Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Навчально-науковий Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедраінформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи бакалавра

студента Атанасов Владислав Андрійович
(ПІБ)

академічної групи 123-20-2
(шифр)

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

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

освітній рівень бакалавр
(назва освітнього рівня)

на тему: «*Комп'ютерна система ТОВ «Сінгл-ойл» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»*

Виконавець: студент 4 курсу, групи 123-20 -2 _____ Атанасов В.А.
(підпис) (прізвище та ініціали)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинг.	**інституційною**	
кваліфікаційної роботи	Доц. Бешта Д.О.			
спеціальної частини	Доц. Бешта Д.О			
Розділів:				
розробка апаратної частини	Доц. Бешта Д.О.			
розробка корпоративної мережі	Ас. Панферова Я.В.			
Рецензент				

Нормоконтролер	Проф.Цвіркун Л.І.			

Дніпро
2024

«ЗАТВЕРДЖУЮ»
Завідувач кафедри
інформаційних технологій та
комп'ютерної інженерії
проф. Гнатушенко В.В.

_____
"____" _____ 2024 р.

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра
(назва освітньо-кваліфікаційного рівня)

студенту групи*123-20-2* *Атанасову Владиславу Андрійовичу*
(група) (прізвище, ім'я та по батькові)

Тема кваліфікаційної роботи *Комп'ютерна система ТОВ «Сінгл-ойл» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі*

затверджена наказом ректора НТУ "Дніпровська політехніка"
від « 23 »05 2024 р. № 469-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	*На основі матеріалів виробничих практик, інших науково-технічних джерел обгрунтувати необхідність модернізації комп'ютерної системи ТОВ «Сінгл-ойл» з детальною розробкою комп'ютерної мережі.*	*15.04.2024 р.*
Технічні вимоги до компютерної системи	*На основі аналізу особливостей і потреб підприємства сформулювати технічні вимоги до розробки комп'ютерної мережі.*	*01.05.2024 р.*
Розробка корпоративної мережі	*Розв'язати завдання з розробки комп'ютерної мережі ТОВ «Сінгл-ойл»з опрацюванням апаратного забезпечення побудови та.*	*01.06.2024 р.*
Розробка компонента системи	*Виконати аналіз використовуваних безпровідних технологій для модеонізованої компютерної системи*	*10.06.2024 р.*

Завдання видано Доц. Бешта Д.О.
(підпис)

Дата видачі *25.01.2024 р.*

Прийнято до виконання Атанасов В.А.
(підпис)

Дата подання до екзаменаційної комісії *14.06.2024 р.*

РЕФЕРАТ

Пояснювальна записка: 93 с., 27 рис., 8 табл., 1 дод. 14 джерел.

СИСТЕМА, КОМП’ЮТЕРНА МЕРЕЖА, АДРЕСАЦІЯ, МОДЕЛЬ

Об'єкт розробки: комп’ютерна система товариства з обмеженою відповідальністю «Сінгл-Ойл» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета: створення комп’ютерної системи для забезпечення відділень, філій, представництв, складських та виробничих підрозділів підприємства «Сінгл-Ойл» інформаційними технологіями, які дозволять ефективно працювати підприємству в сучасному конкурентному середовищі.

На основі аналізу підприємства, його ключових особливостей розроблено технічні вимоги до комп’ютерної мережі, що проектується.

Для реалізації комп’ютерної мережі розроблена структура мережі, обране сучасне мережеве обладнання.

Розрахована адресація усіх пристроїв мережі. Виконана розробка моделі мережі з використанням пакету CiscoPacketTracer. Перевірка на моделі виконаної адресації, налаштувань пристроїв, можливостей в забезпеченні вимог до інформаційного середовища показали працездатність мережі.

Результати роботи викладені у пояснювальній записці.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

ІТ – інформаційні технології;

ІОД – інформація з обмеженим доступом;

ТОВ – товариство з обмеженою відповідальністю;

АРМ – автоматизоване робоче місце;

КІСП – комп’ютерна інформаційна система підприємства;

ЛОМ – локальна обчислювальна мережа;

ВСТУП

Товариство з обмеженою відповідальністю «Сінгл-Ойл» це компанія, яка активно розвивається, має виробничі потужності, філії, представництва, представників по великій території України.

Перша і, мабуть, визначальна ознака філії зводиться до того що, що ні філія, ні представництво не є юридичними особами, тобто самостійними учасниками громадянського обороту, а входять у цивільні, трудові, податкові та інші правовідносини від імені юридичної особи, що їх створила. На практиці ця ознака знаходить своє відображення в наступному:

• угоди від імені філії чи представництва укладає сама юридична особа;

• вона несе відповідальність за зобов'язаннями, що виникли у зв'язку з їх діяльністю;

Основною метою створення корпоративної мережі є формування інформаційного середовища на вирішення функціональних завдань, притаманних організації за умов конкурентних ринкових відносин. Основні функції полягають у наданні інформаційно-сервісних та комунікаційних послуг на основі сучасних програмно-технічних засобів та нових технологій мережевої взаємодії.

Інфраструктура повинна забезпечувати функціонування та розвиток локальних мереж організації та інформаційних вузлів у частині ведення баз даних та серверів, а також надання комфортного доступу до цих засобів користувачам, які мають робочі місця у локальних мережах.

При створенні першої черги необхідно створити інформаційну мережу міського кластера, що характеризується найбільшою насиченістю підрозділів, а також розробити та впровадити базову технологію інформаційної взаємодії вузлів та користувачів.

Технологія інформаційної взаємодії вузлів та користувачів повинна забезпечувати користувачів мережі такими послугами:

електронна пошта;

доступ до баз даних та програм;

доступ до файлів.

Для забезпечення даних послуг інформаційні вузли повинні мати відповідні служби (апаратно-програмні комплекси).

Служба доступу до баз даних та програм повинна надавати користувачам список доступних баз даних, умови надання доступу до баз даних та забезпечувати доступ до як локальних, так і віддалених користувачів до баз даних та програм.

Найефективнішим рішенням створення інфраструктури стає мультисервісна мережа, яка спрощує впровадження нових конвергентних додатків і може підлаштовуватися під бізнес-вимоги, що постійно змінюються, за рахунок інтелектуальної адаптивності та масштабованості.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Галузь застосування комп’ютерної системи

Компанія Сінгл-Ойл в даний час є досить великою, має не лише основний офіс, а й низку центрів технічного обслуговування, складів, регіональних представництв. Успішна робота компанії передбачає подальше розширення та укрупнення.

Внутрішні структурні підрозділи - відділи організації, що включають співробітників зі схожими обов'язками. Наприклад, відділ продажів у компанії – це внутрішній підрозділ. Працівники підрозділу працюють в офісі/будівлі компанії, за основною адресою юрособи. Поділ на відділи обумовлено необхідністю компанії та відображається лише у внутрішніх документах.

Відокремлені структурні підрозділи – будь-які територіально відокремлені підрозділи компанії, де облаштовані стаціонарні робочі місця. Наприклад, розташований на іншому кінці міста склад, де працюють комірники та вантажники, що працюють у тій же компанії. У кожному відокремленому СП можуть бути свої внутрішні підрозділи. Наприклад, відділ логістики складу.

Філія — це відокремлене СП, яке виконує частково чи повністю функції основного структурного підрозділу, зокрема функції представництва. Наприклад, основний офіс компанії розташований у м. Дніпро, а філія відкрита у м. Запоріжжі.

Представництво - це відокремлене СП, яке представляє інтереси основного підрозділу та захищає їх на місці. Наприклад, компанія (субпідрядник) відкрила представництво у м. Кропивницький, де знаходиться основний офіс генпідрядника, та веде переговори, бере участь у зборах.

Якщо СП знаходиться віддалено від основного підрозділу і в ньому є облаштовані робочі місця, воно визнається відокремленим незалежно від бажання керівництва компанії [1].

Враховуючи різноманітність можливостей розширення компанії, необхідно належним чином модернізувати корпоративну комп'ютерну мережу.

Сучасна корпоративна мережа - це листковий пиріг з різних елементів, які об'єднуються в загальну інфраструктуру з формалізованими вимогами до інформаційної безпеки, якості обслуговування та роботи.

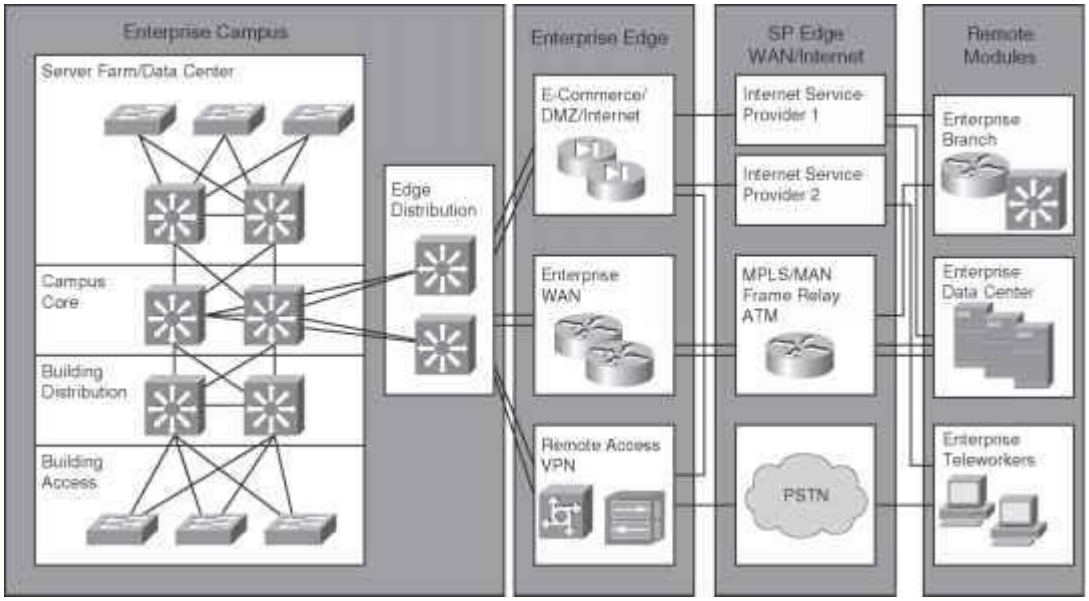

Рисунок 1.1 – Ілюстрація складності сучасних корпоративних мереж

Експлуатація існуючої мережі: моніторинг, проактивне реагування, вирішення проблем, діагностика, усунення несправностей.

Проектування - впровадження в існуючу мережу нового сегмента або масштабування інфраструктури.

Оптимізація — пошук і реалізація рішень, які необхідні, щоб підвищити продуктивність і надійність мережі: збільшення стійкості до відмов, швидкості передачі даних і так далі.

У кожній компанії, залежно від її розміру та специфіки, набір обов'язків для мережного інженера може доповнюватись та розширюватися. Іноді мережному інженеру доводиться займатися завданнями суміжних фахівців

• IP-телефонія.

Навіть якщо телефонією займається окрема людина, мережному інженеру корисно знати, як сервіс телефонії взаємодіє з мережевим обладнанням, щоб діагностувати проблеми та вести діалог із суміжним фахівцем.

• Забезпечення мережевої інформаційної безпеки.

Мережевий інженер повинен розуміти, як робити свою роботу безпечно, незалежно від того, є у компанії відділ інформаційної безпеки чи ні.

• Мережним стеком на операційних системах Linux та Windows.

Операційна система (ОС) теж мережа, і потрібно розуміти, як її налаштувати, як вона взаємодіє з іншою інфраструктурою. Тому при роботі з ОС інженеру знадобляться базові знання системного адміністратора.

• Обслуговування ПЗ для систем моніторингу та збору конфігурацій, сервісів автентифікації та авторизації на мережевих пристроях тощо.

Мережевий інженер повинен вміти взаємодіяти з операційними системами Linux, щоб розгорнути в них службові програми.

• Автоматизація рутинних процесів.

У компаніях із великою командою мережевих інженерів часто висуваються вимоги до вміння автоматизувати рутинні процеси. Тому мережевий інженер повинен вміти писати нескладні скрипти на Python або взаємодіяти з такими засобами, як Ansible, щоб реалізовувати базові дії конфігурації або дії, пов'язані з обробкою текстової інформації.

• Інтеграцією мережі з публічними та приватними хмарами, PaaS- (Platform as a Service, платформа як послуга) та SaaS- (Software as a Service, програмне забезпечення як послуга) рішеннями.

Фахівцю треба розуміти, як працюють та організовані мережі всередині віртуальних середовищ, абстрактні сутності всередині віртуальних комутаторів та маршрутизаторів [4].

1.2 Характеристика і структура об’єкта впровадження

Основний профіль роботи компанії – оптова торгівля мастильними матеріалами.

Сінгл-Ойл є офіційним дистриб'ютором SHELL EAST EUROPE COMPANY LIMITED з 1999р.

Компанія Сінгл-Ойл представляє інтереси Shell на Південному Сході України в наступних областях:

Дніпропетровська область

Запорізька область

Основний офіс та склад компанії розташований у м. Дніпропетровську. Крім цього компанія має у м. Запоріжжі філію та регіональний склад продукції Shell.

Для зручності замовників у Кривому Розі працюють регіональні менеджери з продажу.

Сінгл-Ойл характеризується:

• Повний асортимент мастильних матеріалів Shell в Україні (мастила, мастила та технічні рідини Shell);

• Мінімальний термін постачання мастильних матеріалів;

• Безкоштовна доставка по області;

• Професійні консультації фахівців з будь-яких питань, пов'язаних з вибором та використанням продуктів Shell;

• Персональний менеджмент;

• Вигідні умови роботи.

Крім цього компанія розвиває мережу фірмових центрів експрес заміни олії Shell Helix Express та надає автомобілістам найвищий рівень обслуговування за корпоративними стандартами Shell прийнятими у всьому світі.

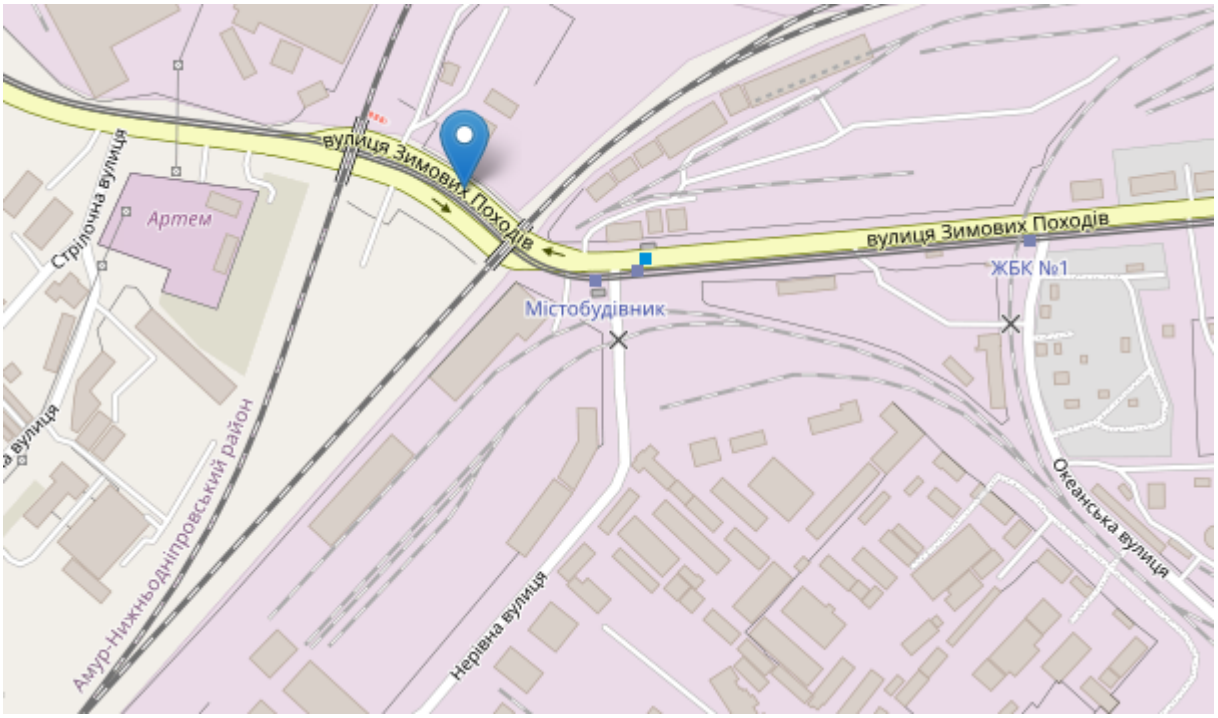

Рисунок 1.2 – Розташування будівлі ТОВ «Сінгл-Ойл»

1.2.1 Структура і інформаційні особливості системи

В ІКС зберігається та обробляється:

- податкові декларації;
- дані про персонал;
- дані про клієнтів;
- прайс-листи;
- інформація про наявність товару на складі;
- трудові договори;

- договори купівлі/продажу;
- банківські реквізити;
- дані для доступу до банківських рахунків;
- сертифікати товарів;
- комерційні пропозиції.

Класифікація інформації:

Інформація, що обробляється в ІКС, класифікована як інформація з обмеженим доступом. За правовим режимом інформація є конфіденційною. Об'єм інформації, що циркулює на об'єкті з найвищим грифом секретності – середній. Інформація, що є конфіденційною чи складає комерційну таємницю – не озвучується.

Процес створення та обробки інформації

Податкові декларації створюються головним бухгалтером на основі документів купівлі/продажу та трудових договорів. Звіти оформлюються в електронному вигляді та зберігаються на робочій станції бухгалтера, податкова інспекція забезпечує шифрування звітів та створення захищеного каналу передачі даних. Звіти оформлені в бумажному вигляді зберігаються у сейфі.

Дані про персонал створюються заступником директора під час влаштування на роботу нового співробітника. Зберігаються в електронному вигляді на робочій станції заступника директора.

Дані про клієнтів зберігаються в електронному вигляді на сервері, створюються менеджерами.

Прайс-листи створюються комерційним директором і зберігаються на сервері в електронному вигляді. У паперовому вигляді вони зберігаються біля кабінетів.

Інформація про наявність товару на складі створюється комерційним директором та зберігається на сервері в електронному вигляді.

Трудові договори заповнюються новим співробітником та заступником директора в паперовому вигляді та зберігаються у сейфі.

Сертифікати товарів надаються постачальниками в електронному вигляді та зберігаються на сервері.

Договори купівлі/продажу оформлюються комерційним директором чи директором з клієнтами чи постачальниками у паперовому вигляді.

Банківські реквізити надаються банком та зберігаються у електронному вигляді на сервері і в паперовому вигляді.

Дані для доступу до банківських рахунків видаються банком, створення захищеного каналу передачі даних та видачу цифрових підписів забезпечує банк. Доступ до них мають комерційний директор, директор та головний бухгалтер.

Комерційні пропозиції створюються комерційним директором та зберігаються в електронному вигляді на сервері [2].

Схема інформаційних потоків відображена на рисунку 1.3.

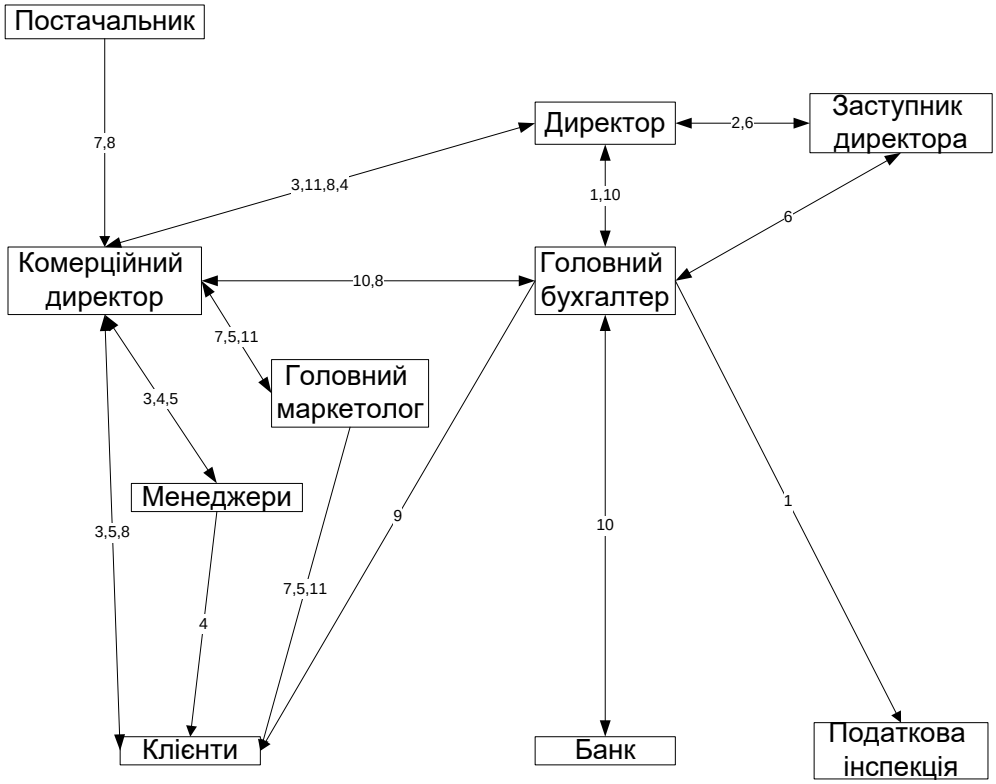

Рисунок 1.3 – Інформаційні потоки ТОВ «Сінгл-Ойл»

Таблиця 1.1 – Користувачі системи та їх обов’язки

№	Користувач ІТС	Кількість	Обов’язки
1	Директор	1	Керування компанією. Планування заходів компанії, напрями діяльності, розширення компанії, оформлення договорів з клієнтами.
2	Заступник директора	1	Під час відсутності директору – виконує його функції, також до його обов’язків відноситься прийняття та звільнення співробітників.
3	Комерційний директор	1	Відповідає за стабільний розвиток економіки підприємства, контроль роботи бухгалтера та відділу маркетингу, пошук нових клієнтів та укладення договорів.
4	Головний бухгалтер	1	Облік діяльності компанії. Створення звітів, також – здача в податкову інспекцію та різноманітні державні фонди звітів про ведення діяльності компанії.
5	Системний адміністратор	1	Підтримка працездатності мережі, оновлення ПО, адміністрування сайту компанії.
6	Головний маркетолог	1	Робота з клієнтами, рекламування продукції, надання клієнтам необхідної інформації про товари, навчання нових співробітників
7	Менеджери	8	Прийняття замовлень від клієнтів, продаж та облік продукції, реєстрація нових користувачів в базі даних.

На приведених схемах і в таблиці показано інформаційні особливості що відносяться до роботи головного підрозділу компанії. Відокремлені підрозділи також мають свої особливості, з урахуванням їх більш вузької спеціалізації.

1.3 Функціональні особливості компютерної системи

У компанії використовується ряд апаратних та програмних рішень, що дозволяють створити всередині публічної мережі (у тому числі в Інтернеті) іншу мережу, захищену від доступу ззовні – віртуальну приватну мережу (VPN). Такі технології дозволяють використовувати двосторонній супутниковий Інтернет у корпоративних мережах зв'язку. У тому числі таких, у яких пред'являються підвищені вимоги до безпеки

Існують зовсім маленькі віддалені філії чи окремі співробітники – наприклад, торгові представництва (агенти) чи точки продажу. Як правило, такі підрозділи розміщуються у невеликих орендованих приміщеннях. Не завжди у них є лінії зв'язку з необхідною якістю. У різних містах зв'язок забезпечують різні провайдери, вони використовують різні технології та застосовують різні тарифи. З усіма з ними головній компанії доводиться укладати договори та вести роздільний облік послуг. Крім того, ці провайдери, як правило, є другою, третьою і т.д. субпровайдерами, перепродавцями трафіку, а до невеликої філії застосовують роздрібні розцінки – зв'язок виходить дорогим.

Використання VSAT-станцій дає постійний, надійний, захищений зв'язок з віддаленими підрозділами, що не залежить від ліній зв'язку, які може запропонувати орендодавець. Зв'язок з усіма філіями, скільки їх не було, забезпечується одним оператором - відповідно:

- менше документів у центральному офісі
- однакове обладнання для всіх філій
- єдина технічна підтримка
- оптова ціна на трафік.

Об'єднання локальних мереж центрального офісу та віддалених філій використовується для відносно великих віддалених підрозділів або філій у місцях, де немає або майже немає каналів зв'язку. Це можуть бути:

Такі структури, розташовані далеко від міст, як правило, мають лише телефонний зв'язок посередньої якості, і підключення їх комп'ютерних мереж до мережі центрального офісу можливе лише через супутник. Воно дозволяє:

• використовувати загальні бази даних

• вести електронний документообіг

• організувати відомчий телефонний зв'язок

Підключення філій до бази даних центрального офісу є дуже зручним, компанія має невеликі віддалені філії, і в своїй роботі використовує великі бази даних. Для забезпечення безпеки та безпеки даних клієнтів на професійному рівні потрібне складне та дороге обладнання. Встановлювати його в кожній філії надто дорого. Тому використовується один сервер, надійно захищений від аварій та від хакерських атак – у центральному офісі. У філіях встановлюються абонентські супутникові станції. Через супутник співробітники віддалених філій підключаються до сервера, вимагають необхідні дані, модифікують їх і зберігають знову ж таки на сервері. Для користувача вся процедура виглядає так, ніби сервер стояв у сусідній кімнаті. Таким чином, у філіях проводиться лише поточна обробка записів, а зберігання даних здійснюється у центральному офісі. Навіть за серйозної аварії у філії будуть втрачені лише останні версії кількох записів - тих, які були у роботі в момент аварії. Таке рішення дозволяє суттєво знизити вимоги до обладнання філій, відповідно значно прискорити розгортання мережі філій [3].

Мультисервісна мережа передачі даних компанії повинна забезпечувати виконання прикладних корпоративних завдань та безперервну роботу IT-додатків, надавати внутрішньокорпоративний голосовий та відеоконференц-

зв'язок, засоби для дистанційного навчання, підтримувати інтегровану систему відеоспостереження служби безпеки, а також автоматизувати обробку звернень клієнтів, партнерів та споживачів послуг компанії [5].

Проектована ІКС повинна надавати кожному абоненту такі послуги зв'язку:

• багатоканальне кабельне телебачення;

• високошвидкісний доступ до Інтернету;

• підключення до телефонної мережі загального користування;

• організація виділених каналів зв'язку;

• організація каналів відеоспостереження;

• організація виділених каналів передачі;

• збирання облікової та телеметричної інформації та управління приладами обліку для ЖКГ;

• інші послуги, які можуть знадобитися.

1.4 Завдання і мета роботи

В цілому проект комп'ютерної мережі повинен забезпечувати виконання всіх функцій, що покладаються на неї:

• обмін усіма видами інформації, включаючи передачу мовних, графічних та відео для проведення телеконференцій;

• забезпечення інформаційної скритності передачі інформації та виключення несанкціонованого доступу до неї;

• інтеграція з існуючими телекомунікаційними системами за рахунок побудови елементів мережі на основі стандартних технічних засобів та методів передачі та обробки інформації;

• можливість зміни конфігурації та легкість розвитку топології (розширення) мережі;

• стійкий зв'язок із віддаленими районними вузлами зв'язку та пунктами, розташованими у сільській місцевості;

• можливість впровадження перспективних інформаційних та телекомунікаційних технологій у майбутньому.

2. РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1Технічні вимоги до комп'ютерної системи

2.1.1Вимоги до системи в цілому

2.1.1.1 Структура і функціонування системи

Корпоративна мережа підприємства «Сінгл-ойл» створюється на базі локальних обчислювальних мереж, що включають функціональні мережеві сервери, робоче місце адміністратора/оператора та робочі місця користувачів.

Мережевий сервер (сервер пам'яті) призначений управління локальної обчислювальної мережею, зберігання даних, і програм.

Для побудови розгалуженої багатосегментної мережі мережевий сервер повинен мати властивості маршрутизації (роутингу) пакетів протоколів IPX і TCP/IP.

Поштовий сервер призначений для забезпечення взаємодії інформаційних вузлів у режимі електронної пошти та надання користувачам РОСА послуг електронної пошти та телеконференцій.

Поштовий сервер повинен виконувати функції вузла комп'ютерної мережі Internet та сервера телеконференцій, забезпечувати зв'язок із регіональним вузлом мережі та мати модемний пул для підключення віддалених користувачів.

Поштовий сервер має бути доступним користувачам локальної мережі.

Сервер доступу призначений для забезпечення доступу віддалених користувачів мережі до баз даних та програм інформаційного вузла в режимі віртуального терміналу.

Сервер доступу повинен забезпечувати доступ до програм і баз даних, що знаходяться на сервері пам'яті ЛВС.

Багатоканальна станція BBS призначена для доступу до інформаційних ресурсів вузлів за допомогою "електронної дошки оголошень", що дозволяє

обмінюватися електронною поштою, файлами при прямих з'єднаннях, а також брати участь у телеконференціях.

Робоче місце адміністратора/оператора призначене для завдань адміністрування ЛОМ та баз даних.

В даний час побудова мультисервісних мереж з інтеграцією різних послуг є одним із найперспективніших напрямів розвитку телекомунікаційних мереж. Основне завдання мультисервісних мереж полягає у забезпеченні співіснування та взаємодії різнорідних комунікаційних підсистем у єдиному транспортному середовищі, коли для передачі звичайного трафіку (даних) та трафіку реального часу (голосу та відео) використовується єдина інфраструктура.

Під час створення мультисервісної мережі досягається:

• Скорочення витрат на канали зв'язку;

• Скорочення витрат на адміністрування та підтримання працездатності мережі, зменшення сукупної вартості володіння;

• Можливість проведення єдиної адміністративно-технічної політики у сфері інформаційного обміну;

• Збільшення конкурентоспроможності організації за рахунок введення в операційну діяльність нових корпоративних сервісів та додатків та, як наслідок, підвищення продуктивності праці співробітників.

Актуальність обумовлена швидкими темпами зростання популярності голосових та мультимедійних послуг на основі IP-протоколу (VoIP, IP-TV, VoD, VCS та ін.). Зміни, що викликаються ними, в структурі телекомунікаційних мереж ставлять на порядок денний питання про будівництво мультисервісних мереж наступного покоління, в яких широкий спектр послуг, включаючи передачу голосу та даних, надаватиметься на єдиній технологічній основі комутації пакетів [10].

2.1.1.2 Чисельність і кваліфікація персоналу, що обслуговує систему і режим роботи

На адміністраторів покладаються такі обов'язки:

- оперативно-адміністративне керівництво мережею;

- вирішення адміністративних та технічних питань взаємодії з користувачами при підключенні до мережі, зміні послуг та відключенні від мережі;

- розробка та реалізація адресної та маршрутної політики мережі;

- проведення робіт, пов'язаних із впровадженням нових технологій та розвитком мережі;

- Організація робіт з моніторингу мережі;

- організація та проведення заходів щодо забезпечення безпеки у мережі;

- управління маршрутизаторами та магістраллю мережі;

- локалізація та усунення збоїв у роботі мережі;

- керівництво роботою із супроводу технічних та програмних засобів мережі;

- управління мережними ресурсами, що розділяються;

- заповнення журналів профілактичних, аварійних та екстрених робіт;

- реєстрацію, підключення та відключення робочих місць.

Структура мережі складається з 5 локальних мереж LAN1 – LAN5.

Кількість вузлів: LAN1 – 7 LAN2 –100 LAN3 – 201 LAN4 – 88 LAN5 - 69.

Інтенсивність трафіку $\mu = 159$ (кадрів/с).

Блок адрес - 10.25.IPn.0/22; для виділення підмереж IPn = 8.

Зовнішня адреса HTTP-сервера: 209.165.200.4.

Середня довжина вихідного повідомлення в мережі – 650 байт.

Затримка передачі пакету в найбільшій мережі $– \leq 6$ мс.

Кількість обслуговуючого персоналу має бути не 5 спеціалістів.

Адміністрацію та відповідальність покладено на начальника IT відділу та його заступника.

2.1.1.3 Вимоги до надійності

Для забезпечення надійності комплексу технічних засобів інформаційних вузлів та локальних мереж бажано використання джерел безперебійного живлення (UPS) та стабілізаторів напруги живлення.

Необхідно, щоб технічні засоби інформаційних вузлів та локальних мереж забезпечували стійку роботу при пікових навантаженнях та мали резерв для розширення числа користувачів та розв'язуваних завдань.

Загальносистемні програмні засоби, що використовуються, повинні мати відмовостійкість і мати засоби оперативного відновлення працездатності систем та інформації при аварійних ситуаціях [13].

2.1.1.4 Вимоги безпеки

Для забезпечення безпеки обслуговуючого персоналу та електронних компонентів технічних засобів інформаційних вузлів від впливів електричного струму необхідно використовувати захисне заземлення використовуваних технічних засобів.

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

Технічне обслуговування локальних обчислювальних мереж є комплексом робіт з:

діагностики, налаштування, підтримки мереж, серверів, мережевих пристроїв;

налагодження роботи ПК та оргтехніки;

встановлення та оновлення ПЗ;

запобігання несанкціонованому проникненню в мережу;

антивірусний захист;

організації бекапів;

удосконалення мережі.

Абонентське обслуговування мереж у рамках планово-попереджувальних ремонтів спрямоване на підтримку цілісності та безперебійної роботи техніки та структурованої кабельної мережі.

До нього входять:

візуальна перевірка елементів ЛОМ щодо пошкоджень та наявності маркувань;

усунення дефектів у разі виявлення;

своєчасна заміна кабелів за результатами оцінки ступеня зношування;

огляд та за необхідності ремонт портів.

Усі роботи документуються, оформляються у вигляді актів та рекомендацій щодо подальшого використання мереж. У ряді випадків може знадобитися проведення позапланового техобслуговування. Найчастіше це пов'язано зі збоями системи, що сталися через:

перевантаженості локально-обчислювальних мереж (наприклад, сховище повністю набито інформацією, пристрій не може впоратися з тим, що йде потік нових даних);

регулярних помилок співробітників підприємства, які здійснюються під час експлуатації техніки;

необхідності переустановки або оновлення програмного забезпечення.

Ремонт комп'ютерної мережі включає:

діагностику апаратної частини (активного обладнання) мережі;

заміну устаткування, що вийшло з ладу;

тестування стабільності роботи мережі;

діагностику з'єднань та цілісності кабельних трас;

заміну абонентських розеток, роз'ємів та сполучних кабелів;

оцінку якості та стабільності бездротових з'єднань;

виявлення та виправлення помилок у налаштуваннях мережного обладнання.

Ремонтні роботи повинні виконуватись стороннім підрядником відповідно до договору.

2.1.1.6 Вимоги до захисту інформації від несанкціонованого доступу

Засоби захисту інформації від несанкціонованого доступу повинні забезпечувати парольний захист, розмежування прав доступу користувачів до інформаційних ресурсів та послуг, а також мати засоби шифрування/дешифрування електронних документів, що передаються та одержуються, та засоби електронного підпису.

Для запобігання несанкціонованому доступу до ресурсів КС використовуються паролі та/або апаратні засоби аутентифікації.

Користувачі зобов'язані забезпечити безпечне зберігання пароля та/або засобів аутентифікації, що унеможливлює їх втрату або розголошення.

Забороняється повідомляти будь-кому навіть адміністраторам мережі свій пароль для доступу до інформаційних ресурсів КС.

У разі підозри на розголошення пароля, необхідно негайно змінити пароль та поінформувати адміністратора КС [12].

При виборі пароля рекомендується дотримуватися таких правил:

- Довжина пароля повинна бути не менше 8 символів;

- пароль не повинен бути легко вгадуваним (пароль не повинен включати повторювану послідовність будь-яких символів (наприклад, "111111", "аааааа", "12345", "qwerty", "йцукен" тощо);

- пароль не повинен включати в себе поєднання символів, що легко підбираються (імена, прізвища, найменування, клички домашніх тварин, дати

народження і т.д.) і загальноприйняті скорочення (ЕОМ, ЛОМ, USER і т.п.));

2.1.1.7 Вимоги до патентної чистоти

В комп'ютерній системі повинні використовуватися елементи та пристрої, програмне забезпечення ліцензовані та сертифіковані для використання на території України.

2.1.1.8 Вимоги до стандартизації й уніфікації

Для спільного функціонування, взаємодії користувачів з інформаційними ресурсами та інформаційними ресурсами інших мереж необхідно забезпечити сумісність програмного забезпечення, що використовується і розробляється. Тому при виборі та розробці програмного забезпечення необхідно керуватися стандартами та угодами, які використовуються для взаємодії завдань.

Ці угоди мають:

1) задовольняти наступним стандартам: Еталонна модель взаємодії відкритих систем OSI/ISO (7498), CCITT, RFC;

2) широко використовуватись (бути масовими);

3) мати програмні реалізації, а ці програмні реалізації мають бути доступними.

2.1.2Вимоги до видів забезпечення

2.1.2.1 Інформаційне забезпечення системи

Вибір оптимальної технології для побудови широкосмугових мультисервісних мереж нині спирається на процеси інтеграції та конвергенції мережевих технологій під час створення сучасних мереж. Сучасний рівень розвитку мережевих технологій цифрових глобальних мереж дозволяє при плануванні архітектури та розробці топології цифрових транспортних або магістральних мереж використовувати такі базові технології:

TCP/IP - технологія мережі Інтернет, основою якої є стек протоколів

TCP/IP або протокол управління передачею/протокол Інтернету;

IP/MPLS – технологія багатопротокольної комутації за мітками;

ATM – технологія асинхронного режиму передачі (перенесення);

SDH – технологія синхронної цифрової ієрархії СЦІ;

WDM – технологія хвильового мультиплексування (ВМП);

DWDM – технологія щільного хвильового мультиплексування (ПВМП).

Gigabit Ethernet (xGE) [14].

Основні системи доступу, що використовуються в абонентських мережах в даний час і заплановані операторами до застосування в найближчому майбутньому:

системи, що базуються на технологіях сімейства xDSL (Digital Subscriber Line - цифрова абонентська лінія);

системи доступу з використанням спеціальних модемів у мережах КАТВ (Cable modems);

комбіновані системи "волокно/коаксіал" (Hybrid Fixed/Coax, HFC);

оптоволоконні системи доступу;

системи радіодоступу;

супутникові системи;

виділені лінії із використанням систем E1/T1.

2.1.2.2 Технічне забезпечення системи

Вибирається обладнання з урахуванням надання послуг, виду технології реалізації мережі зв'язку та типу лінії.

Базові мережеві технології можна використовувати для побудови мереж як магістральних транспортних (і підключення до них мереж доступу та різних користувачів), так і інтегрованих мультисервісних. Основна відмінність між ними полягає у вартості та складності реалізації. Для правильного вибору

базової мережевої технології або їхньої сукупності слід проаналізувати конкретні вимоги до планованої цифрової мережі [14].

Рекомендуються наступні критерії вибору мережевої технології:

• Кількість послуг, що надаються.

• Якість обслуговування QoS (Quality of Service).

• Масштабованість мережі.

• Вартість мережі.

• Окупність інвестицій.

• Підвищення ефективності управління мережею та організацій, на користь яких вона створюється.

• Сумісність із існуючою системою кабельних ліній зв'язку.

• Сумісність із наявним мережевим обладнанням.

• Можливість сумісності чи взаємозв'язку з іншими мережами.

2.1.2.3 Вимоги до організаційного забезпечення

Необхідно, щоб системні програмні засоби інформаційних вузлів мали ефективні засоби управління користувачами та групами користувачів, засоби створення та відновлення резервних копій інформації, що зберігається, а також засоби контролю та управління роботою інформаційних служб у реальному часі.

Організаційно-правові аспекти створення включають:

- Створення мережі інформаційних вузлів;

- Регламенти програмно-технологічного характеру, що забезпечують функціональну єдність інформаційних вузлів;

- Регламенти з питання фінансових відносин, що виникають при взаємодії.

Фінансовим питанням у цьому випадку надається особливе значення, оскільки корпоративна мережа, що має свій внутрішній напружений трафік і має дуже низьку вартість послуг.

2.1.2.4 Вимоги до складу нормативно-технічної документації системи

У документацію мають бути включені:

Топологія мережі. Інформація подається у формі діаграм, на яких показані основні мережеві вузли, такі як маршрутизатори, комутатори, фаєрволи, сервера і як вони взаємопов'язані. Принтери та робочі станції не включаються.

Інформація про сервери. Інформація, яка необхідна для управління та адміністрування серверами, така як ім'я, функції, IP адреси, конфігурація дисків, ОС та сервіс-паки, дата та місце покупки, гарантія тощо.

Призначення портів комутаторів та маршрутизаторів. Сюди включається детальна інформація про конфігурацію WAN, VLAN або призначення портів мережевим вузлам через патч-панель.

Конфігурація мережевих служб. Мережеві служби, DNS, WINS, DHCP, та RAS, критичні для операцій у мережі. Слід детально описати, як вони структуровані.

Політики та профілі доменів. Обмежити можливості користувачів за допомогою Policy Editor у Windows NT або за допомогою Group Policies у Windows 2000. При цьому можна створити профілі користувачів, які зберігаються на сервері, а не на локальній машині. Якщо такі можливості використовуються, то така інформація має бути документована.

Критично важливі програми. Ви повинні включити в документацію, як такі програми підтримуються, що буває з ними найчастіше не так і як вирішувати такі проблеми.

Процедури. Це саме собою може бути великим проектом. Здебільшого процедури — засіб реалізації політик і може бути досить великими. Наприклад, політика може встановлювати, що "Мережа має бути захищена від неавторизованих користувачів". Однак, для реалізації такої політики, буде потрібно багато зусиль. Існують процедури для фаєрволів, мережевих протоколів, паролів, фізичної безпеки тощо. Ви також можете мати окремі процедури для обробки проблем, про які повідомляють користувачі, та процедури для регулярного обслуговування серверів.

2.2 Організаційна структура підприємства

На рисунку 2.1 показана укрупнена організаційна структура підприємства.

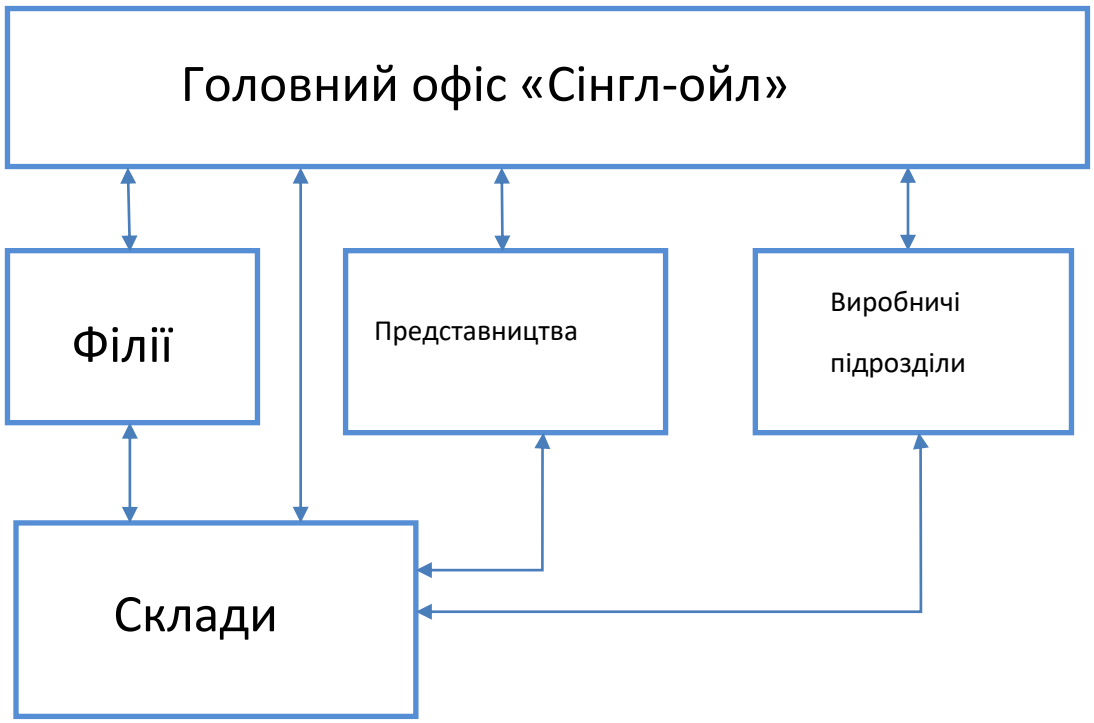

Рисунок 2.1 – Організаційна структура підприємства

Підключення ЛОМ окремих підрозділів до корпоративної обчислювальної мережі виконано за допомогою багатомодового 12-ти жильного оптоволоконного кабелю 50/125, який з'єднує комунікаційний центр корпоративної мережі (розташований у приміщенні головного офісу) з приміщенням комунікаційного вузла ЛОМ підрозділу. Або використовується віддалений доступ через провайдер або супутниковий термінал.

Для забезпечення незалежності робіт мереж ІНТЕРНЕТ та ЛОМ вхідні інформаційні потоки організовані різними оптоволоконними лініями зв'язку, які заведені на окремі комутатори, встановлені в комунікаційній шафі. Для

забезпечення надійності роботи комунікаційного обладнання передбачити їхнє електрозаживлення від джерела безперебійного живлення потужністю 3 кВт.

Все комунікаційне обладнання (комутатори, джерело безперебійного живлення, патч-панелі та кабельні організатори) змонтувати в окремій монтажній шафі заввишки 42U.

2.3 Розробка структурної схеми комп'ютерної системи

В кваліфікаційній роботі показана структурна схема корпоративної мережі, яка охоплює підрозділи, що розташовані у місті Дніпро. Відповідно до кількості підрозділів показано 5 локальних обчислювальних мереж.

LAN1 – головний офіс.

LAN2 – склад.

LAN3 – виробничі сервісні центри.

LAN 4 – філія.

LAN 5 – спеціалізований підрозділ по наданню транспортно-логістичних послуг.

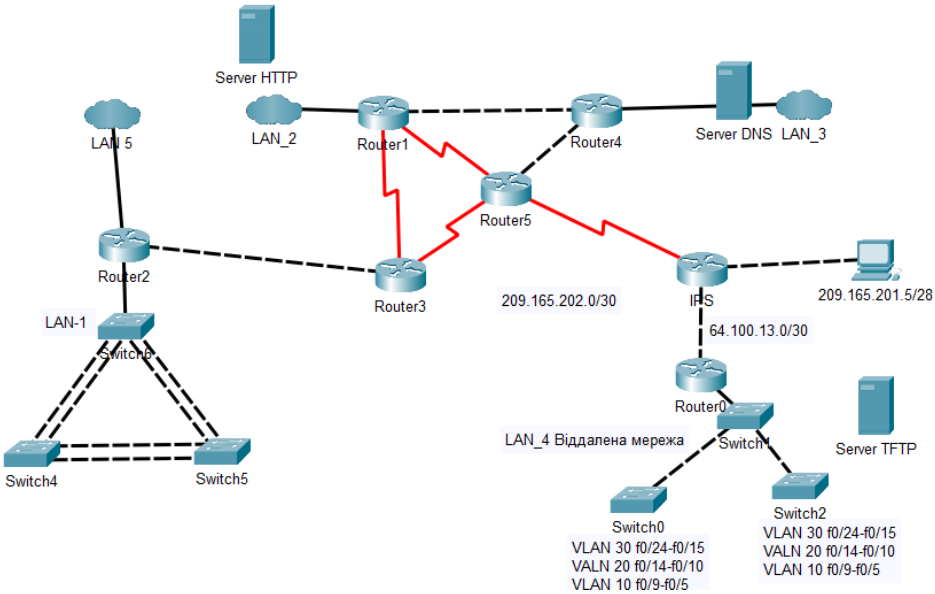

Рисунок 2.2 – Структура комп'ютерної мережі підприємства

2.4 Характеристика технічних пристроїв що складають комп’ютерну мережу

Мережеве обладнання Maipu.

Компанія створена в 1993 році, займається дослідженнями та розробками в галузі передачі даних. Має великий досвід є основним постачальником мережевих рішень в Китаї. У лінійці продуктів вендора представлені маршрутизатори, комутатори, бездротові мережі, SDN-рішення, хмарні послуги для управління мережевим обладнанням. Maipu пропонує обладнання, необхідне для побудови повноцінної мережевої інфраструктури та модернізації мереж. Компанія має понад 1500 патентів, близько 50% її співробітників займаються дослідженнями та новими розробками.

На рішеннях вендора можна будувати 2- та 3-рівневі архітектури. Єдина річ, яка ліцензується, — контролер BD-LAN. В іншому вендор має чітке позиціонування - доступність всього функціоналу обладнання "з коробки".

Обладнання Maipu використовує уніфіковане програмне забезпечення. Тобто немає поділу на комутатор Enterprise або для дата-центрів. Все працює на однаковому софті.

Тестування обладнання Maipu.

Тестовано практично все обладнання Maipu, яке є сьогодні на ринку. Перевірено як якість виробів, так і їхній заявлений функціонал.

У Maipu доступний режим Rapid-VIST, який сумісний з Rapid-PVST у Cicso. Це дозволяє вбудовувати комутатори Maipu у мережу Cicso без необхідності перекладати всю інфраструктуру на відкриті стандарти.

Є MSTP – відкритий стандарт, який дозволяє працювати Maipu в одній мережі з обладнанням інших вендорів.

Можливість стекування доступна лише через інформаційні аплінки.

Апгрейд ПЗ проходить без перезавантаження всього стека, що є далеко не у кожного вендора - деякі виробники вимагають перезавантаження всього стека після оновлення на одному юніті.

Комутатори Maipu можна стекувати з різних моделей, побудованих на одних чіпах.

Site-to-Site VPN. Підтвердили працездатність режиму як між обладнанням Maipu, так і Cicso, Huawei та іншими виробниками. Немає VTI, і поки що невідомо про його реалізацію. Підтримується лише IKEv1, а IKEv2 – у розробці.

Протокол динамічної маршрутизації IRMP сумісний з Cisco EIGRP і має ті ж метрики. Практично ні в кого з інших вендорів немає аналогів. І якщо мережа була побудована на EIGRP, нічого не можна було вибрати, окрім Cisco. Для багатьох це було критичним моментом.

Переваги обладнання Maipu:

Обладнання Maipu використовує Command Line практично аналогічний тому, що використовується на обладнанні компанії Cisco. Тому інженери можуть настроювати обладнання навіть без додаткового навчання.

Маршрутизатори та комутатори Maipu використовують уніфіковане програмне забезпечення Unified IOS, тому немає необхідності платити за ліцензії на додатковий функціонал (такий як: MPLS/L2TPv3/BFD/IPSLA тощо).

Можливості інтегрування пристроїв Maipu із рішеннями Cisco (DMVPN, VXLAN-фабрика).

Maipu надає R&D-підтримку – розробку необхідного замовнику функціоналу.

Кейс, реалізований на нових рішеннях

Враховуючи, що в робочі дні переключення мережевої інфраструктури на нові компоненти було неможливим — філії постійно мали обмінюватися інформацією з головним офісом, проведено монтаж нового мережевого

обладнання паралельно з системою, що діє. Таким чином безболісно для бізнес-процесів проведено перехід усієї IT-інфраструктури компанії на нові рішення.

Удосконалений комутатор 1G/10Gigabit L3 серії NSS3330 - це мультисервісний високопродуктивний Ethernet комутатор нового покоління, розроблений Maipu для корпоративного ринку. Він забезпечує повністю безпечний, контрольований, стабільний та надійний високопродуктивний сервіс комутації L2/L3 від чіпа, апаратного забезпечення до програмного забезпечення. Основні функції комутатора – агрегація мережі або високоякісний гігабітний доступ до мережі.

Ключові особливості

Процесор та мікросхема перемикання нового покоління

Комутатор серії NSS3330 використовує мікросхему ЦП нового покоління та високопродуктивну мікросхему комутації для розробки високопродуктивного, надійного та керованого комутатора L3 Ethernet Lite нового покоління, що задовольняє потреби корпоративних та державних замовників у розгортанні високопродуктивної та безпечної мережі. Він надає користувачам мультисервісне та безпечне інтегроване рішення для забезпечення повних вимог безпеки мережі від чіпа, апаратного до програмного забезпечення.

Нова стабільна, безпечна та надійна ОС

Комутатор серії NSS3330 використовує нову операційну систему, яка є зрілою та стабільною. Він успадкував фінансові та операторські технології, накопичені Maipu за більш ніж 20 років, і майже один мільйон пристроїв було протестовано у роботі мережі. Операційна система комутатора Maipu має незалежні права на інтелектуальну власність та пройшла тест на сканування вразливостей у центрі виявлення продуктів інформаційної безпеки Міністерства громадської безпеки Китаю.

Підтримка шифрування рівня керування, ефективне забезпечення безпеки мережі [8].

Файл конфігурації комутатора серії NSS3330 підтримує шифрування, запобігаючи зламуванню обладнання та доступу до нього, а також крадіжці та витоку даних управління, щоб забезпечити безпеку та надійність рівня управління комутатором. Пристрій підтримує найпоширеніші протоколи управління. Він підтримує шифрування пакетів протоколу, гарантуючи відсутність витоку протоколу топології мережі. Він підтримує автентифікацію довіреного обладнання. Прийміть автентифікацію 802.1X для пристроїв комутатора, підключених до мережі, щоб оцінити достовірність підключених пристроїв та запобігти доступу недійсних пристроїв до мережі, забезпечивши безпеку та надійність рівня керування комутатором.

Рисунок 2.3 – Вигляд комутатора NSS3330

Таблиця 2.1 – Характеристики комутатора NSS3330

Модель	NSS3330-30TXF-AC	NSS3330-54TXF-AC
Конфигурація		
Коммутаційна здатність (Гбіт/с)	168 Гбіт/с	216 Гбіт/с
Пропускна здатність (pps)	125 мілльйонів пакетів в секунду	161 мілльйонів пакетів в секунду
Память (ГБ)	1 ГБ	1 ГБ
Інтерфейси	24 мідних порта 10/100/1000M, 6 портів SFP+ (підтримка 1G/10G)	48 мідних порта 10/100/1000M, 6 портів SFP+ (підтримка 1G/10G)

Джерело живлення	2	2
Інтерфейсикерування	Один консольний порт, один Ethernet-інтерфейс управління DC0, один USB-інтерфейс	
Розміри (Ш×Г×В)	440×320×44,2 мм	
Вхідна напруга	100-240 В, 50/60 Гц	
Температура	Робоча температура: від -5℃ до 55℃ Температура зберігання:від -40℃ до 70℃	
Розмір таблиці MAC адрес	128K	
Кількість VLAN	4K	
Функції програмного забезпечення		
Ethernet-інтерфейси	Ethernet Interface, VLAN L3 Interface, Loopback Interface, Port Isolation, Loop Detection	
L2 Функції	VLAN, Super VLAN, PVLAN, Voice VLAN, MSTP, ERPS(G.8032), LACP, IGMP Snooping, IGMP Snooping Proxy, MVLAN Plus, L2 Static Multicast, MLD Snooping, PPPoE+, ULPP/UDLD, LLDP	
L3 Функції		
IP Protocol	TCP/IP, DNS, DHCP, FTP, TFTP, NTP, Telnet	
IPv4 Routing Protocol	Static Route, RIPv1/v2, OSPFv2, Policy Route	
IPv6 Routing Protocol	Static Routev6, OSPFv3	
Віртуалізація (стекінг)	H-VST; M-VST	
Безпека	802.1X, AAA, ACL, Radius, SPAN, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, Port Security, Attack-Detection, CPU Guard, LAND/SYN Flood/Smurf/Ping Flood/TearDrop Attack Detection	
QoS	802.1P, DSCP, Rate Limitation, CAR, SP, WDRR, SP+WDRR, WRED	
Висока доступність	VRRP, Track, HA Management	
Керування	SNMP, ROM, DDMI, SSH, WEB, Telnet, Syslog	

Маршрутизатори серії MP1900X поєднують функції маршрутизації, комутації та безпеки, підтримують багаті алгоритми шифрування та повністю захищають безпеку даних. Функція перемикання LAN L2/L3 значно підвищила гнучкість фіксованого інтерфейсу.

Маршрутизатор серії MP1900X — версія наступного покоління серії MP1800-35E, яка широко використовується в багатьох країнах. Він включає дві моделі: MP1900X-12-AC, MP1900X-22-AC.

Гнучкий uplink

Роутери серії MP1900X поєднують фіксовані інтерфейси WAN та LAN. У сценарії оптичного доступу каналом MSTP не потрібно налаштовувати фотоелектричний перетворювач; Тим часом порти uplink підтримують різні основні технології доступу до глобальної мережі, такі як Ethernet, 5G/4G LTE, TDM і т.д.

Маршрутизатор серії MP1900X має модульну конструкцію. Роутери підтримують два слоти для розширення, які можна вставляти різні модулі, такі як Ethernet, 3G/4G, E1, V.35, POS тощо. Така конструкція може значно захистити інвестиції клієнтів.

Підвищення продуктивності

Маршрутизатори серії MP1900X досягають швидкості пересилання понад 500 тис. пакетів за секунду, а налаштований ACL і QoS мало впливають на продуктивність пересилання.

Вбудовані LAN порти

Роутери серії MP1900X підтримує до восьми фіксованих гігабітних портів доступу 1000M, забезпечуючи можливість доступу до IP-терміналу та відповідаючи вимогам користувача щодо інтеграції маршрутизації та комутації для побудови мереж доступу.

Розширений безпечний сервіс

Роутери серії MP1900X підтримують всі функції безпеки, такі як технології аутентифікації портів, включаючи аутентифікацію 802.1x та аутентифікацію MAC-адрес, методи аутентифікації пристроїв, включаючи RADIUS та TACACS.

Маршрутизатор серії MP1900X має функцію VPN та може бути підключений до приватного каналу VPDN підприємства на основі мережі 3G/4G/5G. При цьому ці роутери можуть передавати трафік захищеним тунелем MPLS/VPLS, IPSec, GRE, L2TP, запобігаючи доступу до даних та їх підробці, а також забезпечуючи більш високий рівень безпеки додатків у мережі.

Великі програмні можливості

Маршрутизатори серії MP1900X підтримують різні прикладні технології, такі як IPv4/IPv6, VPN, MPLS, багатоадресне розсилання, ACL, прив'язка MAC-адрес, контроль доступу, обмеження пропускної спроможності, MSTP та NAT; Роутери підтримують протоколи резервування ресурсів RSVP та CAR; забезпечує ієрархічну функцію QoS для забезпечення високого пріоритету ключових послуг; MP1900X підтримують політики управління чергами, такі як FIFO, PQ, CQ, FQ, WFQ, CBWFQ та LLQ.

Різні режими керування

Маршрутизатор серії MP1900X підтримує наступні режими управління: SNMPv1/v2c/v3, інтерфейс командного рядка CLI, розгортання USB-накопичувача, MIB, RMON, SYSLOG, TR069, IPFIX і т. д. У поєднанні з платформою Maipu E5G він може забезпечити просте у використанні віддалене керування мережею.

Рисунок 2.4 – Вигляд маршрутизатора серії MP1900X

Таблиця 2.2 – Характеристики маршрутизатора серії MP1900X

Модель	**MP1900X-12-AC**	**MP1900X-22-AC**
Конфігурація обладнання		
CPU	1.0GHZDualCore	1.6GHZDualCore
Memory	512 МБ	512 МБ
Flash	128 МБ	128 МБ
Фіксованіінтерфейси (WAN&LAN)	1GEF WAN + 8GET LAN	1GEF+4GET WAN + 8GET LAN
Продуктивність	≥500 000 пакетів в секунду	≥800 000 пакетів в секунду
Інтерфейс USB2.0	1	1
5G Module Band	5G (N28/N41/N78/N79); 4G:LTE-FDD (B1/B3/B5/B7/B8/B18/B19/B20/B26/B28/B32),LTE-TDD (B34/B38/B39/B40/B41/B42/B43), WCDMA, GSM	
4G Module Band	LTE-FDD mode (band:1/3/5/7/8), TD-LTE mode (band 38/39/40/41), WCDMA/ GSM	
Service slots	Two RM2B slots	
Консольний порт	1	1
Розміри (Ш × Г × В)	340*260*44,2 мм (1U)	
Потужністьь	≤26 Вт	
Источник питания	Входное напряжение (переменный ток): 100–240 В, 50–60 Гц	
Маса	≤3 кг	
Програмне забезпечення		
Протоколи канального рівня	DDR, PPP, Frame-Relay, Bridge, HDLC, SNA, PPPoE, LACP, Port isolation, VLAN(4096), Q-in-Q, MSTP, loopback detection, Error-Disable, MSTP, SPAN, LLDP, MTU(1500bytes)	

TCP/IP-протоколи	DHCP, DHCPv6, DDNS/DNS, NAT/NAT64, NAT session up to 200K, Capability to create new session＞200
Протоколи маршрутизації	Static Route/Static Routev6, RIP/RIPng, OSPFv2/OSPFv3, BGP/BGP4+, IS-IS/IS-ISv6, IRMP, PBR
Безпека	Support ACL security filtering, PPP encryption, SSH, CPU protection, port security, AAA, IKE, PKI, 802.1X, URFP
VPN	MPLS, LDP, L2VPN, L3VPN, MPLS QoS, MPLS OAM, 6PE, GRE/GREv6, IPIP, L2TP, L2TPv3, VRF
QoS	FIFO, PQ, FQ, WFQ, CBWFQ, LLQ, RSVP, CAR, H-QoS, traffic shaping, Rate Limitation
Multicast	IGMP, MLD, PIM-SM/SSM, PIM-DM/SDM PIMv6-SM/SSM, MSDP, MVPN, NG-MVPN, PIMv6-SM/SSM
Надійність	Backup interface, VRRP/VRRPv3, VBRP, Track, BFD/BFDv6, Automatic switching to WAN 2 when WAN 1 loses signal,flow based load balancing on WAN port
Керування і моніторинг	Keepalive gateway, NTP, Mirroring, RMON, CWMP, CLI, SSH, WEB, SNMP V1/V2/V3, Telnet, PING, Trace Route, Login, FTP, TFTP, TR069, IPFIX traffic monitoring, IP-SLA

У часи хмарних розрахунків та мобільного зв'язку зі швидким збільшенням трафіку, тенденція розвитку диверсифікації обслуговування клієнтів та вирівнювання мережі підвищує вимоги щодо можливості агрегації мережі для маршрутизатора. Висока надійність, висока продуктивність, висока щільність портів, високий рівень безпеки та екологічність – ось нагальні вимоги замовника до агрегаційного маршрутизатора. Виходячи з вимог клієнтів, Maipu запускає централізований маршрутизатор агрегації послуг нового покоління серії MP3900X.

Маршрутизатор агрегації серії MP3900X — версія наступного покоління серії MP3900, яка широко використовується в багатьох країнах. Він включає дві моделі: MP3900X-06, MP3900X-08.

MP3900X-06 підтримує 8 гігабітних комбінованих інтерфейсів WAN, 6 слотів RM2B, два джерела живлення змінного струму;

MP3900X-08 підтримує 1 слот SPU, 6 слотів RM2B, 2 слоти RM3E, 2 слоти живлення, 1 слот вентилятора.

Особливості продукту

Гнучкі uplink

Маршрутизатор агрегації серії MP3900X підтримує чотири типи високопродуктивних модулів SPU, які поєднують гігабітні або 10-гігабітні фіксовані інтерфейси WAN, клієнтам не потрібно налаштовувати додатковий модуль WAN; Тим часом, порти uplink MP3900X підтримують основні технології каналів доступу до глобальної мережі, такі як Ethernet, 3G/4G, E1/CE1, POS/CPOS та послідовна лінія V.35.

Більше шести слотів розширення.

Роутер агрегації серії MP3900X має модульну конструкцію із достатньою кількістю слотів розширення. Весь пристрій повністю підтримує 6/6+2 розширених слота. Широкі можливості розширення можуть забезпечити доступ із високою щільністю та захистити інвестиції клієнтів. Усі модулі серії MP3900X підтримують гарячу заміну.

Висока продуктивність.

Маршрутизатор агрегації серії MP3900X підтримує високу продуктивність пересилання, а налаштований ACL та QoS мало впливають на продуктивність пересилання. Крім того, замовник може підвищити продуктивність, змінивши сервісні механізми SPU.

Розширений безпечний сервіс.

Маршрутизатор агрегації серії MP3900X підтримує всі функції безпеки, такі як технології аутентифікації портів, включаючи аутентифікацію 802.1x та аутентифікацію MAC-адрес, методи аутентифікації пристроїв, включаючи RADIUS та TACACS. Агрегуючий роутер серії MP3900X має функцію VPN та

може бути підключений до приватного каналу VPDN підприємства на основі мережі 3G/4G. При цьому дані пристрою можуть передавати трафік захищеним каналам і тунелям MPLS/VPLS, IPSec, GRE, L2TP, запобігаючи доступу до даних та їх підробці, а також забезпечуючи більш високий рівень безпеки програми в мережі.

Багаті програмні можливості.

Маршрутизатор агрегації серії MP3900 надає широкі можливості програмного забезпечення; підтримує різні прикладні технології, такі як IPv4/IPv6, VPN, MPLS, багатоадресне розсилання, ACL, прив'язка MAC-адрес, контроль доступу, обмеження пропускної спроможності, MSTP та NAT; підтримує протокол резервування ресурсів RSVP та CAR; забезпечує ієрархічну функцію QoS для забезпечення високого пріоритету ключових послуг; підтримувати політики управління чергами, такі як FIFO, PQ, CQ, FQ, WFQ, CBWFQ та LLQ.

Великі можливості управління.

Агрегуючий роутер серії MP3900X підтримує наступні режими управління: SNMPv1/v2c/v3, CLI, розгортання USB-накопичувача, MIB, RMON, SYSLOG, TR069, IPFIX і т. д. У поєднанні з платформою управління SNMP Maipu він може забезпечити просте та зручне використання віддаленого управління мережею.

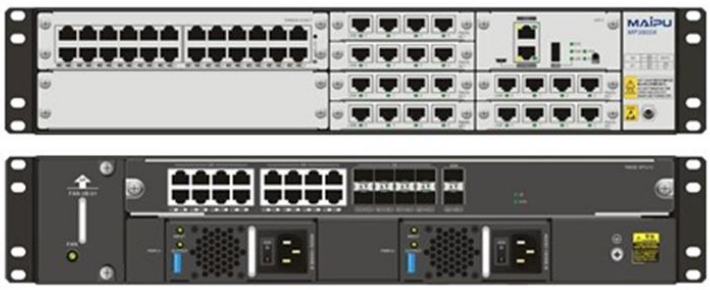

Рисунок 2.5 – Вигляд маршрутизатора серії MP3900X

Таблиця 2.3 – Характеристики маршрутизатора серії MP3900X

Специфікація	**MP3900X-06**	**MP3900X-08**			
Процесор	1.2GHZ 8 Core	1.2GHZ 8 Core	1.2GHZ 8 Core	1.5GHZ 16 Core	1.6GHZ 24 Core
USB2.0 Port	1	1	1	1	1
Console Port (RJ45)	1	1	1	1	1
Micro USB Port	1	1	1	1	1
SPU Module	N/A	SPU03	SPU05	SPU10	SPU40
Memory	2G	2G	2G	4G	8G
Flash	8G	8G	8G	8G	8G
Фиксированные WAN-интерфейсы	8GE Combo	2GE Combo+1GEF	16GET+8GEF	16GET+8GEF +2*10GE	4GET+4GEF+4GE Combo+4*10GE
SPU Slots	N/A	N/A	N/A	N/A	N/A
Service Slots	6*RM2B Slots	6*RM2B Slots + 2*RM3E Slots			
Power Supply	2*Fixed AC Power	2*Modular Power Slots			
Fan	Фіксовані вентилятори	1 * модульний слот для вентилятора			
Розміри Ш*Г*В(мм)	442*380*44.2	442*365*88.2 (2U)			
Вхідна напруга	AC 100-240V	AC 100-240V или DC -48V			
Температура	Робоча температура: 0 - 45 ℃; Температура зберігання: -40 – 70 ℃				
Споживана	60 Вт	110 Вт	120 Вт	180 В	

потужність					

Рішення OpenYard допомагають клієнтам збільшувати потужності, впроваджувати останні розробки та стабільно зростати. Ми створюємо продукти та підбираємо конфігурації, які можна вводити в експлуатацію швидко та без зупинки бізнес-процесів. У портфелі рішень OpenYard дві основні лінійки продуктів: базова для широкого кола завдань і форм-факторі OCP для масштабів ЦОДів.

Багатофункціональний та потужний сервер для обробки великого обсягу даних. Може підключатися до різних пристроїв та обладнання залежно від ваших завдань.

Цей сервер має більше місця для зберігання даних і два резервні блоки живлення потужністю 1600 Вт. Якщо один із блоків вийде з ладу, інший продовжить роботу, щоб сервер не вимкнувся.

До 128 ядер

256 потоків

До8 ТБ RAM

32 роз'єми DIMM

До780 ТБ

на NVMe SSD

До 8 плат розширення PCIe

залежно від реалізації

Таблиця 2.4 – Характеристики сервера серії OpenYard

Модулі памяті	8 каналів памятіDDR4 до 32 модулівRDIMM
Локальні диски	До 26 SFF 2.5" Підтримка NVMe/SAS/SATA Підтримка PCIe Gen4 NVMe Підтримкагарячоїзаміни
Слото розширення	PCIe Gen4 1 разъём PCIe Gen4 x16 OCP 3.0 1 разъём PCIe Gen3 x8 OCP 2.0
Можливості розширения	Апаратний RAID зпідтримкоюRAID 0, 1, 5, 6, 10, 50, 60 Сетевыекарты 10/25/40 GbE или 100 GbE Адаптеры FC 16/32G Другие адаптеры и опции ввода/вывода
Блоки живлення	2 блока живлення 1600 Вт з резервуванням

Рисунок 2.6 – Вигляд сервера серії OpenYard

2.5 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Попередня перевірка придатності пропускної спроможності каналів звязку та можливостей маршрутизаторів для забезпечення швидкої та надійної передачі пакетів проводиться за допомогою розрахунку.

Розрахунок доволяє визначити наступні характеристики:: коефіцієнт зайнятості обслуговуючого маршрутизатора, завантаження каналу передачі даних маршрутизатора, середню затримку кадру, середню довжину черги, середній час перебування пакета в черзі, пропускну здатність каналу.

Для визначення описаних параметрів локальну мережу приймаємо як модель мережі масового обслуговування M/M/1.

Задано:

кількість вузлів в найбільшій мережі: 201

середня інтенсивність трафіку: μ= 159 (кадрів/с)

середня довжина повідомлення: l=650 байт;

вимоги до затримки передачі пакету – ≤6 мс.

Відповдно до кількості пристроїв в мережі на рівні розподілу обираємо роутер MP1900X серії. (1 шт), на рівні доступу комутатор MP3900X (5 шт).

Рішення:

Вихідний трафік пересилається на маршрутизатор в лінію з пропускною здатністю 1000 Мбіт/с.

Для того, щоб комутатор рівня розподілу не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку μ=159 (кадрів/с), а середня довжина повідомлення – 650 байт.

Розрахуємо пропускну здатність мережі на рівні доступу припускаючи, що послугами одночасно користуються 100% користувачів.

Рр.д= μ*l*n*8= 159*650*240*8= 198,43 (Мбіт/с), де

n- кількість портів в комутаторі рівня доступу.

Пропускна здатність мережі на рівні розподілу розраховується наступним чином. Так як до одного роутера рівня розподілу підходять 5 комутаторів рівня доступу, а загальна кількість користувачів дорівнює 201, то пропускна здатність мережі на рівні розподілу буде дорівнює:

Рр.р= μ*l*N*8= 133*650*201*8= 166,2 (Мбіт/с), де

N - кількість вузлів в найбільшій мережі.

Отримані при розрахунку результати не перевищують задані параметри мережі. Отже, перевантажень на обраному обладнанні не буде.

Якщо комутатор рівня розподілу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 1000Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

μвих=1000 000 000/(650*8)=192 307 пакетів/с

Оскільки кожне джерело виробляє в середньому 159 пакетів/с, то ми обмежені приєднанням до комутатора рівня розподілу максимум:

N=192307/159=1209 джерел.

Що повністю задовольняє нашу мережу на 201 ПК.

Інтенсивність вихідного трафіку від всіх користувачів:

λ=N*μ= 201*159=31959 (пакетів/с)

Коефіцієнт затримки на рівні розподілу, тобто показник завантаженості вихідного каналу зв'язку, який впливає на час стояння в черзі:

ρ=λ/μ_вих =31959/192307=0,16

Коефіцієнт зайнятості комутатора рівня розподілу:

r=ρ/(1-ρ)=0,16/(1-0,16)=0.19

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

T=1/((μ-λ))=1/(192307-31959)=6.2 мкс

Середня довжина черги:

L_чер=ρ^2/(1-ρ)= ⟦0,16^2/(1-0,16)]=0.03

Ця цифра може бути корисною при налаштуванні черг на обладнанні - в апаратурі можна вказувати максимальний розмір черги пакетів. В даному випадку в системі на обслуговуванні менше 1 пакету, значення досить умовне; воно свідчить про те, що система працює з великим запасом по продуктивності [9].

Середній час перебування пакета в черзі

T_оч=L_чер/λ=0,03/31959=0.9 мкс

Це значення менше необхідного значення ≤6 мс, що задовольняє вимогам.

Пропускна здатність каналу:

λ=(пропускна здатність)/(довжина кадру)=b/l

b=λ*l=31959*650*8= 166.2 Мбіт/с

Що задовольняє пропускній здатності вихідного каналу.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

Технологія VLSM (Variable Length Subnet Mask, маска підмережі змінної довжини) дозволяє організації використовувати більше однієї маски підмережі всередині того самого адресного простору і ділити мережу на підмережі різних розмірів. Була створена у 1987 році та визначена у RFC 1009.

Маска VLSM дозволяє розбити мережу на підмережі, а потім розбити ще на підмережі з різними масками підмережі. Замість маски підмережі в VLSM використовується нотація IP-адреса/довжина префікса, аналогічна нотації безкласової адресації. Число після "/" означає кількість одиничних розрядів у масці підмережі.

У найширшому сенсі робота з підмережею - це спосіб створення двох або більше підмереж з однієї мережевої адреси. Тобто логічний розподіл мережі IP. Сама по собі IP-адреса розділена маскою підмережі на префікс мережі та адресу вузла. У мережі вузлом може вважатися будь-який мережний пристрій, а саме мережевий інтерфейс цього пристрою, якому присвоєно IP-адресу. Таким чином, комп'ютери, які входять в одну підмережу, належать одному діапазону IP-адрес. Загалом підмережі дозволяють підвищити ефективність використання доступного адресного простору. Для побудови мережі використаний адресний простір 10.25.IPn.0/22IPn=8. Розрахунок схеми адресації виконаний згідно до технічних вимог.

Таблиця 3.1 – Кількість вузлів в підмережах ТОВ «Сінгл-ойл»

LAN1	LAN2	LAN3	LAN4	LAN5
7	100	201	88	69

В таблиці 3.2 наведена схема IP-адресації локальних мереж в корпоративній компютерній мережі.

LAN1	7	14	10.25.10.128	/28	255.255.255.240	10.25.10.129 - 10.25.10.142	10.25.10.143
LAN2	100	126	10.25.9.0	/25	255.255.255.128	10.25.9.1 - 10.25.9.126	10.25.9.127
LAN3	201	254	10.25.8.0	/24	255.255.255.0	10.25.8.1 - 10.25.8.254	10.25.8.255
LAN4	88	126	10.25.9.128	/25	255.255.255.128	10.25.9.129 - 10.25.9.254	10.25.9.255
LAN5	69	126	10.25.10.0	/25	255.255.255.128	10.25.10.1 - 10.25.10.126	10.25.10.127
VLAN11	20	30	10.25.8.0	/27	255.255.255.224	10.25.8.1 - 10.25.8.30	10.25.8.31
VLAN21	20	30	10.25.8.32	/27	255.255.255.224	10.25.8.33 - 10.25.8.62	10.25.8.63
VLAN31	20	30	10.25.8.64	/27	255.255.255.224	10.25.8.65 - 10.25.8.94	10.25.8.95
VLAN99	20	30	10.25.8.96	/27	255.255.255.224	10.25.8.97 - 10.25.8.126	10.25.8.127
WAN1	2	2	10.0.1.0	/30	255.255.255.252	10.0.1.1 - 10.0.1.2	10.0.1.3
WAN2	2	2	10.0.1.4	/30	255.255.255.252	10.0.1.5 - 10.0.1.6	10.0.1.7
WAN3	2	2	10.0.1.8	/30	255.255.255.252	10.0.1.9 - 10.0.1.10	10.0.1.11
WAN4	2	2	10.0.1.12	/30	255.255.255.252	10.0.1.13 - 10.0.1.14	10.0.1.15
WAN5	2	2	10.0.1.16	/30	255.255.255.252	10.0.1.17 - 10.0.1.18	10.0.1.19
WAN6	2	2	10.0.1.20	/30	255.255.255.252	10.0.1.21 - 10.0.1.22	10.0.1.23
WAN7	2	2	10.0.1.24	/30	255.255.255.252	10.0.1.25 - 10.0.1.26	10.0.1.27
WAN8	2	2	10.0.1.28	/30	255.255.255.252	10.0.1.29 - 10.0.1.30	10.0.1.31

Рисунок 3.1 – Адресація мережі з використанням VLSMонлайн калькулятора

Таблиця 3.2 – Схема адресації мережі

Назва підмережі	Розмір	Адреса	Десяткова маска	Діапазон доступних адрес
LAN1	7	10.25.10.128	255.255.255.240	10.25.10.129 - 10.25.10.142
LAN2	100	10.25.9.0	255.255.255.128	10.25.9.1 - 10.25.9.126
LAN3	201	10.25.8.0	255.255.255.0	10.25.8.1 - 10.25.8.254
LAN4	88	10.25.9.128	255.255.255.128	10.25.9.129 - 10.25.9.254
LAN5	69	10.25.10.0	255.255.255.128	10.25.10.1 - 10.25.10.126
VLAN11	30	10.25.8.0	255.255.255.224	10.25.8.1 - 10.25.8.30
VLAN21	30	10.25.8.32	255.255.255.224	10.25.8.33 - 10.25.8.62
VLAN31	30	10.25.8.64	255.255.255.224	10.25.8.65 - 10.25.8.94
VLAN99	30	10.25.8.96	255.255.255.224	10.25.8.97 - 10.25.8.126
WAN1	2	10.0.1.0	255.255.255.252	10.0.1.1 - 10.0.1.2
WAN2	2	10.0.1.4	255.255.255.252	10.0.1.5 - 10.0.1.6
WAN3	2	10.0.1.8	255.255.255.252	10.0.1.9 - 10.0.1.10
WAN4	2	10.0.1.12	255.255.255.252	10.0.1.13 - 10.0.1.14
WAN5	2	10.0.1.16	255.255.255.252	10.0.1.17 - 10.0.1.18
WAN6	2	10.0.1.20	255.255.255.252	10.0.1.21 - 10.0.1.22
WAN7	2	10.0.1.24	255.255.255.252	10.0.1.25 - 10.0.1.26
WAN8	2	10.0.1.28	255.255.255.252	10.0.1.29 - 10.0.1.30

Таблиця 3.3 – Схема адресації пристроїв мережі

Ім'я пристрою	Інтер-фейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
LAN_1						
Atanasov_R2	G0/0	10.25.10.129	/28	-	-	Sw0
	G0/1	10.25.10.1	/25	-	-	Sw1
	G0/2	10.0.1.1	/30	-	-	R3 G0/0
Atanasov _Sw0	G0/0	10.25.10.130	/28	10.25.10.129	-	R2 G0/0
PC1_1 – PC1_7	NIC	10.25.10.131-10.25.10.138	/28	10.25.10.129	-	-
LAN_2						
Atanasov_R1	G0/0	10.25.9.1	/25	-	-	Sw3
	G0/1	10.0.1.5	/30	-	-	R3 G0/1
	G0/2	10.0.1.9	/30	-	-	R5 G0/1
Atanasov _Sw3	Vlan1	10.25.9.2	/25	10.25.9.1	-	R1 G0/0
PC2_1 – PC2_99	NIC	10.25.9.12-10.25.9.111	/25	10.25.9.1	-	-
Server_HTTP	NIC	10.25.9.11	/25	10.25.9.1	-	-
LAN_3						
Atanasov_R4	G0/0	10.25.8.1	/24	-	-	Sw6
	G0/1	10.0.1.21	/30	-		R5_1 G0/1
	G0/0/11	10.25.8.1	/27	-	VLAN11	
	G0/0/21	10.0.1.21	/27	-	VLAN21	
	G0/0/31	10.25.8.1	/27	-	VLAN31	
	G0/0/99	10.0.1.21	/27	-		
Atanasov _Sw6	Vlan99	10.25.8.1	/24	10.25.8.1	VLAN99	
PC3_1 – PC3_18	NIC	10.25.8.12-10.25.8.30	/27	10.25.8.1	VLAN11	-
PC3_19 – PC3_49	NIC	10.25.8.33-10.25.8.62	/27	10.25.8.1	VLAN21	-
PC3_50 – PC3_80	NIC	10.25.8.65-10.25.8.94	/27	10.25.8.1	VLAN31	-
ServerDNS	NIC	10.25.8.11	/24	10.25.8.1	-	-
LAN_4						
Atanasov_R0	G0/1	10.0.1.29	/30	-	-	ISP G0/0
	G0/0	10.25.9.129	/25	-	-	Sw12
Atanasov _Sw12	Vlan1	10.25.9.130	/25	10.25.9.129		R4 G0/0
PC4_1- PC4_87	NIC	10.25.9.140-10.25.9.227	/25	10.25.9.129	-	-
Server_TFTP	NIC	10.25.9.139	/25	10.25.9.129	-	-

Продовження таблиці 3.3

LAN_5						
Atanasov_R2	G0/0	10.25.10.129	/28	-	-	Sw0
	G0/1	10.25.10.1	/25	-	-	Sw1

	G0/2	10.0.1.1	/30	-	-	R3 G0/0
Atanasov _Sw1	Vlan1	10.25.10.2	/25	10.25.10.1	-	R2 G0/1
PC5_1-PC5_69	NIC	10.25.10.3-10.25.10.71	/25	10.25.10.1	-	-
Atanasov_R1	G0/0	10.25.9.1	/28	-	-	Sw3
	G0/1	10.0.1.5	/30	-	-	R3 G0/1
	G0/2	10.0.1.9	/30	-	-	R5 G0/1
Atanasov_R3	G0/0	10.0.1.2	/30	-	-	R2 G0/2
	G0/1	10.0.1.6	/30	-	-	R1 G0/1
	G0/2	10.0.1.13	/30	-	-	R5 G0/0
Atanasov_R5	G0/0	10.0.1.14	/30	-	-	R3 G0/2
	G0/1	10.0.1.10	/30	-	-	R1 G0/2
	G0/2	10.0.1.17	/30	-	-	R5_1 G0/0
Atanasov_R5_1	G0/0	10.0.1.18	/30	-	-	R5 G0/2
	G0/1	10.0.1.22	/30	-	-	R4 G0/1
	G0/2	10.0.1.25	/30	-	-	ISP G0/1
Rout_ISP	G0/0	10.0.1.30	/30	-	-	R0 G0/1
	G0/1	10.0.1.26	/30	-	-	R5_1 G0/2
	G0/2	209.165.200.5	/30	-	-	PC00
PC00	-	209.165.200.6	/30	209.165.200.5	-	ISP G0/2

3.2 Розробка логічної схеми корпоративної мережі

Модель компютерної мережі, розроблена в пакеті Cisco Packet Tracer, показує концепцію організації мережі. Налаштування окремих мережевих пристроїв, адресація та інші можливості дозволяють підтвердити вірність обраної архітектури та топології.

Логічна топологія мережі ТОВ «Сінгл-ойл» об’єднує п’ять підмереж. На рівні розподілу локальні мережі забезпечуються досить складною топологією маршрутизаторів.

Архітектура корпоративної мережі ТОВ «Сінгл-ойл» є ієрархічною, складною зіркою.

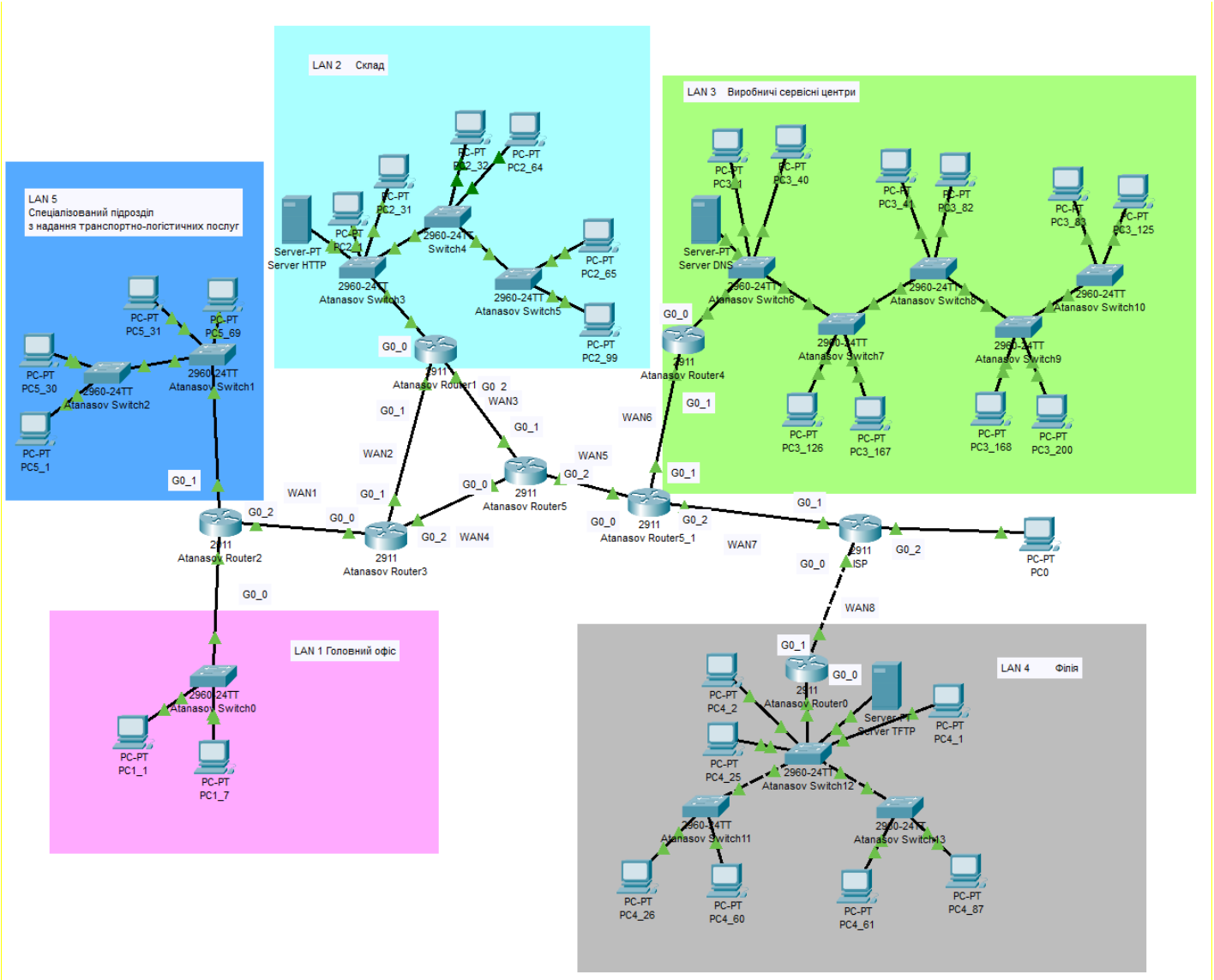

Рисунок 3.2 – Логічна схема корпоративної мережі ТОВ «Сінгл-ойл»

3.3 Розрахунок налаштувань маршрутизації корпоративної мережі

Маршрутизація забезпечує взаємодію між безліччю логічних підмереж. Налаштування маршрутизації за допомогою інтерфейсу командного рядка (CLI) Packet Tracer не відрізняється від конфігурування реального обладнання.

Статична маршрутизація – простий метод, що у тому чи іншому вигляді, представлений у більшості мереж. У Packet Tracer статична маршрутизація може бути налаштована за допомогою графічного інтерфейсу. При цьому методі конфігурування ми вводимо адресу мережі призначення та шлюз, необхідний досягнення цієї мережі. Кожен маршрутизатор у мережі повинен знати спосіб досягнення всіх одержувачів у мережі. При статичній маршрутизації потрібна чимала ручна робота. Так якщо один маршрутизатор додається (або видаляється) з мережі, на всіх, хто залишився, має бути проведено ручне оновлення цих змін.

3.4 Налаштування та перевірка роботи комп’ютерної системи

3.4.1 Базове налаштування конфігурації пристроїв

Використовуємо графічний інтерфейс і така конфігурація матиме мінімальну кількість інструкцій. Виконаємо такі кроки.

- Переходимо на вкладку "Налаштування" (Config). Далі вибираємо необхідний інтерфейс та налаштовуємо IP-адресу. Потім вмикаємо інтерфейс, вибравши опцію «Увімкнено» (On), поставивши прапорець.
- На цій вкладці в секції «Маршрутизація» (Routing) виберіть «Статична маршрутизація» (Static)
- Налаштування статичної маршрутизації полягає в ручному введенні в таблицю маршрутизації всіх маршрутів, які безпосередньо не підключені.

```
Router (config) #hostname Atanasov_R2
Atanasov_R2 (config) #no ip domain-lookup
Atanasov_R2 (config) #service password-encryption
Atanasov_R2 (config) #enable secret cisco
Atanasov_R2 (config) #line conscle 0
Atanasov_R2 (config-line) #password cisco
Atanasov_R2 (config-line) #login
Atanasov_R2 (config-line) #exit
Atanasov_R2 (config) #line vty 0 15
Atanasov_R2 (config-line) #password cisco
Atanasov_R2 (config-line) #login local
Atanasov_R2(config-line)#trans inp ssh
Atanasov_R2 (config-line) #exit
Atanasov_R2 (config) #banner motd #123-20 Atanasov. PROTECTION system. AAA
services Authorized!#
Atanasov_R2 (config) #username 12320_Atanasov password cisco
Atanasov_R2 (config) #ip domain-name Atanasov_R2
Atanasov_R2 (config) #cryp key g r
```

Рисунок 3.3 – Базове налаштування роутера Atanasov_R2

3.4.2 Налаштування маршрутизаторів корпоративної мережі

Використано протокол EIGRP для налаштування динамічної маршрутизації. Головниою перевагою якого є зниження навантаження на пропускну здатність мережі.

```
Atanasov_R2 (config)#router eigrp  2
*Mar 1 0:2:0.287: %SSH-S-ENABLED: SSH 1.99 has been enabled
Atanasov_RA(config-router) #redistribute static
Atanasov_R2(config-router) #no auto-sumary
Atanasov_R2(config-router) #network 10.0.1.0 0.0.0.3
Atanasov_R2[config-router) #network 10.25.10.128 0.0.0.63
Atanasov_R2(config-router) #network 10.25.10.0 0.0.0.63
Atanasov_R2 (config-router) #pas g0/0
Atanasov_R2 (config-rowter) #exit
Atanasov_R2 (config)#ip route 0.0.0.0 0.0.0.0 209.165.200.4
```

Рисунок 3.4 – Налаштування протоколу EIGRP 4 на Atanasov_R2

В Packet Tracer в режимі CiscoIOS перевірка налаштування маршрутизації проводиться *show ip route.* В таблиці маршрутизації повинні бути присутні:

безпосередньо підключені мережі (символ «C»);

локальні мережі (символ «L»);

віддалені мережі (отримані за протоколом EIGRP позначені символом «D»);

запис маршруту за замовчуванням, що складається з восьми нулів.

Виходячи з результатів налаштувань та перевірок робимо висновок про працездатність спректованої мережі.

3.4.3 Налаштування роботи Інтернет

NAT є технологією, яка дозволяє перенаправляти трафік між локальною та глобальною мережами, використовуючи мережеві адреси. Це дозволяє пристроям у локальній мережі зв'язуватися із зовнішньою мережею та навпаки. Тобто це свого роду міст між локальною та глобальною мережею. NAT виконує важливу функцію у мережах, забезпечуючи локальну взаємодію. Вона також підтримує загальну безпеку та приватність даних.

Працює за принципом "1 до 1", коли зіставляє локальні та глобальні адреси. Настанови, виставлені адміністратором для зіставлення, не змінюються. У процесі передачі даних у всесвітню мережу їх початкові локальні адреси трансформуються у глобальні IP-адреси, які заздалегідь встановлені системним адміністратором. Для веб-сервісів та пристроїв, де потрібна доступна погоджена адреса, відмінно підходить Static NAT Type. Щоб реалізувати статичний NAT, необхідно мати певну кількість загальнодоступних адрес. Статичний NAT широко застосовується в корпоративних мережах, тому що там часто є необхідність постійного доступу до IP-адреси з інтернету.

Переваги статичного NAT.

• Постійна доступність. Дозволяє надавати безперебійний доступ до конкретного локального ресурсу. З його допомогою пристрої та послуги завжди доступні.

• Зручність налаштування. Від адміністратора потрібно лише вказати, яка локальна адреса в яку глобальну має бути перетворена. Завдяки цьому можна точніше контролювати перетворення адрес.

Налаштування технології NAT на роутері Atanasov_R5_1.

```
Atanasov_R5_1(config) access-list 4 permit 10.25.10.128 0.0.3.255
Atanasov_R5_1(config) #ip nat pool Internet 209.165.200.5 209.165.200.30 netmask
255.255.255.224
Atanasov_R5_1(config) #ip nat inside source list 4 pool Internet
Atanasov_R5_1(config)#ip nat inside source static 10.25.10.129 209.165.200.6
Atanasov_R5_1(config)#ip route 0.0.0.0 0.0.0.0 205.165.200.5
Atanasov_R5_1(config)#ip route 10.25.10.128 255.255.252.0 so/o/o
Atanasov_R5_1(config) #interface g0/2
Atanasov_R5_1(config -if)#ip nat outside
Atanasov_R5_1(config -if)#interface g0/1
Atanasov_R5_1(config-if)#ip nat inside
Atanasov_R5_1(config -if)#interface g 0/0
Atanasov_R5_1(config -if)#ip nat inside
```

Рисунок 3.5 – Налаштування NATроутері Atanasov_R5_1

3.4.4 Перевірка роботи комп’ютерної системи

CMP (Internet Control Message Protocol) — мережевий протокол, що входить у стек протоколів TCP/IP. В основному ICMP використовується для передачі повідомлень про помилки та інші виняткові ситуації, що виникли при передачі даних.

Ping — утиліта для перевірки з'єднань у мережах на основі TCP/IP. Утиліта відправляє запити (ICMP Echo-Request) протоколу ICMP вказаному вузлу мережі та фіксує відповіді, що надходять (ICMP Echo-Reply). Час між відправкою запиту та отриманням відповіді (RTT) дозволяє визначати двосторонні затримки (RTT) за маршрутом і частоту втрати пакетів, тобто

опосередковано визначати завантаженість на каналах передачі даних та проміжних пристроях.

Повна відсутність ICMP-відповідей може також означати, що віддалений вузол (або будь-який з проміжних маршрутизаторів) блокує ICMP Echo-Reply або ігнорує ICMP Echo-Request.

У Packet Tracer передбачено режим моделювання (Симуляції), в якому показується, як працює утиліта Ping. Щоб перейти до цього режиму, натисніть значок Simulation Mode (Симуляція) у нижньому правому куті робочої області або комбінацію клавіш Shift+S. Відкриється Simulation Panel (Панель симуляції), де будуть відображатися всі події, пов'язані з виконання ping-процесу. Моделювання припиняється при завершенні ping-процесу, або при закритті вікна симуляції.

У режимі симуляції можна не тільки відстежувати протоколи, що використовуються, але і бачити, на якому з семи рівнів моделі OSI даний протокол задіяний. Під час перегляду анімації ми побачили принцип роботи хаба. Концентратор (хаб) повторює пакет на всіх портах, сподіваючись, що на одному з них є одержувач інформації. Якщо пакети якимось вузлам не призначені, ці вузли ігнорують пакети. А коли пакет повернеться відправнику, то ми побачимо галочку "прийняття пакету".

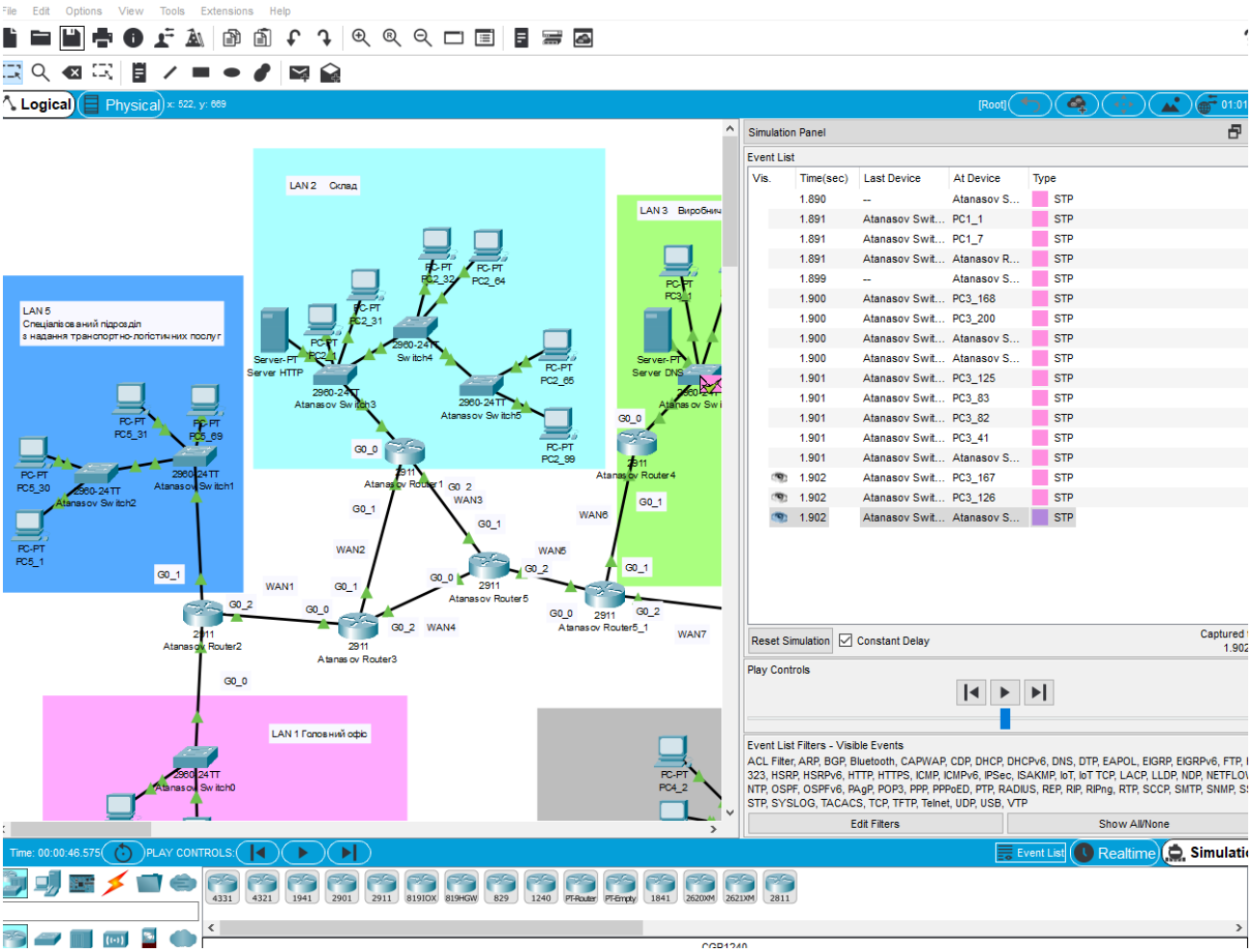

Рисунок 3.6 – Перевірка підключення

3.5 Захист інформації в комп’ютерній системі від несанкціонованого доступу

3.5.1 Розробка методів для захисту інформації в комп’ютерній системі

Усі методи захисту інформації характером дій можна розділити:

на законодавчі (правові);

організаційні;

технічні;

комплексні, які включають елементи всіх попередніх.

З огляду на різноманітність загроз захисту комп'ютерної системи чи мережі необхідно використовувати великий арсенал технічних засобів захисту, проте саме організаційні методи є стрижнем комплексної системи захисту у комп'ютерних системах і мережах. Тільки за допомогою цих методів можливе об'єднання на правовій основі всіх технічних засобів захисту в єдину комплексну систему.

Комплексні системи захисту інформації повинні мати централізоване управління. Централізація управління захистом інформації пояснюється необхідністю проведення єдиної політики у сфері безпеки інформаційних ресурсів у межах організації. Для здійснення централізованого управління в системі захисту інформації повинні бути передбачені спеціальні засоби дистанційного контролю, розподілу ключів, розмежування доступу та ін.

Комплексна система захисту інформації має бути дружньою стосовно користувачів та обслуговуючого персоналу. Вона має бути максимально автоматизована і не повинна вимагати від користувача виконувати значний обсяг дій, пов'язаних із захистом інформації. Разом про те комплексна система захисту інформації має створювати обмежень у виконанні користувачем своїх функціональних обов'язків.

Парольні методи автентифікації суб'єктів при вході в систему можуть застосовуватися на основі простих паролів, що динамічно змінюються.

При використанні методу простого пароля його значення не змінюється протягом встановленого адміністратором служби безпеки часу дії. Такий метод у тому, що суб'єкт набирає лише йому відому комбінацію символів. Даний пароль порівнюється з еталонним, що зберігається в системі, і при позитивному результаті перевірки суб'єкт отримує доступ до неї.

Таблиця 3.4 – Налаштування паролів базової конфігурації пристроїв

Паролі		
консолі і vty	привілейованого режиму	користувача
cisco123-20-2	class123-20-2	Atanasov_Vlad

3.5.2 Налаштування маршрутизаторів на підтримку служби AAA

Ідентифікація та верифікація мережними сервісами здійснюється за допомогою сервісу Authentication Authorization and Accounting та server RADIUS.

```
Atanasov_R5_1(config)#aaa new-model
Atanasov_R5_1(config)#aaa authentication login default local
Atanasov_R5_1(config)#aaa authentication login Login group radius local
Atanasov_R5_1(config)#line vty 0 4
Atanasov_R5_1(config-line)#login authentication default
Atanasov_R5_1(config-line)#radius-server host 10.25.9.145 auth-port 1645
Atanasov_R5_1(config)#radius-server key zzz
Atanasov_R5_1(config)#aaa authentication login SSH-LOGIN local
Atanasov_R5_1(config)#line vty 0 4
Atanasov_R5_1(config-line)#login authentication SSH-LOGIN
Atanasov_R5_1(config-line)#transport input ssh
Atanasov_R5_1(config-line) #exit
Atanasov_R5_1 (config) #
Atanasov_R5_1(config)#@conft t
Atanasov_R5_1(config)#radius-server host 10.25.9.145
Atanasov_R5_1(config)#radius-server key zzz
Atanasov_R5_1(config)#aaa authentication login default group radius local
```

Рисунок 3.7 – Конфігурація служби AAA на маршрутизаторі Atanasov_R5_1

3.5.3 Налаштування мережах VLAN та параметрів безпеки комутаторів

Передача кадрів між різними віртуальними мережами на підставі адреси канального рівня неможлива. Кожна віртуальна мережа утворює свій домен широкомовного трафіку. Перевагою технології віртуальних мереж є те, що вона дозволяє створювати повністю ізольовані сегменти мережі шляхом логічного конфігурування комутаторів, не вдаючись до зміни фізичної структури мережі.

Віртуальні локальні мережі можуть перекриватися, якщо один або більше мережевих пристроїв входять до складу більш ніж однієї віртуальної

мережі. Для зв'язування віртуальних мереж у загальну мережу потрібне залучення засобів мережного рівня (маршрутизатор або комутатор 3-го рівня).

```
Atanasov_Sw6(config)#vlan 11
Atanasov_Sw6(config-vlan) #name Service1
Atanasov_Sw6(config-vlan) #vlan21
Atanasov_Sw6(config-vlan) #name Service2
Atanasov_Sw6(config-vlan) #vlan31
Atanasov_Sw6(config-vlan) #name Service3
Atanasov_Sw6(config-vlan) #vlan 99
Atanasov_Sw6(config-vlan) #name Service4
Atanasov_Sw6(config-vlan) #vlan 1
Atanasov_Sw6(config-vlan) #name Native
Atanasov_Sw6(config-vlan) #exit
```

Рисунок 3.8 – Створення VLAN

```
Atanasov_Sw6(config)#int r f0/12-14
Atanasov_Sw6(config-if-range)#sw m a
Atanasov_Sw6(config-if-range)#no shut
Atanasov_Sw6(config-if-range)#sw av 14
Atanasov_Sw6(config-if-range)#
```

Рисунок 3.9 – Переведення портів в режим доступу

```
Atanasov_Sw6 (config)#int g0/0
Atanasov_Sw6 (config-if)#switchport mode trunk
Atanasov_Sw6 (config-if)#switchport trunk native vlan 1
Atanasov_Sw6 (config-if)#switchport trunk allowed vlan 11,21,31,99
Atanasov_Sw6 (config-if) #no shutdown
```

Рисунок 3.10 – Налаштування транку

4 СИСТЕМИ БЕЗПРОВІДНИХ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

Прийомо-передавальна апаратура останнім часом значно еволюціонувала, багато в чому завдяки переходу на "цифру". Дві області є потужним двигуном бездротових технологій. Одна з них – споживчий ринок, де смартфон – найпопулярніший споживчий пристрій у світі, що використовує технологію GSM, яка дозволяє здійснювати голосові дзвінки, надсилати текстові SMS-повідомлення та підключатися до Інтернету. Важко знайти вражаючий приклад впливу бездротових технологій на життя суспільства по всьому світу. Згадайте подібну революцію у 20 столітті завдяки засобам масової інформації: спочатку радіо, потім телебаченню.

Рисунок 4.1 – Засоби бездротового звязку

Смартфон має і додаткові радіоінтерфейси: Wi-Fi та Bluetooth. Без Wi-Fi неможливо було б підключитися до Інтернету через маршрутизатори доступу,

які дозволяють передавати дані. А одне з найвідоміших, але не єдине застосування Bluetooth – це можливість підключення до віддалених аудіосистем, наприклад, автомобільні комплекти гучного зв'язку або бездротові навушники.

На споживчому ринку використовується все більше передових технологій, що використовують бездротові з'єднання. Крім зв'язку GSM, тепер можна використовувати, наприклад, супутникову GPS навігацію або інші конкуруючі системи супутникової навігації. Ця технологія тепер настільки доступна, що використовується не тільки для комунікаційної навігації, але й для геотегування фотографій та інших подібних справ.

Другий напрямок – технологія Інтернету речей IoT, що динамічно розвивається. Важко уявити, щоб таке динамічне зростання було можливе без радіомереж.

Масове використання радіозв'язку користувачами, які мають кваліфікації до роботи передавальних і приймаючих пристроїв, вимагає спеціальних правил. Для таких девайсів смуги частот виділені без дозволів та зборів. Пристрої, що працюють у цих діапазонах, повинні мати лише законодавчо обмежену малу потужність та використовувати виділені канали. Найчастіше це діапазони ISM, зарезервовані для промислових, наукових та медичних додатків, не пов'язаних із телекомунікаціями. У різних країнах використовуються різні частоти, і при проектуванні пристрою, що працює в діапазонах ISM, необхідно вибрати відповідний частотний діапазон.

Прилади радіозв'язку мають багато переваг. Вони зручні та дешеві, тому що не вимагають дорогої проводки. Вони забезпечують необмежену мобільність у реальному діапазоні. Але вони мають і недоліки. Передача по радіоканалах вимагає все більш складного кодування для запобігання перехопленню даних або модифікації у злочинних цілях [6].

Іншою проблемою можуть бути електромагнітні перешкоди, що викликають згасання чи спотворення сигналу. У важливих програмах використовуються механізми для відновлення деяких втрачених даних за допомогою програмних методів. Але для цього потрібна надмірна передача даних, яка уповільнює фактичну швидкість.

4.1 Інтелектуальні радіоінтерфейси IQRF

Якщо потрібно просте рішення, але водночас надає унікальні можливості, варто поцікавитися пропозицією від компанії MICRORISC. Простий радіомодуль був підключений до невеликого мікроконтролера, і ця схема розміщена на невеликій друкованій платі. Така ідея не здається чимось новим, і вона справді була б такою, якби на цьому зупинилася.

Рисунок 4.2 – Зовнішній вигляд модуля TR72

Продукт набагато більше, ніж просто радіомодуль та мікроконтролер. Уся система була спроектована та зібрана з невеликих, простих у використанні та програмованих радіомодулів, комплектів DCC та пропрієтарних апаратних та

програмних інструментів, що забезпечують всебічну підтримку проектувальника.

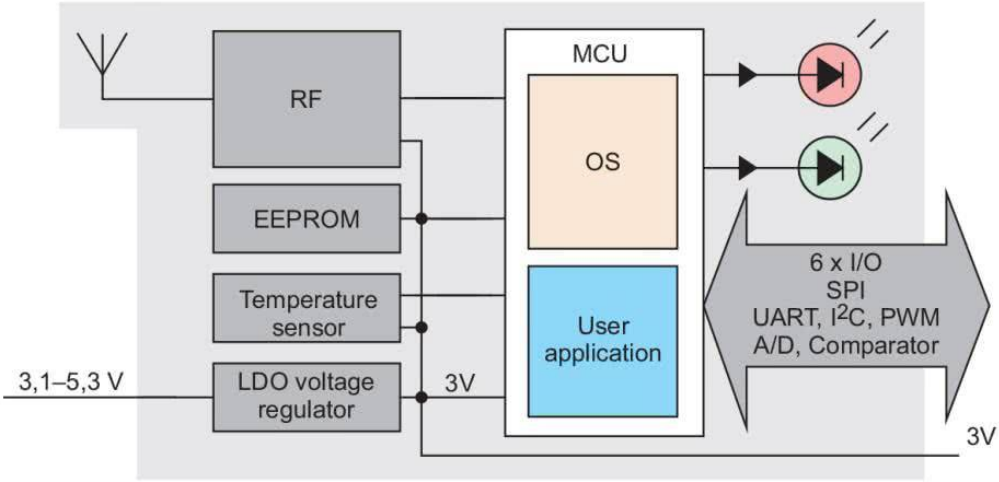

Рисунок 4.3 – Блок-схема модуля TR72

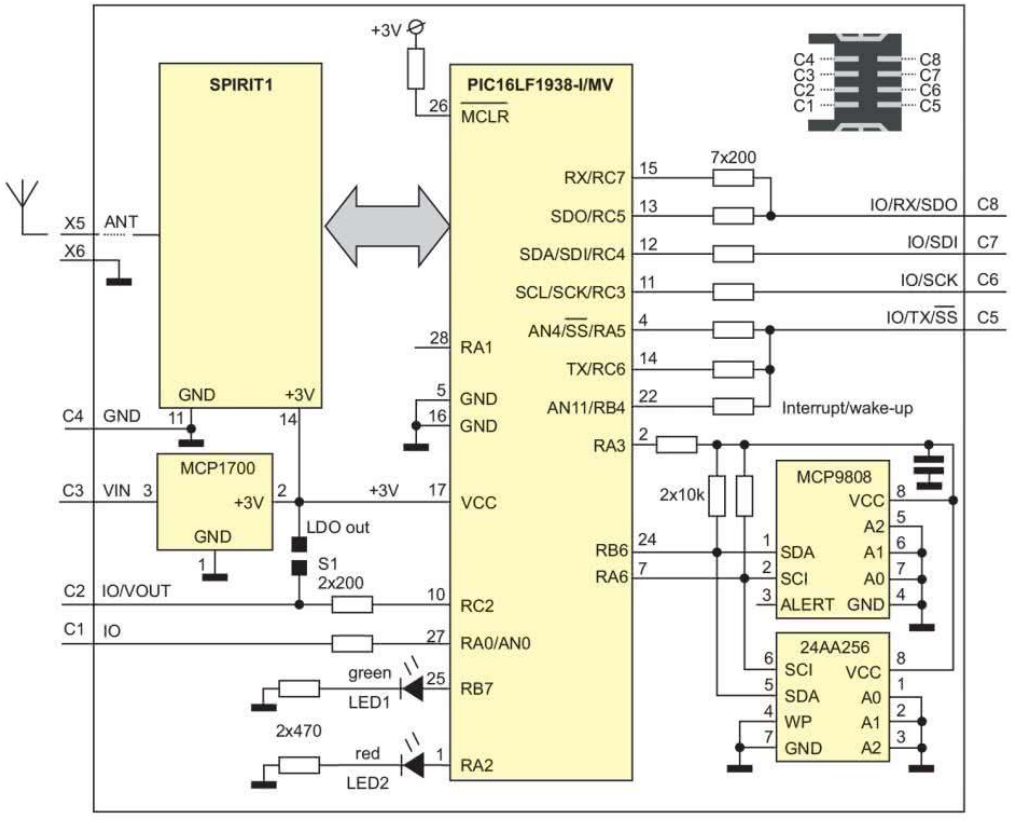

Рисунок 4.4 –Схема принципова модуля TR72

Користувач має у своєму розпорядженні частину пам'яті програм мікроконтролера і може розмістити свою прошивку, написану мовою С, що взаємодіє з вбудованою ОС. Продуктивність дуже простого ядра мікроконтролера PIC16F і доступні ресурси не дозволяють реалізувати більш просунуті протоколи радіозв'язку, але для простих справ дуже корисним є гнучке з'єднання мікроконтролера, що підтримується простий ОС, з радіомодулем [10].

Проста операційна система під назвою IQRF OS була встановлена на заводі на згадку про мікроконтролера модуля. У розпорядженні користувача є набір системних функцій. Вони використовуються передачі даних по радіоканалу і передачі у хост-систему (стандартно через інтерфейс SPI). Функції ОС IQRF підтримують роботу мереж MESH.

Програма користувача написана на С і скомпільована за допомогою компілятора CC5X. І тут виробник подбав про те, щоб вам не довелося турбуватися про необхідні інструменти. Безкоштовна версія компілятора є достатньою для написання великої програми. Слід пам'ятати, що такий модуль є інтелектуальною периферійною системою і на ньому не виконуються великі завдання. При необхідності радіомодуль виконує функції зв'язку, а складніші завдання виконує хост. Розробка програм можлива завдяки пакету IRQF IDE компанії.

Хоча, на перший погляд, це здається простим інструментом, у нього досить багато можливостей. З його допомогою ми можемо виконувати всі проектні дії: редагувати (за допомогою зовнішнього редактора) вихідний файл мови С, компілювати його, програмувати мікроконтролер радіомодуля та налагоджувати програму, що працює. І, нарешті, «програматор» модулів дозволяє з рівня IRQF IDE записувати у Flash пам'ять мікроконтролера програмний код користувача.

IDE також має ряд корисних функцій, наприклад онлайн-моніторинг передачі в радіоканалі і перегляд передачі інтерфейсу SPI, що з'єднує модуль з хостом (в даному випадку хост - це IDE). Просто відредагуйте використовуючи зовнішній редактор вихідний файл мовою C, скомпілюйте його, запрограмуйте мікроконтролер радіомодуля і налагодьте працюючу програму. І, нарешті, «програматор» модулів дозволяє з рівня IRQF IDE записувати у Flash пам'ять мікроконтролера код програми користувача.

Для програмування пам'яті мікроконтролера потрібно додатковий модуль програматора з інтерфейсом USB. У програматорі поміщається радіомодуль, наприклад згаданий TR72, і після підключення за допомогою кабелю USB можна програмувати його. Також розвідник передбачив можливість віддаленого перепрограмування модулів через радіозв'язок. Один окремий модуль може бути перепрограмований або всі підключені одночасно.

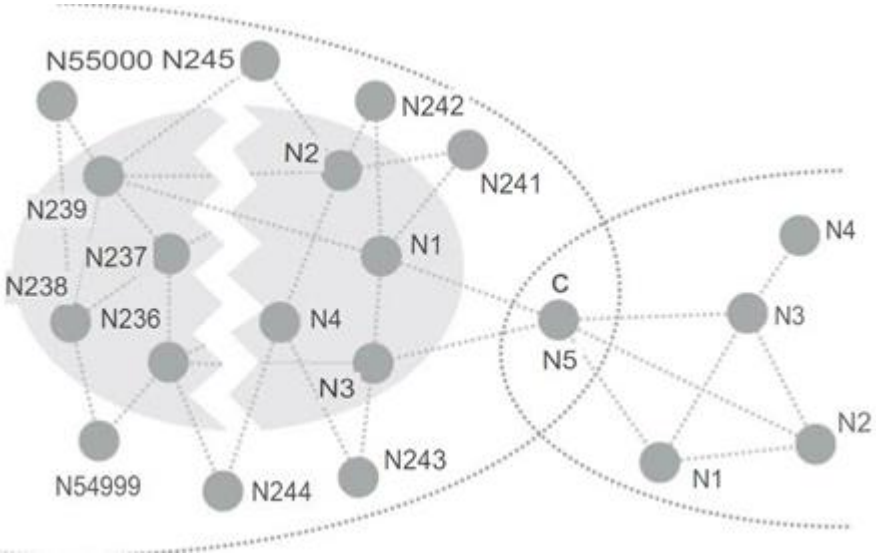

Рисунок 4.5 –Приклад конфігурації мережі IQMESH

У системі IQRF радіомодулі TR52B, що утворюють мережу, можуть працювати у двох режимах: Одноранговий, IQMESH.

Одноранговий режим – це стандартний режим. Він використовується для з'єднання двох або більше сайтів без системного координатора. Пакети даних, надіслані модулем, доступні решті модулів у мережі. Адресація та пакетний трафік не підтримуються ОС IRQF і повинні бути повністю реалізовані на рівні додатків користувача. Кількість модулів у мережі не обмежена. Можна уявити мережу зіркоподібної топології з модулями, запрограмованими до роботи в одноранговом режимі. Модуль, підключений до хоста, працює як майстер і послідовно опитує решту (підлеглий). Кожному підлеглому модулю має бути призначена унікальна адреса на постійній основі, і він повинен відповідати, коли він викликається (адресується) майстром.

Режим IQMESH дозволяє створювати пористу мережу (MESH). У принципі така мережа забезпечує зв'язок між елементами мережі без необхідності використання окремого центрального елемента. Кожен мережний пристрій (радіомодуль) може зв'язуватися з будь-яким іншим пристроєм безпосередньо (якщо є діапазон радіозв'язку) або через будь-які модулі (якщо цільовий елемент знаходиться поза межами прямої зони дії джерела) [7].

4.2 Налаштування обладнання MicrochipSAMR30

З 2018 року компанія заморозила розробку програмного забезпечення Mi-Wi для мікроконтролерів PIC та зосередилася на рішенні, розробленому придбаною компанією Atmel зі спеціальними радіо-мікроконтролерами Microchip SAMR30 та SAMR21 (2,4 ГГц).

Mi-Wi заснований на стандарті радіозв'язку IEEE802.15.4, що описує мережі WPAN, призначений для бездротових мереж із низькими швидкостями передачі даних, низьким енергоспоживанням та низькими витратами. Це дуже важливий стандарт, який лежить в основі багатьох протоколів бездротової мережі, включаючи добре відомі ZigBee або Thread.

Стек протоколу Mi-Wi використовує модифікований рівень MAC стандарту IEEE 802.15.4, який додає команди для спрощення процесу підтвердження з'єднання. Простіше реалізувати процеси підключення та відключення, а також сканування радіоканалів. Однак ряд дій, таких як, наприклад, прийняття рішень про те, коли і як сканувати канали або вводити механізми енергозбереження, не реалізовані в протоколі і повинні виконуватися на рівні додатків.

Mi-Wi може працювати в режимі P2P (одноранговий) або з окремою центральною точкою (зіркоподібна топологія). А мережні пристрої поділяються на три типи в залежності від функцій, що виконуються:

Координатор PAN (координатор персональної мережі),

FFD (повнофункціональний пристрій),

Пристрій RFD (пристрій з обмеженими функціями).

У зіркоподібній топології, показаній на малюнку, координатор PAN ініціює обмін даними та приймає вхідні з'єднання від пристроїв у мережі. Кінцеві пристрої FFD або RFD можуть встановлювати з'єднання лише з координатором PAN. У пристроях FFD трансівер завжди увімкнено, і пристрої отримують живлення від мережі.

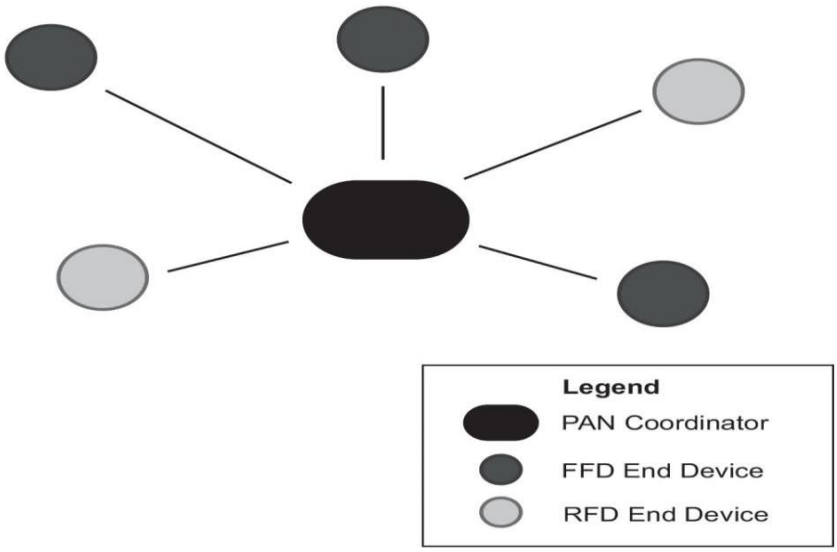

Рисунок 4.6 –Топологія мережі STAR Mi-Wi

RFD живиться від батареї, і його трансівер вимкнений в стані IDLE.

У топології P2P, на відміну зіркоподібних мереж, кінцеві пристрої FFD можуть встановлювати з'єднання як з координатором PAN, а й друг з одним. У такий спосіб можна побудувати сітку MESH. Microchip підтримує технології Mi-Wi, надаючи радіомодулі, оціночні комплекти та безкоштовне програмне забезпечення. Бібліотеки для мікроконтролерів PIC із сімейств PIC16, PIC18 та PIC24, dsPIC33 та PIC32 підтримують радіомодулі з маршрутизаторами MRF24J40 (діапазон 2,4 ГГц) та MRF89XA (діапазон 870 МГц). Стек протоколів використовує кінцевий автомат (без RTOS).

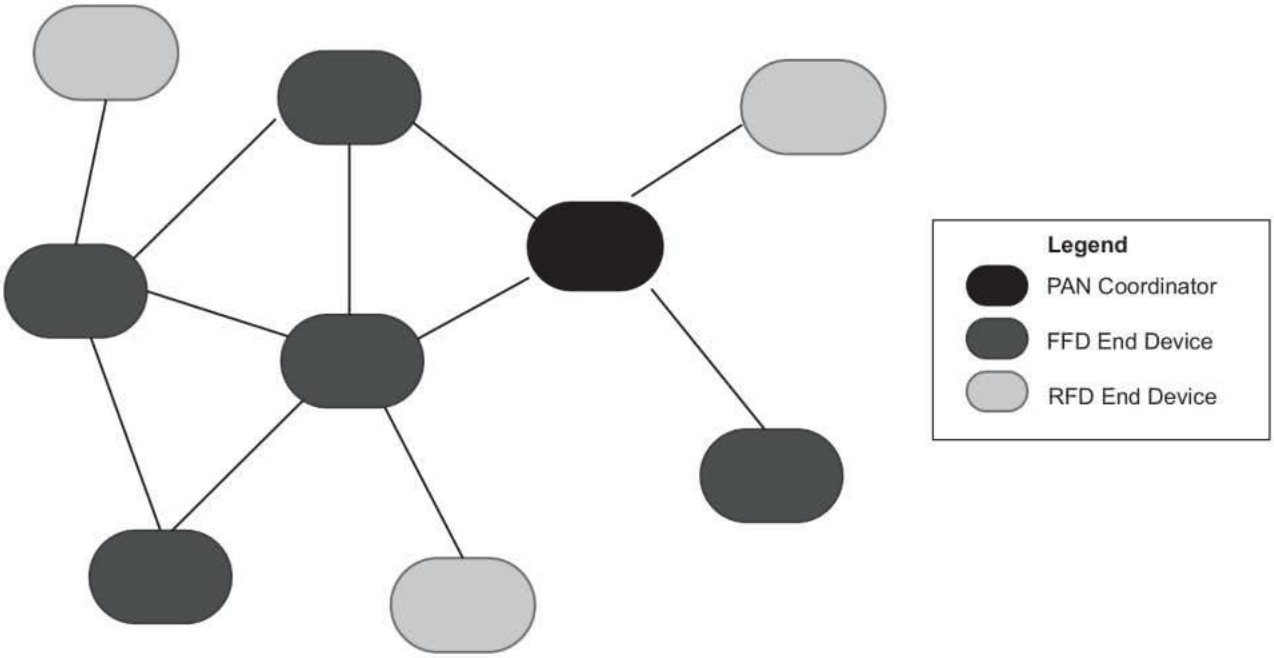

Рисунок 4.7 –Топологія мережі P2P

На додаток до радіомодулів доступні повні модулі оцінки з мікроконтролером для введення в експлуатацію власних демонстраційних прикладів. Один із них – набір DM182018, що складається із трьох плат. Одна з них призначена для роботи як координатор PAN, а дві інші – як кінцеві пристрої. Такий комплект дозволяє повністю протестувати роботу мережі Mi-Wi.

Microchip відмовилася від розвитку мережі Mi-Wi на основі виділених модулів та прошивок, що зберігаються в пам'яті мікроконтролера сімейств PIC micro. Після придбання Atmel нові втілення стеку Mi-Wi працюють із мікроконтролерами сімейств ATSAMR21 та ATSAMR30.

ATSAMR21 – це сімейство мікроконтролерів з ядром Cortex M0+, в якому однією з периферійних систем є радіоприймач для діапазону 2,4 ГГц. Схема має вбудований апаратний прискорювач MAC-рівня IEEE 802.15.4, який значно полегшує реалізацію стека. Достатньо прикріпити антенну схему, щоб побудувати радіомодуль з більшими можливостями програмування.

Стек Mi-Wi - лише одна з можливостей використання цих мікроконтролерів. Іншим варіантом може бути, наприклад, стек ZigBee. На фото показаний модуль ATSAMR21 X Plained PRO із мікроконтролером ATSAMR21G18A, призначений, у тому числі, для тестування роботи в мережі Mi-Wi. Стек MiWI для мікроконтролерів SAMR21 доступний серед IDE Atmel Studio або IAR Workbench.

4.3 Протокол LORAWAN

Більшість радіоліній у діапазонах, призначених для використання без окремої роздільної здатності, мають невелику пряму дальність дії максимум 100 метрів на відкритій місцевості. Це з великим обмеженням потужності передавачів і використовуваної модуляції. Діапазон може бути збільшений за рахунок використання пористих мереж та повторної передачі пакетів даних пристроями, що працюють у мережі. Але є пристрої, які потребують набагато більшого прямого діапазону без можливості повторної передачі даних. Наприклад, датчики Інтернету речей (IoT) розгорнуті в малонаселених районах, де немає розвиненої інфраструктури і з цією метою не можна використовувати радіолінії ближньої дії.

Для мереж пристроїв IoT, що динамічно розвиваються, розподілених на великій території, робляться спроби розробити і реалізувати різні рішення для радіозв'язку. Найбільш перспективними є виділені радіомережі на базі інфраструктури стільникових мереж GSM. Передбачається, що це будуть комерційні рішення, які пропонують платну передачу даних, але з обмеженими витратами через масове використання. І альтернативним рішенням можуть стати мережі LoRaWAN.

LoRaWAN – це протокол радіозв'язку, який дозволяє пристроям IoT з радіоканалом підключатися до Інтернету. Підключення здійснюється не

безпосередньо, а за допомогою спеціальних базових станцій, які називаються концентраторами. Дуже важливою особливістю стандарту є можливість отримання відносно великих діапазонів із дуже низькою потужністю передачі (20 дБ-мВт) між кінцевими пристроями та базовими станціями, рахуючи за кілометри. Мала потужність передавачів забезпечує низьке споживання енергії та можливість роботи від батарей.

Технологія LoRaWan заснована на відкритому стандарті та використовує одну із частот відкритого діапазону ISM – 868 МГц. Це має далекосяжні наслідки, оскільки дозволяє створювати власні недорогі мережі без необхідності отримання адміністративних дозволів та плати за використання смуги пропускання. Оператори зв'язку також зацікавлені у цій технології. На жаль, у нашій країні поки покриття мережами LoRaWAN дуже маленьке, переважно у великих містах.

Для передачі радіоканалом використовується система зв'язку LoRa. Передача даних щодо відносно великі відстані можлива завдяки модуляції CSS (Chirp Spread Spectrum). Цікаво, що це метод, розроблений у 1930-х роках для потреб створених на той час радарів. Він також використовувався для зв'язку у космосі. CSS стійкий до перешкод від відображень (перешкоди сигналу), стійкий до ефекту Доплера, вимагає синхронізації приймача і передавача і, що важливо, амплітуда сигналу мало впливає частоту помилок під час передачі (амплітуда впливає лише діапазон сигналу). З іншого боку, модуляція CSS через свої властивості не дозволяє передавати дані на високих швидкостях.

LoRaWAN – це протокол доступу до каналу зв'язку з протоколом доступу до середовища передачі (MAC). Як ми знаємо, при його розробці наголос робився на роботу з лініями дальньої дії, але з низькою пропускною здатністю, і в основному він призначений для пристроїв IoT, що працюють з низьким оптимізованим енергоспоживанням. Двонаправлена передача даних забезпечує надійну передачу інформації за рахунок можливості реалізації механізму

підтвердження та надсилання команд управління. Безпека передачі забезпечується надійним шифруванням. Важливою функціональною особливістю є можливість бездротової реєстрації нових пристроїв у мережі та передачі даних у режимі багатоадресної розсилки (від одного до багатьох).

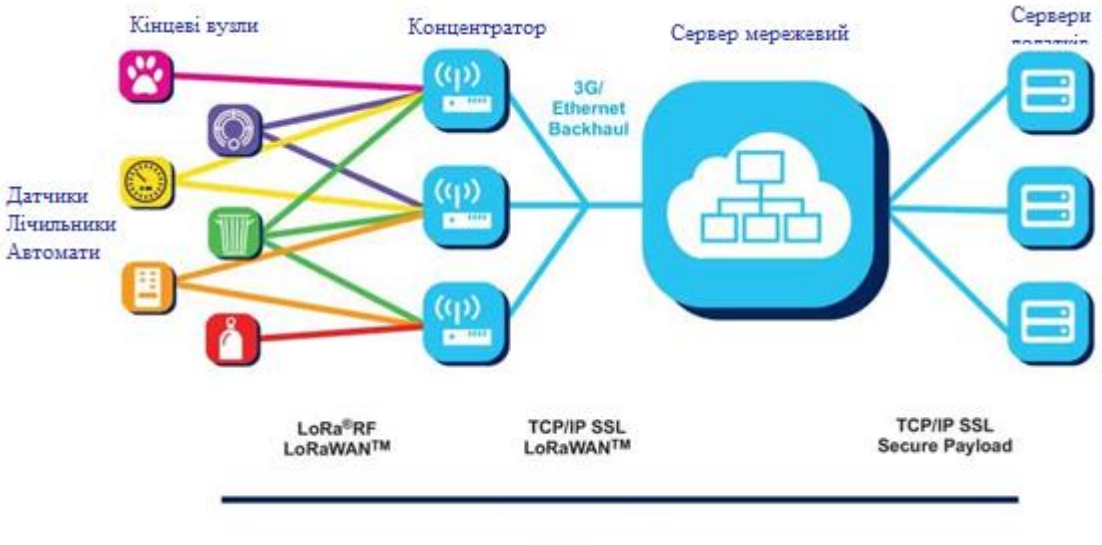

Рисунок 4.8 –Структура мережі LoRaWAN

Вузли (кінцеві пристрої – датчики) підключаються до концентраторів за протоколом LoRaWAN RF. Концентратори надсилають дані на мережеві сервери через стандартне з'єднання з використанням протоколів LoRaWAN TCP/IP SSL (Wi-Fi, Ethernet) або через службу доступу в мережах GSM (3G/LTE). Мережа складається з чотирьох основних компонентів:

кінцеві пристрої (вузли),

концентратори (базові станції, маршрутизатори, шлюзи),

мережевий сервер,

сервери пристроїв.

Термінальні пристрої – це обладнання, яке включає датчики, системи управління, мікроконтролер і модуль радіопередачі. Вони підтримують двонаправлену передачу з концентраторами – вони можуть надсилати дані самі,

але можуть отримувати дані від концентраторів. У принципі, пристрої IoT, які є датчиками та працюють як вузли LoRaWAN, повинні мати можливість працювати від батареї протягом тривалого часу [11].

За типом передачі та споживаної енергії пристрої поділяються на класи: A, B та C. Клас A – споживає найменшу кількість енергії. Пристрої цього класу надсилають коротку інформацію про події, тобто тільки при виникненні події, наприклад, про перевищення значення параметра, що вимірюється. Пристрої класу B можуть передавати довшу інформацію та отримувати довшу інформацію з меншою затримкою відповіді сервера через випадкову відправку даних висхідної лінії зв'язку пристроєм класу A. Пристрій класу C може безперервно отримувати дані, крім тих випадків, коли воно надсилає дані. Цей клас не призначений для роботи від батарей та потребує постійного джерела живлення.

Вузли (кінцеві пристрої) мережі LoRaWAN повинні відрізнятися дуже низьким енергоспоживанням. У пристроях класу A і B режим глибокого сну використовується під час бездіяльності, що дозволяє значно знизити споживання енергії. Але також необхідний певний ступінь ефективності вбудованого мікроконтролера, що дозволяє обробляти стек, кодувати передачу даних і, звичайно, керувати вимірювальним датчиком. Тому багато виробників використовують 32-бітові мікроконтролери з вбудованими розширеними режимами енергозбереження.

ВИСНОВКИ

В кваліфікаційній роботі бакалавра виконане поставлене завдання розробки сучасної корпоративної мережі для товариства з обмеженою відповідальністю «Сінгл-Ойл».

Розроблений проект враховує особливості підприємства, його структуру та інформаційну політику.

Проведений аналіз показав необхідність модернізації компютерної мережі підприємства.

Основою модернізованої компютерної системи повинна стати сучасна корпоративна компютерна мережа.

Обгрунтовано обрані технічні засоби для оснащення компютерної мережі.

Виконано розробку технічних вимог до розробленої мережі, що враховують все більш зростаючі вимоги до використання сучасних інформаційних технологій.

Розроблений проект компютерної мережі та перевірений методами імітаційного моделювання в пакеті Cisco Packet Tracer.

Також передбачена можливість майбутнього розширення та модернізації мережі у разі виникнення такої потреби.

Виконаний аналіз сучасних бездротових технологій для їх використання в елементах компютерної системи для забезпечення роботи IoT технологій.

ПЕРЕЛІК ПОСИЛАНЬ

1. Шведюк О. Визначення мережевої структури як сучасної форми координації економічної діяльності // актуальні проблеми економіки. – 2010. - №5 (107). – с.22-29.

2. Мазіна Н.Є. Мережеві відносини у господарчій діяльності підприємств: інституціональний аспект // Методологія, теорія та практика соціологічного аналізу суспільства. – 2009. – №15 – с.250-253.

3. Вікторов Б. В. Типи мережевих підприємств у міжнародному бізнесі. Вчені записки Університету «КРОК» 2020. № 2(58). URL: https://snku.krok.edu.ua/index.php/vcheni-zapiski-universitetu-krok/article/view/291/313.

4. Журавська І. М. Проектування та монтаж локальних комп’ютерних мереж :[навчальний посібник] / І. М. Журавська. – Миколаїв : Видавництво ЧДУ ім. Петра Могили, 2016. – 396 с.

5. Жуков, І. А. Комп’ютерні мережі та технології : навч. посіб./І. А. Жуков, В. О. Гуменюк, І. Є. Альтман. – К. : НАУ, 2004. – 276 с.

6. Аналогові і цифрові системи відеонагляду(Електрон. ресурс) / Спосіб доступу: URL:http://elites-montage.com.ua/svanalog.php. - Загол. з екрана.

7. ДСТУ4030-2001. Позначення умовні графічні та літерні. Системи охоронного призначення – Київ Держстандарт України,2001. – 115 с.

8. ДСТУ 3396.1-96 Державний стандарт України «Захист інформації. Технічний захист інформації. Порядок проведення робіт»

9. Глухов В.С., Костик А.Т. Дослідження та проектування комп’ютерних систем та мереж. – К.: Магнолія., 2023. – 253 с.

10. Б.І. Масловський, В.І. Дрововозов, О.В. Коба Технології проектування комп'ютерних систем. – К: НАУ, 2015. – 500 с.

11. Парамуд Я.С. Периферійні пристрої, інтерфейси та драйвери. – К.: Магнолія, 2023. – 210 с.

12. Білова М.О., Євсеєв С.П., Жученко О.С. Технологія Ethernet. Лабораторний практикум. – К.: Новий світ-2000, 2024. – 196 с.

13. Микитишин А.Г. та інші. Комп'ютерні мережі. Книга 2. – К.: Магнолія, 2013. – 328 с.

14. Цвіркун Л.І. Розробка програмного забезпечення комп’ютерних систем. Програмування: навч. посіб. [Електронний ресурс] / Л.І. Цвіркун, А.А. Євстігнєєва, Я.В. Панферова ; під заг. ред. проф. Л.І. Цвіркуна ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – 1 електрон. опт. диск (CD-ROM) ; 12 см. – Систем. вимоги (мінімальні): Процесор 32-розрядний (x86) 233 МГц ; 512 МБ RAM ; 128 МБ Video ; від 4-х до 48-х CD-ROM ; Windows 7. – Назва з контейнера. – Дніпро: НТУ «ДП», 2019.

ДОДАТОК А

Текст програми налаштування мережі комп’ютерної системи

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

ПРОГРАМНЕЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.24001-01 12 01

Листів 10

Дніпро

2024

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду програмування та налаштування компонентів мережі комп’ютерної системи.

Програма призначена для забезпечення налаштування, протоколу маршрутизації комп’ютерної системи.

ЗМІСТ

1. Скрипт налаштування ISP

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX1524210H-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.0.2.26 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.2.22 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 209.165.200.1 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
no cdp run
line con 0
line aux 0
line vty 0 4
 login
end
```

2. Скрипт налаштування Atanasov Router0

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
```

```
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX1524Y68M-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.25.9.129 255.255.255.128
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.1.30 255.255.255.128
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
no cdp run
line con 0
line aux 0
line vty 0 4
 login
end
```

3. Скрипт налаштування Atanasov Router1

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX152472XM-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.25.9.1 255.255.255.128
```

```
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.1.5 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.1.9 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
no cdp run
line con 0
line aux 0
line vty 0 4
 login
end
```

4. Скрипт налаштування Atanasov Router2

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX152466VG-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.25.10.129 255.255.255.240
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.25.10.1 255.255.255.128
 duplex auto
 speed auto
interface GigabitEthernet0/2
```

```
 ip address 10.0.1.1 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
no cdp run
line con 0
line aux 0
line vty 0 4
 login
end
```

5. Скрипт налаштування Atanasov Router3

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX1524887I-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.0.1.2 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.1.6 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.1.13 255.255.255.252
```

```
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
no cdp run
line con 0
line aux 0
line vty 0 4
 login
end
```

6. Скрипт налаштуванняAtanasov Router4

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX1524OCIW-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.25.8.1 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.1.21 255.255.255.252
 duplex auto
```

```
 speed auto
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
no cdp run
line con 0
line aux 0
line vty 0 4
 login
end
```

7. Скрипт налаштуванняAtanasov Router5

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX1524VQ3R-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.0.1.14 255.255.255.252
 duplex auto
```

```
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.1.10 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.1.17 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
no cdp run
line con 0
line aux 0
line vty 0 4
 login
end
```

8. Скрипт налаштуванняAtanasov Router5_1

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
```

```
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX15242144-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.0.1.18 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.1.22 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.1.25 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
no cdp run
line con 0
line aux 0
line vty 0 4
 login
end
```