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

студентки Швець Анастасії Дмитрівни
(ПІБ)
академічної групи 123-20з-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

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

на тему "Комп'ютерна система IT компанії «Універсальні інформаційні технології» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"
(назва за наказом ректора)

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

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій та
комп'ютерної інженерії
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)
"___" _____ 2024 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Швець А.Д. **академічної групи** 123-20з-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

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

на тему « Комп'ютерна система ІТ компанії «Універсальні інформаційні технології» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 470-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2024
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2024
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2024
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2024

Завдання видано _____ доц. Шедловський І.А
(підпис керівника) (прізвище, ініціали)

Дата видачі 06.02.2024

Дата подання до екзаменаційної комісії 02.07.2024

Прийнято до виконання _____ Швець А.Д.

РЕФЕРАТ

Пояснювальна записка: с. 79, рис. 28, джерел 20, табл. 6., додатки 3.

CISCO, CISCO PACKET TRACER, DHCP, DNS, HTTP, VPN, КОМП'ЮТЕРНА СИСТЕМА, КОМУТАТОР, КОРПОРАТИВНІ МЕРЕЖІ, МАРШРУТИЗАТОР.

Об'єкт розробки – комп'ютерна система ІТ-компанії «Універсальні інформаційні технології» з реалізацією побудови та налаштування корпоративної мережі.

Мета роботи – побудова комп'ютерної системи ІТ-компанії «Універсальні інформаційні технології» з детальним опрацюванням налаштування безпечного віддаленого доступу до мереж через VPN.

Дана корпоративна мережа може використовуватися у великих і середніх ІТ-компаніях, де необхідно надати співробітникам можливість підключення до віддаленого доступу через VPN.

Ця мережа була спроектована і випробувана в симуляції з використанням Cisco Packet Tracer, що дозволило перевірити теоретичну працездатність проектованої комп'ютерної системи.

Результатом цієї роботи є спроектована комп'ютерна система для великої та середньої ІТ-компанії. Комп'ютерна система і її комп'ютерна мережа складається з 4-х локальних мереж і передбачає можливість віддаленого підключення користувача через VPN.

Спроектована комп'ютерна система дозволяє співробітникам розгортати віртуальні машини в межах однієї локальної комп'ютерної мережі і не засмічувати трафік загальної корпоративної мережі.

Система дає можливість проводити технічну та програмну модернізацію. Комп'ютерну мережу було розроблено відповідно до завдань, поставлених для кваліфікаційної роботи бакалавра. [1]

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

PAgP – Port Aggregation Protocol

AAA – Authenticatio, Authorization and Accounting

DNS – Domain Name System

DHCP – Dynamic Host Protocol

HTTP – HyperText Transfer Protocol

FTP – File Transfer Protocol

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

QA – Quality assurance

IOS – Input/Output System

IT – Information Technology

UTP – Unshielded Twisted Pair

HR – Human Resources

ПЗ – Програмне забезпечення

ПП – Программний продукт

КС – Комп'ютерна система

IPsec – Internet Protocol Security

ВСТУП

Для великої ІТ-компанії, яка працює в місті з населенням 2,8 мільйона чоловік і налічує близько 450 співробітників, розробка і впровадження комп'ютерної системи є основним завданням. Це необхідно для підвищення операційної ефективності та забезпечення високого рівня обслуговування клієнтів. Також наявність комп'ютерної мережі дозволить використовувати загальні мережеві ресурси компанії, що знизить витрати на використання обладнання, а також спростить його використання.

Ця практика призначена для побудови теоретичної комп'ютерної системи для ІТ-компанії «Універсальні інформаційні технології» (далі – «УнІТ»), розташованої в місті Києві. При проектуванні системи враховується можливість підключення співробітників з віддалених офісів або приватних будинків.

Розглянуто та застосовано методи та засоби забезпечення безпеки та цілісності інформації, що передається. Також у тексті роботи було розглянуто та проаналізовано особливості підтримки технологій віддаленого доступу в роботі середніх та великих ІТ-компаній.

У даній роботі описані основні особливості інтеграції і дані рекомендації по впровадженню комп'ютерної системи в робочий процес ІТ-компанії «УнІТ».

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування КС

Компанія «УнІТ», як і багато компаній інтеграторів, займається наданням послуг у галузі розробки програмного та проектного забезпечення. Заснована у 2007 році, «УнІТ» стала однією з провідних світових компаній у галузі ІТ-послуг. Компанія «УнІТ» відкрила філіал на території України у 2007 році. Основні напрямки діяльності компанії включають:

- розробка програмного забезпечення;
- консультації та бізнес-аналітика;
- впровадження у робочий процес цифрових технологій;
- UX/UI-дизайн;
- надання хмарних рішень;
- технічна підтримка та обслуговування клієнтів.

Компанія співпрацює з різними галузями, включаючи фінансові послуги, охорону здоров'я, маркетинг, телекомунікації, пропонуючи технічні та системні рішення, які відповідають потребам клієнта.

ТОВ «Універсальні інформаційні технології» (УнІТ) – компанія, що динамічно розвивається. Швидкий темп розвитку став можливий завдяки професійному керівництву, висококваліфікованій команді та атмосфері ентузіазму. Метою створення компанії була розробка програмного продукту «Універсальна інформаційна система», яка являє собою єдину централізовану систему зберігання, захисту, обробки та доступу до інформації.

Місія компанії – створення універсального програмного забезпечення, що охоплює всі області життєдіяльності та сприяє підвищенню соціальних стандартів, поліпшенню якості життя в цілому. [2]

1.2 Характеристика і структура об’єкта впровадження

Компанія «УнІТ» відіграє ключову роль при проектуванні, розробці та впровадженні комп'ютерних систем і програмно-апаратних комплексів клієнтів.

Характеристика компанії «УнІТ» полягає у розробці програмного забезпечення, а саме створення клієнтських програмних рішень та розробки програмного забезпечення як прикладного, так і корпоративного. [3]

Співробітники компанії надають технологічний та правовий консалтинг для клієнтів, де надають оцінку та можливі шляхи покращення бізнес-процесів. Описують для клієнтів стратегії впровадження цифрових та комп'ютерних систем, а також проводять консультації щодо оптимізації та модернізації наявних ІТ-інфраструктур клієнтів.

При розробці комп'ютерних і цифрових систем співробітники компанії проводять дослідження потреб користувача, складають план з розробки та тестування інтерфейсів користувача, а також контролюють взаємодії між користувачами та технічною підтримкою клієнта.

Компанія відповідає за проектування електронного документообігу у компанії, а також проводить обробку та аналіз потоків даних. Співробітники виконують роботи із забезпечення якості систем, шляхом автоматизованого та ручного тестування програмного забезпечення, що розробляється, та верифікації програмних продуктів.

«УнІТ» надає послуги з навчання персоналу, співробітників та клієнтів. Навчання являє собою організацію та проведення тренінгів та семінарів, а також у наданні курсів для підвищення кваліфікації працівників.

Це дозволяє компанії надавати комплексні послуги, які допомагають клієнтам досягати своїх бізнес-цілей, покращувати операційну ефективність та впроваджувати нові проектні рішення.

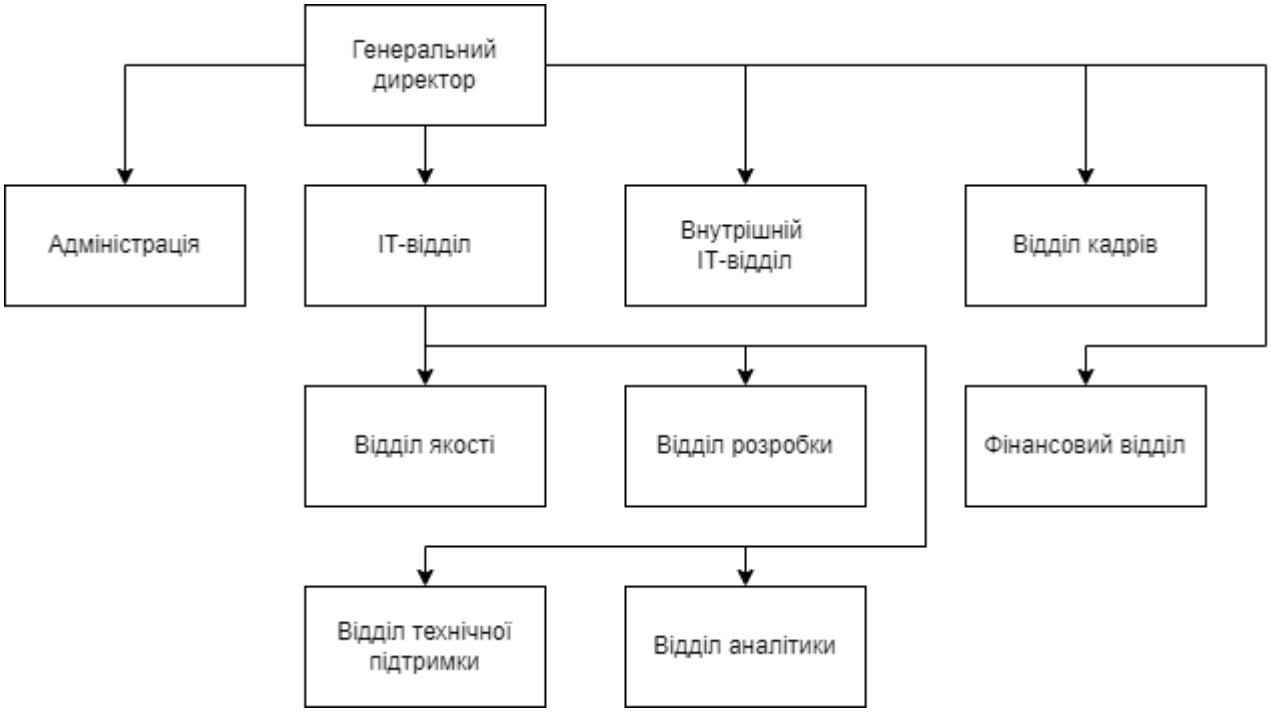

Рисунок 1.1 – Схема організаційної структури компанії

На рисунке 1.1 представлена схема організаційної структури компанії, на якій виділені такі відділи:

- генеральний директор;
- адміністрація – включає директорів, секретарів та заступників;
- фінансовий відділ – включає фінансистів та юристів;
- IT-відділ – включає розробників, QA-інженерів, аналітиків та техпідтримку;
- внутрішній IT-відділ – включає мережевих інженерів та розробників для власних потреб компанії;
- відділ кадрів – включає в себе менеджерів з персоналу;
- фінансовий відділ – включає бухгалтерів та юристів.

Топографічне розміщення структурних відділів компанії знаходиться в одному будинку. Офіс розташований за адресою м. Київ, вул. Велика Васильківська 55, 03150. Географічне розташування представлене на малюнку нижче (Рисунок 1.2).

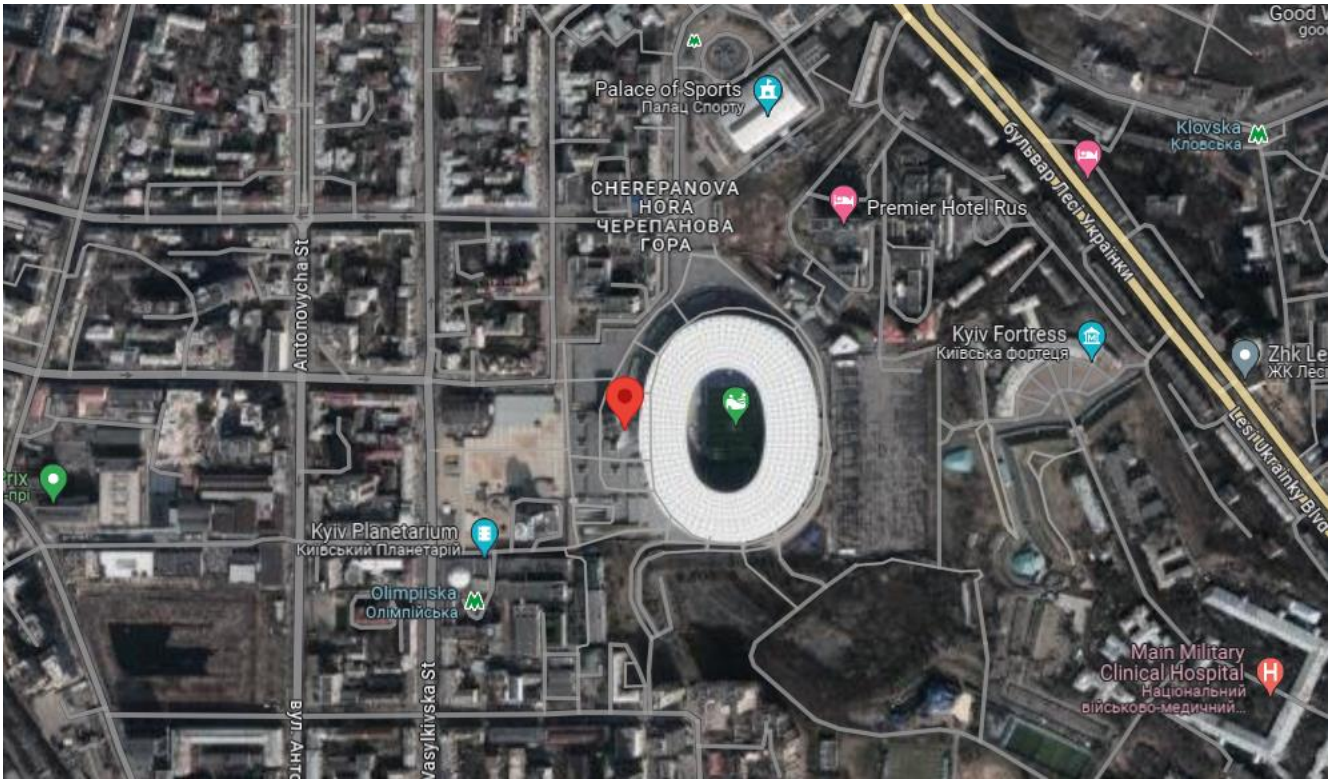

Рисунок 1.2 – Географічне розташування структурних підрозділів

1.3 Стислі відомості про технології збору та передачі інформації для КС підприємства «Універсальні інформаційні технології»

Оскільки це діюча IT-компанія, на момент написання роботи компанія вже мала комп'ютерну систему. Існуюча комп'ютерна система мала недоліки. Єдиної спільної мережі для компанії не існувало. Не було можливості підключити співробітників з домашнього офісу. Вся інформація переносилася на USB-флешки, а бази співробітників зберігалися на комп'ютерах HR-співробітників.

Принципи, методики та математичні методи проектування та розробки інформаційного забезпечення корпоративної системи підприємства «УнІТ» включають сукупність математичних моделей, а також алгоритми розв'язання задач обробки інформації з використанням обраних інформаційних технологій. Крім того, вони включають в себе набір інструментів і методів, що дозволяють створювати економіко-математичні моделі для завдань управління.

Розробка математичної моделі завдань управління доручається фахівцям з організаційно-технологічних рішень, які постачають завдання управління, а також фахівцям з формалізації процесу прийняття управлінських рішень.

Необхідні спрощення в розробленому бізнес-процесі повинні бути в достатній мірі обґрунтовані, щоб уникнути втрат в корисності результатів.

Для поліпшення бізнес-процесів залучається системний аналітик, який оцінює всі можливі потоки даних, а також розробляє електронний документообіг компанії. Впровадження електронного документообігу дозволить заощадити ресурси, прискорити обмін даними, а також скоротити час очікування погодження необхідних документів, таких як заява на відпустку, або заявка на закупівлю господарських ресурсів. Спроектована комп'ютерна мережа дозволить впровадити таку систему електронного документообігу.

Найбільшого поширення в проектуванні набули мережеві методи. Вони дозволяють визначати параметри мережевих моделей і аналізувати хід робіт по виконанню виробничих планів. В рамках мережевого моделювання можлива однокритеріальна або багатокритеріальна оптимізація, що включає оптимізацію за часом і використовуваними ресурсами.

1.4 Огляд існуючих інженерних рішень КС в галузі

Для більш правильного проектування комп'ютерної системи необхідно вивчити наявні технічні та інженерні рішення, які використовуються на підприємстві.

Розробники та тестувальники реєструють та фіксують завдання/баги в IT-проекті або IT-продукті, що розробляється та підтримується.

Аналітики складають технічну та проектну документацію для IT-проектів або IT-продуктів, які розробляються та підтримуються.

Менеджери з персоналу заповнюють особові картки працівників, дублюють дані в електронних таблицях.

Фінансовий відділ веде облік бюджету проектів і компанії, а також веде облік витрат на підтримку компанії.

Служба прибирання номерів веде облік фінансового стану компанії, а також складає список речей, необхідних для покупки або заміни.

Адміністрація компанії і генеральний директор ведуть облік корпоративної документації, а також підписують заяви і документи.

1.5 Завдання і мета роботи

Метою роботи є побудова комп'ютерної системи установи «УнІТ» з можливістю безпечного віддаленого доступу до мережевих пристроїв в рамках корпоративної мережі.

Для досягнення поставленої мети в роботі повинні виконуватися наступні завдання:

- Аналіз потреб компанії та її інфраструктури;
- Формулювання технічних вимог до мережі;
- Підбір мережевої архітектури та обладнання;
- Розробка специфікацій обладнання;
- Налаштування мережевого обладнання;
- Тестування мережі та її компонентів.

1.6 Визначення можливих напрямків рішення поставлених задач

Для виконання поставлених завдань розглядається використання програмно-апаратних засобів від однієї з провідних компаній в області мережевих рішень - Cisco Systems.

Компанія Cisco Systems є лідером серед постачальників мережевого обладнання. До особливостей цього постачальника можна віднести:

- цілодобова клієнтська підтримка;
- повна і вичерпна документація на всю продукцію, що випускається і поставляється;
- наявність програмного забезпечення на базі Cisco IOS;
- наявність функцій мережевої безпеки (налаштування VPN);
- наявність та проведення курсів для підвищення кваліфікації користувачів;
- активний розвиток у сфері інформаційної безпеки.

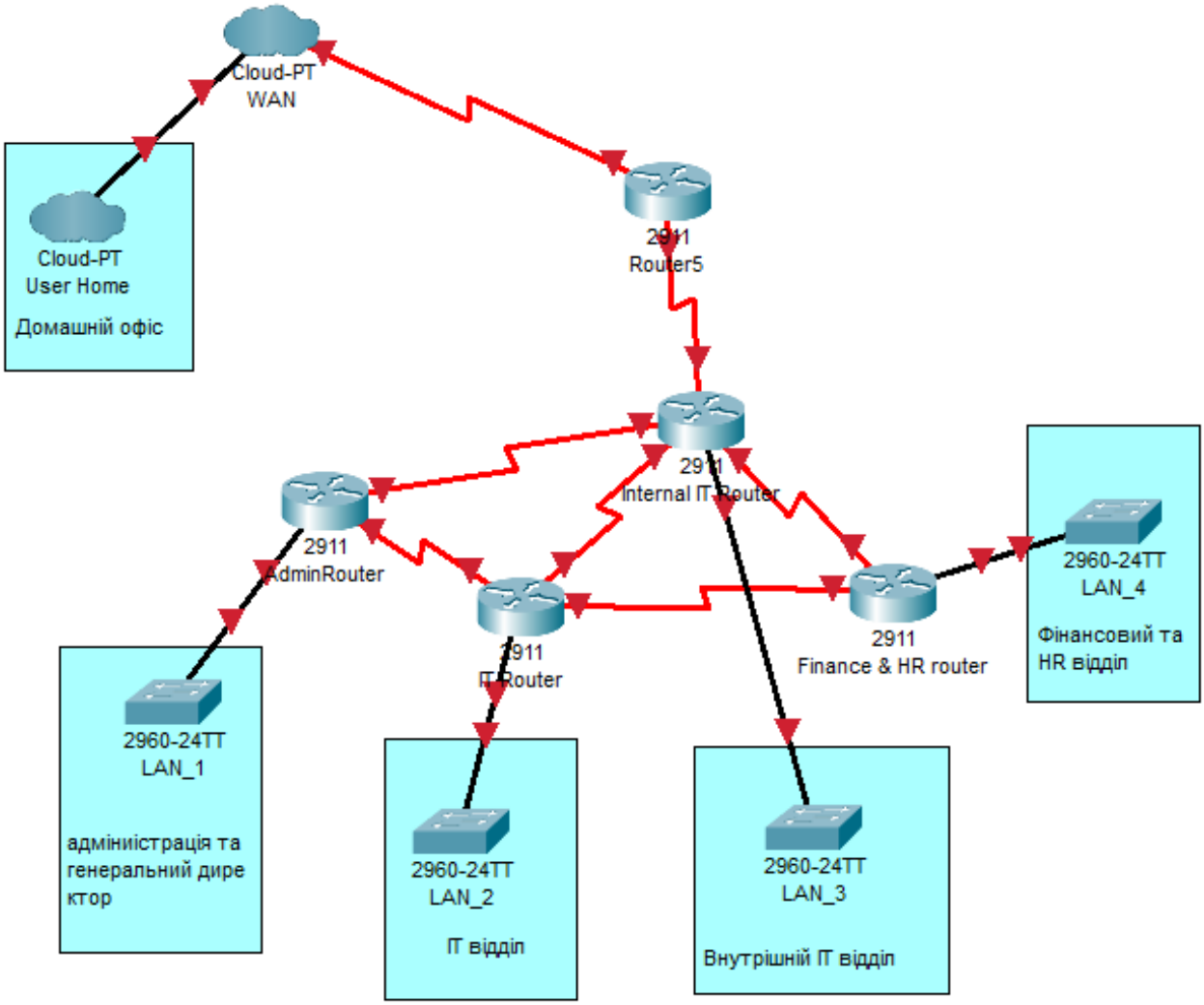

Рисунок.1.3 – Концептуальна схема комп'ютерної мережі

На рисунке 1.3 представлена концептуальна схема комп'ютерної мережі, де видно, що для компанії виділено 4 локальних мереж, плюс вказана можливість віддаленого підключення співробітника з домашнього офісу:

- LAN_1 – локальна мережа адміністрації та генерального директора;
- LAN_2 – локальна мережа IT-відділу;
- LAN_3 – локальна мережа внутрішнього IT-відділу;
- LAN_4 – локальна мережа фінансового та кадрового відділів;
- Домашній офіс - це домашня локальна мережа співробітника, що підключається до комп'ютерної мережі компанії.

На концептуальній схемі також видно, що за доступ до інтернету, а також доступ до комп'ютерної мережі компанії відповідає внутрішній IT-відділ.

2 ТЕХНІЧНІ ВИМОГИ ДО КОМП’ЮТЕРНОЇ СИСТЕМИ

2.1 Вимоги до системи в цілому

Система повинна забезпечити:

- підключення до мережі Інтернет для всіх комп'ютерів у мережі;
- Wi-Fi доступ для адміністрації і генерального директора;
- налаштування безпеки для різних ділянок мережі;
- доступ до файлового сервера компанії, на якому зберігатимуться всі звіти протягом 5 років і більше;
- цілодобовий доступ до серверів компанії з мережі Інтернет.

2.1.1 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему і режиму його роботи

Кількість співробітників для обслуговування комп'ютерної системи – 4 системних адміністратора (мережевих інженерів). Системний адміністратор повинен мати неповну або закінчену вищу освіту в галузі інформаційних технологій, або середню професійну освіту в галузі інформаційних технологій.

Для забезпечення доступності комп'ютерної системи необхідно ввести зміни для мережевих інженерів цілодобово: нічні та денні. Про всі зміни необхідно звітувати.

2.1.2 Вимоги до надійності

Вимоги до надійності комп'ютерної системи включають в себе наступні аспекти:

- система повинна продовжувати працювати в разі виходу з ладу одного або декількох компонентів, а також мати резервні компоненти і механізми для швидкого відновлення;
- система повинна самовідновлюватися після збоїв, а час, необхідний для відновлення системи до нормального стану після збою, повинен бути скорочений;

- система повинна вміти справлятися зі збільшенням навантаження без шкоди для продуктивності;
- система повинна бути доступною для збільшення кількості обчислювальних компонентів без зміни архітектури;
- система повинна протистояти помилкам, викликаним діями користувача або адміністратора, а також повинна забезпечувати механізми запобігання і виправлення помилок, пов'язаних з людською помилкою.

2.1.3 Вимоги безпеки

Мережеві компоненти повинні мати високий рівень захисту налаштувань.

Доступ до сервера повинен бути наданий тільки уповноваженим особам. На всіх комп'ютерах і серверах в мережі має бути встановлено і запущено антивірусне програмне забезпечення. Антивірус використовуються для виявлення та нейтралізації кіберзагроз.

Повний доступ до комп'ютерної системи повинні мати лише користувачі групи Адміністратор. Робота користувачів мережі передбачає використання облікових записів з використанням логіна і пароля облікового запису.

2.1.4 Вимоги до ергономіки та технічної естетики

Вимоги до ергономіки і технічної естетики наступні:

- робоче місце користувача має бути добре освітлене;
- офіси повинні добре провітрюватися;
- Інтернет і телефонні кабелі повинні бути заховані в коробки;
- кабелі повинні мати маркування на обох кінцях;
- мережеве обладнання повинно встановлюватися в спеціальні стійки;
- мережеве обладнання повинно розташовуватися в місцях для швидкого доступу компетентних співробітників.

2.1.5 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи

Використання роутера з можливістю підключення провайдера за допомогою оптоволокна і має 8 портів для підключення комутаторів або бездротових точок доступу.

Напруга мережі має бути 220 В, 50 Гц.

Нормальними кліматичними умовами для роботи системи є:

- температура навколишнього середовища +15 - +25ºС;
- Відносна вологість навколишнього повітря в повітряній атмосфері становить 75%;
- атмосферний тиск 740 – 770 мм рт.ст.

Система повинна зберігати працездатність під впливом наступних кліматичних факторів:

- температура навколишнього повітря +10 °С – +45 °С;
- відносна вологість повітря 40 – 80% при температурі +10°С.

2.1.6 Вимоги до захисту інформації від несанкціонованого доступу

Для проектованої комп'ютерної системи описані наступні вимоги до захисту інформації від несанкціонованого доступу:

- Організаційні заходи:
- необхідно розробити та впровадити внутрішні політики безпеки, які визначають правила та процедури захисту інформації.
- необхідно планувати регулярне навчання співробітників принципам інформаційної безпеки та методам захисту даних.
- необхідно обмежити доступ до інформації на підставі посадових обов'язків (рольова модель доступу).
- необхідно розробити та впровадити процедури для виявлення, обліку, реагування та вирішення інцидентів інформаційної безпеки.
- Технічні заходи:
- для захисту даних необхідно використовувати криптографічні методи.

- необхідно запровадити суворі механізми авторизації.
- регулярно оновлюйте та використовуйте програмне забезпечення для захисту від зловмисного програмного забезпечення.
- резервне копіювання даних має здійснюватися регулярно, щоб запобігти втраті інформації.

- Фізичні заходи:
- необхідно обмежити фізичний доступ до приміщень з важливою інформацією (використання систем контролю доступу, відеоспостереження тощо).
- необхідно забезпечити фізичну безпеку серверів, робочих станцій та іншого обладнання (захист від крадіжки, пошкодження, доступу сторонніх осіб).

2.1.7 Вимоги до схоронності інформації при аваріях

На серверах повинна бути встановлена система резервного копіювання, а також повинна бути можливість відновлення системи на основі раніше створених резервних копій.

2.1.8 Вимоги до захисту від впливу зовнішніх чинників

Серверна кімната повинна добре провітрюватися, а в приміщенні підтримуватися нормальні кліматичні умови.

Всі електроприлади і електрична мережа повинні бути заземлені.

2.1.9 Додаткові вимоги

У комп'ютерній мережі повинні використовуватися кабелі UTP категорії 5 або 6. Розетки повинні бути заземлені. Мережеве обладнання повинно мати близько 20% вільних портів для можливого розширення комп'ютерної мережі.

2.2 Вимоги до функцій, які виконує КС

До проектованої комп'ютерної системи підприємства «УнІТ» описані наступні вимоги:

- корпоративні дані збираються та зберігаються всередині комп'ютерної системи;
- усередині комп'ютерної системи аналізуються зібрані дані;
- комп'ютерна система формує звіти та формує корпоративні документи.

2.2.1 Вимоги до видів забезпечення КС

2.2.1.1 Вимоги до інформаційного забезпечення

Вимоги до інформаційного забезпечення комп'ютерної системи описані нижче:

- Вимоги до даних:
  - Дані повинні бути зібрані і збережені в системі (повнота);
  - дані повинні своєчасно оновлюватися і відповідати поточному стану об'єктів управління (актуальності);
  - дані повинні бути точними і достовірними, без помилок і спотворень (точність і достовірність);
  - дані повинні відповідати завданням, які вирішує система, і бути корисними для користувачів (актуальність);
- Вимоги до організації даних:
  - дані повинні бути організовані відповідно до логічної та фізичної структурою системи (структуровані);
  - Дані повинні бути представлені в стандартизованих форматах, які забезпечують сумісність і обмін між різними системами за допомогою можливого надання API.
- Вимоги до зберігання даних:
  - повинні бути вжиті заходи для захисту даних від несанкціонованого доступу, втрати та пошкодження;
- Вимоги до доступа до даних:
  - вам потрібно встановити дозволи для різних користувачів і груп користувачів на основі їхніх ролей;

- система повинна надавати зручні та інтуїтивно зрозумілі інтерфейси для доступа до даних (API, веб-інтерфейси, додатки тощо);
- журнали доступу та активності даних повинні вестися для моніторингу активності та аналізу безпеки.

2.2.1.2 Вимоги до програмного забезпечення

Проектована комп'ютерна система повинна забезпечувати технічну та програмну підтримку, а також обслуговування мережевої версії програмного комплексу. Програмний комплекс складається з 5 серверів:

- Сервер FTP;
- Сервер HTTP;
- Сервер баз даних;
- Сервер звітів;
- Сервер системи обліку.

2.3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

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

Корпоративна мережа «УнІТ» дозволяє створити єдину базу даних для всіх підрозділів, вести електронний документообіг, організовувати конференц-зв'язок та відеоконференції, мати доступ до мережі Інтернет та інших інтерактивних мереж. Корпоративна мережа об'єднає офісні підрозділи підприємства, створивши єдиний корпоративний інформаційний простір.

До технічних засобів комп'ютерної системи належать:

- маршрутизатор;
- комутатори;
- комутація мережі за допомогою кабелів і бездротових адаптерів;
- вузли (робочі місця, робочі місця);

– корпоративні сервери.

З огляду на невеликий розмір мережі, в маршрутизаторах «УнІТ» будуть об'єднані ядро і розподільні шари.

Структурна схема комплексу технічних засобів комп'ютерної системи компанії «УнІТ» наведена на рисунку 2.4. На малюнку можна побачити, що виділяється 1 рівень ядра і 1 рівень доступу (рівні доступу винесені окремими частинами, але концептуально вони являють собою одне ціле).

Первинний рівень, або основний рівень, складається з п'яти маршрутизаторів, з'єднаних мережами WAN. Також на цьому рівні відбувається перемикання та маршрутизація трафіку компанії.

Доступ до співробітників віддаленої мережі Home Office буде здійснюватися за допомогою технології VPN. Прикордонний маршрутизатор або маршрутизатор Office, який підключає проектовану мережу до Інтернету.

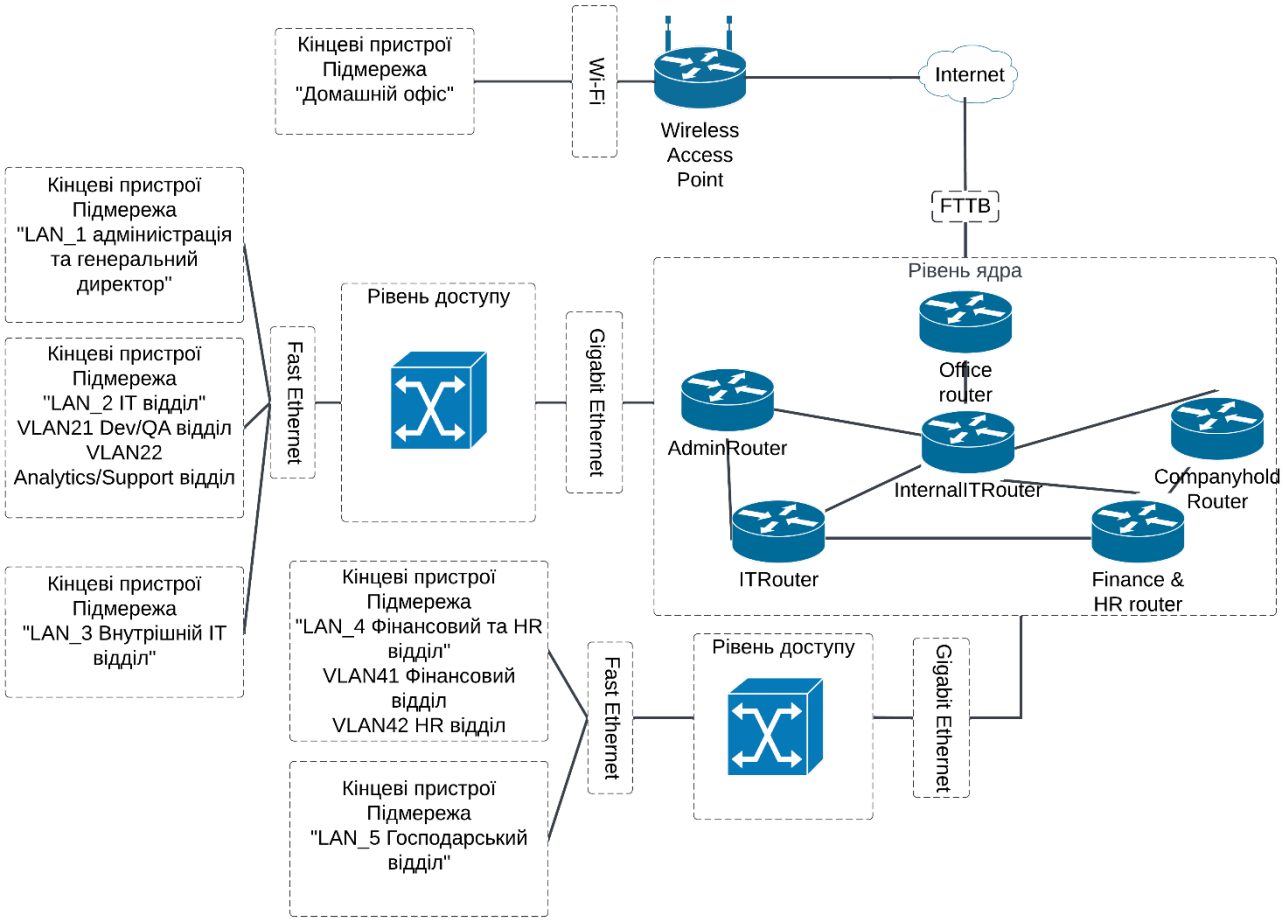

Рисунок 2.4 – Структурна схема комплексу технічних засобів комп'ютерної системи підприємства «УнIT»

Рівень доступу до мережі передачі даних складається з 5 комутаторів. Комутатори забезпечують локальні підмережі локальної мережі та VLAN. Комутатор передає дані безпосередньо одержувачу, що дозволяє підвищити продуктивність в комп'ютерній мережі, а також підвищити безпеку мережі за рахунок обмеження переміщення пакетів даних.

Для підмереж з великою кількістю вузлів виділяються віртуальні підмережі. Це стосується підмереж LAN_2 IT Viddil та LAN_4 Finance & HR Viddil. У цих підмережах є 2 виділені VLAN:

– LAN_2 IT відділ:
– VLAN21 Dev/QA відділ;
– VLAN22 Analytics/Support відділ;
– LAN_4 Фінансовий & HR відділ:

– VLAN41 Фінансовий відділ;

– VLAN42 HR відділ.

У підмережі «LAN_3 Internal IT Viddil» користувачі підключаються до мережі за технологією PAgP, що забезпечує збільшення пропускної здатності та надійності каналу передачі даних.

На рівні доступу використовується технологія передачі даних Fast Ethernet, а на базовому рівні - технологія передачі даних Gigabit Ethernet і Serial. Для доступу до віддаленої мережі використовується технологія Fiber-to-the-building (FTTB).

2.3.2 Розробка специфікації апаратних засобів КС

Побудувати комп'ютерну мережу компанії «УнІТ» Комутатори потрібні для зв'язку між вузлами всередині локальних підмереж і маршрутизаторами для з'єднання окремих підмереж і організації зв'язку між ними.

В якості комутаторів для використання в локальних підмережах був обраний Cisco Catalyst 9200. Комутатор цієї серії підтримується компанією Cisco Systems і рекомендований для використання в IT-компаніях середнього розміру.

Підключайте робочі станції до мереж Fast Ethernet і Gigabit Ethernet зі швидкістю середовища передачі, щоб задовольнити зростаючі потреби в пропускній здатності на периферії. В агрегації використовуються комбіновані гігабітні порти висхідного зв'язку, які можна об'єднати в один канал за допомогою технології Gigabit EtherChannel. Дана серія комутаторів орієнтована в першу чергу на малий і середній бізнес, а також філії великих компаній для вирішення завдання реалізації мережевого рівня доступу. Сімейство Catalyst 9200 забезпечує високий рівень безпеки даних завдяки вбудованим NAC, підтримці QoS і високому рівню відмовостійкості системи.

Технічні характеристики Cisco Catalyst 9200 має 24 порти. Оптимізовано для дротового та бездротового доступу Wi-Fi 6/6E та развертывания сетей с высокой пропускной способностью. 16 портов 1G, 8 портов 10GBASE-T, 10G/5G/2.5G/1G мультигигабитные, 1000M/100M, заменяемые источники

питания и вентиляторы. Заменять источники питания и вентиляторы можно в рабочем состоянии.

Протокол віддаленого адміністрування: RMON, HTTP, TFTP; метод аутентифікації: RADIUS. Комутатори та маршрутизатор поставляються зі стандартною операційною системою Cisco IOS.

Ці особливості роблять C9200-24PXG ідеальним для підприємств, яким потрібна висока пропускна здатність і гнучкість для розгортання мережевої інфраструктури, що підтримує сучасні стандарти і технології.

Для реалізації ядра мережі доцільно вибирати маршрутизатори з сервісною інтеграцією для невеликих офісів із серії Cisco ISR 4000.

Cisco ISR 4461 пропонує комбіновану пропускну здатність до 1,5 Гбіт/с (за замовчуванням) і до 3 Гбіт/с з ліцензією на продуктивність, а також понад 7 Гбіт/с з ліцензією на прискорення CEF. Він має 3 слоти для розширених сервісних модулів, 2 слоти для модулів подвійної ширини, 3 слоти NIM, підтримує всі модулі вводу/виводу з можливістю гарячої заміни та один вбудований слот ISC. Оперативна пам'ять за замовчуванням становить 8 ГБ для контролера та служб, з максимальною ємністю до 4 ГБ та 32 ГБ відповідно. Флеш-пам'ять за замовчуванням становить 8 ГБ з можливістю розширення до 32 ГБ. Також є 2 зовнішні порти USB 2.0, порт консолі USB і послідовні порти. Варіанти живлення включають внутрішній змінний, постійний струм і PoE з резервним живленням від змінного, постійного струму та PoE. Габарити пристрою становлять 3,5 x 17,25 x 18,5 дюймів (88,9 x 438,15 x 469,9 мм), вага – 10,2 кг, а середнє напрацювання на відмову (MTBF) – 480770 годин.

Маршрутизатори цієї моделі також підтримують технології інкапсуляції IPv4, IPv6, OSPF, RIP/RIPv2, IGMPv3, AAA, VPN, GRE, Ethernet, 802.1q VLAN, PPP і PPPoE. Також підтримуються системи та технології QoS, а також ієрархічний QoS. Підтримувані криптографічні алгоритми: DES, 3DES (шифрування), RSA (аутентифікація), MD5, SHA, SHA-256 (перевірка цілісності даних).

Таблица 3.1 – Технічні характеристики мережевого обладнання

Позиція	Найменування та технічні характеристики	Тип, марка, позначення документа	Одиниця вимірювання	Количество
1	2	3	4	5
1	Cisco ISR 4461 500Mbps-1Gbps пропускна здатність, 4 WAN/LAN портов, 4 SFP портов, Intelligent WAN, OnePK, AVC [2]	Office_router It_router Admin_router Internal_it_router Finance_hr_router Companyhold_router	шт	6
2	Cisco 9200-24PXG 16 портів 1G, 8 портів 10GBASE-T, 10G/5G/2.5G/1G, 1000M/100M [3]	Admin_switch It_switch Internal_it_switch_1 Internal_it_switch_2 Finance_hr_switch Companyhold_switch	шт	6

2.4Розробка архітектури мережі підприємства

Архітектура мережі складається з декількох важливих компонентів:

– топологія мережі;

– лінійна кабельна інфраструктура;

– мережеві протоколи;

– активне мережеве обладнання (комутатори, маршрутизатори).

При проектуванні комп'ютерної системи компанії «УнІТ» була обрана логічна топологія мережі - «ієрархічна зірка».

Основною мережевою технологією є Ethernet.

Для з'єднання вузлів використовується технологія Fast Ethernet, а для з'єднання між маршрутизаторами і комутаторами – GigabitEthernet.

Корпоративна мережа «УнІТ» побудована на дворівневій ієрархічній моделі (верхній рівень – ядро, нижній – рівень розподілу) з урахуванням невеликих розмірів мережі. Основний рівень буде реалізований маршрутизаторами і зв'язком між ними, рівень доступу буде реалізований комутаторами.

Основний рівень, на якому здійснюється комутація трафіку, складається з шести маршрутизаторів (R0-R4), підключених до інтернету. Локальний доступ підмережі до ядра здійснюються за допомогою технології передачі даних GigabitEthernet. Через прикордонний маршрутизатор рівня ядра R4 проектується мережа підключається до Інтернету. Підмережа «УнІТ» – це мережа, доступ до якої здійснюється через Інтернет за допомогою технології передачі даних Fiber-to-the-building (FTTB).

Корпоративна мережа має єдиний IP-адресний простір 192.168.27.0/21. Підмережі IP поділяються маршрутизаторами на 4 підмереж. Для адресації використовується IPv4. Доступ до мережі Інтернет для співробітників компанії забезпечується за технологією NAT.

Маршрутизатор Office_router – це периферійний маршрутизатор, розташований у серверній кімнаті. Протокол динамічної маршрутизації пакетів OSPF використовується для забезпечення маршрутизації пакетів у межах комп'ютерної мережі.

Маршрутизатор It_router и Finance_hr_router используют технологию инкапсуляцииVLAN Tagging, описанную в стандарте IEEE 802.1q. [5] Для каналов между маршрутизаторами применяется адресный пул 10.0.19.0/24.

Рівень доступу в область передачі даних складається з 5 комутаторів, які забезпечують формування підмереж LAN і VLAN. Використання комутатора дозволяє домогтися передачі даних безпосередньо адресату, що дозволяє підвищити продуктивність і безпеку мережі, так як немає можливості для інших сегментів мережі перехоплювати і зчитувати чужі дані.

Бездротовий маршрутизатор встановлюється в підмережу «LAN_1 Адміністрація і генеральний директор» з метою забезпечення бездротового зв'язку генерального директора компанії. Мережевий принтер також розташований у підмережі.

Відеопідмережа «LAN_2 IT» має комутатор, робочі станції та сервер віртуальних машин. Комутатор налаштований на поділ підмережі на 2 віртуальні підмережі за технологією VLAN.

У «LAN_3 внутрішня підмережа IT-відео» є два перемикачі. Це дозволить використовувати технологію PAgP. Оскільки внутрішній IT-відділ відповідає за за забезпечуючи доступ до мережевих ресурсів компанії, очікується, що в цьому сегменті мережі буде великий потік даних, а технологія PAgP збільшить пропускну здатність цієї підмережі. Ця підмережа містить HTTP і FTP-сервер і DNS-сервер.

Підмережа «LAN_4 Фінанси та HR Відділ» має комутатор, робочі станції, 2 сервери та 2 мережеві принтери. Комутатор налаштований на поділ підмережі на 2 віртуальні підмережі за технологією VLAN. VLAN41 розділяє підмережі для фінансового відділу, а VLAN42 розділяє підмережу для відділу кадрів. Ця підмережа включає сервер баз даних, а також сервер звітів.

Також архітектура комп'ютерної мережі «УнІТ» враховує співробітників, які працюють з домашнього офісу.

Кінцевими вузлами комп'ютерної мережі є комп'ютери/робочі станції та сервери. На робочих місцях попередньо встановлено програмне забезпечення, необхідне для роботи на його посаді.

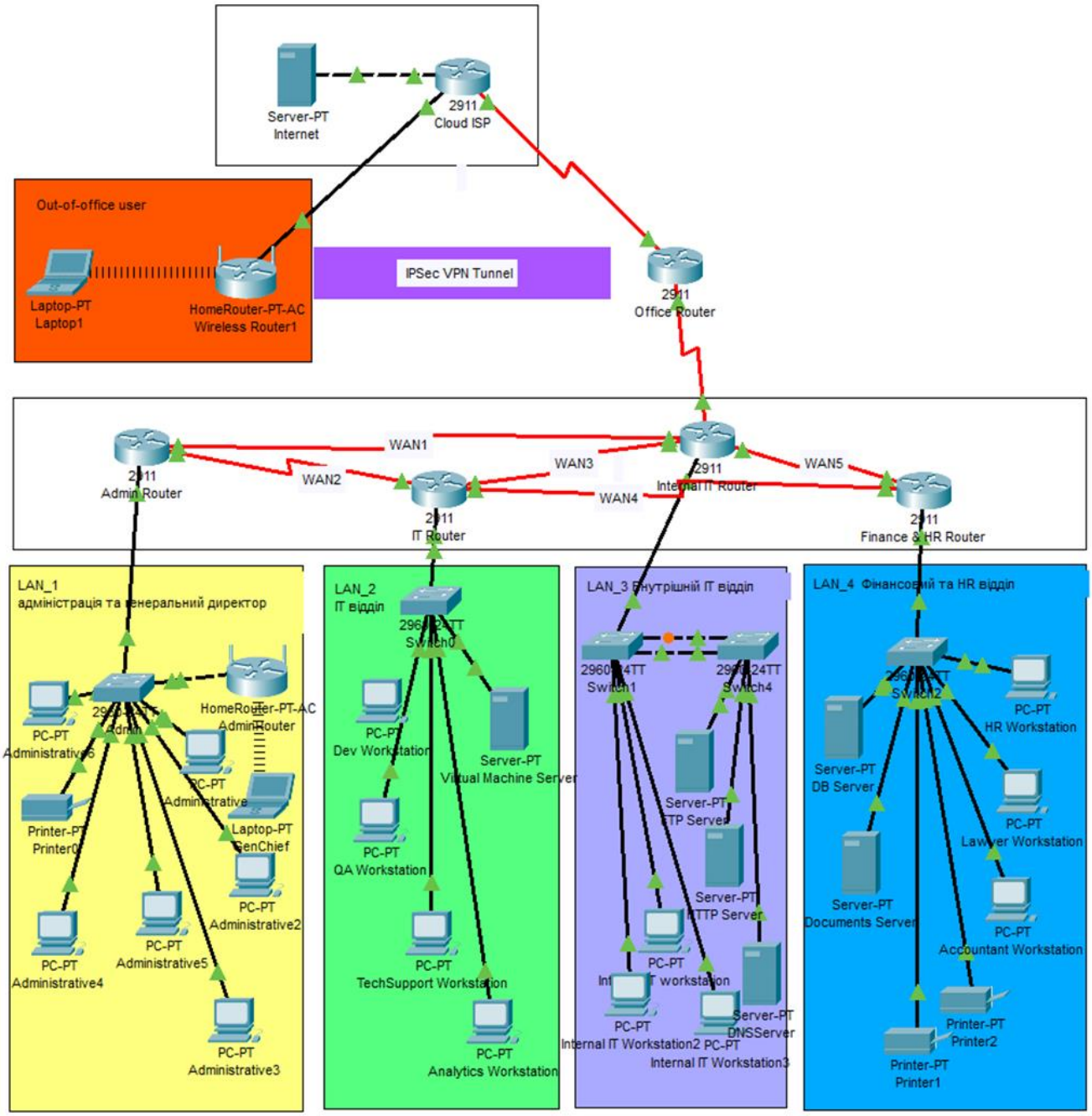

Рисунок 2.5 – Архітектура мережі компанії «УнІТ»

2.5 Розробка фізичної топологічної схеми корпоративної мережі

В рамках робіт планується підключити: 50 абонентів даних на території основного корпусу, 1 віддаленого співробітника, 3 принтери, 6 сервери, 5 роутерів і 5 комутаторів.

Об'єктами обслуговування мережевого сегмента компанії є учасники процесу обміну даними в наступних відділах: «Адміністрація та генеральний

директор», «IT-департамент», «Внутрішній IT-відділ», «Фінансовий та кадровий відділ».

Фізична топологія мережі – це схематичне зображення фізичного розташування компонентів мережі та зв'язків між ними. Він описує, як мережеві пристрої, такі як комп'ютери, сервери, маршрутизатори, комутатори та кабелі, фактично з'єднані один з одним у фізичному просторі. Важливо зазначити, що фізична топологія відрізняється від логічної топології, яка описує, як дані протікають через мережу незалежно від фізичного розташування пристроїв.

В якості базової мережевої технології обрана технологія Ethernet. Кабельна інфраструктура повинна відповідати стандартам TIA/EIA-568-A та TIA/EIA-569. Прокладка кабелю всередині будівлі здійснюється за типом кабелю «неекранована кручена пара» або кабелю UTP категорії 5e, що забезпечує високу надійність і швидкість передачі даних в поєднанні з високою технологічністю. Максимальна довжина кабелю – 100 м. Така довжина відповідає вимогам і не погіршує продуктивність передачі даних.

Волоконна оптика використовується для підключення будівлі до інтернету. Волоконно-оптичний кабель SC G657A застосовується між будівлями. Даний кабель може використовуватися на опорах повітряних ліній зв'язку, міського електротранспорту і повітряних ліній електропередачі при впливі навантажень від вітру, льоду, температури і їх комбінацій. Використовуються роз'єми SC SM MM, також цей кабель можна використовувати для прокладки мережі між будівлями.

Підключення WAN між маршрутизаторами відділів вимагає використання технології передачі даних Serial DCE/DTE. Глобальна мережа використовує послідовний кабель DCE CAB-6060X для послідовних інтерфейсів.

Роутер і сервер розміщуються в серверній кімнаті з точки зору безпеки. Сервер розташований у серверній стійці Hexagona 42U (2055x800x1000 мм) з перфорованими дверцятами. Приміщення обладнане системою вентиляції та

джерелами безперебійного живлення. Кабель прокладається за допомогою металевих коробів, які забезпечують точки доступу для кожної кімнати.

2.6 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

У підмережі «LAN_1 Адміністрація та CEO» розташований комутатор Cisco 9200-24PXG та маршрутизатор Cisco ISR 4461, які об'єднують ПК співробітників IT-відділу. Вихідний трафік спрямовується на маршрутизатор Cisco ISR 4461 по лінії смуги пропускання 1000 Мбіт/с.

Щоб не перевантажувати комутатор, швидкість вхідних пакетів не повинна перевищувати швидкість, з якою пакети відправляються з комутатора. Передбачається, що мережа передбачає роботу всіх користувачів. Середня інтенсивність трафіку

Середня інтенсивність трафіку μ=124 кадрів/с, а середня довжина повідомлення – 1КБ.

Припустимо, що всі користувачі користуються послугами одночасно. Розрахуємо пропускну здатність LAN_1, який складається з 34 вузлів. Пропускна здатність мережі на рівні доступу дорівнюватиме:

$$P_{p.p} = \mu \cdot L_{\text{пов}} \cdot N \cdot 8 = 124 \cdot 1024 \cdot 34 \cdot 8 = 32.94 \text{ Мбіт/с} \quad (3.1)$$

где N – кількість вузлів у мережі;

$L_{\text{пов}}$ – середня довжина повідомлення.

Отримані результати не перевищують заданих параметрів мережі на вихідному каналі, тому перевантажень не буде.

Комутатор рівня доступу перенаправляє трафік на маршрутизатор через вихідний порт зі швидкістю передачі даних 100 Мбіт/с.

Сумарне навантаження на комутатор не повинна перевищувати:

$$\mu_{\text{вих}} = \frac{100\,000\,000}{1024 \cdot 8} = 8192 \text{ пакетів/с} \quad (3.2)$$

Оскільки кожне джерело виробляє в середньому 124 пакетів/с, кількість з'єднань, якими комутує рівень доступу, обмежена:

$$N = \frac{\mu_{\text{вих}}}{\mu} = \frac{8192}{124} = 67 \text{ джерел} \quad (3.3)$$

Це задовольняє найбільшу мережу з 34 ПК.

Кожен з 34 ПК відправляє поток запитів при 124 FPS.

Інтенсивність вихідного трафіку:

$$\lambda = N \cdot \mu = 34 * 124 = 4216 \text{ пакетів/с} \quad (3.4)$$

Коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu_{вих}} = \frac{4216}{8192} = 0.503 \text{ с} \quad (3.5)$$

Рівень зайнятості перемикача рівня доступу:

$$\rho_{\text{зай}} = \frac{\rho}{(1-\rho)} = \frac{0.503}{(1-0.503)} = 1.01 \quad (3.6)$$

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

$$T = \frac{1}{(\mu_{\text{вих}}-\lambda)} = \frac{1}{(8192-4216)} = 2.51 \cdot 10^{-4}\text{с} = 251 \text{ мкс} \quad (3.7)$$

Середня довжина черги:

$$L_{\text{чер}} = \frac{\rho^2}{(1-\rho)} = \frac{0.503^2}{(1-0.503)} = 0.509 \quad (3.8)$$

Середній час перебування пакета в черзі:

$$T_{\text{оч}} = \frac{L_{\text{чер}}}{\lambda} = \frac{0.509}{4216} = 1.207 \cdot 10^{-4}\text{с} = 0.1207 \text{ мс} \quad (3.9)$$

Це значення становить менше 6 мс, що задовольняє вимогам.

Пропускна здатність каналу: λ=пропускна здатність =bl

$$\lambda = \frac{\text{пропускна здатність}}{\text{довжина кадру}} = \frac{b}{l} \quad (3.10)$$

$$b = \lambda \cdot l = 4216 \cdot 1024 \cdot 8 = 21923200 \text{ біт/с} = 33.8 \text{ Мбіт/с} \quad (3.11)$$

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

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

3.1 Розрахунок схеми адресації корпоративної мережі

Для розрахунку схеми адресації корпоративної мережі UnIT, відповідно до вимог, використано адресний простір 192.168.19.0/24. Послідовні канали зв'язку між маршрутизаторами використовують адреси діапазону 10.0.19.0/24.

Розрахунок мережевої адресації виконано за допомогою CIDR і VLSM. CIDR (Classless Inter-Domain Routing) – це метод IP-адресації, який дозволяє гнучко керувати IP-простором, минаючи обмеження класичної адресації. CIDR використовує VLSM (маски підмережі змінної довжини) для призначення IP-адрес підмережам на основі їх фактичних потреб, а не за жорсткими класами. За допомогою VLSM мережа спочатку розбивається на підмережі, які потім можна розбити на менші підмережі. Цей процес можна повторювати багато разів для створення підмереж різного розміру.

Для мережі 192.168.19.0/24 перші 24 біти виділяються для мережевої адреси, а решта 8 біт - для адреси хоста. На основі цих даних можна розрахувати кількість вузлів у мережі. Формула розрахунку кількості вузлів у мережі:

$$2^m - 2 \quad (4.1)$$

де m - кількість бітів, виділених вузлам мережі.

Також кількість можливих вузлів можна розрахувати за такою формулою:

$$2^{32-n} - 2 \quad (4.2)$$

где n – маска сети в нотации CIDR.

Для адрес хостів виділяються нульові біти маски мережі. З результату піднесення до степеня два віднімаються два вузли, так як за замовчуванням в мережі завжди є 2 адреси: мережева адреса і широкомовна адреса. Розрахунки показують, що можна створити комп'ютерну мережу, яка підтримує роботу 2046 вузлів.

Необхідно розділити мережу 192.168.19.0/24 на 4 підмережі з кількістю вузлів - 34, 12, 15, 9. Для кожної з підмереж CIDR визначає мінімальну кількість вузлів підмережі, на які вона може бути розділена.

– Для 34 вузлів - мінімум 64;
– На 12 вузлів – мінімум 16;
– На 15 вузлів - мінімум 32;
– На 9 вузлів - мінімум 16.

Згідно з CIDR, підмережа з 64 вузлів має префікс /26, 32 узла – /27, 16 узлов – /28.

Щоб підтримувати кілька підмереж, потрібно виділити 3 біти з виділеної адреси для підмереж. Це можливо завдяки технології CIDR. Для створення підмереж з діапазону 192.168.19.0/24 з використанням 3-х додаткових бітів для маски підмережі нам необхідно оновити маску підмережі з /21 до /24 (21+3). Таким чином, нова маска підмережі стане 255.255.255.0, яка створить 8 підмереж (2^3).

При VLSM спочатку потрібно розділити мережу на рівну кількість підмереж з префіксом /25. Таких підмереж буде 16. Потрібно виділити 4 підмережі з префіксом /25: підмережі з адресою: 192.168.19.0/25, 192.168.19.128/25, 192.168.9.0/25 і 192.168.9.128/25. Потім розділіть підмережу /25 на підмережу /26. Отже, маємо підмережу з адресою 192.168.19.0/26. І така операція проводиться для масок /27, /28, /29.

Далі нам потрібно визначити діапазон адрес (перша та остання адреса) у кожній підмережі. Представляючи кожну адресу та маску підмережі у двійковому файлі, підмережа 192.168.19.0/25 у двійковому виді виглядатиме так:

11000000.10101000.00001000.00000000

11111111.11111111.11111111.10000000

| Адрес мережі | діапазон хостів

Діапазон адреса буде виглядати наступним шляхом:

Перший адрес - 000 0001

Останній адрес - 111 1110

Адрес сеті – 000 0000

Широкомовна адреса – 111 111

Далі необхідно перевести двійкову форму в десяткову.

Отже, мережа 192.168.19.0/25 матиме такі адреси:

- перший адрес – 192.168.19.1/25;
- останній адрес – 192.168.19.126/25;
- широкомовна адреса – 192.168.19.127/25.

За допомогою адреси 192.168.19.0/24 можна виділити 4 підмережі з маскою /25. У таблиці 3.2 нижче наведені можливі мережеві адреси та їх діапазони.

Таблиця 3.2 – Список можливих підмереж

Номер підмережа	Адреса	Діапазон адрес
1	192.168.19.0/24	192.168.19.0 – 192.168.19.63
2	192.168.19.64/24	192.168.19.64 – 192.168.19.127
3	192.168.19.128/24	192.168.19.128 – 192.168.19.191
4	192.168.19.192/24	192.168.19.192 – 192.168.19.255

Таким чином, розділивши вихідний діапазон на 4 підмережі, можна отримати наступні підмережі, кожна з яких має маску /24 і включає в себе 256 адрес (з яких 254 доступні для використання, одна – мережева адреса і одна – широкомовна адреса).

Для порівняння, технологія VLSM виявилася більш точною, що дозволить будувати більш точні підмережі. Точні підмережі дозволять заощадити на використовуваних адресах, а невикористовувані адреси можуть бути легко включені в комп'ютерну мережу.

У таблиці 3.3 наведена схема IP-адресації комп'ютерної мережі «УнІТ», розрахована методом VLSM.

Таблица 3.3 – Схема мережевої адресації за методом VLSM

Ім'я підмережі	Кількість вузлів	Мережева адреса	Маска мережі	Пул адресів
LAN_1 адміністрація та генеральний директор	34	192.168.19.0/26	255.255.255.192	192.168.19.1 – 192.168.19.62
LAN_2 IT відділ	12	192.168.19.64/27	255.255.255.224	192.168.19.65 – 192.168.19.94
LAN_3 внутрішній IT відділ	15	192.168.19.96/27	255.255.255.224	192.168.19.97 – 192.168.19.126
LAN_4 Фінансовий та HR відділ	9	192.168.19.128/28	255.255.255.240	192.168.19.129 – 192.168.19.142
VLAN21	6	192.168.19.64/29	255.255.255.248	192.168.19.65 – 192.168.19.70
VLAN22	6	192.168.19.72/29	255.255.255.248	192.168.19.73 – 192.168.19.78
VLAN41	5	192.168.19.128/29	255.255.255.248	192.168.19.129 – 192.168.19.133
VLAN42	4	192.168.19.136/29	255.255.255.248	192.168.19.137 – 192.168.19.140
VLAN99	4	192.168.19.80/29	255.255.255.248	192.168.19.81 – 192.168.19.86
WAN1	2	10.0.19.0	255.255.255.252	10.0.19.1 – 10.0.19.2
WAN2	2	10.0.19.4	255.255.255.252	10.0.19.5 – 10.0.19.6
WAN3	2	10.0.19.8	255.255.255.252	10.0.19.9 – 10.0.19.10
WAN4	2	10.0.19.12	255.255.255.252	10.0.19.13 – 10.0.19.14
WAN5	2	10.0.11.16	255.255.255.252	10.0.19.17 – 10.0.19.18
IPS сеті Інтернет	30	209.165.203.0	255.255.255.0	209.165.203.1 – 209.165.203.30

Згідно з початковим пулом IP, кількість доступних IP-адрес становить 2046. Відповідно до необхідної кількості ПК, які потрібно об'єднати в мережу, кількість необхідних IP-адрес становить 450, що становить близько 22% доступного адресного простору.

Згідно з технічними вимогами до проектування комп'ютерної системи компанії «УнІТ» необхідно скласти таблицю адресації мережевих пристроїв. VLAN підмережі використовують адресацію кінцевих точок за допомогою протоколу динамічної конфігурації хоста (DHCP). Перші доступні IP-адреси

призначаються інтерфейси маршрутизаторів в локальній мережі, а другі доступні IP-адреси призначаються для комутаційних інтерфейсів.

У таблиці 3.4 нижче наведено адресацію на всіх пристроях комп'ютерної мережі компанії УнІТ. Таблиця заповнюється адресами, виходячи з даних таблиці 3.4, а також на основі логічної топології корпоративної мережі.

Таблиця 3.4 – Схема адресації пристроїв мережі

Ім'я пристрою	Мережевий інтерфейс	IP-адрес	Маска	Шлюз	VLAN
Адміністрація та генеральний директор					
AdminRouter	Gig0/1	192.168.19.1	/26	-	-
	Ser0/1/1	10.0.19.1	/30	-	-
	Ser0/1/0	10.0.19.5	/30	-	-
Admin_switch	Fa0/1	192.168.19.2	/26	192.168.19.1	-
Administrative1-Administrative34	Мережева карта	192.168.19.3 – 192.168.19.37	/26	192.168.19.1	-
Printer	Мережева карта	192.168.19.38	/26	192.168.19.1	-
IT відділ					
It_router	Gig0/0	192.168.19.65	/27	-	-
	Ser0/2/0	10.0.19.6	/30	-	-
	Ser0/2/1	10.0.19.9	/30	-	-
	Ser0/3/0	10.0.19.13	/30	-	-
It_switch	Fa0/6	192.168.19.66	/27	192.168.19.65	-
Dev_pc_1-Dev_pc_6	Мережева карта	192.168.19.67 – 192.168.19.72	/27	192.168.19.65	21
Techsupport_pc_1 – Techsupport_pc_5	Мережева карта	192.168.19.73 – 192.168.19.77	/27	192.168.19.65	22
VM_server	Мережева карта	192.168.19.78	/27	192.168.19.65	-
Внутрішній IT відділ					
Inner_it_router	Gig0/0	192.168.19.97	/27	-	-
	Ser0/2/0	10.0.19.2	/30	-	-
	Ser0/2/1	10.0.19.17	/30	-	-
	Ser0/3/0	10.0.19.10	/30	-	-
	Ser/0/3/1	209.165.203.1	/30	-	-
Inner_it_switch_1	Fa0/4	192.168.19.98	/27	192.168.19.81	-
Inner_it_switch_2	Fa0/1	192.168.19.99	/27	192.168.19.81	-
HTTP_server	Мережева карта	192.168.19.100	/27	192.168.19.81	-
FTP_server	Мережева карта	192.168.19.101	/27	192.168.19.81	-
DNS_server	Мережева карта	192.168.19.102	/27	192.168.19.81	-
Internal_it_pc_1-Internal_it_pc_13	Мережева карта	192.168.19.103 – 192.68.8.115	/27	192.168.19.81	-
Фінансовий та HR відділ					
Finance_hr_router	Gig0/0	192.168.19.129	/28	-	-

Ім'я пристрою	Мережевий інтерфейс	IP-адрес	Маска	Шлюз	VLAN
	Ser0/1/0	10.0.19.18	/30	-	-
	Ser/0/3/0	10.0.19.14	/30	-	-
Finance_hr_switch	Fa0/6	192.168.19.130	/28	192.168.19.113	-
Db_server	Мережева карта	192.168.19.131	/28	192.168.19.113	-
Documentation_server	Мережева карта	192.168.19.132	/28	192.168.19.113	-
Finance_pc_1 – Finance_pc_5	Мережева карта	192.168.19.133 – 192.168.19.137	/28	192.168.19.113	41
Hr_pc_1 – Hr_pc_4	Мережева карта	192.168.19.138 – 192.168.19.141	/28	192.168.19.113	42
Printer_1	Мережева карта	192.168.19.142	/28	192.168.19.113	41
Printer_2	Мережева карта	192.168.19.143	/28	192.168.19.113	42

3.2 Розробка топологічної схеми корпоративної мережі

Фізична топологія мережі – це схематичне зображення фізичного розташування компонентів мережі та зв'язків між ними. Він описує, як мережеві пристрої, такі як комп'ютери, сервери, маршрутизатори, комутатори та кабелі, фактично з'єднані один з одним у фізичному просторі. Важливо зазначити, що фізична топологія відрізняється від логічної топології, яка описує, як дані протікають через мережу незалежно від фізичного розташування пристроїв.

В якості базової мережевої технології обрана технологія Ethernet. Кабельна інфраструктура повинна відповідати стандартам TIA/EIA-568-A та TIA/EIA-569. Прокладка кабелю всередині будівлі здійснюється за типом кабелю «неекранована кручена пара» або кабелю UTP категорії 5e, що забезпечує високу надійність і швидкість передачі даних в поєднанні з високою технологічністю. Максимальна довжина кабелю – 100 м. Така довжина відповідає вимогам і не погіршує продуктивність передачі даних.

Волоконна оптика використовується для підключення будівлі до інтернету. Волоконно-оптичний кабель SC G657A застосовується між будівлями. Даний кабель може використовуватися на опорах повітряних ліній зв'язку, міського електротранспорту і повітряних ліній електропередачі при впливі навантажень від вітру, льоду, температури і їх комбінацій.

Використовуються роз'єми SC SM MM, також цей кабель можна використовувати для прокладки мережі між будівлями.

Підключення WAN між маршрутизаторами відділів вимагає використання технології передачі даних Serial DCE/DTE. Глобальна мережа використовує послідовний кабель DCE CAB-6060X для послідовних інтерфейсів.

Роутер і сервер розміщуються в серверній кімнаті з точки зору безпеки. Сервер розташований у серверній стійці Hexagona 42U (2055x800x1000 мм) з перфорованими дверцятами. Приміщення обладнане системою вентиляції та джерелами безперебійного живлення. Кабель прокладається за допомогою металевих коробів, які забезпечують точки доступу для кожної кімнати.

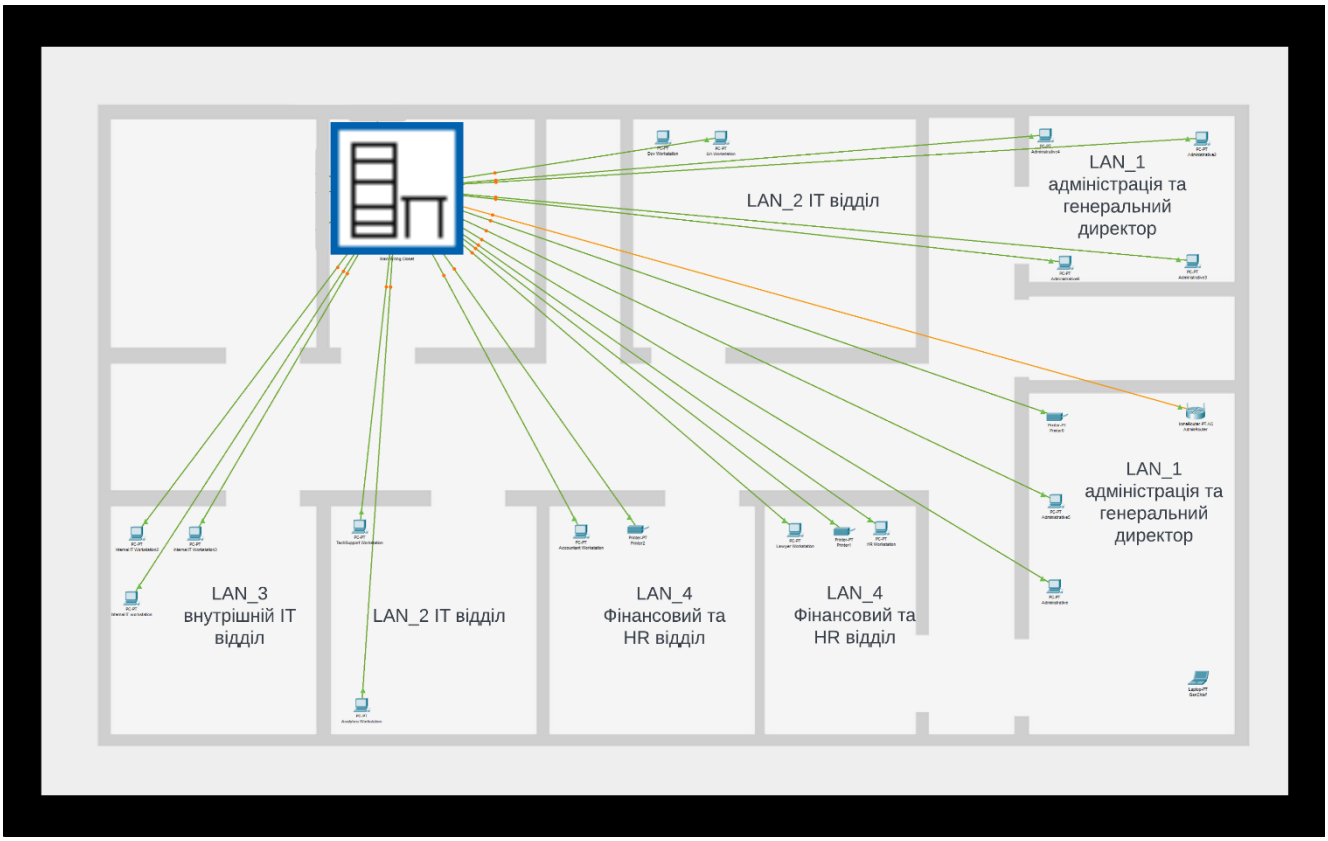

Рисунок 3.6 – Схема фізичної топології корпоративних мереж (модель)

3.3 Розрахунок налаштувань маршрутизації корпоративної мережі

Щоб розрахувати параметри маршрутизації корпоративної мережі, необхідно враховувати топологію мережі, вимоги до безпеки, продуктивність і типи маршрутизаторів.

Структура мережі: офіс;

Кількість пристроїв:

- Маршрутизатор – 5 шт;
- Комутатори – 5 шт;

Адресний простір визначено та обчислено в попередньому розділі, як і розрахунок пропускної здатності підмережі.

В якості основного протоколу маршрутизації обраний протокол динамічної маршрутизації OSPF. Плюси і особливості його експлуатації описані в наступному розділі. Цей протокол маршрутизації відповідає вимогам масштабованості та відмовостійкості.

3.4 Налаштування та перевірка роботи комп’ютерної системи

3.4.1 Базове налаштування конфігурації пристроїв

В рамках роботи було виконано базову настройку мережевих пристроїв комп'ютерної системи «УнІТ».

Додатково в базову комплектацію входять:

- примусове використання пароля для привілейованого режиму, консолі та VTY;
- шифрування всіх паролів, які зберігаються у відкритому вигляді;
- налаштований банер Message Of The Day (MOTD);
- адреси налаштовуються згідно з таблицею 3.4;
- на інтерфейсах маршрутизатора DCE годинник встановлено на 128000.

Нижче наведено приклад налаштування роутера Admin_router.

DNS-пошук заборонено на маршрутизаторах для запобігання перекладу доменного імені у разі помилкового введення неінтерпретованих слів у командний рядок замість допустимих команд:

```
Router(config)#no ip domain-lookup
```

Унікальне ім'я пристрою:

```
Router(config)#hostname Admin_router
```

Зберігання паролів в зашифрованому вигляді:

```
Admin_router(config)#service password-encryption
```

Встановлення пароля в привілейований режим output:

```
Admin_router(config)#enable secret 123_shvets
```

Встановіть вхідну пару на консольний рядок:

```
Admin_router(config)#line console 0
Admin_router(config-line)#password 123_shvets
```

Варіанти запиту пароля для входу:

```
Admin_router(config-line)#login
Admin_router(config-line)#exit
```

Налаштування банера MOTD:

```
Admin_router(config)#banner motd #123-20z ShvetsAD password access#
```

Налаштування протокола SSH, створення 123_20z_Shvets користувач з паролем admin_cisco:

```
Admin_router(config)#username 123_20z_Shvets password admin_cisco
```

Створення домену:

```
Admin_router(config)#ip domain name Admin_router
```

Для шифрування даних був створений ключ RSA довжиною 1024 біти:

```
Admin_router(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Налаштування лінії VTY:

```
Admin_router(config)#line vty 0 4
```

Налаштування необхідності введення логіна та пароля для входу в рядок:

```
Admin_router(config-line)#login local
```

Встановити лінійний вхід лише за допомогою SSH:

```
Admin_router(config-line)#transport input ssh
```

Налаштування IPv4-адрес згідно з таблицею 3.3:

```
Admin_router(config)#in gig0/1
Admin_router(config-if)#ip-address 192.168.19.1 255.255.255.192
```

Щоб запустити інтерфейс, його потрібно включити:

```
Admin_router(config-if)#no sh
```

3.4.2 Налаштування маршрутизаторів корпоративної мережі

Для побудови таблиць маршрутизації на мережевих маршрутизаторах комп'ютерної системи «УнІТ» використовується протокол динамічної маршрутизації OSPF.

Протокол Open Shortest Path First (OSPF) описаний в стандарті RFC 2328, є протоколом динамічної маршрутизації. Він використовується для обміну інформацією про маршрутизацію між маршрутизаторами в єдиній автономній системі (AS). Він заснований на алгоритмі (link-state) і є протоколом внутрішнього шлюзу (Interior Gateway Protocol, IGP).

OSPF був розроблений і стандартизований IETF (Internet Engineering Task Force) наприкінці 1980-х рр. OSPF був створений для заміни старих протоколів маршрутизації, таких як RIP (Routing Information Protocol), для забезпечення більш ефективної та масштабованої маршрутизації між великими мережами.

OSPF має такі переваги:

- Підтримка мережевих масок змінної довжини (VLSM)
- протокол швидко адаптується до змін у мережі, забезпечуючи швидку конвергенцію та відновлення маршрутів у разі збоїв;
- Протокол підтримує ієрархічну структуру, розділену на області. Це дозволяє зменшити розмір таблиць маршрутизації та обсяг трафіку оновлення маршрутів.
- Протокол використовує вартість як метрику для визначення найкращого шляху. Параметр вартості може ґрунтуватися на пропускній здатності, затримці та інших факторах;
- Протокол підтримує аутентифікацію для забезпечення безпеки та запобігання несанкціонованій зміні маршруту.
- Протокол може працювати в мережах з різними типами з'єднань, включаючи мережі point-to-point, multicast і широкомовні мережі.

Для кожного маршрутизатора рекламуються мережі, підключені безпосередньо, а оновлення маршрутизації інтерфейсів локальної мережі вимкнено. Маршрут до Інтернету (ISP) за замовчуванням налаштовано на Inner_it_router і розповсюджується за допомогою оновлень маршрутизації.

Увімкніть OSPF на маршрутизаторі за допомогою кнопки:

```
Inner_it_router(config)#router ospf 11
```

Протокол повинен рекламувати мережі, підключені до роутера.

```
Inner_it_router(config-router)#network 192.168.19.97 0.0.0.31 area
0
Inner_it_router(config-router)#network 10.0.19.2 0.0.0.3 area 0
Inner_it_router(config-router)#network 10.0.19.17 0.0.0.3 area 0
Inner_it_router(config-router)#network 10.0.19.10 0.0.0.3 area 0
Inner_it_router(config-router)#network 10.0.19.21 0.0.0.3 area 0
```

Маршрут за замовчуванням:

```
Inner_it_router(config-router)#ip route 0.0.0.0 0.0.0.0
209.165.203.1
```

На послідовних інтерфейсах DCE згідно зі специфікаціями пропускна здатність встановлюється на рівні 128 Кбіт/с, швидкість каналу 128000, визначається вартість метрики – 7500.

```
Inner_it_router(config)#interface s0/1/0
Inner_it_router(config-if)#bandwidth 128
Inner_it_router(config-if)#clock rate 128000
Inner_it_router(config-if)#ip ospf cost 7500
```

Перевіримо таблиці маршрутизації на маршрутизаторах .Усі маршрутизатори, за винятком мереж, підключених безпосередньо, із символом «C», містять інформацію OSPF про всі віддалені мережі із символом «O». Вони також мають записи маршруту за замовчуванням, які складаються з восьми нулів, для підключення до IPS-маршрутизатора.

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.0.19.0/30 is directly connected, Serial0/3/0
L       10.0.19.1/32 is directly connected, Serial0/3/0
C       10.0.19.4/30 is directly connected, Serial0/3/1
L       10.0.19.5/32 is directly connected, Serial0/3/1
O       10.0.19.8/30 [110/15000] via 10.0.19.2, 00:00:59, Serial0/3/0
                     [110/15000] via 10.0.19.6, 00:00:59, Serial0/3/1
O       10.0.19.12/30 [110/15000] via 10.0.19.6, 00:00:59, Serial0/3/1
O       10.0.19.16/30 [110/15000] via 10.0.19.2, 00:05:36, Serial0/3/0
O       10.0.19.20/30 [110/15000] via 10.0.19.2, 00:06:29, Serial0/3/0
O    12.0.0.0/8 [110/30000] via 10.0.19.2, 00:06:29, Serial0/3/0
O    13.0.0.0/8 [110/30000] via 10.0.19.2, 00:06:29, Serial0/3/0
O    192.168.1.0/24 [110/37500] via 10.0.19.2, 00:06:29, Serial0/3/0
     192.168.8.0/27 is subnetted, 1 subnets
O       192.168.8.64/27 [110/15000] via 10.0.19.6, 00:00:59, Serial0/3/1
     192.168.19.0/24 is variably subnetted, 4 subnets, 4 masks
C       192.168.19.0/26 is directly connected, GigabitEthernet0/0
L       192.168.19.1/32 is directly connected, GigabitEthernet0/0
O       192.168.19.96/27 [110/15000] via 10.0.19.2, 00:06:29, Serial0/3/0
O       192.168.19.128/28 [110/22500] via 10.0.19.2, 00:00:59, Serial0/3/0
                          [110/22500] via 10.0.19.6, 00:00:59, Serial0/3/1
O    209.165.203.0/24 [110/22500] via 10.0.19.2, 00:06:29, Serial0/3/0
```

Рисунок 3.7 – Результат роботи OSPF на роутері Admin_router

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O       10.0.19.0/30 [110/15000] via 10.0.19.5, 00:01:27, Serial0/3/0
                     [110/15000] via 10.0.19.10, 00:01:27, Serial0/3/1
C       10.0.19.4/30 is directly connected, Serial0/3/0
L       10.0.19.6/32 is directly connected, Serial0/3/0
C       10.0.19.8/30 is directly connected, Serial0/3/1
L       10.0.19.9/32 is directly connected, Serial0/3/1
C       10.0.19.12/30 is directly connected, Serial0/2/0
L       10.0.19.13/32 is directly connected, Serial0/2/0
O       10.0.19.16/30 [110/15000] via 10.0.19.14, 00:01:27, Serial0/2/0
                      [110/15000] via 10.0.19.10, 00:01:27, Serial0/3/1
O       10.0.19.20/30 [110/15000] via 10.0.19.10, 00:01:57, Serial0/3/1
O    12.0.0.0/8 [110/30000] via 10.0.19.10, 00:01:57, Serial0/3/1
O    13.0.0.0/8 [110/30000] via 10.0.19.10, 00:01:57, Serial0/3/1
O    192.168.1.0/24 [110/37500] via 10.0.19.10, 00:01:57, Serial0/3/1
     192.168.8.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.8.64/27 is directly connected, GigabitEthernet0/0
L       192.168.8.65/32 is directly connected, GigabitEthernet0/0
     192.168.19.0/24 is variably subnetted, 3 subnets, 3 masks
O       192.168.19.0/26 [110/15000] via 10.0.19.5, 00:01:57, Serial0/3/0
O       192.168.19.96/27 [110/15000] via 10.0.19.10, 00:01:57, Serial0/3/1
O       192.168.19.128/28 [110/15000] via 10.0.19.14, 00:01:57, Serial0/2/0
O    209.165.203.0/24 [110/22500] via 10.0.19.10, 00:01:57, Serial0/3/1
```

Рисунок 3.8 – Результат роботи OSPF на роутері It_router

```
Inner_it_router#
%SYS-5-CONFIG_I: Configured from console by console
show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C       10.0.19.0/30 is directly connected, Serial0/3/0
L       10.0.19.2/32 is directly connected, Serial0/3/0
O       10.0.19.4/30 [110/15000] via 10.0.19.9, 00:03:15, Serial0/3/1
                     [110/15000] via 10.0.19.1, 00:03:15, Serial0/3/0
C       10.0.19.8/30 is directly connected, Serial0/3/1
L       10.0.19.10/32 is directly connected, Serial0/3/1
O       10.0.19.12/30 [110/15000] via 10.0.19.9, 00:02:27, Serial0/3/1
                      [110/15000] via 10.0.19.18, 00:02:27, Serial0/2/0
C       10.0.19.16/30 is directly connected, Serial0/2/0
L       10.0.19.17/32 is directly connected, Serial0/2/0
C       10.0.19.20/30 is directly connected, Serial0/2/1
L       10.0.19.21/32 is directly connected, Serial0/2/1
O    12.0.0.0/8 [110/22500] via 10.0.19.22, 00:04:30, Serial0/2/1
O    13.0.0.0/8 [110/22500] via 10.0.19.22, 00:04:30, Serial0/2/1
O    192.168.1.0/24 [110/30000] via 10.0.19.22, 00:04:30, Serial0/2/1
     192.168.8.0/27 is subnetted, 1 subnets
O       192.168.8.64/27 [110/15000] via 10.0.19.9, 00:04:30, Serial0/3/1
     192.168.19.0/24 is variably subnetted, 4 subnets, 4 masks
O       192.168.19.0/26 [110/15000] via 10.0.19.1, 00:03:15, Serial0/3/0
C       192.168.19.96/27 is directly connected, GigabitEthernet0/0
L       192.168.19.97/32 is directly connected, GigabitEthernet0/0
O       192.168.19.128/28 [110/15000] via 10.0.19.18, 00:02:27, Serial0/2/0
O    209.165.203.0/24 [110/15000] via 10.0.19.22, 00:04:30, Serial0/2/1
```

Рисунок 3.9 – Результат роботи OSPF на роутері Inner_it_router

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O       10.0.19.0/30 [110/15000] via 10.0.19.17, 00:01:04, Serial0/3/1
O       10.0.19.4/30 [110/15000] via 10.0.19.13, 00:01:04, Serial0/2/0
O       10.0.19.8/30 [110/15000] via 10.0.19.13, 00:01:04, Serial0/2/0
                     [110/15000] via 10.0.19.17, 00:01:04, Serial0/3/1
C       10.0.19.12/30 is directly connected, Serial0/2/0
L       10.0.19.14/32 is directly connected, Serial0/2/0
C       10.0.19.16/30 is directly connected, Serial0/3/1
L       10.0.19.18/32 is directly connected, Serial0/3/1
O       10.0.19.20/30 [110/15000] via 10.0.19.17, 00:01:04, Serial0/3/1
O    12.0.0.0/8 [110/30000] via 10.0.19.17, 00:01:04, Serial0/3/1
O    13.0.0.0/8 [110/30000] via 10.0.19.17, 00:01:04, Serial0/3/1
O    192.168.1.0/24 [110/37500] via 10.0.19.17, 00:01:04, Serial0/3/1
     192.168.8.0/27 is subnetted, 1 subnets
O       192.168.8.64/27 [110/15000] via 10.0.19.13, 00:01:04, Serial0/2/0
     192.168.19.0/24 is variably subnetted, 4 subnets, 4 masks
O       192.168.19.0/26 [110/22500] via 10.0.19.13, 00:01:04, Serial0/2/0
                        [110/22500] via 10.0.19.17, 00:01:04, Serial0/3/1
O       192.168.19.96/27 [110/15000] via 10.0.19.17, 00:01:04, Serial0/3/1
C       192.168.19.128/28 is directly connected, GigabitEthernet0/0
L       192.168.19.129/32 is directly connected, GigabitEthernet0/0
O    209.165.203.0/24 [110/22500] via 10.0.19.17, 00:01:04, Serial0/3/1
```

Рисунок 3.10 – Результат роботи OSPF на роутері Finance_hr_router

На малюнках таблиці маршрутизації видно, що в таблицях перераховані всі доступні мережі. Топологія сходиться, тому є можливість відправляти пакети з однієї підмережі в іншу підмережу через сусідні маршрутизатори.

3.4.3 Налаштування роботи Інтернет

Відповідно до вимог, що пред'являються до комп'ютерної мережі, необхідно забезпечити користувачам комп'ютерної мережі доступ до мережі Інтернет. Щоб це забезпечити, потрібно налаштувати технологію на прикордонному роутері NAT.

NAT (Network Address Translation) – технологія, призначена для зміни мережевих адрес в IP-пакетах, які проходять через маршрутизатор. NAT дозволяє декільком пристроям в одній локальній мережі спільно використовувати одну IP-адресу для доступу до Інтернету. Це зберігає адреси IPv4. NAT також підвищує безпеку локальної мережі, приховуючи внутрішні IP-адреси від зовнішніх користувачів. Це ускладнює зловмисникам здійснення

мережевих атак на пристрої всередині комп'ютерної мережі. NAT також дозволяє мережевим адміністраторам використовувати приватні IP-адреси у своїх мережах без конфліктів з іншими мережами в Інтернеті. До недоліків NAT можна віднести те, що для перекладу адрес потрібні обчислювальні ресурси на маршрутизаторі, що може додати невеликі затримки в передачі даних, а в деяких додатках і протоколах можуть виникнути проблеми з роботою через технологію NAT.

На периферійному маршруті NAT має бути налаштований відповідно до вимог:

- виділення пулу адрес (209.165.203.4 – 209.165.203.30) з ім'ям Internet;
- адреса HTTP-сервера в комп'ютерній мережі: 192.168.19.84/27;
- номер списку доступа: 11.

Нижче наведено команди для налаштування NAT на прикордонному маршрутизаторі Office_router:

Конфігурація списку контролю доступу, що дозволяє всі адреси в підмережі:

```
Office_router(config)# access-list 8 permit 192.168.19.0 0.0.7.255
```

Виділення пулу адрес з іменем Internet для динамічного розподілу адрес:

```
Office_router(config)# ip nat pool Internet 209.165.203.1
209.165.203.30 netmask 255.255.255.224
```

Конфігурування підміна адреси підмережі із зовнішньою IP-адресою згідно зі списком контролю доступу:

```
Office_router(config)# ip nat inside source list 11 pool Internet
```

Виділення статичної адреси перекладу для HTTP-сервера:

```
Office_router(config)# ip nat inside source static 192.168.19.84
209.165.203.1
```

Конфігурування порта ser0/2/0 для вхідних пакетів. Нові пакети будуть замінені IP-адресою внутрішньої мережі:

```
Office_router(config)#in ser0/2/0
Office_router(config-if)#ip nat outside
```

Конфігурування порта ser0/2/1 для вихідних пакетів. Нові пакети будуть замінені на зовнішню IP-адресу:

```
Office_router(config-if)#in Serial0/2/1
Office_router(config-if)#ip nat inside
```

```
Office_router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.203.1     192.168.19.84      ---                ---
```

Рисунок 3.11 – Результат налаштування технології NAT на роутері Office_router

3.4.4 Налаштування агрегування каналів PAgP

Port Aggregation Protocol (PAgP) — це протокол від Cisco Systems. Його задача полягає в автоматизації агрегації фізичних портів Ethernet комутатора в єдиний логічний порт.

З метою підвищення пропускної здатності і надійності каналів в LAN_3 мережі на комутаторах були об'єднані фізичні порти для поділу серверної частини підмережі і підмережі з робочими станціями. Це забезпечується технологією EtherChannel, яка дозволяє об'єднати кілька фізичних портів на комутаторах в один логічний.

Головною перевагою такого каналу є збільшення швидкості передачі даних. За надійністю EtherChannel вигідно відрізняється від протоколу Spanning Tree Protocol (STP). У випадку з STP при втраті зв'язку починається перерахунок топології, який займає час, перш ніж резервна ланка буде введена в експлуатацію. З EtherChannel топологія залишається колишньою, і лише швидкість каналу трохи знижується. Іншими словами, EtherChannel не усуває необхідності використання протоколу Spanning Tree Protocol, але якщо з'єднання в агрегованій області втрачається, це позбавляє від необхідності перерахунку топології.

```
Internal_it_sw1(config)#in range Fa0/7-8
Internal_it_sw1(config)#no sh
Internal_it_sw1(config)#channel-group 1 mode desirable
Internal_it_sw1(config)#interface Port-channel 1
Internal_it_sw1(config)#switchport mode trunk
Internal_it_sw1(config)#switchport trunk allowed vlan all
Internal_it_sw1(config)#
```

Для тестування протоколу PAgP використовуємо наступну команду:

```
Internal_it_sw1#sh etherchannel summary
```

```
Inner_it_sw_1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

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

1      Po1(SU)           PAgP   Fa0/7(P) Fa0/8(P)
```

Рисунок 3.12– Результат налаштувань PAgP на комутаторі Internal_sw1

```
Inner_it_sw_2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

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

1      Po1(SU)           PAgP   Fa0/7(P) Fa0/8(P)
```

Рисунок 3.13 – Результат настройки PAgP на комутаторі Internal_sw2

3.4.5 Налаштування віртуальної приватної мережі site-to-site VPN з використанням IPsec

Для того, щоб співробітники з віддаленого домашнього офісу могли підключитися до комп'ютерної мережі компанії, необхідно налаштувати віртуальну приватну мережу (VPN) site-to-site за допомогою протоколу IPsec.

Віртуальна приватна мережа (Virtual Private Network, VPN) – це технологія, яка створює безпечне та зашифроване з'єднання поверх загальнодоступної мережі, такої як Інтернет. Це дозволяє користувачам приховати свою реальну IP-адресу та захистити свої дані від перехоплення та несанкціонованого доступу. VPN – це спосіб налаштування логічних підмереж. VPN шифрує всі дані, що передаються між вашим пристроєм і VPN-сервером, роблячи його недоступним для сторонніх. Коли ви підключаєтеся до VPN, ваша реальна IP-адреса замінюється на IP-адресу VPN-сервера, що допомагає приховати ваше місцезнаходження та забезпечує анонімність.

Для організації зашифрованого VPN-каналу використовується технологія IPsec (IP Security) – набір протоколів, пов'язаних з шифруванням, аутентифікацією та захистом даних під час передачі даних по мережі. За реалізацію процесу відповідає протокол IKE. IKE (Internet Key Exchange protocol) використовується для формування IPSec SA (Security Association).

Для настройки VPN необхідно налаштувати технологію IPsec, з реалізацією протоколу IKE (Internet Key Exchange Protocol). Цей протокол необхідний для створення Асоціацій безпеки (SA). SA визначає параметри шифрування та автентифікації, які використовуються для захисту даних.

Процес складається з двох етапів. На першому етапі учасники проходять аутентифікацію та узгоджують параметри встановлення спеціального захищеного з'єднання. Це з'єднання призначене лише для обміну інформацією про бажані алгоритми шифрування та іншими деталями майбутнього тунелю IPSec. Параметри тунелю (ISAKMP Tunnel) встановлюються політикою ISAKMP.

Потім створюється тунель ISAKMP, через який проходить друга фаза IKE. На другому етапі враховуються правила, визначені в криптографічній карті. При створенні криптографічної карти використовуються такі параметри: прив'язка списку доступу до запису криптографічної карти і адреса партнера, з яким буде встановлено тунель.

Активація ліцензії Security Feature License (securityk9) на маршрутизаторі серії 2900:

```
Home_router(config)#license boot module c2900 technology-package
securityk9
```

Створення списка доступу 100, який дозволяє використовувати весь IP-трафік між корпоративною мережею 192.168.19.0/24 та домашньої мережі 192.168.1.0/24.

```
Home_router(config)#acccess-list 100 permit ip 192.168.19.0
0.0.0.255 192.168.1.0 0.0.0.255
```

Створюють політику ISAKMP з номером 10, що вказує на використання 256-бітного AES для шифрування, автентифікації з попередньо розділеним ключем (pre-shared key) та групи 5 для обміну ключами (DH Group 5).

```
Home_router(config)#crypto isakmp policy 10
Home_router(config)#encryption aes 256
Home_router(config)#authentication pre-share
Home_router(config)#group 5
```

Встановлення попереднього розділеного ключа (secretkey) для вузла з IP-адресою 13.42.56.2.

```
Home_router(config)#crypto isakmp key secretkey address 13.42.56.2
```

Створення IPsec перетворень під ім'ям home-office, з використанням шифрування AES з довжиною ключа 256 біт і алгоритмом хешування SHA для аутентифікації (esp-sha-hmac).

```
Home_router(config)#crypto ipsec transform-set home-office esp-aes
256 esp-sha-hmac
```

Створення криптографічної картки з ім'ям IPSEC_MAP та пріоритетом 10, використовуючи IPsec с ISAKMP. Вона включає в себе наступні параметри:

- Вказівка адреси партнера VPN (13.42.56.2);
- включення Perfect Forward Secrecy (PFS) з використання групи 5;
- налаштування часу життю Асоціації безпеки на 86400 секунд (24 години);
- вказівка набору трансформацій home-office;
- прив'язка до списку доступу 100 для ідентифікації трафіку, який повинен бути захищений.

```
Home_router(config)#crypto map IPSEC_MAP 10 ipsec-isakmp
Home_router(config-isakmp)#set peer 13.42.56.2
Home_router(config-isakmp)#set pfs group5
Home_router(config-isakmp)#set security-association lifetime
seconds 86400
Home_router(config-isakmp)#set transform-set home-office
Home_router(config-isakmp)#match address 100

Home_router(config-isakmp)#int gig0/1
```

```
Home_router(config-interface)#crypto map IPSEC_MAP
```

```
   local  ident (addr/mask/prot/port): (192.168.19.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 13.42.56.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 13.42.56.2, remote crypto endpt.:13.42.56.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x0(0)
```

Рисунок 3.14 – Результат конфігурації IPsec на маршрутизаторі віддаленого офісу

І аналогічні налаштування виконуються на прикордонному роутері Office_router.

```
Office_router#show crypto ipsec sa

interface: Serial0/3/1
    Crypto map tag: IPSEC_MAP, local addr 209.165.203.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.19.0/255.255.255.0/0/0)
   current_peer 209.165.203.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.203.2, remote crypto endpt.:209.165.203.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/1
     current outbound spi: 0x0(0)

     inbound esp sas:
```

Рисунок 3.15 – Результат конфігурації IPsec на маршрутизаторі Office router

3.4.6 Перевірка роботи комп’ютерної системи

Результатом перевірки комп'ютерної системи є виконання команди ping на робочих місцях співробітників. Виконана перевірка вузлів з різних підмереж комп'ютерної системи.

```
C:\>ping 192.168.19.66

Pinging 192.168.19.66 with 32 bytes of data:

Reply from 192.168.19.66: bytes=32 time=2ms TTL=126
Reply from 192.168.19.66: bytes=32 time=14ms TTL=126
Reply from 192.168.19.66: bytes=32 time=1ms TTL=126
Reply from 192.168.19.66: bytes=32 time=17ms TTL=126

Ping statistics for 192.168.19.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 17ms, Average = 8ms

C:\>ping 192.168.19.98

Pinging 192.168.19.98 with 32 bytes of data:

Reply from 192.168.19.98: bytes=32 time=32ms TTL=126
Reply from 192.168.19.98: bytes=32 time=25ms TTL=126
Reply from 192.168.19.98: bytes=32 time=1ms TTL=126
Reply from 192.168.19.98: bytes=32 time=36ms TTL=126

Ping statistics for 192.168.19.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 36ms, Average = 23ms

C:\>ping 192.168.19.130

Pinging 192.168.19.130 with 32 bytes of data:

Reply from 192.168.19.130: bytes=32 time=36ms TTL=125
Reply from 192.168.19.130: bytes=32 time=3ms TTL=125
Reply from 192.168.19.130: bytes=32 time=2ms TTL=125
Reply from 192.168.19.130: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.19.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 36ms, Average = 11ms
```

Рисунок 3.16 – Виконання команди ping на робочій станції з підмережі «LAN_1 адміністрація та генеральний директор»

```
C:\>ping 192.168.19.3

Pinging 192.168.19.3 with 32 bytes of data:

Reply from 192.168.19.3: bytes=32 time=1ms TTL=126
Reply from 192.168.19.3: bytes=32 time=5ms TTL=126
Reply from 192.168.19.3: bytes=32 time=2ms TTL=126
Reply from 192.168.19.3: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.19.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>ping 192.168.19.98

Pinging 192.168.19.98 with 32 bytes of data:

Reply from 192.168.19.98: bytes=32 time=14ms TTL=126
Reply from 192.168.19.98: bytes=32 time=1ms TTL=126
Reply from 192.168.19.98: bytes=32 time=1ms TTL=126
Reply from 192.168.19.98: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.19.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 14ms, Average = 4ms

C:\>ping 192.168.19.130

Pinging 192.168.19.130 with 32 bytes of data:

Reply from 192.168.19.130: bytes=32 time=33ms TTL=126
Reply from 192.168.19.130: bytes=32 time=1ms TTL=126
Reply from 192.168.19.130: bytes=32 time=27ms TTL=126
Reply from 192.168.19.130: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.19.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 33ms, Average = 15ms
```

Рисунок 3.17 – Виконання команди ping на робочій станції з підмережі «LAN_2 IT відділ»

```
C:\>ping 192.168.19.3

Pinging 192.168.19.3 with 32 bytes of data:

Reply from 192.168.19.3: bytes=32 time=30ms TTL=126
Reply from 192.168.19.3: bytes=32 time=1ms TTL=126
Reply from 192.168.19.3: bytes=32 time=1ms TTL=126
Reply from 192.168.19.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.19.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 30ms, Average = 8ms

C:\>ping 192.168.19.66

Pinging 192.168.19.66 with 32 bytes of data:

Reply from 192.168.19.66: bytes=32 time=34ms TTL=126
Reply from 192.168.19.66: bytes=32 time=26ms TTL=126
Reply from 192.168.19.66: bytes=32 time=1ms TTL=126
Reply from 192.168.19.66: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.19.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 34ms, Average = 15ms

C:\>ping 192.168.19.130

Pinging 192.168.19.130 with 32 bytes of data:

Reply from 192.168.19.130: bytes=32 time=38ms TTL=126
Reply from 192.168.19.130: bytes=32 time=2ms TTL=126
Reply from 192.168.19.130: bytes=32 time=1ms TTL=126
Reply from 192.168.19.130: bytes=32 time=4ms TTL=126

Ping statistics for 192.168.19.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 38ms, Average = 11ms
```

Рисунок 3.18 – Виконання команди ping на робочій станції з підмережі «LAN_3 внутрішній IT відділ»

```
C:\>ping 192.168.19.3

Pinging 192.168.19.3 with 32 bytes of data:

Reply from 192.168.19.3: bytes=32 time=2ms TTL=125
Reply from 192.168.19.3: bytes=32 time=42ms TTL=125
Reply from 192.168.19.3: bytes=32 time=103ms TTL=125
Reply from 192.168.19.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.19.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 103ms, Average = 37ms

C:\>ping 192.168.19.66

Pinging 192.168.19.66 with 32 bytes of data:

Reply from 192.168.19.66: bytes=32 time=33ms TTL=126
Reply from 192.168.19.66: bytes=32 time=1ms TTL=126
Reply from 192.168.19.66: bytes=32 time=29ms TTL=126
Reply from 192.168.19.66: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.19.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 33ms, Average = 16ms

C:\>ping 192.168.19.98

Pinging 192.168.19.98 with 32 bytes of data:

Reply from 192.168.19.98: bytes=32 time=33ms TTL=126
Reply from 192.168.19.98: bytes=32 time=2ms TTL=126
Reply from 192.168.19.98: bytes=32 time=2ms TTL=126
Reply from 192.168.19.98: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.19.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 33ms, Average = 9ms
```

Рисунок 3.19 – Виконання команди ping на робочій станції з підмережі «LAN_4 Фінансовий та HR відділ»

Також можливе підключення по SSH до роутера з робочого місця співробітника. Для підключення використовуються конфігураційні дані, зазначені при базовому налаштуванні роутерів. Логін: 123_20z_Shvets, а пароль admin.

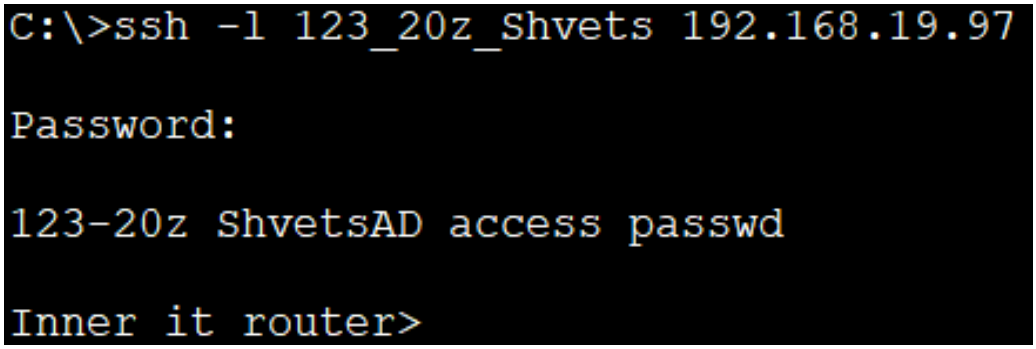

Рисунок 3.20 – SSH-з'єднання з роутером Inner_it_router

Усередині VLAN користувачі мережі отримують налаштування мережі через DHCP. Для цього необхідно налаштувати It_router роутера і хости на підтримку даного протоколу.

DHCP (Dynamic Host Configuration Protocol) – це протокол динамічної конфігурації вузлів мережі. Цей протокол використовується для доставки конфігурацій на комп'ютери користувачів. Протокол працює за схемою клієнт-сервер. Цей протокол зручний тим, що при додаванні нових пристроїв в мережу немає необхідності налаштовувати системного адміністратора, а саме немає необхідності прописувати DNS-сервер, IP-адресу вузла і шлюзу.

Налаштування DHCP для підмереж VLAN на It_router роутері виконується наступним чином:

```
It_router(config)#int gig0/0.21
It_router(config-subinf)#encapsulation dot1Q 21
It_router(config-subinf)#ip address 192.168.19.65 255.255.255.248
It_router(dhcp-config)#ip dhcp pool vlan_net1
It_router(dhcp-config)#network 192.168.19.65 255.255.255.248
It_router(dhcp-config)#default-router 192.168.19.65

It_router(config)#int gig0/0.22
It_router(config-subinf)#encapsulation dot1Q 22
It_router(config-subinf)#ip address 192.168.19.73 255.255.255.248
It_router(dhcp-config)#ip dhcp pool vlan_net2
It_router(dhcp-config)#network 192.168.19.73 255.255.255.248
```

```
It_router(dhcp-config)#default-router 192.168.19.73
```

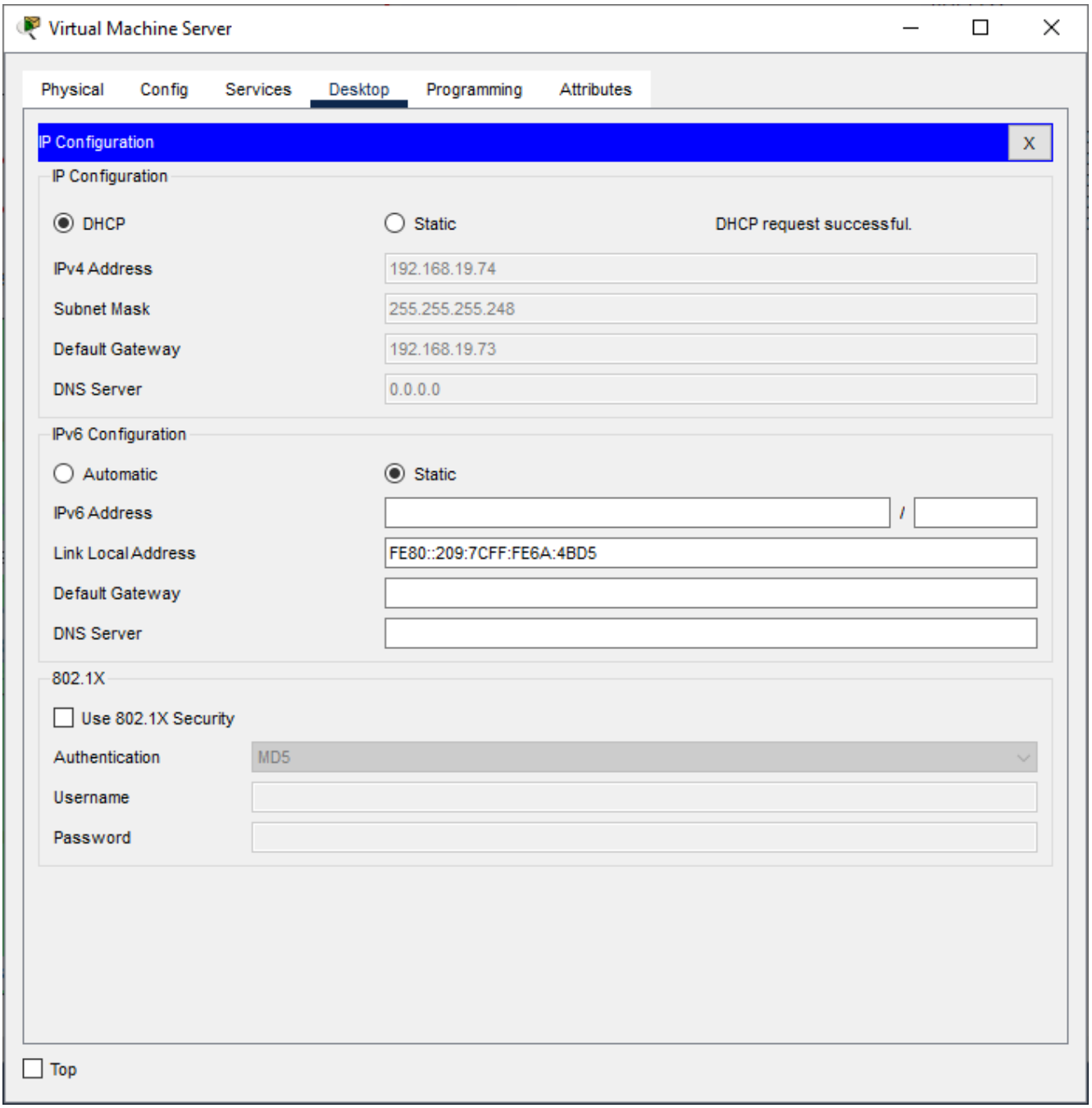

Рисунок 3.21 – Результат роботи DHCP для пристрою з VLAN22

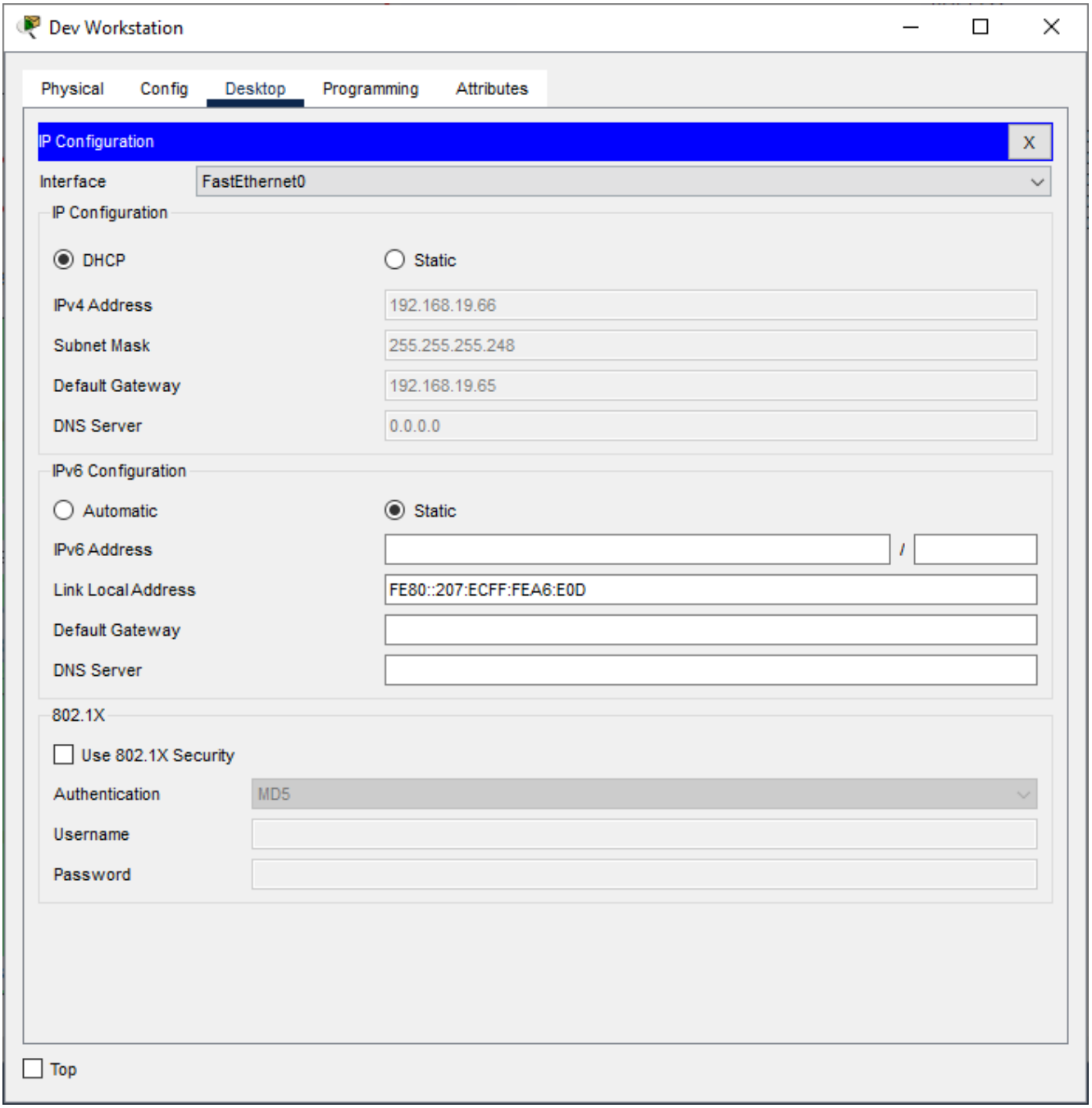

Рисунок 3.22 –Результат роботи DHCP для пристрою з VLAN21

3.5 Захист інформації в комп’ютерній системі від несанкціонованого доступу. Розробка методів для захисту інформації в комп’ютерній системі

Для забезпечення безпеки даних в комп'ютерній системі необхідно:

- Налаштовуйте VLAN і маршрутизуйте пакети між віртуальними підмережами;
- Захистіть порти комутатора, до яких підключені сервери;

– налаштувати сервіс AAA і RADIUS.

3.5.1 Налаштування маршрутизаторів на підтримку служби AAA

Cisco AAA (Authentication, Authorization, and Accounting) – це технологія, яка використовується для контролю доступу до мережевих ресурсів, забезпечення безпеки та відстеження активності користувачів.

Авторизація перевіряє особу користувача або пристрою, ідентифікує користувача, який намагається отримати доступ до мережі, а також підтримує різні методи аутентифікації (пароль, токени, сертифікати).

Аутентифікація визначає, що користувач або пристрій може робити в мережі, а автентифікація також контролює доступ до мережевих ресурсів і служб.

Облік реєструє активність користувачів або пристроїв у мережі, журнали для аналізу використання ресурсів та аудиту безпеки. Додатково він дозволяє відстежувати час і обсяг використовуваних даних, а також ряд інших параметрів.

Cisco AAA підтримує протокол реалізації функції AAA – RADIUS. RADIUS частіше використовується для аутентифікації та авторизації в мережах доступу.

Запуск сервісу AAA:

```
Internal_it_router(config)#aaa new-model
```

Налаштування типового методу аутентифікації з підключенням до локальної бази даних користувачів:

```
Internal_it_router(config)#aaa authentication login default local
```

Налаштування аутентифікації входу за допомогою сервера RADIUS, а якщо він недоступний, то за допомогою локальної бази даних користувачів:

```
Internal_it_router(config)#aaa authentication login Login group
radius local
Internal_it_router(config)#line console 0
```

Використання методу аутентифікації за логіном у терміналі:

```
Internal_it_router(config-line)#login authentication Login
Internal_it_router(config)#line vty 0 4
```

Використання методу автентифікації Login за замовчуванням:

```
Internal_it_router(config-line)#login authentication default
```

Налаштування RADIUS-сервер:

```
Internal_it_router(config)#radius-server host 192.168.19.102 auth-port 1645
Internal_it_router(config)#radius-server key radius12316
```

Налаштування сервера RADIUS відбувається наступним чином. Параметр мережі вказується в тому місці, де вказується IP-адреса маршрутизатора. А також був доданий користувач з логіном Shvets і пароль 123_20z_admin.

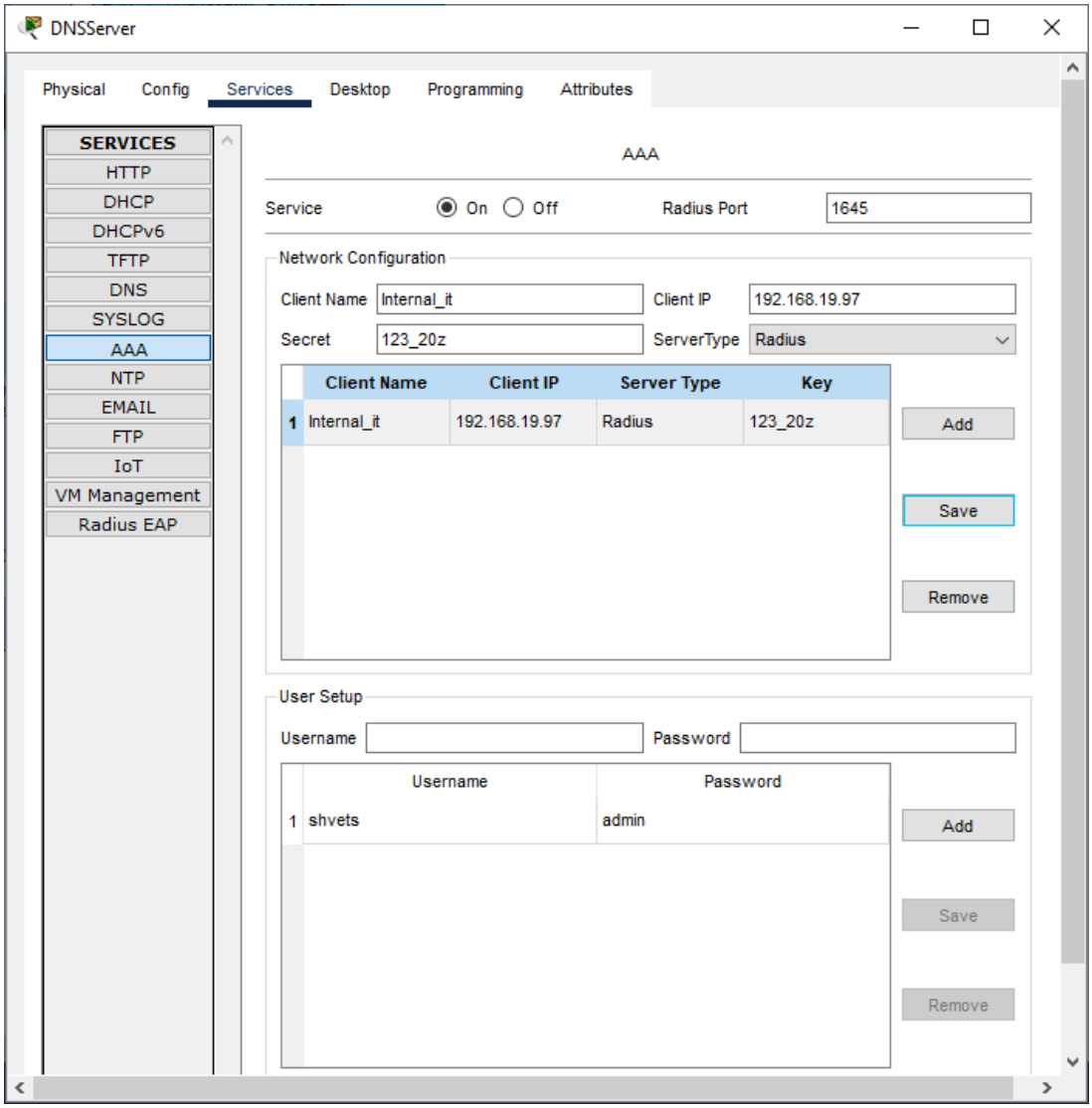

Рисунок 3.23 – Налаштування сервісу RADIUS на сервері.

При спробі авторизації на роутері вам буде запропоновано ввести логін і пароль. Цей процес займає деякий час, оскільки маршрутизатор робить запит до сервера, на якому запущена служба RADIUS.

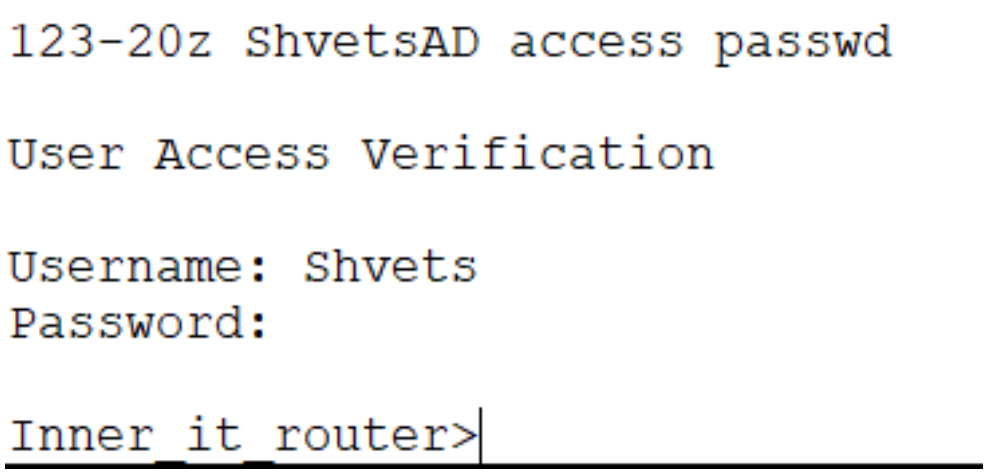

Рисунок 3.24 – Результат авторизації на роутері Inner_it_router

3.5.2 Налаштування мереж VLAN

VLAN (Virtual Private Network) Віртуальна приватна мережа – це технологія, яка використовується для поділу однієї фізичної мережі на кілька логічних мереж. Логічні мережі ізольовані. VLAN дозволяє об'єднувати мережеві пристрої в різні віртуальні мережі, незалежно від їх фізичного розташування. VLAN підвищують безпеку за рахунок ізоляції груп користувачів і мережевих ресурсів, а також полегшують управління мережею, оскільки адміністратори можуть легко змінювати конфігурації та додавати нові пристрої без необхідності фізично змінювати мережу.

Пристрої Cisco використовують протокол VTP (VLAN Trunking Protocol). Якщо потрібно, для підмереж повинні бути налаштовані віртуальні підмережі:

- LAN_2 IT відділ;
- LAN_4 Фінансовий та HR відділ.

Таблиця 3.5 – Опис VLAN комп'ютерної мережі

Ім'я VLAN	Номер VLAN	Примітка
1	За замовчуванням	Не використовується
21	dev_qa_department	Відділ розробників та тестувальників

Ім'я VLAN	Номер VLAN	Примітка
22	analytics_tech_support_department	Відділ аналітики та технічної підтримки
41	financial_department	Фінансовий відділ
42	hr_department	Відділ HR
99	Management	Службовий: Для налаштування
100	Native	власна

Також потрібно зробити наступні налаштування:

- Магістральні порти та порти доступу налаштовуються згідно з технічними вимогами.
- Всі невикористовувані фізичні порти на комутаторі відключені.
- Налаштуйте безпеку портів на портах комутатора, які підключені до серверів: обмежте доступ до портів лише двома унікальними пристроями.
- Налаштування маршрутизації між віртуальними мережами.

Створення VLAN для підмережі LAN_2:

```
It_switch(config)#vlan 21
It_switch(config)#name dev_qa_department
It_switch(config)#vlan 22
It_switch(config)#name analytics_tech_support_department
It_switch(config)#vlan 99
It_switch(config)#name management
It_switch(config)#vlan 100
It_switch(config)#name native
```

налаштування магістральних каналів(trunk mode):

```
It_switch(config)#int fa0/1
It_switch(config-if)#switchport trunk native vlan 100
It_switch(config-if)#switchport trunk allowed vlan 21,22,99-100
It_switch(config-if)#switchport mode trunk
```

Далі потрібно призначити кожному порту комутатора, до якого VLAN він належить, а також призначити режим доступу з номером VLAN.

```
It_switch(config)#int range fa0/2-5
It_switch(config-range)#switchport mode access
It_switch(config-range)#switchport access vlan 21
```

```
It_switch(config)#int range fa0/6-8
It_switch(config-range)#switchport mode access
It_switch(config-range)#switchport access vlan 22
```

І аналогічні налаштування виконуються для комутатора підмережі фінансового та HR-відділу.

```
Device Name: Switch0
Custom Device Model: 2960 IOS15
Hostname: it_switch

Port                Link   VLAN   IP Address          MAC Address
FastEthernet0/1     Up     --     --                  0090.2BBE.8B01
FastEthernet0/2     Up     21     --                  0090.2BBE.8B02
FastEthernet0/3     Up     21     --                  0090.2BBE.8B03
FastEthernet0/4     Up     21     --                  0090.2BBE.8B04
FastEthernet0/5     Up     21     --                  0090.2BBE.8B05
FastEthernet0/6     Up     22     --                  0090.2BBE.8B06
FastEthernet0/7     Down   22     --                  0090.2BBE.8B07
FastEthernet0/8     Down   22     --                  0090.2BBE.8B08
FastEthernet0/9     Down   1      --                  0090.2BBE.8B09
FastEthernet0/10    Down   1      --                  0090.2BBE.8B0A
FastEthernet0/11    Down   1      --                  0090.2BBE.8B0B
FastEthernet0/12    Down   1      --                  0090.2BBE.8B0C
FastEthernet0/13    Down   1      --                  0090.2BBE.8B0D
FastEthernet0/14    Down   1      --                  0090.2BBE.8B0E
FastEthernet0/15    Down   1      --                  0090.2BBE.8B0F
FastEthernet0/16    Down   1      --                  0090.2BBE.8B10
FastEthernet0/17    Down   1      --                  0090.2BBE.8B11
FastEthernet0/18    Down   1      --                  0090.2BBE.8B12
FastEthernet0/19    Down   1      --                  0090.2BBE.8B13
FastEthernet0/20    Down   1      --                  0090.2BBE.8B14
FastEthernet0/21    Down   1      --                  0090.2BBE.8B15
FastEthernet0/22    Down   1      --                  0090.2BBE.8B16
FastEthernet0/23    Down   1      --                  0090.2BBE.8B17
FastEthernet0/24    Down   1      --                  0090.2BBE.8B18
GigabitEthernet0/1  Down   1      --                  0090.2BBE.8B19
GigabitEthernet0/2  Down   1      --                  0090.2BBE.8B1A
Vlan1               Down   1      <not set>           00E0.F935.6BA7
Vlan99              Up     99     192.168.19.83/28    00E0.F935.6B01
```

Рисунок 3.25 – Результат конфігурації VLAN на комутаторі підмережі IT

```
Device Name: Switch2
Custom Device Model: 2960 IOS15
Hostname: it_switch

Port                Link   VLAN   IP Address         MAC Address
FastEthernet0/1     Up     --     --                 0060.4731.2A01
FastEthernet0/2     Up     41     --                 0060.4731.2A02
FastEthernet0/3     Up     41     --                 0060.4731.2A03
FastEthernet0/4     Up     41     --                 0060.4731.2A04
FastEthernet0/5     Up     41     --                 0060.4731.2A05
FastEthernet0/6     Up     42     --                 0060.4731.2A06
FastEthernet0/7     Up     42     --                 0060.4731.2A07
FastEthernet0/8     Up     42     --                 0060.4731.2A08
FastEthernet0/9     Down   1      --                 0060.4731.2A09
FastEthernet0/10    Down   1      --                 0060.4731.2A0A
FastEthernet0/11    Down   1      --                 0060.4731.2A0B
FastEthernet0/12    Down   1      --                 0060.4731.2A0C
FastEthernet0/13    Down   1      --                 0060.4731.2A0D
FastEthernet0/14    Down   1      --                 0060.4731.2A0E
FastEthernet0/15    Down   1      --                 0060.4731.2A0F
FastEthernet0/16    Down   1      --                 0060.4731.2A10
FastEthernet0/17    Down   1      --                 0060.4731.2A11
FastEthernet0/18    Down   1      --                 0060.4731.2A12
FastEthernet0/19    Down   1      --                 0060.4731.2A13
FastEthernet0/20    Down   1      --                 0060.4731.2A14
FastEthernet0/21    Down   1      --                 0060.4731.2A15
FastEthernet0/22    Down   1      --                 0060.4731.2A16
FastEthernet0/23    Down   1      --                 0060.4731.2A17
FastEthernet0/24    Down   1      --                 0060.4731.2A18
GigabitEthernet0/1  Down   1      --                 0060.4731.2A19
GigabitEthernet0/2  Down   1      --                 0060.4731.2A1A
```

Рисунок 3.26 – Результат конфігурації VLAN на комутаторі підмережі фінансового та HR відділу

Поділ підмереж на віртуальні підмережі дозволить логічно розмежувати трафік, а також забезпечить безпеку даних, що передаються.

Для передачі трафіку між VLAN необхідно додатково налаштувати роутер. Щоб передати трафік з однієї мережі VLAN в іншу, необхідно описати інтерфейс у кожній мережі.

Маршрутизація між VLAN буде налаштована на роутері It_router на інтерфейсі GigabitEthernet0/1 за допомогою технології інкапсуляції 802.1Q. [5]

На коммутаторі It_switch порт Fa0/1, веде до роутера, налаштованого як магістрального (trunk) порт.

Для логических портов на маршрутизаторе необходимо указать, что интерфейс будет получать трафик с метко, а также необходимо указать номер VLAN, соответствующий этому интерфейсу.

```
It_router(config)#interface g0/0
It_router(config-if)#no shutdown
It_router(config)#interface g0/0.21
It_router(config-subif)#encapsulation dot1Q 21
It_router(config-subif)#ip address 192.168.19.65 255.255.255.248
```

Такі ж кроки необхідно зробити і для VLAN22. Аналогічно налаштовується маршрутизатор підмережі «Фінанси та HR».

Результат налаштування маршрутизації між підмережами VLAN показаний на малюнку нижче.

```
Device Name: Router2
Device Model: 2911
Hostname: It_router

Port                  Link   VLAN   IP Address         IPv6 Address                          MAC Address
GigabitEthernet0/0    Up     --     <not set>          <not set>                             00D0.FF4D.3001
GigabitEthernet0/0.21 Up     --     192.168.19.65/29   <not set>                             00D0.FF4D.3001
GigabitEthernet0/0.31 Up     --     192.168.19.73/29   <not set>                             00D0.FF4D.3001
GigabitEthernet0/1    Down   --     <not set>          <not set>                             00D0.FF4D.3002
GigabitEthernet0/2    Down   --     <not set>          <not set>                             00D0.FF4D.3003
Serial0/2/0           Up     --     10.0.19.13/30      <not set>                             <not set>
Serial0/2/1           Down   --     <not set>          <not set>                             <not set>
Serial0/3/0           Up     --     10.0.19.6/30       <not set>                             <not set>
Serial0/3/1           Up     --     10.0.19.9/30       <not set>                             <not set>
```

Рисунок 3.27 – Результат налаштування маршрутизації VLAN на роутері It_router

3.5.3 Налаштування параметрів безпеки та адресації ПК в мережах VLAN

Для забезпечення безпеки та адресації ПК у VLAN необхідно:

- Дозволити доступ до порту лише одному вузлу;
- MAC-адреса пристрою додається до поточної конфігурації комутатора та є статичною.
- У разі порушення безпеки порт комутатора вимикається.

Для настройки комутатора виконуються наступні команди:

Включение режима інтерфейса для отримання доступу:

```
It_switch(config)#interface fa0/24
It_switch(config)#switchport mode access
```

Вхід до налаштування безпеки порту:

```
It_switch(config)#switchport port-security
```

Дозволити тільки одному вузлу доступ до порту:

```
It_switch(config)#switchport port-security maximum 1
```

Увімкнення запам’ятовування MAC-адрес:

```
It_switch(config)#switchport port-security mac-address sticky
```

Налаштування реакції на порушення безпеки порту: у разі порушення безпеки інтерфейс переходить у стан error-disabled і негайно вимикається:

```
It_switch(config)#switchport port-security violation shutdown
```

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Аналіз предметної галузі

У компанії «УнІТ» для HR відділ потребує інформаційної підтримки про співробітників. Для цього був проведений аналіз предметної області всередині компанії «УнІТ».

Аналіз предметної області – це процес дослідження та оцінки певної галузі знань або діяльності з метою виявлення її структури, ключових елементів, проблем і можливостей. Цей процес важливий при розробці нових інформаційних систем, створенні бізнес-стратегій, проектуванні продуктів тощо.

Результатом аналізу предметної області стала база даних, яка дозволить зберігати інформацію про співробітників компанії, про їх відпустки, про місця роботи, а також їх особисту інформацію.

4.2 Проектування бази даних співробітників компанії

На рисунку нижче представлена діаграма реляційних взаємозв'язків бази даних співробітників компанії. Під час аналізу предметної області було визначено 6 сутностей:

- Працівник (Employee).
- Особиста інформація (Personal Information).
- Кабінет (Cabinet).
- Відділ (Department).
- Позиція (Position).
- Відпустка (Vacation).

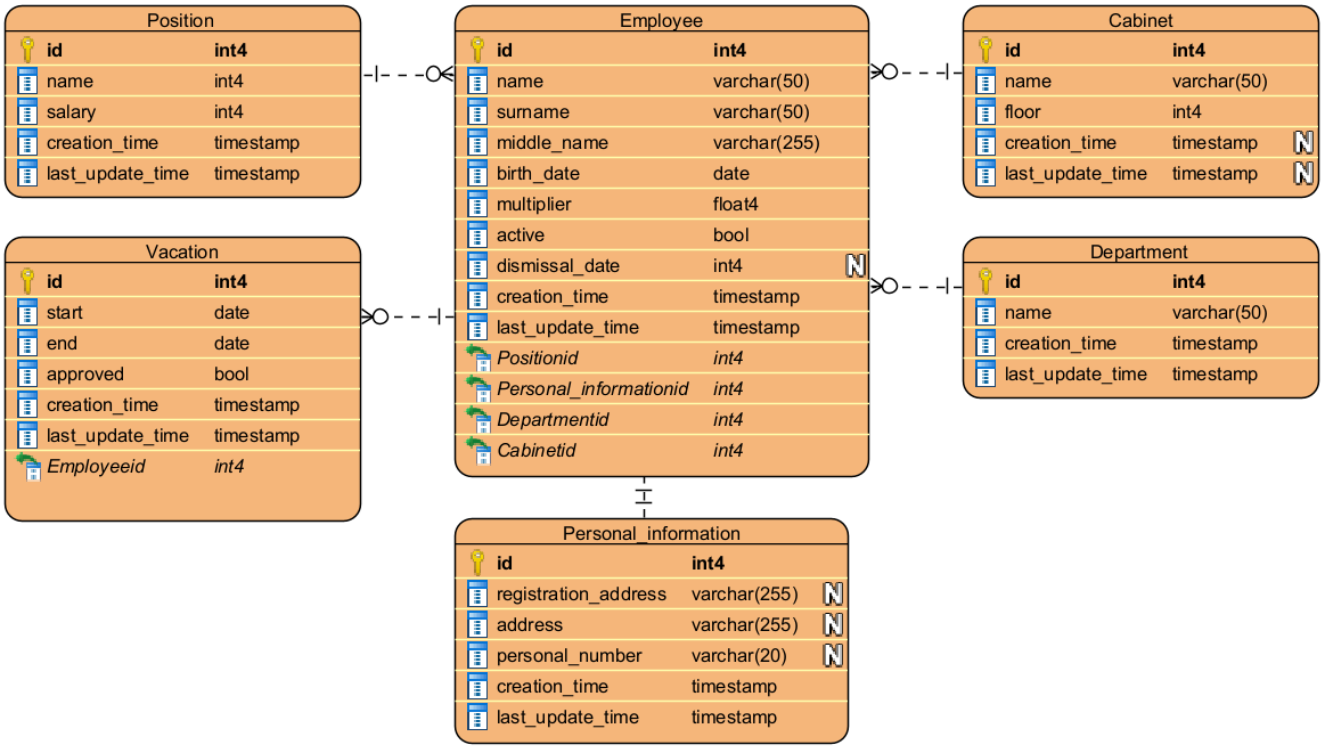

Рисунок 4.28 – Діаграма реляційних взаємозв'язків бази даних співробітників компанії

Сутність «Працівник» містить інформацію про працівника, прізвище, ім'я, по батькові, дату народження, діючого працівника або звільненого. Також сутність «Співробітник» має розширення у вигляді сутності «Особиста інформація», що дозволяє додатково зберігати інформацію про працівника. Ці дані розміщуються в окремій сутності, оскільки це зменшить навантаження на сервер бази даних при роботі з сутністю «Працівник».

Сутність «Відділ» носить довідковий характер і містить лише назву відділа.

Суб'єкт «Відпустка» зберігає інформацію про відпустки працівників, дати початку та закінчення, а також інформацію про те, чи підтверджена відпустка.

Сутність «Позиція» зберігає інформацію про позиція всередині компанії та про те, яка заробітна плата за цією позпцією.

Сутність «Кабінет» є довідковим і зберігає інформацію про офіси, де можуть знаходитися співробітники, і де цей офіс знаходиться.

4.2 Опис розробленої бази даних

У таблиці 4.6 описана фізична модель бази даних співробітників. Фізична модель побудована на основі діаграми реляційних зв'язків бази даних співробітників компанії (Рисунок 4.28).

Таблица 4.6 – Опис моделі фізичної бази даних

Поле	Тип	Опис
Працівник – Employee		
id	INTEGER	Ідентифікатор працівника. Ключове поле.
name	VARCHAR	Ім'я.
surname	VARCHAR	Прізвище.
middle_name	VARCHAR	По батькові.
email	VARCHAR	Корпоративна електронна пошта співробітника.
birth_date	DATE	Дата народження.
multiplier	REAL	Множитель плати.
active	BOOL	Активний працівник.
dismissal_date	DATE	Дата звільнення.
creation_time	TIMESTAMP	Час створення запису.
last_update_time	TIMESTAMP	Час останнього оновлення запису.
position_id	INTEGER	Ідентифікатор позиції. Довідковий ключ.
personal_information_id	INTEGER	Ідентифікатор персональної інформації. Довідковий ключ.
department_id	INTEGER	Ідентифікатор відділу. Довідковий ключ.
cabinet_id	INTEGER	ID кімнати. Довідковий ключ.
Позиція – Position		
id	INTEGER	Ідентифікатор позиції. Ключове поле.
name	VARCHAR	Назва.
salary	INTEGER	Ставка.
creation_time	TIMESTAMP	Час створення запису.
last_update_time	TIMESTAMP	Час останнього оновлення запису.
Отпуск – Vacation		
id	INTEGER	Ідентифікатор відпустки. Ключове поле.
start	DATE	Початок відпустки.
end	DATE	Закінчення відпустки.
approved	BOOL	Підтверджена відпустка чи ні.
creation_time	TIMESTAMP	Час створення запису.

Поле	Тип	Опис
last_update_time	TIMESTAMP	Час останнього оновлення запису.
Особиста інформація – Personal_information		
id	INTEGER	Ідентифікатор позиції. Ключове поле.
registration_address	TEXT	Адреса реєстрації працівника.
address	TEXT	Адреса проживання працівника.
personal_number	VARCHAR	Номер мобільного телефону.
creation_time	TIMESTAMP	Час створення запису.
last_update_time	TIMESTAMP	Час останнього оновлення запису.
Кабінет – Cabinet		
id	INTEGER	Ідентифікатор позиції. Ключове поле.
name	VARCHAR	Назва кабінета/кімнати.
floor	INTEGER	Поверх.
creation_time	TIMESTAMP	Час створення запису.
last_update_time	TIMESTAMP	Час останнього оновлення запису.
Відділ – Department		
id	INTEGER	Ідентифікатор позиції. Ключове поле.
name	VARCHAR	Назва відділу.
creation_time	TIMESTAMP	Час створення запису.
last_update_time	TIMESTAMP	Час останнього оновлення запису.

Для сутності «Кабінет», «Посада», «Відділ» і їх поля з ім'ям «name» накладаються обмеження унікальності – всі записи в цих таблицях повинні мати унікальні імена.

ВИСНОВКИ

В ході даної роботи детально розглядається комп'ютерна система IT-компанії «УнІт», в якій враховується можливість віддаленого доступу до мережевих ресурсів корпоративної мережі через VPN.

У результаті аналізу було встановлено, що впровадження комп'ютерної системи в «УнІт» є критично важливим для надання якісних IT-послуг. Також під час роботи було враховано специфіку роботи великої IT-компанії та висвітлено момент захисту корпоративних та клієнтських даних, запропоновано налаштування системи віддаленого доступу для співробітників компанії.

Запропонований графік роботи технічних фахівців компанії дозволяє підтримувати працездатність і оперативно вирішувати виникаючі проблеми з IT-інфраструктурою.

Результатом цієї роботи є спроектована комп'ютерна система для великої та середньої IT-компанії. Комп'ютерна система і її комп'ютерна мережа складається з 4-х локальних мереж і передбачає можливість віддаленого підключення користувача через VPN.

Спроектована комп'ютерна система дозволяє співробітникам розгортати віртуальні машини в межах однієї локальної комп'ютерної мережі і не засмічувати трафік загальної корпоративної мережі.

Впровадження комп'ютерної системи у великій IT-компанії є стратегічно важливим кроком, спрямованим на підвищення ефективності роботи, підвищення якості обслуговування клієнтів та забезпечення безпеки даних. Така система дозволить компанії не тільки підтримувати високі стандарти роботи, а й адаптуватися до швидко мінливих ринкових умов, залишаючись при цьому конкурентоспроможною та інноваційною.

ПЕРЕЛІК ПОСИЛАНЬ

[1] Л. І. Цвіркун, Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія, Л. І. Циркун, С. М. Ткаченко, Я. В. Панферова, Д. О. Бешта и Л. В. Бешта, Ред., Дніпро: НТУ «ДП», 2024, p. 63.

[2] UNIT, «About UNIT company,» UNIT, [В Інтернеті]. Available: https://www.linkedin.com/company/unitcomua.

[3] Cisco Systems, «Cisco 4461 Integrated Services Router,» Cisco, 2024. [В Інтернеті]. Available: https://www.cisco.com/c/en/us/support/routers/4461-integrated-services-router/model.html#~tab-documents. [Дата звернення: 2024].

[4] Cisco Systems, «Cisco Catalyst 9200 Switch Series,» [В Інтернеті]. Available: https://www.cisco.com/site/us/en/products/networking/switches/catalyst-9200-series-switches/index.html.

[5] IEEE Standards Association, IEEE Standards Association, 2022. [В Інтернеті]. Available: https://standards.ieee.org/ieee/802.1Q/6844/. [Дата звернення: 2024].

[6] Вінницький національний технічний університет, «Застосування масок під час IP-адресації,» Вінницький національний технічний університет, [В Інтернеті]. Available: https://web.posibnyky.vntu.edu.ua/fitki/3yarovijk_komp_merezhi/1.4.html. [Дата звернення: Апрель 2024].

[7] JavaRush, «Підмережі,» JavaRush, [В Інтернеті]. Available: https://javarush.com/ua/quests/lectures/ua.questservlets.level08.lecture02.

[8] International Organization for Standardization, «ISO/IEC 27001:2022,» International Organization for Standardization, 2022. [В Інтернеті]. Available: https://www.iso.org/standard/27001.

[9] YouControl, «УНІВЕРСАЛЬНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ,» YouControl, 3 6 2024. [В Інтернеті]. Available: https://youcontrol.com.ua/catalog/company_details/34891802/. [Дата звернення: 3 4 2024].

[10] UNIT, «ПРО КОМПАНІЮ “УНІТ”,» UNIT, 2024. [В Інтернеті]. Available: http://unit.com.ua/ua/o-kompanii-unit/.

[11] UNIT, «КЕРІВНИЦТВО КОМПАНІЇ,» UNIT, 2024. [В Інтернеті]. Available: http://unit.com.ua/ua/rukovodstvo/.

[12] А. О. Мельник, В. А. Мельник, В. С. Глухов и А. М. Сало, Кіберфізичні системи: багаторівнева організація та проектування, Магнолія, 2023.

[13] М. О. Хомуляк, Адміністрування комп'ютерних систем і мереж, Магнолія, 2023.

[14] Е. С. Таненбаум, Computer Networks, т. I, Pearson, 2010.

[15] Cisco, Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide, Cisco Systems, 2013.

[16] Cisco Networking Academy, «Cisco Packet Tracer,» Cisco Networking Academy, 2024. [В Інтернеті]. Available: https://skillsforall.com/learningcollections/cisco-packet-tracer.

[17] NetwerkKabel, «42U Server Rack Cabinet Hexagonal vented curved door (WxDxH) 800x1000x2055mm,» NetwerkKabel, 2024. [В Інтернеті]. Available: https://www.netwerkkabel.eu/en/42u-server-rack-cabinet-hexagonal-vented-79356068.html.

[18] Cisco Systems, «Configuring Administrator Usernames and Passwords,» Cisco Systems, 2024. [В Інтернеті]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3-2_0_se/system_management/configuration_guide/b_sm_32se_3850_cg_chapter_01001.html.

[19] IEEE, «IEEE 802.1Q,» IEEE, 2022. [В Інтернеті]. Available: https://standards.ieee.org/ieee/802.1Q/6844/.

[20] Wikipedia, «IEEE 802.1Q,» Wikipedia, 2024. [В Інтернеті]. Available: https://en.wikipedia.org/wiki/IEEE_802.1Q.

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖЕВОГО ОБЛАДНАННЯ

Текст програми
04.02070743.24012-01 12 01

Листів Х

2024

АНОТАЦІЯ

Ця програма містить частину налаштувань мережевого обладнання (комутатора та маршрутизатора) за допомогою Cisco IOS для компонентів корпоративної мережі компанії «УнІТ». Команди призначені для налаштування протоколу динамічної маршрутизації, роботи сервісів AAA та DHCP, налаштування мережевих інтерфейсів пристроїв та налаштування Internet.

ЗМІСТ

Додаток А. Налаштування маршрутизатора Internal_it_router

```
en
conf t
no ip domain-lookup
hostname Inner_it_router
service password-encryption
enable secret 123_shvets
line console 0
password 123_shvets
login
exit
banner motd #123-20z ShvetsAD access passwd#

username 123_20z_Shvets password admin
ip domain name Inner_it_router
crypto key generate rsa
yes
1024
line vty 0 4
login local
transport input ssh
in gig0/0
ip address 192.168.19.97 255.255.255.224
no sh

in ser0/3/0
ip address 10.0.19.2 255.255.255.252
no sh

in ser0/2/0
ip address 10.0.19.17 255.255.255.252
no sh

in ser0/3/1
ip address 10.0.19.10 255.255.255.252
no sh

in ser0/2/1
ip address 10.0.19.21 255.255.255.252
no sh



exit
```

```
en
conf t
router ospf 11
network 192.168.19.97 0.0.0.31 area 0
network 10.0.19.2 0.0.0.3 area 0
network 10.0.19.17 0.0.0.3 area 0
network 10.0.19.10 0.0.0.3 area 0
network 10.0.19.21 0.0.0.3 area 0

in gig0/0
ip ospf cost 7500

in ser0/2/0
bandwidth 128
clock rate 128000
ip ospf cost 7500

in ser0/2/1
bandwidth 128
clock rate 128000
ip ospf cost 7500

in ser0/3/0
bandwidth 128
clock rate 128000
ip ospf cost 7500

in ser0/3/1
bandwidth 128
clock rate 128000
ip ospf cost 7500

aaa new-model
aaa authentication login default local
aaa authentication login Login group radius local

line console 0
login authentication Login

line vty 0 4
login authentication default

radius-server host 192.168.19.102 auth-port 1645
radius-server key 123_20z
```

Додаток Б. Налаштування комутатора It_switch

```
en
conf t
no ip domain-lookup
hostname it_switch
service password-encryption
enable secret 123_shvets
line console 0
password 123_shvets
login
exit
banner motd #123-20z ShvetsAD access passwd#

username 123_20z_Shvets password admin
ip domain name it_switch
crypto key generate rsa
yes
1024
line vty 0 4
login local
transport input ssh

end
conf t
vlan 21
name dev_qa_department
vlan 22
name analytics_tech_support_department
vlan 99
name management
vlan 100
name native

int fa0/1
switchport trunk native vlan 100
switchport trunk allowed vlan 21, 22, 99-100
switchport mode trunk

int range fa0/2-5
switchport mode access
switchport access vlan 21

int range fa0/6-8
switchport mode access
```

```
switchport access vlan 22

interface Vlan99
ip address 192.168.19.83 255.255.255.240
no shutdown
ip default-gateway 192.168.19.82


interface fa0/24
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
```

Додаток В. Створення таблиць бази даних

```
CREATE TABLE Cabinet (
  id              INTEGER NOT NULL PRIMARY KEY AUTOINCREMENT,
  name            varchar(50) NOT NULL UNIQUE,
  floor           integer(2) NOT NULL,
  creation_time    timestamp,
  last_update_time timestamp);

CREATE TABLE Department (
  id              INTEGER NOT NULL PRIMARY KEY AUTOINCREMENT,
  name            varchar(50) NOT NULL UNIQUE,
  creation_time    timestamp NOT NULL,
  last_update_time timestamp NOT NULL);

CREATE TABLE Employee (
  id                  INTEGER NOT NULL PRIMARY KEY AUTOINCREMENT,
  name                varchar(50) NOT NULL,
  surname             varchar(50) NOT NULL,
  middle_name         varchar(255) NOT NULL,
  birth_date          date NOT NULL,
  multiplier          real(10) NOT NULL,
  active              integer(1) NOT NULL,
  dismissal_date      integer(10),
  creation_time       timestamp NOT NULL,
  last_update_time    timestamp NOT NULL,
  Positionid          integer(10) NOT NULL,
  Personal_informationid integer(10) NULL,
  Departmentid        integer(10) NOT NULL,
  Cabinetid           integer(10) NOT NULL,
  FOREIGN KEY(Cabinetid) REFERENCES Cabinet(id),
  FOREIGN KEY(Departmentid) REFERENCES Department(id),
  FOREIGN KEY(Personal_informationid) REFERENCES Personal_information(id),
  FOREIGN KEY(Positionid) REFERENCES Position(id));

CREATE TABLE Personal_information (
  id                  INTEGER NOT NULL PRIMARY KEY AUTOINCREMENT,
  registration_address varchar(255),
  address             varchar(255),
  personal_number     varchar(20),
  creation_time       timestamp NOT NULL,
  last_update_time    timestamp NOT NULL);

CREATE TABLE Position (
  id              INTEGER NOT NULL PRIMARY KEY AUTOINCREMENT,
```

```
  name            varchar(50) NOT NULL UNIQUE,
  salary          integer(10) NOT NULL,
  creation_time    timestamp NOT NULL,
  last_update_time timestamp NOT NULL);

CREATE TABLE Vacation (
  id              INTEGER NOT NULL PRIMARY KEY AUTOINCREMENT,
  "start"         date NOT NULL,
  "end"           date NOT NULL,
  approved        integer(1) NOT NULL,
  creation_time    timestamp NOT NULL,
  last_update_time timestamp NOT NULL,
  Employeeid      integer(10) NOT NULL,
  FOREIGN KEY(Employeeid) REFERENCES Employee(id));
```