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 Акімова В.В.
(ПІБ)

академічної групи 123-21ск
(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 туристичної компанії «Альфа тур» з детальним опрацюванням побудови та налаштування корпоративної мережі»

(назва за наказом ректора)

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

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

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

« » _____ 2024 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Акімов В.В. **академічної групи** 123-21ск
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

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

на тему «Комп'ютерна система туристичної компанії «Альфа тур» з детальним опрацюванням побудови та налаштування корпоративної мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 29.04.2024 № 375-с

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел розглянути призначення та завдання побудови мережі компаніїї «Альфа тур»	05.05.2024
Розробка апаратної частини	Розробити вимоги до функцій, виконуваними системою корпоративною мережою	13.05.2024
Розробка корпоративної мереж	Побудувати в Packet Tracer модель корпоративної мережі компанії, виконати налаштування та перевірку роботи системи	25.05.2024
Розробка компонента системи	Розробити детальне опрацювання побудови та налаштування корпоративної мережі	09.06.2024

Завдання видано 14.04.2024 Шедловська Я.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі _____

Дата подання до екзаменаційної комісії 18.06.2024

Прийнято до виконання Акімов В.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 90 с., 32 рис., 6 табл., 1 додатки, 6 джерел.

КЛЮЧОВІ СЛОВА: комп'ютерна система, розробка, об'єкт, мета, методи, результати, новизна, характеристики, впровадження, взаємозв’язок, рекомендації, сфера застосування, значимість, висновки.

Об’єкт розробки – комп'ютерна система. Мета роботи – розробка та впровадження комп'ютерної системи для покращення процесів у туристичній компанії. Здійснено аналіз сучасних технологій, розробку та налаштування корпоративної мережі, встановлення програмного забезпечення та здійснено тестування системи.

У результаті проведеного дослідження розроблена комп'ютерна система забезпечує ефективну роботу туристичної компанії, підвищує швидкість обробки даних та забезпечує безпеку і конфіденційність інформації.

Основні конструктивні, технологічні й техніко-експлуатаційні характеристики системи включають високу стабільність роботи, можливість розширення та високий рівень захисту даних.

Комп'ютерна система успішно впроваджена у роботу туристичної компанії, що підтверджується позитивними відгуками користувачів та підвищенням продуктивності праці. Розроблена система має широкі можливості застосування у сфері туризму та подорожей, що робить її важливим інструментом для розвитку компанії.

Значимість кваліфікаційної роботи полягає у покращенні ефективності та конкурентоспроможності туристичної компанії, а також у внесенні новаторських рішень у сферу технологій.

На основі проведеного дослідження можна зробити висновок, що розроблена комп'ютерна система є ефективним інструментом для покращення бізнесу та підвищення якості обслуговування клієнтів у туристичній галузі.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

VPN - Віртуальна Приватна Мережа (укр.), Virtual Private Network (англ.)

AAA - Аутентифікація, Авторизація та Облік (укр.), Authentication, Authorization, and Accounting (англ.)

OSPF - Відкритий Коротший Шлях Першим (укр.), Open Shortest Path First (англ.)

EtherChannel - Ефірний Канал (укр.), EtherChannel (англ.)

мережева інфраструктура - network infrastructure (англ.)

пристрій - device (англ.)

маршрутизація - routing (англ.)

аутентифікація - authentication (англ.)

авторизація - authorization (англ.)

облік - accounting (англ.)

трафік - traffic (англ.)

конфіденційність - confidentiality (англ.)

цілісність - integrity (англ.)

пропускна здатність - bandwidth (англ.)

моделювання - modeling (англ.)

ресурс - resource (англ.)

аналіз - analysis (англ.)

ВСТУП

У сучасному світі, де швидкість і ефективність є ключовими чинниками успіху, роль інформаційних технологій в туристичній індустрії набуває особливої ваги. Туристичні компанії, які використовують передові IT-рішення, здатні значно покращити якість обслуговування клієнтів, оптимізувати внутрішні процеси та підвищити свою конкурентоспроможність. Розробка ефективної комп'ютерної системи та її мережевої архітектури стає вирішальним кроком у трансформації бізнес-операцій і забезпеченні сталого розвитку компанії.

Ця робота присвячена проектуванню та аналізу комп'ютерної системи для туристичної компанії «Альфа Тур». Головна мета полягає у створенні інтегрованої і безпечної мережевої інфраструктури, яка забезпечить надійний зв'язок між відділеннями компанії, оптимізує управління ресурсами та покращує взаємодію з клієнтами.

У першому розділі детально аналізуються поточні тенденції і виклики в туристичній індустрії, що впливають на використання комп'ютерних систем. Далі, на основі цього аналізу, розробляється комплексний план створення мережі, який включає вибір технологій, проектування мережевої структури та стратегії безпеки.

Особлива увага приділяється питанням безпеки, оскільки збереження конфіденційності та інтегральності даних є критично важливим у туристичному бізнесі. Відповідно, у роботі розглядаються сучасні технічні засоби та методики, що застосовуються для захисту інформаційних систем від несанкціонованого доступу та інших кіберзагроз.

Завершальна частина роботи присвячена аналізу ефективності запропонованої мережевої архітектури. Результати тестування та впровадження системи в дію демонструють підвищення продуктивності операцій, поліпшення обслуговування клієнтів та зниження витрат компанії.

Таким чином, розробка комп'ютерної системи для «Альфа Тур» не лише вирішує оперативні завдання компанії, але й відкриває нові можливості для росту та інновацій у майбутньому.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп'ютерної мережі

Туристична галузь, насичена різноманітними бізнес-процесами та обміном великих обсягів інформації, вимагає високоефективної інформаційної інфраструктури. Основним інструментом в цьому контексті є комп'ютерна мережа, яка забезпечує зв'язок між різними відділами компанії, а також між компанією та її клієнтами.

Комп'ютерна мережа в туристичній компанії має вирішувати кілька ключових завдань. Перш за все, вона повинна забезпечити швидкий доступ до баз даних з пропозиціями, бронюванням, історією клієнтів, фінансовими даними та іншими критично важливими для бізнесу інформаційними ресурсами. Також важливим є підтримка комунікацій через електронну пошту, веб-сайти, онлайн-чати та інші сервіси, що дозволяють ефективно взаємодіяти з клієнтами та партнерами.

Умови застосування комп'ютерної мережі включають в себе не тільки її функціональність, але й вимоги до безпеки. Захист даних є критично важливим, адже сектор часто стикається з викликами, пов'язаними з захистом персональної інформації клієнтів та комерційної таємниці. Тому, сучасні комп'ютерні мережі повинні бути оснащені засобами криптографічного захисту, механізмами ідентифікації та автентифікації користувачів, а також засобами захисту від зовнішніх і внутрішніх загроз.

Враховуючи динамічний характер туристичної індустрії, мережева інфраструктура також повинна бути гнучкою та масштабованою, щоб відповідати змінюваним вимогам бізнесу, наприклад, зростанню кількості клієнтів або географічній експансії компанії.

1.2 Характеристика підприємства та умов застосування КС

Туристична компанія "Альфа Тур" займається організацією індивідуальних та групових турів по всьому світу. Як комплексне агентство, воно пропонує послуги з бронювання готелів, авіаквитків, трансферів, екскурсій, а також страхування подорожей. Різноманіття послуг вимагає високої організації внутрішніх процесів та ефективної взаємодії між відділами компанії.

Комп'ютерна система "Альфа Тур" є ключовим інструментом у підтримці цих процесів. Вона складається з корпоративної мережі, що об'єднує всі робочі станції, сервери та мобільні пристрої співробітників. Мережа дозволяє здійснювати централізоване управління даними, спрощує обмін інформацією між відділами та забезпечує надійний доступ до корпоративних ресурсів.

Умови застосування комп'ютерної системи включають:

1) Безперервність бізнес-процесів: Система має забезпечувати стабільність і доступність послуг 24/7, оскільки туристичний бізнес часто вимагає оперативного реагування на запити клієнтів в різних часових зонах.

2) Захист даних: З огляду на великі обсяги персональної інформації, які обробляються (включаючи паспортні дані, фінансову інформацію тощо), система повинна містити розширені засоби захисту даних та механізми виявлення та реагування на інформаційні загрози.

3) Масштабованість: З огляду на потенційне зростання компанії та розширення кількості послуг, мережева інфраструктура має бути готова до швидкого масштабування, включаючи додавання нових робочих станцій та серверів без втрати продуктивності.

4) Інтеграція систем: Комп'ютерна система має інтегруватися з зовнішніми системами партнерів і постачальників послуг, що вимагає високого рівня сумісності і безпеки при обміні даними.

1.3 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства

Інформаційне забезпечення підприємства, особливо в такій динамічній і чутливій сфері як туризм, вимагає застосування продуманих принципів, передових технічних рішень і математичних методів для ефективного управління даними, забезпечення безпеки та підтримки бізнес-процесів.

Принципи інформаційного забезпечення:

– інтегрованість: Дані з усіх відділів і філій підприємства мають бути інтегровані в єдину систему, що забезпечує їх актуальність та доступність у будь-який час;

– централізація управління: Єдине управління ресурсами і безпекою через централізовані IT-сервіси, що полегшує моніторинг, адміністрування та швидке вирішення проблем;

– конфіденційність, Цілісність, Доступність (CIA): Забезпечення конфіденційності інформації, захист її цілісності і забезпечення доступності для авторизованих користувачів.

Технічні способи:

– шифрування: Використання сучасних криптографічних алгоритмів для захисту даних під час зберігання та передачі;

– брандмауери та інтрузивні детекційні системи (IDS): Захист мережевих ресурсів від несанкціонованих доступів і атак;

Математичні методи:

– статистичний аналіз: Використання статистичних методів для аналізу даних та виявлення аномалій в поведінці користувачів або системних журналів, що може вказувати на спроби несанкціонованого доступу;

– криптографічні алгоритми: Застосування симетричних і асиметричних шифрів для забезпечення конфіденційності та цілісності інформації;

– оптимізаційні алгоритми: Розробка і впровадження алгоритмів для оптимізації маршрутів даних у мережі, що дозволяє зменшити затримки і збільшити пропускну здатність.

Застосування цих принципів, технічних засобів і математичних методів дозволяє "Альфа Тур" підтримувати високий рівень інформаційної безпеки, ефективності обробки даних і оперативності реагування на запити клієнтів, що є критично важливим для успіху в сучасному туристичному бізнесі.

1.4 Огляд існуючих інженерних рішень КС в галузі та визначення можливих напрямків рішення поставлених завдань

Туристична індустрія активно використовує інформаційні технології для оптимізації своєї діяльності, підвищення ефективності обслуговування клієнтів та забезпечення безпеки даних. Існує ряд інженерних рішень, які використовуються в галузі, особливо ті, що базуються на обладнанні відомих виробників, таких як Cisco. Ці рішення можуть бути інтегровані в комп'ютерні системи туристичних компаній для досягнення високого рівня продуктивності та безпеки.

Використання обладнання Cisco у туристичній галузі:

Cisco Meraki Cloud Managed Networks:

Опис: Ця платформа надає повний набір рішень для управління мережами, включаючи бездротові засоби, перемикачі та засоби безпеки, управляючи їх через хмару.

Застосування: Ідеально підходить для туристичних компаній з багатьма локаціями, де потрібне централізоване управління мережею.

Cisco Catalyst Switches:

Опис: Серія комутаторів, що забезпечує високу продуктивність і надійність, підтримує передові функції безпеки та управління мережею.

Застосування: Використання в офісних центрах і дата-центрах для забезпечення ефективної роботи мережевих ресурсів.

Cisco ASA Firewalls:

Опис: Міцні брандмауери, які забезпечують комплексний захист від загроз і уніфіковане управління безпекою.

Застосування: Забезпечення високого рівня захисту даних в туристичних компаніях, особливо важливо для захисту інформації клієнтів.

Cisco Unified Communications:

Опис: Рішення для інтеграції голосового, відео- та текстового спілкування в єдину платформу.

Застосування: Поліпшення внутрішньої та зовнішньої комунікації в туристичних компаніях, сприяння кращому обслуговуванню клієнтів.

Cisco Security Solutions:

Опис: Різноманітні рішення для захисту корпоративних мереж, включаючи захист кінцевих точок, антивірус, антишпигунські програми та інші засоби кібербезпеки.

Застосування: Забезпечення всебічного захисту інформаційних систем і даних в туристичній індустрії, особливо важливо для збереження довіри клієнтів.

Можливі напрямки рішення поставлених завдань

Використання зазначеного обладнання та технологій дозволяє туристичним компаніям досягати кращої інтеграції, безпеки, продуктивності та надійності своїх інформаційних систем. Поставлені завдання, такі як підвищення ефективності обробки запитів клієнтів, забезпечення безперервності бізнесу та захисту даних, можуть бути вирішені шляхом розгортання гнучких і масштабованих мережевих рішень від Cisco, що адаптовані під специфіку туристичної галузі.

1.5 Розробка схеми організаційної структури підприємства

Структура компанії має таку ієрархію:

1) Виконавче керівництво: Включає керівника компанії та вищих менеджерів, які відповідають за стратегічне планування, розвиток бізнесу та прийняття стратегічних рішень.

2) Відділ маркетингу та продажів: Цей відділ займається рекламою, просуванням бренду, просуванням туристичних пакетів та приваблennям клієнтів.

3) Відділ бронювання та обслуговування клієнтів: Відповідає за прийом і обробку бронювань, консультування клієнтів, вирішення їх запитів та вирішення проблем, що виникають у ході подорожей.

4) Фінансовий відділ: Відповідає за фінансове планування, облік та контроль над фінансами компанії, включаючи обробку платежів від клієнтів та розрахунки з постачальниками послуг.

5) Відділ технічної підтримки та IT: Забезпечує підтримку технічних систем компанії, у тому числі комп'ютерних програм та інфраструктури для оброблення даних та забезпечення безперебійної роботи.

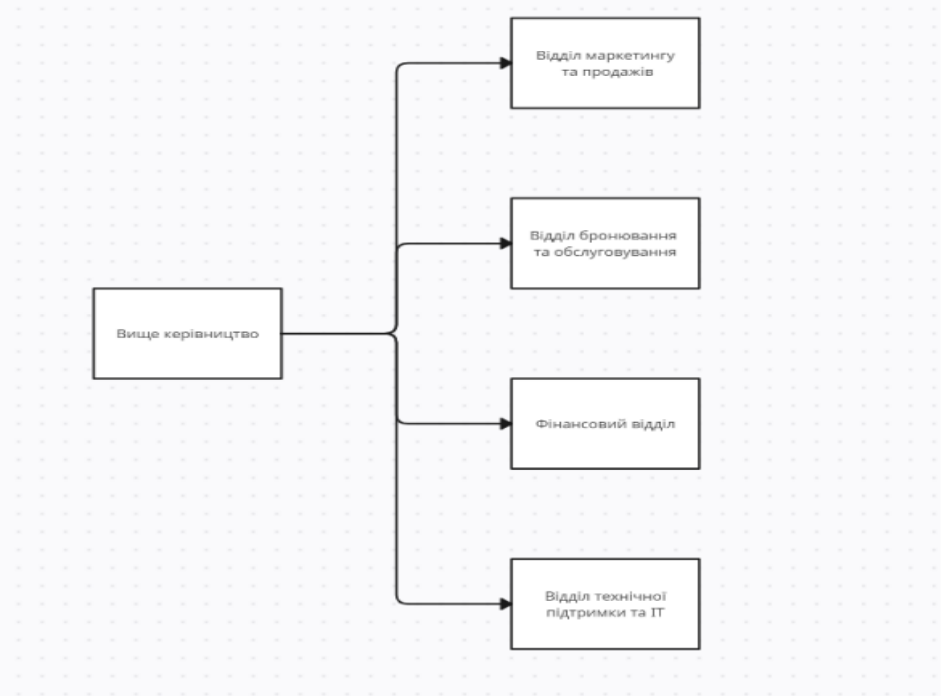

Рисунок 1.1 – Схема організаційної структури компанії

1.6 Завдання і мета роботи

Метою роботи є розробка Комп'ютерної системи для туристичної компанії «Альфа тур» з детальним опрацюванням побудови та налаштування корпоративної мережі.

Для вирішення поставленої задачі, в роботі слід виконати наступні етапи:

– аналіз потреб компанії та її інфраструктури;

– формулювання технічних вимог до мережі;

– вибір мережевої архітектури та обладнання;

– розробка специфікації апаратних засобів;

– конфігурування мережевого обладнання;

– тестування мережі та її компонентів.

Результатом цієї роботи має бути корпоративна мережа, яка відповідає потребам компанії «Альфа тур», є масштабованою, надійною та безпечною для забезпечення ефективної діяльності туристичної компанії

1.7 Визначення можливих напрямків рішення поставлених завдань

У рамках розробки та оптимізації комп'ютерної системи для туристичної компанії "Альфа Тур" та побудови ефективної корпоративної мережі, можливі напрямки рішення включають наступні стратегії та технології:

Модернізація мережевої інфраструктури:

Оновлення обладнання: Вибір сучасного мережевого обладнання, такого як маршрутизатори, комутатори та точки доступу від провідних виробників, як Cisco, для підвищення продуктивності та надійності мережі.

Впровадження віртуалізації: Використання віртуальних мереж та серверів для забезпечення гнучкості, масштабованості та спрощення управління ресурсами.

Захист даних та безпека мережі:

Розгортання брандмауерів та IDS/IPS систем: Встановлення комплексних систем безпеки для захисту мережі від зовнішніх та внутрішніх загроз.

Застосування шифрування: Імплементація сильних алгоритмів шифрування для забезпечення конфіденційності персональних даних клієнтів та корпоративної інформації.

Оптимізація мережевого трафіку:

Конфігурація QoS (Quality of Service): Налаштування політик якості обслуговування для забезпечення пріоритизації трафіку критичних додатків.

Моніторинг та управління пропускною спроможністю: Використання інструментів моніторингу для аналізу використання мережі та оптимізації розподілу ресурсів.

Підвищення доступності системи:

Розробка стратегії відновлення після збоїв: Впровадження рішень для резервного копіювання та відновлення даних для мінімізації часу простою в результаті збоїв.

Розгортання фейловер рішень: Використання технологій фейловер для забезпечення безперервності сервісу під час планових або непланових перерв.

Автоматизація процесів:

Використання інструментів автоматизації: Впровадження програмного забезпечення для автоматизації рутинних завдань управління мережею, таких як резервне копіювання конфігурацій, встановлення патчів та розгортання оновлень.

Широкосмуговий доступ до мережі:

Розгортання технологій Wi-Fi 6: Використання нового стандарту бездротового зв'язку для підвищення швидкості та ефективності бездротового підключення клієнтів до мережі.

Інтеграція хмарних сервісів:

Використання хмарних рішень для зберігання даних та виконання обчислень: Інтеграція з провідними хмарними платформами, такими як Amazon Web Services або Microsoft Azure, для забезпечення масштабованості та надійності зберігання даних та виконання обчислень.

Стратегія управління життєвим циклом мережевих пристроїв:

Впровадження системи управління конфігураціями: Створення централізованої системи для управління конфігураціями мережевих пристроїв, що дозволить ефективно впроваджувати зміни та відслідковувати їх стан.

Ці напрямки та технології спрямовані на створення надійної, безпечної та ефективної корпоративної мережі для "Альфа Тур", що допоможе оптимізувати бізнес-процеси та підвищити задоволеність клієнтів.

1.8 Обґрунтування вибраного напрямку інженерного рішення

Обґрунтування вибору напрямків інженерних рішень важливе для забезпечення ефективності та успішності проекту. Ось деякі обґрунтування для вибраних напрямків:

Модернізація мережевої інфраструктури:

Оновлення обладнання: Вибір сучасного обладнання від провідних виробників, таких як Cisco, дозволить підвищити продуктивність та надійність мережі за рахунок нових функцій та підтримки передових технологій.

Впровадження віртуалізації: Використання віртуальних мереж та серверів сприятиме гнучкості та масштабованості мережі, зниженню витрат на обслуговування та поліпшить загальну ефективність інфраструктури.

Захист даних та безпека мережі:

Розгортання брандмауерів та IDS/IPS систем: Це дозволить ефективно виявляти та блокувати загрози зовнішніх та внутрішніх атак, забезпечуючи високий рівень безпеки для корпоративних даних і даних клієнтів.

Застосування шифрування: Шифрування даних за допомогою сильних алгоритмів забезпечить конфіденційність інформації та допоможе в уникненні неправомірного доступу до цієї інформації.

Оптимізація мережевого трафіку:

Конфігурація QoS: Налаштування якості обслуговування дозволить забезпечити пріоритетний доступ для критичних додатків, забезпечуючи ефективне використання мережевих ресурсів.

Моніторинг та управління пропускною спроможністю: Це дозволить вчасно виявляти та вирішувати проблеми зі згущенням мережі та оптимізувати використання ресурсів.

Підвищення доступності системи:

Розробка стратегії відновлення після збоїв: Це зменшить час простою системи, що дозволить мінімізувати втрати часу та зберегти надійність обслуговування для клієнтів.

Розгортання фейловер рішень: Використання технологій фейловер допоможе забезпечити безперервну доступність сервісів навіть під час непланових перерв у роботі.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ АБО КІБЕРФІЗИЧНОЇ СИСТЕМИ

2.1 Технічні вимоги до комп'ютерної системи «Альфа тур»

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонуванню системи

2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації Системи

Корпоративна мережа компанії розділена на локальні мережі відповідно до загальної архітектури. Ця мережа включає 5 локальних систем

з метою задоволення певних вимог та переваг, а саме:

Зручне управління: Розділення мережі на локальні системи дозволяє мережевим адміністраторам ефективніше керувати мережею. Діагностика та вирішення невеликих проблем відбувається локально, що не призводить до зупинки всієї мережі.

Підвищена продуктивність: Швидкість передачі даних по локальним мережам значно вища, оскільки шлях пролягає через короткий відстань, а не через всю мережу.

Масштабованість: Легкість заміни та додавання пристроїв до локальної мережі сприяє зручній розширюваності та адаптації інфраструктури до змін у потребах компанії.

Забезпечення безпеки: Це дозволяє ефективно реалізувати більш точні системи безпеки, такі як брандмауери або VPN, що забезпечують захист мережі від потенційних загроз.

Додатково, існує підсистема, яка складається з IoT пристроїв. Ця підсистема в основному складається з систем поліпшення життя, таких як розумна система вентиляції та інше за завданням замовника.

Для відповідності вимогам, рекомендується використовувати Ip-блок-адресу для призначення підмережі. Потрібно розбити IP-адресу 172.24.8.0/21 на 5 підмереж враховуючи таку кількість вузлів 14, 92, 178, 118, 104 та за методом VLAN взято підмережі від більшої до меншої для LAN:

– LAN1 – 178 вузлів;

– LAN2 – 118 вузлів;

– LAN3 – 104 вузлів;

– LAN4 – 92 вузлів;

– LAN5 – 14 вузлів.

2.1.1.1.2 Вимоги до способів і засобів зв’язку між компонентами комп’ютерної системи

Надійність зв'язку:

Вимога до надійності зв'язку між компонентами системи передбачає мінімізацію можливості втрати зв'язку або перерв у його роботі. Це може включати в себе використання дублювання каналів зв'язку, резервних маршрутів та механізмів відновлення після збоїв.

Безпека зв'язку:

Вимога до безпеки зв'язку передбачає застосування шифрування трафіку між компонентами системи для запобігання несанкціонованому доступу до інформації. Це може включати в себе використання протоколів шифрування, таких як SSL/TLS, а також встановлення внутрішньої мережі забезпечення, такої як VPN.

Швидкість та пропускна здатність:

Вимога до швидкості та пропускної здатності зв'язку між компонентами системи передбачає забезпечення достатньої пропускної здатності для передачі даних без затримок та забезпечення задовільної реакції системи. Це може включати в себе використання високошвидкісних мережевих технологій, таких як Gigabit Ethernet або навіть 10-Gigabit Ethernet.

Гнучкість та масштабованість:

Вимога до гнучкості та масштабованості зв'язку між компонентами системи передбачає можливість легко розширювати або змінювати конфігурацію зв'язку відповідно до потреб бізнесу. Це може включати в себе використання технологій, які підтримують гнучкість мережевої інфраструктури, таких як віртуалізація мереж та SDN (Software-Defined Networking).

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

Сумісність та інтеграція з іншими системами:

Вимога до сумісності та інтеграції з іншими системами передбачає здатність нової системи взаємодіяти з існуючими системами в агентстві, такими як системи бронювання авіаквитків, готелів, та інших послуг. Це може включати розробку API або використання стандартних протоколів обміну даними для забезпечення сумісності.

Безпека взаємодії:

Вимога до безпеки взаємодії передбачає захист від несанкціонованого доступу та збереження конфіденційності даних, що передаються між системами. Це може включати в себе застосування механізмів автентифікації, авторизації та шифрування даних.

Ефективність взаємодії:

Вимога до ефективності взаємодії передбачає мінімізацію затримок та оптимізацію обміну даними між системами. Це може включати в себе використання оптимізованих протоколів передачі даних та кешування інформації для зменшення навантаження на мережу.

Надійність взаємодії:

Вимога до надійності взаємодії передбачає забезпечення стабільності та доступності обміну даними між системами. Це може включати в себе

використання механізмів резервування та відновлення після збоїв для забезпечення безперебійної роботи.

2.1.1.1.4 Вимоги до режимів функціонування системи

Основний режим роботи:

Система повинна забезпечувати безперервну доступність для користувачів та співробітників агентства в основний робочий час. В цьому режимі система повинна функціонувати з високою надійністю, швидкістю та ефективністю.

Режим обробки завдань в позаурочний час:

Система також повинна бути доступною для користувачів та співробітників агентства поза основним робочим часом для виконання важливих завдань або в разі необхідності негайного доступу до інформації.

Режим резервного копіювання та відновлення:

Система повинна мати можливість автоматичного або ручного резервного копіювання даних та налаштувань для забезпечення їх безпеки та можливості відновлення у разі виникнення непередбачуваних ситуацій, таких як видалення даних чи збій обладнання.

Режим відладки та тестування:

Для забезпечення стабільності та ефективності роботи системи, необхідно мати можливість в режимі відладки та тестування проводити відповідні випробування, виправляти помилки та вдосконалювати функціонал системи.

Режим аварійного відновлення:

Система повинна мати план аварійного відновлення, що передбачає можливість оперативного відновлення роботи системи після виникнення непередбачених ситуацій, таких як збої обладнання чи програмне забезпечення.

Режим оновлення та модернізації:

Система повинна мати можливість для виконання оновлень та модернізації, щоб відповідати змінюваним потребам бізнесу та технологічним вимогам.

2.1.1.1.5 Вимоги до діагностування системи

Моніторинг та відстеження стану системи:

Система повинна мати можливість постійного моніторингу та відстеження стану основних компонентів, таких як сервери, мережеве обладнання, бази даних тощо. Це дозволить оперативно виявляти можливі проблеми та уникати серйозних відмов.

Журналювання подій та помилок:

Система повинна автоматично журналювати всі події та помилки, які виникають в процесі роботи. Це допоможе адміністраторам швидко виявити та усунути проблеми, а також забезпечить необхідні дані для подальшого аналізу та вдосконалення системи.

Автоматичне сповіщення про проблеми:

Система повинна мати можливість автоматичного сповіщення адміністраторів про виявлені проблеми або потенційні загрози. Це дозволить оперативно реагувати на проблеми та зменшити час простою системи.

Аналіз та звітність:

Система повинна мати можливість проводити аналіз зібраних даних щодо стану системи та генерувати звіти для адміністраторів та керівництва. Це допоможе зрозуміти тенденції у роботі системи та приймати обгрунтовані рішення щодо покращення її ефективності та надійності.

Доступ до діагностичної інформації:

Адміністраторам системи повинен бути доступний широкий спектр діагностичної інформації щодо стану різних компонентів системи. Це може включати в себе інформацію про навантаження процесорів, використання пам'яті, стан мережевих підключень тощо.

2.1.1.1.6 Перспективи розвитку, модернізації системи

Розширення функціоналу:

Постійне оновлення та розширення функціональності системи для задоволення зростаючих потреб бізнесу та користувачів. Нові можливості

можуть включати покращену підтримку клієнтів, впровадження нових сервісів та збільшення зручності користування.

Вдосконалення безпеки:

Постійне підвищення рівня безпеки системи шляхом впровадження нових технологій шифрування, захисту від кібератак та посилення заходів контролю доступу.

Оптимізація продуктивності:

Постійне вдосконалення архітектури системи та оптимізація її продуктивності для забезпечення швидкої та ефективної роботи. Це може включати в себе оптимізацію баз даних, вдосконалення алгоритмів обробки даних та розробку швидших та ефективніших інтерфейсів.

Використання новітніх технологій:

Постійне впровадження новітніх технологій, таких як штучний інтелект, аналіз даних, блокчейн та Інтернет речей (IoT), для поліпшення якості обслуговування, збільшення ефективності та забезпечення конкурентоспроможності.

Інтеграція з внутрішніми та зовнішніми системами:

Постійна робота над інтеграцією з іншими внутрішніми та зовнішніми системами для поліпшення обміну даними та співпраці. Це може включати в себе інтеграцію з системами бронювання, платіжними системами та іншими партнерами агентства.

Розширення мережевої інфраструктури:

Постійне оновлення та розширення мережевої інфраструктури для забезпечення швидкого та надійного доступу до системи для всіх користувачів та співробітників агентства.

2.1.1.2 Вимоги до показників призначення

Ефективність обробки даних:

Система повинна забезпечувати швидку та ефективну обробку та аналіз великих обсягів даних про клієнтів, готелі, тури, платежі та інші важливі дані для забезпечення оперативного прийняття рішень та виконання запитів користувачів.

Надійність та стабільність роботи:

Система повинна працювати безперервно та надійно, мінімізуючи можливість виникнення збоїв чи відмов у роботі. Недостатність таких випадків дозволить забезпечити неперервну доступність для користувачів.

Легкість використання:

Система повинна мати інтуїтивно зрозумілий і простий інтерфейс, що дозволить користувачам легко здійснювати бронювання, переглядати інформацію та взаємодіяти з сервісами агентства без значних зусиль або додаткової підготовки.

Забезпечення конфіденційності та безпеки даних:

Система повинна гарантувати захист особистої та фінансової інформації клієнтів, а також конфіденційності корпоративної інформації агентства. Це включає в себе застосування сучасних методів шифрування, захисту від несанкціонованого доступу та регулярну перевірку на вразливості.

Масштабованість та гнучкість:

Система повинна бути легко масштабованою для відповіді на зростання обсягів роботи агентства та змін потреб бізнесу. Крім того, вона повинна бути гнучкою для адаптації до змін вимог та регуляцій у сфері туризму.

2.1.1.3 Вимоги до патентної чистоти

Оскільки «Альфа тур» знаходиться в Україні, патентна чистота у цій країні є важливою для забезпечення відповідності законодавству та уникнення можливих правових проблем. Обладнання та програмне забезпечення, яке використовується у комп'ютерній системі, повинно відповідати вимогам патентного законодавства. Це вимагає використання авторизованого програмного забезпечення, проведення детальних аналізів елементів системи для

ідентифікації можливих патентних ризиків, залучення юридичних консультантів, а також ведення точної документації про проектування системних компонентів, щоб мати надійні докази відсутності порушень патентів у разі юридичних спорів.

2.1.1.4 Додаткові вимоги

Вимоги до особливих умов експлуатації:

Врахування особливостей робочого середовища, таких як температурні умови, вологість, пил, а також необхідність забезпечення захисту від несприятливих зовнішніх впливів.

Вимоги до активного обладнання:

Уточнення функціональних вимог до активного мережевого обладнання, включаючи необхідну кількість портів, їх розташування, технічні характеристики та можливості масштабування.

Вимоги до кабель-каналів та розеток:

Специфікація типу, розміру та розташування кабельних каналів, інформаційних та електричних розеток, а також вимоги до їх варіантів розміщення з урахуванням потреб системи.

Вимоги до комунікаційного обладнання:

Визначення місць розташування комунікаційного обладнання у приміщенні, типів шаф, підводу кабельних трас, а також вимоги до розміщення обладнання усередині шафи.

Вимоги до однорідності:

Стандартизація типів кабелів, роз'ємів, магістралей та інших елементів мережевої інфраструктури для забезпечення їхньої сумісності та легкості обслуговування.

Вимоги до резервування:

Специфікація вимог до резервування системи для забезпечення неперервності роботи та захисту від можливих відмов.

2.1.2 Вимоги функцій, виконуваним системою

1) Підсистема управління ресурсами

Функції та задачі: Управління розкладами та наявністю готельних номерів, авіаквитків. Оптимізація використання ресурсів.

Часовий регламент та якість реалізації: Забезпечення постійного оновлення даних про ресурси. Мінімальний час відгуку на зміни в наявності – до 5 секунд. Висока точність представлення вихідної інформації.

2) Підсистема безпеки

Функції та задачі: Забезпечення захисту даних та систем від несанкціонованого доступу. Моніторинг та відповідь на загрози безпеки.

Часовий регламент та якість реалізації: Неперервний моніторинг системи на наявність потенційних загроз. Швидкість реагування на інциденти безпеки – не більше 10 хвилин з моменту виявлення.

3) Підсистема управління клієнтськими даними

Функції та задачі: Збір та збереження даних клієнтів. Управління історією бронювань. Підтримка персоналізованого маркетингу.

Часовий регламент та якість реалізації: Всі дані повинні оброблятися та зберігатися в реальному часі. Відповідь на запити користувачів – до 1 секунди. Забезпечення конфіденційності та цілісності даних відповідно до GDPR.

2.1.3 Вимоги до видів забезпечення комп’ютерної системи

2.1.3.1 Вимоги до математичного забезпечення

Вимоги не передбачаються.

2.1.3.2 Вимоги до інформаційного забезпечення

Конфіденційність: Система інформаційного забезпечення має використовувати надійні методи захисту конфіденційності даних.

Масштабованість: Система має бути гнучкою та готовою до розширення в разі зростання потреб.

Доступність: Забезпечення безперебійної роботи системи цілодобово.

Резервне копіювання: Гарантування наявності резервних копій інформації у випадку відмови сервера.

2.1.3.3 Вимоги до лінгвистичного забезпечення

Для розробки системи використовуються сучасні мови програмування високого рівня, які забезпечують надійність, масштабованість та легкість підтримки. На back-end можуть використовуватися такі мови як Java, C#, або Python, в той час як для front-end ідеально підходять JavaScript з фреймворками React або Angular. Ці технології дозволяють ефективно впоратися з вимогами сучасного програмування та забезпечують стабільність додатків.

Система підтримує багатомовні інтерфейси, що включають англійську, українську, російську, іспанську та інші мови, забезпечуючи доступність і зручність для інтернаціональної аудиторії. Це розширює досяжність системи та сприяє кращій взаємодії з користувачами з різних країн.

Кодування та декодування даних виконується за допомогою стандартів, як UTF-8 для текстових даних, що гарантує коректне відображення мовних символів, а також використання стандартних криптографічних бібліотек для захисту чутливих даних, забезпечуючи високий рівень безпеки інформації.

Для маніпулювання даними використовується SQL для реляційних баз даних і спеціалізовані мови запитів для NoSQL баз, що дозволяє ефективно управляти великими обсягами даних. Система також використовує Unified Modeling Language (UML) для візуалізації та документування архітектур і бізнес-процесів, що забезпечує чіткість розуміння структури системи і сприяє ефективній комунікації між розробниками та іншими зацікавленими сторонами.

2.1.3.4 Вимоги до технічного забезпечення

Для забезпечення високої продуктивності, кожен робочий стан повинен бути обладнаний комп'ютером, що відповідає наступним вимогам: процесор має

мати щонайменше чотири ядра і тактову частоту не менше 2 ГГц. Також необхідно мати щонайменше 8 ГБ оперативної пам'яті, дискретний відеоадаптер, внутрішню пам'ять об'ємом не менше 256 ГБ, а також встановлену операційну систему Windows 11, щоб забезпечити сумісність та ефективність виконання програм.

Що стосується серверів, вони мають відповідати спеціальним вимогам для оптимальної ефективності і надійності. Ключові характеристики включають процесор із тактовою частотою не менше 1,5 ГГц та мінімальний об’єм оперативної пам’яті 16 ГБ. Ці вимоги допомагають забезпечити швидку обробку даних та стабільність серверного обладнання під час виконання важливих завдань.

2.1.3.5 Вимоги до організаційного забезпечення

Працівники ІТ-відділу повинні мати доступ до технічного приміщення за допомогою методів аутентифікації наприклад ключ-картками..

2.1.3.6 Вимоги до методичного забезпечення

Внутрішні стандарти та політики:

– Політика безпеки інформації.

– Політика обробки та зберігання даних.

– Політика конфіденційності.

– Політика доступу до системи та її компонентів.

Міжнародні та національні стандарти:

– ISO/IEC 27001 - Міжнародний стандарт з управління інформаційною безпекою.

– GDPR - Загальний регламент захисту даних (для обробки даних громадян ЄС).

– PCI DSS - Стандарт безпеки даних для індустрії платіжних карток (якщо компанія здійснює транзакції платіжними картками).

Стандарти звітності та документування:

– Стандарти для складання технічних документів і звітів.

– Методики ведення документації проектів, включно з вимогами до форматування та представлення.

Методики управління проектами та розробки:

– Agile, Scrum, або Kanban для управління розробкою ПЗ.

– ITIL для управління IT-послугами.

– COBIT для управління інформацією та технологіями.

Методики тестування та якості:

– Стандарти та методики забезпечення якості програмного забезпечення.

– Методики тестування програмного забезпечення, включаючи модульне, інтеграційне, системне та приймальне тестування.

Вимоги до дотримання та виконання нормативів:

Регулярний перегляд та оновлення документації:

– Забезпечення актуальності всієї нормативно-технічної документації шляхом періодичного перегляду та оновлення згідно з останніми змінами в законодавстві, технологіях та бізнес-процесах.

Навчання персоналу:

– Проведення регулярних тренінгів для співробітників з питань дотримання політик безпеки, обробки даних та інших критично важливих стандартів.

Забезпечення відповідності до стандартів:

– Використання інструментів аудиту та моніторингу для перевірки дотримання стандартів та політик у реальному часі.

2.2 Розробка апаратної частини комп’ютерної системи

2.2.1 Розробка загальної архітектури мережі підприємства

Загальна архітектура мережі підприємства «Альфа Тур» включає різні локальні мережі (LAN), з'єднані через маршрутизатори, що дозволяє

забезпечувати розподілені, але інтегровані мережеві сервіси. Розглянемо ключові аспекти архітектури:

1. Сегментація мережі та VLAN

На схемі виділені кілька VLAN, які використовуються для сегментації мережі:

VLAN 10, 20, 30 на Switch2 і Switch3 дозволяють ізолювати трафік між різними відділами або групами користувачів, забезпечуючи поліпшену безпеку та зменшення мережевих заторів.

2. Маршрутизація між VLAN

Маршрутизатори (Router1, Router2, Router3, і Router4) управляють маршрутизацією між VLAN та різними LAN. Це важливо для контролю доступу до ресурсів та забезпечення безпеки мережі.

3. Централізовані та розподілені сервери

Сервери (HTTP, DNS, TFTP) розміщені в різних сегментах мережі для надання специфічних служб:

HTTP сервер в LAN 2 для веб-сервісів.

DNS сервер у LAN 5 для розв'язання імен доменів.

TFTP сервер у LAN 3 для зберігання та передачі файлів конфігурації обладнання.

4. Безпека мережі

Поєднання фізичної та логічної топології з'єднань забезпечує стратегічний розподіл трафіку та безпеку.

5. Маршрутизація зовнішніх з'єднань

Зовнішнє з'єднання через Router3 на 209.165.202.0/28 забезпечує доступ до інтернету або іншим зовнішнім мережам, важливий для забезпечення доступу до глобальних ресурсів і сервісів.

6. Резервування та надійність

Використання багатошляхової маршрутизації між Router1, Router2 та Router4 для забезпечення відмовостійкості та збалансування навантаження.

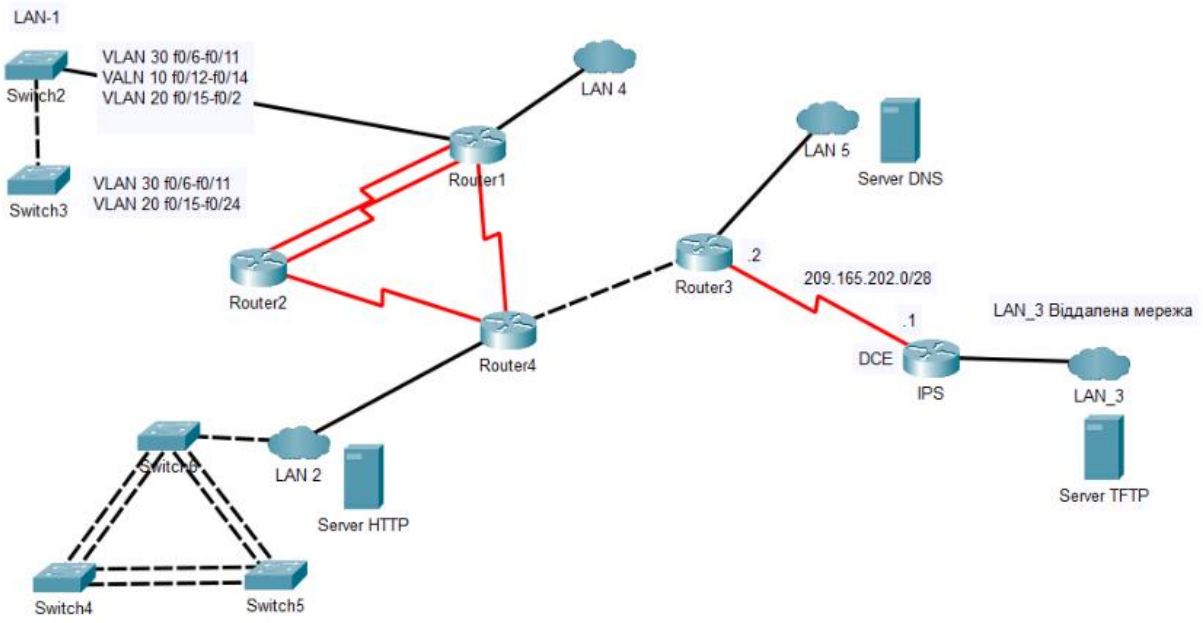

Рисунок 2.1 – Схема загальної архітектури мережі

2.2.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

Для забезпечення ефективної роботи комп'ютерної системи "Альфа Тур", структурна схема технічних засобів повинна включати наступні ключові компоненти:

Центральні сервери:

– сервери додатків для розміщення веб-додатків і спеціалізованого ПЗ (наприклад, CRM, ERP);

– сервери баз даних для забезпечення зберігання і швидкого доступу до даних;

– файлові сервери для зберігання і розподілу корпоративних файлів і резервних копій.

Мережеве обладнання:

– маршрутизатори для з'єднання внутрішніх і зовнішніх мереж;

– комутатори для розподілу трафіку внутрішньої мережі;

– брандмауери і IPS (Intrusion Prevention Systems) для забезпечення безпеки мережі.

Клієнтські пристрої:

– персональні комп'ютери та мобільні пристрої для доступу співробітників до корпоративних ресурсів.

Системи забезпечення безперервності бізнесу:

– джерела безперервного живлення (UPS);

– системи резервного копіювання та відновлення даних.

Системи моніторингу та управління мережею:

– системи моніторингу мережі для відстеження стану мережевого обладнання та трафіку;

– системи управління мережею для конфігурації та управління мережевими параметрами.

Обґрунтування вибору

Централізація серверів:

– централізація критичних серверів (наприклад, серверів баз даних і додатків) забезпечує легший контроль, кращу інтеграцію даних і ефективніше управління ресурсами.

Масштабованість і гнучкість мережевого обладнання:

– використання модульних маршрутизаторів і комутаторів дозволяє легко розширювати мережу у відповідності з ростом компанії.

Забезпечення безпеки:

– впровадження сучасних брандмауерів і IPS гарантує захист від зовнішніх та внутрішніх загроз, що є критично важливим для захисту конфіденційної інформації компанії.

Підвищення надійності:

– використання UPS і систем резервного копіювання забезпечує безперервність роботи критично важливих систем і швидке відновлення даних після можливих збоїв.

Ефективне управління мережею:

– системи моніторингу та управління мережею забезпечують можливість постійно відстежувати стан мережі та оперативно реагувати на проблеми, підвищуючи загальну продуктивність і стабільність системи.

Така структурна схема дозволяє компанії максимально ефективно використовувати технологічні ресурси, підвищувати продуктивність роботи співробітників, знижувати ризики втрати даних та забезпечувати високий рівень задоволеності клієнтів завдяки надійності та доступності інформаційних ресурсів.

2.2.3 Розробка специфікації апаратних засобів комп'ютерної системи

Вибір апаратної частини корпоративної мережі є важливим кроком для забезпечення надійності та продуктивності системи. У якості маршрутизатора було обрано Cisco 1808. Ця модель має високу продуктивність та розширені можливості для обробки даних мережі. Технічні характеристики моделі наступні: має два WAN портів, дев'ять портів під підключення комутаторів швидкістю до 1 Gbps(9x10/1000) та мережевий екран швидкістю до 5Gbps. Маршрутизатор Cisco ASR1001-X відповідає потребам компанії для забезпечення стабільного та захищеного зв'язку між мережевими пристроями.

Для подальшої побудови локальної мережі, обрано комутатор Cisco Nexus 2960X-24TS-L. Даний комутатор має: 24 порти Fast Ethernet (10/100 Mbps) та два порти зі швидкістю до 1 Gbps(9x10/1000). Комутатор підтримує такі функції як VLAN, Quality of Service (QoS), Spanning Tree Protocol (STP), Access Control Lists (ACLs), що дозволяють налаштовувати та керувати роботою комутатора, також він забезпечує швидку передачу даних, надає широкі можливості управління, безпеки та масштабованості, відповідає потребам компанії для забезпечення надійного з'єднання робочих станцій, серверів та інших мережевих пристроїв.

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість
1	**2**	**3**	**4**	**5**
1	Cisco ASR1001-X System, Crypto, 4 built-in GE, Dual P/S, 20Gbit, 6x1000Base-X (SFP), 2x10G SFP+ інтегровані RP, SIP та ESP, 1xNIM, 1xSPA, RAM 8Gb, 2xAC	Cisco 1808	Од.	5
2	Комутатор 24 x Ethernet 10/100/1000 Мбіт/сек, RIP v1, RIP v2, OSPF, USB-порт, LAN Base, 4 SFP слоти	Cisco Nexus	Од.	23
4	Сервер: 2 шт x Intel Xeon E5-2650L v2 (1.70-2.10 GHz), 8 GB DDR3, 2x порта 1 Gb Ethernet	Cisco UCS C220 M3 LFF	Од.	3
5	Комп'ютер: AMD Ryzen 3 3400G (3.9 — 4.4 ГГц), 8 ГБ DDR4, 256 Гб SSD, AMD Radeon Vega 5, Windows 11 Pro	AMD Ryzen	Од.	506

2.2.4 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

В підмережі LAN1 встановлений комутатор Cisco2960, що об'єднує 178 ПК працівників. Вихідний трафік з комутатора надсилається до роутера в лінію з пропускною здатністю, що становить 1000 Мбіт/с.

Для того, щоб комутатор не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку μ=143 (кадрів/с), а середня довжина повідомлення – 1150 байт.

Теоретично припустимо, що всі користувачі найбільшої підмережі DLS одночасно використовують мережу. В такому разі, пропускна здатність на рівні доступу буде дорівнювати:

$$P_{р.р.} = \mu * L_{пов} * N * 8 = 143 * 1150 * 178 * 8 = 23.4 \text{ Мбіт/с} \quad (2.1)$$

де $L_{пов}$ – середня довжина повідомлення;

N – кількість вузлів в мережі.

Отриманий результат не перевищуватиме заданих параметрів мережі по вихідному каналу, отже перенавантажень не трапиться.

Комутатор також передає трафік до маршрутизатора зі швидкістю 1000 Мбіт/с. Отже, загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих} = 10^9 / (1150 * 8) = 108\,696 \text{ пакетів/с} \quad (2.2)$$

Оскільки в середньому, кожне джерело виробляє 143 пакетів/с, то маршрутизатор обмежений кількістю приєднань, яку ми можемо дізнатись наступним чином:

$$N = \mu_{вих} / \mu = 108\,696/ 143 \approx 760 \text{ джерела} \quad (2.3)$$

Ця кількість задовольняє кількості вузлів у найбільшій нашій локальній мережі, до якої входить 178 ПК.

Кожен з 178 ПК посилає потік заявок з інтенсивністю у 143 кадрів/с. Звідси, можем розрахувати інтенсивність вихідного трафіку:

$$\lambda = N * \mu = 178*143 = 25454 \text{ пакетів/с.} \quad (2.4)$$

Коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu вих} = \frac{25454}{108696} = 0{,}23 \quad (2.5)$$

Коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho} = \frac{0{,}23}{1-0{,}23} = 0{,}29 \quad (2.6)$$

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

$$T = \frac{1}{(\mu-\lambda)} = \frac{1}{(108696 - 25454)} = 12{,}01 \text{ мкс} \quad (2.7)$$

Середня довжина черги:

$$L_{чер} = \frac{\rho^2}{1-\rho} = \frac{0{,}23^2}{1-0.23} = 0.068 \quad (2.8)$$

Середній час перебування пакета у черзі:

$$T_{оч} = \frac{Lчер}{\lambda} = \frac{0{,}068}{254540} = 0{,}27 \text{ мкс} \quad (2.9)$$

Це значення задовольняє вимогам до затримки в ЛМ.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Проектування логічної топології мережі

Проектування логічної топології мережі є важливим етапом у створенні комп'ютерної інфраструктури для туристичної компанії «Альфа тур». Логічна топологія визначає, як дані будуть передаватися між різними вузлами мережі, незалежно від їх фізичного розташування.

Один з підходів до проектування логічної топології - це використання звичайних структур мережі, таких як зірка, шина, кільце або дерево. У випадку туристичної компанії "Альфа тур" зазвичай оптимальним вибором є зіркова топологія, де всі комп'ютери та пристрої підключені до центрального комутатора чи маршрутизатора. Це забезпечує простоту управління та підтримки, а також підвищує надійність мережі, оскільки випадок відмови одного пристрою не призведе до відмови всієї мережі.

Крім того, важливо враховувати потреби компанії у високій пропускній здатності та надійності мережі, особливо при передачі великого обсягу даних, таких як бронювання квитків або готелів. Тому рекомендується використання швидкісних комутаторів та встановлення резервних з'єднань для забезпечення надійності.

Крім того, важливо враховувати засоби забезпечення безпеки, такі як налаштування віртуальної приватної мережі (VPN) для захисту конфіденційності даних під час віддаленого доступу до корпоративної мережі.

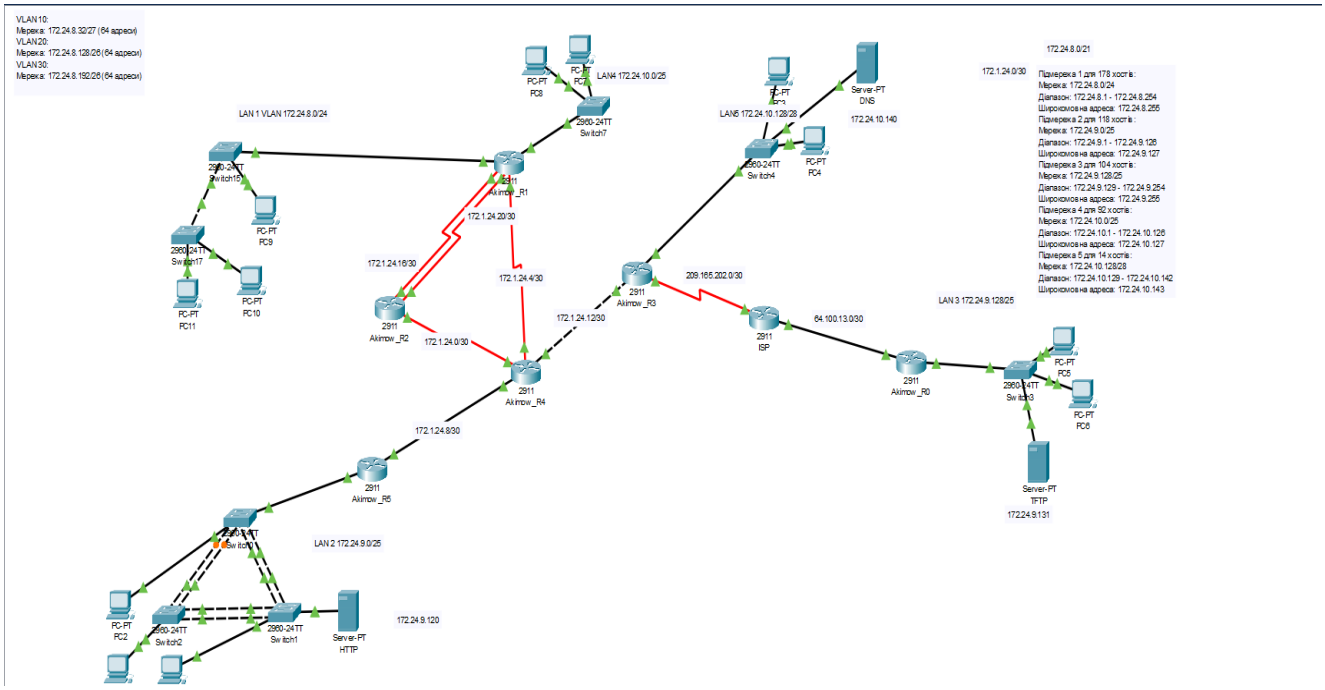

Рисунок 3.1 – Кінцева топологія мережі

3.2 Вибір та опис мережного обладнання

У рамках проектування мережі компанії необхідно вибрати обладнання, що забезпечить надійність, високу пропускну здатність та можливість масштабування мережі. Нижче описано основне мережеве обладнання, яке було вибрано для імплементації мережевої інфраструктури.

– Маршрутизатор: Cisco ASR1001-X

Технічна характеристика:

Інтегровані інтерфейси: 4 вбудованих GE порти, 6 портів 1000Base-X (SFP), 2 порти 10G SFP+.

Маршрутизація та обробка: Інтегровані Routing Processor (RP), SPA Interface Processor (SIP) та Embedded Services Processor (ESP).

Пропускна здатність: до 20 Гбіт/с.

Модульність: 1 слот для Network Interface Modules (NIM) та 1 слот для Shared Port Adapters (SPA).

Захист: Система підтримує криптографічні механізми, Dual Power Supply (P/S) для збільшення надійності.

Пам'ять: 8 ГБ оперативної пам'яті.

Живлення: 2 x AC.

– Комутатор: Cisco Nexus LAN Base

Технічна характеристика:

Порти: 24 x Ethernet 10/100/1000 Мбіт/сек.

Маршрутизація: Підтримка RIP v1, RIP v2 та OSPF.

Додаткові інтерфейси: 4 SFP слоти для підключення волоконно-оптичних ліній.

Функціональні можливості: USB-порт для локального управління та оновлення програмного забезпечення.

Керування: Вбудоване програмне забезпечення LAN Base забезпечує базові можливості керування мережею.

– Сервер: Cisco UCS C220 M3 LFF

Технічна характеристика:

Процесори: 2 шт x Intel Xeon E5-2650L v2 (1.70-2.10 GHz).

Оперативна пам'ять: 8 GB DDR3.

Мережеві інтерфейси: 2x порти 1 Gb Ethernet для забезпечення мережевих з'єднань та управління.

Розширення: Сервер має можливість для додавання жорстких дисків та додаткових мережевих карт, що дозволяє збільшити об'єм зберігання та пропускну здатність.

Це обладнання було обране з метою забезпечення високої продуктивності, надійності та гнучкості мережевої інфраструктури. Модульність та можливість розширення дозволяють компанії з легкістю масштабувати мережу у відповідь на змінюючи бізнес-потреби.

3.3 Розрахунок схеми адресації корпоративної мережі

Для кожної підмережі визначаємо необхідну маску:

– Для 178 хостів: Мінімально необхідна маска = $\log_2(178+2)$ =8 біт (178 хостів + 2 адреси для мережі і широкомовної розсилки). Таким чином, необхідна маска /24 (255.255.255.0).

– Для 118 хостів: Мінімально необхідна маска = $\log_2(118+2)$ =7 біт. Таким чином, необхідна маска /25 (255.255.255.128).

– Для 104 хостів: Мінімально необхідна маска = $\log_2(104+2)$ =7 біт. Таким чином, необхідна маска /25 (255.255.255.128).

– Для 92 хостів: Мінімально необхідна маска = $\log_2(92+2)$ =7 біт. Таким чином, необхідна маска /25 (255.255.255.128).

– Для 14 хостів: Мінімально необхідна маска = $\log_2(14+2)$=4 біт. Таким чином, необхідна маска /28 (255.255.255.240).

На основі визначених масок і початкової мережі 172.24.8.0/21, розподіляємо адресний простір:

1) Підмережа для 178 хостів:

– Мережа: 172.24.8.0/24

– Діапазон: 172.24.8.1 - 172.24.8.254

– Широкомовна адреса: 172.24.8.255

2) Підмережа для 118 хостів:

– Мережа: 172.24.9.0/25

– Діапазон: 172.24.9.1 - 172.24.9.126

– Широкомовна адреса: 172.24.9.127

3) Підмережа для 104 хостів:

– Мережа: 172.24.9.128/25

– Діапазон: 172.24.9.129 - 172.24.9.254

– Широкомовна адреса: 172.24.9.255

4) Підмережа для 92 хостів:

– Мережа: 172.24.10.0/25

– Діапазон: 172.24.10.1 - 172.24.10.126

– Широкомовна адреса: 172.24.10.127

5) Підмережа для 14 хостів:

– Мережа: 172.24.10.128/28

– Діапазон: 172.24.10.129 - 172.24.10.142

– Широкомовна адреса: 172.24.10.143

Таблиця 3.1 – Схема адресації мережі

Назва підмережі	Необхідна кіл-ть вузлів	Адреса підмережі	Маска Підмережі у Десятковому форматі	Діапазон допустимих IP-адрес вузлів
LAN 1	178	172.24.8.0	/24	172.24.8.1 - 172.24.8.254
LAN 2	118	172.24.9.0	/25	172.24.9.1 - 172.24.9.126
LAN 3	104	172.24.9.128	/25	172.24.9.129 - 172.24.9.254
LAN 4	92	172.24.10.0	/25	172.24.10.1 - 172.24.10.126
LAN 5	14	172.24.10.128	/28	172.24.10.129-172.24.10.142

У таблиці 3.2 наведено схему адресації маршрутизаторів мережі.

Таблиця 3.2 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска
Akimow_R3	Se0/0/0	209.165.202.0	255.255.255.252
	Gig0/0	172.1.24.13	255.255.255.252
	Gig0/1	172.24.10.128	255.255.255.240
Akimow_R1	Gig0/1	172.24.8.1	255.255.255.255
	Gig0/0	172.24.10.1	255.255.255.128
	Se0/0/0	172.1.24.17	255.255.255.252
	Se0/0/1	172.1.24.21	255.255.255.252
	Se0/1/0	172.1.24.5	255.255.255.252
Akimow _R2	Se0/0/1	172.1.24.18	255.255.255.252
	Se0/0/0	172.1.24.22	255.255.255.252
	Se0/1/0	172.1.24.1	255.255.255.252

Продовження таблиці 3.2

Akimow _R4	Se0/0/0	172.1.24.2	255.255.255.252
	Se0/0/1	172.1.24.6	255.255.255.252
	Gig0/0	172.1.24.14	255.255.255.252
	Gig0/1	172.1.24.9	255.255.255. 252
Akimow _R5	Gig0/0	172.1.24.10	255.255.255. 252
	Gig0/1	172.24.9.1	255.255.255.128
Akimow _R0	Gig0/0	64.100.13.1	255.255.255.128
	Gig0/1	172.24.9.129	255.255.255.252

3.4 Базове налаштування конфігурації пристроїв

Базове налаштування конфігурації пристроїв на прикладі Akimow_R3:

hostname Akimow_R3// призначення назви пристрою

line console 0 // вхід в конфігураційний режим лінії консолі

password cisco // призначення паролю до консолі

login // вимикання анонімного доступу

line vty 0 15 // вхід в конфігураційний режим лінії VTY

password cisco // призначення паролю до лінії VTY

login // вимикання анонімного доступу

enable secret class // встановлення зашифрованого паролю для привілейного режиму

service password-encryption // шифрування паролів

banner motd #Akimow_R3# // налаштування банера MOTD

line vty 0 15 // вхід в конфігураційний режим лінії VTY

transport input ssh // назначення використання протоколу SSH

login local // налаштування локальної аутентифікації

username 12321ck_Akimow password admincisco // призначення імені користувача та паролю

ip domain-name Akimow_R3 // налаштування імені домена

crypto key generate rsa // створення ключа шфируваня

1024 // вибір довжини ключа шифрування

У мережі LAN_2 активно використовується технологія Etherchannel Завдяки об'єднанню портів, мережа стає менш чутливою до збоїв окремих каналів, оскільки втрата одного з фізичних з'єднань не призводить до повного переривання зв'язку, що є критично важливим для підтримки безперебійної роботи виробничих та комерційних систем.

Налаштування Etherchannel на прикладі комутатора:

interface range fa0/1-2 // вибір інтерфейсів

channel-group 1 mode active // налаштування режиму портової групи

interface port-channel 1 // вибір інтерфейсу портової групи

switchport mode trunk // налаштування портової групи в режим транку

switchport trunk allowed vlan all // встановлення всіх VLAN як дозволених для проходженя даних через транковий порт

interface range fa0/3-4

channel-group 2 mode active

interface port-channel 2

switchport mode trunk

switchport trunk allowed vlan all

3.5 Захист інформації в комп’ютерній системі технологію AAA

У якості захисту від несанцкіонованого доступу обрано технологію AAA це фреймворк, призначений для управління доступом до мережевих ресурсів, забезпечення авторизації користувачів та їх ідентифікації. Однією з ключових складових системи AAA є сервер RADIUS, який виконує централізовану аутентифікацію та авторизацію для користувачів, що намагаються здійснити доступ до мережі через такі пристрої, як комутатори чи маршрутизатори.

В рамках нашої мережевої інфраструктури, ми налаштовуємо підтримку служби AAA на всіх маршрутизаторах, використовуючи як приклад маршрутизатор Akimow_R1:

```
aaa new-model
radius server host
address ipv4 172.24.9.120 auth-port 1645
key radius123
aaa authentication login console group radius local
line console 0
login authentication console
aaa authentication login default local
username Akimow password admin123
line vty 0 15
login authentication default
```

3.6 Налаштування мереж VLAN

Для ефективного управління мережею та розподілу трафіку між різними відділами чи службами компанії необхідно створити добре структуровані VLAN та налаштувати маршрутизацію між ними. Застосування техніки Variable Length Subnet Masking (VLSM) дозволяє оптимально використовувати адресний простір та забезпечувати гнучкість мережі. Цей метод дає можливість різним підмережам мати різну довжину маски, що ефективно задовольняє мережеві вимоги різних підсистем.

Основою для створення VLAN є підмережа 172.24.8.0/24, яка розподіляється між п'ятьма VLAN. Перші дві підмережі, призначені для керування (VLAN 99 і 100), мають маску /28, що дозволяє підтримувати до 14 хостів у кожній.

– VLAN 99:

Мережа: 172.24.8.0/28

Діапазон хостів: 172.24.8.1 - 172.24.8.14

Широкомовна адреса: 172.24.8.15

– VLAN 100:

Мережа: 172.24.8.16/28

Діапазон хостів: 172.24.8.17 - 172.24.8.30

Широкомовна адреса: 172.24.8.31

– VLAN 10:

Мережа: 172.24.8.32/26

Діапазон хостів: 172.24.8.33 - 172.24.8.94

Широкомовна адреса: 172.24.8.95

– VLAN 20:

Мережа: 172.24.8.96/26

Діапазон хостів: 172.24.8.97 - 172.24.8.158

Широкомовна адреса: 172.24.8.159

– VLAN 30:

Мережа: 172.24.8.160/26

Діапазон хостів: 172.24.8.161 - 172.24.8.222

Широкомовна адреса: 172.24.8.223

У таблиці 3.3 наведена адресація під інтерфейсів мережі.

Таблиця 3.3 – Адресація мереж VLAN

Назва	Мережева адреса	/маска	Маска мережі	Діапазон адрес
VLAN10	172.24.8.32	/26	255.255.255.192	172.24.8.33 - 172.24.8.94
VLAN20	172.24.8.96	/26	255.255.255.192	172.24.8.97 - 172.24.8.158
VLAN30	172.24.8.160	/26	255.255.255.192	172.24.8.161 - 172.24.8.222
VLAN99	172.24.8.0	/28	255.255.255.240	172.24.8.1 - 172.24.8.14
VLAN100	172.24.8.16	/28	255.255.255.240	172.24.8.17 - 172.24.8.30

Налаштування VLAN на прикладі комутатора:

int range fa0/6-11 // вибір портів

switchport mode access // налаштування портів

switchport access vlan 42 // присвоювання портам влану

int range fa0/12-14

switchport mode access

switchport access vlan 22

int range fa0/15-24

switchport mode access

switchport access vlan 32

int range fa0/1-5

switchport mode trunk // налаштування портів в режим транку

switchport trunk native vlan 100 // налаштування власної мережі на транковому порті

Налаштовуємо підінтерфейси на маршрутизаторі Akimow_R1, що будуть виступати в ролі шлюзу для вказаних VLAN:

interface GigabitEthernet0/1.10

encapsulation dot1Q 10

ip address 172.24.8.33 255.255.255.224

interface GigabitEthernet0/1.20

encapsulation dot1Q 20

ip address 172.24.8.129 255.255.255.192

interface GigabitEthernet0/1.30

encapsulation dot1Q 30

ip address 172.24.8.193 255.255.255.192

interface GigabitEthernet0/1.99

encapsulation dot1Q 99

ip address 172.24.8.1 255.255.255.240

Для автоматичного призначення IP-адрес вузлам в різних VLAN буде використовуватись протокол DHCP. Налаштування DHCP на маршрутизаторі Akimow_R1, який буде виступати в ролі DHCP-сервера:

```
ip dhcp pool LAN1-VLAN20
network 172.24.8.128 255.255.255.192
default-router 172.24.8.129
dns-server 172.24.10.140
ip dhcp pool LAN1-VLAN10
network 172.24.8.32 255.255.255.224
default-router 172.24.8.33
dns-server 172.24.10.140
ip dhcp pool LAN1-VLAN30
network 172.24.8.192 255.255.255.192
default-router 172.24.8.193
dns-server 172.24.10.140
```

3.7 Налаштування способу маршрутизації

Налаштування OSPF допомагає управляти маршрутизацією в складних мережевих структурах, забезпечуючи, що дані ефективно розподіляються між різними вузлами мережі, з мінімальними затримками і втратами. А також невідчепною частиною налаштування маршрутизації є налаштування маршрутизації

У мережевих налаштуваннях існують два основних методи маршрутизації: статична і динамічна. При статичній маршрутизації адміністратор вручну встановлює маршрути, що є часом затратним та менш гнучким варіантом. З іншого боку, динамічна маршрутизація дозволяє автоматично оновлювати маршрути, роблячи мережу більш адаптивною і легкою в управлінні.

Щодо розподілу IP-адрес у мережі, використовується протокол DHCP, який автоматично призначає IP-адреси мережевим пристроям. Це значно спрощує

процес конфігурації мережі та управління нею, оскільки зменшує кількість ручних налаштувань і покращує зручність використання.

Налаштування DHCP на прикладі маршрутизатора Akimow_R3:

ip dhcp excluded-address 172.24.10.129 172.24.10.131

ip dhcp excluded-address 172.24.10.140// виключення вказаних адрес з dhcp пулів

ip dhcp pool LAN-4 // створення та вказання адреси dhcp пулу

network 172.24.10.128 255.255.255.240 // вказання IP-адреси мережі

default-router 172.24.10.129// вказання IP-адреси шлюзу

dns-server 172.24.10.140// вказання IP-адреси dns сервера

У проекті ми застосуємо протокол OSPF для динамічної маршрутизації, який є одним із найбільш використовуваних у сучасних мережевих середовищах. OSPF використовує алгоритм SPF для визначення найкоротших можливих маршрутів, що значно підвищує швидкість роботи мережі. Цей протокол відомий своєю здатністю масштабування, високим рівнем безпеки, підтримкою VLSM та гарною сумісністю з мережевим обладнанням різних виробників.

Налаштування протоколу OSPF на прикладі маршрутизатораAkimow_R3:

router ospf 1

log-adjacency-changes

passive-interface default

no passive-interface GigabitEthernet0/0

no passive-interface GigabitEthernet0/1

no passive-interface Serial0/0/0

auto-cost reference-bandwidth 1000

network 172.1.24.12 0.0.0.3 area 0

network 172.24.10.128 0.0.0.15 area 0

network 209.165.202.0 0.0.0.3 area 0

3.8 Налаштування роботи Інтернет

Для забезпечення доступу системи до глобальної мережі Інтернет, необхідно імплементувати технологію Network Address Translation (NAT).

Визначений пул адрес для NAT, який використовується в цьому процесі, охоплює діапазон від 209.165.202.5 до 209.165.202.30. Ці адреси дозволяють розподілити зовнішні з'єднання серед численних внутрішніх пристроїв, забезпечуючи ефективне використання Інтернет-ресурсів.

Розглянемо налаштування NAT, використовуючи як приклад прикордонний маршрутизатор Akimow_R3:

```
ip nat pool Internet 209.165.200.6 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT1 pool Internet
ip nat inside source static 172.24.9.120 209.165.200.5
ip nat inside source static 172.24.10.140 209.165.200.4
ip nat inside source static 172.24.9.131 209.165.200.3
ip classless
ip flow-export version 9
ip access-list extended NAT1
deny ip 172.24.10.0 0.0.0.127 172.24.9.128 0.0.0.127
deny ip 172.24.10.128 0.0.0.15 172.24.9.128 0.0.0.127
deny ip 172.24.8.0 0.0.0.255 172.24.9.128 0.0.0.127
deny ip 172.24.9.0 0.0.0.127 172.24.9.128 0.0.0.127
deny ip 172.1.24.0 0.0.0.255 172.24.9.128 0.0.0.127
permit ip 172.24.10.0 0.0.0.127 any
permit ip 172.24.9.0 0.0.0.127 any
permit ip 172.24.10.128 0.0.0.15 any
permit ip 172.24.8.0 0.0.0.255 any
permit ip 172.1.24.0 0.0.0.255 any
```

3.9 Перевірка комп'ютерної Системи підприємства

Перевіряємо базове налаштування пристроїв на прикладі маршрутизатора Akimow_R1. За допомогою команди show running-config перевіряємо назву пристрою (рис. 3.2), призначення паролю до консолі (рис. 3.3) паролю до ліній vty та використання на них протоколу ssh (рис. 3.4), паролю до привілейованого режиму (рис. 3.5), банеру MOTD (рис. 3.6), імені та паролю користувача (рис. 3.7), імені домену (рис. 3.8).

```
!
hostname Akimow_R1
!
```

Рисунок 3.2 – Ідентифікація пристрою

```
line con 0
 password 7 0822455D0A16
 login authentication console
!
```

Рисунок 3.3 – Консольний пароль

```
line vty 0 4
 password 7 0822455D0A16
 login authentication default
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login authentication default
 transport input ssh
```

Рисунок 3.4 – Пароль для ліній vty та використання протоколу SSH

```
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
```

Рисунок 3.5 – Пароль для привілейованого режиму

```
banner motd ^CAkimow_R1^C
```

Рисунок 3.6 – Повідомлення дня (MOTD)

```
!
username 12321ck_Akimow password 7 0820484300170616010803
username Akimow password 7 08204843001754454l
!
```

Рисунок 3.7 – Ім'я користувача та пароль

```
!
ip domain-name Akimow_R1
```

Рисунок 3.8 – Доменне ім'я

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


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

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

1      Po1(SU)           LACP   Fa0/1(P) Fa0/2(P)
2      Po2(SU)           LACP   Fa0/3(P) Fa0/4(P)
```

Рисунок 3.9 – Конфігурація EtherChannel

```
Akimow_R3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.165.202.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.1.24.12 0.0.0.3 area 0
    172.24.10.128 0.0.0.15 area 0
    209.165.202.0 0.0.0.3 area 0
  Passive Interface(s):
    Vlan1
    GigabitEthernet0/2
    Serial0/0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.1.24.13           110      00:25:33
    172.1.24.21           110      00:26:09
    172.24.9.1            110      00:25:34
    172.24.9.129          110      00:25:33
    172.24.10.1           110      00:26:07
    209.165.202.1         110      00:25:37
    209.165.202.2         110      00:25:33
  Distance: (default is 110)
```

Рисунок 3.10 – Налаштування OSPF

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete	
	Successful	PC2	PC7	ICMP		0.000	N	0	(edit)		(delete)
	Successful	PC7	PC2	ICMP		0.000	N	1	(edit)		(delete)

Рисунок 3.11 – Зв'язок між підмережами LAN_4 та LAN_2

```
     209.165.201.0/28 is subnetted, 1 subnets
S       209.165.201.0 [1/0] via 209.165.202.2
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Рисунок 3.12 – Налаштований маршрут за замовчуванням на маршрутизаторі

```
Username: Akimow
Password:
Akimow_R1>en
Password:
Akimow_R1#
```

Рисунок 3.13 – Налаштування маршрутизатора для підтримки служби AAA

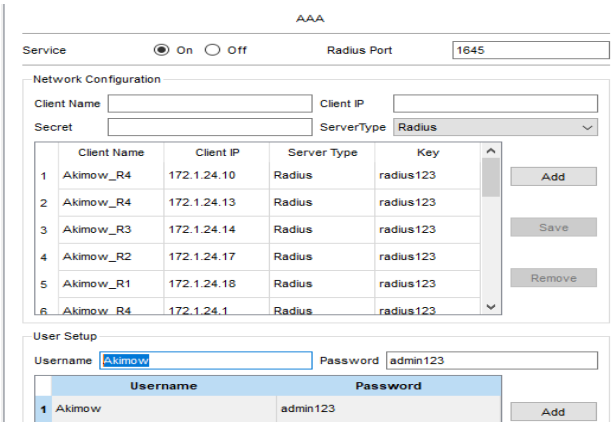

Рисунок 3.14 – Налаштування RADIUS-сервера

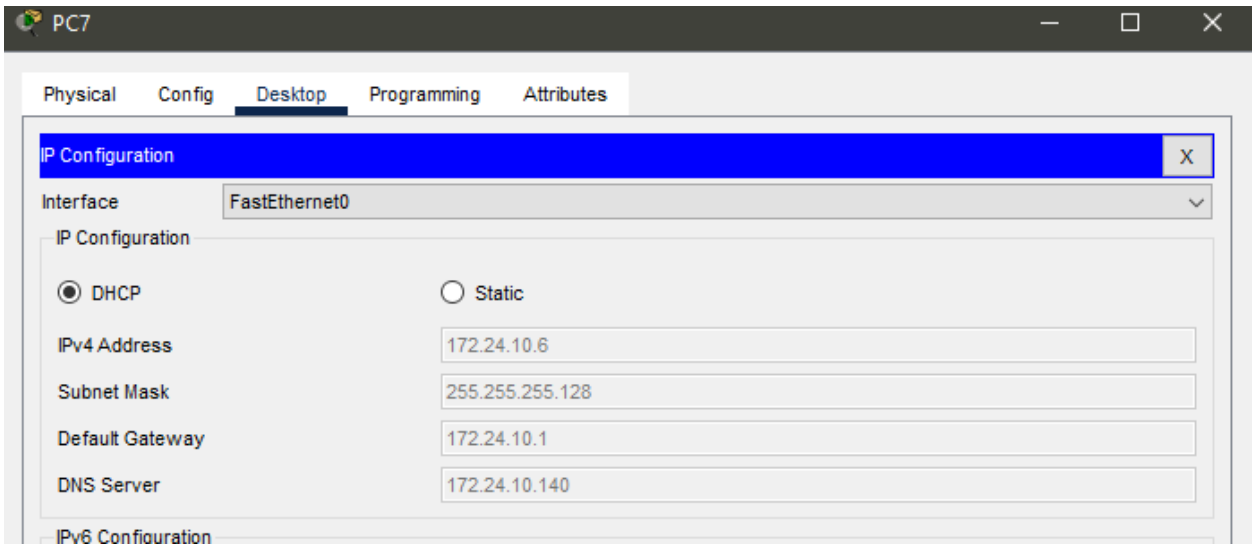

Рисунок 3.15 – IP-адреса комп'ютера в LAN_4

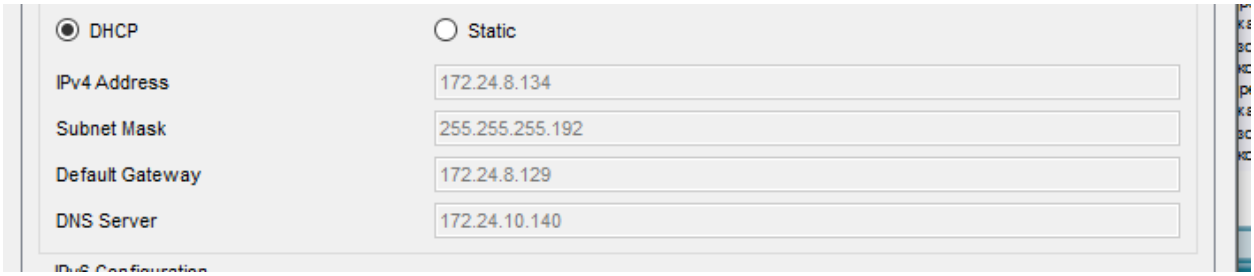

Рисунок 3.16 – IP-адреса комп'ютера в VLAN20

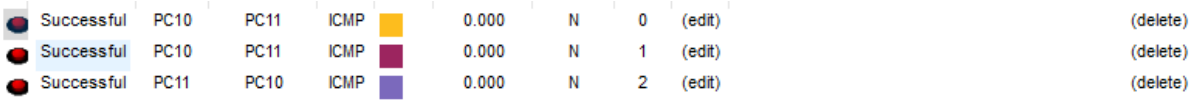

Рисунок 3.17 – Зв'язок між VLAN

Перевіряємо відкриття веб-сайту з відомостями про тему та завдання на кваліфікаційну роботу студента на прикладі PC0 (рис. 3.19)

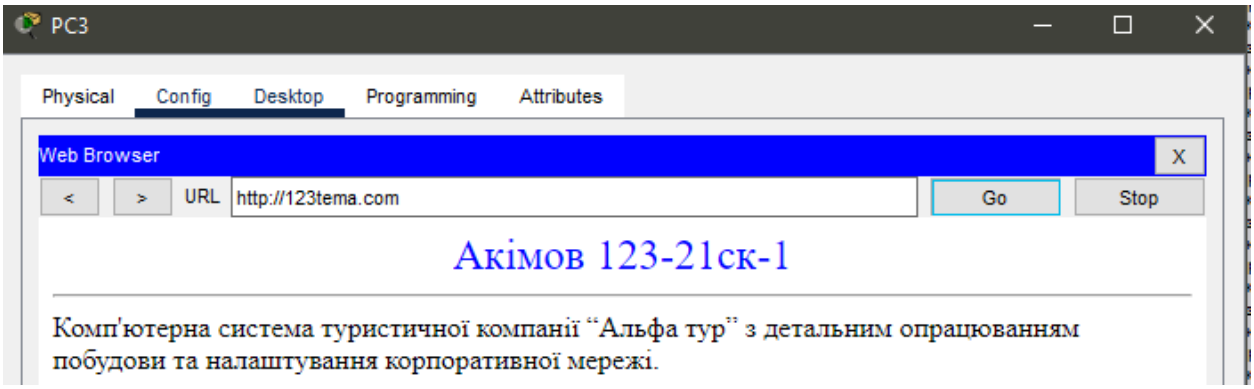

Рисунок 3.18 – Відкритий веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Інженерне рішення по розробці компонента Системи

При проектуванні корпоративної мережі детально розглянуто розробку компоненту IoT системи, яка забезпечує контроль клімату та управління вікнами у приміщеннях. Основна мета даного компонента – підтримувати оптимальні умови для комфорту та безпеки користувачів шляхом автоматизації процесів регулювання температури та відкривання/закривання вікон а також сповіщення персоналу про загрозу за допомогою сигналізації, також при спрацюванні тривоги замикаються вікна та вимикаються все кліматичне обладнання для забезпечення меншого притоку кисню для локалізації пожежі. Система без використання системи тушіння, у будівлі офісу вона не передбачена.

Система реалізована таким чином, щоб моніторити стан навколишнього середовища і реагувати на зміну температури. Ключовими елементами системи є датчики температури, кондиціонери, автоматизовані вікна датчики задимленості та сирени.

Дана IoT система інтегрується в локальну мережу і використовує сучасні протоколи передачі даних для забезпечення надійної та ефективної роботи.

Застосування IoT технологій дозволяє створити розумну систему, яка може автоматично адаптуватися до змін зовнішніх умов та забезпечувати комфортне середовище без втручання користувачів.

4.2 Налаштування обладнання та сервісів системи IoT

Для створення IoT-системи офісу спочатку інсталюємо IoT-пристрої, датчики під’єднуючи їх до Home Gateway-ї. На Home Gateway-ях мережі налаштовуємо бездротову точку доступу на прикладі з мережі LAN4 з SSID " Akimow_LAN4" та паролем " Akimow_LAN4", застосовуючи протокол безпеки WPA2-PSK з методом шифрування AES.

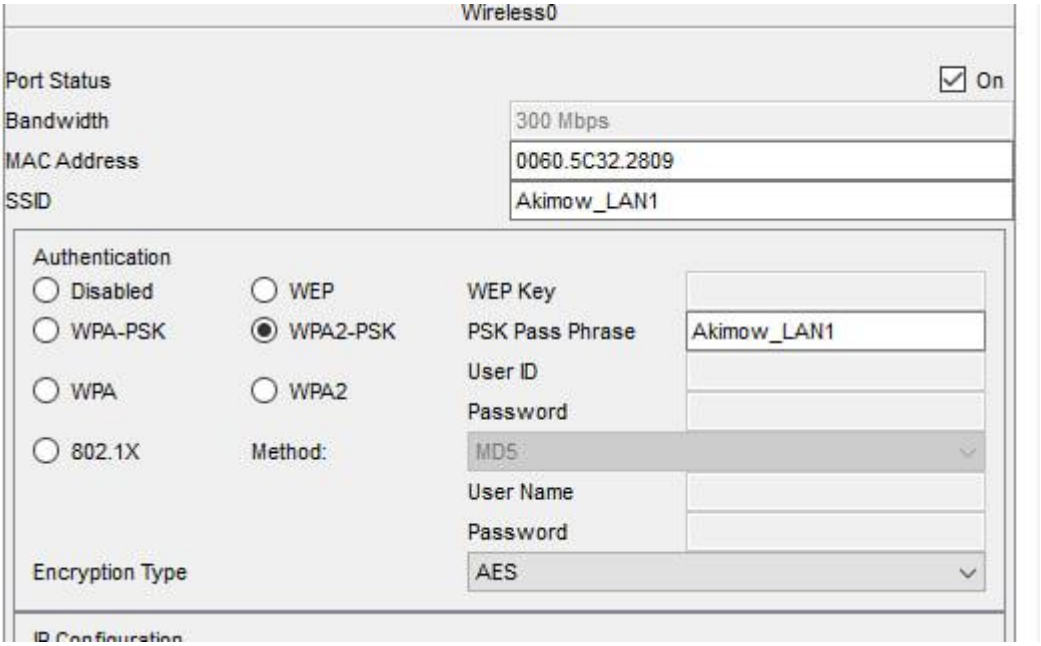

Рисунок 4.1 – Налаштування бездротової мережі

Кожен IoT-пристрій налаштовуємо для підключення до Home Gateway, вводячи відповідні SSID та пароль. В якості IoT-сервера використовується віддалений IoT сервер з адресою "172.24.10.100". Топологічна схема корпоративної мережі клініки з розміщенням IoT-пристроїв зображена на рис. 4.4

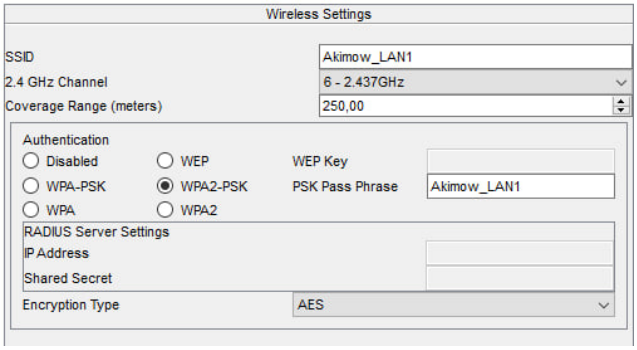

Рисунок 4.2 – Налаштування бездротової мережі на пристроях

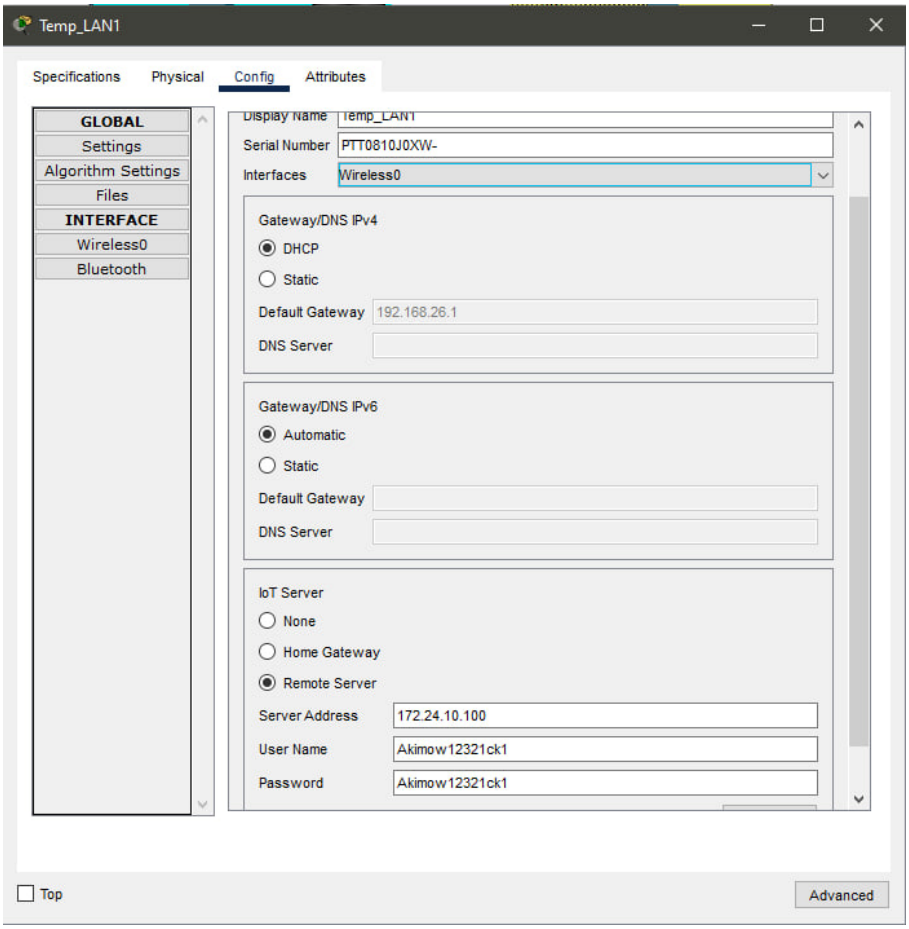

Рисунок 4.2 – Налаштування підключення до віддаленого серверу

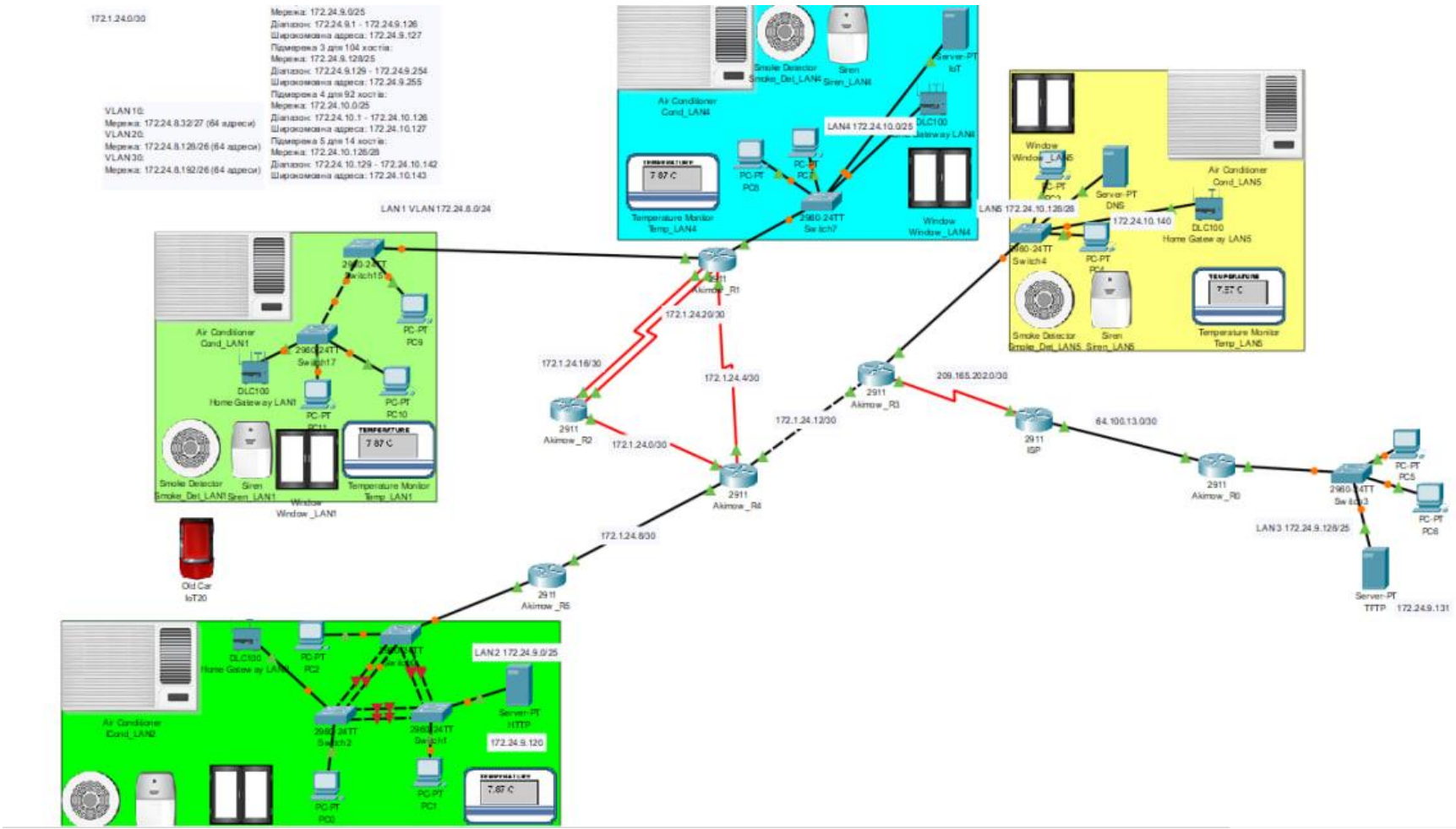

Рисунок 4.4 – Топологічна схема корпоративної мережі компанії з розміщенням IoT пристроїв

Для налаштування умов роботи IoT-системи у любій машині мережі відкриваємо IoT Monitor, вводимо адресу шлюзу та логін з паролем. Після цього відкривається сторінка з усіма підключеними IoT-пристроями, яка показана на рисунку 4.2

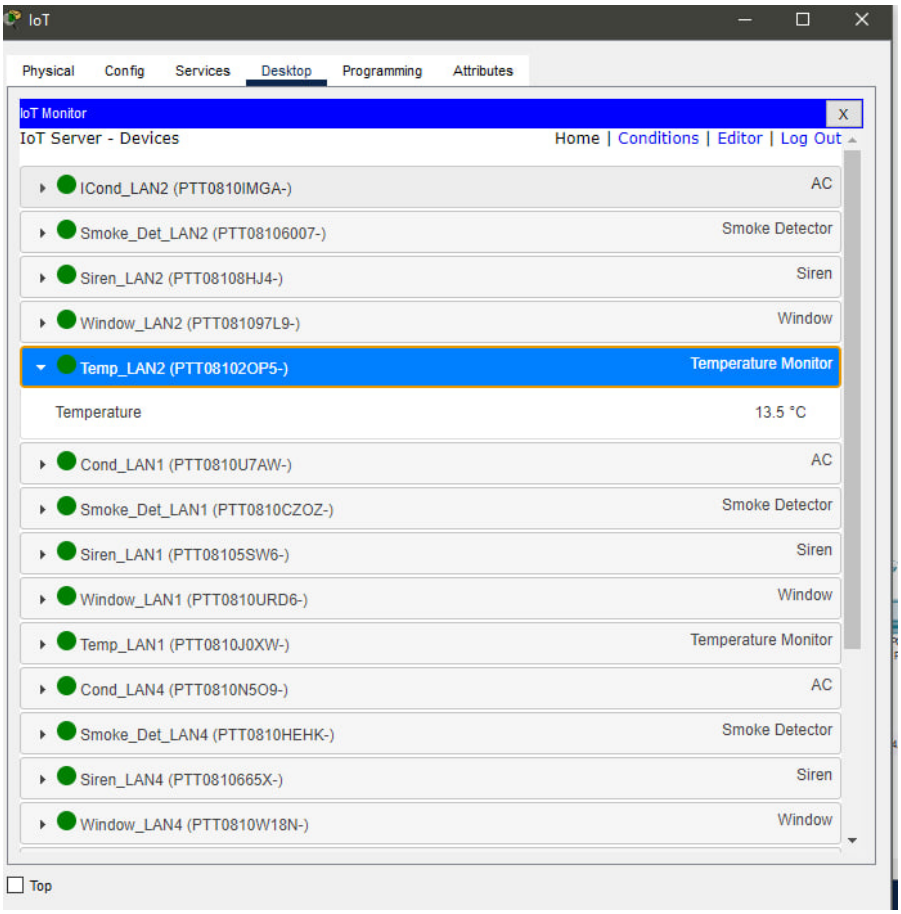

Рисунок 4.5 – Під’єднані IoT-пристрої основної мережі

Для спрацювання сирен потрібні умови що при виявлені диму у будь якій кімнаті, вмикалися сирени, вимикалось кліматична апаратура та замикалися вікна будь де у мережі. Після відбою небезпеки, вікна переводяться у своє звичне положення за іншими сценаріями вмикається кліматичне обладнання та вимикаються сирени.

При спрацюванні кліматичного сценарію, при температурі вище за 25 градусів у приміщені вмикається кондиціонер та зачиняється вікно, при температурі нижче за 25 градусів, вимикається кондиціонер та відчиняється вікно. Вікна зачиняються при температурі меншої за 19 градусі. Та за всіма

показниками можливо спостерігати з IoT монітору бо на сервер передаються всі значення.

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Siren_ON	Match any: • Smoke_Det_LAN1 Level > 2 • Smoke_Det_LAN4 Level > 2 • Smoke_Det_LAN2 Level > 2 • Smoke_Det_LAN5 Level > 2	Set Siren_LAN4 On to true Set Siren_LAN2 On to true Set Siren_LAN1 On to true Set Siren_LAN5 On to true Set Window_LAN2 On to false Set Window_LAN1 On to false Set Window_LAN4 On to false Set Window_LAN5 On to false
Edit Remove	Yes	Siren_OFF	Match all: • Smoke_Det_LAN2 Level < 2 • Smoke_Det_LAN1 Level < 2 • Smoke_Det_LAN4 Level < 2 • Smoke_Det_LAN5 Level < 2	Set Siren_LAN2 On to false Set Siren_LAN1 On to false Set Siren_LAN4 On to false Set Siren_LAN5 On to false
Edit Remove	Yes	COND_ON_LAN1	Match all: • Temp_LAN1 Temperature >= 25.0 °C • Siren_LAN1 On is false	Set Cond_LAN1 On to true Set Window_LAN1 On to false
Edit Remove	Yes	COND_OFF_LAN1	Temp_LAN1 Temperature < 25.0 °C	Set Cond_LAN1 On to false
Edit Remove	Yes	Window_OPEN_LAN1	Match all: • Siren_LAN1 On is false • Cond_LAN1 On is false • Temp_LAN1 Temperature > 19.0 °C	Set Window_LAN1 On to true
Edit Remove	Yes	COND_ON_LAN2	Match all: • Temp_LAN2 Temperature > 25.0 °C • Siren_LAN2 On is false	Set ICond_LAN2 On to true Set Window_LAN2 On to false
Edit Remove	Yes	COND_OFF_LAN2	Temp_LAN2 Temperature < 25.0 °C	Set ICond_LAN2 On to false
Edit Remove	Yes	Window_OPEN_LAN2	Match all: • Siren_LAN2 On is false • ICond_LAN2 On is false • Temp_LAN2 Temperature > 19.0 °C	Set Window_LAN2 On to true
Edit Remove	Yes	COND_ON_LAN4	Match all: • Siren_LAN4 On is false • Temp_LAN4 Temperature > 25.0 °C	Set Cond_LAN4 On to true Set Window_LAN4 On to false
Edit Remove	Yes	COND_OFF_LAN4	Temp_LAN4 Temperature < 25.0 °C	Set Cond_LAN4 On to false
Edit Remove	Yes	Window_OPEN_LAN4	Match all: • Temp_LAN4 Temperature > 19.0 °C • Siren_LAN4 On is false • Cond_LAN4 On is false	Set Window_LAN4 On to true
Edit Remove	Yes	COND_ON_LAN5	Match all: • Siren_LAN5 On is false • Temp_LAN5 Temperature > 25.0 °C	Set Cond_LAN5 On to true Set Window_LAN5 On to false
Edit Remove	Yes	COND_OFF_LAN5	Temp_LAN5 Temperature < 25.0 °C	Set Cond_LAN5 On to false
Edit Remove	Yes	Window_OPEN_LAN5	Match all: • Temp_LAN5 Temperature > 19.0 °C • Cond_LAN5 On is false • Siren_LAN5 On is false	Set Window_LAN5 On to true
Edit Remove	Yes	Window_CLOSE_LAN4	Match all: • Siren_LAN4 On is false • Temp_LAN4 Temperature < 19.0 °C	Set Window_LAN4 On to false
Edit Remove	Yes	Window_CLOSE_LAN5	Match all: • Siren_LAN5 On is false • Temp_LAN5 Temperature < 19.0 °C	Set Window_LAN5 On to false
Edit Remove	Yes	Window_CLOSE_LAN1	Match all: • Siren_LAN1 On is false • Temp_LAN1 Temperature < 19.0 °C	Set Window_LAN1 On to false
Edit Remove	Yes	Window_CLOSE_LAN2	Match all: • Siren_LAN2 On is false • Temp_LAN2 Temperature < 19.0 °C	Set Window_LAN2 On to false

Add

Рисунок 4.6 – Сценарії мережі

4.3 Перевірка роботи компонента Системи

Для перевірки роботи налаштовано середовище Cisco Packet Tracer для періодичного змінення температури та додано елемент який симулює задимленість.

Перевірка системи при температурі нижчої за 25 градусів на прикладі LAN5(рис. 4.7)

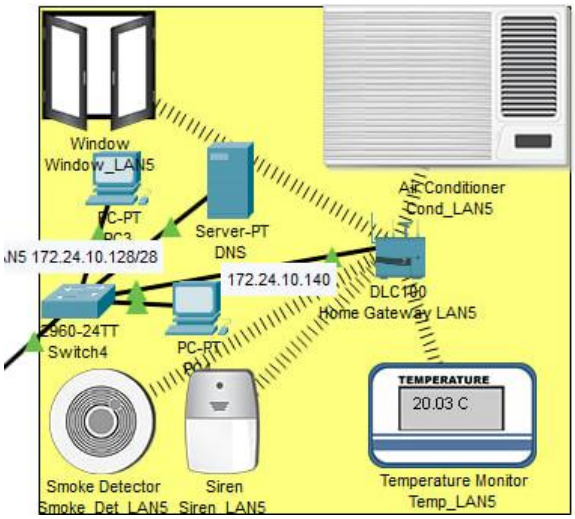

Рисунок 4.7 – Поведінка системи при температурі < 25

Перевірка системи при температурі вище за 25 градусів на прикладі системи з LAN5(рис. 4.8)

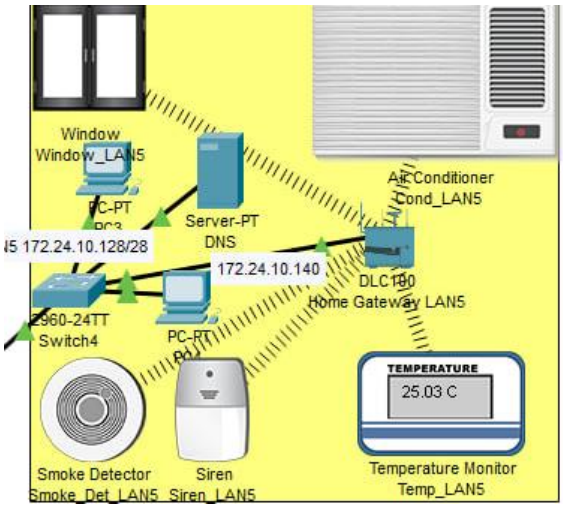

Рисунок 4.8 – Поведінка системи при температурі > 25

Перевірка системи при температурі нижче за 19 градусів на прикладі системи з LAN5(рис. 4.9)

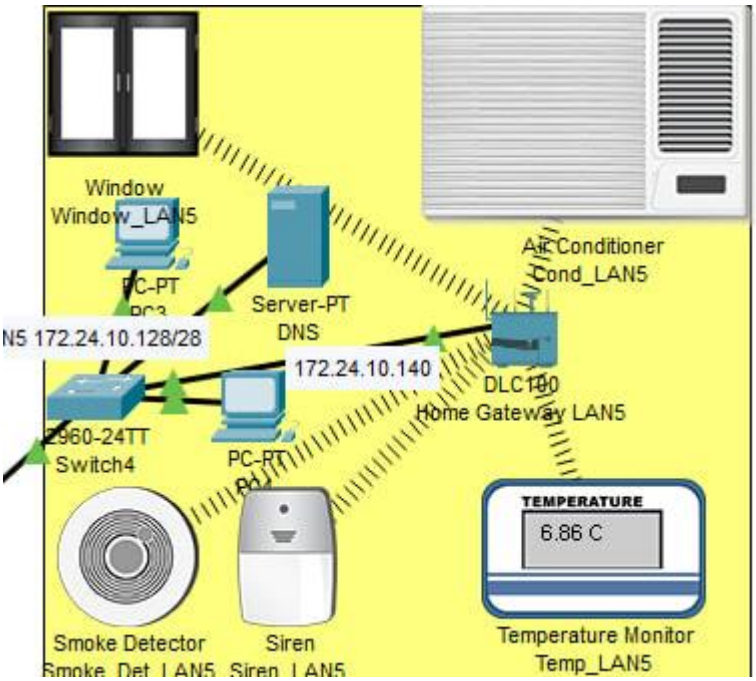

Рисунок 4.9 – Поведінка системи при температурі < 19

При виявлені диму, включення оповіщення відбувається по всій системі, поведімка системи зображена на рисунку 4.10

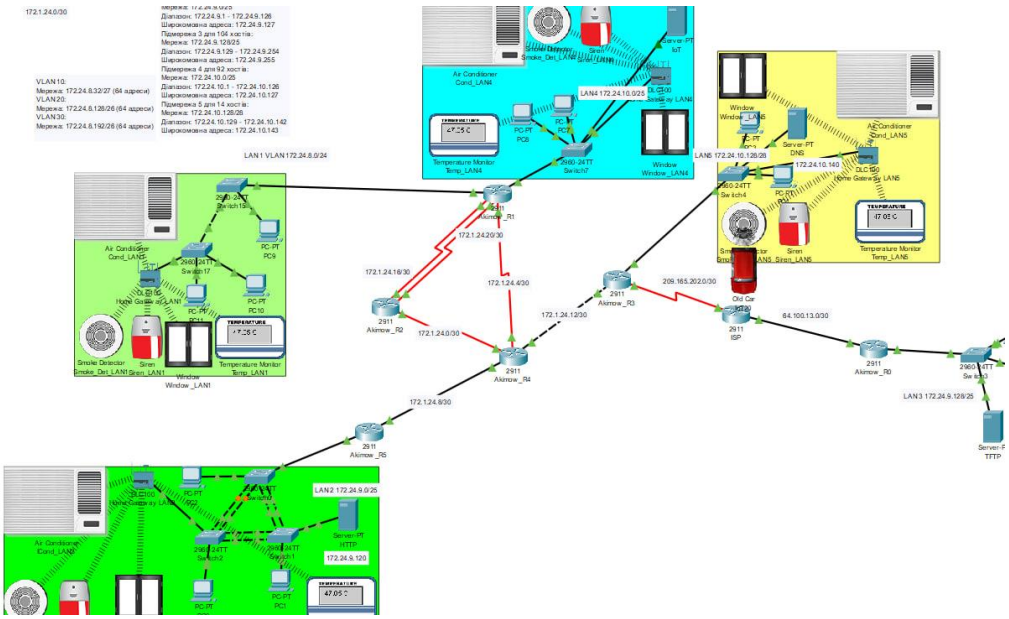

Рисунок 4.10 – Поведінка системи при виявлені диму у LAN5

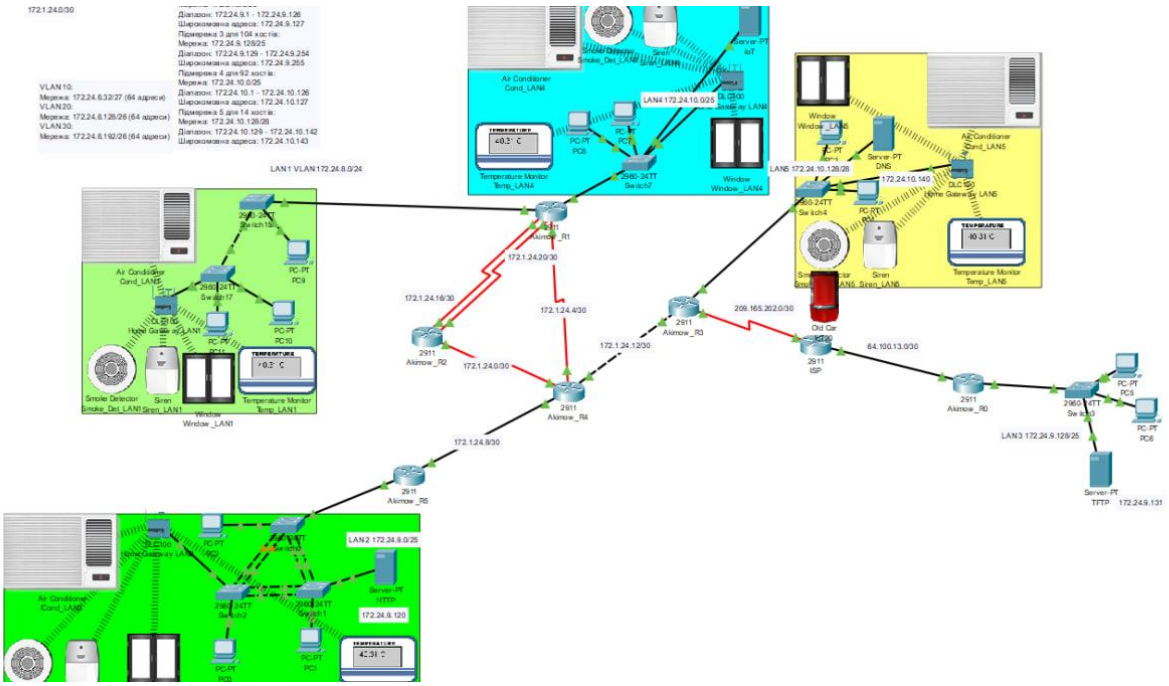

Рисунок 4.11 – Поведінка системи при стабільній ситуації

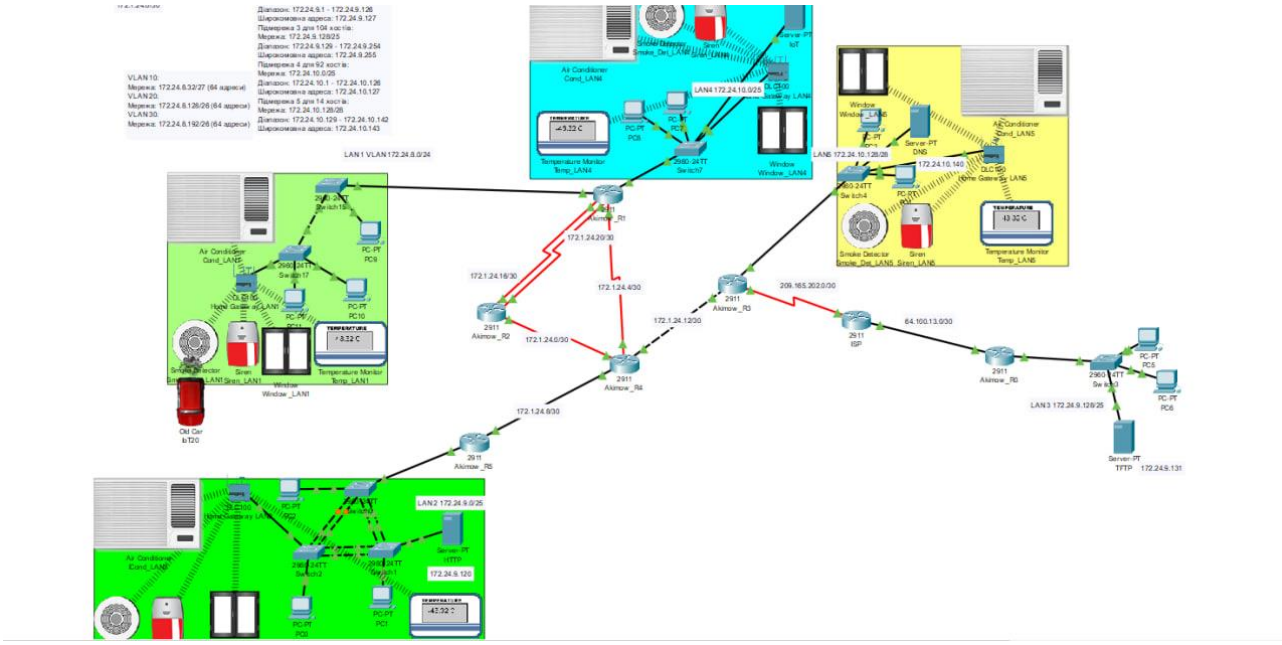

Рисунок 4.12 – Поведінка системи при виявлені диму у LAN1

ВИСНОВКИ

Загальний процес побудови та налаштування корпоративної мережі для туристичної компанії «Альфа тур» виявився складним, але водночас надзвичайно важливим для забезпечення оптимальної роботи всіх аспектів її діяльності. Починаючи з аналізу потреб та вимог бізнесу, інженери з мережевих технологій здійснили моделювання та проектування мережі, враховуючи такі ключові аспекти, як масштабируваність, надійність, безпека та ефективне управління трафіком.

Використання технології AAA дозволило забезпечити аутентифікацію, авторизацію та облік користувачів у мережі, що є критично важливим для забезпечення безпеки та конфіденційності даних. Застосування VPN для віддаленої мережі забезпечило безпечний доступ до ресурсів компанії для працівників, які працюють з віддалених місць.

Впровадження протоколу OSPF для динамічної маршрутизації в мережі дозволило оптимізувати шляхи передачі даних та забезпечити швидкий реагування на зміни у мережевому трафіку. Технологія EtherChannel дозволила підвищити пропускну здатність та надійність мережевих з'єднань, що є важливим для підтримки високого рівня сервісу для користувачів.

Під час налаштування мережі були враховані особливості діяльності компанії «Альфа тур«, зокрема, потреби у безперервному доступі до бази даних клієнтів та інших важливих ресурсів. Були встановлені механізми захисту даних, що забезпечили високий рівень конфіденційності та цілісності інформації.

Важливим аспектом проєктування корпоративної мережі було впровадження компоненту IoT системи для контролю клімату та управління вікнами у приміщеннях. Основна мета цього компонента – підтримувати оптимальні умови для комфорту та безпеки користувачів шляхом автоматизації процесів регулювання температури та відкривання/закривання вікон, а також сповіщення персоналу про загрозу за допомогою сигналізації. У разі тривоги

система автоматично замикає вікна та вимикає все кліматичне обладнання для зменшення притоку кисню і локалізації пожежі. Система не включає функцію пожежогасіння.

Застосування IoT технологій дозволяє створити розумну систему, яка автоматично адаптується до змін зовнішніх умов та забезпечує комфортне середовище без втручання користувачів.

В підсумку, побудова та налаштування корпоративної мережі для компанії «Альфа тур» виявилися успішними, забезпечивши не лише оптимальну роботу бізнесу, але й створивши основу для подальшого розвитку та вдосконалення інфраструктури.

Ця мережа стала не лише інструментом підтримки операційного процесу, але й стратегічним активом, який дозволить компанії успішно конкурувати на ринку туристичних послуг та задовольняти потреби своїх клієнтів у надійному та ефективному обслуговуванні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2023-2024. – 62 с.

2. Toshiba Europe: Рішення для IoT та корпоративних мереж [Електронний ресурс] – Режим доступу до ресурсу: toshiba.eu (дата звернення 15.06.2024р.).

3. Мережа Ланет: Налаштування корпоративних мереж та IoT [Електронний ресурс] – Режим доступу до ресурсу: lanet.ua (дата звернення 1.06.2024р.).

4. Human: Підтримка корпоративних систем [Електронний ресурс] – Режим доступу до ресурсу: id.human.ua(дата звернення 2.06.2024р.).

5. Електронний кабінет платника: Моделі управління мережами [Електронний ресурс] – Режим доступу до ресурсу: cabinet.tax.gov.ua (дата звернення 2.06.2024р.).

6. Статистика цифрової економіки та суспільства - використання ERP, CRM та хмарних обчислень в європейських підприємствах [Електронний ресурс] – Режим доступу до ресурсу: ec.europa.eu (дата звернення 15.06.2024р.)

7. AAA – Education [Електронний ресурс] – Режим доступу до ресурсу: ec.europa.eu (дата звернення 3.05.2023р

Додаток А

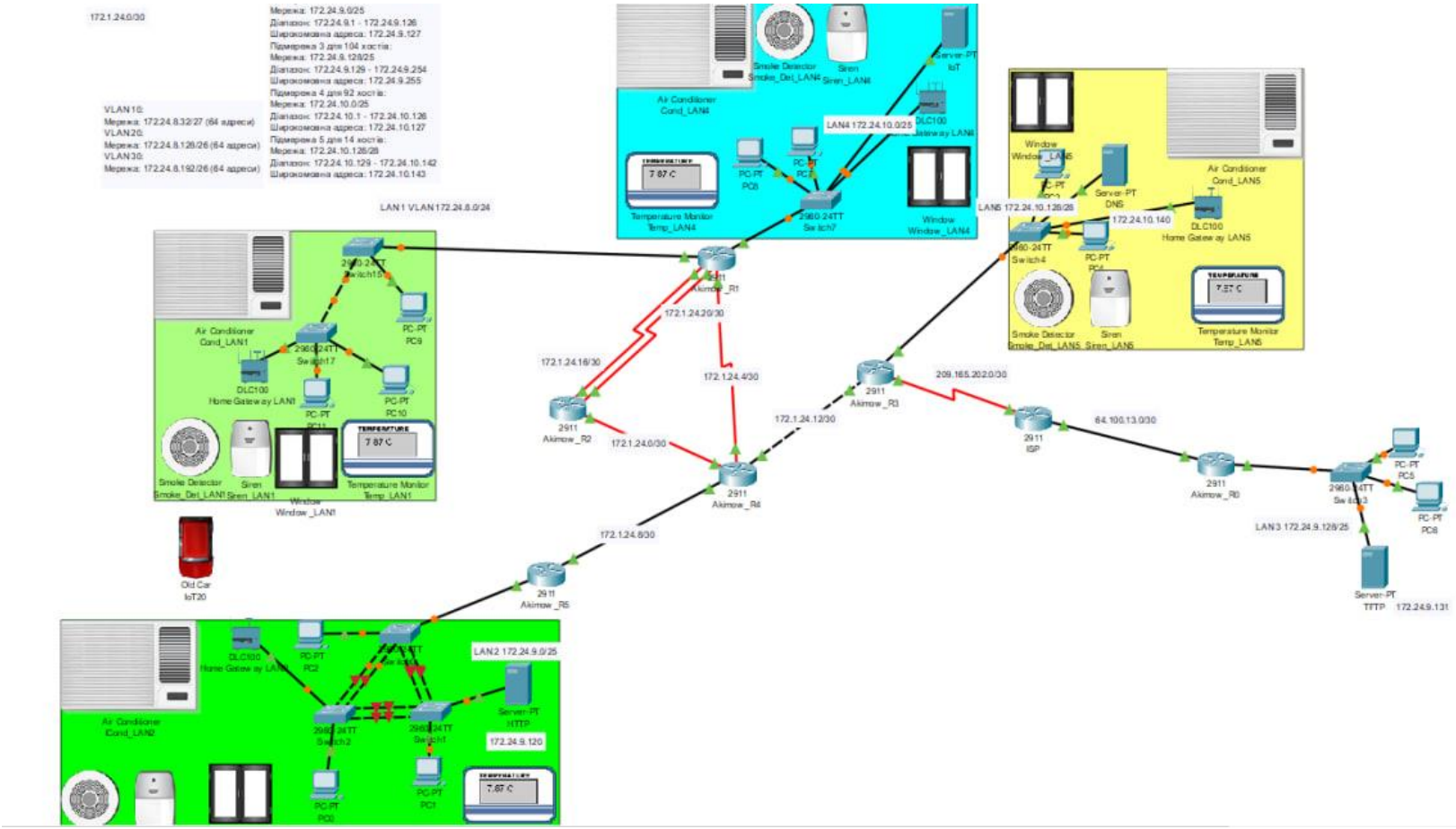

Рисунок ДА.1 – Загальна архітектура мережі

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.23004-01 12 01

Листів 16

2024

АНОТАЦІЯ

Дана програма містить в собі команди для налаштування маршрутизаторів та комутаторів корпоративної мережі. Команди призначені для налаштування IP-адрес, базового налаштування пристроїв, налаштування DHCP, NAT, VPN, AAA, OSPF, VLAN, статичних маршрутів, EtherChannel та безпеки портів.

ЗМІСТ

1. Akimow_R1

```
Current configuration : 3547 bytes
!ersion 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname Akimow_R1
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 172.24.10.126
ip dhcp excluded-address 172.24.10.127
ip dhcp excluded-address 172.24.10.1 172.24.10.5
ip dhcp excluded-address 172.24.8.129 172.24.8.133
ip dhcp excluded-address 172.24.8.33 172.24.8.35
ip dhcp excluded-address 172.24.8.193 172.24.8.195
ip dhcp pool LAN-4
network 172.24.10.0 255.255.255.128
default-router 172.24.10.1
dns-server 172.24.10.140
ip dhcp pool LAN1-VLAN20
network 172.24.8.128 255.255.255.192
default-router 172.24.8.129
dns-server 172.24.10.140
ip dhcp pool LAN1-VLAN10
network 172.24.8.32 255.255.255.224
default-router 172.24.8.33
dns-server 172.24.10.140
ip dhcp pool LAN1-VLAN30
network 172.24.8.192 255.255.255.192
default-router 172.24.8.193
dns-server 172.24.10.140
```

```
aaa new-model
aaa authentication login console group radius local
aaa authentication login default local
no ip cef
no ipv6 cef
username 12321ck_Akimow password 7 082048430017061E010803
username Akimow password 7 082048430017544541
license udi pid CISCO2911/K9 sn FTX15242XKN-
ip domain-name Akimow_R1
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 172.24.10.1 255.255.255.128
duplex auto
speed auto
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 172.24.8.33 255.255.255.224
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 172.24.8.129 255.255.255.192
interface GigabitEthernet0/1.30
encapsulation dot1Q 30
ip address 172.24.8.193 255.255.255.192
interface GigabitEthernet0/1.99
encapsulation dot1Q 99
ip address 172.24.8.1 255.255.255.240
```

```
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
interface Serial0/0/0
ip address 172.1.24.18 255.255.255.252
clock rate 128000
interface Serial0/0/1
ip address 172.1.24.22 255.255.255.252
clock rate 128000
interface Serial0/1/0
ip address 172.1.24.6 255.255.255.252
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
interface Vlan1
no ip address
shutdown
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
no passive-interface Serial0/0/0
no passive-interface Serial0/0/1
no passive-interface Serial0/1/0
no passive-interface GigabitEthernet0/1.10
no passive-interface GigabitEthernet0/1.20
```

```
no passive-interface GigabitEthernet0/1.30
no passive-interface GigabitEthernet0/1.99
auto-cost reference-bandwidth 1000
network 172.1.24.4 0.0.0.3 area 0
network 172.1.24.16 0.0.0.3 area 0
network 172.1.24.20 0.0.0.3 area 0
network 172.24.10.0 0.0.0.127 area 0
network 172.24.8.32 0.0.0.31 area 0
network 172.24.8.128 0.0.0.63 area 0
network 172.24.8.192 0.0.0.63 area 0
ip classless
ip flow-export version 9
banner motd ^CAkimow_R1^C
radius server host
address ipv4 172.24.9.120 auth-port 1645
key radius123
radius server 172.24.9.120
address ipv4 172.24.9.120 auth-port 1645
key radius123
line con 0
password 7 0822455D0A16
login authentication console
line aux 0
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
```

transport input ssh
end

2. Akimow_R3

Current configuration : 2909 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname Akimow_R3
enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 172.24.10.129 172.24.10.131
ip dhcp excluded-address 172.24.10.140
ip dhcp pool LAN-5
network 172.24.10.128 255.255.255.240
default-router 172.24.10.129
dns-server 172.24.10.140
aaa new-model
aaa authentication login console group radius local
aaa authentication login default local
no ip cef
no ipv6 cef
username 12321ck_Akimow password 7 082048430017061E010803
username Akimow password 7 082048430017544541
license udi pid CISCO2911/K9 sn FTX15244H8L-
ip domain-name Akimow_R3
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 172.1.24.14 255.255.255.252
ip nat inside

duplex auto
speed auto
interface GigabitEthernet0/1
ip address 172.24.10.129 255.255.255.240
ip nat inside
duplex auto
speed auto
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
interface Serial0/0/0
ip address 209.165.202.1 255.255.255.252
ip nat outside
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
interface Vlan1
no ip address
shutdown
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
no passive-interface Serial0/0/0
auto-cost reference-bandwidth 1000
network 172.1.24.12 0.0.0.3 area 0

```
network 172.24.10.128 0.0.0.15 area 0
network 209.165.202.0 0.0.0.3 area 0
ip nat pool Internet 209.165.200.6 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT1 pool Internet
ip nat inside source static 172.24.9.120 209.165.200.5
ip nat inside source static 172.24.10.140 209.165.200.4
ip nat inside source static 172.24.9.131 209.165.200.3
ip classless
ip flow-export version 9
ip access-list extended NAT1
deny ip 172.24.10.0 0.0.0.127 172.24.9.128 0.0.0.127
deny ip 172.24.10.128 0.0.0.15 172.24.9.128 0.0.0.127
deny ip 172.24.8.0 0.0.0.255 172.24.9.128 0.0.0.127
deny ip 172.24.9.0 0.0.0.127 172.24.9.128 0.0.0.127
deny ip 172.1.24.0 0.0.0.255 172.24.9.128 0.0.0.127
permit ip 172.24.10.0 0.0.0.127 any
permit ip 172.24.9.0 0.0.0.127 any
permit ip 172.24.10.128 0.0.0.15 any
permit ip 172.24.8.0 0.0.0.255 any
permit ip 172.1.24.0 0.0.0.255 any
banner motd ^CAkimow_R3^C
radius server host
address ipv4 172.24.9.120 auth-port 1645
key radius123
radius server 172.24.9.120
address ipv4 172.24.9.120 auth-port 1645
key radius123
line con 0
password 7 0822455D0A16
login authentication console
```

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

3. Akimow_R0

Current configuration : 1917 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname Akimow_R0
enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 172.24.9.129 172.24.9.131
ip dhcp excluded-address 172.24.9.254
ip dhcp excluded-address 172.24.9.255
ip dhcp pool LAN-3
network 172.24.9.128 255.255.255.128
default-router 172.24.9.129
dns-server 172.24.10.140
aaa new-model
aaa authentication login console group radius local
aaa authentication login default local

```
ip cef
no ipv6 cef
username 12321ck_Akimow password 7 082048430017061E010803
username Akimow password 7 082048430017544541
license udi pid CISCO2911/K9 sn FTX1524W291-
ip domain-name Akimow_R0
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 64.100.13.2 255.255.255.252
duplex auto
speed auto
interface GigabitEthernet0/1
ip address 172.24.9.129 255.255.255.128
duplex auto
speed auto
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
interface Vlan1
no ip address
shutdown
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
auto-cost reference-bandwidth 1000
network 64.100.13.0 0.0.0.3 area 0
```

network 172.24.9.128 0.0.0.127 area 0
ip classless
ip flow-export version 9
banner motd ^CAkimow_R0^C
radius server host
address ipv4 172.24.9.120 auth-port 1645
key radius123
radius server 172.24.9.120
address ipv4 172.24.9.120 auth-port 1645
key radius123
line con 0
password 7 0822455D0A16
login authentication console
line aux 0
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
end

4.switch15

Current configuration : 1828 bytes
!
version 15.0
no service timestamps log datetime msec

```
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
switchport mode trunk
!
interface FastEthernet0/5
switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
!
```

```
interface FastEthernet0/8
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 20
!
interface FastEthernet0/12
switchport access vlan 20
!
interface FastEthernet0/13
switchport access vlan 20
!
interface FastEthernet0/14
switchport access vlan 20
!
interface FastEthernet0/15
switchport access vlan 20
!
interface FastEthernet0/16
switchport access vlan 20
!
```

```
interface FastEthernet0/17
switchport access vlan 30
!
interface FastEthernet0/18
switchport access vlan 30
!
interface FastEthernet0/19
switchport access vlan 30
!
interface FastEthernet0/20
switchport access vlan 30
!
interface FastEthernet0/21
switchport access vlan 30
!
interface FastEthernet0/22
switchport access vlan 30
!
interface FastEthernet0/23
switchport access vlan 30
!
interface FastEthernet0/24
switchport access vlan 30
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
```

shutdown

line con 0

!

line vty 0 4

login

line vty 5 15

login

5.switch10

Current configuration : 1420 bytes

!

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname Switch

spanning-tree mode pvst

spanning-tree extend system-id

!

interface Port-channel1

description Link to Other Switch

switchport mode trunk

!

interface Port-channel2

switchport mode trunk

!

interface FastEthernet0/1

switchport mode trunk

channel-group 1 mode active

```
!
interface FastEthernet0/2
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/3
switchport mode trunk
channel-group 2 mode active
!
interface FastEthernet0/4
switchport mode trunk
channel-group 2 mode active
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
```

```
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
```

```
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
end
```