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 Залізняка Максима Григоровича
(ПІБ)
академічної групи 123-19ск-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 ігрової студії "Ubisoft Ukraine (Kyiv)" з опрацюванням побудови відмовостійкової корпоративної мережі"
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Цвіркун Л.І.			
розділів:				
розробка апаратної частини	доц. Бешта Д. О.			
розробка корпоративної мережі	ас. Панферова Я.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2022

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

"25" січня 2022 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Залізняк М. Г. **академічної групи** 123-19ск-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 ігрової студії "Ubisoft Ukraine (Kyiv)" з опрацюванням побудови відмовостійкової корпоративної мережі"

затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022 № 268-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2022
Розробка апаратної частини	На основі аналізу підприємства формуються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2022
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для відмовостійкості в системі	24.05.2022
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2022

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

Дата видачі 25.01.2022

Дата подання до екзаменаційної комісії 14.06.2022

Прийнято до виконання _____ Залізняк М. Г.
(підпис керівника) (прізвище, ініціали)

РЕФЕРАТ

CISCO, МЕРЕЖА, КОМПЮ'ТЕРНА СИСТЕМА, ТОПОЛОГІЯ, БЕЗПЕКА.

Пояснювальна записка: 106 с., 46 рис., 9 табл., 1 дод., 11 джерел.

Об'єкт: Комп'ютерна система ігрової студії «Ubisoft Ukraine (Kyiv)» з опрацюванням побудови відмовостійкової корпоративної мережі

Мета: розробка технічних вимог та проектування, для створення і виконання проекту корпоративної мережі із детальним опрацюванням її структури мережі для підрозділів ігрової студії «Ubisoft Ukraine (Kyiv)» та забезпеченню відмовостійкості.

Розробити мережеву для підрозділів ігрової студії з урахуванням можливості швидкої зміни конфігурацій і додавання набору виконуваних функцій шляхом доукомплектування або вилученням потрібних сегментів мережі, також з урахуванням для збору, пересилання та підготовки статистичної інформації.

Систему виконано відкритою що дозволяє технічну і програмну модернізацію системи, так само забезпечує виконання функцій взаємодії підрозділів у різних мережах, збір та обробку, накопичення матеріалів студії на серверах, комунікацію між кінцевими користувачами у різних відділах та доступ до інтернет ресурсів поза мережі, зв'язок між віддаленими сегментами мережі, та забезпечення відмовостійких концептів в сегментах мережі.

Реалізована схема мережі у вигляді графічних схема.

Робота системи перевірена за допомогою моделі схеми корпоративної мережі із застосуванням програми Cisco Packet Tracer версії 8.

Реалізацію подано у вигляді таблиць, графіків які описані і наводяться у пояснювальній записці та додатках.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

КС – Комп’ютерна система

DHCP – Dynamic Host Configuration Protocol

DNS –Domain Name System

Ether Channel – Технологія агрегації на канальному рівні.

LAN – Local Area Network

NAT – Network Address Translation

VLAN – Віртуальна локальна комп'ютерна мережа

VPN – Virtual Private Network

ВСТУП

На теперішній час жодне велике підприємств не може уявити своє існування без використання та впровадження комп’ютерних систем та мереж в ній.

Також дуже важливим аспектом використання мережі на підприємствах є надання можливості забезпечити співробітникам та різним відділам цієї організації доступ в будь який момент часу до внутрішнім ресурсам для виконання поставлених перед організацією задач. В нинішній час швидкого розвитку ігрової індустрії дуже важливо мати швидкий доступ до ресурсів які використовуються організацією та їх співробітниками для якісного та швидкого вирішення да усунення помилок в створених продуктах цієї студії, так як потрібні відділи можуть мати різне географічне розташування і в таких умовах якісно спроектована мережа буде забезпечувати взаємодію між потрібними сегментами при будь яких обставинах та захищати внутрішню критичну інформацію цієї організації.

В даній роботі розглядається комп’ютерна система ігрової студії «Ubisoft Ukraine (Kyiv)». На сьогодні у сфері діяльності ігрової студії «Ubisoft Ukraine (Kyiv)» надаються послуги: створення 3D моделей, наповнення та створе рівнів відеоігри, розробка та створення сінглових та мультиплеірних ігрових проектів, написання сюжетного наповнення для подальшого створення віртуального світу, видавництво комп'ютерних ігор, підтримка та створення оновлень для мережевих проектів, підтримка користувачів, проведення та організація виставок видавництва.

Для ефективного ведення бізнесу організації необхідно впровадження сучасної комп’ютерної системи, що дозволить оптимізувати робочий процес, здійснювати зберігання даних на сервері та обмін файлами, спільне використання обладнання та периферійних пристроїв, а також ефективну взаємодію співробітників за допомогою чатів і відео конференцій та інше.

Для вирішення цієї задачі необхідно провести дослідження і аналіз предметної області, спроектувати логічну схему мережі підприємства, спроектувати фізичну схему мережі, вибрати активне і пасивне устаткування, виконати налаштування мережних пристроїв та впровадити заходи з безпеки мережі та принципів забезпечення відмовостійкості.

1 ПОСТАНОВА ЗАВДАННЯ

1.1 Стан питання і постановка задачі для «Ubisoft Ukraine (Kyiv)»

Компанія «Ubisoft Ukraine (Kyiv)» відноситься до галузі ігрової індустрії та створення ігрових продуктів та левил-дизайну. Таким чином в цій галузі дуже важливу роль займає якісне проектування комп’ютерної мережі для подальшого запобігання відсутності доступу до окремих сегментів мережі та забезпечення відмовостійкості системи.

1.1.1 Характеристика і структура об’єкта впровадження

Компанія, яка замовила модернізацію комп'ютерної мережі, – це ігрова студія «Ubisoft Ukraine (Kyiv)», одна з провідних студій України з біль ніж 13-ти річним досвідом надання послуг в сфері гейм-девелопмент по всьому світі. Основні відомості про юридичне лице компанії-замовника: «Ubisoft Ukraine (Kyiv)»; має в своєму складі 683 працівників; адреса головного офісу 04112, Україна, Київська обл., м. Київ, вул. Дегтярівська 52, «Ubisoft Kyiv»; адреса другої студії 65000, Україна, Одеська обл., м. Одеса, вул. Віце-Адмірала Жукова, 17/19, «Ubisoft Odesa».

Фахівці компанії досвідчені програмісти які знають такі мови як C++, C #, Git, Jira, гейм дизайнери, сценаристи, художники персонажів, художники рівнів, спеціалісти з роботи в Unity3d, художник створення рекламних аратів, директор видавництва ігрових проектів, гейм-дизайнер проектів, гейм-дизайнер рівнів та світу, бекент розробник, фронтент розрадник.

Ігрова студія «Ubisoft Ukraine (Kyiv)» успішно співпрацює з великими світовими видавництвами та іншими міжнародними студіями.

Основні напрямки діяльності компанії «Ubisoft Ukraine (Kyiv)».

Взяття проекту в своє видавництво для подальшого розповсюдження через свою мережу реалізації.

Аналіз взятого проекту на унікальність сюжетного розповіді ідеї, перевірка на унікальність та регулювання авторського права з видавництвом

та розробником проекту.

Консультація с юридичним відділом та подання документації для створення унікальної торгової марки та затвердження кінцевого вигляду іродового проекту с іншими інтернет магазинами через які в подальшому розповсюджується продукт.

Регулювання проекту с законодавством інших країн та вікового ліміту.

Створення арт-буків та рекламних банерів.

Створення рекламної компанії проекту та закрите представлення фінального продукту.

Початок продаж та створення декількох версій для попереднього замовлення та створення бази підтримки клієнтів та зворотного зв’язку, та подальшого створення потрібних оновлень, і усунення помилок в продукті які не виявилися в ході тестувань.

Проектування рівня для проекту замовленої ігрового продукту.

Аналіз та обговорення с замовником сюжету гри та даного рівня, та створення арт макетів для утвердження с замовником стилістику та концепт рівнів в цьому проекті.

Створення заготовки 3D моделей, і створення анімацій для них та реалізація текстур і матеріалів які будуть використані в кінці на них.

Збирання в фінальний проект та накладання програмного коду якщо потрібно та тестування на наявність богів та представлення його замовнику і передання йому.

Написання сюжету для подальшого концепту створення комп’ютерної гри.

Визначення та опрацювання концепту гри с головним сценаристом.

Розробка рекомендацій які повинні бути включені в ході написання сюжету для головної та побічних ліній сюжету.

Написання та опрацювання побічних гілок завдань та мотивації голонога героя проекту.

Представлення написаного сюжету замовнику та внесення мілких

коректив, і обговорення для подальшої реалізації цього сюжету в фінальний проект, і створення авторських прав на цей сюжетний концепт та сценарій проекту.

Створення власного ігрового проекту.

Обрання або створення сюжету і узгодження концепту проекту.

Реалізація та створення концепт-артів головних героїв та їх 3D моделей.

Створення віртуального світу який було обговорено на початку роботи та реалізація рівнів та локацій які його.

Предфінальна збірка проекту та тестування на наявність первинних помилок та багів в проекті та внесення коректив.

Фінальне тестування та перед показ кінцевого продукту на закритій виставці.

Створення рекламної компаній та арт-буків по цьому проекту та утвердження торгової марки проекту для прийому перед замовлень і початку продаж проекту.

Для розробки проекту комп’ютерної системи для ігрової студії «Ubisoft Ukraine (Kyiv)» із застосуванням сучасних мережних технологій, необхідно проаналізувати структурні підрозділи, що будуть поєднані мережею.

Ігрова студія «Ubisoft Ukraine (Kyiv)» має організаційну структуру, представлену на рисунку 1.1. У фірмі реалізований лінійно-функціональний тип організаційної структури, тобто, організована вона ієрархічна і характеризується поділом зон відповідальності і єдиноначальністю, діяльність структурних підрозділів спеціалізована і визначається основним функціональним ознакою.

Організаційно-управлінська структура студії представляється у вигляді трьох рівнів управління: верхнього, середнього і нижчого.

Верхній рівень управління відповідає директорська підсистема.

На чолі верхнього рівня керування знаходиться директор студії. Він здійснює загальне керування діяльністю ігрової студії «Ubisoft Ukraine (Kyiv)» і несе відповідальність за виконання замовлень, які безпосередньо входять в

його обов'язки.

У практичному підпорядкуванні у директора знаходяться усі посадові особи, що входять до підрозділів ігрова студії.

Середній рівень керування ігрової студії забезпечує функції, що входять в забезпечення підсистем. До цього рівня відносяться директори всіх структурних підрозділів, що забезпечують робочу діяльність студії та виконання поставлених завдань, поставлених на вищому рівні.

Оперативний рівень управління включає в себе персонал всіх підрозділів структури, які безпосередньо виконують визначені здачі керівництвом, поставлені на верхньому і середньому рівнях керування.

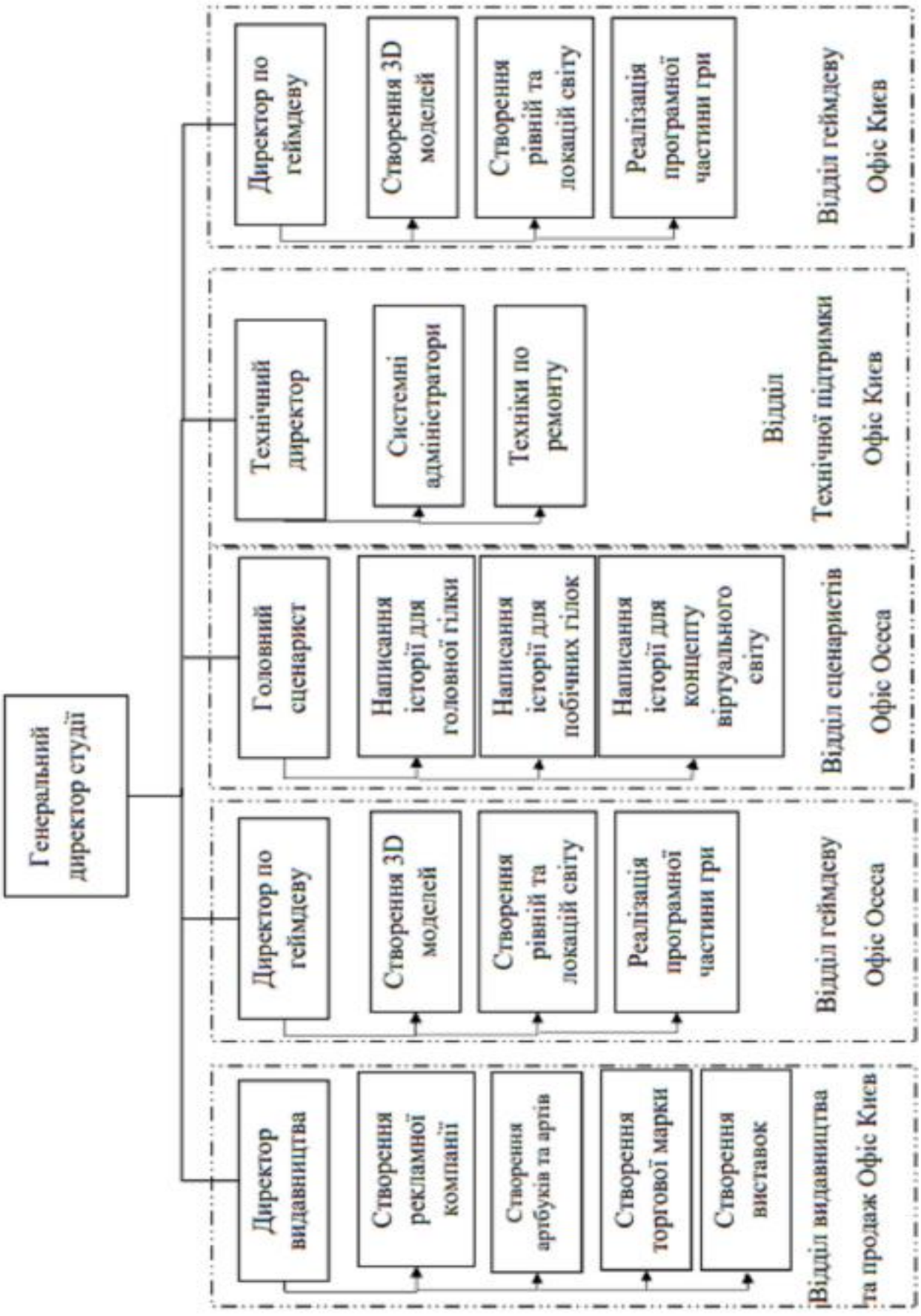

Рисунок 1.1 – Організаційна структура ігрової студії «Ubisoft Ukraine (Kyiv)»

1.1.2 Стислі відомості про технології передачі інформації та збору для КС ігрової студії «Ubisoft Ukraine (Kyiv)»

Компанія «Ubisoft Ukraine (Kyiv)» в своєму складі має два офіси. Перший розташований в Києві рисунок 1.2 за адрескою Україна, Київська обл., м. Київ, вул. Дегтярівська 52, «Ubisoft Kyiv», та другий в Одесі рисунок 1.3 адреса Україна, Одеська обл., м. Одеса, вул. Віце-Адмірала Жукова, 17/19, «Ubisoft Odesa». Таким чином компанія висуває вимоги до мережевого комплексу комп'ютерної та інформаційної безпеки для збереження цілісності розробок самої компанії та її персоналу.

До складу приміщень ігрової студії «Ubisoft Ukraine (Kyiv)» входять: головний офіс за адресую Україна, Київська обл., м. Київ, вул. Дегтярівська 52, «Ubisoft Kyiv» (приміщення на третьому поверсі в 2700 м^2) та офіс «Ubisoft Odesa» за адресую Україна, Одеська обл., м. Одеса, вул. Віце-Адмірала Жукова, 17/19 (приміщення на четвертому поверсі в 1100 м^2).

План приміщень офісну зображено на рисунках 1.5 – 1.6.

В приміщені будівлі «Ubisoft Kyiv» в офісних приміщеннях розташовані наступні підрозділи зі своїми структурними групами: відділ видавництва та продаж, відділ гейм-девелопмент, відділ технічної підтримки.

В приміщені будівлі «Ubisoft Odesa» розташований відділ сценаристів, відділ гейм-девелопмент.

Рисунок 1.2 – Схема топологічного розташування ігрової студії «Ubisoft Kyiv»

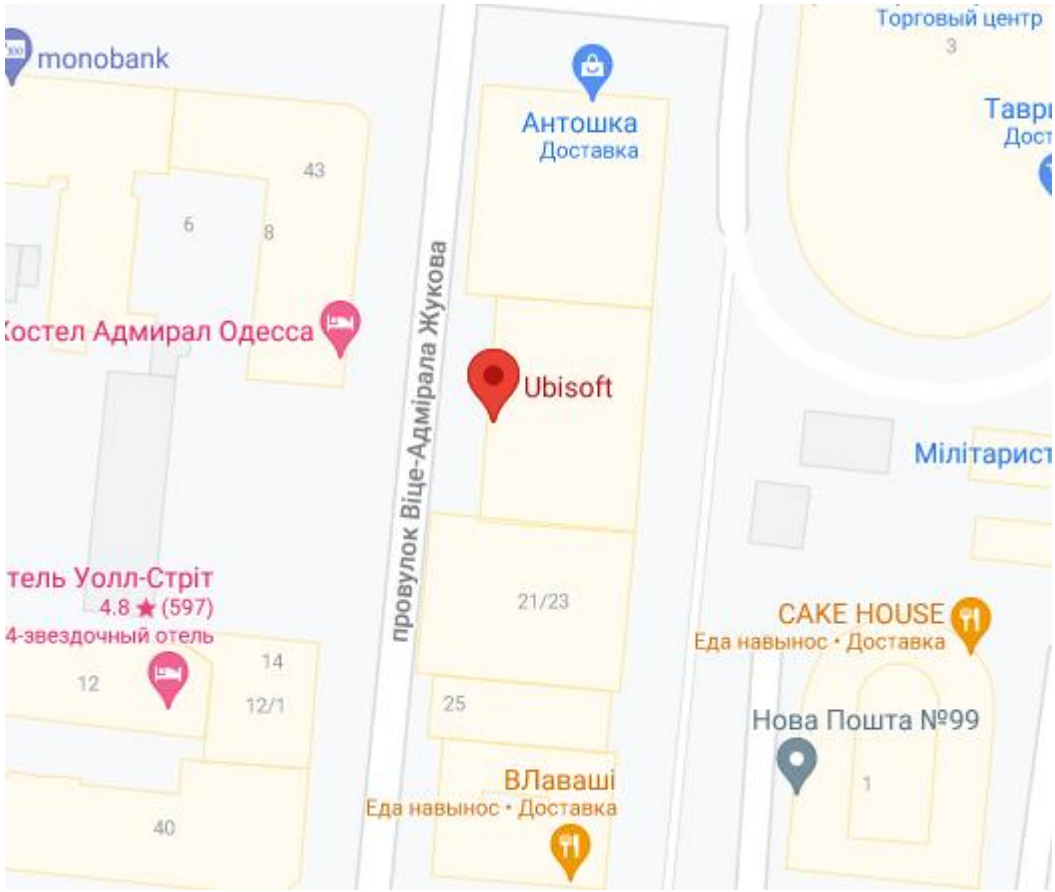

Рисунок 1.3 – Схема топологічного розташування ігрової студії «Ubisoft Odesa»

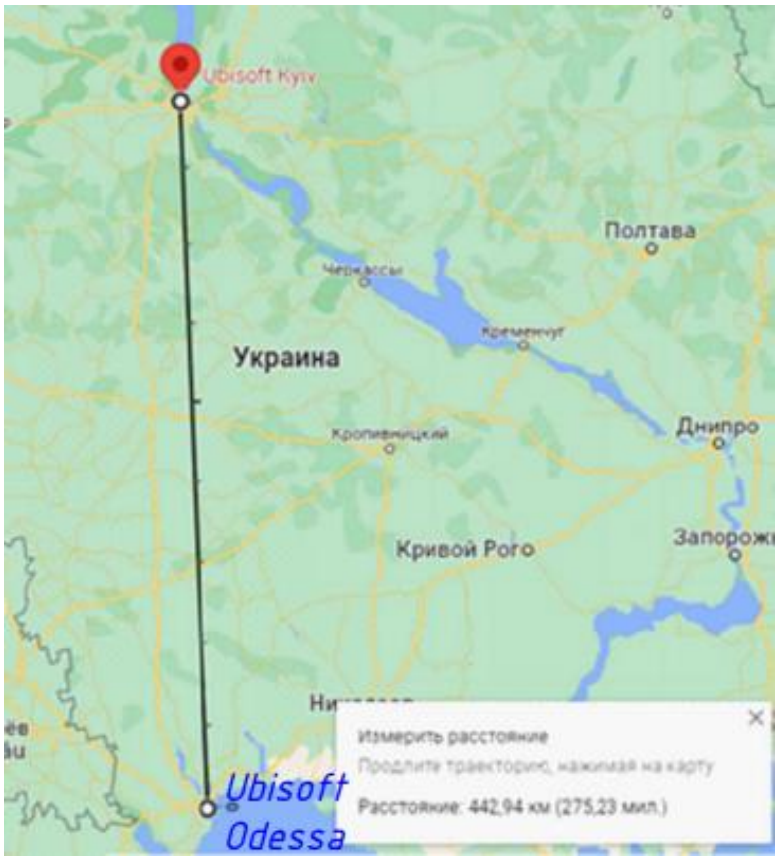

Рисунок 1.4 – Зображення відстані між двома офісами яка складає 442,94 км

Розгортання корпоративної мережі дозволить підприємству краще задовольняти поставленим вимогам сучасного бізнесу. Корпоративна мережа – це система, що включає багато різних компонентів комп’ютерних технологій різних типів, системне і прикладне програмне забезпечення, мережне обладнання, кабельну систему [5]. Основне завдання системних інтеграторів і адміністраторів полягає в тому, щоб ця дуже дорога система як найкраще справлялася з обробкою потоків інформації, що циркулюють між офісами підприємства і дозволяла приймати їм своєчасні та найкращі рішення, що забезпечують якісну комунікацію та більш продуктивну роботу організації.

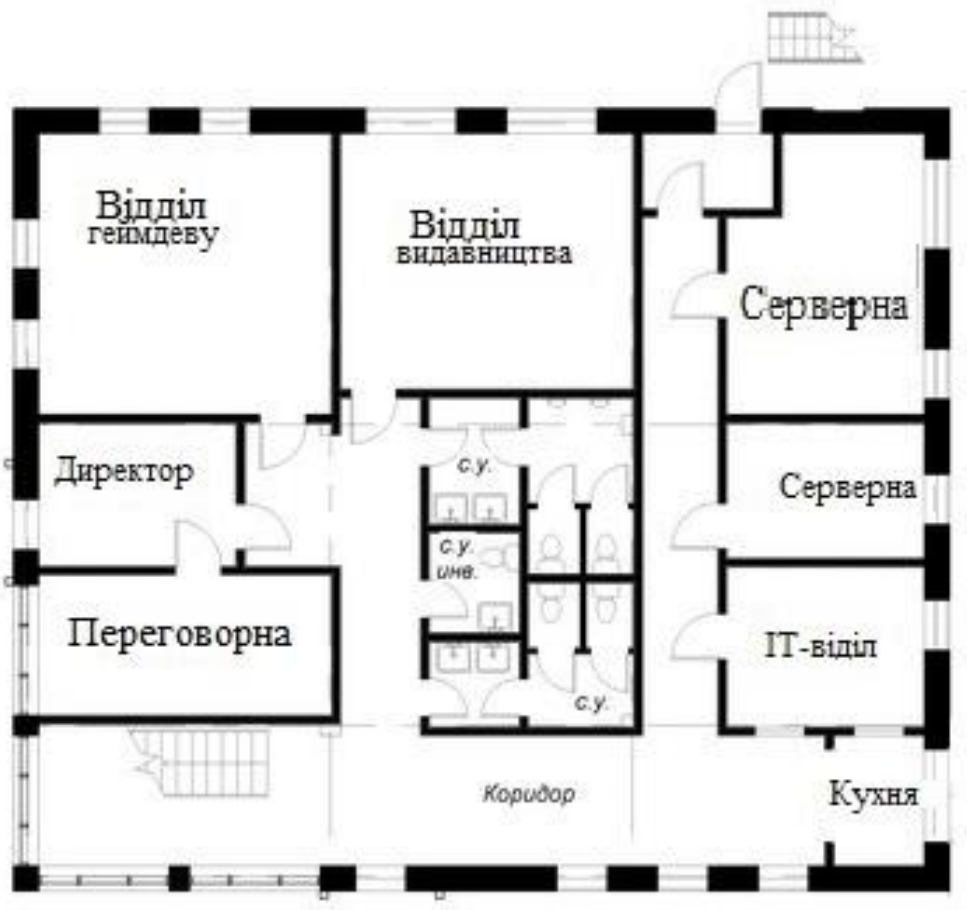

Рисунок 1.5 – План приміщення ігрової студії «Ubisoft Kyiv»

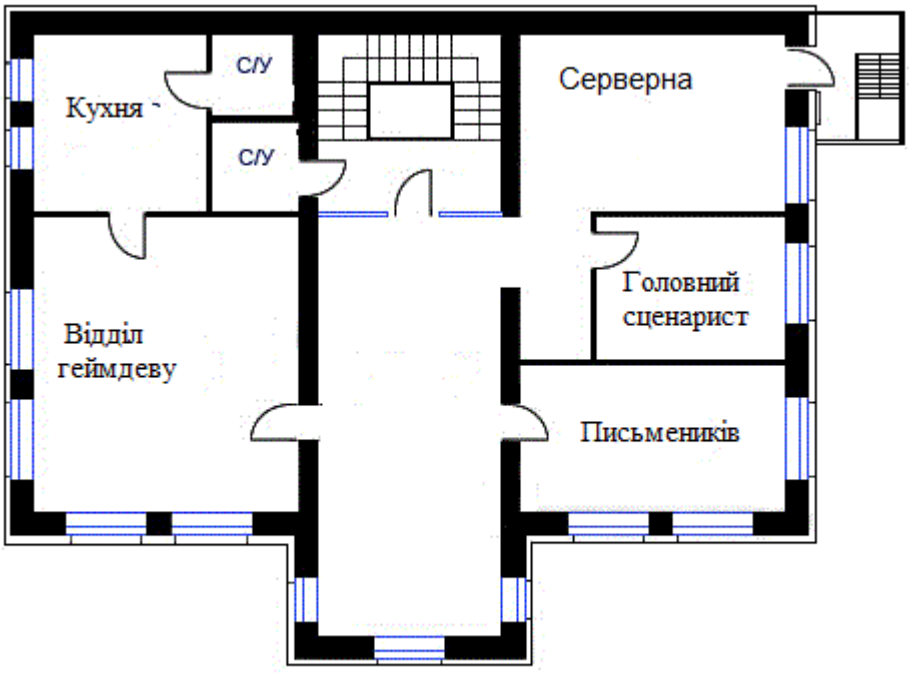

Рисунок 1.6 – План офісного приміщення ігрової студії «Ubisoft Odesa»

Ступінь комп'ютеризації робочих місць підприємства приведена в таблиці 1.1.

Таблиця 1.1 – Комп'ютеризовані робочі місця підприємства

Структурний підрозділ	Кількість		
	Робітники	ПК	Додаткові пристрої
Директор	1	1	
Секретар	1	1	1
Відділ гейм-девелопмент	293	293	3
Відділ сценаристів	97	97	3
Відділ видавництва	127	127	1
Підрозділ технічної підтримки	167	167	3
Загалом пристроїв	686	686	11

1.2 Технічні способи та технології інформаційного забезпечення КС ігрової студії «Ubisoft Ukraine (Kyiv)»

В даний час для проектування корпоративних мереж застосовуються два підходи. Перший заснований на використанні набору стандартних рішень при побудові мереж (під стандартними рішеннями маються на увазі рішення, пропоновані відомими компаніями – Cisco, HP, і т.д.). Даний підхід характеризується відносно низьким рівнем витрат на проектування, однак отримана мережа може не повною мірою відповідати вимогам, що пред'являються. Мережі, побудовані з використанням другого підходу, містять крім стандартних рішень ще й унікальні розробки, які дозволяють максимально адаптувати мережу до структури бізнес-процесів підприємства.

При застосуванні даних підходів для побудови корпоративної мережі підприємства, необхідно слідувати наступним крокам проектування.

Першими етапами розробки є огляд комп'ютерів: центрів обробки і зберігання інформації; і транспортна система, що забезпечує передачу інформаційних пакетів між комп'ютерами. Наступним етапом є розгляд питання мережевих операційних систем, який організовує роботу програм в комп'ютерах і надає через транспортну систему ресурси свого кінцевого

пристрою в загальне користування. Далі розглядається питання застосованих в комп’ютерній системі підприємства системних додатків. На наступному етапі опрацьовуються сервіси, які користуючись СУБД, як інструментом для пошуку потрібної інформації серед іншої, що зберігаються в датацентрі, надають кінцевим користувачам цю інформацію в зручній для сприйняття рішенні формі. До цих сервісів відноситься служба WWW, система електронної пошти та багато інших. Верхній рівень мережі представляють спеціальні налаштовані системи, які виконують завдання, згідно вимог даного підприємства.

Відповідно до запропонованого фірмою Cisco Systems підходом, комп'ютерні мережі зручно представляти у вигляді трирівневої ієрархічної моделі. Ця модель включає в себе наступні три рівня ієрархії: рівень ядра; рівень розподілу; рівень доступу.

Принципи побудови мереж наступні.

Масштабованість. Мережа забезпечує можливість розширення. Все обладнання вибирається з резервом, як по продуктивності, так і по можливості установки додаткових модулів і розширення функціональності.

Надмірність. Використовується об'єднання фізичних каналів в єдиний логічний канал.

Віртуалізація. Застосування технології DHCP та протоколів OSPF та EIGRP.

Відмовостійкість. Використання технологій та принципів реалізації відмовостійкості на канальному та мережевому рівні для мережі LAN 1.

Безпека. Захист всіх пристроїв мережі системою паролів.

Уніфікація і стандартизація. При створенні мережі в якості активного мережного обладнання застосовується обладнання компаній, що мають міжнародні сертифікати.

В КС офісу ігрової студії «Ubisoft Kyiv», враховуючи великий розмір мережі, рівень ядра і розподілу будуть розбито на декілька пристрої для підвищення надійності. В центрі мережі будуть маршрутизатори ядра. Вони будуть з’єднувати з маршрутизаторами робочих груп підприємства. Через

маршрутизатор ядра виконуватиметеся підключення мережі до Інтернет за допомогою технології NAT та VPN.

В КС офісу ігрової студії «Ubisoft Odesa», враховуючи невеликий розмір мережі, як базову доцільно застосувати технологію Ethernet. На даний момент це найпопулярніша і відносно проста технологія, отже, асортимент обладнання широкий, саме воно дешево і просто в установці.

1.3 Огляд існуючих інженерних рішень для ігрової студії

Одна з провідних компаній з впровадження мережних рішень, компанія «ЛанКей». Цією компанією виконуються рішення для замовників за напрямками: для великих корпоративних мереж; для корпоративних мереж середнього розміру; для невеликих офісів; для операторів зв'язку.

Показовим є проєкт побудови корпоративної мережі середнього розміру з використанням маршрутизаторів Cisco UCS C220 M3 LFF для компаній з кількістю працівників біля 500 чоловік представлено на рисунку 1.7.

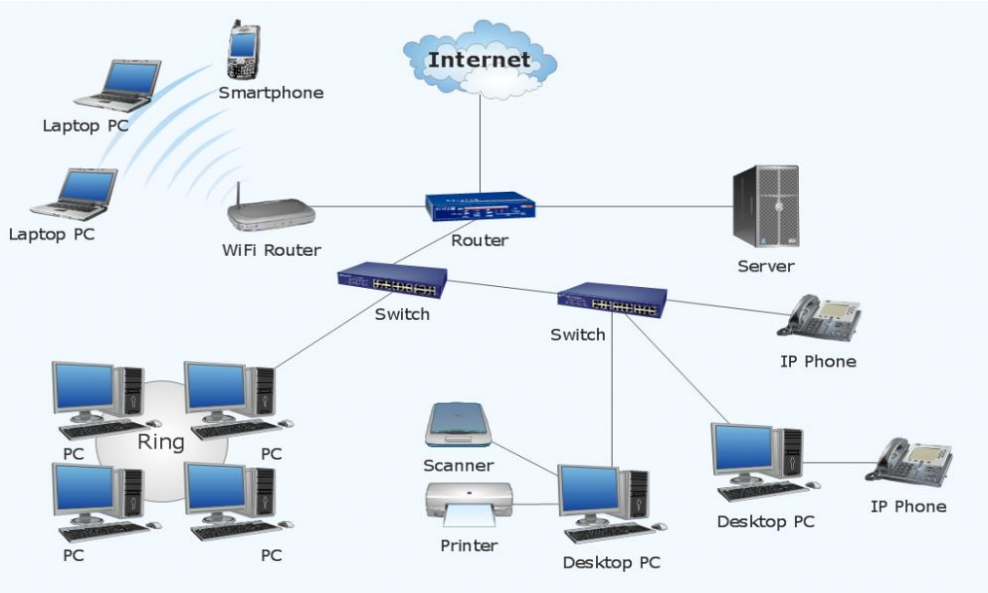

Рисунок 1.7 – Приклад рішення компанії «ЛанКей» проекту корпоративної мережі середнього розміру

Майже будь-яка невелика компанія в даний час має розподілену структуру. Рішення з побудови корпоративної мережі середнього розміру

підходить для малих підприємств, яким потрібна стабільна мережа дозволяє підключати співробітників на швидкості до 1Гбіт / с, підключати обладнання з застосуванням технології PoE, а так само реалізовувати відмовостійку структуру на рівні агрегації.

Пропоноване рішення має наступні переваги: низька вартість обладнання; висока продуктивність; підвищена безпека; масштабованість; висока надійність; модульність і можливість швидкого розгортання.

1.3.1 Напрямки рішення висунутих завдань

Компанія Cisco Systems є світовим лідером на ринку мережевих рішень. Для корпоративної мережі середнього розміру перевагами застосування рішень корпорації Cisco System є:

– використання програмного забезпечення Cisco IOS для управління мережним обладнання Cisco. Cisco IOS – операційна система, яка забезпечує функціонування мережного обладнання Cisco, що є основою мережі Інтернет і найбільших приватних мереж;

– забезпечення мережевої безпеки широкого функціоналу в обладнанні Cisco. В лінійці обладнання присутні моделі з інтегрованими засобами безпеки

– ОС Cisco IOS підтримує механізми забезпечення мережевої безпеки: списки контролю доступу (ACL) для пакетної фільтрації трафіку; підтримку протоколів SSH, SNMPv3 і HTTPS, що забезпечують шифрування каналів управління; підтримку централізованої автентифікації, авторизації та обліку адміністративної діяльності, віддаленого доступу і підключень до мережі за допомогою протоколів RADIUS, забезпечення цілісності та конфіденційності даних на мережному рівні з використанням стека протоколів IPSec. Також для забезпечення відмовостійкості було обрано такі технології як HSRP, EtherChannel, принцип гарячої заміни, дублювання критичних точок системи.

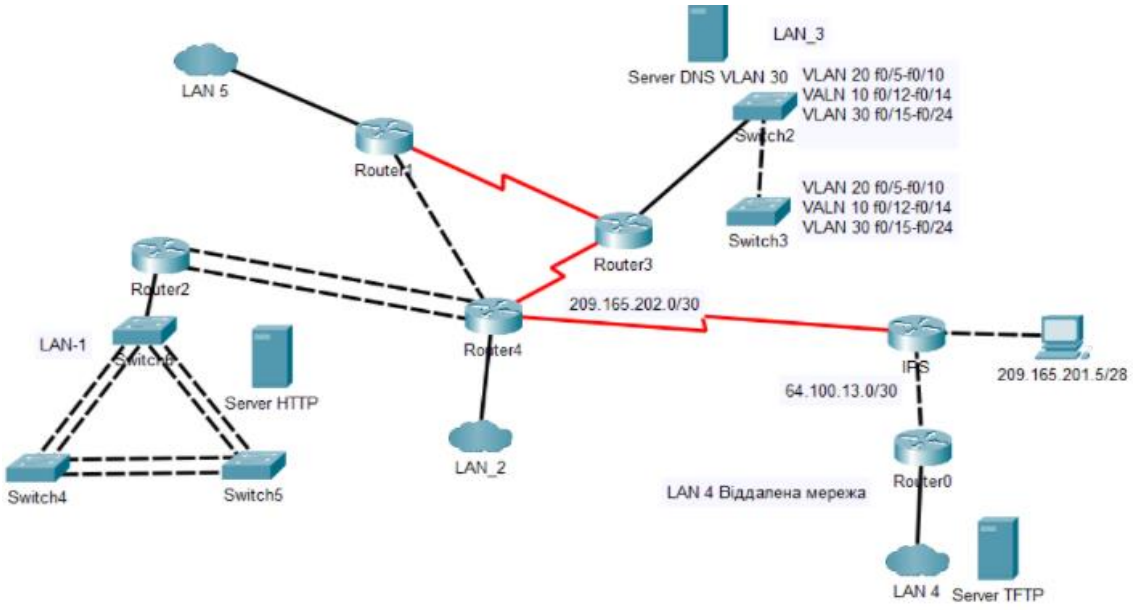

Рисунок 1.8 – Загальна архітектура мережі ігрової студії «Ubisoft Ukraine (Kyiv)»

Відповідно до наведених принципів проектування, КС ігрової студії «Ubisoft Kyiv» та «Ubisoft Odesa» повинна складається загалом з п’яти мереж сумарною кількістю в обох офісах, що забезпечує зв'язок між маршрутизаторами мережу провайдера та віддаленими сегментами мережі за допомогою VPN та NAT.

В підмережах обох офісах потрібно створити динамічну маршрутизацію та використати сервіс DHCP та протоколи динамічної маршрутизації EIGRP. Також в мережі видавництва та продаж реалізувати агрегацію каналів для підвищення відмовостійкості та пропускної здатності так як там знаходиться основана маса даних судії та проектів. Виконати налаштування ACL списків для мережі VPN для підвищення безпеки. Налаштувати динамічний NAT для зв’язку між двома офісами та серверами.

Виконати захист мережі відповідно до архітектури Cisco SAFE. Налагодити передачу трафіка між віддаленими мережами відділів. Налагодити вихід користувачів до мережі Internet.

1.4 Завдання і мета роботи згідно тематики роботи

Метою роботи є організація корпоративної комп'ютерної мережі ігрової студії «Ubisoft Ukraine (Kyiv)» із детальним опрацюванням нюансів налаштування відмовостійкості апаратно-програмного мережного комплексу для подальшого розгортання цієї мережі.

Для вирішення поставленої мети в роботі вирішуються наступні завдання:

– вибір мережевої архітектури для корпоративної мережі;

– вибір технології та топології корпоративної мережі;

– вибір кабельної системи корпоративної мережі;

– вибір способу управління мережею;

– розробка фізичної та логічної топології мережі підприємства;

– конфігурація мережного обладнання;

– вибір технологій відмовостійкості;

– запровадження безпеки мережі;

– розробка системи IoT пристроїв системи пожежного попередження.

Висуваються вимоги що до розробити гнучкої структури мережі фірми, передбачити режими швидкого оновлення оперативної інформації на мережевих пристроях, а так само опрацювати питання забезпечення необхідного рівня захисту даних та відмовостійкості мережі на усіх можливих рівнях.

В цій мережі поставлено задача по створенню систему використання розумних пристроїв з можливістю відстеження станів системи пожежної безпеки за допомогою технології 3G/4G для «Відділ технічної підтримки Офіс Киев».

Також були поставлені такі здачі при реалізації цієї системі такі як:

– налаштування серверів таких як DNS та IoT для віддаленого підключення до виконуючих вистроїв;

– забезпечити DHCP сервіс для кожної с підмереж таких як «Мережа розумних пристроїв в LAN 5» та «Мережа віддаленого доступу до розумних пристроїв»;

– налаштування сценаріїв пристроями у разі спрацювання датчиків пожежної безпеки;

– реалізувати систему пожежної безпеки в яку входять два датчики вогню та датчик диму як головні компоненти;

– налаштувати контролер MCU та написати програмний додаток на мові Python.

Також висунуто наступний сценарій до функціоналу пожежної безпеки а саме за наявністю вогню в кімнаті необхідно вмикати розприскувач на 1000 с, відкривати вікно та вмикати сирену. В приміщенні за сигналом датчика диму та детектору вогню вмикати систему туману та вентилятор. Вікно відкрити після вимкнення системи туману.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ІГРОВОЇ СУДІЇ

2.1 Технічні вимоги до КС ігрової студії «Ubisoft Ukraine (Kyiv)»

2.1.1 Вимоги до системи та компонента системи в цілому

Для створення комп'ютерної мережі для ігрової студії повинні буди розроблені основні підмережі організаційних відділів:

– підмережа відділу видавництва та продаж;

– підмережа відділу гейм-девелопмент;

– підмережа відділу сценаристів;

– підмережа відділу технічної підтримки.

Дана система призначена для управління інформаційними ресурсами вона включає в себе таку інформацію як напрацювання в сценарії, створені моделі, створені локації, заготовки арт-буків та інші матеріалів інтелектуальної власності студії які будуть створені в ході роботи.

Також висуваються вимоги по збереженню протягом 5 або більше років усіх матеріалів інтелектуальної власності компанії та забезпечення до них захищеного доступу для запобігання витоку даних та забезпечення виконаного відмовостійкого рішення в окремих сегментах мережі. Також цілодобовий доступ до серверу з мережі Інтернет. Налаштування безпеки усіх частин мережі.

Передача інформації між відділами реалізований у вигляді передачі інформації через локальну мережу, засоби телефонного зв'язку та електронну пошту, або доступу на сервер зберігання даних по проекту.

При розробці системи закласти можливість її подальшої модернізації та масштабування при мінімальних затратах часу у випадку необхідності додавання нових користувачів системи в конкретну підсистему; прискорення роботи системи шляхом нарощування обчислювальних потужності у разі збільшення навантаження. Нові робочі місця повинні бути інтегровані в

існуючу мережу і максимально використовувати наявні, власні, орендовані ресурси.

Також для підвищення пожежної безпеки створити систему розумних інтернет пристроїв для запобігання пожежі в відділі технічної безпеки яка буде задовольняти такі вимоги побудови системи IoT пристроїв.

Задача по створенню систему використання розумних пристроїв з можливістю відстеження станів системи пожежної безпеки за допомогою технології 3G/4G для «Відділ технічної підтримки Офіс Київ».

Також вирішити такі здачі при реалізації цієї системі такі як:

– налаштування серверів таких як DNS та IoT для віддаленого підключення до виконуючих вистроїв;

– забезпечити DHCP сервіс для кожної з підмереж таких як «Мережа розумних пристроїв в LAN 5» та «Мережа віддаленого доступу до розумних пристроїв»;

– налаштування сценаріїв пристроями у разі спрацювання датчиків пожежної безпеки;

– реалізувати систему пожежної безпеки в яку входять два датчики вогню та датчик диму як головні компоненти;

– налаштувати контролер MCU та написати програмний додаток на мові Python.

Також висунуто наступний сценарій до функціоналу пожежної безпеки а саме за наявністю вогню в кімнаті необхідно вмикати розприскувач на 1000 с, відкривати вікно та вмикати сирену. В приміщенні за сигналом датчика диму та детектору вогню вмикати систему туману та вентилятор. Вікно відкрити після вимкнення системи туману.

2.1.1.1 Вимоги до структури і функціонуванню ігрової студії

Створені рішення для системи будуть вимагати не менш ніж 16-х фахівців по 8 в кожному офісі з певною роллю та відповідним рівнем кваліфікації, які повинні забезпечувати:

− супроводження та підтримки на усіх етапах роботи;

− необхідний режим роботи мережі за призначенням в повному обсязі;

− контроль працездатності та відмовостійкості мережі;

− усунення негараздів роботи мережі та її відповідних компонентів;

− своєчасне налагодження під час експлуатації створеної мережі;

− доцільне та перевірене застосування оновлень програмного продукту.

2.1.1.2 Показники призначення ігрової студії

Данна система призначається для організації мережі ігрової студії «Ubisoft Kyiv» за закладеними такими вимогами як:

– відмовостійної мережі для цілодобового використання ;

– зберігання та доступність даних на серверному обладнані ;

– віддалене взаємодія працівників з робочім місцем у разі потреби;

– використання технологій для захисту мережі та інтелектуальної власності.

2.1.1.3 Вимоги до надійності в провадженій мережі

Надійність компонентів мережі забезпечується виробниками обладнання та додатковими протоколами, і програмними засобами та деяким принципами відмовостійкості, які буде застосовуватись. Забезпечення здатності швидкої заміни мережевого обладнання, яке вийшло з ладу без зупинки самої системи. Також використання безперебійного живлення серверного обкладення та дублювання їх, також доступності цілодобово.

2.1.1.4 Вимоги безпеки для ігрової студії

Компоненти мережі повинні впровадити високий рівень захисту за допомогою додаткових налаштувань. Забезпечувати доступ до серверу тільки особам які пройшли автентифікацію. Для виявлення і пригнічування дії шкідливого програмного забезпечення використовувати антивірусне програмне забезпечення або системи запобігання вторгнень таких порт

безпеки та створених облікових записів на ААА серверах. Кабельні з’єднання повинні знаходитися в прокладених кабель каналах. Повний доступ лише адміністрації та системному адміністратору, для відділів лише доступ до особистих робочих місць та зони відпочинку. Доступ до документів тільки для читання. Забезпечення усіх користувачів доступу до мережі: ім'я користувача і пароль.

2.1.1.5 Вимоги до ергономіки та технічної естетики для КС ігрової студії

Для користувача системи повинен бути зручним та інтуїтивно зрозумілим користувачам. Введення інформації повинні мати підказки щодо обов’язковості заповнення полів та формату їх заповнення. користувацька системи повинен бути орієнтований на використання клавіатури та маніпулятора «миша» (з можливістю використання тільки клавіатури, для пришвидшення введення інформації) з мінімізацією кількості дій для виконання простих операцій.

Кольорове оформлення інтерфейсу повинне бути виконане в єдиному строгому стилі. Сигналізація про помилки несанкціонованого доступу повинна супроводжуватися підказкою про подальші дії.

2.1.1.6 Вимоги до технічного обслуговування, ремонту для збереження компонентів системи ігрової студії

Уся проектована система орієнтована на використання у приміщеннях.

Данна система повинна мати напрацювання на відмову протягом 200 годин в звичайному режимі. Також чисельність співробітників та вимоги до них відповідно пункту 1.1.2.

Склад комплексу запасного мережевого обладнання складає:

– комутатор – 2 шт.;

– маршрутизатор –2 шт.;

– безперебійний блок живлення – 5 шт..

Вимоги що до зберігання резервного устаткування від подівають умовам експлуатаційного обладнання

Для запобіганню виходу з ладу обладнання потрібно виконувати такі кроки як:

– огляд обладнання раз у тиждень;

– ознайомлення зі статистикою збою, порушень на моніторинговому сервісі;

– моніторинг роботи КС в штатному темпі для виявлення несправностей;

– планові роботи с збереження конфігурації обладнання та резервування матеріалів організації;

– своєчасне обслуговування апаратної частини раз на місяць.

2.1.1.7 Вимоги до захисту інтелектуальних даних від стороннього доступу

Для запобігання утраті інтелектуальної цінності компанії використовують такі методи:

– спеціалізоване програмне забезпечення;

– відповідні безпекові налаштування на обладнанні;

– використання ліцензійного ПЗ;

– копіювання самих важливіших розробок на віддалені дата-центри;

– контроль ідентифікованих користувачів;

– захист доступу до обладнання від сторонніх осіб.

2.1.1.8 Вимоги до зберігання інформації при аваріях на підприємстві

На сервері реалізована система резервного копіювання інформації. Та виконувати резервування налаштувань обладнання у мережі для подальшого відновлення налаштованих конфігурацій або їх модифікацій.

Для забезпечення захисту інтелектуальній власності від недозволеного доступу передбачаються такі заходи:

– захист створеними паролем які знають тільки довірені особи;

– підключення до портів тільки зареєстрованих пристроїв;

– захист шифруванням для застосування віддаленого підключення;

– фіксування логауту співробітників.

2.1.1.9 Вимоги до захисту від дії зовнішніх чинників на КС

Стійкі для фіксації мережевого обладнання та корпуси робочих станцій повинні бути виконані с міцних матеріалів які витримають вагу встановленого обладнання та зовнішнього впливу на встановлені компоненти. Стійкість системи циркуляції повітря в діапазоні робочих температур від 6 до +45°С. Умови до вологості в привішені не перевищувати умови від 40% до 80%.

2.1.1.10 Вимоги до патентної чистоти

Патентна чистота комп’ютерної мережі повністю забезпечується розробниками фірмами виробниками програмних та апаратних засобів. Також забезпечується на території України

2.1.2 Вимоги до функцій які виконує КС ігрової студії

Побудована комп’ютерна мережа підприємства яка забезпечує наступних функцій:

– збір даних;

– резервування налаштувань;

– зберігання інформації;

– передача інформації у одній єдиній системі;

– аналіз даних та формування документів;

– забезпечення відмовостійкості в відділі сценаристів ;

– забезпечення системи IoT пристроїв у мережі «Відділ підтримки».

2.1.2.1 Вимоги ігрової студії до функцій підсистем

Данна система ігрової студії Ubisoft Ukraine (Kyiv) повинна забезпечити такі функції:

– зберігання розроблених цифрових товарів студії;

– отримання та обробка і збереження відповідних замовлень від клієнтів;

– додавання та видалення інформації про звернення клієнтів;

– обробка звернень клієнтів до відділу мережевої підтримки.

2.1.2.2 Вимоги ігрової студії до якості реалізації

Серверне обладнання і комп'ютерна мережа повинні забезпечувати функції виконання описані у попередніх розділах.

Вимоги для мережевого обладнання ігрової студії.

– завантаження документації згідно виконання не нижче рівня 600 надсилань протягом 2 годин;

– моніторинг стану актуальних даних за потреби;

– резервування критичних наробіток;

– повідомлення про аварійний режим роботи устаткування.

2.1.3 Вимоги до видів забезпечення КС

2.1.3.1 Вимоги до інформаційного забезпечення

Адміністрування роботи локальної мережі для наступних інформаційних систем та програмних модулів:

– системи відділення видавництва та продаж;

– системи відділу гейм-девелопмент;

– системи відділу сценаристів;

– системи відділу технічної підтримки;

– запровадження зв'язку між офісами технологією VPN;

– реалізація відмовостійких технологій у мережі сценаристів.

Також носії інформації повинні зберігати накоплену інформацію не менше 5 років. Сервери AAA повинні мати централізований доступ головним

директором відділу підтримки для внесення нових користувачі. Система моніторингу у кінці робочого дня презентує статистику роботи система та журнал помилок.

2.1.3.2 Вимоги до програмного та апаратного забезпечення ігрової студії

Технічне супроводження та надання обслуговування мережевого варіанту програмного комплексу у складі 3 серверів (сервер систем рекламного відділу та сайтів проектів ігрової студії, FTP-сервер, сервер для зберігання архівних даних), комутатора та маршрутизатора глобальної мережі, мережевих комутаторів локальної комп'ютерної мережі. Фізичний сервер – x86/x64-сумісні автоматизовані системи з такими мінімальними (min) і рекомендованими (opt) основними характеристиками: CPU: min-2.5 GHz/opt-3.2 GHz; RAM: min-4Gb/opt-8Gb; VRAM: min-100Tb/opt-200 Tb;

Також обрана апаратна частина повинна задовольняти такі вимоги:

– швидкість роботи та обробки мережевого обладнання;

– мережеві порти новині підтримувати мінімум 10мб/с або 1гб /с швидкості інтернет з'єднань;

– змога гарячої заміні;

– підтримки технологій для мережевої безпеки;

– підтримка функції агрегації каналів;

– також містка пам'ять мережевих пристроїв для запису та збереження налагоджень та образів.

2.2 Розробка інженерного рішення частини КС ігрової студії

Згідно с зазначеними планами приміщень які були опрацьовані у першому розділі розробляється структура об'єкту згідно вказаних параметрів.

Приватне підприємство має два відділення – основний офіс у Києві та офіс розробників у Одесі. Для доступу до корпоративної мережі віддаленого доступу впроваджено технологію VPN типу site to site — спосіб реалізації якої

призначений для створення захищеного віртуального тунельованого з’єднання між декількома сегментами мережі.

Всього для реалізації в мережі рівня ядра потрібно використати 5 маршрутизаторів, до яких будуть підключатися комутатори в залежності від кількості користувачів в кінцевих підрозділах.

В студії є відділ гейм-девелопменту, в який входить 3 підрозділи. Для цієї мережі використовується технології VLAN, так як це сприяє скороченню широкомовного трафіку між всіма користувачами мережі, та надає більше безпеки цій структурі.

Також для реалізації компоненту системи інтернет речах пристроїв в мережі відділу технічної підтримки використати розумні пристрої а саме: датчики диму, розприскувачі, сирену, головний контролер, та контролер розумних пристроїв. Відображення топології зображено в розділі 1.1.2.

2.2.1 Розробка топологічної фізичної схеми мережі ігрової студії

Топологія фізичного розташування мережі відображає, як обладнання розташовано в мережі на плані приміщення, де і якого типу буде розташовано кабелі, де і яке обладнання розташовано, підключення живлення обладнання мережі, яка довжина у якого кабельного з’єднання.

Базовою технологією мережі застосовують Ethernet. Застосована технологія здатна забезпечити найбільшу швидкість, надійність і якість передачі даних та найбільш вживана. На рівні доступу для під’єднання робочих груп застосовано технологію Fast Ethernet. Між маршрутизатором і комутатором технологія передачі Gigabit Ethernet.

Для кабельної структури обрано стандарт TIA/EIA-568-A та TIA/EIA-569. Кабельні з’єднання в середині приміщення виконується неекранованою крученою парою (FTP-кабель категорії 5e), таким чином надається висока надійність і швидкість передачі пакетів в поєднанні з використаними технологіями.

Між офісом Києва та Одеси відстають сягає 442,94 км. Тож щоб забезпечити з’єднання між віддаленими сегментами мережі було прийнято рішення використати посередником мережу провайдера інтернет, але для підвищення захисту виконати застосування технології VPN. В середині офісних приміщень встановлюються інтернет розетки типу RJ-45 для підключення кінцевих пристроїв до мережі.

Для забезпечення з’єднання між маршрутизаторами в офісному приміщені Києва використовується технологія передачі Serial DCE/DTE, та Gigabit Ethernet.

В офісному приміщені Києва мережеве обладнання перебуває у серверному приміщені, і так само применшення оснащене системою вентиляції і резервними блоками безперебійного живлення також там в стійках розміщено дублююче обладнання на якому проведено аналогічне налаштування як і на робочому обладнані. Також для підвищення відмовостійкості у деяких сегментах мережі а саме на рівні комутаторів Zaliznyak_Router_2, Zaliznyak_Router_4 використання протоколу HSRP та PAgP який дозволить продовжувати роботу відділу «Видавництва та продаж» у разі виникнення несправносте на рівні ядра чи на рівні доступу.

Таким чином ра рисунках 2.1 – 2.2 відображено схему фізичної топології мережі офісів Києва та Одеси.

Рисунок 2.1 – Фізична схема топології мережі «Ubisoft Kyiv»

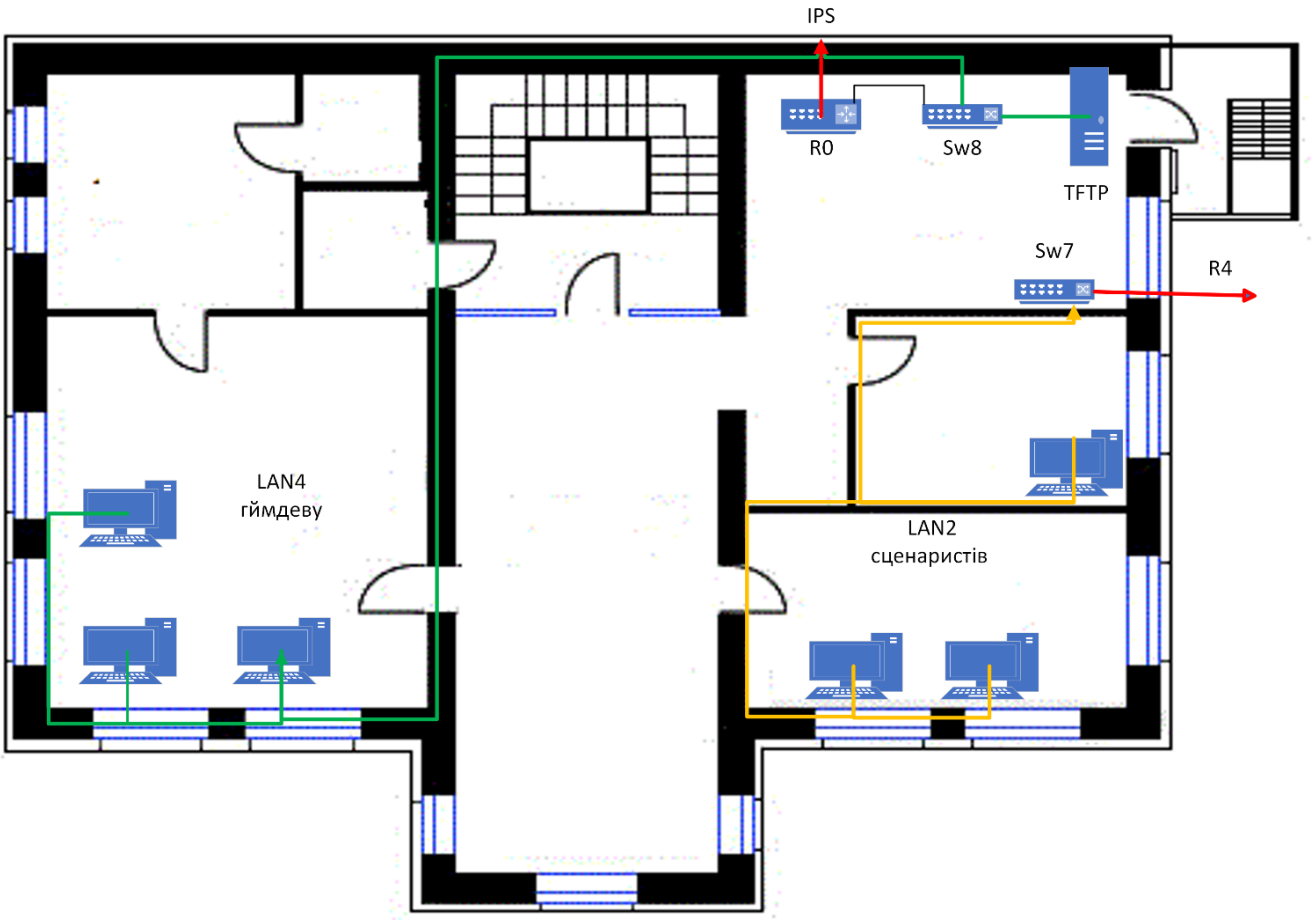

Рисунок 2.2 – Фізична схема топології мережі «Ubisoft Odesa»

2.2.2 Структурна схема комплексу технічних засобів

Структурна схема технічних засобів комп'ютерної системи підприємства «Ubisoft Ukraine (Kyiv)» наведена на рисунку 2.3.

На структурній схемі комплексу технічних засобів показані основні компоненти комп'ютерної системи підприємства «Ubisoft Ukraine (Kyiv)» з обладнанням. Відображені рівні організації мережі та підмереж, на які поділена ігрова студія.

До складу технічних засобів КМ відносяться: маршрутизатори, комутатори і мережні комунікації у вигляді кабелів, робочі станції, сервери підприємства.

Враховуючи невеликий розмір, рівень ядра і розподілу будуть реалізовані на маршрутизаторах КС підприємства «Ubisoft Ukraine (Kyiv)» між різними офісами.

Рівень ядра, де виконується комутація трафіка, складається з чотирьох маршрутизаторів, що знаходяться в мережах WLAN. Доступ до віддалених сегментів мережі «Гейм-девелопмент» і «Сценаристи» офісу Одеси та «Технічної підтримки» офісу Києва здійснено за допомогою технології VPN та NAT. Через прикордонний маршрутизатор виконується підключення до віддаленої мережі через мережу інтернет .

Рівень доступу для реалізації передачі даних складається з восьми комутаторів, що забезпечують формування підмереж та віртуальних мереж для кінцевих користувачі. Комутатор передає дані кінцевому отримувачу. Це підвищує швидкість роботи та безпеку у мережах, позбавляючи інші сегменти мережі від необхідності тратити ресурси на оброблення непотрібних даних, які їм не призначалися. У підприємства в підмережі «Гейм-девелопмент» в офісі Києва встановлено 2 комутатори. Всі користувачі цієї підмережі підключаються до неї і з використанням технології VLAN.

В підмережі «Відділ видавництва та продажу» встановлено 3 комутатори. Всі користувачі цього підрозділу для підвищення відмовостійкого з’єднання та пропускної здатності підключаються до мережі з використанням технології PAgP на комутаторах. Також для реалізації відмовостійкості використовується технологія HSRP.

Кабельна система. На рівні доступу застосована технологія передачі даних Fast Ethernet, на рівня ядра застосована технологія передачі даних Gigabit Ethernet та Serial.

Для реалізації компонента системи на інтернет речах пристроях використовуються для шлюз керування для підключення розумних пристроїв та забезпечити застосування підключення віддалених користувачів та технології 3g/4g для зв’язку з сервером моніторингу станів та сценаріїв

виконуючих пристроїв. Така система становить наявність датчику вогню та диму також розприскувачі і додаткових розумні пристрої.

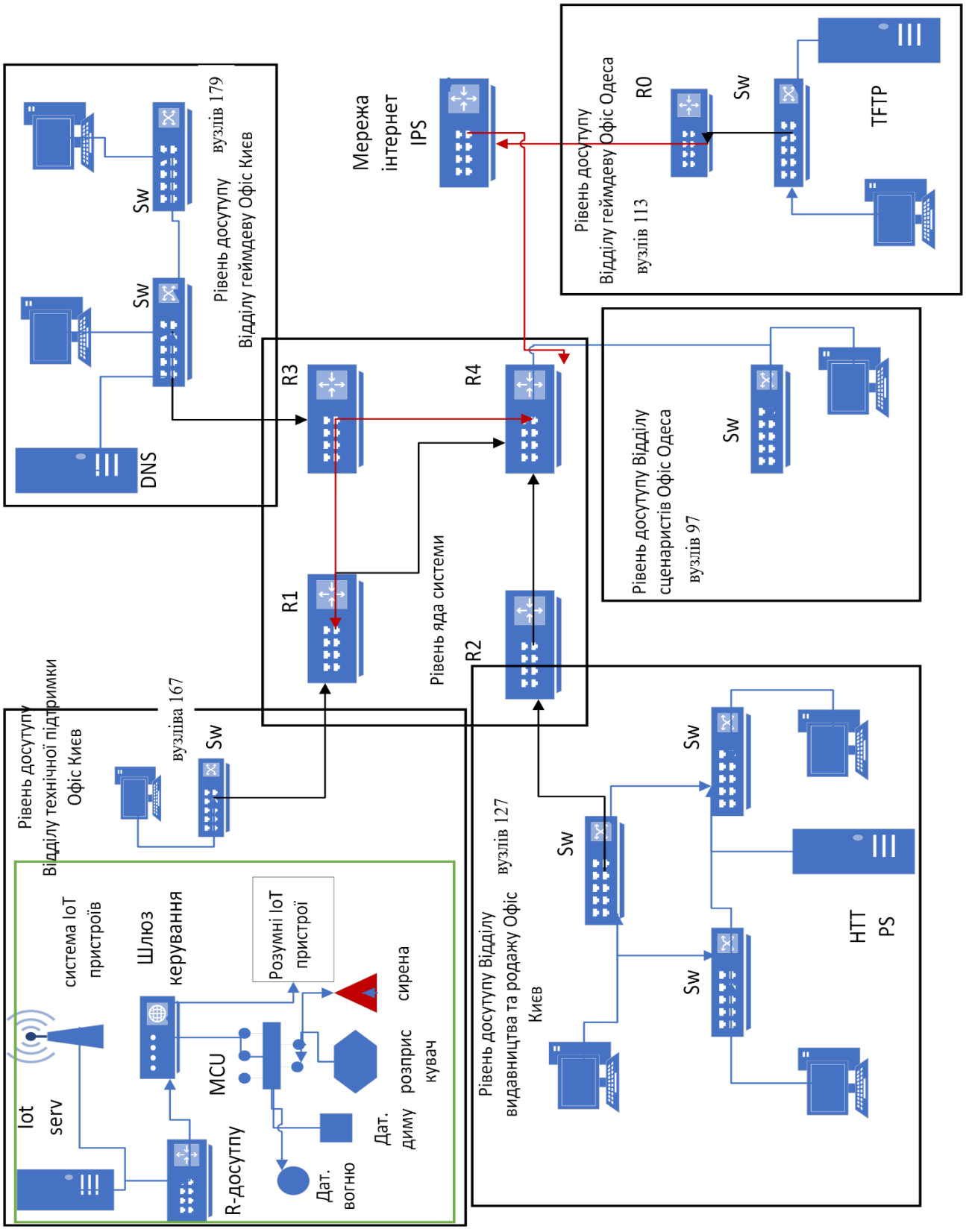

Рисунок 2.3 – Схема структурна комплексу технічних засобів «Ubisoft Ukraine (Kyiv)»

2.2.2.1 Специфікації апаратних засобів комп’ютерної системи

Для побудови мережі підприємства «Ubisoft Ukraine (Kyiv)» необхідні комутатори для зв'язку всередині локальних підмережі та маршрутизатори для з'єднання окремих підмереж та організації зв'язку між ними. В якості комутаторів локальних підмереж обраний Catalyst Cisco 2960 – це сімейство комутаторів другого рівня з фіксованою конфігурацією, яка дозволяє підключати робочі станції до мереж Fast Ethernet і Gigabit Ethernet на швидкості середовища передачі, задовольняючи зростаючі потреби в пропускній здатності на периферії мережі. Для агрегації застосовуються комбіновані гігабітні uplink-порти, які можуть об'єднуватися в єдиний канал за технологією Gigabit Ether Channel. Дана серія комутаторів орієнтована на підприємства малого і середнього бізнесу, а також філіали великих компаній для вирішення завдання реалізації рівня доступу до мережі. Сімейство Catalyst 2960 дозволяє забезпечити високу безпеку даних за рахунок вбудованого NAC, підтримки QoS і високого рівня стійкості системи.

Технічні характеристики комутатора 2960-24TC-L: порти: 24 x 10/100; 2 x 1000/SFP; підтримка PoE, 180W; пропускна здатність: 8,8 Гбіт/с; максимальна кількість VLAN: 255; об’єм ОЗУ/flash пам’яті: 64/32 Мб; протокол віддаленого адміністрування: RMON, HTTP, TFTP; спосіб автентифікації: RADIUS. Разом з комутаторами та маршрутизатором поставляється стандартна операційна система Cisco IOS.

Для реалізації рівня мережі комутації було обрано маршрутизатори з інтеграцією додаткових функціональних блоків з серії Cisco 2800.

До особливостей маршрутизаторів Cisco 2811 серії можна віднести Gigabit Ethernet порти з можливістю переходу в оптику SFP-роз'єми, і комірки розширення під модулі Service Modules. Також, є внутрішні роз'єми під модулі ISM (Internal Service Modules), Новітня технологія Services Ready Engine (SRE) забезпечує окреме, за запитом, розгортання апаратних і програмних сервісів, а підтримка VPN-мереж.

Технічні характеристики Cisco 2811: пам'ять: RAM 512 Мб; флеш пам'ять 256 Мб; мережа: технологія з'єднання провідна; протокол передачі даних Ethernet, Fast Ethernet, Gigabit Ethernet; підтримка мережі VPN; протоколи маршрутизації BGP, GRE, OSPF, DVMRP, EIGRP, IGMPv3, PIM-SM, PIM-SSM, статична IPv4 і IPv6 маршрутизація; відповідність стандартам IEEE 802.1Q, IEEE 802.1ag; інтерфейси: 2 порти 100Base-TX / 1000Base-T, роз'єм RJ-45, 1 консольний порт управління, роз'єм RJ-45, 2 слоти HWIC, 1 порт USB 4-пін USB тип A; ОС базова Cisco IOS IP Base.

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Типи, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
	Маршрутизатори				
1	Cisco 2811 ISR 4 EHWIC slots, IP Base, 2x-10/100/1000Base-T, Gigabit Ethernet, VPN	Cisco 2800	Шт.	5	Призначені для маршрутизації трафіку в локальний мережі та до віддалених сегментів
	Комутатори				
2	Cisco 2960-24TC-L 24 x 10Base-T/100Base-TX - RJ-45; 2 x Gigabit Ethernet	Cisco Catalyst 2960	Шт	31	Підключення кінцевих користувачів налаштування VLAN

Продовження таблиці 2.1

1	2	3	4	5	6
	Сервера				
3	Cisco UCS C220 M3 Rack(DBUN-C220-352)	Cisco UCS C220 M3	Шт.	3	Сервера AAA, DNS, HTTP, HTTPS
	Робочі станції				
4	Моноблок для персоналу Apple iMac 27" Retina 5K	Процесор: 6 ядерний Intel Core i7 (3.7 - 4.6 ГГц) Об’єм оперативної пам’яті: 16 ГБ Об’єм накопичувача: 512 ГБ SSD Тип оперативної пам’яті:DDR4-2400 МГц Графічний адаптер: дискретний, AMD Radeon Pro 580x, 8 ГБ відео пам’ять GDDR5	Шт.	687	Використовую ться для роботи співробітників підприємства
6	Датчик диму Mi Smart Home	Модель JTYJ-GD-01LM / BW	Шт.	1	
7	Розумне віно Vekaa38	Vekaa38	Шт.	2	
8	Датчика вогню Омега СППТА	Омега СППТА	Шт.	2	
9	Сирена EvoLogic S-03	EvoLogic S-03	Шт.	2	
10	Вентилятор SOLER&PALAU HTB-140 RC	SOLER&PALAU HTB-140 RC	Шт.	1	
11	MCU Arduino Mega 2560	Arduino Mega 2560	Шт.	1	
12	Xiaomi Mi Smart Home Multifunction Gateway 3	Xiaomi Mi Smart Home Multifunction Gateway 3	Шт.	1	
13	Стійка мережева 42U, подвійна,	42U Розміри: 2025x550x960 мм	Шт.	1	

Розглянуто згідно попереднього рисунку 2.2 розраховано необхідна кількість кабельної системи та виходячи с плану було розраховано

протяжність з’єднань склала для офісу Одеси склала 620м протяжність кабельної системи. З яких 10 метрів на з’єднання між мережевим обладнання потім 214 метрів на підключення пристроїв до в відділі сценаристів и 396 метрів для відділу геймдевелопменту.

Таблиця 2.2 – Специфікація загальної кабельної прокладки

Позиція	Найменування і технічна характеристика	Типи, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	Розетка інформаційна RJ45 кат.5E UTP, 1-порт, ITK	RJ45	Шт.	687	
2	Коннектор комп’ютерний 8P8C (RJ-45) "джек" екранований	RJ-45	Шт.	690	
3	Кабель мережевий КППЭ-ВП (100) 4х2х0,51 (FTP-cat,5E)	КППЭ-ВП (100)	м/п	1500	
4	Кабель канал 25Х16 ММ	E.NEXT	м.	1500	

2.2.3 Розрахунок інтенсивності вихідного трафіку для найбільшої локальної мережі ігрової студії

В підмережі «Відділ гейм-деву» встановлений комутатор Cisco 2960-24TC-L та маршрутизатор Cisco 2811, що об’єднують ПК працівників служб будівлі адміністративної. Вихідний трафік пересилається на маршрутизатор Cisco 2811 в лінію з пропускною здатністю 1000 Мбіт/с. Для того, щоб комутатор Cisco 2960-24TC-L не був завантаженій, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня

інтенсивність трафіку μ=204 (кадрів/с), а середня довжина повідомлення – 650 байт.

Розрахується пропускну здатність мережі офісної будівлі допускаючи, що послугами одночасно користуються 100% користувачів. Пропускна здатність мережі розраховується наступним чином. Так як в нас 2 комутатори рівня доступу, а загальна кількість користувачів дорівнює 179, то пропускна здатність мережі на рівні доступу буде дорівнювати:

$P_{р.р}$=μ*1*N*8=204*650*179*8= 189,8 (Мбіт/с), де

N – кількість вузлів в мережі.

Отримані при розрахунку результати не перевищують задані параметри мережі. Отже, перевантажень на обраному обладнанні не буде.

Комутатор рівня доступу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 1000 Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

$\mu_{вих}$=100000000/(650*8)=110000 пакетів/с

Оскільки кожне джерело виробляє в середньому 204 пакетів/с, то ми обмежені приєднанням до комутатора рівня доступу максимум:

N=11000/204=539 джерел.

Що задовольняє нашу мережу на 179 ПК.

Кожен з 179 ПК посилає потік заявок з інтенсивністю 170 кадрів/с. Інтенсивність вихідного трафіку від всіх користувачів:

λ=N*μ=179*204=36516(пакетів/с)

Коефіцієнт затримки на рівні розподілу, тобто показник завантаженості вихідного каналу зв'язку, який впливає на час стояння в черзі:

$$\rho = \frac{\lambda}{\mu_{\text{вих}}} = \frac{36516}{110000} = 0{,}33$$

Коефіцієнт зайнятості комутатора рівня розподілу:

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

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

$$T = \frac{1}{(\mu - \lambda)} = \frac{1}{110000 - 36516} = 1{,}36 * 10^{-5} c$$

Середня довжина черги:

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

Ці розрахунки можуть бути корисною при налаштуванні черг на обладнанні – в апаратурі можна вказувати максимальний розмір черги пакетів. В даному випадку в системі на обслуговуванні менше 1 пакету, значення досить умовне, воно свідчить про те, що система працює з дуже великим запасом по продуктивності

Середній час перебування пакета в черзі:

$$T_{оч} = \frac{\mathcal{L}_{\text{чер}}}{\lambda} = \frac{0{,}001}{36516} = 2{,}73 \text{ мс}$$

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

Пропускна здатність каналу:

$$\lambda = \frac{\text{пр}o\text{пускна здатність}}{d o\text{вжина кадру}} = \frac{b}{l}$$

b=λ*1=36516*650*8= 189800000 біт/с=189,8 Мбіт/с

Що задовольняє пропускній здатності вихідного каналу в 1000 Мбіт/с

3 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА ІГРОВОЇ СТУДІЇ

3.1 Розрахунок схеми адресації корпоративної мережі

Щоб спроектувати мережу ігрової студії виконати розподіл обраних адрес мережі та так використати критерії такі як доцільна витрата простору мережі з урахуванням на розширення підмереж в подальшому для забезпечення масштабування мережі. Також при проектовані було враховано блок виділених адрес для мережевих та кінцевих пристрої, кількість підмереж та кінцевих вузлів в них, підмережа повинна мати єдиний простір IP-адресації.

Розрахунок схеми IP-адресації було виконано за допомогою принципу поділу VLSM [5]. За допомогою цього методу маски змінної довжини було виконано поділ адресний простір на невеликі сегменті мережі, які відповідають поставленим розмірам відділів у ігровій студії. За допомогою VLSM була використана можливість більш доцільно використати IP-адреси та закласти запас для подальшого масштабування цих підмереж у разі потреби організації.

Використанні VLSM довжина маски підмережі залежить від числа бітів які будуть запозичені для окремої підмережі від частини ідентифікатора адреси для створення кінцевої підмережі. Тобто від «змінної» частини маски підмережі змінної довжини. VLSM дозволяє розділити простір мережі на нерівні частини [5].

Щоб виконати поділ на сегменти мережі було використано адресний простір 172.22.80.0/20. Розподіл був виконаний в відповідності с поставленими вимогами розміру підмереж організації я наявної кількості кінцевих пристроїв, які наведені в таблиці 3.1.

Таблиця 3.1 – Поділ підмереж на вузли

172.22.80.0/20				
LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
Відділ видавництва та продаж офіс Київ	Відділ сценаристів офіс Одеса	Відділ гейм девелопменту офіс Київ	Відділ гейм девелопменту Офіс Одеса	Відділ технічної підтримки офіс Київ
127	97	179	113	167

З рисунка 2.2 можна побачити, що кожна пара маршрутизаторів також з'єднується між собою окремою під мережею з адресним простором 10.1.5.0/24, та ще мережа провайдера зовнішньою адресую мережі 209.165.202.0/30. Та від віддаленого сегменту LAN 4 за адресую 64.100.13.0/30

В приграничних маршрутизаторах корпоративної мережі та зовнішнім шлюзом було виділено 2 IP-адреси кожному.

Виділений блок 172.22.80.0/20 дає можливість адресувати 4094 пристроїв. Для потреб організації потрібно 683 адрес, таким чином тільки 30% адресного простору використано.

Мережа LAN1 на 127вузли: маска 255.255.255.0 (або префікс /24). Діапазон адрес 172.22.82.1 – 172.22.82.254. Широкомовлення 172.22.82.255. Для адресації 127 пристроїв використовуємо адреси 172.22.82.1 – 172.22.82.127. Блок адрес – 172.22.82.128 – 172.22.82.254 залишається вільним. Для адресації серверів використані адреси 172.22.82.16 /24.

Мережа LAN2 на 97 вузли: маска 255.255.255.128 (або префікс /25). Діапазон адрес 172.22.83.129 – 172.22.83.254. Широкомовлення 172.22.83.255. Для адресації 97 пристроїв використовуємо адреси 172.22.83.129 – 172.22.83.226. Блок адрес – 172.22.83.227 – 172.22.83.254 залишається вільним.

Мережа LAN3 на 179 вузли: маска 255.255.255.0 (або префікс /24). Діапазон адрес 172.22.80.1 – 172.22.80.254. Широкомовлення 172.22.80.255. Для адресації 179 пристроїв використовуємо адреси 172.22.80.1 – 172.22.80.179. Блок адрес – 172.22.80.180 – 172.22.80.254 залишається вільним. Для адресації серверів використані адреси 172.22.80.16 /24.

Мережа LAN4 на 113 вузли: маска 255.255.255.128 (або префікс /25). Діапазон адрес 172.22.83.1 – 172.22.83.126. Широкомовлення 172.22.83.127. Для адресації 113 пристроїв використовуємо адреси 172.22.83.1 – 172.22.83.113. Блок адрес – 172.22.83.114 – 172.22.83.126 залишається вільним. Для адресації серверів використані адреси 172.22.83.16 /24.

Мережа LAN4 на 167 вузли: маска 255.255.255.0 (або префікс /24). Діапазон адрес 172.22.81.1 – 172.22.81.254. Широкомовлення 172.22.81.255. Для адресації 167 пристроїв використовуємо адреси 172.22.81.1 – 172.22.81.167. Блок адрес – 172.22.81.168 – 172.22.81.254 залишається вільним.

В таблиці 3.2 представлена схема IP-адресації мережі КС ігрової студії «Ubisoft Ukraine (Kyiv)», розрахована згідно принципу VLSM.

Таблиця 3.2 – Схема адресації мережі

Назва мережі	Кількість вузлів	Адреса мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
LAN 1	127	172.22.82.0	/24	172.22.82.1	172.22.82.254
LAN 2	97	172.22.83.128	/25	172.22.83.129	172.22.83.254
LAN 3	179	172.22.80.0	/24	172.22.80.1	172.22.80.254
VLAN 15	62	172.22.80.0	/26	172.22.80.1	172.22.80.62
VLAN 25	62	172.22.80.64	/26	172.22.80.65	172.22.80.126
VLAN 35	62	172.22.80.128	/26	172.22.80.129	172.22.80.190
VLAN 99	3	172.22.80.192	/29	172.22.80.193	172.22.80.198
LAN 4	113	172.22.83.0	/25	172.22.83.1	172.22.83.126
LAN 5	167	172.22.81.0	/24	172.22.81.1	172.22.81.254
WAN 1	2	10.1.5.0.0	/30	10.1.5.0.1	10.1.5.0.2
WAN 2	2	10.1.5.0.4	/30	10.1.5.0.5	10.1.5.0.6
WAN 3	2	10.1.5.0.8	/30	10.1.5.0.9	10.1.5.0.10
WAN 4	2	10.1.5.0.12	/30	10.1.5.0.13	10.1.5.0.14
WAN 5	2	10.1.5.0.16	/30	10.1.5.0.17	10.1.5.0.18

Згідно технічних вимог проектування КС ігрової студії «Ubisoft Ukraine (Kyiv)», необхідно скласти таблицю адресації мережевих пристроїв з урахуванням таких вимог [1]:

− перші можливі для використання IP-адреси призначено інтерфейсам і під інтерфейсам маршрутизаторів у LAN;

− другі з можливих IP-адрес призначаються комутаторам у кожній LAN;

− сервери налаштовано і їм привласнено IP-адреси за правилом: IP–адрес дорівнює першому можливому адресу у мережі+9+5;

− останні з використовуваних IP-адрес призначено вузлам;

− в мережах VLAN використовується адресація кінцевих пристроїв по протоколу DHCP.

У таблиці 3.3 представлена адресація всіх пристроїв мережі Державної податкової служби. Таблиця заповнюється на основі даних таблиці 3.2 та логічної топології корпоративної мережі Державної податкової служби.

Таблиця 3.3 – Адресації пристроїв мережі

Пристрій	Інтерфейс	IP-адреса	Ма-ска	Шлюз	VLAN	Інтер-фейс підклю-ченого при-строю
Відділ видавництва та продаж офіс Київ						
Zaliznyak_Router_2	G0/0	10.1.5.14	/30	-	-	Fa1/0
	G0/1	10.1.5.18	/30	-	-	Fa1/1
	G0/2	172.22.82.5	/24	172.22.82.1	-	G0/1
Zaliznyak_Switch_6	Vlan1	172.22.82.2	/24	172.22.82.1	-	G0/2
	Vlan1	172.22.82.2	/24	172.22.82.1	-	Fa0/3
Zaliznyak_Switch_5	Vlan1	172.22.82.4	/24	172.22.82.1	-	Fa0/23
Zaliznyak_Switch_4	Vlan1	172.22.82.3	/24	172.22.82.1	-	Fa0/21
PC0-5	NIC	172.22.82.7-172.22.82.9	/24	172.22.82.1	-	Fa0/1
Server HTTP	NIC	172.22.82.16	/24	172.22.82.1	-	Fa0/2
Відділ сценаристів офіс Одеса						
Zaliznyak_Router_4	Fa0/0	10.1.5.10	/30	-	-	G0/0
	Fa0/1	172.22.82.6	/24	-	-	Fa0/3
	S0/0/0	10.1.5.6	/30	-	-	S0/3/0
	S0/0/1	209.165.202.1	/30	-	-	S0/3/1
	G0/2/0	172.22.83.129	/25	-	-	G1/1/1
	Fa1/0	10.1.5.13	/30	-	-	G0/0
	Fa1/1	10.1.5.17	/30	-	-	G0/1
Zaliznyak_Switch_7	Vlan1	172.22.83.130	/25	172.22.83.129		G1/1/1

Продовження таблиці 3.3

Пристрій	Інтерфейс	IP-адреса	Ма-ска	Шлюз	VLAN	Інтер-фейс підклю-ченого при-строю
PC3-4	NIC	172.22.83.131–172.22.83.132	/25	172.22.83.129		G1/0/1-2
Відділ гейм девелопменту офіс Київ						
Zaliznyak_Router_3	G0/0.15	172.88.1	/26	-		G0/2
	G0/0.25	172.88.65	/26	-		G0/2
	G0/0.35	172.88.129	/26	-		G0/2
	G0/0.99	172.88.193	/29	-		G0/2
	S0/3/0	10.1.5.2	/30	-		S0/3/0
	S0/3/1	10.1.5.5	/30	-		S0/0/0
Zaliznyak_Switch_2	Vlan99	172.22.80.194	/29	172.22.80.193	Vlan99	G0/0
	Fa0/11	172.22.80.16	/26	172.22.80.1	Vlan15	G0/2
	Fa0/15	172.22.80.140	/26	172.22.80.129	Vlan35	NIC
	Fa0/5	172.22.80.76	/26	172.22.80.65	Vlan25	NIC
Zaliznyak_Switch_3	Vlan99	172.22.80.195	/29	172.22.80.193	Vlan99	G0/1
	Fa0/11	172.22.80.11	/26	172.22.80.1	Vlan15	NIC
	Fa0/15	172.22.80.141	/26	172.22.80.129	Vlan35	NIC
	Fa0/5	172.22.80.77	/26	172.22.80.65	Vlan25	NIC
PC8,10	NIC	172.22.80.140–172.22.80.141	/26	172.22.80.129	Vlan35	Fa0/15
PC9	NIC	172.22.80.11	/26	172.22.80.1	Vlan15	Fa0/11
Server DNS	G0/2	172.22.80.16	/26	172.22.80.1	Vlan15	Fa0/11
PC7-6	NIC	172.22.80.76–172.22.80.77	/26	172.22.80.65	Vlan25	Fa0/5
Відділ гейм девелопменту Офіс Одеса						
Zaliznyak_Router_0	Fa0/0	64.100.13.2	/30	-	-	G0/0
	Fa0/1	172.22.83.1	/25	-	-	G0/1
Zaliznyak_Switch_8	Vlan1	172.22.83.2	/25	172.22.83.1	-	Fa0/1
	Fa0/1	172.22.83.5	/25	172.22.83.1	-	NIC
	Fa0/2	172.22.83.6	/25	172.22.83.1	-	NIC
	Fa0/3	172.22.83.7	/25	172.22.83.1	-	NIC
	G0/2	172.22.83.16	/25	172.22.83.1	-	Fa0
PC14-16	NIC	172.22.83.5–172.22.83.7	/25	172.22.83.1		Fa0/1-3
Server TFTP	Fa0	172.22.83.16	/25	172.22.83.1	-	G0/2

Продовження таблиці 3.3

Пристрій	Інтерфейс	IP-адреса	Ма-ска	Шлюз	VLAN	Інтер-фейс підклю-ченого при-строю
Відділ технічної підтримки офіс Київ						
Zaliznyak_Router_1	G0/1	10.1.5.9	/30	-	-	G0/1
	G0/0	172.22.81.1	/24	-	-	Fa0/0
	S0/3/0	10.1.5.1	/30	-	-	S0/3/0
Zaliznyak_Switch_0	G0/1	172.22.81.2	/24	172.22.81.1	-	
	Fa0/1	172.22.81.3	/24	172.22.81.1	-	NIC
	Fa0/2	172.22.81.4	/24	172.22.81.1	-	NIC
	Fa0/3	172.22.81.5	/24	172.22.81.1	-	NIC
PC11-13	NIC	172.22.81.3–172.22.81.5	/24	172.22.81.1	-	Fa0/1-3

В мережі «Відділ гейм девелопменту офіс Київ», в якій створено віртуальні мережі Vlan15,25,35. Для цих віртуальних мереж на маршрутизаторі Zaliznyak_Router_3 був налаштований DHCP сервіс для динамічного видання адрес кінцевих користувачів за протоколом динамічної маршрутизації EIGRP. Тим самим користувачі в кожному з віртуальних мереж відокремлені один від одного що підвищує безпеку мережі у разі атаки.

3.2 Розробка архітектури мережі підприємства

Архітектура мережі являє основою і є фундаментом для повноцінної подальшої розробці системи. Вона складається з декількох важливих складових: мережева топологія; інфраструктура кабельного прокладення; протоколи мережевого рівня; апаратна частина [5].

Мережа організації «Ubisoft Ukraine (Kyiv)» створена по дворівневій ієрархічній моделі. За верхній рівень відповідає ядро мережі яке складається с набору маршрутизаторів, а зобов’язання нижнього рівня представлено рівнем доступу представлено комутаторами кінцевих пристроїв, таке рішення будо ухвалено виходячи с невеликого розміру мережі

На рівні ядра розташовано 4 маршрутизатори які знаходяться в будівлі Київського офісу. Мережа ігрової студії являє єдиний простір IP-адрес

172.22.80.0/20. Сегменти підмереж поділяються на маршрутизаторами на 5 підмереж.

Використовується в даній мережі IP-адреси 4 версії. Для доступу у віддалений сегмент мережі використана технологія VNP та NAT. Пограничним маршрутизатор виступає саме Zaliznyak_Router_4 для зв'язку через мережу Internet с пулом адрес 209.165.201.0/28. Для забезпечення динамічної маршрутизації всередині мережі використовується протокол EIGRP який призначений для виконання динамічної маршрутизації. На маршрутизаторі Zaliznyak_Router_3 застосована технологія інкапсуляції 802.1Q для забезпечення маршрутизації між VLAN. Для зв'язку між маршрутизаторами було застосовано адреси пулу 10.1.5.0./24. У всіх п'яти підмережах використовується протокол DHCP для присвоєння IP-адрес кінцевим пристроям у мережі. Для мережі «Відділ видавництва та продаж» для підвищення пропускної здатності мережі було застосовано технологію PAgP агрегації на канальному рівні.

Як базовою технологією мережі використовується Ethernet. На рівні доступу для під'єднання кінцевих пристроїв застосовано технологію FastEthernet. Між маршрутизатором і комутатором використовується технологія GigabitEthernet.

Зважаючи на функціонал і напрямок роботи підрозділів було розділено на п'ять підмереж зважаючи зі специфіки підрозділів. У підмережі LAN 1 «Відділ видавництва та продаж Офіс Київ» має 127 кінцевих підключень. Підмережі LAN 2 «Відділ сценаристів Офіс Одесса» має 97 кінцевих підключень. Підмережі LAN 3 «Відділ гейм–девелопменту Офіс Київ» має 179 кінцевих підключень. Підмережі LAN 4 «Відділ гейм–девелопменту Офіс Одесса» має 113 кінцевих підключень. Підмережі LAN 5 «Відділ технічної підтримки Офіс Київ» містить в собі 167 кінцевих підключень.

З огляду на підвищення безпеки підмережа Підмережі LAN 3 «Відділ гейм–девелопменту Офіс Київ» на три мережі VLAN 15 «Accounting», 25 «ResourcesDepartment»,35 «Guest». На комутаторах, де створено VLAN с

застосуванням протоколу VTP. Підмережа «Відділ видавництва та продаж» для швидкої передачі даних реалізовано протокол PAgP і тим самим забезпечується відмовостійкість цього сегменту мережі також в цій мережі використовується протокол HSRP на маршрутизаторах Zaliznyak_Router_2, Zaliznyak_Router_4. Загальна архітектура мережі наведена на рисунку 3.1.

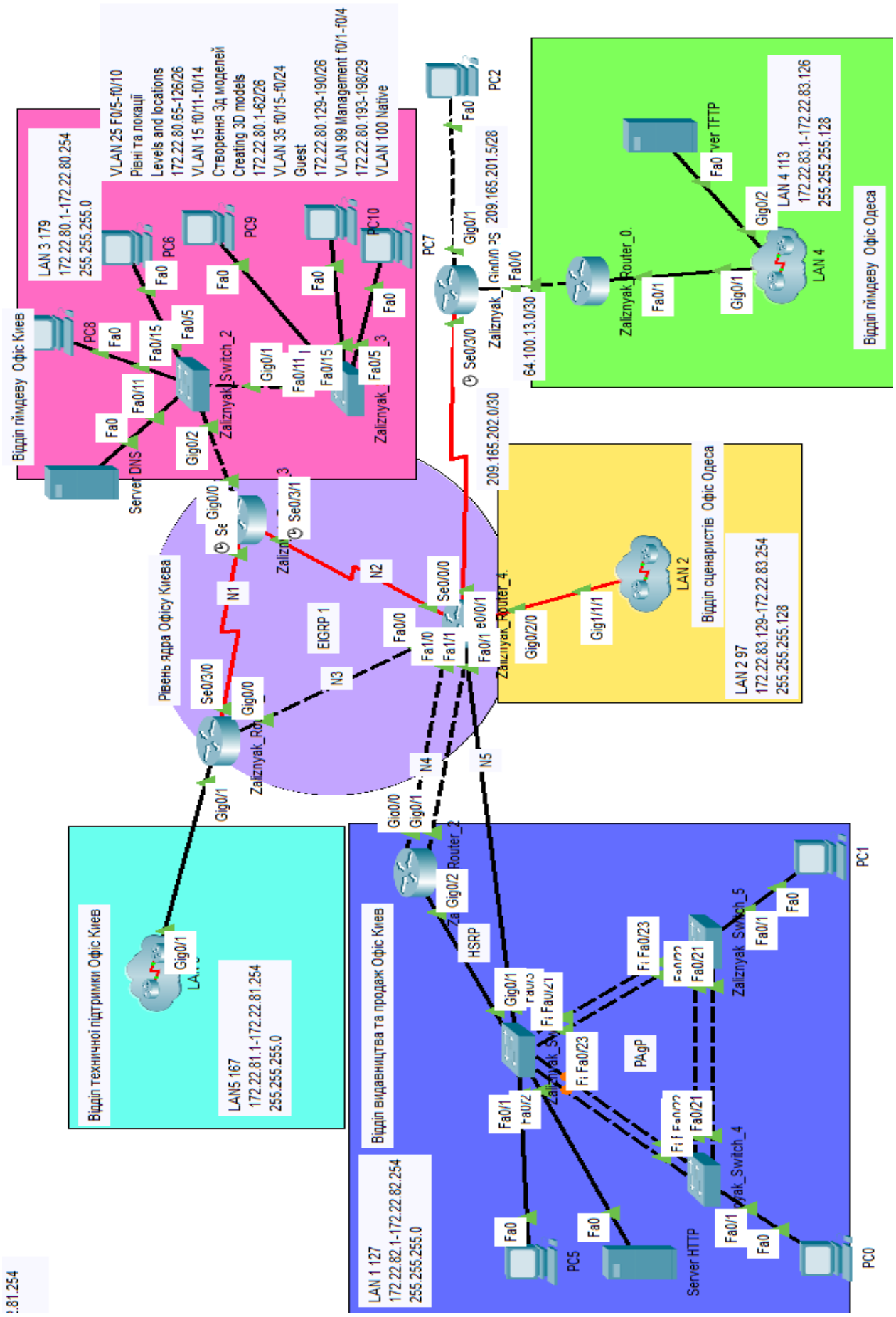

Рисунок 3.1 –Мережева архітектура ігрової студії «Ubisoft Ukraine (Kyiv)»

3.3 Налаштування та перевірка роботи комп’ютерної системи

Cisco Packet Tracer – це програмний інструмент візуального моделювання, розроблений компанією Cisco Systems, що дозволяє користувачам створювати мережеві топології та імітувати сучасні комп'ютерні мережі [2]. Програмне забезпечення дозволяє користувачам імітувати конфігурацію маршрутизаторів і комутаторів Cisco за допомогою імітаційного інтерфейсу командного рядка. Packet Tracer використовує користувальницький інтерфейс drag-and-drop, що дозволяє користувачам додавати та видаляти модельовані мережеві пристрої, як вони вважають за потрібне [2]. Програма спрямована переважно на сертифікованих користувачів Cisco Network Associate Academy як навчальний інструмент, який допомагає вивчати фундаментальні концепції CCNA.

Packet Tracer включає наступні особливості [2]:

– підтримка IOS 15;

– моделювання логічної топології: робочий простір для того, щоб створити мережі будь-якого розміру на CCNA-рівні складності;

– моделювання в режимі реального часу;

– режим симуляції; – нові роутери cisco (Cisco 4331, Cisco 4321, Cisco 2911);

– підтримка HSRP;

– BGP конфігурації;

– HWIC-2T та HWIC-8A модулі;

– моделювання фізичної топології: більш зрозуміла взаємодія з фізичними пристроями, використовуючи такі поняття як місто, будинок, стійка;

– покращений GUI Activity Wizard і Variable Manager, необхідний для більш якісного розуміння організації мережі, принципів роботи пристрою;

– багатомовна підтримка: можливість перекладу даного програмного продукту практично на будь-яку мову, необхідну користувачеві;

– удосконалене зображення мережевого устаткування зі здатністю додавати/видаляти різні компоненти;

– наявність Activity Wizard дозволяє користувачам створювати шаблони мереж і використовувати їх надалі;

– підтримка одночасного підключення багатьох користувачів.

Додаткова функціональність Multiuser Connection дозволяє інтерактивно будувати мережу, окремі сегменти якої конфігуруються on-line різними користувачами. В PacketTracer розроблена модель спроектованої комп'ютерної мережі. Від розробленого проекту мережі модель відрізняється тим, що замість запроектованої кількості кінцевих пристроїв у локальних мережах в моделі використані тільки декілька пристроїв для демонстрації робото здатності мережі.

3.3.1 Базове конфігурування апаратної частини

Відповідно до висунутих технічних вимог проведено базове налаштування мережевих пристроїв даної комп'ютерної системи.

Зроблено базові конфігурації та додатково виконано такі налаштування [1]:

– застосувати паролі для привілейованого режиму, консолі і vty;

− зашифровано усі паролі, що зберігаються у відкритому вигляді;

− налаштування банер MOTD;

− настроєно на усіх лініях vty використання протоколу ssh і локальних облікових записів. Для достоту створено користувача Zaliznyak з паролем cisco. В якості імені домена використано назви пристроїв. Для шифрування даних створено ключ RSA завдовжки 1024 біт;

− налаштовано IPv4-адреси відповідно до таблиці 3.4;

Приклад налаштування на Zaliznyak_Router_4.

Router>en

Router# configure terminal

Router(config)#hostname Zaliznyak_Router_4

Zaliznyak_Router_4 (config)#username Zaliznyak password cisco

//створення локального користувача

Zaliznyak_Router_4 (config)# ip domain-name Zaliznyak_Router_4 //присвоєння доменного ім'я

Zaliznyak_Router_4 (config)# banner motd #If you are not a network administrator, login is prohibited# //створення повідомлення при авторизації

Zaliznyak_Router_4 (config)# line con 0

Zaliznyak_Router_4 (config-line)# password cisco //присвоєння пароля на консоль

Zaliznyak_Router_4 (config-line)# login

Zaliznyak_Router_4 (config-line)#line vty 0 4

Zaliznyak_Router_4 (config-line)#password cisco //присвоєння пароля на лінії

Zaliznyak_Router_4 (config-line)#login

Було виконано даним блоком команд: перейменування пристрою; створення локального користувача з його паролем; створення доменного імені пристрою; створення банерного повідомлення при захищеність при вході до пристрою; захист паролем входу до пристрою при підключеннях консольно.

За технічними вимогами, на лініях VTY виконано налаштування протоколу SSH.

SSH –це протокол прикладного рівня, що дозволяє виконувати віддалене та шифроване підключення до обладнання.

Zaliznyak_Router_4 (config-line)#line vty 0 4

Zaliznyak_Router_4 (config-line)#password cisco

Zaliznyak_Router_4 (config-line)#login

Zaliznyak_Router_4 (config-line)#transport input ssh // застосування протокол ssh

Zaliznyak_Router_4 (config)#interface g0/2/0 //використання інтересу

Zaliznyak_Router_4 (config-if)# ip address 172.22.83.129 255.255.255.128 //призначення адреси на інтерфейс

Так само згідно таблиці 3.5 біло виконано налаштування IP-адрес інтерфейсах. Базове налаштування усіх інших пристроїв було виконано аналогічно та наведено в Додаткові А.

3.3.2 Опрацювання налаштувань маршрутизатора обладнання

Відповідно поставлених задач в мережі ігрової студії «Ubisoft ukraine» використано протокол динамічної маршрутизації EIGRP 1. 1 – це номер автономної системи, являє собою сукупність мереж які знаходяться в одній області адміністративного керування, що забезпечує загальну маршрутизацію в мережі.

Протокол динамічної маршрутизації під назвою EIGRP або (Enhanced Interior Gateway Routing Protocol) являє собою пропріетарний протокол компанії Cisco. Переваги EIGRP на відміну від протоколу RIP і IGRP закладаються в тому шо це модифікована версія протоколу IGRP[2].

Як і RIP, IGRP відомий як дистанційно-векторний протокол, але в порівнянні з ним він має покращені характеристики розрахунку оптимального шляху до точки призначення. Метрики IGRP ґрунтуються на таких параметрах як затримка та смуга пропускання, в той же час для протоколу RIP важливим є довжина маршруту, виражена в «хопах», або кількості вузлів на шляху прямування. EIGRP протокол включає в себе алгоритм, який часто застосовується в покращених протоколах маршрутизації, які працюють за принципами «стану каналу». EIGRP використовує оптимізований в порівнянні з RIP і IGRP метод запобігання петель в мережі, забезпечуючи 100-відсоткову відсутність створення петель [2]. Важлива перевага EIGRP – це висока масштабованость і висока швидкість збіжності мережі. Підтримка CIDR безкласової адресації і VLSM маска підмережі змінної довжини, та впровадження використання досконалішого алгоритму DUAL, для визначення якості маршруту.

Для кожного маршрутизатора оголошуються безпосередньо підключені мережі до нього та відключається поширення оновлень маршрутизації на інтерфейси у локальні мережі.

На Zaliznyak_Router_4 налаштований маршрут за замовчуванням в інтернет (ISP) і поширене його через оновлення маршрутизації.

Налаштування протоколу EIGRP на маршрутизаторі командою:

Zaliznyak_Router_4 (config)#router eigrp 1

Протоколу потрібно об’явити мережі, підключені до маршрутизатора.

Zaliznyak_Router_4 (config-router)#network 10.1.5.10 0.0.0.3

Zaliznyak_Router_4 (config-router)# network 10.1.5.13 0.0.0.3

Zaliznyak_Router_4 (config-router)# network 10.1.5.17 0.0.0.3

Zaliznyak_Router_4 (config-router)# network 10.1.5.6 0.0.0.3

Zaliznyak_Router_4 (config-router)# network 172.22.83.129 0.0.0127

Zaliznyak_Router_4 (config-router)# network 209.165.202.1 0.0.0.3

Перевірка таблиці маршрутизації наведено на рисунках 3.3 – 3.7. Кожний маршрутизатор окрім безпосередньо підключених мереж позначено символом «C» має відомості про всі віддалені мережі, а отримані мережі за протоколом EIGRP з символом «D». Також мають записи маршруту за замовчуванням, який складається з восьми нулів, для підключення до маршрутизатора IPS який моделює інтернет.

```
Zaliznyak_Router_0#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 64.100.13.1 to network 0.0.0.0

     64.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       64.100.13.0/30 is directly connected, FastEthernet0/0
L       64.100.13.2/32 is directly connected, FastEthernet0/0
     172.22.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.22.83.0/25 is directly connected, FastEthernet0/1
L       172.22.83.1/32 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 64.100.13.1
```

Рисунок 3.3 – Таблиця маршрутизації на Zaliznyak_Router_0

```
Zaliznyak_Router_1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.1.5.10 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.1.5.0/30 is directly connected, Serial0/3/0
L       10.1.5.1/32 is directly connected, Serial0/3/0
D       10.1.5.4/30 [90/2172416] via 10.1.5.10, 00:04:00, GigabitEthernet0/0
C       10.1.5.8/30 is directly connected, GigabitEthernet0/0
L       10.1.5.9/32 is directly connected, GigabitEthernet0/0
D       10.1.5.12/30 [90/30720] via 10.1.5.10, 00:04:04, GigabitEthernet0/0
D       10.1.5.16/30 [90/30720] via 10.1.5.10, 00:04:04, GigabitEthernet0/0
     172.22.0.0/16 is variably subnetted, 8 subnets, 5 masks
D       172.22.80.0/26 [90/2172416] via 10.1.5.2, 00:03:59, Serial0/3/0
D       172.22.80.64/26 [90/2172416] via 10.1.5.2, 00:03:59, Serial0/3/0
D       172.22.80.128/26 [90/2172416] via 10.1.5.2, 00:03:59, Serial0/3/0
D       172.22.80.192/29 [90/2172416] via 10.1.5.2, 00:03:59, Serial0/3/0
C       172.22.81.0/24 is directly connected, GigabitEthernet0/1
L       172.22.81.1/32 is directly connected, GigabitEthernet0/1
D       172.22.82.0/24 [90/30720] via 10.1.5.10, 00:04:04, GigabitEthernet0/0
D       172.22.83.128/25 [90/5376] via 10.1.5.10, 00:04:04, GigabitEthernet0/0
D*EX 0.0.0.0/0 [170/6780416] via 10.1.5.10, 00:04:00, GigabitEthernet0/0
```

Рисунок 3.4 – Таблиця маршрутизації на Zaliznyak_Router_1

```
Zaliznyak_Router_2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.22.82.6 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
D       10.1.5.0/30 [90/2172672] via 172.22.82.6, 00:05:22, GigabitEthernet0/2
D       10.1.5.4/30 [90/2170112] via 172.22.82.6, 00:05:22, GigabitEthernet0/2
D       10.1.5.8/30 [90/28416] via 172.22.82.6, 00:05:22, GigabitEthernet0/2
C       10.1.5.12/30 is directly connected, GigabitEthernet0/0
L       10.1.5.14/32 is directly connected, GigabitEthernet0/0
C       10.1.5.16/30 is directly connected, GigabitEthernet0/1
L       10.1.5.18/32 is directly connected, GigabitEthernet0/1
     172.22.0.0/16 is variably subnetted, 8 subnets, 5 masks
D       172.22.80.0/26 [90/2172672] via 172.22.82.6, 00:05:22, GigabitEthernet0/2
D       172.22.80.64/26 [90/2172672] via 172.22.82.6, 00:05:22, GigabitEthernet0/2
D       172.22.80.128/26 [90/2172672] via 172.22.82.6, 00:05:22, GigabitEthernet0/2
D       172.22.80.192/29 [90/2172672] via 172.22.82.6, 00:05:22, GigabitEthernet0/2
D       172.22.81.0/24 [90/28672] via 172.22.82.6, 00:05:22, GigabitEthernet0/2
C       172.22.82.0/24 is directly connected, GigabitEthernet0/2
L       172.22.82.5/32 is directly connected, GigabitEthernet0/2
D       172.22.83.128/25 [90/3072] via 172.22.82.6, 00:05:22, GigabitEthernet0/2
D*EX 0.0.0.0/0 [170/6778112] via 172.22.82.6, 00:05:22, GigabitEthernet0/2
```

Рисунок 3.5 – Таблиця маршрутизації на Zaliznyak_Router_2

```
Zaliznyak_Router_3#sh ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.1.5.6 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.1.5.0/30 is directly connected, Serial0/3/0
L       10.1.5.2/32 is directly connected, Serial0/3/0
C       10.1.5.4/30 is directly connected, Serial0/3/1
L       10.1.5.5/32 is directly connected, Serial0/3/1
D       10.1.5.8/30 [90/2172416] via 10.1.5.1, 00:06:55, Serial0/3/0
                    [90/2172416] via 10.1.5.6, 00:00:05, Serial0/3/1
D       10.1.5.12/30 [90/2172416] via 10.1.5.6, 00:00:05, Serial0/3/1
D       10.1.5.16/30 [90/2172416] via 10.1.5.6, 00:00:05, Serial0/3/1
     172.22.0.0/16 is variably subnetted, 11 subnets, 5 masks
C       172.22.80.0/26 is directly connected, GigabitEthernet0/0.15
L       172.22.80.1/32 is directly connected, GigabitEthernet0/0.15
C       172.22.80.64/26 is directly connected, GigabitEthernet0/0.25
L       172.22.80.65/32 is directly connected, GigabitEthernet0/0.25
C       172.22.80.128/26 is directly connected, GigabitEthernet0/0.35
L       172.22.80.129/32 is directly connected, GigabitEthernet0/0.35
C       172.22.80.192/29 is directly connected, GigabitEthernet0/0.99
L       172.22.80.193/32 is directly connected, GigabitEthernet0/0.99
D       172.22.81.0/24 [90/2170112] via 10.1.5.1, 00:06:55, Serial0/3/0
D       172.22.82.0/24 [90/2172416] via 10.1.5.6, 00:00:05, Serial0/3/1
D       172.22.83.128/25 [90/2170112] via 10.1.5.6, 00:00:05, Serial0/3/1
D*EX 0.0.0.0/0 [170/7289856] via 10.1.5.6, 00:00:05, Serial0/3/1
```

Рисунок 3.6 – Таблиця маршрутизації на Zaliznyak_Router_3

```
Zaliznyak_Router_4#sh ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
D       10.1.5.0/30 [90/2172416] via 10.1.5.9, 00:07:54, FastEthernet0/0
C       10.1.5.4/30 is directly connected, Serial0/0/0
L       10.1.5.6/32 is directly connected, Serial0/0/0
C       10.1.5.8/30 is directly connected, FastEthernet0/0
L       10.1.5.10/32 is directly connected, FastEthernet0/0
C       10.1.5.12/30 is directly connected, FastEthernet1/0
L       10.1.5.13/32 is directly connected, FastEthernet1/0
C       10.1.5.16/30 is directly connected, FastEthernet1/1
L       10.1.5.17/32 is directly connected, FastEthernet1/1
     172.22.0.0/16 is variably subnetted, 9 subnets, 5 masks
D       172.22.80.0/26 [90/2172416] via 10.1.5.5, 00:00:59, Serial0/0/0
D       172.22.80.64/26 [90/2172416] via 10.1.5.5, 00:00:59, Serial0/0/0
D       172.22.80.128/26 [90/2172416] via 10.1.5.5, 00:00:59, Serial0/0/0
D       172.22.80.192/29 [90/2172416] via 10.1.5.5, 00:00:59, Serial0/0/0
D       172.22.81.0/24 [90/28416] via 10.1.5.9, 00:07:54, FastEthernet0/0
C       172.22.82.0/24 is directly connected, FastEthernet0/1
L       172.22.82.6/32 is directly connected, FastEthernet0/1
C       172.22.83.128/25 is directly connected, GigabitEthernet0/2/0
L       172.22.83.129/32 is directly connected, GigabitEthernet0/2/0
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/30 is directly connected, Serial0/0/1
L       209.165.202.1/32 is directly connected, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Рисунок 3.7 – Таблиця маршрутизації на Zaliznyak_Router_4

Виходячи с таблиць маршрутизації зроблено висновок, що всі мережі присутні в конфігурації, тому топологія повністю робоча, а це свідчить про те що будь який сегмент мережі може відправити повідомлення до іншого і воно буде виконано успішно.

Також на декількох комутаторах для підвищення відмовостійкості використовується протоко HSRP. Призначений щоб досягти практично 100% доступності та відмови стійкості першого хопу від відправника «маршрут за замовчуванням». Це досягається шляхом використання у двох або більше маршрутизаторів або комутаторів третього рівня однієї IP-адреси і MAC-адреси так званого віртуального маршрутизатора[2]. Така група називається HSRP-групою. Налаштування виконані на *Zaliznyak_Router_4 та Zaliznyak_Router_2*.

Zaliznyak_Router_4 (config)#int fa0/1

Zaliznyak_Router_4 (config)# int add 172.22.83.6 255.255.255.128

Zaliznyak_Router_4 (config-if)#standby version 2

Zaliznyak_Router_4 (config-if)#standby 1 ip 172.22.82.1

Zaliznyak_Router_4 (config-if)#standby 1 preempt

Zaliznyak_Router_2 (config)#int g0/2

Zaliznyak_Router_2 (config)# int add 172.22.83.5 255.255.255.128

Zaliznyak_Router_2 (config-if)#standby version 2

Zaliznyak_Router_2 (config-if)#standby 1 ip 172.22.82.1

Zaliznyak_Router_2 (config-if)#standby 1 preempt

Zaliznyak_Router_2 (config-if)#standby 1 priority 105

3.3.3 Налаштування мережі імітованого провайдера

Відповідно висунутим технічним вимогам для впровадження корпоративної мережі заданий блок адрес з визначеним діапазоном приватних адрес. Для надання доступу співробітникам організації вихід до мережі

Internet, на прикордонному маршрутизаторі було застосовано технологію NAT.

NAT – це відповідний механізм зміни мережевого адресу в заголовках IP датаграм, поки вони проходять через маршрутизуючий пристрій з метою зміни одного адресного простору в інший [2]. Завдяки NAT можна, використовуючи кілька зовнішніх IP-адрес, виданих мережевим провайдером. Маршрутизовані пристрої дозволяють виконувати трансляцію адрес, завдяки чому їх використовують для підключення невеликих мереж до мережі інтернет, використовуючи одну зовнішню IP-адресу.

NAT на прикордонному маршрутизаторі виконано налаштування згідно з вимогами роботи[1]:

− пул адрес: з 209.165.200.5 по 209.165.200.30;

− 172.22.82.16/25 адреса Server HTTP;

− номер списку доступу: 5;

− ім'я пулу: Internet.

NAT на Zaliznyak_Router_IPS.

Zaliznyak_Router_IPS (config)#access-list 5 permit 209.165.201.0 0.0.0.15 //список доступу, що дозволяє внутрішньої мережі

Zaliznyak_Router_IPS (config)# ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224// пул для динамічного виділення інтернет адрес

Zaliznyak_Router_IPS (config)# ip nat inside source list 5 pool Internet// підміна адреси внутрішньої мережі на інтернет адреси згідно з списком контролю доступу

Zaliznyak_Router_IPS (config)#interface Serial0/3/0

Zaliznyak_Router_IPS (config-if)#ip nat outside // коли пакет надходить на порт то відбувається заміна інтернет адреси на адресу внутрішної мережі при проходженні через порт

Zaliznyak_Router_IPS (config-if)#interface G0/1

Zaliznyak_Router_IPS (config-if)#ip nat inside // коли пакет надходить на порт то відбувається заміна адреси внутрішньої мережі на інтернет адресу

Для перевірки роботи NAT відобразим таблицю перетворювань на рисунку 3.8.

NAT Table for Zaliznyak_Router_IPS

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.200.5:24	209.165.201.5:24	10.1.5.18:24	10.1.5.18:24
icmp	209.165.200.5:25	209.165.201.5:25	172.22.82.1...	172.22.82.16:25
icmp	209.165.200.5:26	209.165.201.5:26	10.1.5.9:26	10.1.5.9:26
icmp	209.165.200.5:27	209.165.201.5:27	172.22.81.3:27	172.22.81.3:27

Рисунок 3.8 – Таблиця перетворювань NAT на Zaliznyak_Router_IPS

3.3.4 Налаштування приватної мережі з використанням IPsec site-to-site VPN

Налаштувати віртуальну приватну мережу site-to-site VPN з використанням IPsec для трафіку, що проходить між офісом у Києві та офісом у Одесі через Internet.

Налаштування на Zaliznyak_Router_4:

Налаштування параметрів ISAKMP.

Zaliznyak_Router_4 (config)#crypto isakmp policy 10

Zaliznyak_Router_4 (config-isakmp)#encryption 3des

Zaliznyak_Router_4 (config-isakmp)#hash md5

Zaliznyak_Router_4 (config-isakmp)#authentication pre-share

Zaliznyak_Router_4 (config-isakmp)#group 2

Zaliznyak_Router_4 (config-isakmp)#exit

Zaliznyak_Router_4 (config)#crypto isakmp key cisco address 64.100.13.2

Zaliznyak_Router_4 (config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac

Створення ACL для визначення дозволених мереж.

Zaliznyak_Router_4 (config)# ip access-list extended V5-VPN

Zaliznyak_Router_4 (config-ext-nacl)# permit ip 172.22.82.0 0.0.0.255 172.22.83.0 0.0.0.127

Zaliznyak_Router_4 (config-ext-nacl)# permit ip 172.22.83.128 0.0.0.127 172.22.83.0 0.0.0.127

Zaliznyak_Router_4 (config-ext-nacl)# permit ip 172.22.80.0 0.0.0.255 172.22.83.0 0.0.0.127

Zaliznyak_Router_4 (config-ext-nacl)# permit ip 172.22.81.0 0.0.0.255 172.22.83.0 0.0.0.127

Створення крипто мапи шляху для VPN.

Zaliznyak_Router_4 (config)# crypto map CMAP 10 ipsec-isakmp

Zaliznyak_Router_4 (config-crypto-map)# set peer 64.100.13.2

Zaliznyak_Router_4 (config-crypto-map)# set transform-set TS

Zaliznyak_Router_4 (config-crypto-map)# match address V5-VPN

Присвоєння крипто мапи до зовнішнього інтерфейсу мережі.

Zaliznyak_Router_4 (config)#interface Serial 0/0/1

Zaliznyak_Router_4 (config-if)#crypto map VPN-MAP

Перевірка роботи VPN наведено в рисунках 3.9 – 3.10.

```
Zaliznyak_Router_4#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
64.100.13.2     209.165.202.1   QM_IDLE           1088    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Рисунок 3.9 – Демонстрація VPN тунелям між офісами

```
Zaliznyak_Router_4#show crypto ipsec sa

interface: Serial0/0/1
    Crypto map tag: CMAP, local addr 209.165.202.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.22.82.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.22.83.0/255.255.255.128/0/0)
   current_peer 64.100.13.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 0
   #pkts decaps: 22, #pkts decrypt: 22, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.202.1, remote crypto endpt.:64.100.13.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
     current outbound spi: 0xE39AC28B(3818570379)

     inbound esp sas:
      spi: 0x2EA04257(782254679)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4525504/3253)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:
```

Рисунок 3.10 – Робота IPSec SA для Zaliznyak_Router_4

3.3.5 Перевірка роботи КС ігрової студії

Для демонстрації роботи SSH підключення з командного рядка PC8 з підмережі «Відділ гейм девелопменту офіс Київ» маршрутизатора Zaliznyak_Router_3 від користувача Zaliznyak з паролем cisco використано команду:

ssh -l Zaliznyak 172.22.80.1

Для демонстрації роботи доступності пристроїв мережі застосовано команду ping на робочих станціях з різних підмереж, с PC5 з підмережі «Відділ видавництва та продаж Офіс Київ» пінгує станцію PC6 з підмережі «Відділ гейм девелопменту офіс Київ».

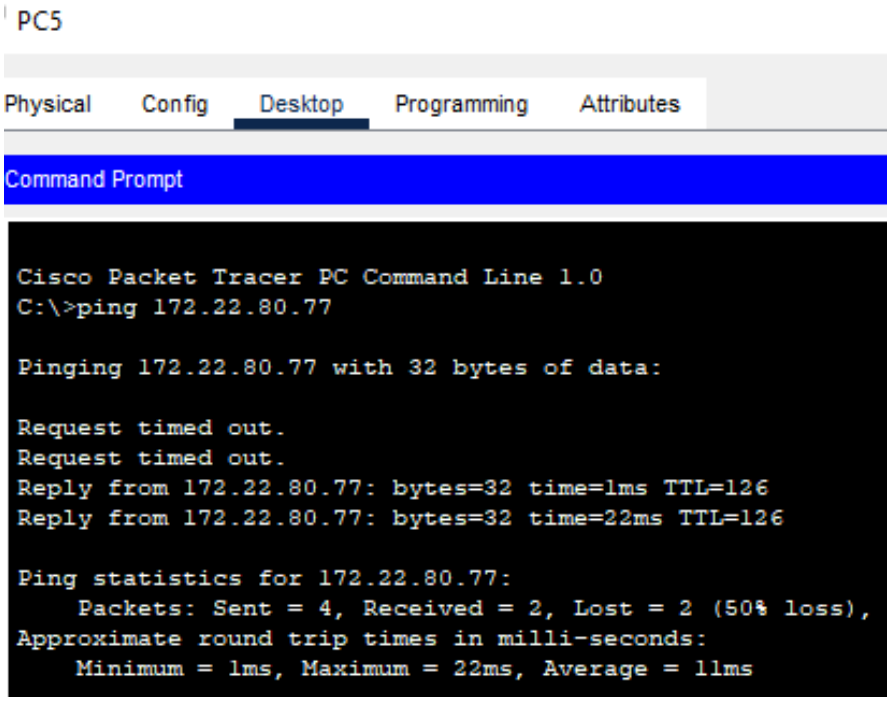

Рисунок 3.11 – Результат роботи доступності кінцевих пристроїв мережі

Згідно вимог мережі VLAN кінцеві користувачі отримують мережеві налаштування за протоколом DHCP. Для цього налаштовано маршрутизатор Zaliznyak_Router_3 та підтримку DHCP сервісу для динамічного виділення адрес.

DHCP – це протокол який дозволяє комп'ютерам автоматично отримувати виділений пул IP-адресу та інші параметри, необхідні для роботи в мережі. Протокол DHCP виконує роботу за схемою клієнт-сервер[2]. Під час запуску системи робоча станція, який являє себе DHCP-клієнтом, відправляє в мережу запит на отримання IP-адреси. DHCP-сервер відповідає на запит і відправляє повідомлення-відповідь, яка містить IP-адресу і інші конфігураційні параметри. При цьому налаштований в проекті сервер DHCP працює в режимі динамічного розподілу на сервері DHCP присвоєний діапазон IP-адрес і кожна клієнтська робоча станція в мережі повинен запросити IP-адресу від DHCP-сервера [2].

Відповідно до вимог поставленої задачі виконано налаштування маршрутизаторів, що в свою чергу здійснює маршрутизацію між VLAN і виступає в якості DHCP-серверу для мереж VLAN. Для неї створені пули

DHCP під назвою pollvlan15,25,35. Виключені з пулу перші 10 адрес. Для кожного пулу вказана адреса DNS-сервера і шлюз за замовчуванням.

Налаштування маршрутизації між VLAN за допомогою технології інкапсуляції на маршрутизаторі Zaliznyak_Router_3:

Zaliznyak_Router_3 (config)#interface GigabitEthernet0/0

Zaliznyak_Router_3 (config-if)#no shutdown

Zaliznyak_Router_3 config-if)#interface GigabitEthernet 0/0.15

Zaliznyak_Router_3 (config-if)#encapsulation dot1Q 15

Zaliznyak_Router_3 (config-if)#ip address 172.22.80.1 255.255.255.192

Zaliznyak_Router_3 config-if)#interface GigabitEthernet 0/0.25

Zaliznyak_Router_3 (config-if)#encapsulation dot1Q 25

Zaliznyak_Router_3 (config-if)#ip address 172.22.80.65 255.255.255.192

Zaliznyak_Router_3 config-if)#interface GigabitEthernet 0/0.35

Zaliznyak_Router_3 (config-if)#encapsulation dot1Q 35

Zaliznyak_Router_3 (config-if)#ip address 172.22.80.129 255.255.255.192

Zaliznyak_Router_3 config-if)#interface GigabitEthernet 0/0.99

Zaliznyak_Router_3 (config-if)#encapsulation dot1Q 99

Zaliznyak_Router_3 (config-if)#ip address 172.22.80.193 255.255.255.248

Перевірка динамічного присвоєння виділених IP-адрес вузлам за протоколом DHCP, які знаходяться у VLAN–3, і виконана перевірка роботи сервісу представлено рисунок 3.13.

Для виконання перевірки роботи мережі виконано команду ping на робочій станції для удостовірення налаштування безпечного віддаленого доступу до активних мережних пристроїв, перевірку зв'язку між вузлами з різних VLAN при автоматичному призначенні адрес рисунок 3.12.

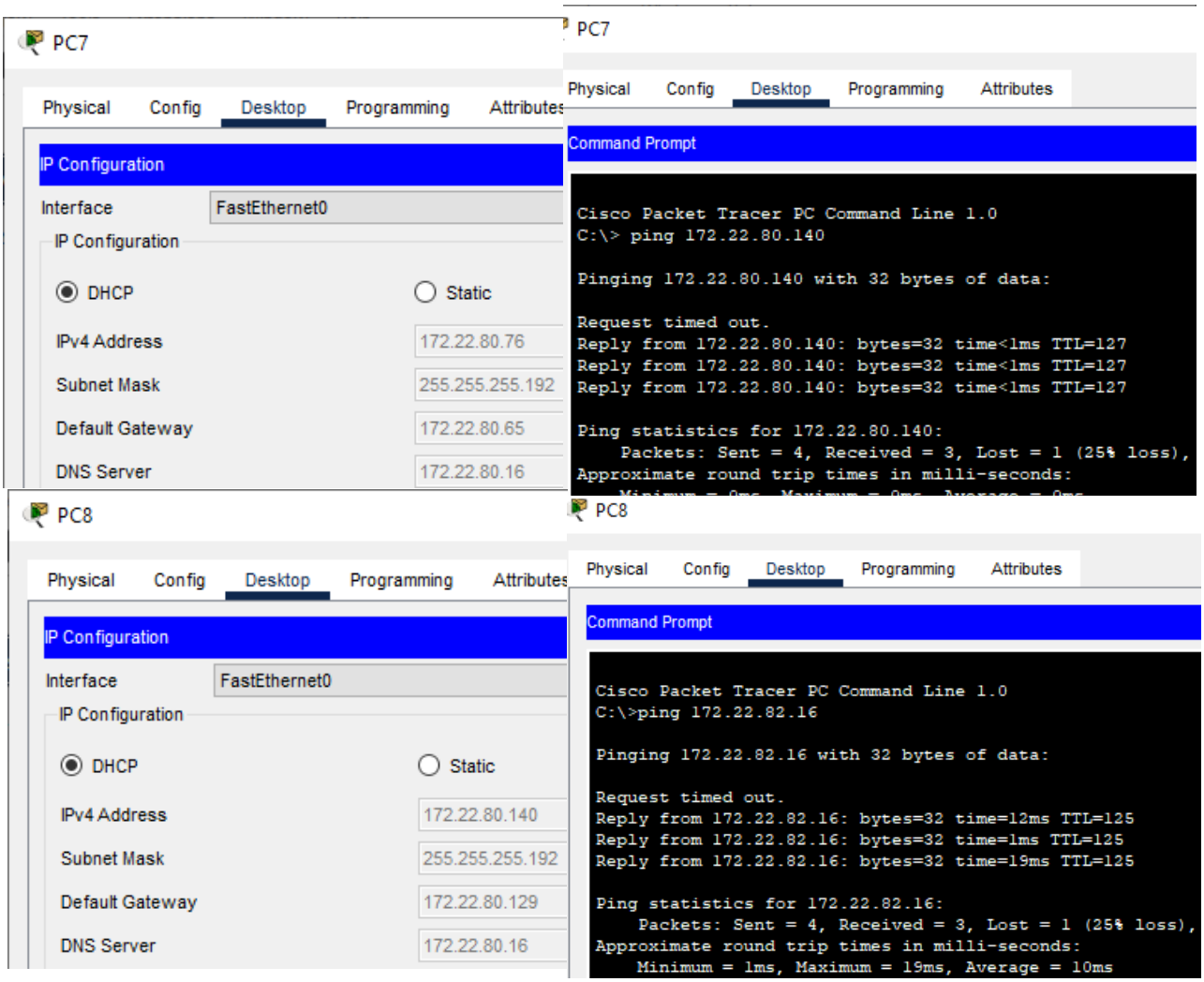

Рисунок 3.12 – Перевірка зв'язку між пристроями з різних VLAN при адресації через DHCP

```
Zaliznyak_Router_3#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.22.80.11     000C.CF04.3E5D            --                    Automatic
172.22.80.76     000B.BED6.8092            --                    Automatic
172.22.80.77     0040.0BDB.4CEC            --                    Automatic
172.22.80.140    00E0.F94A.1AA5            --                    Automatic
172.22.80.141    0040.0B8B.3BB4            --                    Automatic
```

Рисунок 3.13 – Таблиця призначення IP-адрес вузлам за протоколом DHCP для Zaliznyak_Router_3

3.4 Впровадження відмовостійскості на канальному рівні та мережевому рівні для мережі LAN1

Згідно висунутих вимог для мережі LAN 1 потребує впровадження методів для підвищення відмовостійкості мережі тому були впроваджено деякі налаштування які наведені нижче у розділах.

3.4.1 Налаштування об’єднання каналів за технологією PAgP

Реалізація відмовостійкості на канальному рівні потрібна для запобігання обриву з’єднань у силу різних технічних чи фізичних обставин. Тому було застосовано протокол Port Aggregation Protocol (PAgP) – протокол пропріетарної розробки компанії Cisco Systems, служить для автоматизування об’єднання декількох фізичних портів комутатора в один логічний. Таке об'єднання дозволяє збільшувати пропускну здатність і підвищити відмовостійкості та надійність канального рівня. Агрегування каналів може бути налаштоване між двома комутаторами, комутатором і маршрутизатором, між комутатором і хостом [2].

Налаштування EtherChannel на Zaliznyak_Switch_6:

Zaliznyak_Switch_6 (config)#interface range f0/23-24

Zaliznyak_Switch_6 (config-if-range)#switchport mode trunk

Zaliznyak_Switch_6 (config-if-range)#channel-group 1 mode auto

Zaliznyak_Switch_6 (config)#interface Port-channel 1.

Zaliznyak_Switch_6 (config)#switchport mode trun

Zaliznyak_Switch_6 (config)#interface range f0/21-22

Zaliznyak_Switch_6 (config-if-range)#switchport mode trunk

Zaliznyak_Switch_6 (config-if-range)#channel-group 1. mode auto

Zaliznyak_Switch_6 (config)#interface. Port-channel 1.

Zaliznyak_Switch_6 (config)#switchport mode trun

Налаштування EtherChannel на Zaliznyak_Switch_5:

Zaliznyak_Switch_5 (config)#interface. range f0/23-24

Zaliznyak_Switch_5 (config-if-range)#switchport mode trunk

Zaliznyak_Switch_5 (config-if-range)#channel-group 1. mode auto

Zaliznyak_Switch_5 (config)#interface Port-channel 1.

Zaliznyak_Switch_5 (config)#switchport mode trun

Zaliznyak_Switch_5 (config)#interface range f0/21-22

Zaliznyak_Switch_5 (config-if-range)#switchport mode trunk

Zaliznyak_Switch_5 (config-if-range)#channel-group 1 mode auto

Zaliznyak_Switch_5 (config)#interface Port-channel 1

Zaliznyak_Switch_5 (config)#switchport mode trun

Налаштування EtherChannel на Zaliznyak_Switch_4:

Zaliznyak_Switch_4 (config)#interface range f0/23-24

Zaliznyak_Switch_4 (config-if-range)#switchport mode trunk

Zaliznyak_Switch_4 (config-if-range)#channel-group 1 mode auto

Zaliznyak_Switch_4 (config)#interface Port-channel 1.

Zaliznyak_Switch_4 (config)#switchport mode trun

Zaliznyak_Switch_4 (config)#interface range f0/21-22

Zaliznyak_Switch_4 (config-if-range)#switchport mode trunk

Zaliznyak_Switch_4 (config-if-range)#channel-group 1. mode auto

Zaliznyak_Switch_4 (config)#interface Port-channel 1.

Zaliznyak_Switch_4 (config)#switchport mode trun

Для перевірки роботи протоколу PAgP застосуємо команду Rukavytsia_Sw0.1#sh etherchannel summary.

Результат роботи команди показано на рисунку 3.14, що налаштування протоколу PAgP виконані вірно.

```
Zaliznyak_Switch_6#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------

1      Po1(SU)           PAgP   Fa0/21(P) Fa0/22(P)
2      Po2(SU)           PAgP   Fa0/23(P) Fa0/24(P)
```

Рисунок 3.14 – Демонстрація PAgP

3.4.2 Налаштування HSRP для LAN 1

Згідно вимог на декількох комутаторах для підвищення відмовостійкості використовується протоко HSRP. Цей призначений для того, щоб досягти практично 100% доступності та відмовостійкості першого хопу від відправника «маршрут за замовчуванням» [2]. Це досягається шляхом використання у двох або більше маршрутизаторів або комутаторів третього рівня однієї IP-адреси і MAC-адреси так званого віртуального маршрутизатора. Така група називається HSRP-групою. Налаштування виконані на *Zaliznyak_Router_4 ma Zaliznyak_Router_2.*

Zaliznyak_Router_4 (config)#int fa0/1

Zaliznyak_Router_4 (config)# int add 172.22.83.6 255.255.255.128

Zaliznyak_Router_4 (config-if)#standby version 2

Zaliznyak_Router_4 (config-if)#standby 1 ip 172.22.82.1

Zaliznyak_Router_4 (config-if)#standby 1 preempt

Zaliznyak_Router_2 (config)#int g0/2

Zaliznyak_Router_2 (config)# int add 172.22.83.5 255.255.255.128

Zaliznyak_Router_2 (config-if)#standby version 2

Zaliznyak_Router_2 (config-if)#standby 1 ip 172.22.82.1

Zaliznyak_Router_2 (config-if)#standby 1 preempt

Zaliznyak_Router_2 (config-if)#standby 1 priority 105

3.5 Захист інформації в комп'ютерній системі від небажаного доступу

3.5.1 Розробка методів для захисту інформації в комп'ютерній системі

Для захисту інформації в комп'ютерній системі від небажаного доступу з метою крадіжки інтелектуальної власності компанії впроваджено і описуються такі методи[1]:

– налаштування мереж VLAN і маршрутизації між ними;

– на портах комутаторів, підключених до серверів, налаштовуються функції безпеки портів;

– тільки двом унікальним пристроям був дозволений доступ до порту;

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

– маршрутизатори мережі налаштовуються на підтримку служби AAA та RADIUS-сервера.

3.5.2 Налаштування маршрутизаторів на підтримку служби AAA

Служба авторизація та автентифікації користувачів при підключені до мережевих пристроїв виконується за допомогою сервісів AAA. Це система автентифікації, авторизації і обліку підключень та подій, вона являє собою частину операційну систему IOS Cisco, служить для забезпечення користувачам безпечного віддаленого доступу до мережного обладнання Cisco [2]. Вона дозволяє централізовано керувати користувачами та доступом їх до мережевого обладнання. В ній присутні різні методи ідентифікації користувача, авторизації, а також збору і відправки інформації на сервер.

Zaliznyak_Router_1 (config)# aaa new-model.//увімкнення AAA

Zaliznyak_Router_1 (config)# #aaa authentication login default group radius local // налаштування методу автентифікації з використанням сереверу RADIUS, а якщо він недоступний, то з використанням локальної бази користувачів

Zaliznyak_Router_1 (config)# aaa authentication login SSH-LOGIN local.// налаштування методу автентифікації з використанням локальної бази користувачів

Zaliznyak_Router_1 (config)#line console 0

Zaliznyak_Router_1(config-line)#login authentication default// застосування методу аутентифікай серверу RADIUS на консольній лінії

Zaliznyak_Router_1 (config)#line vty 0 4

Zaliznyak_Router_1 (config-line)#login .authentication .SSH-LOGIN// застосування локальних облікових записів на vty-лінії

Zaliznyak_Router_1 (config)#radius-server host 172.22.80.16 auth-port 1645

Zaliznyak_Router_1 (config)#radius-server key radius123

В якості локальної облікового запису користувачів використовується Zaliznyak з паролем cisco. Так як обліковий запис на сервері RADIUS створено radius123 з паролем admin123.

Для виконання авторизації в режимі користування консолі потрібно ввести ім'я користувача та пароль, що був налаштований на сервері RADIUS.

3.5.3 Налаштування мереж VLAN

VLAN– віртуальна мережа, являє собою групу кінцевих підключень із загальним набором вимог, які взаємодіють наче вони були підключені до одного пристрою з рівня доступу, незалежно від їх фізичного місцезнаходження. Віртуальна мережі має ті ж властивості, що й фізична локальна мережа, але дозволяє кінцевим станціям, групуватися разом в об’єднаному вілани для комунікації, навіть якщо вони не знаходяться в одній фізичній мережі[2]. Таке об’єднання відбувається за допомогою програмного

забезпечення замість фізичного переміщення пристроїв. На пристроях Cisco, протокол VTP передбачає VLAN-домени для спрощення адміністрування. Відповідно до вимог підмережа «Відділ геймдеву Офіс Київ» розділяється на три підмережі VLAN, та до них ще одна підмережа для керування. Відповідно до архітектури мережі в КС ігрової студії створені мережі VLAN з присвоєним кожній з них найменувань.

Таблиця 3.4 – Назви VLAN для підмережі «Відділ геймдеву Офіс Київ»

Номер VLAN	Ім’я VLAN	Примітка
1	default	Не використовується
15	Creating 3D models	Створення 3д моделей
25	Levels and locations	Рівні та локації
35	Guest	Для гостей
99	Management	Для управління пристроями
100	Native	Власна мережа

Додатково виконані налаштування для підвищення безпеки в цій мережі [1]:

− відповідно до вимог налаштовано транкові порти і порти доступу;

− вимкнено усі невикористовувані фізичні порти комутаторів;

− на портах комутаторів, підключених до серверів, налаштовано функцію безпеки портів так щоб [1]:

– тільки двом унікальним пристроям був дозволений доступ до порту;

– MAC- адреса пристрою розпізнавалася динамічно і додавалася в поточну конфігурацію;

– при порушенні системи безпеки вирушало повідомлення, а порт залишався включеним;

− налаштовано SVI-інтерфейси на комутаторах, призначивши по таблиці 3.3 IPv4- адреси з мережі Management VLAN 99;

− налаштовано маршрутизацію між мережами VLAN.

Налаштування на Zaliznyak_Switch_2:

Об’ява VLAN:

Switch (config)#hostname Zaliznyak_Switch_2

Zaliznyak_Switch_2 (config)#vlan 15

Zaliznyak_Switch_2 (config-vlan)#name Creating_3D_models

Zaliznyak_Switch_2 (config-vlan)# vlan 25

Zaliznyak_Switch_2 (config-vlan)#name Levels_and_locations

Zaliznyak_Switch_2 (config-vlan)#vlan 35

Zaliznyak_Switch_2 (config-vlan)#name Guest

Zaliznyak_Switch_2(config-vlan)#vlan 99

Zaliznyak_Switch_2 (config-vlan)# name Management

Zaliznyak_Switch_2 (config-vlan)#vlan 100

Zaliznyak_Switch_2 (config-vlan)# name Native

Налаштування транкових каналів:

Zaliznyak_Switch_2 (config)# interface g0/2

Zaliznyak_Switch_2 (config-if)#switchport trunk native vlan 100

Zaliznyak_Switch_2 (config-if)#switchport mode trunk

Zaliznyak_Switch_2 (config-if)#exi

Налаштування портів доступу:

Zaliznyak_Switch_2 (config)# interface range f0/11-14

Zaliznyak_Switch_2 (config-if)#switchport mode access // включити режим access

Zaliznyak_Switch_2 (config-if)# switchport access vlan 15 // вказати інтерфейси для vlan 15

Zaliznyak_Switch_2 (config)# interface range f0/5-10

Zaliznyak_Switch_2 (config-if)#switchport mode access

Zaliznyak_Switch_2 (config-if)# switchport access vlan 25

Zaliznyak_Switch_2 (config)# interface range f0/15-24

Zaliznyak_Switch_2 (config-if)#switchport mode access

Zaliznyak_Switch_2 (config-if)# switchport access vlan 25

Налаштування SVI-інтерфейсу:

Zaliznyak_Switch_2 (config)# interface Vlan99

Zaliznyak_Switch_2 (config-if)# ip address 172.22.80.194 255.255.255.248

Zaliznyak_Switch_2 (config-if)#no shutdown

Для демонстрації налаштувань відображено загальне зображення таблиці згідно налаштування VLAN на комутаторах і відповідних їм портів зображено на рисунках 3.15, 3.16.

Device Name: Zaliznyak_Switch_2
Custom Device Model: 2960 IOS15
Hostname: Zaliznyak_Switch_2

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Down	99	--	000D.BD78.15E7
FastEthernet0/2	Down	99	--	0000.0CD9.4D9A
FastEthernet0/3	Down	99	--	0060.7014.2B49
FastEthernet0/4	Down	99	--	0050.0F36.CE68
FastEthernet0/5	Up	25	--	0007.ECD6.A65C
FastEthernet0/6	Down	25	--	00E0.F7B1.A5BC
FastEthernet0/7	Down	25	--	0001.9779.2D88
FastEthernet0/8	Down	25	--	00D0.BCE8.2255
FastEthernet0/9	Down	25	--	0001.43C9.E2B2
FastEthernet0/10	Down	25	--	000A.4173.D453
FastEthernet0/11	Up	15	--	000C.8532.1375
FastEthernet0/12	Down	15	--	00D0.5818.3385
FastEthernet0/13	Down	15	--	0007.ECA8.03AB
FastEthernet0/14	Down	15	--	0060.5C8D.2D92
FastEthernet0/15	Up	35	--	000A.41A9.C91E
FastEthernet0/16	Down	35	--	0010.11CA.159E
FastEthernet0/17	Down	35	--	00D0.D31E.EB75
FastEthernet0/18	Down	35	--	0060.5CA9.9D40
FastEthernet0/19	Down	35	--	0090.2B58.23BA
FastEthernet0/20	Down	35	--	0030.F2BB.C6D5
FastEthernet0/21	Down	35	--	0030.A3B8.C803
FastEthernet0/22	Down	35	--	000A.4173.6B22
FastEthernet0/23	Down	35	--	00E0.B08D.4E86
FastEthernet0/24	Down	35	--	0060.5C61.A060
GigabitEthernet0/1	Up	--	--	00E0.B092.B3D1
GigabitEthernet0/2	Up	--	--	000C.85B9.A6AC
Vlan1	Up	1	<not set>	000A.F3CA.D90D
Vlan99	Up	99	172.22.80.194/29	000A.F3CA.D901

Рисунок 3.15 – Налаштування VLAN на Zaliznyak_Switch_2

```
Device Name: Zaliznyak_Switch_3
Custom Device Model: 2960 IOS15
Hostname: Zaliznyak_Switch_3

Port                Link   VLAN   IP Address         MAC Address
FastEthernet0/1     Down   99     --                 0001.97B8.0627
FastEthernet0/2     Down   99     --                 000D.BD13.8745
FastEthernet0/3     Down   99     --                 0002.4AC2.7356
FastEthernet0/4     Down   99     --                 0001.C794.227B
FastEthernet0/5     Up     25     --                 0001.43BE.09AE
FastEthernet0/6     Down   25     --                 00E0.A3B7.747A
FastEthernet0/7     Down   25     --                 00D0.5885.5114
FastEthernet0/8     Down   25     --                 00D0.BCA4.AB1E
FastEthernet0/9     Down   25     --                 0040.0B73.C169
FastEthernet0/10    Down   25     --                 0000.0C1E.2D25
FastEthernet0/11    Up     15     --                 0030.A395.1432
FastEthernet0/12    Down   15     --                 00D0.D389.ED53
FastEthernet0/13    Down   15     --                 0001.439B.734E
FastEthernet0/14    Down   15     --                 0090.0CA6.EE71
FastEthernet0/15    Up     35     --                 0002.1711.5256
FastEthernet0/16    Down   35     --                 0001.43D6.3321
FastEthernet0/17    Down   35     --                 00D0.BA0B.B98D
FastEthernet0/18    Down   35     --                 0002.1630.59DE
FastEthernet0/19    Down   35     --                 000A.F3CA.D8B1
FastEthernet0/20    Down   35     --                 00D0.BC71.9210
FastEthernet0/21    Down   35     --                 0002.1616.6C6B
FastEthernet0/22    Down   35     --                 00E0.8F0D.B748
FastEthernet0/23    Down   35     --                 0004.9A57.BB46
FastEthernet0/24    Down   35     --                 0060.47D8.EE09
GigabitEthernet0/1  Up     --     --                 000A.4112.0041
GigabitEthernet0/2  Down   1      --                 0060.479C.C14D
Vlan1               Up     1      <not set>          000A.F368.D64B
Vlan99              Up     99     172.22.80.195/29   000A.F368.D601
```

Рисунок 3.16 – Налаштування VLAN на Zaliznyak_Switch_3

3.5.4 Параметри безпеки комутаторів та адресації ПК в мережах VLAN ігрової студії

На портах комутаторів, підключених до серверів, використана функція безпеки портів таким чином, що [1]:

− тільки двом унікальним пристроям був дозволений доступ до порту;

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

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

Команди виконані на комутаторі Zaliznyak_Switch_2 згідно технічних вимог:

Zaliznyak_Switch_2 (config)#int fa0/11 // вхід в інтерфейс

Zaliznyak_Switch_2 (config-if)#switchport port-security // ввімкнення засобів безпеки

Zaliznyak_Switch_2 (config-if)#switchport port-security maximum 2 // забезпечення доступу до порту тільки двом унікальним пристроям

Zaliznyak_Switch_2 (config-if)#switchport port-security mac-address sticky// MAC-адрес пристрою розпізнавався динамічно і додавався в поточну конфігурацію

Zaliznyak_Switch_2 (config-if)# switchport port-security violation restrict// під час порушенні системи безпеки з'являлося повідомлення, а порт залишався включеним

Для здійснення передавання трафіку між VLAN проведено декілька додаткових налаштувань на Zaliznyak_Router_3. Для того щоб забезпечити передавання трафік з одного сегменту VLAN в інший та с однієї мережі в іншу. Для того щоб не використовувати окремі порти під мережу кожного VLAN на окремий фізичний інтерфейс, для цього створено логічні під інтерфейсів на фізичному інтерфейсі GigabitEthernet 0/0 з використанням технологією інкапсуляції 802.1Q для кожного VLAN.

Для логічних під інтерфейсів на маршрутизаторі необхідно вказувати, що інтерфейс буде присвоєне отримування тегованого трафік і вказувати номер VLAN відповідний цьому інтерфейсу.

Zaliznyak_Router_3 (config)#interface g0/0

Zaliznyak_Router_3 (config-if)#no shutdown

Zaliznyak_Router_3 (config)#interface g0/0.15 // налаштування підінтерфейсу для маршрутизації трафіку між VLAN

Zaliznyak_Router_3 (config-subif)#encapsulation dot1Q 15 // тегування пакетів для даного під інтерфейсу.

Zaliznyak_Router_3 (config-subif)#ip address 172.22.80.1 255.255.255.192

4 РОЗРОБКА IOT СИСТЕМИ

4.1 Аналіз використання розумних IoT пристроїв

В цій мережі була розроблена задача по створенню систему використання розумних пристроїв з можливістю відстеження станів системи пожежної безпеки за допомогою технології 3G/4G для «Відділ технічної підтримки Офіс Київ».

Також були вирішені такі здачі при реалізації цієї системі такі як:

– налаштування серверів таких як DNS та IoT для віддаленого підключення до виконуючих вистроїв;

– забезпечити DHCP сервіс для кожної с підмереж таких як «Мережа розумних пристроїв в LAN 5» та «Мережа віддаленого доступу до розумних пристроїв»;

– налаштування сценаріїв пристроями у разі спрацювання датчиків пожежної безпеки;

– реалізувати систему пожежної безпеки в яку входять два датчики вогню та датчик диму як головні компоненти;

– налаштувати контролер MCU та написати програмний додаток на мові Python.

Також висунуто наступний сценарій до функціоналу пожежної безпеки а саме за наявністю вогню в кімнаті необхідно вмикати розприскувач на 1000 с, відкривати вікно та вмикати сирену. В приміщенні за сигналом датчика диму та детектору вогню вмикати систему туману та вентилятор. Вікно відкрити після вимкнення системи туману.

4.2 Реалізація системи IoT пристроїв

4.2.1 Налаштування мережі віддаленого доступу до розумних пристроїв

Мережа «Віддаленого доступу до розумних пристроїв» згідно початкової топології виконує функції емалювання вежі мобільного зв'язку для підключення мобільних пристроїв за допомогою технології 3G/4G.

Відповідно для налаштування мережі «Віддаленого доступу до розумних пристроїв» було виконано декілька кроків.

На першому кроці було піддавано вежу Cell tower та Central office server та налаштовано сервіс DHSP для підключення зовнішнього мобільного пристрою отримали IP-адреси та одержали змогу підключення до мережі «Віддаленого моніторингу».

На другому кроці на маршрутизаторі ISP, а саме на його інтерфейсі G0/0 була призначена IP-адреси 119.5.201.225 /27 та налаштування DHSP сервіс такими командами.

```
Router_ISP(config-if)# int g0/0
Router_ISP(config-if)#ip add 119.5.201.225 255.255.255.224
Router_ISP(config-if)# exit
Router_ISP(config)# ip dhcp excluded-address 119.5.201.225 119.5.201.229
Router_ISP(config)# ip dhcp pool CELL
Router_ISP(dhcp-config)#net 119.5.201.224 255.255.255.24
Router_ISP(dhcp-config)#def 119.5.201.225
Router_ISP(dhcp-config)#dns-server 10.5.0.254
```

Після виконання всіх попередніх крокі можна спостерігати на Central office server як він отримує інформацію на інтерфейс Backbone одержуються динамічна виділена IP-адреса та додаткова інформація для мережі представлено рисунок 4.1.

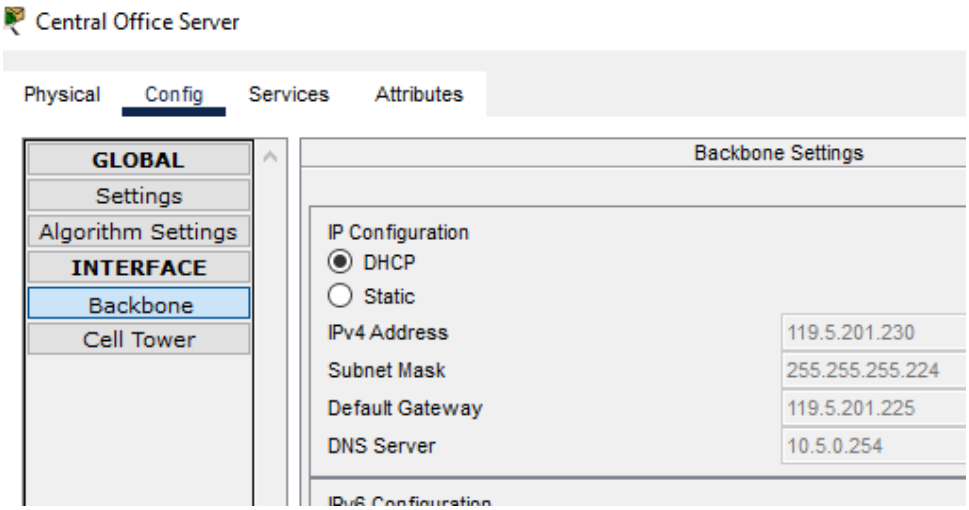

Рисунок 4.1 – Демонстрація динамічного налаштування інтерфейсу Backbone

4.2.2 Налаштування мережі мережа віддаленого моніторингу

Ця мережа віддаленого моніторингу призначення для керування мережі за допомогою Server_IoT та динамічного призначення IP-адрес кінцевим пристроям у мережі.

В цій мережі були виконання декілька кроків налаштування на пристрої Router_ISP які зображені на рисунку 4.2– 4.4.

```
Router(config)#int g0/1
Router(config-if)#ip add 10.5.0.1 255.255.255.0
Router(config-if)#
Router(config-if)#int g0/0
Router(config-if)#ip add 119.5.201.225 255.255.255.224
Router(config-if)#int g0/2
Router(config-if)#ip add 119.5.200.225 255.255.255.224
```

Рисунок 4.2 – Налаштування IP-адрес на інтерфейсах

```
Router(config)#ip dhcp excluded-address 119.5.201.225 119.5.201.229
Router(config)#ip dh
Router(config)#ip dhcp pool CELL
Router(dhcp-config)#net
Router(dhcp-config)#network 119.5.201.224 255.255.255.224
Router(dhcp-config)#deg
Router(dhcp-config)#def
Router(dhcp-config)#default-router 119.5.201.225
Router(dhcp-config)#dns
Router(dhcp-config)#dns-server 10.5.0.254
```

Рисунок 4.3 – Налаштування DHSP для мережі «віддаленого доступу до розумних пристроїв»

```
Router(config)#ip dhcp excluded-address 119.5.200.225 119.5.200.229
Router(config)#ip dh
Router(config)#ip dhcp ex
Router(config)#ip dhcp pool WAN
Router(dhcp-config)#net
Router(dhcp-config)#network 119.5.200.224 255.255.255.224
Router(dhcp-config)#def
Router(dhcp-config)#default-router 119.5.200.225
Router(dhcp-config)#dns
Router(dhcp-config)#dns-server 10.5.0.254
```

Рисунок 4.4 – Налаштування DHSP для мережі «розумні пристроїв в LAN 5»

Також були виконано налаштування на сервалах DNS та IoT для віддаленого керування розумними пристроями які зображені на рисунку 4.5 – 4.8.

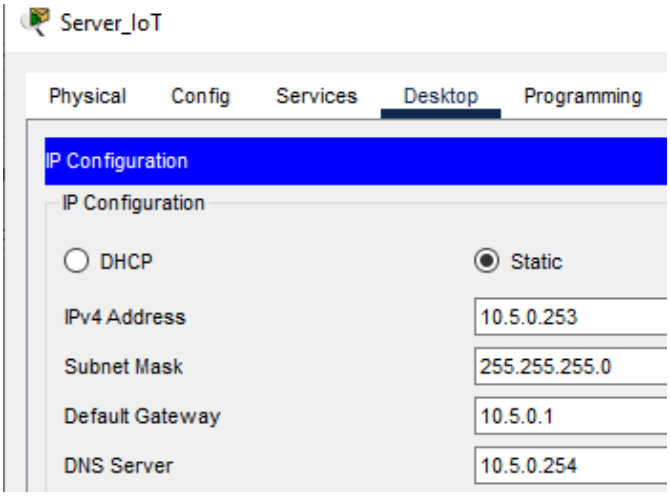

Рисунок 4.5 – Налаштування IP-конфігурації

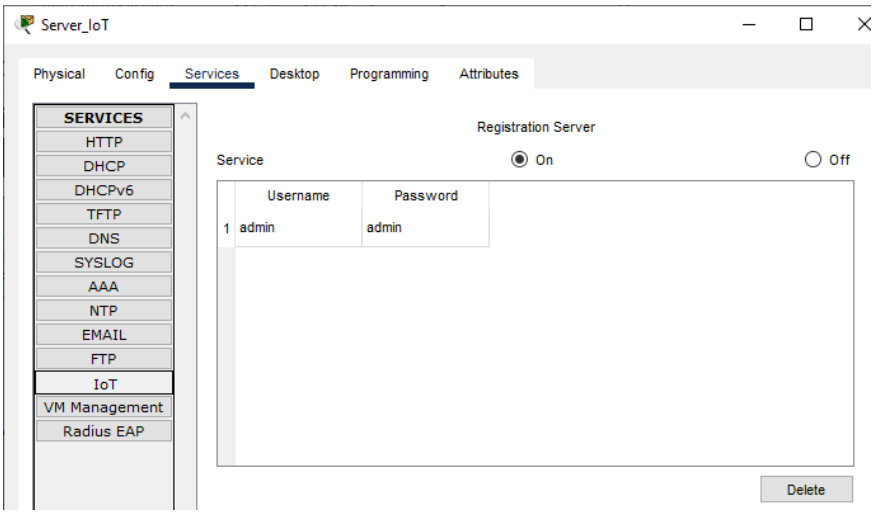

Рисунок 4.6– Налаштування IoT сервера

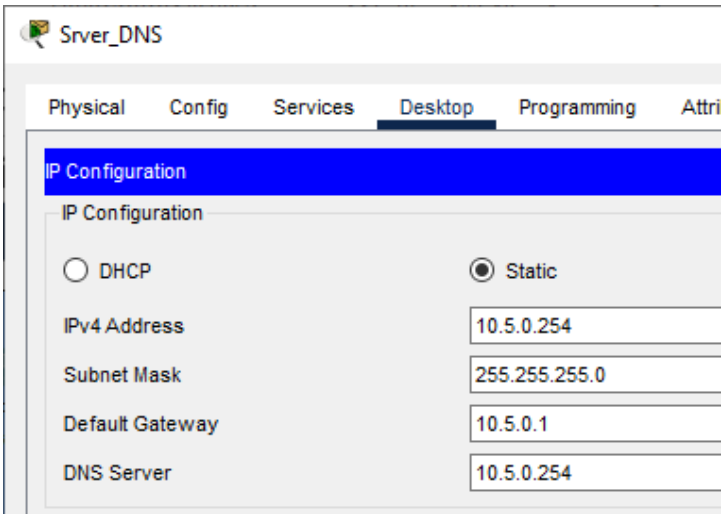

Рисунок 4.7 – Налаштування IP-конфігурації

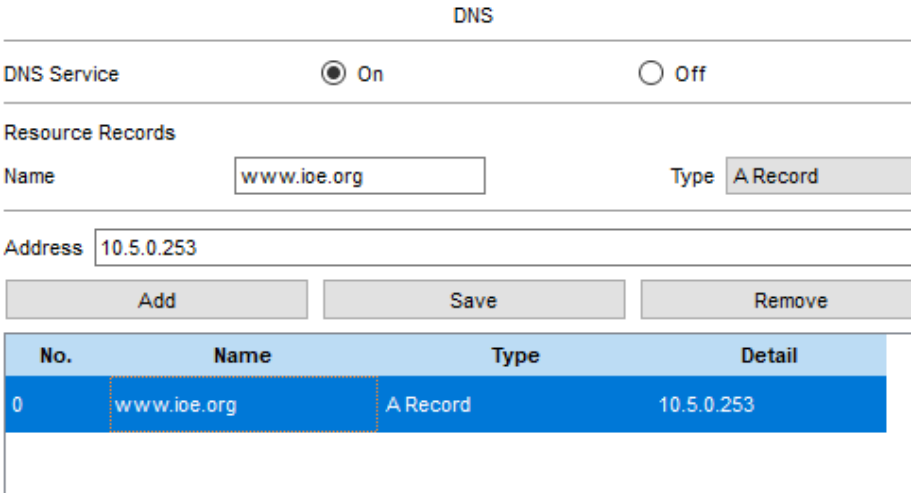

Рисунок 4.8 – Налаштування конфігурації DNS – сервера

4.2.3 Налаштування мережі «розумних пристроїв в LAN 5»

Мережа «розумних пристроїв в LAN 5» призначена для керуванням та підключенням кінцевих розумних пристрої та головного керуючого контролера Home Gateway та контролера пожежної безпеки MCU. А саме на керуючому контролері Home Gateway було виконано налаштування інтерфейсів бездротового підключення, локального підключення та інтернет підключення які зображено на рисунках 4.9 – 4.11.

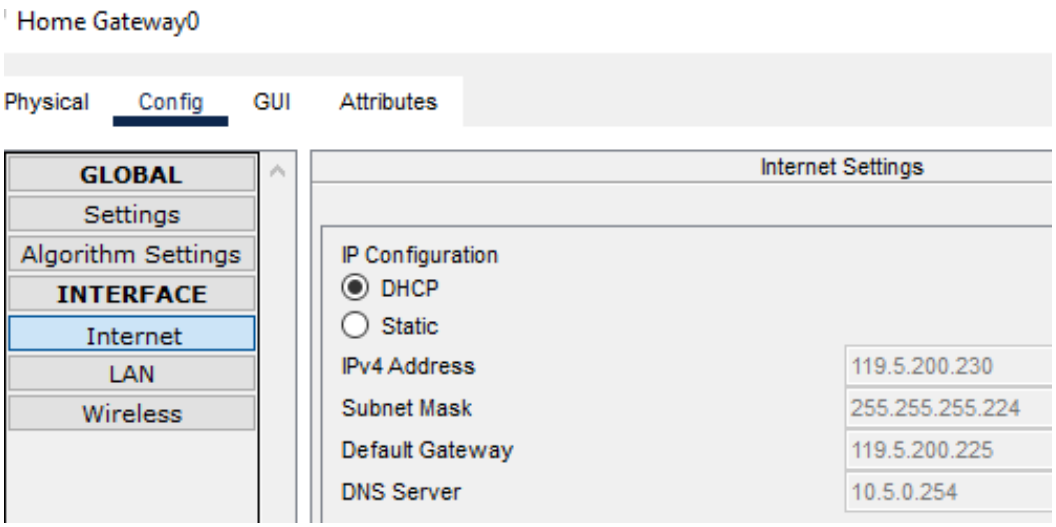

Рисунок 4.9 – Демонстрація налаштувань на інтернет інтерфейсі

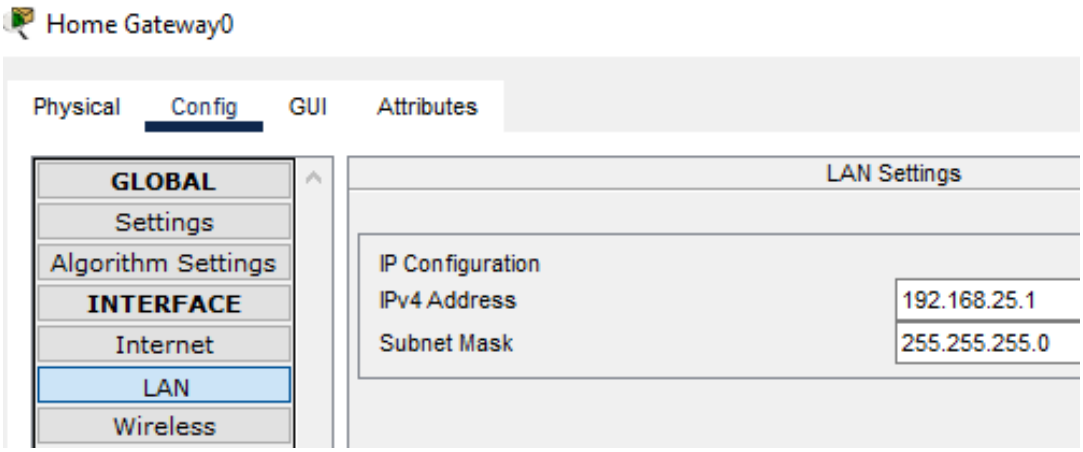

Рисунок 4.10 – Демонстрація налаштувань на інтерфейсі локальної мережі

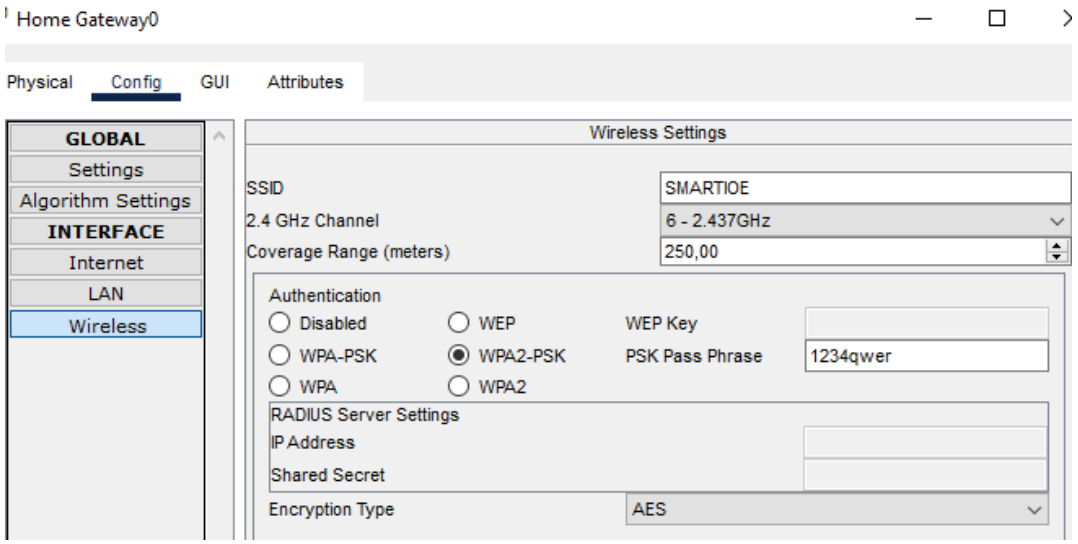

Рисунок 4.11 – Демонстрація налаштувань на інтерфейсі бездротового підключення

4.2.4 Реалізація контролерних обчислень

Для виконання реалізації контролерних обрахувань було виконано за допомогою системи пожежної безпеки, а саме контролера MCU для якого було створено програму на мові Python та розумники приладами які підключаються до Home Gateway який дозволяє взаємодіяти з ними представлені на рисунках 4.12 – 4.14.

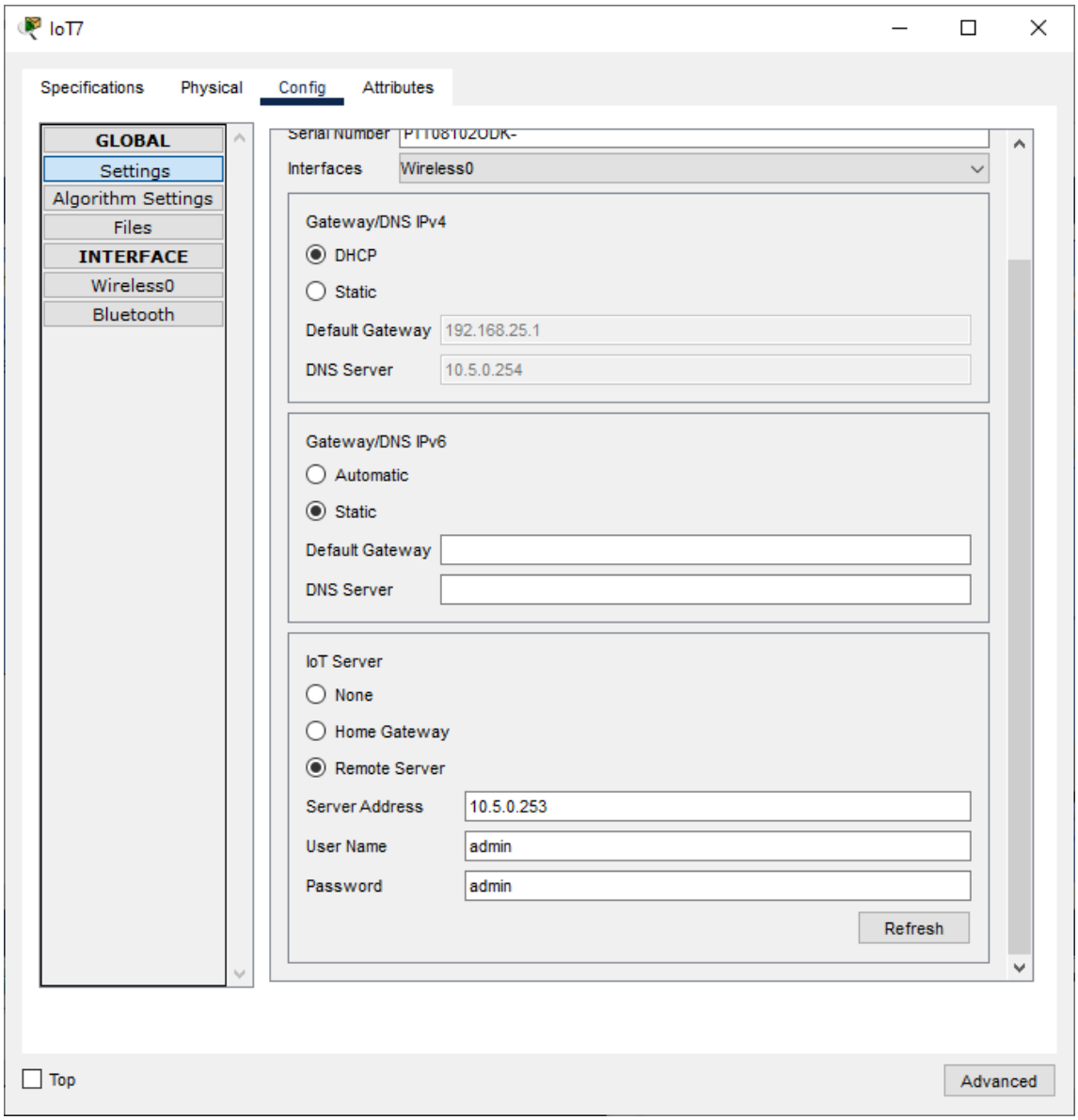

Рисунок 4.12 – Приклад глобальних налаштувань розумних пристроїв

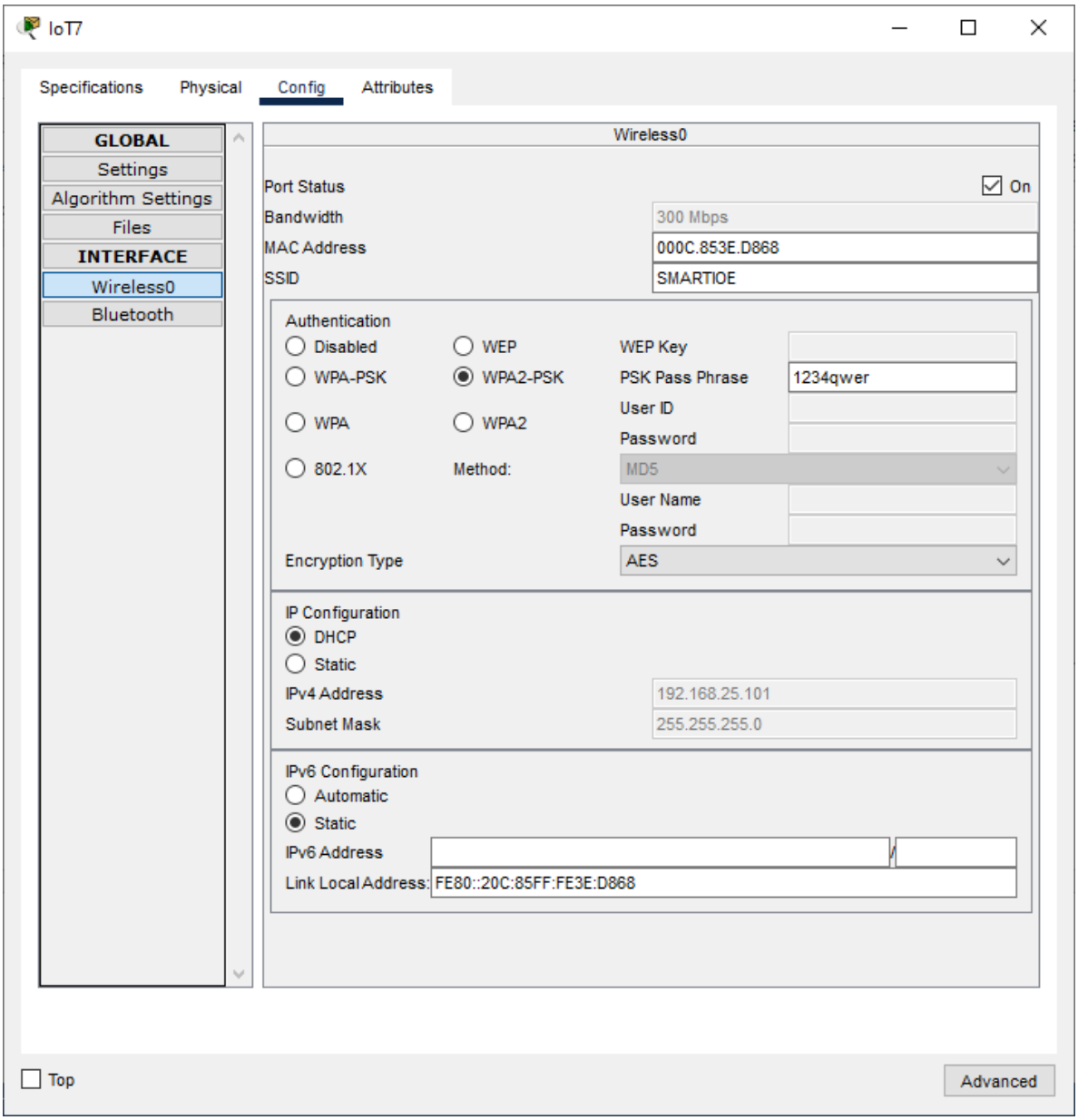

Рисунок 4.13 – Приклад налаштувань бездротового з’єднання розумних пристроїв

```
from gpio import *
from time import *

def handleSensorData():
    value = digitalRead(0)
    if value == 0:

        customWrite(2, '0')
        customWrite(3, '0')
        digitalWrite(5, LOW)

    else:
        customWrite(2, '1')
        customWrite(3, '1')
        digitalWrite(5, HIGH)

def handleSensorData1():
    value = digitalRead(1)
    if value == 0:

        customWrite(2, '0')
        customWrite(3, '0')
        digitalWrite(5, LOW)
    else:

        customWrite(2, '1')
        customWrite(3, '1')
        digitalWrite(5, HIGH)

def main():
    add_event_detect(0, handleSensorData)
    add_event_detect(1, handleSensorData1)

    while True:
        delay(1000)


if __name__ == "__main__":
    main()

```

Рисунок 4.14 – Код програми мовою Python для реалізації роботи системі пожежної безпеки на контролері MCU

4.2.5 Реалізація хмарних обчислень

Хмарні обрахування являють собою виконання певних закладених функцій на головному керуючому елементі системи. Згідно вимоги це було реалізовано за допомогою віддаленого сервера IoT до якого підключаються усі розумні пристрої через шлюз керування та в подальшому на нього передані стан цих приладів і керування ними за допомогою мобільних чи комп’ютерних пристроїв. Також за допомогою сервера IoT було створені сценарії які відповідають за взаємодію пристроїв у разі спрацювання датчиків вогню та задимлення зображено на рисунку 4.15– 4.16.

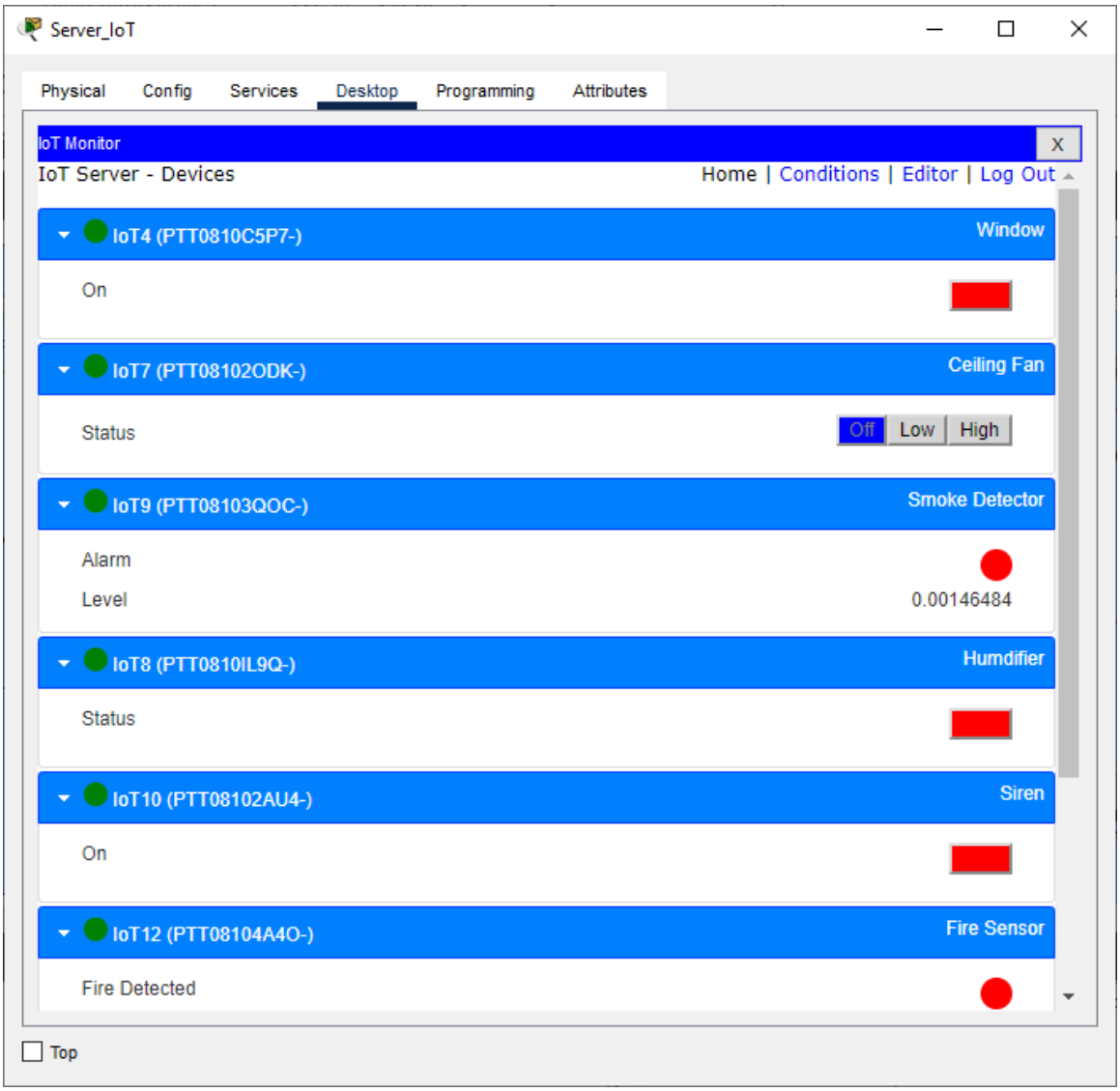

Рисунок 4.15– Відображення розумних пристроїв та їх станів на віддаленому сервері IoT

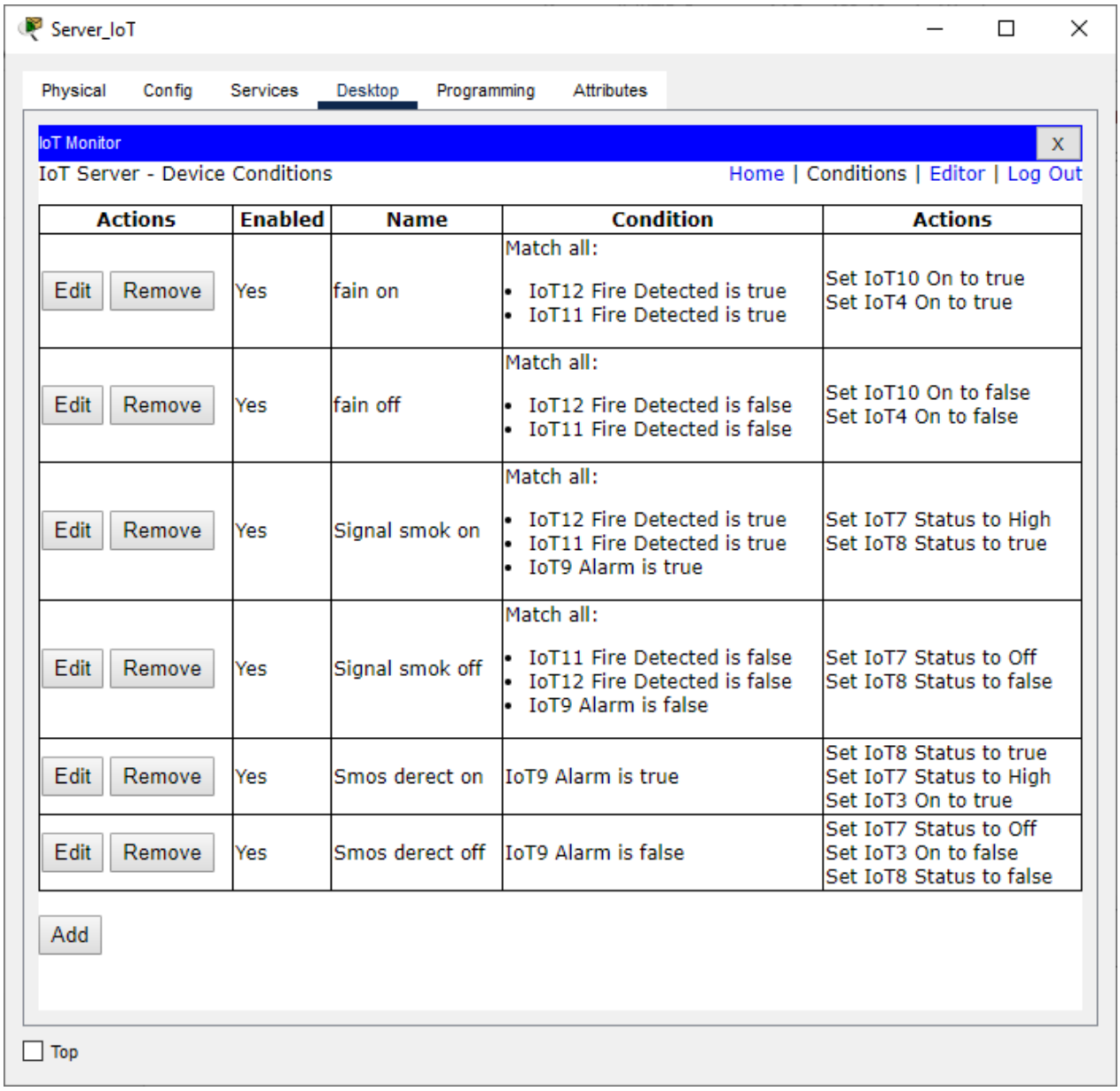

Рисунок 4.16 – Відображення налаштованих сценаріїв керування розумних пристроїв у разі спрацювання датчиків вогню та диму

4.3 Перевірка роботи системи IoT пристроїв

Виконання перевірки працездатності та тестування закладених функцій у систему IoT яка відповідає за пожежну безпеку відбулося у програмному застосунку PacketTracer. Таким чином було змодельована ситуацію згідно якої по-перше коли датчики вогню спрацьовують то в свою чергу вони повинні активувати розприскувачі, сирену та відкрити вікно, по друге коли спрацьовує датчик диму то в свою чергу спрацьовує система туману та вмикається

вентилятор та відчиняється вікно, а після вимкнення системи туману відкрити вікно представлено на рисунках 4.18 – 4.21.

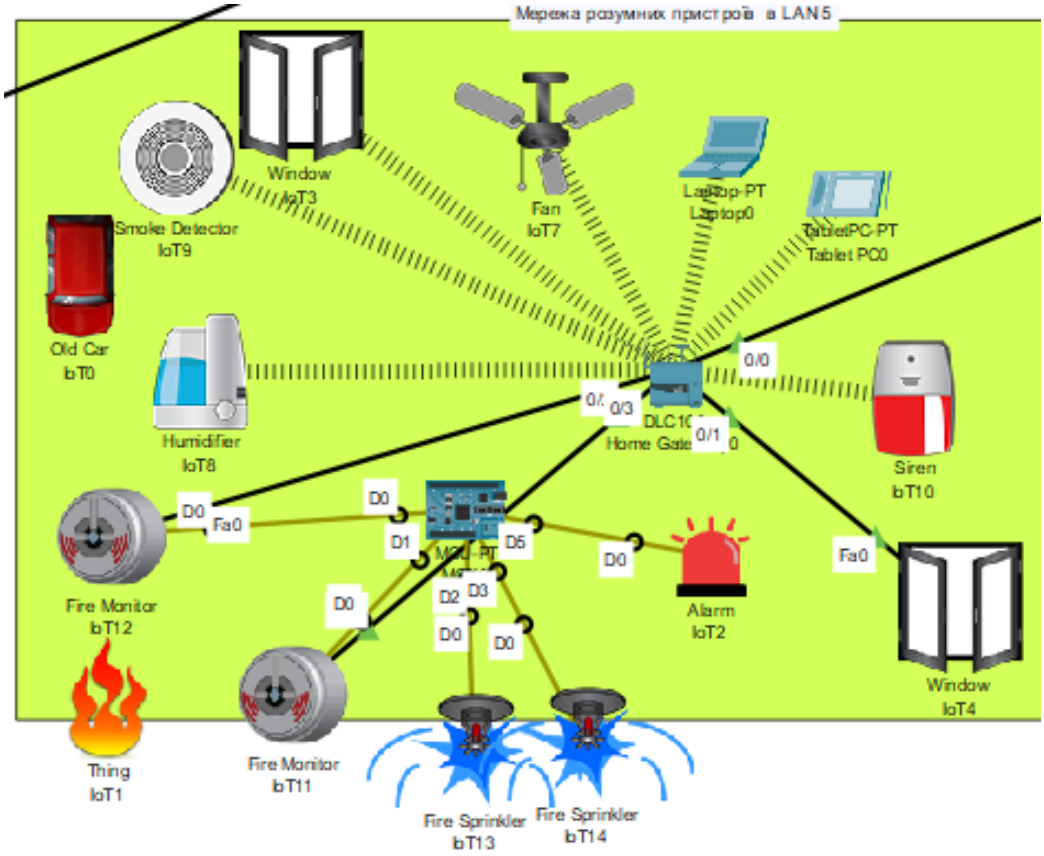

Рисунок 4.18 – Демонстрація роботи датчику вогню та зв’язаного сценарію з ним

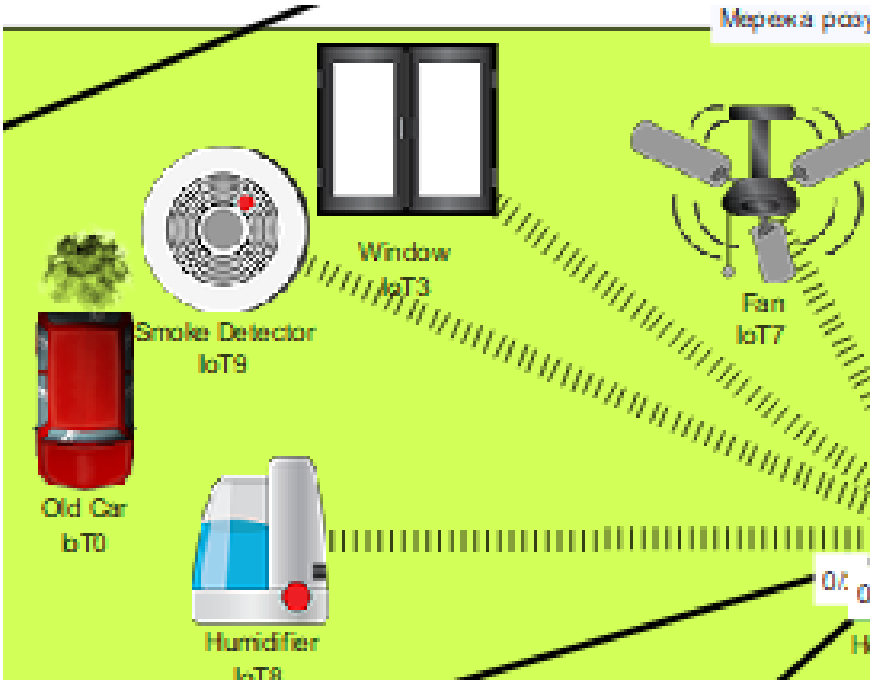

Рисунок 4.19 – Демонстрація перевірки працездатності датчика диму та зв’язаного сценарію з ним

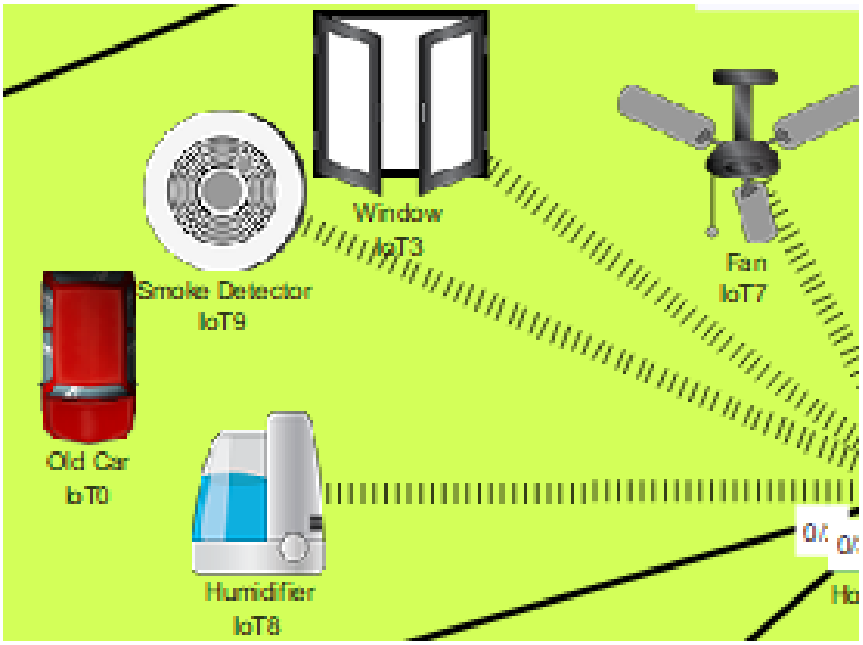

Рисунок 4.20 – Демонстрація перевірки відкриття вікна коли вимикається система туману

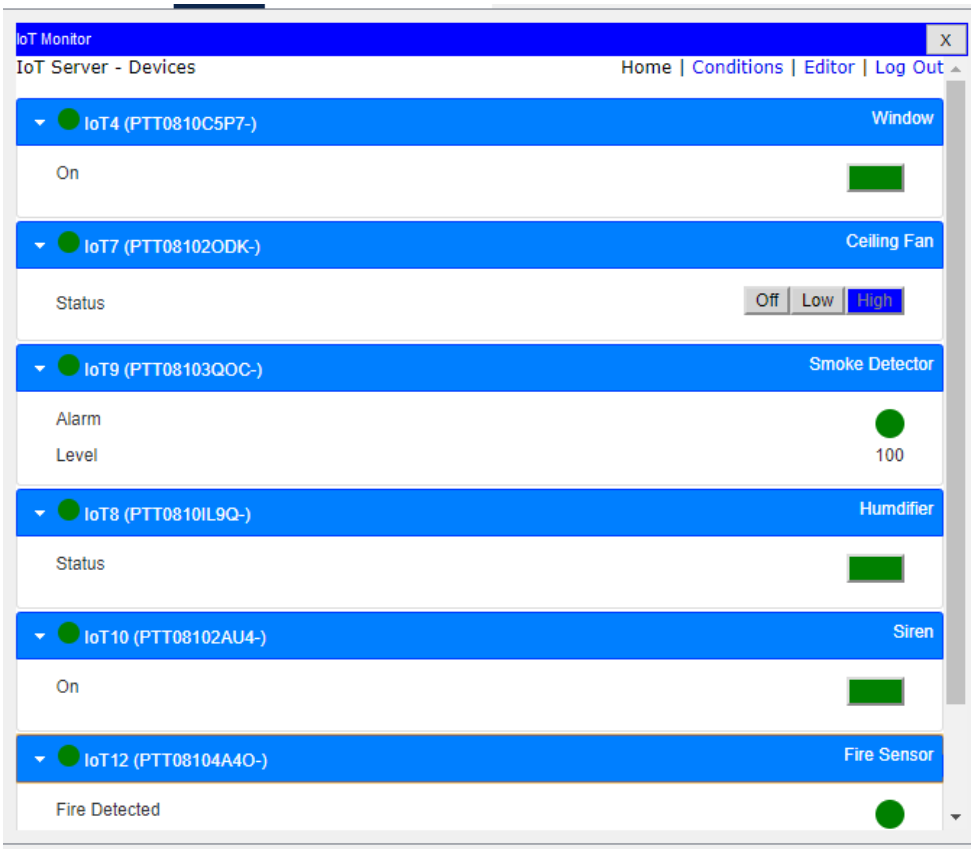

Рисунок 4.21 – Демонстрація перевірки доступності моніторингу розумних пристроїв та їх стани через смартфон

ВИСНОВКИ

У кваліфікаційній роботі було проведено аналіз та опрацьовано вимоги до ігрової студії «Ubisoft Ukraine (Kiyv)», за якими спроектовано мережу, яка має використання змішаної топології та забезпечення впровадження відмовостійкого рішення для окремих сегментів. В процесі проектування мережі було створене технічне завдання та обрані технології для забезпечення роботи на канальному та фізичному рівнях.

Згідно створеної архітектури мережі, функціональним призначеннями структурних відділів, і вимог потреб мережі було обрано мережеве обладнання фірми Cisco і проведене його налаштування згідно висунутих вимог до безпеки, надійності, та відмовостійкості.

Розробка моделі мережі була виконана за допомогою програмного продукту Cisco Packet Tracer версії 8. Таким чином, було досліджено деякі обмеження програмного продукту моделювання та мінімізовано їх вплив на кінцеве рішення. В мережі ігрової студії в повному обсязі застосовані та налаштовані майже усі існуючі технології такі як: PAgP, HSRP, DHCP, EIGRP, STP, RADIUS, NAT, AAA, VLAN та VPN. Також було проведено налаштування безпеки на мережевих пристроях для запобігання витоку інформації і інтелектуальної власності та несанкціонованого втручання у мережу зовні.

Також згідно вимог до відділу технічної підтримки офіс Київ було розроблено систему з впровадженням IoT пристроїв, для покрашення та запобігання пожежної небезпеки. В цій мережі були реалізовані технології хмарового та контролерного обчислень, і впровадження технологій дистанційного моніторингу за допомогою IoT серверів.

Відповідно до завдання кваліфікаційної роботи – створення комп’ютерної мережі для ігрової студії «Ubisoft ukraine» з опрацюванням побудови відмовостійкої корпоративної мережі була виконана в повній мірі з використанням усіх навичок здобутих вході навчання.

ПЕРЕЛІК ПОСИЛАНЬ

1. Дипломування. Методичні вказівки для бакалаврів 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.М.: НТУ «Дніпровська політехніка», 2022. – 62 с.

2. Мережева академія Cisco курс CCNA1, 2, 3: [Електронний ресурс] – Режим доступу: URL: https://www.netacad.com.

3. Валецька Т. М. Комп'ютерні мережі: Апаратні засоби. Навч. посібник. К.: Ельга, 2004.3. 3-е вид. / В. Г. Олифер, Н. А. Олифер. – СПб.:, 2008. – 958 с.

4. Біячуєв, Т.А. «Безпека корпоративних мереж»/ Т. А. Біячуєв – М.: 2014. – 481 с.

5. Джон Купер Архітектура комп’ютерних мереж: [Навчальний посібник] / Netskills Ver 1.0, 2014. – 265 с.

6. Цвіркун Л.І. Інженерна та комп'ютерна графіка. AutoCAD: навч. посіб. / Л.І. Цвіркун, Л.В. Бешта ; під. заг. ред. Л.І. Цвіркуна; М-во освіти і науки України, НТУ «Дніпровська політехніка». – Дніпро: НТУ «ДП» , 2018. – 209 с.

7. Оліфер В.Г. Комп'ютерні мережі. Принципи, технології, протоколи: Підручник для вишів. 3-тє вид. / В. Г. Оліфер, Н. А. Оліфер. - СПб.: Берлін, 2008.

8. Кульгін, М. Технологія корпоративних мереж. Енциклопедія/ М. Кульгін - СПб.: Чехія, 2014. - 541 с.

9. Кулаков Ю.А., Луцький Г.М. Локальні мережі. - К.: Юніор, 1998. – 336 с.

10. Кулаков Ю.А., Омелянський С.В. Комп'ютерні мережі. Вибір, встановлення, використання та адміністрування. - До: Юніор, 1999. - 544 с.

11. Жуков, І. А. Комп’ютерні мережі та технології: навч. посіб./ І. А. Жуков, В. О. Гуменюк, І. Є. Альтман. – К. : НАУ, 2004. – 276 с.

Додаток А

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.22005-01 12 01

Листів 9

2022

АНОТАЦІЯ

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

ЗМІСТ

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
//Шифрування паролів
service password-encryption
!
//Ім'я пристрою
hostname Zaliznyak_Router_4
!
//Пароль до привілейованого режиму
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
//Виключення адрес з пулу DHCP
ip dhcp excluded-address 172.22.83.129 172.22.83.130
!
// 1.1 Налаштування DHCP
ip dhcp pool polllan2
 network 172.22.83.128 255.255.255.128
 default-router 172.22.83.129
 dns-server 172.22.80.16
 domain-name Zaliznyak_Router_4
!
//1.2 Налаштування AAA
aaa new-model
!
aaa authentication login SSH-LOGIN local
aaa authentication login default group radius local

!
no ip cef
no ipv6 cef
!
//1.3 Створення користувача з паролем
```

```
username Zaliznyak secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
license udi pid CISCO2811/K9 sn FTX10176328-
!
```

// 1.4 Створення VPN

```
crypto isakmp policy 1
 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 CMAP 10 ipsec-isakmp
 set peer 64.100.13.2
 set transform-set TS
 match address V5-VPN
```

//1.5 Створення домену

```
no ip domain-lookup
ip domain-name Zaliznyak_Router_4
!
spanning-tree mode pvst
!
```

//1.5 Налаштування інтерфейсів

```
interface FastEthernet0/0
 ip address 10.1.5.10 255.255.255.252
 duplex auto
 speed auto
!
```

// 1.6 Налаштування HSRP

```
interface FastEthernet0/1
 ip address 172.22.82.6 255.255.255.0
 duplex auto
 speed auto
 standby version 2
 standby 1 ip 172.22.82.1
 standby 1 preempt
!
interface Serial0/0/0
 ip address 10.1.5.6 255.255.255.252
 ip nat inside
!
interface Serial0/0/1
 ip address 209.165.202.1 255.255.255.252
 ip nat outside
 crypto map CMAP
!
interface Ethernet0/1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2/0
 ip address 172.22.83.129 255.255.255.128
 ip nat inside
!
interface Ethernet0/3/0
 no ip address
 duplex auto
 speed auto
```

```
 shutdown
!
interface FastEthernet1/0
 ip address 10.1.5.13 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 10.1.5.17 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface Ethernet1/0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
```

//1.7 Налаштування протоколу маршрутизації

```
router eigrp 1
 redistribute static
 network 10.1.5.8 0.0.0.3
 network 10.1.5.12 0.0.0.3
 network 10.1.5.16 0.0.0.3
 network 10.1.5.4 0.0.0.3
 network 172.22.83.128 0.0.0.127
 network 172.22.82.0 0.0.0.255
```

//1.8 Налаштування NAT

```
ip nat inside source list V5-NAT interface Serial0/0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.2
!
ip flow-export version 9
!
ip access-list extended V5-VPN
 permit ip 172.22.82.0 0.0.0.255 172.22.83.0 0.0.0.127
 permit ip 172.22.83.128 0.0.0.127 172.22.83.0 0.0.0.127
 permit ip 172.22.80.0 0.0.0.255 172.22.83.0 0.0.0.127
 permit ip 172.22.81.0 0.0.0.255 172.22.83.0 0.0.0.127
ip access-list extended V5-NAT
 deny ip 172.22.82.0 0.0.0.255 172.22.83.0 0.0.0.127
 deny ip 172.22.83.128 0.0.0.127 172.22.83.0 0.0.0.127
 deny ip 172.22.80.0 0.0.0.255 172.22.83.0 0.0.0.127
 deny ip 172.22.81.0 0.0.0.255 172.22.83.0 0.0.0.127
 permit ip 172.22.82.0 0.0.0.255 any
 permit ip 172.22.83.128 0.0.0.127 any
 permit ip 172.22.80.0 0.0.0.255 any
 permit ip 172.22.81.0 0.0.0.255 any
!
```

//Налаштування банеру

```
banner motd #If you are not a network administrator, login is prohibited#
!
```

//Налаштування RADIUS

```
radius-server host 172.22.80.16 auth-port 1645 key radius123
!
radius server 172.22.80.16
 address ipv4 172.22.80.16 auth-port 1645
 key radius123
```

```
//1.8 Налаштування консольних та vty ліній
line con 0
 login authentication default
line aux 0
line vty 0 4
 login authentication SSH-LOGIN
 transport input ssh
end
```