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 Басараба Данила Руслановича
(ПІБ)
академічної групи 123-18-1
(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 IT-компанії «BAS-IQ» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Бешта Д.О.			
розділів:				
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.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 Басараба Д.Р. **академічної групи** 123-18-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

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

на тему "Комп'ютерна система IT-компанії «BAS-IQ» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.05.2022 № 771-л

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 формулюються 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 захисту інформації в системі	24.05.2022
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2022

Завдання видано _____ доц. Бешта Д.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.01.2022

Дата подання до екзаменаційної комісії 15.06.2022

Прийнято до виконання _____ Басараб Д.Р.

РЕФЕРАТ

Пояснювальна записка: 103 с., 65 рис., 6 табл., 2 додатки, 18 джерел.

КОМП'ЮТЕРНА МЕРЕЖА, ІТ-КОМПАНІЯ, КОМП'ЮТЕРНА СИСТЕМА, ПОБУДОВА МЕРЕЖІ, НАЛАШТУВАННЯ МЕРЕЖЕВИХ ПРИСТРОЇВ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ПРОГРАМА МОНІТОРИНГУ.

Об'єкт розробки − комп'ютерна система ІТ-компанії, що займається розробкою мобільних та веб-додатків мовами програмування високого рівня.

Мета роботи – створення комп'ютерної системи для ІТ-компанії з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Комп'ютерна мережа, що була спроектована, складається із сучасних апаратних приладів для обробки та передачі інформації. Система може бути легко масштабувана шляхом додавання до існуючих підмереж нових робочих місць. Даний проєкт може бути використаний для створення подібних мереж не лише в сфері інформаційних технологій, а також, наприклад, для проектування офісів фінансових чи маркетингових компаній.

Комп'ютерна система дозволяє виконувати оновлення окремих апартних компонентів мережі, а також модернізацію встановленого програмного забезпечення для виконання наступних функцій:

– збільшення швидкості передачі інформації;
– збільшення продуктивності окремих робочих місць та системи в цілому;
– покращення системи безпеки комп'ютерної мережі.

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

Робота комп'ютерної системи протестована за допомогою моделі топології корпоративної мережі із використанням програмного застосунку Cisco Packet Tracer.

Підсумки перевірки системи у вигляді таблиць та діаграм описані й наводені в пояснювальній записці та додатках до неї.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

AAA – протокол авторизації, автентифікації та обліку;

DHCP – протокол динамічного розподілу адрес вузлам;

DNS – система доменних імен;

EIGRP – протокол динамічної маршрутизації;

HTTP – протокол передачі гіпертексту;

IP-адреса - унікальний ідентифікатор комп'ютера локальної мережі або мережі Інтернет;

ISP – компанія-постачальник Інтернет-послуг;

LAN – локальна мережа;

SSH – мережевий протокол рівня застосунків віддаленого адміністрування.

TCP/IP - набір протоколів мережі Інтернет;

VLAN – віртуальна локальна мережа;

VPN -віртуальна приватна мережа;

VTY – віртуальний інтерфейс, який забезпечує віддалений доступ до пристрою;

WAN – глобальна мережа;

ЕОМ – електронно-обчислювальна машина

КМ – корпоративна мережа;

КС – комп’ютерна система;

ПК – персональний комп’ютер;

ВСТУП

Концепція об’єднання окремих комп’ютерів в мережі набула свого розвитку майже одразу після винайдення перших обчислювальних машин. Тоді електронно-обчислювальні машини займали набагато більше місця ніж зараз: один комп’ютер міг займати ціле приміщення, тому мережа зазвичай складалася суто з двох взаємно-підключених між собою робочих станцій. Завдяки стрімкому розвитку технологій побудови комп’ютерних пристроїв сучасні мережі складаються не лише з ПК, а й з серверів, комутуючих та маршрутизуючих девайсів, мобільних телефонів та, навіть, розумних розеток.

Ключовим нововведенням, що фахівці з комп’ютерних мереж почали використовувати відносно недавно, є гнучка архітектура програмно-конфігурованих мереж. Цей підхід проектування та налаштування мережі дозволяє розділити процес управління та передачі даних за допомогою протокола «OpenFlow», що був розроблений співробітниками Стендфордського університету у 2007 році. До переваг використання саме такої реалізації мережі відносять зменщення рівня навантаження на окремі канали мережі, підвищений рівень безпеки та можливість запрограмувати мережу під свої потреби з використанням мережевого контролера.

В даній кваліфікаційній роботі бакалавра буде розроблено комп’ютерну мережу для ІТ-компанії, а, як відомо, подібних компаній з кожним днем відкривається все більше. Для реалізації якісної комп’ютерної системи варто обирати розробки передових компаній зі світовим ім’ям, як наприклад Cisco, мережеві прилади якої використовують по всьому світу.

Метою кваліфікаційної роботи є проектування комп’ютерної системи ІТ-компанії з детальним пропрацюванням побудови, особливостей налаштування мережевих пристроїв та системи безпеки корпоративної мережі.

Актуальність даної кваліфікаційної роботи вкрай висока, адже кількість ІТ-компаній, що будують свої офіси у великих містах зростає кожен день. Лише у Дніпрі існує більше десяти офісів компаній ІТ-сфери, а в Києві їх взагалі більше в рази. Побудова офісу для компанії, що надає послуги з розробки

програмного забезпечення це не лише важлива частина економічної статегії для централізації працівників та поліпшення комунікації між ними, а й можливість залучити нових клієнтів за рахунок більш високого іміджевого рівня компанії. Це пов’язано з тим, що невеликі аутсорсингові компанії працюють переважно з такими ж за рівнем клієнтами. ІТ-компанії, що прагнуть розвиватися в сфері намагаються відкрити фізичні офіси в найбільших містах України, та працювати з великими замовниками. Саме тому запит на створення подібних комп’ютерних систем буде актуальним ще довгі роки.

Результати виконаної кваліфікаційної роботи можливо застосовувати не лише для компаній в сфері інформаційних технологій, а й для подібних за структурою установ, наприклад маркетингових, бухгалтерських, туристичних чи фінансових фірм.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп’ютерної системи ІТ-компанії «BAS-IQ»

Об'єктом проектування в даній кваліфікаційній роботі є мережа ІТ-компанії «BAS-IQ», отже галузь виробництва це інформаційні технології. Ця сфера є надзвичайно розвиненою на сьогоднішній день, адже інформаційними продуктами користується майже кожен житель не тільки України, а й світу.

Інформаційні технології (ІТ) – це сфера, що включає в себе сукупність методів та засобів, що необхідні для обробки та обміну даними. Сфера інформаційних технологій включає в себе як розроблення локальних мереж та невеликих мобільних додатків, так і величезних систем з використанням терабайтних серверів для збереження інформації в базах даних.

Зазвичай, коли людина уявляє собі галузі ІТ, то відносить туди лише програмістів, але це не вірно, адже над створенням програмного забезпечення працюють ще й тестувальники, дизайнери, маркетологи та менеджери. Саме через кількість залучених фахівців та високі економічні показники ця галузь є однією з ключових в нашій країні.

Існує велика кількість українських компаній, що надають послуги з розробки програмного забезпечення як на внутрішній ринок, так і за кордон. Серед них є такі світові гіганти як «SoftServe», «EPAM», «Luxoft» та інші. За рахунок іноземних капіталів економіка країни посилюється, отже держава дуже зацікавлена в розвитку ІТ-сфери. Про це свідчить не лише наявність спеціальних регуляторних умов для таких компаній (наприклад «Дія City»), а й загальне збільшення рівня цифровізації державних послуг.

Зараз цифровізація не лише державних, а й будь-яких послуг поступово набирає оберти. Кожна компанія вважає за необхідність мати власний веб-сайт та можливість працювати з онлайн-клієнтами. Саме такий підхід ведення бізнесу в поточних реаліях надає конкурентну перевагу, тому фірми різних рівнів вкладають великі гроші в побудови власних веб-платформ для залучення нових

клієнтів. Кількість подібних замовлень зростає, тому й пропозиції щодо виконання таких завдань закономірно збільшуються.

На теперішній час в Україні працює близька 100 тисяч розробників програмного забезпечення, що значно переважає кількість фахівців в будь-якій європейській країні. Це зумовлено високим рівнем заробітної плати та великою кількістю можливостей працевлаштування. Бонусом для таких співробітників є можливість переїзду до більш розвинених кран, адже зазвичай головні офіси компаній знаходяться поза межами України.

Мережа, що проектується в рамках даної кваліфікаційної роботи повинна забезпечити з'єднання між трьома офісами компанії та підключення їх до глобальної мережі Інтернет. Робочі комп'ютери повинні бути об'єднані в локальні підмережі за допомогою комутуючих пристроїв та маршрутизаторів.

Потужність комп'ютерів повинна задовільняти рекомендованим вимогам таких програм розробки програмного забезпечення як VS Code, Sublime Text, PyCharm, Android Studio. Кожен комп'ютер повинен бути оснащений операційною системою Windows 10 Pro.

Крім того необхідно забезпечити високий рівень захисту даних, адже це є дуже важливим фактором для замовника при виборі аутсорсингових компаній-партнерів.

1.2 Характеристика і структура IT-компанії «BAS-IQ»

IT-компанія «BAS-IQ» є провідним постачальником послуг зі створення програмних застосунків для середнього та великого бізнесу. Клієнтська база компанії включає в себе як українських, так й іноземних клієнтів (Франція, Німеччина, США).

Основними напрямками діяльності компанії є:

- розробка програмного забезпечення;
- тестування програмного забезпечення;
- створення UI/UX дизайну для програмних продуктів;
- покращення продуктивності вже існуючих кодових рішень;

- переписування аплікацій на більш новітні мови програмування.

Компанія «BAS-IQ» використовує сучасні технології програмування для розробки аплікацій, серед яких мови високого рівня Python, Kotlin, JavaScript з фреймворками React, Angular, NodeJS. Такий стек технологій дозволяє бути конкурентними на зарубіжних ринках та успішно виконувати клієнтські замовлення.

Крім того фірма проводить навчальні курси в одному з філіалів для подальшого працевлаштування нових співробітників. Така система вже зарекомендувала себе як чудова альтернатива звичайному пошуку співробітників на сайтах вакансій, адже коли людина без досвіду приходить до компанії, яка навчає її працювати на реальних проектах, то вона буде ставитися більш лояльно до поточного місця роботи.

Крім того працівники компанії, які виділяють час навчанню студентів академії можуть швидше просуватися по кар'єрній драбині, бо для того, щоб навчати необхідно постійно поновлювати свої знання в тій чи іншій технології розробки.

Для розробки вимог до комп'ютерної системи IT-компанії «BAS-IQ» із застосуванням сучасних мережних технологій, необхідно проаналізувати структурні підрозділи, що будуть поєднані в мережу.

Компанія базується в місті Дніпро, Дніпропетровської області, та має в своїй структурі три офіси, серед яких є головний офіс та два філіали. Основні відомості про компанію-замовника. В штаті компанії 89 співробітників.

Організаційна структура компанії «BAS-IQ» представлена на рисунку 1.1.

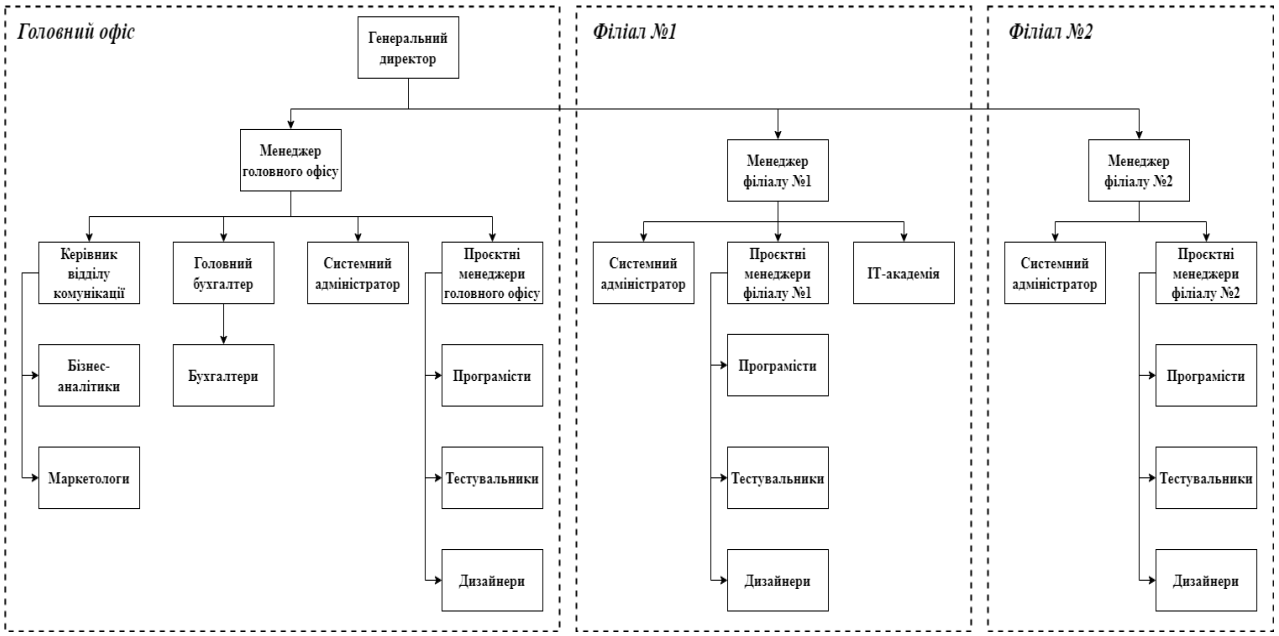

Рисунок 1.1 – Організаційна структура IT-компанії «BAS-IQ»

Штат компанії включає в себе топ-менеджмент, керівників відділів, маркетологів, бізнес-аналітиків, бухгалтерів, системних адміністраторів, проєктних менеджерів та фахівців в різних напрямках IT-індустріїї, а саме дизайнерів, розробників та тестувальників програмного забезпечення. Крім того є одна людина, що займається менторством та організацією проведення занять в академії при компанії.

Таблиця 1.1 – Штат компанії «BAS-IQ»

Посада	Кількість співробітників
1	2
Генеральний директор	1
Менеджер офісу	3
Керівник відділу комунікацій	1
Бізнес-аналітик	4
Маркетолог	2
Головний бухгалтер	1
Бухгалтер	2

Продовження таблиці 1.1

1	2
Системний адміністратор	3
Проєктний менеджер	11
Програміст	38
Тестувальник ПЗ	14
Дизайнер	8
Ментор ІТ-академії	1

Найбільше повноважень має генеральний директор. Саме він приймає ключові рішення, що можуть кардинально впливати на розвиток компанії, її економічні показники. Такі рішення директор приймає на основі звітів та рекомендацій менеджерів та керівників відділів.

На другому рівні після нього знаходяться топ-менеджери офісів, по одній людині в кожній будівлі.

Відділ комунікацій включає в себе спеціалістів з бізнес-аналізу та маркетингу.

Бухгалтерія підприємства налічує 3 працівники, з яких одна людина виконує роль головного бухгалтера. Основна задача цього відділу – забезпечення коректності розрахунків заробітних плат та перевірка договорів з клієнтами.

Системний адміністратор забезпечує швидке усунення проблем з апаратним та програмним забезпеченням, створює облікові записи для працівників компанії, а також стежить за цілісністю даних на серверах.

Команда, що безпосередньо займається розробкою ПЗ складається з проєктних менеджерів, програмістів, тестувальників та дизайнерів.

Менеджер проєкту повинен забезпечити продуктивну роботу команди та організовувати зустрічі (у тому числі онлайн) для обговорення вимог до програмних продуктів із замовниками.

Основним завданням дизайнера в компанії є візуалізація програмного продукту, виходячи з ідей та технічних вимог клієнтів.

До обов’язків розробників програмного забезпечення входить:

- написання програмного коду згідно клієнтським вимогам;
- виправлення недоліків у власному коді, або у legacy-проєктах;
- перевірка правильності написання кодових конструкцій інших розробників (так зване «code-review»);
- участь у демонстраційних сесіях із замовниками.

Обов’язки тестувальників програмного забезпечення:

- перевірка того, що функціонал створених аплікацій задовольняє клієнтським вимогам;
- написання тест-кейсів та чек-лістів;
- проведення регресійного тестування з певною періодичністю;
- написання тестової документації та уточнення вимог із замовником.

Як було зазначено раніше, деякі з фахівців проводять лекції із навчання сучасним технологіям у створенні програмних продуктів для студентів IT-академії в офісі філіалу №2. Організацією занять займається ментор IT-академії, крім того він проводить деякі з них.

1.3 Стислі відомості про технології збору й передачі даних та топологічна схема розміщення структурних підрозділів IT-компанії «BAS-IQ»

IT-компанія «BAS-IQ» до моменту проектування корпоративної мережі не мала централізованих офісів та центрів збору та передачі інформації. Замість цього співробітники працювали в коворкінгах або в дистанційному форматі із дому.

До створення локальних мереж у філіалах та головному офісі інформація, що стосується програмних розробок зберігалася на віддалених хмарних серверах систем контролю версій накшталт GitHub та Bitbucket. Проєктна документація та файли з клієнтськими вимогами зберігалися на приватних хмарних сховищах, зокрема Google Drive та Atlassian Confluence.

Передача інформації між комп’ютерами співробітників з різних районів

міста виконувалась за допомогою пересилання через сервіси файлообміну, але цей спосіб є неприпустимим для компаній більш високого рівня.

Отже для того, щоб розвиватися та заохотити нових клієнтів керівництвом компанії було прийняте рішення побудови корпоративної мережі в фізичних офісах та використання власних серверів в додаток до раніше використовуваних систем контролю версій.

Компанія базується в місті Дніпро, Дніпропетровської області, та має в своїй структурі три офіси, серед яких є головний офіс та два філіали:

- адреса головного офісу 49000, Україна, Дніпропетровська обл., м. Дніпро, вул. Барикадна 16, бізнес-центр «Кудашевський»;
- адреса філіалу №1 49000, Україна, Дніпропетровська обл., м. Дніпро, пр. Яворницького 22, бізнес-центр «Atrium»;
- адреса філіалу №2 49000, Україна, Дніпропетровська обл., м. Дніпро, пров. Шевченка 9.

На рисунку 1.2 зображена схема розташування офісів компанії в місті Дніпро, Дніпропетровська область.

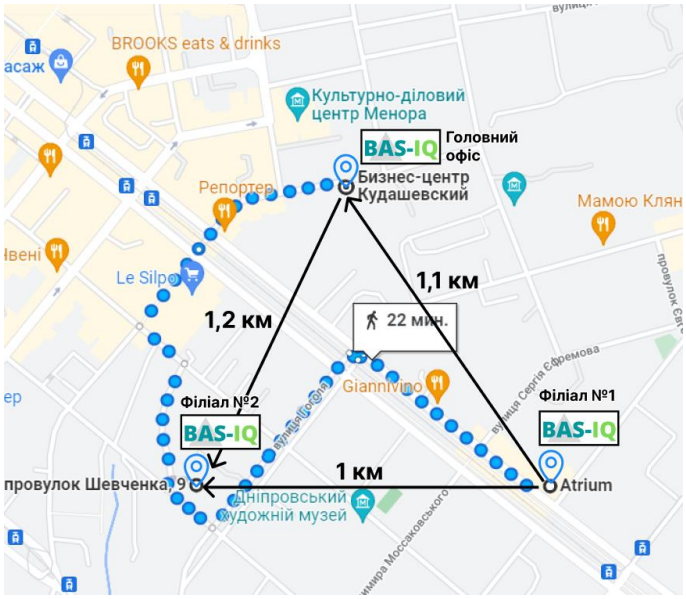

Рисунок 1.2 – Схема топологічного розміщення офісів IT-компанії «BAS-IQ»

Офіси розташовані в центрі міста, що є сприятливим фактором для

співробітників, адже дістатися до місця роботи можна буде різними видами громадського транспорту. Відстань між офісами близька одного кілометра, тому за необхідності спіробітники зможуть переходити між приміщеннями. На рисунках 1.3 – 1.7 зображено плани приміщень, в які необхідно буде інтегрувати мережу.

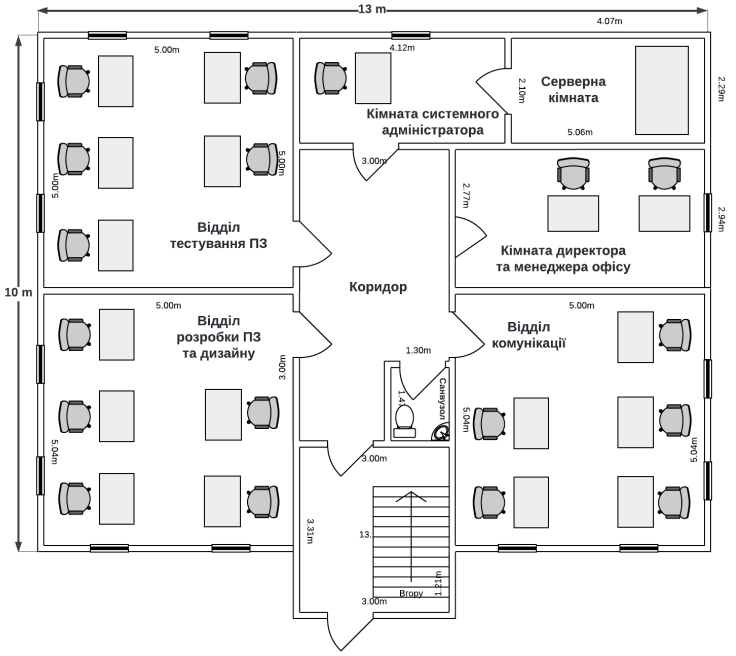

Рисунок 1.3 – План першого поверху головного офісу

Рисунок 1.4 - План другого поверху головного офісу

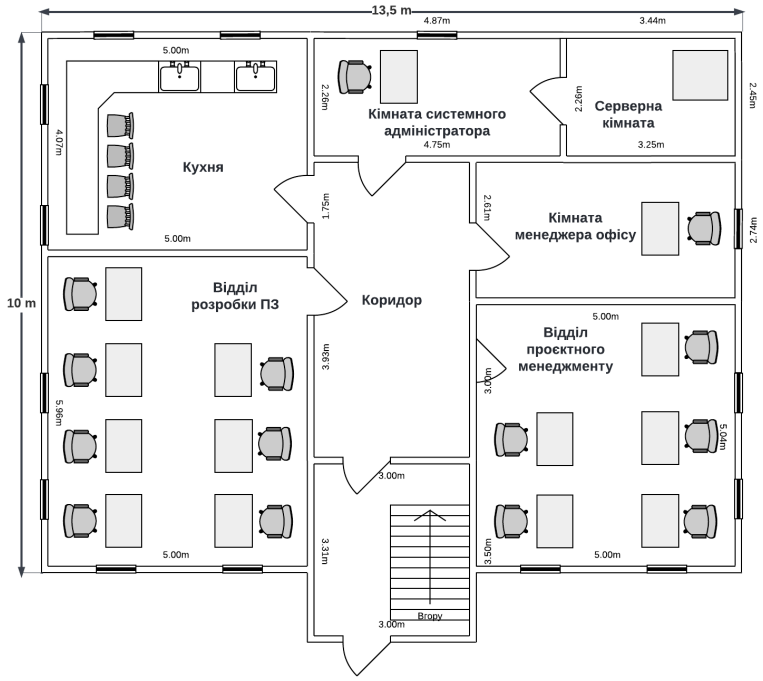

Рисунок 1.5 - План першого поверху офісу філіалу №1

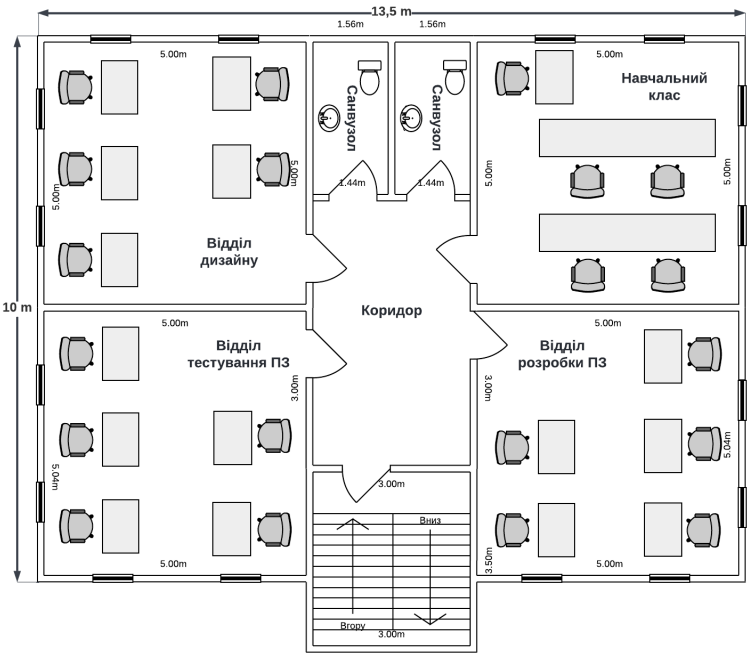

Рисунок 1.6 - План другого поверху офісу філіалу №1

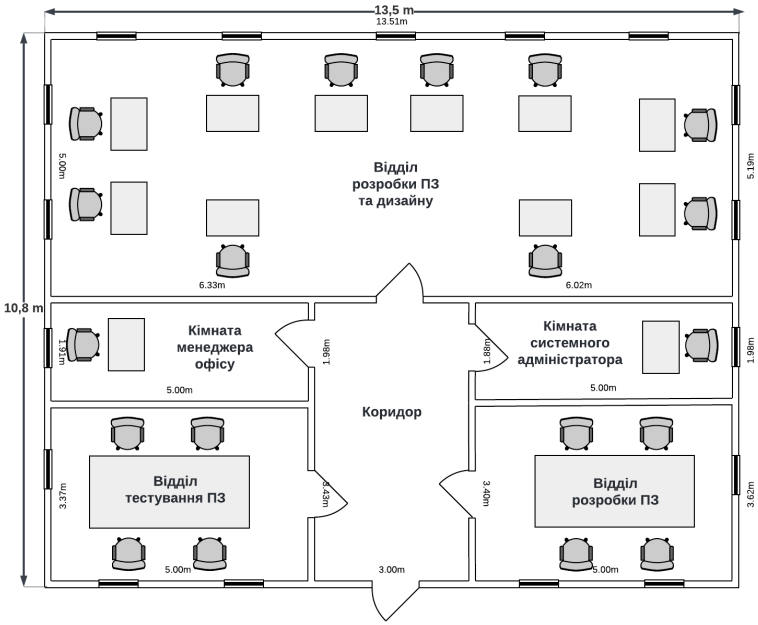

Рисунок 1.7 - План офісу філіалу №2

Плани офісних будівель є дуже важливими, адже саме на основі них будуть написані технічні вимоги, зокрема для системи кабелів.

1.4 Принципи та технічні способи інформаційного забезпечення IT-компанії «BAS-IQ»

Інформаційне забезпечення будь-якої IT-компанії розвинене на високому рівні порівняно з іншими сферами виробництва. Воно являє собою сукупність даних, метрик, технічної документації, програмних кодів, записів корпоративних засобів спілкування та персональної інформації клієнтів та співробітників.

Інформаційне забезпечення поділяється на внутрішнє і зовнішнє. До внутрішнього забезпечення відносять інформацію, що з’являється всередині мережі та зберігається на фізичних носіях в межах офісів компанії, наприклад локальні копії кодових репозиторіїв або створеної проєктної документації. Здатність обмінюватися даними в межах локальних мереж також відносять до внутрішньої системи інформаційного забезпечення.

Зовнішнє інформаційне забезпечення – це в першу чергу здатність отримувати інформацію з глобальної мережі Інтернет та обмінюватися даними

поза межами корпоративної локальної мережі. Сюди відносять файли, що зберігаються на віддалених хмарних сховищах, наприклад розроблені програмні продукти, що обслуговуються на стороннії хостингах.

Інформаційне забезпечення корпоративної мережі компанії «BAS-IQ» базується на наступних принципах:

- доступність (кожен співробітник має змогу використати інформаційне забезпечення для задовільнення робочих потреб);
- надійність (у разі виходу з ладу системи збереження та обміну інформацією дані не будуть зруйновані);
- безпечність (при користуванні інформаційним забезпеченням співробітники не мають загроз зараження робочих станцій вірусом);
- стандартизація (наявність стандартів обміну та обробки інформації).

Інформація може зберігатися та оброблюватися в комп'ютерній мережі за виконання декількох умов. Перш за все інформація має існувати у певному файловому вигляді. На етапі створення дані зберігаються локально на комп'ютері співробітника та для того, щоб передати їх колегам необхідно встановити інформаційний зв'язок.

Цей зв'язок може бути наданий або шляхом прямої передачі даних через переносні носії, або з використанням Інтернету. В першому випадку для забезпечення передачі даних необхідно завантажити інформацію на оптичний або флеш-носій та підключити до іншої робочої станції. Цей варіант передачі даних є надійним, адже конфіденційні дані ніхто не зможе викрасти, але процес передачі інформації занадто довгий, порівняно з веб-шерінгом. Другий спосіб, де інформація поширюється мережею через певні файлообмінники або хмарні сервіси накопичення даних, є широкопоширеним та працівники компанії «BAS-IQ» використовують саме його.

Далі, після отримання інформації її можна передати іншим колегам, редагувати або використати для створення програмного забезпечення. Інформацію, що працівники потребують зберегти для архіву або подальшого використання можна зберігати на корпоративних серверах або хмарних

сховищах даних. Друга опція дуже поширена саме у маленьких стартапах, де грошей на власний сервер просто немає. В інформаційній системі об’єкта впровадження інформація зберігається як на локальних серверах так і хмарі, адже такий комбінований спосіб мінімізує можливість втрати даних.

1.5 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об’єкта проєктування, відомих рішень у галузі проєктування комп’ютерних систем

Стрімкий розвиток інформаційних технологій зумовив появу декількох різних способів передачі інформації в комп’ютерних мережах. Раніше дані могли передавати лише за допомогою радіохвиль та електричних сигналів, але зараз можливо використовувати також магнітні та світлові імпульси.

Магнітні імпульси є більш застарілою технологією саме для сфери передачі дискретних даних, але вони широко використовуються в медичній сфері, наприклад для томографічних досліджень. Раніше цей спосіб збереження даних був дуже актуальним, проте зараз магнітні дискети не використовуються, адже вони морально застаріли й мають занадто малий вміст пам’яті.

Для швидкісної передачі даних в між підмережами прийнято використовувати оптоволоконні світлові кабелі, які здатні передавати дані зі швидкістю 1 Гбіт/с., а от для об’єднання хостів підмереж доцільно використати більш дешеву «виту пару».

Крім того розвиток смартфонів зумовив поширення використання технологій бездротової передачі даних Wi-Fi. За допомогою такого способу можна підключити портативний прилад, за умови наявності потрібного адаптера для встановлення зв’язку, до комп’ютерної мережі та обмінюватися даними. Особливу популярність зараз набирає 5G-підключення, адже швидкість завантаження даних на портативні пристрої значно збільшується, порівняно із попереднім стандартом 4G.

Далі варто розглянути сучасні методи та принципи проєктування комп’ютерних мереж. З поміж всіх методів побудови об’єкта проектування

зазвичай виділяють два. Перший метод базується на виборі вже спроектованих рішень від відомих мережних компаній, таких як Cisco. Перевага такого способу полягає в бюджетності, але з іншого боку така мережа може не задовольнити абсолютно всі потреби, хоча зазвичай для простих замовлень цього може вистачити.

Інший метод включає використання унікальних розробок в сфері комп'ютерних мереж, які дозволяють зробити систему максимально гнучкою під конкретні вимоги замовника. Але й такий метод за основу бере використання стандартних рішень.

Перш ніж вибрати один з підходів для побудови корпоративної мережі, необхідно оглянути поточний стан приладів, а саме маршрутизаторів, комутаторів, серверів та комп'ютерів. Далі треба обрати системне програмне забезпечення для серверів та хостів мережі. Після цього варто перевірити системні сервіси та бази даних, адже обмін інформацією є однією з ключових функцій мережі. До цих сервісів відноситься веб-служба, домен електронної пошти та інші потрібні служби корпоративного спілкування.

При впровадженні мережі необхідно спиратися на наступні принципи:

- можливість масштабування (підключення додаткових хостів чи облікових записів без кардинальної зміни заданих налаштувань);
- самостійність (збереження робочого стану системи за умови виходу з ладу окремого елементу чи підмережі);
- ефективність (означає забезпечення необхідної якості передачі даних при мінімальних витратах);
- відновлювальність (створення резервних копій користувацької інформації та мережевих налаштувань для відновлення системи у разі критичних збоїв).

Для полегшення процесу моніторингу стану елементів корпоративної мережі можна зробити її програмованою, тобто додати в топологію контролер.

Програмовані мережі стали одним із найпопулярніших способів організації розгортати системи різного масштабу за останні роки. Ця технологія

допомагає організаціям швидше розгортати програми та знижувати загальну вартість імплементації [1].

Програмовані мережі мають низку ключових переваг перед традиційною моделлю орагнізації, так наприклад одна з головних переваг, наданих SDN, це можливість управління мережею з централізованої точки моніторингу. Це надзвичайно корисно, оскільки традиційну інфраструктуру може бути важко контролювати, особливо якщо є безліч різних систем, якими потрібно керувати індивідуально.

Крім того такі мережі значно легше масштабувати. З точки зору безпеки такі SDN є більш надійними ніж звичайні мережі, адже контролер надає адміністратору централізоване управління та моніторинг стану безпеки системи в цілому та окремих компонентів.

1.6 Завдання і мета роботи

Метою роботи є проектування корпоративної комп'ютерної мережі IT-компанії «BAS-IQ» із докладною обробкою питань налаштування апаратно-програмного мережного комплексу для подальшого впровадження цієї мережі в експлуатацію. Топологічна схема мережі задана замовником та наведена на рисунку 1.8.

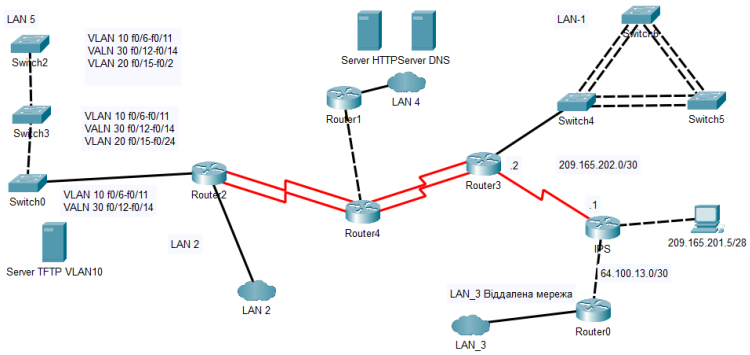

Рисунок 1.8 - Топологія за умовами технічного завдання

Для того, щоб вирішити поставлену мету в кваліфікаційній роботі необхідно виконати наступні завдання:

- аналіз мережевої архітектури для корпоративної мережі;
- аналіз заданої схеми топології корпоративної мережі;
- розробка схеми комплексу технічних засобів;
- вибір апаратного забезпечення корпоративної мережі;
- налаштування мережевого обладнання для успішної передачі даних;
- налаштування адресації кінцевих пристроїв;
- запровадження заходів щодо підвищення рівня безпеки мережі;
- розробка програми моніторингу досяжності мережевого обладнання.

Для успішного вирішення поставлених завдання потрібно уважно проаналізувати вимоги та потреби клієнта. Після цього можна починати процес проектування мережі та вибору компонентів. На наступному етапі, а саме налаштування корпоративної мережі, варто приділити особливу увагу захисту від несанкціонованого доступу до клієнтської інформації. Крім того при налаштуванні та побудові необхідно створити умови для легкого масштабування мережі за необхідності.

1.7 Визначення можливих напрямків рішення поставлених завдань

Першим етапом виконання роботи є вибір мережевої архітектури, тобто методу реалізації фізичиного та канального рівнів моделі OSI в корпоративній мережі. Вдалий вибір архітектури для комп’ютерної мережі це основа успішного проектування і побудови, адже системи кодування сигналів, швидкість передачі даних, формати мережевих кадрів і методи доступу можуть сильно відрізнятися в залежності від вимог клієнта.

Найбільш відомі мережеві архітектури це Ethernet, Token Ring та ARCnet. Вирішальними факторами при виборі з поміж цих опцій є:

- вимоги до пропускної здатності каналів;
- відстань між вузлами мережі;
- вимоги до надійності систем зв’язку;
- фінансові можливості замовника.

В даній роботі обрано архітектуру Ethernet, адже вона задовольняє всім

вимогам та є найпоширенішею серед інших варіантів.

Наступний етап роботи це розробка схеми топології корпоративної мережі. Завдяки запропонованому варіанту завдання, що крім схеми адресації містить й схему топології, можна одразу переходити до моделювання мережі в Packet Tracer за поставленим умовами розташування приладів.

Після визначення кількості апаратних засобів, та того, як вони будуть з'єднані між собою можна переходити до вибору конкретних моделей приладів. На даному етапі необхідно визначити компанію, що буде постачати мережеве обладнання та комп'ютери. Компанія Cisco є одним з лідерів експорту мережевих девайсів на міжнародний ринок, тому доцільно вибирати моделі маршрутизаторів та комутаторів саме з каталогу цієї фірми. Крім того навчальні курси Cisco були імплементовані в освітню програму спеціальності «Комп'ютерна інженерія», тому не потрібно витрачати час на вивчення способів налаштування мережевих приладів та сервісів на них.

Для вирішення завдання моніторингу та контролю корпоративної мережі можливо впровадити контролер, що буде збирати інформацію про поточний стан приладів з усіх підмереж. За допомогою веб-додатку «Cisco Network Controller» адміністратор може отриматити дані про кількість активних маршрутизаторів, комутаторів та хостів, а також графіки стану мережі за певний проміжок часу.

Завдання конфігурації апаратної частини корпоративної мережі може бути виконано завдяки великій кількості офіційної документації, де можна ознайомитися з принципами використання всеможливих команд в Cisco OS. Необхідні веб-ресурси доступні не лише англійською мовою, а й перекладені на українську на спеціальних форумах. Також вище було зазначено, що в освітній програмі спеціальності були практичні курси з налаштування обладнання та запровадження сучасних сервісів, наприклад DNS, DHCP чи створення тунельних приватних з'єднань VPN.

Для виконання завершального завдання, а саме запровадження захисту від несанкціонованого доступу, перш за все варто використовувати систему корпоративного облікового доступу. Тобто кожен співробітник компанії буде

мати унікальний обліковий запис та пароль до нього. Таким чином лише справжні співробітники зможуть отримувати доступ до корпоративної пошти, ввімкнення робочих комп'ютерів та зміни будь-яких налаштувань елементів корпоративної мережі. Крім того сучасним трендом IT-компаній є використання віддаленого сервісу VPN для роботи, що забезпечує надійне шифрування даних в мережі.

1.8 Обґрунтування вибраного напрямку інженерного рішення

Для проектування було обрано мережеві прилади компанії Cisco, адже вони надають змогу реалізувати корпоративну мережу якісно та надійно. Мережеві прилади цієї компанії відзначається своєю високою ефективністю та великою кількістю допоміжних матеріалів. У разі виникнення питань шодо установки чи конфігурації маршрутизаторів чи комутаторів цієї компанії інженер може звернутися до офіційної англомовної документації чи знайти відповідь на спеціалізованих інтернет-форумах.

Крім того рівень безпеки обладнання від Cisco дуже високий, що реалізовано зокрема присутністю вбудованих брандмауерів для виявлення можливих загроз. Обладнання від Cisco Systems підтримує всі найсучасніші мережні технології, зокрема:

- списки контролю доступу для пакетної фільтрації трафіку;
- підтримка протоколів SSH, SNMPv3 і HTTPS, що забезпечують шифрування каналів управління;
- підтримка централізованої автентифікації, авторизації та обліку адміністративної діяльності;
- забезпечення цілісності та конфіденційності даних на мережному рівні з використанням стека протоколів IPSec.

Також до переваг співпраці з таким постачальником мережевих технологій є програма Cisco Packet Tracer, за допомогою якої можна моделювати комп'ютерну мережу, тренуватися в її налаштуванні чи запровадити нові сервіси в тестовому середовищі без ризику для корпоративного обладнання.

Завдання передбачає налаштування віртуальних локальних мереж (VLAN) в одному з філіалів компанії. Метод налаштування буде викладений в одному з наступних розділів кваліфікаційної роботи, а от ключові переваги та недоліки VLAN необхідно розуміти заздалегіть. До переваг віртуальних локальних мереж відносять:

- підвищення рівня безпеки окремих віртуальних мереж;
- скорочення кількості широкомовних запитів, що зменшують пропускну здатність каналів мережі;
- зменшення витрат на кабельне та комутуюче забезпечення, адже віртуальні мережі налаштовуються суто кодовим способом;
- можливість об’єднати в мережу хости, що під’єднані до різних комутаторів.

До недоліків запровадження VLAN відносять необхідність використання спеціалізованого протоколу GVRP для складних корпоративних мереж. Проте цей недолік не є критичним та не завадить запровадити створення віртуальних локальних підмереж для співробітників раізних відділів на одному з філіалів фірми.

На додачу до того вдалим рішенням буде налаштування віртуальної приватної мережі (VPN) між головним офісом компанії та Інтернет провайдером, адже це значно підвищить рівень безпеки для користувачів мережі. З використанням такої технології дані співробітників буде досить складно викрасти, адже вони будуть зашифровані. Таким чином співробітники, що працюють віддалено з коворкінгів або з дому зможуть отримати захищений доступ до корпоративних ресурсів без ризику для важливої клієнтської інформації, що зберігається на серверах компанії.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до системи ІТ-компанії «BAS-IQ»

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонування системи ІТ-компанії «BAS-IQ»

2.1.1.1.1 Перелік підсистем, їх призначення й основні характеристики

Комп'ютерна система ІТ-команії «BAS-IQ» призначена для забезпечення задач комутації кінцевих пристроїв співробітників та маршрутизації даних, що вони генерують та повинна складатися з наступних підсистем:

- підсистема «1 поверх головного офісу», яка містить мережу для робочого простіру з 18 комп'ютерів, а також серверну кімнату, де розташовано 2 сервери;

- підсистема «2 поверх головного офісу», яка в свою чергу містить мережу, що виділена на 21 комп'ютер та 1 мережевий контролер;

- підсистема «1 поверх філіалу №1», що містить в собі робочий простір з 14 комп'ютерів та 1 сервер для автентифікації користувачів на маршрутизаторах;

- підсистема «2 поверх філіалу №1», що містить в собі мережу на 20 комп'ютерів, 5 з яких розміщені в навчальному класі ІТ-академії та не використовуються співробітниками для професійної розробки ПЗ;

- підсистема «Філіал №2», що є віддаленою мережею та має 20 комп'ютерів в своєму адресному просторі.

Кожна підсистема в свою чергу повинна забезпечити можливість надійного обміну та обробки інформації всередині локальних підмереж та захист її від несанкціонованого доступу. Обмін даними в мережі має здійснюватися за допомогою стеку протоколів, що підтримують віртуалізацію локальних мереж, створення приватних тунельних з'єднання та використання засобів керування базами даних MS SQL та засобів програмування Python, React та Node JS, Kotlin, Java.

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

Зв'язок між компонентами системи повинен забезпезпечуватися за допомогою об'єднання їх в єдину мережу шляхом кабельного LAN-підключення між собою кабелем типу «вита пара». Для об’єднання між собою роутерів різних структурних підрозділів використовується оптоволоконний кабель. Передача даних відбувається за допомогою протоколу Ethernet зі швидкістю до 100Мбіт/сек на рівні доступу та до 1Гбіт/сек на рівні розподілу та ядра.

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

Доступ до внутрішніх корпоративних, зовнішніх ресурсів чи суміжних систем має здійснюватися через мережу Інтернет.

Зокрема необхідно забезпечити взаємодію з серверами GitHub та Bitbucket для передачі файлів на хмарні сховища цих сервісів. Крім того для бухгалтерського обліку необхідно забезпечити створення корпоративного робочого простору у програмі «WorkDay», а для роботи системних адміністраторів – у сервісі «HelpDesk».

2.1.1.1.4 Вимоги до режимів функціонування системи

Система повинна забезпечити декілька режимів функціонування, а саме режим повної активності, режим часткової активності та режим економії електроенергії.

Режим повної активності передбачає ввімкнення серверів, мережевого обладнання та більше 50% комп’ютерів одночасно. Такий режим функціонування буде використовуватися кожен робочий день, тому необхідно забезпечити високий рівень якості компонентів мережі та виконаних консольних налаштувань.

Режим часткової активності передбачає те, що крім серверів та мережевих пристроїв буде ввімкнено менше 49% робочих комп’ютерів. Такий режим

зумовлений можливими карантинними обмеженнями, коли урядовчі органи вводять обмеження на кількість працівників в офісі.

Режим економії електроенергіїї функціонує у вихідні дні, коли крім роутерів, комутаторів та серверів ввімкнено менше 10% робочих комп'ютерів.

Варто зазначити, що режим роботи різних офісів в певні дні може відрізнятися, що зумовлює більший рівень децентралізації системи, що знижує ризики у разі поламки або хакерських атак.

2.1.1.1.5 Вимоги до діагностування системи

Для діагностування стану системи необхідно розробити алгоритм, що буде збирати та оброблювати дані про стан досяжності мережевих приладів. Для цього необхідно інтегрувати в одну з підмереж компанії мережевий контролер від компанії Cisco. Cisco Network Controller API дає можливість отримати дані у зручному JSON форматі та обробити їх взалежності від потреб адміністратора.

В якості компонента системи треба розробити програму мовою Python, що за допомогою зібраної контролером інформації, може відправляти електронні листи на корпоративну пошту адміністратора у разі виявлення поламок. Сформований електронний лист буде містити ім'я приладу, його MAC-адресу та причину недосяжності. Всі ці дані будуть зібрані з JSON файлу та оброблені програмним кодом.

2.1.1.1.6 Перспективи розвитку, модернізації системи

Система повинна мати можливість масштабування, тобто розширення існуючої кількості хостів без додаткових складнощів. Для цього необхідно виділити додаткові порти на комутаторах та розетки. Зважаючи на можливе розширення компанії за рахунок аренди додаткових поверхів тих же приміщень, де базуються структурні підрозділи, необхідно забезпечити можливість обслуговування 504 кінцевих пристроїв за умови придбання необхідної кількості додаткових комутаторів та кабельного забезпечення.

Крім того необхідно вибирати робочі комп'ютери, виходячи з тенденцій

розвитку середовищ розробки програмного забезпечення. Запас продуктивності процесора та кількості оперативної пам’яті має мінімум вдвічі перевищувати рекомендовані апаратні вимоги.

2.1.1.2 Показники призначення

Комп’ютерна мережа IT-компанії «BAS-IQ» має функціонувати безперебійно та з виконанням всіх необхідних функцій, а саме обмін інформацією між робочими комп’ютерами, доступ до Інтернет-ресурсів та систем корпоративного зв’язку.

Для того, щоб зрозуміти ступінь відповідності системи її призначенню використовують наступні показники:

- кількість робочих комп’ютерів, що оснащенні необхідним для роботи програмним забезпеченням повинна дорівнювати 93;
- швидкість Інтернет-з’єднання має бути не менша за 100 Мбіт/сек;
- кількість запитів на перегляд даних в кодових репозиторіях не менше 8 на секунду;
- кількість запитів на редагування кодових репозиторіїв не менше за 5 на секунду;
- продуктивність робочого місця має мінімум вдвічі перевищувати рекомендовані вимоги середовища розробки програмного забезпечення PyCharm, Android Studio, VSCode;
- швидкість обробки 1 ехо-запита має бути не більшою за 1 секунду;
- цілодобове керування даними на серверах та хмарних сховищах;
- кількість облікових записів на поштовому сервері повинна дорівнювати кількості співробітників.

2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи ІТ-компанії «BAS-IQ»

2.1.1.3.1 Умови і регламент експлуатації, що повинні забезпечувати використання технічних засобів системи

Кількість персоналу було наведено в таблиці 1.1. Співробітники компанії «BAS-IQ» працюють за схемою 5 робочих та 2 вихідних дня. Робочий день складається 8 годин, та починається о 9.00 й закінчується о 18.00. Проте після закінчення робочого дня вимикаються лише робочі комп’ютери, а серверне й комутуюче обладнання залишається ввімкненим. Такий підхід не передбачує значних витрат електроенергії, та компенсується тим, що доступ до даних на сервері можна отримати й не в регламентований час, що є корисним для дистанційного формату роботи.

Система повинна бути експлуатована без додаткового обслуговування за умови справності ключових елементів мережі. Планове обслуговування комп’ютерної мережі має проводитися раз на 6 місяців, а термінове – за потреби.

2.1.1.3.2 Вимоги до параметрів мереж енергопостачання

Вимоги до параметрів мереж енергопостачання стандартні для України, регламентуються ДСТУ EN 50160:2014 «Характеристики напруги електропостачання в електричних мережах загального призначення» [2], та становлять:

- напруга 220 В (±10%);
- частота 50 Гц (±1%).

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

Для адміністрування мережі необхідно 3 системних адміністратора, по одному в кожний офіс компанії. Саме така кількість працівників дозволить швидко й якісно усувати будь-які збої в роботі мережі чи окремих комп'ютерів.

Системний адміністратор повинен мати релевантний досвід (від 1 року) в сфері моніторингу мережі подібного, або більшого розміру. Крім того компанія буде надавати доступ до освітніх курсів для покращення знань адміністраторів у сфері “Network troubleshooting”.

Контроль знань повинен відбуватися раз на півроку з можливістю кар’єрного розвитку в разі успішного проходження іспитів.

Оскільки компанія працює за схемою 5 робочих / 2 вихідних, режим роботи адміністраторів ідентичний.

2.1.1.3.4 Вимоги до складу, розміщенню запасних виробів і приладів

Для можливості швидкої заміни певних одиниць мережевого устаткування необхідний резерв з розрахунку по 1 запасній одиниці для кожного унікального типу приладу. Таким чином резерв кожного офісу повинен містити 1 маршрутизатор, 1 комутатор такого ж виробника та типу, що й використовуються в корпоративній мережі.

Крім того необхідно зберігати резервні периферійні прилади (клавіатури, комп’ютерні миші) у розрахунку +10% від загальної кількості працівників. Резервні прилади повинні зберігатися в кімнаті системного адміінстратора кожного офісу.

2.1.1.3.5 Вимоги до регламенту обслуговування КС

Обслуговування корпоративної мережі регламентується наступними правилами:

- технічне обслуговування здійснюється системним адміністратором;
- обслуговування маршрутизаторів та комутаторів відбувається не рідше ніж раз на 6 місяців;
- проведення технічного обслуговування здійснюється на основі заявки, що співробітник має створити в спеціалізованій програмі «HelpDesk»;
- якщо пристрій потребує ремонту адміністратор створює заявку в

спеціалізованій програмі «HelpDesk» та повідомляє менеджеру офіса про необхідність взяти зі складу або замовити певний прилад.

2.1.1.4 Вимоги до патентної чистоти

Апаратні засоби, що використовуються в корпоративній мережі повинні мати сертифікати для використання на території України.

Операційні системи, середовища розробки ПЗ та програми корпоративного зв'язку повинні бути ліцензійні. Забороняється завантаження будь-яких неліцензійних програм для уникнення небезпеки втрати даних.

2.1.1.5 Додаткові вимоги

2.1.1.5.1 Вимоги до кабельної системи

В додаткових вимогах доцільно розглянути вимоги до кабельної системи. Кабельна системи повинна мати стандартизовану структуру й топологію. Кабелі, що з'єднують між собою комп'ютери в локальну мережу мають бути достатньої довжини та мати входи до портів RJ-45. Швидкість передачі даних по таким кабельним каналам має бути не менша за 100 Мбіт/с. Зовнішні кабелі, що будуть з'єднувати офіси повинні мати захисне покриття від ультрафіолетових променів, отже доцільно використовувати оптоволокно.

2.1.1.5.2 Вимоги до налаштування корпоративної мережі

Забезпечити використання пристроями мережі єдиного адресного простору, що регламентується клієнтськими вимогами. Мережа повинна мати адресу 10.22.248.0/21. Цей адресний простір адрес необхідно розбити на 5 підмереж таким чином, щоб кількість адрес задовільняла таблиці 2.1.

Таблиця 2.1 - Кількість адрес в кожній з підмереж

LAN1	LAN2	LAN3	LAN4	LAN5
1	2	3	4	5
62	68	52	108	214

Блок адрес для каналів між маршрутизаторами задано клієнтом та становить 10.1.1.0/24. Цю мережу необхідно також розбити аби кожна з підмереж мала в своєму пулі по 2 доступні адреси. Середня інтенсивность вихідного трафіку в найбільшій мережі (другий поверх першого філіалу) становить 41 кадр/сек. Зовнішня адреса HTTP-сервера має бути 209.165.200.4. Середня довжина вихідного повідомлення в підмережі двугого поверху філіалу №1 становить 650 байт. Затримка передачі пакету в найбільшій мережі має бути меншою або дорівнювати 6 мс [3].

Крім того необхідно запровадити розподіл на 3 віртуальні локальні мережі на другому поверсі філіалу №1, при чому номери VLAN мають бути 11, 21 та 31. Management VLAN має ідентифікатор 99, а Native VLAN – 100. На серверах необхідно налаштувати служби HTTP, DNS та AAA. Доступ до Інтернету реалізувати через динамічну трансляцію адрес NAT. Між філіалом №2 та другим поверхом головного офісу необхідно створити приватний тунель VPN.

2.1.1.5.3 Вимоги до захисту інформації від несанкціонованого доступу

Запровадити обмеження на максимальну кількість унікальних MAC-адрес для портів комутаторів, що підключено до серверів. У разі виявлення підключення більше чим двох унікальних MAC-адрес до зазначеного інтерфейсу заборонити надсилання ехо-запитів, при цьому інтерфейс залишити ввімкненим.

Запровадити приватне тунельне з’єднання між філіалом №2 та другим поверхом головного офісу через Інтернет.

В підмережі другого поверху філіалу №1 розбити адресний простір на віртуальні локальні мережі.

Налаштувати сервер електронного листування та створити облікові записи для співробітників, щоб пересилання даних було максимально безпечне.

Для доступу до налаштування мережевого обладнання запровадити паролі з кількістю символів не менше за 5, а також налаштувати AAA-службу для авторизації на маршрутизаторах.

2.1.1.5.4 Вимоги до схоронності інформації при аваріях

Важливі дані по типу кодових репозиторіїв, договорів, електронних документів повинні мати резервні копії на хмарних сховищах, що формуються кожні 2 тижні. У разі виникнення аварійної ситуації дані повинні бути завантажені вручну до віртуальних сховищ за допомогою спеціальної корпоративної утиліти.

2.1.1.5.5 Вимоги до захисту від впливу зовнішніх чинників

Кожна будівля структурних підрозділів IT-компанії «BAS-IQ» повинна забезпечити захист персоналу та обладнання всередині від кліматичних чинників та стихійних лих, що не спричиняють фізичні руйнування корпусів будинків. Оптимальна температура повітря в офісному приміщенні згідно ДСН 3.3.6.042-99 [4] становить 21-24°C в теплу пору року, та 22-25°C в холодну. Оптимальна вологість в офісному приміщенні згідно того ж документа становить 40-60%. Ступінь захисту згідно ДСТУ IEC 60529:2019 [5] для розміщення в приміщенні офісу IP40.

Приміщення для серверної кімнати повинно бути без вікон, із потужною системою кондеціонування. Температура серверної кімнати має коливатися в межах 18 – 24 градусів Цельсія, а вологість має бути в межах 30 – 50%.

2.1.1.5.6 Вимоги до розрахунку інтенсивності вихідного трафіку найбільшої підмережі

Розрахувати трафік для найбільшої локальної підмережі, якою є мережа другого поверху філіалу №1 (LAN5). Кількість вузлів в цій підмережі регламентовано учбовим завданням та становить 214 хостів. Середня інтенсивність трафіку дорівнює 41 кадр/с. Середня довжина повідомлення чисельно становить 650 байт. Затримка передачі пакету має бути менша або дорівнювати 6 мс.

В ході виконання обчислень необхідно розрахувати наступні значення:

- коефіцієнт зайнятості обслуговуючого маршрутизатора;

- завантаження каналу передачі даних маршрутизатора;
- середня затримку кадру;
- середня довжину черги;
- середній час перебування пакета в черзі;
- пропускна здатність каналу.

Для розрахунку необхідно прийняти модель ділянки мережі як моделі СМО M/M/1 [3]. Після проведення розрахунків й отримання даних їх необхідно порівняти з максимально допустими параметрами обраних мережевих приладів.

2.1.2 Вимоги до функцій, виконуваних системою

2.1.2.1 Вимоги до функцій підсистем

Кожна з підсистем корпоративної мережі компанії «BAS-IQ», що описані в розділі 2.1.1.1.1, повинна забезпечувати наступні функції:

- працездатність кожного окремого вузла мережі;
- зберігання й обробка інформації щодо кодових застосунків та вимог клієнтів;
- можливість обміну інформацією між вузлами мережі;
- підтримка застосунків для корпоративного спілкування Zoom, Teams, Outlook;
- коректність роботи служб DNS, AAA та HTTP;
- задовільнення рекомендованих потреб додатків для розробки та тестування програмного забезпечення;
- зберігання даних як локально так і за допомогою хмарних сховищ;
- доступ кожного вузла до будь-яких дозволених чинним законодавством Інтернет-ресурсів;
- отримання та обробка даних з мережевого контролера з метою моніторингу стану системи;
- використання приватного тунельного з’єднання до віддаленої мережі через Інтернет;
- регулярне створення резервних копій даних на вузлах;

- шифрування паролів на мережевому обладнанні;
- можливість завантаження та відправки копій кодових репозиторіїв через системи контролю версій GitHub та Bitbucket.

2.1.2.2 Вимоги до якості реалізації функцій

Якість реалізація необхідних функцій комп'ютерної системи напряму залежить від вибраного обладання (апаратного й програмного забезпечення), а також коректності виконаних налаштувань. Вибір робочих комп'ютерів має ґрунтуватися на рекомендованих вимогах середовищ розробки програмних аплікацій, адже саме такими програмами будуть користуватися співробітники кожного дня.

Для раціонального вибору комутуючого обладнання необхідно знати майбутню кількість хостів мережі, бажану пропускну здатність та типи портів, що будуть використовуватися для підключення. Обрані маршрутизатори повинні бути оснащені необхідними портами для підключення комутаторів та мати можливість бездротового підключення хостів. Програмне ж забезпечення включає в себе як прикладні програми так і операційні системи. Як зазначалося раніше коже програмний продукт повинен бути ліцензованим, бо такий підхід мінімізує ризики втрати інформації та проникнення в мережу хакерів.

Ключовим аспектом безпеки мережі є облікова система, яка забезпечить підвищення рівня захисту від несанкціонованого доступу до корпоративної інформації. В таких системах важливим є видалення акаунтів працівників, що завершили роботу в компанії, адже в іншому випадку незакритий доступ може бути використаний шахрами з метою дискредитації компанії шляхом викриття важливої клієнтської або корпоративної інформації.На додачу до того, комп'ютерна система повинна забезпечити схоронність даних у випадку назвичайних ситуацій. Для цього вкрай важливо роботи копії важливих документів, баз даних та кодових репозиторіїв на надійних хмарних сховищах, адже будь-який фізичний носій інформації може вийти з ладу.

2.1.3 Вимоги до видів забезпечення

2.1.3.1 Вимоги до інформаційного забезпечення

Інформаційний обмін між компонентами комп’ютерної системи має відбуватися за допомогою передачі даних через Інтернет. Інформація, що була оброблена на комп’ютерах співробітника повинна бути завантажена на сервер, а у випадках кодових репозиторіїв ще й в хмарні системи контролю версій. Бази даних повинні мати актуальні резервні копії, що будуть використані у разі необхідності відновлення працездатності інформаційного забезпечення мережі.

Інформаційне забезпечення повинно бути надано в необхідній кількості та включати в себе інструкції з налаштування та виправлення помилок для апаратної та програмної частини системи.

Також необхідно надати рекомендації щодо експлуатації робочих станцій працівниками та перелік дій у разі виникнення надзвичайних ситуацій на робочому місці (включаючи хакерські атаки та фішинг).

2.1.3.2 Вимоги до лінгвістичного забезпечення

Все лінгвістичне забезпечення комп'ютерної системи для організації взаємодії з користувачем повинно використовувати українську або англійську мову. В якості мови операційної системи та окремих програмних продуктів співробітник може обрати будь-яку на свій розсуд.

Для обробки даних з мережевого контролера в системі використовується мова програмування високого рівня Python. Програмісти повинні використовувати мови програмування, що регламентуються клієнтськими вимогами та створеним на їх основі технічним завданням. Як було зазначено раніше для комп'ютерів в якості операційної системи треба використовувати Windows 10 Pro, для серверів Windows Server 2019, а для мережевих приладів стандартні ОС, які пропонуються виробников (наприклад Cisco OS для роутерів та комутаторів виробника Cisco).

В якості системи комунікації всередині команди використовується Jira або Trello. Для написання коду розробники можуть обрати один з наступни х

редакторів на власний розсуд: VS Code, Sublime Text, JetBrains PyCharm, Android Studio.

2.1.3.4 Вимоги до технічного забезпечення

Технічні елементи системи повинні мати сертифікати якості та бути протестовані після встановлення. Програмне забезпечення для робочих станцій повинно бути ліцензованим та протестованим на відсутність інсталяційних чи будь-яких інших помилок.

Маршрутизатори повинні забезпечити підтримку протоколу Ethernet для передачі даних зі швидкість не менше 100 Мбіт/сек. Комутатори повинні мати не менше 20 портів типу FastEthernet для підключення кінцевих пристроїв.

Комп’ютери повинні мати технічні характеристики, що задовільняють рекомендованим апаратним вимогам середовища розробки додатків для смартфонів Android Studio [6], а саме:

- ОС Windows 8 або 10 (64-bit);
- архітектуру процесора x86_64;
- процесор 2-го покоління Inter Core або більш новітній;
- 8 Гбайт оперативної пам’яті або більше;
- 8 Гбайт вільного місця на жорсткому диску.

Такі вимоги є мінімальними, отже для забезпечення можливості використання більш новітніх середовищ розробки та у режимі багатозадачності необхідно обирати модель ПК із запасом продуктивності.

2.1.3.5 Вимоги до організаційного забезпечення

Як зазначалося раніше для розмежування доступу до корпоративних ресурсів слід використовувати облікову систему персоналу. Вона передбачає створення облікового запису, що може бути використаний для доступу до корпоративних засобів зв’язку та хмарних сховищ даних. Обліковий запис є власністю компанії, тому співробітник, котрий вирішив піти з роботи автоматично втрачає доступ до свого акаунту та не може використовувати його

надалі для будь-яких цілей. Існують різні рівні доступу до інформації – «читання», «обмежене редагування», «редагування». Доступ для читання корпоративної документації, до якої входять технічні вимоги до програмних продуктів, файли з кодом та записи відео-конференцій, може отримати кожен співробітник компанії. Рівні доступу «обмежене редагування» та «редагування» передбачають наявність в обліковому записі позначки «editor» та «admin» відповідно. Такі позначки видаються шляхом запиту в менеджера офісу та для конкретного робочої області, отже доступ до зміни інформації отримують лише деякі співробітники, найчастіше менеджери своїх команд.

У разі помилкової дії співробітника адміністратор може відновити стан окремих документів або всієї робочої області на момент до внесення змін.

Також на комп’ютерах потрібно налаштувати засоби корпоративного спілкування, а саме Microsoft Teams та Outlook із присвоєнням корпоративного облікового запису для кожного працівника компанії. За допомогою цього запису кожен співробітник зможе отримати лізензований доступ до інших продуктів Microsoft, таких як Word, Excel, PowerPoint.

2.2 Розробка інженерних рішень для комп’ютерної системи IT-компанії «BAS-IQ»

2.2.1 Результати обстеження об'єкту

Для проектування будь-якої системи чи мережі необхідно розуміти цілі створення та вдало розрахувати виділений бюджет. Оскільки в кваліфікаційній роботі бюджет не був заданий, то доцільним буде обрати сучасні та потужні апаратні засоби. Компанія потребує 93 комп’ютери для забезпечення робочим місцем кожного співробітника та студентів IT-академії.

При виборі основної одиниці апаратної частини, комп’ютера, з якою персонал буде працювати весь робочий час необхідно приділити увагу таким параметрам як якість, надійність та зручність. Саме тому в якості ПК пропонується брати моноблочні системи, де все «залізо» може вміститися в невеликий корпус, при цьому не поступаючись в потужності повногабаратним

системним блокам. Такі комп'ютери не займають багато місця та повністю задовольняють вимогам для розробки та тестування програмного забезпечення.

Наступним етапом є вибір мережевих пристроїв, від яких буде залежати злагоджена робота цілої системи. Кожен з трьох офісів обладнаний двома комутаторами та одним маршрутизатором, з виходом до Інтернету. Наявність не одного, а двох комутаторів виконує функцію додаткової надійності, адже у разі виходу з ладу одного пристрою можна підключити хости до іншого. Як зазначалося раніше було обрано використовувати маршрутизатори та комутатори від компанії Cisco через їх високу якість та надійність.

Додатковим елементом в мережі виступає мережевий контролер, що підключено до маршрутизатора головного офісу. Завдяки цьому приладу системний адміністратор головного офісу отримає змогу використовувати Cisco Monitoring System для перегляду стану мережевих приладів у всіх офісах.

2.2.2 Розробка структурної схеми мережі

На основі створених вимог до системи було розроблено схему комплексу технічних засобів, що зображена на рисунку 2.1. На рисунку наведено схематичне розміщення апаратних пристроїв та їх кількість в кожному структурному підрозділі IT-компанії «BAS-IQ».

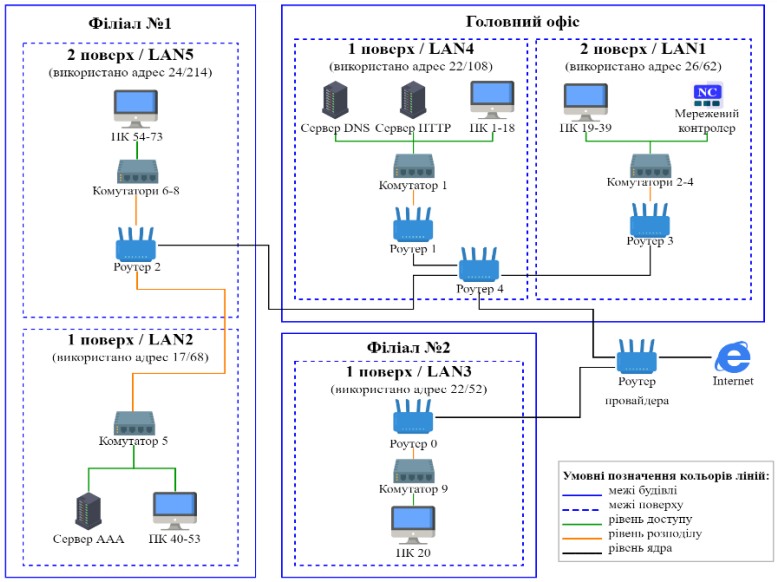

Рисунок 2.1 – Структурна схема комплексу технічних засобів

2.2.3 Розробка специфікації апаратної частини

Після проведення аналізу вимог та створення структурної схеми комплексу технічних засобів, необхідно розробити таблицю специфікації апаратних засобів що буде включати найменування, тип, технічні характеристики та кількість певного апаратного обладнання.

При виборі моделі комп'ютерів було взято до уваги фактор зручності встановлення та використання, саме цьому було обрано моноблочні комп'ютери, адже вони зручні у використанні та інтеграції в мережу, а також мають достатню потужність. Моноблочний комп’ютер Lenovo IdeaCentre 5i 27IOB6 має високу продуктивність, яскравий та чіткий дисплей, а також компактний апаратний корпус. Подібні апаратні рішення досить часто використовується в сучасних офісах IT-компаній, особливо за кордоном.

Рисунок 2.2 – Зовнішній вигляд комп’ютера Lenovo IdeaCentre 5i 27IOB6

Наступним елементом мережевого обладнання є сервери, які будуть виконувати ролі HTTP та DNS серверів. Ключовим при виборі серверу є його потужність, обсяг пам’яті для зберігання інформації та доступні порти. В якості сервера було обрано ARTLINE Business T65 v04, що маж всі вищезгадані характеристики.

Рисунок 2.3 – Зовнішній вигляд сервера ARTLINE Business T65 v04

Комутатори є дуже важливим елементом мережі, адже вони об’єднують хости мережі між собою. При виборі комутаторів необхідно зважати на кількість комп’ютерів що буде підключено а також навні мережеві порти й підтримка сучасних технології передачі даних. Компанія Cisco пропонує велику кількість комутуючих приладів серед яких було обрано Smart Gigabit Ethernet Cisco SG220-26-K9-EU. Наявність 24 портів типу GigabitEthernet дозволяє використати меншу кількість комутаторів, адже найбільша мережа включає в себе 214 комп’ютерів.

Рисунок 2.4 – Зовнішній вигляд комутатора Smart Gigabit Ethernet Cisco SG220-26-K9-EU

В якості маршрутизатора пропонується обрати Cisco ISR4331, адже він має 3 Gigabit Ethernet порти, що зумовить можливість передачі інформації на високій швидкості без утворення черг. Також цей роутер підтримує стандарти бездротового підключення Wi-Fi. Більш детальна технічна характеристика міститься в таблиці 2.1.

Рисунок 2.5 – Зовнішній вигляд маршрутизатора Cisco ISR4331

Для покращення надійності системи було прийнято рішення використовувати блоки безперебійного живлення (ББЖ), що можуть накопичувати електроенергію та підтримувати роботу комп’ютерів за умови вимкнення в офісі енергопостачання. Блок живлення LPM-L625VA, що був

обраний для інтеграції в комп’ютерну систему, окрім достатньої потужність та ємності акамулятора, має інформативний дисплей. Кількість таких пристроїв на розрахована як сума ПК, серверів, комутаторів та маршрутизаторів в корпоративній мережі, що становить: 93+3+9+6=111 штук.

Рисунок 2.6 – Зовнішній вигляд ББЖ LPM-L625VA

Крім того для поліпшення системи моніторингу в комп’ютерній системі було додано мережевий контролер, переваги використання якого були описані в попередніх розділах. Для того, щоб вся мережева архітектура працювала в єдиній екосистемі було обрано девайс від компанії Cisco - AIR-CT5508-25-K9. Велика кількість способів підключення та висока продуктивність дозволить отримувати дані про стан мережевих приладів швидко й надійно.

Рисунок 2.7 – Зовнішній вигляд мережевого контролера Cisco AIR-CT5508-25-K9

Для розрахунку рекомендованої кількості кабелів для підключення пристроїв між собою необхідно додати маршрутизатор, комутатори та кінцеві пристрої на схему офісу та з’єднати умовними лініями, довжина яких буде відповідати мінімальній довжині кабелю. На рисунку 2.8 зображена схема підключення пристроїв для другого поверху філіалу №1.

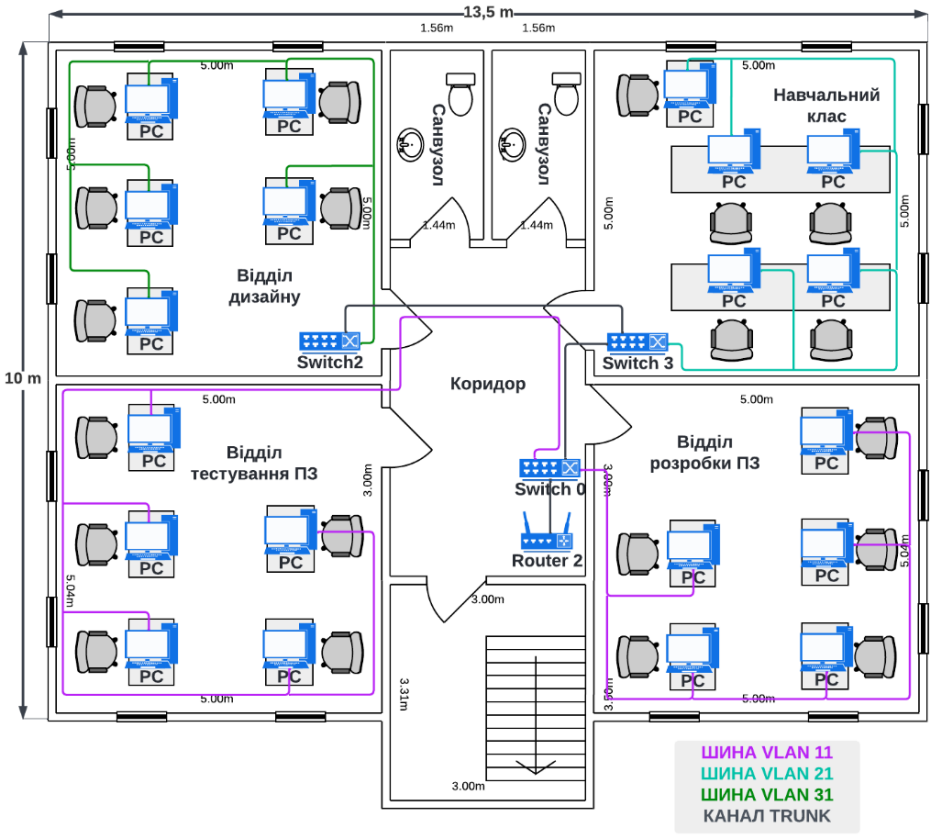

Рисунок 2.8 – Схема підключення пристроїв на другому поверсі філіалу №1

На рисунку видно, що для підключення пристроїв в певних відділах кабелі було об’єднано в шини та прокладено біля стін. Виходячи з розрахунку, що кожна кімната має довжину стіни 5 метрів, а кабель прокладається максимум через 3 сторони кімнати, можна зробити висновок, що для підключення 1 комп’ютера до комутатора необхідно максимум 15 метрів «витої пари». Кількість комп’ютерів в підмережі другого опверху філіалу №1 становить 20 штук. Отже необхідно 300 метрів кабелю типу «вита пара» для підключення лише комп’ютерів. Проте комутатори теж з’єднуються кабелями з маршрутизатором, таким чином можна взяти ще 20 метрів кабелю. Таким чином загальна кількість кабелю для об’єднання даної підмережі становить 320 метрів. Цей результат вже містить в собі резервну довжину, адже не кожен ПК буде прокладатися через 3 стіни, тобто 15 метрами LAN-кабелю.

Інші офіси мають приблизно таку ж площу та плани будівель, отже 320 необхідно помножити на 5 (загальна кількість підмереж), щоб отримати рекомендовану кількість LAN-кабелів. Отже до специфікації можна занести значення 1600 метрів. До того ж необхідно брати до уваги, що кабель необхідно обжимати конекторами RJ-45 з обох боків. Кількість конекторів буде дорівнювати подвоєнній сумі кількості ПК та комутаторів, а також необхідно додати 10 % в якості резерву ((93+9)*2+10% = 225).

Офіси з'єднані між собою зовнішніми оптоволоконними кабелями, що забезпечують надійну передачу інформації без ризику втрати даних через потрапляння прямих сонячних променів. Зважаючи на те, що структурні підрозділи знаходяться на відстані 1 км один від одного (див. рисунок 1.1) знадобиться 2 км такого кабелю, бо головний офіс буде з'єднувати з одного боку філіал №1, а з іншого – філіал №2. Проте необхідно забезпечити певний запас довжини, що буде складати +10%. Таким чином в специфікацію необхідно занести значення 2,2 км для зовнішнього оптоволоконного кабеля.

Комутатори в кімантах відділ стоять на столах, а от в коридорах вони монтовані в мережеві шафи, що вже були надані клієнтом, отже не потребують занесення в специфікацію.

Для введення даних на кожен ПК передбачено комплект периферії, що складається з клавіатури та миші. Кількість таких комплектів більша за кількість ПК на 10%, що забезпечує створення певного резерву на складі.

Технічні характеристики та необхідна кількість обраних пристроїв наведено в таблиці 2.2.

Таблиця 2.2 – Специфікація апаратних засобів

Позиція	Найменування	Тип	Одиниці виміру	Кількість	Технічні характеристики
1	2	3	4	5	6
1	Моноблок Lenovo IdeaCentre 5i 27IOB6 (F0G4002AUA) [7]	Комп'ютер	штуки	93	Процесор: Intel Core i5-10400T (2.0 — 3.6 ГГц); Оперативна пам’ять: 16 ГБ; Відеокарта: 4 GB GeForce RTX 3050; Дисплей: 27" WQHD (2560x1440); Жорсткі диски: HDD 2 ТБ, SSD 512GB; Мережеві адаптери: Gigabit Ethernet, Bluetooth 5.2.
2	ARTLINE Business T65 v04 [8]	Сервер	штуки	3	Процесор: 12-ядерний AMD Ryzen 9 5900X (3.7 — 4.8 ГГц); Оперативна пам’ять: 64 ГБ; Материнська плата: AMD X470; Жорсткий диск: HDD: 2 x 2 ТБ, SSD: 2 x 500 ГБ.
3	Smart Gigabit Ethernet Cisco SG220-26-K9-EU [9]	Комутатор	штуки	10	24 порти GigabitEthernet; 2 порти SFP; 1 порт RS-232.
4	Cisco ISR4331 [10]	Маршрутизатор	штуки	7	3 порти GigabitEthernet (10/100/1000); порт RJ-45; 1 порт NIM; 2 порти SFP; 1 порт USB 2.0.

Продовження таблиці 2.2

1	2	3	4	5	6
5	Cisco AIR-CT5508-25-K9 [11]	Мережевий контролер	штуки	1	8 портів для трансіверів 1000BaseT, 1000Base-SX і 1000Base-LH (аплінки); 1 порт x RJ45 10/100/1000 Ethernet (службовий порт); 1 порт x RJ45 10/100/1000 Ethernet (порт утиліт); 1 порт RS232 (консольний порт, DB-9 male, DTE-інтерфейс); 1 порт mini-usb.
6	LPM-L625VA [12]	Блок безперебійного живлення	штуки	110	Потужність: VA/W:625/437; Вихідна напруга: V:220±10%; Час роботи від АКБ: 10-15 хв; Кількість виходів: 2.
7	Кабель DIGITUS CAT 5e U-UTP Gray [13]	Вита пара	метри	1600	Кількість провідників: 8; Ізоляція: PE; Категорія: 5E.
8	Конектор RJ-45	Конектор	штуки	225	-
9	Corning 012TEY-13188A2G [14]	Оптоволоконний кабель	метри	2200	Кількість волокон: 12; Тип волокна: Multimode; Оболонка кабелю: LSZH; Броня: Стальна гофроброня; Передбачено захист від ультрафіолету та вологи.
10	Комплект бездротовий Logitech MK235 [15]	Клавіатура та миша	штуки	103	Тип підключення: бездротовий. Інтерфейс підключення: USB.

2.2.4 Розрахунок інтенсивності вихідного трафіку найбільшої підмережі

Для розрахунку інтенсивності вихідного трафіку та інших метрик найбільшої локальної мережі необхідно спиратися на вхідні дані, що регламентуються учбовим завданням та описані в пункті 2.1.1.5.6. Прямого відношення до об’єкту впровадження ці розрахунки не мають, бо виконуються виключно в аналітичних цілях.

Таким чином вхідні змінні будуть мати значення:

- N=214 вузлів (Кількість вузлів в найбільшій підмережі);
- μ=41 кадрів/сек (Середня інтенсивність трафіку);
- l=650 байт (Середня довжина повідомлення).

Оскільки кількість хостів в найбільшій мережі складає 214, то спираючись на те, що обраний в специфікації комутатор Smart Gigabit Ethernet Cisco SG220-26-K9-EU має 24 порти (*n*) для підключення комп’ютерів, можна зробити висновок, що їх знадобиться 9 штук.

Знаючи це можна розрахувати пропускну здатність мережі на рівні доступу ($P_{р.д}$), враховуючи 100% рівень завантаження користувачами:

$$P_{р.д}= \mu \times l \times n \times 8 = 41 \times 650 \times 24 \times 8 = 5{,}1 \text{ Мбіт/с}, \quad (2.1)$$

де n - це кількість портів в комутаторі рівня доступу.

Пропускна здатність мережі на рівні розподілу обчислюється виходячи з кількості вузлів в мережі (214):

$$P_{р.р}= \mu \times l \times N \times 8 = 41 \times 650 \times 214 \times 8 = 45{,}6 \text{ Мбіт/с}, \quad (2.2)$$

де N – це кількість вузлів в мережі LAN5.

Отримані показники не перевищують граничне значення передачі даних (1000 Мбіт/с), отже перевантаженнь ліній зв’язку не буде.

Комутатор рівня розподілу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 1000 Мбіт/с. Сумарне навантаження на комутатор не повинно перевищувати наступне значення інтенсивності вихідного трафіку:

$$\mu_{вих}=1000\ 000\ 000/(650 \times 8)=192308 \text{ пакетів/с}. \quad (2.3)$$

Оскільки кожен відправник виробляє в середньому 41 пакет на секунду, то максимальна кількість таких джерел буде обчислюватися наступним чином:

$$N_{макс}=192308/41=4690 \text{ джерел.} \quad (2.4)$$

Таке значення цілком задовольняє вимогам до кількості користувачів, адже в мережу LAN5 входить 214 ПК.

Кожен з 214 ПК надсилає запити з інтенсивністю 41 кадрів/с. Інтенсивність вихідного трафіку від всіх користувачів таким чином буде обчислюватися як добуток двох цих значень:

$$\lambda=N\cdot\mu= 214\times41=8774 \text{ пакетів/с.} \quad (2.5)$$

Коефіцієнт затримки на рівні розподілу, інакше кажучи, показник завантаженості вихідного каналу передачі інформації, який впливає на час перебування в черзі запитів буде чисельно дорівнювати:

$$\rho=\lambda/\mu_{вих}=8774/192308=0,046. \quad (2.6)$$

Коефіцієнт зайнятості комутатора рівня розподілу обчислюється як частка від ділення коефіцієнта затримки на рівні розподілу на одиницю, від якої віднято той самий коефіцієнт:

$$r=\rho/(1-\rho)=0,046/(1-0,046)=0,0482 \quad (2.7)$$

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

$$T_{сер}=1/((\mu-\lambda))=1/(192308-8774)=1/183534=5.4\cdot10^{-6}\text{с}$$

Середня довжина черги:

$$L_{сер.черг}=\rho^2/(1-\rho)=0,046^2/(1-0,046) = 0,0022 \quad (2.8)$$

Отримане значення середньої довжини черги може бути корисним при конфігурації черг на девайсах, бо є можливість вказати максимальний розмір черги пакетів. В цьому випадку система має менше одного пакету на обслуговуванні. Таке значення свідчить про значний запас продуктивності мережевого обладнання, що буде корисним при бажанні масштабувати мережу.

Середній час очікування пакета в черзі дорівнює частці від ділення середньої довжини черги на інтенсивність вихідного трафіку:

$$T_{очік}=L_{сер.черг}/\lambda=0,0022/8774=2,51\times10^{-7} \text{ с} \quad (2.9)$$

Отримане значення менше того, що висувається у вимогах (≤6 мс), отже мережеві прилади обрані вірно.

Значення пропускної здатності каналу визначається добутком інтенсивності вихідного трафіку на довжину кадру:

$$b=\lambda\times l=8774\cdot 650\cdot 8=45624800 \text{ біт/с}=45{,}625 \text{ Мбіт/с}. \quad (2.10)$$

Розрахована метрика задовольняє пропускній здатності вихідного каналу в 1000 Мбіт/с.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі ІТ-компанії «BAS-IQ»

Першим завданням розробки корпоративної мережі є розрахунок схеми адресації в підмережах компанії. За умовами технічного завдання кваліфікаційної роботи загальна мережа компанії має адресу 10.22.248.0/21.

Комп’ютерна система складається із п’яти підмереж, кількість вузлів в кожній з них наводилось в таблиці 2.1.

Головний офіс компанії включає мережі LAN4 (перший поверх) та LAN1 (другий поверх). Філіал №1 відповідає мережі LAN2 (перший поверх) та LAN5 (другий поверх), а філіал №2 – мережі LAN3.

Крім користувацьких підмереж необхідно створити й каналів зв’язку між маршрутизаторами, адже кожна пара роутерів також з'єднується між собою окремою підмережею. За схемою топології, що пропонується умовами варіанту, необхідно з’єднати 6 маршрутизаторів, тому для цього потрібно 5 невеликих підмереж. Блок адрес для каналів між маршрутизаторами задано клієнтом та становить 10.1.1.0/24. Зважаючи на те, що такі підмережі містять тільки по два вузли, для них досить використати маску 255.255.255.252.

Для розрахунку використовується метод VLSM (Variable Length Subnet Masks), адже кількість вузлів у кожній підмережі різна. Метод VLSM передбачує мережа поділ на підмережі, які в свою чергу також можуть бути розділені [16]. Кількість таких ітерацій залежить від максимальної кількості вузлів у вихідній мреежі, що розділяється, й бажаного розміру підмереж. Наданий блок адрес (10.22.248.0/21) дає змогу вмістити 2046 пристроїв. Для потреб організації потрібно 504 адреси, отже лише 25% адресного простору буде використано.

Для мережі LAN1, в який входить 62 вузли, маска становить 255.255.255.192 (префікс /26). Допустимі адреси знаходяться в межах діапазону 10.22.250.1 – 10.22.250.62. Широкомовлення доступне за адресою 10.22.250.63. Мережа LAN2 на 68 вузлів має маску 255.255.255.128 (префікс /25). Діапазон адрес становить 10.22.249.129 – 10.22.249.254. Широкомовна адреса

10.33.249.255. Для мережі LAN3, що включає 52 вузли маска 255.255.255.192 (префікс /26). Діапазон допустимих адрес 10.22.250.65 – 10.22.250.126. Широкомовлення 10.22.250.127. Для мережі LAN4 на 108 вузлів маска 255.255.255.128 (префікс /25). Діапазон адрес 10.22.249.1 – 10.22.249.126. Адреса для широкомовного віщання 10.22.249.127. Ця мережа містить два сервери, які також потребують адреси. За умовами завдання серверам слід виділяти адреси, що більше на 10 (9 + номер варіанту, тобто 9 + 1) аніж перша допустима. Таким чином для адресації сервера HTTP використано адресу 10.22.249.11, а для сервера DNS 10.22.249.12. Мережа LAN5 є найбільшою і включає 214 вузлів, маска 255.255.255.0 (префікс /24). Діапазон адрес 10.22.248.1 – 10.22.248.254. Адреса широкомовлення 10.22.248.255.

Як зазначалося раніше для запровадження зв’язку між маршрутизаторами необхідно розбити блок адрес 10.1.1.0/24 для створення 6 підмереж, по 2 вузли в кожній. Для такої задачі доцільно використати префікс /30 для кожної підмережі між маршрутизаторами. В таблиці 3.2 міститься схема адресації локальних підмереж, що описувалися вище.

Таблиця 3.1 – Схема адресації мереж

Назва мережі	Кількість вузлів	Адреса мережі	Маска мережі	Діапазон адрес вузлів мережі
1	2	3	4	5
LAN1	62	10.22.250.0	255.255.255.192	10.22.250.1 – 10.22.250.62
LAN2	68	10.22.249.128	255.255.255.128	10.22.249.129 – 10.22.249.254
LAN3	52	10.22.250.64	255.255.255.192	10.22.250.65 – 10.22.250.126
LAN4	108	10.22.249.0	255.255.255.128	10.22.249.1 – 10.22.249.126
LAN5	214	10.22.248.0	255.255.255.0	10.22.248.1 – 10.22.248.254
WAN1	2	10.1.1.0	255.255.255.252	10.1.1.1 – 10.1.1.2
WAN2	2	10.1.1.4	255.255.255.252	10.1.1.5 – 10.1.1.6
WAN3	2	10.1.1.8	255.255.255.252	10.1.1.9 - 10.1.1.10
WAN4	2	10.1.1.12	255.255.255.252	10.1.1.13 - 10.1.1.14
WAN5	2	10.1.1.16	255.255.255.252	10.1.1.17 - 10.1.1.18

Вищезазначені адреси будуть використані для подальшого проєктування комп’ютерної системи в програмі Cisco Packet Tracer.

3.2 Розробка топологічної схеми корпоративної мережі IT-компанії «BAS-IQ»

Модель, що проєктується в програмі Cisco Packet Tracer повинна відповідати схемі топології, яка була надана у вимогах до налаштування корпоративної мережі (рисунок 1.8).

Для побудови моделі комп’ютерної мережі перш за все необхідно обрати мережеві прилади, що будуть використані в топології. Програма Cisco Packet Tracer має велику кількість видів маршрутизаторів, комутаторів, кабелів, кінцевих пристроїв та інших елементів для моделювання. Внаслідок того, що в якості мережевих приладів в специфікацію було обрано саме прилади від виробника Cisco, з’являється можливість використання та конфігурації вищезазначених девайсів на практиці. Так наприклад, в якості маршрутизаторів обрано Cisco ISR4331, а Cisco 2960 – в якості комуторів підмереж. На рисунку 3.1 зображена побудована модель мережі, що повністю відповідає умовам ум завдання.

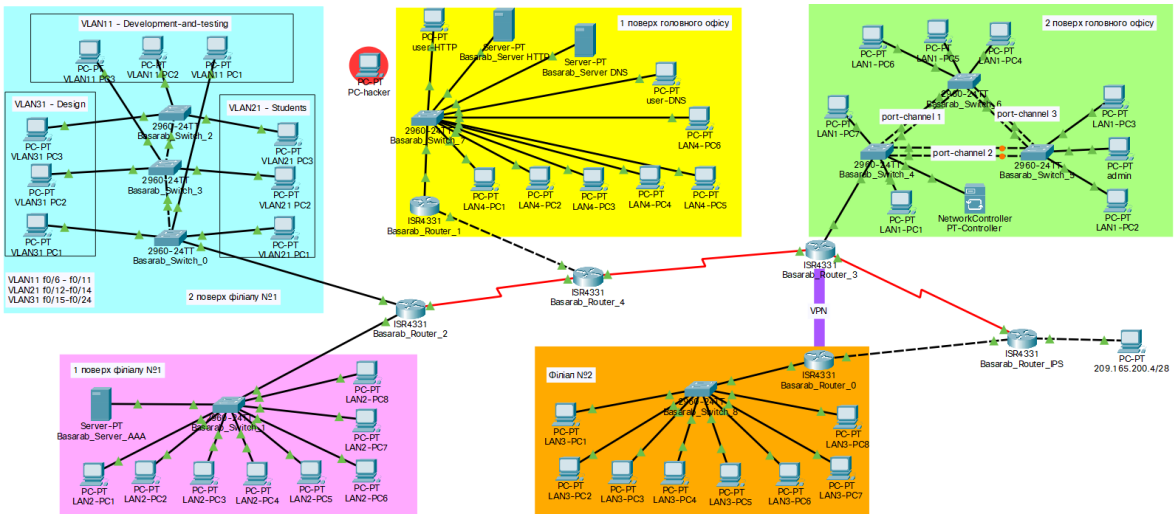

Рисунок 3.1 – Архітектура мережі в програмі Cisco Packet Tracer

3.3 Налаштування моделі КС IT-компанії «BAS-IQ»

3.3.1 Базове налаштування конфігурації пристроїв

Базове налаштування конфігурації пристроїв передбачає призначення імені девайсам за правилом Прізвище_тип пристрою_номер. Так наприклад маршрутизатор під номером 5 отримав ім’я Basarab_Router_5.

Для покращення рівня безпеки на всіх пристроях призначено пароль «cisco» до консолі та віртуальних ліній (vty). Ключове слово «class» служить паролем до привілейованого режиму пристроїв. Команди для налаштуань наведено на рисунку 3.2.

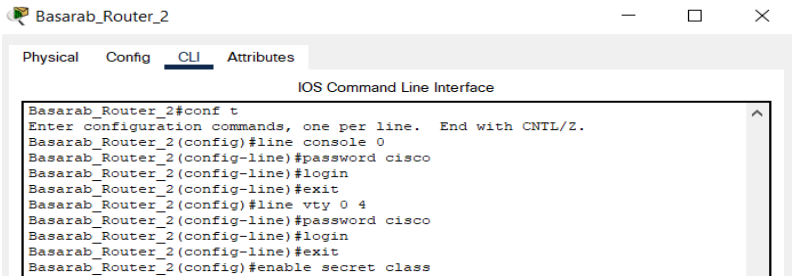

Рисунок 3.2 – Базове налаштування паролів

Всі відкриті паролі шифруються за допомогою команди *service password-encryption*. Крім того, на кожний комутатор та маршрутизатор було додано банер MOTD (Message of the day). Цей банер потрібен для відображення повідомлення перед спробою користувача взаємодії з мережевим пристроєм. На рисунку 3.3 можна побачити, що користувач, який хоче отримати консольний доступ отримує повідомлення «This is a secure system/ Authorized Access Only. Created by Danylo Basarab».

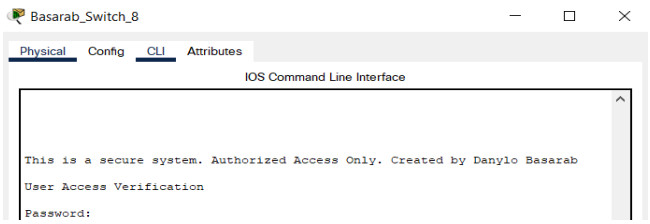

Рисунок 3.3 – Вікно автентифікації в консольний режим налаштувань комутатора

Наступним етапом базового налаштування є створення користувача на кожному приладі (123181_Basarab) та задання домену, що потрібен для подальшого шифрування даних. Домен повинен мати таку ж назву, як і пристрій, на якому проводиться налаштування (наприклад Basarab_Router_5). Після вказування домену необхідно згенерувати RSA-ключ, що буде мати довжину 1024 біт. На всіх віртуальних лініях (vty) було призначено використання протоколу SSH, що надасть можливість для безпечного віддаленого адміністрування мережевого устаткування компанії. Для цього були використані команди *Transport input ssh* та *Login local*, при цьому версія протоколу SSH була змінена на більш новітню командою *ip ssh version 2*. Приклад впровадження вищезгаданих налаштувань зображено на рисунку 3.4.

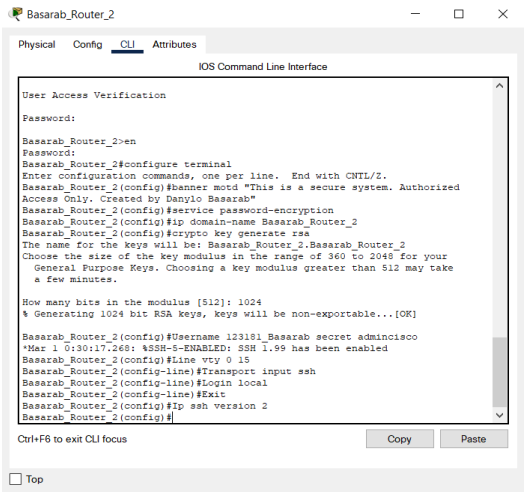

Рисунок 3.4 – приклад базового налаштування маршрутизатора

На всіх DCE-Serial портах маршрутизаторів, що служать для з’єднання підмереж, було встановлено уніфіковану тактову частоту 128000 за допомогою команди clock rate 128000. Cisco Packet Tracer надає змогу працювати не лише з конфігураційною консоллю, а й з графічним інтерфейсом для впровадження деяких налаштувань. На рисунку 3.5 наводиться приклад задання тактової частоти саме через графічний інтерфейс. Нижче в консоль дублюються відповідні команди налаштувань.

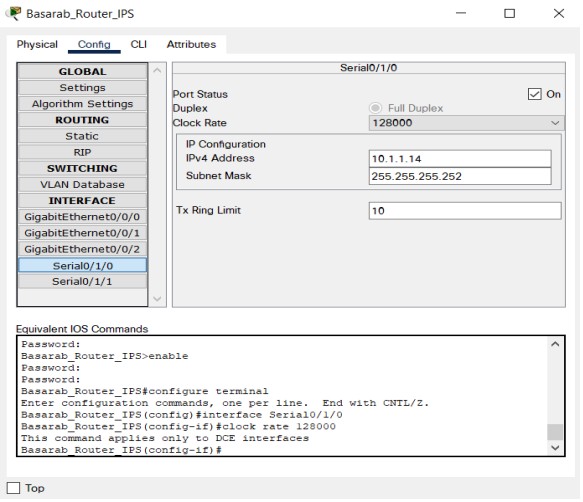

Рисунок 3.5 – Графічний інтерфейс конфігурації інтерфейса Serial0/1/0 на роутері

IP-адреса, що надається пристрою залежить від його типу, адже за умовами завдання маршрутизатори отримують першу допустиму адресу в мережі, комутаторам задається друга, а кінцевим вузлам, тобто комп'ютерам – остання з діапазону. Адресація серверів регламентується правилом перша допустима адреса + 10, отже вони отримають одинадцяту допустиму адресу в своїх підмережах. Схема адресації пристроїв наводиться в таблиці 3.3.

Таблиця 3.2 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
1	2	3	4	5	6	7
2 поверх головного офісу (LAN1)						
Basarab_ Router_3	Gig0/0/0	10.22.250.1	/26			Basarab_Switch _4 Gig0/1
	Se0/2/0	10.1.1.9	/30			Basarab_Router _4 Se0/2/0
	Se0/1/0	10.1.1.13	/30			Basarab_Router _IPS SE0/1/0
Basarab_ Switch_4	Vlan1	10.22.250.2	/26	10.22.250.1		-
Basarab_ Switch_5	Vlan 1	10.22.250.3	/26	10.22.250.1		-
Basarab_ Switch_6	Vlan1	10.22.250.4	/26	10.22.250.1		-
PC	Fa0	10.22.250.5-10.22.250.62	/26	10.22.250.1		-

Продовження таблиці 3.2

1	2	3	4	5	6	7
1 поверх філіалу №1 (LAN2)						
Basarab_ Router_2	Se0/1/0	10.1.1.1	/30			Basarab_Router _4 Se0/1/0
	Gig0/0/1	10.22.249.129	/25			Basarab_Switch _1 Gig0/1
Basarab_ Switch_1	Vlan1	10.22.249.130	/25	10.22.249.129		-
Basarab_ Server AAA	Fa0	10.22.249.240	/25	10.22.249.129		Basarab_Switch _1 Fa0/9
PC	Fa0	10.22.249.131 – 10.22.249.254	/25	10.22.249.129		-
Філіал №2 (LAN3)						
Basarab_ Router_0	Gig0/0/0	10.1.1.17	/30			Basarab_Router _IPS Se0/1/0
	Gig0/0/1	10.22.250.65	/26			Basarab_Switch _8 Gig0/1
Basarab_ Switch_8	Vlan1	10.22.250.66	/26	10.22.250.65		-
PC	Fa0	10.22.250.67 – 10.22.250.126	/26	10.22.250.65		-
1 поверх головного офісу (LAN4)						
Basarab_ Router_1	Gig0/0/1	10.1.1.5	/30			Basarab_Router _4 Gig0/0/0
	Gig0/0/0	10.22.249.1	/25			Basarab_Switch _7 Gig0/1
Basarab_ Switch_7	Vlan1	10.22.249.2	/25	10.22.249.1		-
Basarab_ Server DNS	Fa0	10.22.249.11	/25	10.22.249.1		Basarab_Switch _7 Fa0/3
Basarab_ Server HTTP	Fa0	10.22.249.12	/25	10.22.249.1		Basarab_Switch _7 Fa0/4
PC	Fa0	10.22.249.3 – 10.22.249.10, 10.22.249.13 – 10.22.249.126	/25	10.22.249.1		-
2 поверх філіалу №1 (LAN5)						
Basarab_ Router_2	Gig0/0/0.11	10.22.248.1	/26		11	-
	Gig0/0/0.21	10.22.248.65	/26		21	-
	Gig0/0/0.31	10.22.248.129	/26		31	-
Basarab_ Switch_0	Vlan99	10.22.248.2	/26	10.22.248.1	99	-

Продовження таблиці 3.2

1	2	3	4	5	6	7
Basarab_ Switch_3	Vlan99	10.22.248.3	/26	10.22.248.1	99	-
Basarab_ Switch_2	Vlan99	10.22.248.4	/26	10.22.248.1	99	-
PC	Fa0	10.22.248.11 – 10.22.248.62	/26	10.22.248.1	11	-
	Fa0	10.22.248.76 – 10.22.248.127	/26	10.22.248.165	21	-
	Fa0	10.22.248.140 – 10.22.248.191	/26	10.22.248.129	31	-
ЗАГАЛЬНЕ						
Basarab_ Router_I PS	Se0/1/0	10.1.1.14	/30			Basarab_Router _3 Se0/1/0
	Gig0/0/0	10.1.1.18	/30			Basarab_Router _0 Gig0/0/0
Basarab_ Router_4	Gig0/0/0	10.1.1.6	/30			Basarab_Router _1 Gig0/0/0
	Se0/1/0	10.1.1.2	/30			Basarab_Router _2 Se0/1/0
	Se0/2/0	10.1.1.10	/30			Basarab_Router _3 Se0/2/0

Для поліпшення надійності та збільшення пропускної здатності каналів між комутаторами в мережі LAN1 було об’єднано фізичні порти. Для цього було налаштовано протокол PAGP, що був розроблений спеціиально для пристроїв від Cisco. На першому етапі конфігурації необхідно призначити транковий статус фізичним портам, що будуть об’єднані в логічні канали. Варто зазначити, що для успішного об’єднання фізичних портів необхідно, щоб їх статус був однаковий. Для перевірки статусу портів використовується команда *show interface trunk* (рисунок 3.6)

```
Basarab_Switch-5#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      1
Fa0/4       on           802.1q         trunking      1
```

Рисунок 3.6 – Перевірка транкового статусу портів

Кількість об’єднаних каналів прямолінійно залежить від кількості комутаторів. Мережа LAN1 містить 3 комутатори, отже необхідно створити загалом 3 канали, по два на кожному комутаторі. Для створення каналу між комутаторами необхідно на кожному з них прописати команду *channel-group № mode desirable*, де № слід замінити на порядковий номер каналу. Приклад створення об’єднаного каналу наведено на рисунку 3.7.

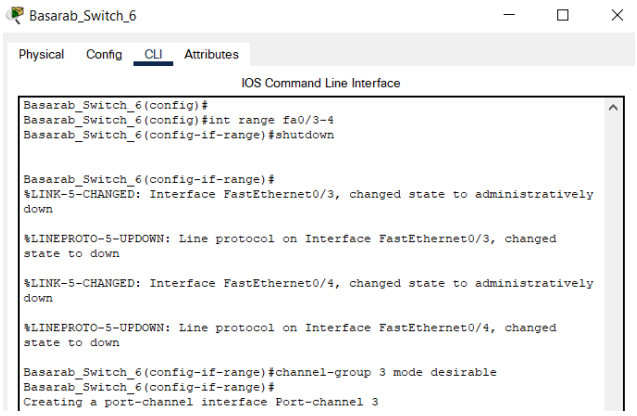

Рисунок 3.7 – Приклад створення об’єднаного каналу з кількох портів

Після оголошення канальної групи необхідно зайти на створений інтерфейс логічного каналу на задати йому транковий статус. Такі ж дії необхідно розробити на кожному комутаторі підмережі. Для перевірки налаштування PAGP використовується команда *show etherchannel summary*, результат виконання якої наведено на рисунку 3.8.

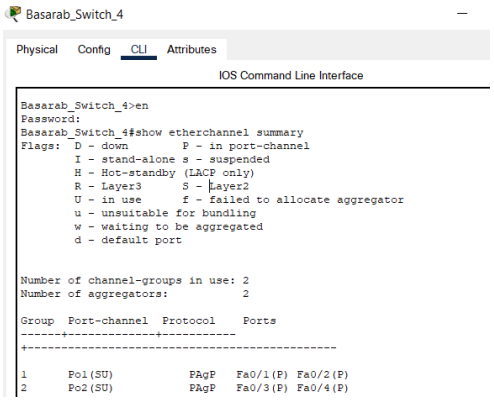

Рисунок 3.8 – Перевірка існуючих каналів на комутаторі

Можна побачити, що було успішно створено два порт-канали, один з яких об’єднує порти Fa0/1-2, а інший – Fa0/3-4. Завдяки реалізації об’єднання фізичних інтерфейсів в значній мірі покращиться відмовостійкість підмережі, адже у випадку поламки одного з фізичних інтерфейсів зв’язок не буде перерваний. Крім того пропускна здатність таких логічних каналів більша завдяки можливості розподілення трафіку між фізичними лініями.

Додатково в мережі LAN5 реалізовано систему віртуальних локальних мереж (VLAN). Мета їх проєктування – розділити на окремі сегменти працівників різних відділів. Так наприклад команди з розробки та тестування програмного забезпечення перебувають у VLAN 10, працівники бухгалтерського відділу входять до складу VLAN20, а співробітники, що займаються комунікаціями всередині компанії та з клієнтами – в VLAN30.

3.3.2 Налаштування маршрутизаторів корпоративної мережі IT-компанії «BAS-IQ»

Для забезпечення обміну даними в корпоративній мережі необхідно виконати певні налаштвування маршрутизаторів. Крім базових налаштувань, зокрема задання паролів для привілегійованого режиму та консольних ліній, необхідно обрати та впровадити певний протокол маршрутизації. За умовами завдання цей протокол має бути динамічним. До таких протоколів відносять EIGRP, RIP, OSPF. Для впровадження маршрутизації в даному проєкті було обрано протокол EIGRP, адже він має низку переваг, зокрема:

- швидкість передачі даних в потрібну підмережу;
- відсутність розсилки періодичних повідомлень, що зумовлює зниження навантаження на пропускні канали;
- простота налаштування;
- менша ресурсомісткість [17].

Для налаштування такого протоколу динамічної маршрутизації необхідно увійти в режим конфігурації роутера, задати спільний для кожного

роутера ідентифікатор EIGRP (наприклад 100) та записати всі адреси мереж, до яких напряму підключено роутер, а також мережі між маршрутизаторами.

Приклад налаштування протоколу EIGRP для конкретного роутера в мережі зображено на рисунку 3.9. Для повноцінного обміну інформацією між вузлами різних мереж подібні налаштування були виконані для кожного з маршрутизаторів.

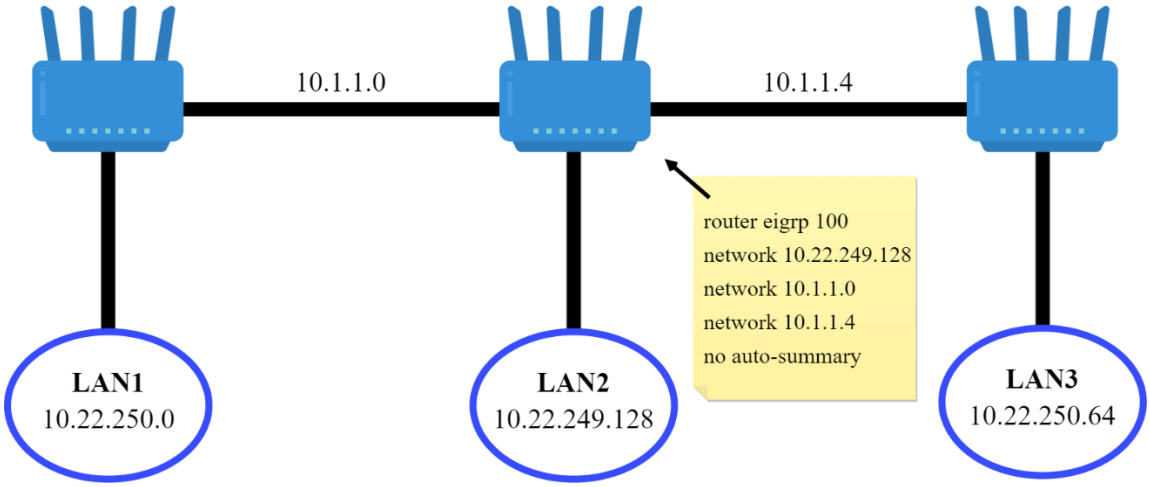

Рисунок 3.9 – Приклад налаштування протоколу EIGRP

Додатково на кожному маршрутизаторі корпоративної мережі було встановлено модель авторизації AAA, що дозволяє здійснювати авторизацію за допомогою облікових записів, які зберігаються на окремому сервері. AAA – це система автентифікації, авторизації та обліку подій, що має декілька переваг перед звичайною локальною авторизацією, зокрема можливість додавання облікових записів та зміни даних про користувача на віддаленому сервері, що забезпечить уніфікований процес вхооду в консольні налаштування маршрутизаторів. Такий підхід економить час адміністратора, адже зміни облікових записів не треба прописувати вручну на кожному пристрої. В Cisco Packet Tracer AAA-сервер налаштовується за допомогою графічного інтерфейсу. На рисунку 3.10 зображено вікно служби AAA на виділеному для цього сервері.

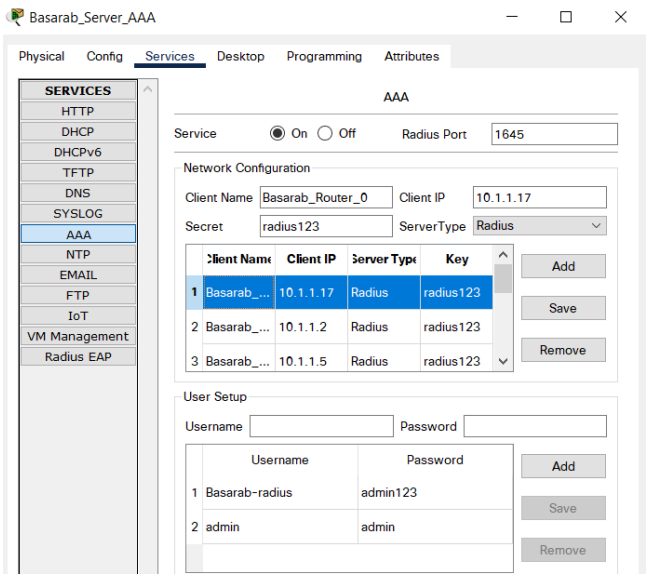

Рисунок 3.10 – Налаштування AAA-серверу

У вкладці Network configuration адміністратор задає список клієнтів, що будуть використовувати послуши AAA-служби, тобто маршрутизаторів. Для коректної роботи необхідно для кожного роутера вказати ім’я, адресу, до якої буде звертатися сервер, секретний ключ (за умовами завдання radius123) та тип серверу, тобто Radius. Вкладка User Setup містить всі облікові записи, що можуть бути використані на будь-якому з клієнтських роутерів для авторизації в консольний режим. Після додавання всіх клієнтів та створення записів для авторизації можна перейти до клієнтських конфігурацій. На кожному з роутерів необхідно виконати послідовність команд, що зображено на рисунку 3.11.

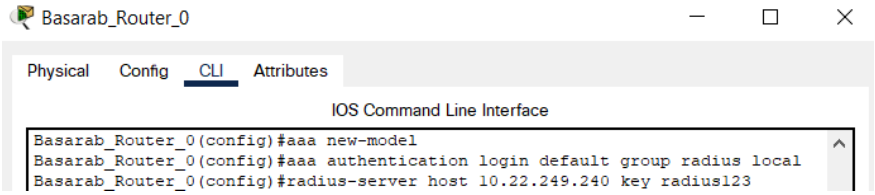

Рисунок 3.11 – Скрипт конфігурації служби AAA на маршрутизаторі

Перша команда необхідна для активації нової моделі типу AAA. Друга команда встановить порядок входу через AAA за замовчуванням, а в разі втрати зв’язку з сервером атворизація пройде через локальну базу пристрою. Остання

команда вказує адресу серверу, що надає послуги та секретний ключ для успішного встановлення зв’язку.

Після впровадження налаштувань на кожному з роутерів можна перевірити працездатність налаштованого сервісу. Для цього необхідно вийти з конфігураційного та привілегійованого режимів. Очікуваним результатом буде поле вводу імені користувача та його пароля. На рисунку 3.12 зображена успішна авторизація за допомогою облікового запису, що збережений на сервері AAA (ім’я: Basarab-radius, пароль: admin123).

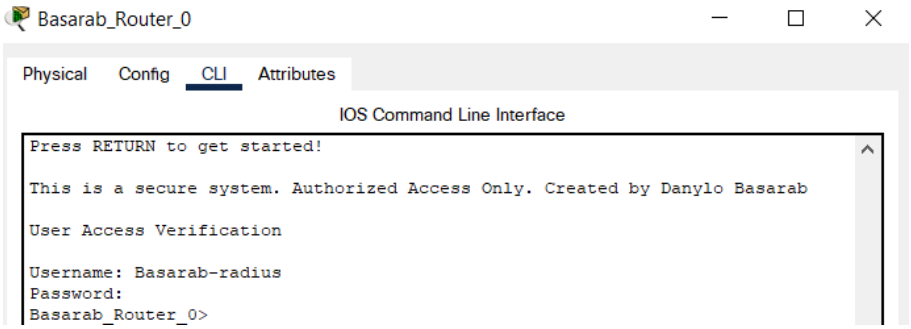

Рисунок 3.12 – Авторизація за допомогою AAA-служби

3.3.3 Налаштування роботи Інтернет

3.3.3.1 Налаштування та перевірка динамічного NAT

Для того, щоб користувачі мережі мали доступ до Інтернету необхідно налаштувати динамічне перетворення адрес на маршрутизаторі Basarab_Router_IPS. Ця функція називається NAT (Network Address Translation), її використовують для заміни локальних адрес на глобальні. Це потрібно для того, аби зовнішні користувачі не дізналися адресу, що використовується в локальній мережі.

Для налаштування динамічної трансляції адрес на маршрутизаторі перш за все необхідно вказати які інтерфейси будуть вважатися внутрішніми, а які зовнішніми. Цей етап є дуже важливим, адже неправильно вказаний тип інтерфейса буде заважати коректній роботі NAT. На рисунку 3.13 зображені команди, що необхідні для розподілу інтерфейсів роутера на зовнішні та внутрішні.

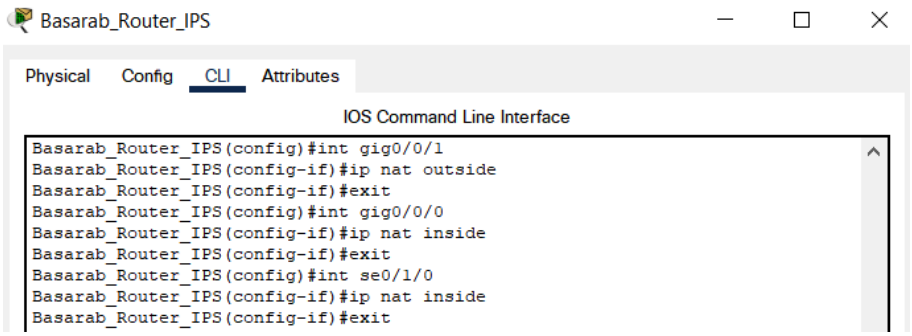

Рисунок 3.13 – Конфігурація типів портів на маршрутизаторі для NAT

Після цього за допомогою списку доступу під номером 1 дозволяється трафік, що буде мати змінену адресу. В даному випадку вся локальна мережа компанії потребує трансляції інформації про джерело повідомлення, отже адреса мережі буде 10.22.248.0.

Динамічна трансляція NAT передбачає створення певного пулу адрес, що будуть використовуватися як глобальні. Межі пулу були задані умовами завдання: 209.165.200.5 – 209.165.200.30. Вякості імені пулу було задано «Basarab_Internet» для додаткової унікальності кваліфікаційної роботи й моделі.

Скрипт команд для налаштування й перевірки динамічного NAT зображено на рисунку 3.14.

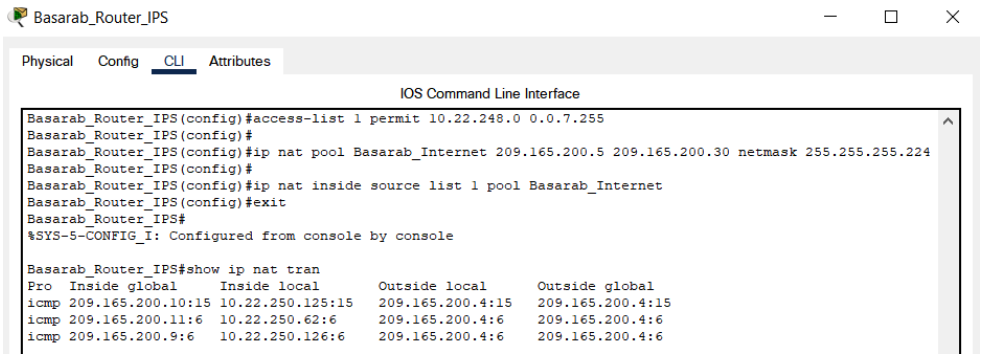

Рисунок 3.14 – Налаштування й перевірка динамічного NAT

На рисунку можна побачити, що локальні адреси мережі 10.22.248.0 перетворюються на глобальні із пулу 209.165.200.5 – 209.165.200.30. Наприклад перший запис в таблиці свідчить про те, що пакет відправлений із адреси 10.22.250.15, а потім, пройшовши через граничний роутер інтернет-провайдера,

змінив адресу на глобальну 209.165.200.10 та потрапив на зовнішній комп’ютер з адресою 209.165.200.4.

3.3.3.2 Налаштування та перевірка HTTP та DNS серверів

HTTP сервер, або веб-сервер, служить для обміну гіпертекстовою інформацією. Клієнт, тобто браузер, посилає http-запит на сервер та у відповідь отримує html-документ, тобто веб-сайт. В середовищі моделювання Cisco Packet Tracer сервер HTTP містить файли, що можуть бути відображені як веб-сайт за умови запиту у браузері адреси сервера. Головний документ, що буде відображений як первинна сторінка має назву index.html, саме його потрібно відредагувати таким чином, щоб він містив тему кваліфікаційної роботи та прізвище студента. Для редагування було використано базовий тег заголовку другого рівня <h2> та додано зображення логотипу компанії «BAS-IQ» із використанням тегу <img> (рисунок 3.15).

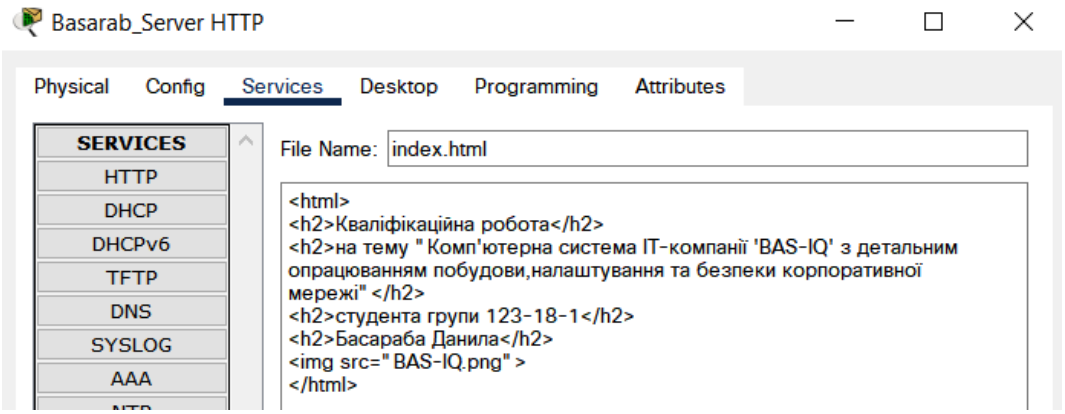

Рисунок 3.15 – вміст файлу index.html на HTTP сервері

Після збереження документу index.html кожен користувач корпоративної мережі зможе відкрити сайт за допомогою введення IP-адреси сервера в пошуковий рядок браузера. Проте такий спосіб є застарілим та вже давно не використовується, адже цифри запам’ятовувати дуже складно, особливо коли потрібно знати адреси десятків сайтів. Саме для вирішення цієї задачі існує система доменних імен (DNS). Механізм такої системи полягає у співставленні

мережевої адреси текстовій. Користувач, що вводить текстову адресу веб-ресурсу посилає запит на DNS-сервер, який в свою чергу шукає IP-адресу, що відповідає запиту. Після цього запит переадресується на веб-сервер, який надає доступ до перегляду сайту в браузері користувача.

Налаштування DNS сервера в моделі мережі передбачає створення нового запису в таблиці доменних імен, що зображено на рисунку 3.16.

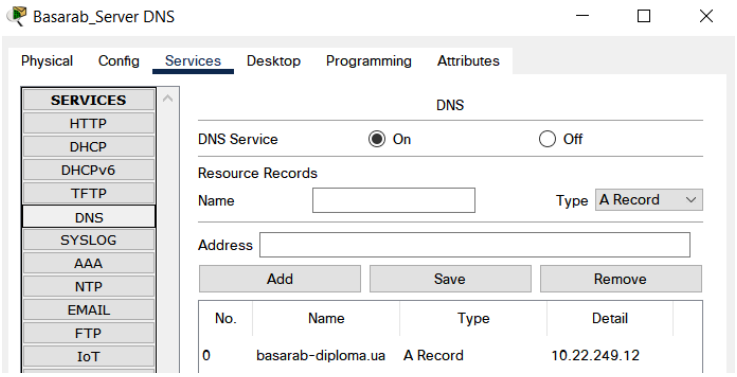

Рисунок 3.16 – Налаштування сервера DNS

В якості текстової адреси було обрано *basarab-diploma.ua*. Результат перевірки спільної роботи DNS та HTTP серверів наведено на рисунку 3.17. На рисунку можна побачити, що текст та зображення успішно завантажилися в браузері комп’ютера з іншої підмережі.

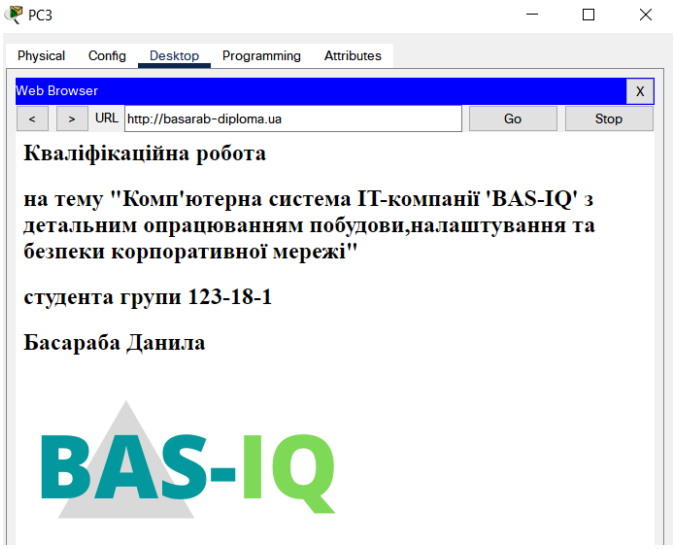

Рисунок 3.17 – Перевірка роботи DNS та HTTP серверів

3.3.3.3 Налаштування та перевірка VPN

Віртуальні приватні мережі (VPN) потрібні для створення зашифрованого тунельного з'єднання між маршрутизаторами через загальнодоступні мережі, наприклад Інтернет. Спосіб реалізації site-to-site дозволяє створити приватний канал навіть за умови наявності проміжних маршрутизаторів. За умовами завдання необхідно було з'єднати віддалену мережу, тобто LAN3, та підмережу LAN1. Схема функціонування VPN зображена на рисунку 3.18.

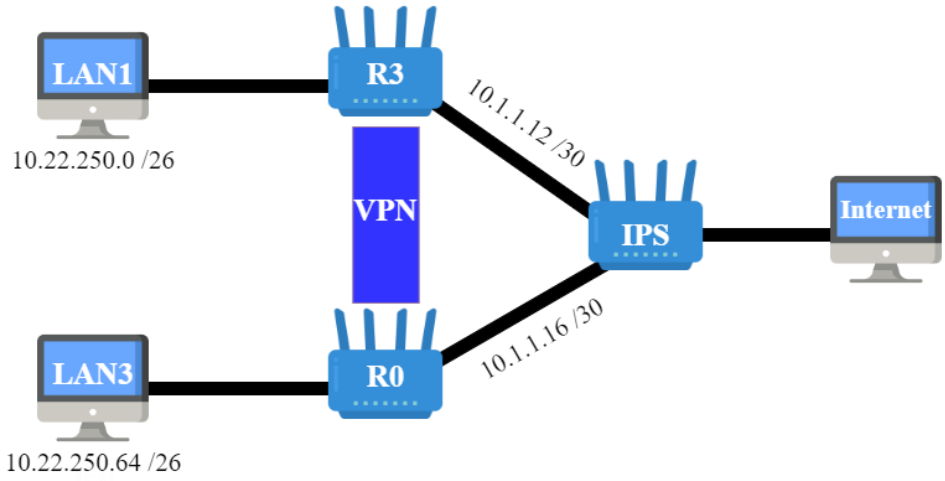

Рисунок 3.18 – Схема функціонування VPN

Налаштування VPN-тунелю передбачає введення конфігураційних команд лише на роутерах, що будуть граничними для приватної мережі, отже маршрутизатор Інтернет-провайдера не треба налаштовувати. Першим етапом налаштування є створення списку доступу, котрий буде дозволяти проходження трафіку з підмережі організації. Після цього необхідно створити нову криптограічну політику та зазначити тип шифрування даних й метод автентифікації. Варто зауважити, що створена криптографічна група та тип шифрування мають збігатися у маршрутизаторів, між якими створюється приватна мережа. Надалі необхідно створити VPN-мапу та вказати список доступу, що був створений на першому етапі конфігурації. Після цього на інтерфейсі, що є вихідним до Інтернету задається криптографічна мапа й peer-

роутер (10.1.1.17). Скрипт налаштувань для Basarab_Router_3 зображено на рисунку 3.19.

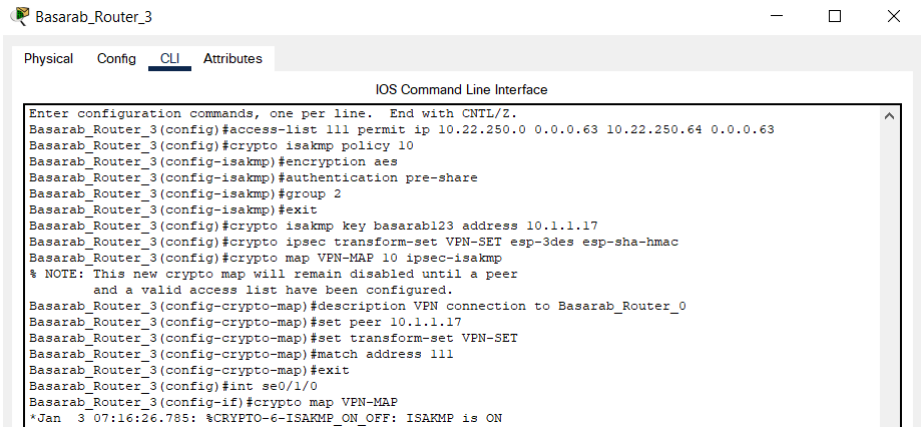

Рисунок 3.19 – Приклад налаштування VPN на маршрутизаторі

Аналогічні налаштування необхідно виконати на іншому роутері, з яким буде утворено віртуальну приватну мережу, замінивши адреси в списку доступу та в якості peer-роутера задати WAN-адресу інтерфейсу Basarab_Router_3.

Після завершення конфігурації обох маршрутизаторів необхідно перевірити правильність роботи VPN-тунелю. Для цього потрібно надіслати exa-запит від вузла мережі LAN1 до вузла LAN3. Відкривши пакет, котрий був щойно створений, можна побачити, що адреса відправника та отримувача відповідають їх локальним адресам (рисунок 3.20).

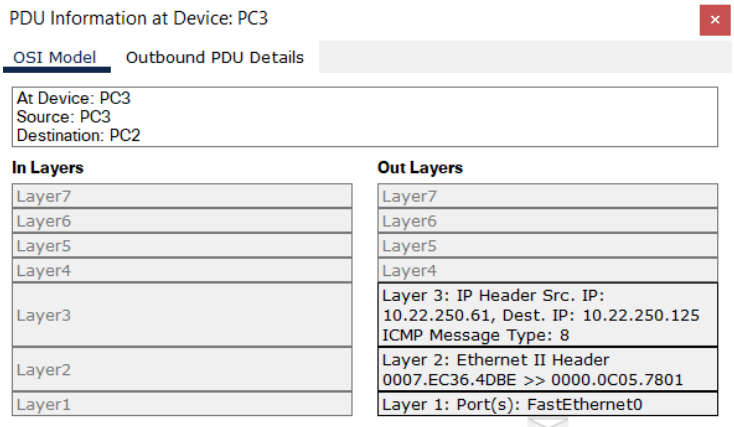

Рисунок 3.20 – Зміст пакету до проходження через приватний тунель

Після проходження через перший тунельний роутер зміст пакету змінюється, тому Інтернет провайдер бачить лише WAN-адреси в якості джерела запиту й отримувача (рисунок 3.21).

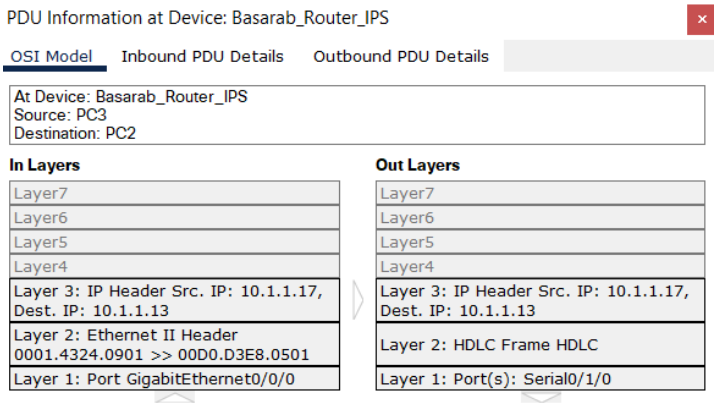

Рисунок 3.21 – Зміст пакету на роутері провайдера

На виході з приватного тунелю адреси змінюються на оригінальні, отже VPN працює правильно (рисунок 3.22).

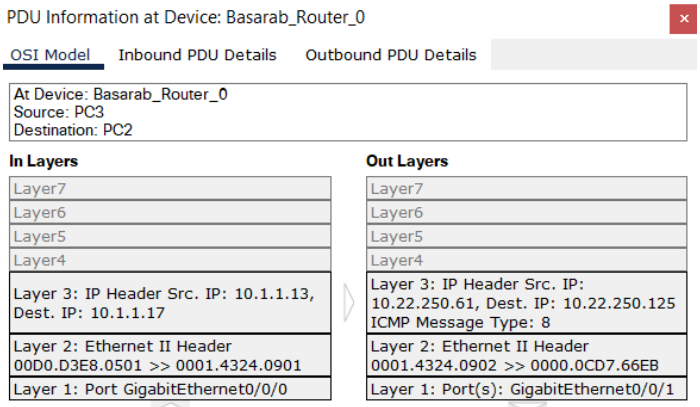

Рисунок 3.22 – Зміст пакету на другому тунельному роутері

3.4 Захист інформації в комп'ютерній системі IT-компанії «BAS-IQ»від несанкціонованого доступу

3.4.1 Налаштування безпеки портів комутаторів

Захист інформації є дуже важливим елементом кожної сучасної корпоративної мережі. Перш за все через те, що надійність ситеми безпеки це не лише гарантія схоронності даних, а й великий бонус до репутації компанії.

Клієнти повинні бути впевненими в приватності особистих та бізнес-даних всередині комп'ютерної системи IT-компанії.

Особливу увагу варто приділяти серверам, адже вся інформація проходить саме через них, й порушники безпеки дуже часто намагаються проникнути саме в серверні системи. Для поліпшення надійності системи безпеки на кожному комутаторі вімкнені порти, що не задіяні в даний момент та не мають адреси. Крім того інтерфейси комутаторів, що під'єднано до HTTP та DNS серверів мають особливу політику безпеки, котра передбачає обмеження максимальної кількості унікальних MAC-адрес до двох. Скрипт налаштування такої політики безпеки наведено на рисунку 3.23, де вказано, що у разі порушення політики безпеки портів зловмисник не зможе відправляти запити до корпоративної мережі, при цьому інтерфейс залишиться ввімкненим.

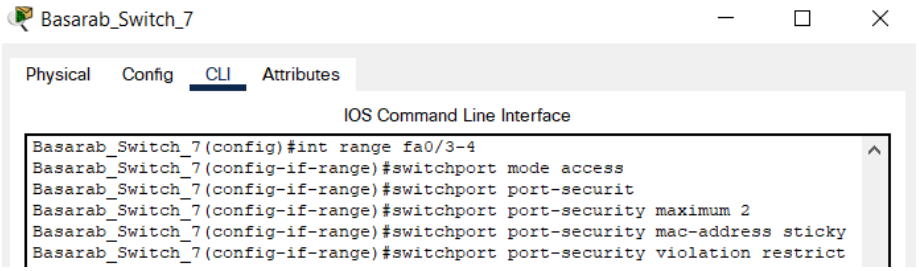

Рисунок 3.23 – Обмеження підключення більше двох унікальних MAC-адрес до портів комутатора, що приєднані до серверів

При моделюванні ситуації підключення комп'ютера хакера до зазначеного порта адміністратор з використанням команди *show port-security*, побачить, що лічильник SecurityViolations змінюється із кожною безуспішною спробою пінгування мережі (рисунок 3.24).

```
Basarab_Switch_7#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
------------------------------------------------------------------------
        Fa0/3        2           2                0         Restrict
        Fa0/4        2           2                3         Restrict
------------------------------------------------------------------------
```

Рисунок 3.24 – Перевірка кількості порушень політики безпеки комутатора

Ехо-запити, що відправляються з комп'ютера порушника будуть заблоковані, що видно на рисунку 3.25. При цьому після відключення порушника від мережі та повернення серверу на його місце система продовжує функціонувати у штатному режимі.

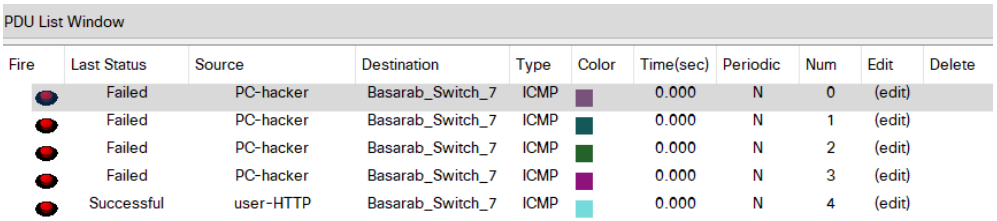

Рисунок 3.25 – Безуспішне надсилання порушником безпеки ехо-запитів

3.4.2 Налаштування мереж VLAN

Детальний опис та переваги впровадження віртуальних локальних мереж було надано в розділі 1, тому цей підрозділ описує лише особливості налаштування цієї технології в Cisco Packet Tracer. За умовами завдання необхідно запровадити поділ на віртуальні локальні мережі підсистему LAN5. Для цього знову необхідно розбити адресний простір мережі другого поверху філіалу №1 (LAN5) за допомогою методу VLSM та вказати для зручності номери й назви відповідних VLAN (таблиця 3.3).

Таблиця 3.3 – Список мереж VLAN

Номер VLAN	Ім'я VLAN	Пул адрес	Призначення
1	2	3	4
1	Default	-	Не використовується
11	Development-and-testing	10.22.248.0/26	Відділ розробки й тестування
21	Students	10.22.248.64/26	IT-академія
31	Design	10.22.248.128/26	Відділ дизайну
99	Management	10.22.248.0/24	Для управління пристроями
100	Native	-	Власна мережа

Першим етапом налаштування віртуальних локальних мереж є створення інтерфейсів та їх назв в консолі кожного комутатора мережі LAN5 (рисунок 3.26), та зазначення проміжку фізичних інтерфейсів, що будуть входити в ту чи іншу віртуальну локальну мережу (рисунок 3.27). Ці порти мають бути в режимі доступу (*switchport mode access*).

```
Basarab_Switch_3(config)#vlan 11
Basarab_Switch_3(config-vlan)#name Development-and-testing
Basarab_Switch_3(config-vlan)#vlan 21
Basarab_Switch_3(config-vlan)#name Students
Basarab_Switch_3(config-vlan)#vlan 31
Basarab_Switch_3(config-vlan)#name Design
Basarab_Switch_3(config-vlan)#vlan 99
Basarab_Switch_3(config-vlan)#name Management
Basarab_Switch_3(config-vlan)#vlan 100
Basarab_Switch_3(config-vlan)#name Native
```

Рисунок 3.26 – Створення та призначення імен для VLAN на комутаторі

```
Basarab_Switch_2(config-if-range)#int range fa0/12-fa0/14
Basarab_Switch_2(config-if-range)#switchport mode access
Basarab_Switch_2(config-if-range)#switchport access vlan 21
```

Рисунок 3.27 – Зазначення проміжку портів, що відносить до VLAN

Перевірити задані налаштування можна за допомогою команди show *vlan brief*. На рисунку 3.28 можна побачити, що налаштовані інтерфейси були зарезервовані під вказані віртуальні мережі.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5
11   Development-and-testing           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11
21   Students                          active    Fa0/12, Fa0/13, Fa0/14
31   Design                            active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
99   Management                        active
100  Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 3.28 – Таблиця VLAN та їх фізичних портів

Для успішної маршрутизації в підмережі необхідно встановити статус портів, що з’єднують мережеве обладнання між собою, як транковий, а також

дозволити переселання даних між всіма віртуальними підмережами із зазначенням native vlan. Скрипт команд на рисунку 3.29 необхідно виконати на кожному комутаторі підмережі.

```
Basarab_Switch_3(config)#int range gig0/1-2
Basarab_Switch_3(config-if-range)#switchport mode trunk
Basarab_Switch_3(config-if-range)#switchport trunk allowed vlan all
Basarab_Switch_3(config-if-range)#switchport trunk native vlan 100
Basarab_Switch_3(config-if-range)#no shut
```

Рисунок 3.29 – Налаштування транкових каналів на комутаторі

Крім того на SVI-інтерфейси кожного з комутаторів було задано IP-адресу із Management VLAN, що буде використана для управління пристроями у разі необхідності (рисунок 3.30).

```
Basarab_Switch_0(config)#int vlan 99
Basarab_Switch_0(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

Basarab_Switch_0(config-if)#ip address 10.22.248.2 255.255.255.0
Basarab_Switch_0(config-if)#no shut
```

Рисунок 3.30 – Задання адреси для SVI-інтерфейсу комутатора

3.4.3 Налаштування адресації ПК в мережах VLAN

За умовами завдання, адресацію кінцевих пристроїв у віртуальних локальних мережах необхідно замінити зі статичної на динамічну. Для цього необхідно налаштувати на роутері протокол динамічного розподілу адрес хостів (DHCP). Перевага використання динамічної адресації полягає в значній економії часу, адже для цього необхідно лише один раз налаштувати список допустимих адрес, шлюз за замовчуванням та адресу серверу доменних імен на роутері, а потім просто замінити на кожному ПК тип отримання адреси зі статичного на динамічний. Цей метод є дуже актуальним для мереж, що містять сотні хостів.

Для налаштування протоколу DHCP необхідно в конффігураційному терміналі виключити зарезервовані під мережеве обладнання адреси та створити

новий іменований пул. Створення пулів та вказування їх параметрів зображено на рисунку 3.31.

```
ip dhcp pool basarab_poolvlan11
 network 10.22.248.0 255.255.255.192
 default-router 10.22.248.1
 dns-server 10.22.249.11
ip dhcp pool basarab_poolvlan21
 network 10.22.248.64 255.255.255.192
 default-router 10.22.248.1
 dns-server 10.22.249.11
ip dhcp pool basarab_poolvlan31
 network 10.22.248.128 255.255.255.192
 default-router 10.22.248.1
 dns-server 10.22.249.11
```

Рисунок 3.31 – Налаштування пулів для динамічного розподілу адрес

Після оголошення пулів на кожному комутаторі необхідно вказати IP-адресу (рисунок 3.32), при цьому через резервування перших десяти адрес для кожного пулу не буде відбуватися конфлікт DHCP-розподілу.

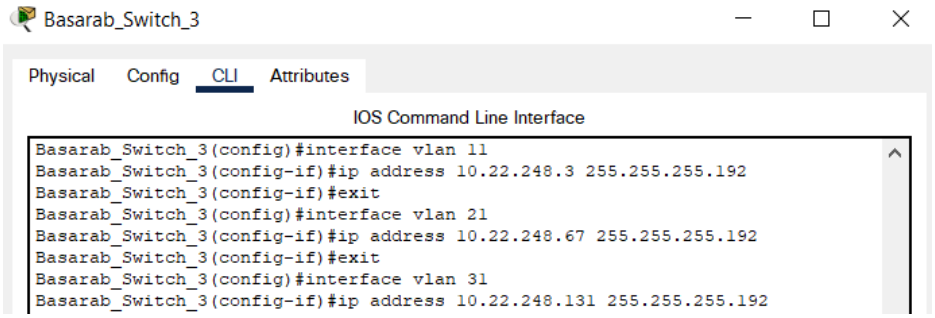

Рисунок 3.32 – Призначення адрес VLAN до комутаторів

Для ввімкнення протоколу DHCP та забезпечення можливості вузлам з різних віртуальних локальних мереж обмінюватися інформацією необхідно на роутері створити під-інтерфейси на порті, що безпосередньо виходить на підмережу LAN5. Після створення такого віртуального порту необхідно ввімкнути технологію інкапсуляції dot1Q із вказівкою номера віртуальної локальної мережі, а згодом задати IP-адресу, що є першою допустимою із пулу

VLAN. На рисунку 3.33 зображено скрипт налаштування для кожного під-інтерфейсу.

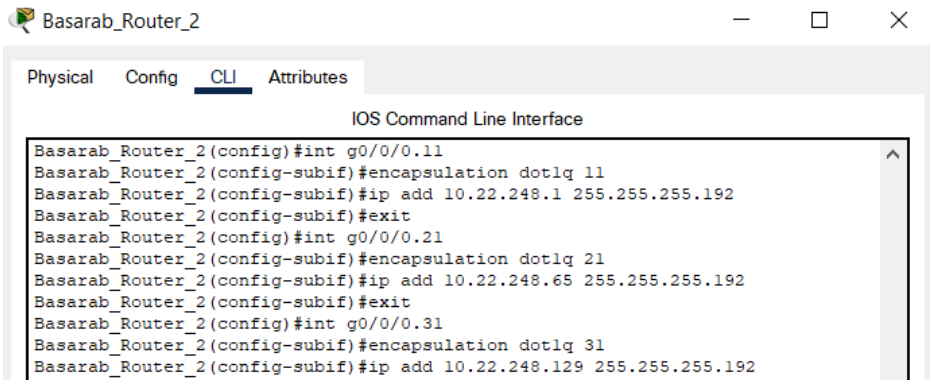

Рисунок 3.33 – Налаштування під-інтерфейсів на маршрутизаторі

Для перевірки валідності налаштувань динамічного розподілу адрес необхідно вибрати на ПК підмережі LAN5 отримання IP-адреси (рисунок 3.34) та параметрів шлюзу за замовчуванням та серверу DNS (рисунок 3.35) за допомогою протоколу DHCP.

Рисунок 3.34 – Перевірка отримання вузлом адреси через DHCP

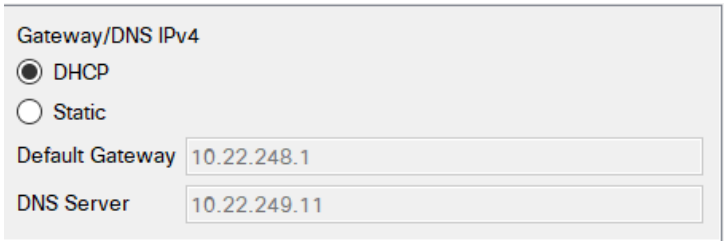

Рисунок 3.35 – Перевірка отримання вузлом Gateway/DNS через DHCP

Як видно на рисунках отримана адреса належить до заданого VLAN-пулу, отже динамічна адресація налаштована успішно.

Після виконання всіх налаштувань віртуальних локальних мереж необхідно перевірити чи мають зв'язок вузли з різних VLAN. Результатом перевірки впроваджених налаштувань віртуальних локальних мереж є успішні ехо-запити між комп'ютерами в одній та різних VLAN. Крім того кожен вузол будь-якої підмережі організації має змогу обмінюватися інформацією із хостами налаштованих віртуальних мереж, що можна побачити на рисунку 3.36.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	VLAN11 PC1	VLAN11 PC3	ICMP		0.000	N	0	(edit)
	Successful	VLAN21 PC1	VLAN21 PC3	ICMP		0.000	N	1	(edit)
	Successful	VLAN31 PC3	VLAN31 PC1	ICMP		0.000	N	2	(edit)
	Successful	VLAN11 PC1	VLAN21 PC3	ICMP		0.000	N	3	(edit)
	Successful	VLAN21 PC1	VLAN31 PC3	ICMP		0.000	N	4	(edit)
	Successful	VLAN31 PC2	VLAN11 PC3	ICMP		0.000	N	5	(edit)

Рисунок 3.36 – Результат надсилання ехо-запитів між різними VLAN

Команди для налаштувань наведено в додатку А.

3.5 Перевірка роботи КС ІТ-компанії «BAS-IQ»

Спроектована комп'ютерна система повністю відповідає вимогам завдання на кваліфікаційну роботу та має високий рівень унікальності внаслідок використання прізвища студента для іменування мережевих пристроїв та інших параметрів комп'ютерної моделі системи.

Після виконання всіх вищезазначених налаштувань система працює коректно, про що свідчить успішні ехо-запити між хостами різних підмереж (рисунок 3.37).

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	LAN1-PC1	LAN2-PC2	ICMP		0.000	N	1	(edit)
	Successful	VLAN21 PC1	LAN3-PC1	ICMP		0.000	N	2	(edit)
	Successful	VLAN31 PC3	LAN1-PC2	ICMP		0.000	N	3	(edit)
	Successful	LAN2-PC1	LAN4-PC1	ICMP		0.000	N	4	(edit)
	Successful	VLAN31 PC1	LAN3-PC2	ICMP		0.000	N	5	(edit)

Рисунок 3.37 – Перевірка зв'язку між комп'ютерами різних підмереж

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Обґрунтування обраного напрямку розробки компонента системи та принцип його роботи

В якості компонента системи було розроблено програму, що перевіряє поточний стан мережевих приладів та, у разі виявлення збоїв, інформує системного адміністратора за допомогою email-повідомлення. Подібні способи моніторингу стану комп'ютерних систем є вкрай актуальними особливо для IT-компаній, що представлють середній та великий бізнес, адже кількість мережевого устаткування в їх офісах може сягати декілької сотень штук, що означає нераціональність мануальної перевірки правильності роботи мережі системними адміністраторами.

Мережевий контролер (PT-Controller) було додано в підмережу другого поверху головного офісу. IP-адреса була виділена із сегменту допустимих для цієї підмережі, а саме 10.22.250.50/26. На рисунку 4.1 наведено топологію підмережі другого поверху головного офісу після підключення до неї контролера.

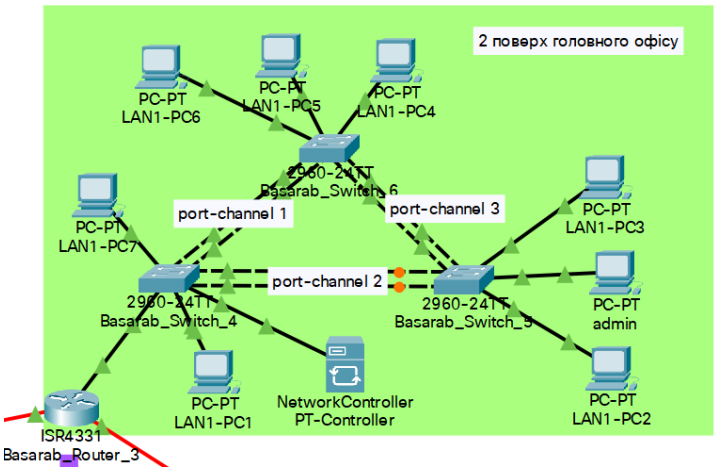

Рисунок 4.1 – Мережевий контролер в топологічній схемі підмережі 2 поверху головного офісу

Для під'єднання контролера до комутатора було використано інтерфейс FastEthernet, а для його живлення – звичайну розетку. В цій же підмереже

розміщено комп’ютер системного адміністратора (admin) та комп’ютер, на якому буде запущено код програми для моніторингу (LAN1-PC2).

Загальна схема взаємозв’язків між контролером та комп’ютерами зображена на рисунку 4.2.

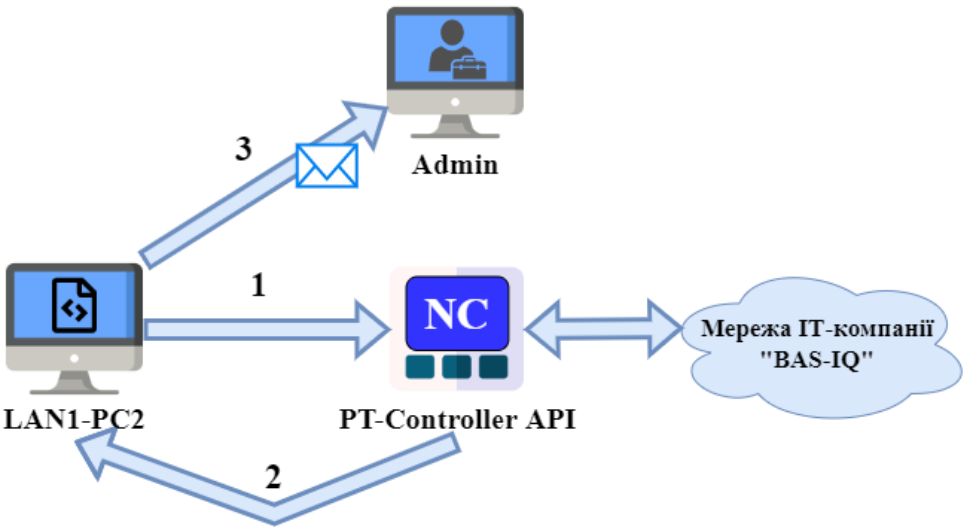

Рисунок 4.2 – Принцип взаємодії комп’ютерів з мережевим контролером

Цифри над стрілками означають послідовність дій, зокрема:

1. Надсилання запиту від комп’ютера, де запущено код, до API мережевого контролера з метою запиту файлу з повною інформацією про мережеві пристрої;

2. Після успішного встановлення зв’язку алгоритм отримує файл із актуальними даними про мережеве устаткування з усієї комп’ютерної системи. Дані автоматично оновлюються протягом кожних 10 хвилин за рахунок вбудованого в функції контролера таймера на «inner healtcheck»;

3. Після отримання JSON-файлу з інформацією, алгоритм перевіряє параметр досяжності кожного приладу в списку та у разі знаходження помилки додає ім’я та MAC-адресу до списку, котрий буде надіслано електронним листом системному адміністратору.

4.2 Опис розробленої програми для моніторингу досяжності мережевого обладнання

Для створення облікового запису в додатку Cisco Network Controller на будь-якому комп'ютері корпоративної мережі необхідно ввести адресу мережевого контролера в пошуковий рядок браузера (Рисунок 4.2). Цей обліковий запис знадобиться для доступу до API мережевого контролера під час написання програмного коду.

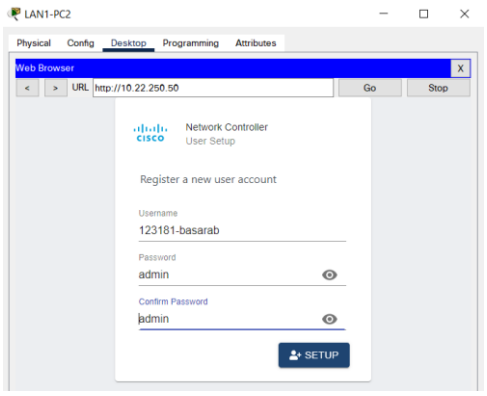

Рисунок 4.3 – Реєстація користувача в Cisco Network Controller

Вбудовані функції середовища моделювання Cisco Packet Tracer дозволяють налаштувати та перевірити розроблений скрпт для моніторингу в інтеграції з вже з існуючою мережевою схемою. Для цього необхідно налаштувати поштовий сервер та створити облікові записи для користувачів. Налаштування поштового серверу передбачає задання імені поштового домену. На рисунку 4.4 зображено вікно налаштування служби електронного листування на сервері в Packet Tracer.

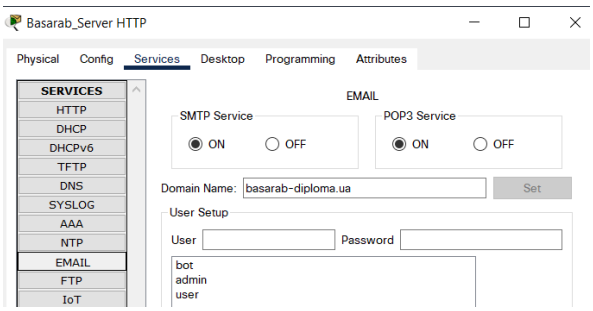

Рисунок 4.4 – Вікно налаштування служби Email на сервері

Ім’я вказаного домена та IP-адреса сервера, що надає можливість корпоративного листування, мають бути додані в таблицю DNS-сервера. Цей етап вже виконано, адже в третьому розділі кваліфікаційної роботи було описано налаштування серверу DNS з таким же доменом (basarab-diploma.ua) для веб-сервера.

Для перевірки коректності роботи поштового сервера необхідно створити декілька облікових засобів користувачів системи. Для цього в секції «User Setup» в тому ж вікні конфігурації необхідно задати ім’я користувача та його пароль. На рисунку 4.5 зображено перелік існуючих поштових облікових записів та обрано користувачем з іменем «admin» та паролем «cisco».

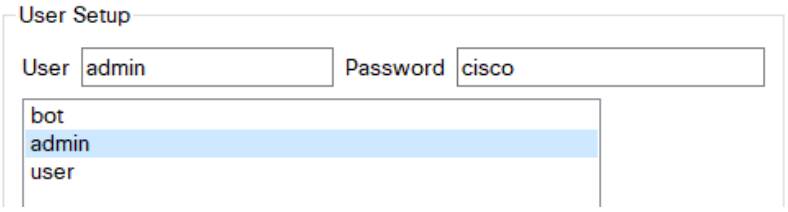

Рисунок 4.5 – Перелік існуючих поштових облікових записів

Після створення кількох поштових абонентів треба на комп’ютерах, що будуть виконувати роль поштових клієнтів задати параметри їх облікового запису, а саме видане на сервері ім’я, поштову адресу, наприклад admin@basarab-diploma.ua, адресу поштового серверу та пароль для входу. Приклад вікна налаштувань поштової служби на ПК наведено на рисунку 4.6.

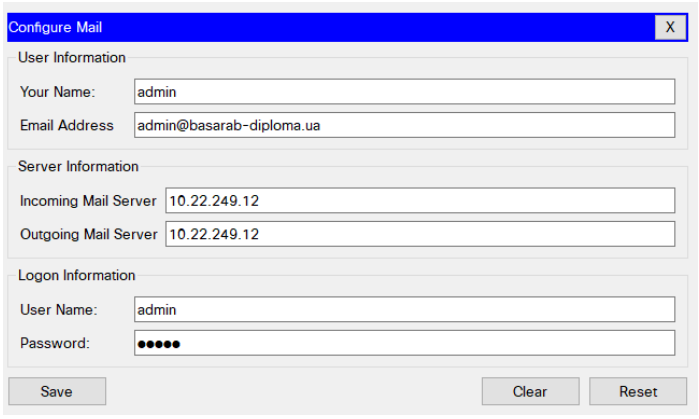

Рисунок 4.6 – Налаштування електронної пошти на ПК адміністратора

Після збереження коректно заданих налаштувань можна відправити тестове повідомлення іншому клієнту поштової служби. Для цього необхідно натиснути кнопку «Compose» та вказати адресата, тему листа й текст повідомлення. Після натискання кнопки «Send» лист буде відправлено на сервер та звідти на інший комп’ютер. Інтерфейс відправки електронного повідомлення із заповненими полями наведено на рисунку 4.7.

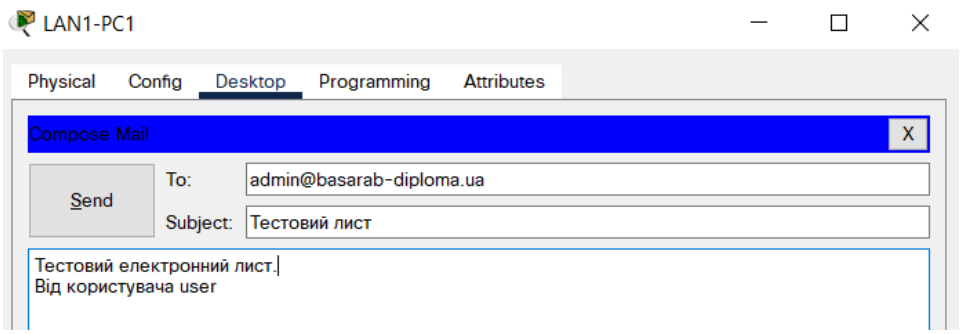

Рисунок 4.7 – Створення тестового електронного листа

Цей електронний лист повинен з’явитися в списку доступних після натискання кнопки «Receive». На рисунку 4.5 можна побачити, що лист було успішно доставлено до адресата, при чому тема й текст повністю збігаються.

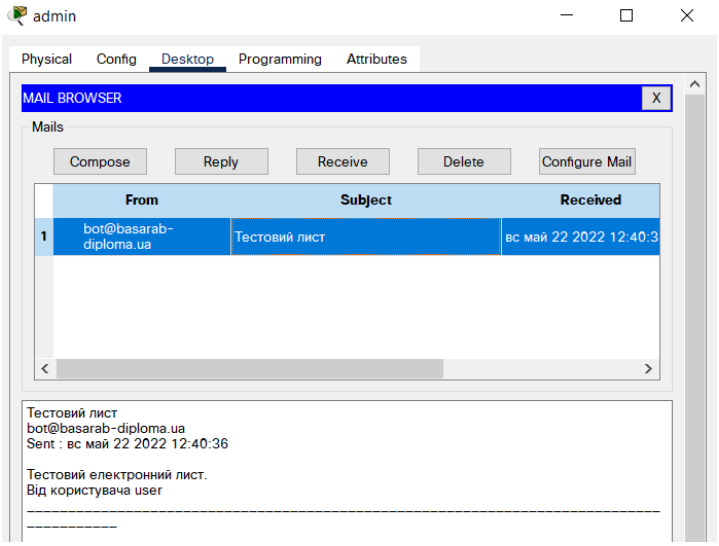

Рисунок 4.8 – Успішне отримання відправленого листа

На цьому етапі налаштування та перевірка поштового зв’язку успішно завершена що означає перехід до етапу написання програмного коду. Для написання скрипту збору та обробки інформації було використано високорівневу мову програмування Python, адже її модулі для роботи з архітектурою REST API та JSON-файлами значно полегшують процес розробки програмного забезпечення.

Програмний код, що реалізує відправлення сповіщень про недосяжність мережевих приладів, складається з наступних компонентів:

– відправка запиту на Network Controller API з метою отримання сервісного квитка процесу;

– відправка запиту для отримання мережевої інформації;

– виведення мережевої інформації на екран комп’ютера;

– перевірка стану маршрутизаторів та комутаторів;

– відправка електронного листа адміністратору у разі знаходження недосяжних спристроїв.

Повний лістинг розробленої програми наведено в додатку Б.

4.3 Перевірка працездатності розробленої програми для моніторингу досяжності мережевого обладнання

Після запуску програми для моніторингу перш за все на екрані з’явиться унікальний номер сервісного квитка, а також код відповіді на запит, що відповідає кодовій HTTP-моделі відповіді [18]. Ця модель передбачає класифікації кодів відповіді на інформаційні (100-199), успішні (200-299), перенаправлені (300-399), клієнтські помилки (400-499) та серверні помилки (500-599). На рисунку 4.9 наведено приклад виведення на екран номера квитка, а також 200 статусу, що свідчить про успішність запиту.

```
Starting main.py (Python)...
Service Ticket: NC-77-c260d62c049e4d15be9d-nbi
Request to API has code:200
```

Рисунок 4.9 – Виведення на екран сервісного квитка та коду запиту

Наступним, що побачить на екрані користувач буде вміст json-файлу, в якому зібрана інформація про поточний стан маршрутизаторів та комутаторів. Серед другорядної інформації там місяться дійсно важливі параметри, такі як список підключених пристроїв та їх адрес, ідентифікатор, MAC та IP-адреса, статус досяжності, номер версії та інше.

На рисунку 4.10 зображено приклад словника інформації для комутатора «Basarab_Switch_8», що програма виводить на екран користувача.


```
{
    "collectionStatus": "Unreachable",
    "connectedInterfaceName": [
        "FastEthernet0",
        "FastEthernet0",
        "GigabitEthernet0/0/1"
    ],
    "connectedNetworkDeviceIpAddress": [
        "10.22.250.126",
        "10.22.250.125",
        "10.22.250.65"
    ],
    "connectedNetworkDeviceName": [
        "LAN3-PC1",
        "LAN3-PC2",
        "Basarab_Router_0"
    ],
    "errorDescription": "",
    "globalCredentialId": "6ef2fbce-87ed-4029-8ddb-7ba4da12b8db",
    "hostname": "Basarab_Switch_8",
    "id": "CAT101086NV-uuid",
    "interfaceCount": "27",
    "inventoryStatusDetail": "Unreachable",
    "lastUpdateTime": "34",
    "lastUpdated": "2022-05-29 16:51:21",
    "macAddress": "000C.CF6A.2C02",
    "managementIpAddress": "10.22.250.66",
    "platformId": "2960",
    "productId": "2960-24TT",
    "reachabilityFailureReason": "Unable to ping to device. ",
    "reachabilityStatus": "Unreachable",
    "serialNumber": "CAT101086NV-",
    "softwareVersion": "15.0",
    "type": "Switch",
    "upTime": "1 hours, 20 minutes, 42 seconds"
}
```


Рисунок 4.10 – Приклад отриманої інформації про один прилад

Після того, як алгоритм вивів на екран всю інформації настає етап перевірки на досяжність пристроїв. В загальному розумінні досяжність – це можливість відправити ехо-запит на девайс, отже ця властивість може свідчити як про помилки фізичного підключення пристроя (наприклад вимкнений вручну інтерфейс чи непідключений кабель), так і про помилки в налаштуванні IP-адреси інтерфейса мережевого пристроя. Значення поля reachabilityStatus може бути або «Reachable», що означає досяжність пристроя контролером, або «Unreachable», тобто пристрій не може пінгуватися із мережевого контролера. Саме у разі виявлення того, що пристрій має недосяжний статус алгоритм видасть повідомлення з поміткою «!!! Warning» та сповістить користувача програми повідомленням про виявлену помилку. В іншому випадку, тобто коли пристрій успішно приймає ехо-запит, алгоритм виведе на екран повідомлення

про коректну роботу приладу й список підключених до нього пристроїв. На рисунку 4.9 наведено приклад консольного вікна, в якому алгоритм виявив помилку досяжності в трьої пристроях, про що свідчить останній рядок тексту.

```
('Basarab_Router_3 is working fine. List of connected devices:', ['Basarab_Switch_4', 'Basarab_Router_IPS',
'Basarab_Router_4'])
----------
('Basarab_Switch_4 is working fine. List of connected devices:', ['Basarab_Switch_6', 'Basarab_Switch_6',
'Basarab_Switch-5', 'Basarab_Switch-5', 'LAN1-PC1', 'Basarab_Router_3', 'NetworkController'])
----------
('Basarab_Switch_6 is working fine. List of connected devices:', ['Basarab_Switch_4', 'Basarab_Switch_4',
'Basarab_Switch-5', 'Basarab_Switch-5'])
----------
('Basarab_Switch-5 is working fine. List of connected devices:', ['Basarab_Switch_4', 'Basarab_Switch_4',
'Basarab_Switch_6', 'Basarab_Switch_6', 'LAN1-PC2', 'admin'])
----------
('Basarab_Router_IPS is working fine. List of connected devices:', ['Basarab_Router_0', '209.165.200.4/28',
'Basarab_Router_3'])
----------

!!! Warning
('Basarab_Router_0', ' is unreachable')
----------
('Basarab_Router_4 is working fine. List of connected devices:', ['Basarab_Router_1', 'Basarab_Router_2',
'Basarab_Router_3'])
----------
('Basarab_Router_1 is working fine. List of connected devices:', ['Basarab_Switch_7', 'Basarab_Router_4'])
----------
('Basarab_Router_2 is working fine. List of connected devices:', ['Basarab_Switch_0', 'Basarab_Router_4'])
----------
('Basarab_Switch_0 is working fine. List of connected devices:', ['VLAN11 PC1', 'Basarab_Server_AAA', 'VLAN21 PC1',
'VLAN31 PC1', 'Basarab_Router_2', 'Basarab_Switch_3'])
----------
('Basarab_Switch_3 is working fine. List of connected devices:', ['VLAN11 PC3', 'VLAN21 PC2', 'VLAN31 PC2',
'Basarab_Switch_2', 'Basarab_Switch_0'])
----------
('Basarab_Switch_7 is working fine. List of connected devices:', ['LAN4-PC2', 'LAN4-PC1', 'Basarab_Server DNS',
'Basarab_Server HTTP', 'Basarab_Router_1'])
----------
('Basarab_Switch_2 is working fine. List of connected devices:', ['VLAN11 PC2', 'VLAN21 PC3', 'VLAN31 PC3',
'Basarab_Switch_3'])
----------

!!! Warning
('Basarab_Switch_1', ' is unreachable')
----------

!!! Warning
('Basarab_Switch_8', ' is unreachable')
----------
3 issues were found and reported to admin by email
```

Рисунок 4.11 – Виведення на екран імені пристроя, його статусу й під’єднаний приладів у разі досяжності

Після цього ініціалізується відправка електронного листа на корпоративну поштову адресу адміністратора. Такий лист має тему «Network errors» для того, аби системний адміністратор одразу зміг ідентифікувати його як важливий серед інших електронних листів. Текст електронного повідомлення містить інформацію про імена та MAC-адреси мережевих пристроїв, що є недосяжними для контролера. Крім того адміністратор побачить причину недосяжності запиту, що було взято з поля “ReachabilityFailureReason” файлу з повним списком інформації про пристрої. Приклад успішно отриманого електронного листа з переліком мережевих поламок наведено на рисунку 4.11.

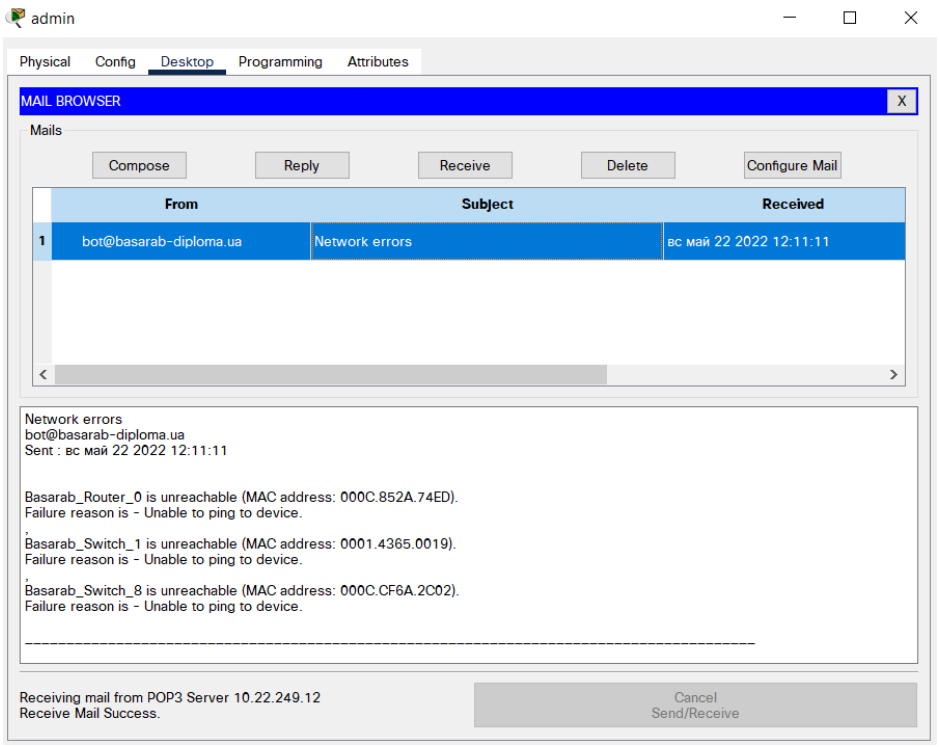

Рисунок 4.11 – Вміст отриманого адміністартором листа з переліком недосяжних мережевих приладів

ВИСНОВКИ

В даній кваліфікаційній роботі бакалавра було виконано дослідження об’єкта впровадження, тобто сукупності офісів IT-компанії «BAS-IQ», проєктування корпоративної мережі та написання технічних вимог до неї, налаштування мережевих приладів та перевірка їх роботи в середовищі моделювання Cisco Packet Tracer, а також розробка програми, що реалізує отримання та обробку даних щодо стану досяжності мережевого устаткування системи.

Робота виконана з урахуванням сучасних тенденцій розвитку побудови корпоративних мереж, адже для проєктування були використані актуальні технології передачі даних та високоякісні апаратні пристрої від розробника Cisco, що забезпечують швидкісний обмін інформації в системі. Крім того програмний код для реалізації моніторингу стану мережі написаний мовою Python, що є однією з найпопулярніших мов програмування на теперішній час.

Конфігураційні налаштування елементної бази корпоративної мережі забезпечують відповідність адресного простору до поставлених клієнтських вимог, динамічну маршрутизацію за допомогою протоколу EIGRP, впровадження віртуальних локальних мереж та тунельного VPN-з’єднання для підвищення рівня безпеки. Також було налаштовано динамічну трансляцію адрес для виходу користувачів локальних мереж в Інтернет. Конфігурації серверного обладнання надають змогу для роботи HTTP, DNS та AAA сервісів.

Отримані результати кваліфікаційної роботи доцільно використовувати не лише в сфері проєктування комп’ютерних систем для розробки програмного забезпечення, а й для побудови систем із подібними задачами, наприклад для фінансово-аналітичних компаній, новітніх навчальних центрів, маркетингових агенцій тощо.

Програма для моніторингу стану досяжності мережевого обладнання, яка працює на базі інформації, що отримує мережевий контролер може значно поліпшити процес знаходження помилок в роботі комп’ютерної системи.

Алгоритм реалізований таким чином, щоб у разі знаходження проблем з досяжністю інтерфейсу маршрутизатора чи комутатора, сповістити системного адміністартора електронним листом зі списком приладів та їх MAC-адрес. Враховуючи перспективи розвитку корпоративної мережі компанії «BAS-IQ», ця програма може в значній мірі економити час мережевої діагностики цілої системи, що в свою чергу зменшує економічні витрати підприємства.

Зважаючи на стрімкий розвиток IT-сфери, тематика роботи є вкрай актуальною, що надає сенс подальшому дослідженню її для проєктування нових комп’ютерних систем суміжного призначення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Software-defined networking [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Software-defined_networking.

2. ДСТУ EN 50160:2014 «Характеристики напруги електропостачання в електричних мережах загального призначення» [Електронний ресурс] – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page?id_doc=51529.

3. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. –Д.: НТУ «ДП», 2022. – 63 с

4. ДСН 3.3.6.042-99 [Електронний ресурс] – Режим доступу до ресурсу: http://nbuviap.gov.ua/images/nub/Dmap/15_sanitar%20normy%20mikroklimatu.pdf.

5. ДСТУ IEC 60529:2019 [Електронний ресурс] – Режим доступу до ресурсу: http://online.budstandart.com/ru/catalog/doc-page?id_doc=88654.

6. System requirements for Android Studio [Електронний ресурс] – Режим доступу до ресурсу: https://developer.android.com/studio.

7. Моноблок Lenovo IdeaCentre 5i 27IOB6 [Електронний ресурс] – Режим доступу до ресурсу: https://hard.rozetka.com.ua/ua/324328834/p324328834/.

8. Сервер ARTLINE Business T65v04 [Електронний ресурс] – Режим доступу до ресурсу: https://artline.ua/product/server-artline-business-t65v04.

9. Комутатор Smart Gigabit Ethernet Cisco SG220-26-K9-EU [Електронний ресурс] – Режим доступу до ресурсу: https://comtrade.ua/cisco-sg220-26-k9-eu/.

10. Маршрутизатор Cisco ISR4331/K9 [Електронний ресурс] – Режим доступу до ресурсу: https://stack-systems.com.ua/marshrutizator-cisco-isr4331-k9.

11. Контролер Cisco AIR-CT5508-25-K9 [Електронний ресурс] – Режим доступу до ресурсу: https://stack-systems.com.ua/kontroller-cisco-air-ct5508-25-k9.

12. Лінійно-інтерактивне ДБЖ LPM-L625VA (437Вт) [Електронний ресурс] – Режим доступу до ресурсу: https://logicpower.ua/ua/product/4977.

13. Кабель «вита пара» DIGITUS CAT 5e U-UTP Gray [Електронний ресурс] – Режим доступу до ресурсу: https://www.moyo.ua/ua/kabel_digitus_cat_5e_u-utp_gray/400050.html.

14. Кабель оптоволоконний Corning 012TEY-13188A2G [Електронний ресурс] – Режим доступу до ресурсу: https://e-server.com.ua/opticheskie-komponenty/opticheskij-kabel/kabel-multimode/kabel-volokonno-opticheskij-universalnyj-corning-012tey-13188a2g-detail.

15. Комплект бездротовий Logitech MK235[Електронний ресурс] – Режим доступу до ресурсу: https://hard.rozetka.com.ua/ua/logitech_mk235_black/p8370356.

16. CIDR/VLSM Calculator [Електронний ресурс] – Режим доступу до ресурсу: https://subnettingpractice.com/vlsm.html.

17. Переваги протоколу EIGRP [Електронний ресурс] – Режим доступу до ресурсу: https://studfile.net/preview/5759717/page:31/.

18. HTTP коди [Електронний ресурс] – Режим доступу до ресурсу: https://hostiq.ua/wiki/ukr/http-status-codes/.

ДОДАТОК А

Конфігураційні команди для налаштування комп’ютерної мережі

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.22001-01 12 01

Листів 7

Дніпро
2022

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду програмування та налаштування компонентів корпоративної мережі комп’ютерної системи.

Програма призначена для виконання базових конфігурацій інтерфейсів, запровадження DHCP для VLAN, AAA за протоколом RADIUS, створення локального користувача, налаштування динамічної маршрутизації за протоколом EIGRP, консолі та віртуальних ліній, VPN та динамічного NAT.

ЗМІСТ

//1. Базові налаштування маршрутизатора
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
//Ввімкнення шифрування паролів
service password-encryption
!
//Налаштування імені пристрою
hostname Basarab_Router_2
!
//Задання пароля для привілегійованого режиму
enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1
!
//1.1 Налаштування DHCP для VLAN
ip dhcp excluded-address 10.22.248.1 10.22.248.10
!
ip dhcp pool basarab_poolvlan11
network 10.22.248.0 255.255.255.192
default-router 10.22.248.1
dns-server 10.22.249.11
ip dhcp pool basarab_poolvlan21
network 10.22.248.64 255.255.255.192
default-router 10.22.248.1
dns-server 10.22.249.11
ip dhcp pool basarab_poolvlan31
network 10.22.248.128 255.255.255.192
default-router 10.22.248.1
dns-server 10.22.249.11
!
//1.2 Налаштування AAA-моделі за протоколом RADIUS
aaa new-model
!
aaa authentication login default group radius local
!
no ip cef
no ipv6 cef
!
//1.3 Створення локального користувача
username 123181_Basarab secret 5 1mERr$MKp6WULHmjLdYVBw6rbD11
username admin password 7 082048430017
!
//Налаштування протоколу для віддаленого підключення
ip ssh version 2
ip domain-name Basarab_Router_2
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
no ip address
duplex auto
speed auto

//1.4 Налаштування підінтерфейсів для маршрутизації між VLAN
interface GigabitEthernet0/0/0.11
encapsulation dot1Q 11
ip address 10.22.248.1 255.255.255.192
!
interface GigabitEthernet0/0/0.21
encapsulation dot1Q 21
ip address 10.22.248.65 255.255.255.192
!
interface GigabitEthernet0/0/0.31
encapsulation dot1Q 31
ip address 10.22.248.129 255.255.255.192
!
//1.5 Налаштування адреси для фізичних інтерфейсів
interface GigabitEthernet0/0/1
ip address 10.22.249.129 255.255.255.128
duplex auto
speed auto
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
ip address 10.1.1.1 255.255.255.252
clock rate 128000
!
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
//1.6 Налаштування динамічної маршрутизації EIGRP
router eigrp 100
network 10.0.0.0
!
ip classless
!
ip flow-export version 9
!
// Налаштування MOTD банеру
banner motd ^CThis is a secure system. Authorized Access Only. Created by Danylo Basarab^C
!
//Вказування адреси RADIUS-сервера та ключа
radius-server host 10.22.249.240 auth-port 1645 key radius123

//1.7 Налаштування консолі та віртуальних ліній
line con 0
password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
transport input ssh
line vty 5 15
transport input ssh
!
end

//2 Приклад налаштування VPN на маршрутизаторі
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
crypto isakmp key basarab123 address 10.1.1.17
crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
description VPN connection to Basarab_Router_0
set peer 10.1.1.17
set transform-set VPN-SET
match address 111
!
interface Serial0/1/0
ip address 10.1.1.13 255.255.255.252
clock rate 128000
crypto map VPN-MAP
!
access-list 111 permit ip 10.22.250.0 0.0.0.63 10.22.250.64 0.0.0.63

//3 Приклад налаштування динамічного NAT
access-list 1 permit 10.22.248.0 0.0.7.255
!
interface GigabitEthernet0/0/0
ip address 10.1.1.18 255.255.255.252
ip nat inside
!
interface GigabitEthernet0/0/1
ip address 209.165.200.3 255.255.255.240
ip nat outside
!
interface Serial0/1/0
ip address 10.1.1.14 255.255.255.252
ip nat inside
ip nat pool Basarab_Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list 1 pool Basarab_Internet

ДОДАТОК Б

Лістинг програми для моніторингу стану досяжності мережевих приладів

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.22001-01 12 01

Листів 6

Дніпро
2022

АНОТАЦІЯ

Дана програма містить в собі код для моніторингу стану досяжності маршрутизаторів та комутаторів в корпоративній мережі IT-компанії «BAS-IQ».

Програма призначення для отримання та обробки інформації про мережеві прилади шляхом запиту на Cisco Network Controller API. У разі виявлення помилок досяжності приладів програма відправить електронного листа на корпоративну пошту системного адміністратора.

Програма написана мовою Python, відлагоджена й протестована в середовищі моделювання Cisco Packet Tracer.

ЗМІСТ

#1. Лістинг програми для моніторингу стану досяжності мережевих приладів

```
#Імпортування необхідних для роботи програми модулів
import requests
import json
from email import *

#Вказання посилання на API мережевого контролера
baseUri = "http://10.22.250.50/api/v1"

#Запит на отримання сервісного квитка автентифікації
headers = {"Content-Type": "application/json"}
data = json.dumps({"username": "123181-basarab", "password": "admin"})
resp = requests.post(baseUri+"/ticket", data=data, headers=headers)
result = resp.json()

#Отримання сервісного квитка та виведення його на екран
ticket = result["response"]["serviceTicket"]
print("Service Ticket: "+ticket)

#Запит на отримання інформації про мережеві девайси
headers = {"X-Auth-Token": ticket }
resp = requests.get(baseUri+"/network-device", headers=headers)

#Виведення статусу запиту
print ('Request to API has code:' + str(resp.status_code))

#Переформатування файлу в JSON та виведення його на екран
result = resp.json()
print (json.dumps(result, indent=4))

error = 0
mail_text = []

#Перевірка статусу досяжності кожного мережевого пристроя з отриманого файлу
for i in result["response"]:
        hostname = str(i.get('hostname'))
        mac = str(i.get('macAddress'))
        failure_reason = str(i.get('reachabilityFailureReason'))
        connected_devices = i.get('connectedNetworkDeviceName')
        #Перевірка статусу досяжності мережевого приладу
        if i["reachabilityStatus"] == 'Unreachable':
                error += 1
```

```
                print('\n!!! Warning')
                print(hostname, ' is unreachable')

                current_text = "\n" + hostname + " is unreachable (MAC address: " +
mac + ").\n" + "Failure reason is - " + failure_reason + "\n"
                mail_text.append(current_text)

        else:
                print(hostname + ' is working fine. List of connected devices:' ,
connected_devices)

#Виведення на екран результатів перевірки
if error < 1:
        print('Everything is OK!')
else:
        #Ініціалізація клієнта поштового сервісу
        EmailClient.setup(
                        "bot@basarab-diploma.ua",
                        "basarab-diploma.ua",
                        "bot",
                        "cisco"
                )
        #Відправка електронного листа зі списком недосяжних пристроїв
адміністартору
        EmailClient.send("admin@basarab-diploma.ua", 'Network errors' , mail_text)
        print(str(error) + ' issues were found and reported to admin by email')
```