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

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Бічевник Дмитро Вікторович
(ПІБ)

академічної групи 123-21ск-1
(шифр)

спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

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

на тему «Комп'ютерна система Управління Придніпровської залізниці з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Олевський В.І.			
розділів:				
розробка апаратної частини				
розробка корпоративної мережі				
Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2024

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

ЗАВДАННЯ

на кваліфікаційну роботу ступеня бакалавр

студента Бічевник Д.В. **академічної групи** 123-21ск-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 Управління Придніпровської залізниці з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі» затверджену наказом ректора НТУ «Дніпровська політехніка» від 29.04.2024 № 375-с.

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постанова завдання	26.02.2024
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	19.03.2024
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	03.05.2024
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2024

Завдання видано _____ проф. Олевський В.І.
(підпис керівника) (прізвище, ініціали)
Дата видачі 12.02.2024
Дата подання до екзаменаційної комісії 03.06.2024 р.
Прийнято до виконання _____ Бічевник Д.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 86 с., 32 рис., 5 табл., 1 додаток, 12 джерел.

Об’єкт розробки: комп’ютерна система Управління Придніпровської залізниці.

Мета: розробка та налаштування комп'ютерної системи для потреб Придніпровської залізниці з метою впровадження віддаленого управління залізничним переїздом на основі технологій Інтернету речей (IoT).

Для досягнення цієї мети важливо враховувати різноманітні технічні деталі та аспекти, включаючи:

1. Вибір оптимальної мережевої архітектури, яка відповідає вимогам ефективності та безпеки. Для забезпечення ефективності та надійності мережі необхідно вибрати архітектуру, яка забезпечить оптимальне розподілення ресурсів та мінімізує можливість виникнення перешкод.

2. Підбір кабельної системи для комп'ютерної мережі з урахуванням вимог щодо швидкості передачі даних та надійності зв'язку.

3. Проведення аналізу мережного трафіку для оптимізації роботи системи та підвищення її продуктивності.

4. Вибір методу управління мережею для забезпечення її ефективності та стабільності.

5. Налаштування та конфігурація мережного обладнання з урахуванням конкретних потреб та вимог залізничної інфраструктури.

6.Забезпечення високого рівня безпеки мережі для захисту від потенційних кіберзагроз та зловмисників. Застосування відповідних заходів безпеки дозволить убезпечити мережу від несанкціонованого доступу та зберегти конфіденційність інформації.

Ключові слова: залізниця, віддалене управління, залізничний переїзд, Інтернет речей (IoT), мережева архітектура, кабельна система, мережний трафік, управління мережею.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ ТА ТЕРМІНІВ

КС – комп’ютерна система

ЗДП– залізо дорожній переїзд

IoT – Internet of Things

LAN – локальна під мережа

ЦОД – центр обробки даних

RBTC – системи радіоуправління рухом поїздів (

ДН – дирекція перевезень

FCC – Federal Communications Commission

CE – Conformité Européenne

ВСТУП

У сучасному світі, де швидкість та ефективність перевезення товарів та пасажирів має велике значення, безпека залізничного транспорту залишається однією з найважливіших проблем. Залізничні переїзди, які з'єднують залізничні колії із дорожніми маршрутами, стають місцем частих аварій та нещасних випадків через недбале використання, людські помилки та технічні несправності.

У залізничній галузі та системах залізничної сигналізації традиційно використовувалися фіксовані блочні поділи поїздів та сигнали прямої видимості для забезпечення контролю руху та уникнення зіткнень. Цей підхід призвів до розділення функціональності та розвитку підсистем, що часто дотримувалися вузького та послідовного проектного підходу. Проте нещодавні розробки, такі як системи радіоуправління рухом поїздів (RBTC), виявилися складнішими, з більшою взаємодією між підсистемами. Це призвело до потреби в застосуванні системного інженерного підходу до розробки та розгортання таких систем.

Залізнична галузь, хоча й намагалася прийняти системну інженерію, спочатку зіткнулася з опором через високий статус підходу, орієнтованого на безпеку. Багато інженерів, звиклих до традиційного підходу, намагаються співвіднести нові системи з цими принципами. У цьому контексті поява технологій Інтернету речей (IoT) відкриває нові можливості для вдосконалення систем залізничної сигналізації та безпеки руху поїздів. У цьому контексті виникає потреба у впровадженні нових технологій, спрямованих на покращення безпеки та ефективності управління залізничними переїздами. Однією з перспективних технологій є використання систем управління на основі Інтернету речей (IoT), які дозволяють автоматизувати процеси та забезпечити постійний моніторинг та контроль.

Ця робота спрямована на розробку та налаштування комп'ютерної мережі для впровадження віддаленого управління залізничним переїздом на основі технологій IoT. Вона охоплює аналіз вимог, вибір оптимальних технічних рішень та розробку системи, яка забезпечить надійний та ефективний контроль залізничного переїзду.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Опис об’єкта розробки та умов застосування КС

Об'єктом дослідження є комп'ютерна система управління Придніпровської залізниці. Придніпровська залізниця є одним із ключових відділень залізничного транспорту України, забезпечуючи перевезення пасажирів та вантажів між важливими промисловими та адміністративними центрами країни. Основні напрямки діяльності залізниці включають роботу з вантажними та пасажирськими перевезеннями, розвиток інфраструктури, а також удосконалення технологій управління рухом та безпеки.

Історія розвитку Придніпровської залізниці свідчить про значний внесок у розвиток транспортної інфраструктури регіону та всієї країни.

Все почалося в 1862 році, коли перший міністр шляхів сполучення Росії висунув проєкт будівництва залізниці від Катеринослава до Донбасу. Протягом наступних десятиліть залізниця поступово розширювалась і розвивалась. У 1873 році відкрито регулярний рух поїздів на дільницях Лозова — Олександрівськ та Синельникове І — Катеринослав. У 1875 році затверджено план будівництва дільниць залізниці від Казанки до Катеринослава і від Ясинувата до Синельникове І. Згодом, у 1884 році, було відкрито рух поїздів на цих дільницях, а також зданий в експлуатацію залізничний міст через річку Дніпро.

У наступні роки були побудовані нові лінії і відкрито нові дільниці, що значно розширило можливості залізничного сполучення в регіоні. Наприклад, у 1898 році була побудована залізнична лінія Колачевске — П'ятихатки — Любомирівка. У 1904 році введено в експлуатацію другу Катеринінську залізницю: Кривий Ріг — Олександрівськ — Царекостянтинівка. Найбільш значущим подією стало введення в експлуатацію Кічкаського моста у 1908 році, що відкрило наскрізний рух по Другій Катеринінській залізниці.

У період до Першої світової війни були введені в експлуатацію додаткові дільниці, зокрема в напрямку з Донбасу до Криму. Після війни почали діяти одноколійні гілки, що забезпечили прямий шлях з Донбасу до Криму, а також закінчено будівництво лінії Євпаторія — Сарабуз.

У період радянської влади було проведено значні реформи та модернізація залізничної інфраструктури. У 1935 році вперше в УРСР почали курсувати поїзди на електричній тязі на дільниці Запоріжжя — Нікополь — Кривий Ріг, що стало найбільшою електрифікованою магістраллю в країні.

У 1961 році залізницю перейменували на Сталінську, а в 1973 році відзначили 100-річчя заснування. Згодом, у 1991 році, утворили Державну адміністрацію залізничного транспорту України («Укрзалізниця»), до складу якої входить Придніпровська залізниця.

Проте після анексії Криму Росією в 2014 році відбулися зміни у роботі залізниці, зокрема, обмежено рух поїздів між материковою частиною України та Кримом. Також змінилася структура управління залізницею, а в 2015 році Придніпровська залізниця ввійшла до складу ПАТ «Укрзалізниця» [1].

На сьогоднішній день Придніпровська залізниця охоплює значну частину східної та центральної України, є стратегічно важливою для зв'язку промислових центрів з портами Чорного моря та західними регіонами країни. Залізниця включає основні маршрути, такі як Київ-Дніпро, Дніпро-Запоріжжя, Дніпро-Кривий Ріг, а також багато інших місцевих маршрутів, які забезпечують доступ до менших міст і селищ. Всього система управління залізницею координує рух на понад 3000 км колій (рис.1.1).

Колійна інфраструктура Придніпровської залізниці (рис.1.2) включає одноколійні та двоколійні ділянки, оснащені електрифікованими та неелектрифікованими коліями. Більшість основних магістралей є електрифікованими, що забезпечує ефективне і швидке пересування поїздів, зокрема високошвидкісних. Система управління залізницею також включає складні технічні вузли, які дозволяють виконувати маневрові операції, технічне обслуговування рухомого складу та логістику вантажних перевезень. Загальна протяжність залізничних колій становить понад 3250 км, з них 58,3% електрифіковано. 83,5% колій обладнано автоматичним регулюванням руху. 90% станцій мають електричну централізацію.

Перевізна робота виконується 244 станціями, з них 4 сортувальні, 7 пасажирських, 67 вантажних, 19 дільничних.

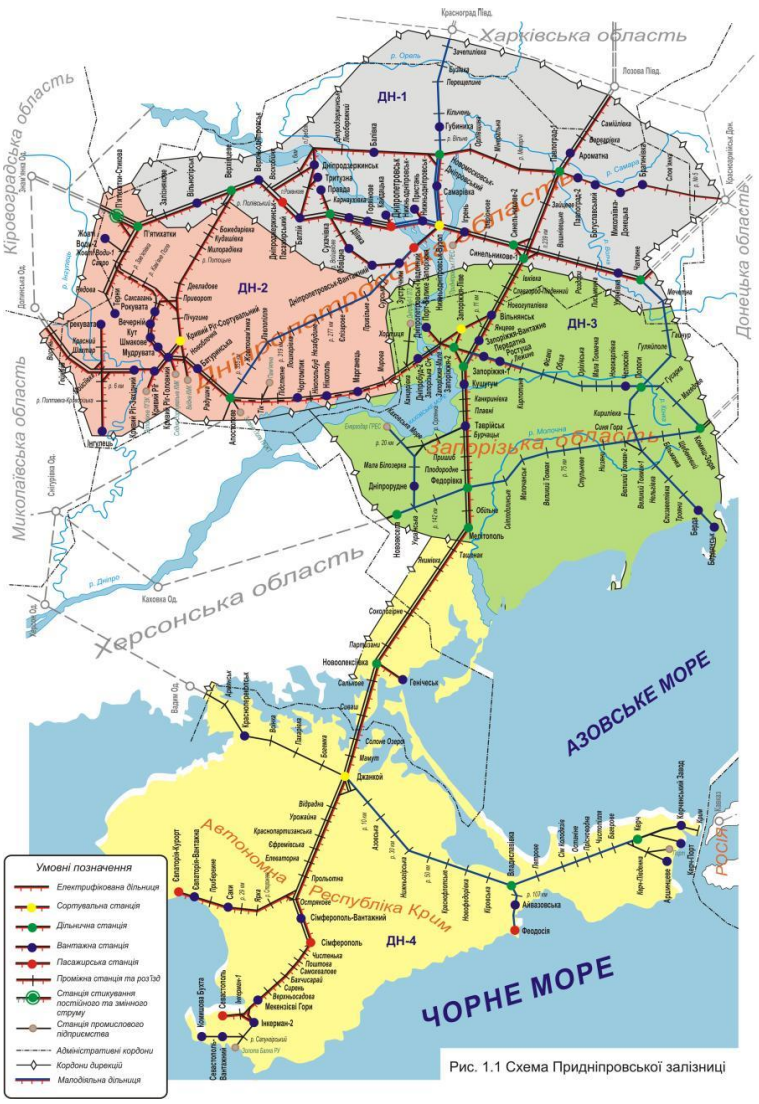


Рисунок 1.1 – Структурна схема Придніпровської залізниці

Планування розкладів руху є важливою складовою комп'ютерної системи управління Придніпровської залізниці. Ця система враховує різноманітні фактори, такі як пасажирські потреби, вантажні об'єми, технічні можливості та інші обмеження, для оптимального використання інфраструктури та забезпечення ефективного та безпечного руху поїздів. З огляду на великий обсяг перевезень та значну кількість запитів на бронювання маршрутів, система управління Придніпровської залізниці має завдання підтримувати прибутковість маршрутів, забезпечувати ефективну роботу всіх типів поїздів та організовувати регулярне технічне обслуговування.

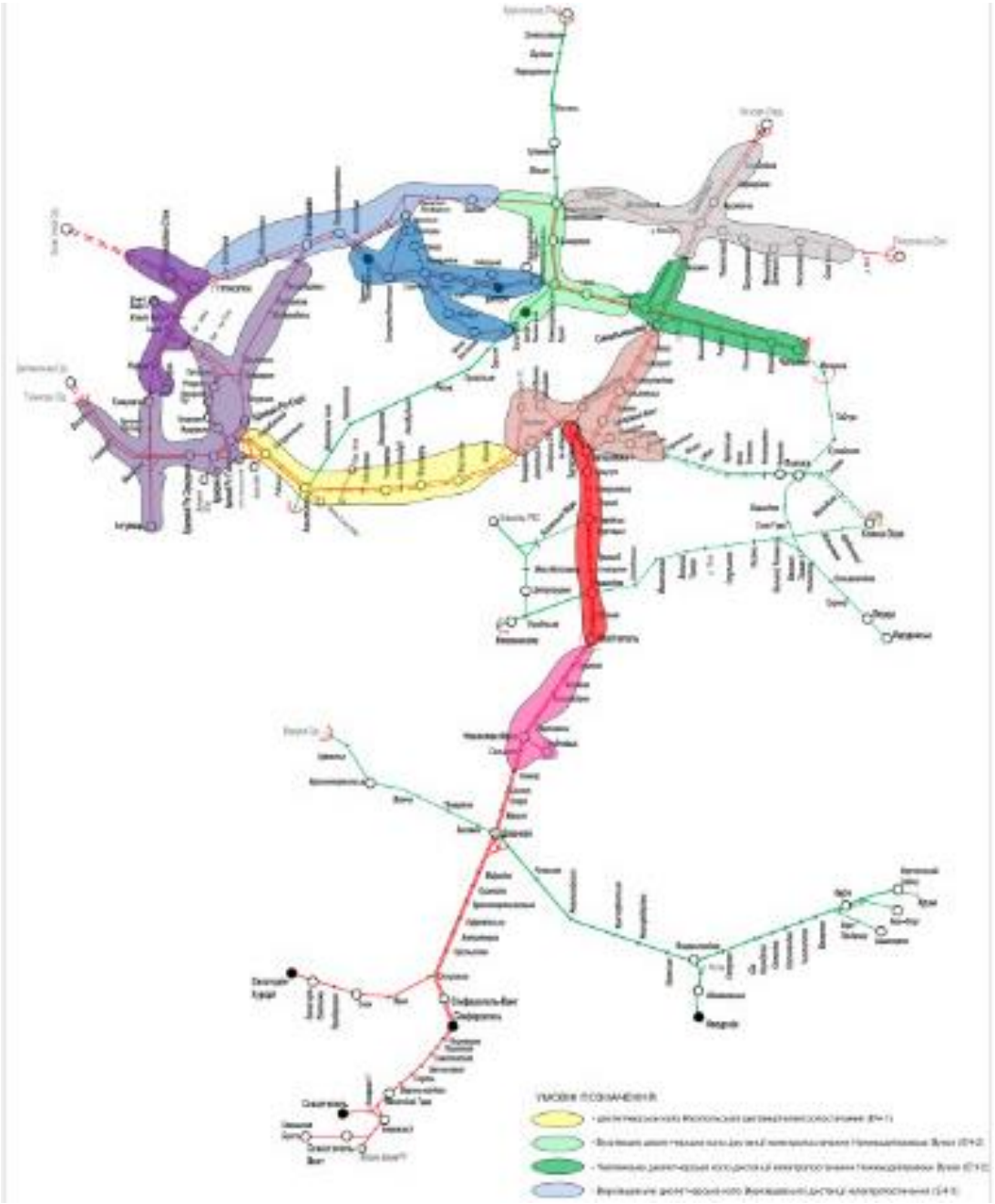


Рисунок 1.2 – Схема обслуговування колій Придніпровської залізниці

Пасажирські розклади руху розробляються з урахуванням попиту на перевезення між різними містами та населеними пунктами. На Придніпровській залізниці надходить значна кількість запитів на бронювання маршрутів, які потребують уважного планування. Розклади руху пасажирських поїздів враховують різні фактори, такі як відстань, популярність маршруту, час подорожі та час року.

Вантажні розклади руху також розробляються з урахуванням попиту на перевезення різних видів товарів між промисловими центрами та іншими місцями

призначення. Розклади вантажних поїздів визначаються відповідно до обсягів вантажів, термінів доставки та інших обмежень.

На Придніпровській залізниці існують різні типи поїздів, кожен з яких має свої особливості та призначення. Серед них:

- пасажирські поїзди – регулярні поїзди для перевезення пасажирів між різними населеними пунктами;
- швидкісні поїзди – поїзди, які забезпечують швидкий та комфортний транспорт між великими містами;
- вантажні поїзди – призначені для перевезення великих обсягів товарів та вантажів між промисловими центрами.

Частота маршрутів на Придніпровській залізниці визначається відповідно до попиту та обсягів перевезень. Найбільш популярні маршрути можуть мати більш часті рейси, в той час як менш популярні маршрути можуть мати меншу частоту рейсів. Планування розкладів руху виконується таким чином, щоб забезпечити ефективне використання інфраструктури та задовольнення попиту на перевезення [2].

1.2 Організаційна структура об’єкта впровадження

На Придніпровській залізниці офіси та диспетчерські центри розташовані в різних місцях, що відповідає їх функціональному призначенню та потребам управління залізничними операціями. Структура Придніпровської залізниці складається з різних ділянок та диспетчерських районів, які обслуговують певні території та мережі залізниць.

Головний офіс регіональної філії «Придніпровська залізниця» знаходиться за адресою: 49602, Дніпро, проспект Дмитра Яворницького, 108.

У складі Придніпровської залізниці функціонують 3 дирекції залізничних перевезень:

- Дніпровська (ДН-1);
- Криворізька (ДН-2);
- Запорізька (ДН-3).

До 2014 року повністю функціонувала також Кримська дирекція залізничних

перевезень (ДН-4). Проте після тимчасової окупації Криму дільниці Кримської дирекції на материковій частині обслуговуються сусідніми дирекціями.

Центральний офіс управління залізницею відповідає за загальне керівництво та стратегічне планування, зазвичай розташований у великому місті, яке є центральним вузлом залізничної мережі, у місті Дніпро, що обслуговує як головний вузол Придніпровської залізниці.

Регіональні офіси розташовані у великих містах, які обслуговуються залізницею та відповідають за оперативне управління на певній території. Такими регіональні офіси знаходяться у м. Дніпро, м. Запоріжжя, м. Кривий Ріг.

Диспетчерські центри на коліях вздовж залізничних трас та відповідають за нагляд та керівництво рухом поїздів на певній ділянці колії. Розташування таких центрів визначається з урахуванням географічних та технічних особливостей конкретних маршрутів.

Технічні та обслуговуючі підрозділи це майстерні, депо, а також інші технічні об'єкти, які відповідають за обслуговування та ремонт залізничної техніки та інфраструктури [2].

1.3 Огляд інженерних рішень у галузі комп'ютерних систем залізничного транспорту

У реалізації комп'ютерних систем (КС) для залізничної мережі Придніпровської залізниці важливо враховувати існуючі інженерні рішення, спрямовані на оптимізацію руху поїздів та управління станціями. Використання сучасних технологій, таких як Інтернет речей (IoT), може сприяти створенню ефективних та інноваційних рішень.

Для забезпечення оптимального використання залізничної інфраструктури важливо проводити аналіз пропускної спроможності станцій. Це допомагає визначити максимальну кількість поїздів, яку може обслуговувати станція протягом певного часу. Для цього використовуються різноманітні підходи та інструменти, такі як моделі руху та аналітичні методи [3].

Наприклад, компанії, які спеціалізуються на розробці комп'ютерних систем для залізничного транспорту, надають програмне забезпечення для аналізу

пропускної спроможності. Розглянемо детально приклади.

DEMIURGE, розроблений SNCF та Eurodecision у 2004 році, є програмним забезпеченням, призначеним для допомоги у проведенні досліджень пропускної спроможності залізничної мережі. Це програмне забезпечення може оцінити здатність мережі поглинути додатковий трафік, визначити вузькі місця, допомогти у прийнятті рішень щодо інвестицій в інфраструктуру, оптимізувати поточні та майбутні графіки руху, а також розрахувати залишкову пропускну спроможність розкладу.

CMS (AEA Technology Rail) надає систему для планування ефективного використання залізничних потужностей. Вона пропонує просту оцінку сценаріїв "що, якщо", автоматичну генерацію розкладів, моделювання операцій для прогнозування продуктивності та визначення шляхів виправлення ситуації, визначення пропускної спроможності, доступної для продажу, та прогнози використання на основі покращених розкладів. Однак, щоб забезпечити достовірність прогнозів, CMS потребує калібрування з використанням оновлених даних про пунктуальність.

RAILCAP (Stratec) вимірює, скільки доступної пропускної спроможності використовується в рамках певної операційної програми, і пропонує дуже детальний аналіз вузьких місць. Однак він має один суттєвий недолік, оскільки моделювання вимагає значних зусиль. RAILCAP вимагає детального опису колій, стрілочних переводів, переїздів, сигналів та обмежень швидкості.

VIRIATO (SMA і Partner) в основному використовується для адаптації інфраструктури до майбутніх концепцій обслуговування і координації роботи декількох операторів або продуктів, які використовують одну і ту ж інфраструктуру. Він дозволяє користувачеві визначити ступінь насиченості певної лінії. Він стискає заданий розклад і визначає рівень насиченості лінії або частини лінії у відсотках.

CAPRES, розроблений Lucchini та Curchod у 2001 році, є моделлю для розробки та насичення варіантів розкладу руху. За допомогою ітерацій ця модель визначає всі доступні додаткові маршрути руху поїздів, враховуючи всі обмеження та взаємозв'язки між лініями. Недоліком цієї моделі є те, що традиційні мережеві та експлуатаційні дані мають бути доповнені інформацією про те, де, коли і як має

бути використана пропускна спроможність мережі.

FASTTRACK II (Мультимодальні прикладні системи) - це комп'ютерна модель диспетчеризації поїздів і зустрічних поїздів, яка здатна створювати реальний план диспетчеризації поїздів для обраного користувачем коридору, враховуючи набір запропонованих розкладів руху поїздів і конфігурацію колії коридору. Вона може бути використана для вивчення доцільності запропонованих графіків руху поїздів, перевірки впливу запропонованих змін в операційній політиці на залізничне сполучення та вимірювання теоретичної і практичної пропускної спроможності ліній.

Система MOM, розроблена Барбером та ін. у 2006 році, є високофункціональним інструментом, який допомагає керівникам залізниць забезпечувати ефективне та оперативне управління залізничною інфраструктурою. Система MOM може генерувати оптимізовані залізничні графіки як в автономному режимі, так і в режимі он-лайн (при виникненні збоїв). Вона також надає інформацію про пропускну спроможність залізничної мережі та надійність розкладу, допомагаючи менеджерам приймати кращі рішення. Цей модуль надає кілька аналітичних та емпіричних методів, які можна використовувати для отримання висновків про пропускну здатність залізничних мереж і які підтримують процес адаптації залізничної інфраструктури до потреб перевезень. Проект системи MOM був розроблений відповідно до вимог Іспанської адміністрації залізничної інфраструктури (ADIF).

AFAIG - це комплексний програмний пакет, розроблений LITEP Федеральної політехнічної школи Лозанни для планування розташування та операційних планів основних залізничних пасажирських станцій. AFAIG використовує базу даних, що описує інфраструктуру, рухомий склад, правила експлуатації та розклади руху. У діалоговому режимі AFAIG дозволяє планувальнику розмістити рух поїздів, після чого розраховує час зайнятості послідовних ділянок для кожного маршруту, виявляє і вимірює конфлікти між рухами, перевіряє дотримання всіх операційних обмежень і бере на себе виконання нудних завдань зі складання розкладу. Звільнившись від операцій, які можна автоматизувати, планувальник великої залізничної станції може ефективно присвятити свій час завданням проектування, аналізу та

багатокритеріальної оцінки. AFAIG було впроваджено у відділі планування розкладу руху головних станцій Швейцарської федеральної залізниці (SBB), щоб допомогти планувальникам керувати маршрутами, коліями платформ і сполученнями відповідно до стратегії "Rail 2000".

Вище описанні інструменти допомагають у забезпеченні ефективності та оптимізації використання залізничної інфраструктури [3].

1.4 Постановка проблеми та завдання роботи

Проблема, що стоїть перед дослідженням, полягає у розробці сучасної мережевої системи для залізничного вокзалу з метою поліпшення обслуговування пасажирів та оптимізації графіка руху поїздів. Залізничний вокзал, яким користується понад 30 000 пасажирів щоденно, потребує ефективної системи керування, оскільки обслуговування цієї кількості пасажирів викликає постійні виклики для керівництва залізниці. Нинішня мережа станції не задовольняє сучасні стандарти, що призводить до затримок у руху поїздів та непридатності інфраструктури для пасажирів та машиністів локомотивів. Відсутність інтелектуальних пристроїв та доступу до сучасних технологій призводить до помилок та збоїв в передачі інформації, що ускладнює розклад руху поїздів. Інтеграція інтелектуальних IoT-пристроїв та модернізація обладнання може поліпшити сервіс для пасажирів, автоматизувати процеси та зменшити кількість помилок для операторів вокзалу.

Впровадження віддаленого управління залізничним переїздом на основі технологій Інтернету речей (IoT) передбачає використання сучасних інноваційних методів для підвищення ефективності та безпеки залізничного руху. Ця ініціатива включає в себе використання сенсорів, збирачів даних та засобів зв'язку для забезпечення безпечного та оптимального функціонування залізничних переїздів.

Інтернет речей (IoT) відкриває широкі можливості для залізничного транспорту, дозволяючи збирати велику кількість даних про стан переїздів, рух поїздів та навколишнє середовище в реальному часі. Ці дані можуть використовуватися для аналізу та прогнозування ризиків, виявлення несправностей та аварійних ситуацій, а також для вчасного втручання та управління з метою

запобігання можливих проблем.

Однією з ключових переваг впровадження IoT в управління залізничним переїздом є можливість дистанційного моніторингу та керування. Це дозволяє операторам в реальному часі відслідковувати стан переїздів, виявляти будь-які аномалії або несправності та вчасно реагувати на них безпосередньо з центрального пункту керування.

Додатково, впровадження IoT може покращити ефективність управління технічним обслуговуванням та плануванням ремонтних робіт, дозволяючи збирати дані про стан обладнання та прогнозувати потреби в обслуговуванні заздалегідь. Це допоможе зменшити час простою переїздів та забезпечити їх надійну роботу.

Узагальнюючи, впровадження віддаленого управління залізничним переїздом на основі технологій Інтернету речей (IoT) сприятиме підвищенню безпеки, ефективності та надійності залізничного руху, що стане важливим кроком у модернізації та оптимізації інфраструктури залізниць.

Мета даної роботи полягає в розробці та налаштуванні комп'ютерної мережі для потреб Придніпровської залізниці з метою впровадження віддаленого управління залізничним переїздом на основі технологій Інтернету речей (IoT). Для досягнення цієї мети важливо враховувати різноманітні технічні деталі та аспекти, включаючи:

1 Вибір оптимальної мережевої архітектури, яка відповідає вимогам ефективності та безпеки.

2 Підбір кабельної системи для комп'ютерної мережі з урахуванням вимог щодо швидкості передачі даних та надійності зв'язку.

3 Проведення аналізу мережного трафіку для оптимізації роботи системи та підвищення її продуктивності.

4 Вибір методу управління мережею для забезпечення її ефективності та стабільності.

5 Налаштування та конфігурація мережного обладнання з урахуванням конкретних потреб та вимог залізничної інфраструктури.

6 Забезпечення високого рівня безпеки мережі для захисту від потенційних кіберзагроз та зловмисників.

Отже, успішна реалізація проекту передбачає розробку гнучкої та оптимальної мережевої структури, що забезпечить надійний захист та легкість налаштування для подальшого розвитку та вдосконалення.

1.5 Потенційні шляхи вирішення поставлених завдань

Для впровадження сучасної мережевої інфраструктури на залізничному вокзалі та реалізації віддаленого управління залізничним переїздом повинна складатися з чотирьох підмереж, кожна з яких буде відповідати певним функціональним аспектам вокзалу та переїзду (рис.1.3):

- пасажирська зона;
- адміністративний блок та касові пункти;
- служба безпеки та відеоспостереження;
- центр обробки даних (ЦОД).

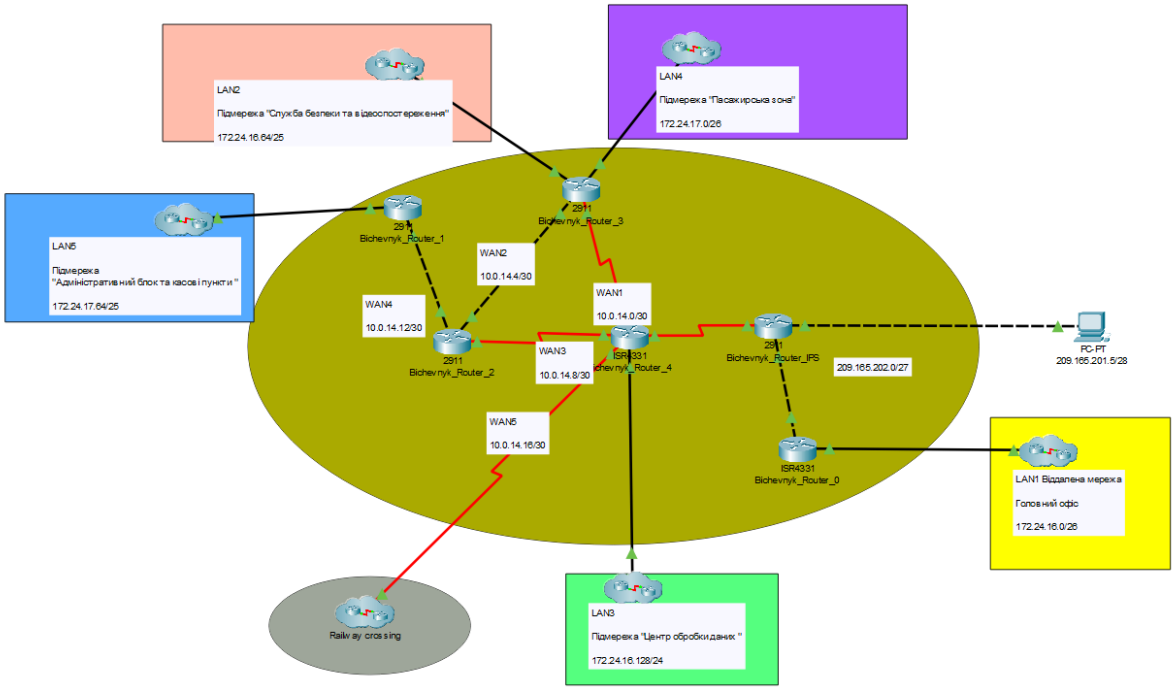


Рисунок 1.3 – Топологія мережі підприємства

Окрема мережа буде призначена для забезпечення зв'язку та керування переїздом. Ця мережа повинна мати високу надійність та ефективність, оскільки безпека руху поїздів та персоналу залежить від її нормального функціонування.

Система керування мережею повинна бути гнучкою та легко конфігуруватися

для відповіді на зміни в потребах вокзалу та переїзду. Це дозволить швидко адаптувати мережу до нових вимог та уникнути затримок у руху поїздів.

Розробка та впровадження заходів забезпечення безпеки мережі та даних, що передаються через неї. Це включає в себе застосування шифрування, мережевих брандмауерів, систем виявлення вторгнень та інших заходів безпеки.

Навчання персоналу з експлуатації та підтримки нової мережевої інфраструктури. Це допоможе забезпечити ефективне та безперебійне функціонування мережі після її впровадження.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до комп'ютерної системи

2.1.1 Вимоги до системи Придніпровської залізниці в цілому

Система повинна забезпечувати ефективну підтримку прийняття рішень пасажирами під час придбання інтернет-квитків на потяг, а також забезпечувати зручну взаємодію з потенційними клієнтами.

2.1.1.1 Вимоги до структури і функціонуванню системи

Комп'ютерна система Управління Придніпровської залізниці повинна складатися з чотирьох підмереж, кожна з яких буде відповідати певним функціональним аспектам вокзалу та переїзду (рис.1.3):

- пасажирська зона;
- адміністративний блок та касові пункти;
- служба безпеки та відеоспостереження;
- центр обробки даних (ЦОД).

Рекомендується використовувати IP-адресний блок для розподілу підмережі 172.24.16.0/21. Кількість вузлів для кожної локальної мережі така: LAN1 – 59; LAN2 – 124; LAN3 – 236; LAN4 – 42; LAN5 – 81. Необхідно забезпечити зв'язок між підмережами та контролювати трафік між ними, регулюючи доступ відповідно до рівня доступу [4].

2.1.1.2 Вимоги до експлуатації

Кожен компонент системи повинен мати індивідуальний логін та пароль для захисту від несанкціонованого доступу. Ця вимога ставить перед собою завдання забезпечити, щоб кожен користувач або пристрій, який намагається отримати доступ до системи, мав власний унікальний логін та пароль. Це захищає систему від несанкціонованого доступу та зловживань.

Комп'ютери мають бути з'єднані за допомогою надійних каналів передачі даних та обладнання, що забезпечує ефективну передачу даних.

Мережа повинна мати достатню кількість кваліфікованого персоналу для підтримки та управління. Це гарантує, що система може ефективно функціонувати та реагувати на можливі проблеми.

Обслуговуючий персонал повинен мати розуміння мережевих протоколів, здатність виявляти та усувати несправності, а також вміння налаштовувати та конфігурувати мережеве обладнання.

Персонал повинен працювати у визначених режимах, забезпечуючи нагляд, підтримку та реагування на проблеми в мережі. Це включає цілодобовий моніторинг, готовність до реагування на аварійні ситуації та планування регулярного обслуговування.

2.1.1.3 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему інтелектуального паркінгу, їх режим роботи

Забезпечення ефективної експлуатації та безперебійної роботи комп'ютерної системи Управління Придніпровської залізниці є важливим завданням, яке вимагає конкретних вимог до персоналу, який обслуговує систему, а також ретельно встановлених режимів роботи. Враховуючи значення безперебійної та ефективної роботи залізничної системи, нижче наведені докладні вимоги до чисельності та кваліфікації персоналу, а також опис режиму його роботи.

Чисельність персоналу:

- мережевий адміністратор: 2 особи;
- технічний підтримка: 5 осіб;
- системні адміністратори: 3 особи;
- IT-спеціалісти з безпеки: 2 особи.

Кваліфікаційні вимоги:

- мережевий адміністратор: досвід роботи з мережевим обладнанням, знання мережевих протоколів, сертифікація Cisco CCNA або еквівалент;
- технічний підтримка: вміння вирішувати технічні проблеми, досвід роботи з підтримкою користувачів, знання операційних систем Windows та Linux;
- системні адміністратори: досвід адміністрування серверів, вміння налаштовувати та управляти СХД, знання віртуалізації, сертифікація Microsoft MCSE або еквівалент;
- IT-спеціалісти з безпеки: досвід управління кібербезпекою, знання засобів захисту мережі, сертифікація CompTIA Security+ або еквівалент.

Режим роботи:

− обслуговуючий персонал повинен працювати у змінах по 8 годин на день з понеділка по п'ятницю;

− забезпечення цілодобового моніторингу мережі та оперативної реакції на можливі проблеми в роботі системи;

− встановлення регулярних періодичних перевірок стану мережі та профілактичного обслуговування з метою запобігання можливим аваріям та збоям.

2.1.1.4 Вимоги до надійності системи Управління Придніпровської залізниці

Забезпечення надійності системи Управління Придніпровської залізниці є однією з найважливіших складових для забезпечення безперебійної та ефективної роботи всієї інфраструктури залізничного транспорту. Для цього встановлюються конкретні вимоги до рівня надійності, які мають бути забезпечені системою. Нижче наведено конкретні параметри, які повинні бути враховані при розробці та експлуатації системи Управління Придніпровської залізниці.

Максимальний час відновлення системи (MTTR) не більше ніж 2 години після виникнення будь-якої системної помилки або аварії.

Середній час між відмовами (MTBF) мінімум 10 000 годин безвідмовної роботи передбачається для критичних компонентів системи.

Максимальний час простою системи (MTP) не більше ніж 1% від часу робочої місячної доби (тобто не більше ніж 7,2 години на місяць).

Рівень доступності (Availability) система повинна забезпечувати доступність не менше 99,9%, що відповідає перерві в роботі не більше 8 годин на рік.

Всі дані повинні резервуватися щоденно і зберігатися на резервних серверах протягом принаймні 30 днів.

Система повинна мати можливість автоматичної рестарту в разі аварій або відмови системи без необхідності вручного втручання.

Повинна бути належно налаштована система моніторингу, яка надсилає сповіщення адміністраторам про будь-які помилки або відмови в реальному часі.

Проведення щомісячних аудитів безпеки та регулярних тестів на відновлення даних, щоб перевірити ефективність процесів відновлення.

Встановлення резервних джерел живлення для усіх критичних компонентів

системи для запобігання відмовам через перебої в живленні.

2.1.1.5 Вимоги до захисту інформації від несанкціонованого доступу

Система Управління Придніпровської залізниці повинна мати мінімум 256-бітне шифрування для захисту конфіденційної інформації від несанкціонованого доступу.

Кожен користувач повинен мати унікальний ідентифікатор (логін) та пароль для отримання доступу до системи. Паролі повинні бути захищені та відповідати наступним вимогам: мінімум 10 символів, включати хоча б одну велику та малу літеру латиниці, хоча б одну цифру та хоча б один спеціальний символ. Пароль має змінюватись кожні 90 днів.

Реалізація рівнів доступу до системи включає наступне: користувацький рівень, який дає можливість користувачам керувати обладнанням, вносити та редагувати дані та створювати звіти; адміністративний рівень, що надає доступ адміністраторам для керування користувачами, обробки даних та створення звітів; та сервісний рівень, який дозволяє спеціалістам управляти обладнанням, вносити зміни в дані та проводити тестування функцій системи.

Встановлення механізмів контролю доступу для обмеження прав користувачів до конфіденційних даних та ресурсів мережі.

Моніторинг та аналіз активності мережі з метою виявлення та усунення можливих загроз безпеці.

Вживання заходів фізичної безпеки для захисту обладнання та інфраструктури від несанкціонованого доступу

2.1.1.6 Вимоги до безпеки

Вимоги до безпеки Управління Придніпровської залізниці включають дотримання нормативних актів та стандартів, серед яких:

Державний стандарт України ДСТУ 3434:2007 "Системи автоматизованого проектування. Загальні вимоги до безпеки".

Державний стандарт України ДСТУ 3025:2003 "Засоби автоматизації та управління. Вимоги до безпеки електронно-обчислювальних засобів. Загальні

положення".

Нормативні акти, регулюючі безпеку інформаційних технологій у сфері залізничного транспорту.

Вимоги до захисту персональних даних згідно із Законом України "Про захист персональних даних".

Дотримання цих стандартів та нормативів забезпечить високий рівень безпеки інформаційних технологій та даних, використовуваних в Управлінні Придніпровської залізниці [5, 6].

2.1.1.7 Вимоги до уніфікації та стандартизації обладнання в системі Управління Придніпровської залізниці

Вимоги до уніфікації та стандартизації обладнання в системі управління Придніпровської залізниці для віддаленого управління залізничним переїздом на основі технологій Інтернету речей вимагають дотримання різних стандартів та сертифікацій, щоб забезпечити високу якість, безпеку та сумісність обладнання.

Стандарт IEEE 802.11 (Wi-Fi) визначає протоколи та технології бездротового зв'язку, які використовуються для забезпечення зв'язку між різними пристроями у системі.

ISO/IEC 27001 стандарт встановлює вимоги до систем управління інформаційною безпекою, зокрема, забезпечення конфіденційності, цілісності та доступності інформації.

Стандарти ISO 9001 (Система управління якістю) спрямовані на забезпечення якості продукції та послуг, включаючи вимоги до процесів та систем управління.

IEC 62443 (Кібербезпека) визначає вимоги до кібербезпеки для промислових автоматизованих систем, зокрема, управління залізничним переїздом.

Сертифікація FCC (Federal Communications Commission) гарантує відповідність обладнання електромагнітним стандартам та безпеці, що є важливим для безперебійної роботи системи.

Сертифікація CE (Conformité Européenne) свідчить про відповідність продукції європейським стандартам безпеки та якості, що є необхідним для впровадження

системи на території Європейського Союзу.

2.1.2 Вимоги до функцій, які виконує система управління Придніпровської залізниці

Розглянемо вимоги до функцій системи управління Придніпровської залізниці

Підсистема «Пасажирська зона» забезпечує керування та моніторингу руху поїздів, видача та обробка квитків, надання інформаційного обслуговування пасажирів, забезпечення їхньої безпеки та майнових інтересів.

«Адміністративний блок та касові пункти» відповідає за управління персоналом та ресурсами, обробка фінансової звітності, здійснення касового обслуговування та оплати послуг.

Підсистема «Служба безпеки та відеоспостереження» повинна забезпечувати моніторинг та аналіз даних в реальному часі, виявлення потенційних загроз та захисту, запис та збереження відеоінформації для подальшого аналізу.

«Центр обробки даних (ЦОД)» відповідає за збереження, обробка та аналіз даних про рух поїздів та обслуговування пасажирів, забезпечення безпеки та надійності мережі та інформаційних систем, підтримка та розвиток інфраструктури ЦОД.

2.2 Вимоги до видів забезпечення

2.2.1 Вимоги до технічного забезпечення системи

Мережеве обладнання повинно відповідати вимогам стандартів та забезпечувати надійну та ефективну роботу системи. Нижче наведено конкретні вимоги до мережевого обладнання

Рекомендовано обрати виробника Cisco для маршрутизаторів з підтримкою віртуальної локальної мережі (VLAN) і протокол маршрутизації OSPF. Вони також повинні мати можливість розширення за допомогою модулів для додавання серійних портів. Шлюзові маршрутизатори мають підтримувати віртуальні приватні мережі (VPN).

Комутатори також рекомендуємо обрати виробника Cisco з підтримкою VLAN і мати не менше 24 портів Fast Ethernet. Комутатори в підмережі паркінгу повинні

мати порти Fast Ethernet з підтримкою технології передачі енергії через Ethernet (PoE).

Датчики повинні мати ступінь захисту не нижче IP65 для захисту від вологості та конденсації у паркінговому середовищі. Вони повинні працювати в широкому діапазоні температур від -20°C до +60°C для ефективної роботи в будь-яких кліматичних умовах. Датчики повинні забезпечувати високу точність та швидкість вимірювання параметрів, таких як вологість, температура та задимленість. Вони повинні бути легкими у встановленні та мають міцну конструкцію для витримки умов паркінгового середовища, таких як вібрації та удари.

Для керування системою рекомендується використання програмованих логічних контролерів від Siemens.

2.2.2 Мікроконтролер ESP8266

Мікроконтролер ESP8266 (NodeMCU) є популярним пристроєм у сфері Інтернету речей (IoT) та вбудованих систем. ESP8266 має вбудований мікропроцесор з тактовою частотою до 80 або 160 МГц. Це дозволяє виконувати широкий спектр завдань, від керування пристроями до обробки даних та зв'язку з мережами. NodeMCU має вбудовану флеш-пам'ять для зберігання програмного забезпечення та даних. Зазвичай це близько 4 МБ флеш-пам'яті. Мікроконтролер має різноманітні інтерфейси, включаючи цифрові входи/виходи (GPIO), аналогові входи, шину I2C, SPI та UART. Це дозволяє легко підключати до нього різноманітні сенсори, периферійні пристрої та модулі комунікації. Однією з ключових особливостей ESP8266 є його можливість працювати в мережах Wi-Fi. Вбудований Wi-Fi чіп дозволяє здійснювати зв'язок з бездротовою мережею, що робить його ідеальним вибором для проектів IoT. ESP8266 працює від напруги живлення 3.3 В, що потребує відповідного живлення для правильної роботи. Деякі версії NodeMCU мають вбудований регулятор напруги, який дозволяє живити їх від більш високих джерел живлення. NodeMCU має компактний розмір та зручний форм-фактор, що дозволяє легко використовувати його в різних проектах без необхідності розробки власної плати.

Вимоги до ESP8266 (NodeMCU) включають належне живлення з джерела 3.3

В, наявність програматора для завантаження програмного забезпечення, а також належне заземлення та електростатичний захист при роботі з пристроєм. Також важливо враховувати особливості роботи з Wi-Fi модулем, такі як потужність сигналу та інтерференція від інших пристроїв у мережі.

2.3 Розробка апаратної частини комп'ютерної системи

2.3.1 Розробка загальної структури компютерної системи управління Придніпровської залізниці

Комп'ютерна система управління Придніпровської залізниці є складною інформаційно-технічною системою, яка включає в себе різноманітні компоненти, призначені для ефективного контролю та управління різними аспектами залізничного транспорту. Розробка загальної структури такої системи включає в себе розподіл функцій, визначення архітектури мережі, вибір необхідного обладнання та програмного забезпечення, а також встановлення стандартів безпеки та надійності.

Система управління Придніпровської залізниці складається з різних підсистем, які відповідають за різні аспекти діяльності залізниці, такі як пасажирські перевезення, керування переїздами, безпека та відеоспостереження, адміністрування та обробка даних у Центрі обробки даних (ЦОД). Кожна з цих підсистем має власні функції та завдання, які потрібно враховувати при розробці загальної структури системи.

Для забезпечення ефективної комунікації між різними компонентами системи необхідно визначити архітектуру мережі. Це може бути класична зіркова або розгалужена мережа залежно від розміру та потреб системи. Кожна підсистема повинна мати власний сегмент мережі для забезпечення безпеки та надійності.

Для ефективної роботи системи необхідно вибрати відповідне обладнання та програмне забезпечення. Це може бути серверне обладнання для ЦОД, мережеве обладнання для підключення компонентів мережі, а також спеціалізовані програмні засоби для керування та моніторингу різних аспектів залізничної діяльності.

У системі управління Придніпровської залізниці розглядається структурна схема комплексу технічних засобів (рис.2.1), що включає в себе рівні доступу та рівень ядра для забезпечення ефективної роботи системи.

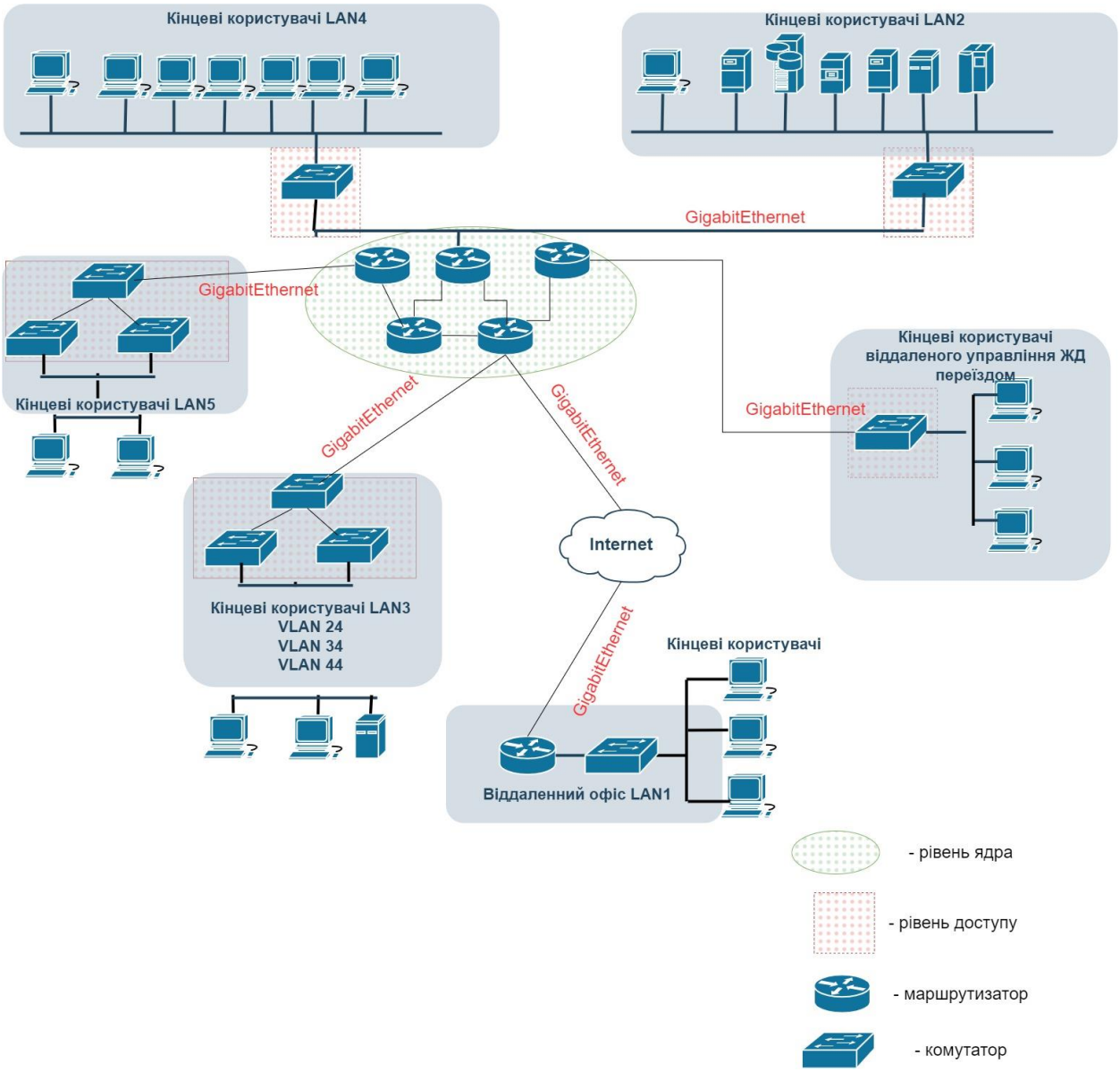


Рисунок 2.1 – Структурна схема комп’ютерної системи управління Придніпровської залізниці

Рівень ядра (Core) складається з шести маршрутизаторів, які забезпечують маршрутизацію трафіка та підключені мережами WAN. За допомогою технології VPN та шлюзового маршрутизатора рівня ядра здійснюється підключення проектованої мережі до Інтернету.

Рівень доступу (Access) включає тринадцять комутаторів, які розгорнуті для формування LAN та VLAN підмереж. До підмережі "Відділ продажу" та "Технічний відділ" використовуються відповідно два та три комутатори з використанням

технологій VLAN, PAgP та LACP. Це дозволяє забезпечити ізольований доступ та збільшити пропускну здатність та надійність каналу передачі даних.

Така архітектура розподілу мережі (рис.2.1) дозволяє забезпечити ефективну роботу системи управління Придніпровської залізниці, покращує продуктивність та забезпечує безпеку мережі. Вона також гарантує, що дані передаються безпосередньо від відправника до отримувача, що сприяє оптимізації робочих процесів та запобігає несанкціонованому доступу до інформації.

В таблиці 2.1 вказано кількість обладнання, яке забезпечує доступ користувачам або працівникам відділу до ресурсів та послуг. Ця таблиця складена відповідно до організаційної структури, топологічної схеми розміщення структурних підрозділів та робочих місць.

Таблиця 2. 1 – Кількість кінцевих пристроїв

Підмережа	Ідентифікатор	Тип	Кількість
LAN 4	Bichevnyk_PC_2.1	ПК	1
	Bichevnyk_PC_2.2	ПК	1
	Bichevnyk_PC_2.3	ПК	1
	Bichevnyk_PC_2.4	ПК	1
	Bichevnyk_PC_2.5	ПК	1
	Bichevnyk_PC_2.6	ПК	1
	Бездротова точка доступу	ПК, смартфони	
LAN2	Bichevnyk_PC_3.1	ПК	2
	Bichevnyk_PC_3.2	ПК	1
	Bichevnyk_PC_3.3	ПК	1
	Bichevnyk_PC_3.4	ПК	1
	Bichevnyk_PC_3.5	ПК	1
	Bichevnyk_PC_3.6	ПК	1
	Server HTTP	Server	1

	Server DNS	Server	1
	Server RADIUS	Server	1
LAN5	Bichevnyk_PC_1.1.1	ПК	1
	Bichevnyk_PC_1.1.2	ПК	1
	Bichevnyk_PC_1.1.3	ПК	1
	Bichevnyk_PC_1.1.4	ПК	1
	Bichevnyk_PC_1.1.5	ПК	1
	Bichevnyk_PC_1.1.6	ПК	1
	Bichevnyk_PC_1.1.7	ПК	1
	Bichevnyk_PC_1.1.8	ПК	1
LAN3	Bichevnyk_PC_4.2.34.1 - Bichevnyk_PC_4.2.34.4 VLAN 34	ПК	4
	Bichevnyk_PC_4.2.44.1 - Bichevnyk_PC_4.2.44.3 VLAN 44	ПК	3
	Bichevnyk_PC_4.2.24.1 - Bichevnyk_PC_4.2.24.3 VLAN 24	ПК	3
	Bichevnyk_ServerFTP	Сервер	1
LAN1	Bichevnyk_PC_5.1	ПК	1
	Bichevnyk_PC_5.1	ПК	1

2.3.2 Вибір і обґрунтування комплексу технічних засобів комп’ютерної системи

Обрання обладнання Cisco для комп'ютерної системи управління Придніпровської залізниці є обґрунтованим через їхню відомість, надійність та

розширені можливості. Комутатори Cisco забезпечують високу швидкість передачі даних і підтримують технології VLAN, що дозволяє створювати віртуальні локальні мережі для безпечного та ефективного розподілу трафіку. Маршрутизатори Cisco підтримують широкий спектр протоколів маршрутизації, включаючи OSPF та VPN, що забезпечує надійне з'єднання з віддаленими мережами та безпеку передачі даних.

Модель Cisco Catalyst 2960-L являє собою серію комутаторів, що підтримують VLAN та PoE (Power over Ethernet) і мають 24 порти Fast Ethernet. Технічні характеристики включають швидкість передачі даних 10/100 Мбіт/с, можливість керування через веб-інтерфейс та підтримку різноманітних мережевих протоколів [4].

Модель Cisco ISR 4000 Series є ідеальним вибором для підтримки великих об'ємів трафіку та безпеки мережі. Вона підтримує розширені функції маршрутизації, включаючи OSPF, VPN та QoS. Ці маршрутизатори мають велику швидкість передачі даних та високу надійність.

Обрано датчики Vaisala HMD60U. Цей датчик вологості і температури має високу точність вимірювання в межах ±1% для вологості та ±0,5°C для температури. Він має захист від вологи згідно з класом IP65 та може працювати в широкому діапазоні температур від -20°C до +60°C.

Контролер Siemens SIMATIC S7-1500 має потужний процесор, що дозволяє обробляти великий обсяг даних та виконувати складні завдання у реальному часі. Він підтримує різні мережеві інтерфейси та може інтегруватися з іншими системами керування.

Система відеоспостереження Hikvision DS-2CD2347G1-LU має високу роздільну здатність 4 Мп, великий кут огляду та підтримку відеозапису в умовах низького освітлення. Вона також має функцію виявлення руху та може передавати відео в реальному часі через мережу Ethernet.

В таблиці 2.2 наведена специфікація мережевого обладнання комп’ютерної системи управління Придніпровської залізниці. На рис.2.2 наведено загальну архітектуру КС управління Придніпровської залізниці, розробленої в Cisco PT.

Таблиця 2.2 – Специфікація обладнання

Позиція	Найменування	Виробник	Одиниця вимірювання	Кількість
1	Маршрутизатор ISR 4000 Series	Cisco	шт.	6
2	Комутатор Cisco Catalyst 2960-L	Cisco	шт.	12
3	Система відеоспостереження DS-2CD2347G1-LU	Hikvision	шт	6
4	Датчики HMD60U	Vaisala	шт	10

Для підключення мережевого обладнання рекомендується використовувати високоякісний мережевий кабель категорії 6 (Cat6). Кабель Cat6 забезпечує підтримку швидкості передачі даних до 10 Гбіт/с на відстані до 55 метрів і має покращену екранировку, що зменшує перешкоди та сприяє стабільності сигналу.

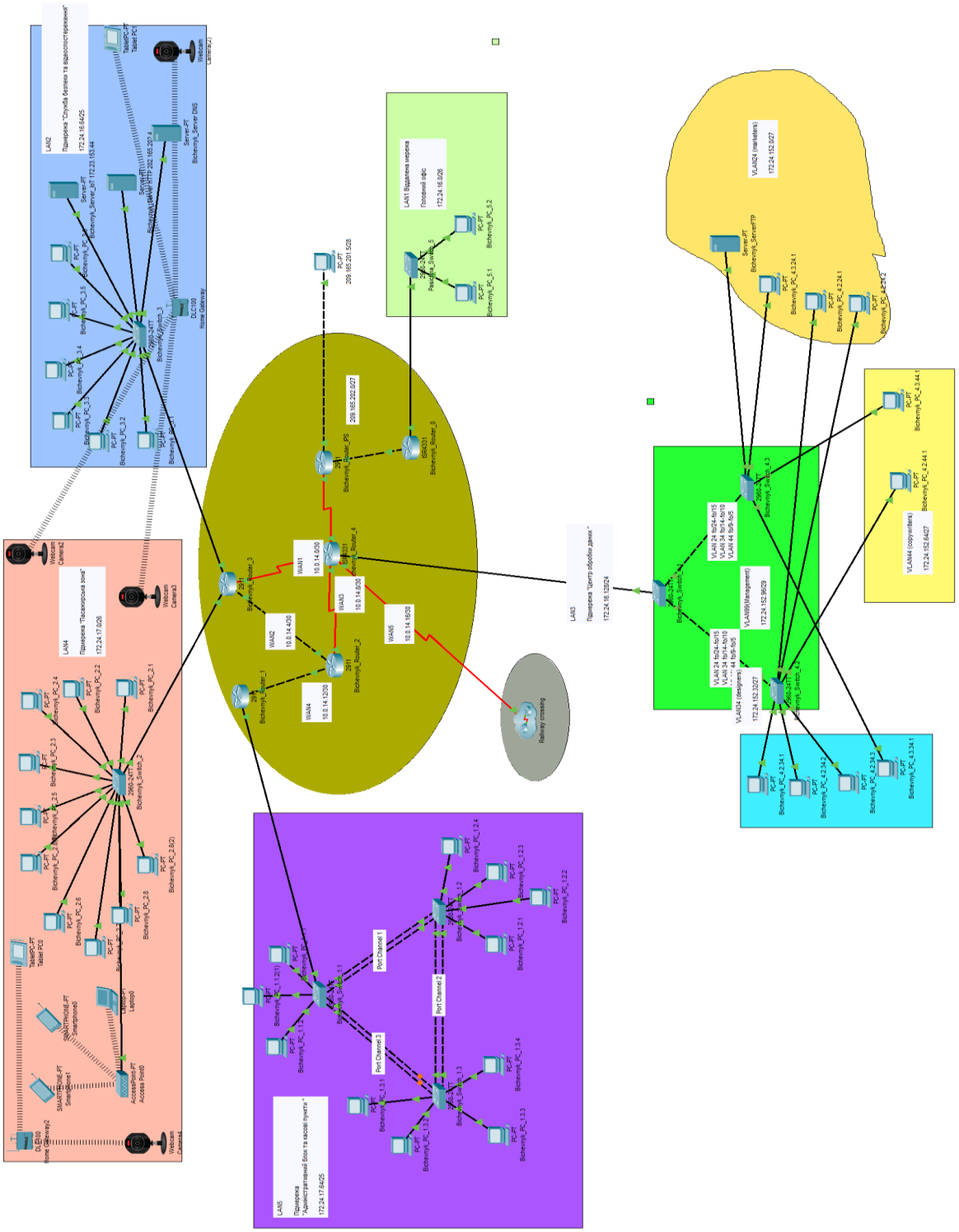


Рисунок 2.2 – Архітектура КС управління Придніпровської залізниці

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

3.1 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Згідно з дами організації дано:

– кількість вузлів найбільшої підмережі 236;

– середня інтенсивність трафіку складає μ=87 (кадрів/с);

− середня довжина повідомлення становить l=650 байт;

– затримка передачі пакету ≤ 6 мс;

– кількість портів комутатора – 24 шт.

Нижче наведено рішення наданої задачі.

Використовуючи формулу (3.1) розрахуємо пропускну здатність [4]:

$$Pp.p = \mu * l * n, \quad (3.1)$$

де

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

μ – інтенсивність обслуговування, кадрів/с;

l – середня довжина повідомлення, байт;

n – кількість портів комутатора.

Підставляємо відомі значення:

μ = 134 кадри/с;

l = 650 байт;

n = 24;

Pp.p = 87×650×24=2,597,200 біт/с або 2.6 Мбіт/с

Для розрахунку інтенсивності виходу трафіку застосуємо формулу (3.2) [5]:

$$\mu вих = C/ (8 * l), \quad (3.2)$$

де C – пропускна здатність лінії, біт/с;

l – середня довжина повідомлення байт.

Підставляємо відомі значення:

C = 1 000 000 000 біт/с;

l = 650 байт.

μвих = 1,000,000,000біт/с / 8×650байт =192,307пакетів/с

Для розрахунку максимальної кількості вузлів використовуємо формулу (3.3) [4].

$$N = \mu_{вих} / \mu, \quad (3.3)$$

де N – кількість вузлів, яку можна приєднати;

μвих – інтенсивність виходу, пакетів/с;

μ – середня інтенсивність трафіку, пакетів/с.

За наданими значеннями, інтенсивність виходу становить 192 307 пакетів/с, а середня інтенсивність трафіку дорівнює 134 пакетів/с.

Виходячи з цього отримуємо:

N = 192,307 / 134 ≈1436вузлів

За формулою (3.4) розрахуємо загальну інтенсивність трафіку [5]:

$$\lambda = x * \mu, \quad (3.4)$$

де λ – загальна інтенсивність трафіку, пакети/с;

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

μ - середня інтенсивність трафіку, пакети/с.

Підставляємо відомі значення:

x = 236;

μ = 87.

λ = 236×87= 20,532пакетів/с

Для розрахунку коефіцієнту затримки на рівні розподілу, використовується формула (3.5) [4]:

$$\rho = \lambda / \mu_{вих}, \quad (3.5)$$

де ρ – коефіцієнт затримки на рівні розподілу;

λ – загальна інтенсивність трафіку від всіх користувачів;

μвих – інтенсивність виходу, яка вказує на кількість пакетів, що виходять з комутатора за одиницю часу.

Підставляємо відомі значення:

λ = 20,532 пакетів/с;

μвих = 192,307 пакетів/с.

ρ = 192307.69/20,532 ≈0.1067

Розрахунок коефіцієнта зайнятості комутатора на рівні розподілу [4]:

$$r = \rho / (1 - \rho), \quad (3.6)$$

де r – коефіцієнт зайнятості комутатора;

ρ – коефіцієнт затримки на рівні розподілу.

Задано значення коефіцієнта затримки на рівні розподілу ρ ≈ 0.0592.

Підставимо ці значення в формулу:

r = 0.1067 / 1−0.1067 ≈0.12

Середня затримка кадру:

$$T = 1 / (\mu вих - \lambda), \quad (3.7)$$

де T – середня затримка кадру;

λ – загальна інтенсивність трафіку від всіх користувачів;

μвих – інтенсивність виходу, яка вказує на кількість пакетів, що виходять з комутатора за одиницю часу.

T = 1 / (192 307 – 20532) ≈ 0.0053 (секунд) = 53 * 10^{-6}(секунд)

Середня довжина черги:

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

де Lчерги – середня довжина черги;

ρ – коефіцієнт затримки на рівні розподілу.

Отримане значення коефіцієнта затримки на рівні розподілу ρ ≈ 0.0592, підставимо це значення в формулу:

Lчерги = $(0.1067)^2$ / (1 - 1067) ≈ 0.012

Середній час перебування пакета в черзі:

$$Точік = Lчерги / \lambda, \quad (3.8)$$

де Точік – середній час перебування пакета в черзі;

Lчерги – середня довжина черги;

λ – загальна інтенсивність трафіку від всіх користувачів.

Точік = 0.012 / 20532 = 0.585 (мс)

Пропускна здатність каналу:

$$b = \lambda * l, \quad (3.9)$$

де b - пропускна здатність каналу, біт/с;

λ - інтенсивність трафіку, пакетів/с;

l - середня довжина пакету, байт.

Замінивши значення у формулу, отримаємо:

b = 20532×650=13,359,600біт/с=13.3596Мбіт/с

Отримані результати розрахунків для комп'ютерної системи управління Придніпровської залізниці вказують на те, що мережа має достатню пропускну здатність та ефективно впорається з навантаженням від користувачів.

Загальна інтенсивність трафіку складає приблизно 20,532 пакети/с, що вказує на активність користувачів в мережі. Коефіцієнт затримки на рівні розподілу становить приблизно 0.1067, а коефіцієнт зайнятості комутатора - приблизно 0.12, що свідчить про те, що мережа оптимально використовується.

Середня затримка кадру складає близько 53 мікросекунд, що є прийнятним значенням для більшості застосувань. Середня довжина черги та середній час перебування пакета в черзі також показують, що мережа ефективно впорається з навантаженням без значних затримок та перевантажень.

Пропускна здатність каналу становить близько 13.36 Мбіт/с, що відповідає вихідним характеристикам каналу та вказує на те, що канал забезпечить необхідну пропускну здатність для передачі даних у мережі.

Отже, отримані результати свідчать про те, що комп'ютерна система

управління Придніпровської залізниці має стабільну та ефективну мережну інфраструктуру, яка може задовольнити потреби користувачів та забезпечити надійне та швидке функціонування системи управління.

3.2 Розрахунок схеми адресації корпоративної мережі

Для розподілу адрес з мережі 172.24.16.0/21 за методом VLSM (Variable Length Subnet Mask), спочатку розподілимо максимальну кількість IP-адрес на найбільшу мережу, а потім будемо зменшувати кількість адрес для кожної наступної мережі, враховуючи потреби кожної LAN [7].

Крок 1: Визначення необхідної кількості адрес для кожної LAN:

- LAN1 = 59 адресів. Для LAN1 нам потрібно мінімум 59 адрес. Найменша потужність двійки, що перевищує 59, - 64 (/26). Залишаємо 2048 - 64 = 1984 адрес.;
- LAN2 = 124 адреси. Для LAN2 нам потрібно мінімум 124 адреси. Найменша потужність двійки, що перевищує 124, - 128 (/25). Залишаємо 1984 - 128 = 1856 адрес.;
- LAN3 = 236 адресів. Для LAN3 нам потрібно мінімум 236 адресів. Найменша потужність двійки, що перевищує 236, - 256 (/24). Залишаємо 1856 - 256 = 1600 адрес;
- LAN4 = 42 адреси. Для LAN4 нам потрібно мінімум 42 адреси. Найменша потужність двійки, що перевищує 42, - 64 (/26). Залишаємо 1600 - 64 = 1536 адрес;
- LAN5 = 81 адрес. Для LAN5 нам потрібно мінімум 81 адрес. Найменша потужність двійки, що перевищує 81, - 128 (/25). Залишаємо 1536 - 128 = 1408 адрес.

Крок 2: Розподіл мереж з врахуванням потреб кожної LAN.

Максимальна кількість адрес для мережі /21 - 2048.

LAN1: Потрібно мінімум 59 адрес. Вибираємо підмережу /26.Кількість адрес для підмережі /26:

$$2^{32-26}-2=64-2=62 \text{ адреси}$$

Розподілені адреси для LAN1: 172.24.16.0/26

LAN2: Потрібно мінімум 124 адреси. Вибираємо підмережу /25.Кількість

адрес для підмережі /25:

$$2^{32-25}-2=128-2=126 \text{ адресів.}$$

Розподілені адреси для LAN2: 172.24.16.64/25

LAN3: Потрібно мінімум 236 адресів. Вибираємо підмережу /24.Кількість адрес для підмережі /24:

$$2^{32-24}-2=256-2=254 \text{ адреси.}$$

Розподілені адреси для LAN3: 172.24.16.128/24

LAN4: Потрібно мінімум 42 адреси. Вибираємо підмережу /26.Кількість адрес для підмережі /26:

$$2^{32-26}-2=64-2=62 \text{ адреси.}$$

Розподілені адреси для LAN4: 172.24.17.0/26

LAN5: Потрібно мінімум 81 адрес. Вибираємо підмережу /25.Кількість адрес для підмережі /25:

$$2^{32-25}-2=128-2=126 \text{ адресів}$$

Розподілені адреси для LAN5: 172.24.17.64/25

Результати розрахунків наведено в таблиці 3.1.

Таблиця 3.1 – Схема адресації корпоративної мережі Придніпровської залізниці

Назва підмережі	Необхідна кількість вузлів	Номер мережі	Префікс мережі	Діапазон доступних адрес
LAN1	61	172.24.16.0	/26	172.24.16.1 до 172.24.16.62
LAN2	32	172.24.16.64	/25	172.24.16.65 до 172.24.16.126
LAN3	10	172.24.16.128	/24	172.24.16.129 до 172.24.16.254
LAN4	85	172.24.17.0	/26	172.24.17.1 до 172.24.17.62
VLAN24	27	172.24.152.0	/27	172.24.17.1 – 172.24.17.30
VLAN34	27	172.24.152.32	/27	172.24.17.33 –

				172.24.17.62
VLAN44	27	172.24.152.64	/27	172.24.17.65 – 172.24.152.94
VLAN99	4	172.24.152.96	/29	172.24.17.97 – 172.24.17.102
LAN5	19	172.24.17.64	/25	172.24.17.65 до 172.24.17.126
WAN1	2	10.0.14.0	/30	10.0.14.1 _ 10.0.14.2
WAN2	2	10.0.14.4	/30	10.0.14.5 – 10.0.14.6
WAN3	2	10.0.14.8	/30	10.0.14.9 – 10.0.14.10
WAN4	2	10.0.14.12	/30	10.0.14.13 – 10.0.14.14
WAN5	2	10.0.14.16	/30	10.0.14.17 – 10.0.14.18
WAN_IPS	2	209.165.202.0	/30	209.165.202.1 – 209.165.202.30

3.3 Розрахунок схеми адресації пристроїв

Для розрахунку схеми адресації пристроїв, потрібно визначити IP-адреси для кожного пристрою в мережі, враховуючи вимоги проектування, таких як [8]:

– інтерфейсам і підінтерфейсам маршрутизаторів у LAN призначаються перші можливі для використання IP-адреси;

– комутаторам призначаються другі з можливих IP-адрес для кожної LAN;

– вузлам призначаються останні з використовуваних IP-адрес;

– в мережах VLAN використовується адресація кінцевих пристроїв за допомогою протоколу DHCP.

На основі розрахованих даних, наведених у таблиці 3.1, була складена схема адресації пристроїв, яка представлена у таблиці 3.2.

Таблиця 3.2 – Схема адресації пристроїв мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Bichevnyk_Router_1	Gig0/0	10.0.14.14	/30	-	-	Gig0/0
	Gig0/1	172.24.17.65	/25	-	-	Fa0/1
Bichevnyk_Router_2	Se0/1/1	10.0.14.9	/30	-	-	Se0/0/1
	Gig0/0	10.0.14.13	/30	-	-	Gig0/0
	Gig0/1	10.0.14.5	/30	-	-	Gig0/1
Bichevnyk_Router_3	Se0/2/0	10.0.14.2	/30	-	-	Se0/1/0
	Gig0/0	172.24.16.65	/25	-	-	Gig0/1
	Gig0/1	10.0.14.6	/30	-	-	Gig0/1
	Gig0/2	172.24.17.1	/27	-	-	Gig0/2
Bichevnyk_Router_4	Se0/1/0	209.165.202.2	/27	-	-	Se0/0/0
	Se0/1/1	10.0.14.10	/30	-	-	Se0/0/1

Продовження таблиці 3.2

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Bichevnyk_Router_4	Se0/2/0	10.0.14.1	/30	-	-	Se0/1/0
	Gig0/1	-	-	-	-	Gig0/1
	Gig0/1.24	172.24.17.1	/27	-	24	Gig0/1
	Gig0/1.34	172.24.17.33	/27	-	34	Gig0/1
	Gig0/1.44	172.24.17.65	/27	-	44	Gig0/1
	Gig0/1.99	172.24.17.97	/29	-	99	Gig0/1
Bichevnyk_Router_0	Gig0/0/1	172.24.17. 0	/27	-	-	Gig0/1
	Gig0/0/0	64.100.13.2	/30	-	-	Gig0/2
Bichevnyk_Router_IPS	Se0/0/0	209.165.202.1	/30	-	-	Se0/1/0
	Gig0/0	209.165.201.1	/28	-	-	NIC
	Gig0/2	64.100.13.1	/27	-	-	Gig0/0/1
Bichevnyk_Switch_1	VLAN1	172.24.17.130	/26	172.24.17.129	-	Gig0/1
						F0/2
						F0/3
						F0/6

.1						F0/7
Bichevnyk_Switch_1.2	VLAN1	172.24.17.131	/26	172.24.17.129	-	F0/2 F0/3 F0/4 F0/5
Bichevnyk_Switch_1.3	VLAN1	172.24.17.132	/26	172.24.17.129	-	F0/4 F0/5 F0/6 F0/7
Bichevnyk_Switch_2	VLAN1	172.24.17.194	/26	172.24.17.193	-	Gig0/2
Bichevnyk_Switch_3	VLAN1	172.24.17.34	/28	172.24.17.33	-	Gig0/0
Bichevnyk_Switch_4.1	VLAN99	172.24.17.98	/29	172.24.17.97	-	Gig0/1 F0/1 F0/2
Bichevnyk_Switch_4.2	VLAN99	172.24.17.99	/29	172.24.17.97	-	F0/1

Кінець таблиці 3.2

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Bichevnyk_Switch_4.3	VLAN99	172.24.17100	/29	172.24.17.97	-	F0/2
Bichevnyk_Switch_5	VLAN1	172.24.16.2	/27	172.24.16.1	-	Gig0/0

3.4 Налаштування роботи комп’ютерної системи

3.4.1 Базове налаштування конфігурації пристроїв КС

Для базового налаштування мережевих пристроїв у корпоративній мережі Придніпровської залізниці, основні кроки включають конфігурацію маршрутизаторів та комутаторів через CLI. В рамках базової конфігурації потрібно налаштувати:

- унікальні імена пристроїв - кожен мережевий пристрій отримає унікальне ім'я, що полегшить ідентифікацію та управління в мережі;
- паролі для доступу - будуть встановлені паролі для доступу до консолі та через лінії vty (Virtual Teletype). Для консольного доступу та vty ліній буде використано пароль "cisco";
- пароль для привілейованого режиму - пароль "class" буде використано для доступу до привілейованого режиму, що забезпечує більш глибокий контроль над конфігурацією пристрою;
- шифрування паролів - всі паролі будуть зашифровані, щоб забезпечити безпеку ваших даних та унеможливити їхнє прочитання у відкритому вигляді;
- банер MOTD (Message of the Day) - буде налаштовано банер, який показуватиметься усім користувачам при спробі з'єднання з пристроєм, як нагадування про політику безпеки або важливі повідомлення;
- використання SSH на лініях vty - для забезпечення захищеного віддаленого доступу буде налаштоване використання протоколу SSH замість не захищеного Telnet;
- створення користувацького облікового запису - користувач "12321sk1_Bichevnyk" з паролем "admincisco" буде створено для адміністрування пристроїв;
- конфігурація імені домену та ключів RSA - буде налаштовано ім'я домену та згенеровано ключі RSA для забезпечення захищеного ключового обміну при використанні SSH.
- налаштування тактової частоти на DCE-інтерфейсах - для інтерфейсів з роллю DCE буде налаштовано значення тактової частоти, що важливо для синхронізації при передачі даних.
- аудит та відправка повідомлень - за допомогою локальної бази буде налаштовано аудит, який фіксує початок та завершення сесій exec, забезпечуючи можливість відстеження активності користувачів на пристрої.

Виконуємо налаштування для пристроїв Bichevnyk_Router_1, Bichevnyk_Router_2, Bichevnyk_Router_3, Bichevnyk_Router_4, Bichevnyk_Router_0, Bichevnyk_Router_IPS, Bichevnyk_Switch_1.1, Bichevnyk_Switch_1.2,

Bichevnyk_Switch_1.3, Bichevnyk_Switch_2, Bichevnyk_Switch_3, Bichevnyk_Switch_4.1, Bichevnyk_Switch_4.2, Bichevnyk_Switch_4.3, Bichevnyk_Switch_5.

Фрагмент налаштування маршрутизатора Bichevnyk_Router_1:

Router(config)#hostname Bichevnyk_Router_1

Bichevnyk_Router_1(config)#line console 0

Bichevnyk_Router_1(config-line)#password cisco

Bichevnyk_Router_1(config-line)#login

Bichevnyk_Router_1(config-line)#exit

Bichevnyk_Router_1(config)#line vty 0 15

Bichevnyk_Router_1(config-line)#password cisco

Bichevnyk_Router_1(config-line)#login

Bichevnyk_Router_1(config-line)#exit

Bichevnyk_Router_1(config)#enable secret class

Bichevnyk_Router_1(config)#service password-encryption

Bichevnyk_Router_1(config)#banner motd #Bichevnyk_Router_1. This is a secure system. Authorized Access Only!#

Bichevnyk_Router_1(config)#ip domain name Bichevnyk_Router_1

Bichevnyk_Router_1(config)#ip ssh version 2

Bichevnyk_Router_1(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

Bichevnyk_Router_1(config)#username 12321sk1_Bichevnyk privilege 15 password admincisco

Bichevnyk_Router_1(config)#line vty 0 15

Bichevnyk_Router_1(config-line)#transport input ssh

Bichevnyk_Router_1(config-line)#login local

Bichevnyk_Router_1(config-line)#exec-time 60 0

Bichevnyk_Router_1(config)#int g0/0

Bichevnyk_Router_1(config-if)#no sh duwn

Bichevnyk_Router_1(config-if)#ip addr 10.0.14.14 255.255.255.252

Bichevnyk_Router_1(config-if)#exit

Bichevnyk_Router_2(config-if)#clock rate 128000

Фрагмент налаштування маршрутизатора Bichevnyk_Switch_1.1:

Switch(config)#hostname Bichevnyk_Switch_1.1

Bichevnyk_Switch_1.1 (config)#line console 0

Bichevnyk_Switch_1.1 (config-line)#password cisco

Bichevnyk_Switch_1.1 (config-line)#login

Bichevnyk_Switch_1.1 (config-line)#exit

Bichevnyk_Switch_1.1 (config)#line vty 0 15

Bichevnyk_Switch_1.1 (config-line)#password cisco

Bichevnyk_Switch_1.1 (config-line)#login

Bichevnyk_Switch_1.1 (config-line)#exit

Bichevnyk_Switch_1.1 (config)#enable secret class

Bichevnyk_Switch_1.1 (config)#service password-encryption

Bichevnyk_Switch_1.1 (config)#banner motd # Bichevnyk_Switch_1.1. This is a secure system. Authorized Access Only!#

3.4.2 Налаштування маршрутизаторів в КС Придніпровської залізниці

Протокол OSPF (Open Shortest Path First) - це протокол маршрутизації, який використовується в комп'ютерних мережах для визначення найкоротших шляхів для передачі даних. OSPF є одним з найбільш поширених протоколів маршрутизації в Інтернеті та корпоративних мережах через його ефективність, гнучкість та масштабованість [9].

Обираючи OSPF для мережі Придніпровської залізниці, ми раціонально обираємо цей протокол з наступних причин:

− ефективність у мережах з множинним доступом: OSPF ефективно працює в мережах з множинним доступом, таких як Ethernet, завдяки механізму обрання призначеного маршрутизатора (DR) і резервного призначеного маршрутизатора (BDR). Це дозволяє зменшити кількість непотрібного трафіку LSA і зменшує навантаження на процесори маршрутизаторів;

− оптимізація роботи великих мереж: OSPF є масштабованим протоколом,

що дозволяє працювати великим мережам. Він динамічно адаптується до змін у мережі, шукаючи найкоротші шляхи до кожного вузла;

− динамічне виявлення змін у мережі: OSPF виявляє зміни в топології мережі та швидко виконує перерахунок маршрутів для адаптації до нових умов. Це дозволяє забезпечити стабільну та ефективну роботу мережі навіть у разі збоїв або змін в топології;

− підтримка різних типів маршрутів: OSPF підтримує різні типи маршрутів, що дозволяє використовувати його в різноманітних мережних середовищах.

На рис.3.1 наведено фрагмент налаштування протоколу OSPF для Bichevnyk_Router_1.

```
Bichevnyk_Router_1>enable
Bichevnyk_Router_1#configure terminal
Bichevnyk_Router_1(config)#ip dhcp excluded-address 172.24.17.65 172.24.17.70
Bichevnyk_Router_1(config)#exit
Bichevnyk_Router_1#configure terminal
Bichevnyk_Router_1(config)#ip dhcp pool Lan5pool
Bichevnyk_Router_1(config-dhcp)#network 172.24.17.64 255.255.255.128
Bichevnyk_Router_1(config-dhcp)#default-router 172.24.17.65
Bichevnyk_Router_1(config-dhcp)#dns-server 172.24.17.66
Bichevnyk_Router_1(config-dhcp)#domain-name wr
Bichevnyk_Router_1(config-dhcp)#exit
Bichevnyk_Router_1(config)#interface GigabitEthernet0/0
Bichevnyk_Router_1(config-if)#ip address 10.0.14.14 255.255.255.252
Bichevnyk_Router_1(config-if)#duplex auto
Bichevnyk_Router_1(config-if)#speed auto
Bichevnyk_Router_1(config-if)#exit
Bichevnyk_Router_1(config)#interface GigabitEthernet0/1
Bichevnyk_Router_1(config-if)#ip address 172.24.17.64 255.255.255.128
Bichevnyk_Router_1(config-if)#duplex auto
Bichevnyk_Router_1(config-if)#speed auto
Bichevnyk_Router_1(config-if)#exit
Bichevnyk_Router_1(config)#interface GigabitEthernet0/2
Bichevnyk_Router_1(config-if)#no ip address
Bichevnyk_Router_1(config-if)#duplex auto
Bichevnyk_Router_1(config-if)#speed auto
Bichevnyk_Router_1(config-if)#shutdown
Bichevnyk_Router_1(config-if)#exit
Bichevnyk_Router_1(config)#interface Vlan1
Bichevnyk_Router_1(config-if)#no ip address
Bichevnyk_Router_1(config-if)#shutdown
Bichevnyk_Router_1(config-if)#exit
Bichevnyk_Router_1(config)#router ospf 9
Bichevnyk_Router_1(config-router)#log-adjacency-changes
Bichevnyk_Router_1(config-router)#network 172.24.17.64 0.0.0.127 area 0
Bichevnyk_Router_1(config-router)#network 10.0.14.12 0.0.0.3 area 0
Bichevnyk_Router_1(config-router)#exit
Bichevnyk_Router_1(config)#exit
Bichevnyk_Router_1#write memory
```

Рисунок 3.1 – Налаштування маршрутизатора Bichevnyk_Router_1

На рис.3.2 наведено фрагмент налаштування протоколу OSPF для Bichevnyk_Router_3.

```
Bichevnyk_Router_3(config)# ip dhcp pool Lan4pool
Bichevnyk_Router_3(dhcp-config)# network 172.24.17.0 255.255.255.192
Bichevnyk_Router_3(dhcp-config)# default-router 172.24.17.1
Bichevnyk_Router_3(dhcp-config)# dns-server 172.24.17.2
Bichevnyk_Router_3(config)# ip dhcp pool Lan5pool
Bichevnyk_Router_3(dhcp-config)# network 172.24.17.0 255.255.255.128
Bichevnyk_Router_3(dhcp-config)# default-router 172.24.17.65
Bichevnyk_Router_3(dhcp-config)# dns-server 172.24.17.66
Bichevnyk_Router_3(dhcp-config)# domain-name wr
Bichevnyk_Router_3(config)# interface GigabitEthernet0/0
Bichevnyk_Router_3(config-if)# ip address 172.24.16.65 255.255.255.128
Bichevnyk_Router_3(config-if)# duplex auto
Bichevnyk_Router_3(config-if)# speed auto
Bichevnyk_Router_3(config)# interface GigabitEthernet0/1
Bichevnyk_Router_3(config-if)# ip address 10.0.14.6 255.255.255.252
Bichevnyk_Router_3(config-if)# duplex auto
Bichevnyk_Router_3(config-if)# speed auto
Bichevnyk_Router_3(config)# interface GigabitEthernet0/2
Bichevnyk_Router_3(config-if)# ip address 172.24.17.1 255.255.255.192
Bichevnyk_Router_3(config-if)# duplex auto
Bichevnyk_Router_3(config-if)# speed auto
Bichevnyk_Router_3(config)# interface Serial0/1/0
Bichevnyk_Router_3(config-if)# bandwidth 128
Bichevnyk_Router_3(config-if)# ip address 10.0.14.2 255.255.255.252
Bichevnyk_Router_3(config-if)# ip ospf cost 7500
Bichevnyk_Router_3(config)# interface Serial0/1/1
Bichevnyk_Router_3(config-if)# no ip address
Bichevnyk_Router_3(config-if)# clock rate 2000000
Bichevnyk_Router_3(config-if)# shutdown
Bichevnyk_Router_3(config)# interface Vlan1
Bichevnyk_Router_3(config-if)# no ip address
Bichevnyk_Router_3(config-if)# shutdown
Bichevnyk_Router_3(config)# router ospf 9
Bichevnyk_Router_3(config-router)# log-adjacency-changes
Bichevnyk_Router_3(config-router)# network 10.0.14.4 0.0.0.3 area 0
Bichevnyk_Router_3(config-router)# network 172.23.153.32 0.0.0.15 area 0
Bichevnyk_Router_3(config-router)# network 172.24.17.0 0.0.0.127 area 0
Bichevnyk_Router_3(config-router)# network 172.24.16.0 0.0.0.127 area 0
Bichevnyk_Router_3(config-router)# network 10.0.14.12 0.0.0.3 area 0
```

Рисунок 3.2 – Налаштування маршрутизатора Bichevnyk_Router_3

3.4.3 Налаштування служби AAA на маршрутизаторах

Служба AAA (Authentication, Authorization, and Accounting) є важливою складовою будь-якої мережевої інфраструктури і відповідає за забезпечення безпеки та керування доступом до ресурсів мережі [10].

Аутентифікація - це процес перевірки ідентичності користувача або пристрою перед наданням доступу до мережевих ресурсів.Завдяки службі AAA, мережеві пристрої можуть перевіряти облікові дані користувачів, такі як ім'я користувача та пароль, для забезпечення вірогідності їхньої ідентичності.

Авторизація - це процес визначення прав доступу після успішної аутентифікації користувача. Після успішної аутентифікації служба AAA дозволяє

налаштувати, які ресурси, послуги або операції може виконувати користувач в рамках мережі.

Accounting (облік) - це процес ведення журналів інформації про використання мережевих ресурсів користувачем під час сеансу взаємодії з мережею.

Служба AAA дозволяє реєструвати і зберігати дані про вхід і вихід користувача, обсяг переданих даних, час використання послуг тощо. Це корисно для аналізу використання ресурсів, аудиту та звітності.

Використання служби AAA в мережевій інфраструктурі дозволяє підвищити безпеку, контроль доступу та ефективність використання ресурсів, роблячи мережу більш управляючою і безпечною.

```
Bichevnyk_Router_3(config)#aaa new-model
Bichevnyk_Router_3(config)#aaa authentication login default group radius local

#Налаштування RADIUS-сервера:
Bichevnyk_Router_3(config)#radius server serverRadius
Bichevnyk_Router_3(config-radius-server)#addr ipv4 172.24.16.67
Bichevnyk_Router_3(config-radius-server)#key radius123
Bichevnyk_Router_3(config-radius-server)#exit

#Налаштування аутентифікації для консольної лінії та VTY:
Bichevnyk_Router_3(config)#line console 0
Bichevnyk_Router_3(config-line)#login authentication default
Bichevnyk_Router_3(config-line)#line vty 0 15
Bichevnyk_Router_3(config-line)#login authentication default
```

Рисунок 3.3 – Налаштування служби AAA на Bichevnyk_Router_3

Для налаштування RADIUS-сервера (рис.3.4) потрібно:

– створення нового користувача або використання існуючого: додати нового користувача на RADIUS-сервері або використовуйте існуючих;

– визначити IP-адресу RADIUS-сервера, ключ для автентифікації (пароль) та інші необхідні параметри;

– зберегти налаштування і перезавантажте службу RADIUS для застосування змін.

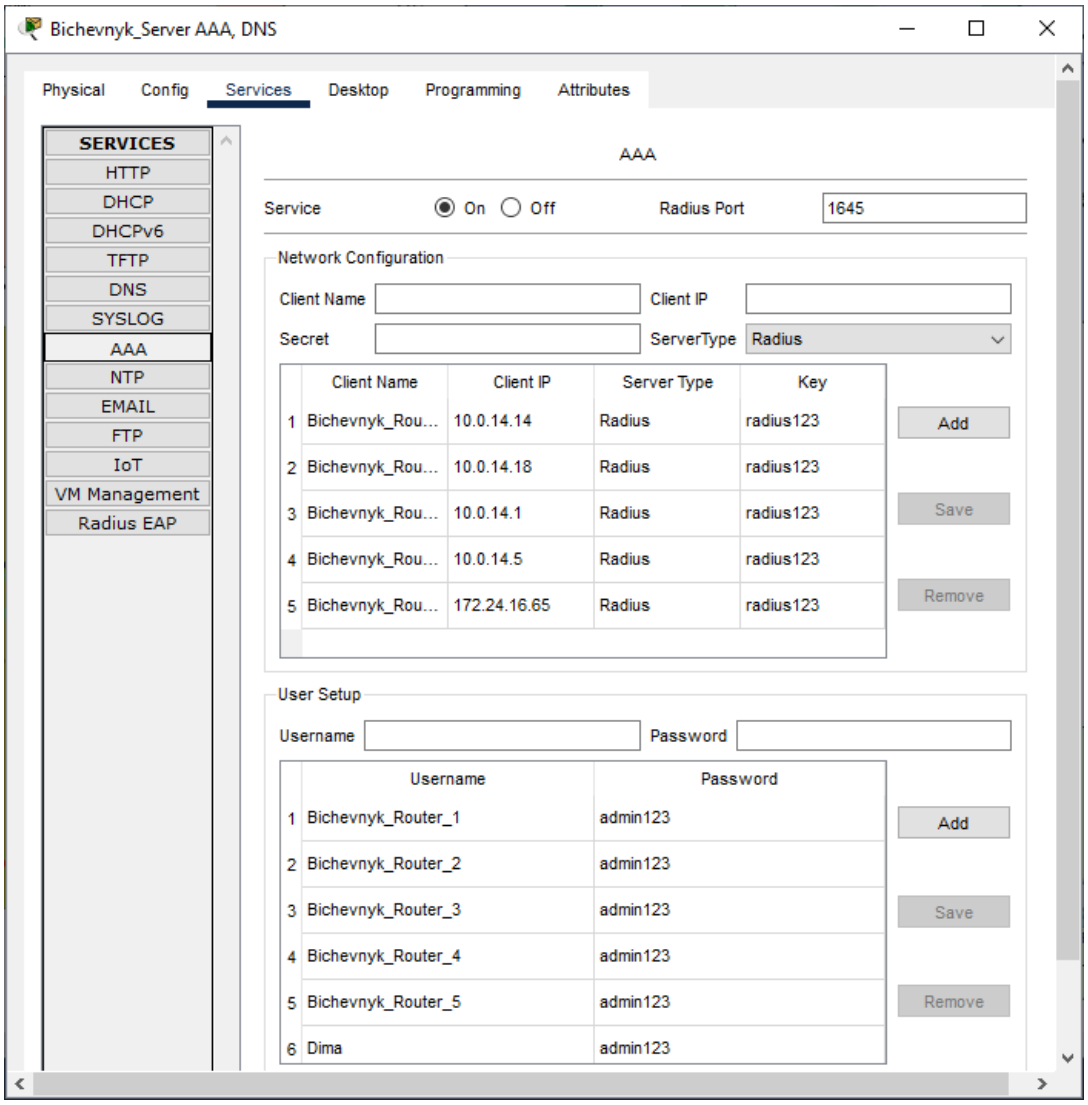


Рисунок 3.4 – Налаштування RADIUS-сервера

На рис.3.5 представлено успішний доступ до маршрутизатора Bichevnyk_Router_3 з використанням сервера RADIUS.

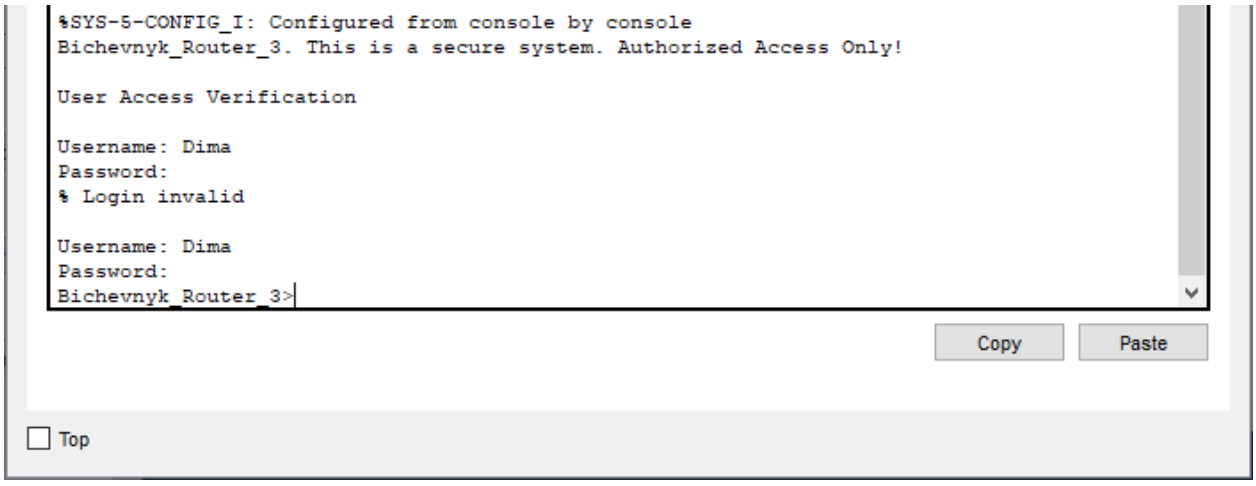


Рисунок 3.5 – Вхід через RADIUS сервер

3.4.4 Налаштування роботи Інтернету в КС Придніпровської залізниці

NAT (Network Address Translation) - це технологія, що використовується в комп'ютерних мережах для перетворення IP-адрес. Головною метою NAT є перетворення локальних IP-адрес (зазвичай внутрішньої мережі) на глобальні IP-адреси, які використовуються в Інтернеті, і навпаки. Це дозволяє більш ефективно використовувати обмежений пул доступних IP-адрес [11].

Static NAT встановлює постійний відповідний зв'язок між локальною та глобальною IP-адресами. Це часто використовується для доступу до внутрішніх ресурсів з Інтернету.

Dynamic NAT автоматично надає доступну глобальну IP-адресу з пулу для кожного внутрішнього пристрою, який виходить в Інтернет. Це дозволяє економити глобальні IP-адреси, оскільки вони не прив'язані до конкретних пристроїв.

PAT (Port Address Translation) відомий як NAT з використанням перекладу портів, PAT використовує одну глобальну IP-адресу для перетворення локальних IP-адрес разом з номерами портів TCP або UDP. Це робить можливим використання однієї глобальної IP-адреси для багатьох пристроїв одночасно.

Щоб налаштувати NAT на маршрутизаторі Cisco, виконано наступні кроки.

Спочатку потрібно створити списки контролю доступу (ACL), які визначають, які IP-адреси та порти будуть перекладені.

Налаштовуємо статичний NAT.

Встановлюємо правила перекладу, вказавши, які локальні IP-адреси мають бути перекладені на глобальні IP-адреси.

Визначаємо, які інтерфейси маршрутизатора будуть використовуватися для NAT.

Вмикаємо NAT на маршрутизаторі, застосувавши налаштування, які ви створили.

```
Bichevnyk_Router_4(config)#ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.25!
Bichevnyk_Router_4(config)#ip nat inside source list 114 pool Internet
Bichevnyk_Router_4(config)#ip nat inside source static 172.23.153.45 209.165.202.4
Bichevnyk_Router_4(config)#ip classless
Bichevnyk_Router_4(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1
Bichevnyk_Router_4(config)#ip flow-export version 9
Bichevnyk_Router_4(config)#ip access-list extended VPN
Bichevnyk_Router_4(config-ext-nacl)#permit ip 172.24.152.0 0.0.7.255 172.24.153.0 0.0.0.31
Bichevnyk_Router_4(config)#access-list 14 permit 172.24.152.0 0.0.7.255
Bichevnyk_Router_4(config)#access-list 114 deny ip 172.24.152.0 0.0.7.255 172.24.153.0 0.0.0.31
Bichevnyk_Router_4(config)#access-list 114 permit ip 172.24.152.0 0.0.7.255 any
Bichevnyk_Router_4(config)#access-list 100 permit ip any 209.165.202.0 0.0.0.31
Bichevnyk_Router_4(config)#access-list 100 permit ospf any any
```

Рисунок 3.6 – Фрагмент налаштування протоколу NAT

На рисунку 3.7 зображено таблицю перетворень NAT на маршрутизаторі Bichevnyk_Router_4.

NAT Table for Bichevnyk_Router_4

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.202.9:4	172.24.152.37:4	209.165.201.5:4	209.165.201.5:4
icmp	209.165.202.9:5	172.24.152.37:5	209.165.201.5:5	209.165.201.5:5
icmp	209.165.202.8:2	172.24.17.6:2	209.165.201.5:2	209.165.201.5:2
icmp	209.165.202.7:5	172.24.17.7:5	209.165.201.5:5	209.165.201.5:5
icmp	209.165.202.7:6	172.24.17.7:6	209.165.201.5:6	209.165.201.5:6
icmp	209.165.202.7:7	172.24.17.7:7	209.165.201.5:7	209.165.201.5:7

Рисунок 3.7 – Таблиця NAT for Bichevnyk_Router_4

3.4.5 Налаштування роботи VPN в КС Придніпровської залізниці

Для забезпечення безпеки та конфіденційності у мережевих комунікаціях

запропоновано налаштувати протокол IPsec (Internet Protocol Security) і VPN (Virtual Private Network).

IPsec використовується для захисту IP-пакетів шляхом шифрування та аутентифікації даних, що передаються через мережу. Він забезпечує конфіденційність, цілісність та аутентифікацію даних у відкритих мережах, таких як Інтернет.

Для налаштування IPsec потрібно визначити параметри шифрування, аутентифікації та ключі шифрування. Це включає в себе вибір алгоритмів шифрування (наприклад, AES, 3DES), методів аутентифікації (наприклад, HMAC, RSA) та обміну ключів (наприклад, через протокол IKE).

VPN використовується для створення захищеної тунелювання між двома або більше вузлами через ненадійну мережу, таку як Інтернет. Він дозволяє організаціям підключати віддалені мережі або працівників до центральної мережі з використанням шифрування трафіку та ідентифікації користувачів (рис.3.8).

Налаштування VPN включає в себе вибір протоколів тунелювання (наприклад, IPsec, SSL/TLS), налаштування ідентифікації користувачів (наприклад, з використанням ім'я користувача та пароля або сертифікатів), а також налаштування параметрів маршрутизації для віртуальних інтерфейсів VPN.

Ці технології дозволяють організаціям захищати свої мережі від несанкціонованого доступу та перехоплення даних, що є критично важливим у сучасному світі інтернет-комунікацій.

```
Bichevnyk_Router_4(config)#ip access-list extended VPN

Bichevnyk_Router_4(config-ext-nacl)#permit ip 172.24.152.0 0.0.7.255 172.24.153.0 0.0.0.31

Bichevnyk_Router_4(config)#access-list 14 permit 172.24.152.0 0.0.7.255

Bichevnyk_Router_4(config)#access-list 114 deny ip 172.24.152.0 0.0.7.255 172.24.153.0 0.0.0.31

Bichevnyk_Router_4(config)#access-list 114 permit ip 172.24.152.0 0.0.7.255 any

Bichevnyk_Router_4(config)#access-list 100 permit ip any 209.165.202.0 0.0.0.31

Bichevnyk_Router_4(config)#access-list 100 permit ospf any any

Bichevnyk_Router_4(config)#crypto isakmp policy 1
Bichevnyk_Router_4(config-isakmp)#encryption aes 256
Bichevnyk_Router_4(config-isakmp)#authentication pre-share
Bichevnyk_Router_4(config-isakmp)#group
Bichevnyk_Router_4(config-crypto-map)#set peer 64.100.13.2
```

Рисунок 3.8 – Фрагмент налаштування VPN, IPsec for Bichevnyk_Router_4

Результат працездатності налаштованих протоколів наведено на рис. 3.9.

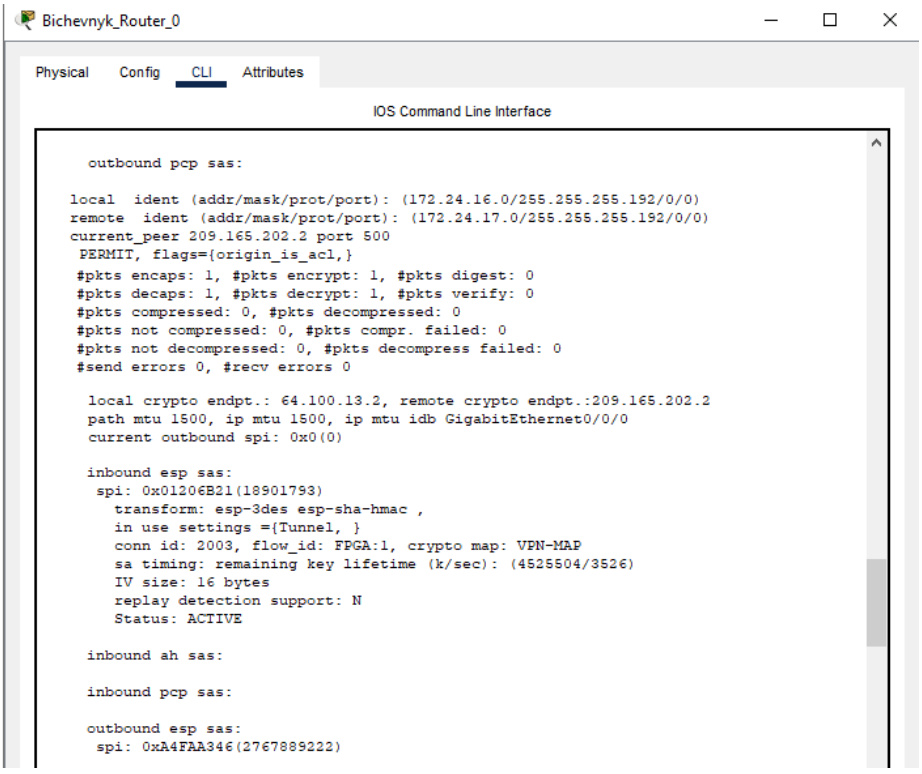


Рисунок 3.9 – Перевірка роботи протоколів VPN, IPsec for Bichevnyk_Router_4

3.4.6 Налаштування агрегування каналів в підмережі «Центр обробки даних»

Протоколи PAgP (Port Aggregation Protocol) та LACP (Link Aggregation Control Protocol) використовуються для створення та керування агрегованими з'єднаннями, що дозволяють об'єднати кілька фізичних інтерфейсів в один логічний канал з метою збільшення пропускної здатності та надійності мережі.

PAgP - це Cisco-специфічний протокол, який працює тільки на комутаторах Cisco. Він дозволяє автоматично створювати та управляти агрегованими з'єднаннями портів між комутаторами. PAgP має різні режими роботи, такі як «auto», «desirable» та «on», які контролюють спосіб утворення та підтримки агрегованих з'єднань між комутаторами.

LACP - це стандарт IEEE 802.3ad, який може використовуватись на різних виробниках комутаторів. Він забезпечує створення та керування агрегованими з'єднаннями портів. LACP також має режими роботи, такі як «active» та «passive», які визначають, яка сторона ініціює утворення та підтримку агрегованого з'єднання.

Шляхом використання технології EtherChannel було здійснено злиття фізичних портів на комутаторах мережі LAN_3 з метою підвищення ефективності передачі даних. Це сприяє поєднанню кількох портів в одне віртуальне з'єднання, що забезпечує велику пропускну здатність та надійність мережі. Такий підхід дозволяє передавати дані паралельно через кілька портів одночасно, забезпечуючи балансування навантаження та підвищення пропускної здатності. В разі відмови одного з портів, інші продовжують працювати безперервно, що підвищує надійність каналу зв'язку.

На рис.3.10 наведено налаштування комутаторів.

```
Bichevnyk_Switch_1.1(config)#int range fa0/2-3, fa0/6-7
Bichevnyk_Switch_1.1(config-if-range)#switchport mode trunk

#Налаштування EtherChannel за допомогою протоколу Cisco PAgP   Bichevnyk_Switch_1.1:

Bichevnyk_Switch_1.1(config)#int range fa0/6-7
Bichevnyk_Switch_1.1(config-if-range)#sh
Bichevnyk_Switch_1.1(config-if-range)#channel-group 3 mode desirable
Bichevnyk_Switch_1.1(config-if-range)#
Creating a port-channel interface Port-channel 3
Bichevnyk_Switch_1.1(config-if-range)#no sh
Bichevnyk_Switch_1.1(config-if-range)#exit
Bichevnyk_Switch_1.1(config)#int port-channel 3
Bichevnyk_Switch_1.1(config-if)#switchport mode trunk

#Налаштування EtherChannel LACP 802.3ad :
Bichevnyk_Switch_1.2(config-if)#int range fa0/4-5
Bichevnyk_Switch_1.2(config-if-range)#sh
Bichevnyk_Switch_1.2(config-if-range)#channel-group 2 mode passive
Bichevnyk_Switch_1.2(config-if-range)#
Creating a port-channel interface Port-channel 2
Bichevnyk_Switch_1.2(config-if-range)#no sh
Bichevnyk_Switch_1.2(config-if-range)#exit
Bichevnyk_Switch_1.2(config)#int port-channel 2
Bichevnyk_Switch_1.2(config-if)#switchport mode trunk
```

Рисунок 3.10 – PAgP та LACP для Bichevnyk_Switch_1.2

Командою *show etherchennal summary* перевіряємо налаштування (рисунок 3.11). Аналогічно виконали для решти комутаторів в цій під мережі.

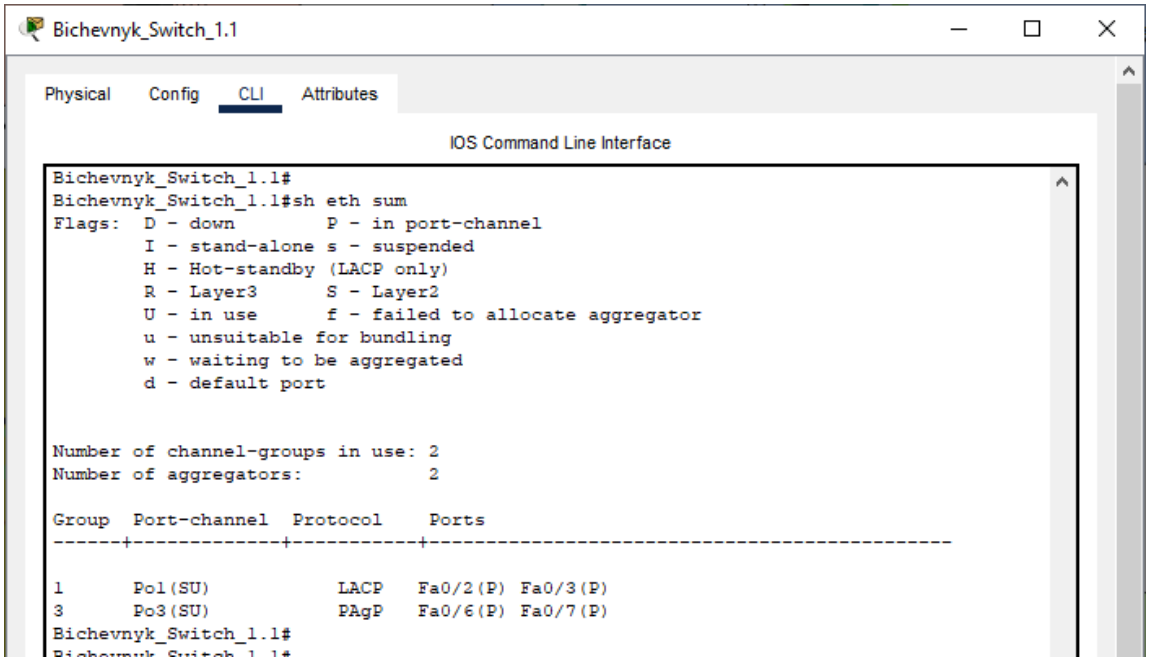


Рисунок 3.11 – Перевірка стану та конфігурації порт-каналів на комутаторі Bichevnyk_Switch_1.1

3.5 Захист інформації в КС Придніпровської залізниці

3.5.1 Налаштування VLAN в підмережі «Центр обробки даних»

Віртуальні локальні мережі (VLAN) є одним з ключових концепцій у мережевому дизайні, яка дозволяє розділити фізичну мережу на логічні групи. Кожна VLAN уявляє собою окремий домен мовлення, в якому пристрої можуть спілкуватися між собою без прямого зв'язку з пристроями з інших VLAN.

Таблиця 3.3 відображає розподіл підмережі "Центр обробки даних" на віртуальні локальні мережі (VLAN).

Таблиця 3.3 – Список мереж VLAN

Номер VLAN	Назва VLAN
1	default
24	Server
34	Storage
44	Network
99	Management
100	Native

Налаштування пристрої для виконання розподілення мережі на VLAN представлено на рис.3.12.

```
#Налаштування інтерфейсу GigabitEthernet0/1:

Bichevnyk_Switch_4.1 (config)#int g0/1
Bichevnyk_Switch_4.1 (config-if)#switchport mode trunk
Bichevnyk_Switch_4.1 (config-if)#switchport trunk native vlan 100
Bichevnyk_Switch_4.1 (config-if)#switchport trunk allowed vlan 24,34,44,99-100
Bichevnyk_Switch_4.1 (config-if)#no sh
```

Рисунок 3.12 – VLAN на комутаторі Bichevnyk_Switch_4.1

Далі створюємо VLAN 24, 34, 44, 99, 100 та привласнюємо ім’я кожному VLAN згідно табл. 3.3. Реалізація з використаними командами наведено на рис.3.13.

```
Bichevnyk_Switch_4.1 (config)#vlan 24
Bichevnyk_Switch_4.1 (config-vlan)#name Server
Bichevnyk_Switch_4.1 (config-vlan)#vlan 34
Bichevnyk_Switch_4.1 (config-vlan)#name Storage
Bichevnyk_Switch_4.1 (config-vlan)#vlan 44
Bichevnyk_Switch_4.1 (config-vlan)#name Network
Bichevnyk_Switch_4.1 (config-vlan)#vlan 99
Bichevnyk_Switch_4.1 (config-vlan)#name Management
Bichevnyk_Switch_4.1 (config-vlan)#vlan 100
Bichevnyk_Switch_4.1 (config-vlan)#name Native

Bichevnyk_Switch_4.1 (config)#int vlan 99
Bichevnyk_Switch_4.1 (config-if)#description LAN vlan_99_Sw4.1
Bichevnyk_Switch_4.1 (config-if)#ip add 172.24.152.98 255.255.255.248
Bichevnyk_Switch_4.1 (config-if)#no shut
Bichevnyk_Switch_4.1 (config-if)#ip default-gateway 172.24.152.97
```

Рисунок 3.13 – VLAN 24, 34, 44, 99, 100 на комутаторі Bichevnyk_Switch_4.1

Конфігурація інтерфейсів на комутаторах та визначення діапазону інтерфейсів для певних VLAN було налаштовано, прикладом цього є налаштування на комутаторі Bichevnyk_Switch_4.2 представлено на рис.3.14.

```
Bichevnyk_Switch_4.2(config-if-range)#int range fa0/15-24
Bichevnyk_Switch_4.2(config-if-range)#switchport mode access
Bichevnyk_Switch_4.2(config-if-range)#switchport access vlan 24
Bichevnyk_Switch_4.2(config-if-range)#no sh

Bichevnyk_Switch_4.2(config-if-range)#int range fa0/10-14
Bichevnyk_Switch_4.2(config-if-range)#switchport mode access
Bichevnyk_Switch_4.2(config-if-range)#switchport access vlan 34
Bichevnyk_Switch_4.2(config-if-range)#no sh

Bichevnyk_Switch_4.2(config-if-range)#int range fa0/5-9
Bichevnyk_Switch_4.2(config-if-range)#switchport mode access
Bichevnyk_Switch_4.2(config-if-range)#switchport access vlan 44
Bichevnyk_Switch_4.2(config-if-range)#no sh

Bichevnyk_Switch_4.2(config-vlan)#int range fa0/1, fa0/3-4, g0/1
Bichevnyk_Switch_4.2(config-if-range)#switchport mode access
Bichevnyk_Switch_4.2(config-if-range)#switchport access vlan 100
Bichevnyk_Switch_4.2(config-if-range)#do wr
```

Рисунок 3.14 – VLAN на комутаторі Bichevnyk_Switch_4.2

Рисунок 3.15 демонструє конфігурацію маршрутизатора, зокрема налаштування підінтерфейсів. Subinterface - це метод розділення фізичного інтерфейсу на кілька віртуальних логічних інтерфейсів. Кожен subinterface має свій власний ідентифікатор VLAN і може мати окремі налаштування мережевих параметрів.

```
Bichevnyk_Router_4(config)#int g0/0/0
Bichevnyk_Router_4(config-if)#no sh
Bichevnyk_Router_4(config-if)#int g0/0/0.24
Bichevnyk_Router_4(config-subif)#encapsulation dot1Q 24
Bichevnyk_Router_4(config-subif)#ip addr 172.24.152.1 255.255.255.224
Bichevnyk_Router_4(config-subif)#no sh
Bichevnyk_Router_4(config-subif)#int g0/0/0.34
Bichevnyk_Router_4(config-subif)#encapsulation dot1Q 34
Bichevnyk_Router_4(config-subif)#ip addr 172.24.152.33 255.255.255.224
Bichevnyk_Router_4(config-subif)#no sh
Bichevnyk_Router_4(config-subif)#int g0/0/0.44
Bichevnyk_Router_4(config-subif)#encapsulation dot1Q 44
Bichevnyk_Router_4(config-subif)#ip addr 172.24.152.65 255.255.255.224
Bichevnyk_Router_4(config-subif)#no sh
Bichevnyk_Router_4(config-subif)#int g0/0/0.99
Bichevnyk_Router_4(config-subif)#encapsulation dot1Q 99
Bichevnyk_Router_4(config-subif)#ip addr 172.24.152.97 255.255.255.248
Bichevnyk_Router_4(config-subif)#no sh
```

Рисунок 3.15 – Налаштування Subinterface

3.5.2 Перевірка роботи комп’ютерної системи

Для внутрішньої мережі було проведено тестування за допомогою команди ping. Конкретно, з мережі LAN4 було відправлено запит на exo до мережі LAN2. Наведені результати на рисунку 3.16 підтверджують працездатність мережі.

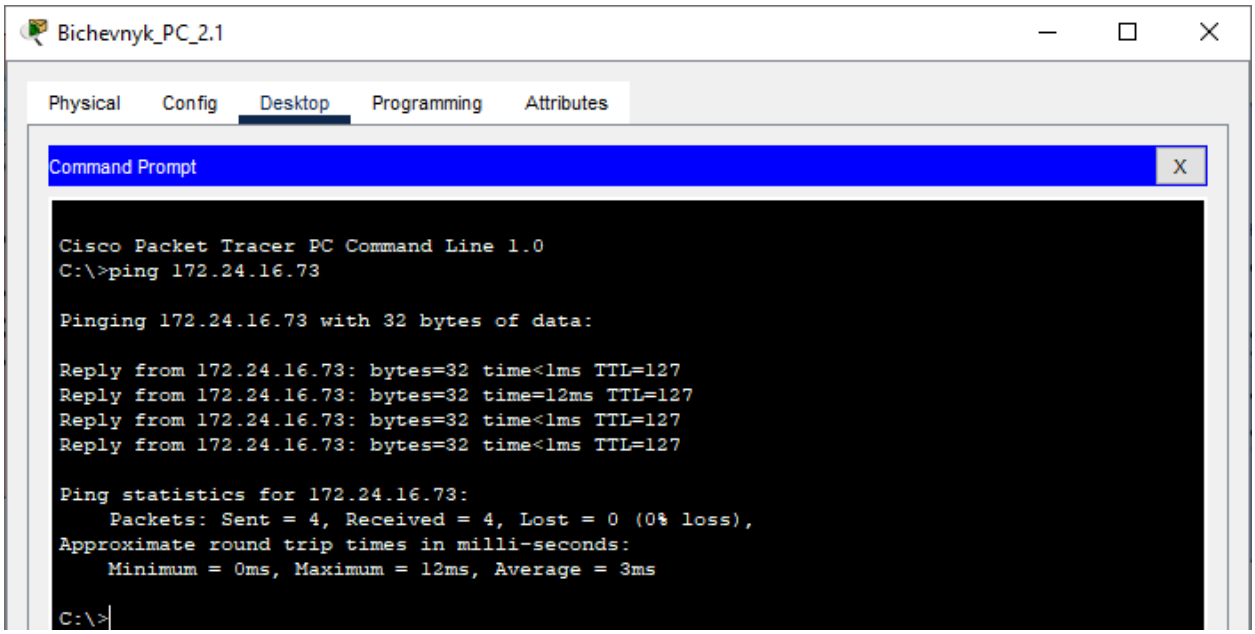


Рисунок 3.16 – Пінгування від ПК в мережі LAN4 до LAN2

Аналогічно було протестовані передачу пакетів з віддаленої мережі LAN3 на сервер HTTP (рисунок 3.17).

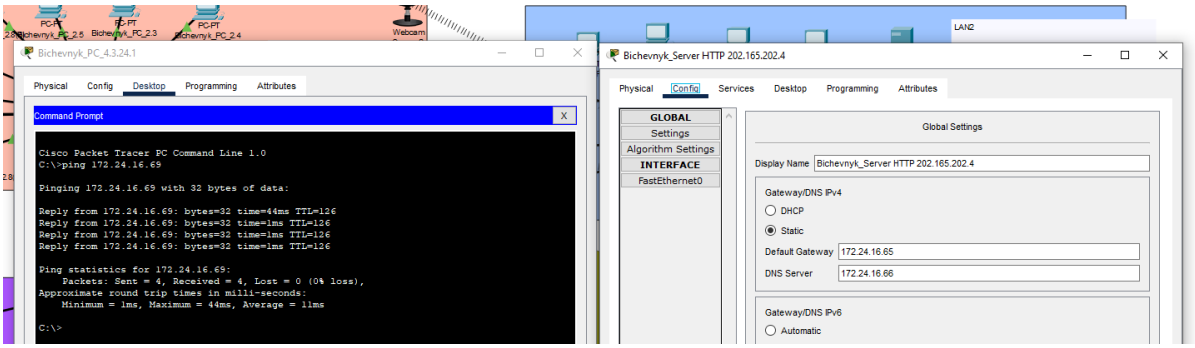


Рисунок 3.17 – Пінгування з LAN3 на сервер HTTP

Для тестування SSH з підмережі «LAN3» до маршрутизатора Bichevnyk _Router_5 можна використати командний рядок або програми клієнтського доступу SSH, такі як PuTTY. У командному рядку можна ввести команду типу ssh 12321sk1_ Bichevnyk. Після цього вас буде запрошено ввести пароль користувача (рис.3.18).

У випадку використання програми PuTTY, ви введете IP-адресу або ім'я пристрою, а потім натиснете кнопку "Open", після чого буде відкрито вікно терміналу, де вас буде запрошено ввести ім'я користувача та пароль.

Після успішного введення ім'я користувача та пароля, ви отримаєте доступ до командного рядка пристрою через протокол SSH, де зможете виконувати необхідні дії та налаштування.

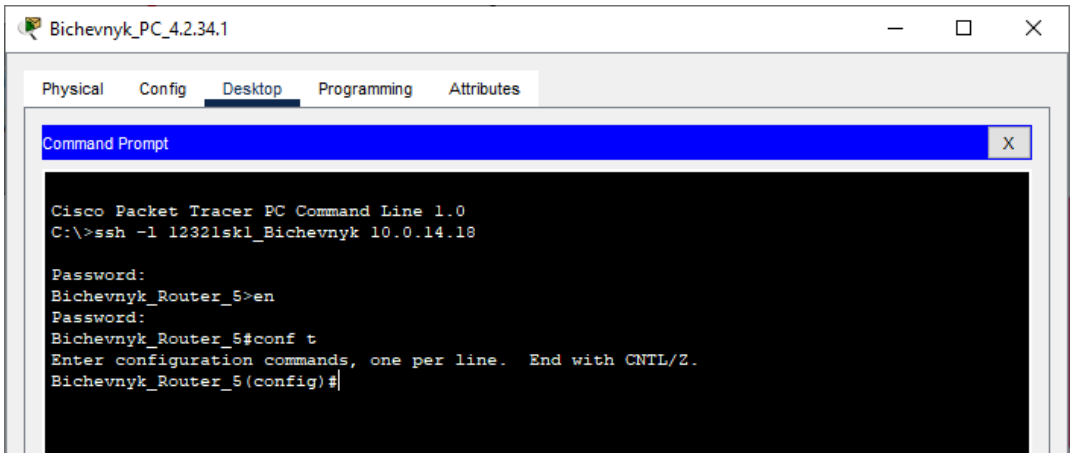


Рисунок 3.18 – Тестування SSH Bichevnyk _Router_5

Наступним етапом є використання команди show ip dhcp binding для відображення інформації про прив'язки DHCP-адрес до MAC-адрес інтерфейсів на маршрутизаторі Cisco. Вона показує, які IP-адреси були надані DHCP-сервером та яким пристроям (за їх MAC-адресами) ці адреси були надані (рис.3.19).

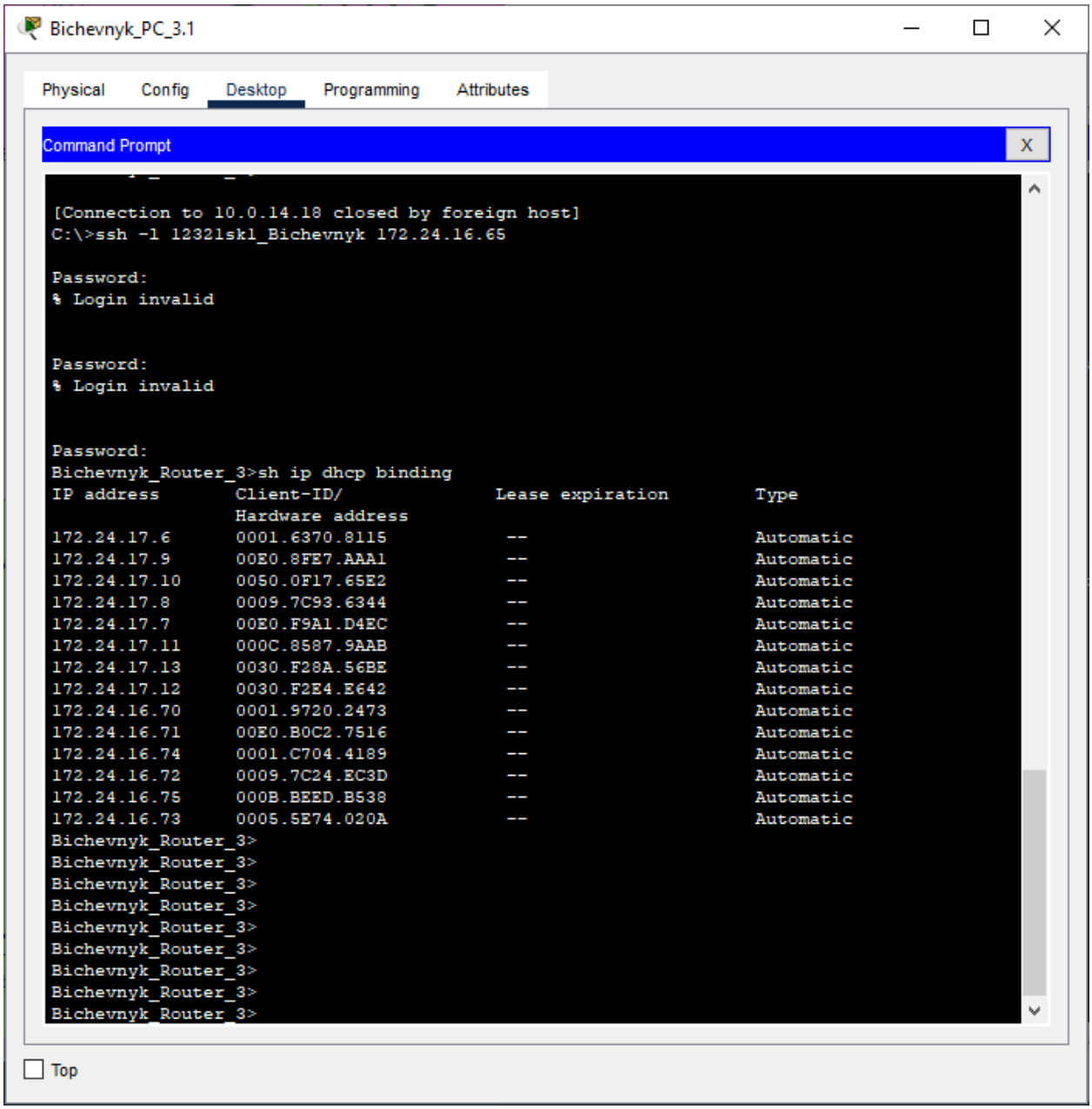


Рисунок 3.19 – Перевірка розподілу DHCP-адрес

З рис.3.19 можна побачити список усіх активних прив'язок ip-адрес до mac-адрес інтерфейсів, що були надані через dhcp. інформація може містити ip-адреси, mac-адреси, час виділення адреси, а також інші відомості, такі як використані параметри dhcp. це допомагає відстежувати, які пристрої отримали які ip-адреси від dhcp-сервера.

На рис.3.20 наведено результат налаштування протоколу OSPF.

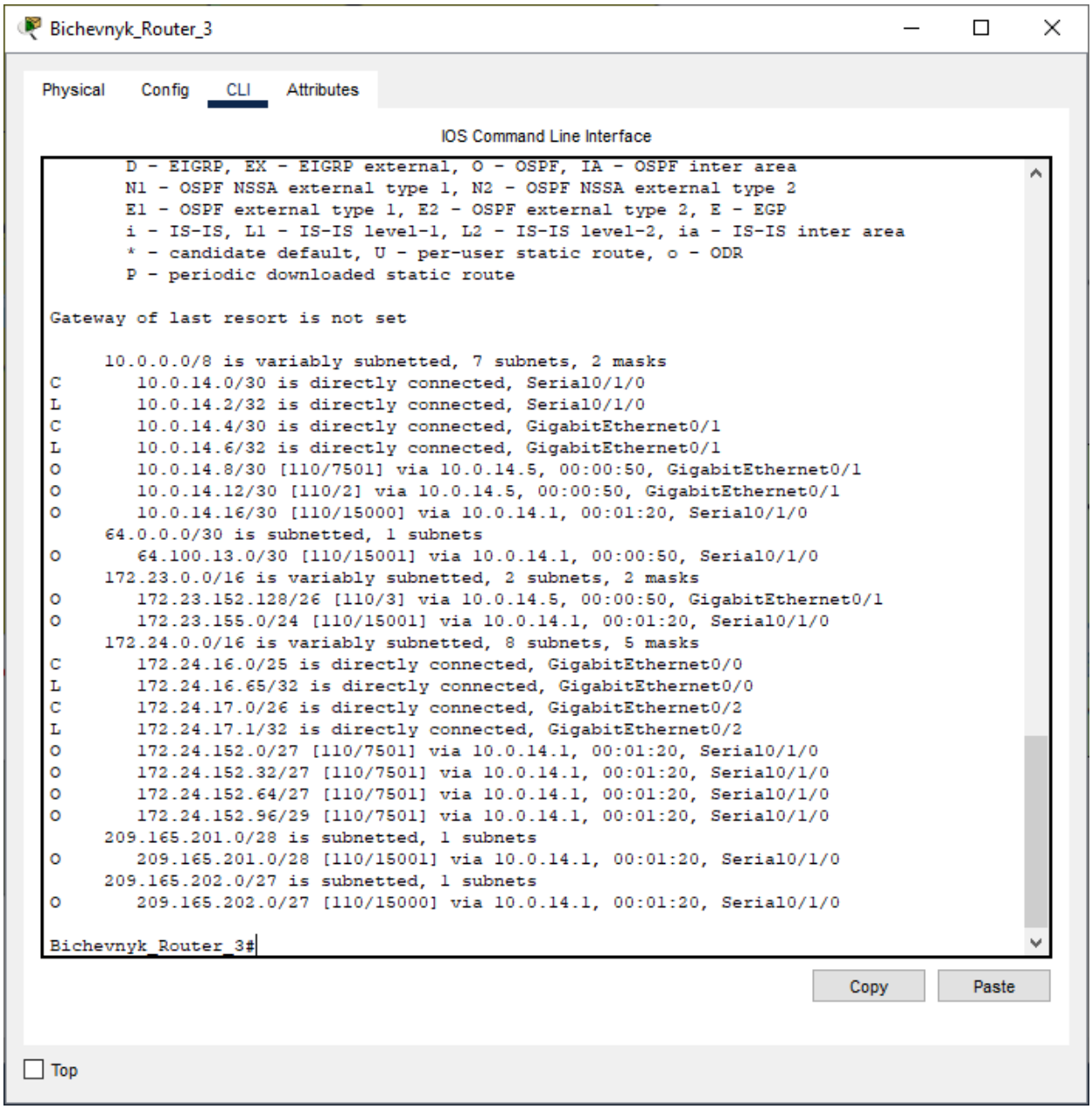


Рисунок 3.20 – Перевірка налаштування протоколу OSPF

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Розробка системи автоматичного управління залізничним переїздом

Термін "залізничний переїзд" описує місце, де залізнична колія або шлях перетинає автомобільну дорогу на одному рівні. За результатами соціологічних досліджень, 40% залізничних аварій стаються на залізничних переїздах через використання ручного відкривання воріт та необережність пасажирів. У багатьох випадках неможливо зупинити потяг на переїзді через наявність мандрівників або некваліфікованих операторів залізничних переїздів. Це пояснюється тим, що потяг має велику масу в порівнянні з гальмівним шляхом і потребує значного простору для зупинки. З метою попередження можливих аварій та смертельних випадків пропонується використання мікроконтролера і датчика зчитування для автоматизованого управління залізничним переїздом. Ця технологія дозволяє контролювати прохід переїзду для пішоходів і транспортних засобів, а також автоматично формувати міст на платформі для безпечного проходження потягів. Датчики зчитування надсилають сигнали мікроконтролеру під час проїзду потяга, який вживає відповідні заходи для керування приводним двигуном шлпгбауму і формування мосту на платформі, коли потяг покидає станцію.

Система автоматичного управління залізничним переїздом включає різноманітні компоненти, які разом утворюють його повний каркас. Серед цих компонентів можна виділити наступні:

- мікроконтролер ESP8266 (NodeMCU);
- датчик зчитування перемикача;
- фільтр випрямляч;
- трансформатор 12В;
- гвинтовий мотор-редуктор;
- рейковий механізм.

Ці компоненти відіграють ключову роль у забезпеченні роботи смарт-залізничного переїзду, кожен з них має свою функціональну важливість для забезпечення безпеки та ефективності переїзду. Для належної роботи кожного компонента системи потрібно виконати його апаратне підключення, як показано на

Рисунку 4.1. Цифрові виводи D1 та D4 NodeMCU повинні бути підключені до виводів Tring для забезпечення правильної роботи ультразвукових датчиків. Крім того, цифрові виводи D2 та D3 NodeMCU мають бути з'єднані з виводами Echo відповідних датчиків. До цифрових виводів D5 та D6 слід підключити зелений та червоний світлодіоди відповідно, а вивід D7 - до серводвигуна, а D8 - до зумера. Всі контакти GND компонентів мають бути підключені до контакту GND на NodeMCU. Крім того, живлення серводвигуна (5V) та VCC ультразвукового датчика також повинні бути підключені до контакту 3V на NodeMCU.

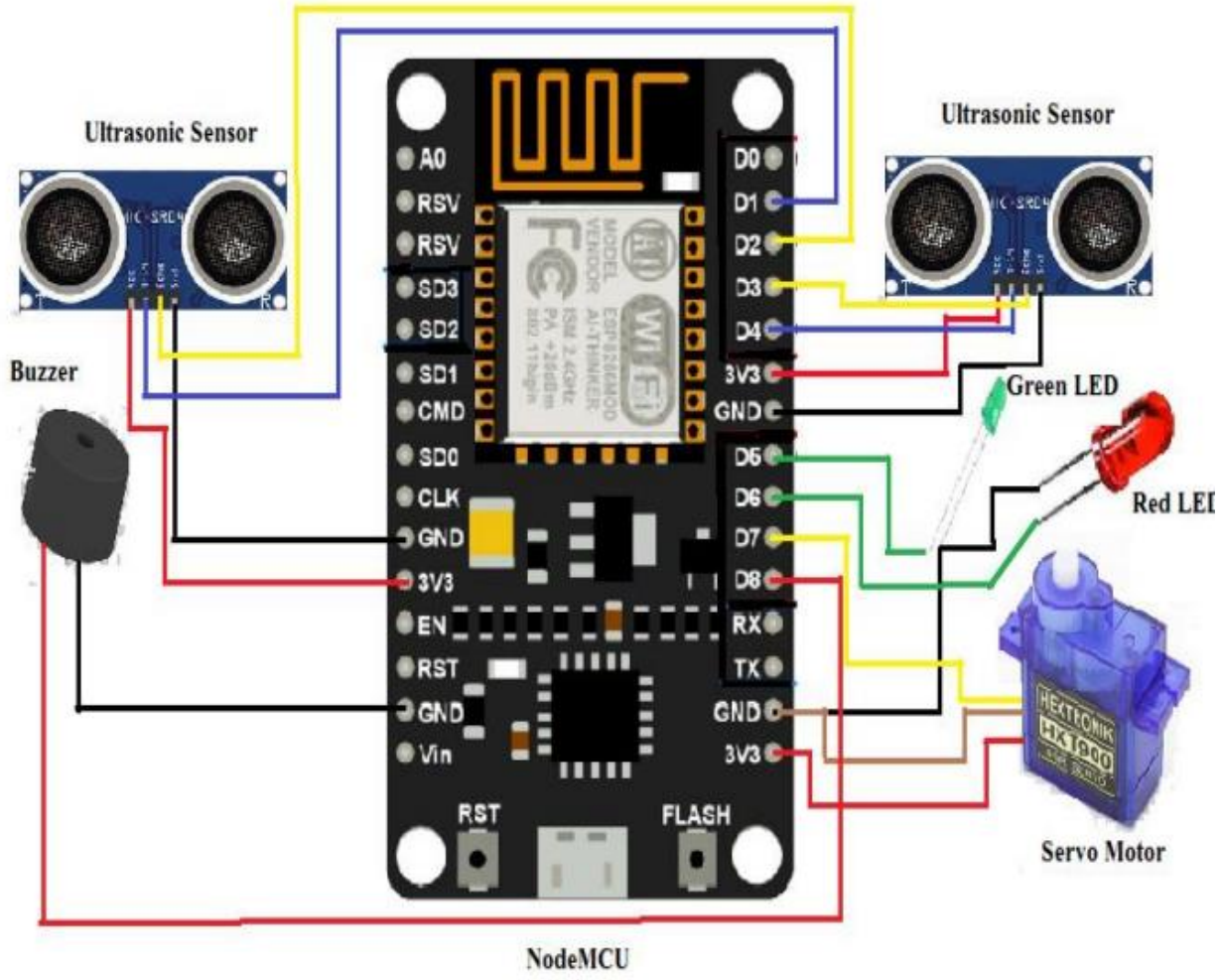


Рисунок 4.1 – Апаратне забезпечення та фізичне підключення

4.2 Алгоритм роботи системи автоматичного управління залізничним переїздом

У запропонованій системі використано датчики, чутливі до сили резистора, виявляє потяг, і мікроконтролер автоматично закриває шлагбаум. Після того, як

потяг перетне колію, стрілка буде піднята для транспортних засобів. Ми будемо використовувати Wi-Fi (Інтернет), щоб зробити систему більш ефективною, оскільки підключення до Інтернету не буде потрібне. Ця система зменшить навантаження, пов'язане з ручним переміщенням стрілочного переводу. Коли датчик FSR виявить потяг, пролунатиме звуковий сигнал. Після цього шлагбаум автоматично опускається, і жоден транспортний засіб не зможе проїхати через колію. З іншого боку, коли потяг рушить з місця, перекладина підніметься, щоб інші транспортні засоби могли проїхати через колію (рис.4.2).

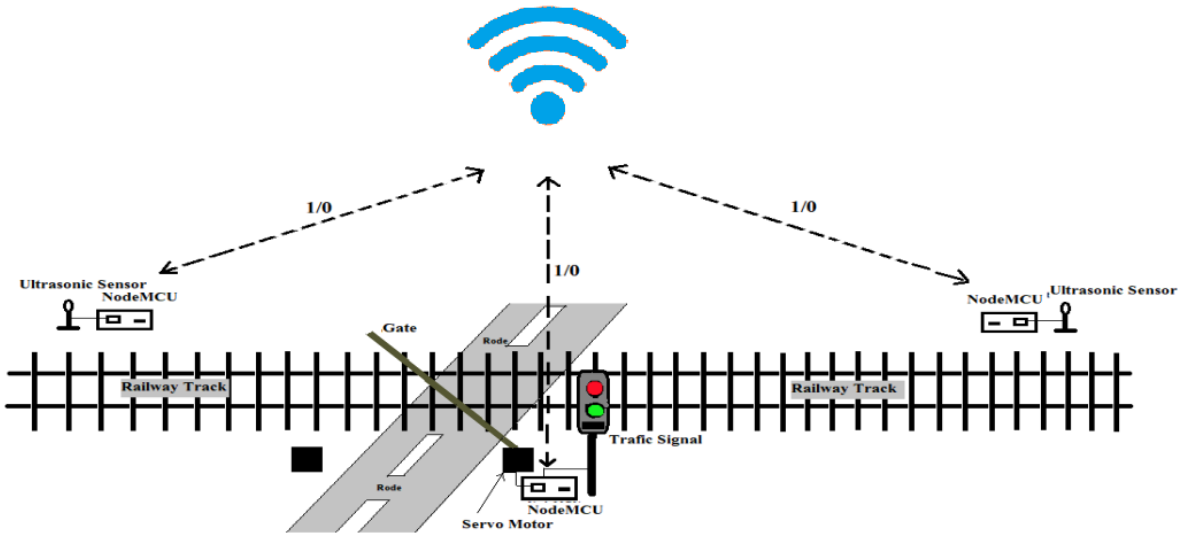


Рисунок 4.2 – Структурна схема автоматичного управління залізничним переїздом

Кожного разу, коли потяг прибуває і фіксується датчиком, він надсилає сигнал "1" до NodeMCU, який потім пересилає ці дані до Google Firebase. При отриманні змінених даних від датчика 1, розташованого на рівні переїзду, NodeMCU автоматично виконує виклик в центр управління переїздом.

NodeMCU, що розташований на рівні переїзду, відтворює звуковий сигнал зумера протягом декількох секунд, вимикає зелений світлодіод і увімкнює червоний, а також автоматично закриває ворота. Шлагбаум залишається зачиненим до моменту, коли поїзд від'їде від датчика 2.

Коли потяг від'їжджає від датчика 2, він знову відправляє дані "1" до бази даних Google. При зміні цих даних у базі та їх отриманні NodeMCU автоматично

відкриває ворота, вимикає червоний світлодіод і увімкнює зелений.

На рисунку 4.3 наведено алгоритм управління залізничним переїздом.

Рисунок 4.3 – Алгоритм системи управління залізничним переїздом

Алгоритм автоматичного опускання шлагбаума на залізничному переїзді можна розглядати з точки зору електромеханічної системи, що базується на деяких датчиках та регулюючих пристроях. Основні етапи цього процесу включають:

1. Активація системи. Підключення сенсорів, які реагують на фізичний тиск або рух потягу. Увімкнення звукового сигналу для попередження про наближення потягу.

2. Вимірювання відстані. Датчик дистанції аналізує відстань до потягу або його складових. Порівняння виміряної відстані з попередньо заданою нормою.

3. Керування шлагбаумом. Якщо виміряна відстань менша за норму, система вважає, що потяг наближається. Опускання шлагбаума для блокування дороги для

транспортних засобів.

4. Моніторинг потягу. Система виявляє, що потяг проходить через переїзд за допомогою силових чутливих резисторів або інших датчиків.

5. Підняття шлагбаума. Після того, як потяг пройшов, шлагбаум піднімається для відкриття шляху для транспорту.

6. Зупинка звукового сигналу. Після повного пройдення потягу звуковий сигнал вимикається.

4.3 Проектування моделі системи автоматичного управління залізничним переїздом

Проектування моделі системи автоматичного управління залізничним переїздом в Cisco PT використовує інтеграцію різноманітних компонентів, таких як датчики, поїзд з Wi-Fi модулем, два шлагбауми та системи відеоспостереження, для забезпечення безпеки та ефективності на залізничних переїздах. На рис.4.4 наведено реалізовану систему.

Рисунок 4.4 – Реалізація системи з IoT-датчиками

Налаштовуємо маршрутизатори та комутатори для забезпечення комунікації між всіма пристроями у мережі. Надаємо IP-адреси та налаштовуємо безпеку мережі. Встановлюємо поїзд у мережі та додаємо до нього Wi-Fi модуль.

Налаштовуємо модуль для передачі сигналів про своє місцезнаходження та стан до системи керування. Додаємо шлагбауми до мережі та налаштовуємо їх, щоб вони автоматично опускалися, коли система отримує сигнал від датчиків про наближення поїзда. Додаємо камери відеоспостереження до мережі та налаштовуємо їх для моніторингу руху транспорту та дій пасажирів на переїзді.

На рисунку 4.5 наведено алгоритм на JavaScript для опису проектування моделі системи автоматичного управління залізничним переїздом в середовищі Cisco Packet Tracer [12].

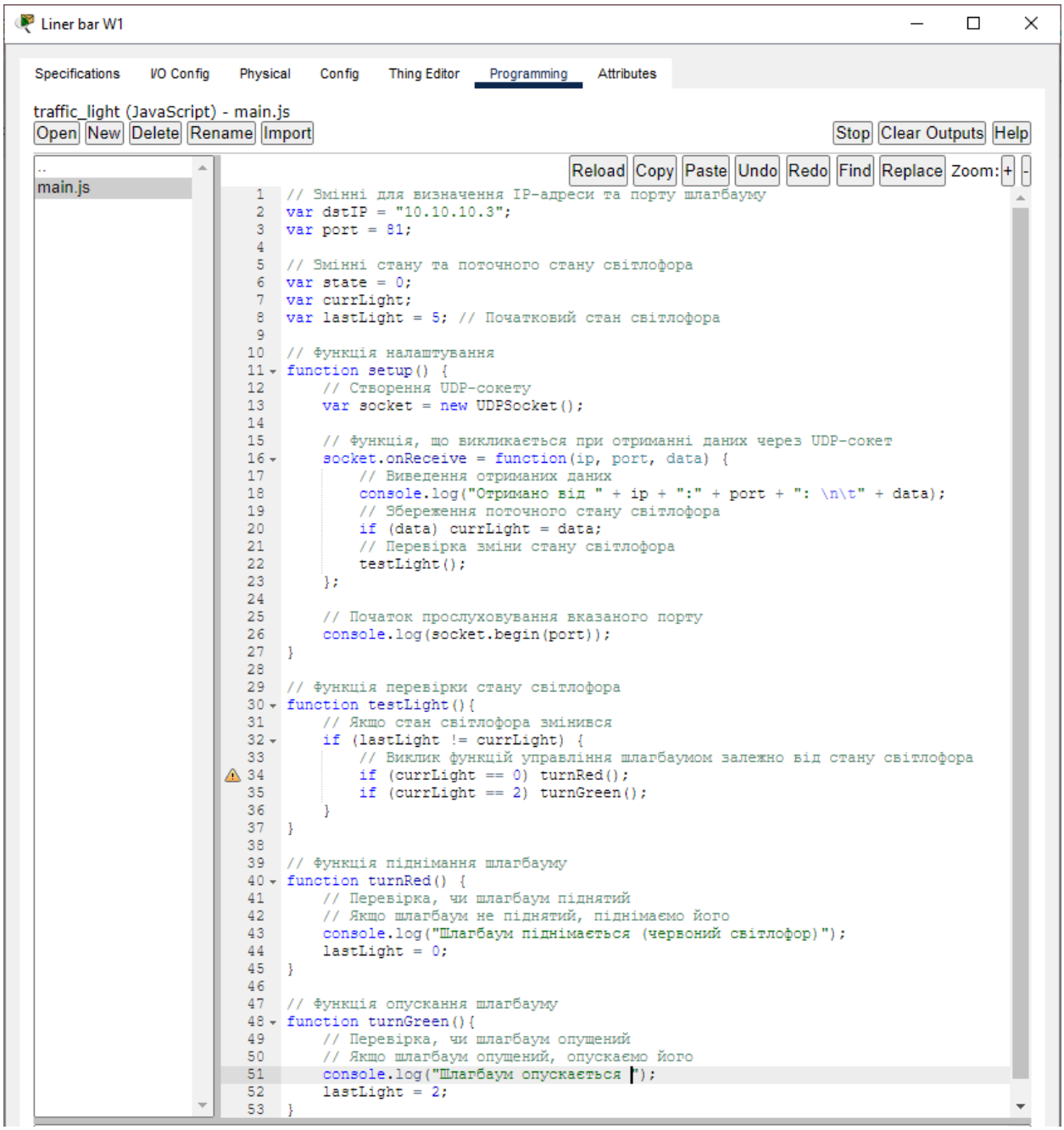


Рисунок 4.5 – JavaScript управління шлагбаумом

На рисунку 4.6 зображено дорогу, яка перетинає залізничну колію. Це місце, де автомобілі повинні перетнути залізничну колію. Поруч з дорогою розташований шлагбаум, який може опускатися та підніматися. Цей шлагбаум призначений для блокування руху автотранспорту під час перетину залізничної колії. На залізничній колії видно наближаючийся поїзд. Поїзд може мати вбудований Wi-Fi модуль або будь-який інший пристрій, який надсилає сигнали про своє наближення до системи управління переїздом.

Рисунок 4.6 – Автоматичне управління шлагбаумом

Усі "розумні" пристрої, які входять до складу системи, підключені до бездротової мережі, яка керується через домашній шлюз. Для їх підключення до цієї мережі налаштовані такі параметри, як ідентифікатор SSID, метод аутентифікації, ключ аутентифікації, отримання IP-адреси через DHCP, та вказано IoT-сервер (рис.4.7-рис.4.8).

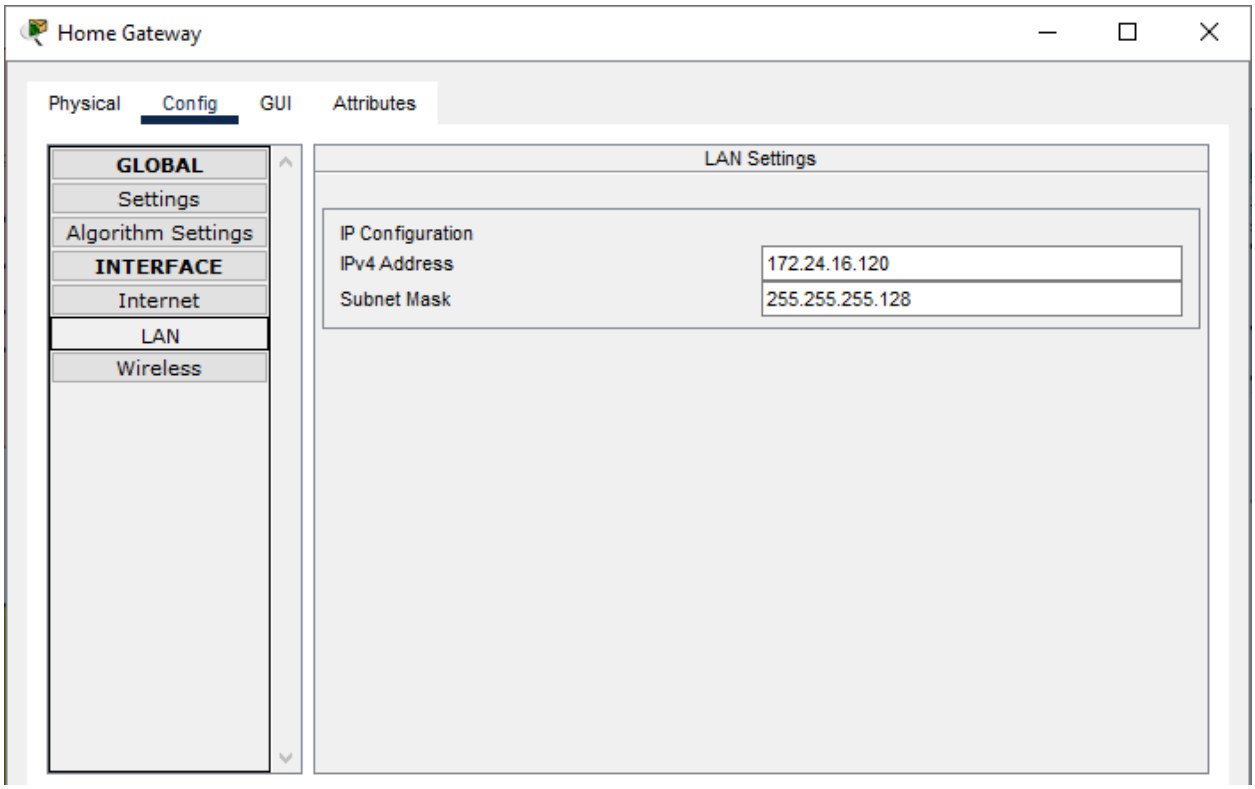


Рисунок 4.7 – Налаштування Home Gateway

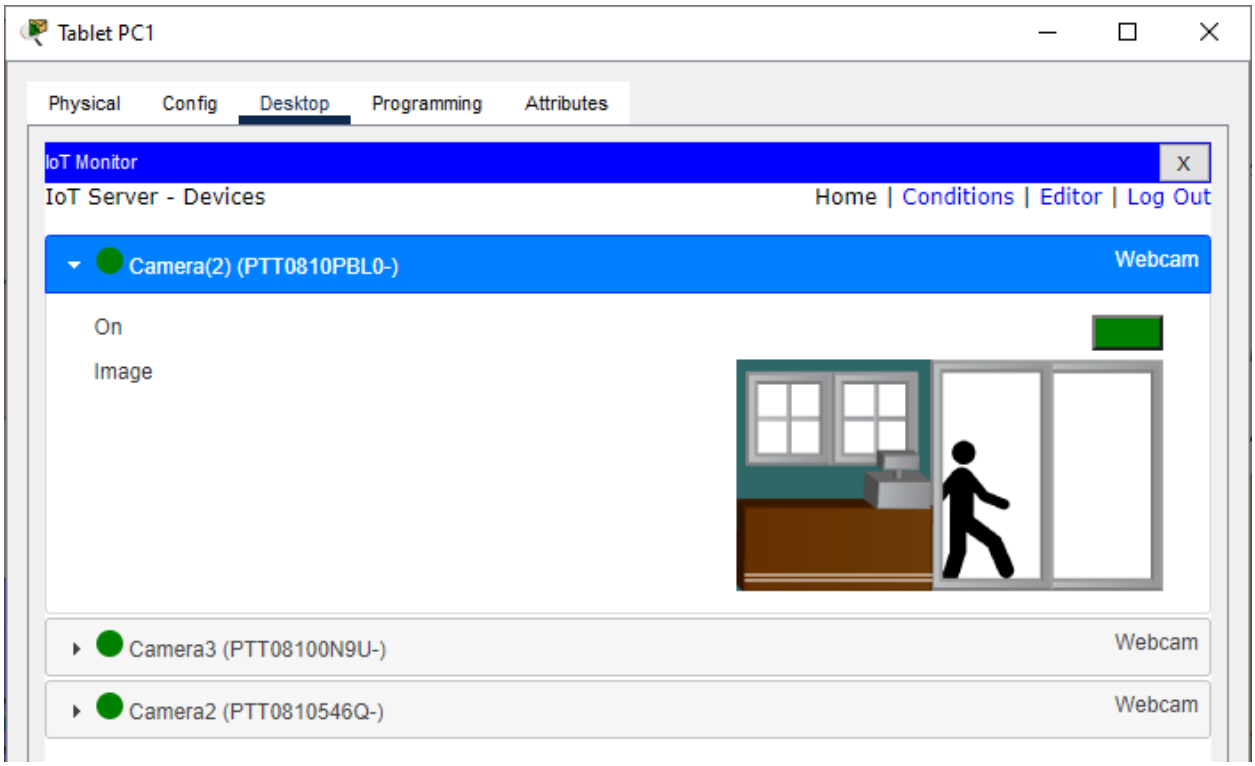


Рисунок 4.8 – Налаштування Home Gateway

ВИСНОВКИ

У кваліфікаційній роботі успішно здійснено розробку та налаштування комп'ютерної мережі для потреб Придніпровської залізниці з метою впровадження віддаленого управління залізничним переїздом на основі технологій Інтернету речей (IoT). Для досягнення цієї мети враховано різноманітні технічні аспекти, включаючи вибір оптимальної мережевої архітектури, підбір відповідної кабельної системи, аналіз мережного трафіку, вибір методів управління мережею, налаштування мережного обладнання та забезпечення високого рівня безпеки мережі.

Побудова корпоративної мережі була детально розглянута, зокрема її архітектура, складові компоненти, встановлення та налаштування. Особлива увага була приділена забезпеченню безпеки мережі, зокрема застосуванню заходів для захисту від зовнішніх загроз та внутрішніх атак.

Автоматична система управління залізничним переїздом ґрунтується на ідеї зменшення участі людини в закритті та відкритті шлагбауму, що є причиною багатьох смертей та нещасних випадків на залізничних коліях. Автоматизація воріт може забезпечити надійний контроль над ними, зменшуючи ймовірність помилок або збоїв у їх роботі. Використання ланцюга перемикачів для автоматизації закриття та відкриття залізничних воріт значно зменшить кількість нещасних випадків та сприятиме створенню екологічно чистого середовища. Таким чином, запропонована система виявляється ефективним і практичним рішенням для покращення безпеки та ефективності управління залізничним транспортом.

ПЕРЕЛІК ПОСИЛАНЬ

1. Вікі Залізнична Вікі України. [Електронний ресурс] – Режим доступу до

ресурсу: https://zaliznichna-viki-ukrayini.fandom.com/uk/wiki/%D0%9F%D1%80%D0%B8%D0%B4%D0%BD%D1%96%D0%BF%D1%80%D0%BE%D0%B2%D1%81%D1%8C%D0%BA%D0%B0_%D0%B7%D0%B0%D0%BB%D1%96%D0%B7%D0%BD%D0%B8%D1%86%D1%8F

2. Регіональна філія «Придніпровська залізниця» [Електронний ресурс] – Режим доступу до ресурсу: https://dp.uz.gov.ua/ukr/way_department

3. Acy M. Kottalil, Abhijith S, Ajmal M M, Abhilash L J,Ajith Babu. Automatic Railway Gate Control System,International Journal Of Advanced Research In Electrical, Electronics and Instrumentation Engineering,Volume 3, Issue 2, February 2014

4. Комп'ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с.

5. Державний стандарт України ДСТУ 3434:2007 "Системи автоматизованого проектування. Загальні вимоги до безпеки".

6. Державний стандарт України ДСТУ 3025:2003 "Засоби автоматизації та управління. Вимоги до безпеки електронно-обчислювальних засобів. Загальні положення".

7. "Design and Simulation of a Secured Enterprise Network for Faculty of Engineering, Rivers State University," Computer Engineering and Intelligent Systems, Jun. 2019, doi: 10.7176/ceis/10-5-04.

8. A. Bawa and M. L. Selby, "Network and Complex Systems Design and Simulation of the Internet of Things for Accra Smart City Effective use of the scarce and costly internet bandwidth in higher learning institutions in developing countries View project Network and Complex Systems Design and Simulation of the Internet of Things for Accra Smart City," 2018

9. OSPF [Електронний ресурс] – Режим доступу до ресурсу: https://www.metaswitch.com/knowledge-center/reference/what-is-open-shortest-path-first-ospf

10. AAA. FreeRADIUS Documentation – NetworkRADIUS)? [Електронний

ресурс] – Режим доступу до ресурсу: https://networkradius.com/doc/current/concepts/introduction/AAA.html

11. NAT [Електронний ресурс] – Режим доступу до ресурсу: https://voipzeker.nl/alles-over-bellen-met-voip/nat

12. G. Ordabayeva, G. Dzhsupbekova, and N. Rakhymbek, “DESIGN AND SIMULATION OF VIRTUAL LOCAL AREA NETWORK USING CISCO PACKET TRACER,” Number, vol. 6, pp. 6–14, 2020.

ДОДАТОК А

Конфігураційний файл шлюзового маршрутизатора Bichevnyk_Router_4

```
!
version 15.4
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
service password-encryption
!
hostname Bichevnyk_Router_4
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 172.24.152.1 172.24.152.10
ip dhcp excluded-address 172.24.152.24
ip dhcp excluded-address 172.24.152.33 172.24.152.43
ip dhcp excluded-address 172.24.152.65 172.24.152.75
!
ip dhcp pool Vlan24pool
 network 172.24.152.0 255.255.255.224
 default-router 172.24.152.1
 dns-server 172.24.153.46
ip dhcp pool Vlan34pool
 network 172.24.152.32 255.255.255.224
 default-router 172.24.152.33
 dns-server 172.24.153.46
ip dhcp pool Vlan44pool
 network 172.24.152.64 255.255.255.224
 default-router 172.24.152.65
 dns-server 172.24.153.46
!
!
aaa new-model
!
```

```
aaa authentication login default group radius local
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username 12321sk1_Bichevnyk privilege 15 password 7 082048430017061E010803
!
!
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
!
crypto isakmp key cisco address 64.100.13.2
crypto isakmp key cisco address 209.165.202.1
!
!
!
crypto ipsec transform-set VPN-IPSEC-SET esp-aes esp-sha-hmac
!
crypto map MAP 14 ipsec-isakmp
 set peer 64.100.13.2
 set transform-set VPN-IPSEC-SET
```

```
 match address VPN
!
!
!
!
ip ssh version 2
ip domain-name Bichevnyk_Router_4
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/0.24
 encapsulation dot1Q 24
 ip address 172.24.152.1 255.255.255.224
 ip nat inside
!
interface GigabitEthernet0/0/0.34
 encapsulation dot1Q 34
 ip address 172.24.152.33 255.255.255.224
 ip nat inside
!
```

```
interface GigabitEthernet0/0/0.44
 encapsulation dot1Q 44
 ip address 172.24.152.65 255.255.255.224
 ip nat inside
!
interface GigabitEthernet0/0/0.99
 encapsulation dot1Q 99
 ip address 172.24.152.97 255.255.255.248
 ip nat inside
!
interface GigabitEthernet0/0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 ip address 209.165.202.2 255.255.255.224
 ip ospf cost 7500
 ip access-group 100 in
 ip nat outside
 crypto map MAP
!
interface Serial0/1/1
 ip address 10.0.14.10 255.255.255.252
```

```
 ip ospf cost 7500
 ip nat inside
 clock rate 128000
!
interface Serial0/2/0
 ip address 10.0.14.1 255.255.255.252
 ip ospf cost 7500
 ip nat inside
 clock rate 128000
!
interface Serial0/2/1
 ip address 10.0.14.17 255.255.255.252
 ip ospf cost 7500
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 9
 log-adjacency-changes
 network 10.0.14.8 0.0.0.3 area 0
 network 10.0.14.0 0.0.0.3 area 0
 network 209.165.202.0 0.0.0.31 area 0
 network 10.0.14.16 0.0.0.3 area 0
 network 172.24.152.0 0.0.0.31 area 0
 network 172.24.152.32 0.0.0.31 area 0
 network 172.24.152.64 0.0.0.31 area 0
 network 172.24.152.96 0.0.0.7 area 0
!
ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224
ip nat inside source list 114 pool Internet
```

```
ip nat inside source static 172.23.153.45 209.165.202.4
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!
ip flow-export version 9
!
!
ip access-list extended VPN
permit ip 172.24.152.0 0.0.7.255 172.24.153.0 0.0.0.31
access-list 14 permit 172.24.152.0 0.0.7.255
access-list 14 permit 172.24.17.0 0.0.0.63
access-list 114 deny ip 172.23.152.0 0.0.7.255 172.23.153.0 0.0.0.31
access-list 114 permit ip 172.23.152.0 0.0.7.255 any
access-list 114 deny ip 172.24.152.0 0.0.7.255 172.24.153.0 0.0.0.31
access-list 114 permit ip 172.24.152.0 0.0.7.255 any
access-list 114 permit ip 172.24.17.0 0.0.0.63 any
access-list 100 permit ip any 209.165.202.0 0.0.0.31
access-list 100 permit ospf any any
access-list 100 permit ip 172.24.17.0 0.0.0.127 any
!
banner motd #Bichevnyk_Router_4. This is a secure system. Authorized Access Only!#
!
radius server serverRadius
 address ipv4 172.24.16.67 auth-port 1645
 key radius123
radius server 172.24.16.67
 address ipv4 172.24.16.67 auth-port 1645
 key radius123
!
!
```

```
!
line con 0
 password 7 0822455D0A16
 login authentication default
!
line aux 0
!
line vty 0 4
 exec-timeout 60 0
 password 7 0822455D0A16
 login authentication default
 transport input ssh
line vty 5 15
 exec-timeout 60 0
 password 7 0822455D0A16
 login authentication default
 transport input ssh
!
```

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

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

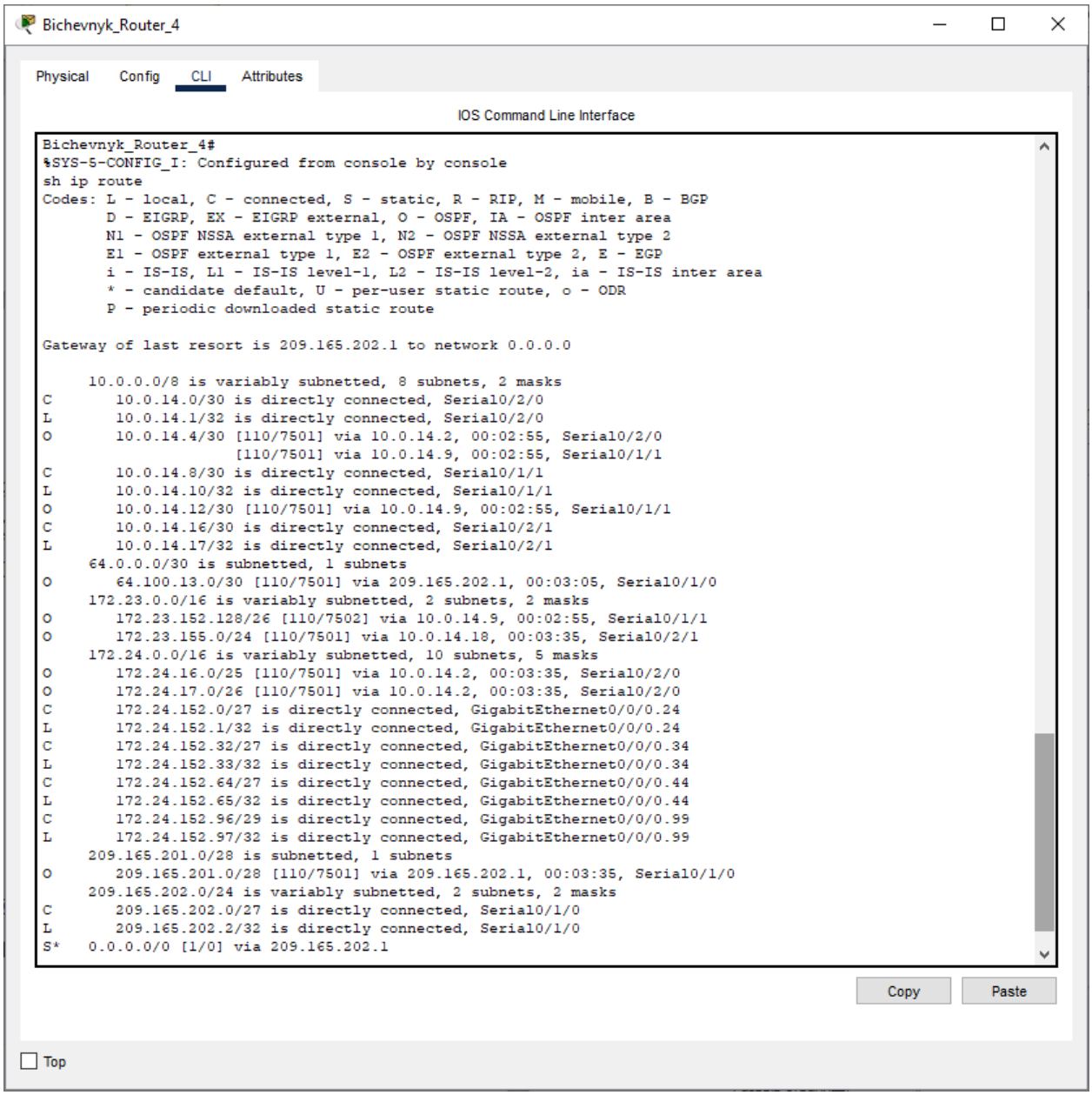
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Таблиці маршрутизації

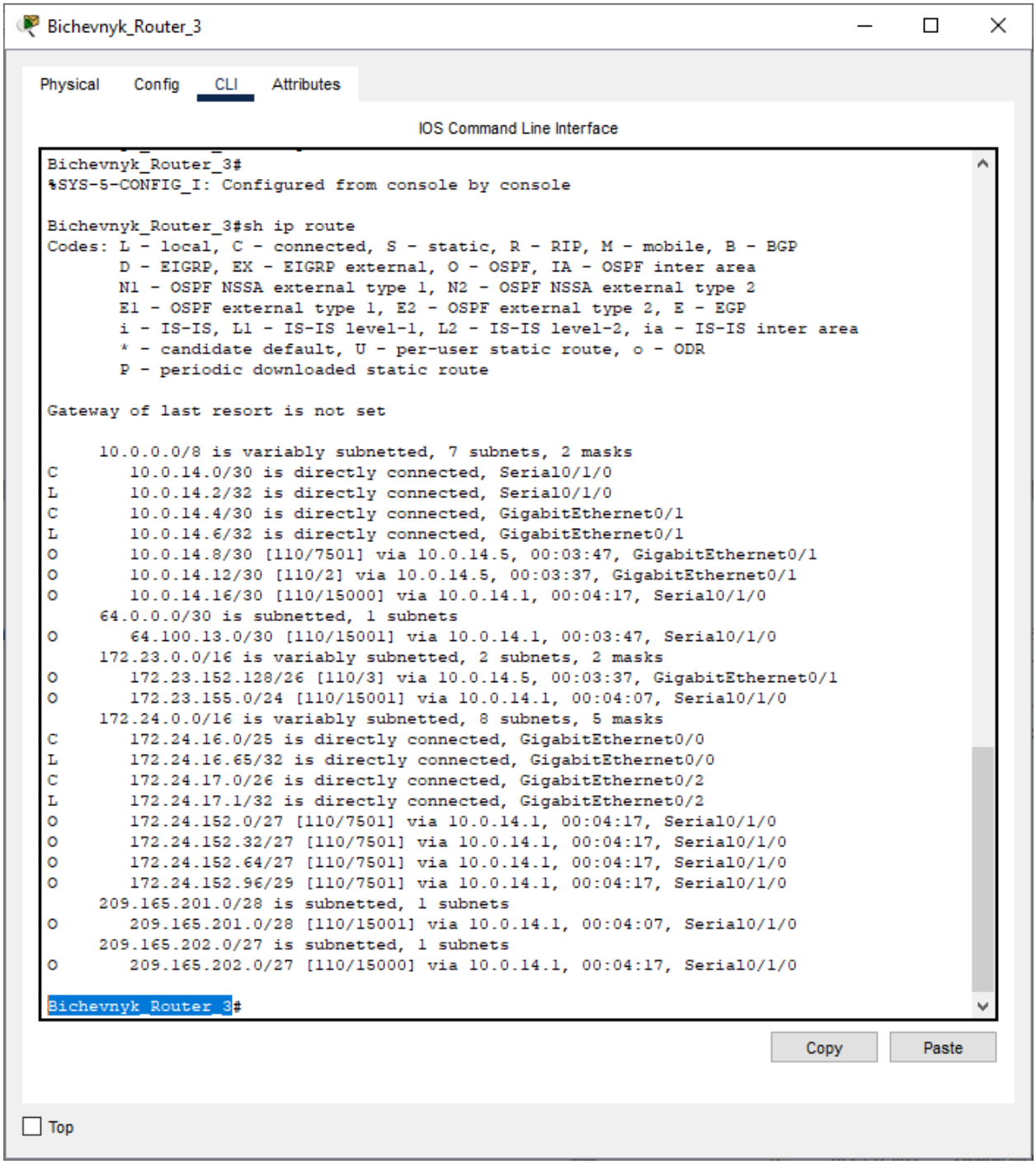
Листів 5

2024

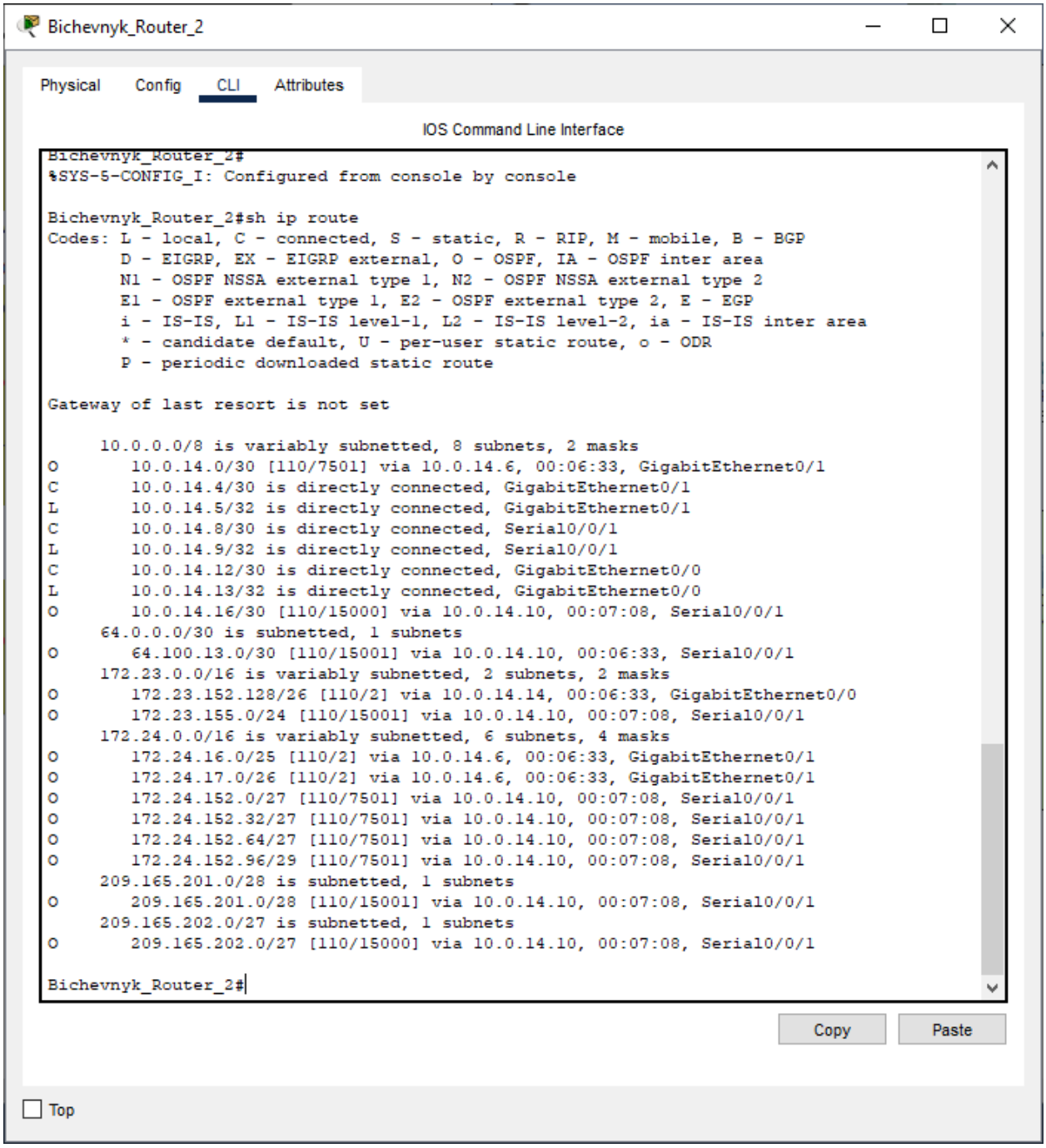
Таблиця маршрутизації Bichevnyk_Router_4



Таблиця маршрутизації Bichevnyk_Router_3



Таблиця маршрутизації на Bichevnyk_Router_2



Таблиця маршрутизації на ISP