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

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

здобувача Діденко Нікіта Володимирович
(ПІБ)
академічної групи 123-21-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

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

на тему "Комп'ютерна система проєктно-технологічного будівельного інституту з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"
(назва за наказом ректора)

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

Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2025

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

"___" ____ 2025 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

здобувача Діденко Н.В. **академічної групи** 123-21-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

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

на тему "Комп'ютерна система проєктно-технологічного будівельного інституту з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"

затверджену наказом ректора НТУ «Дніпровська політехніка» від 05.05.2025 № 336-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	05.05.2025
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	12.05.2025
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	26.05.2025
Розробка компонента системи	Виконується детальна розробка компонента системи	02.06.2025

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

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії 16.06.2025

Прийнято до виконання _____ Діденко Н.В.

РЕФЕРАТ

Пояснювальна записка: 107 с., 42 рис., 8 табл., 2 дод., 15 джерел.

КОМПАНІЯ, БЕЗПЕКА, СИСТЕМА, ЛОКАЛЬНА МЕРЕЖА, КОРПОРАТИВНА МЕРЕЖА, МЕРЕЖЕВІ ЗАСОБИ

Об’єкт розробки – комп'ютерна система акціонерного товариство «проектно-технологічний інститут з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета роботи – створення комп'ютерної система для акціонерного товариство «проектно-технологічний інститут» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Здійснено розробку комп’ютерної системи, яка по структурі та функціоналу є гнучкою. Система орієнтована на застосування в комп'ютерній системі для акціонерного товариство «проектно-технологічний інститут.

Розроблена комп'ютерна система забезпечить оновлення технології та програм, автоматичний контроль працездатності, має автоматизований облік та управління для обслуговування обладнання, має значну надійність роботи, забезпечує збір статистичної інформації, здійснює її класифікацію та підготовку рекомендацій.

Комп'ютерна система для акціонерного товариство «проектно-технологічний інститут виконана відповідно до методичного завдання для кваліфікаційної робот бакалавра. Комп’ютерна системи протестована за допомогою моделі схеми у програмному застосунку Cisco Packet Tracer. Результати перевірки працездатності комп’ютерної системи акціонерного товариство «проектно-технологічний інститут представлені у вигляді таблиць та графіків описані і наводяться у пояснювальній записці та додатках.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

КС – комп’ютерна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

Ethernet – технологія передачі даних по мережі;

Wi–Fi – технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11;

ВСТУП

Тема кваліфікаційної роботи – «Комп'ютерна система акціонерного товариство «проектно-технологічний інститут з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі».

Обсяг даних, що передаються через канали зв'язку, продовжує зростати з кожним днем. Пропускна здатність на одного користувача збільшується. Мережа вимагає належного захисту інформації. Тому необхідно надавати корпоративним мережевим системам рекомендації та рішення, що відповідають потребам і вимогам користувачів і підходять для поточних завдань, щоб збільшити швидкість каналів зв'язку.

Надання інтегрованих телекомунікаційних послуг наразі ефективно впроваджується в мережах підприємств. Найважливішим з них є вимога до швидкості передачі з використанням таких технології, як HSRP, STP тощо, для оновлення мережі.

У роботі пропонується загальне рішення для побудови корпоративних мереж, що відповідає потребам користувачів та постійно зростаючим вимогам до швидкості каналів зв'язку. У роботі досліджуються сучасні проблеми розширення сфери послуг, покращення їхньої якості та збільшення їх доступності.

За результатами роботи буде складено рекомендації щодо можливості повноти вирішення поставленого завдання.

.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Умови використання комп'ютерної системи будівельного інституту

1.1.1 Будівельна галузь в Україні

1.1.1.1 Загальна інформація

Розглянемо показники будівельної галузі України до середини 2024 року, відповідно до дотримання вимог Закону України «Про офіційну статистику» щодо забезпечення статистичної конфіденційності державними статистичними органами, дані Державної служби статистики України припиняють публікуватися після середини 2024 року.

Рисунок 1.1 – Сучасна архітектура

Показники загальної експлуатаційної площі різних типів житлових будівель наведено на рис. 1.2.

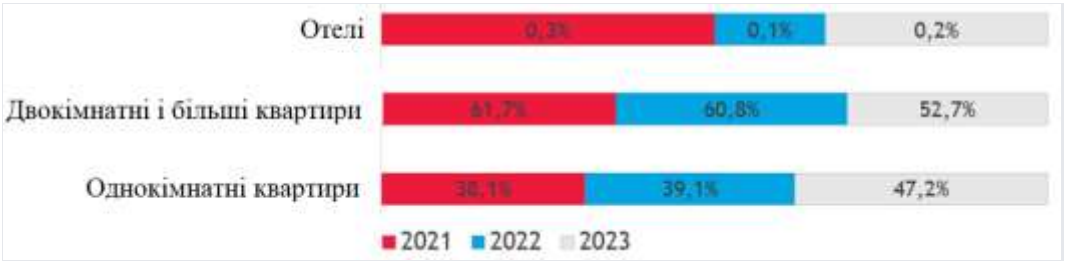


Рисунок 1.2 – Показник загальної житлової площі

2023 рік – це вже другий рік повної окупації Росією, і всі сфери економіки стикаються з новими викликами. Окрім ризиків, пов’язаних із вибухами та іншими

конфліктами, підприємства повинні адаптуватися до змін у правилах, як правових, так і регуляторних, а також до зміни настроїв споживачів щодо продуктів та послуг. Особливо минулого року на ринку нерухомості спостерігалося зростання попиту на купівлю приватного житла.

Загальні показники типів об'єктів, введених в експлуатацію, наведено на рис. 1.3.

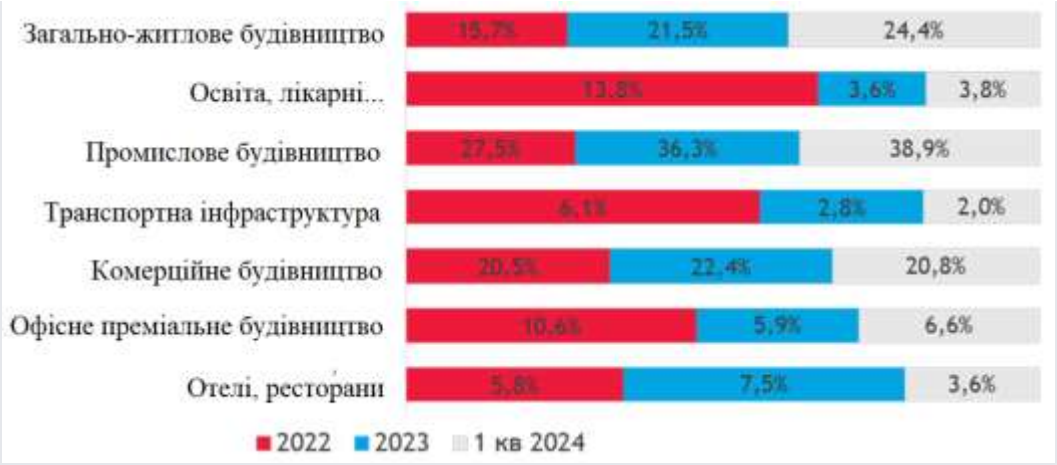


Рисунок 1.3 – Загальні структурні показники

На рис. 1.4 показано, що ціна на однокімнатну квартиру зросла в районах, віддалених від зони бойових дій. Єдиним винятком стала столиця, де середні ціни впали до найнижчого рівня з моменту припинення відключень електроенергії навесні 2023 року. Це може бути пов'язано з імміграційним процесом.

Що стосується однокімнатних квартир, то ціни в Києві впали на 3%, тоді як у Львові вони зросли на 12%. Івано-Франківськ став рекордсменом за зростанням цін, зміцнивши свою валюту на 18%.

Що стосується двокімнатних квартир: ціни впали на 18% у Вінниці, на 17% в Івано-Франківську, на 9% у Львові та на 1% у Києві.

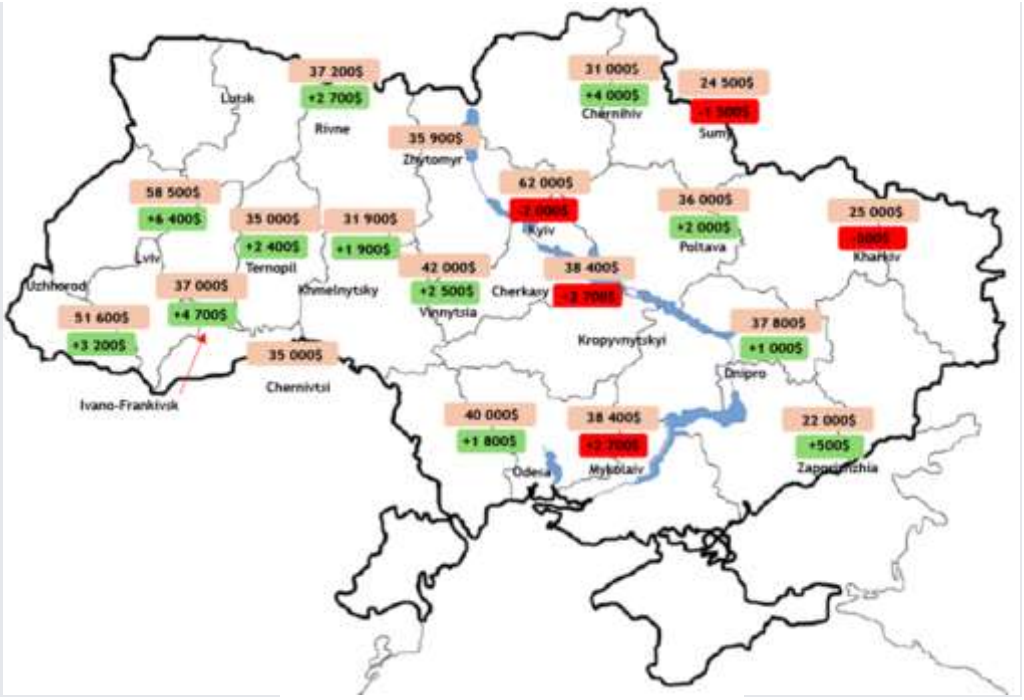


Рисунок 1.4 – Ціни на житло

У валюті ціни на трикімнатні квартири у столиці впали на 6%, у Вінниці та Івано-Франківську – на 13%, а у Львові – на 8%.

В абсолютному вираженні найпопулярнішим вибором серед українців є однокімнатна квартира, і столиця постраждала найбільше, ціни на квартири впали в середньому на 2 000 доларів. Найбільше зростання цін спостерігалося у Львові (6 400 доларів США), Івано-Франківську (4 700 доларів США) та Чернігові (4 000 доларів США), далі йде Ужгород (3 200 доларів США).

Київ та Львів традиційно були найдорожчими містами для купівлі житла, але з початком масштабної війни до списку потрапив Ужгород, де для купівлі квартири потрібно заощаджувати понад дев'ять років повної місцевої зарплати [2].

1.1.1.2 Урядові проекти стають рушійною силою попиту на ринку нерухомості

Ринок нерухомості пожвавився після того, як уряд запровадив план "Оселя". Програма сприяла відновленню продажів шляхом надання пільгових кредитів певним групам населення, а також надання житлових кредитів із річною

процентною ставкою 3% військовослужбовцям Збройних Сил України, Служби безпеки України, Головного управління розвідки Міністерства оборони України, лікарям, науковцям та вчителям. Крім того, за даними Державного агентства житлово-комунального господарства, з 2023 року уряд розширив програму житлового кредитування: відповідно до статті 10 Закону України «Про соціальний захист ветеранів війни», ветерани війни та їхні сім'ї, учасники бойових дій, особи, які стали інвалідами війни, та сім'ї загиблих ветеранів війни розподіляються по різних регіонах. Захисники України, внутрішньо переміщені особи та інші громадяни, які не мають власного житла або площа житла яких становить менше 52,5 квадратних метрів та менше 21 квадратного метра на кожного додаткового члена сім'ї.

За даними банку «Глобус», з 1 жовтня 2022 року по серпень цього року банки видали 2898 кредитів за програмою «Оселя» на загальну суму понад 4 мільярди гривень. Окрім квартир, «Оселя» також охоплює купівлю окремих будинків та дуплексів. Згідно з публічними даними, це означає, що за півтора місяці дії схеми, що охоплює приватні будинки, кількість пропозицій щодо приватного житла на платформі OLX зросла на 12%, кількість відгуків – на 38%, а середня ціна – трохи більше ніж на 1%.

Рисунок 1.4 – «Оселя» – Програма допомоги у отриманні кредитів

Щодо будинків для відпочинку, кількість оголошень зросла на 6,3%, кількість відповідей – на 37%, а середня ціна – на 0,5%. За півтора місяця з моменту запуску програми кількість будинків у списку очікування зросла трохи більше ніж на 6%, а кількість відгуків від користувачів платформи – на 37%. Тим часом середні ціни

зросли на 1,5% порівняно з кінцем січня 2024 року. Кількість оголошень про продаж часткової нерухомості зросла більш ніж на 9%, при цьому кількість відповідей зросла на 60%, а середні ціни – на 11,6%.

Перші договори на купівлю житла за програмою «Оселя» були підписані з середини березня. Наразі план активно впроваджується в різних регіонах, і деякі категорії мають можливість скористатися 0% процентною ставкою. Розвиток «Оселя» позитивно впливає на попит на житлові будинки, дуплекси та подібні об'єкти та є одним із факторів, що призводять до розвитку всього ринку нерухомості. За стабільного фінансування довіра людей до програми зростатиме, що, своєю чергою, пожвавить ринок, збільшить кількість забудовників, схвалених програмою, нових житлових проектів та створить нові робочі місця.

Водночас первинний ринок перебуває у дуже складній ситуації, попит все ще млявий, а інвестиції майже нульові. Ризики безпеки та економіки в будівельній галузі залишаються величезними. Тому немає підстав очікувати зростання в цій галузі найближчим часом.

1.1.1.3 Комерційна нерухомість

1.1.1.3.1 Офісна будівля

На тлі військових операцій та тривалої економічної рецесії ринок офісної нерухомості Києва продемонстрував високий ступінь гнучкості та адаптивності.

Загальна площа конкурентних офісних площ залишилася незмінною на рівні 2,22 мільйона квадратних футів. метрів з початку цього року. Середній рівень вакансій залишався стабільним на рівні 25% (зниження на 1% з початку року). Фактичні ціни на оренду залишалися стабільними, в середньому становлячи 20 доларів за квадратний метр. м/місяць (без ПДВ та експлуатаційних витрат).

Незважаючи на триваючі військові операції та тривалу економічну рецесію, ринок офісної нерухомості Києва продемонстрував надзвичайну стабільність та стійкість у 2023 році.

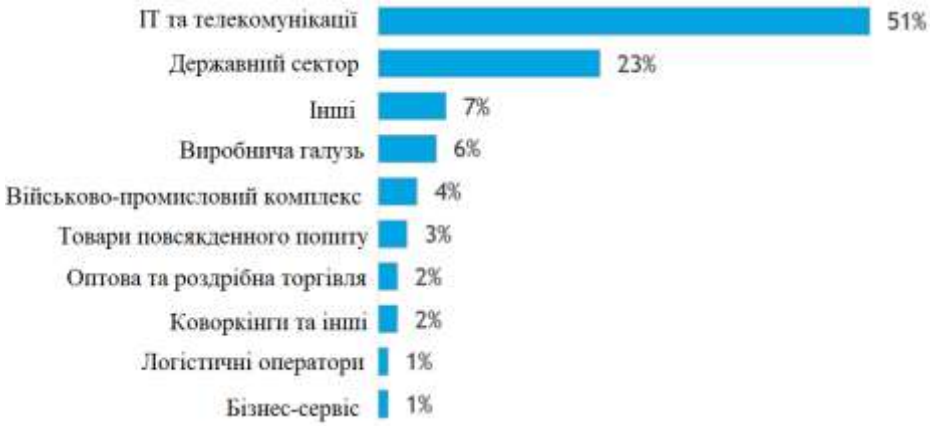


Рисунок 1.5 – Офісна будівля

Більшість компаній припинили скорочення штатів та активно шукають способи оптимізації витрат на нерухомість, ремонтують та оптимізують офісні приміщення шляхом перегляду договорів оренди або переїзду.

Попит орендарів демонстрував ознаки відновлення, а загальний річний дохід від оренди сягнув приблизно 91 000 квадратних метрів. метрів, що в чотири рази більше, ніж у 2022 році, але все ще на 32% нижче довоєнного рівня у 2021 році. На структуру діяльності вплинули переїзди (55%) та перегляд існуючих контрактів (17%), тоді як розширення офісних площ було відносно рідкісним явищем (6%). Як і минулого року, у 2023 році спостерігається явний дефіцит великих офісних приміщень, причому площа найбільших офісних приміщень коливається від 1 500 до 3 000 м^2.

Війна змінює повсякденне життя та привносить нові тенденції на ринок комерційної нерухомості. Деякі компанії залишаються у своїх початкових офісах і відмовляються переїжджати в інші місця, оскільки вартість переїзду є занадто високою, і компанії часто утримують свої офіси, сплачуючи орендну плату та

пов'язані з нею витрати, хоча фактичний рівень заповнюваності офісів співробітниками залишається низьким і коливається від 15% до 50%.

Попит у різних бізнес-секторах показує, що сектор ІКТ продовжує домінувати (51%). Однак темпи зростання цієї галузі, яка колись була основним рушієм попиту та розвитку торговельних центрів, сповільнилися через скорочення фізичної присутності офісних працівників. Тим часом ринок ще не бачить подібного попиту на нові офіси з боку традиційних галузей, таких як фармацевтика, бізнес та фінансові послуги чи сільське господарство. Державний сектор, на який припадає 23% загального попиту, залишається активним і, ймовірно, продовжуватиме робити це до 2024 року. Потенційне зростання попиту також може відбуватися за рахунок компаній військово-промислового комплексу, хоча їхня поточна частка в структурі попиту є незначною.

Середній рівень безробіття залишається відносно стабільним у 2023 році, знизившись лише на 1% до 25% до кінця року. Вигідні умови оренди дозволяють компаніям переїжджати з офісів нижчої якості до високоякісних приміщень класу В та класу А з нижчою орендною платою. Рівень безробіття для квартир класу В становив 27%, що вище, ніж 24,7% для квартир класу А, особливо в будинках нижчої якості. Велика кількість вільних земель зосереджена в новозбудованих будівлях, які ще не досягли високого рівня заповнюваності, та в низькоякісних будівлях, розташованих переважно за межами центрального ділового району.

Орендна плата впала на 5% з початку року, стабілізуючись на рівні 20 доларів за квадратний фут на місяць. Угоди на такому рівні оренди все ще рідкість. Орендна плата класу А знизилася в середньому на 7 відсотків, з 18 до 24 доларів за квадратний метр. рис. щомісяця, тоді як ціни на нерухомість класу В значно знизилися (-11%), а ціни коливалися від 8 до 16 м^2/міс.

1.1.1.3.2 Складські приміщення

Ринок складської нерухомості залишався стабільним у першому кварталі 2024 року, без суттєвих змін. Орендна діяльність залишається обмеженою, але деякі великі орендарі досліджують ринок з метою розширення.

Оптовий та роздрібний сектори продовжували домінувати в орендній діяльності, тоді як сектори охорони здоров'я та фармацевтики дещо зросли. Загальна площа оренди зменшилася на 21% до приблизно 23 тис. м^2 протягом кварталу порівняно з минулим роком.

У першому кварталі 2024 року на ринок не з'явилося жодної нової нерухомості. Рівень безробіття залишався на рівні 1,8% на кінець першого кварталу 2024 року через брак нової пропозиції та дефіцит існуючих площ.

Дохід від оренди в доларах США зріс до 4,9 долара США за квадратний метр. преміального складського простору на місяць (без ПДВ та експлуатаційних витрат).

Бізнес підвищив свої очікування щодо ділової активності протягом наступних 12 місяців. Незважаючи на ризики безпеки та логістичні труднощі, включаючи проблеми з перетином кордону, респонденти прогнозують помірне зростання виробництва товарів і послуг і позитивно оцінюють розвиток свого бізнесу. Інфляційні очікування продовжували покращуватися, тоді як монетарні очікування дещо погіршилися.

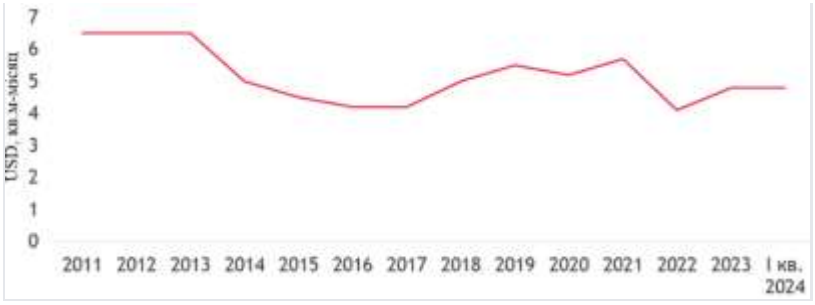


Рисунок 1.6 – Результат бізнесу забудовників

У другому кварталі 2024 року індекс ділової довіри в будівельній галузі знизився на 1,1 пункту до 40,9% порівняно з першим кварталом 2024 року.

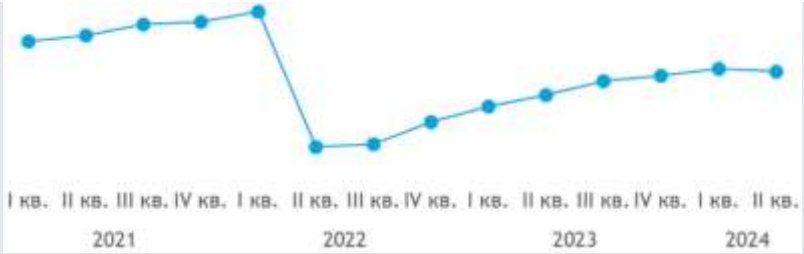


Рисунок 1.7 – Індекс довіри в будівельній галузі

За даними Державної служби статистики України, очікується, що дефіцит поточного надходження замовлень зросте на 3 процентні пункти до -53%. 54% опитаних компаній вважають, що поточний обсяг замовлень є недостатнім, а 45% опитаних компаній вважають, що обсяг замовлень у поточному сезоні є нормальним.

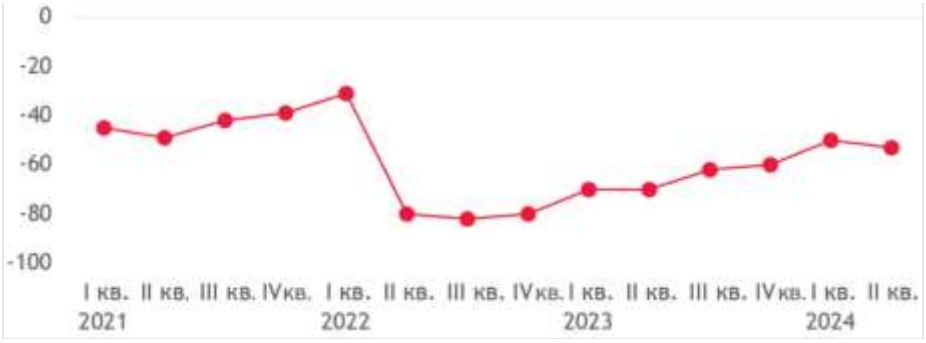


Рисунок 1.8 – Очікувана поточна кількість замовлення

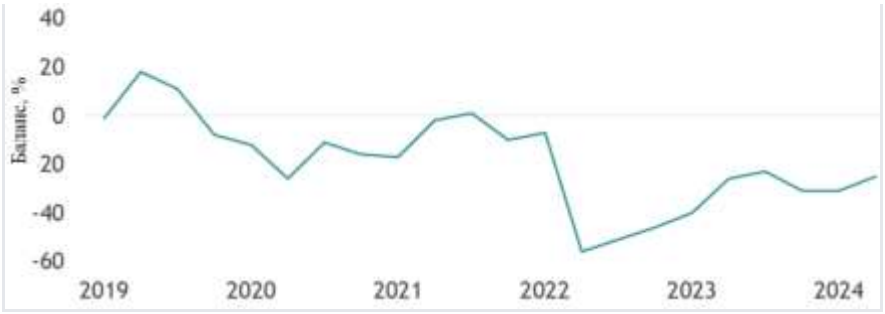


Рисунок 1.9 – Очікувані зміни кількості працівників у будівельних компаніях

Серед основних факторів, що негативно впливають на кількість працівників на будівельних майданчиках, респонденти одноголосно вказали на мобілізацію. Прогнозована зміна кількості працівників з квітня по червень 2024 року становить -31%.

Майже у всіх професійних сферах відчувається нестача робочих рук. Сьогодні спільний досвід робітників, електриків, сантехніків, фахівців з фасадів та професійних водіїв будівельної техніки є безцінним.

В Україні триває загальна мобілізація, будівельників часто призивають на військову службу.

Приватні будівельні компанії можуть використовувати своїх працівників лише для відбудови будинків, зруйнованих під час війни, або будівництва критично важливої інфраструктури.

Тривалий пошук працівників уповільнить будівельну активність, що окрім підвищення заробітної плати також вплине на ціни на будівництво. Крім того, ціни на будівельні матеріали продовжують зростати. У деяких категоріях витрати зросли на 30…200%. Існують прогнози, що виробники можуть відкласти запуск заводів цього року, оскільки нестача робочої сили стає серйознішою. Отже, ціна за квадратний метр значно зросте.

1.1.1.3.3 Майбутні перспективи будівельної галузі України

У 2024 році українська будівельна галузь зосередиться на реконструкції та модернізації інфраструктури, а також розвитку житлових та промислових будівель. Незважаючи на економічні труднощі, галузь має величезний потенціал для зростання, особливо за підтримки урядів та міжнародних партнерів. Інновації та ефективне управління ресурсами будуть ключем до успішного розвитку будівельної галузі.

Будівельна галузь зіткнеться з двома основними проблемами: нестачею кваліфікованої робочої сили та цінами на будівельні матеріали, які залишаються високими через світову інфляцію та проблеми з постачанням.

Усі вищезазначені фактори можуть вплинути на загальну вартість будівельного проєкту, що призведе до зростання вартості нерухомості та затримок у введенні в експлуатацію.

Будь ласка, прочитайте нижче, щоб дізнатися більше, або зв’яжіться з нами, якщо у вас виникнуть будь-які запитання. Ми будемо раді надати вам необхідну консультацію.

1.1.2 будівельного інституту

Інституту є надійним партнером та професійним експортером у сфері досліджень, геодезичних досліджень та випробувань у сфері будівництва.

Співробітники компанії своєю роботою ефективно продовжують найкращі традиції піввікової історії організації. Вони дотримуються своїх обіцянок, поважають своїх партнерів та звертають увагу на їхні потреби.

Наразі інститут проводить набір сертифікованих експертів, а також інших вузькоспеціалізованих спеціалістів, готових виконувати термінові роботи в галузі проектування та обстеження будівель та конструкцій.

Компанія готує проектну документацію та попередню кошторисну документацію на будівництво, реконструкцію, ремонт та модернізацію об'єктів (житлових, громадських та промислових будівель, включаючи електростанції тощо).

Компанія готує проектну та попередню розрахункову документацію для будівництва, реконструкції, модернізації та ремонту енергетичних об'єктів: ліній електропередачі 0,4 кВ і вище, підстанцій 6…10 кВ і вище, а також здійснює авторський нагляд за виконанням будівельно-монтажних робіт.

Компанія виконує інженерно-геодезичні роботи (топографо-геодезичні роботи на етапі проектування, геодезичне забезпечення точності геометричних параметрів конструкцій).

Компанія проводить технічні огляди електроустановок, будівель та споруд.

Проектування виконується поетапно. Вирішуючи нові завдання, експерти завжди прагнуть знайти найкращі технічні рішення, враховуючи тенденції сучасного технологічного ринку та спираючись на можливості замовника. Фахівці компанії володіють усіма необхідними управлінськими та технічними знаннями та досвідом.

Головний офіс компанії знаходиться за адресою: вулиця Михайла Омеляновича-Павленка, 4/6, Київ, Україна, 01010.

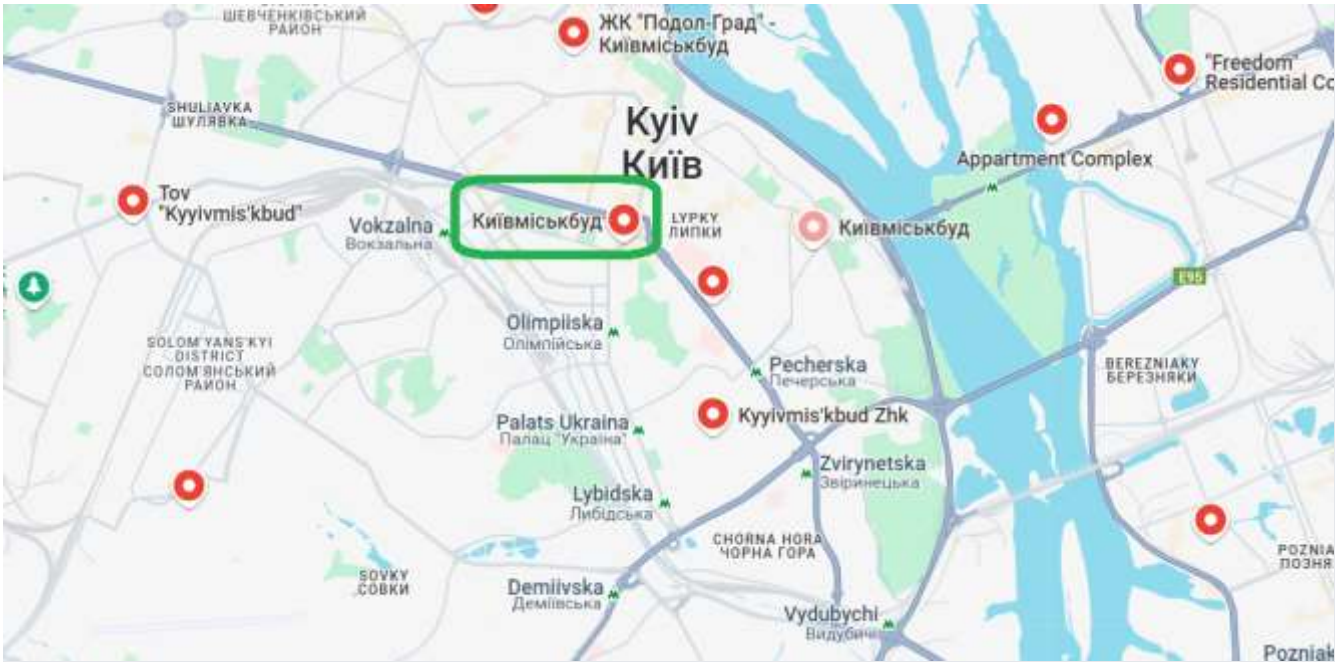


Рисунок 1.10 – Географічне розташування будівельного інституту

Штаб-квартира розташована в історичному центрі Києва. На восьми поверхах розміщуються інженерна команда, адміністративний та конструкторський відділи. Представницькі функції тісно пов'язані з першим поверхом. Серед них виставки, лекції та виставка учасників спільного. Високі стелі можуть створити приголомшливий вхід. Будівлю було збудовано після війни, а її інтер'єр оформлений у футуристичному стилі. Кварцова плитка широко використовується в оздобленні інтер'єрів, покриваючи площу 1 500 м^2. Систему освітлення було ретельно розроблено, а проєкт поєднує технологічні інновації та креативність.

Рисунок 1.11 – Офіс будівельного інституту

1.2 Технічні та математичні методи інформаційного забезпечення

1.2.1 Інформаційні та комп'ютерні системи

Комп'ютерна система підприємства повинна базуватися на методі роботи, а кілька невеликих мереж повинні бути об'єднані в одну велику мережу в будівельного інституту.

Основні характеристики корпоративних обчислювальних систем полягають у наступному. Цей тип мережі з'єднує кілька мереж різних відділів компанії в межах однієї будівлі або на площі в кілька квадратних кілометрів. Також глобальні зв'язки не використовуються в бізнес-мережах. Ці мережеві послуги включають з'єднання між мережами відділів, доступ до баз даних усієї компанії, а також доступ до швидкісних модемів і швидкісних принтерів. Це дозволяє співробітникам компанії отримувати доступ до певних файлів та ресурсів веб-сайту з інших відділів.

На цьому рівні комп'ютерної мережі компанії виникли проблеми з інтеграцією різного апаратного та програмного забезпечення. Типи комп'ютерів, мережевих операційних систем та мережевого обладнання можуть відрізнятися залежно від відділу. Це створює проблеми для управління мережею організації. У цьому випадку адміністраторам потрібні кращі та просунуті інструменти керування мережею.

Корпоративну мережу також називають мережею корпоративного рівня – мережею корпоративного рівня, яка з’єднує кілька комп’ютерів у компанії. Кількість

користувачів і комп'ютерів може обчислюватися тисячами, кількість серверів – сотнями, а відстані між мережами в різних регіонах можуть вимагати використання глобального з'єднання. Підключати віддалені локальні мережі та персональні комп'ютери до корпоративної мережі за допомогою різноманітних телекомунікаційних засобів, включаючи телефонні канали, радіоканали та супутниковий зв'язок. Корпоративні мережі можна розглядати як «острови локальної мережі», що плавають у телекомунікаційному середовищі.

Корпоративні мережі з'єднують усі комп'ютери в різних компаніях. Корпоративні мережі включають:

– використання засобів зв'язку для глобального зв'язку, включаючи радіоканали, телефонні канали та космічний зв'язок, інтегрований у мережу магазину.

– різнорідні високотехнологічні комп'ютери, різноманітне телекомунікаційне обладнання, операційні системи та аксесуари;

– масштабованість – багато користувацьких комп'ютерів, сотні серверів, великі обсяги даних, що зберігаються та передаються, різноманітні та значні додаткові витрати.

Головною особливістю корпоративних мереж є швидкий обмін інформацією. Але це не єдина відмінність, наприклад, під час передачі даних менше помилок. Для цього мережа підприємства повинна використовувати високоякісну комунікаційну мережу.

Передача даних під час роботи є головною особливістю системи. Якщо механізм керування обміном даними, що використовується в мережі, неефективний, комп'ютерам, можливо, доведеться годинами чекати в черзі, щоб відправити дані, і навіть якщо вони можуть надсилати дані з дуже високою швидкістю або без помилок, час очікування підключення до мережевої системи може не відповідати потребам користувачів мережі.

Будь-який механізм контролю обміну даними може гарантувати повноцінну та якісну роботу лише за умови, що заздалегідь відомо, скільки комп'ютерів буде

підключено до мережі. Усі механізми дають збій, коли кількість користувачів, підключених до мережі, перевищує очікування. Крім того, мережа стосується системи великої кількості комп'ютерів, з'єднаних між собою, тоді як два комп'ютери, з'єднані між собою через звичайні порти, не можна назвати мережею [1].

1.3 Огляд існуючих інженерних рішень

1.3.1 Проблеми комп'ютерних систем

Під час використання комп'ютерних систем виникають проблеми через взаємовигідну організацію частин розподіленої системи.

Перш за все, ці проблеми стосуються програмного забезпечення. Зокрема: у програмах та операційних системах. Розподілене системне програмування відрізняється від централізованого системного програмування. Координація спільної роботи компонентів різних конструкцій транспортних засобів для управління навантаженням мережі є складною. Забезпечення сумісності програмного забезпечення, встановленого на вузлах мережі, є найскладнішим питанням.

По-друге, існує багато проблем із передачею інформації через канали зв'язку між комп'ютерами. Головне питання тут полягає в забезпеченні надійності, запобіганні втраті переданої інформації та забезпеченні надійної роботи обміну даними між пов'язаними терміналами.

По-третє, проблеми безпеки комп'ютерних мереж вирішити складніше, ніж проблеми безпеки окремих машин.

Водночас можна знайти як багато переваг, так і недоліків. Однак, незаперечний факт широкого використання Інтернету створює серйозну проблему для його ефективного використання. Сьогодні важко знайти організацію, яка не має мережі персональних комп'ютерів. Це пояснюється тим, що мережі з багатьма робочими станціями та десятками серверів стали поширеним явищем. Деякі великі

організації створюють власні глобальні мережі, що з'єднують філії на відстані тисяч кілометрів. У деяких випадках мережа створюється з певної причини.

Бізнес-системи забезпечують передачу даних між різними програмами, що використовуються компанією. У зв'язку з цим ми розглянемо різні підходи до створення такої системи з метою наповнення корпоративних мереж автентичним контентом. Водночас мережа має бути максимально глобальною, тобто вона має забезпечувати інтеграцію існуючих та майбутніх програм з найнижчими можливими витратами та обмеженнями.

Корпоративна система часто є географічно розподіленою, тобто вона поєднує офіси, відділи та інші структури, розташовані далеко один від одного. Вузли корпоративної мережі часто розташовані в різних містах, а іноді навіть у різних країнах. Принципи, що лежать в основі такої системи, дуже відрізняються від принципів створення локальної мережі, що охоплює кілька будівель. Основна відмінність полягає в тому, що приватні мережі використовують низькошвидкісні місцеві орендовані лінії. Якщо основною статтею витрат на створення локальної мережі є придбання обладнання та кабелів, то в географічно розподіленій мережі найважливішим елементом витрат є орендна плата за користування каналом, яка швидко зростає зі покращенням якості та швидкості передачі даних. Це обмежувальний принцип, і під час проектування корпоративної мережі слід докласти всіх зусиль, щоб мінімізувати обсяг переданих даних.

Додатки – це системне програмне забезпечення, таке як бази даних, системи електронної пошти, обчислювальні ресурси, файлові служби тощо. Головним завданням корпоративної мережі є взаємодія системних програм, розташованих у різних місцях, та доступність для віддалених користувачів.

Перше питання, яке слід врахувати при створенні корпоративної мережі, це організація каналів зв'язку. Якщо в межах міста ви можете розраховувати на оренду приватної мережі (включаючи високошвидкісні мережі), то в міру переїзду у

віддалені географічні райони вартість оренди каналів стає непомірно високою, а їхня якість та надійність зазвичай не високі.

Природним способом вирішення цієї проблеми є використання сучасної глобальної мережі. У цих випадках достатньо забезпечити канал від офісу до найближчого вузла мережі. Це завдання виконує мережа вузлів передачі інформації по всьому світу.

Проектування корпоративної мережі включає такі кроки:

1. Створіть фізичну модель мережі підприємства. Модель фізичної бізнес-мережі – це опис апаратних та програмних засобів і методів зв'язку.

2. Створіть технологічну модель мережевої системи підприємства. Технологічна модель — це набір технічних інструментів, необхідних для реалізації проекту в корпоративній мережі. На цьому етапі визначаються технічні параметри мережі, такі як набори функцій апаратного та програмного забезпечення пристроїв. Отже, відповідно до технічних параметрів, отриманих у технічній моделі, вибирається технічна модель мережі, а також обрані протоколи та мережеве обладнання. Результатом цього кроку є виконання мережі з використанням графа структури, параметрів та алгоритмів.

3. Розробіть бізнес-модель для компанії. Модель бізнесу та корпоративної ефективності – цей продукт управління та підтримки описує бізнес-процеси, інформаційні потоки між етапами та ієрархічні потоки. Він показує структурну функціональність виробничих систем, інформаційних об'єктів та середовища, яке їх пов'язує.

4. Оптимізація та моделювання організаційних мереж. Під час цього етапу виконується моделювання для оптимізації та оцінки характеристик продуктивності мережі підприємства.

5. Тестування бізнес-мережі. Протягом цього періоду мають бути проведені необхідні випробування, зазначені в договорі.

6. Ремонт та монтаж організаційних мереж. На цьому етапі працівники проходять навчання з налаштування, використання, обслуговування та встановлення обладнання.

7. Аналіз вимог. На цьому етапі цілі компанії визначені.

8. Організувати використання та обслуговування мережі. Заключна стадія не має певної тривалості та являє собою безперервний рух. [8]

1.3.2 Технології в корпоративних мережах

Надання інтегрованих телекомунікаційних послуг наразі ефективно впроваджується в мережах підприємств. Однак доступ до таких послуг створює додаткові труднощі. Найважливішим з них є вимога до швидкості передачі. Ці вимоги можуть бути виконані за допомогою оптичних мереж.

Давайте розглянемо технології, що використовуються в корпоративних мережах:

1. Цифрова абонентська лінія (DSL) – це високошвидкісний інтернет-сервіс, який конкурує з кабельним інтернетом і забезпечує доступ до інтернету місцевим користувачам. Це типова мідна телефонна лінія.

Інтернетом можна користуватися, але dial-up інтернет швидший ніж у інституті. Також, на відміну від комутованого з'єднання, Digital Subscriber Line – високошвидкісний інтернет-сервіс (DSL) не підключений до телефонної мережі. Спільне використання телефонного з’єднання дозволяє користувачам одночасно переглядати Інтернет та здійснювати телефонні дзвінки.

2. Волоконно-оптична мережа зв'язку є типом зв'язку. У цьому випадку інформація передається через оптичне середовище, яке називається «оптичне волокно». Оптичне волокно наразі вважається найсучаснішим фізичним середовищем для передачі інформації та найперспективнішим середовищем для передачі великих потоків даних на великі відстані.

3. General Packet Radio Service (GPRS) – це технологія для надсилання пакетів даних через мережі мобільного зв'язку. Основою послуги є GPRS-телефон або GPRS-модем та мережа Інтернет із постійним підключенням. Оскільки підтримуються всі протоколи, користувачі мобільних телефонів можуть використовувати будь-який Specific Groupe Mobile (GSM) термінал, що підтримує GPRS, для доступу до мережі компанії.

4. Інтернет-протокол (IP) – це протокол мережевого рівня, який стосується протоколу, що організовує з’єднання на основі комутації каналів. Його основна функція — передача даних, зокрема доступ до Інтернету. Принцип організації IP-з'єднань полягає в наступному: інформація від джерела розділяється на невеликі сегменти або блоки, які не можуть мати однакову довжину.

5. Супутникові рішення можуть ефективно організовувати мережі каналів.

1.4 Розробка організаційної структури будівельного інституту.

1.4.1 Ієрархія будівельної компанії

Організаційна структура є важливим компонентом будь-якої будівельної компанії, що забезпечує візуальне уявлення про ієрархію та визначає відповідальність за прийняття рішень всередині компанії. Ефективна організаційна структура чітко розподіляє обов'язки, сприяє прийняттю розумних рішень та усуває вузькі місця. У цій статті описано поширені ролі в будівельній компанії та їх типове розміщення на організаційній схемі, а також різні способи організації команд для ефективної роботи в великих масштабах.

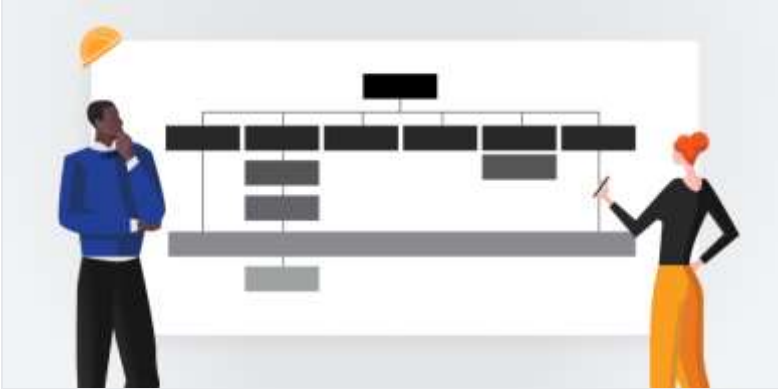


Рисунок 1.11 – Проектування організаційної структури

Важливість організаційної схеми:

1. Запобігайте перекриттю. Організаційна схема запобігає дублюванню та плутанині, визначаючи конкретні ролі та обов'язки. Кожне робоче місце має чітко визначене робоче навантаження, щоб мінімізувати ризик перевтоми.

2. Сприяти належній децентралізації. Організаційна схема допомагає правильно розподіляти завдання та підтримувати ефективність. Правильне делегування допомагає уникнути вузьких місць.

3. Навчання допоміжним інструментам. Новим співробітникам може бути важко зрозуміти організаційну структуру компанії. Добре розроблена організаційна схема може чітко відобразити ієрархію компанії та допомогти новим співробітникам швидко зрозуміти, хто за що відповідає та яке їхнє місце в організації.

4. Ієрархія будівельних компаній. Хоча кожна будівельна компанія унікальна за місцем розташування, типами проектів та робочою силою, добре спроектовані компанії зазвичай дотримуються спільної організаційної структури. Незалежно від розміру компанії, обов'язки на різних рівнях однакові. Великі компанії можуть розподіляти ці обов'язки між кількома особами, тоді як менші компанії можуть поєднувати кілька обов'язків в одну роль. Будівельні компанії мають різні рівні відповідальності. У міру просування вниз по організаційній схемі ролі змінюються від стратегічних та управлінських до тих, що пов'язані з виконанням завдань. На

нижчих рівнях може бути кілька співробітників, кожен з яких відповідає за певну частину загальної роботи.

5. Нерухомість. У великих будівельних компаніях рада директорів зазвичай визначає загальний напрямок діяльності компанії та очолює її головний виконавчий директор (CEO). У дрібних підрядників може бути одна особа, яка виконує обов'язки менеджера або власника.

6. Виконавчий директор. Виконавча команда тісно співпрацює з генеральним директором для розробки та комунікації стратегії компанії. Великі будівельні компанії часто мають різні команди керівників, кожен член яких очолює певний відділ. Серед поширених посад є посади віце-президента або старшого керівника, такі як «віце-президент з операційної діяльності» або «фінансовий директор» (CFO).

7. Директори. У великих будівельних компаніях багато менеджерів працюють під керівництвом керівника. Наприклад, може бути менеджер з маркетингу, менеджер з інженерії, менеджер з продажу та менеджер з операційної діяльності. Як правило, менеджери з інженерії та операцій можуть звітувати перед головним операційним директором (COO), тоді як менеджери з продажу та маркетингу можуть звітувати перед директором з маркетингу (CMO).

8. Директори. Нижче рівня менеджера знаходиться рівень управління. Менеджери керують своїми командами та виконують такі обов'язки, як фінансовий менеджер, бухгалтер, керівник будівництва, керівник об'єкта, керівник проекту та менеджер з маркетингу. У великих компаніях може бути кілька менеджерів у різних відділах та проектах.

9. Підтримка. Допоміжний персонал виконує важливі завдання та допомагає менеджерам і керівникам у різних відділах. Він звітує перед менеджером і обіймає такі посади, як помічник менеджера, офіс-менеджер, менеджер з обслуговування

клієнтів та помічник керівника проектів. У великих компаніях ці посади можуть включати кількох людей для ефективного розподілу обов'язків.

10. Початковий рівень. Початкові посади, особливо у великих будівельних фірмах, – чудове місце для початку. Цей рівень зазвичай включає адміністративних помічників, стажерів та спеціалістів. Деякі помічники керівників проектів також можуть починати з цього рівня.

1.4.2 Система управління радою директорів будівельного інституту

Матрична система управління, розроблена для будівельного інституту, включає елементи як горизонтальної, так і вертикальної систем управління.

Як і в лінійній моделі, існує також вертикальна структура: створення відділів (наприклад, виробництва, закупівель, маркетингу тощо). Різні проекти можна об'єднати в одну програму. Система відіграє дуже ефективну та результативну роль у досягненні складних технологічних досягнень та наукового виробництва.

Рисунок 1.12 - Організаційна схема управління будівельного інституту

Такий стиль керівництва забезпечує високий ступінь гнучкості, адаптивності та ефективності у використанні людей та ресурсів. Однак, він також має недоліки, такі як складна архітектура та нестабільність. Важливо зазначити, що ці типи стилів

керівництва часто помилково описуються як ефективні або неефективні. Ієрархічна структура управління повинна чітко визначати обов'язки. Важливо пам'ятати, що лише після оцінки зовнішнього та внутрішнього стану вашої компанії можна визначити тип системи, яку потрібно побудувати.

1.5 Постановка завдання

Кваліфікаційна робота виконуються для розробки комп'ютерні системи будівельного інституту. У цьому випадку слід звернути особливу увагу на ретельне встановлення та налаштування для безпечної роботи корпоративної мережі.

В рамках кваліфікаційної оцінки були проаналізовані телекомунікаційні та технічні характеристики будівельного інституту. Оцінені характеристики існуючих мережевих елементів, які будуть додані до корпоративної мережі.

Для розробки комп'ютерної системи будівельного інституту необхідно підібрати мережеве обладнання відповідно до кількості користувачів у будівлі. Необхідно проаналізувати та вибрати найкращий метод передачі сигналу та обладнання, яке буде використовуватися.

Проектування мережі базується на валідації Cisco Packet Tracer, оскільки вибрані продукти повинні бути сумісними з продуктами Cisco.

Якщо мережа має зростати в майбутньому, її архітектура має бути простою та економічно ефективною.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ БУДІВЕЛЬНОГО ІНСТИТУТУ

2.1 Технічні вимоги до комп'ютерної системи будівельного інституту

Метою цього розділу є опис основних техніко-технологічних принципів розробки комп'ютерної системи будівельного інституту, опису системи, категорій та концепцій, що використовуються в IT-інфраструктурі будівельного інституту, продемонструвати економічно ефективні принципи створення, управління та динамічної трансформації IT-інфраструктури.

Розробити вимоги та технології для побудови, розвитку та інтеграції IT-інфраструктури, визначити формальні механізми технічної взаємодії між різними рівнями IT-інфраструктури та рівні продуктивності, необхідні для ефективної роботи комп'ютерних систем.

Це забезпечує цілісність подібних елементів IT-інфраструктури на різних рівнях.

2.1.1 Загальні вимоги до комп'ютерної системи

2.1.1.1 Вимоги до структури та роботи комп'ютерної системи

Рекомендується надавати пріоритет сучасним, багаторівневим, сервісно-орієнтованим IT-рішенням з архітектурою.

2.1.1.1.1 Сервісно-орієнтована архітектура

Найперспективнішою архітектурою для створення додатків сьогодні є сервісно-орієнтована архітектура (SOA). Головною метою SOA є сприяння інтеграції застосунків - як нових програмних рішень, так і систем попереднього покоління. Архітектура SOA не залежить від мови програмування, платформи чи специфікацій протоколу, на яких базуються сервіси, а також від того, де і як вони розгортаються. На практиці, архітектура SOA вимагає не лише сервісів, але й

засобів для виявлення та підключення цих сервісів, а також кількох компонентів, таких як сервери додатків, проміжне програмне забезпечення, репозиторії та навіть спеціалізовані централізовані пакети управління SOA.

2.1.1.1.2 Багаторівнева клієнт-серверна архітектура

Термін «клієнт-сервер» стосується архітектури комп'ютера або мережі, в якій завдання або мережеві робочі навантаження розподіляються між постачальниками послуг, відомими як сервери, та одержувачами послуг, відомими як клієнти. Дані зазвичай обмінюються між клієнтом і сервером через комп'ютерну мережу та можуть використовувати різні фізичні пристрої або програмне забезпечення.

Наразі більшість мікропроцесорів розроблені з трирівневою архітектурою "клієнт-сервер", яка представляє інформаційну систему як комбінацію трьох компонентів: сервера бази даних, сервера додатків, відповідального за виконання логіки програми, та клієнтського додатку або клієнтського інтерфейсу ("тонкий клієнт"). Основними перевагами розділення логіки програми на окремі компоненти є повторне використання коду, легка заміна центральних компонентів, покращена продуктивність використовуваного сервера бази даних, підвищена масштабованість усієї системи та незалежність системи від фізичного розташування бази даних. Крім того, системи, побудовані з трирівневою архітектурою, є простішими та дешевшими, оскільки всі зміни конфігурації та налаштування здійснюються централізовано.

Елементи трирівневої архітектури:

- Рівень представлення (виконує функції введення та відображення даних); Прикладний рівень (реалізує загальні сервіси та функції, пов'язані з конкретними предметними областями);

- Рівень доступу до інформаційних ресурсів (виконує основні завдання зберігання та управління інформацією та обчислювальними ресурсами).

2.1.1.1.4 Модель SaaS

Програмне забезпечення як послуга (SaaS) – це модель споживання програмного забезпечення, в якій постачальник самостійно розробляє та керує веб-додатком і дозволяє користувачам отримувати доступ до програмного забезпечення через мережу. Головна перевага моделі SaaS для користувачів полягає в тому, що їм не потрібно нести витрати, пов'язані з встановленням, оновленням та обслуговуванням апаратного та програмного забезпечення, яке на ній працює. Використання SaaS є кращим варіантом, оскільки це дешевше та простіше, ніж внутрішні джерела даних.

2.1.2 Вимоги до мультисервісних мереж

2.1.2.1 Вимоги до розподілених мультисервісних мереж

У цьому розділі розглядаються технічні вимоги до розподілених мультисервісних мереж. Описує архітектуру, протоколи та вимоги до обладнання.

2.1.2.2 Загальні вимоги

Ключові стратегічні наслідки та підходи до організації розподілених багато-сервісних мереж підприємства: шлях до архітектури мережі наступного покоління (NGN).

Телефонія, аудіо-конференції, відеоконференції та передача даних повинні базуватися на єдиній конвергентній мультисервісній мережі, яка може надавати ці послуги, забезпечуючи при цьому необхідний та належний рівень якості обслуговування.

Мережа базується на таких принципах:

- розподілена корпоративна архітектура, що забезпечує QoS.
- висока доступність та надійність мережі;

- продуктивність, керованість та масштабованість мережі;

- проектування мультисервісних мереж повинно враховувати інформаційну безпеку.

Весь трафік має належати до таких категорій пріоритету послуг:

- трафік у режимі реального часу (телефон, голос та відео)

- трафік даних користувача;

- циркуляція технологій.

Якщо технічний пристрій вимагає найвищого рівня обслуговування, його переміщення повинно мати найвищий пріоритет. Далі слід дослідити живий трафік, а потім трафік користувацьких додатків. Крім того, пропускна здатність мережі та активні мережеві пристрої повинні завжди забезпечувати якість трафіку в режимі реального часу.

У надзвичайній ситуації мережеві ресурси слід розподілити на технічний трафік, частину трафіку реального часу та трафік користувачів, щоб забезпечити безперебійну роботу важливого технічного обладнання та його обслуговуючого персоналу. Ці правила мають бути впроваджені в налаштуваннях пристрою та автоматично виконуватися в надзвичайних ситуаціях.

2.1.2.3 Вимоги до архітектури мережі

Архітектура мультисервісної мережі повинна відповідати таким принципам:

Будівництво велося за поетапною моделлю:

- резервування пристроїв та каналів;

- сервіс VLAN.

Архітектурно вона поділена на зони. Мережа повинна забезпечувати продуктивність, необхідну для вирішення проблеми. Мережа повинна забезпечувати QoS для різних класів трафіку.

Мультисервісна мережа центру обробки даних повинна бути спроектована на основі трирівневої моделі комутації:

Рівень доступу - OSI рівні 3…4 Інтелектуальний шлюз OSI рівня 2 (забезпечує безпеку мережі, QoS тощо).

Рівень розподілу – поширюється на рівні 3 та 4 моделі OSI.

Основний рівень – комутатори рівня OSI 3-4.

Дозволяє передавати функції розподільних комутаторів базовим комутаторам, коли виділені розподільні комутатори не можуть використовуватися в кожній частині мережі через деградацію мережевої інфраструктури, зниження надійності або інші причини.

Обрана архітектура мережі повинна дозволяти масштабування мережі шляхом додавання нових блоків, забезпечувати високу надійність роботи мережі та вимагати мінімальних зусиль та усунення несправностей. Інтелектуальні сервіси OSI рівня 3, включаючи протоколи маршрутизації, повинні забезпечувати балансування навантаження та швидку конвергенцію між рівнями/всередині них, а також зменшувати обсяг проблем, спричинених різними проблемами, пов'язаними з відмовою обладнання або помилками конфігурації.

Для проектування три-рівневої конструкції слід дотримуватися таких загальних правил:

- проблеми з обладнанням та лініями зв'язку нижчого рівня не повинні впливати на вищі рівні.

- допоміжні транспортні маршрути для певного рівня не повинні перетинати нижні рівні.

- класифікацію трафіку слід виконувати лише на рівні входу.

Усі мережеві рівні повинні підтримувати пріоритизацію трафіку. Рівень розподілу повинен лише збирати трафік. Ядру мережі потрібно лише виконувати швидку комутацію пакетів та маршрутизацію:

- час конвергенції та розмір таблиці маршрутизації на кожному рівні слід оптимізувати шляхом вибору найкращої схеми резервування.

- віддалені користувачі та зовнішні канали зв'язку не повинні бути підключені безпосередньо до ядра мережі. Комутатори доступу слід використовувати для запобігання перевантаженню таблиць маршрутизації всієї мережі.

- не використовувати некеровані комутатори, мінімально прийнятним мережевим комутатором є керований комутатор другого рівня.

Резервування місць для основних центрів обробки даних слід здійснювати таким чином:

- мережа повинна мати щонайменше два комутатори рівня ядра, що використовують 10-гігабітний Ethernet (або швидший) або еквівалентну пропускну здатність для підключення відмовостійкого стеку.

- кожен комутатор рівня доступу повинен мати до двох гігабітних каналів Ethernet для комутаторів розподільчого рівня.

- кожен комутатор розподільчого рівня повинен мати гігабітне Ethernet (або швидше) з'єднання з обома центральними комутаторами.

Для забезпечення відмовостійкості мережа повинна мати два прикордонні маршрутизатори. Кожен маршрутизатор підключений щонайменше до двох різних інтернет-провайдерів і маршрутизує пакети за допомогою протоколу BGP. Кожен прикордонний маршрутизатор має бути підключений до двох пристроїв, що забезпечують функціональність ITU або IDS/IPS.

Для забезпечення незалежності від інтернет-провайдерів слід використовувати автономну систему (AS) з власними IP-адресами (принаймні /23).

Продуктивність мережі повинна відповідати наступним вимогам:

- поверхові комутатори (комутатори доступу) повинні бути підключені до розподільчих комутаторів Gigabit Ethernet або 10 Gigabit Ethernet.

- сервер має бути підключений до розподільчого рівня Gigabit Ethernet або 10 Gigabit Ethernet.

За бажанням, сервери можна підключити до основного комутатора. Для належної роботи необхідно вибрати розподільний та головний рівні вимикачі. Вибираючи рівень продуктивності, важливо враховувати, чи потрібно підтримувати всі необхідні протоколи на бажаному рівні QoS.

Рекомендується встановити світловий канал між двома будівлями. Для потреб передачі великих обсягів трафіку на великі відстані та з високими швидкостями передачі даних рекомендується організовувати канали зв'язку на основі технології оптичного мультиплексування (xWDM) та агрегації каналів.

Для забезпечення надійності мережі слід дотримуватися таких стратегій:

1. Обладнання магістрального рівня повинно мати резервування всіх компонентів. Проект мережі повинен відповідати вимогам щодо забезпечення цілісності, стабільності роботи та безпеки інформаційних систем загального користування, затвердженим Наказом Міністерства зв'язку та масових комунікацій Російської Федерації від 25 серпня 2009 року № 104.17.

2. Мережа повинна використовувати VLAN. Віртуальні локальні мережі (VLAN) повинні захищати всі мережеві ресурси та користувачів, які обробляють захищені дані.

Розширення мережі має бути підтримане:

- правильно застосовувати трирівневу модель переходу.

- через масштабованість комутаторів цього необхідно досягти шляхом об'єднання комутаторів у групи (стеки) таким чином, щоб кожен комутатор у стеку працював у двох режимах - як головний комутатор стеку та як процесор комутації пакетів.

Відмовостійкість системи має бути гарантована за схемою 1:N (незалежно від виконуваної нею функції, якщо один комутатор у стеку вийде з ладу, інші

комутатори продовжуватимуть виконувати свої завдання, не порушуючи роботу всієї мережі).

Рекомендується використовувати протоколи динамічної внутрішньої маршрутизації, такі як OSPF або EIGRP, оскільки вони мають добру масштабованість, швидку конвергенцію, враховують якість каналу зв'язку та займають мінімальну пропускну здатність каналу.

Система IP-адресації мережі повинна забезпечувати наступне:

1. Розділіть адресного простору на блоки послуг (мережі, підключені до маршрутизаторів, віртуальні інтерфейси тощо) та блоки адрес локальної мережі. Цей розділ дозволяє ефективно створювати правила доступу для мережевих пристроїв.

2. Розділіть адресного простору локальної мережі на блоки залежно від розташування. Модуль підтримує агрегацію адрес, що зменшує кількість таблиць маршрутизації та спрощує управління мережею.

Щоб забезпечити автентифікацію на рівні з’єднання для всіх пристроїв, що підключаються до мережі, та забезпечити доступ до консолі керування для всіх пристроїв, мережа повинна мати такі можливості:

1. Безпека порту означає, що порт комутатора має бути доступним за заздалегідь визначеною фізичною адресою (MAC-адресою) комп'ютера користувача. Якщо неавторизований пристрій намагається підключитися, порт слід закрити та повідомити систему керування мережею.

2. Порт комутатора має автоматичну конфігурацію, тобто автоматизацію.

3. Перевірте, чи має адміністратор доступ до сервера Radius, тобто під час доступу до командного рядка пристрою потрібна ідентифікація особи, авторизація та реєстрація. Обмеження доступу на основі IP-адрес, з урахуванням обмежень доступу до командних рядків пристроїв та системних консолей, а також SNMP-трафіку.

4. Порт комутатора повинен мати функцію автоматичної фільтрації невикористаного протокольного трафіку.

Для досягнення високого рівня доступу до мережі ми рекомендуємо такі функції:

- підтримує RSTP/MSTP або інші протоколи резервування 2-го рівня.

- підтримує об'єднання кількох фізичних з'єднань між комутаторами в один логічний канал.

- автоматичне перемикання з основного маршрутизатора на резервний маршрутизатор у разі збою основного маршрутизатора.

Балансування навантаження між резервними маршрутизаторами. Внутрішнє програмне забезпечення зосереджено на покращенні часу конвергенції протоколів маршрутизації та балансуванні навантаження між еквівалентними шляхами.

Для підтримки програм на основі багатоадресної розсилки IP мережа повинна мати такі можливості:

На рівні доступу/розподілу – багатоадресні IP-пакети надсилаються на канальному рівні зі швидкістю фізичного з'єднання, використовуючи протоколи IGMP та PIM для динамічної реєстрації.

Базовий рівень – використовує масштабований протокол маршрутизації багатоадресного IP-трафіку для транспортування багатоадресних IP-пакетів на канальному та мережевому рівнях зі швидкістю фізичного каналу.

2.1.2.4 Вимоги до телефонних, аудіо- та відеоконференцій

Основним протоколом для передачі аудіо- та відеоданих є IP. Використання традиційних аналогових телефонів дозволено за таких обставин:

- існуючий Call-центр застарів;

- економічна ефективність, цей виняток застосовується до тих пір, поки ціни на VoIP-телефони не стануть порівнянними з цінами на аналогові телефони.

VoIP слід впроваджувати переважно з використанням технології SIP, оскільки вона використовується в мережах наступного покоління та має потужніші функції, ніж H.323. На цьому етапі необхідно звернути увагу на сумісність реалізації протоколу SIP між термінальним пристроєм та програмно-апаратним пакетом, що забезпечує функцію комутатора офісного телефону. Ця сумісність має проявлятися в підтримці базових можливостей обробки вхідних викликів на термінальні пристрої. Щоб уникнути проблем, пов'язаних з несумісними реалізаціями протоколу SIP, рекомендується встановлювати термінальне обладнання (телефони) та апаратно-програмні комплекси, що забезпечують функціональність офісної телефонної станції, від одного виробника, або проводити комплексні лабораторні випробування сумісності обладнання різних виробників.

Система відео-конференц-зв'язку повинна підтримувати веб-конференції та інтегруватися з офісними програмами.

Сервер аудіо-конференцій повинен підтримувати відеоконференції або бути розроблений для підтримки відеоконференцій.

Відеоконференції повинні бути організовані з використанням IP-технологій та впроваджувати стандарти H.323/H.264.

У випадку пакетної передачі рівень якості, еквівалентний 4 (середній бал) за шкалою MOS/PAMS, слід розглядати як міру якості мовлення. Рекомендовано використовувати кодек G.729 (MOS = 4.07).

Вимоги до якості пакетів даних: максимальна затримка пакетів даних становить 150 мс, а максимальне коливання сигналу – 50 мс.

Якщо у вас є два або більше постачальників послуг, включаючи традиційний телефонний зв'язок та VoIP, рекомендується використовувати LCR. Водночас, VoIP-обладнання повинно забезпечувати моніторинг якості каналу зв'язку.

2.1.2.5 Вимоги до обладнання

Пристрої рівня доступу повинні мати можливість класифікувати трафік, тобто бути «доступними». Трафік можна класифікувати на основі типу програми, фізичних та мережевих адрес джерела та призначення, а також портів переадресації. Класифікований трафік слід позначати таким чином, щоб вказувати пріоритет, призначений пакету, щоб мережеві пристрої могли належним чином маршрутизувати трафік. Пакети необхідно пере-класифікувати відповідно до політик QoS, визначених адміністратором. Наприклад, користувачі призначають високий пріоритет своєму трафіку та надсилають його через мережу. Цей пріоритет можна знизити на основі політики мережі, а не вимог користувача. Цей механізм має бути основою для забезпечення якості обслуговування по всій мережі.

Обладнання магістрального рівня повинно мати такі можливості:

1. Запобігання та управління перевантаженням, тобто здатність контролювати поведінку мережі, пов'язану з перевантаженням, шляхом відкидання певних пакетів на основі класифікації або політики та кількох черг на інтерфейсі, коли мережа перевантажена. Адміністратори повинні встановлювати обмеження для різних рівнів пріоритету.

2. Планування, яке полягає в можливості використання кількох черг для визначення пріоритетів пакетів на основі класифікації або політик QoS.

3. Резервування ключових компонентів, таких як блок живлення, блок вентилятора та процесорний блок.

4. Виконайте детальний аналіз мережевого та транспортного трафіку за допомогою протоколу IPFIX (RFC 3917), Netflow, J-Flow або інших протоколів, надаючи повну статистику IP-потоку.

У центрах обробки даних Tier I та Tier II, окрім забезпечення резервування ключових вузлів обладнання на магістральному рівні, рекомендується забезпечити таке ж резервування обладнання на розподільчому рівні.

Усе активне мережеве обладнання повинно мати інструменти для моніторингу QoS та політик безпеки, а також планування мережі та послуг:

1. Статистику можна збирати щонайбільше для одного мережевого порту, щоб оцінити його продуктивність та виявити вузькі місця в мережі.

2. Трафік з окремих портів, груп портів та віртуальних портів може бути спрямований до аналізатора протоколів для детального аналізу.

3. Для розширення можливостей діагностики за межі зовнішнього аналізу необхідно забезпечити розширений моніторинг подій у режимі реального часу. За допомогою технології Syslog можна збирати та зберігати інформацію про важливі мережеві події, включаючи зміни в конфігурації пристроїв, зміни топології, а також помилки програмного та апаратного забезпечення.

4. Доступ до інтерфейсів керування пристроями та звітності має здійснюватися через стандартний веб-браузер за протоколом HTTPS.

5. Ви повинні мати можливість підключитися до пристрою за допомогою протоколу ssh та налаштувати його.

6. Порти швидкого /гігабітного Ethernet, віртуальні мережі та транкінг VLAN повинні мати можливості автоматичного налаштування.

7. Для забезпечення автоматичного виявлення топології мережі слід використовувати агент виявлення топології.

Використання вузлів для забезпечення роботи локальної мережі, її розширення, дотримання вимог інформаційної безпеки та забезпечення якості обслуговування багато-сервісного трафіку заборонено. Натомість слід використовувати лише ключ.

Усе активне обладнання має бути спроектоване з використанням 19-дюймової стійки.

2.1.3 Вимоги до комп'ютера

У цьому розділі розглядаються загальні технічні вимоги до комп'ютерного парку, що експлуатується інститутом.

Якщо парк комп'ютерів не відповідає конфігурації, зазначеній у технічних вимогах (парк комп'ютерів застарів), а також якщо мінімальні технічні вимоги до загальносистемного програмного забезпечення перевищують використану технічну конфігурацію, рекомендується оновлювати парк комп'ютерів до поточного стану, зазначеного у технічних вимогах, зі швидкістю 20% від загальної кількості робочих станцій на рік.

Під час встановлення комп'ютерного парку та вибору моделей комп'ютерів для придбання, IT-відділ будівельного інституту Це слід зробити наступним чином:

- апаратна та програмна платформа ПК повинна бути стандартизованою та сертифікованою, а також мати гнучку та масштабовану архітектуру.

- технічні характеристики комп'ютера повинні відповідати або перевищувати мінімальні системні вимоги для використовуваного програмного забезпечення. Якщо характеристики обладнання перевищують мінімальні системні вимоги для використовуваного програмного забезпечення, конфігурація повинна відповідати виконуваним завданням і не повинна суттєво перевищувати мінімальні вимоги.

- для забезпечення єдиного рівня обслуговування управління даними для всіх комп'ютерів має бути уніфікованим, тобто для організації централізованого розповсюдження програмного забезпечення на комп'ютери має використовуватися єдиний інструмент розповсюдження оновлень програмного забезпечення.

- персональний комп'ютер (робоча станція) з встановленою операційною системою та прикладним програмним забезпеченням повинен мати апаратну або програмну систему дистанційного керування.

- для покращення якості та швидкості адміністрування слід обмежити кількість різних апаратних та програмних конфігурацій персональних комп'ютерів. Рекомендується максимум 4 стандартні конфігурації.

Для визначення технічних вимог перераховані такі основні параметри комп'ютера:

1. Продуктивність персонального комп'ютера повинна забезпечувати наступне:

- налаштування швидкості процесора;

- потрібно достатньо оперативної пам'яті;

- швидкість внутрішньої шини даних;

- якість та швидкість роботи графічної підсистеми;

- пристрої введення /виведення.

2. Надійність має бути досягнута як за допомогою апаратного, так і програмного забезпечення та визначається середнім часом напрацювання на відмову (MTBF). Масштабованість. Масштабованість Архітектура та дизайн персональних комп'ютерів повинні забезпечувати масштабованість:

- кількість та потужність процесорів;

- об'єм оперативної пам'яті та зовнішнього сховища.

2.1.4 Вимоги до видів забезпечення

2.1.4.1 Вимоги до системного програмного забезпечення для робочих станцій користувачів

Адміністративні основні засоби повинні:

- сумісний з типом операційної системи клієнта;

- підтримувати всі мережеві служби, що забезпечують роботу мережі компанії;

- забезпечити необхідний рівень інформаційної безпеки;

- повинні дотримуватися організаційних стандартів щодо використовуваних офісних процедур.

2.1.4.2 Вимоги до підтримки

У цьому розділі перелічені основні технічні вимоги до периферійних пристроїв, що використовуються та придбані інститутом як частина її IT-інфраструктури.

Для наступних категорій периферійних пристроїв необхідно враховувати конкретні мінімальні технічні вимоги:

- друкарські верстати (принтери);

- багатофункціональний пристрій?

Вимоги до спеціального обладнання з обмеженим технічним застосуванням (термо-принтери, принтери штрих-кодів, принтери етикеток, друкарські верстати тощо) не враховуються. Використання спеціального обладнання залежить від конкретних технічних вимог процесу.

Для опису мінімальних вимог до периферійних пристроїв використовуються такі класифікації пристроїв:

- особисті пристрої, що часто використовуються співробітниками;

- командний пристрій – використовується групою співробітників у режимі спільного використання ресурсів.

- пристрої підприємства – для завдань, що передбачають використання високопродуктивних пристроїв (графіка, формати виведення великих даних).

2.1.4.3 Загальні вимоги

У цьому розділі описано загальні вимоги, які інститут повинен застосовувати під час вибору та придбання нового периферійного обладнання для розвитку

інформаційних технологій. Периферійні пристрої повинні відповідати таким основним вимогам:

1. Продуктивність. Периферійне обладнання повинно відповідати потребам бізнес-процесів та вимогам, визначеним кількісними показниками (такими як кількість копій за хвилину, роздільна здатність сканованого зображення тощо).

2. Надійність периферійного обладнання повинна забезпечувати безперервність роботи та відповідати вимогам, заданим кількісними показниками.

3. Досконалість. Якщо на робочому місці ваших співробітників потрібні різні типи периферійних пристроїв, вам слід пріоритетна придбати багатофункціональні пристрої (МФП), які підтримують усі або деякі з перелічених нижче функцій:

- друкарські;
- сканування пристрою;
- копірайтер.

4. Сумісність - незалежно від типу процесора та операційної системи, периферійні пристрої повинні взаємодіяти з персональними комп'ютерами (включаючи сервери під час використання командних або корпоративних пристроїв) з точки зору технологій та програмного забезпечення.

5. Безпека - вихід з ладу будь-якого периферійного пристрою не повинен впливати на стабільну роботу персональних комп'ютерів (або серверів для корпоративного чи корпоративного обладнання) та інших периферійних пристроїв.

6. Контроль - підключення та керування персональними аксесуарами має бути максимально простим і не вимагати швидкого перегляду інструкцій та описів пристроїв.

7. Загальна вартість обладнання низька, запасні частини та витратні матеріали для периферійного обладнання повинні бути легкодоступними та мати помірну ціну.

8. Низький рівень шуму - периферійні пристрої не повинні заважати іншим під час роботи. Для роботи з обладнанням, що генерує шум, слід передбачити спеціальні приміщення.

9. Низьке енергоспоживання. Рекомендується купувати пристрій з режимом низького енергоспоживання (режимом очікування).

10. Загалом, перевагу слід надавати периферійним пристроям, які можуть обмінюватися даними через локальну мережу.

11. Периферійні пристрої, які можна підключити як до комп'ютера, так і до локальної мережі, повинні бути підключені до локальної мережі.

2.1.4.4 Вимоги до спорядження команди та компанії

До командних та корпоративних пристроїв повинні застосовуватися суворіші вимоги, ніж до особистих пристроїв. Вибираючи пристрої для своєї команди та компанії, слід приймати рішення на основі передбачуваної кількості користувачів, які їх використовуватимуть.

Багатофункціональне обладнання слід регулярно обслуговувати, що допомагає підвищити його доступність та знизити загальну вартість володіння. Частоту цього технічного обслуговування слід визначати на основі технічних вимог кожної конкретної операції з обладнанням.

2.2 Розробка системного обладнання

2.2.1 Розробка спільної архітектури корпоративної мережі

Наразі будівельного інституту має територіальну адміністративну структуру, тому використовує глобальні мережеві технології для організації зв'язків між усіма елементами.

Головною метою глобальної мережі (WAN) є забезпечення широкого доступу до різних ресурсів і послуг у корпоративній мережі, таких як доступ до баз даних, IP-телефонія, електронна пошта в інтрамережі, веб-сайти тощо.

Тому впроваджуються мережі типу WAN: виділені лінії, мережі MPLS, мобільні мережі, Інтернет та приватні мережі, побудовані безпосередньо компанією.

Ключовим моментом у кожному з цих випадків є те, що з'єднання між локальними мережами або окремими користувачами можуть бути встановлені через посередника (наприклад, інтернет-провайдера) або незалежно від компанії.

Інститут має стандартизовану дротову мережеву структуру. Зазвичай мережі, такі як одна локальна мережа або ціла глобальна мережа, централізовано керуються через систему керування мережею (NMS), оскільки фізичне налаштування мережевих пристроїв є складним, коли вони географічно розділені. Зазвичай система керування мережею вже встановлена на сервері компанії або хмарному сервісі.

Мета цих систем — спростити роботу мережевих інженерів з обслуговування та розвитку нових сегментів мережі. Ці системи можуть відстежувати помилки через SNMP та дистанційно налаштовувати, оновлювати та діагностувати пристрої через SSH.

Популярні платформи NMS включають Cisco, Huawei, Netco тощо [5].

Інституту характеризується проблемами та труднощами, пов'язаними з традиційними дротовими мережевими структурами, географічною мережею.

1. Дистанційне керування, але ручні налаштування. Хоча мережеві інженери можуть керувати мережевими пристроями віддалено, саме управління все ще здійснюється вручну. Інші конфігурації, особливо під час розгортання нових сегментів мережі, такі як налаштування підключення для користувацького трафіку, моніторингу, ведення журналу та служб безпеки, все ще вимагають підключення до

мережевих компонентів через SSH та ручного введення всіх необхідних команд конфігурації в інтерфейсі командного рядка (CLI). Звичайно, можна використовувати скрипти мовою програмування Python для встановлення параметрів шаблонів (наприклад, призначення IP-адрес мережевим інтерфейсам), але з одного боку, не всі мережеві інженери мають достатні навички програмування, а з іншого боку, ризик інженерних помилок завжди високий, тому використання таких інструментів автоматизації небезпечне для стабільності мережі. Крім того, платформи NMS не можуть забезпечити конфігурацію для великої кількості мережевих пристроїв, тому інженери завжди повинні налаштовувати мережеві пристрої один за одним, що збільшує ризик помилок та час, необхідний для розширення та модернізації мережі.

2. Низька точність виявлення помилок. Оскільки більшість платформ NMS використовують протокол SNMP для виявлення помилок, вони можуть виявляти помилки з інтервалом щонайменше 10 хвилин [6]. Це пояснюється тим, що архітектура протоколу SNMP вимагає обробки пакетів, що містять діагностичну інформацію про мережеві пристрої, та надсилання отриманої інформації про помилки на існуючі платформи NMS, що зрештою збільшує навантаження на процесор мережевого пристрою, уповільнюючи не лише швидкість обробки SNMP-пакетів, але й швидкість роботи всього мережевого пристрою.

Крім того, SNMP може лише контролювати стан пристроїв у мережі, але не може контролювати стан послуг, що надаються пристроями в мережі (таких як відеотрафік, трафік IP-телефонів тощо).

Враховуючи вищезазначену важливість впровадження програмної архітектури в мережах будь-якого розміру, доведено, що використання ручного управління мережею призводить до високих часових витрат на впровадження, обслуговування мережі та діагностику помилок, а також зниження якості послуг

інформаційної інфраструктури, що негативно впливає на розвиток будь-якого бізнесу.

Крім того, концепції нової IT-системи, її компоненти та принципи архітектури програмного забезпечення повинні забезпечувати чіткий, якісний опис процесу впровадження мережі відповідно до нових принципів.

Згідно з рекомендаціями Cisco, кожна мережева конструкція складається з двох шарів:

1. Низько-рівневе проектування (LLD) – описує проект фізичних з'єднань, де мережеве обладнання буде розташоване в приміщенні, куди і як буде підключено живлення тощо. Мета цього проекту – точно описати реалізацію «локальних» мережевих пристроїв.

2. Високо-рівневе проектування (HLD) – описове проектування, яке визначає логічні з'єднання мережевих пристроїв, їх зіставлення з відповідними підмережами та сервісами VLAN, реалізацію протоколів тощо.

Відповідно до завдання в проекті є підготовка пропозиції високого рівня, і описанню деяких основних елементів проектування, такі як вибір мережевих пристроїв та їх підключення.

Для цього завдання було створено спеціальний документ, який описує фізичні з'єднання та схему IP, яка по суті є комбінацією схем LLD та HLD.

Незалежно від того, хто створює програмоване мережеве рішення, програмована мережа та її архітектура (рис 2.1) мають спільну та чітко визначену технічну реалізацію, якої всі повинні дотримуватися.

У традиційних мережах рівень управління, рівень контролю та транспортний рівень логічна незалежні один від одного в межах мережевих пристроїв, що унеможливлює централізоване керування пристроями. Під час використання програмованих мереж рівень управління та контролю переміщується на

програмовану сторону, тоді як передача даних все ще знаходиться за мережевими пристроями.

Таким чином, архітектура SDN складається з трьох рівнів, як показано на рис. 2.2 [7]:

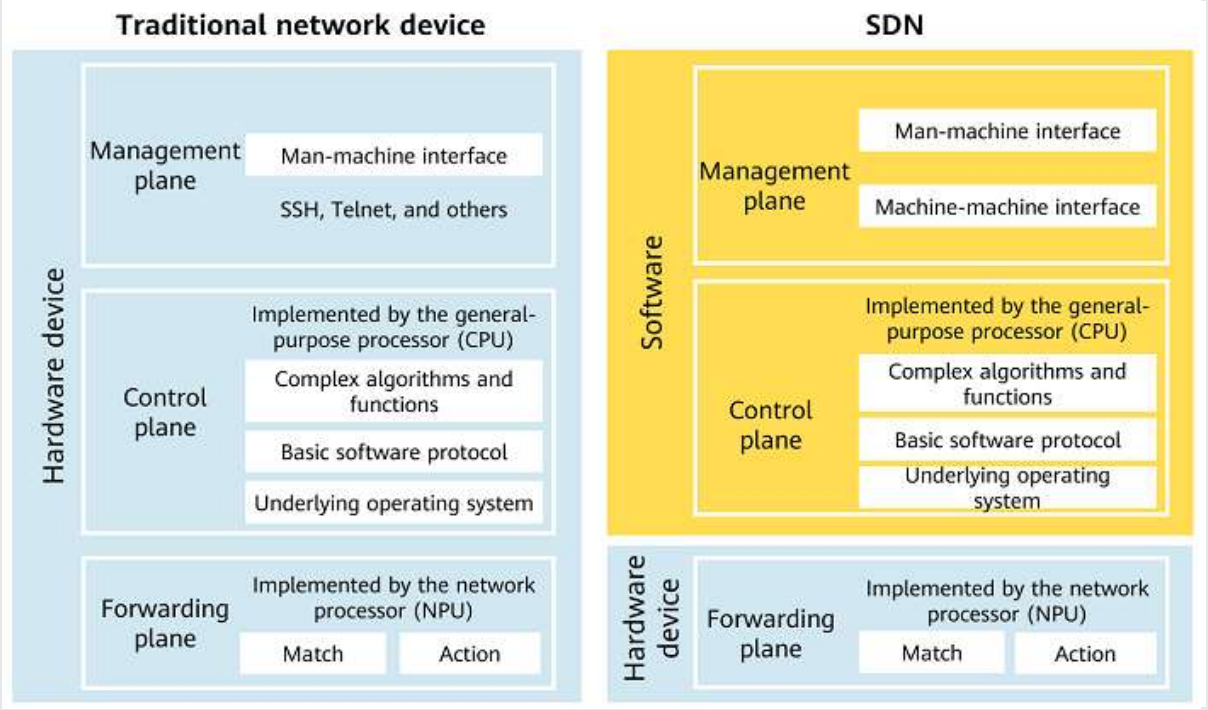


Рисунок 2.1 – Аналіз програм керування мережевими пристроями [11]

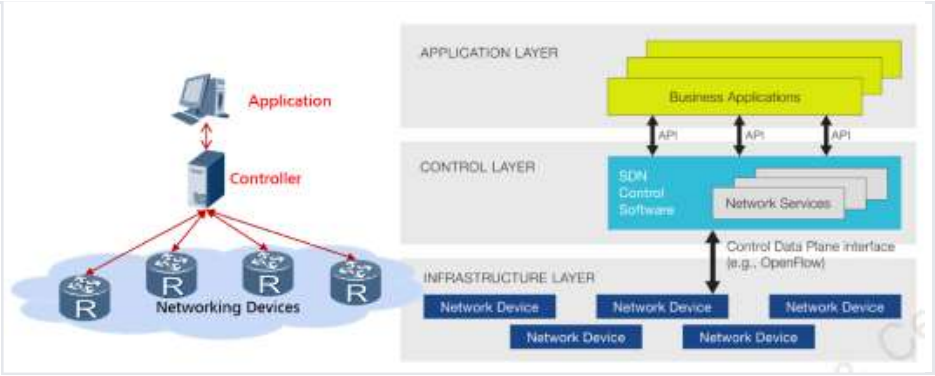


Рисунок 2.2 - Архітектура програмованої мережі

1. Рівень додатків – цей рівень містить додатки для моніторингу, безпеки та управління мережею (зазвичай різні типи платформ управління мережею, такі як NMS).

2. Рівень управління – відповідає за обробку та виконання команд, отриманих мережевими пристроями від прикладного рівня. Цей рівень зазвичай фізично представлений SDN-контролером, який може бути представлений як окремий спеціалізований пристрій, що вирішує певні завдання (наприклад, для мережевих архітектур типу WAN), або як сервер.

3. Інфраструктурний рівень – виконує команди на прикладному рівні. Іншими словами, будь-який мережевий елемент (маршрутизатор, комутатор, брандмауер, точка доступу тощо) може бути компонентом.

Ці три рівні мають ієрархічну структуру та, з точки зору управління, пов'язані двома логічними інтерфейсами:

1. Південний інтерфейс – забезпечує зв’язок між SDN-контролером та фізичними (або віртуальними) пристроями в мережі, дозволяючи їм контролювати свою поведінку. Прикладами таких інтерфейсів є протокол NETCONF, який використовується для керування налаштуваннями мережевих пристроїв або для забезпечення пропускної здатності, маршрутизації, налаштувань безпеки тощо для мережевих пристроїв.

2. Північно-східний інтерфейс – забезпечує зв’язок між програмним контролером або системою управління SDN та програмним забезпеченням або додатками вищого рівня. Це дозволяє програмам або службам підключатися до контролера SDN та отримувати доступ до мережевих ресурсів і функцій. Типовим прикладом такого інтерфейсу є API передачі презентаційного стану, який дозволяє програмам взаємодіяти з контролером програм SDN за допомогою стандартних HTTP-запитів.

2.2.2 Опис запропонованої концепції мережі

Концепцію проекційної мережі показано на рис. 2.3. Характеристики налаштування мережі такі:

Сервер оснащений платформою управління iMaster NCE, а сам сервер підключений до комутатора через два мережеві порти. Комутатор служить інтерфейсом між локальною демонстраційною мережею та брандмауером, який забезпечує доступ до Інтернету.

Агрегаційний комутатор підключений до платформного комутатора та може використовувати технологію PoE для живлення точок доступу WLAN через мережевий інтерфейс.

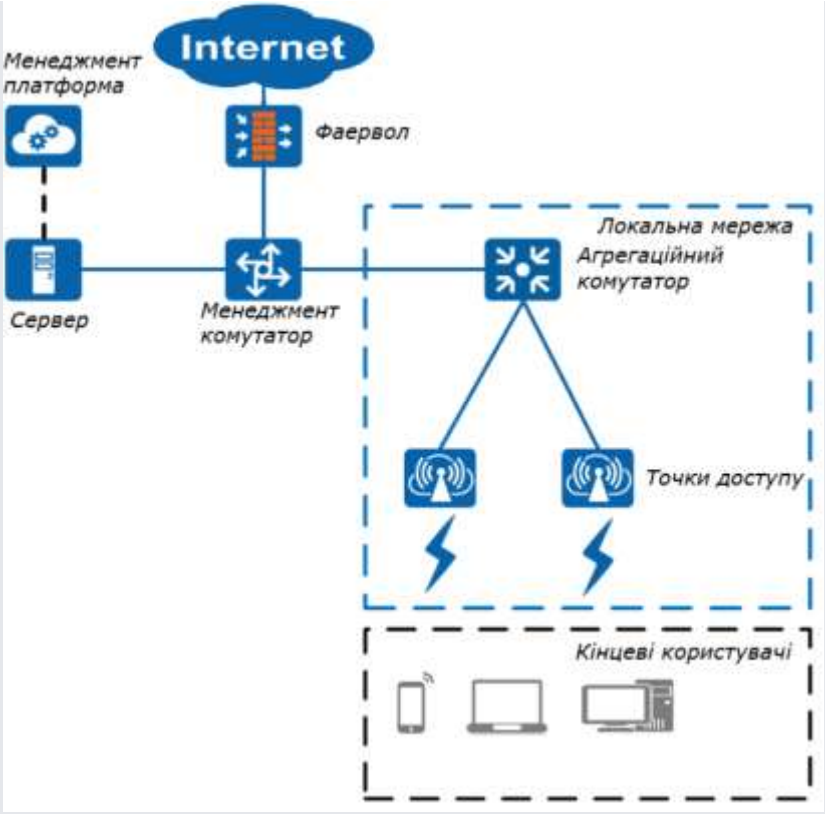


Рисунок 2.3 – Логічна топологія мережі

Кілька точок доступу підключаються до агрегаційного комутатора, який бездротово зв'язується з кінцевими користувачами за допомогою протоколу Wi-Fi.

Важливо зазначити, що з міркувань безпеки сама локальна демонстраційна мережа не може отримати доступ до Інтернету: саме обладнання демонстраційної мережі розташоване в офісній будівлі, де застосовуються суворі правила доступу до мережі: управління трафіком, встановлення обмежень безпеки Radius. Отже,

метою цього проєкту є не доступ до зовнішньої мережі, а підключення гіпотетичного користувача до цієї мережі та перевірка з'єднання, наприклад, за допомогою агрегаційного комутатора. Детальна інформація про тестування та перевірку мережі наведена в наступних розділах. Топологія вхідних даних приблизно показана на рис. 2.4.

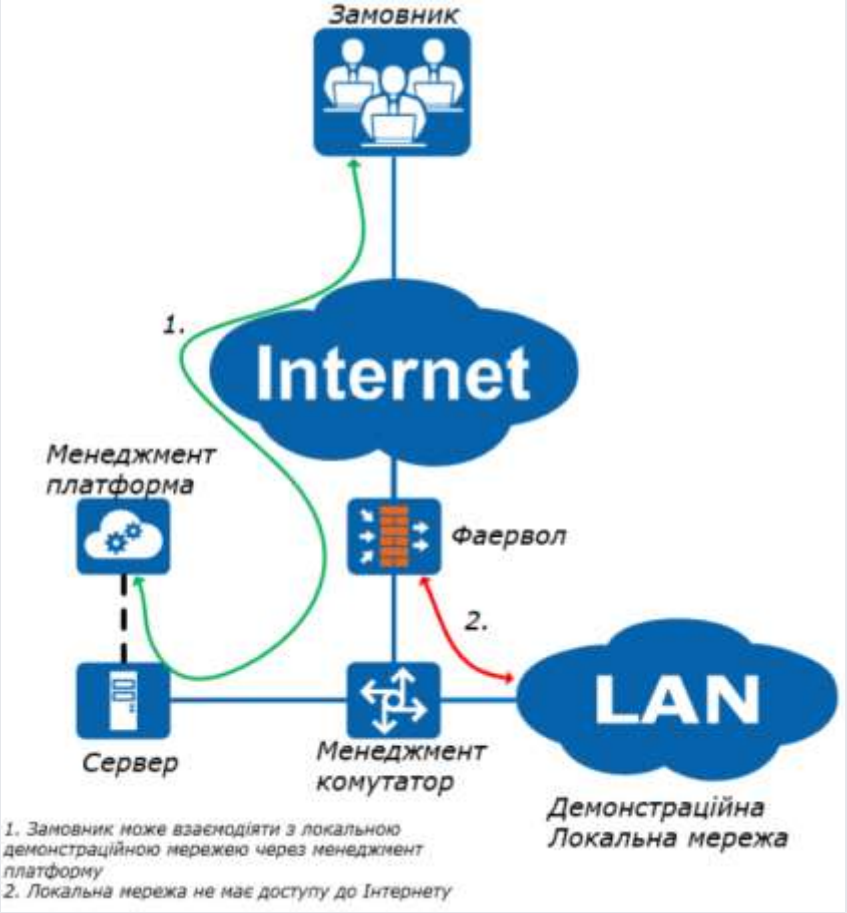


Рисунок 2.4 - Топологія входу

Як видно, можна підключитися до платформи керування iMaster NCE через Інтернет, але не можете віддалено підключитися до окремих мережевих елементів, інтегрованих у платформу. Також неможливо підключитися до Інтернету через точку доступу в тестовій мережі.

Згідно з організаційною структурою будівельного інституту необхідно, щоб усі команди IT-фахівців були підключені до комп'ютерної мережі.

Архітектура комп'ютерної системи компанії була «сумісною з визначенням, наведеним у кваліфікаційній роботі».

Загальна мережева структура компанії будівельного інституту показана на рис. 2.5.

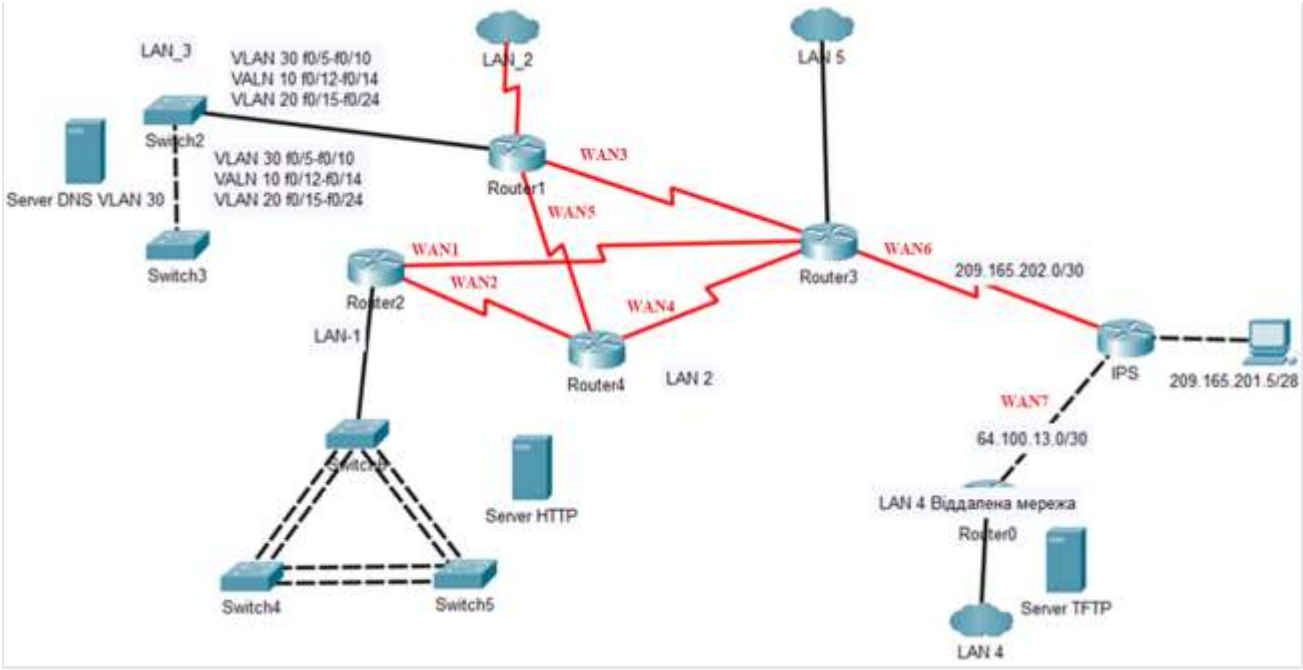


Рисунок 2.5 – Топологія мережі будівельного інституту

Розподіл мережі між маршрутизаторами (WAN):

- адресні блоки для тунелів між маршрутизаторами 10.23.44.0/22;

- номер варіанту 7;

- першу доступну IP-адресу слід призначити інтерфейсу та підмережі маршрутизатора в локальній мережі, інші можливі IP-адреси комутаторам локальної мережі.

- слід використовувати DHCP-адресацію для кінцевих пристроїв у VLAN.

2.2.3 Апаратна частина комп'ютерної системи будівельного інституту

2.2.3.1 Сервер керування платформою Cisco

Вибір сервера для корпоративної мережі будівельного інституту залежить від характеристик, які він повинен мати для встановлення та коректного запуску

сервісних програм на платформі управління та для роботи на самій платформі управління.

Згідно з технічною документацією управління Cisco UCS [8], було обрано сервер Cisco UCS серії B - CISCO (UCSB-B200-M6-U) UCS B200 M6 Blade (рисунок 2.6) [9], який не має процесора, жорсткого диска та обмежень.

Рисунок 2.6 – Блейд-сервер CISCO (UCSB-B200-M6-U) UCS B200 M6 (без процесора, жорсткого диска, Mezz)

Згідно з технічними документами пристрою, його основні технічні показники такі:

1. Блейд-сервер Cisco UCS B200 M6 забезпечує неперевершену продуктивність, гнучкість та щільність для обробки широкого спектру робочих навантажень, від IT- та веб-інфраструктури до розподілених баз даних.

2. Блейд-сервер корпоративного класу Cisco UCS B200 M6 розширює портфоліо мережевих обчислювальних систем Cisco до середнього класу. Cisco UCS B200 M6 працює на базі найновіших масштабованих процесорів Intel® Xeon® 3-го покоління (Ice Lake):

– до 4 ТБ оперативної пам’яті на процесор із 16 модулями DRAM по 256 ГБ або до 6 ТБ на процесор із 8 модулями пам’яті по 256 ГБ та 8 модулями постійної пам’яті Intel Optane™ (PMEM) по 512 ГБ.

- невеликий накопичувач даних з двома SSD-накопичувачами або двома накопичувачами PCIE NVMe або накопичувачами M.2 SATA.

- швидкість з'єднання до 80 Гбіт/с.

2.2.3.2 Керування комутаторами Cisco

Вибір комутаторів платформи Cisco залежав від двох критеріїв: висока продуктивність пакетної комутації та швидка передача даних для обробки даних з кількох мереж, а також можливість подальшого розширення IT-мережі без необхідності заміни комутаторів найближчим часом.

Для мережевих завдань, що потребують великої кількості портів та високої пропускної здатності для окремих мережевих портів, а також високої швидкості для всього комутатора, підійде комутатор Cisco Catalyst 2960-Plus 48TC-L (рисунок 2.7).

Рисунок 2.7 – Комутатор Cisco Catalyst 2960-Plus 48TC-L

Основні технічні параметри комутатора такі [10].

Комутатори Cisco® Catalyst® серії 2960 Plus – це комутатори Fast Ethernet з фіксованою конфігурацією, які забезпечують комутацію другого рівня корпоративного класу для філій, традиційних настільних комп’ютерів та інфраструктурних застосувань. Завдяки широкому спектру функцій програмного

забезпечення Cisco IOS®, включаючи Cisco Catalyst SmartOperations, вони забезпечують надійну та безпечну роботу з низькою загальною вартістю володіння.

Основні характеристики продукту:

- комутатор Cisco Catalyst 2960-Plus: 24 або 48 портів Fast Ethernet;

- канали Gigabit Ethernet 1000BASE-T та SFP (Small Form-factor Pluggable)

- живлення через Ethernet (PoE) відповідає стандарту IEEE 802.3af.

- набір функцій LAN Base або LAN Lite програмного забезпечення Cisco IOS®.

- інструменти SmartOperations спрощують розгортання та зменшують витрати на управління мережею.

- технологія Cisco EnergyWise керує споживанням енергії підключеними пристроями.

- розширена обмежена довічна гарантія на обладнання (E-LLW) із заміною наступного робочого дня.

Серія Cisco Catalyst 2960 Plus забезпечує економічно ефективну комутацію Ethernet корпоративного класу для таких застосувань:

- філії, офіси та роздрібні магазини;

- стандартний настільний комп'ютер;

- розвиток інфраструктури, фізична охорона та інші нетрадиційні методи впровадження.

Переваги моделі 2960-Plus включають:

- надійна якість обслуговування (QoS), яка надає пріоритет голосу та критично важливим для бізнесу додаткам;

- гнучкі функції безпеки для обмеження доступу до мережі та обмеження загроз.

- інструменти для зниження загальних витрат шляхом оптимізації та автоматизації процесів.

2.2.3.3 Маршрутизатор Cisco

Маршрутизатори підключають комп'ютери та інші пристрої до Інтернету. Маршрутизатор діє як хаб, вибираючи найкращий шлях для передачі даних через мережу. Мережа об'єднує підприємства по всьому світу, захищає інформацію від загроз безпеці та навіть може вирішувати, які комп'ютери мають пріоритет над іншими.

Вибір маршрутизаторів Cisco визначається такими критеріями:

1. Спільний доступ до програм для підвищення продуктивності, особливо для співробітників, які працюють віддалено або поза межами центрального офісу. Можливість додавання спеціальних послуг, таких як VoIP, відеоконференції та мережі Wi-Fi.

2. Швидко отримуйте інформацію. Маршрутизатори можуть допомогти компаніям покращити реагування на запити клієнтів та полегшити доступ до даних клієнтів. В епоху, коли клієнти вимагають швидких відповідей на свої запитання та персоналізованого обслуговування, це справжні переваги. Маршрутизатори є важливими для малого бізнесу, оскільки вони дозволяють створювати швидку та надійну мережу, щоб співробітники могли краще та розумніше реагувати на потреби клієнтів.

3. Зменшити експлуатаційні витрати. Маршрутизатори можуть позитивно впливати на прибуток бізнесу, спільно використовуючи такі пристрої, як принтери та сервери, а також послуги, такі як доступ до Інтернету. Мережа швидких та надійних маршрутизаторів може зростати разом з вашим бізнесом, тому вам не доведеться постійно оновлювати та купувати нове обладнання в міру зростання вашого бізнесу.

4. Безпечніше. Маршрутизатори захищають цінні бізнес-дані від атак, перевіряючи вхідні дані та блокуючи їх за необхідності за допомогою вбудованих брандмауерів або мережевих фільтрів.

5. Увімкніть безпечні віддалені з'єднання. Маршрутизатори дозволяють компаніям надавати безпечний віддалений доступ співробітникам, які перебувають у русі та потребують спілкування з іншими співробітниками або використання корпоративних програм. Це поширений сценарій для багатьох компаній з віртуальними командами та віддаленими співробітниками, яким потрібно ділитися важливою бізнес-інформацією в будь-який час доби.

Виходячи з вищезазначених вимог, було обрано маршрутизатор Cisco 2911 C2911-VSEC-SRE/K9 (рисунок 2.8).

Рисунок 2.8 – Маршрутизатор Cisco 2911 моделі C2911-VSEC-SRE/K9

Основні технічні деталі, цілі та переваги, згадані в технічному документі, наведені нижче [11].

Інтегровані сервісні маршрутизатори Cisco серії 2900 базуються на 25-річному досвіді інновацій та лідерства у виробництві. Ці нові платформи розроблені для максимізації операційної економії, водночас забезпечуючи наступний етап еволюції філій – співпрацю з медіа та віртуалізацію філій.

Платформа маршрутизаторів другого покоління є новаторською та оснащена багатоядерними процесорами, високопродуктивними DSP (цифровими сигнальними процесорами), що підтримують майбутні відеофункції,

високопродуктивними сервісними блоками з підвищеною доступністю, комутацією Gigabit Ethernet з покращеним POE та новими функціями керування живленням та моніторингу, одночасно покращуючи загальну продуктивність системи.

Крім того, новий модуль Cisco IOS® Universal Image та Services Ready Engine дозволяють роз'єднати апаратне та програмне забезпечення, забезпечуючи гнучку технологічну основу, яка може швидко адаптуватися до змінних потреб мережі. Загалом, Cisco серії 2900 забезпечує безпрецедентну цінність економії коштів на володінні та гнучкості мережі завдяки інтелектуальній інтеграції передових засобів безпеки, уніфікованих комунікацій, бездротових послуг та служб додатків.

2.2.3.4 Точка доступу Cisco

Вимоги до точок доступу такі: підтримка Wi-Fi 6, функціональність PoE та можливість керування такими точками доступу в режимі хмарної точки доступу, тобто можливість керування цими точками доступу через платформу управління.

Загалом, більшість сучасних точок доступу Cisco відповідають цим вимогам. Однак остаточним вибором стала Cisco Catalyst 9105AXI, яка є найпотужнішою та найширше використовуваною точкою доступу в комерційних проектах (рис. 2.9).

Нижче наведено опис технічних специфікацій на основі документа [12].

Високо-гнучка точка доступу Cisco Catalyst 9105 виходить за рамки стандарту Wi-Fi 6 (802.11ax) та забезпечує високу щільність, гнучкість та мережевий інтелект для підтримки розгортання IoT-додатків. До них належать стельові кріплення для дистанційних працівників, філій та малих та середніх підприємств, а також настінні кріплення для гуртожитків, кімнат для студентів-студентів та інших житлових будівель.

Рисунок 2.9 – Точка доступу Cisco Catalyst 9105AXI

Точка доступу Cisco Catalyst 9105AXI компактна та потужна, оснащена 2x2 Wi-Fi 6 MU-MIMO, швидкістю передачі даних до 1,49 Гбіт/с та оптимізованим енергоспоживанням.

Готовий до Інтернету речей – інтегрований радіомодуль Інтернету речей підтримує технології BLE 5.0 та Zigbee, а також розробку користувацьких IoT-застосунків у контейнерах у стилі Docker.

Пристрій пропонує кілька варіантів кріплення: стельове кріплення для оптимального покриття, настінне кріплення для легкого встановлення та розширені можливості підключення кабелів.

2.3 Висновки за розділом

В розділі розробка апаратної частини комп'ютерної системи будівельного інституту були ретельно виконані наступні кроки: сформовані технічні вимоги до комп'ютерної системи, здійснена розробка архітектури корпоративної мережі системного обладнання, обрана апаратна частина комп'ютерної системи.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ ПРОЕКТНО-ТЕХНОЛОГІЧНОГО БУДІВЕЛЬНОГО ІНСТИТУТУ

3.1 Початкові данні для проектування корпоративної мережі

Згідно з завданням до роботи необхідно спроектувати комп'ютерну систему проектно-технологічного будівельного інституту з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Початкові дані для розрахунку діапазонів адресів при проектування корпоративної мережі:

адрес для виділення підмереж:	10.23.44.0/22;
- кількості хостів підмережі LAN1:	22;
- кількості хостів підмережі LAN2, од.:	14;
- кількості хостів підмережі LAN3, од.:	42;
- кількості хостів підмережі LAN4, од.:	47;
- кількості хостів підмережі LAN5, од.:	62;
- адрес WAN каналів для маршрутизаторів	10.0.7.0/24;

3.2 Адресація в корпоративній мережі

3.2.1 IP-адресація для корпоративних мереж

IP-адреса (Інтернет-протокол) - це унікальна цифрова мітка, яка присвоюється кожному пристрою, підключеному до комп'ютерної мережі, яка використовує протокол Інтернету для зв'язку. Такі пристрої, як ПК, ноутбуки та смартфони, можуть використовувати IP-адреси для ідентифікації один одного та передачі даних через Інтернет.

Поняття IP-адрес було введено Інтернет-суспільством, яке займається його розвитком і стандартизацією. З моменту своєї появи IP-адреса зазнала різних ітерацій.

Сьогодні використовуються дві версії IP-адрес: IPv4 та IPv6. Перший є більш поширеним, але обмежений своєю 32-бітною структурою, тоді як другий пропонує значно більше доступних адрес завдяки своєму 128-бітному формату. Обидва компоненти є важливими компонентами для забезпечення безперебійного онлайн-зв'язку між пристроями по всьому світу.

IPv4: складається з чотирьох наборів чисел, розділених крапками (наприклад, 192.168.1.1). Кожен набір знаходиться в діапазоні від 0 до 255, що дозволяє створити приблизно 4 мільярди унікальних комбінацій.

IPv6: використовує вісім груп шістнадцяткових цифр, розділених двокрапкою (наприклад, fe80::200:f8ff:fe21:67cf). Цей розширений формат надає трильйони й трильйони потенційних адрес.

На додаток до цих основних класифікацій, існують різні типи залежно від їх використання або методу розподілу - наприклад, публічні та приватні IP або статичні чи динамічні IP - які ми обговоримо далі в наступних розділах.

IP-адреса – це унікальний ідентифікатор пристроїв, підключених до Інтернету або локальної мережі. Ці адреси мають вирішальне значення для забезпечення зв'язку між різними пристроями, оскільки вони допомагають направляти пакети даних з одного пристрою на інший. Протокол Інтернету (IP) регулює призначення та використання цих адрес.

IP-адреса складається з двох основних компонентів: ідентифікатора мережі та ідентифікатора хоста. Ідентифікатор мережі визначає конкретну мережу, до якої належить пристрій, тоді як ідентифікатор хоста ідентифікує окремі пристрої в цій мережі. Кожен пристрій повинен мати унікальну комбінацію цих ідентифікаторів для забезпечення ефективної маршрутизації пакетів даних.

Двійкове представлення: IP-адреси - це двійкові числа, представлені в десятковій формі для легшого читання людьми. Десяткові числа від 0 до 255,

розділені крапками (наприклад, 192.168.1.1), однозначно ідентифікують кожен пристрій для точної маршрутизації пакетів даних.

Пунктирна десяткова система числення: цей формат складається з чотирьох наборів десяткових чисел, розділених крапками, відомих як октети (наприклад, 172.XX.YY. ZZ). Кожен октет представляє вісім бітів або один байт у двійковій системі числення.

Маршрутизація пакетів даних: коли ви надсилаєте інформацію через Інтернет або локальну мережу (LAN) перед її передачею, вона розбивається на менші блоки, які називаються пакетами даних. Мережі використовують маршрутизатори та комутатори для надсилання пакетів даних, покладаючись на IP-адреси для належної доставки.

Щоб підтримувати ефективний зв'язок між пристроями, також існує важлива відмінність між публічними та приватними IP-адресами. Публічні IP-адреси призначаються вашим інтернет-провайдером і дозволяють доступ з будь-якого місця в Інтернеті. З іншого боку, приватні IP-адреси призначаються вашим мережевим маршрутизатором і обмежені відповідними мережами. Розуміння використання IP-адреси має важливе значення як для технічних експертів, так і для звичайних користувачів, оскільки воно відіграє вирішальну роль у загальній продуктивності Інтернету.

Протокол Інтернету (IP) – це основа зв'язку між мережами, яка з часом еволюціонувала, щоб задовольнити зростаючу кількість пристроїв, підключених до Інтернету. Дві найпоширеніші версії, які використовуються сьогодні, це IPv4 та IPv6.

IPv4, або Інтернет-протокол версії 4, був розроблений на початку 1980-х років і залишається широко використовуваним, незважаючи на свої обмеження. Він використовує 32-бітну систему адрес, що дозволяє використовувати приблизно 4,3

мільярда унікальних адрес. Оскільки все більше пристроїв підключаються до Інтернету, цей обмежений пул доступних адрес є недостатнім.

Переваги IPv4: Широко підтримується існуючою інфраструктурою та пристроями.

Недоліки IPv4: Обмежена кількість доступних IP-адрес; підвищений ризик конфліктів у сфері інтелектуальної власності через повторне використання.

У відповідь на ці виклики було представлено протокол IPv6, або Інтернет-протокол версії 6, як оновлення, яке забезпечує значно розширений адресний простір за допомогою довшої 128-бітної системи адресації. Цей новий формат може підтримувати приблизно до 340 унікальних IP-адрес – майже неймовірна кількість, розроблена з урахуванням майбутнього зростання.

Переваги IPv6: Практично необмежена поставка IP-адрес; покращені функції безпеки; Краща ефективність маршрутизації пакетів даних.

Недоліки IPv6: Повільніша швидкість впровадження через необхідність оновлення щодо сумісності апаратного та програмного забезпечення.

Міграція з IPv4 на IPv6 є складним, але важливим процесом для подальшого зростання та безпеки Інтернету. Команди IT та кібербезпеки повинні знати про ці відмінності та працювати над впровадженням IPv6, щоб гарантувати, що їхні мережі захищені від потенційної нестачі адрес у майбутньому.

Існує два основних типи IP-адрес, кожен з яких має свої унікальні характеристики та варіанти використання, розуміння відмінностей між цими типами адрес може допомогти краще керувати безпекою мережі та підключенням:

1. Публічні IP-адреси. Постачальник послуг Інтернету (ISP) призначає загальнодоступну IP-адресу пристрою, підключеному до Інтернету. Ці адреси є глобальна унікальними, тобто немає двох пристроїв, які мають однакову загальнодоступну IP-адресу. Публічні IP-адреси дозволяють підключеним пристроям взаємодіяти один з одним з будь-якого місця по всьому світу.

2. Приватні IP-адреси. І навпаки, приватні IP-адреси використовуються лише в закритих мережах, таких як підприємства та установи, і не можуть бути доступні зовнішнім сторонам. Приватні IP-адреси забезпечують обмін даними між пристроями всередині мережі відповідно до діапазонів Authority Assigned Numbers Authority (IANA). Тому доступ до них не можна отримати ззовні мережі. Приватні IP-адреси відповідають певним діапазонам, зарезервованим для цієї мети, встановленим IANA.

IPv4: 10.x.x.x, 172.16.x.x - 172.31.x.x і 192.168.x.x

IPv6: fd00::/8

3. Статичні та динамічні IP-адреси. Ще одна відмінність між IP полягає в тому, чи є вони статичними чи динамічними:

- статичні IP-адреси після призначення пристрою залишаються незмінними з часом, якщо адміністратор не змінить їх вручну;

- динамічні IP-адреси періодично змінюються, що їх призначає сервер протоколу динамічної конфігурації хоста (DHCP).

Статичні IP-адреси часто використовуються для серверів і пристроїв, яким потрібні стабільні точки доступу, тоді як динамічні IP-адреси частіше зустрічаються для резидентних користувачів або пристроїв з менш критичними мережевими функціями.

Знайти свою IP-адресу просто і можна виконати за допомогою кількох підходів. Знання різниці між публічними та приватними IP-адресами має важливе значення для точної ідентифікації обох:

1. Визначення публічної IP-адреси можна легко знайти, провівши пошук в Інтернеті. Просто слід ввести запит «яка моя IP-адреса» в будь-якій пошуковій системі, і в результаті відобразить поточну публічну IP-адресу. Крім того, можна використовувати спеціальні онлайн-інструменти, такі як WhatsMyIP.org, які

надають інформацію про публічну IP-адресу разом із додатковими деталями, такими як дані геолокації.

2. Визначення приватної IP-адреси – на комп'ютері з Windows, слід відкрити командний рядок, натиснувши клавішу Windows + R, ввівши «cmd» і натиснувши Enter. У вікні командного рядка введіть "ipconfig" і натиснути Enter. Отриманий список мережевих підключень включатиме приватні IPv4 та IPv6 адреси під відповідними заголовками. Якщо використовується операційні системи macOS або Linux, слід відкритим Термінал (macOS) або Shell (Linux), а потім ввести «ifconfig» для користувачів macOS або «ip addr show» для користувачів Linux, а потім натиснути Enter. Ця команда відображає інформацію про мережеве підключення, подібну до Windows, але може вимагати прокручування більшої кількості тексту, щоб знайти особисті IP-адреси. Можна знайти приватні IP-адреси за допомогою онлайн-інструментів, таких як WhatIsMyLocalIP.com, який працює на різних платформах, включаючи мобільні пристрої.

Проблеми безпеки IP-адреси:

1. IP-адреса, публічна чи приватна, може бути потенційною ціллю для зловмисників. Кіберзлочинці, які отримують доступ до вашої IP-адреси, можуть виконувати зловмисні дії, які можуть загрожувати вашій безпеці та конфіденційності в Інтернеті. Деякі з поширених загроз, пов'язаних із відкритими IP-адресами, включають:

2. Відстеження місцезнаходження: Кіберзлочинці можуть використовувати такі інструменти, як служби геолокації IP, щоб визначити приблизне місцезнаходження на основі публічної IP-адреси.

3. Моніторинг онлайн-активності: маючи доступ до IP-адреси, зловмисники потенційно можуть відстежувати та аналізувати веб-сайти, які були відвідані, та інші дії в Інтернеті.

4. Розподілені атаки типу «відмова в обслуговуванні» (DDoS): зловмисник може розпочати DDoS-атаку, переповнивши мережеве з'єднання надмірним трафіком за допомогою ботнетів, націлених на ваші конкретні публічні або приватні IP-адреси.

5. Витік даних і крадіжка особистих даних: якщо хакер отримує несанкціонований доступ до систем, підключених через відкриту внутрішню /приватну IP-адресу в корпоративній мережі, він може викрасти конфіденційні дані, такі як особиста інформація, що призведе до крадіжки особистих даних.

6. Ідеальні цілі для фішингових шахрайств: кіберзлочинці, які отримали чиюсь IP-адресу, з більшою ймовірністю переслідуватимуть їх за допомогою цільових кампаній електронною поштою, які виглядають законними, але містять посилання на шкідливе програмне забезпечення. При натисканні на ці посилання заражають їх комп'ютерну систему без попереджувальних знаків.

7. Як фізичні особи, так і компанії повинні зменшити ці ризики, вживаючи профілактичних заходів для захисту своїх цифрових активів від потенційної шкоди, спричиненої розкриттям їхніх відповідних IP-адрес, як загальнодоступних, так і тих, що призначені в локальних мережах.

IP-адреса схожа на цифровий відбиток пальця, що ідентифікує пристрій і місцезнаходження в Інтернеті, що необхідно для підключення до Інтернету, але створює загрозу безпеці, якщо потрапить у чужі руки.

Одним із способів, за допомогою якого зловмисник може отримати IP-адресу, є тактика соціальної інженерії, така як фішингові електронні листи або телефонні дзвінки. Вони можуть видавати себе за представників законної організації та просити перейти за посиланням або завантажити вкладення, яке містить шкідливе програмне забезпечення, призначене для збору інформації про пристрій.

Зловмисник із розвиненими хакерськими навичками може використовувати різні методи, такі як сканування портів, аналізація пакетів або використання

вразливостей у програмному забезпеченні, запущеному на вашому комп'ютері, щоб отримати доступ до вашої мережі та викрасти конфіденційні дані, включаючи IP-адреси.

Коли відвідується веб-сайти або буде користування програмами в Інтернеті, вони можуть реєструвати інформацію, зокрема файли cookie, що зберігаються у веб-переглядачах і часто містять ідентифікатори користувачів (унікальні номери, призначені сайтами), а також інші методи відстеження, які використовують рекламодавці, як-от пікселі, які відстежують переміщення користувачів на різних сторінках. Усі ці дані, зібрані протягом тривалого часу, можуть допомогти зловмиснику ідентифікувати пристрої користувачів, не знаючи їхніх IP-адрес.

Захист IP-адреси:

1. Щоб захистити свої публічні та приватні IP-адреси від доступу зловмисників, застосовуйте наведені нижче заходи, які допоможуть захистити конфіденційність і безпеку в Інтернеті.

2. Слід використовувати віртуальну приватну мережу: VPN шифрує інтернет-з'єднання та приховує фактичну IP-адресу, що ускладнює кіберзлочинцям відстеження або перехоплення ваших даних.

3. Безпечні мережі Wi-Fi: якщо можливо, слід підключатися до безпечних мереж Wi-Fi, для яких потрібні паролі. Слід уникати використання загальнодоступних точок доступу Wi-Fi, оскільки вони можуть розкрити IP-адресу вашого пристрою потенційним зловмисникам.

4. Слід уникати натискання підозрілих посилань або завантаження невідомих файлів /програм: шкідливе програмне забезпечення може містити код, призначений для виявлення або використання вразливостей системи, включаючи розкриття інформації про вашу IP-адресу.

5. Слід підтримувати програмне забезпечення в актуальному стані за допомогою регулярно встановлених виправлень безпеки: оновлювати всі

операційні системи, програми та антивірусні програми останніми виправленнями безпеки. Це допомагає запобігти використанню хакерами відомих вразливостей, які можуть призвести до виявлення конфіденційної інформації, наприклад IP-адреси особи.

7. Слід розглянути можливість використання таких інструментів, як брандмауери та системи виявлення вторгнень (IDS), для додаткового захисту від спроб несанкціонованого доступу, спрямованих як на особисті пристрої, так і на корпоративні мережі.

8. Вживаючи необхідні запобіжні заходи і впроваджуючи передові рішення з кібербезпеки, компанії можуть захистити свої цифрові активи, зберігаючи при цьому оптимальну операційну ефективність, рухаючись вперед у сучасному ландшафті загроз, що постійно розвивається.

Встановлення з’єднання між комп’ютерами в мережі здійснюється завдяки IP-адресу. Кожен комп’ютер в корпоративній мережі має окрему унікальну IP-адресу, кожен комп'ютер може мати кілька унікальних IP-адрес для випадку коли він має кілька мережевих адаптерів.

3.2.2 Маска підмережі змінної довжини

Для розуміння, що таке маскування підмереж змінної довжини (VLSM), розглянемо бізнес-приклад, припустимо, компанія зарезервувала діапазон IP-адрес 37.1.1.0/24 (256 адрес). Компанія має 5 офісів, як показано на рис. 4.1.

Завдання розбити на підмережі блок IP-адрес 37.1.1.0/24 і призначити кожному офісу підмережу IP. Давайте подивимося, які є два способи це зробити.

Перший підхід до цього завдання полягає в поділі блоку з 256 адресами на чотири підмережі рівного розміру. Ця техніка називається фіксованою довгою маскою підмережі (FLSM). Перевага цього підходу полягає в тому, що всі підмережі мають однакову маску підмережі, що робить процес дуже простим і менш схильним до помилок, нижче рис. 3.2 ілюструє цей приклад.

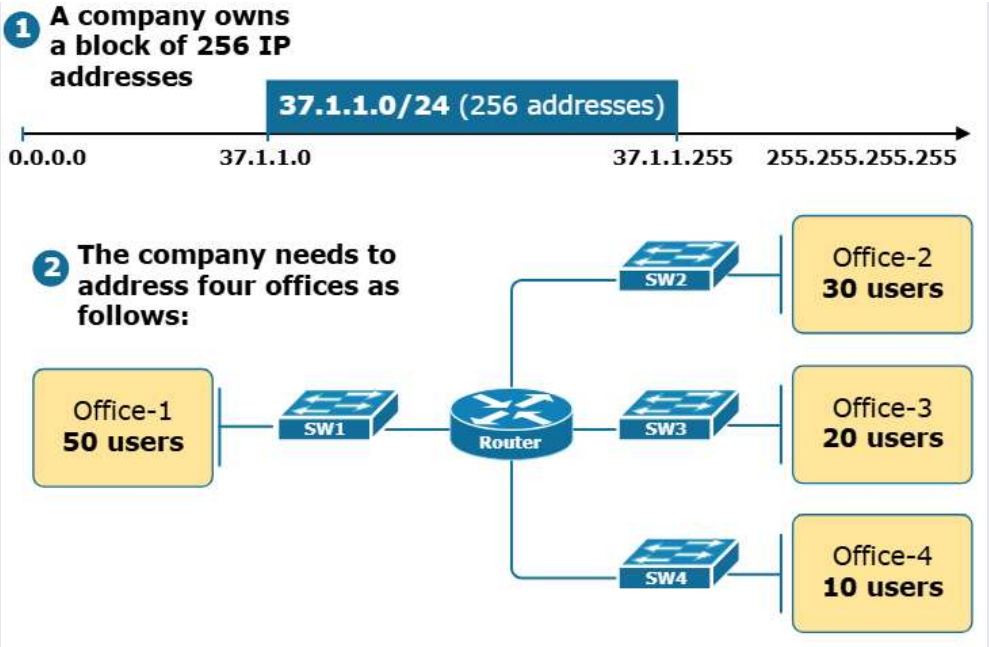


Рисунок 3.1 - Бізнес-вимоги за поділом на підмережі

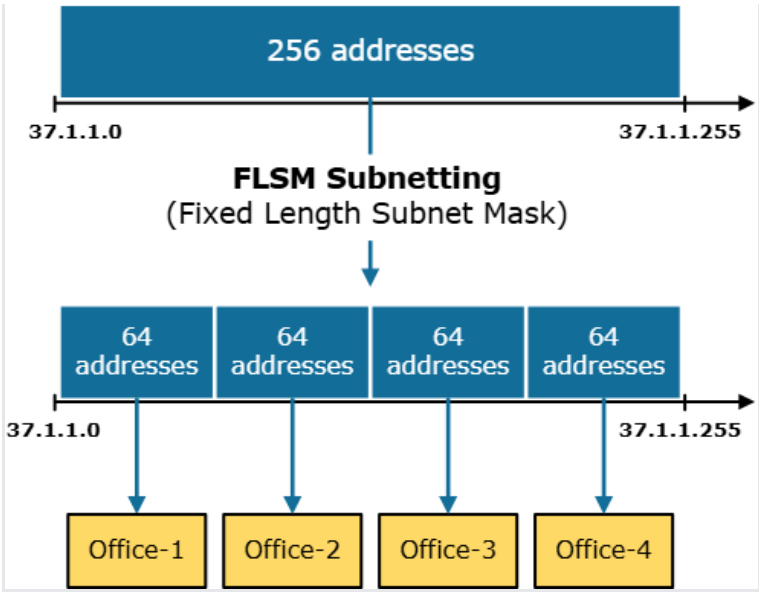


Рисунок 3.2 – FLSM поділ IP-адресації

Однак цей метод призводить до значної витрати IP-адрес. Наприклад, в office-4 всього 10 користувачів, але ми призначаємо підмережу з 64 IP-адресами. Отже, 54 адреси залишаються невикористаними. З точки зору компанії, це погане використання ресурсів.

VLSM розшифровується як маска підмережі змінної довжини. VLSM – це техніка підмережі, яка дозволяє адміністраторам мережі більш ефективно розподіляти IP-адреси за допомогою різних масок підмереж для різних сегментів мережі. Він забезпечує більшу

гнучкість у призначенні IP-адрес шляхом створення підмереж різного розміру залежно від конкретних потреб і кількості хостів у кожній підмережі. Цей метод допомагає зменшити витрати IP-адрес і краще використовувати доступний IP-простір.

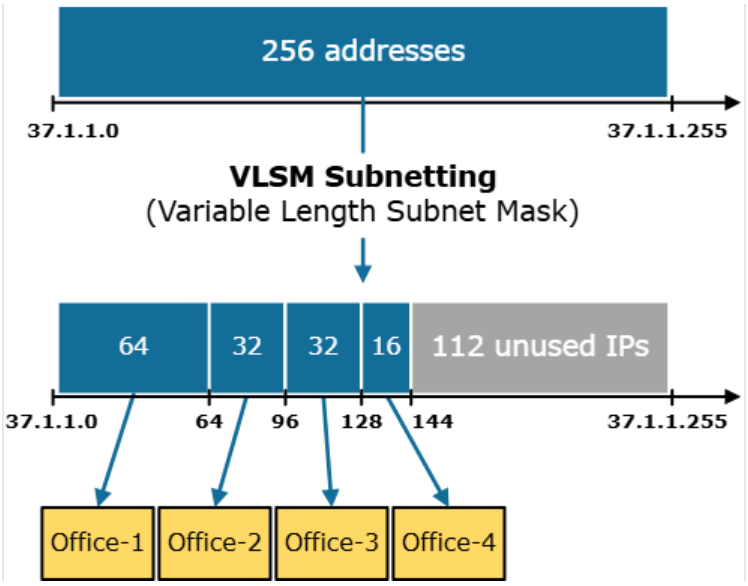


Рисунок 3.3 – VLSM поділ IP-адресації?

Зверніть увагу, що за допомогою VLSM у нас залишається 112 зайвих IP-адрес, які ми можемо виділити в інше місце в майбутньому. У порівнянні з підходом FLSM, цей метод набагато ефективніший. Основна ідея полягає в тому, що VLSM дозволяє розділити простір IP-адрес на підмережі різного розміру залежно від конкретних вимог кожного офісу. Це допомагає мінімізувати витрати IP-адрес, оскільки кожній підмережі призначається лише необхідна кількість IP-адрес замість використання підмереж фіксованого розміру, які можуть бути занадто великими або занадто малими для цієї мети.

З іншого боку, єдиним мінусом такого підходу є його складність. Метод підмережі VLSM вимагає більш складного планування, проектування та адміністрування, ніж підхід FLSM. Якщо не ретельно планувати заздалегідь, як поділити на підмережі блоки IP-адрес, то можна отримати фрагментацію IP-адрес, тобто деякі діапазони IP-адрес можуть бути між собою «конфліктними».

У табл. 3.1 порівнюються обидва методи. [13]

Таблиця 3.1 - Методи FLSM та VLSM

Підмережа FLSM (маски підмережі фіксованої довжини)	Підмережа VLSM (маски підмережі змінної довжини)
Одна мережа поділяється на кілька підмереж однакового розміру.	Одна мережа розділена на кілька підмереж різного розміру.
Кожна підмережа містить рівну кількість хостів.	Кількість хостів у кожній підмережі варіюється.
Одна і та ж маска підмережі використовується для всіх підмереж.	Для кожної підмережі використовуються різні маски підмережі.
Конфігурація та адміністрування прості.	Конфігурація та адміністрування є більш складними.
Цей метод призводить до значної витрати IP-адрес.	Втрати IP-адреси зведені до мінімуму.

VLSM підтримує декілька протоколів безкласових протоколів маршрутизації: RIP v2, EIGRP, OSPF, BGP.

3.3 Розрахунок схеми адресації корпоративної мережі будівельного інституту

Використовуючи VLSM калькулятор можна швидко та ефективно налаштувати мережу.

Кількість вузлів в підмережах L1…L5 наведена табл. 3.2.

Таблиця 3.2 – Кількість вузлів в підмережах корпоративної мережі будівельного інституту

Підмережі	L1	L2	L3	L4	L5
Кількість хостів	22	14	42	47	62

Результат розрахунку для корпоративної мережі будівельного інституту з використанням заданого блоку адрес 10.23.44.0/22 для підмереж L1…L5 представлено в табл. 3.2.

Таблиця 3.3 – Розподіл адресів для L1…L5 корпоративної мережі будівельного інституту

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast
L5	5O	62	12	10.23.0.0	/26	255.255.255.192	10.23.0.1 - 10.23.0.62	10.23.0.63
L4	38	47	24	10.23.0.64	/26	255.255.255.192	10.23.0.65 - 10.23.0.126	10.23.0.127
L3	37	42	25	10.23.0.128	/26	255.255.255.192	10.23.0.129 - 10.23.0.190	10.23.0.191
L2	15	14	15	10.23.0.192	/27	255.255.255.224	10.23.0.193 - 10.23.0.222	10.23.0.223
L1	13	22	1	10.23.0.224	/28	255.255.255.240	10.23.0.225 - 10.23.0.238	10.23.0.239

Таблиця 3.4 – Розподіл адресів для WAN1…WAN5 корпоративної мережі будівельного інституту

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast
WAN1	2	2	0	10.0.8.0	/30	255.255.255.252	10.0.8.1 - 10.0.8.2	10.0.8.3
WAN2	2	2	0	10.0.8.4	/30	255.255.255.252	10.0.8.5 - 10.0.8.6	10.0.8.7
WAN3	2	2	0	10.0.8.8	/30	255.255.255.252	10.0.8.9 - 10.0.8.10	10.0.8.11
WAN4	2	2	0	10.0.8.12	/30	255.255.255.252	10.0.8.13 - 10.0.8.14	10.0.8.15
WAN5	2	2	0	10.0.8.16	/30	255.255.255.252	10.0.8.17 - 10.0.8.18	10.0.8.19
WAN6	2	2	0	209.165.13.0	/30	255.255.255.252	209.165.13.1 - 209.165.13.2	209.165.13.3
WAN7	2	2	0	64.100.13.0	/30	255.255.255.252	64.100.13.1 - 64.100.13.2	64.100.13.3

Таблиця 3.5 – Схема адресації підмережі мережі VLAN

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast
VLAN20	14	14	0	10.23.0.128	/28	255.255.255.240	10.23.0.129 - 10.23.0.142	10.23.0.143
VLAN30	14	14	0	10.23.0.144	/28	255.255.255.240	10.23.0.145 - 10.23.0.158	10.23.0.159
VLAN40	14	14	0	10.23.0.160	/28	255.255.255.240	10.23.0.161 - 10.23.0.174	10.23.0.175
VLAN50	14	14	0	10.23.0.176	/28	255.255.255.240	10.23.0.177 - 10.23.0.190	10.23.0.191

Таблиця 3.6 – Схема адресації підмережі мережі VLAN

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast
Remount	2	2	0	209.165.202.0	/29	255.255.255.252	209.165.202.1 - 209.165.206.	209.165.202.7

Таблиця 3.7 – Адресація корпоративної мережі будівельного інституту

Ім'я пристрою	Інтерфейс	IP-адреса	Маска	Шлюз
Маршрутизатори				
R_Didenko_0	Fa0/0	10.23.0.64	/26	-
	Se0/1/0	64.100.13.1	/30	-
R_Didenko_1	Fa0/1	10.23.0.193	/27	-
	Fa0/0	10.23.0.129	/26	-
	Se0/1/0	10.0.8.17	/30	-
	Se0/1/1	10.0.8.9	/30	-
R_Didenko_2	Fa0/0	10.23.0.225	/28	-
	Se0/1/0	10.0.8.1	/30	-
	Se0/1/1	10.0.8.5	/30	-
R_Didenko_3	Fa0/0	10.23.0.129	/26	-
	Se0/1/0	10.0.8.2	/30	-
	Se0/1/1	10.0.8.14	/30	-
	Se0/3/0	10.0.8.10	/30	-
	Se0/3/1	209.165.13.2	/30	-
R_Didenko_4	Se0/1/0	10.0.8.13	/30	-
	Se0/1/1	10.0.8.17	/30	-
	Se0/3/0	10.0.8.6	/30	-
R_Didenko_SPS	Fa0/0	209.165.202.1	/29	-
	Se0/1/0	209.165.13.2	/30	-
	Se0/1/1	64.100.13.1	/30	-
LAN1				
L1PC0	Fa0	10.23.0.225	/28	10.23.0.224
L1PC1	Fa0	10.23.0.226	/28	10.23.0.224
L1PC2	Fa0	10.23.0.227	/28	10.23.0.224
L1PC3	Fa0	10.23.0.228	/28	10.23.0.224
L1PC4	Fa0	10.23.0.229	/28	10.23.0.224
L1PC5	Fa0	10.23.0.230	/28	10.23.0.224
L1PC6	Fa0	10.23.0.231	/28	10.23.0.224
L1PC7	Fa0	10.23.0.232	/28	10.23.0.224
Server_HTTP	Fa0	10.23.0.240	/28	10.23.0.224
LAN2				
L2PC0	Fa0	10.23.0.194	/27	10.23.0.192
L2PC1	Fa0	10.23.0.195	/27	10.23.0.192
L2PC2	Fa0	10.23.0.196	/27	10.23.0.192
L2PC3	Fa0	10.23.0.197	/27	10.23.0.192
LAN3				
L3PC0	Fa0	10.23.0.129	/26	10.23.0.128
L3PC1	Fa0	10.23.0.130	/26	10.23.0.128
L3PC2	Fa0	10.23.0.145	/26	10.23.0.128
L3PC3	Fa0	10.23.0.146	/26	10.23.0.128
L3PC4	Fa0	10.23.0.161	/26	10.23.0.128
L3PC5	Fa0	10.23.0.162	/26	10.23.0.128
L3PC6	Fa0	10.23.0.177	/26	10.23.0.128

Продовження таблиці 3.7

L3PC7	Fa0	10.23.0.176	/26	10.23.0.128
LAN4				
L4PC0	Fa0	10.23.0.65	/26	10.23.0.64
L4PC1	Fa0	10.23.0.66	/26	10.23.0.64
L4PC2	Fa0	10.23.0.67	/26	10.23.0.64
L4PC3	Fa0	10.23.0.68	/26	10.23.0.64
Server_TFTP	Fa0	10.23.0.69	/26	10.23.0.64
LAN5				
L5PC0	Fa0	10.23.0.129	/26	10.23.0.128
L5PC1	Fa0	10.23.0.130	/26	10.23.0.128
L5PC2	Fa0	10.23.0.131	/26	10.23.0.128
L5PC3	Fa0	10.23.0.132	/26	10.23.0.128
Provider				
LRemountPC0	Fa0	209.165.202.2	/29	209.165.202.0
LRemountPC1	Fa0	209.165.202.3	/29	209.165.202.0
LRemountPC2	Fa0	209.165.202.4	/29	209.165.202.0
LRemountPC3	Fa0	209.165.202.5	/29	209.165.202.0
LRemountPC4	Fa0	209.165.202.6	/29	209.165.202.0

Розрахуємо IP-адресацію між маршрутизаторами для визначення підмереж між WAN1…WAN7 маршрутизаторами корпоративної мережі будівельного інституту.

Максимальна кількість хостів в підмережах WAN1…WAN7 дорівнює. 2, замінено блок адрес 10.0.8.0/24 блок адрес 10.0.8.0/30.

Результат розподілу IP-адрес для підмереж WAN1…WAN7 показано в табл. 3.4.

Розрахуємо IP-адресацію в підмережі LAN3 для в мережі VLAN, яка складається мінімум з 42 комп'ютерів, для чотирьох підмереж: WLAN20, WLAN30, WLAN40 та WLAN5O (резерв) із застосуванням розрахованого блоку адрес для L3 з табл. 3.3 10.23.0.128/26.

Результат розподілу IP-адрес для чотирьох підмереж VLAN20, VLAN30, VLAN40 та VLAN5O представлено в табл. 3.4.

Розрахуємо SP-адресацію для підмережі провайдера IPS, що має в своєму складі 4 комп'ютерів під назвою Remount. При розрахунку IP-адресації для

підмережі провайдера IPS застосовано блоку адрес 209.165.202.O/30. Схема IP-адресації для пристроїв підмережі наведена в табл. 3.5.

3.4 Розробка топологічної схеми корпоративної мережі будівельного інституту

Розроблена топологічна схема корпоративної мережі будівельного інституту, яка показана на рис. 3.4.

3.5 Налаштування корпоративної мережі будівельного інституту

Для корпоративної мережі будівельного інституту, відповідно до технічних вимог, застосовано дистанційно-векторний протокол, з номером автономної системи 6 (протокол динамічної маршрутизації типу EIGRP).

При налаштуванні маршрутизації на роутерах даної корпоративної мережі будівельного інституту, на serial-інтерфейсах, згідно з технічними умовами, встановлено пропускну здатність на рівні 128 кб/с , вага метрики становить 7 500, а та швидкість каналу 128’000.

R_Didenko_4(config)#interface s0/1/0;

R_Didenko_4(config-if)#bandwidth 128;

R_Didenko_4(config-if)# clock rate 128000.

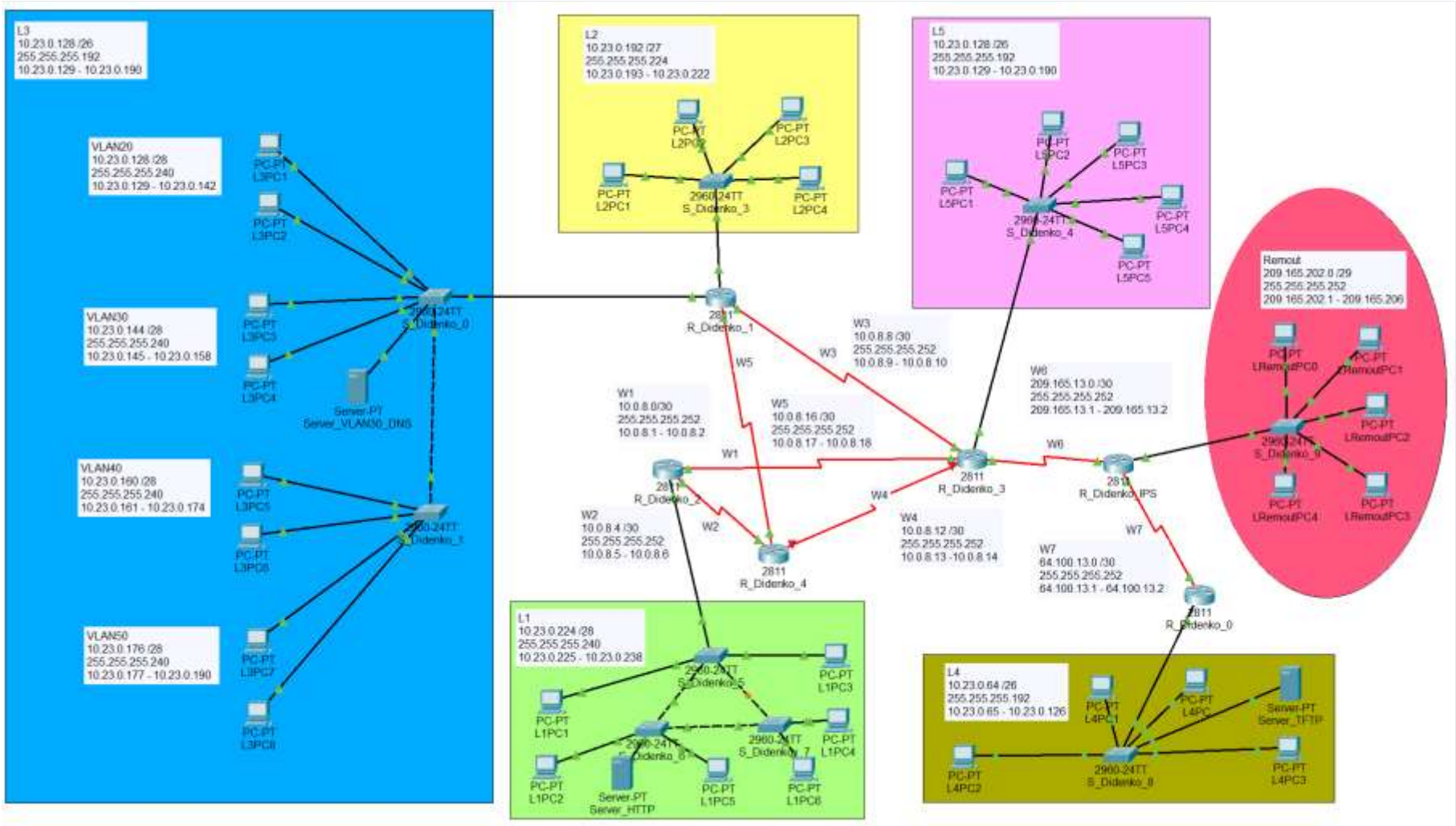


Рисунок 3.3 – Топологічна схема корпоративної мережі будівельного інституту

3.6 Налаштування та перевірка роботи корпоративної мережі будівельного інституту

3.6.1 Базове налаштування пристроїв корпоративної мережі будівельного інституту

Налаштування базової конфігурації активних мережних пристроїв включає наступні кроки:

- застосувати сервісу для шифрування паролів;

- захисти привілейований режиму ОС для консольного порту та ліній vty;

- призначити інформацію для банера MOTD;

- для віддаленого доступу до пристрою на лініях vty застосувати протокол SSH;

- створити локальні облікові записи (username 123211_Didenko) з паролем admincisco123211;

- створити доменне ім’я пристрою (ip domain-name R_Didenko_1);

- створити ключ RSA завдовжки 1024 біт для шифрування даних.

Приклад базових налаштувань на роутері R_Didenko_1:

- заборонити пошук DNS на маршрутизаторі: Router(config)#no ip domain-lookup;

- задання пристрою унікального імені: Router(config)#hostname R_Didenko_1;

- зашифрувати всі паролі, що зберігаються у відкритому вигляді: R_Didenko_1(config)#service password-encryption;

- встановити пароль на вхід до привілейованого режиму: R_Didenko_1(config)#enable secret class123211;

- встановити пароль на вхід до консольної лінії: R_Didenko_1(config)#line console 0, R_Didenko_1(config-line)#password cisco123211;

- налаштувати запит пароля при вході: R_Didenko_1(config-line)#login, R_Didenko_1(config-line)#exit;

- налаштувати банер MOTD: R_Didenko_1(config)#banner motd # 123211 Didenko. Enter only have key#;

- налаштувати протокол створення користувача SSH: R_Didenko_1(config)#username 123211_Didenko password admincisco;

- створити домен: R_Didenko_1(config)#ip domain-name R_Didenko_1;

- створити ключ RSA довжиною 1024 біт для шифрування даних: R_Didenko_1(config)#crypto key generate rsa, How many bits in the modulus [512]: 1024, % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

- налаштувати лінії VTY: R_Didenko_1(config)#line vty 0 4;

- встановити необхідність введення логіну та пароля для входу лінії: R_Didenko_1(config-line)#login local;

- встановити протоколу SSH для входу на лінію: R_Didenko_1(config-line)#transport input ssh;

- встановити IPv4-адрес відповідно до табл. 3.4: R_Didenko_1(config)#interface g0/1, R_Didenko_1 (config-if)# ip address 10.22.208.1 255.255.255.0;

- запустити інтерфейсу до початку роботи (обов'язково увімкнути): R_Didenko_1(config-if)#no shutdown.

3.6.2 Налаштування маршрутизаторів корпоративної мережі будівельного інституту

Приклад налаштування маршрутизації на R_Didenko_2:

- включення протоколу EIGRP на маршрутизаторі: R_Didenko_2(config)#router eigrp 6, R_Didenko_2(config-router)#)#eigrp router-id 8.8.8.8;

- об'явлення мережі, підключення до маршрутизатора: R_Didenko_2(config-router)#network 10.0.6.1 0.0.0.3, R_Didenko_2(config-router)#network 10.23.209.0 0.0.0.255;

- завдання інтерфейсу, на який не надсилаються оновлення для таблиці маршрутизації: R_Didenko_2(config-router) #passive-interface G0/1;

- встановлення маршруту за замовчуванням на R_Didenko_2: ip route 0.0.0.0 0.0.0.0 209.165.202.2;

- вимкнення підсумування маршрутів: R_Didenko_2(config-router) #no auto-summary;

зберігання файлу конфігурації роутера в енерго-незалежну пам'ять: R_Didenko_4#copy running-config startup-config;

- перевірка таблиці маршрутизації роутера командою: R_Didenko_4#show ip route;

Перевірка таблиці маршрутизації для роутера R_Didenko_2 показана на рис. 3.4, а рисунки з таблицями маршрутизації інших роутерів корпоративної мережі будівельного інституту розташовано в додатку А.

```
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 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 14 subnets, 6 masks
C       10.0.6.0/30 is directly connected, Serial0/0/0
L       10.0.6.1/32 is directly connected, Serial0/0/0
D       10.0.6.4/30 [90/21024000] via 10.0.6.2, 00:29:02, Serial0/0/0
D       10.0.6.8/30 [90/21024000] via 10.0.6.2, 00:07:00, Serial0/0/0
D       10.22.208.0/24 [90/21024256] via 10.0.6.2, 00:29:02, Serial0/0/0
C       10.22.209.0/24 is directly connected, GigabitEthernet0/1
L       10.22.209.1/32 is directly connected, GigabitEthernet0/1
D       10.22.210.0/24 [90/21024256] via 10.0.6.2, 00:06:54, Serial0/0/0
D       10.22.211.0/27 [90/20519680] via 10.0.6.2, 00:08:29, Serial0/0/0
D       10.22.211.32/27 [90/20519680] via 10.0.6.2, 00:08:29, Serial0/0/0
D       10.22.211.64/27 [90/20519680] via 10.0.6.2, 00:08:29, Serial0/0/0
D       10.22.211.96/28 [90/20519680] via 10.0.6.2, 00:08:29, Serial0/0/0
C       10.22.211.128/26 is directly connected, GigabitEthernet0/2
L       10.22.211.129/32 is directly connected, GigabitEthernet0/2
D    53.0.0.0/8 [90/20517120] via 10.0.6.2, 00:29:03, Serial0/0/0
D    64.0.0.0/8 [90/20517120] via 10.0.6.2, 00:08:30, Serial0/0/0
D    209.165.202.0/24 [90/20514560] via 10.0.6.2, 00:29:03, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Рисунок 3.4 – Таблиця маршрутизації на R_Didenko_2 корпоративної мережі будівельного інституту

3.6.3 Налаштування роботи Інтернет корпоративної мережі будівельного інституту

Протокол NAT на прикордонному маршрутизаторі корпоративної мережі будівельного інституту налаштовано наступним чином:

- діапазон пул адрес становить: 10.23.0.65 - 10.23.0.126;
- IP-адреса 10.23.0.126 та маска 255.255.255.192 Server HTTP;
- номер списку доступу: 6;
- ім'я пулу: Internet.

Приклад налаштування NAT на R_Didenko_3:

- список параметрів налаштування контролю доступу, які дозволяють всі можливі IP- адреси для внутрішньої мережі: R_Didenko_3(config)# access-list 6 permit 10.22.208.0 0.0.7.255;

- пул для динамічного виділення інтернет IP-адрес: R_Didenko_3(config)#ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224;

- підмінаIP-адреси для внутрішньої мережі на інтернет IP-адреси згідно з списком контролю доступу: R_Didenko_3(config)#ip nat inside source list 6 pool Internet;

- IP-адреса статичного NAT для серверу HTTP: R_Didenko_3(config)#i ip nat inside source static 10.22.210.10…209.165.200.5;

- призначення інтерфейсу для вихідного для трафіку з мережі приватних IP-адрес: R_Didenko_3(config)#interface F4/0, R_Didenko_3(config-if)#ip nat outside;

- призначення інтерфейсу в якості вхідного для трафіку з мережі приватних адрес: R_Didenko_3(config-if)#interface Serial2/0, R_Didenko_3(config-if)#ip nat inside.

Перевірка роботи NAT-перетворювань показана на рис. 3.5.

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.202.5:3	10.22.209.15:3	10.22.211.11:3	10.22.211.11:3
icmp	209.165.202.5:4	10.22.209.15:4	10.22.211.11:4	10.22.211.11:4
icmp	209.165.202.5:5	10.22.209.15:5	53.1.9.10:5	53.1.9.10:5
icmp	209.165.202.6:1	10.22.211.145:1	10.22.211.44:1	10.22.211.44:1
icmp	209.165.202.6:2	10.22.211.145:2	10.22.211.44:2	10.22.211.44:2
icmp	209.165.202.6:3	10.22.211.145:3	53.1.9.10:3	53.1.9.10:3
---	209.165.202.3	10.22.210.10	---	---

Рисунок 3.5 – Таблиця перетворювань NAT на R_Didenko_3 корпоративної мережі будівельного інституту

3.6.4 Перевірка роботи корпоративної мережі будівельного інституту

Пінгування комп'ютерів між підмережами LAN5 та LAN1 корпоративної мережі будівельного інституту.

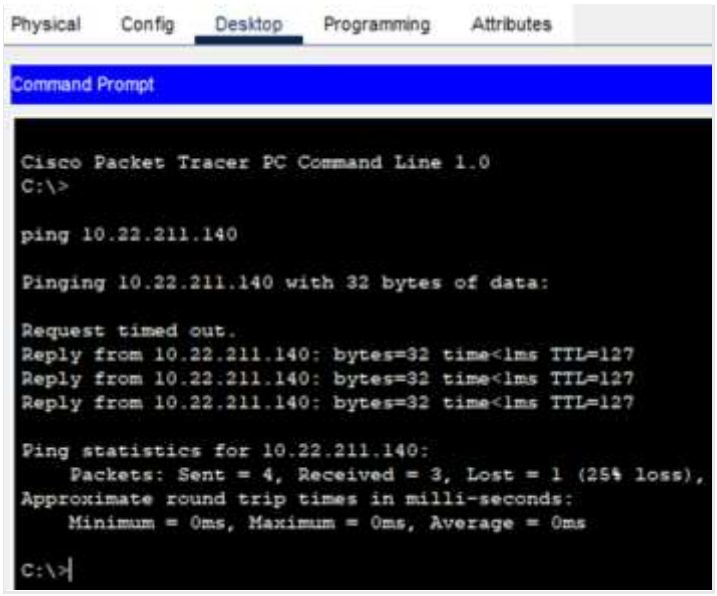


Рисунок 3.6 – Результат команди «ping» між корпоративними мережами будівельного інституту

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	GL_Agronom.	Gl_Engineer	ICMP		0.000	N	0	(edit)	
	Successful	Admin_IT	Director	ICMP		0.000	N	1	(edit)	
	Successful	Admin_IT	Brigadir	ICMP		0.000	N	2	(edit)	
	Successful	Admin_IT	Tehnolog	ICMP		0.000	N	3	(edit)	

Рисунок 3.7 – Пінгування хостів корпоративної мережі будівельного інституту засобами PacketTracer

Перевірка SSH підключення з командного рядка Gl_Engineer з підмережі «LAN4» до маршрутизатора R_Didenko_1 від користувача 123211_Didenko з паролем admincisco123211 командою ssh –l username ip-address показана на рис. 3.8.

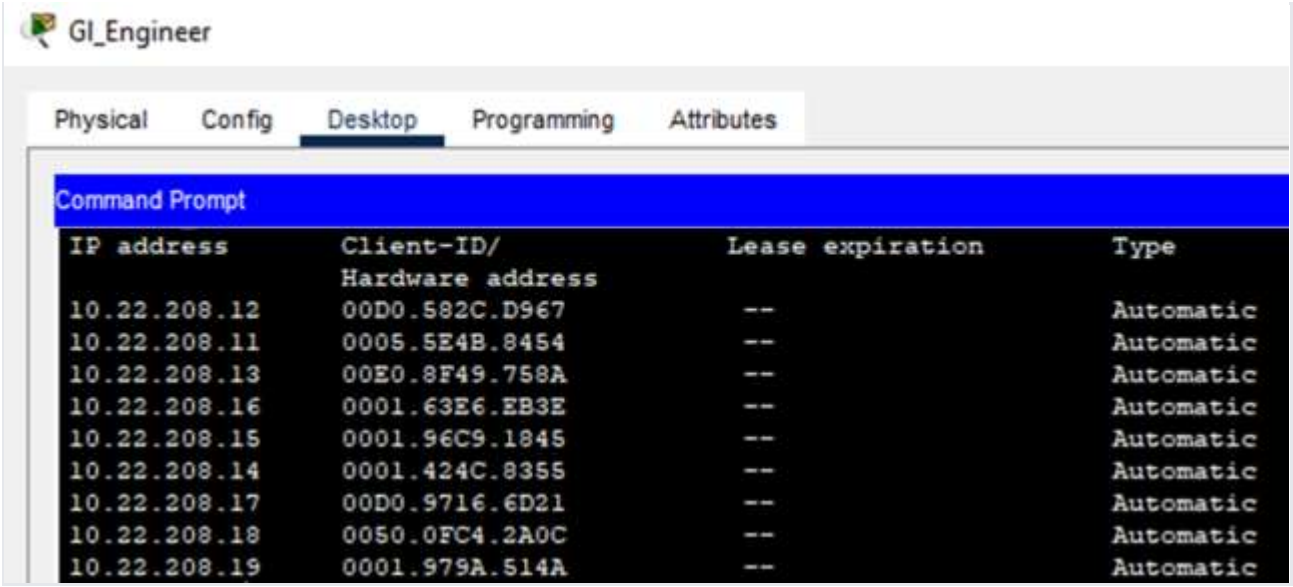


Рисунок 3.8– Перевірка підключення до маршрутизатора R_Didenko_1 корпоративної мережі будівельного інституту за допомогою протоколу SSH

В підмережі «LAN1» корпоративної мережі будівельного інститутуна комутаторах виконано об'єднання фізичних портів f0/1-4 в port-channel (агрегування каналів). Для цього застосовано для агрегування каналів PAgP в якості канального протоколу. Port Aggregation Protocol (PAgP) – це протокол компанії Cisco Systems, який спеціально служить для автоматичного агрегування фізичних Ethernet портів комутатора в один логічний порт. Агрегування каналів

підмережі LAN1 виконане для збільшення пропускної здатності та організації належної надійності для каналів між трьома комутаторами.

Усі канали комутаторів в працюють активному стані, крім одного - канал f0/3-4 є запасним каналом, який перейде в активний стан, якщо основні канали раптом стануть неактивними. Цей канал призначений в якості запасного за допомогою протоколу spanning-tree.

Було успішно створено два порт-канали, один з яких об'єднує порти Fa0/1-2, а інший – Fa0/3-4. На рис. 3.9 показано результат налаштування агрегації каналів за допомогою PAgP на для комутатора S_Didenko_2.

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


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

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

1      Po1(SU)           PAgP   Fa0/1(P) Fa0/2(P)
3      Po3(SD)           PAgP   Fa0/3(I) Fa0/4(I)
```

Рисунок 3.9 – Налаштування агрегації каналів на S_Didenko_2 корпоративної мережі будівельного інституту

В підмережах корпоративної мережі будівельного інституту хости в мережі налаштовані за протоколом DHCP.

Приклад налаштування DHCP на R_Didenko_2 (R_Didenko_2(config)#interface g0/1):

- активовано протокол DHCP: R_Didenko_2(config-if)#service DHCP;

- створений пул DHCP з ім'ям Organization_department: R_Didenko_2(config-if)#ip dhc pool LAN1;

- вилучено з пулу перші 10 адрес: R_Didenko_2(config-if)#ip dhc ex 10.22.211.129 10.22.211.139;

- зазначена мережа і шлюз за замовчуванням: R_Didenko_2(config-if)#net 10.22.111.128 255.255.255.192, R_Didenko_2(config-if)#def 10.22.211.129, R_Didenko_2(config-if)#dns 10.22.210.10

IP address	Client-ID/ Hardware address	Lease expiration	Type
10.22.209.12	0001.4243.2DE6	--	Automatic
10.22.209.13	0007.ECD3.27E4	--	Automatic
10.22.209.14	0090.21A2.01EA	--	Automatic
10.22.209.11	00E0.F9E1.81DE	--	Automatic
10.22.209.15	0009.7C42.630E	--	Automatic
10.22.209.16	000C.8512.A747	--	Automatic
10.22.209.17	00D0.BA2B.4745	--	Automatic
10.22.209.18	000C.CF2B.9001	--	Automatic
10.22.211.141	0001.4214.C6C4	--	Automatic
10.22.211.140	00D0.97D3.5C3C	--	Automatic
10.22.211.142	0030.A349.87E6	--	Automatic
10.22.211.143	000A.F37D.0793	--	Automatic
10.22.211.144	0040.0B9C.7B22	--	Automatic
10.22.211.145	00E0.F93A.9B8A	--	Automatic
10.22.211.146	0060.3EC1.B4A4	--	Automatic
10.22.211.147	0007.EC4C.88DB	--	Automatic
10.22.211.148	0030.F294.C618	--	Automatic
10.22.211.149	0002.179A.8CE9	--	Automatic
10.22.211.150	00E0.8F03.DA94	--	Automatic
10.22.211.151	0060.7013.10C4	--	Automatic

Рисунок 3.10 – Таблиця призначення IP-адрес вузлам корпоративної мережі будівельного інституту за протоколом DHCP

3.7 Захист інформації в корпоративної мережі будівельного інституту від несанкціонованого доступу

3.7.1 Розробка методів для захисту інформації в корпоративної мережі будівельного інституту

Наведемо приклад послідовності налаштування сервісу AAA та серверу RADIUS на маршрутизаторі R_Didenko_4:

- запуск служби AAA: R_Didenko_4(config)#aaa new-model;

- налаштування методу аутентифікації з використання локальної бази користувачів: R_Didenko_4(config)#aaa authentication login default local;

- налаштування методу аутентифікації Login на сервері Radius, а якщо він недоступний, то з використанням локальної бази користувачів: R_Didenko_4(config)#aaa authentication login Login group radius local;

- застосування методу аутентифікайфії Login на консольній лінії та vty: R_Didenko_4(config)#line console 0, R_Didenko_4(config-line)#login authentication Login, R_Didenko_4(config)#line vty 4, R_Didenko_4(config-line)#login authentication default;

- налаштування RADIUS-серверу: R_Didenko_4(config)#radius-server host 10.22.210.10 auth-port 1645, R_Didenko_4(config)#radius-server key Radius + Didenko_123211.

Для доступу використовується доменне ім’я пристрою R_Didenko_4 з паролем Radius + Didenko_123211, що був попередньо налаштований на сервері Radius.

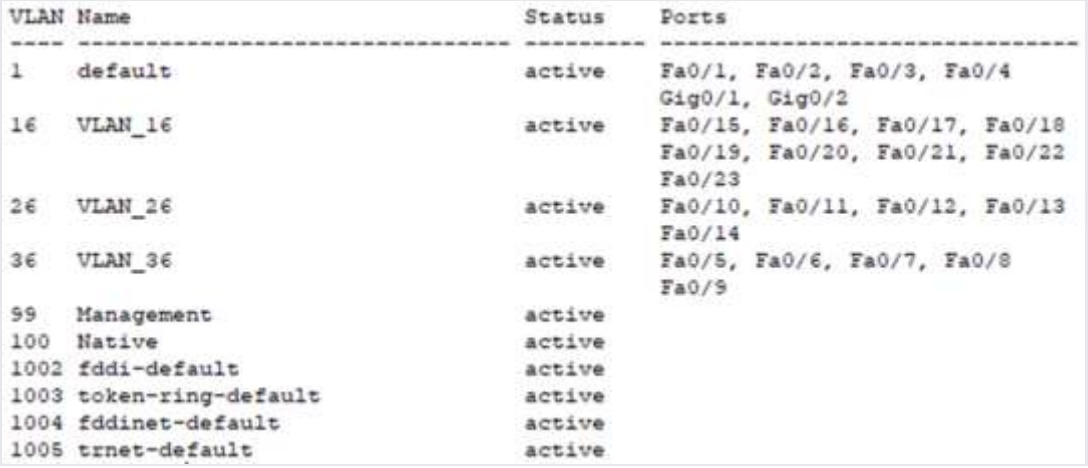
На портах комутатора, де підключені сервери корпоративної мережі будівельного інституту, налаштовані наступні засоби безпеки: тільки одному вузлу дозволено доступ до порту, MAC-адреса пристрою додається статично в поточну конфігурацію, а при порушенні системи безпеки порт виключається.

3.7.2 Налаштування мережах VLAN та параметрів безпеки комутаторів корпоративної мережі будівельного інституту

Згідно з технічними вимогами в підмережі «Департамент маркетингу» корпоративної мережі будівельного інституту були створені три окремі підмережі VLAN.

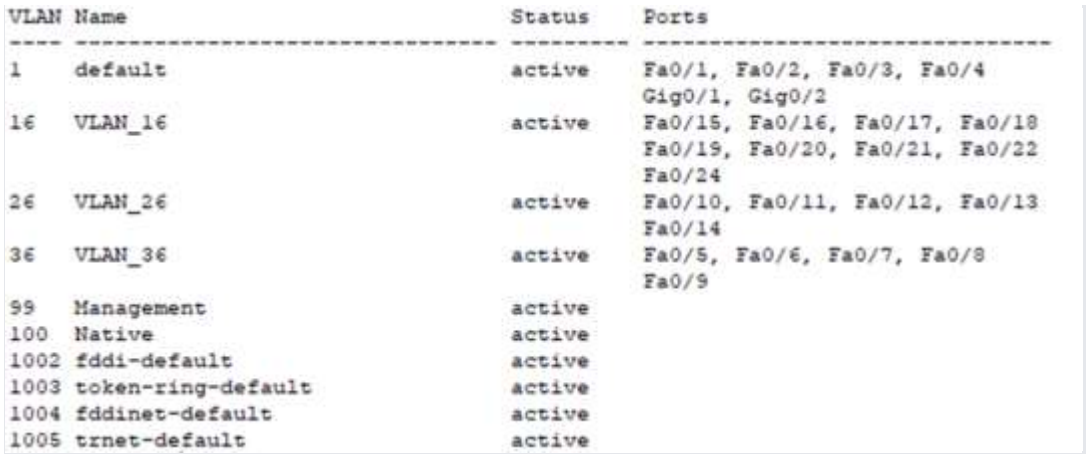
Таблиця 3.8 – Назви VLAN для підмережі корпоративної мережі будівельного інституту

Номер VLAN	Ім'я VLAN	Назва департаменту
16	VLAN20	Департамент сервісного обслуговування
26	VLAN30	Департамент зовнішньої реклами
36	VLAN40	Департамент продажу
99	VLAN5O	Департамент аналізу та розвитку перспективних напрямків



```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Gig0/1, Gig0/2
16   VLAN_16                           active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23
26   VLAN_26                           active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14
36   VLAN_36                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9
99   Management                        active
100  Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 3.11 – Налаштування VLAN на S_Didenko_0 корпоративної мережі будівельного інституту



```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Gig0/1, Gig0/2
16   VLAN_16                           active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/24
26   VLAN_26                           active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14
36   VLAN_36                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9
99   Management                        active
100  Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 3.12 – Налаштування VLAN S_Didenko_1 корпоративної мережі будівельного інституту

На рис. 3.11-рис.3.13 наведено розподіл портів для комутаторів за віртуальними мережами, які було створено та призначені інтерфейси керування.

Налаштувати порту GigabitEthernet0/1 на маршрутизатора R_Didenko_0:

- для здійснення передачі трафіку між VLAN включена підтримка функції технології інкапсуляції 802.1Q: R_Didenko_0(config)#interface g0/1, R_Didenko_0(config-if)#no shutdown;

- налаштовано підінтерфейсу для маршрутизації трафіку між VLAN: R_Didenko_0(config)#interface g0/0.16;

Перевірка роботи порту GigabitEthernet0/1 на маршрутизатора R_Didenko_0 проведена за допомогою тегування пакетів для даного підінтерфейсу - R_Didenko_0(config-subif)#encapsulation dot1Q 16 //, R_Didenko_0(config-subif)#ip address 10.22.211.1 255.255.255.224, що і показано на рис. 3.13.

Port	Link	VLAN	IP Address	IPv6 Address
GigabitEthernet0/0	Up	--	64.100.13.2/30	<not set>
GigabitEthernet0/1	Up	--	<not set>	<not set>
GigabitEthernet0/1.16	Up	--	10.22.211.1/27	<not set>
GigabitEthernet0/1.26	Up	--	10.22.211.33/27	<not set>
GigabitEthernet0/1.36	Up	--	10.22.211.65/27	<not set>
GigabitEthernet0/1.99	Up	--	10.22.211.97/28	<not set>
GigabitEthernet0/2	Down	--	<not set>	<not set>
Serial0/0/0	Down	--	<not set>	<not set>
Serial0/0/1	Down	--	<not set>	<not set>
FastEthernet0/1/0	Up	1	--	<not set>
FastEthernet0/1/1	Up	1	--	<not set>
FastEthernet0/1/2	Up	1	--	<not set>
FastEthernet0/1/3	Up	1	--	<not set>
Vlan1	Down	1	<not set>	<not set>

Рисунок 3.13 – Перевірка налаштування 802. 1Q на R_Didenko_0 корпоративної мережі будівельного інституту

Таким чином можна вважати, що інкапсуляція 802. 1Q R_Didenko_0 для корпоративної мережі будівельного інституту повністю налаштована.

3.8 Висновки за розділом

В розділі розробка корпоративної мережі, поставлено завдання по створенню корпоративної мережі будівельного інституту, де були описані принципи IP-адресація в корпоративній мережі, проведено розрахунок схеми IP-

адресації для корпоративної мережі, розроблена топологічна схеми корпоративної мережі на базі мережевих продуктів Cisco, проведено налаштування корпоративної мережі, здійснена перевірка роботи корпоративної мережі на симуляторі Cisco Packet Tracer та розроблені заходи з захисту інформації в корпоративної мережі від несанкціонованого доступу.

4 РОЗРОБКА СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ КОРПОРАТИВНОЇ МЕРЕЖІ БУДІВЕЛЬНОГО ІНСТИТУТУ

4.1 Додаткові сервіси корпоративної мережа комп'ютерної системи будівельного інституту

Тема кваліфікаційної роботи бакалавра комп'ютерна система для акціонерного товариства «проектно-технологічний інститут.

Розробимо система інтернету речей призначену для використання в адміністративних будівлях де корпоративна мережа будівельного інституту, яка буде підключена до Інтернету речей, та має достатню пропускну здатність для передачі значних обсягів даних.

4.2 Інтернет речі

Інтернет речі (IoT) трансформують контроль доступу до офісних будівель шляхом підключення пристроїв безпеки до централізованої корпоративної мережі, що дозволяє здійснювати моніторинг, контроль, управління для точок доступу в режимі реального часу. Це включає такі функції, як безключовий доступ, керування віддаленим доступом і сповіщення в режимі реального часу про несанкціонований доступ.

У сфері сучасної безпеки бездоганна інтеграція Інтернету речей (IoT) із системами контролю доступу змінила ландшафт захисту наших приміщень. У цій статті ми розглянемо потужне поєднання IoT і контролю доступу, досліджуючи способи, за допомогою яких пристрої з підтримкою IoT підвищують безпеку за допомогою моніторингу та аналізу даних у реальному часі.

Системи контролю доступу, які колись покладалися на традиційні методи, зазнали значної трансформації завдяки інтеграції IoT. Ця трансформація призвела до того, що системи контролю доступу стали більш ефективними, проактивними та оперативними.

Перевагою IoT є моніторинг у режимі реального часу за допомогою таких брендів, як Hikvision та Polimek. Системи відстежують переміщення, оперативно виявляючи аномалії.

Рисунок 4.1 - Інтернет речі для контролю доступу до офісних будівель

Поєднання IoT і контролю доступу надає експертам з безпеки інформацію на основі даних. Інформація з таких пристроїв, як зчитувачі контролю доступу, дає змогу прогнозувати та запобігати порушенням, розширенню можливостей сучасних будівель за допомогою централізованого керування, та централізованого підходу до безпеки.

Інтеграція IoT із системами контролю доступу відкриває можливості централізованого керування. Це дає змогу персоналу служби безпеки віддалено керувати кількома точками доступу, забезпечуючи злагоджену та синхронізовану стратегію безпеки.

Існує WEB-орієнтоване ПЗ для контролю доступу, яке є продуктом інтеграції IoT та технічного обладнання для організації обмеженого доступу, спрощує управління доступом. Він надає адміністраторам можливість ефективно контролювати та регулювати привілеї доступу в усьому приміщенні.

Обладнання IoT та контролю доступу вже є вбудованою в розумні будівлі. Ці інтелектуальні структури адаптуються до поведінки користувачів, оптимізуючи заходи безпеки та підвищуючи зручність.

Впровадження IoT у контроль доступу призводить до безперебійного входу для користувачів. Такі пристрої, як турнікети, забезпечують безконтактний доступ, забезпечуючи безпечний, але плавний процес входу.

Інтеграція технології IoT з контролем доступу підвищує безпеку та ефективність. Завдяки пристроям IoT, таким як зчитувачі контролю доступу та централізованому управлінню, сучасні будівлі захищені від загроз. Партнерство з контролю доступу до Інтернету речей змінить безпеку в розумних будівлях та за їх межами. [14]

Підприємства, які прагнуть покращити безпеку у своїх офісах, складах та інших приміщеннях, повинні керувати доступом співробітників та відвідувачів до поверхів, кімнат та інших зон будівлі. Порушення встановлених процедур може спричинити серйозні проблеми.

Сьогодні ідентифікація персоналу, біометрична верифікація, виявлення заборонених вибухових речовин, радіоактивних матеріалів та наркотиків використовуються у спеціальних критичних зонах та контрольно-пропускних пунктах (КПП) державних та військових установ. Це включає заходи щодо запобігання нападам, переміщенню заборонених предметів і матеріалів та крадіжці цінностей.

Окрім бар'єрів та турнікетів, існують наступні Інтернет речі: біометричні зчитувачі, путівники, обмеження часу подорожі та розумні замки.

Програмне забезпечення спрощує процес реєстрації для нових відвідувачів та скорочує час на перевірку прав доступу, тим самим економлячи кошти персоналу. ПЗ має бути сумісним з багатьма офісними програмами та може адаптувати управління до конкретних завдань, тим самим підвищуючи надійність та ефективність.

Рисунок 4.2 – Обладнання з інтегрованим IoT

В системі управління спочатку необхідно зупинити та «зафіксувати» контрольований об’єкт (людину). Для цього використовуються різні ворота, що входять до складу РК-керування: турнікети, призначені для різного застосування та потоків транспорту (напів-розсувні ворота, турнікети, повно-зростові ворота, ворота зі стійками), обертові двері, блокувальні ворота, хвіртки тощо. Захисні ворота встановлюються на скляних дверях та вікнах у місцях з великим потоком людей (торгові центри, автостанції, залізничні вокзали, офіси), а також у приміщеннях, пов’язаних із входами офісів, банків, лікарень, військових будівель та в’язниць. На входах та гаражних воротах встановлюються екрани.

Важливо, щоб усі контролери доступу були підключені до однієї мережі та могли взаємодіяти один з одним для отримання інформації про належну роботу системи. Інформація про кожного відвідувача чи співробітника негайно надсилається до центру керування. Програмне забезпечення SKD має численні інтерфейси для підключення до веб-сайтів та різних зовнішніх відео-дисплеїв.

Головною особливістю засобу керування є успішна інтеграція датчиків на основі різних фізичних джерел: спектральна радіометрія, пасивна та активна магнітометрія тощо.

Турнікети або бар'єри можуть бути оснащені простими зчитувачами RFID або новішими біометричними зчитувачами, які розпізнають обличчя, сканування вен долонь, відбитки пальців або інші типи інформації. У поєднанні зі зчитувачами або біометричними рішеннями бар'єри можуть бути інтегровані в системи високого рівня безпеки.

Рисунок 4.3 – Біометричні системи контролю доступу

Вони встановлені на всіх входах, головних входах, виходах та воротах, підключені до мережі компанії та підключені до центральної системи. Програмне забезпечення автоматизує реєстрацію співробітників та відвідувачів, відстежує їх прибуття та вибуття та обмежує доступ до певних кімнат, зон будівлі або до самої будівлі певним групам. Водночас система працює ефективно, значно зменшуючи кількість необхідного персоналу охорони. Комп'ютерна система значно підвищує ефективність усієї системи: вона може організовувати відвідування за скороченим графіком. Наприклад, більшість співробітників працюють з 9:00 до 20:00. [15]

4.3 Налаштування IoT обладнання та сервісів

Корпоративна мережа будівельного інституту має наступне мережеве обладнання: маршрутизатор DLC100, які використовується для всіх IoT пристроїв та кінцевих мережевих пристроїв: електричні замки в кількості чотири одиниці, смарт лампи - чотири одиниці, датчики руху - чотири одиниці, карт рідери - чотири одиниці, один персональний настільний комп'ютер, RFID мітки

для кожного співробітника та можливих декількох гостей офісу будівельного інституту «КИЇВОРГБУД.

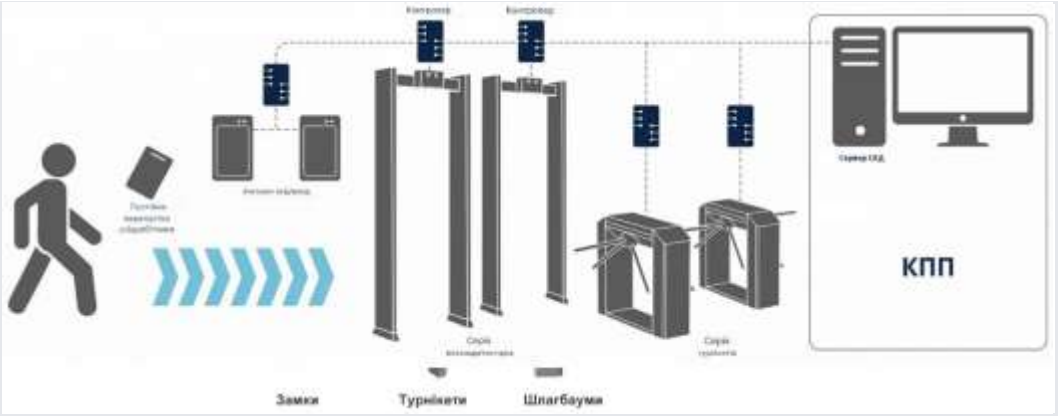


Рисунок 4.4 – Обладнання IoT для обладнання КПП

Структура системи доступу на основі IoT з точки зору взаємодії мережевих пристроїв продемонстрована на рис. 4.5.

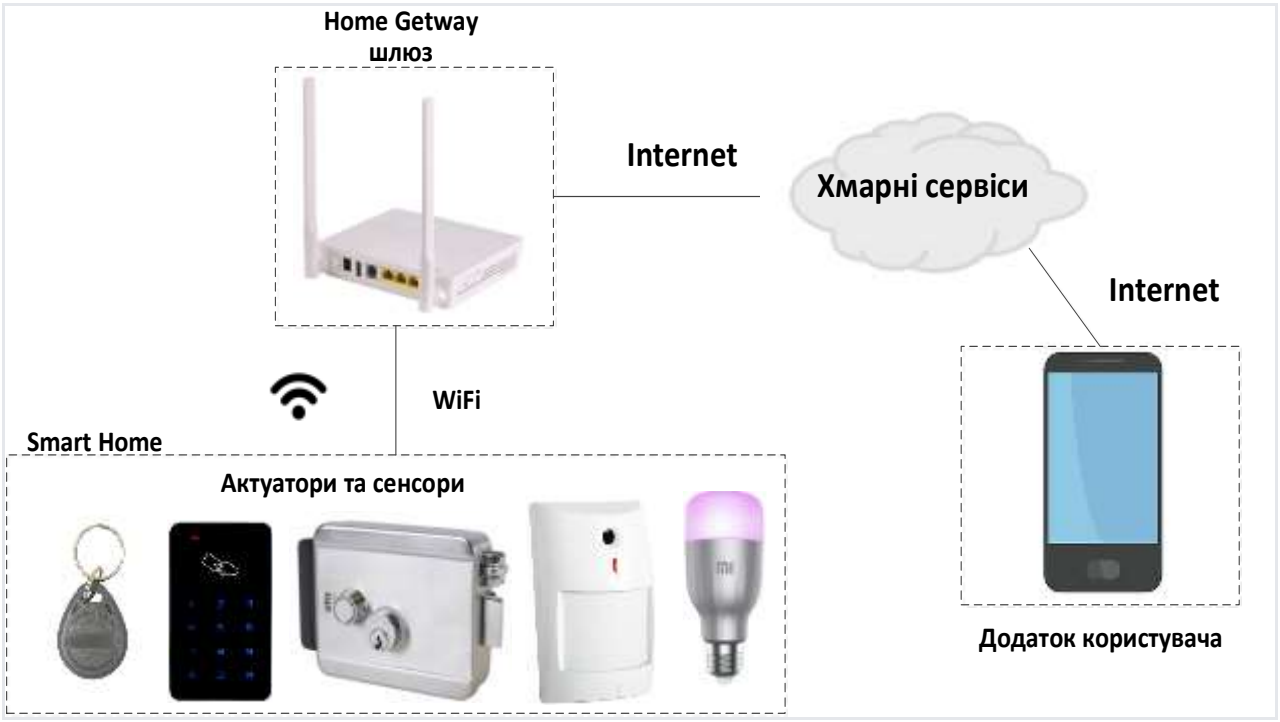


Рисунок 4.5 – Структурна схема обмеження доступу (мережа IoT) корпоративної мережі будівельного інституту

Загалом на першому етапі розробки система IoT для корпоративної мережі будівельного інституту складається з двох частин: управління освітлення за датчиком руху та зчитування інформації з RFID-пропусків.

Конфігурація зчитувачів RFID-пропусків у Packet Tracer здійснюється наступним чином:

- кожна RFID-мітка має власний унікальний ідентифікатор;

- зчитувач може знаходитися в трьох робочих станах: очікування, зчитування валідної мітки, зчитування невалідної мітки.

Розглянимо ситуацію для випадку коли ідентифікатор валідної RFID-картки знаходиться в межах діапазону можливих номерів 1 000…1 100, тоді пропуск у приміщення буде організовано за правилами: ValidCard де ID-card в межах діапазону 1 000…1 100, та In ValidCard де ID-card або більше 0, або більше 1 100, або менше 1 000.

Комунікація мережевих IoT пристроїв для корпоративної мережі будівельного інституту виконана на базі технології WiFi для базі маршрутизатора DLC100.

Для управління роботою мережі з метою отримання доступу до веб-інтерфейсу системи безпеки користувачів дуло сконфігуровано налаштування Home Gateway та IoT-сервер.

Для під’єднаних пристроїв на IoT-сервер за допомогою Home Gateway забезпечено розподіл SP-адрес з приватного блоку за допомогою протоколу DHCP.

Таблиця 4.1 – Налаштування домашнього шлюзу

Параметр	Значення
IP-адреса шлюзу IoT	192.168.25.1
маска підмережі IoT	255.255.255.0
SSID бездротової мережі IoT	Door_Security
Метод автентифікації IoT	WPA2-PSK AES
Ключ автентифікації (пароль для IoT)	Key_RFID123211

Усі IoT системи доступу до офісних приміщень будівельного інституту підключені до бездротової мережі, яку підтримує Home Gateway.

Для під'єднання до корпоративної мережі будівельного інституту на IoT налаштовані: ідентифікатор SSID, метод автентифікації, ключ автентифікації, отримання IP-адреси за DHCP, то вказаний IoT-сервер.

Усі IoT контролю доступу до офісу будівельного інституту підключені до бездротової корпоративної мережі, яку підтримує Home Gateway.

Для під'єднання до корпоративної мережі на IoT-пристроях доступу налаштовані: ідентифікатор SSID, метод автентифікації, ключ автентифікації, отримання IP-адреси за DHCP, то вказаний IoT-сервер.

В якості IoT-серверу налаштовано сервер в з IP-адресом 10.23.226.139/26.

На головній сторінці веб-сайту сервера відображено перелік IoT-пристроїв, для кожного з яких є можливість віддаленого управління (увімкнення /вимкнення).

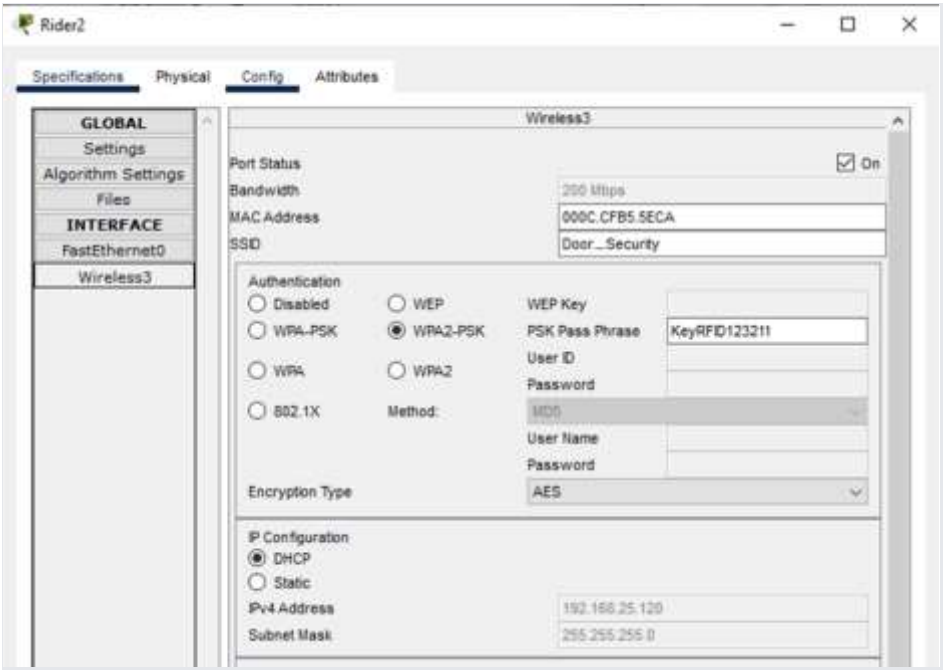


Рисунок 4.6 – Налаштування інтерфейсу бездротового IoT-пристрою

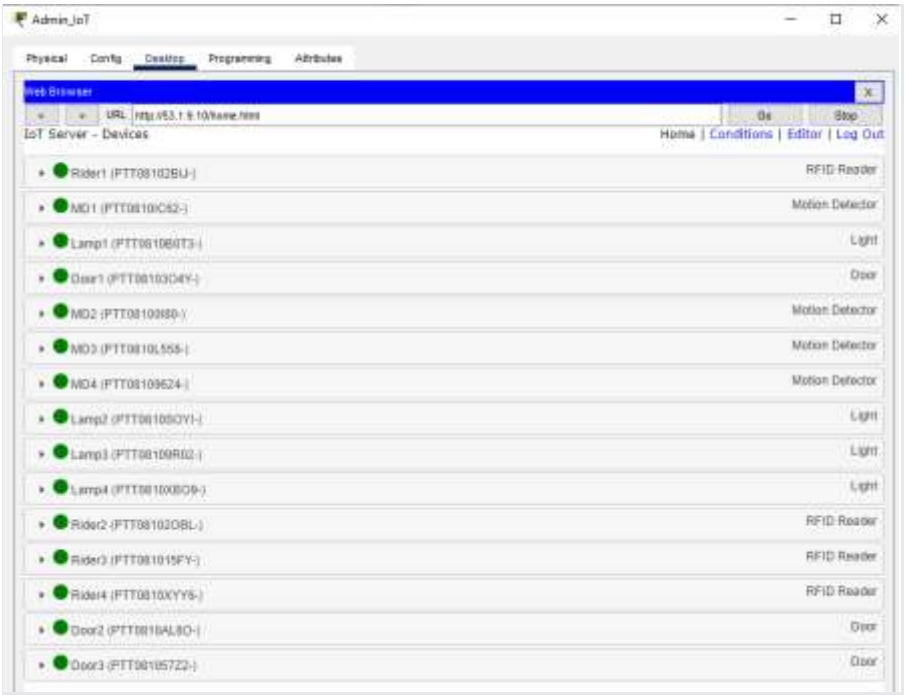


Рисунок 4.7 – Веб-інтерфейс керування бездротовими IoT-пристроями

За допомогою WEB-інтерфейсу IoT-сервера налаштований сценарій системи доступу до офісу будівельного інституту. На рис. 8 показано сценарій функціонування системи доступу до офісних приміщень.

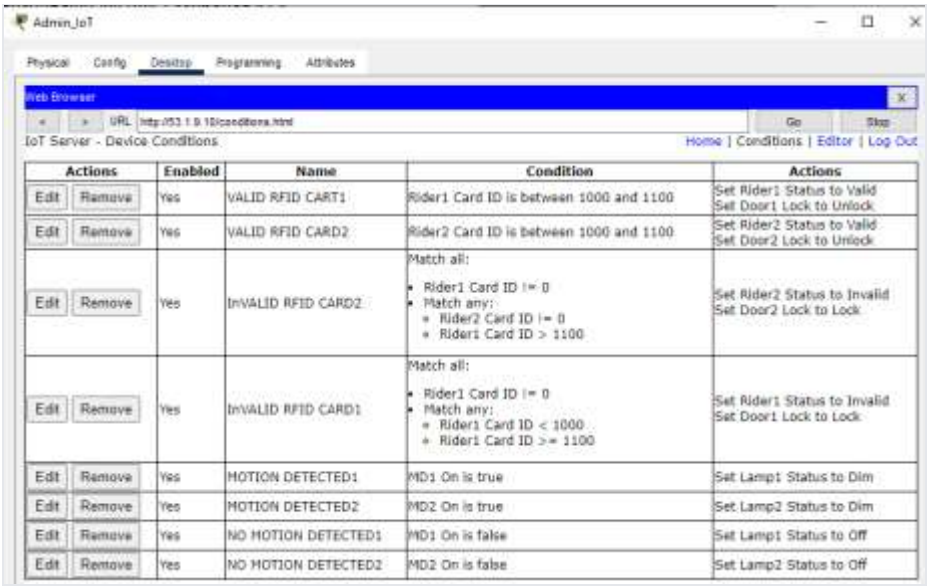


Рисунок 4.8 – Сценарій функціонування системи доступу до офісних приміщень будівельного інституту

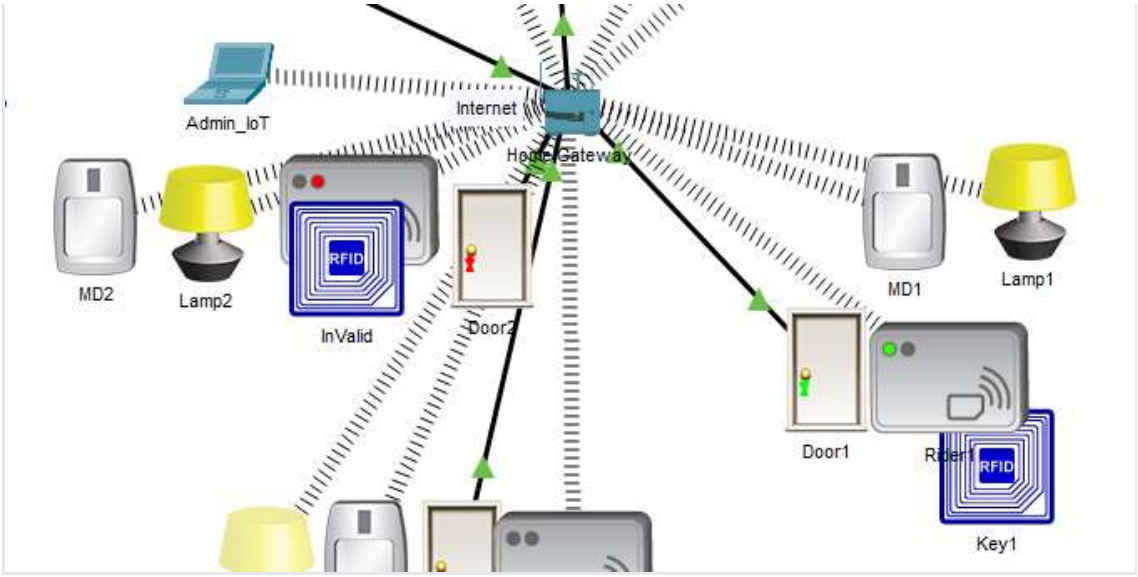


Рисунок 4.9 – Робота системи обмеженого доступу до офісних приміщень будівельного інституту

4.4 Висновки за розділом

У кваліфікаційній роботі для корпоративної мережі комп'ютерної системи будівельного інституту в розділі розробка компоненту IoT визначено завдання на розробку, зроблено огляд загальної інформація про IoT, розробка функціональної схеми та здійснено налаштування обладнання та сервісів для обраної системи IoT.

ВИСНОВКИ

В кваліфікаційній роботі бакалавра виконана поетапна розробки комп'ютерні системи будівельного інституту.

В загальній частині роботи були проаналізовані телекомунікаційні та технічні характеристики будівельного інституту, оцінені характеристики існуючих мережевих елементів, які будуть додані до корпоративної мережі.

Була проведена ретельна розробка апаратної частини комп’ютерної системи будівельного інституту де були виконані наступні кроки: сформовані технічні вимоги до комп’ютерної системи, здійснена розробка архітектури корпоративної мережі системного обладнання , обрана апаратна частина комп’ютерної системи.

В розділі розробка корпоративної мережі, поставлено завдання по створенню корпоративної мережі будівельного інституту, де були описані принципи IP-адресація в корпоративній мережі, проведено розрахунок схеми IP-адресації для корпоративної мережі, розроблена топологічна схеми корпоративної мережі на базі мережевих продуктів Cisco, проведено налаштування корпоративної мережі, здійснена перевірка роботи корпоративної мережі на симуляторі Cisco Packet Tracer та розроблені заходи з захисту інформації в корпоративної мережі від несанкціонованого доступу.

У кваліфікаційній роботі для корпоративної мережі комп’ютерної системи будівельного інституту в розділі розробка компоненту IoT визначено завдання на розробку, зроблено огляд загальної інформація про IoT, розробка функціональної схеми та здійснено налаштування обладнання та сервісів для обраної системи IoT.

ПЕРЕЛІК ПОСИЛАНЬ

1. КИЇВСТАР Інтернет-провайдер. Режим доступу: https://uanet.info/

2. Український будівельний ринок у 2024 році. Режим доступу: https://www.bdo.ua/en-gb/insights-1/information-materials/2024/ukrainian-construction-market-in-2024

3. АТ «ПТІ „КИЇВОРГБУД“». Режим доступу: https://opendatabot.ua/c/04012951

4. Адрушко Л.М., Смірнов В.І. Волоконно-оптичні лінії // Електрозв'язок 2007. с 20-28.

5. Competitors and Alternatives to iMaster NCE-Campus. Режим доступу до ресурсу: https://www.gartner.com/reviews/market/net-work-access-control/vendor/huawei/product/imaster-nce-campus/alternatives.

6. Quality of Service (QoS) Configuration Guide, Cisco IOS XE Everest 16.6.x (Catalyst 9400 Switches). Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/soft-ware/release/16-6/configura-tion_guide/qos/b_166_qos_9400_cg/b_166_qos_9400_cg_chapter_01.html.

7. Cisco solutions. Режим доступу: https://www.cisco.com

8. Cisco UCS Management. Режим доступу: https://www.cisco.com/c/en/us/products/servers-unified-computing/cisco_ucs_management.html

9. CISCO (UCSB-B200-M6-U) UCS B200 M6 Blade w/o CPU mem HDD mezz. Режим доступу: https://www.melbourneglobal.com.au/cisco-ucsb-b200-m6-u-ucs-b200-m6-blade-w-o-cpu-mem-hdd-mezz/

10. Cisco Catalyst 2960-Plus Series Switches Data Sheet. Режим доступу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-plus-series-switches/data_sheet_c78-728003.html

11. Cisco 2900 Series Integrated Services Routers Data Sheet. Режим доступу: https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html

12. Cisco Catalyst 9105AXI - Бездротова точка доступу - Bluetooth, Wi-Fi. Режим доступу: https://www.inmac-wstore.com

13. What is VLSM?. Режим доступу: https://www.networkacademy.io/ccna/ip-subnetting/what-is-vlsm

14. The Internet of Things (IoT) Integration in Access Control: Enhancing Security in Smart Buildings. Режим доступу: https://www.polimek.com/iot-integration-in-access-control-enhancing-security-in-smart-buildings/

15. Сучасні засоби обмеження доступу та система керування відвідувачами. Режим доступу: https://www.bezpeka-shop.com/ua/blog/poleznye-sovety/suchasni-zasoby-obmezennia-dostupu-ta-systema-keruvannia-vidviduvachamy/

ДОДАТОК А
ТЕКСТ ПРОГРАМИ

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.2506-01 12 01

Листів 5

2025

АНОТАЦІЯ

Розроблена в бакалаврській кваліфікаційні й роботі програма містить необхідну для програмування налаштувань компонентів корпоративної мережі комп'ютерної система акціонерного товариство «проектно-технологічний інститут.

ПЗ призначено для забезпечення налаштування параметрів динамічної маршрутизації, DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній, створення мереж VPN, домену и SSH для комп'ютерна система акціонерного товариство «проектно-технологічний інститут.

ЗМІСТ

1 Налаштування роутера R_Didenko_2

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R_Didenko_2
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded-address 10.22.209.1 10.22.209.10
ip dhcp excluded-address 10.22.211.129 10.22.211.139
!
ip dhcp pool POOL_LAN5
 network 10.22.209.0 255.255.255.0
 default-router 10.22.209.1
 dns-server 10.22.210.10
ip dhcp pool POOL_LAN1
 network 10.22.211.128 255.255.255.192
 default-router 10.22.211.129
 dns-server 10.22.210.10
!
!
aaa new-model
!
aaa authentication login Login group radius local
aaa authentication login SSH-LOGIN local
aaa authentication login default group radius local
!
username 123211_Didenko password 7 0822455D0A16
!
!
license udi pid CISCO2911/K9 sn FTX1524CED0-
!
no ip domain-lookup
ip domain-name R_Didenko_2
!
!
spanning-tree mode pvst
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description TO LAN 5
 ip address 10.22.209.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 description TO LAN1
 ip address 10.22.211.129 255.255.255.192
 duplex auto
 speed auto
!
interface Serial0/0/0
 description to WAN1
 bandwidth 128
 ip address 10.0.6.1 255.255.255.252
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet0/1/0
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 6
 redistribute static
 passive-interface GigabitEthernet0/1
 passive-interface GigabitEthernet0/2
 network 10.22.209.0 0.0.0.255
 network 10.0.6.0 0.0.0.3
 network 10.22.211.128 0.0.0.63
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.2
!
```

```
ip flow-export version 9
!
banner motd #123211 Didenko. Enter only have key#
!
radius-server host 10.22.210.10 auth-port 1645
radius-server key zzz
!
radius server 10.22.210.10
 address ipv4 10.22.210.10 auth-port 1645
!
line con 0
 password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 login authentication SSH-LOGIN
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 transport input ssh
!
end
```

1 Налаштування комутатора S_Didenko_0

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S_Didenko_5
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
ip domain-name S_Didenko_5
!
username 123211_Didenko privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 36
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 36
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 36
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 36
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 36
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 26
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 26
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 26
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 26
```

```
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 26
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 16
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 16
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 16
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 16
 switchport mode access
interface FastEthernet0/23
 switchport access vlan 16
 switchport trunk native vlan 100
 switchport trunk allowed vlan 16,26,36,99-
100
 switchport mode trunk
!
interface FastEthernet0/24
 switchport access vlan 16
 switchport trunk native vlan 100
 switchport trunk allowed vlan 16,26,36,99-
100
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 16,26,36,99-
100
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 description LAN Vnutr_99
 ip address 10.22.211.98 255.255.255.240
!
ip default-gateway 10.22.211.97
!
banner motd #123211 Didenko. Enter only
have key#
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
!
!
!
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

2025

Таблиця маршрутизації R_Didenko_1

```
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 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 13 subnets, 6 masks
D       10.0.6.0/30 [90/21024000] via 10.0.6.6, 02:38:16, Serial0/0/0
C       10.0.6.4/30 is directly connected, Serial0/0/0
L       10.0.6.5/32 is directly connected, Serial0/0/0
D       10.0.6.8/30 [90/21024000] via 10.0.6.6, 02:16:14, Serial0/0/0
C       10.22.208.0/24 is directly connected, GigabitEthernet0/1
L       10.22.208.1/32 is directly connected, GigabitEthernet0/1
D       10.22.209.0/24 [90/21026560] via 10.0.6.6, 02:38:16, Serial0/0/0
D       10.22.210.0/24 [90/21024256] via 10.0.6.6, 02:16:09, Serial0/0/0
D       10.22.211.0/27 [90/20519680] via 10.0.6.6, 02:17:43, Serial0/0/0
D       10.22.211.32/27 [90/20519680] via 10.0.6.6, 02:17:43, Serial0/0/0
D       10.22.211.64/27 [90/20519680] via 10.0.6.6, 02:17:43, Serial0/0/0
D       10.22.211.96/28 [90/20519680] via 10.0.6.6, 02:17:43, Serial0/0/0
D       10.22.211.128/26 [90/21024256] via 10.0.6.6, 02:38:16, Serial0/0/0
D    53.0.0.0/8 [90/20517120] via 10.0.6.6, 02:38:16, Serial0/0/0
D    64.0.0.0/8 [90/20517120] via 10.0.6.6, 02:17:44, Serial0/0/0
D    209.165.202.0/24 [90/20514560] via 10.0.6.6, 02:38:16, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Таблиця маршрутизації R_Didenko_2

```
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 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 14 subnets, 6 masks
C       10.0.6.0/30 is directly connected, Serial0/0/0
L       10.0.6.1/32 is directly connected, Serial0/0/0
D       10.0.6.4/30 [90/21024000] via 10.0.6.2, 00:29:02, Serial0/0/0
D       10.0.6.8/30 [90/21024000] via 10.0.6.2, 00:07:00, Serial0/0/0
D       10.22.208.0/24 [90/21024256] via 10.0.6.2, 00:29:02, Serial0/0/0
C       10.22.209.0/24 is directly connected, GigabitEthernet0/1
L       10.22.209.1/32 is directly connected, GigabitEthernet0/1
D       10.22.210.0/24 [90/21024256] via 10.0.6.2, 00:06:54, Serial0/0/0
D       10.22.211.0/27 [90/20519680] via 10.0.6.2, 00:08:29, Serial0/0/0
D       10.22.211.32/27 [90/20519680] via 10.0.6.2, 00:08:29, Serial0/0/0
D       10.22.211.64/27 [90/20519680] via 10.0.6.2, 00:08:29, Serial0/0/0
D       10.22.211.96/28 [90/20519680] via 10.0.6.2, 00:08:29, Serial0/0/0
C       10.22.211.128/26 is directly connected, GigabitEthernet0/2
L       10.22.211.129/32 is directly connected, GigabitEthernet0/2
D    53.0.0.0/8 [90/20517120] via 10.0.6.2, 00:29:03, Serial0/0/0
D    64.0.0.0/8 [90/20517120] via 10.0.6.2, 00:08:30, Serial0/0/0
D    209.165.202.0/24 [90/20514560] via 10.0.6.2, 00:29:03, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Таблиця маршрутизації R_Didenko_3

```
Codes: C - connected, S - static, I - IGRP, 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 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 13 subnets, 7 masks
D       10.0.0.0/8 is a summary, 02:39:00, Null0
C       10.0.6.0/30 is directly connected, Serial2/0
C       10.0.6.4/30 is directly connected, Serial3/0
C       10.0.6.8/30 is directly connected, Serial6/0
S       10.22.208.0/21 is directly connected, FastEthernet4/0
D       10.22.208.0/24 [90/20512256] via 10.0.6.5, 02:38:59, Serial3/0
D       10.22.209.0/24 [90/20514560] via 10.0.6.1, 02:39:00, Serial2/0
D       10.22.210.0/24 [90/2170112] via 10.0.6.9, 02:16:51, Serial6/0
D       10.22.211.0/27 [90/33280] via 209.165.202.2, 02:18:26, FastEthernet4/0
D       10.22.211.32/27 [90/33280] via 209.165.202.2, 02:18:26, FastEthernet4/0
D       10.22.211.64/27 [90/33280] via 209.165.202.2, 02:18:26, FastEthernet4/0
D       10.22.211.96/28 [90/33280] via 209.165.202.2, 02:18:26, FastEthernet4/0
D       10.22.211.128/26 [90/20512256] via 10.0.6.1, 02:39:00, Serial2/0
D    53.0.0.0/8 [90/30720] via 209.165.202.2, 02:39:07, FastEthernet4/0
D    64.0.0.0/8 [90/30720] via 209.165.202.2, 02:18:27, FastEthernet4/0
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
D       209.165.202.0/24 is a summary, 02:39:00, Null0
C       209.165.202.0/27 is directly connected, FastEthernet4/0
S*   0.0.0.0/0 is directly connected, FastEthernet4/0
                [1/0] via 209.165.202.2
```

Таблиця маршрутизації R_Didenko_4

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
Dulidov_R4#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 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 13 subnets, 6 masks
D       10.0.6.0/30 [90/21024000] via 10.0.6.10, 02:17:15, Serial0/0/0
D       10.0.6.4/30 [90/21024000] via 10.0.6.10, 02:17:15, Serial0/0/0
C       10.0.6.8/30 is directly connected, Serial0/0/0
L       10.0.6.9/32 is directly connected, Serial0/0/0
D       10.22.208.0/24 [90/21024256] via 10.0.6.10, 02:17:15, Serial0/0/0
D       10.22.209.0/24 [90/21026560] via 10.0.6.10, 02:17:15, Serial0/0/0
C       10.22.210.0/24 is directly connected, GigabitEthernet0/1
L       10.22.210.1/32 is directly connected, GigabitEthernet0/1
D       10.22.211.0/27 [90/20519680] via 10.0.6.10, 02:17:15, Serial0/0/0
D       10.22.211.32/27 [90/20519680] via 10.0.6.10, 02:17:15, Serial0/0/0
D       10.22.211.64/27 [90/20519680] via 10.0.6.10, 02:17:15, Serial0/0/0
D       10.22.211.96/28 [90/20519680] via 10.0.6.10, 02:17:15, Serial0/0/0
D       10.22.211.128/26 [90/21024256] via 10.0.6.10, 02:17:15, Serial0/0/0
D    53.0.0.0/8 [90/20517120] via 10.0.6.10, 02:17:15, Serial0/0/0
D    64.0.0.0/8 [90/20517120] via 10.0.6.10, 02:17:15, Serial0/0/0
D    209.165.202.0/24 [90/20514560] via 10.0.6.10, 02:17:15, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Таблиця маршрутизації R_Didenko_0

```
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 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 13 subnets, 6 masks
D       10.0.6.0/30 [90/21024000] via 10.0.6.10, 02:17:15, Serial0/0/0
D       10.0.6.4/30 [90/21024000] via 10.0.6.10, 02:17:15, Serial0/0/0
C       10.0.6.8/30 is directly connected, Serial0/0/0
L       10.0.6.9/32 is directly connected, Serial0/0/0
D       10.22.208.0/24 [90/21024256] via 10.0.6.10, 02:17:15, Serial0/0/0
D       10.22.209.0/24 [90/21026560] via 10.0.6.10, 02:17:15, Serial0/0/0
C       10.22.210.0/24 is directly connected, GigabitEthernet0/1
L       10.22.210.1/32 is directly connected, GigabitEthernet0/1
D       10.22.211.0/27 [90/20519680] via 10.0.6.10, 02:17:15, Serial0/0/0
D       10.22.211.32/27 [90/20519680] via 10.0.6.10, 02:17:15, Serial0/0/0
D       10.22.211.64/27 [90/20519680] via 10.0.6.10, 02:17:15, Serial0/0/0
D       10.22.211.96/28 [90/20519680] via 10.0.6.10, 02:17:15, Serial0/0/0
D       10.22.211.128/26 [90/21024256] via 10.0.6.10, 02:17:15, Serial0/0/0
D    63.0.0.0/8 [90/20517120] via 10.0.6.10, 02:17:15, Serial0/0/0
D    64.0.0.0/8 [90/20517120] via 10.0.6.10, 02:17:15, Serial0/0/0
D    209.165.202.0/24 [90/20514560] via 10.0.6.10, 02:17:15, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```