативною пам'яттю, що дозволяє забезпечити високу продуктивність обчислювальних завдань. Вони здатні обробляти великі обсяги даних і запускати вимогливі додатки з високою швидкістю. Дані сервери забезпечують високий рівень надійності та доступності. Вони підтримують резервування жорстких дисків, дозволяючи забезпечити безперебійну роботу при випадку відмови диска. Крім того, сервери Cisco UCS використовують технологію віртуалізації, що дозволяє розподіляти завантаження і резервувати ресурси, забезпечуючи високу доступність додатків.

Для зв’язку між IoT пристроями обрано бездротовий маршрутизатор Cisco RV130. Він підтримує бездротовий стандарт 802.11n, що дозволяє досягати швидкості передачі даних до 300 Мбіт/с. RV130 має функціональні можливості для керування мережевим трафіком, які дозволяють обробляти велику кількість одночасних підключень. Він підтримує різні функції безпеки, такі як брандмауер, VPN-підтримка (Virtual Private Network), контроль доступу та інші заходи безпеки мережі.

Специфікація обраного для мережі компанії обладнання та його характеристики наведені у таблиці 2.1.

Таблиця 2.1 – Специфікація обладнання для мережі компанії «Avaris»

Позиція	Найменування і технічна характеристика	Тим, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1	Комутатор Cisco WS-C2960 24 x Fast Ethernet Network, 2 x Gigabit Ethernet Uplink; 64 MB DRAM; 32 MB flash memory; Ethernet: IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z.	Cisco WS-C2960-24TT-L	од	22	Підтримка технологій: Intelligent features, QoS, Link Aggregation, Port Security; Вхідна напруга: 110 V AC/220 V AC;
2	Маршрутизатор Cisco 2911 3 вбудовані GE, 4 EHWIC, 2 DSP, 1 ISM, 256 МБ CF, 512 МБ DRAM; Максимальна пропускна здатність до 180 Мбіт/с.	Cisco 2911/K9	од	5	Підтримка мережевих протоколів: IPv4, IPv6, OSPF, BGP, EIGRP, RIP, IS-IS; Вхідна напруга: 110 V AC/220 V AC;
3	Сервер Cisco UCS C240 Intel Xeon E5 v3/v4; DDR4 RDIMM; Cisco UCSC-MRAID12G.	Cisco UCS C240 M4 24 SFF 2U	од	3	Форм-фактор 2U та може вмістити до 24 жорстких дисків формату SFF. Підтримує до 1536 ГБ оперативної пам'яті DDR4 з розширенням до 24 слотів DIMM.

Продовження таблиці 2.1

Позиція	Найменування і технічна характеристика	Тим, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
4	Бездротовий маршрутизатор Cisco RV130 4 Ethernet 10/100/1000 Mbps (LAN); 1 Ethernet 10/100/1000 Mbps (WAN); IEEE 802.11b/g/n; 300 Мбіт/с.	Cisco RV130W-E	од	2	Підтримка WEP, WPA, WPA2 для безпеки мережі Wi-Fi; Веб-інтерфейс для керування маршрутизатором; Підтримка віртуальних приватних мереж (VLANs): до 16 VLAN.

Далі розглянемо специфікацію кабельної структури на прикладі частини віддаленого офісу компанії (рисунок 2.3).

Усі кабель-канали розміщуються на стінах. ПК під’єднуються до мережі через мережеві розетки RJ-45. Ethernet кабелі було обрано кручену пару UTP, так як немає необхідності в екранованій крученій парі.

Специфікацію мережевого обладнання віддаленого офісу компанії наведено у таблиці 2.2.

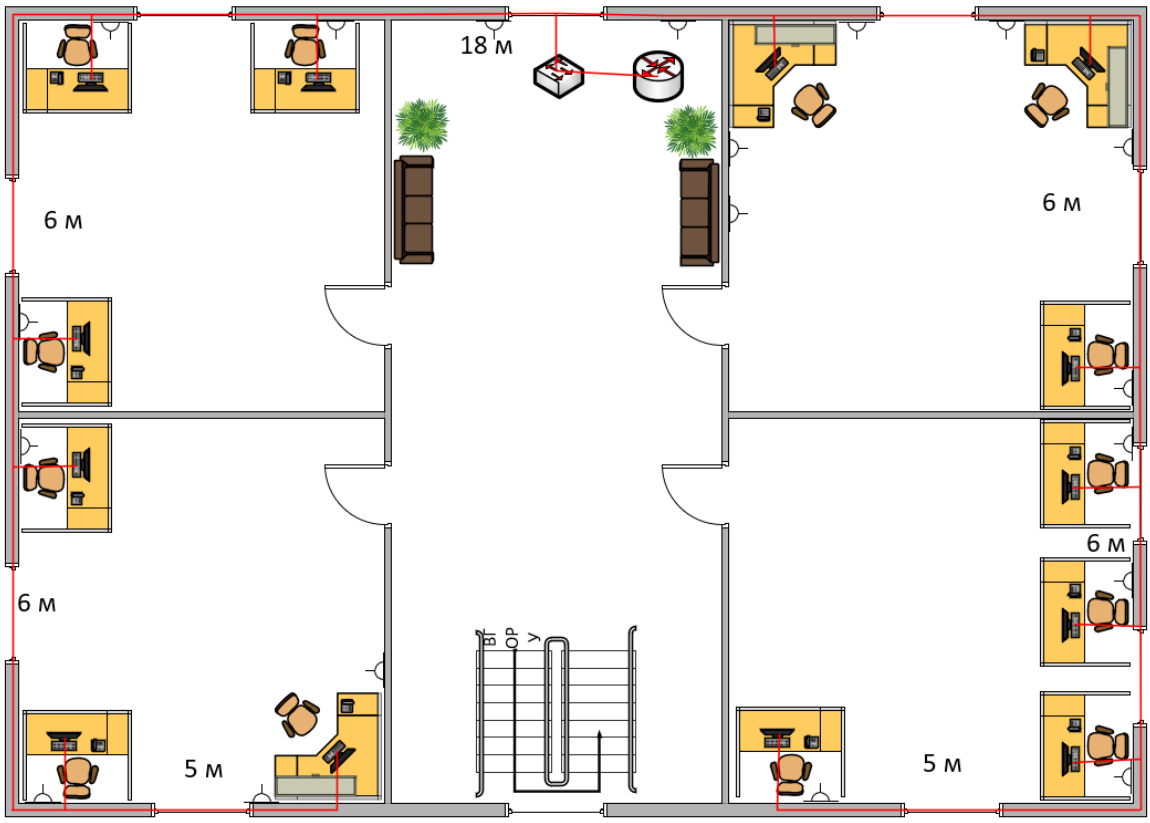

Рисунок 2.3 -Кабельна структура частини віддаленого офісу компанії

Таблиця 2.2 – Специфікація обладнання віддаленого офісу компанії

Позиція	Найменування і технічна характеристика	Тим, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
4	Комутатор Cisco WS-C2960 24 x Fast Ethernet Network, 2 x Gigabit Ethernet Uplink; 64 MB DRAM; 32 MB flash memory; Ethernet: IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z.	Cisco WS-C2960-24TT-L	од	5	Підтримка технологій: Intelligent features, QoS, Link Aggregation, Port Security; Вхідна напруга: 110 V AC/220 V AC;

Продовження таблиці 2.2

Позиція	Найменування і технічна характеристика	Тим, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
2	Маршрутизатор Cisco 2901 2 вбудовані GE, 4 EHWIC, 2 DSP, 1 ISM, 256 МБ CF, 512 МБ DRAM; Максимальна пропускна здатність до 180 Мбіт/с.	Cisco 2901/K9	од	1	Підтримка мережевих протоколів: IPv4, IPv6, OSPF, BGP, EIGRP, RIP, IS-IS; Вхідна напруга: 110 V AC/220 V AC;
4	Бездротовий маршрутизатор Cisco RV130 4 Ethernet 10/100/1000 Mbps (LAN); 1 Ethernet 10/100/1000 Mbps (WAN); IEEE 802.11b/g/n; 300 Мбіт/с.	Cisco RV130W-E	од	1	Підтримка WEP, WPA, WPA2 для безпеки мережі Wi-Fi; Веб-інтерфейс для керування маршрутизатором; Підтримка віртуальних приватних мереж (VLANs): до 16 VLAN.

Результати розробки специфікації кабельної структури частини віддаленого офісу компанії наведено у таблиці 2.2.

Таблиця 2.3 – Специфікація кабельної структури

Позиція	Найменування і технічна характеристика	Тим, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1	Кабельний канал 30х25 мм	Kopos	м	52	Матеріал: полівінілхлорид (ПВХ); Ступінь захисту IP40,
2	Розетка комп’ютерна подвійна RJ-45 5E	Aling-Conel Eon	од	25	Матеріал: ABS-пластик та полікарбонат. Ступінь захисту IP20.
3	Розетка подвійна із заземленням	Makel Siva Ustu	од	45	Матеріал: ABS-пластик; Ступінь захисту IP20.
4	Патч-корд RJ45 5E LAN кабель	HLV	м	85	Структура 4х2 AWG 26/7.
5	Кабель силовий мідний ПВС 3х1.5	ЗЗКМ	м	105	Матеріал зовнішньої оболонки: ПВХ пластикат; Максимальна напруга, В: 660.

2.2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Найбільша підмережа – LAN1. Вона складається з 100 ПК. Пропускна здатність лінії, в яку маршрутизується трафік – 1000 Мбіт/с.

Для стабільної роботи маршрутизатора необхідно, щоб швидкість відправлення пакетів була більшою, за швидкість надходження. Тобто, навантаження не повинно бути більше, ніж:

$$\mu_{вих} = \frac{1000000000}{650 \times 8} = 192\ 300 \text{ пакетів/с} \quad (2.1)$$

В середньому кожне джерело виробляє 50 пакетів на секунду. Виходячи з цього, максимальна кількість пристроїв, які можуть бути під'єднані до маршрутизатора розраховується наступним чином:

$$N = \frac{192300}{50} = 3846 \text{ пристроїв} \quad (2.2)$$

Це підходить для підмережі на 100 ПК та залишає можливості для масштабування.

Кожен зі 100 ПК надсилає потік з інтенсивністю 50 кадрів/с.

Виходячи з цього, інтенсивність вихідного трафіку дорівнюватиме:

$$\lambda = 100 * 50 = 5\ 000 \text{ пакетів/с} \quad (2.3)$$

Коефіцієнт затримки розраховується наступним чином:

$$\rho = \frac{\lambda}{\mu_{вих}} = 5000/192300 = 0.02 \quad (2.4)$$

Коефіцієнт зайнятості маршрутизатора розраховується наступним чином:

$$\frac{\rho}{1-\rho} = \frac{0.02}{1-0.02} = 0.02 \quad (2.5)$$

Середня затримка кадру, пов'язана з чергою M/M/1, дорівнює:

$$T = \frac{1}{\mu - \lambda} = \frac{1}{192300-5000} = 5.3 \text{ мкс} \quad (2.6)$$

Середня довжина черги дорівнює:

$$L_{чер}=\frac{\rho^2}{1-\rho}=\frac{0.02^2}{1-0.02}=0.0004 \quad (2.7)$$

Середній час перебування пакета в черзі дорівнює:

$$T_{очікування}=\frac{L_{чер}}{\lambda}=\frac{0.0004}{5000}=80 \text{ нс} \quad (2.8)$$

Пропускну здатність каналу виведемо з наступної формули:

$$\lambda=\frac{\text{пропускна здатність}}{\text{довжина кадру}}=\frac{b}{l} \quad (2.9)$$

Звідси отримуємо:

$$b=\lambda\times l=5000\times 650\times 8=26000000 \text{ біт/с} =26 \text{ Мбіт/с} \quad (2.10)$$

Це повністю задовольняє пропускну здатність нашого вихідного каналу в 1000 Мбіт/с.

3 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРАХУНОК ЇЇ НАЛАШТУВАНЬ

3.1 Розрахунок адресації мережі

В таблиці 3.1 наведено блок адрес, який буде використовуватися для розрахунку адресації в підмережах компанії. Також наведено кількість ПК в кожній підмережі.

Таблиця 3.1 – Виділений блок адрес

№	Блок адрес	LAN1	LAN2	LAN3	LAN4	LAN5
13	10.23.64.0/22	100	97	95	32	41

У таблиці 3.2 наведено відділи компанії та LAN, які їм відповідають.

Таблиця 3.2 – Розподілення відділів мережі між LAN

Номер LAN	Назва відділу
LAN1	Відділи нерухомості та морського права
LAN2	Відділи антимонопольного та конкурентного права та інтелектуальної власності
LAN3	Відділи ліквідації бізнесу та банкрутства та контрактного права
LAN4	Відділ бухгалтерії
LAN5	Відділи корпоративного права та судової практики

Розрахунок адресації виконується за методом VLSM (Variable Length Subnet Masking), так як даний метод забезпечує найбільш ефективне використання простору адрес. Даний метод дозволяє розраховувати підмережі розміром, який відповідає ступеню двійки. Під час розрахунку варто враховувати адресу мережі та широкомовну адресу, тому кількість доступних адрес завжди менша на 2. Таким чином кількість адрес у підмережі визначається за формулою $2^n - 2$, де n – кількість біт, виділених для підмережі. Розрахунок підмереж необхідно проводити від найбільшої до найменшої.

Найбільша підмережа – LAN1, має 100 ПК. Для неї виділимо $2^7 - 2 = 126$ адрес. Так як ми використовуємо 7 біт для хостової частини адреси, то маска підмережі буде /25. Відділимо з правого боку 7 біт, які утворюють хостову частину, решта бітів будуть мережевою частиною.

10.23.01000000.0|0000000

Виходячи з цього отримуємо адресу підмережі – 10.23.64.0/25.

Заповнимо хостову частину одиницями та таким чином отримаємо широкомовну адресу підмережі – 10.23.64.127/25.

10.23.01000000.0|1111111

Діапазон доступних для пристроїв адрес: 10.23.64.1 – 10.23.64.126.

Наступна за розміром підмережа – LAN2 з 97 ПК. Для неї також виділимо $2^7 - 2 = 126$ адрес. Для розрахунку збільшимо значення мережевої частини на 1 біт. Звідси маємо адресу мережі: 10.23.01000000.1|0000000 – 10.23.64.128/25. Широкомовну адресу: 10.23.01000000.1|1111111 – 10.23.64.255. Та діапазон доступних для пристроїв адрес: 10.23.64.129 – 10.23.64.254.

Наступна за розміром підмережа – LAN3 з 95 ПК. Аналогічно виділяємо $2^7 - 2 = 126$ адрес та знову збільшуємо значення мережевої частини на 1 біт. Отримуємо адресу мережі: 10.23.01000001.0|0000000 – 10.23.65.0/25. Широкомовну адресу: 10.23.01000001.0|1111111 - 10.23.65.127. Та діапазон доступних для пристроїв адрес: 10.23.65.1 – 10.23.65.126.

Наступна за розміром підмережа – LAN5 з 41 ПК. Мінімальна кількість адрес, необхідних для даної підмережі - $2^6 - 2 = 62$ адрес. Але, так як дана підмережа в майбутньому буде розбиватися на підмережі VLAN, виділимо для неї блок в $2^7 - 2 = 126$ адрес. Знову збільшуємо значення мережевої частини на 1 біт. Отримуємо адресу мережі: 10.23.01000001.1|0000000 – 10.23.65.128/25. Широкомовну адресу: 10.23.01000001.1|1111111 – 10.23.65.255. Та діапазон доступних для пристроїв адрес: 10.23.65.129 – 10.23.65.254.

Остання за розміром підмережа – LAN4 з 32 ПК. Виділимо для неї $2^6 - 2 = 62$ адрес. Так як для хостової частини виділено усього 6 біт, маска підмережі буде /26. Збільшимо значення мережевої частини на 1 біт. Отримаємо адресу мережі:
10.23.01000010.00|000000 – 10.23.66.0/26. Широкомовну адресу: 10.23.01000010.00|111111 – 10.23.66.63. Та діапазон доступних для пристроїв адрес: 10.23.66.1 – 10.23.66.62.

Схема розрахованої адресації для мережі компанії представлена у таблиці 3.3.

Таблиця 3.3 – Схема адресації мережі

Назва мережі	Кількість вузлів	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
LAN1	100	126	10.23.64.0	/25	10.23.64.1 - 10.23.64.126	10.23.64.127
LAN2	97	126	10.23.64.128	/25	10.23.64.129 - 10.23.64.254	10.23.64.255
LAN3	95	126	10.23.65.0	/25	10.23.65.1 - 10.23.65.126	10.23.65.127
LAN4	32	62	10.23.66.0	/26	10.23.66.1 - 10.23.66.62	10.23.66.63
LAN5	41	126	10.23.65.128	/25	10.23.65.129 - 10.23.65.254	10.23.65.255

Для розрахунку підмереж для каналів між маршрутизаторами використовується блок адрес 10.1.13.0/24. Після аналогічних розрахунків за методом VLSM отримуємо таблицю 3.4 з відповідною схемою адресації.

Таблиця 3.4 – Схема адресації каналів між маршрутизаторами

Підмережа	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
WAN1	2	2	10.1.13.0	/30	10.1.13.1 - 10.1.13.2	10.1.13.3
WAN2	2	2	10.1.13.4	/30	10.1.13.5 - 10.1.13.6	10.1.13.7
WAN3	2	2	10.1.13.8	/30	10.1.13.9 - 10.1.13.10	10.1.13.11
WAN4	2	2	10.1.13.12	/30	10.1.13.13 - 10.1.13.14	10.1.13.15

3.2 Розрахунок адресації пристроїв

У таблиці 3.5 наведено адресацію всіх маршрутизаторів у мережі.

Таблиця 3.5 – Схема адресації маршрутизаторів

Пристрій	Інтерфейс	IP-адреса	Маска
Tymchenko_Router_0	Gig0/0	64.100.13.2	255.255.255.252
	Gig0/1	10.23.65.1	255.255.255.128
Tymchenko_Router_1	Gig0/0	10.23.66.1	255.255.255.192
	Gig0/1	10.1.13.13	255.255.255.252
	Se0/3/1	10.1.13.6	255.255.255.252
Tymchenko_Router_2	Gig0/1	10.1.13.14	255.255.255.252
	Se0/3/1	10.1.13.10	255.255.255.252
	Gig0/0.23	10.23.65.129	255.255.255.224
	Gig0/0.33	10.23.65.161	255.255.255.224
	Gig0/0.43	10.23.65.193	255.255.255.224
	Gig0/0.99	10.23.65.225	255.255.255.240
Tymchenko_Router_3	Gig0/0	10.23.64.1	255.255.255.128
	Se0/3/0	10.1.13.1	255.255.255.252
	Se0/3/1	209.165.202.2	255.255.255.252
Tymchenko_Router_4	Gig0/0	10.23.64.129	255.255.255.128
	Se0/2/0	10.1.13.9	255.255.255.252
	Se0/3/0	10.1.13.2	255.255.255.252
	Se0/3/1	10.1.13.5	255.255.255.252

Продовження таблиці 3.5

Пристрій	Інтерфейс	IP-адреса	Маска
Tymchenko_Router_ISP	Gig0/0	64.100.13.1	255.255.255.252
	Gig0/1	209.165.201.1	255.255.255.240
	Se0/3/0	209.165.202.1	255.255.255.252

У таблиці 3.6 наведено адресацію SVI-інтерфейсів комутаторів у підмережах.

Таблиця 3.6 – IP-адреси комутаторів у підмережах

Підмережа	Пристрій	IP-адреса SVI інтерфейсу	Маска підмережі	Адреса шлюзу
LAN1	Tymchenko_Switch_6	10.23.64.2	255.255.255.128	10.23.64.1
	Tymchenko_Switch_7	10.23.64.3	255.255.255.128	10.23.64.1
	Tymchenko_Switch_8	10.23.64.4	255.255.255.128	10.23.64.1
LAN2	Tymchenko_Switch_4	10.23.64.130	255.255.255.128	10.23.64.129
LAN3	Tymchenko_Switch_0	10.23.65.2	255.255.255.128	10.23.65.1
LAN4	Tymchenko_Switch_5	10.23.66.2	255.255.255.192	10.23.66.1
LAN5	Tymchenko_Switch_1	10.23.65.226	255.255.255.240	10.23.65.225
	Tymchenko_Switch_2	10.23.65.227	255.255.255.240	10.23.65.225
	Tymchenko_Switch_3	10.23.65.228	255.255.255.240	10.23.65.225

3.3 Налаштування моделі комп’ютерної системи

На рисунку 3.1 зображено логічну топологію корпоративної мережі компанії.

На топології зображено підмережі LAN1 – LAN5 та канали між ними. При проектуванні кабельних з’єднань для зв’язку підмереж було обрано інтерфейси SerialEthernet та GigabitEthernet. Для з’єднання пристроїв з комутаторами використовується стандартний FastEthernet.

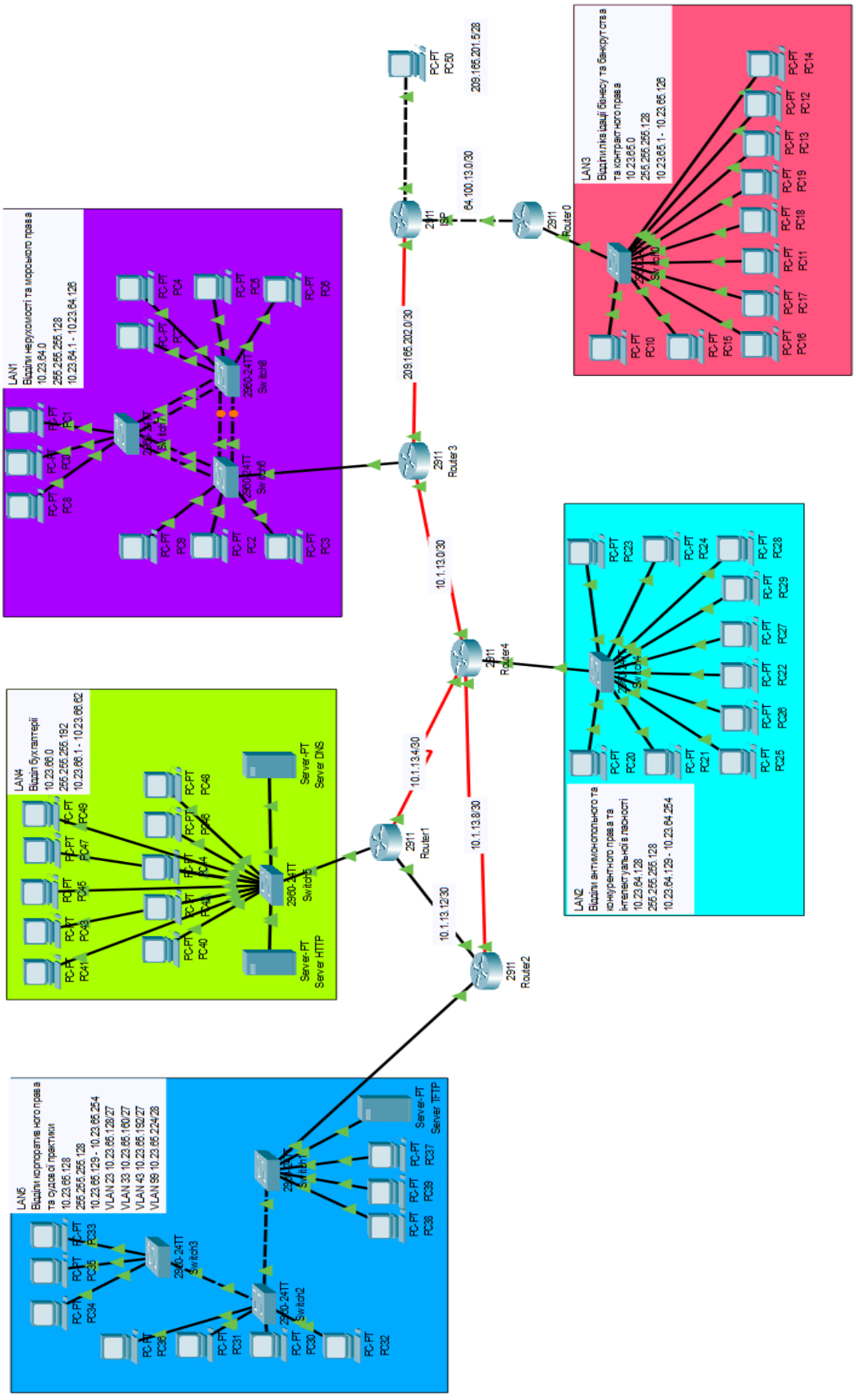

Рисунок 3.1 – Логічна топологія мережі

3.4 Налаштування та перевірка роботи комп’ютерної системи

3.4.1 Базове налаштування конфігурації пристроїв

На кожному мережевому пристрої необхідно виконати базове налаштування, до якого входить: призначення назви пристрою, встановлення паролів до ліній console та vty, призначення паролю до привілейованого режиму, налаштування шифрування усіх паролів, встановлення банеру MOTD, призначення використання протоколу ssh на лініях console та vty, створення користувача, доменного імені, ключа RSA довжиною 1024 біт. Нижче наведено приклад налаштування маршрутизатора Tymchenko_Router 0.

Використання захищеного протоколу SSH замість відкритого Telnet дозволить значно підвищити безпеку даних у мережі. Встановлення аутентифікації на мережевих пристроях забезпечить їм захист від несанкціонованого доступу.

```
enable
Conf t //режим конфігурації
Hostname Tymchenko_Router_0 //призначення назви пристрою
Line console 0
Password cisco //встановлення паролю до лінії console
Login
Line vty 0 15
Password cisco // встановлення паролю до ліній vty
Login
Enable secret class //встановлення паролю до привілейованого режиму
Service password-encryption //шифрування паролів
Banner motd ‘Tymchenko_Router_0’ //створення Banner MOTD
ip domain-name Tymchenko_Router_0 //створення доменного імені
```

```
Crypto key generate rsa //налаштування використання протоколу ssh на лініях vty
1024
Username 123191_Tymchenko password admincisco
Line vty 0 15
Transport input ssh
Login local
```

Для того, щоб збільшити пропускну здатність у мережі LAN1, необхідно виконати об’єднання фізичних ліній комутаторів. Це реалізовується за допомогою технології EtherChannel та дозволяє значно підвищити стабільність з’єднань у мережі та збільшити пропускну спроможність у даній підмережі. Нижче наведено приклад налаштування комутатора Tymchenko_Switch_6.

```
interface range fa0/1-2 //вибір діапазону портів
channel-group 1 mode active //об’єднання портів у групу
interface port-channel 1 //вибір об’єднаного інтерфейсу
switchport mode trunk //увімкнення режиму trunk
switchport trunk allowed vlan all ///дозвіл усім VLAN на передачу трафіку
interface range fa0/3-4
channel-group 2 mode active
interface port-channel 2
switchport mode trunk
switchport trunk allowed vlan all
```

Як бачимо на рисунку 3.2, агрегація каналів налаштована правильно та працює.

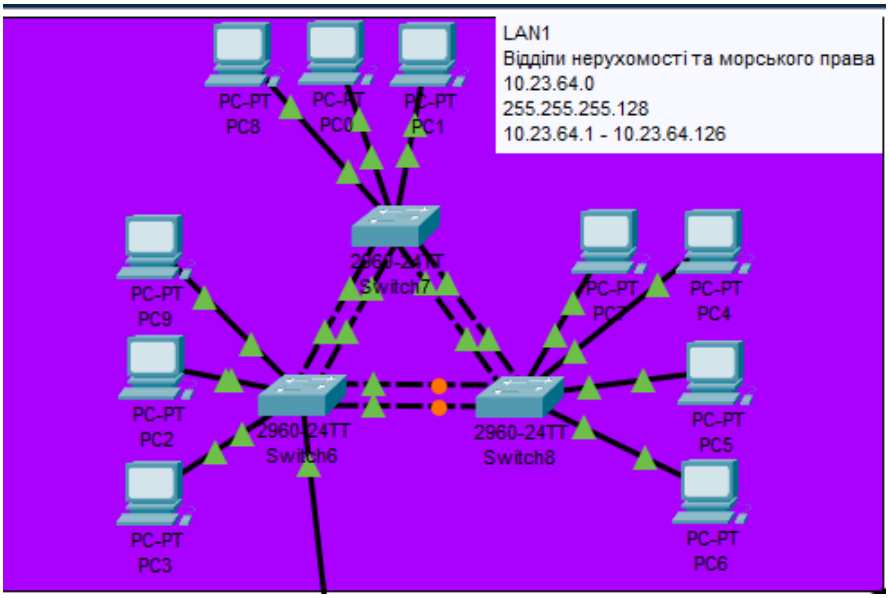

Рисунок 3.2 – Агрегація каналів комутаторів

3.4.2 Налаштування маршрутизаторів

Для забезпечення зв’язку між підмережами необхідно виконати налаштування маршрутизації у мережі. Для мережі компанії обрано протокол динамічної маршрутизації OSPF, завдяки якому маршрутизатори будуть автоматично сповіщати сусідів про мережі з їхньої таблиці маршрутизації. Даний протокол чудово працює у великих мережах, підтримує різні типи мереж, швидко адаптується до змін в мережі та підтримує велику кількість пристроїв, що робить його хорошим вибором для мережі компанії.

Під час налаштування протоколу OSPF необхідно вимкнути поширення оновлень маршрутизації на інтерфейси локальних мереж та налаштувати розповсюдження мереж, які під’єднанні безпосередньо до маршрутизатора.

Нижче наведено приклад налаштування протоколу OSPF на маршрутизаторі Tymchenko_Router_1.

```
router ospf 1 //увімкнення протоколу OSPF
passive-interface GigabitEthernet0/0 //налаштування пасивного інтерфейсу
 network 10.23.66.0 0.0.0.63 area 0 //оголошення мережі
 network 10.1.13.12 0.0.0.3 area 0
 network 10.1.13.4 0.0.0.3 area 0
```

На маршрутизаторі, який під’єднано безпосередньо до маршрутизатору провайдера (Tymchenko_Router_3), необхідно налаштувати статичний маршрут за замовчуванням до мережі провайдера, вказавши у якості наступного переходу адресу інтерфейсу Se0/3/0 маршрутизатора ISP.

```
ip route 0.0.0.0 0.0.0.0 209.165.202.1 //створення статичного маршруту
```

Також додаємо ще один статичний маршрут таким чином, щоб забезпечити доступ з локальної мережі до мережі ISP.

```
ip route 209.165.201.0 255.255.255.240 209.165.202.1 //створення статичного маршруту
```

На інтерфейсах SerialEthernet встановимо пропускну спроможність та тактову частоту.

```
interface Serial0/3/1
bandwidth 128 //налаштування пропускної спроможності
clock rate 128000 //налштування частоти
```

Необхідно налаштувати службу AAA на всіх маршрутизаторах мережі. Дана служба дозволяє перевіряти ідентичність користувачів шляхом аутентифікації перед тим, як надати їм доступ до мережевого обладнання. Дана служба забезпечує потужний захист від несанкціонованого доступу у мережі. Для налаштування потрібно увімкнути службу, вказати адресу AAA Radius серверу, призначити аутентифікацію для доступу до консолі за допомогою Radius протоколу (в разі відсутності зв’язку використовується локальна база даних), для перевірки підключень до лінії VTY необхідно створити локальну базу користувачів.

Приклад налаштування служби AAA на маршрутизаторі наведено нижче.

```
aaa new-model //створення нової aaa-моделі
radius-server host 10.23.66.23 auth-port 1645 key radius123 //призначення адреси Radius-сервера
```

```
aaa authentication login CONSOLE group radius local //налаштування аутентифікації до консолі
line console 0
login authentication CONSOLE
aaa authentication login default local //створення локальної бази даних користувачів
username Tymchenko_Router_1 password admin123 //створення користувача
line vty 0 15
login authentication default
```

Також необхідно налаштувати службу AAA безпосередньо на сервері. Для цього використаємо DNS-сервер компанії задля збереження коштів. Налаштування серверу зображено на рисунку 3.4.

Перевірку роботи аутентифікації через службу AAA наведено на рисунку 3.3.

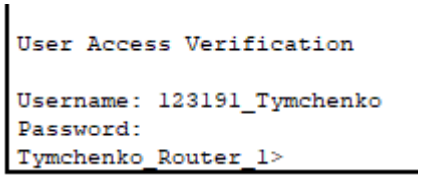

Рисунок 3.3 – Аутентифікація за допомогою служби AAA

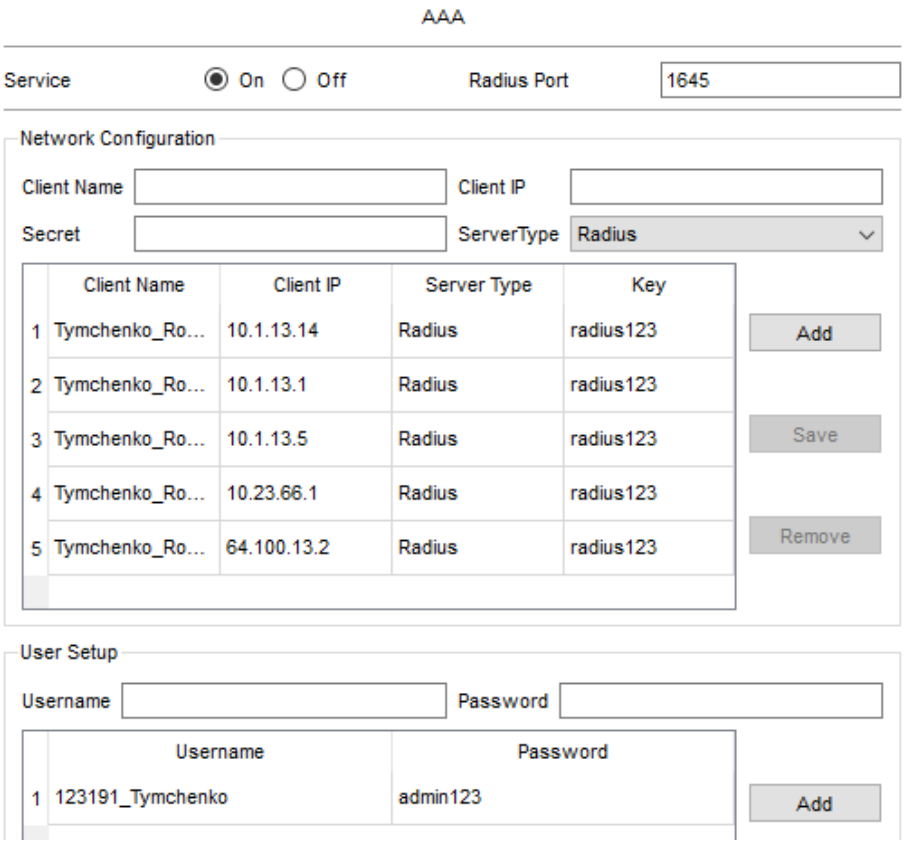

Рисунок 3.4 – Налаштування AAA сервісу

3.4.3 Налаштування роботи Інтернет

Для того, щоб налаштувати роботу Інтернет, необхідно налаштувати на пограничному маршрутизаторі мережі динамічну трансляцію NAT. Пул адрес, який використовується для трансляції: 209.165.200.5 по 209.165.200.30.

Для забезпечення роботи динамічного NAT необхідно створити ACL-список, в якому дозволимо проходження трафіку з локальних підмереж. Також у даному ACL-списку заборонимо проходження трафіку з локальних мереж до віддаленої мережі компанії, так як у майбутньому даний трафік буде проходити через захищений VPN-канал. ACL-список та налаштування NAT наведено нижче.

```
ip access-list extended NAT13 //створення списку
deny ip 10.23.64.0 0.0.0.127 10.23.65.0 0.0.0.127
//блокування трафіку з локальної мережі у віддалену
deny ip 10.23.65.128 0.0.0.127 10.23.65.0 0.0.0.127
```

```
deny ip 10.23.64.128 0.0.0.127 10.23.65.0 0.0.0.127
deny ip 10.23.66.0 0.0.0.63 10.23.65.0 0.0.0.127
deny ip 10.1.13.0 0.0.0.3 10.23.65.0 0.0.0.127
permit ip 10.23.66.0 0.0.0.63 any //дозвіл трафіку
permit ip 10.23.64.128 0.0.0.127 any
permit ip 10.1.13.0 0.0.0.255 any
permit ip 10.23.65.128 0.0.0.127 any
permit ip 10.23.64.0 0.0.0.127 any
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask
255.255.255.224 //створення NAT пулу
ip nat inside source list NAT13 pool Internet //увімкнення
трансляції відповідно до ACL-списку
interface Serial0/3/1
ip nat outside //налаштування зовнішнього порту
interface Serial0/3/0
ip nat inside //налаштування внутрішнього порту
```

Для перевірки роботи динамічної трансляції NAT виконаємо надсилання ICMP пакету з мережі головного офісу до ПК провайдера. Як бачимо на рисунку 3.5, пограничний маршрутизатор мережі успішно виконує трансляцію локальної адреси у глобальну.

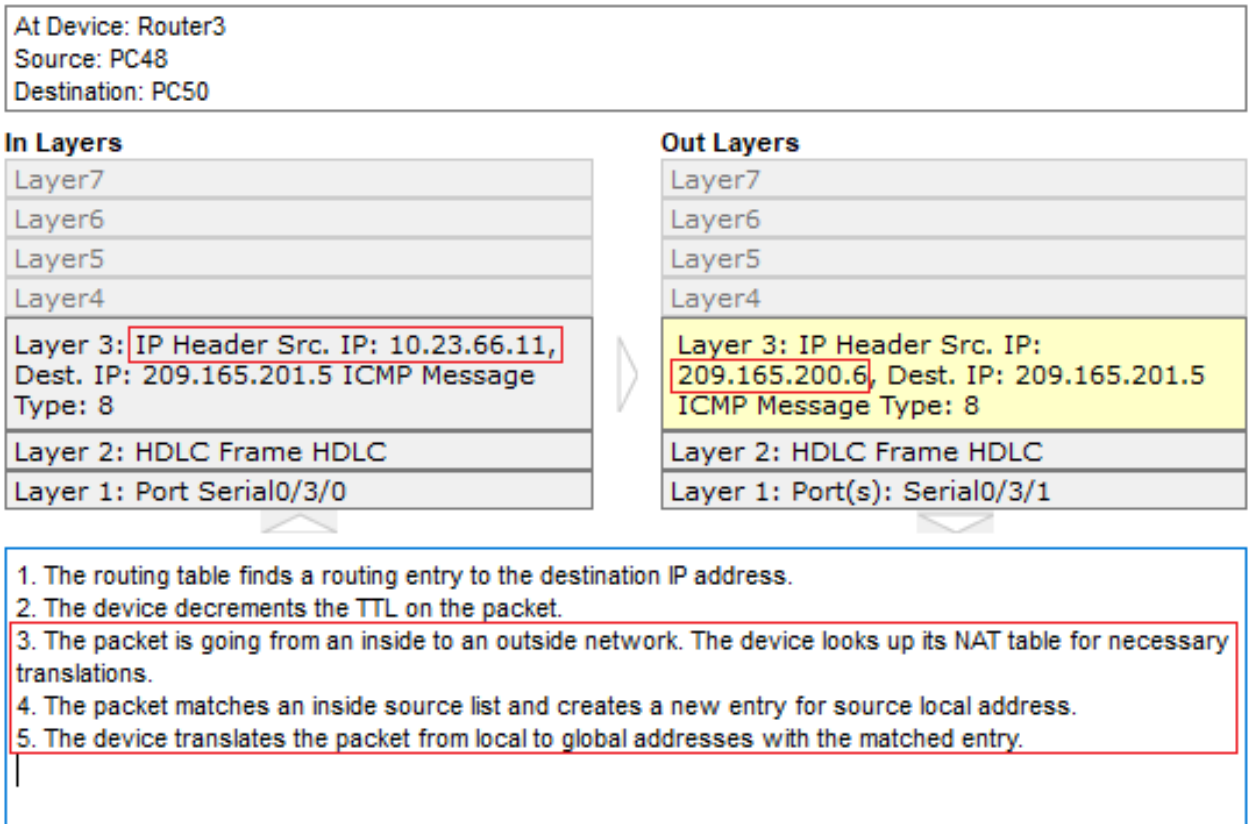

Рисунок 3.5 – Пакет під час трансляції NAT

Далі необхідно налаштувати HTTP-сервер таким чином, щоб щоб на вузлах при вводі в рядку браузера http://123.dnipro.ua (http://209.165.200.4) відкривався веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу.

Для того, щоб це реалізувати, необхідно налаштувати статичну трансляцію на пограничному маршрутизаторі, де локальна адреса сервера буде транслюватися в адресу 209.165.200.4. Після цього на DNS-сервері необхідно створити доменне ім’я 123.dnipro.ua та прив’язати до нього глобальну адресу HTTP-сервера.

Нижче наведено команду для налаштування статичної трансляції.

ip nat inside source static 10.23.66.24 209.165.200.4

Налаштування доменного імені наведено на рисунку 3.6.

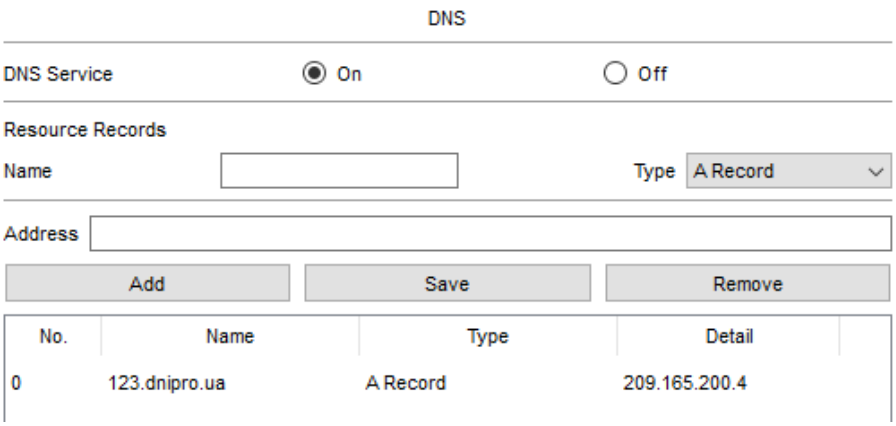

Рисунок 3.6 – Налаштування доменного імені на DNS-сервері

Після всіх налаштувань можна отримати доступ до вебсайту з веб-браузеру комп’ютерів у мережі за доменним ім’ям (рисунок 3.7).

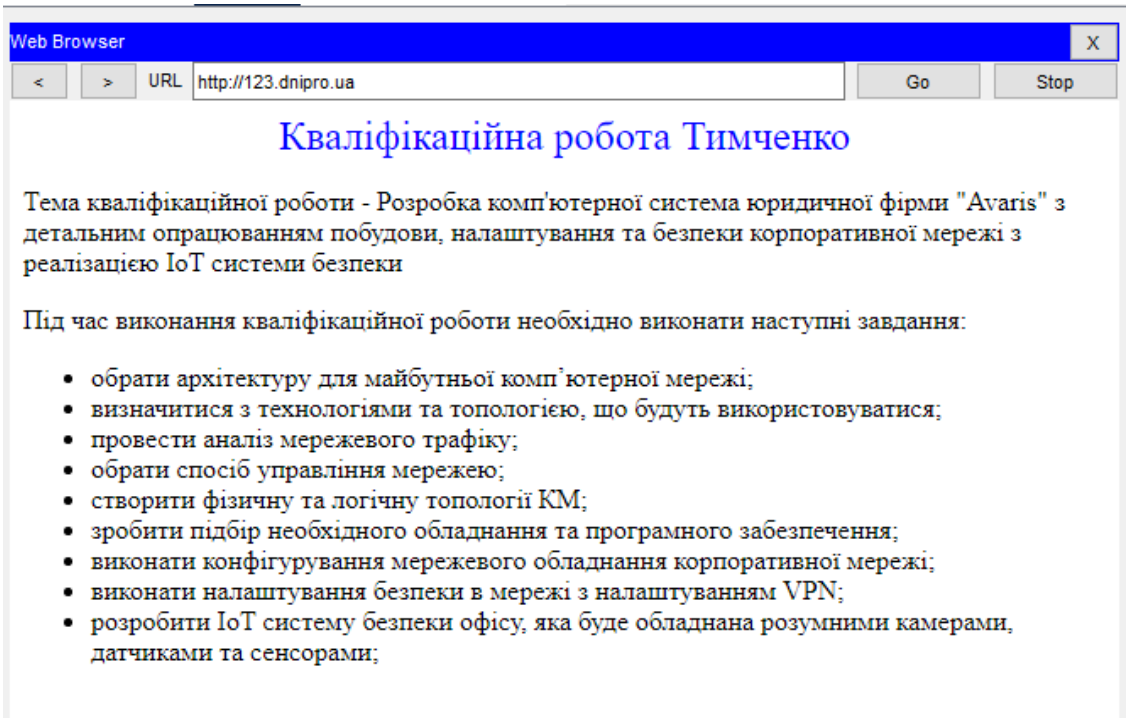

Рисунок 3.7 – Відображення вебсайту в браузері ПК

Для зв’язку між основною та віддаленою мережою необхідно виконати налаштування site-to-site VPN на основі IPsec. Для цього необхідно створити ACL-список, який буде дозволяти проходження відповідного трафіку. Даний ACL-список з маршрутизатора Tymchenko_Router_3 наведено нижче.

```
ip access-list extended VPN13 //створення списку
permit ip 10.23.66.0 0.0.0.63 10.23.65.0 0.0.0.127
//дозвіл трафіку з локальної мережі у віддалену
```

```
permit ip 10.23.64.0 0.0.0.127 10.23.65.0 0.0.0.127
permit ip 10.23.66.0 0.0.0.192 10.23.65.0 0.0.0.127
permit ip 10.23.65.128 0.0.0.127 10.23.65.0 0.0.0.127
permit ip 10.23.64.128 0.0.0.127 10.23.65.0 0.0.0.127
```

Після цього необхідно виконати безпосереднє налаштування VPN.

Спочатку активуємо модуль securityk9:

```
license boot module c2900 technology-package securityk9
```

Після цього на маршрутизаторі створюємо політику ISAKMP 10 та виконуємо її налаштування.

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
```

Далі створюємо ключ cisco та вказуємо адресу зовнішнього інтерфейсу маршрутизатора віддаленої мережі.

```
crypto isakmp key cisco address 64.100.13.2
```

Після цього створюємо набір перетворень з назвою TS.

```
crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

Далі створюємо крипто-зіставлення з назвою MAP та налаштовуємо його.

```
crypto map MAP 10 ipsec-isakmp
 set peer 64.100.13.2
 set transform-set TS
 match address VPN13
```

На зовнішньому інтерфейсі маршрутизатора вмикаємо крипто-зіставлення.

```
interface Serial0/3/1
crypto map MAP
```

Аналогічні налаштування виконуються на маршрутизаторі у віддаленій мережі.

Як бачимо з рисунку 3.8, при відправці пакету з підмережі головного офісу до віддаленого, пограничний маршрутизатор виконує шифрування пакету за протоколом IPsec та пересилає його то маршрутизатора провайдера.

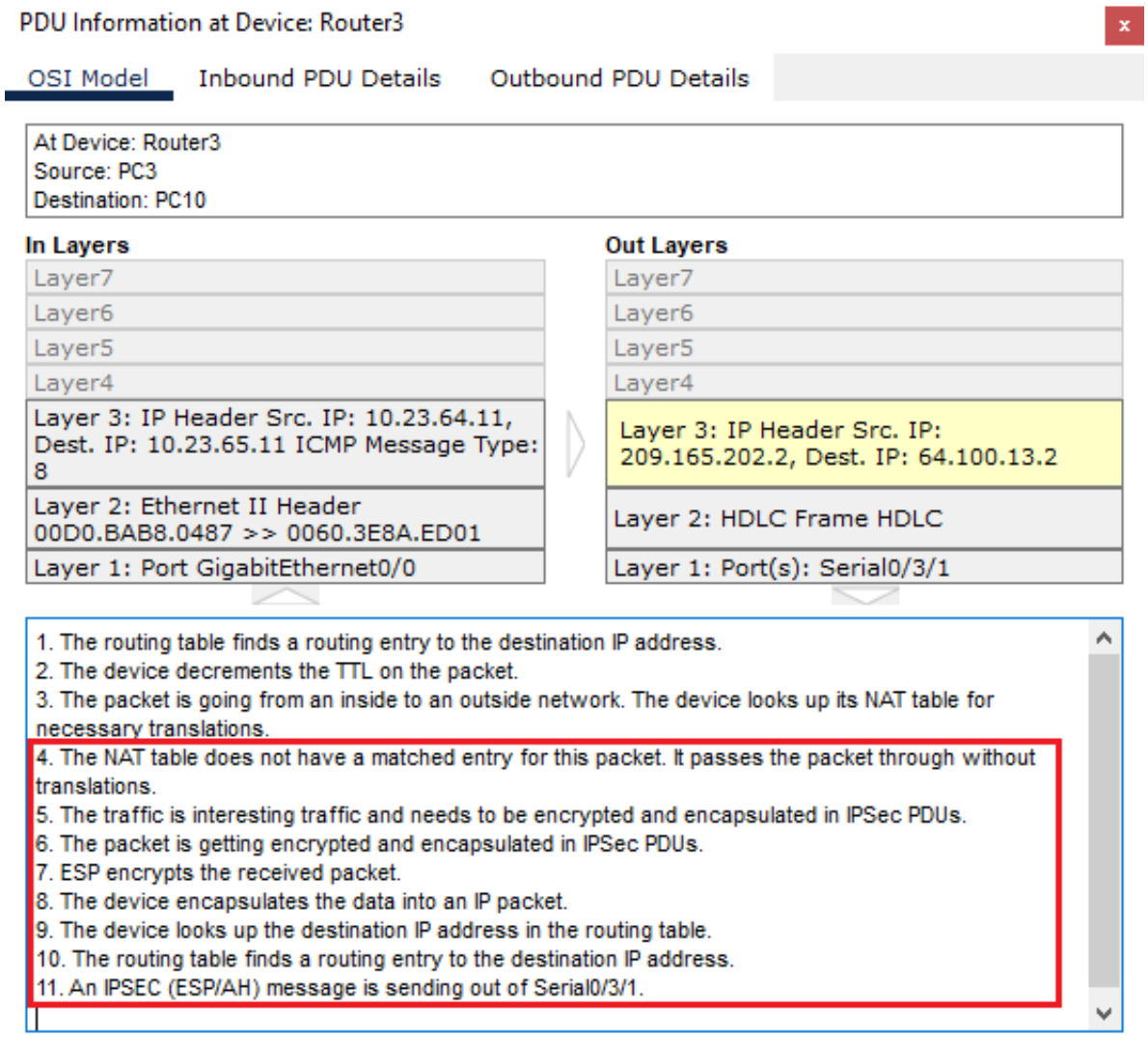

Рисунок 3.8 – Шифрування пакету на пограничному маршрутизаторі

3.5 Захист інформації в комп’ютерній системі від несанкціонованого доступу

3.5.1 Розробка методів для захисту інформації в комп’ютерній системі

Захист інформації в комп'ютерній системі є важливою задачею для забезпечення конфіденційності, цілісності та доступності даних. Нижче наведено методи, які використовуються для захисту інформації в комп'ютерних системах:

1. Аутентифікація: Аутентифікація є процесом перевірки та підтвердження ідентичності користувача або системи. Для забезпечення безпеки інформації необхідно використовувати міцні методи аутентифікації.
2. Шифрування даних: Шифрування забезпечує конфіденційність даних, оскільки зашифровані дані не можуть бути зрозумілими без правильного ключа.
3. Антивірусне програмне забезпечення: Антивірусне програмне забезпечення допомагає захистити комп'ютерну систему від шкідливих атак і запобігає пошкодженню або втраті даних.
4. Фізична безпека: Забезпечення фізичної безпеки комп'ютерної системи включає контроль доступу до приміщення, де розміщені сервери та інші пристрої, які містять важливу інформацію.

3.5.2 Налаштування віртуальних мереж VLAN

У мережі LAN5 необхідно виконати розділення робітників на три робочі групи. Для цього застосуємо технологію віртуальних локальних мереж (VLAN). Використання даної технології забезпечить створення нових підмереж без використання нових маршрутизаторів, це дозволяє суттєво зберегти кошти компанії при купівлі мережевого обладнання.

У таблиці 3.7 вказано номери створених VLAN та їх призначення.

Таблиця 3.7 – Мережі VLAN

Номер VLAN	Ім’я VLAN	Примітка
23	VLAN23	Корпоративне право
33	VLAN33	Судова практика
43	VLAN43	Керівники
1	Default	Не використовується
99	Management	Для керування пристроями
100	Native	Власна

Адресацію віртуальних мереж VLAN наведено у таблиці 3.8.

Таблиця 3.8 – Схема адресації VLAN

Назва підмережі	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
VLAN23	30	30	10.23.65.128	/27	10.23.65.129 – 10.23.65.158	10.23.65.159
VLAN33	30	30	10.23.65.160	/27	10.23.65.161 – 10.23.65.190	10.23.65.191
VLAN43	30	30	10.23.65.192	/27	10.23.65.193 – 10.23.65.222	10.23.65.223
Management	14	14	10.23.65.224	/28	10.23.65.225 - 10.23.65.238	10.23.65.239
Native	6	6	10.23.65.240	/29	10.23.65.241 - 10.23.65.246	10.23.65.247

У таблиці 3.9 наведено розподіл портів комутаторів для мереж VLAN

Таблиця 3.9 – Розподіл портів комутаторів

Назва підмережі	VLAN	Розподіл портів
VLAN23	23	Fa0/6-Fa0/11
VLAN33	33	Fa0/15-Fa0/24
VLAN43	43	Fa0/12-Fa0/14

У таблиці 3.10 наведено адресацію портів пристроїв у мережі LAN5.

Таблиця 3.10 – Адресація портів пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN
Tymchenko_Switch_1	SVI	10.23.65.226	/28	10.23.65.225	99
Tymchenko_Switch_2	SVI	10.23.65.227	/28	10.23.65.225	99
Tymchenko_Switch_3	SVI	10.23.65.228	/28	10.23.65.225	99
Tymchenko_Router_2	G0/0.23	10.23.65.129	/27	-	23
	G0/0.33	10.23.65.161	/27	-	33
	G0/0.43	10.23.65.193	/27	-	43
	G0/0.99	10.23.65.225	/28	-	99

Далі необхідно виконати налаштування VLAN на комутаторах. Нижче наведено приклад налаштування комутатора.

```
int range fa0/6-11 //вибір діапазону портів
switchport mode access //налаштування режиму access
switchport access vlan 23 //призначення VLAN на портах
int range fa0/12-14
switchport mode access
switchport access vlan 43
int range fa0/15-24
```

```
switchport mode access
switchport access vlan 33
int range Gig0/1-2
switchport mode trunk //налаштування режиму trunk
switchport trunk native vlan 100 //призачення native vlan
switchport trunk allowed vlan 46,26,36,99-100
//встановлення VLAN, яким дозволено передавання трафіку
через trunk канали
interface Vlan99 //вибір інтерфейсу SVI
ip address 10.23.65.226 255.255.255.240 //призначення
адреси
ip default-gateway 10.23.65.225 //встановлення шлюзу
```

Переглянути розподілення портів можна за допомогою команди show vlan (рисунок 3.9).

```
Tymchenko_Switch_1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
23   VLAN23                           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11
33   VLAN33                           active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
43   VLAN43                           active    Fa0/12, Fa0/13, Fa0/14
99   Managment                        active
100  Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Рисунок 3.9 – Призначення vlan інтерфейсам комутатора

Нижче наведено налаштування суб-інтерфейсів на маршрутизаторі.

```
interface GigabitEthernet0/0.23 //створення суб-
інтерфейсу
encapsulation dot1Q 23 //увімкнення інкапсуляції
```

```
ip address 10.23.65.129 255.255.255.224 //призначення адреси
interface GigabitEthernet0/0.33
encapsulation dot1Q 33
ip address 10.23.65.161 255.255.255.224
interface GigabitEthernet0/0.43
encapsulation dot1Q 43
ip address 10.23.65.193 255.255.255.224
interface GigabitEthernet0/0.99
encapsulation dot1Q 99
ip address 10.23.65.225 255.255.255.240
```

3.5.3 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

В мережах VLAN адресація пристроїв повинне виконуватися динамічне розподілення адрес за протоколом DHCP. У якості DHCP-серверу налаштуємо маршрутизатор мережі.

Спочатку виключимо з роздачі перші 10 адрес, які використовуються для мережевого обладнання.

```
ip dhcp excluded-address 10.23.65.129 10.23.65.139
ip dhcp excluded-address 10.23.65.161 10.23.65.171
ip dhcp excluded-address 10.23.65.193 10.23.65.203
```

Далі створюємо та налаштовуємо DHCP-пули, з яких вузли будуть динамічно отримувати адреси. В кожному пулі вказуємо шлюз за замовчуванням та адресу DNS-серверу.

```
ip dhcp pool VLAN23 //створення пулу
network 10.23.65.128 255.255.255.224 //призначення мережі
default-router 10.23.65.129 //шлюз за замовчуванням
dns-server 10.23.66.23 //DNS-сервер
```

```
ip dhcp pool VLAN33
 network 10.23.65.160 255.255.255.224
default-router 10.23.65.161
dns-server 10.23.66.23
ip dhcp pool VLAN43
network 10.23.65.192 255.255.255.224
default-router 10.23.65.193
dns-server 10.23.66.23
```

Робота протоколу DHCP показана на рисунку 3.10.

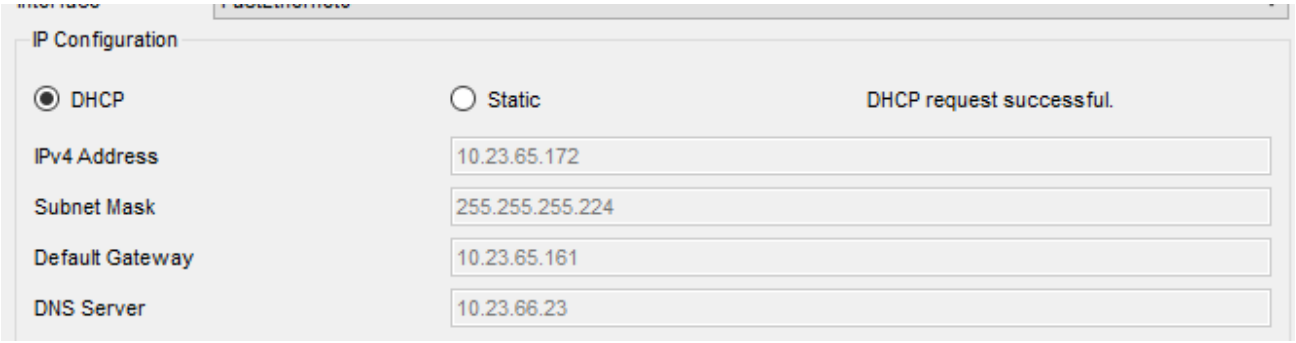

Рисунок 3.10 – Динамічне отримання адреси за протоколом DHCP

На портах комутаторів, до яких під’єднано сервери, необхідно налаштувати функцію безпеки портів. Дозволимо тільки двом унікальним пристроям доступ до порту. MAC-адреса пристрою розпізнаватиметься динамічно і додаватиметься в поточну конфігурацію.

```
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
```

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Інженерне рішення по розробці компонента системи

Інтернет речей (IoT) - це концепція, що описує мережу фізичних пристроїв, обладнаних сенсорами, програмним забезпеченням та здатністю обмінюватися даними через Інтернет. IoT дозволяє автоматизувати рутинні задачі та забезпечує зручність керування пристроями та системами.

За вимогами замовника необхідно впровадити IoT-систему безпеки офісу, яка буде забезпечувати контроль та спостереження за офісними приміщеннями.

Система повинна складатися з наступних пристроїв: камери спостереження, сирени, датчики руху, датчики вогню, та RFID-зчитувачі з картками для дверей.

Система повинна виконувати наступні функції:

1. При спрацюванні датчиків руху повинна вмикатися сирена та камери спостереження;
2. При спрацюванні датчику вогню повинна вмикатися сирена;
3. Відчинення дверей повинно виконуватися за RFID-картками;
4. Сирена вимикається тільки в тому разі, коли всі показники у нормі.

Зв’язок між пристроями повинно бути реалізовано за допомогою HomeGateway. Він же буде виступати у ролі IoT-сервера. Зв’язок пристроїв з шлюзом реалізовується за допомогою стандарту IEEE 802.11 (Wi-Fi), датчики вогню та RFID-зчитувачі під’єднуються за допомогою Ethernet кабелів.

4.2 Налаштування обладнання та сервісів системи IoT

Першим кроком розмістимо обладнання у середовищі Cisco Packet Tracer та під’єднаємо його до HomeGateway. З’єднання виконується з використанням протоколу безпеки WPA2-PSK (Пароль - HomeGateway). Результуючу схему наведено на рисунку 4.1.

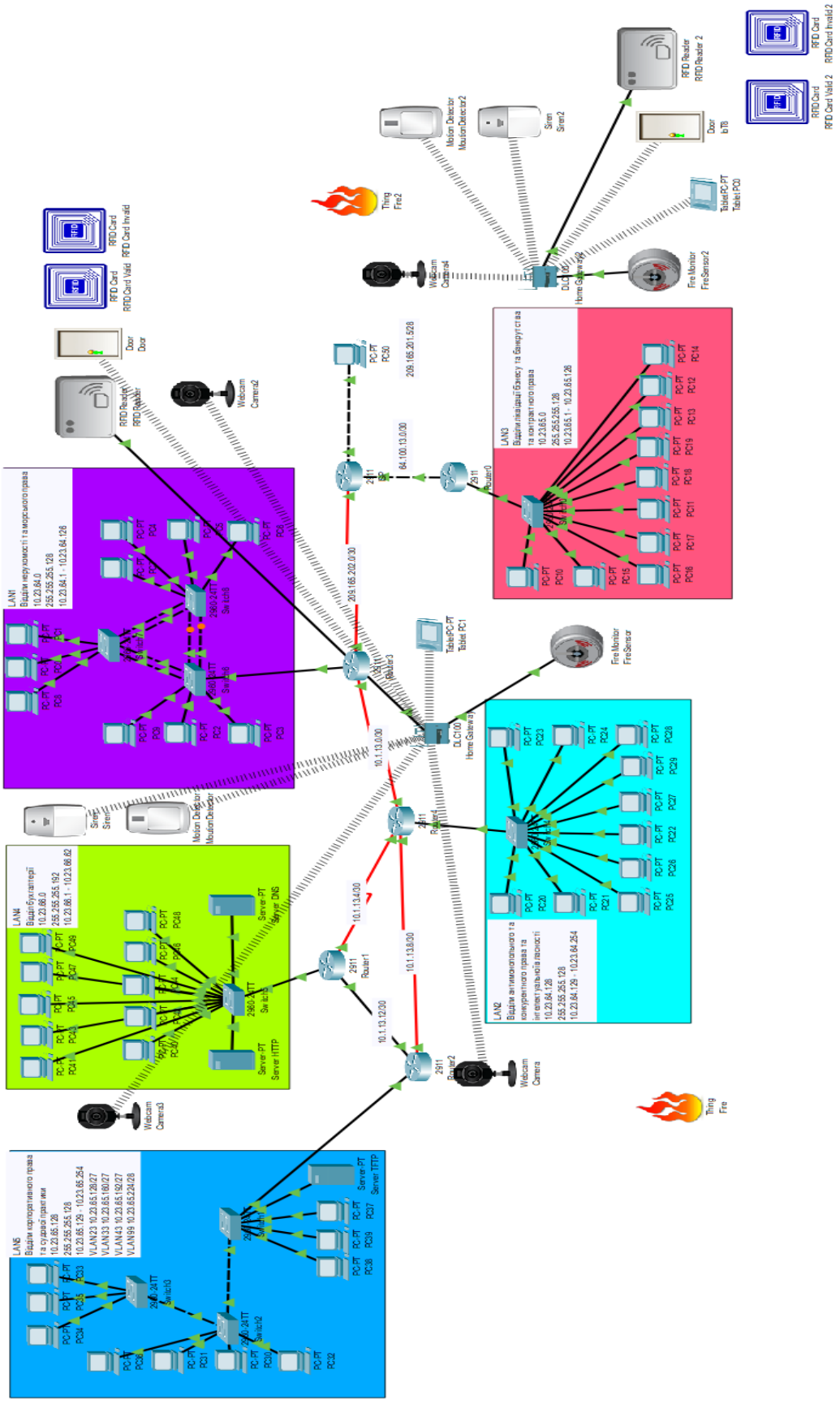

Рисунок 4.1- Схема підключення IoT-пристроїв

Далі перейдемо до налаштування роботи системи. Першим кроком необхідно виконати налаштування усіх пристроїв на динамічне отримання адрес а також вказати HomeGateway у якості IoT сервера (рисунок 4.2).

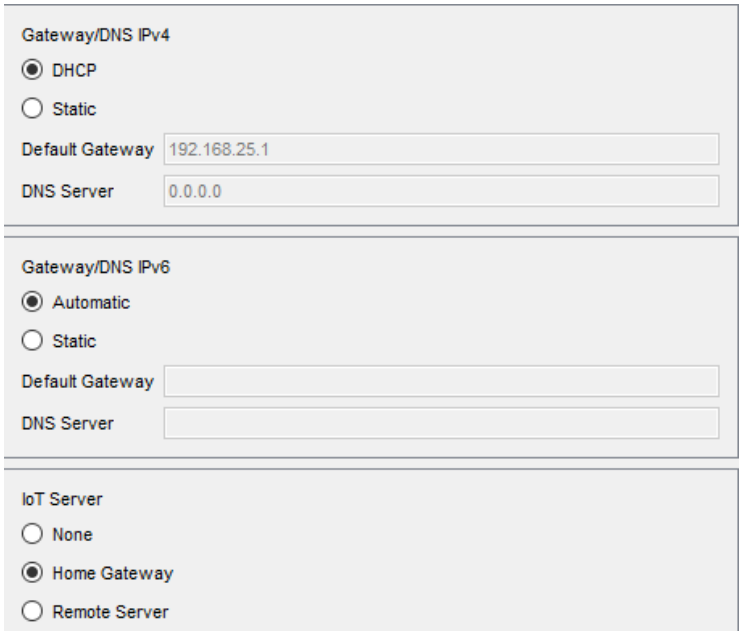

Рисунок 4.2 – Конфігурація пристроїв

Після того, як усі пристрої виконують з’єднання з шлюзом, ми можемо побачити їх перелік на головній сторінці IoT-Monitor (рисунок 4.3). Для доступу до серверу використовуємо пристрій Tablet PC.

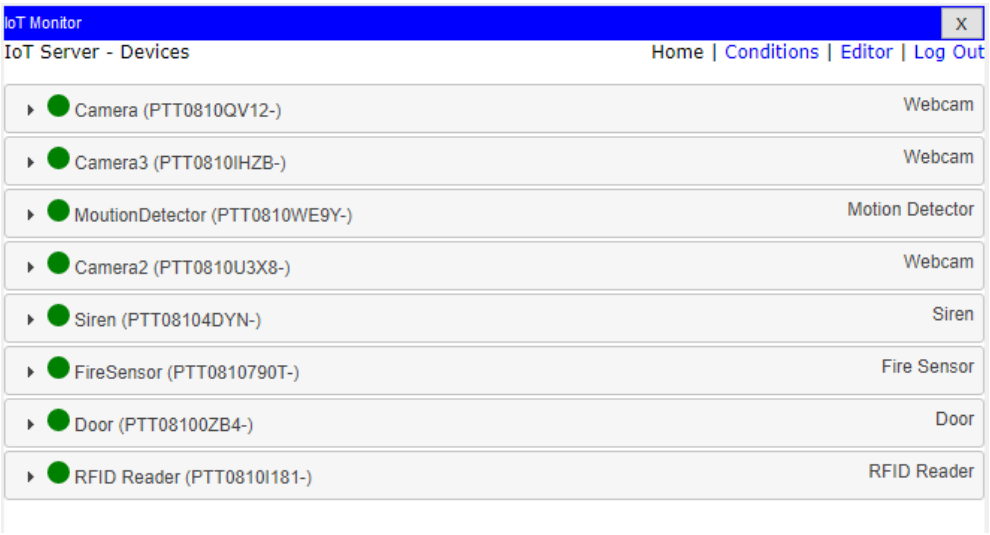

Рисунок 4.3 – Перелік під’єднаних пристроїв

Далі виконаємо налаштування роботи сирени та камер спостереження під час спрацювання датчика руху. Для цього створимо відповідний сценарій на сервері (рисунок 4.4).

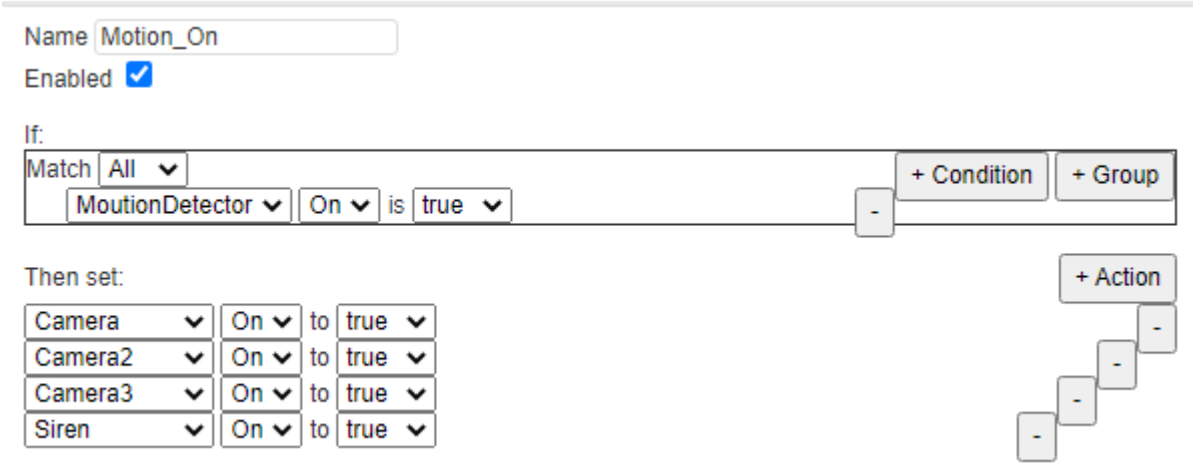

Рисунок 4.4 – Сценарій для спрацювння датчика руху

Наступним кроком налаштуємо вмикання сирени під час спрацювння датчика вогню. Створюємо сценарій на сервері (рисунок 4.5).

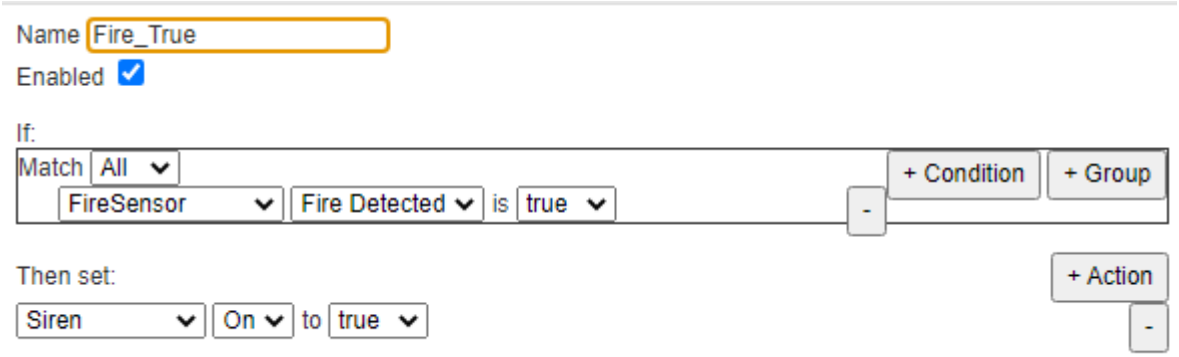

Рисунок 4.5 – Сценарій для спрацювання датчика вогню

Далі налаштуємо роботу RFID-зчитувача для замикання та відмикання дверей. Створюємо сценарії на сервері (рисунок 4.5 – рисунок 4.6).

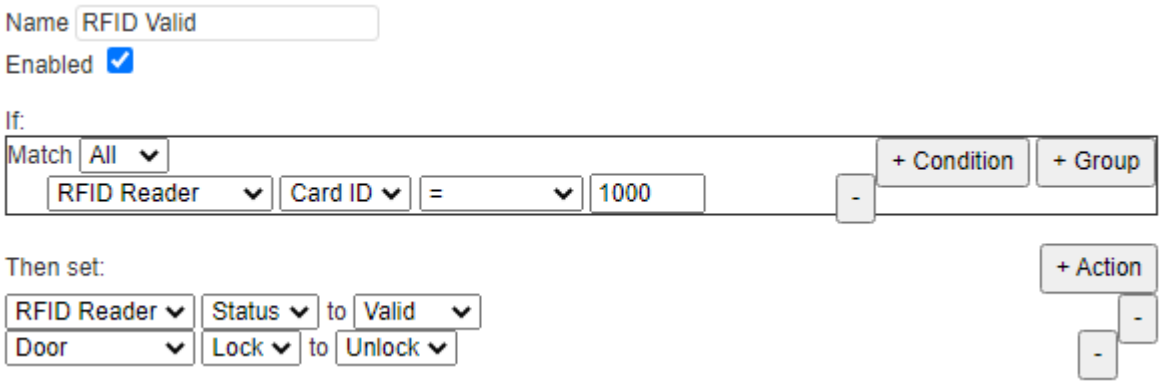

Рисунок 4.5 – Сценарій для відмикання дверей

Рисунок 4.6 – Сценарій для замикання дверей

Після цього налаштуємо вимикання камер спостереження за умови, що датчик руху не активний. Створюємо сценарій на сервері (рисунок 4.7).

Рисунок 4.7 – Сценарій для вимикання камер спостереження

Останнім налаштуємо сценарій для вимикання сирени за умови, що датчики руху та вогню неактивні (рисунок 4.8).

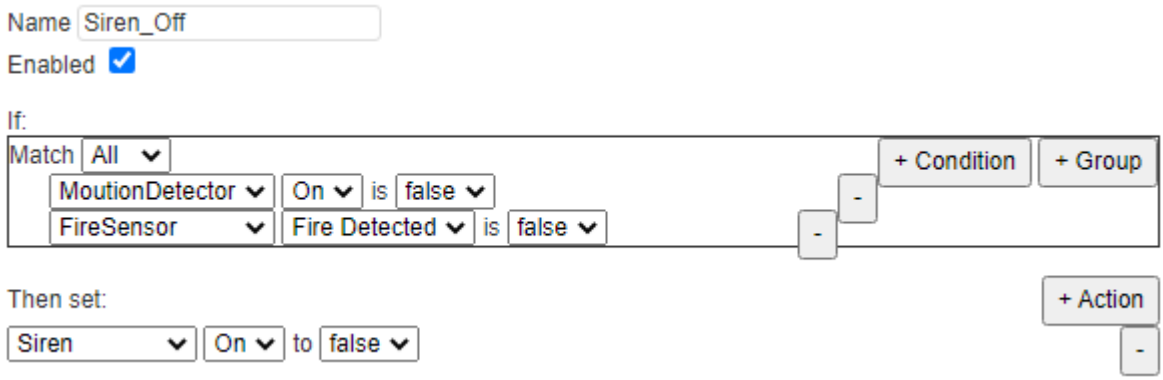

Рисунок 4.8 – Сценарій для вимикання сирени

Повний перелік створених сценаріїв наведено на рисунку 4.9.

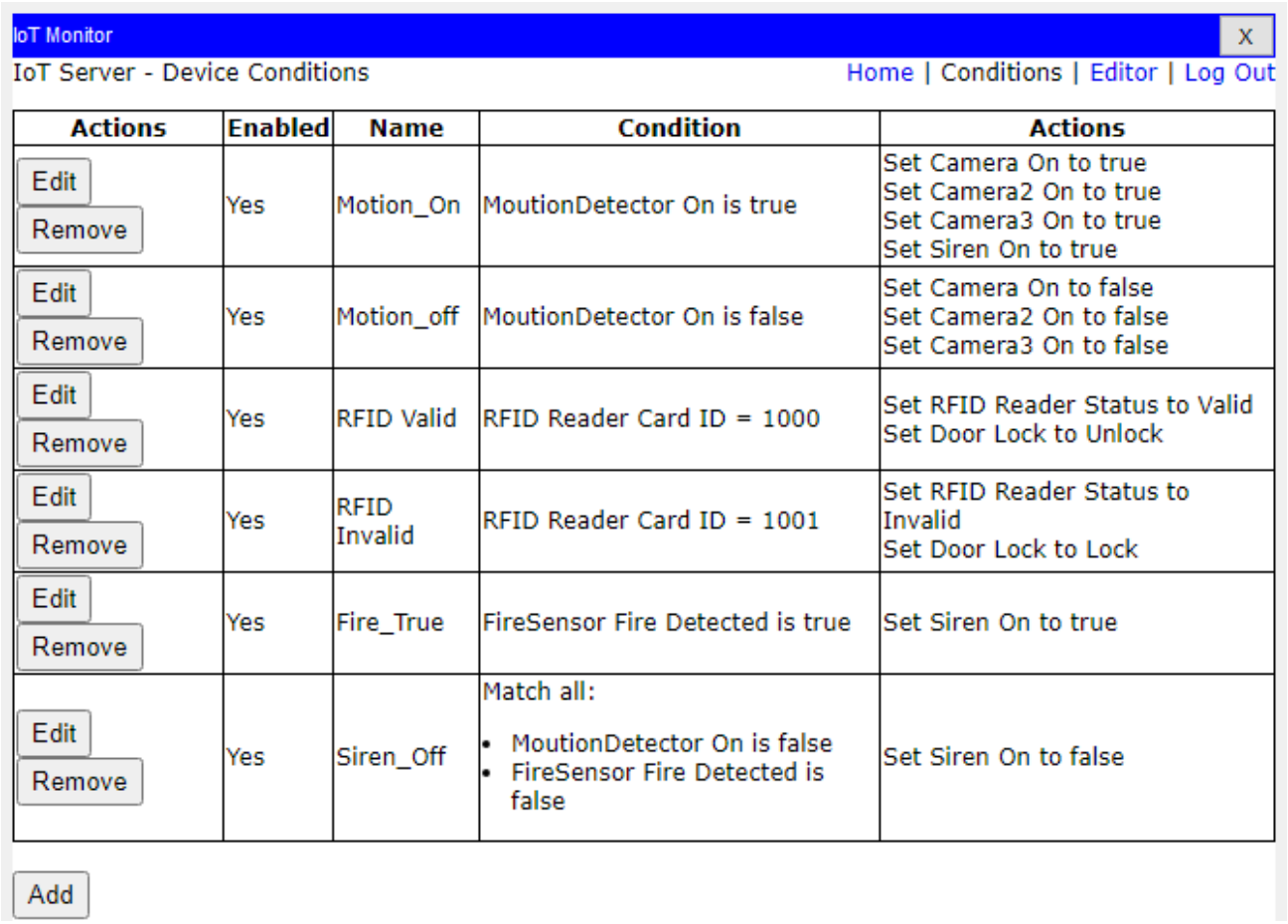

Рисунок 4.9 – Перелік сценаріїв на сервері

Також, для перевірки спрацювання датчику вогню було створено компонент «Fire». Код роботи компоненту наведено на рисунку 4.10.

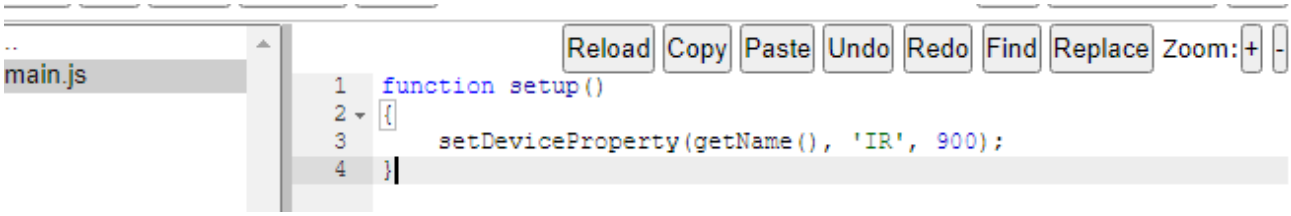

Рисунок 4.10 – Налаштування компоненту «Fire»

Аналогічні налаштування виконуються для IoT-системи віддаленого офісу.

ВИСНОВКИ

В даній кваліфікаційній роботі було детально досліджено основні аспекти проєктування мережі для підприємств, зокрема її архітектуру, безпеку, пропускну здатність та масштабованість.

У якості підприємства, для якого виконувалось проєктування мережі, було обрано юридичну компанію «Avaris».

Під час виконання кваліфікаційної роботи було виконано аналіз потреб компанії та сформовано вимоги до проектування мережі. Відповідно потребам компанії виконано вибір мережевого обладнання для системи. Моделювання проєкту було виконано у середовищі Cisco Packet Tracer. Було виконано налаштування всіх основних параметрів мережевого обладнання, реалізовано технологію VLAN, налаштовано динамічну маршрутизацію за протоколом OSPF, реалізовано доступ до інтернету за допомогою динамічного NAT, налаштовано ACL-списки, реалізовано технологію VPN для забезпечення зв’язку між головним та віддаленим офісом, налаштовано динамічне призначення адрес вузлам за протоколом DHCP, також було налаштовано об’єднання фізичних ліній комутаторів за технологією EtherChannel. Було реалізовано IoT систему безпеки офісів компанії.

Мережу було спроєктовано та змодельовано згідно сформованих вимог та теми роботи. Поставлена мета була досягнута та усі завдання виконано. Робота оформлена згідно з усіма нормами.

ПЕРЕЛІК ПОСИЛАНЬ

1. Компанія Avaris – [Електронний ресурс] – https://avaris.com.ua/ (дата звернення 10.05.2023)
2. Електронний документообіг: види систем та їхні функції – [Електронний ресурс] – https://dealssign.com/blog/elektronnij-dokumentoobig-vidi-sistem-ta-yixni-funkciyi/ (дата звернення 11.05.2023)
3. What is cloud computing? – [Електронний ресурс] – https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/ (дата звернення 12.05.2023)
4. Що таке VLAN: логіка, технологія і налаштування. Реалізація VLAN в пристроях CISCO – [Електронний ресурс] - https://e-server.com.ua/uk/poradi/shho-take-vlan-logika-tehnologija-i-nalashtuvannja-realizacija-vlan-v-pristrojah-cisco (дата звернення 18.05.2023)
5. Cisco IOS VPN Configuration Guide – [Електронний ресурс] - https://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html (дата звернення 25.05.2023)
6. Dave Hucaby, Steve McQuerry, Andrew Whitaker. Cisco Router Configuration Handbook Second Edition. – [Посібник] – Indianapolis, 2010 – 364 с. (дата звернення 25.05.2023)
7. Атестація здобувачів вищої освіти. 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. – 62 с.

ДОДАТОК А

Текст програми налаштування обладнання корпоративної мережі

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.23013-01 12 01

Листів 10

2023

АНОТАЦІЯ

В даному додатку наведено ПЗ налаштувань мережевого обладнання Cisco у середовищі моделювання «Cisco Packet Tracer».

Тексти програм написані мовою конфігураційних скриптів для мережевого обладнання Cisco.

Програма призначена для забезпечення налаштування DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній та створення мереж VPN, домену комп’ютерної системи.

ЗМІСТ

1. Скрипт налаштування Router3

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Tymchenko_Router_3
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 10.23.64.1 10.23.64.10
!
ip dhcp pool LAN1
network 10.23.64.0 255.255.255.128
default-router 10.23.64.1
dns-server 10.23.66.23
!
!
aaa new-model
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username 123191_Tymchenko password 7 082048430017061E010803
username Tymchenko_Router_3 password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX1524174Y-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
```

```
!
crypto isakmp key cisco address 64.100.13.2
!
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map MAP 10 ipsec-isakmp
set peer 64.100.13.2
set transform-set TS
match address VPN13
!
!
!
!
ip domain-name Tymchenko_Router_3
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 10.23.64.1 255.255.255.128
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
bandwidth 128
ip address 10.1.13.1 255.255.255.252
ip nat inside
clock rate 128000
!
interface Serial0/3/1
bandwidth 128
```

```
ip address 209.165.202.2 255.255.255.252
ip nat outside
crypto map MAP
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
redistribute static subnets
passive-interface GigabitEthernet0/0
network 10.23.64.0 0.0.0.127 area 0
network 10.1.13.0 0.0.0.3 area 0
network 209.165.202.0 0.0.0.3 area 0
!
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask
255.255.255.224
ip nat inside source list NAT13 pool Internet
ip nat inside source static 10.23.66.24 209.165.200.4
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
ip route 209.165.201.0 255.255.255.240 209.165.202.1
ip route 209.165.202.0 255.255.255.252 Serial0/3/1
!
ip flow-export version 9
!
!
ip access-list extended VPN13
permit ip 10.23.66.0 0.0.0.63 10.23.65.0 0.0.0.127
permit ip 10.23.64.0 0.0.0.127 10.23.65.0 0.0.0.127
permit ip 10.23.66.0 0.0.0.192 10.23.65.0 0.0.0.127
permit ip 10.23.65.128 0.0.0.127 10.23.65.0 0.0.0.127
permit ip 10.23.64.128 0.0.0.127 10.23.65.0 0.0.0.127
permit ip 10.1.13.0 0.0.0.255 10.23.65.0 0.0.0.127
ip access-list extended NAT13
deny ip 10.23.64.0 0.0.0.127 10.23.65.0 0.0.0.127
deny ip 10.23.65.128 0.0.0.127 10.23.65.0 0.0.0.127
deny ip 10.23.64.128 0.0.0.127 10.23.65.0 0.0.0.127
deny ip 10.23.66.0 0.0.0.63 10.23.65.0 0.0.0.127
deny ip 10.1.13.0 0.0.0.255 10.23.65.0 0.0.0.127
permit ip 10.23.66.0 0.0.0.63 any
permit ip 10.23.64.128 0.0.0.127 any
permit ip 10.1.13.0 0.0.0.255 any
permit ip 10.23.65.128 0.0.0.127 any
permit ip 10.23.64.0 0.0.0.127 any
!
banner motd ^CTymchenko_Router_3^C
!
radius server 10.23.66.23
address ipv4 10.23.66.23 auth-port 1645
```

```
key radius123
!
!
!
line con 0
password 7 0822455D0A16
login authentication CONSOLE
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
!
!
End
```

2. Скрипт налаштування Router0

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Tymchenko_Router_0
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 10.23.65.1 10.23.65.10
!
ip dhcp pool LAN3
network 10.23.65.0 255.255.255.128
default-router 10.23.65.1
dns-server 10.23.66.23
!
!
aaa new-model
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
!
```

```
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username 123191_Tymchenko password 7 082048430017061E010803
username Tymchenko_Router_0 password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX152488A0-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
!
crypto isakmp key cisco address 209.165.202.2
!
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map MAP 10 ipsec-isakmp
set peer 209.165.202.2
set transform-set TS
match address VPN13
!
!
!
!
ip domain-name Tymchenko_Router_0
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 64.100.13.2 255.255.255.252
```

```
ip nat outside
duplex auto
speed auto
crypto map MAP
!
interface GigabitEthernet0/1
ip address 10.23.65.1 255.255.255.128
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip nat pool Internet 209.165.205.5 209.165.205.30 netmask
255.255.255.224
ip nat inside source list NAT13 pool Internet
ip classless
ip route 0.0.0.0 0.0.0.0 64.100.13.1
ip route 64.100.13.0 255.255.255.252 64.100.13.1
ip route 209.165.201.0 255.255.255.240 64.100.13.1
!
ip flow-export version 9
!
!
ip access-list extended VPN13
permit ip 10.23.65.0 0.0.0.127 10.23.64.0 0.0.0.127
permit ip 10.23.65.0 0.0.0.127 10.23.65.128 0.0.0.127
permit ip 10.23.65.0 0.0.0.127 10.23.64.128 0.0.0.127
permit ip 10.23.65.0 0.0.0.127 10.23.66.0 0.0.0.63
permit ip 10.23.65.0 0.0.0.127 10.1.13.0 0.0.0.255
ip access-list extended NAT13
deny ip 10.23.65.0 0.0.0.127 10.23.64.0 0.0.0.127
deny ip 10.23.65.0 0.0.0.127 10.23.64.128 0.0.0.127
deny ip 10.23.65.0 0.0.0.127 10.23.65.128 0.0.0.127
deny ip 10.23.65.0 0.0.0.127 10.23.66.0 0.0.0.63
deny ip 10.23.65.0 0.0.0.127 10.1.13.0 0.0.0.255
permit ip 10.23.65.0 0.0.0.127 any
!
banner motd ^CTymchenko_Router_0^C
!
radius server 10.23.66.23
address ipv4 10.23.66.23 auth-port 1645
key radius123
```

```
!
!
!
line con 0
password 7 0822455D0A16
login authentication CONSOLE
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
!
!
end
```