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

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Дробот Денис Юрійович
(П.І.Б.)
академічної групи 123−20ск−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 компанії «LANARS» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
кваліфікаційної роботи	доц. Булана Т.М.			
розділів:				
апаратний розділ	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2023

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

"___" _____ 2023 року.

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Дробот Д.Ю. **академічної групи** 123−20ск−1
(прізвище, ініціали) (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 компанії «LANARS» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі
(назва за наказом ректора)

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

Розділ	Зміст завдання	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	
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	

Завдання видано _____ доц. Булана Т.М.
(підпис керівника) (прізвище та ініціали)

Дата видачі _____

Дата подання до атестаційної комісії _____

Прийнято до виконання _____ Дробот Д. Ю.
(підпис студента) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 108 с., 27 рис., 2 табл., 1 дод., 8 джерел.

СЕРВЕРИ, ВІДДІЛЕНА МЕРЕЖА, ДИНАМІЧНІ ПРОТОКОЛИ, МЕРЕЖЕВІ КОМПОНЕНТИ, НАЛАШТУВАННЯ ПРИСТРОЇВ

Об'єкт розробки: Комп'ютерна система компанії «LANARS» з детальним опрацюванням побудови, налаштування та забезпечення безпеки корпоративної мережі.

Мета: Створення комп'ютерної системи для компанії «LANARS» з фокусом на побудові, налаштуванні та забезпеченні безпеки корпоративної мережі.

Розроблена комп'ютерна система забезпечує гнучку зміну числа і набору основних функцій шляхом перепрограмування. Вона орієнтована на побудову та налаштування корпоративної мережі компанії «LANARS».

Система розроблена з відкритим доступом і надає можливість технічної та програмної модернізації, а також забезпечує об'єднання підрозділів в мережу. Вона здійснює збір, обробку та накопичення інформації у базах даних, забезпечує комунікацію між кінцевими користувачами в різних підрозділах та забезпечує доступ до загальних ресурсів.

Розробка комп'ютерної мережі була виконана відповідно до завдання кваліфікаційної роботи бакалавра. Схема мережі була реалізована у вигляді моделі на симуляторі Cisco Packet Tracer, і її робота була перевірена

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

ГО	- громадська організація;
ЗІРКА	- Захист і Реконструкція Країни;
КС	– комп’ютерна система;
ПК	– персональний комп’ютер;
Ethernet	– технологія передачі даних по мережі;
UTP	– не екранована кручена пара;
FTP	– екранована кручена пара;
WAN	– (Wide Area Network) це глобальна комп'ютерна мережа;
VPN	– (ViRual Private Network) віртуальна приватна мережа;
QoS	– (Quality of Service) технологія надання різних класів трафіку різних пріоритетів в обслуговуванні;
Wi−Fi	– технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11;
GSM	– (Global System for Mobile Communications) глобальний стандарт цифрового мобільного стільникового зв'язку з розділенням каналів за часом та частотою

ВСТУП

У сучасному світі комп'ютерні системи та мережі є невід'ємною частиною ефективної роботи компаній. Комп'ютерні мережі дозволяють забезпечувати швидку та безперебійну передачу даних, сприяють спільній роботі з використанням спільних ресурсів та забезпечують високу рівень безпеки і захисту інформації.

У рамках кваліфікаційної роботи бакалавра, метою дослідження є детальне опрацювання побудови та налаштування корпоративної комп'ютерної системи для компанії «LANARS». Компанія «LANARS» є провідним розробником програмного забезпечення та надає широкий спектр послуг у сфері інформаційних технологій. З метою забезпечення високоефективної роботи та підвищення продуктивності, важливо розробити та налаштувати оптимальну корпоративну мережу, яка відповідатиме потребам компанії.

Дослідження включатиме аналіз потреб компанії «LANARS», виявлення технічних вимог та визначення оптимальної конфігурації мережі. Будуть розглянуті різні аспекти побудови мережі, включаючи вибір мережевого обладнання, налаштування протоколів зв'язку, забезпечення безпеки та резервування даних. При розробці корпоративної мережі, будуть враховані поточні стандарти та рекомендації у сфері мережевих технологій. Окрему увагу буде приділено аналізу особливостей компанії «LANARS», зокрема, потребам її співробітників, обсягу трафіку, вимог до безпеки даних та доступу до ресурсів віддалених робочих місць. На основі цього аналізу буде розроблений детальний план побудови мережі, включаючи розташування мережевого обладнання, розподіл підмереж та налаштування мережевих пристроїв.

Завершення даної кваліфікаційної роботи надасть компанії «LANARS» детальну стратегію побудови та налаштування корпоративної мережі, що

відповідає її потребам та сприятиме підвищенню продуктивності та ефективності роботи співробітників. Результати цього дослідження можуть бути використані як основа для реалізації проекту з побудови мережі у компанії.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Цифрова трансформація ІТ компаній України в умовах війни

Українська ІТ-індустрія знаходиться в стадії швидкого росту і займає третє місце в структурі експорту послуг з України за даними минулого року. Цей сектор відрізняється значним обсягом ІТ-фахівців, експортною виручкою та сумою податків, сплачених до державного бюджету [1].

На сьогоднішній день кількість ІТ-фахівців у галузі розвитку інформаційних технологій перевищує 100 тисяч програмістів, а за прогнозами експертів, ця цифра продовжить зростати в Україні. Це обумовлено переважно високою ІТ-експертизою українських розробників, які мають міцну освітню базу і розробляють технологічні продукти і рішення для відомих світових брендів і компаній зі списку FoRune 500.

Цифрові девайси світових брендів домінували на ринку персональних комп'ютерів в корпоративному та приватному секторах в Україні до 2022 року. Однак, з початком воєнних дій спостерігається стрімкий ріст попиту на повноформатні та мікроформатні персональні комп'ютери. Після знищення складів і виробничих потужностей багатьох дистриб'юторів та виробників ПК в Україні, лише виробничий підрозділ "ІТ-Інтегратор" Prime залишився одним з небагатьох підприємств, здатних виробляти й поставляти до двох тисяч персональних комп'ютерів на місяць.

Умови воєнного часу, зростаючі кібератаки, перевантаження мереж та потреба в захисті комунікацій змусили клієнтів Prime Computers з різних галузей економіки переглянути свій підхід до проектування та модернізації інформаційних систем на своїх підприємствах. Навіть в умовах війни, ІТ-інфраструктура установ і організацій банківського та освітнього секторів, військових підрозділів, державних підприємств, приватних компаній та холдингів активно модернізується [2].

Корпоративні замовники вибирають комп'ютерні системи вітчизняного виробництва Prime не лише через їх надійність та доступні ціни, але й завдяки швидкості виробництва оптових та дрібногуртових партій комп'ютерів будь-яких конфігурацій. Навіть у сьогоднішні часи Prime Computers гордиться тим, що навіть в найбільш напружених фазах війни, воно не припиняло виробництво та зберігало ланцюжки постачання іноземних комплектуючих. Крім того, воно здатне задовольнити не лише масові замовлення стандартних моделей PrimePC Solo30, але й виконувати індивідуальні конфігурації з доставкою по всій території України.

Незалежно від розміру офісу компанії, контакт-центру, кіберспортивної команди чи потреби в комплексному оснащенні інформаційної системи організації, мережі, відомства або корпорації, комп'ютери Prime залишаються найкращим та надійним рішенням для технічної модернізації та своєчасного інвестування в сучасні IT-системи в Україні.

Крім продажу комп'ютерів, Prime Computers надає послуги з налаштування та оновлення програмного забезпечення, а також забезпечує сервісну підтримку протягом 3 років з гарантійним та постгарантійним обслуговуванням.

Не дивлячись на вище перераховані умови. Які виникли під час війни, українська IT-індустрія продовжує розширюватися, забезпечуючи високу якість та інноваційні рішення для глобального ринку. Її вагомий внесок у економіку виявляється через зростання кількості IT-фахівців, виручки від експорту та сплачених податків, сприяючи розвитку країни та зміцненню позицій у міжнародному IT-середовищі.

Згідно з даними IT-комітету Союзу європейських бізнесменів у 2022 році більшість респондентів (83%) очікували зростання свого бізнесу, 15% директорів сподівалися зберегти показники на рівні 2021 року, а лише 2%

прогнозували погіршення стану справ у своєму бізнесі (у порівнянні з 14% минулого року) [2].

Прогнози фінансових результатів компаній на наступний рік значно зросли. Більшість підприємців, а саме 67%, очікували зростання доходів на рівні 10-20% у гривні. Цей показник повернувся до рівня 2020 року після значного спаду минулого року. 36% директорів очікували зростання доходів до 10% у натуральному виразі, а майже половина (49%) розраховувала на зростання від 10% до 20% [2].

Прогнози щодо курсу долара на наступний рік були схожі на минулорічні. Керівники компаній планували включати вартість валюти у свої бюджети в середньому на рівні 29 гривень за долар.

Усі респонденти опитування цього року заявили, що планують підвищувати заробітну плату своїм співробітникам у 2022 році. Більшість керівників (55%) планували підвищення заробітної плати на 5-10%. Інші 30% планували підвищення у розмірі 10-20%. Варто зазначити, що минулого року 15% компаній не мали можливості підвищити заробітну плату своїм працівникам.

Плани бізнесу щодо створення нових робочих місць також змінилися. У порівнянні з минулим роком, коли 60% підприємців не планували жодних змін у штаті.

Серед опитаних IT-компаній немає планів повністю закрити свій бізнес в Україні. Більшість IT-компаній (63%) не мають наміру здійснювати часткову або повну релокацію до кінця 2022 року. Тільки 14% опитаних розглядають часткову або повну релокацію за кордон до кінця року. Деякі компанії (23%) планують комбінувати релокацію, здійснюючи її як за кордоном, так і в межах України. Загалом, 37% компаній розглядають релокацію як можливий варіант до кінця поточного року. Однак, якщо ситуація в країні значно не зміниться, можна очікувати подальший зріст цього показника [2].

У 2023 році 28% керівників планують зберегти бізнес-показники на поточному рівні, тоді як 25% очікують погіршення стану справ у своєму бізнесі (проти 2% минулого року). Результат наведено на рис.1.1 [2].

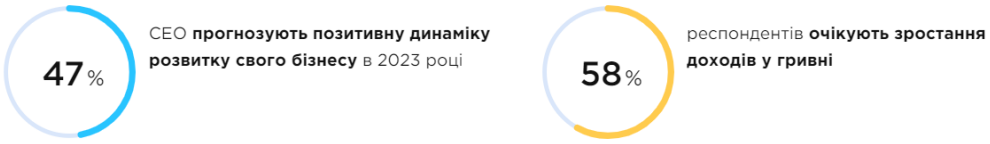


Рисунок 1.1 – Статистичні прогнози на 2023 рік [2]

Більшість компаній сподіваються на позитивний фінансовий результат у наступному році. Зокрема, 58% опитаних розраховують на зростання доходів у гривні, а 43% - у натуральному виразі. З цих, 31% очікують зростання доходів у гривні до 10%. Водночас 31% директорів передбачають зниження доходів у гривні, а 36% - у натуральному виразі.

1.2 Аналіз галузі та сценарії для застосування комп'ютерної системи "LANARS"

Галузь розробки апаратного та програмного забезпечення є однією з найбільш динамічних і швидко зростаючих галузей сучасного світу. У цьому конкурентному середовищі, компанія "LANARS" виділяється як міжнародний постачальник інноваційних рішень, спрямованих на розв'язання складних завдань бізнесу та забезпечення його конкурентоспроможності [3].

"LANARS" відома своїм глибоким зануренням у кожен проект та індивідуальним підходом до розробки IT-рішень. Компанія прагне зрозуміти потреби своїх клієнтів і надати їм найкращі технологічні рішення, що

допомагають бізнесу адаптуватися до постійно змінюючих умов ринку та ефективно виконувати завдання майбутнього.

Компанія "LANARS" використовує комп'ютерну систему, яка стала невід'ємною частиною її інфраструктури. Ця система допомагає забезпечувати безперебійну роботу компанії та сприяє підвищенню продуктивності її співробітників. Комп'ютерна система "LANARS" має на меті оптимізувати процеси внутрішньої комунікації, спільної роботи, обміну даними та забезпечення безпеки інформації [3].

Умови застосування комп'ютерної системи "LANARS" включають в себе потреби компанії у швидкій та безперебійній передачі даних, ефективному спілкуванні та спільній роботі співробітників усередині компанії та зовнішніми партнерами. Компанія "LANARS" розподілена на різні підрозділи та має глобальну присутність, тому необхідно, щоб комп'ютерна система забезпечувала ефективний обмін даними та спільну роботу між різними розташованими у різних місцях відділами та командами.

Крім того, важливими умовами застосування комп'ютерної системи "LANARS" є безпека даних та захист інформації. З урахуванням специфіки галузі, в якій працює компанія, захист конфіденційної інформації та інтелектуальної власності має вирішальне значення. Комп'ютерна система повинна бути належним чином захищена від несанкціонованого доступу та зловживань, забезпечуючи конфіденційність та цілісність даних.

У силу своїх міжнародних проектів та співпраці з різними бізнес-секторами, компанія "LANARS" також має потребу у масштабованій і гнучкій комп'ютерній системі. Вона повинна бути здатна відповідати зростаючим потребам компанії, легко масштабуватися та адаптуватися до нових вимог та технологічних тенденцій.

Отже, комп'ютерна система "LANARS" має вирішувати такі завдання, як забезпечення ефективної комунікації, спільної роботи та обміну даними між співробітниками, підрозділами та партнерами компанії, забезпечення безпеки та захисту інформації, а також масштабованості та гнучкості для відповіді на зростаючі потреби та вимоги компанії "LANARS".

1.3 Стислі відомості про технології збору та передачі інформації дляоб’єкта впровадження

Об’єкт впровадження комп'ютерної системи "LANARS" є комплексною корпоративною мережею, яка використовується в міжнародній компанії "LANARS" для оптимізації та ефективного управління їхніми виробничими процесами. Все частіше,ми зустрічаємо поняття цифровий бізнес (е-бізнес), що був визначений як зв'язуючий елемент цього діалогу та "співпраці". Поняття цифровий бізнес можна розглядати як найширший термін для характеристики цих процесів. Необхідно підкреслити різницю між електронним бізнесом та електронною комерцією. "Електронний бізнес - це не те саме, що й електронна комерція. Натомість, електронний бізнес охоплює те, що було названо електронною комерцією - купівлю та продаж товарів і послуг в Інтернеті [4].

Електронний бізнес має на меті покращити ефективність бізнесу за рахунок збільшення зв'язку в ланцюжку створення вартості та між бізнесами (див. рис. 1.2) [4]. Він використовує інтернет-технології з метою покращення послуг, зниження витрат та створення нових можливостей для бізнесу. Однак, окрім такого широкого розуміння, термін "електронний бізнес" часто використовується в більш вузькому значенні, коли споживачі купівля товарів через Інтернет. Відповідно до останніх промислових і дослідницьких розробок у цій роботі ми будемо використовувати термін "Електронний

бізнес" у його ширшому значенні - використання інтернет-технологій по всьому ланцюжку створення вартості.

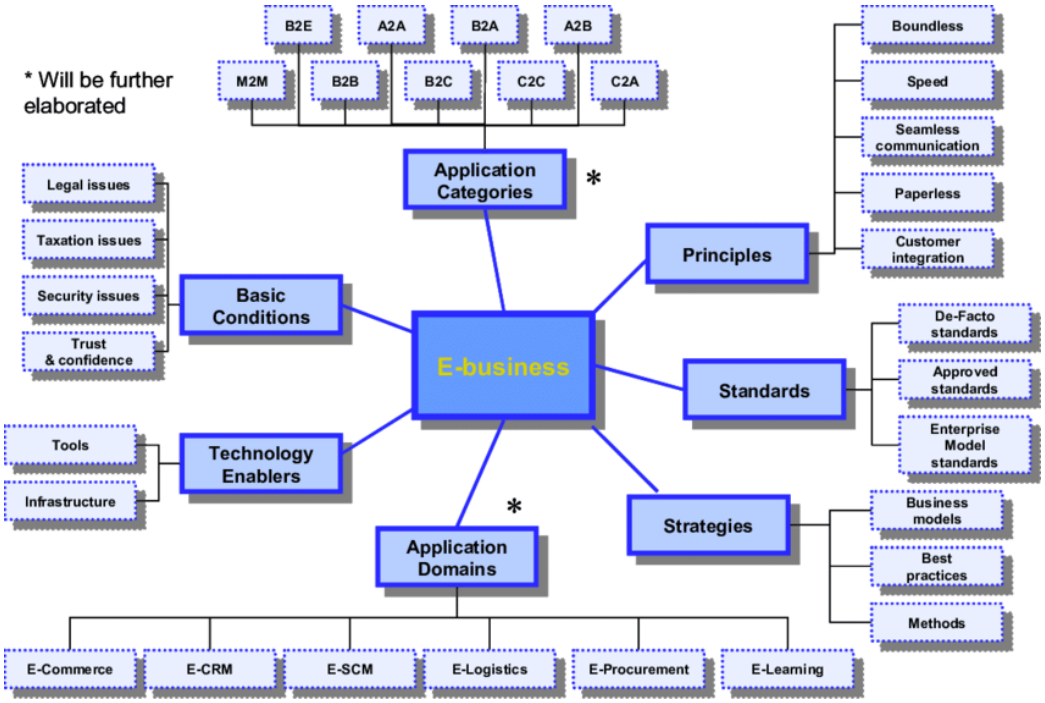


Рисунок 1.2 – Структура концептуальної моделі електронного бізнесу

Ця концептуальна модель цифрового або електронного бізнесу була розроблена авторами з метою інтегрувати основні аспекти при обговоренні терміну "електронний бізнес" Мета концептуальної моделі полягає в тому, щоб включити та інтегрувати різні точки зору на термін "електронний бізнес", такі як точка зору користувачів, функціональна точка зору, технічна точка зору. користувачів, функціональну точку зору, технічну точку зору та точку зору бізнесу. На малюнку показано розбивку терміну "електронний бізнес" на сім вимірів: категорії застосування, принципи стандарти, стратегії, сфери застосування, засоби та основні умови.

На основі вище вкладеного структура об’єкта впровадження включає такі складові як сервери, робочі станції, системи збору даних, тощо. Розглянемо детально.

Сервери. Об'єкт впровадження має централізовані сервери, що виконують різноманітні функції, включаючи зберігання та обробку даних, керування мережею та виконання розрахунків. Сервери забезпечують високу доступність та надійність системи, а також забезпечують безперервну роботу виробничих процесів.

Робочі станції. В об’єкті впровадження КС "LANARS" використовуються робочі станції, які є робочими місцями працівників. Вони підключені до централізованої мережі та використовуються для взаємодії з системою, отримання та передачі даних, а також керування виробничими процесами.

Комунікаційна інфраструктура. Об’єкт впровадження КС "LANARS" має розвинуту комунікаційну інфраструктуру, що забезпечує підключення всіх компонентів системи до мережі. Вона включає в себе комутатори, маршрутизатори, кабельну і безпроводову мережу, а також інші пристрої для забезпечення швидкого та надійного обміну даними між всіма складовими системи.

Системи збору даних. В об’єкті впровадження КС "LANARS" використовуються спеціальні системи збору даних, які забезпечують моніторинг та збір інформації з різних джерел. Ці системи можуть включати датчики, сенсори, вимірювальні пристрої та інші засоби для отримання реального часу даних про рух сировини, параметри виробничих процесів, якість продукції та іншу важливу інформацію. Зібрані дані передаються до централізованих серверів для подальшої обробки та аналізу.

Програмне забезпечення. Об’єкт впровадження КС "LANARS" включає різноманітне програмне забезпечення, яке забезпечує функціональність та управління системою. Це можуть бути спеціалізовані програми для контролю виробничих процесів, системи збору та аналізу даних, інструменти для візуалізації та моніторингу, а також програмне забезпечення для керування та налаштування мережі.

Об’єкт впровадження КС "LANARS" має структуровану архітектуру, що дозволяє забезпечити ефективну і надійну роботу системи. Всі компоненти та елементи системи взаємодіють між собою, щоб забезпечити оптимальний контроль та керування виробничими процесами. Ця структура дозволяє підвищити продуктивність, якість та ефективність виробництва, а також забезпечує зручність управління та моніторингу з будь-якої точки світу.

Організаційна структура КС "LANARS" включає різні рівні та підрозділи, які співпрацюють між собою для ефективного функціонування системи. Реалізована у вигляді єрархічної моделі, що є найпопулярнішим типом організаційної діаграми. Є кілька моделей, які є похідними від цієї моделі.

В ієрархічній організаційній структурі співробітники згруповані, і кожен працівник має одного чіткого керівника (рис.1.3) [4]. Групування здійснюється на основі кількох факторів, тому багато моделей виведено з цього. Нижче наведено деякі з цих факторів

Функція – співробітники групуються відповідно до функцій, які вони виконують. На зображенні нижче показано функціональну організаційну схему з фінансовими, технічними, кадровими та адміністраторськими групами.

Географія – співробітники групуються за регіонами. Наприклад, у США співробітники можуть бути згруповані відповідно до штату. Якщо це глобальна компанія, її можна згрупувати за країнами.

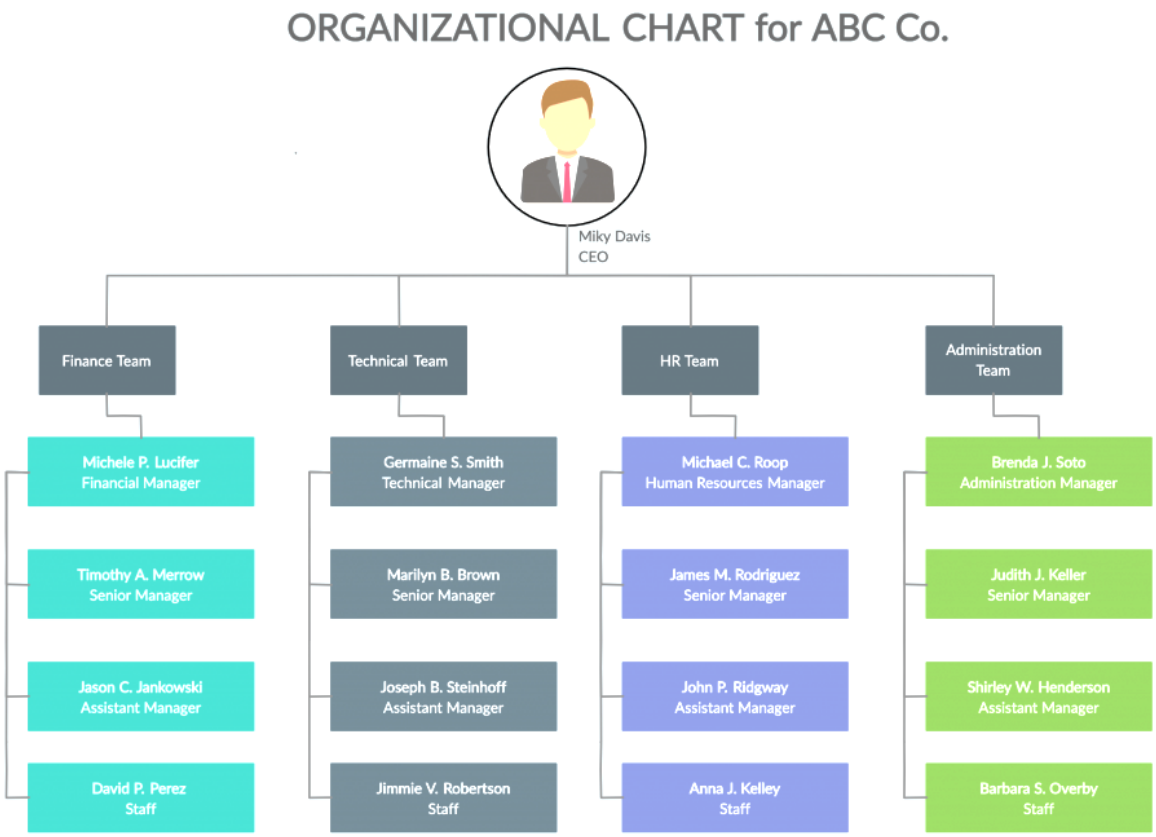


Рисунок 1.3 – Структура ієрархічної моделі

Продукт – якщо компанія виробляє кілька продуктів або пропонує різні послуги, її можна згрупувати відповідно до продукту чи послуги.

Плюси [4]:

– допомагає встановити чітку лінію повноважень і звітності в організації;

– уточнює ролі та обов’язки співробітників;

– встановлює чіткий шлях кар’єри для працівників, що, у свою чергу, може підтримувати їхню мотивацію;

– дозволяє співробітникам бути глибокими фахівцями, оскільки вони, швидше за все, займатимуть ніші.

Мінуси [5]:

– повільне прийняття рішень через складний ланцюжок командування;

– відключення співробітників нижчого рівня від співробітників вищого рівня управління;

– неузгодженість у спілкуванні через вертикальні та горизонтальні рівні між командами;

– обмежена інформація через дуже невеликий низхідний потік інформації до нижчих службовців.

Основні елементи організаційної структури компанії "LANARS" описано нижче.

Виконавче керівництво: Цей рівень включає вище керівництво компанії "LANARS". Виконавчі керівники встановлюють загальну стратегію розвитку КС, приймають важливі рішення та відповідають за розробку та впровадження комп’ютерних систем.

Відділ проектування: Цей підрозділ займається розробкою та проектуванням КС "LANARS". Він складається з інженерів та спеціалістів з різних областей, які спільно працюють над створенням архітектури системи, вибором необхідного обладнання та програмного забезпечення.

Відділ розробки: Цей підрозділ відповідає за програмування та розробку програмного забезпечення для КС "LANARS". Він включає розробників, програмістів та тестувальників, які працюють над створенням функціональних модулів, інтерфейсів та інших компонентів системи.

Відділ інтеграції: Цей підрозділ відповідає за інтеграцію різних компонентів КС "LANARS" в єдину функціональну систему. Він забезпечує взаємодію між апаратними пристроями, програмним забезпеченням та системами збору даних, щоб забезпечити їх взаємодію та спільну роботу.

Відділ підтримки: Цей підрозділ надає технічну підтримку та обслуговування К С "LANARS" після впровадження. Він складається з команди фахівців, які забезпечують надійну та ефективну роботу КС. Цей відділ відповідає за вирішення проблем, підтримку користувачів, виявлення і усунення помилок, а також проведення оновлень та модернізації системи.

Відділ безпеки: Оскільки безпека є ключовим аспектом в комп'ютерних системах, "LANARS" має спеціальний відділ, який відповідає за захист системи від зовнішніх загроз, забезпечення конфіденційності та цілісності даних, а також впровадження заходів для запобігання несанкціонованому доступу.

Відділ збору та аналізу даних: Цей підрозділ відповідає за збір, обробку та аналіз даних, які зібрані з КС "LANARS". Він використовує різні інструменти та методи для отримання цінної інформації з даних, що допомагає в прийнятті управлінських рішень та вдосконаленні процесів.

Організаційна структура КС "LANARS" побудована таким чином, щоб забезпечити високу координацію та співпрацю між підрозділами, що дозволяє ефективно виконувати завдання, забезпечувати надійну роботу системи та задовольняти потреби користувачів. Кожен відділ має свої

функціональні обов'язки та взаємодіє з іншими, щоб забезпечити гармонійну роботу всієї системи "LANARS".

1.4 Принципи, технічні способи інформаційного забезпечення об’єкта впровадження

На сьогоднішній день кожна компанія використовує системи управління базами даних (СУБД). Компанія LANARS є не виключенням і використовує розподілені бази даних, які забезпечують переваги розподілених обчислень у сфері систем управління базами даних.

Розподілене управління базами даних пропонується з різних причин, від організаційної децентралізації до економічної оптимізації та більшої автономії.

Основні переваги такого типу СУБД є:

– організаційну структуру. Наприклад, всі філії компанії мають доступ до централізованої бази даних, а співробітники філій можуть отримувати доступ лише до локальних баз даних;

– сепаратизм і місцеву автономію. Адміністратор бази даних на глобальному рівні відповідає за всю систему, але може делегувати відповідальність на місцевий рівень, де можуть керувати локальними базами даних;

– підвищення доступності та надійності даних. Відмова одного з вузлів або лінії зв'язку між ними не призводить до повної недоступності системи, а лише до обмеженого впливу на деякі компоненти;

– економічні переваги. Створення мережі з розподіленими базами даних може бути ефективнішим з економічної точки зору. Такі бази даних

можна легко масштабувати вгору або вниз залежно від потреб;

– модульність системи. Розширення системи шляхом додавання нових вузлів мережі не впливає на функціонування існуючих компонентів, що спрощує майбутнє розширення і розвиток.

Крім розподілених баз даних, компанія LANARS також активно використовує хмарні обчислення для забезпечення своїх послуг та розробок.

Використання хмарних обчислень [5] дозволяє компанії зберігати, обробляти та надавати доступ до даних та додатків через Інтернет, замість розміщення їх на локальних серверах. Це надає такі переваги:

– масштабованість: Хмарні платформи надають можливість збільшувати або зменшувати обчислювальні ресурси в залежності від потреб. Це дозволяє LANARS гнучко реагувати на змінюються вимоги проектів та забезпечувати ефективне використання ресурсів.

– висока доступність: Хмарні платформи зазвичай мають географічну розподіленість дата-центрів, що дозволяє забезпечувати високу доступність даних та додатків.

Це важливо для компанії LANARS, оскільки вони надають послуги з управління базами даних, які потребують неперервного доступу до інформації:

– безпека даних: хмарні платформи надають механізми захисту даних, такі як шифрування та механізми автентифікації. це дозволяє lanars забезпечувати конфіденційність та цілісність даних своїх клієнтів;

– швидкість розгортання: використання хмарних обчислень дозволяє швидко розгортати середовища для розробки, тестування та виконання проектів. це дозволяє компанії lanars ефективно впроваджувати

нові рішення та швидко реагувати на потреби клієнтів;

– економічність: використання хмарних обчислень дозволяє компанії LANARS зменшити витрати на придбання та утримання власних серверів і обладнання. Замість цього, вони можуть користуватись інфраструктурою, наданою хмарним провайдером, оплачуючи лише за використані ресурси. Це дозволяє компанії ефективно використовувати свої фінансові ресурси та зосередитись на розробці та наданні якісних послуг своїм клієнтам;

– застосування хмарних обчислень в LANARS дозволяє їм забезпечувати високу продуктивність, масштабованість та доступність своїх сервісів. Клієнти компанії можуть впевнено розраховувати на надійність та швидкість обробки даних завдяки використанню сучасних хмарних технологій;

– додатково, LANARS використовує хмарні обчислення для резервного копіювання та відновлення даних. Це дозволяє забезпечити надійне збереження і доступ до даних у випадку виникнення аварійних ситуацій або втрати даних.

– загалом, використання хмарних обчислень стало важливою складовою стратегії LANARS для забезпечення ефективного функціонування та надання якісних IT-послуг своїм клієнтам. Це дозволяє компанії використовувати передові технології, забезпечувати безпеку даних та масштабованість ресурсів, що відповідає сучасним вимогам у галузі інформаційних технологій.

Захист даних, інформаційна безпека та конфіденційність клієнтів [6] є важливими пріоритетами для компанії "LANARS". Компанія розуміє, що

володіння та обробка конфіденційної інформації є великою відповідальністю і зобов'язується забезпечувати високий рівень захисту даних своїх клієнтів.

LANARS використовує сучасні методи та технології для захисту інформації від несанкціонованого доступу, втрати або пошкодження. Компанія має в силу строгі політики безпеки, які включають в себе застосування шифрування, використання механізмів аутентифікації та авторизації, а також контроль доступу до систем та даних.

Крім того, LANARS регулярно оновлює свої системи та програмне забезпечення, щоб запобігти використанню вразливостей. Компанія також веде моніторинг систем та мережі, щоб вчасно виявляти можливі загрози та аномалії в роботі, та приймає необхідні заходи для їх усунення.

Компанія "LANARS" дотримується вимог законодавства щодо захисту персональних даних та конфіденційності інформації. Всі співробітники підлягають обов'язковому навчанню з питань кібербезпеки та ведення ділової комунікації, що допомагає забезпечити належний рівень конфіденційності та запобігти можливим витокам даних.

Крім того, LANARS встановлює процедури резервного копіювання даних, що дозволяє відновлювати інформацію в разі непередбачуваних ситуацій, таких як технічні збої або кібератаки. Застосування регулярних резервних копій допомагає зберегти дані клієнтів у безпеці та гарантує їх доступність навіть в надзвичайних обставинах.

Компанія "LANARS" також встановлює політики доступу до інформації, обмежуючи доступ до даних лише необхідним співробітникам та використовуючи механізми контролю доступу. Це допомагає попередити несанкціоноване використання та розголошення конфіденційної інформації.

Враховуючи важливість захисту даних, інформаційної безпеки та конфіденційності, компанія "LANARS" забезпечує своїх клієнтів високим рівнем захисту та надійності, що дозволяє їм впевнено співпрацювати та довіряти свою конфіденційну інформацію компанії. Захист даних дозволяє уникнути витоку конфіденційних даних, втрати важливої інформації або її пошкодження, а також забезпечує дотримання приватності клієнтів.

Надійний захист даних має кілька важливих переваг для клієнтів компанії "LANARS":

1. Конфіденційність: Клієнти можуть бути впевнені, що їх конфіденційна інформація, така як особисті дані, комерційні та фінансові відомості, буде оброблятися з належною обережністю і буде захищена від несанкціонованого доступу.

2. Довіра: Забезпечення безпеки даних сприяє створенню довіри між компанією "LANARS" та її клієнтами. Клієнти можуть бути впевнені, що їх інформація буде оброблятися з високим рівнем захисту, що сприяє побудові довгострокових взаємовигідних стосунків.

3. Законознавство: Компанія "LANARS" дотримується вимог законодавства щодо захисту даних і конфіденційності. Це дозволяє клієнтам бути впевненими, що їх дані обробляються згідно зі стандартами і вимогами безпеки, що забезпечує їх легальне та етичне використання.

4. Збереження репутації: Надійний захист даних допомагає уникнути ситуацій, пов'язаних з втратою або витоком конфіденційної інформації, що може негативно позначитися на репутації клієнтів.

5. Виконання регуляторних вимог: Багато галузей мають специфічні вимоги щодо захисту даних, наприклад, у сфері фінансів, охорони здоров'я, юриспруденції тощо. Забезпечення високого рівня захисту даних допомагає

компанії "LANARS" відповідати цим вимогам і запобігати можливим санкціям або правовим проблемам.

6. Зменшення ризику втрати даних: Надійний захист даних дозволяє зменшити ризик втрати важливої інформації, що може призвести до фінансових втрат, порушення довіри та втрати конкурентної переваги. Забезпечення безпеки даних допомагає уникнути непередбачуваних наслідків та зберегти цінні активи компанії та її клієнтів.

Усі ці аспекти важливі для компанії "LANARS", оскільки вона прагне забезпечити надійний захист даних, інформаційну безпеку та конфіденційність своїх клієнтів. Це дозволяє клієнтам впевнено співпрацювати з компанією, знаючи, що їх дані захищені та обробляються з найвищим рівнем уважності та застережності.

1.5 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об’єкта проектування, відомих рішень у галузі

При проведенні аналітичного огляду існуючих способів обробки та передачі інформації та принципів побудови об’єкта проектування, одним з розглянутих варіантів є Cisco Enterprise Architecture. Cisco Enterprise Architecture є комплексною моделлю для проектування та впровадження корпоративних мереж. Вона надає фреймворк та рекомендації щодо організації мережі, враховуючи вимоги до безпеки, доступності та ефективності.

Cisco Enterprise Architecture базується на концепції розбиття мережі на функціональні модулі та шари. Ця модель включає такі ключові компоненти:

– інфраструктурний шар включає мережеві пристрої, такі як комутатори, маршрутизатори та файрволи. Він забезпечує фізичне підключення та передачу даних у мережі;

– прикладний шар охоплює програмне забезпечення та сервіси, необхідні для роботи додатків і послуг. Він включає сервери додатків, системи керування та інші компоненти, що забезпечують функціонування додатків;

– корпоративний шар орієнтований на підтримку бізнес-процесів і включає рішення, спрямовані на управління обліком, безпекою, керуванням політиками та іншими бізнес-аспектами.

В рамках Cisco Enterprise Architecture доступні різні технології та рішення, які можуть бути використані для побудови комплексної мережевої інфраструктури.

1.6 Завдання і мета роботи

Завданням даної кваліфікаційної роботи бакалавра є розробка комп'ютерної системи для IT-компанії "LANARS" з детальним опрацюванням побудови та налаштування корпоративної мережі.

З урахуванням існуючої мережевої архітектури в компанії, її підмереж, взаємозв'язків та кількості комп'ютерів і обладнання, необхідно здійснити наступні кроки:

Крок 1 – налаштування топології мережі. Вибір оптимальної топології, яка відповідає потребам компанії "LANARS". Це може бути зіркова, шина, кільцева або ієрархічна топологія, в залежності від розміру мережі і вимог щодо масштабованості та надійності.

Крок 2 – вибір інтерфейсів каналів зв'язку. Визначення найкращих інтерфейсів передачі даних для підключення комп'ютерів і обладнання до мережі. Це можуть бути Ethernet, Wi-Fi, оптоволоконний кабель тощо.

Крок 3 – вибір протоколу обміну. Визначення протоколу, який буде використовуватися для ефективного обміну даними в мережі. Наприклад, TCP/IP, UDP, HTTP тощо.

Крок 4 – розрахунок топологічної схеми комп'ютерної системи. Розроблення детальної схеми, яка включає всі підмережі, мережеві вузли, комутатори, роутери та інше обладнання. Врахування логіки з'єднань, адресації та маршрутизації даних.

Крок 5 – налаштування маршрутизації комп'ютерної мережі. Встановлення оптимальних маршрутів для передачі даних між різними підмережами та вузлами.

Крок 6 – моделювання і перевірка комп'ютерної системи. Використовуючи спеціалізовані інструменти, проведення моделювання та симуляції роботи комп'ютерної системи. Це дозволяє виявити потенційні проблеми та перевірити ефективність мережі перед її фактичним впровадженням.

Крок 7 – аналіз об'єкта проектування нової мережі. Детальний аналіз потреб і вимог компанії "LANARS" щодо мережі, включаючи засоби збору і передачі даних. Врахування особливостей роботи компанії, її бізнес-процесів та вимог щодо безпеки та надійності.

Крок 8 – Вибір фізичного середовища, кабелів, портів і роз'ємів. Визначення оптимального фізичного з'єднання для підключення мережевих пристроїв та вузлів. Врахування стандартів та вимог щодо швидкості передачі даних, надійності та ефективності.

Крок 9 – Вибір мережевих пристроїв і компонентів. Визначення необхідного мережевого обладнання, яке відповідає потребам компанії. Це можуть бути комутатори, роутери, маршрутизатори, файрволи та інше обладнання.

Крок 10 – Розрахунок енергоспоживання, обсягів і швидкості передачі даних. Врахування параметрів мережевих каналів, їх пропускної здатності та затримок в обробці даних. Розрахунок енергоспоживання мережевого обладнання та оптимізація його роботи.

Загальною метою проекту є розробка та впровадження корпоративної мережі для компанії "LANARS", яка буде відповідати її потребам та вимогам щодо безпеки, надійності та ефективності. Після завершення розробки та налаштування мережі, будуть проведені тестування та перевірки для забезпечення її правильної роботи.

1.7 Визначення можливих напрямків рішення поставлених завдань

Визначення можливих напрямків рішення поставлених завдань включає розгляд різних підходів та варіантів, які можуть бути використані для досягнення поставлених цілей. Основним завданням є виявлення оптимальних шляхів вирішення проблеми та забезпечення найкращих результатів. Для вирішення завдань кваліфікаційної роботи з проектування корпоративної мережі було обрано таку мережеву топологію представлену на рис.1.4.

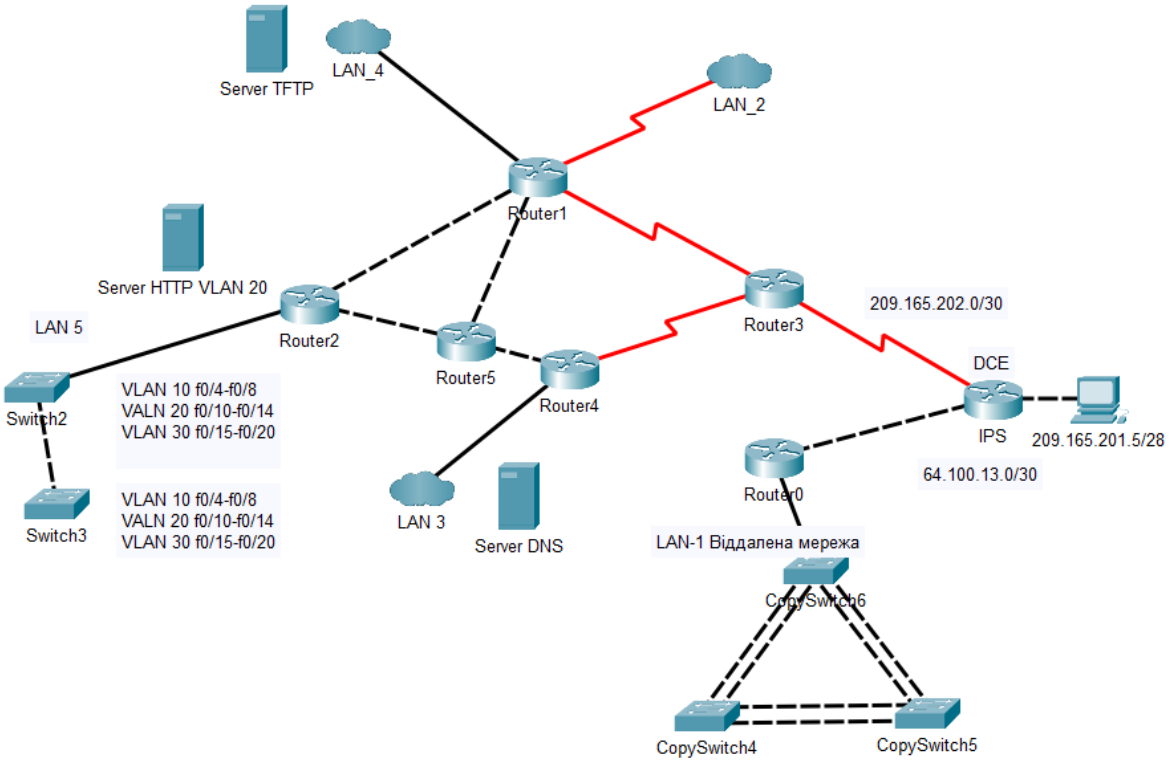


Рисунок 1.4 – Мережева топологія

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до комп'ютерної системи

Компанія "LANARS" замовила розробку корпоративної мережі, з вказанням топології на рис.2.1. Усі етапи розробки мережі повинні виконуватись відповідно до цієї архітектури.

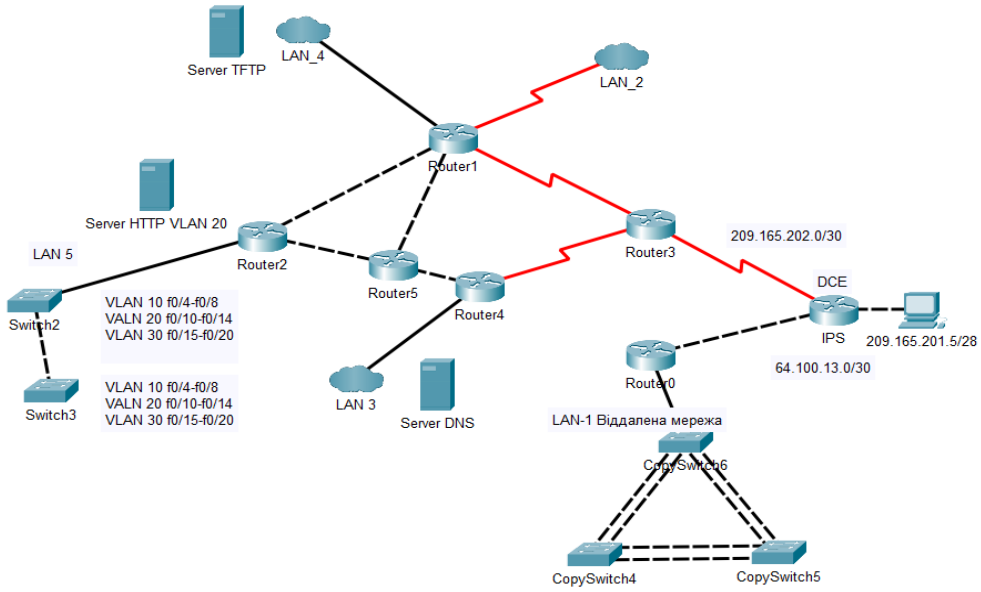


Рисунок 2.1 – Архітектура КМ від замовника

Замовник встановив вимогу щодо кількості вузлів, які мають бути розташовані в кожній з підмереж компанії: LAN1 має 63 пристрої, LAN2 має 67 пристрої, LAN3 має 88 пристрої, LAN4 має 94 пристрої, а LAN5 має 67 пристрої.

Комп'ютерна система IT-компанії "LANARS" має включати необхідне обладнання для підключення до загальнопромислової мережі, пристрій управління, датчики, програмне забезпечення, яке реалізує алгоритм управління, персональний комп'ютер з SCADA системою та сервер баз даних.

При побудові, налаштуванні та забезпеченні безпеки корпоративної мережі, система повинна задовольняти такі вимоги:

- система має працювати без перебоїв та виконувати всі необхідні операції;
- система повинна мати мінімальний час простою, а також бути стійкою до випадків відмов;
- система повинна мати можливість працювати в різних режимах залежно від потреб користувачів.
- система має автоматизувати певні домашні процеси, щоб зменшити навантаження на користувача;
- система повинна мати заходи безпеки, щоб уникнути можливих загроз та забезпечити безпеку користувачів;
- система повинна бути ефективною з точки зору енергоспоживання та допомагати зменшити споживання електроенергії;
- система має забезпечувати швидкий та надійний обмін інформацією між різними компонентами, що дозволяє забезпечити ефективну взаємодію між ними.

Для досягнення цих цілей компанія "LANARS" повинна провести детальне опрацювання побудови, налаштування та забезпечення безпеки корпоративної мережі. Опрацювання побудови включає вибір потрібного обладнання та його розташування, налаштування мережевої інфраструктури та встановлення необхідного програмного забезпечення. Налаштування мережі включає налаштування параметрів мережевих пристроїв, забезпечення безпеки мережі, налаштування доступу до ресурсів та інші аспекти, необхідні для оптимальної роботи мережі.

Особлива увага повинна бути приділена безпеці корпоративної мережі. Це включає застосування захисних заходів, таких як брандмауери, антивірусне

програмне забезпечення, системи виявлення вторгнень та інші механізми, що допомагають захистити мережу від несанкціонованого доступу, витоку даних та інших загроз.

2.2 Вимоги до системи

2.2.1 Вимоги до структури і функціонуванню системи

У процесі розробки комп'ютерної системи для компанії «LANARS» з детальним опрацюванням побудови, налаштування та забезпечення безпеки корпоративної мережі, необхідно розробити наступні ключові підсистеми:

- підсистема розробки програмного забезпечення;
- підсистема інфраструктури та мережі;
- підсистема технічної підтримки;
- підсистема проектного управління;
- підсистема маркетингу та продажу.

Головні функціональні вимоги до системи включають:

- забезпечення підключення всіх комп'ютерів до мережі;
- забезпечення передачі та зберігання інформації;
- налаштування безпеки різних частин мережі;
- наявність файлового сервера, що зберігає всі звіти протягом тривалого періоду;
- забезпечення доступу до сервера через мережу Інтернет.

2.2.2 Вимоги до показників призначення

Для «LANARS» необхідно врахувати такі вимоги щодо призначення системи:

- забезпечення належного функціонування обладнання згідно з вимогами технологічного процесу, включаючи;
- використання передових технологій для забезпечення безпеки мережі;

- можливість здійснювати віддалений доступ співробітників до робочих місць;
- забезпечення стійкості мережі для неперервного використання протягом усієї доби;
- ефективне зберігання даних на серверному обладнанні.

Дані вимоги ставляться з метою забезпечення оптимальної функціональності, надійності та безпеки нашої IT-системи.

2.2.3 Вимоги до експлуатації, технічного обслуговування, ремонту і зберігання компонентів системи

Вимоги щодо експлуатації, обслуговування, ремонту і зберігання компонентів системи для розробленої системи повинно включати:

– технічне та фізичне захист апаратних компонентів системи, неперебійне енергопостачання для серверів та поточне обслуговування забезпечуються за допомогою відповідних технічних та організаційних засобів;

– періодичне технічне обслуговування технічних засобів повинно проводитися відповідно до вимог технічної документації виробників, але не рідше одного разу на рік;

– періодичне технічне обслуговування і тестування технічних засобів повинні включати обслуговування і тестування всіх використовуваних технічних засобів;

– у процесі проведення періодичного технічного обслуговування необхідно виконати зовнішній та внутрішній огляд технічних засобів, провести чищення, перевірити контактні з'єднання, перевірити параметри налаштувань для забезпечення працездатності технічних засобів і протестувати їх взаємодію;

– розміщення обладнання та технічних засобів повинно відповідати

вимогам щодо техніки безпеки, санітарних норм і пожежної безпеки.

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

Для забезпечення взаємозв'язку всіх пристроїв у мережі використовується технологія Ethernet, яка передбачає застосування різних інтерфейсів залежно від пропускної здатності. Наприклад, для підключення ПК до мережі використовуються інтерфейси FastEthernet, для з'єднання комунікаційного обладнання з маршрутизаторами - інтерфейси GigabitEthernet, а для з'єднання маршрутизаторів між собою використовуються Serial інтерфейси.

Для забезпечення зв'язку між мережею головного офісу та мережею віддаленого офісу необхідно використати технологію Virtual Privat Network. Це дозволить забезпечити безпечний тунельний зв'язок між цими мережами.

Для забезпечення доступу вузлів до Інтернету необхідно налаштувати конфігурацію Network Address Translation на маршрутизаторах, які підключені до постачальника послуг Інтернету (ISP). Це дозволить привести внутрішні IP-адреси вузлів до зовнішніх IP-адресів, що надаються провайдером, для забезпечення доступу до Інтернету.

2.2.5 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему компанії «LANARS»

Ефективна робота системи компанії "LANARS" залежить від належної чисельності та кваліфікації персоналу, який обслуговує цю систему. Нижче наведені вимоги до персоналу, які допоможуть забезпечити високу якість обслуговування та оптимальну функціональність системи.

Режим роботи персоналу повинен бути гнучким, щоб забезпечити постійну доступність обслуговування та контролю системи. Розподіл робочого часу між змінами та днем/ноччю повинен бути розрахований таким чином, щоб

покрити пікові навантаження та забезпечити належну реагування в разі виникнення проблем. Загальний склад персоналу наведено в табл.2.1.

Таблиця 2.1 – Чисельний склад основного персоналу

Посада	Кількість персоналу	Кваліфікаційні вимоги	Досвід
IT-менеджер	1	Вища освіта зі спеціальності інформаційних технологій або управління IT-проектами	Досвід управління IT-проектами не менше 5 років
Системний адміністратор	2	Вища або середня технічна освіта	Досвід у роботі зі системними адміністраційними задачами протягом 2-3 років
Технічний спеціаліст з мережевої інфраструктури	3	Вища або середня технічна освіта Сертифікати Cisco CCNA або аналогічні	Досвід у розгортанні та підтримці мережевої інфраструктури протягом 2-3 років
Спеціаліст зі збереження даних	2	Вища технічна освіта	Досвід у розгортанні та підтримці систем збереження д аних (наприклад, систем резервного копіювання) протягом 2-3 років
Технічний підтримки - працівники	4	Вища або середня технічна освіта	2-3 років

Режим роботи:

– IT-менеджер: повний робочий день;

– системний адміністратори, технічний спеціаліст з мережевої

інфраструктури, спеціаліст зі збереження даних: змінна робота, згідно з графіком змін;

– технічний підтримки: змінна робота, включаючи надання підтримки поза робочими годинами у випадку невідкладних ситуацій або аварій.

Для успішного функціонування системи компанії "LANARS" необхідно, щоб персонал був не тільки технічно кваліфікованим, але й володів комунікативними навичками та вмінням ефективно спілкуватися зі співробітниками та клієнтами. Крім того, постійне професійне самовдосконалення та оновлення знань з технологій інформаційної безпеки є важливими аспектами для персоналу, який обслуговує систему компанії "LANARS".

Забезпечення відповідної чисельності та кваліфікації персоналу є важливою складовою успішної експлуатації системи компанії "LANARS". Відповідність персоналу вимогам сприятиме ефективній роботі системи, зниженню ризику виникнення проблем та покращенню задоволення клієнтів.

2.2.6 Вимоги до характеристик взаємозв'язків комп’ютерної системи із суміжними системами

Комп'ютерна система компанії "LANARS" повинна мати здатність до обміну даними з іншими суміжними системами. Це досягається шляхом підтримки стандартів комунікації, таких як TCP/IP, SMTP, FTP, SSH. Ці стандарти комунікації використовуються для різних цілей, від передачі даних у веб-сервісах до керування мережевими пристроями та обміну файлами. Окрім цього, комп'ютерна система має бути стійкою та надійною при взаємодії зі суміжними системами. Забезпечення безпеки даних під час їх передачі та обробки між суміжними системами також є важливим аспектом для комп'ютерної системи.

Система повинна забезпечувати ефективний обмін даними з іншими системами, дотримуючись встановлених стандартів комунікації. Це забезпечить сумісність і синхронізацію даних між комп'ютерною системою та суміжними системами. Додатково, система повинна мати надійну та стабільну роботу під час взаємодії з іншими системами, що дозволить уникнути втрати даних або відмов у передачі. Захист даних є важливою складовою функціональності системи та повинен забезпечуватись під час передачі та обробки інформації між суміжними системами.

Вимоги до характеристик взаємозв'язків комп’ютерної системи з суміжними системами мають на меті забезпечити ефективну та безперебійну обмін даними між ними, дотримуючись встановлених стандартів комунікації. Надійність, стабільність та безпека є ключовими аспектами, які допоможуть підтримувати належну функціональність та цілісність інформації під час її передачі та обробки між комп’ютерною системою та суміжними системами. Забезпечення взаємозв'язку з іншими системами дозволяє ефективно обмінюватися даними і спільно використовувати ресурси між різними системам.

2.3 Вимоги до функцій, які виконує КС

Вимоги до функцій, які виконує комп'ютерна система IT-компанії "LANARS" з детальним опрацюванням побудови та налаштування корпоративної мережі включають наступне:

1. Підключення всіх комп'ютерів до мережі. Система повинна забезпечити можливість підключення всіх комп'ютерів співробітників компанії до корпоративної мережі. Це включає налаштування мережевих портів, прокладку мережевих кабелів та використання бездротових технологій, якщо потрібно.

2. Передача даних між кінцевими вузлами та зберігання інформації. Система повинна забезпечувати надійну передачу та зберігання інформації

всередині корпоративної мережі. Це включає використання мережевих протоколів, мережевого обладнання і систем зберігання даних, таких як файлові сервери або хмарні рішення.

3. Налаштування безпеки різних частин мережі. Система повинна мати механізми для захисту корпоративної мережі від несанкціонованого доступу, злому, вірусів та інших загроз. Це включає використання фаєрволів, антивірусного програмного забезпечення, систем контролю доступу, шифрування даних тощо.

4. Файловий сервер для зберігання даних. Система повинна мати файловий сервер, який забезпечує централізоване зберігання та керування даними компанії. Це дозволяє співробітникам зручно обмінюватися файлами, зберігати документи та забезпечує резервне копіювання важливої інформації.

5. Доступ до сервера з мережі Інтернет: Система повинна надавати можливість віддаленого доступу до корпоративного сервера з мережі Інтернет. Це дозволить співробітникам займатися роботою поза офісом, підключатися до корпоративних ресурсів і виконувати робочі завдання незалежно від місця перебування.

6. Моніторинг та аналіз мережевої активності. Система повинна мати засоби для моніторингу та аналізу мережевої активності, що дозволить виявляти потенційні проблеми, витрати ресурсів та оптимізувати роботу мережі. Це включає використання мережевих моніторів, систем реєстрації подій та аналітичного програмного забезпечення.

7. Безперебійне енергопостачання для серверів. Система повинна мати механізми для забезпечення безперебійного енергопостачання серверів. Це може включати в себе використання резервних джерел живлення, UPS (унінтераптебл павер суплай) та генераторів електроструму, щоб уникнути відмов серверів через перебої в електропостачанні.

8. Резервне копіювання та відновлення даних. Система повинна мати механізми для резервного копіювання та відновлення даних, щоб забезпечити захист від втрати інформації в разі аварій, видалення або пошкодження даних. Це може включати використання резервних серверів, систем архівації, хмарних резервних копій або інших методів резервного копіювання.

9. Система моніторингу безпеки. Система повинна мати засоби моніторингу безпеки, які виявляють потенційні загрози, атаки або порушення безпеки мережі. Це може включати в себе використання інтра- та екстра-надзвичайних систем спостереження, систем виявлення вторгнень (IDS) та систем захисту периметра (firewalls). Такі системи допоможуть вчасно виявляти потенційні загрози та недопущення несанкціонованого доступу до мережі.

10. Резервування мережевих з'єднань. Система повинна мати можливість резервування мережевих з'єднань для забезпечення неперервності роботи мережі в разі відмови основних мережевих ліній або пристроїв. Це може бути досягнуто за допомогою маршрутизації з резервними шляхами, використанням резервних ліній зв'язку або використанням протоколів резервування, таких як VRRP (ViRual Router Redundancy Protocol).

11. Система керування мережею. Система повинна мати засоби керування мережею, що дозволяють адміністраторам моніторити та керувати роботою всієї корпоративної мережі. Це може включати централізоване керування мережевим обладнанням, налаштування параметрів мережі, виявлення проблем та виконання різних адміністративних завдань.

12. Система управління доступом. Система повинна мати механізми контролю доступу, що дозволяють обмежувати доступ до різних ресурсів мережі на основі прав доступу та рівня авторизації користувачів. Це забезпечує захист конфіденційної інформації та запобігає несанкціонованому доступу до важливих ресурсів.

13. Система масштабування. Система повинна бути гнучкою та масштабованою, щоб відповідати зростаючим потребам компанії.

14. Встановлення зв'язку з віддаленою підмережею з використанням VPN.

15. Регулювання потоку даних у корпоративній мережі (ACL-списки).

16. Забезпечення доступу до Інтернету з будь-якого відділу.

2.4 Вимоги до засобів забезпечення системи

2.4.1 Вимоги до інформаційного забезпечення

Вимоги до інформаційного забезпечення системи включають наступні пункти:

– автоматичний збір та початкова обробка інформації;

– автоматичний моніторинг стану технологічного процесу з оповіщенням про перевищення лімітів;

– контроль технологічних процесів у режимі реального часу;

– подання інформації в зручному форматі для аналізу, включаючи графіки, мнемосхеми, гістограми та таблиці;

– автоматична обробка, запис і зберігання виробничої інформації, розрахунок показників;

– автоматичне формування облікових записів і електронних таблиць згідно з встановленими формами і графіком випуску;

– прийом інформації з системи аварійного захисту, сигналізація та взаємодія з нею;

– контроль стану експлуатації об'єктів мережі, включаючи польове обладнання;

– підготовка даних для розрахунків матеріальних і енергетичних балансів, розрахунків сировини та енергоспоживання;

– автоматична передача даних у внутрішню мережу компанії;

– захист баз даних та програмного забезпечення від несанкціонованого доступу;

– діагностика та видача повідомлень про вихід з ладу елементів системи з точністю модуля.

Крім того, система компанії "LAVARUS" має відповідати наступним вимогам для забезпечення швидкого доступу до даних та ефективної обробки інформації:

– максимальний час відповіді на запити користувача повинен становити не менше 9 секунди. Це дозволить користувачам отримувати оперативні та безперебійні результати своїх запитів;

– система повинна мати достатню пропускну здатність для обробки одночасних запитів великої кількості користувачів, що забезпечить швидку обробку та відображення даних. наприклад, система повинна бути здатною опрацьовувати паралельно запити на перегляд вільних місць на паркінгу від багатьох користувачів одночасно;

– забезпечення реального моніторингу, що передбачає надання актуальної інформації контролю роботи персоналу. Це дозволить операторам системи відстежувати поточний стан паркінгу та приймати оперативні рішення на основі актуальних даних;

– швидка обробка інформації про інтенсивність задимленості, вологості та температури в приміщенні паркінгу. Це допоможе вчасно виявляти та реагувати на можливі проблеми або аварійні ситуації;

– система повинна бути оптимізована для швидкого виконання складних запитів та аналізу даних. наприклад, система має ефективно обробляти запити на аналіз використання паркінгу протягом певного періоду часу для виявлення тенденцій та оптимізації розподілу ресурсів.

2.3.2 Вимоги до програмного забезпечення

Вимоги до програмного забезпечення для комп'ютерної системи IT-компанії "LANARS" включають:

1. Конфігурацію та управління мережевим обладнанням. Програмне забезпечення повинно забезпечувати можливість конфігурування і управління мережевими пристроями, такими як маршрутизатори, комутатори, файрволи і точки доступу. Це включає налаштування параметрів, маршрутизацію, фільтрацію трафіку та безпеку мережі.

2. Моніторинг та аналіз мережі. Програмне забезпечення повинно забезпечувати моніторинг і аналіз стану мережі, включаючи пропускну здатність, завантаженість, пінг, латентність та інші показники продуктивності. Рекомендовано PRTG Network Monitor: Ця програма надає широкий спектр можливостей для моніторингу мережі, включаючи моніторинг пропускної здатності, завантаженості, пінгу, латентності, а також моніторинг стану мережевих пристроїв. Вона надає гнучкі налаштування та візуалізацію даних через зручний інтерфейс. Воно має надавати зручні інструменти для візуалізації даних і створення звітів.

3. Управління безпекою мережі. Програмне забезпечення повинно забезпечувати захист мережі шляхом виявлення, блокування та моніторингу потенційних загроз безпеці, таких як вторгнення, злами, віруси і шкідливі програми. Воно має підтримувати механізми аутентифікації, авторизації та шифрування для забезпечення конфіденційності та цілісності даних. Рекомендовано Cisco Adaptive Security Appliance. Це програмне забезпечення, яке використовується для управління безпекою мережі, включаючи виявлення та блокування загроз, налаштування правил файрволу і забезпечення безпеки вхідних і вихідних з'єднань.

4. Керування політиками доступу. Програмне забезпечення повинно надавати можливість налаштування політик доступу до ресурсів мережі. Це

включає контроль прав доступу користувачів, установлення рівнів привілеїв і обмежень, а також аудит доступу до системи.

5. Керування мережевими сервісами: Програмне забезпечення повинно забезпечувати керування різними мережевими сервісами, такими як DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), VPN (ViRual Private Network) і іншими. Воно має дозволяти налаштовувати параметри цих сервісів, керувати їх роботою та забезпечувати їх надійну та ефективну роботу.

6. Централізоване керування мережевими налаштуваннями: Програмне забезпечення повинно надавати можливість централізованого керування налаштуваннями мережевих пристроїв і параметрами мережі. Це дозволяє забезпечити єдиноформатність налаштувань, спростити процес управління мережею і забезпечити її стабільну та оптимальну роботу.

7. Резервне копіювання та відновлення даних. Програмне забезпечення повинно забезпечувати можливість резервного копіювання і відновлення даних мережі. Це дозволяє запобігти втраті даних в разі випадкового видалення, помилок або випадку відмови обладнання.

2.3.3. Вимоги до технічного забезпечення

Вимоги до технічного забезпечення комп'ютерної системи IT-компанії "LANARS":

– сервери. Необхідно мати потужні сервери для забезпечення оптимальної продуктивності мережі. Сервери повинні мати достатню кількість процесорних ядер, оперативної пам'яті і місця на жорсткому диску для виконання завдань серверних додатків і забезпечення швидкого доступу до ресурсів мережі;

– комутатори. Комутатори відіграють важливу роль у побудові мережі. Вони повинні мати достатню кількість портів для підключення комп'ютерів, принтерів, серверів і інших мережевих пристроїв. Крім того, комутатори повинні

підтримувати високу швидкість передачі даних і функції керування трафіком;

– маршрутизатори. Маршрутизатори відповідають за направлення мережевого трафіку між різними підмережами і віддаленими мережами. Вони повинні мати високу продуктивність, підтримувати різні протоколи маршрутизації і забезпечувати безпеку мережі;

– брандмауери (файрволи). Брандмауери відповідають за захист мережі від несанкціонованого доступу і зовнішніх загроз. Вони повинні мати механізми фільтрації трафіку, інтеграцію з системою виявлення вторгнень і підтримувати VPN-з'єднання для безпечного доступу до мережі зовнішніх користувачів;

– бездротові точки доступу. Для забезпечення бездротового доступу до мережі необхідно використовувати бездротові точки доступу (Access Points). Вони повинні підтримувати стандарти бездротового зв'язку, такі як Wi-Fi 6 або Wi-Fi 5, і мати достатню покриття для всіх зон офісу. Бездротові точки доступу повинні підтримувати механізми безпеки, такі як WPA2 або WPA3, і мати можливість керування доступом до бездротової мережі.

2.3.3.1 Вимоги до активного мережевого обладнання

Активне обладнання мережі повинно мати достатню кількість портів для підключення до мережевих пристроїв, комп'ютерів та інших пристроїв. Також важливо враховувати типи портів, які підтримуються (наприклад, GigabitEthernet, Serial) та кількість 24 або 48 портів Ethernet, для підключення комп'ютерів та інших мережевих пристроїв. Запропоновано використати Cisco Catalyst 2960 Series. Це комутатор серії Catalyst, який забезпечує широкі можливості управління та надійну роботу в мережі. Маршрутизатор повинен підтримувати різні типи портів, такі як GigabitEthernet для швидкого передавання даних і Serial для підключення до зовнішніх мереж або інших пристроїв. Обрано модель маршрутизатора: Cisco ISR 4000 Series. Це маршрутизатор серії Integrated Services Router (ISR) з підтримкою різних

мережевих протоколів та функцій, що забезпечують безпеку, масштабованість та продуктивність мережі. Активне мережеве обладнання повинно підтримувати необхідні мережеві протоколи, такі як ICMP, IP, TCP/UDP, DHCP, OSPF та інші, для забезпечення взаємодії з іншими пристроями у мережі.

2.4 Вимоги до програмного забезпечення системи компанії "LANARS"

Вимоги до програмного забезпечення для IT-компанії включають широкий спектр програм та інструментів, необхідних для ефективної роботи та досягнення бізнес-цілей.

Для роботи на комп'ютерах співробітників IT-компанії зазвичай використовуються операційні системи, такі як Windows, macOS або Linux. Ці операційні системи забезпечують базовий функціонал для роботи з комп'ютером і запуску програмного забезпечення. Використовують останні актуальні версії.

IT-компанії зазвичай потребують середовища розробки програмного забезпечення (IDE), яке надає інструменти для написання, тестування і налагодження програмного коду. Приклади таких IDE включають Visual Studio, Eclipse, IntelliJ IDEA. Ці програми забезпечують зручну роботу програмістів і дозволяють створювати якісне програмне забезпечення.

Використовують системи контролю версій для керування та відстеження змін у програмному коді. Такі системи дозволяють програмістам працювати одночасно над одним проектом, вносити зміни у код та відновлювати попередні версії коду при потребі. Приклади систем контролю версій включають Git, Subversion, Mercurial.

При розробці програмного забезпечення, зазвичай потребують баз даних для зберігання, організації та обробки даних. Приклади систем управління базами даних (СУБД), які використовуються, включають Oracle Database,

MySQL, Microsoft SQL Server. Ці СУБД надають потужні можливості для зберігання та маніпулювання великими обсягами даних. Вибір конкретного виду ПЗ залежить від технічного завдання клієнта.

Для роботи з документами, електронними таблицями, презентаціями та іншими офісними завданнями, IT-компанії використовують офісні програми. Найпопулярнішим прикладом є Microsoft Office, який включає програми, такі як Microsoft Word для обробки текстових документів, Microsoft Excel для створення електронних таблиць і Microsoft PowerPoint для створення презентацій. Інші альтернативи офісних пакетів включають Google Docs, Google Sheets, LibreOffice і OpenOffice.

Антивірусне ПЗ IT-компанії повинні забезпечувати безпеку своїх систем і даних від шкідливих програм і загроз. Тому вони використовують антивірусне програмне забезпечення, яке сканує, виявляє і блокує віруси, шпигунське програмне забезпечення, троянські програми та інші загрози. Приклади антивірусних програм включають ESET Smart Security, Norton Antivirus, McAfee Antivirus.

Для спілкування та співпраці між співробітниками в IT-компанії використовуються комунікаційні програми. Приклади таких програм включають електронну пошту, таку як Microsoft Outlook або Gmail, миттєві обмінники повідомленнями, такі як Slack або Microsoft Teams, і програми для відеоконференцій, такі як Zoom або Microsoft Teams. Ці програми дозволяють співробітникам легко спілкуватися, обмінюватися інформацією та співпрацювати над проектами.

2.4.1 Вимоги до інтеграції та сумісності програмного забезпечення

Програма повинна забезпечувати інтерактивне відстеження об'єкта та відображення всіх змін, які відбуваються, а також вносити всі дані про зміну стану датчиків та виконавчих механізмів у базу даних. Програмне забезпечення

має точно відображати графічне місцезнаходження об'єктів управління та їх параметри і стан [5, 7].

2.4.2 Вимоги до збереження інформації

Рекомендується зберігати програмне забезпечення на будь-якому зручному носії інформації, з резервною копією на знімному носії. Рекомендується встановлювати обмеження доступу до програми, крім персоналу, що безпосередньо обслуговує програмний продукт [7].

2.4.3 Вимоги до захисту інформації від несанкціонованого доступу

З метою запобігання аваріям та нещасним випадкам строго заборонено допускати осіб до монтажу, налаштування, обслуговування та ремонту системи, які не мають відповідного дозволу та не ознайомлені з керівництвом, а також вносити зміни в апаратуру без погодження з виробником заводом.

Повинні бути забезпечені програмний та апаратний захист від некваліфікованих дій користувачів та спроб несанкціонованого доступу до внутрішньосистемної інформації. Залежно від статусу користувача мають бути передбачені різні рівні доступу до внутрішньосистемної інформації.

Також необхідно забезпечити цілісність даних, які передаються по радіоканалу. Це можна здійснити за допомогою засобів радіоапаратури та додаткових заходів безпеки, які не потребують додаткових вимог [6].

2.5 Розробка інженерного рішення комп’ютерної системи компанії "LANARS"

Розробка інженерного рішення комп'ютерної системи для IT-компанії "LANARS" включає процес створення технічного забезпечення, програмного забезпечення і мережевої інфраструктури, що відповідає потребам компанії і її бізнес-цілям. Основна мета розробки інженерного рішення полягає у створенні

надійної, ефективної та масштабованої комп'ютерної системи, яка задовольняє вимоги компанії і сприяє її успіху.

Процес розробки інженерного рішення передбачає виконая етапів, які опишемо нижче.

Крок 1. Аналіз потреб. Спочатку проводиться аналіз потреб компанії "LANARS". Цей етап включає збір вимог, спілкування з ключовими зацікавленими сторонами, вивчення бізнес-процесів і встановлення цілей, які повинна виконувати комп'ютерна система.

Крок 2. Проектування системи. На основі аналізу потреб розробляється детальний план комп'ютерної системи. Цей план включає визначення архітектури системи, вибір технічного забезпечення, розробку мережевої інфраструктури та програмного забезпечення.

Крок 3. Розробка програмного забезпечення. Залежно від потреб компанії "LANARS" розробляється програмне забезпечення, яке може включати в себе корпоративні додатки, системи управління базами даних, веб-додатки, інтеграцію зовнішніх систем тощо. Процес розробки програмного забезпечення включає створення специфікацій, програмування, тестування та впровадження.

Крок 4. Вибір технічного забезпечення: На основі потреб і проекту системи визначаються необхідні комп'ютери, сервери, мережеві пристрої, засоби зберігання даних та інші компоненти технічного забезпечення. При виборі технічного забезпечення враховуються такі фактори, як потужність, масштабованість, надійність, сумісність з існуючою інфраструктурою, вартість та підтримка.

Крок 5. Розгортання мережевої інфраструктури. Після вибору технічного забезпечення проводиться розгортання мережевої інфраструктури. Це включає установку та налаштування серверів, комутаторів, маршрутизаторів, бездротових точок доступу та інших мережевих пристроїв. Також проводиться

налаштування мережевих сервісів, які забезпечують безпеку, моніторинг та керування мережею.

Крок 6. Тестування та оптимізація. Після розгортання мережевої інфраструктури проводиться тестування для перевірки працездатності, надійності та продуктивності системи. Якщо виявляються проблеми, вони виправляються, а система оптимізується для досягнення максимальної ефективності та відповідності вимогам компанії.

Крок 7. Впровадження та підтримка. Після успішного тестування система готова до впровадження. Це включає міграцію даних, навчання персоналу та підтримку під час переходу до нової комп'ютерної системи. Після впровадження забезпечується підтримка системи, включаючи виправлення помилок, оновлення та управління забезпеченням.

Для реалізації комп'ютерної системи компанії "LANARS" була обрана логічна топологія "розширена зірка". Основна технологія мережі була обрана Ethernet. Для підключення робочих груп використовується FastEthernet, між маршрутизаторами - Serial Interface, а між маршрутизатором і комутатором - GigabitEthernet. Для підключення кінцевих пристроїв до мережі встановлюються роз'єми типу RJ-45.

Схему розташування відділів компанії наведено на рис.2.1.

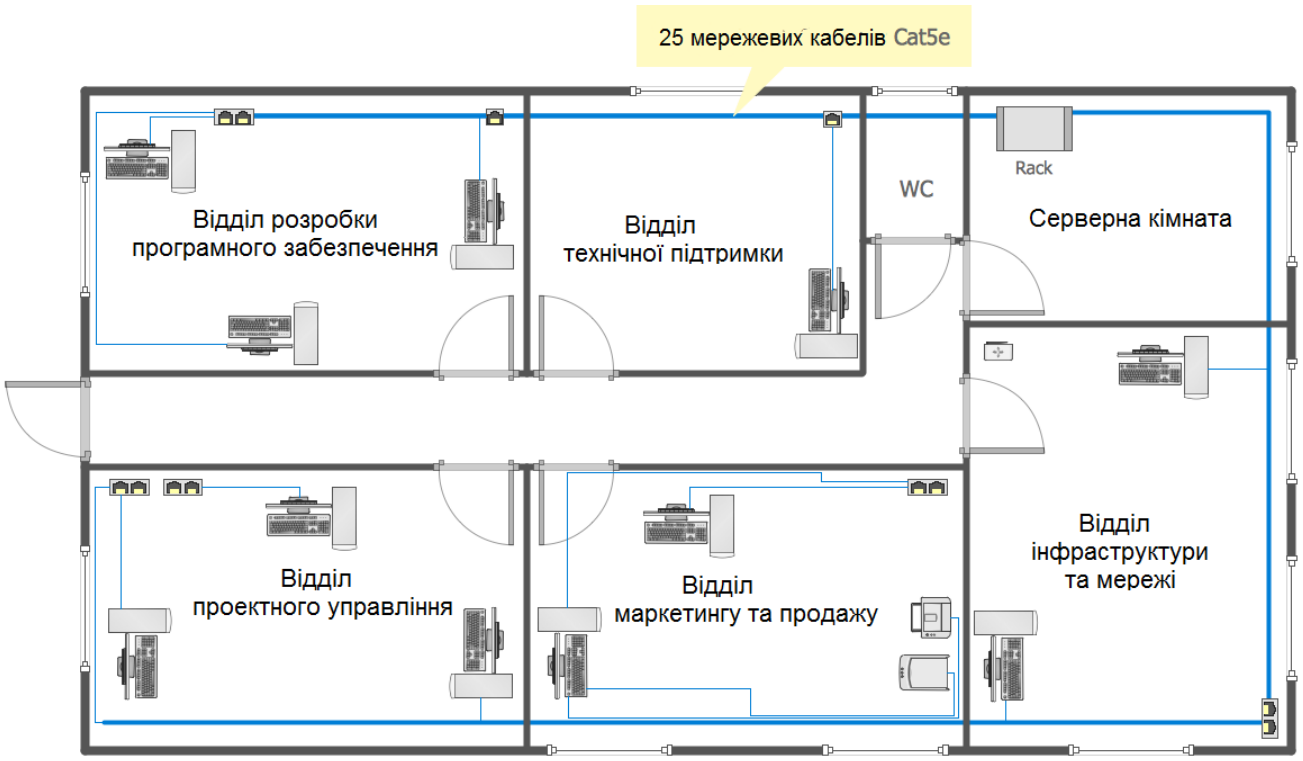


Рисунок 2.1 – План-схема розташування відділів

Після того, як були розроблені всі технічні вимоги до комп'ютерної системи і проведений аналіз структури компанії, наступним кроком є розробка схеми технічних засобів КС (див. Рис. 2.2). Ця схема відображає підключення мережевих пристроїв до комп'ютерів та серверів мережі, а також містить інформацію про назви відділів та кількість персональних комп'ютерів.

На розробленій схемі показано, як взаємодіють мережеві пристрої, комп'ютери та сервери, як вони підключені між собою. Також на схемі вказана інформація про назви відділів компанії та кількість персональних комп'ютерів, які використовуються в кожному відділі з назвою LAN.

Дана схема є важливим документом для визначення структури технічних засобів комп'ютерної системи, допомагає зрозуміти, як компоненти системи пов'язані між собою і як вони використовуються в різних відділах компанії.

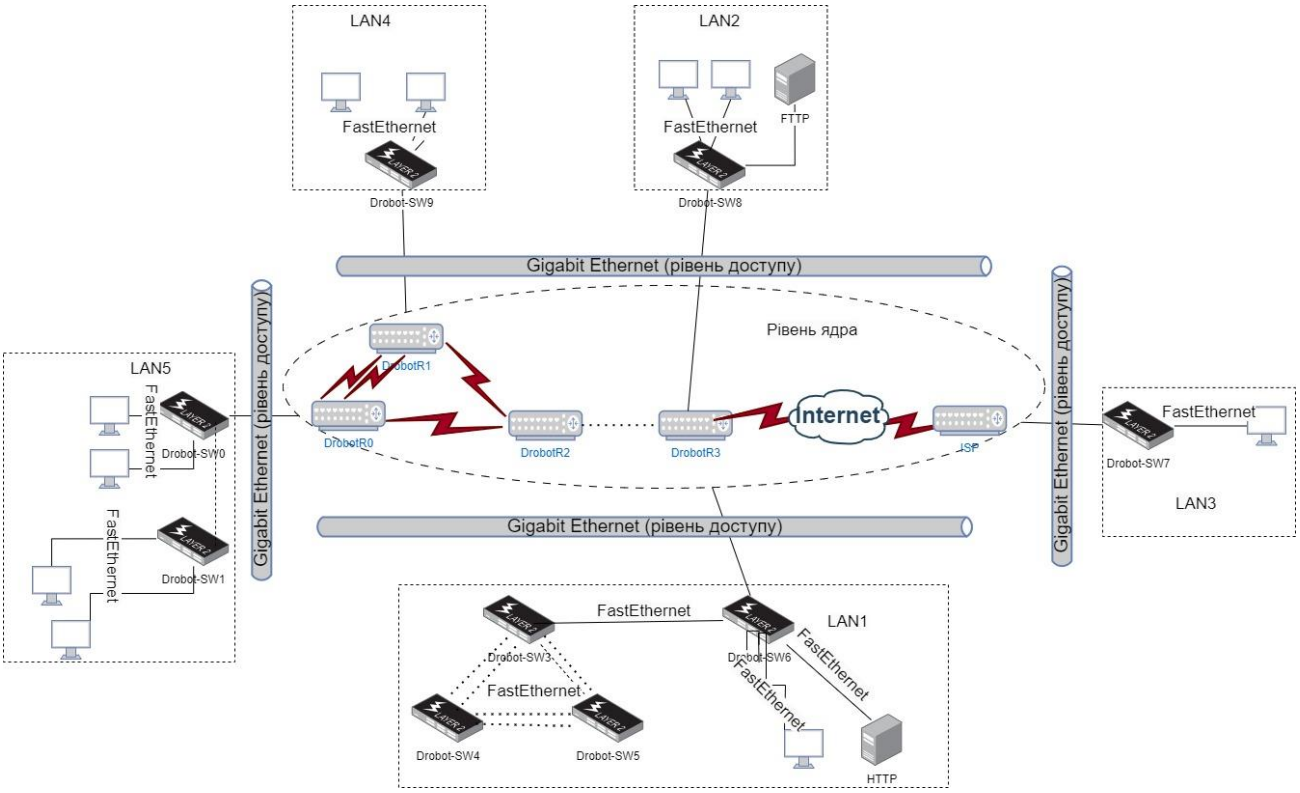


Рисунок 2.2 - Схема технічних засобів КС

2.6 Розробка специфікації апаратних засобів комп’ютерної системи "LANARS"

Проведемо розробку технічної специфікації апаратних засобів комп'ютерної системи для мережі віддаленого офісу компанії.

Для мережі віддаленого офісу був обраний маршрутизатор Cisco ISR 4000 Series спеціально розроблені для малих та середніх організацій, які шукають сучасні технологічні рішення, що забезпечують надійний та продуктивний доступ до Інтернету зі швидкістю маршрутизації до 75 Мбіт/с.

Для комутації в підмережі були обрані комутатори Cisco Catalyst 2960 Series. Ці комутатори мають доступну ціну і відповідають усім потребам компанії. Вони належать до серії комутаторів з фіксованою конфігурацією та мають порти FastEthernet і GigabitEthernet. Комутатори серії також надають

розширені LAN-сервіси для підприємств початкового рівня та мереж віддалених офісів.

У табл. 2.2 наведено специфікацію апаратних засобів комп'ютерної системи.

Таблиця 2.2 − Специфікація обладнанням

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Кількість	Примітки
1	Cisco ISR 4000 Series	Drobot_Router_1 Drobot_Router_2 Drobot_Router_3 Drobot_Router_4 Drobot_Router_5	5 Шт.	атні мережі (VPN) та системи виявлення вторгнень (IDS/IPS)
2	Cisco Catalyst 2960 Series	Drobot_SW_1 Drobot_SW_2 Drobot_SW_3 Drobot_SW_4 Drobot_SW_5 Drobot_SW_6 Drobot_SW_7 Drobot_SW_8 Drobot_SW_9	9 Шт.	-
3	NZXT H710i	Server FTP Server_HTTP	2 Шт.	-
4	Периферійні пристрої	PC0-40	38 Шт.	48

2.7 Вимоги до технічного забезпечення

Комп'ютерна система повинна мати відповідне комп’ютерне обладнання, яке забезпечує потрібні функції та можливості для її функціонування.

Технічні характеристики системного блоку:

– корпус middle tower Cooler Master MasterBox MB511 RGB;

– материнська плата Asus Pro Q670M-C-CSM s-1700 Q670;

– процесор Intel Core i7 або вище, або AMD Ryzen 7 ;

– пперативна пам'ять (RAM) 16 ГБ RAM для ефективної роботи з багатозадачними програмами та великими обсягами даних.

– жорсткий диск SSD обсягом 500 ГБ або більше для швидкого доступу до даних та оптимальної продуктивності.

– графічна карта з підтримкою сучасних графічних технологій для роботи з вимогливими графічними програмами та іграми.

Монітори:

– монітори з роздільною здатністю Full HD (1920 x 1080 пікселів) або вище для чіткого відображення зображень та тексту;

– Монітори розміром 24 дюйми або більше для комфортної роботи з додатками та багатозадачним середовищем.

Сервери:

– двох- або багатопроцесорні системи з потужними процесорами Intel Xeon або AMD EPYC для обробки великого обсягу даних та завдань;

– оперативна пам'ять (RAM) 32 ГБ RAM або більше для ефективної обробки та зберігання даних;

– жорсткі диски (SSD), RAID-масиви SSD або HDD для надійного та швидкого зберігання даних;

– високопропускна мережева карта з підтримкою Gigabit Ethernet або 10 Gigabit Ethernet для швидкого обміну даними в мережі.

2.8 Вимоги до безпеки і надійності

Підсистема повинна забезпечувати механізми автентифікації та авторизації користувачів, що забезпечують обмежений доступ до даних залежно від ролей та прав доступу [6].

Підсистема повинна мати механізми захисту даних, включаючи шифрування, контроль доступу, аудит дій користувачів та моніторинг системи на виявлення можливих загроз безпеці.

Підсистема повинна бути стійкою до відмов та забезпечувати неперервну доступність сервісів.

Вимоги до надійності включають резервування даних, механізми реплікації, резервні копії та відновлення системи у разі виникнення аварійних ситуацій.

2.9 Розрахунок інтенсивності вихідного трафіку

Найбільшою мережею підприємства є підмережа LAN_4. Щоб розрахувати інтенсивність вхідного трафіку дано:

– кількість вузлів в підмережі 85;

– середня інтенсивність трафіку складає μ=84 (кадрів/с);

− середня довжина повідомлення становить l=650 байт;

– затримка передачі пакету ≤ 6 мс;

– кількість портів комутатора – 24 шт.

Нижче наведено рішення наданої задачі.

Для розрахунку пропускної здатності мережі на рівні доступу використовуємо формулу (2.1)

$$Pp.p = \mu * l * n, \quad (2.1)$$

де

Pp.p – пропускна здатність мережі, біт/с;

μ – інтенсивність обслуговування, кадрів/с;

l – середня довжина повідомлення, байт;

n – кількість портів комутатора.

Підставляємо відомі значення:

μ = 84 кадри/с;

l = 650 байт;

n = 24

Pp.p = 84 * 650 * 24 = 1,352,800 біт/с ≈ 1.35 (Мбіт/с).

Для розрахунку значення інтенсивності виходу використовуємо формулу (2.2). При розрахунках враховується, що навантаження на комутаторі розраховується через лінію 1000 Мбіт/с.

$$\mu_{вих} = C/ (8 * l), \quad (2.2)$$

де

C – пропускна здатність лінії, біт/с;

l – середня довжина повідомлення байт.

Підставляємо відомі значення:

C = 1,000,000,000 біт/с;

l = 650 байт.

μвих = 1,000,000,000 біт/с / (8 * 650) байт = 192,307 (пакетів/с)

Розрахунок максимальної кількості вузлів, яку можна приєднати до комутатора рівня розподілу на основі заданої середньої інтенсивності трафіку, робимо за допомогою формули (2.3).

$$N = \mu_{вих} / \mu, \quad (2.3)$$

де N – кількість вузлів, яку можна приєднати;

μвих – інтенсивність виходу, пакетів/с;

μ – середня інтенсивність трафіку, пакетів/с.

Кількість вузлів: За наданими значеннями, інтенсивність виходу становить 192,307 пакетів, а середня інтенсивність трафіку дорівнює 134 пакетів/с. Тому кількість вузлів (N) можна обчислити, розділивши інтенсивність

виходу на середню інтенсивність трафіку:

N = 192,307 / 134 ≈ 1436.42 (вузлів)

Заокруглення кількості вузлів: Оскільки кількість вузлів зазвичай є цілим числом, результат можна заокруглити до найближчого цілого значення. Тому максимальна кількість вузлів, яку можна приєднати, складатиме 1436.Для розрахунку загальної інтенсивності трафіку від всіх користувачів застосовуємо формулу (2.4).

$$\lambda = x * \mu, \quad (2.4)$$

де λ – загальна інтенсивність трафіку, пакети/с;

x – коефіцієнт, який представляє кількість користувачів або вузлів в мережі;

μ - середня інтенсивність трафіку, пакети/с.

Підставляємо відомі значення:

x = 85,

μ = 134,

λ = 85 * 134 = 11,390 (пакетів/с)

Для розрахунку коефіцієнту затримки на рівні розподілу, використовується формула (2.5):

$$\rho = \lambda / \mu_{вих}, \quad (2.5)$$

де ρ – коефіцієнт затримки на рівні розподілу;

λ – загальна інтенсивність трафіку від всіх користувачів;

$\mu_{вих}$ – інтенсивність виходу, яка вказує на кількість пакетів, що виходять з комутатора за одиницю часу.

Підставляємо відомі значення:

λ = 11,390 пакетів/с,

μвих = 192,307 пакет.

ρ = 11,390 / 192,307 ≈ 0.0592

Щоб розрахувати коефіцієнт зайнятості комутатора на рівні розподілу, використовується формула (2.6).

$$r = \rho / (1 - \rho), \quad (2.6)$$

де r – коефіцієнт зайнятості комутатора;

ρ – коефіцієнт затримки на рівні розподілу.

Задано значення коефіцієнта затримки на рівні розподілу ρ ≈ 0.0592.

Підставимо ці значення в формулу:

r = 0.0592 / (1 - 0.0592) ≈ 0.063

Отже, отримані результати розрахунків:

Максимальна кількість вузлів, яку можна приєднати до комутатора рівня розподілу, складає приблизно 1436 вузлів.

Загальна інтенсивність трафіку від всіх користувачів становить приблизно 11,390 пакетів в секунду.

Коефіцієнт затримки на рівні розподілу складає близько 0.0592.

Коефіцієнт зайнятості комутатора на рівні розподілу становить близько 0.063.Для розрахунку середньої затримки кадру, використовується формула (2.7).

$$T = 1 / (\mu вих - \lambda), \quad (2.7)$$

де T – середня затримка кадру;

λ – загальна інтенсивність трафіку від всіх користувачів;

μвих – інтенсивність виходу, яка вказує на кількість пакетів, що виходять

з комутатора за одиницю часу.

Підставляємо відомі значення:

$\lambda = 11{,}390$ пакетів/с

$\mu_{вих} = 192{,}307$ пакетів/с

$T = 1 / (192\,307 - 11\,390) \approx 0.0052$ (секунд) $= 52 * 10^{-6}$(секунд)

Для розрахунку середньої довжини черги використовується формула (2.8).

$$L_{черги} = \rho^2 / (1 - \rho), \qquad (2.8)$$

де $L_{черги}$ – середня довжина черги;

ρ – коефіцієнт затримки на рівні розподілу.

Отримане значення коефіцієнта затримки на рівні розподілу $\rho \approx 0.0592$, підставимо це значення в формулу:

$L_{черги} = (0.0592)^2 / (1 - 0.0592) \approx 0.00361 / 0.9408 \approx 0.0038$

Отже, отримали середню довжину черги приблизно рівною 0.0038.

Для розрахунку середнього часу перебування пакета в черзі використовується формула (2.9).

$$T_{очік} = L_{черги} / \lambda, \qquad (2.8)$$

де $T_{очік}$ – середній час перебування пакета в черзі;

$L_{черги}$ – середня довжина черги;

λ – загальна інтенсивність трафіку від всіх користувачів.

Задане значення середньої довжини черги $L_{черги} \approx 0.0038$ і загальна інтенсивність трафіку $\lambda = 11\,390$ пакетів/с.

Підставимо ці значення в формулу:

$T_{очік} = 0.0038 / 11\,390 = 0.334$ (мс)

Значення Точік менше ніж у наданих вимогах (6 мс), а отже вимоги виконані.

Розрахунок пропускної здатності каналу можна виконати за формулою (2.9).

$$b = \lambda * l, \quad (2.9)$$

де b - пропускна здатність каналу, біт/с;

λ - інтенсивність трафіку, пакетів/с;

l - середня довжина пакету, байт.

Замінивши значення у формулу, отримаємо:

λ = 11 390 пакетів/с;

l = 650 байт.

b = 11 390 * 650 = 7 403 500 біт/с.

Отже, результат розрахунку пропускної здатності каналу 7.4035 Мбіт/с співпадає з вихідною пропускною здатністю каналу 1000 Мбіт/с.

2.10 Висновки до розділу

Узагальнюючи, технічні вимоги до системи ГО "ЗІРКА" включають в себе необхідність дотримання фізичних параметрів, модульного виконання пристроїв, ліцензування та дозволів на використання радіоустаткування, вимог до функцій, програмного забезпечення, збереження інформації, захисту інформації від несанкціонованого доступу та забезпечення безпеки. Дотримання цих вимог гарантуватиме ефективну та безпечну роботу системи ГО "ЗІРКА" у виконанні своїх завдань.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

Перед тим, як виконувати налаштування кінцевих та проміжних пристроїв треба виконати розрахунки IP-адресації для компанії "LANARS" з мережі 172.23.6.0/21, де LAN1 має 63 пристрої, LAN2 має 67 пристрої, LAN3 має 88 пристрої, LAN4 має 94 пристрої, а LAN5 має 67 пристрої, будемо використовувати VLSM.

Оскільки метод VLSM дозволяє виділяти мережі розміром у 2^n, для розрахунку адресації VLSM для компанії "LANARS" з мережі 172.23.6.0/21 ми будемо розбивати цю мережу на підмережі різного розміру, враховуючи потреби кожної LAN.

Виділимо спочатку найбільші підмережі. За допомогою формули 2^n оберемо підмережу розміром у 2^7 (128) адрес. Маска підмережі буде /25 (255.255.255.128). Перша підмережа буде мати IP-адресу 172.23.6.0 і остання підмережа - 172.23.7.0.

Друга найбільша підмережа буде розміром у 2^6 (64) адреси. Маска підмережі буде /26 (255.255.255.192). Початкова IP-адреса першої підмережі буде 172.23.6.0, а остання - 172.23.6.64.

Розподілимо адреси для кожної LAN, враховуючи їх потреби:

LAN1 має 63 пристрої, тому використовуємо підмережу розміром /26 (64 адреси). Початкова IP-адреса буде 172.23.6.0, а остання - 172.23.6.63.

LAN2 має 67 пристрої, тому також використовуємо підмережу розміром /26 (64 адреси). Початкова IP-адреса буде 172.23.6.64, а остання - 172.23.6.127.

LAN3 має 88 пристрої, тому використовуємо підмережу розміром /25 (128 адрес). Початкова IP-адреса буде 172.23.6.128, а остання - 172.23.6.255.

LAN4 має 94 пристрої, тому також використовуємо підмережу розміром /25 (128 адрес). Початкова IP-адреса буде 172.23.7.0, а остання - 172.23.7.127.

LAN5 має 67 пристрої, тому використовує мо підмережу розміром /26 (64 адреси). Початкова IP-адреса буде 172.23.7.128, а остання - 172.23.7.191.

В таблиці 3.1 наведено адресацію для компанії "LANARS" з використанням VLSM.

Таблиця 3.1 – Адресація для компанії "LANARS"

LAN	Кількість пристроїв	Маска підмережі	Початкова IP-адреса	Кінцева IP-адреса
LAN1	63	/26	172.23.6.1	172.23.6.62
LAN2	67	/26	172.23.6.65	172.23.6.126
LAN3	88	/25	172.23.6.129	172.23.6.254
LAN4	94	/25	172.23.7.1	172.23.7.126
LAN5	67	/26	172.23.7.129	172.23.7.190
WAN1	2	/30	10.0.4.1	10.0.4.2
WAN2	2	/30	10.0.4.5	10.0.4.6
WAN3	2	/30	10.0.4.9	10.0.4.10
WAN4	2	/30	10.0.4.13	10.0.4.14
WAN5	2	/30	10.0.4.17	10.0.4.18

Схема адресації всіх пристроїв у компанії є важливою складовою комп'ютерної інфраструктури. Вона забезпечує унікальність та організованість IP-адрес для кожного пристрою в мережі.

Схема адресації дозволяє призначити унікальну IP-адресу кожному пристрою в мережі. Це дозволяє ідентифікувати та взаємодіяти з кожним пристроєм окремо, що є необхідним для ефективної комунікації та управління мережею.

Використання підмереж у схемі адресації дозволяє логічно розділити мережу на більш маневрені сегменти. Це полегшує управління мережевим трафіком, забезпечує кращу безпеку та підвищує продуктивність.

Використання VLSM дозволяє ефективно використовувати доступний адресний простір. За допомогою розумного розподілу IP-адрес можна зменшити кількість використаних адрес та економити ресурси.

Схема адресації, побудована з урахуванням масштабованості, дозволяє легко розширювати мережу. Задіяння нових підмереж або зміна розміру поточних підмереж можливі без необхідності повного перебудовування адресації всієї мережі.

Таблиця 3.2 – Схема адресації

Ім’я пристрою	Інтерфейс	IP–адреса	Маска	Шлюз	Vlan	Для ПК інтерфейс підключеного пристрою
DrobotR0	G0/0	172.23.7.129	255.255.255.192	–	–	DrobotSW0
	G0/1	172.23.7.1	255.255.255.128	–	–	DrobotSW6
	G0/0.14	172.23.7.36	255.255.255.128		14	
	G0/0.24	172.23.7.47	255.255.255.128		24	

Продовження таблиці 3.2

Ім’я пристрою	Інтерфейс	IP–адреса	Маска	Шлюз	Vlan	Для ПК інтерфейс підключеного пристрою
	G0/0.34	172.23.7.54	255.255.255.128		34	
	G0/0.99	172.23.7.123	255.255.255.128		99	
	Se0/1/0	10.0.4.2	255.255.255.252	–	–	DrobotR1
	Se0/1/1	10.0.4.6	255.255.255.252	–	–	DrobotR1
	Se0/2/0	10.0.4.13	255.255.255.252	–	–	DrobotR2
DrobotSW0	G0/1	–	255.255.255.192	172.23.6.129	–	DrobotR1
	F0/2	–	255.255.255.192	–	–	DrobotSW1
	F0/6–11	–	255.255.255.192	172.23.6.129	Vlan 34	PC12
	F0/15–24	–	255.255.255.192	172.23.6.129	Vlan 24	PC14
	F0/12–14	–	255.255.255.192	172.23.6.129	Vlan 14	PC13
DrobotSW1	F0/2	–	255.255.255.192	172.23.6.129	–	DrobotSW0
	F0/6–11	–	255.255.255.192	172.23.6.129	Vlan 34	PC15

Продовження таблиці 3.2

Ім’я пристрою	Інтерфейс	IP–адреса	Маска	Шлюз	Vlan	Для ПК інтерфейс підключеного пристрою
	F0/15–24	–	255.255.255.192	172.23.6.129	Vlan 24	PC17
	F0/12–14	–	255.255.255.192	172.23.6.129	Vlan 14	PC16
PC12	F0	172.23.6.137	255.255.255.192	172.23.6.129	–	DrobotSW0
PC13	F0	172.23.6.138	255.255.255.192	172.23.6.129	–	DrobotSW0
PC14	F0	172.23.6.139	255.255.255.192	172.23.6.129	–	DrobotSW0
PC15	F0	172.23.6.140	255.255.255.192	172.23.6.129	–	DrobotSW1
PC16	F0	172.23.6.141	255.255.255.192	172.23.6.129	–	DrobotSW1
PC17	F0	172.23.6.142	255.255.255.192	172.23.6.129	–	DrobotSW1
DrobotR1	Se0/1/1	10.0.4.2	255.255.255.252	–	–	DrobotR0
	Se0/1/0	10.0.4.6	255.255.255.252	–	–	DrobotR0
	Se0/2/0	10.0.4.9	255.255.255.252	–	–	DrobotR2

Продовження таблиці 3.2

Ім’я пристрою	Інтерфейс	IP–адреса	Маска	Шлюз	Vlan	Для ПК інтерфейс підключеного пристрою
DrobotR2	G0/1	172.23.6.65	255.255.255.192	–	–	SW_5
	G0/2	10.0.4.17	255.255.255.252	–	–	DrobotR3
	Se0/1/0	10.0.4.10	255.255.255.252	–	–	DrobotR1
	Se0/2/0	10.0.4.13	255.255.255.252	–	–	DrobotR0
DrobotSW5	G0/2	–	255.255.255.192	172.23.6.65	–	DrobotR2
	F0/4	–	255.255.255.192	172.23.6.65	–	SW_4
PC0	F0	172.23.6.3	255.255.255.192	172.23.6.65	–	DrobotSW5
PC1	F0	172.23.6.4	255.255.255.192	172.23.6.65	–	DrobotSW5
PC2	F0	172.23.6.5	255.255.255.192	172.23.6.65	–	DrobotSW5
HTTP	F0	172.23.6.16	255.255.255.192	172.23.6.65	–	DrobotSW5
IPS	G0/0	172.22.65.0	255.255.255.0	–	–	DrobotSW8

Продовження таблиці 3.2

Ім’я пристрою	Інтерфейс	IP–адреса	Маска	Шлюз	Vlan	Для ПК інтерфейс підключеного пристрою
	Se0/1/0	209.165.202.1	255.255.255.240	–	–	DrobotR3
DrobotSW8	G0/1	–	–	–	–	IPS
PC6–8	F0	172.22.65.2–172.22.65.4	255.255.255.224	172.22.65.1	–	DrobotSW8
TFTP	F0	172.22.65.5	255.255.255.224	172.22.65.1	–	DrobotSW8
DrobotR3	Se0/1/0	209.165.202.2	255.255.255.240	–	–	IPS
	G0/1	172.23.6.67	255.255.255.192	–	–	DrobotR2
	G0/0	10.0.4.18	255.255.255.252	–	–	DrobotSW7
DrobotR0	G0/0	172.23.7.1	255.255.255.128	–	–	DrobotSW6
PC3–4	F0	172.23.7.10–172.23.7.14	255.255.255.128	172.23.7.1	–	DrobotSW6
DrobotSW7	G0/1	–	–	–	–	DrobotR3

Продовження до таблиці 3.2

Ім’я пристрою	Інтерфейс	IP–адреса	Маска	Шлюз	Vlan	Для ПК інтерфейс підключеного пристрою
PC9–11	F0	172.23.6.70–				
172.23.64.72	255.255.255.192	172.23.6.67	–	DrobotSW7		

3.2 Налаштування та перевірка роботи комп’ютерної системи

3.2.1 Базове налаштування конфігурації пристроїв

Перед тим як виконати базові налаштування, в середовищі Cisco PT потрібно розробити топологію компютерної мережі для компанії "LANARS" . Планування і проектування мережі в Cisco Packet Tracer (PT) включає кілька кроків, які допоможуть створити ефективну і надійну мережу. Ось кілька кроків, які можна виконати при проектуванні мережі в Cisco PT:

1 Визначити вимоги. Розуміння потреб вашої мережі є ключовим кроком при проектуванні. Визначте, які пристрої, додатки та послуги будуть використовуватися, скільки користувачів планується підключити і які функції мережі необхідні для підтримки бізнес-потреб.

2 Створити топологію. Розташуйте пристрої мережі на полі в Cisco PT. Розташуйте маршрутизатори, комутатори, сервери, комп'ютери та інші пристрої відповідно до вимог вашої мережі. Враховуйте фізичну локацію пристроїв, зони безпеки та потребу в резервуванні.

3 Налаштувати пристрої. Для кожного пристрою встановіть необхідні налаштування. Налаштувати інтерфейси, IP-адреси, маршрутизацію, VLAN, безпеку, сервіси та інші параметри залежно від вимог мережі.

4 Провести тестування мережі. Переконатись, що мережа працює належним чином, проведіть тестування з'єднання, маршрутизації, передачі даних і безпеки. Використовуйте інструменти та можливості Cisco PT для перевірки та налагодження мережі.

На рисунку 3.1 наведено топологію комп’ютерної мережі для компанії "LANARS"

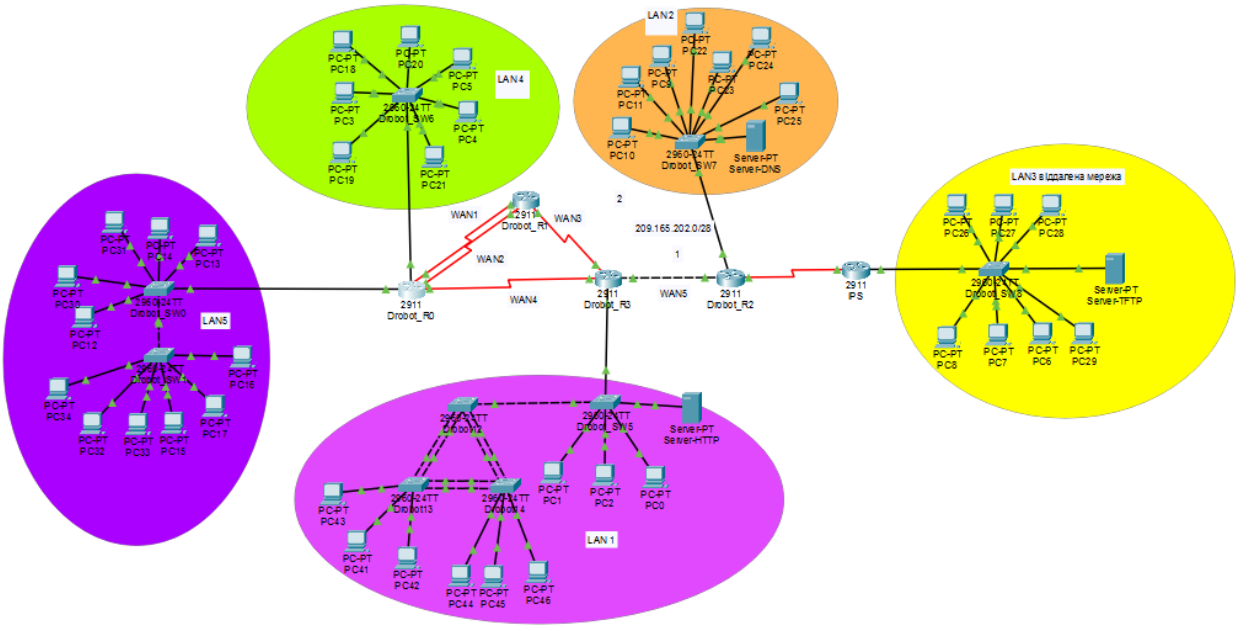


Рисунок 3.1 – Топологія для компанії "LANARS"

Відповідно до вимог технічного завдання, було виконано базову настройку мережевих пристроїв комп'ютерної системи. Базові налаштування пристроїв включають наступні конфігурації:

– встановлення пароля для користувацького режиму exec;

– встановлення пароля для віддаленого доступу до telnet/ssh;

– зашифрування всіх відкритих паролів;

– налаштування банеру MOTD;

– створення унікального імені користувача 123-20ск1_Drobot з паролем admincisco;

– встановлення ключа RSA довжиною 1028 біт для шифрування даних;

– налаштування IP-адресації пристроїв згідно з таблицею 3.2;

– встановлення унікальної назви пристрою (в нашому випадку всі проміжні пристрої починаються з імені Drobot);

– встановлення пароля для привілейованого режиму.

Нижче наведений приклад налаштування на маршрутизаторі Drobotv_R0:

Приклад налаштування наведенно на маршрутизаторі Drobot_R0 .

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

Встановлення унікального імені пристрою:

```
Router(config)#hostname Drobot_R0
```

Шифрування паролів, які зберігаються у відкритому вигляді:

```
Drobot_R0(config)#service password-encryption
```

Встановлення пароля для входу до привілейованого режиму:

```
Drobot_R0(config)#enable secret class
```

Встановлення паролю для входу д до консольного рядка:

```
Drobot_R0(config)#line console 0
Drobot_R0(config-line)#password cisco
```

Налаштування запиту пароля:

```
Drobot_R0(config-line)#login
Drobot_R0(config-line)#exit
```

Налаштування банера MOTD:

```
Drobot_R0(config)#banner motd #123-20ck1 Drobot access only
with password#
```

Створення користувача 123–20ck1_Drobot з паролем admincisco:

```
Drobot_R0(config)#username 123-20ck1_Drobot password admincisco
```

Створення домену:

```
Drobot_R0(config)#ip domain-name Drobot_R0
```

Встановлення ключ шифрування RSA довжиною 1024 біт:

```
Drobot_R0(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-expoRable...[OK]
```

Налаштування лінії vty:

```
Drobot_R0(config)#line vty 0 4
*Mar 1 0:2:50.849: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Встановлення логіна та пароля для входу лінії:

```
Drobot_R0(config-line)#login local
```

Встановлення протоколу SSH для входу на лінію:

```
Drobot_R0(config-line)#transpoR input ssh
Drobot_R0(config-line)#exit
```

Зберігання даних

```
Drobot_R0(config)#do write
```

Результат налаштування на маршрутизаорі наведено на рис.3.2.

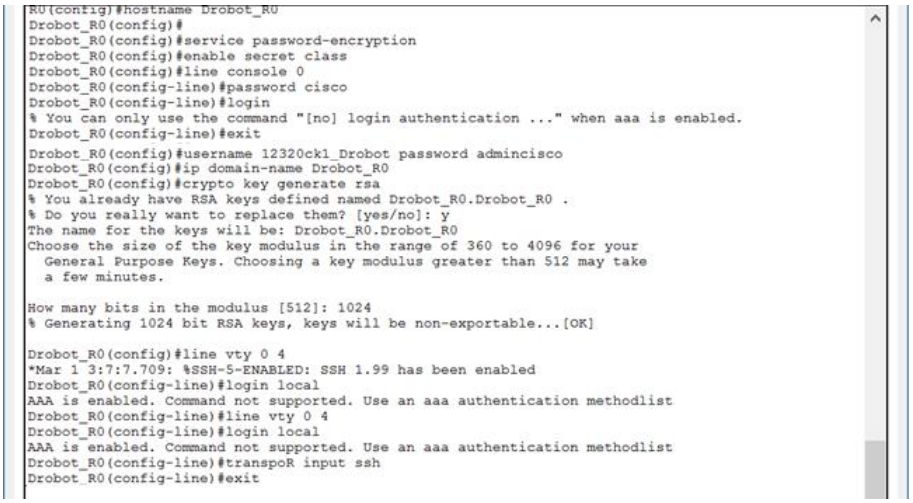


Рисунок 3.2 – Налаштування Drobotv_R0

Аналогічно виконуємо базові налаштування на решті маршрутизаторів як показано на рис.3.3 -3.4 та в додатку А.

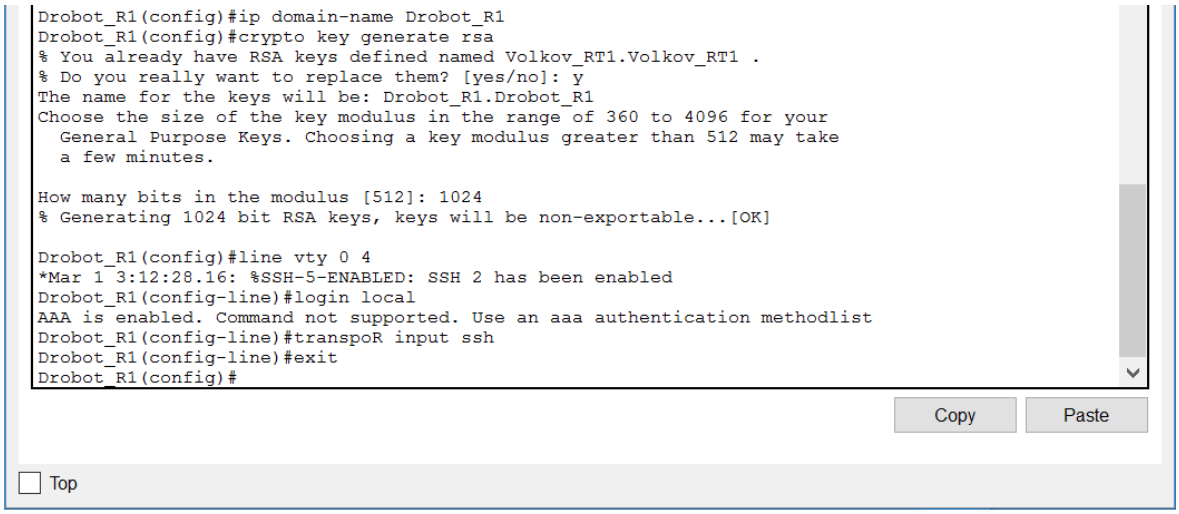


Рисунок 3.3 – Налаштування Drobotv_R1

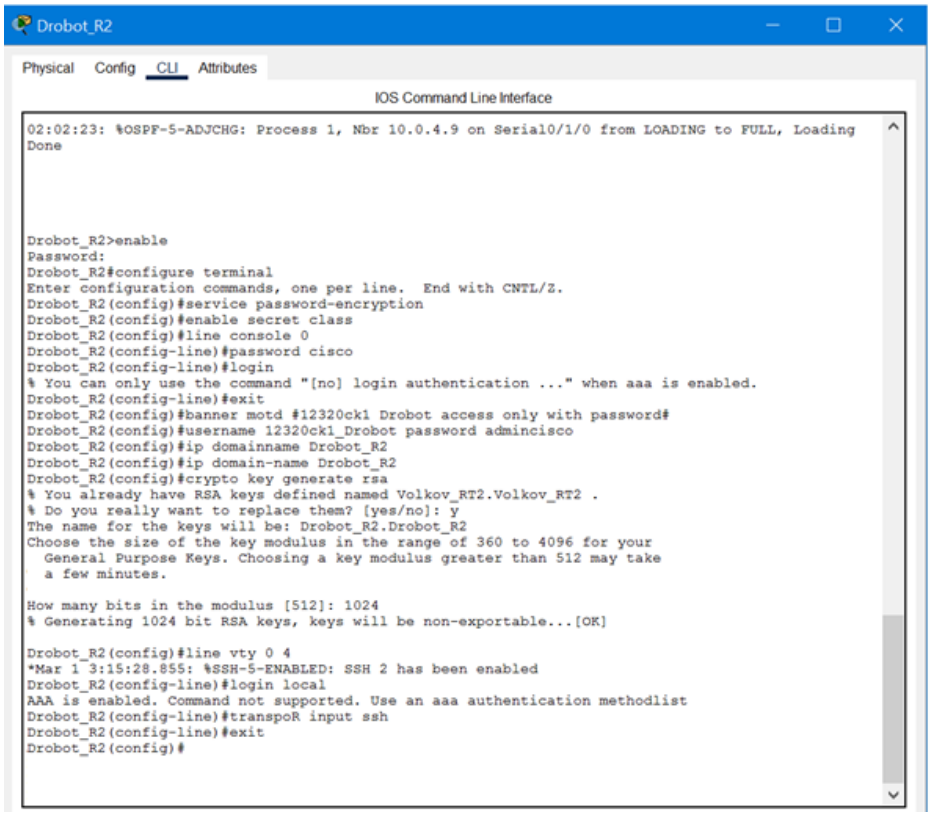


Рисунок 3.4 – Налаштування Drobotv_R2

Виконаємо перевірку базового налаштування. Так як, ми створили унікального користувача та паролі, то ОС Cisco повинна перевірити наші дані. На рис.3.5 наведено, що при вході в налаштування маршрутизатора з'являється запис про попередження входу в систему та запит пароля. При введенні коректних даних входимо в консольний режим, а для входу в привілейований знову треба ввести пароль. Все працює коректно.

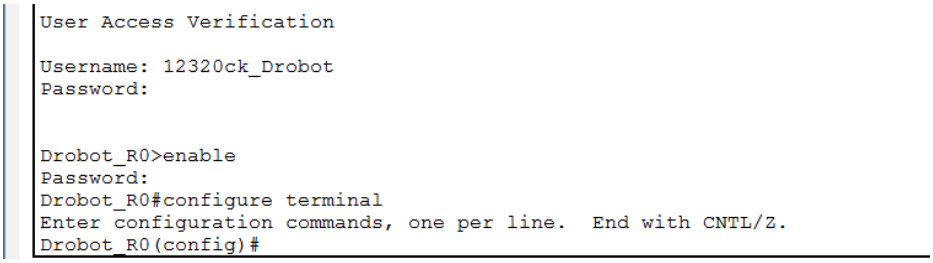


Рисунок 3.5 – Перевірка налаштування паролів для входу в налаштування

Тепер потрібно налаштувати всі інтерфейси відповідно до табл. 3.2. для цього потрібно звернутись до інтерфесу, який потрібно налаштувати, використати команду *ip address* та ввести адресу та її маску:

```
    Drobot_R0(config)#interface GigabitEthernet0/0
    Drobot_R0(config-if)#ip address 172.23.7.1
255.255.255.128
    Drobot_R0(config-if)#
    Drobot_R0(config-if)#exit
    Drobot_R0(config)#interface GigabitEthernet0/1
    Drobot_R0(config-if)#ip address 172.23.7.129
255.255.255.128
    Drobot_R0(config-if)#ip address 172.23.7.129
255.255.255.192
    Drobot_R0(config-if)#ip     address     172.23.7.129
255.255.255.192
    Drobot_R0(config)#interface Serial0/1/0
    Drobot_R0(config-if)#ip       address       10.0.4.1
255.255.255.252
```

3.2.2 Налаштування маршрутизаторів корпоративної мережі

Для розгортання мережі "LANARS" використовується протокол динамічної маршрутизації OSPF з ідентифікатором зони 1, в якій працюватиме інтерфейс маршрутизатора.

OSPF є протоколом маршрутизації, який використовує об'явлення стану каналу (link-state) для передачі інформації про стан мережевих з'єднань. Це означає, що кожен маршрутизатор в межах однієї ієрархічної області отримує об'явлення про стан каналів (link-state adveRisement - LSA). Об'явлення LSA містять інформацію про підключені інтерфейси. Зібравши інформацію про стан каналів, маршрутизатори OSPF використовують алгоритм SPF (ShoRest Path First) для обчислення найкоротших шляхів до кожного вузла.

Налаштування протоколу OSPF на маршрутизаторі Drobot_R0 включає наступні кроки:

Крок 1. Ввімкнення OSPF з ідентифікатором 1 на маршрутизаторі:

```
Drobot_R0(config)#router ospf 1
```

Крок 2. Визначити мережі, підключених до маршрутизатора:

```
Drobot_R0(config-router)#network 172.23.7.0 0.0.0.127 area 0
Drobot_R0(config-router)#network 172.23.7.128 0.0.0.127 area 0
Drobot_R0(config-router)#network 10.0.4.0 0.0.0.3 area 0
Drobot_R0(config-router)#network 10.0.4.4 0.0.0.3 area 0
Drobot_R0(config-router)#network 10.0.4.12 0.0.0.3 area 0
Drobot_R0(config-router)#network 172.23.6.0 0.0.0.63 area 0
Drobot_R0(config-router)#network 172.23.6.64 0.0.0.63 area 0
Drobot_R0(config-router)#network 172.23.6.128 0.0.0.63 area 0
```

Крок 3. Оголошення маршруту за замовчуванням:

```
Drobot_R0(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1
```

Крок 4. На serial–інтерфейсах згідно технічних вимог задано пропускну спроможність 128 Кб/с та вартість метрики 7500.

```
Drobot_R0(config)#int se0/1/0
Drobot_R0(config-if)#bandwidth 128
Drobot_R0(config-if)#ip ospf cost 7500
Drobot_R0(config-if)#exi
Drobot_R0(config)#int se0/1/1
Drobot_R0(config-if)#bandwidth 128
Drobot_R0(config-if)#ip ospf cost 7500
Drobot_R0(config-if)#exi
Drobot_R0(config)#int se0/2/0
Drobot_R0(config-if)#bandwidth 128
Drobot_R0(config-if)#ip ospf cost 7500
Drobot_R0(config-if)#exit
```

Перевіримо налаштування протоколу OSPF , на рисунках 3.6–3.8, можна визначити різні характеристики мережі. Символ "C" вказує на підключені інтерфейси в мережі, тоді як символ "O" вказує на віддалені мережі, які використовують протокол OSPF. Рядок "S*" надає інформацію про статичний маршрут за замовчуванням.

```
Drobot_R3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O       10.0.4.0/30 [110/15001] via 10.0.4.17, 02:05:47, GigabitEthernet0/2
O       10.0.4.4/30 [110/15001] via 10.0.4.17, 00:23:11, GigabitEthernet0/2
O       10.0.4.8/30 [110/7501] via 10.0.4.17, 02:05:47, GigabitEthernet0/2
O       10.0.4.12/30 [110/7501] via 10.0.4.17, 02:05:47, GigabitEthernet0/2
C       10.0.4.16/30 is directly connected, GigabitEthernet0/2
L       10.0.4.18/32 is directly connected, GigabitEthernet0/2
     172.23.0.0/16 is variably subnetted, 4 subnets, 3 masks
C       172.23.6.64/26 is directly connected, GigabitEthernet0/1
L       172.23.6.67/32 is directly connected, GigabitEthernet0/1
O       172.23.7.0/25 [110/7502] via 10.0.4.17, 00:15:39, GigabitEthernet0/2
O       172.23.7.128/26 [110/7502] via 10.0.4.17, 00:15:29, GigabitEthernet0/2
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/28 is directly connected, Serial0/1/0
L       209.165.202.2/32 is directly connected, Serial0/1/0
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Рисунок 3.6 – Перевірка динамічного протоколу на Drobot_R3

```
Drobot_R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.0.4.18 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O       10.0.4.0/30 [110/15000] via 10.0.4.13, 02:24:06, Serial0/2/0
                    [110/15000] via 10.0.4.9, 02:24:06, Serial0/1/0
O       10.0.4.4/30 [110/15000] via 10.0.4.13, 00:41:30, Serial0/2/0
                    [110/15000] via 10.0.4.9, 00:41:30, Serial0/1/0
C       10.0.4.8/30 is directly connected, Serial0/1/0
L       10.0.4.10/32 is directly connected, Serial0/1/0
C       10.0.4.12/30 is directly connected, Serial0/2/0
L       10.0.4.13/32 is directly connected, Serial0/2/0
C       10.0.4.16/30 is directly connected, GigabitEthernet0/2
L       10.0.4.17/32 is directly connected, GigabitEthernet0/2
     172.23.0.0/16 is variably subnetted, 4 subnets, 3 masks
C       172.23.6.64/26 is directly connected, GigabitEthernet0/1
L       172.23.6.65/32 is directly connected, GigabitEthernet0/1
O       172.23.7.0/25 [110/7501] via 10.0.4.13, 00:33:58, Serial0/2/0
O       172.23.7.128/26 [110/7501] via 10.0.4.13, 00:33:48, Serial0/2/0
O*E2 0.0.0.0/0 [110/1] via 10.0.4.18, 02:24:06, GigabitEthernet0/2

Drobot_R2#
```

Рисунок 3.7 – Перевірка динамічного протоколу на Drobot_R2

```
Drobot_R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.0.4.10 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.0.4.0/30 is directly connected, Serial0/1/0
L       10.0.4.2/32 is directly connected, Serial0/1/0
C       10.0.4.4/30 is directly connected, Serial0/1/1
L       10.0.4.6/32 is directly connected, Serial0/1/1
C       10.0.4.8/30 is directly connected, Serial0/2/0
L       10.0.4.9/32 is directly connected, Serial0/2/0
O       10.0.4.12/30 [110/15000] via 10.0.4.10, 02:29:27, Serial0/2/0
                     [110/15000] via 10.0.4.1, 02:29:27, Serial0/1/0
O       10.0.4.16/30 [110/7501] via 10.0.4.10, 02:29:27, Serial0/2/0
     172.23.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.23.6.64/26 [110/7501] via 10.0.4.10, 00:32:04, Serial0/2/0
O       172.23.7.0/25 [110/7501] via 10.0.4.1, 00:39:19, Serial0/1/0
O       172.23.7.128/26 [110/7501] via 10.0.4.1, 00:39:09, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 10.0.4.10, 02:29:27, Serial0/2/0

Drobot_R1#
```

Рисунок 3.8 – Перевірка динамічного протоколу на Drobot_R1

3.2.3 Налаштування роботи Інтернет

Відповідно до вказаної задачі кваліфікаційної роботи, для забезпечення доступу робочих станцій до Інтернету необхідно налаштувати технологію NAT на прикордонному маршрутизаторі. NAT (Network Address Translation)

використовується для спрощення та збереження IP-адрес. Ця технологія дозволяє приватним IP-мережам, що використовують незареєстровані IP-адреси, підключатися до Інтернету. Робота NAT здійснюється на маршрутизаторі, який зазвичай об'єднує дві мережі, і перетворює приватні адреси внутрішньої мережі на дійсні адреси перед відправленням пакетів в іншу мережу.

На прикордонному маршрутизаторі Drobot_R3 виконано налаштування NAT. Особливості цього налаштування включають розподіл вхідних/вихідних інтерфейсів (рис.3.9):

```
Drobot_R3(config)#int s0/1/0
Drobot_R3(config-if)#ip nat outside
Drobot_R3(config-if)#exi
Drobot_R3(config)#int g0/1
Drobot_R3(config-if)#ip nat inside
Drobot_R3(config-if)#exi
Drobot_R3(config)#int g0/2
Drobot_R3(config-if)#ip nat inside
Drobot_R3(config-if)#exi
```

Створення access–list для вихідного трафіку в Інтернет

```
Drobot_R3(config)#ip access-list standard Internet
Drobot_R3(config-std-nacl)#permit 172.23.7.0 0.0.0.127
Drobot_R3(config-std-nacl)#permit 172.23.7.128 0.0.0.127
Drobot_R3(config-std-nacl)#permit 172.23.6.0 0.0.0.63
Drobot_R3(config-std-nacl)#permit 172.23.6.64 0.0.0.63
Drobot_R3(config-std-nacl)#permit 172.23.6.128 0.0.0.63
Drobot_R3(config-std-nacl)#exi
```

Ввімкнення NAT на інтерфейсі

```
Drobot_R3(config)#ip nat inside source list Internet int s0/1/0 overload
```

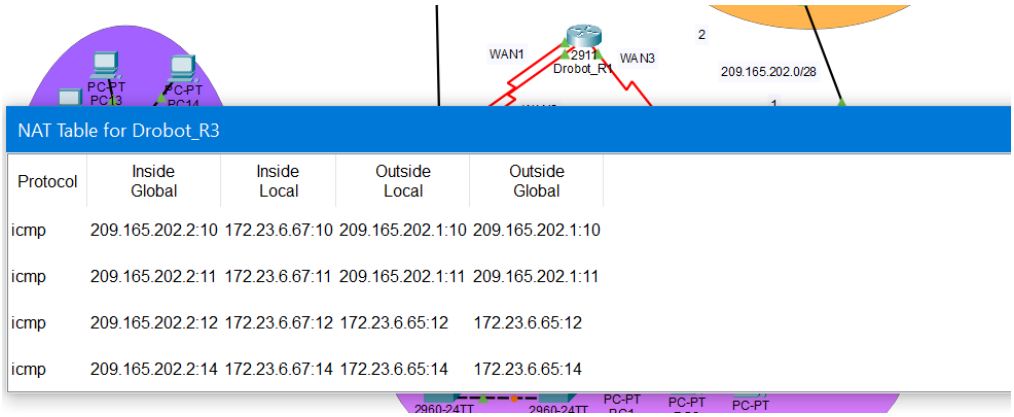


Рисунок 3.9 – Таблиця перетворень NAT

3.2.4 Налаштування агрегування каналів PAgP

Протокол агрегації портів (PAgP) є технологією EtherChannel, розробленою компанією Cisco. Вона використовується для логічного об'єднання портів комутатора Cisco Ethernet з метою балансування навантаження та трафіку. PAgP EtherChannel може поєднувати до 8 фізичних каналів в один віртуальний канал. Крім того, існує стандарт IEEE для управління агрегацією каналів під назвою LACP.

В мережі LAN2 для підвищення пропускної здатності та надійності каналів здійснюється об'єднання фізичних портів за допомогою технології EtherChannel на комутаторах. Ця технологія дозволяє об'єднати кілька фізичних портів на комутаторі в один логічний канал. Однією з переваг такого каналу є підвищення швидкості передачі даних.

Приклад налаштування наведено з комутатора Drobot_SW12:

```
Drobot_SW12(config)#interface range fastEthernet 0/6-7
Drobot_SW12(config-if-range)#shutdown
Drobot_SW12(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
Drobot_SW12(config-if-range)#no shutdown
Drobot_SW12 (config-if-range)#int port-channel 1
Switch(config-if)#switchport  mode trunk
```

Перевірити налаштування протоколу PAgP, можна використавши команду `sh etherchannel summary`. Результат на рис.3.10.

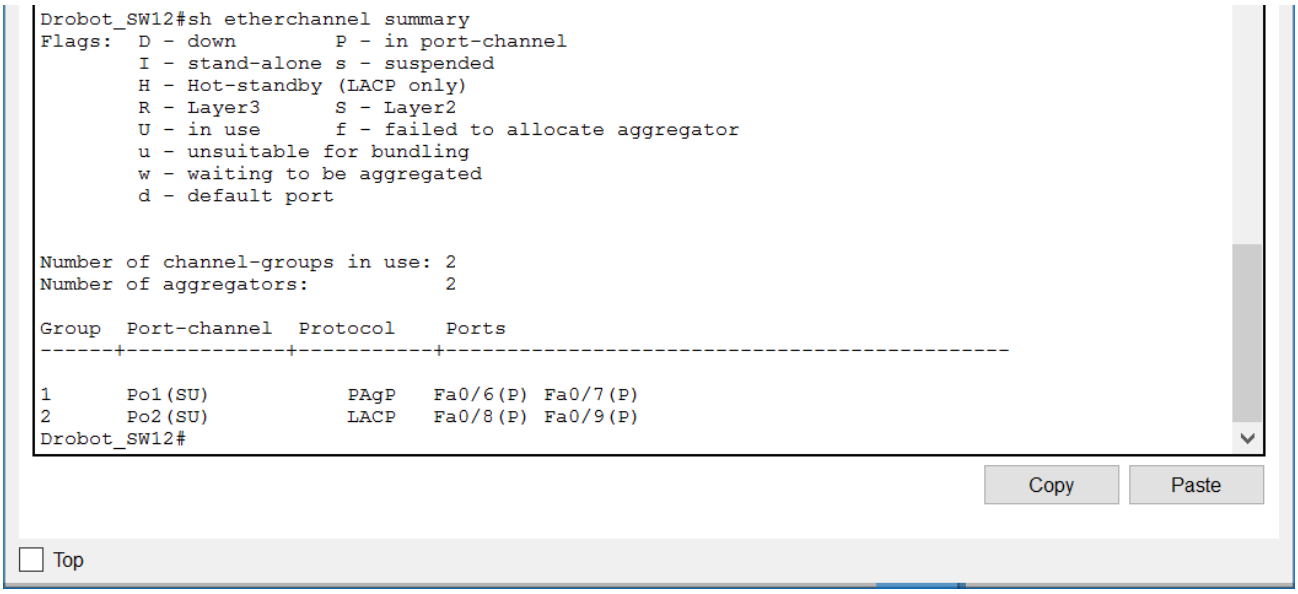


Рисунок 3.10 – Перевірка параметрів PAgP

3.2.5 Налаштування віртуальної приватної мережі

Для налаштування віртуальної приватної мережі (VPN) типу site-to-site з використанням IPsec (Internet Protocol Security) потрібно виконати наступні кроки:

Визначте параметри мережі:

– ідентифікуваати локальну мережу, з якої ви плануєте створити VPN;

– визначити віддалену мережу, з якою ви хочете встановити VPN-з'єднання;

– визначити ip-адреси тунельних інтерфейсів (один для локальної мережі, інший для віддаленої мережі);

Налаштувати основний мережевий обладнання:

– налаштувати маршрутизатор або брандмауер, який використовується як шлюз для локальної мережі.

– створити IPsec політику для шифрування трафіку між локальною і

віддаленою мережами.

– встановити ключі шифрування (pre-shared keys) для аутентифікації між мережами.

– налаштувати IPsec тунельні параметри, такі як протоколи шифрування, алгоритми і ключі.

– налаштувати віддалений мережевий обладнання;

Перевіритии підключення:

– запустіть VPN-з'єднання і перевірте статус з'єднання.

– переконайтеся, що трафік вільно перетинає VPN-тунель між локальною і віддаленою мережами.

Налаштування VPN з використанням Ipsec в даній роботі виконано для підмережі LAN4 та віддаленої мережі LAN3 (рис.3.11).

```
Drobot_R3(config)#access-list 110 permit ip 172.22.64.0
0.0.0.255 172.22.65.0 0.0.0.255
Drobot_R3(config)#crypto isakmp policy 10
Drobot_R3(config-isakmp)#encryption aes
Drobot_R3(config-isakmp)#authentication pre-share
Drobot_R3(config-isakmp)#group 2
Drobot_R3(config-isakmp)#exi
Drobot_R3(config)#crypto isakmp key cisco address
209.165.202.1
Drobot_R3(config)#crypto ipsec transform-set VPN-SET esp-3des
esp-sha-hmac
Drobot_R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Drobot_R3(config-crypto-map)#description VPN connection to IPS
Drobot_R3(config-crypto-map)#set peer 209.165.202.1
Drobot_R3(config-crypto-map)#set transform-set VPN-SET
Drobot_R3(config-crypto-map)#match address 110
Drobot_R3(config-crypto-map)#exi
Drobot_R3(config)#int s0/1/0
Drobot_R3(config-if)#crypto map VPN-MAP
```

```
Drobot_IPS#sh crypto  ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 209.165.202.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.22.65.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.22.64.0/255.255.255.0/0/0)
   current_peer 209.165.202.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
   #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.202.1, remote crypto endpt.:209.165.202.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x0(0)
```

Рисунок 3.11 – Результат роботи Ipsec SA на маршрутизаторі IPS

3.2.6 Налаштування серверів

В нашій системі наявні три сервера: DNS, HTTP, FTP, які потрібно налаштувати.

Налаштування сервера DNS (Domain Name System):

1 Встановити і налаштуйте DNS-сервер, такий як BIND (Berkeley Internet Name Domain), на відповідному сервері.

2 Створити і налаштуйте DNS-записи (A-записи, CNAME-записи, MX-записи тощо) для вашого домену або піддомену.

3 Налаштувати параметри безпеки, такі як DNSSEC (DNS Security Extensions), якщо вони є необхідними. Результат наведено на рис.3.12.

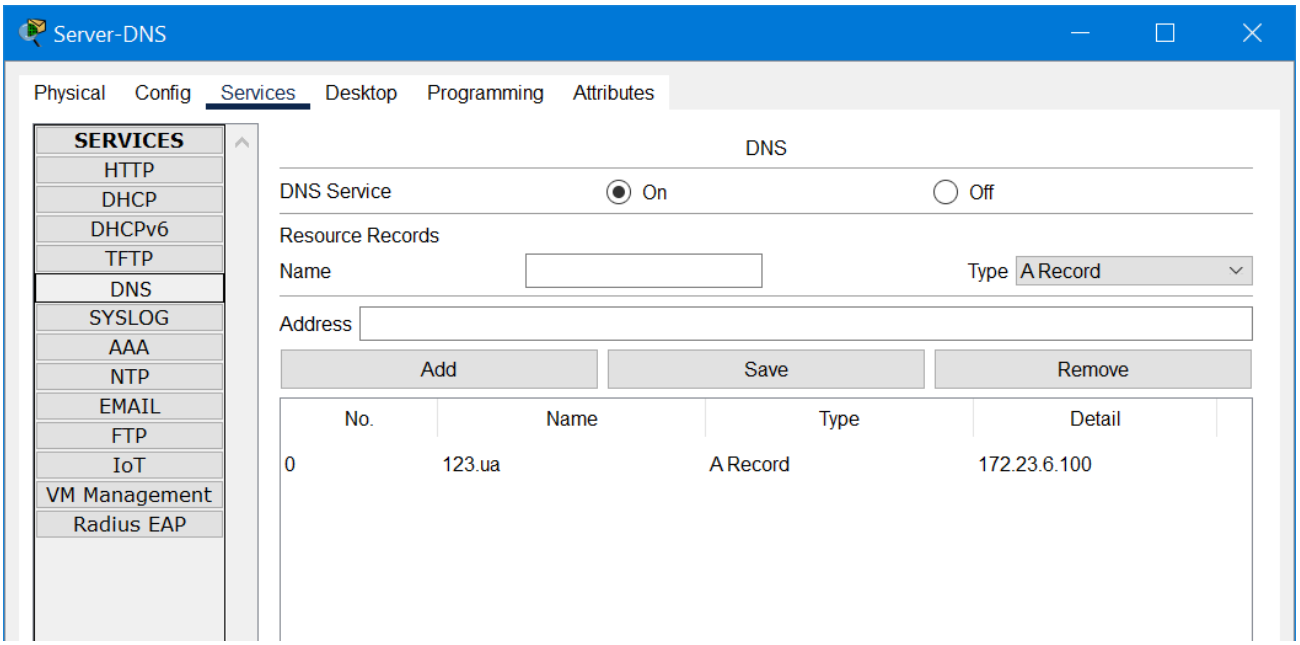


Рисунок 3.12 – Налаштування DNS-сервера

Налаштування сервера HTTP (Hypertext Transfer Protocol):

1 Встановити та налаштуйвати веб-сервер, такий як Apache HTTP Server або Nginx, на відповідному сервері.

2 Створіть та налаштуйте веб-сайт, включаючи конфігураційні файли, директорії, віртуальні хости, SSL-сертифікати (якщо потрібно), аутентифікацію тощо.

3 Налаштуйте файрвол та мережеві правила для дозволу доступу до веб-сервера зовнішнім користувачам.

На рис.3.13 наведено використані файли для сервера. Головним є index.html, яка і містить головну сторінку веб-сайту.

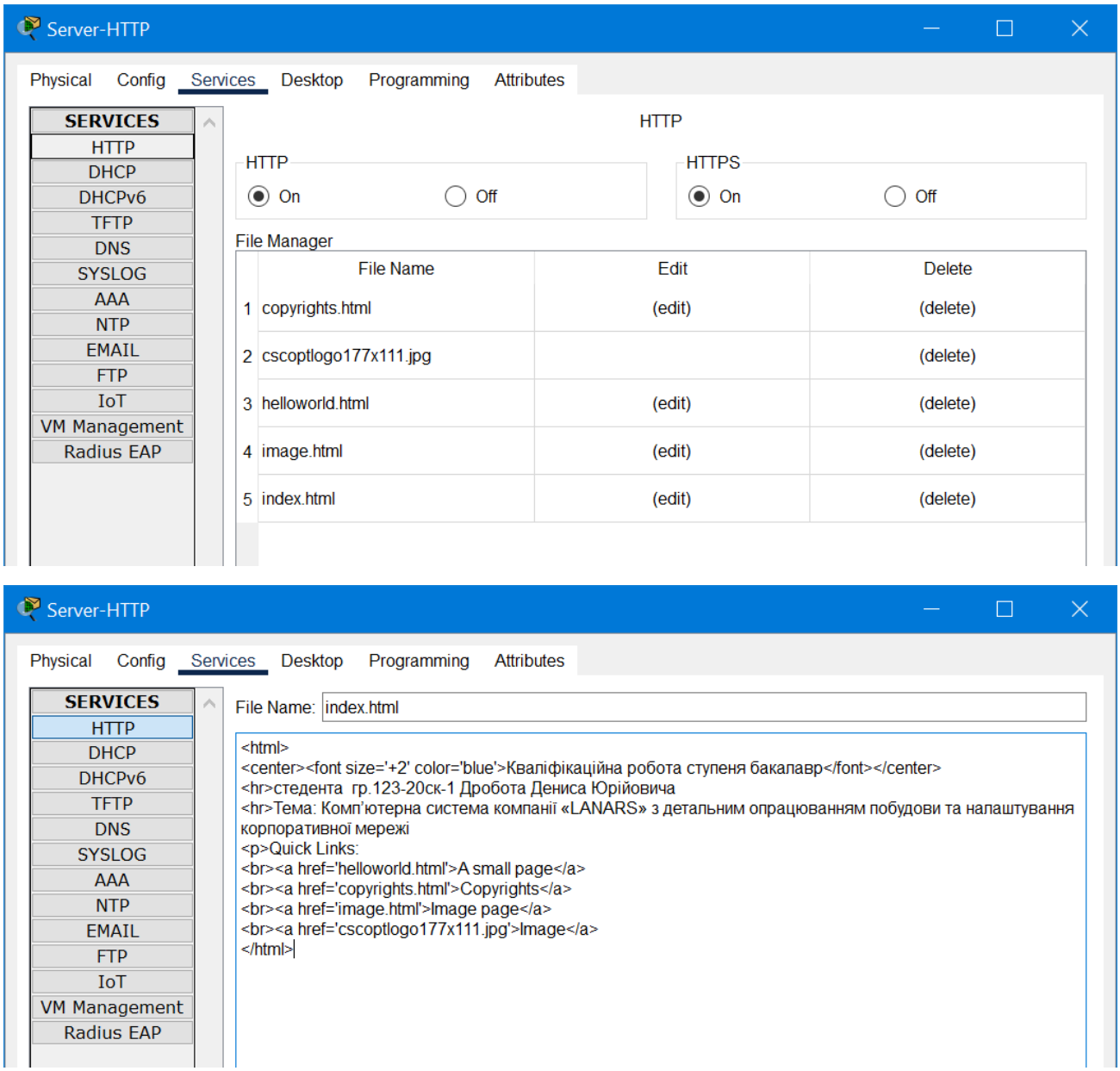


Рисунок 3.13 – Налаштування сервера HTTP

Налаштування сервера FTP (File Transfer Protocol):

1 Встановити та налаштувати FTP-сервер, такий як vsftpd (Very Secure FTP Daemon) або ProFTPD, на відповідному сервері.

2 Створити і налаштувати FTP-користувачів з відповідними правами доступу до файлів та каталогів.

3 Налаштувати шифрування (якщо необхідно) за допомогою SSL-сертифікатів для безпечного передавання файлів по FTP.

3.2.7 Перевірка роботи комп’ютерної системи

Для проведення випробування функціональності комп'ютерної системи, ми здійснимо перевірку доступності вузлів мережі та перевіримо налаштування безпечного віддаленого доступу.

Для перевірки доступності SSH, ми виконаємо з'єднання з командного рядка ПК14, що знаходиться в підмережі LAN5, до маршрутизатора Drobot_R0 з використанням облікового запису 123-20ck1_Drobot та паролю admincisco. Результат перевірки можна знайти на рисунку 3.14. Ми навмисно перший раз ввели не правильний пароль, і система запросила ще раз пароль. Другий раз ми ввели правильний пароль і увійшли в користувальницький режим, потім був запит пароля для входу в привілейований режим. Перевірка виконана успішно.

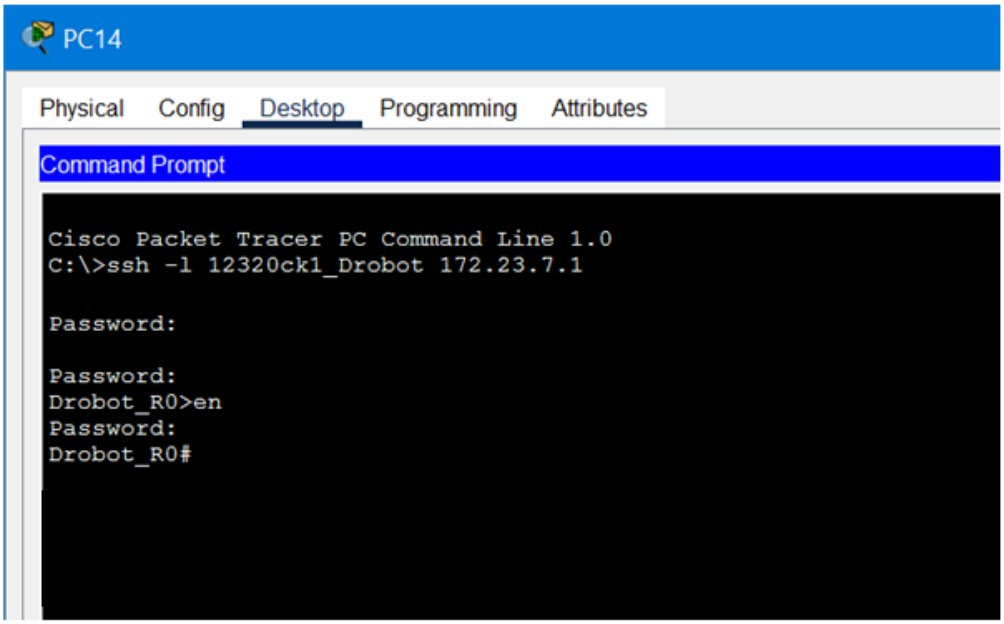


Рисунок 3.14 – Перевірка роботи SSH

Перевіримо роботу DHCP. Для цього перейдемо в підмережу LAN2 і на ПК10 відкриємо налаштування , як показано на рис.3.15 протокол працює правильно та розподіляє адреси відповідно до схеми адресації табл.3.2.

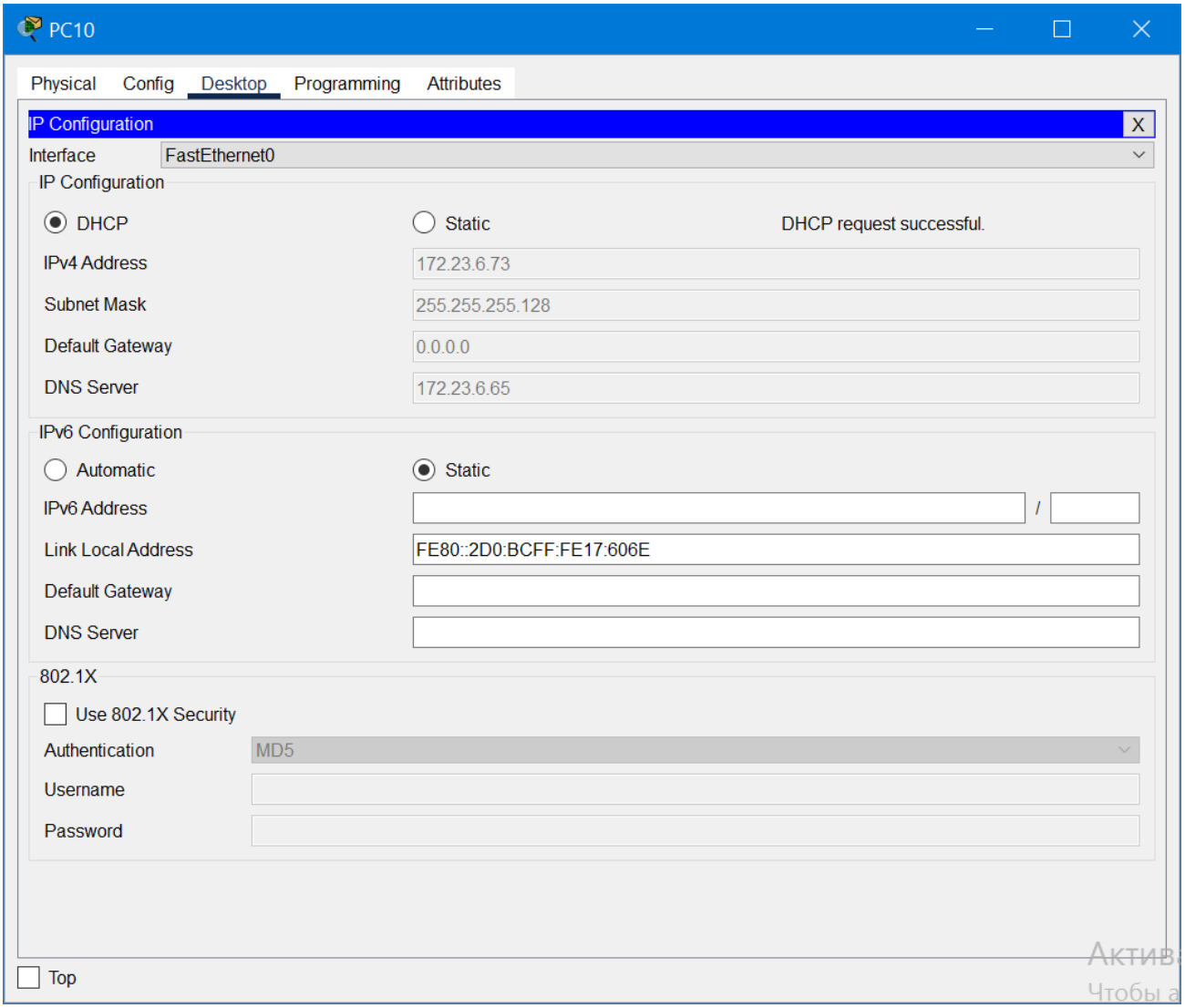


Рисунок 3.15 – Перевірка протоколу DHCP

Для перевірки наявності зв'язку між різними підрозділами, будемо використовувати команду ping з різних підмереж. Результат наведено на рис.3.16.

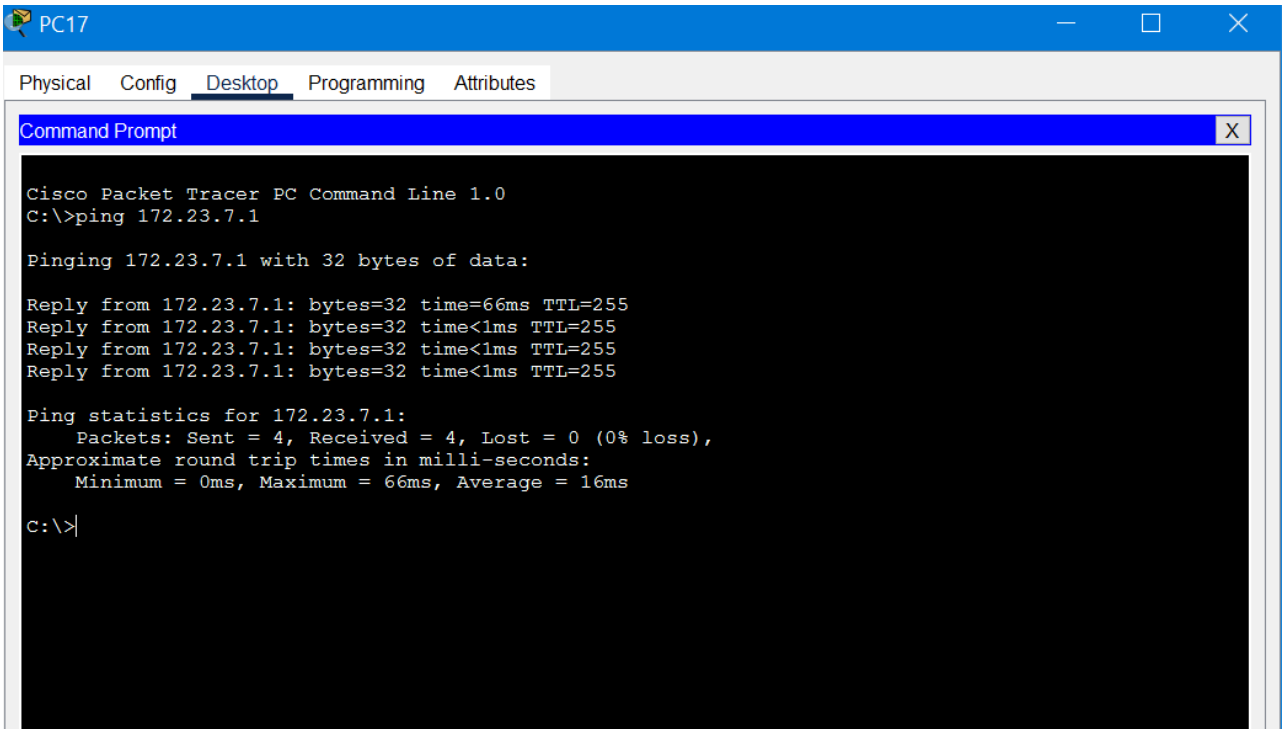


Рисунок 3.16 – Пінгування під мереж

Для перевірки HTTP-сервера на ПК0 введемо доменне ім'я 123.ua у вікні браузера. Результат цієї перевірки можна побачити на рисунку 3.17.

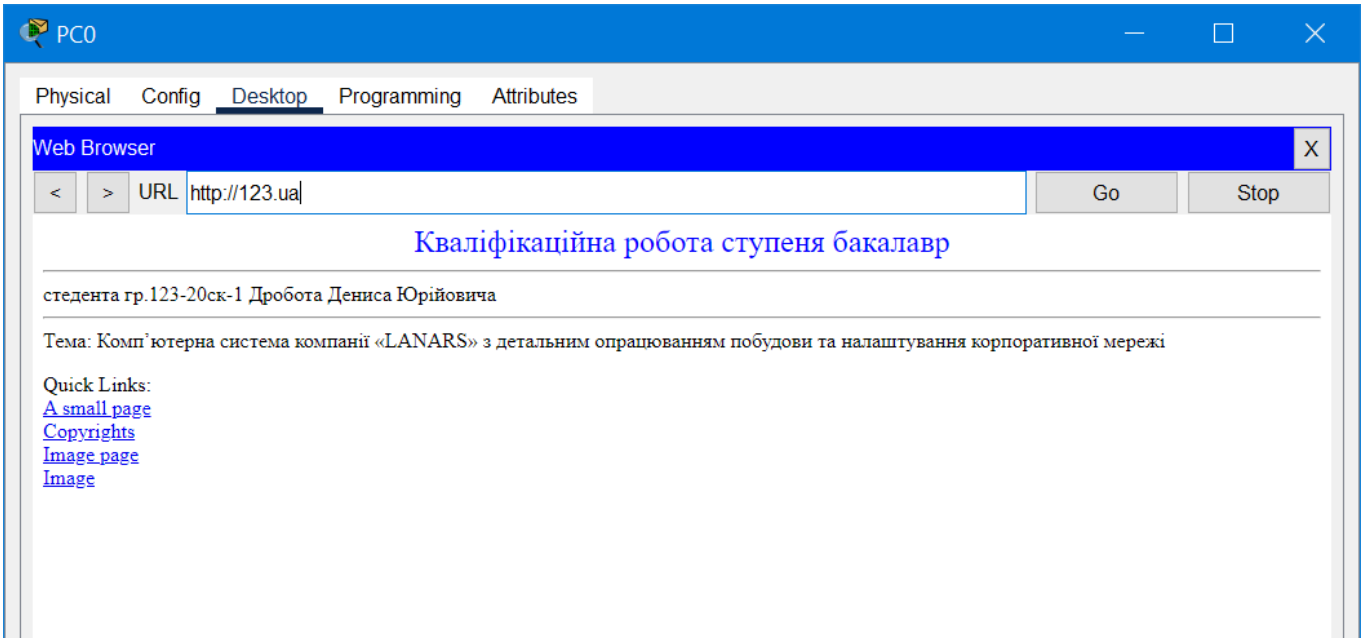


Рисунок 3.17 – Перевірка HTTP-сервера та відображення сайту

3.3 Захист інформації в КСС від несанкціонованого доступу

3.3.1. Розробка методів для захисту інформації в комп’ютерній системі

Віртуальна локальна мережа (VLAN) - це логічна локальна мережа, яка розширює межі традиційної локальної мережі шляхом групування сегментів локальної мережі згідно з певними конфігураціями [8]. VLAN є логічним об'єктом, тому його створення і налаштування повністю здійснюються програмним забезпеченням. Використовуючи VLAN, кілька мереж можуть працювати практично як одна локальна мережа. Однією з найбільш корисних функцій VLAN є усунення затримки в мережі, що дозволяє економити мережеві ресурси і підвищувати її ефективність. Крім того, VLAN створені для сегментації мережі та підтримки питань безпеки, управління мережею і масштабованості.

Для налаштування мереж VLAN і маршрутизації між ними потрібно виконати етапи, описаны нижче.

Етап 1. Створити список VLAN і присвоїти кожному з них ім'я згідно з таблицею 3.3.

Етап 2. Налаштувати транкові порти та порти доступу.

Етап 3. Налаштувати інтерфейси SVI (Switched Virtual Interface) на комутаторах.

Етап 4. Налаштувати маршрутизацію між мережами VLAN.

Підмережу LAN4 сегменутємо на окремі віртуальні мережі, згідно таблиці 3.3.

Таблиця 3.3— Список мереж VLAN

Номер VLAN	Ім’я VLAN	Інтерфейс підключення
14	Accounting	Fa0/12–14
24	Resources Department	Fa0/15–24
34	Guest	Fa0/6–11
99	Management	Fa0/1–5
100	Native	G0/1

Налаштування технології VLAN на Drobot_SW0.

```
Drobot_SW0(config)#vlan 14
Drobot_SW0(config-vlan)#name Accounting
Drobot_SW0(config-vlan)#vlan 24
Drobot_SW0(config-vlan)#name Resources_Department
Drobot_SW0(config-vlan)#vlan 34
Drobot_SW0(config-vlan)#
Drobot_SW0(config-vlan)#name Guest
Drobot_SW0(config-vlan)#vlan 99
Drobot_SW0(config-vlan)#name Management
Drobot_SW0(config-vlan)#vlan 100
Drobot_SW0(config-vlan)#name Native
Drobot_SW0(config-vlan)#exit
Drobot_SW0(config)#int range fastEthernet 0/12-14
Drobot_SW0(config-if-range)#switchport access vlan 14
Drobot_SW0(config-if-range)#exit
Drobot_SW0(config)#int range fastEthernet 0/15-24
Drobot_SW0(config-if-range)#switchport access vlan 24
Drobot_SW0(config-if-range)#exit
Drobot_SW0(config)#int range fastEthernet 0/6-11
Drobot_SW0(config-if-range)#switchport access vlan 34
Drobot_SW0(config-if-range)#exit
```

```
Drobot_SW0(config)#int range fa0/1-5
Drobot_SW0(config-if-range)#switchport access vlan 99
Drobot_SW0(config-if-range)#exit
Drobot_SW0(config)#int range gi0/1-2
Drobot_SW0(config-if)# switchport trunk native vlan 100
Drobot_SW0(config-if)#switchport trunk allowed vlan 14,24,34,99,100
Drobot_SW0(config-if-range)#switchport mode trunk
Drobot_SW1(config)#int Vlan99
Drobot_SW1(config-if)#ip address 172.22.66.81 255.255.255.240
Drobot_SW1(config-if)#no sh
Drobot_SW1(config-if)#ip default-gateway 172.22.66.80
255.255.255.240
```

На рис.3.18 наведено результат налаштувань коду, описаного вище.

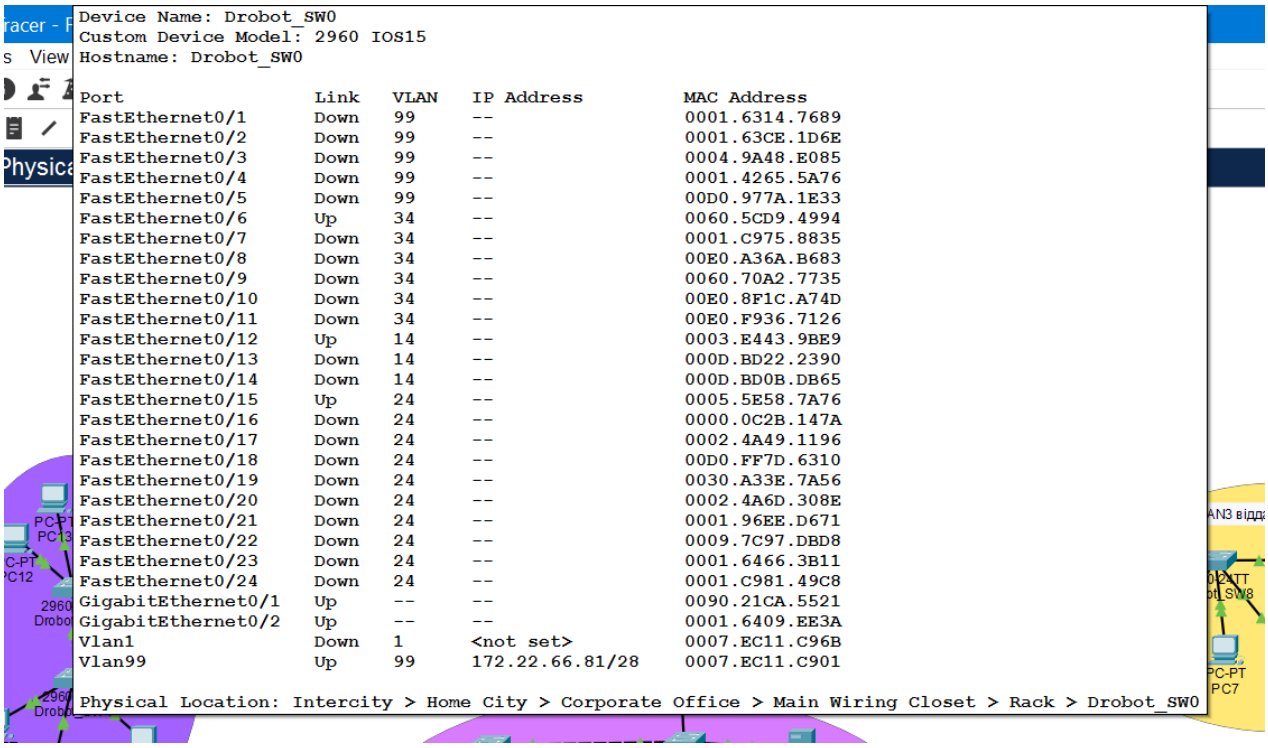


Рисунок 3.18 – Налаштування VLAN

3.3.2. Налаштувати всі маршрутизатори на підтримку служби AAA та RADIUS–сервер

Протокол RADIUS забезпечує централізований метод аутентифікації користувачів шляхом звернення до зовнішнього сервера, і використовується для аутентифікації, авторизації та обліку. Шляхом звернення до бази даних користувачів на RADIUS-сервері, яка містить дані автентифікації для кожного користувача, протокол RADIUS забезпечує безпеку при доступі до ресурсів мережі.

Відповідно до технічних вимог, на всіх маршрутизаторах необхідно налаштувати підтримку служби AAA (Authentication, Authorization, and Accounting) за такими принципами:

Використовувати локальну базу даних користувачів для перевірки підключень до VTY ліній.

- для доступу до консолі використовувати аутентифікацію на основі radius, а якщо це неможливо, то використовувати локальну базу даних;
- на сервері radius налаштувати ключове слово "radius123", а в якості облікового запису користувачів використовувати ім'я пристрою з паролем "admin123".

Результат налаштувань:

```
Drobot_R3(config)#aaa new-model
Drobot_R3(config)#aaa auth
Drobot_R3(config)#aaa authentication login default local
Drobot_R3(config)#aaa authentication login Drobot_R2 group radius
local
Drobot_R3(config)#line console 0
Drobot_R3(config-line)#login authentication Drobot_R2
Drobot_R3(config-line)#exit
Drobot_R3(config)#line vty 0 4
Drobot_R3(config-line)#login authentication default
```

```
Drobot_R3(config-line)#username Drobot_R2 password admin123
Drobot_R3(config)#radius-server host 172.22.64.5 auth-port 1645
Drobot_R3(config)#radius-server key radius123
```

На рис.3.19 наведено параметри AAA та на рис.3.20 та рис.3.21 результат роботи.

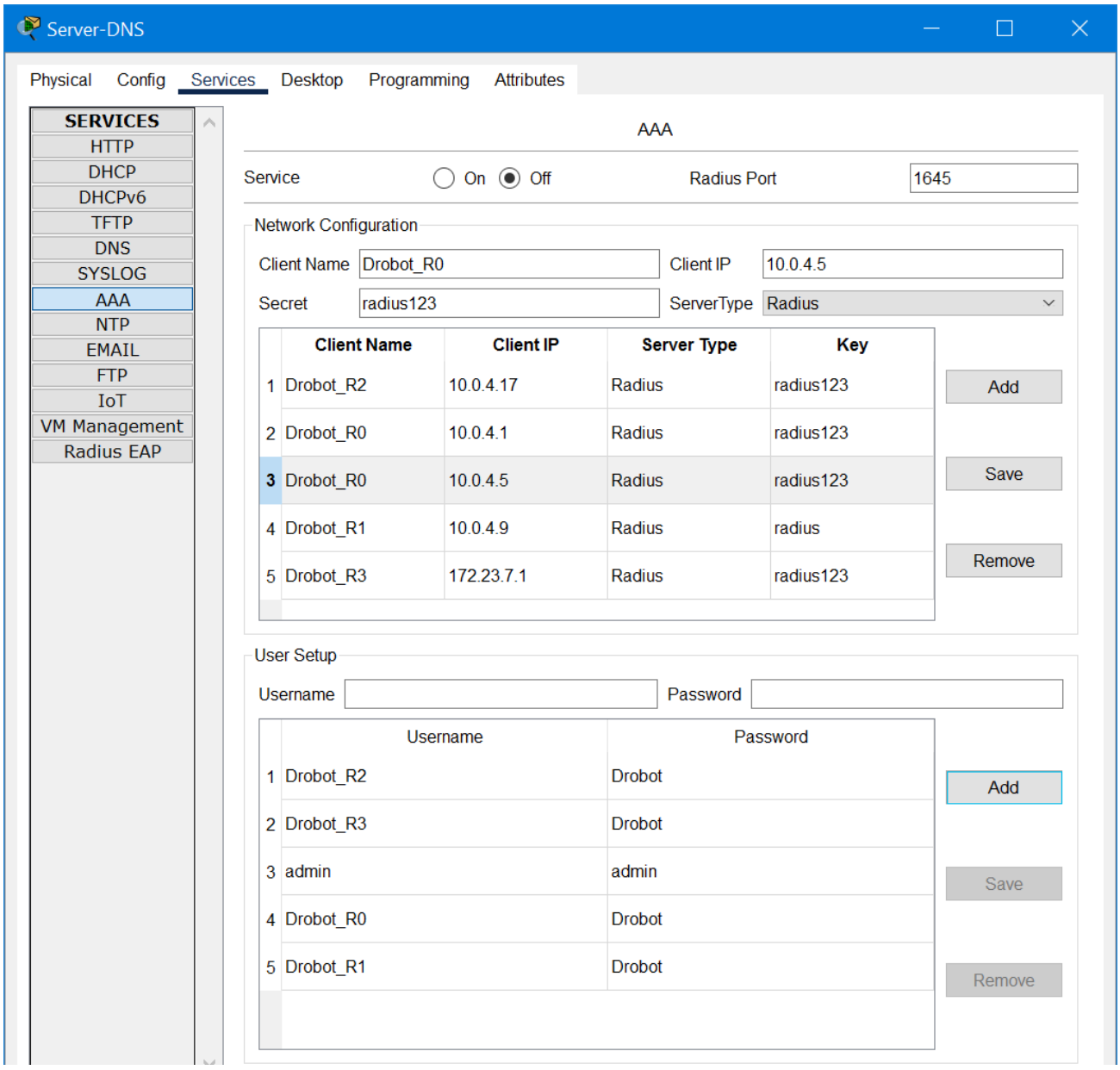


Рисунок 3.19 – AAA налаштування

```
12320ck1 Drobot access only with password

User Access Verification

Username: admin
Password:


Drobot_R1>enable
Password:
Drobot_R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Drobot_R1(config)#
```

Рисунок 3.20 – Перевірка AAA налаштування Drobot_R1

```
12320ck1 Drobot access only with password

User Access Verification

Username: Drobot_R0
Password:
Drobot_R0>enable
Password:
Drobot_R0#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Drobot_R0(config)#
```

Рисунок 3.21 – Перевірка AAA налаштування Drobot_R0

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було проведено детальний аналіз об’єкту для проектування нової мережі комп’ютерної системи компанії «LANARS». Результати аналізу включали вибір відповідного фізичного середовища, підключення портів мережевих пристроїв до інших пристроїв та вузлів, вибір необхідних мережевих пристроїв і компонентів для задоволення технічних вимог обробки даних в мережевих вузлах.

Корпоративна мережа є важливою складовою інфраструктури компанії "LANARS", яка забезпечує зв'язок та обмін даними між різними підрозділами та пристроями в організації. Побудова корпоративної мережі базується на використанні сучасних мережевих технологій та протоколів, таких як Ethernet, TCP/IP, VLAN тощо.

Процес побудови мережі включає планування топології, вибір необхідного мережевого обладнання, налаштування комутаторів, маршрутизаторів та інших пристроїв, а також конфігурацію мережевих сервісів, таких як DNS, DHCP, FTP, HTTP.

Важливим аспектом налаштування корпоративної мережі є забезпечення безпеки. Для цього використовуються протоколи шифрування, файрволи, системи аутентифікації та авторизації, такі як RADIUS.

Корпоративна мережа "LANARS" успішно пройшла процес налаштування, що дозволяє забезпечити безперебійний та надійний обмін даними між всіма підрозділами компанії. Правильно налаштована корпоративна мережа сприяє підвищенню продуктивності працівників, покращенню комунікації, поліпшенню безпеки і зниженню затрат на обслуговування та розширення мережі.

Всі вимоги та потреби компанії "LANARS" щодо побудови та налаштування корпоративної мережі були успішно виконано.

ПЕРЕЛІК ПОСИЛАНЬ

1. Політехніка уклала угоду про співпрацю з найбільшою українською глобальною IT-компанією. Режим доступу: https://nupp.edu.ua/news/politekhnika-uklala-ugodu-pro-spivpratsyu znaybilshoyu-ukrainskoyu-globalnoyu-it-kompanieyu.html

2. Європейська Бізнес Асоціація. Режим доступу: http://eba.com.ua/uk/lobbying/committees/item/4049-eba-it-committee#eba-itcommittee

3. Компанія «LANARS». Режим доступу: https://jobs.dou.ua/companies/lanars/

4. Thoben, Klaus-Dieter & Kirisci, Pierre & Kicin, Sébastien & Eschenbacher, Jens & Higgins, Paul. (2002). Holistic approach for structuring the various facets of e-business in enterprise networks. 17-19.

5. Ст Оліфер, Н. Оліфер. Комп'ютерні мережі. Принципи, технології, протоколи: Підручник для вузів. - 4-те вид. – Київ: Ліра, 2012. – 944 с.

6. Оглад мережевого обладнання Cisco: [електронний ресурс] — Режим доступу: URLhttps://gta.group/cisco–equipment–overview/

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

8. Стандарт динамічної мартшрутизації протокола OSPF. [Електронний ресурс] – Режим доступа:URL: https://www.ibm.com/docs/en/i/7.4?topic=routing-open-shortest-path-first

ДОДАТОК А ТЕКСТ ПРОГРАМИ

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.22006−01 12 01

Листів 5

2023

АНОТАЦІЯ

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

ЗМІСТ

1 Налаштування роутера Drobot_R2

```
Current configuration : 2307 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Drobot _R2
!
!
!
!
ip dhcp excluded-address 172.23.6.1
ip dhcp excluded-address 172.23.6.65
ip dhcp excluded-address 172.23.6.129
ip dhcp excluded-address 172.23.7.1
!
ip dhcp pool LAN3
 network 172.23.6.0 255.255.255.0
 default-router 172.23.6.1
 dns-server 8.8.8.8
ip dhcp pool DHCP31
 network 172.23.6.0 255.255.255.192
 default-router 172.23.6.1
 dns-server 8.8.8.8
ip dhcp pool DHCP32
 network 172.23.6.64 255.255.255.192
 default-router 172.23.6.65
 dns-server 8.8.8.8
ip dhcp pool DHCP33
 network 172.23.6.128 255.255.255.192
 default-router 172.23.6.129
 dns-server 8.8.8.8
!
!
aaa new-model
!
aaa authentication login Login group radius
local
aaa authentication login default local
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Loopback0
 ip address 172.23.6.2 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.31
 encapsulation dot1Q 31
 ip address 172.23.6.1 255.255.255.192
!
interface FastEthernet0/0.32
 encapsulation dot1Q 32
 ip address 172.23.6.65 255.255.255.192
!
interface FastEthernet0/0.33
 encapsulation dot1Q 33
 ip address 172.23.6.129 255.255.255.192
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial1/0
```

```
 ip address 10.10.12.2 255.255.255.252
!
interface Serial1/1
 ip address 10.10.23.1 255.255.255.252
 clock rate 56000
!
interface Serial1/2
 ip address 10.10.24.1 255.255.255.252
!
interface Serial1/3
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 172.23.6.0 0.0.0.63 area 0
 network 172.23.6.64 0.0.0.63 area 0
 network 172.23.6.128 0.0.0.63 area 0
 network 10.10.12.0 0.0.0.3 area 0
 network 10.10.23.0 0.0.0.3 area 0
 network 10.10.24.0 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial1/0
!
ip flow-expoR version 9
!
!
!
no cdp run
!
!
radius-server host 10.10.23.1 auth-poR 1645
radius-server key cisco
!
!
!
!
line con 0
 login authentication Login
!
line aux 0
!
line vty 0 4
 login authentication default
!
!
!
end
```

1 Налаштування комутатора Drobot_Sw V0.1

```
Current configuration : 2678 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sapko_SW0.1
!
enable secret 5 $1$mERr$NK8mve7aY79HRdsS779Mw.
!
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface PoR-channel1
 switchpoR mode trunk
!
interface PoR-channel2
 switchpoR mode trunk
!
interface FastEthernet0/1
 switchpoR mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface FastEthernet0/2
 switchpoR mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface FastEthernet0/3
 switchpoR mode trunk
 channel-protocol lacp
```

```
 channel-group 2 mode active
!
interface FastEthernet0/4
 switchpoR mode trunk
 channel-protocol lacp
 channel-group 2 mode active
!
interface FastEthernet0/5
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/6
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/7
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/8
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/9
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/10
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/11
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/12
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/13
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/14
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/15
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/16
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/17
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/18
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/19
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/20
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/21
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/22
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/23
 switchpoR access vlan 10
 switchpoR mode access
!
interface FastEthernet0/24
 switchpoR access vlan 10
 switchpoR mode access
!
interface GigabitEthernet0/1
 switchpoR access vlan 10
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
```

```
banner motd ^C^C
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login
 transpoR input telnet
line vty 5 15
 login
!
!
!
!
end
```

ДОДАТОК Б − НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ. ТАБЛИЦІ МАРШРУТИЗАЦІЇ

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

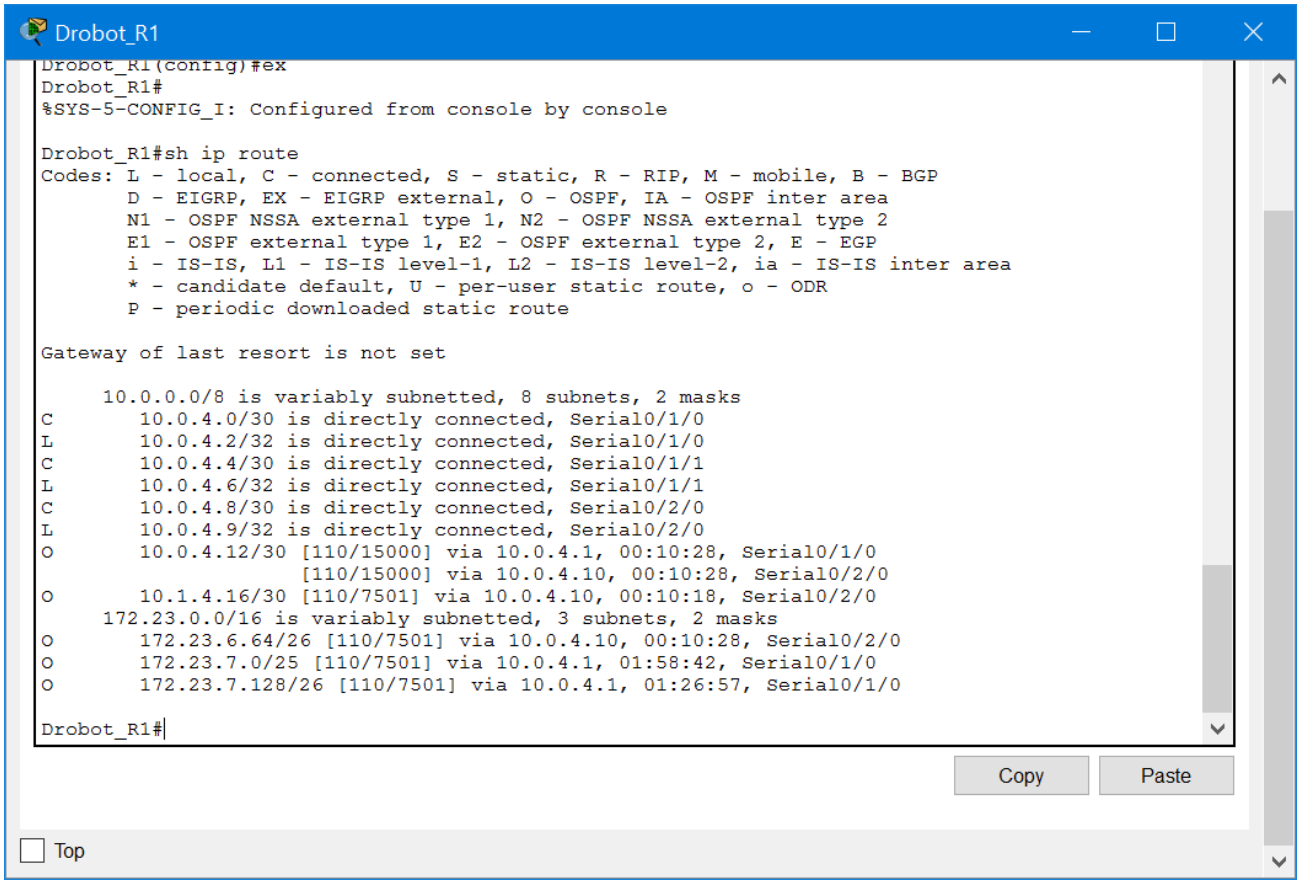
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Таблиці маршрутизації

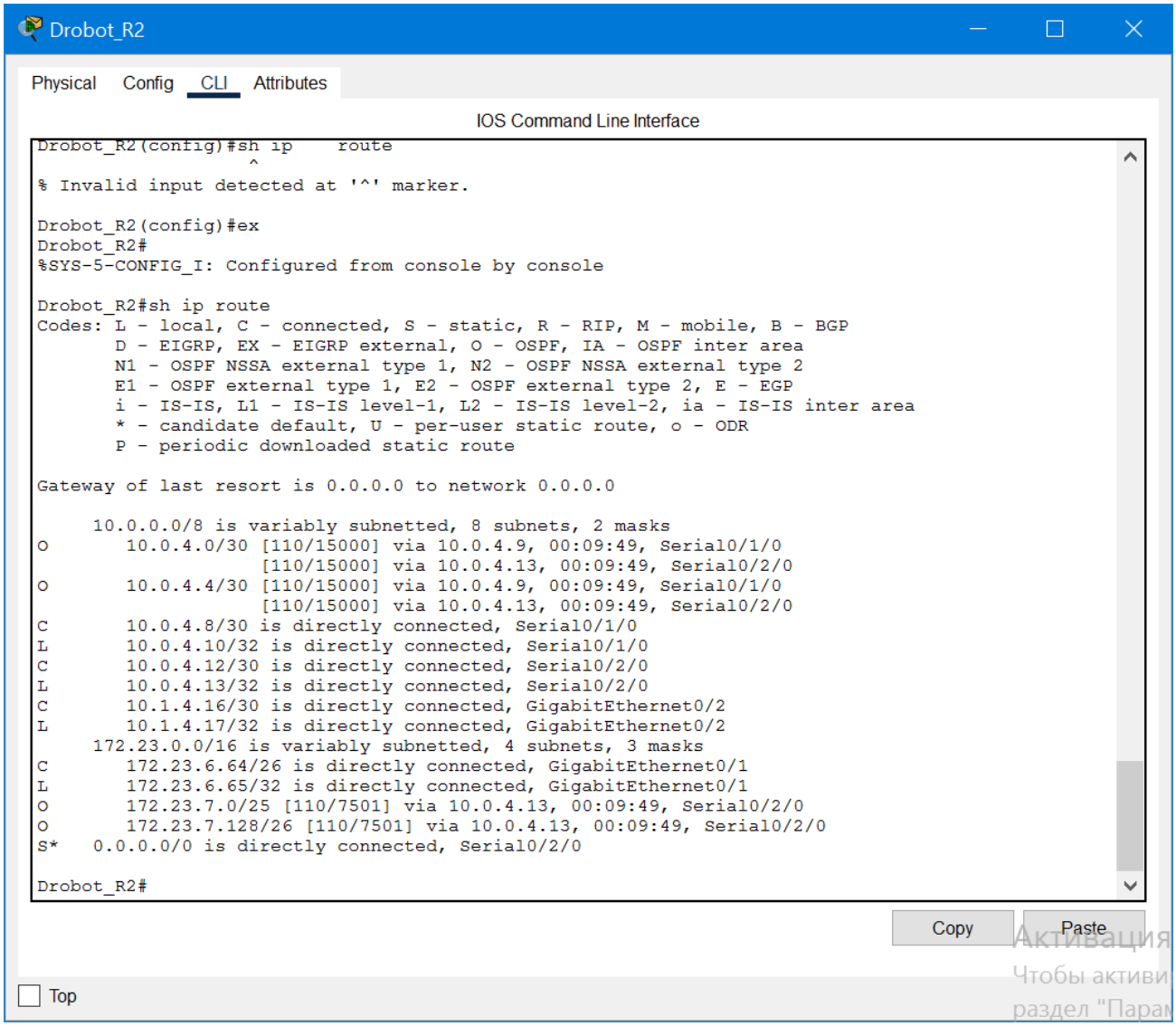
Листів 5

2023

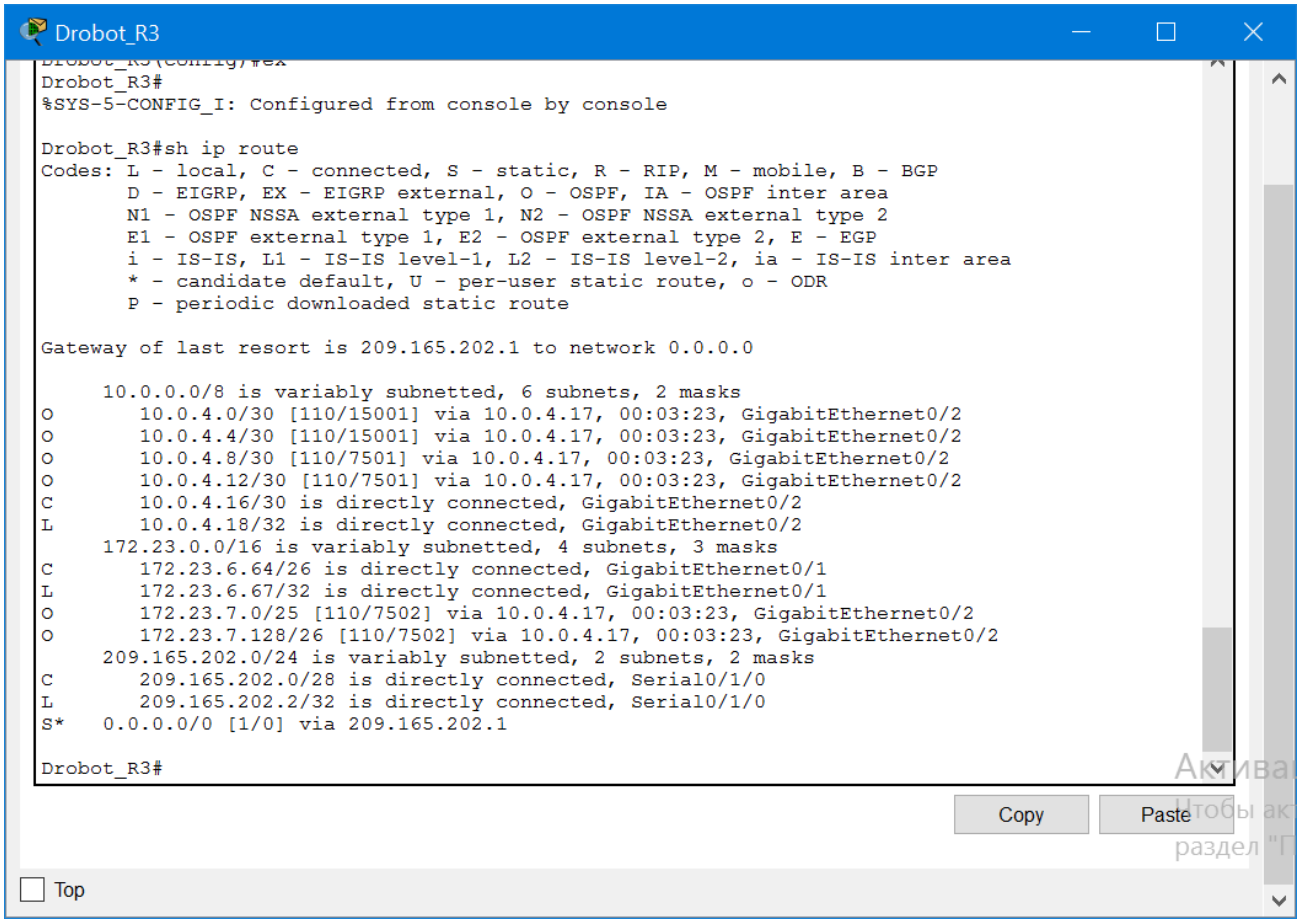
Таблиця маршрутизації на Drobot_R1



Таблиця маршрутизації на Drobot_R2



Таблиця маршрутизації на Drobot_R3



Таблиця маршрутизації на ISP