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

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Кулініча Андрія Андрійовича
(ПІБ)
академічної групи 123-20ск-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)
на тему «Комп'ютерна система ТОВ «ЕР ДЖІ БІ» з детальною реалізацією побудови та налаштування корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Ткаченко С.М.			
розділів:				
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро

2023

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)
« 16 » 05 2023 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Кулініча А. А. **академічної групи** 123-20ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

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

на тему «Комп'ютерна система ТОВ «ЕР ДЖІ БІ» з детальною реалізацією побудови та налаштування корпоративної мережі»
затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 № 350-с

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	20.05.2023
Розробка апаратної частини	На основі аналізу підприємства сформулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	30.05.2023
Розробка корпоративної мереж	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	10.06.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	30.06.2023

Завдання видано _____ доц. Ткаченко С.М.
(підпис керівника) (прізвище, ініціали)

Дата видачі 19.04.2023

Дата подання до екзаменаційної комісії 13.07.2023

Прийнято до виконання _____ Кулініч А.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 80 с., 47 рис., 8 табл., 1 дод., 7 джерел.

СИСТЕМА, МЕРЕЖА, ЛОКАЛЬНА МЕРЕЖА, МЕРЕЖЕВІ ЗАСОБИ

Об’єкт розробки: комп’ютерна система ТОВ «ЕР ДЖІ БІ» з детальною реалізацією побудови та налаштування корпоративної мережі.

Мета: створення комп’ютерної система ТОВ «ЕР ДЖІ БІ» з детальною реалізацією побудови та налаштування корпоративної мережі.

Для досягнення цієї мети використано програму Cisco Packet Tracer, що надає можливість моделювати мережеві сценарії та конфігурувати пристрої.

Розглянуті стан питання, наведена характеристика консалтингових послуги в Україні, послуги ТОВ «ЕР ДЖІ БІ».

Розроблена комп’ютерна система ТОВ «ЕР ДЖІ БІ» з детальною реалізацією побудови та налаштування корпоративної мережі.

При розробці системи вибрані апаратні засоби. Система забезпечує виконання функцій з об’єднання підрозділів у мережу, збір обробку та комунікацію між кінцевими споживачами у різних підрозділах та доступ до загальних ресурсів.

В рамках кваліфікаційної роботи в 4-му розділі було розроблено систему, яка забезпечує збір, аналіз та візуалізацію потоків даних з різних пристроїв у мережі.

У процесі розробки системи було проведено дослідження протоколу NetFlow, його особливостей та можливостей. Було проведено експерименти з різними сценаріями трафіку для перевірки працездатності системи моніторингу та оцінки її ефективності.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМОВЛІВ ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

КС – комп’ютерна система;

ПК – персональний комп’ютер;

ТП – Технологічний процес;

ЛОМ – Локальна обчислювальна мережа;

СКС – Структурована кабельна систем;

Ethernet – Технологія передачі даних по мережі;

PT – Packet Tracer

LAN – Local area network;

WAN – Wide Area Network;

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

ВСТУП

Сьогодні, при всіх процесах глобалізації, консалтинг став дуже популярним, особливо серед країн з високими витратами, а також великих і швидкозростаючих компаній, оскільки дає можливість поліпшити економічно і ефективно не принципові для них бізнес-процеси. Консалтинг в Україні – це вид міжнародної діяльності у сфері послуг, який здійснює спеціалізована компанія ТОВ «ЕР ДЖІ БІ», яка задовольняє цей глобальний попит на аутсорсингові послуги. Основними замовниками є міжнародні малі та середні компанії, їх філії або представництва в Україні, приватні підприємці, а також громадяни іноземних держав. Своєчасна і точна інформація, добре висвітлені професійні консультації управлінської команди, можуть не тільки привести до більш ефективного поліпшення і управління, але і можуть істотно знизити ризики, пов'язані з підприємництвом, оподаткуванням і дотриманням правових норм на основі попереднього досвіду роботи з європейськими та американськими партнерами.

Консалтинг в м. Києві – це ключовий напрямок роботи ТОВ «ЕР ДЖІ БІ», де західний менеджмент пропонує знання і досвід роботи на вітчизняному ринку за конкурентною ціною.

ТОВ «ЕР ДЖІ БІ» багато інвестує в своїх співробітників, надається доступ як до своїх тренінгів, так і до тренінгів від зовнішніх провайдерів, платних семінарів, вебінарів, а також компенсації витрат на різні міжнародні сертифікати, такі як ACCA, CAP, SIPA та інші. Є складна система внутрішнього контролю, що допомагає знизити ризик людського фактору. У своїй діяльності компанія ТОВ «ЕР ДЖІ БІ» керується тільки новітніми методами, технологіями, стандартами і регламентами, ми використовуємо тільки офіційну і сучасну новітню ERP-систему. Вартість послуг залежить від багатьох факторів, таких як розмір клієнта, кількість співробітників, характер і складність роботи, обрана податкова модель [3].

Успішна діяльність сучасної консалтингової компанії спирається на надійну комп'ютерну мережу, побудовану, як правило на сертифікованому обладнанні Cisco, Juniper, HPE, Fortinet та іншими провідними IT-компаніями. Тому IT-фахівці проектують мережі LAN/WAN для різних підприємств і державних установ на професійному рівні. Основною метою кваліфікаційної роботи бакалавра є синтез комп'ютерної системи для ТОВ «ЕР ДЖІ БІ» з детальною реалізацією побудови та налаштування корпоративної мережі, що направлено в першу чергу для забезпечення надійності, довговічності та безпеки застосовуваних систем, а також створення IT-мережевої інфраструктури.

У кваліфікаційні роботі при синтезі комп'ютерної мережі буде використовуватись сертифіковане обладнання Cisco, яке здатне охопити всі сегменти мережі з точки зору безпеки, оптимізації та управління. А програмне забезпечення мережевої безпеки наступного покоління, пристрої та веб-додатки, інструменти DDoS збалансувати навантаження на обладнання мережі, проксі-пристрої. Широкий спектр рішень сертифікованого обладнання Cisco у цій галузі роблять мережу клієнта більш надійною та безпечною. Спроектовані рішення для управління IT-інфраструктурою легко інтегруються в мережу, можна швидко виявити інструменти, які використовуються в мережі, а також постійно контролювати, перенаправляти та керувати інтегрованою інфраструктурою та життєвим циклом використаних програм.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика і структура об’єкта впровадження

1.1.1 Консалтингові послуги

Консалтингові організації надають різноманітні консалтингові послуги своїм клієнтам. У більшості випадків вони представляють іноземну компанію і безпосередньо пов'язані з фірмами своїх клієнтів. Консалтинг – це надання необхідних консультацій продавцям, виробникам, а також покупцям. Вони можуть отримати допомогу в технічній, технологічній та експертній сферах своєї діяльності. Основним завданням такої фірми є надання допомоги в сфері управління, пов'язаної з поставленими перед клієнтами питаннями.

Рисунок 1.1 – Ілюстрація роботи консалтингові організації

Немає однозначної відповіді на питання, що таке консалтингова компанія. Він може вирішувати складні завдання, визначати цілі фінансового становища підприємства і брати безпосередню участь в організації виробничої діяльності, а також у вирішенні стратегічних питань. Фахівці, які займаються

консультуванням клієнтів з необхідних питань. Однак вони не можуть нести повну відповідальність за кінцевий результат діяльності. Консалтингові компанії надають конкретні та точні поради, які допоможуть застосувати під час подальшої реалізації послуг чи товарів. Проте фахівці-консультанти не можуть реалізувати всі запропоновані плани та завдання.

Консалтингові послуги мають кілька аспектів:

1) Аналітика – фахівці можуть провести консультації для своїх клієнтів, під час яких вирішуються питання ефективності на майбутнє, розробити план може будь-яка консалтингова компанія. Що це за напрямки сучасного вигляду ? Відповісти можуть лише кваліфіковані працівники, які розробляють схему впровадження ефективних процесів у виробництві, аналізують рух цін, а також комплексно аналізують усі етапи діяльності на підприємстві.

2) Прогнозування – цей вид консалтингу передбачає попереднє визначення прогнозів на кілька місяців наперед. Для цього враховується аналіз діяльності компанії клієнта. Усі поради стосуються будь-якої сфери діяльності клієнта.

3) Проведення аудиту – всім цікаво, які консалтингові компанії існують на сучасному ринку. Професійні експерти не тільки консультують, а й проводять планові аудити. Вони визначають його послідовні етапи, підбирають персонал і проводять необхідне навчання. Деякі клієнти покладаються на фахівців для планування майбутніх організаційних та управлінських заходів, а також впровадження сучасних інформаційних систем.

Можна спостерігати швидкі темпи розвитку сучасної бізнес- ринкової технології. Звичайно, всі організації хочуть бути конкурентоспроможними та успішними у наданні консалтингових послуг. Підприємці ставлять за мету досягти успіху та постійно розвивати свій бізнес чи виробництво. Тому вони вирішують звернутися до послуг консалтингової компанії. Послуги цієї компанії коштують чималих грошей, тому варто вибирати тільки перевірених фахівців. Справжні консультанти повинні не тільки організувати всі необхідні

дії, а й привести підприємця до потрібного йому результату. Цей процес дій обов'язково повинен супроводжуватися практичними порадами і допомогою.

Щоб правильно вибрати для себе консалтингову компанію, слід звернути особливу увагу на такі особливості:

1) вартість наданих послуг;

2) професійна кваліфікація та досвід роботи;

3) термін дії консалтингової компанії;

4) відгуки про роботу попередніх клієнтів;

Існують певні принципи, яких дотримуються консалтингові компанії:

1) Наукова обґрунтованість. Фахівці не можуть приступити до виконання завдання, використовуючи лише накопичений досвід консалтингової фірми. Консультанти повинні застосовувати дані.

2) Наявність додаткових інструментів, які повинні бути у будь-якої професійної консалтингової компанії. Це може включати інформаційні технології для відстеження та визначення місцезнаходження організації клієнта та ефективної системної допомоги.

3) Динамічність не тільки підтримується під час консультації з клієнтом, але й використовується в роботі організації після завершення роботи.

4) Наукові перспективи. Експерти можуть запропонувати свої наукові ідеї, щоб допомогти клієнтам визначити найкращі напрямки розвитку бізнесу клієнта в майбутньому.

Сьогодні можна зустріти фахівців, які розуміються на багатьох питаннях організаційної діяльності на сучасному ринку. Такі підприємства можуть мати вузьку або широку спеціалізацію. Консалтингові компанії в Україні надають ряд послуг або проводять аудит підприємства. Залежно від методів діяльності можна виділити наступні напрямки консалтингу:

1) експертний;

2) освітній;

3) управлінський.

Фахівці не тільки ретельно відстежують можливі шляхи підвищення ефективності всередині підприємства, а й приділяють увагу налагодженню відносин з міжнародними партнерами. Консультанти вирішують різноманітні питання та виконують завдання будь-якої складності. Сьогодні ви можете знайти експертів для вирішення комерційних, фінансових, юридичних, технологічних та екологічних питань.

Рисунок 1.2 – Напрямки надання консультативних послуг

Компанії, що працюють на українському консалтинговому ринку, можуть надавати свої послуги наступним структурам:

1) Українські підприємства державного та приватного секторів. Вони можуть займатися виробничою діяльністю та надавати різноманітні послуги.

2) Іноземні компанії, що працюють на ринку України. Діяльність консалтингових компаній створює можливості для надання послуг підприємствам із західними інвесторами або тим, що тільки вийшли на український ринок. Фахівці консалтингу займаються реалізацією сучасних проектів і демонструють масштабні проекти.

3) Державні організації. Це мерія, міністерство, різні відомчі структури, державні комітети та адміністративні органи.

Сьогодні до послуг таких фахівців звертаються люди, які займаються приватним бізнесом. Консалтингова компанія допомагає підприємствам, які хочуть мати статус надійної фірми. Менеджери отримують оптимальну схему перебудови всієї системи діяльності та виробничого процесу. Консультанти можуть запропонувати оптимальні зміни в поточній діяльності підприємства, а також нові прибуткові сфери для ведення бізнесу.

Якщо підприємство знаходиться на межі банкрутства або веде збиткову виробничу діяльність, то консалтингові компанії допоможуть вибратися зі складної ситуації. Клієнтам пропонуються послуги кризового консалтингу, де фахівці шляхом аналізу знаходять необхідні внутрішні ресурси для вирішення поставленого завдання.

Будь-який консультант або велика консалтингова компанія повинна відповідати ряду основних вимог. Вони можуть включати такі елементи:

Фахівці повинні мати перевірені технології, які допомагають вирішувати навіть складні завдання. Консалтингова компанія володіє навичками в області формування організації.

1.1.2 Консалтингова компанія ТОВ "ЕР ДЖІ БІ"

Українська компанія "Товариство з обмеженою відповідальністю "ЕР ДЖІ БІ", скорочена назва ТОВ "ЕР ДЖІ БІ", зареєстрована 01.06.2021, адреса центрального офісу: вул. Волинська, 40, м. Київ, 03151.

Види діяльності – бізнес, управлінський консалтинг. У цю категорію входять консалтингові послуги, адміністративна та організаційна підтримка компаній та інших організацій з питань управління, стратегічного та операційного планування компаній, розвитку бізнесу, управління змінами, зниження витрат та інших фінансових питань, маркетингових цілей і політики, кадрової політики, компенсаційних і пенсійних стратегій, планування і контролю виробництва.

Надання комерційних послуг може включати надання консультаційної, управлінської та організаційної підтримки компаніям і державним установам щодо:

1) розробки методології та правил бухгалтерського обліку, програм звітності та процедур контролю за виконанням кошторисів;

2) процедури контролю за виконанням кошторисів; надання консультацій та підтримки компаніям та державним установам у сфері планування, регуляторних заходів, забезпечення ефективності, контролю, інформування з питань управління тощо.

До цієї категорії також належать:

1) діяльність арбітражних керуючих установ (керуючих майном, керуючих санацією, ліквідаторів);

2) діяльність арбітраже-спроможних установ (керуючих майном, керуючих санацією, ліквідаторів);

3) діяльність арбітраже-одержувачів (розпорядників майна; до цієї категорії не належать: розробка програмних додатків та програмного забезпечення для ведення бухгалтерського обліку;

4) юридичні послуги та представництво;

5) діяльність у сфері бухгалтерського обліку, банківської справи та аудиту, консультування з питань податків; консалтинг в архітектурі та інжинірингу;

6) консультування з питань екології, сільськогосподарської техніки, безпеки тощо;

7) консультування з питань заповнення вакансій та пошук персоналу;

8) наставництво в освіті [1].

Цінності та принципи ТОВ "ЕР ДЖІ БІ":

1) щирість – важлива чесна і прозора співпраця, орієнтована на рішення, а не проблеми і працює на благо клієнта;

2) замовник – це не нагорода, а партнери;

3) перевершення очікувань – швидкість є запорукою успіху, але без безглуздої якості кожен піксель повинен бути ідеальним і перевершувати очікування;

4) відповідальність за результат – довгострокові партнерські відносини з клієнтами мають бути націлені на результат і досягнення бізнес-цілей клієнта;

5) орієнтування на користувача, а все інше додається – прагнення створювати веб-продукти, які надихають, дивують і вирішують проблеми користувачів [2].

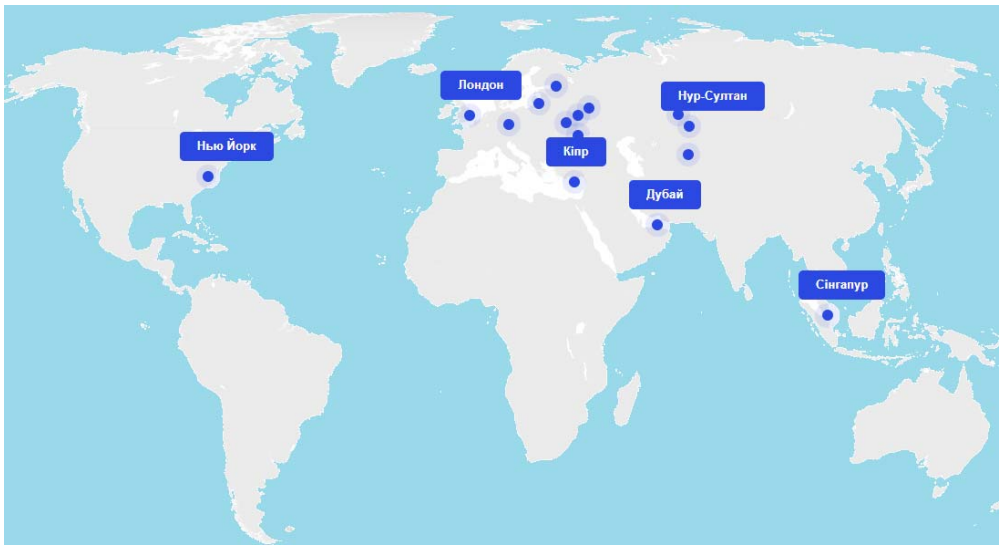

Рисунок 1.3 – Географія співпраці з ТОВ "ЕР ДЖІ БІ":

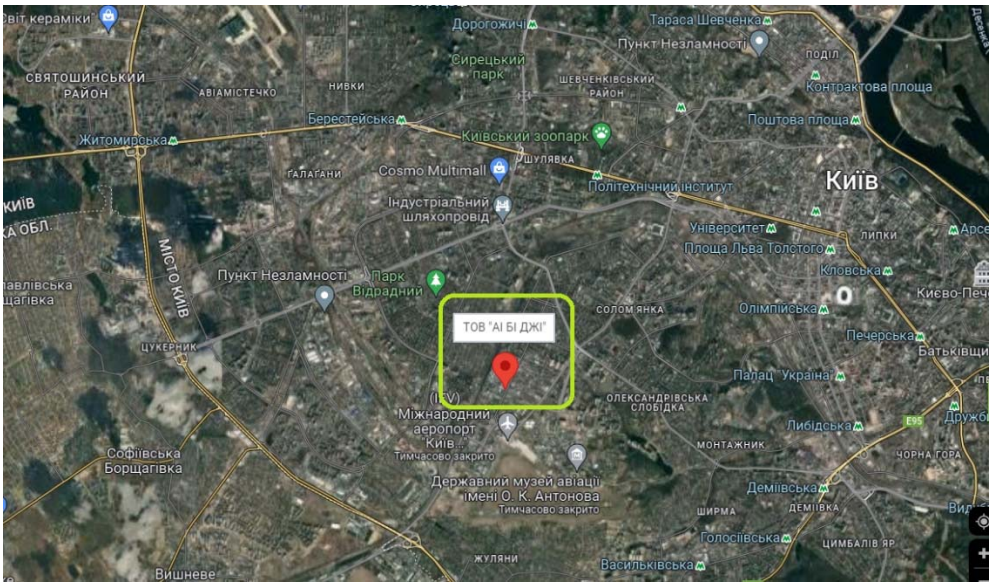

Рисунок 1.4 – Геолокація центрального офісу ТОВ "ЕР ДЖІ БІ"

1.2 Організаційно-управлінська структура об’єкта впровадження

Консалтингова компанія ТОВ "ЕР ДЖІ БІ" гарантує повну конфіденційність і гідність в процесі надання послуг своїм клієнтам. Фахівці надають висококваліфіковану допомогу у всіх необхідних нюансах, що стосуються житлових, цивільних, сімейних, земельних та адміністративних питань, розробки та впровадження спеціалізованого програмного забезпечення. Консультанти захищають законні інтереси громадян, а також організацій, що працюють на українському ринку.

Організаційна структура повинна чітко відповідати стратегії розвитку організації. Розробка нової стратегії може зажадати змін в існуючій організаційній структурі, які відповідають новим видам діяльності, новим зовнішнім зв'язкам, новим напрямкам розвитку організації і т. д.

Слід зазначити, що жодна існуюча організаційна структура не є досконалою. Таким чином повинна відбуватися постійна адаптація структури до зовнішніх і внутрішніх факторів і стратегій, що реалізуються. Оптимальна організаційна структура - це та організаційна структура, яка забезпечує ефективність роботи організації найбільш економічним способом. При розробці структури управління важливо досліджувати специфіку існуючих організаційних відносин, так як саме існуючі зв'язки повинні стати основою для створення раціональної організаційної структури управління.

Для забезпечення ефективної роботи компанії необхідно, щоб її структура була більш адаптована до зовнішнього середовища, забезпечуючи незалежну присутність і можливість подальшого розвитку. Організаційна структура повинна бути оптимальною. Існують критерії, що визначають оптимальні організаційні структури. Ці стандарти включають:

1) найкоротший маршрут від системи управління до керованої системи;

2) оптимальна кількість рівнів управління і ланок;

3) найменша кількість «входів» і «виходів» на одну ланку;

4) чітка конфігурація видів робіт з управління кожною ланкою; відсутність дублювання робіт.

Питаннями вдосконалення організаційних структур займаються фахівці з організації праці, менеджменту та психології. Структура функціонального типу рекомендується в тому випадку, якщо компанія відмінно справляється з однорідною роботою і має високий ступінь надмірності. У цих умовах інтеграція може бути забезпечена за допомогою узгодження планів, а конфліктів можна уникнути завдяки системі ієрархічних залежностей. У тому випадку, якщо робота пов'язана з вирішенням нових завдань, більш доцільна організація товарів або товарних груп. Тому в кожній з різних завдань необхідно ретельно аналізувати поставлені завдання і вибирати відповідну організаційну структуру. Послідовність вибору оптимальної організаційної структури компанії показана на рис. 1.5.

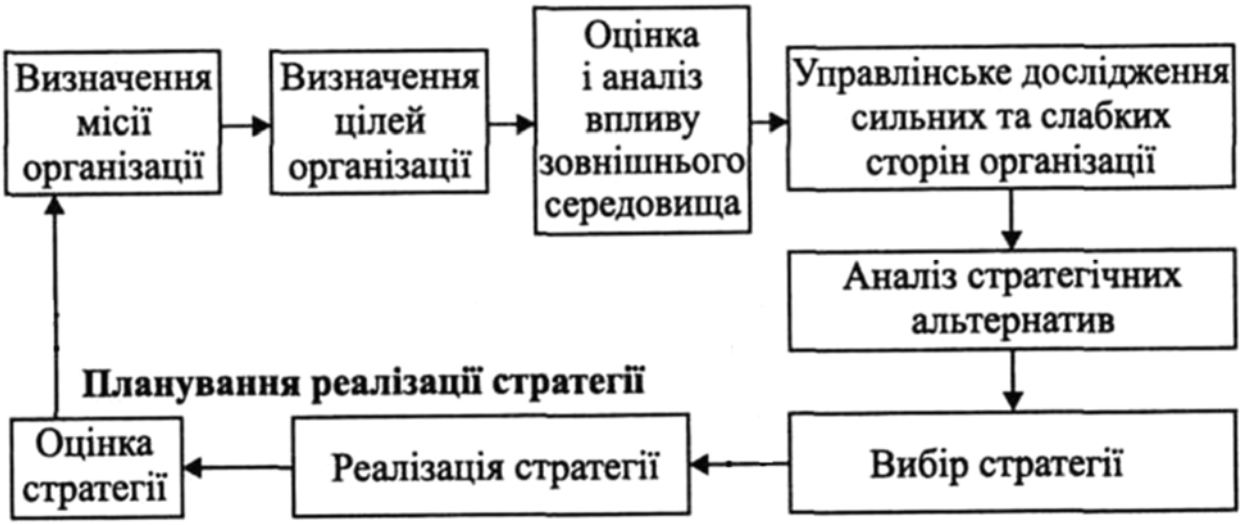

Рисунок 1.5 – Послідовність вибору оптимальної організаційної структури корпорації

1.3 Стислі відомості про технології збору та передачі інформації ТОВ "ЕР ДЖІ БІ"

1.3.1 Інформаційний центр

Діяльність сучасних центрів обробки інформації (ЦОД) базується на хмарних обчисленнях, Інтернеті речей, великих даних тощо. може змінюватися в залежності від таких факторів і понять. Для того, щоб дата-центри були ефективними, надійними та гнучкими у використанні, їх

інфраструктура повинна працювати стабільно за будь-яких умов. Для цього дата-центр повинен відповідати наступним основним вимогам:

1) паралельна робота інженерних підсистем;

2) резервна система охолодження;

3) резервна система енергопостачання;

4) резервна телекомунікаційна інфраструктура.

BestComp Group — професіонал у будівництві центрів обробки даних, що відповідають сучасним стандартам. У компанії є експерти, сертифіковані в цій галузі Uptime Institute, Schneider Electric, HPE, Cisco, Juniper. Компанія брала активну участь у будівництві кількох ЦОД в Азербайджані, була головним виконавцем і підрядником.

ТОВ "ЕР ДЖІ БІ" є надійним партнером у сфері дата-центрів, який надає наступні послуги на найвищому рівні:

1) оцінка центру обробки даних;

2) встановлення ЦОД;

3) дизайн (включаючи планування та компонування);

4) вентиляція та охолодження приміщення;

5) електропостачання та безперебійне живлення;

6) повна здача проекту;

7) профілактичні заходи;

8) служба екстреної підтримки;

9) здійснення процесу витіснення.

1.3.2 Системна інтеграція

Системна інтеграція – це комплексне рішення, важливе для автоматизації бізнес-процесів підприємства, а також для інтеграції існуючих і нових інформаційних систем в єдиний інформаційний простір.

Системна інтеграція – одна з основних послуг, які надає ТОВ "ЕР ДЖІ БІ". Наша компанія, яка має багаторічний досвід у цій сфері, реалізувала сотні інтеграційних проектів у державному та приватному секторах.

Уміння створювати оптимальні рішення, що відповідають потребам і запитам клієнтів, є однією з головних переваг ТОВ "ЕР ДЖІ БІ".

Діяльність ТОВ "ЕР ДЖІ БІ" у сфері системної інтеграції зосереджена в різних сферах економіки:

1) фінансові установи та банки;

2) телекомунікації;

3) охорона здоров'я та медичні установи;

4) будівельна площадка;

5) промислові об'єкти;

6) торгівля та сервіс;

7) державні та приватні компанії;

Як системний інтегратор ТОВ "ЕР ДЖІ БІ" виділяється такими особливостями:

1) зі своїми консультантами, аналітиками, системними архітекторами, інженерно-технічним персоналом і виробничо-технічною базою;

2) з досвідом роботи в сфері реалізації проектів різного обсягу з використанням обладнання різних виробників;

3) з досвідом як створення апаратного забезпечення, так і розробки власного програмного забезпечення;

4) з можливістю знайти найбільш оптимальне технічне рішення для даного замовника в рамках виділеного бюджету, надійно відповідаючи поточним вимогам і забезпечуючи передбачуваний розвиток;

5) з можливістю надати клієнту кілька варіантів вирішення проблеми;

6) структурування бізнес-процесів, розробка єдиної концепції інформаційних систем для компаній з інформаційними потоками будь-якого рівня та складності;

7) виконуючи всі види робіт у процесі створення та експлуатації системи зв’язку, забезпечуючи застосування комплексного підходу при побудові телекомунікаційних та інформаційних систем різного обсягу;

8) проведення аудиту телекомунікаційних систем та надання рекомендацій щодо подальшого розвитку;

9) проведення передпроектного обстеження та експертної оцінки, визначення системних вимог;

10) підготовка професійного технічного завдання, проектування, постачання обладнання та засобів зв'язку, інтеграція обладнання різних виробників в єдину систему, виконання монтажних та пусконалагоджувальних процесів, надання замовнику системи під ключ та навчання персоналу замовника;

11) з наданням спеціалізованого сервісного, гарантійного та післягарантійного обслуговування.

1.4 Огляд існуючих рішень

1.4.1 Інформаційні системи

Як правило, існують три види задач, для вирішення яких створюють інформаційні системи: структуровані (формалізовані), неструктуровані (неформалізовані) і частково структуровані.

Структурована (формалізована) задача - задача, в якій відомі всі її елементи та зв'язки між ними.

Неструктуроване (неформалізоване) завдання - завдання, в якому немає можливості виділити елементи та встановити зв'язки між ними.

У структурованій задачі можна виразити її зміст у вигляді математичної моделі з точним алгоритмом розв’язання. Такі завдання, як правило, доводиться вирішувати неодноразово і носять рутинний характер. Метою використання інформаційної системи для вирішення структурованих задач є повна автоматизація їх вирішення, т. зведення ролі людини до нуля.

Типи інформаційних систем, що використовуються для вирішення пів-структурованих задач. Комп’ютерні системи (КС), які використовуються для вирішення частково структурованих завдань, поділяються на два типи, які створюють управлінські звіти і в основному орієнтовані на обробку даних

(пошук, сортування, збір, фільтрація). Використовуючи інформацію, що міститься в цих звітах, керівник приймає рішення;

КС, створення управлінських звітів, забезпечення інформаційної підтримки користувача, тобто. надання доступу до даних бази даних та їх часткова обробка. Процедури маніпулювання даними в інформаційній системі повинні надавати такі можливості:

1) складання комбінацій інформації, отриманої з різних джерел;

2) швидке додавання або видалення того чи іншого джерела даних і автоматична заміна джерел під час пошуку даних;

3) управління даними з використанням можливостей систем управління базами даних;

4) логічну незалежність даного типу даних від інших баз даних, що входять до підсистеми інформаційного забезпечення;

5) автоматичне відстеження потоку даних для заповнення баз даних.

6) інформаційні системи, розробка альтернативних рішень можуть бути зразковими та експертними.

Модельні інформаційні системи надають користувачеві математичні, статичні, фінансові та інші моделі, використання яких полегшує розробку та оцінку альтернативних рішень. Користувач може отримати відсутню інформацію для прийняття рішень шляхом діалогу з моделлю в процесі навчання.

Основними функціями модельної КС та інформаційної системи є:

1) вміння працювати в середовищі стандартних математичних моделей, включаючи «як це зробити?», «що якщо?», аналіз чутливості тощо. для вирішення ключових питань моделювання, таких як;

2) достатньо швидка та адекватна інтерпретація результатів моделювання;

3) оперативна підготовка та коригування вхідних параметрів і обмежень моделі;

4) можливість графічного відображення динаміки моделі;

5) можливість пояснити користувачеві необхідні кроки для формування та роботи моделі.

Створюючи експертні інформаційні системи, користувач забезпечує розробку та оцінку можливих альтернатив Експертні системи пов’язані з обробкою знань. Експертна підтримка рішень, які приймає користувач, реалізована на двох рівнях.

Робота експертного забезпечення першого рівня випливає з концепції «стандартних управлінських рішень», тому проблемні ситуації, які часто виникають в процесі управління, можна звести до деяких однорідних класів управлінських рішень, тобто. до деякого набору альтернатив за замовчуванням. На цьому рівні створюється база даних для зберігання та аналізу типових альтернатив для реалізації експертної підтримки.

Якщо проблемна ситуація не пов'язана з наявними класами типових альтернатив, має вступати в дію другий рівень експертної підтримки управлінських рішень. Цей рівень генерує альтернативи на основі інформації, наявної в інформаційній базі, правил перетворення та процедур оцінки синтезованих альтернатив.

Залежно від ступеня автоматизації інформаційні процеси в системі управління підприємством визначаються як ручні, автоматичні, автоматизовані інформаційні системи.

Ручні інформаційні системи (ІС) характеризуються відсутністю сучасних технічних засобів обробки інформації та виконанням усіх операцій однією особою. Наприклад, у компанії без комп’ютерів можна сказати, що менеджер працює з ручною ІС.

Автоматичні ІС виконують усі операції обробки даних без втручання людини.

Автоматизовані ІС передбачають участь як людини, так і технічних засобів у процесі обробки інформації, при цьому головну роль відіграє комп’ютер. У сучасному трактуванні термін «інформаційна система» обов'язково включає поняття автоматизованої системи.

Автоматизовані інформаційні системи мають різні модифікації з урахуванням їх широкого використання в організації процесів управління і можуть бути класифіковані, наприклад, за характером використання інформації та сферою застосування.

Інформаційно-пошукові системи вводять, систематизують, зберігають, надають інформацію за запитом користувача без складних перетворень даних. Наприклад, інформаційно-пошукова система в бібліотеці, залізничних і авіакасах.

Системи інформаційних рішень виконують усі операції обробки інформації за певним алгоритмом. Серед них отриману інформацію можна класифікувати за ступенем впливу на процес прийняття рішень і виділити два класи: менеджери та консультанти.

Менеджери ІБ готують інформацію для прийняття людських рішень. Ці системи характеризуються типом обчислювальних завдань і обробкою великих обсягів даних. Прикладом цього є система оперативного планування виробництва, система бухгалтерського обліку.

Консультативна ІС виробляє інформацію, яка враховується людиною і не перетворюється відразу на ряд конкретних дій. Ці системи мають вищий інтелект, оскільки вони характеризуються обробкою знань, а не даних.

Інформаційні системи призначені для автоматизації функцій управління організаційним менеджментом . Враховуючи найширше застосування та різноманітність цього класу систем, часто будь-яка інформаційна система чітко розуміється під цим визначенням. До цього класу відносяться системи управління інформацією як для промислових фірм, так і для непромислових об'єктів: готелів, банків, торговельних фірм і т. д. Основними функціями таких систем є: оперативний контроль і регулювання, оперативний облік і аналіз, перспективне і оперативне планування, облік, управління збутом і постачанням та інші економічні та організаційні завдання.

ІС управління технологічними процесами (ТП) служить для автоматизації функцій виробничого персоналу. Вони широко використовуються в організаціях

для обслуговування технологічних процесів металургійної та машинобудівної промисловості.

ІС автоматизованого проектування (САПР) призначена для автоматизації функцій інженерів-конструкторів, конструкторів, архітекторів, конструкторів при створенні нової техніки чи технології. Основними функціями таких систем є: інженерні розрахунки, створення графічних документів (креслень, схем, планів), створення проектної документації, моделювання проектованих об'єктів.

Інтегрована (корпоративна) ІС використовується для автоматизації всіх функцій компанії та охоплює весь бізнес-цикл від проектування до реалізації продукції. Створення таких систем дуже складне, тому що вимагає системного підходу з точки зору головної мети, наприклад, отримання прибутку, завоювання ринку збуту і т. д.

1.5 Визначення можливих напрямків рішення поставлених завдань

Завданням кваліфікаційної роботи на тему «Комп’ютерна система ТОВ «ЕР ДЖІ БІ» з детальною реалізацією побудови та налаштування корпоративної мережі виступає побудова та моделювання роботи комп’ютерної мережі ТОВ «ЕР ДЖІ БІ», розробка апаратної частини та конфігурування IP-адресації кінцевих вузлів мережі.

В ході розробки проекту були визначені основні завдання реалізації:

1) проаналізувати існуючі мережеві рішення;

2) розробка апаратних рішень;

3) вибір апаратних пристроїв;

4) побудувати в PT модель КМ корпоративної мережі та виконати базові налаштування;

5) розрахунок щільності трафіку для найбільшої мережі;

6) конфігурація та підключення фізичного обладнання;

7) базова настройку мережевих інтерфейсів;

8) поділ IP-адреси згідно завдання;

9) налаштування безпеки на мережевого обладнання;

10) реалізація протоколу NAT;

11) розробити моніторинг мережного трафіку по протоколу Netflow;

12) налаштувати Netflow на мережному обладнанні;

13) протестувати та поспостерігати за роботою системи моніторингу потоків даних по протоколу NetFlow.

Моделювання роботи мережі комп’ютерної системи ТОВ «ЕР ДЖІ БІ» необхідно виконувати в додатку Cisco Packet Tracer з повною конфігурацією для всіх пристроїв.

1.6 Завдання і мета роботи, що виконується

Завданням кваліфікаційної роботи є розробка «Комп’ютерна система ТОВ «ЕР ДЖІ БІ» з детальною реалізацією побудови та налаштування корпоративної мережі виступає побудова та моделювання роботи комп’ютерної мережі ТОВ «ЕР ДЖІ БІ».

Беручи до уваги поточну мережеву структуру підприємства, кількість підмереж, їх взаємозв'язок, кількість комп'ютерів і обладнання, необхідно розрахувати настройки топології конкретної мережі, визначити інтерфейс каналів зв'язку і протокол обміну, розрахувати топологічну схему комп'ютерної системи, розрахувати параметри маршрутизації для комп'ютерної мережі, а також провести подальше моделювання і верифікацію комп'ютерної системи.

Крім того, необхідно проаналізувати конструкцію мережі нового підприємства, визначити відповідне фізичне середовище, кабелі, порти і роз'єми для підключення мережевих пристроїв до інших мережевих пристроїв і вузлів, визначити мережеві пристрої і компоненти, необхідні для задоволення технічних вимог мережі і аналітичні розрахунки споживаної потужності, обсягів і швидкостей передачі даних по мережевих каналах з урахуванням зазначених пристроїв, затримок в обробці даних на вузлах мережі.

Відповідно до методичних вказівок до кваліфікаційної роботи бакалавра для реалізації побудови та налаштування корпоративної мережі ТОВ «ЕР ДЖІ БІ» слід використати наступні дані для адресації корпоративної мережі:

– блок адрес для виділення підмереж: 172.23.112.0/21;

– кількості вузлів для мережі LAN1: 63;

– кількості вузлів для мережі LAN2, од.: 77;

– кількості вузлів для мережі LAN3, од.: 15;

– кількості вузлів для мережі LAN4, од.: 94;

– кількості вузлів для мережі LAN5, од.: 85.

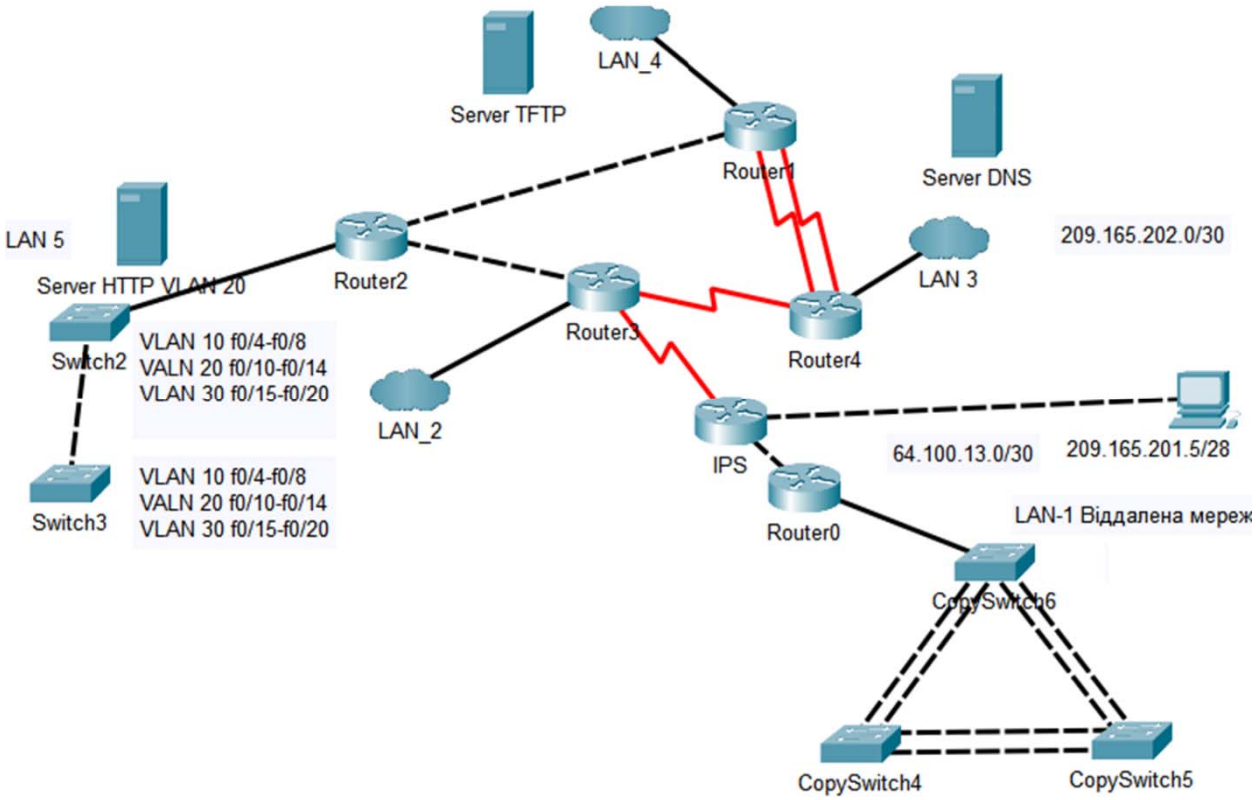

Рисунок 1.6 – Топологія мережі ТОВ «ЕР ДЖІ БІ»

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПИЄМСТВА ТОВ «ЕР ДЖІ БІ»

2.1 Технічні вимоги до комп'ютерної системи

2.1.1 Загальні відомості

Замовник - ТОВ «ЕР ДЖІ БІ».

Роботи з проектування локальної комп'ютерної мережі виконуються відповідно до документації:

– затвердженим технічним завданням на проектування локальної обчислювальної мережі;

– Договір на проектування локальної мережі. Терміни і етапи виконання робіт з проектування локальної комп'ютерної мережі визначаються здійснюваним трудовим договором.

2.1.2 Призначення та цілі створення локальної обчислювальної мережі

Локальна обчислювальна мережа призначена для організації середовища передачі інформації в комп'ютерній системі ТОВ «ЕР ДЖІ БІ».

Вимоги, викладені в Технічному завданні, повинні служити основою для проектування локальної обчислювальної мережі.

2.1.3 Вимоги до локальної обчислювальної мережі

2.1.3.1 Вимоги до локальної обчислювальної мережі загалом

Нове приміщення ЛВС має бути інтегроване в існуючу мережу та максимально використовувати наявні ресурси, як приватні, так і неорендовані, а локальна мережа повинна включати наступні елементи:

– інформаційна кабельна підсистема пропускною здатністю 1 000 Мб/с;

– активне обладнання (комутатори, роутери);

– підсистема інформаційного кабелю повинна бути побудована відповідно до вимог стандарту ISO/IEC 11801 Class D, Class 5E.

– загальна кількість автоматизованих робочих місць -24.

Максимальна довжина кабелю між інформаційним портом RJ45 і розподільним щитом не повинна перевищувати 90 метрів. ЛВС в цілому повинна відповідати класу не менше 5Е, а всі компоненти (кабелі, розетки, розподільні щити, з'єднувальні дроти) - класу не менше 5Е. Кожне автоматизоване робоче місце повинно складатися з інформаційного прийому RJ-45 в кількості 2 штук.

Для створення локальної мережі необхідно використовувати тільки якісні комплектуючі, які пройшли повну перевірку відповідно до вимог стандарту ISO 9001. Всі кабельні системи локальних комп'ютерних мереж повинні виконуватися з урахуванням вимог фізичного захисту доріг від пошкоджень, в тому числі:

Прокладка кабелів за підвісними стелями, за гіпсокартонними стінами, в металевих лотках і кабель-каналах. Встановіть кабелі вздовж траси за допомогою спеціальних ланок по всій довжині. Обладнання локальної мережі та схеми її підключення повинні забезпечувати подвійне резервування каналів передачі даних.

2.1.3.2 Загальні вимоги до інформаційної кабельної підсистеми

Підсистема інформаційного кабелю призначена для передачі інформації між локальними пристроями автоматизованих приміщень (комп'ютери, активне обладнання, багатофункціональні пристрої) і повинна забезпечувати підключення до мережі в комп'ютерній системі компанії ТОВ «ЕР ГБ». Кількість автоматизованих приміщень може бути змінено виконавцем за погодженням із замовником на етапі проектування локальної мережі.

Всі порти RJ-45, розташовані в приміщенні, а також розподільний щит повинні бути позначені таким чином, щоб їх можна було однозначно ідентифікувати. Маркування повинна виконуватися лазерним друком або принтером. Технологія прокладки кабелю повинна забезпечувати збереження естетичного вигляду приміщення після проведення монтажних робіт.

2.1.3.3 Вимоги до активного обладнання

Обладнання повинно працювати 24 години на добу, 7 днів на тиждень, без урахування часу, необхідного для регламентного обслуговування відповідно до рекомендацій виробника. Кількість активних торгових точок обладнання повинна забезпечувати працездатність 100 % автоматизованих робочих місць і наявність принаймні на 20% більшого інвентарю. Устаткування повинно бути здатним монтуватися в 19-дюймову розподільчу шафу. Технічні вимоги до активного обладнання. 1. Маршрутизатор – повинен бути з функціоналом брандмауера і можливістю призначення листів доступу для мережевої інтеграції до комп'ютерної системи ТОВ «ЕР ГБ»:

– процесор ARM, щонайменше, 680MHz;

– пам'ять не менше: 256MB DDR;

– жорсткий диск не менше: 512MB на чіпі пам'яті NAND, microSD слот;

– Ethernet порти щонайменше: п'ять 10/100/1000 Mbit/s Ethernet портів з підтримкою Auto MDI/X;

– продуктивність у режимі екрану не менше 1 Гбіт/с;

– маршрутизації RIP, OSPF, BGP так;

– EoIP тунелі не обмежено;

– PPPoE тунелі щонайменше 500;

– тунелі PPTP щонайменше 500;

– L2TP тунелі не менше 500;

– OVPN тунелі не обмежено;

– інтерфейсів VLAN не обмежено;

– правила брандмауера P2P не обмежено;

– NAT правила не обмежено;

– активних користувачів Хот-Спот 500;

– багаторівн. L2/L3/L4 списки доступу для інтеграції з мережею; 2. Комутатор:

– порти Gigabit Ethernet 10/100/1000 не менше 24 порти;

– порти SFP	не менше 4 слоти;
– пропускна здатність	не менше 48 Гбіт/сек;
– системна пам'ять	не менше 128 Мбайт;
– об'єм буфера пакетів	не менше 0,75 Мбайт;
– вбудована флеш-пам'ять	не менше 32 Мбайт;
– розмір бази даних адрес	не менше 8000 MAC-адрес;
– число VLAN	не менше 1024;
– число транків	не менше 64;
– число черг	не менше 8;
– число маршрутизованих VLAN	не менше 32.

2.1.3.4 Вимоги до кабелів-каналів, інформаційних та електричних розеток

Для реалізації проекту підрядник самостійно вибирає виробника кабельної системи. Тип і розмір канального кабелю для горизонтальної кабельної підсистеми повинні бути однаковими у всіх приміщеннях.

2.1.3.5 Вимоги до комутаційної системи

Серверна кімната знаходиться в будівлі за адресою центрального офісу ТОВ «ЕР ГБ»: вул. Волинська, 40, м. Київ, 03151, обладнана шафою зв'язку 42У. До цієї шафи підключаються кабелі від вертикальних і горизонтальних електро-установочних систем. У ньому також повинно бути встановлене в шафі активне обладнання, потрібно дотримуватися наступне розташування. Зверху вниз: регулятор, інтегровані мідні патч-панелі з 48-портовими регуляторами, активне мідне обладнання, сервери, джерела безперебійного живлення.

2.1.3.6 Вимоги до електроживлення та заземлення

Система живлення локальної мережі на робочому місці призначена для підключення робочих комп'ютерів від структурованої кабельної системи

(СКС) до електричної мережі 220 В і 50 Гц. Кожна робоча станція в локальній мережі повинна бути обладнана двома електричними розетками 220 В, 50 Гц з підключенням на землю. Комп'ютерні розетки повинні бути іншого кольору, ніж ліжка, або мати відповідне маркування. Система електропостачання на робочих станціях локальної мережі являє собою електричну мережу, призначену для розподілу 380 /220 В, 50 Гц, яка підключена до загальної системи електропостачання будівлі в центральному розподільчому пристрої.

Система електропостачання повинна працювати за 5-провідної схемою (TN-C-S) в магістральної частини і за 3-провідною схемою в комплектної деталі. Рівномірний розподіл тягаря повинен забезпечуватися поетапно. Електропостачання колективних заземлювальних щитів від головних розподільних щитів здійснюється відповідно до радіальної схеми живлення. Щити встановлені повністю. Конструкція екранування повинна забезпечувати дотримання вимог безпеки і високий рівень надійності. в силових щитах забезпечити 30% резервування на місці для додаткової установки вимикача.

Необхідно забезпечити підключення джерела безперебійного живлення, що забезпечує живлення мережі і сервера (при наявності вільного місця), розташованого в розподільній шафі, окремої лінії електропередачі і від окремого автоматичного вимикача. Для полегшення підключення активного обладнання та телекомунікацій в шафі необхідно забезпечити електричні щити, підключені до інвертора, з достатньою кількістю розеток для підключення встановленого в шафі обладнання і запасом не менше 20% на розробку.

Розподільні щити, автоматичні вимикачі та кабелі повинні бути забезпечені сертифікатами відповідності відповідно до нормативних документів і мати відповідне маркування. Електричні кабелі повинні бути ізольовані з негорючих матеріалів з низьким вмістом галогену (маркування нг LS). Заземлення елементів системи повинно відповідати вимогам глави 1.7 ПУЕ (сьома версія). Корпус шафи управління СКС повинен бути заземлений окремим роз'ємом безпосередньо з основною шиною заземлення.

Електричні кабелі прокладаються в металевих лотках при прокладці кабельних рейок, прихованих за високим дахом або в кабель-каналах з відкритим розширенням. В офісах монтаж повинен здійснюватися на окремих ділянках пластикових кабель-каналів з СКС.

Силові розетки і розетки СКС в приміщеннях локальної мережі повинні встановлюватися в стандартні елементи конструкції - супорти, шини і т.д. І він має таку ж конструкцію.

Перед початком робіт підрядник повинен розробити єдину лінійну схему системи розподільчого електропостачання приміщення локальної мережі та узгодити з особою, відповідальною за електропостачання, включаючи електропостачання шафи зв'язку, розрахунок навантаження, плани поверхів прокладки та прокладання електричних кабелів, графік підключення кабелів. При розрахунках передбачається, що споживана потужність робочої станції ЛВС становить 350 Вт. Сумарна споживана потужність комутаційної шафи повинна бути прийнята в розмірі 3 000 Вт (з урахуванням встановленого додаткового серверного обладнання).

2.1.4 Надійність

Обладнання, що входить до складу локальної комп'ютерної мережі, повинно забезпечувати узгодженість фізичних характеристик каналу між портом активного обладнання і абонентським обладнанням незалежно від шляху комутації на комутаційних щитах розподільних вузлів. Стабільність фізичних параметрів каналу повинна забезпечуватися при наступних видаленнях, незалежно від їх кількості (але не більше, ніж зазначено виробником обладнання LAN).

Будь-який канал в локальній комп'ютерній мережі може бути перерваний тільки при включенні розподільних щитів для вузлів розподілу.

Обладнання та матеріали, що використовуються в локальній комп'ютерній мережі, не повинні дозволяти змінювати фізичні та хімічні параметри внаслідок впливу навколишнього середовища протягом усього

гарантійного терміну за умови дотримання умов експлуатації, визначених виробником.

У разі обриву каналу повинна бути передбачена можливість переходу на використання альтернативного каналу серед резервних каналів шляхом зміни підключень на комутаційних щитах розподільчих вузлів.

2.1.5 Безпека

Використовуване обладнання та матеріали не повинні допускати можливості пошкодження здоров'я або персоналу електричним струмом або електромагнітним випромінюванням за умови дотримання правил експлуатації апарату.

2.1.6 Однорідність

Застосування стандартизованих типів кабелів і роз'ємів в приміщеннях, горизонтальних підсистемах, внутрішніх системо-утворюючих пристроїв, а також розподільних вузлах незалежно від типів абонентського обладнання, що підключається і активного обладнання різних підсистем.

2.1.7 Розширюваність

Передбачити можливість збільшення абонентської ємності локальної комп'ютерної мережі шляхом включення додаткових ліній горизонтальної підсистеми без необхідності прокладання нових кабельних доріг і кабельних каналів і виведення з ладу внутрішніх приміщень, а також без зупинки роботи співробітників установки.

2.2 Вибір апаратних засобів КС

2.2.1 Мережевий комутатор

Мережевий комутатор VAN в основному забезпечує базову комунікаційну платформу та в основному використовується в галузі телекомунікацій. Комутатори LAN зазвичай використовуються для

підключення термінальних пристроїв, таких як комп’ютери та мережеві принтери, і зазвичай використовуються в локальних мережах.

З точки зору середовища передачі та швидкості передачі комутатори локальної мережі можна розділити на комутатори Ethernet, комутатори високошвидкісних Ethernet, комутатори Gigabit Ethernet, комутатори ATM, комутатори FDDI та комутатори Token Ring. Ці комутатори застосовні до мереж Ethernet, Fast Ethernet, FDDI, ATM і Token Ring. Серед усіх мереж найпоширенішою є бізнес-мережа, побудована на комутаторах Ethernet.

Мережевий комутатор - це пристрій, який виконує функції обміну інформацією в системі зв'язку. Він може забезпечити ексклюзивний шлях електричної сигналізації для будь-яких двох мережевих вузлів комутатора доступу. Основні функції комутатора включають фізичну адресацію, топологію мережі, перевірку помилок, послідовність кадрів і контроль потоку. Наразі комутатор також має деякі нові функції, такі як підтримка VLAN (віртуальної локальної мережі), підтримка агрегації посилань, а деякі навіть мають функцію брандмауера.

Наступні 4 види перемикачів:

1. Комутатори PoE +. Розшифровується як Power over Ethernet Plus, що називається «Enhanced Power over Ethernet», що є оновленою версією POE. Комутатор POE+ відноситься до технології, яка може забезпечити постійний струм для таких пристроїв, а також передавати сигнали даних на деякі базові термінали без будь-яких змін в існуючій кабельній інфраструктурі Ethernet Cat5. Перемикач. Він використовується в основному на рівні доступу в архітектурі мережі малого бізнесу.

2 Фотоелектричний гібридний перемикач - означає, що порт комутатора має як оптичний роз’єм для вставлення оптичних модулів, так і електричний роз’єм RJ45 для вставлення мережевих кабелів. Наші фотоелектричні гібридні комутатори - це в основному комутатори L2, L2 +, які в основному використовуються на рівні доступу та рівні агрегації малих підприємств у мережевій архітектурі.

3. Комутатори S5800 – комутатори S5800 в основному використовуються в додатках Ethernet для центрів обробки даних і метро. Комутатор працює належним чином з незалежними правами інтелектуальної власності та підтримує різні функції, такі як L2 / L3 / Data Center / Metro Ethernet, включаючи комплексні протоколи та програми керування моніторингом. У мережевій архітектурі він в основному застосовується до ядра, магістралі та листя малих і середніх підприємств.

4. N перемикачів. Серія N – це високорентабельний комутатор нового покоління високої щільності. Комутатори серії N поділяються на системні «голі метали» та ICOS. У продуктах використовуються мікросхеми Broadcom і процесори Intel, чудові конфігурації, висока продуктивність і низька ціна. Він в основному використовується на базовому рівні Інтернет-компаній або мережах передачі даних, Spine і Leaf в мережевій архітектурі.

Для побудови мережі передачі даних для комп'ютерної системи ТОВ «ЕР ДЖІ БІ» будемо використовувати сертифікований в Україні комутатор Catalyst 2960.

Комутатор Catalyst 2960 − це комутатор Ethernet, який може підключатися до робочих станцій, бездротових точок доступа Cisco, та інших мережевих 27 пристроїв, таких як сервери, маршрутизатори та інші комутатори. Зовнішній вигляд маршрутизатора Catalyst 2950 представлено на рисунку 2.1. В таблиці 2.1 наведені його технічні характеристики.

Рисунок 2.1 – Комутатор Cisco 2960

Таблиця 2.1 – Технічні характеристики комутатора Cisco 2950

Manufacturer:	Cisco
Product ID:	WS-C2950X-24PS-L
Product Description:	Cisco Catalyst 2950-X 24 GigE PoE 370W, 4 x 1G SFP
Product Type:	Ethernet Switch
Total Number of Network Ports:	24
Number of PoE (RJ-45) Ports:	24
Port/Expansion Slot Details:	24 x Gigabit Ethernet Network
	4 x Gigabit Ethernet Expansion Slot
Media & Performance	
Media Type Supported:	Twisted Pair
Twisted Pair Cable Standard:	Category 5
Ethernet Technology:	Gigabit Ethernet
Network Technology:	10/100/1000Base-T
Network & Communication	
Layer Supported:	2
Management & Protocols	
Manageable:	Yes
Management:	Web-based Management;VLAN; QoS; Syslog; Telnet; RMON I, II; SNMP v1, v2c, v3; CLI; DHCP
Memory	
Standard Memory:	512 MB
Memory Technology:	DRAM
Flash Memory:	128 MB

2.2.2 Мережевий маршрутизатор

Подібно до того, як комутатор з’єднує кілька пристроїв, щоб сформувати мережу, маршрутизатор з’єднує кілька комутаторів та окремі мережі, щоб сформувати більшу мережу. Ці мережі можуть бути розташовані в центрі або розподілені в кількох місцях. При створенні мережі малого бізнесу вам знадобиться один або кілька маршрутизаторів. Окрім з’єднання кількох мереж разом, маршрутизатори також дозволяють мережевим пристроям і кільком користувачам отримувати доступ до Інтернету.

Зрештою, маршрутизатори діють як диспетчери, направляючи трафік і вибираючи найбільш ефективний маршрут для інформації. Інформація передається по мережах у вигляді пакетів даних. Маршрутизатори з’єднують компанії зі світом, захищають інформацію від загроз безпеці та навіть визначають, які пристрої мають пріоритет.

З мережевого обладнання будуть використанні маршрутизатори Cisco.

Зовнішній вигляд маршрутизатора Cisco 1841 представлено на рисунку 2.2 а технічні характеристики в таблиці 2.2. Cisco 1841 можна використовувати для підключення мереж малого та середнього розміру (small-middle office), забезпечуючи сервіси VPN, систем IPS (intrusion prevention system) та функцій firewall (Modular Router w/2xFE, 2WAN slots, 64 FL/256 DR).

Рисунок 2.2 – Маршрутизатор Cisco 1841

Таблиця 2.2 – Технічні характеристики Cisco 1841

Виробник	Cisco Systems, Inc
Модель	CISCO 1841
Form Factor	Desktop
Розміри (WxDxH)	43.8 cm x 30.5 cm x 8.9 cm
Вага	6 фунтів
Standard Memory:	128 MB (installed) / 384 MB (max)
Flash	32 MB
Загальна кількість WAN та LAN портів	2
Протоколи маршрутизації	OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, static IPv4 routing, static IPv6 routing

2.2.3 Бездротовий маршрутизатор

Бездротовий маршрутизатор - це пристрій, який забезпечує пересилання та маршрутизацію пакетів бездротової мережі та діє як точка доступу в локальній мережі (LAN). Він дуже схожий на дротовий маршрутизатор, але замінює дроти бездротовими радіосигналами для зв’язку з внутрішнім і зовнішнім мережевим середовищем. Він може працювати як комутатор, інтернет-маршрутизатор і точка доступу.

Бездротовий маршрутизатор - це маршрутизатор у бездротовій локальній мережі (WLAN) для домашніх і невеликих офісних мереж. Є доступ до Інтернету та локальної мережі. Як правило, бездротові маршрутизатори підключаються безпосередньо до дротової або бездротової глобальної мережі. Користувачі, підключені до бездротового маршрутизатора, мають доступ не лише до локальної мережі, а й до зовнішніх глобальних мереж, таких як Інтернет. Залежно від можливостей бездротового маршрутизатора він може підтримувати від сотень до сотень одночасних користувачів. Більшість бездротових маршрутизаторів також здатні виконувати функцію брандмауера, що дозволяє блокувати, контролювати, контролювати та фільтрувати вхідний і вихідний мережевий трафік.

Бездротовий маршрутизатор Linksys WRT-300N (рис. 2.3) зазвичай використовується в домашніх мережах (а не в корпоративних), оскільки він має один порт Ethernet для підключення до Інтернету та чотири додаткові порти Ethernet для підключення кінцевих пристроїв.

Рисунок 2.3 – Linksys WRT-300N

Маршрутизатор Linksys WRT-300N можна налаштувати за допомогою графічного інтерфейсу користувача в Cisco Packet Tracer так само, як отримати доступ до маршрутизатора за допомогою веб-браузера . Усі меню доступні для

натискання та забезпечують доступ до сторінок конфігурації. Розробники намагалися змоделювати реальну функціональність для налаштування маршрутизатора.

2.2.4 Комп’ютерна робоча станція

Робоча станція (PC) – це комп’ютер, призначений для користувача або групи користувачів, зайнятих бізнесом або професійною роботою. Це включає один або кілька дисплеїв із високою роздільною здатністю та процесор, швидший за персональний комп’ютер (ПК). Робочі станції також мають чудові багатозадачні можливості завдяки додатковій пам’яті з довільним доступом (RAM), накопичувачам і ємності дисків. Робочі станції також можуть мати високошвидкісні графічні адаптери та інші периферійні пристрої.

Термін робоча станція також використовувався для позначення ПК або терміналу мейнфрейму в локальній мережі (LAN). Ці робочі станції можуть спільно використовувати мережеві ресурси з одним або кількома великими клієнтськими комп’ютерами та мережевими серверами.

Робочі станції зазвичай будуються за дизайном, оптимізованим для складних маніпуляцій даними та візуалізації. Приклади включають візуалізацію та редагування зображень, автоматизоване проектування (CAD), анімацію та математичне малювання. Робочі станції були першим галузевим сегментом, який представив на ринок інструменти для співпраці, преміальні аксесуари та вдосконалення. До них відносяться 3D-миші, кілька дисплеїв і високопродуктивні/ємні пристрої зберігання даних.

Робочої станції виконує такі функції, як:

– підтримка пам'яті коду виправлення помилок (EEC);

– додаткові роз'єми пам'яті для зареєстрованих модулів;

– мультипроцесорні сокети для більш потужних ЦП;

– кілька дисплеїв;

– стабільна операційна система (ОС) з розширеними функціями;

– високопродуктивна відеокарта.

Сьогодні виробляються робочі станції, які використовують мікропроцесори x64 і дистрибутивні операційні системи Windows, Mac OS X, Solaris і Linux.

В якості робочої станції обрано робочу станцію Alfa Server #136 (рис.2.4).

Рисунок 2.4 – Робоча станція Alfa Server #136

HikCentral-Workstation/64 - це робоча станція з вбудованим програмним забезпечення HikCentral Professional та операційною системою Windows 11. Комбінуючи сервер та клієнт HikCentral Professional забезпечує ефективне керування прямою трансляцією, відтворенням, розпізнаванням осіб, ANPR, контролем доступу, відеодомофонією, керуванням сигналами тривоги тощо.

Особливості робочої станції hikcentral:

– Operating System - Microsoft® Windows 11 IoT Ent (64-bit);

– Memory - 2 × 4GB 2666MHz DDR4 UDIMM;

– Graphics Card - Integrated Intel HD Graphics 630;

– Storage - M.2 256GB SATA Class 20 solid state drive;

– NIC - Integrated Intel I219-LM Ethernet LAN 10/100/1000;

– I/O Ports - 10 External USB: 1 × USB Type-C 3.1 Gen 2, 5 × 3.1 Gen 1 Type-A (1 Front, 4 Rear), 4 × USB 2.0, 1 × RJ-45, 2 × Displayport, 1 × Serial, 2 × PS/2.

2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

В найбільшій підмережі LAN4 встановлений комутатор Cisco2960, що об’єднує 94 ПК працівників. Вихідний трафік з комутатора SW_LAN4 надсилається до роутера KULINICH_R5 в лінію з пропускною здатністю, що становить 100 Мбіт/с.

Для того, щоб комутатор не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку μ=119 (кадрів/с), а середня довжина повідомлення – 950 байт.

Теоретично припустимо, що всі користувачі найбільшої підмережі LAN4 одночасно використовують мережу. В такому разі, пропускна здатність на рівні доступу буде дорівнювати:

$$P_{р.р.} = \mu * L_{пов} * N * 8 = 119 * 950 * 94 * 8 = 85 \text{ Мбіт/с} \quad (2.1)$$

де $L_{пов}$ – середня довжина повідомлення;

N – кількість вузлів в мережі.

Отриманий результат не перевищуватиме заданих параметрів мережі по вихідному каналу, отже перенавантажень не трапиться.

Комутатор SW_LAN4 також передає трафік до маршрутизатора зі швидкістю 100 Мбіт/с. Отже, загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих} = 10^9 / (950 * 8) = 131\,579 \text{ пакетів/с} \quad (2.2)$$

Оскільки в середньому, кожне джерело виробляє 119 пакетів/с, то маршрутизатор обмежений кількістю приєднань, яку ми можемо дізнатись наступним чином:

$$N = \mu_{вих} / \mu = 131\,579 / 119 \approx 1106 \text{ джерела} \quad (2.3)$$

Ця кількість задовольняє кількості вузлів у найбільшій нашій локальній мережі, до якої входить 94 ПК.

Кожен з 94 ПК посилає потік заявок з інтенсивністю у 119 кадрів/с. Звідси, можем розрахувати інтенсивність вихідного трафіку:

$$\lambda = N * \mu = 94*119 = 11186 \text{ пакетів/с.} \quad (2.4)$$

Коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu вих} = \frac{11186}{131\,579} = 0{,}085 \quad (2.5)$$

Коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho} = \frac{0{,}085}{1-0{,}085} = 0{,}093 \quad (2.6)$$

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

$$T = \frac{1}{(\mu-\lambda)} = \frac{1}{(131\,579 - 11186)} = 8{,}3 \text{ мкс} \quad (2.7)$$

Середня довжина черги:

$$L_{чер} = \frac{\rho^2}{1-\rho} = \frac{0{,}085^2}{1-0.085} = 0.0079 \quad (2.8)$$

Середній час перебування пакета у черзі:

$$T_{оч} = \frac{Lчер}{\lambda} = \frac{0{,}079}{11186} = 7{,}06 \text{ мкс} \quad (2.9)$$

Це значення задовольняє вимогам до затримки в ЛМ.

3 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ ТОВ «ЕР ДЖІ БІ»

3.1 Моделювання мережі в Packet Tracer

Для рішення поставлених задач була спроектована модель мережі комп'ютерної системи ТОВ «ЕР ДЖІ БІ» в середовищі Cisco Packet Tracer (рис. 3.1).

Створена мережа складається з декількох підмереж, які взаємодіють між собою для забезпечення комунікації та забезпечення безпеки мережевих пристроїв.

Відповідно до організаційної структури ТОВ «ЕР ДЖІ БІ» мережа складається з 5-ти локальних підмереж:

– підмережа керівництва (LAN1);

– виробництво (LAN2);

– фінансовий відділ (LAN3).

– відділ зовнішніх консультацій (LAN4)

– внутрішні консультанти (LAN5)

В локальних мережах застосовується технологія FastEthenet.

Вихід в Інтернет змодельована маршрутизатором ISP, до якого під'єднано мережу LAN4. Мережа LAN4 моделює роботу віддаленого офісу, який знаходиться в Internet.

Кінцеві пристрої в локальних мережах представлені ПК, ноутбуками, принтерами, бездротовими пристроями. В мережу LAN2 додано сервер, на якому розгорнуто сервіс email для створення поштового трафіку.

IP-адреси пристроям в дротових мережах призначені динамічна, в інших мережах статично, а в мережі LAN2 хости отримують IP-адреси по DHCP. В табл. 3.2 представлені відомості про адресацію всіх кінцевих пристроїв в відповідних мережах.

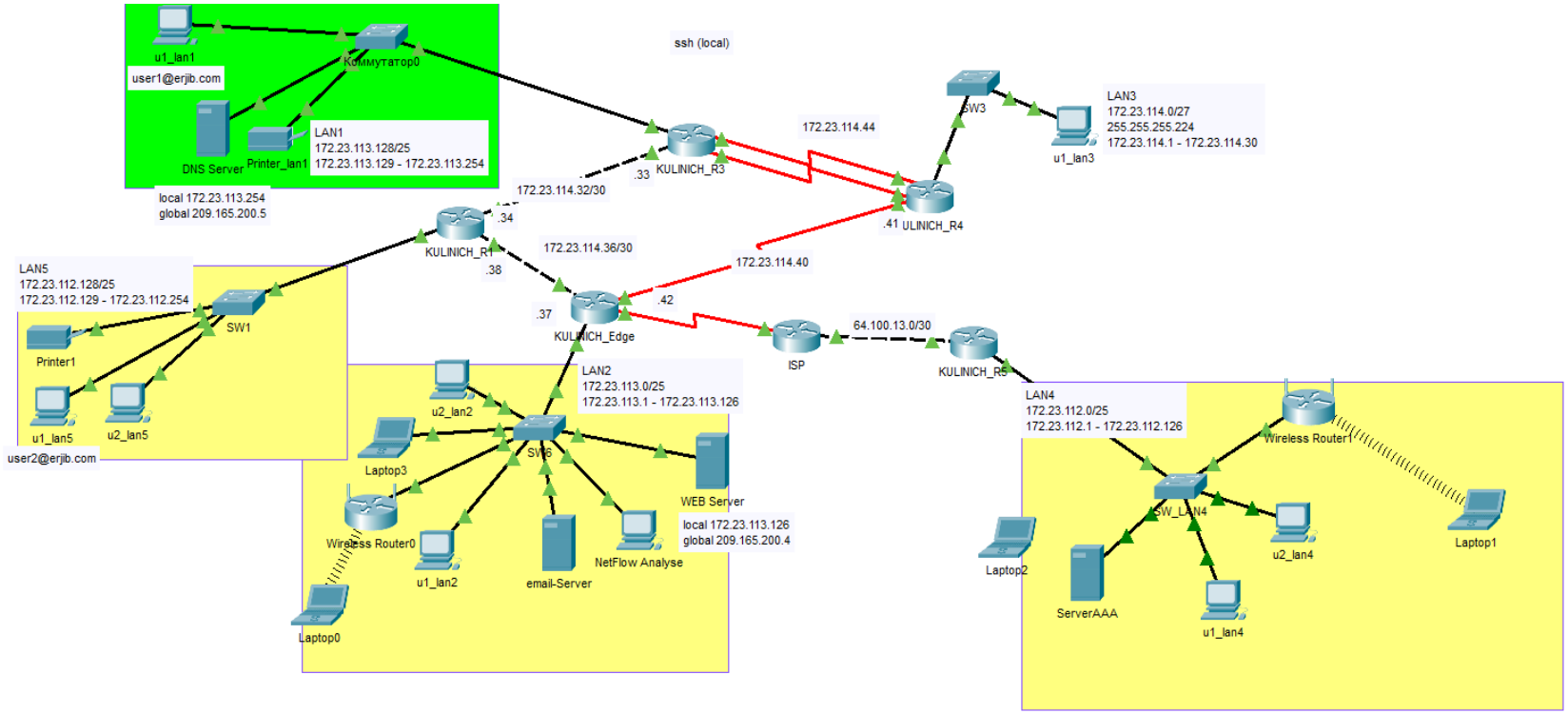

Рисунок 3.1 – Логічна топологія комп’ютерної мережі ТОВ «ЕР ДЖІ БІ»

3.2 Розрахунок схеми адресації корпоративної мережі

Відповідно до методичних вказівок до кваліфікаційної роботи бакалавра для реалізації побудови та налаштування корпоративної мережі ТОВ «ЕР ДЖІ БІ» слід використати наступні дані для адресації корпоративної мережі:

– блок адрес для виділення підмереж: 172.23.112.0/21;

– кількості вузлів для мережі LAN1: 63;

– кількості вузлів для мережі LAN2, од.: 77;

– кількості вузлів для мережі LAN3, од.: 15;

– кількості вузлів для мережі LAN4, од.: 94;

– кількості вузлів для мережі LAN5, од.: 85.

Завданий префікс /21 дозволяє адресувати до 2046 хостів. Відповідно до вимог в кількість хостів в ТОВ «ЕР ДЖІ БІ» необхідно 344 адрес для хостів, а це займає майже 17% з адресного простору. Таким чином 83% адрес не використовується.

Для виконання адресації мережі слід застосувати метод VLS, який надає можливість заощаджувати адреси за рахунок розділення на підмережі розміром за потребами в необхідній кількості користувачів. За цим методом мережі сортуються від найбільшої до найменшої і визначаються маски відповідно до потрібної кількості хостів.

Адресація обладнання та хостів виконується за наступними правилами:

– перші IP-адреси призначати інтерфейсам і підінтерфейсам маршрутизаторів у LAN;

– наступні IP-адреси призначати комутаторам у LAN;

– адреса серверів: останній можливий адресу у мережі.

– адреса вузлів: інші з використаних;

– в мережах VLAN використовувати адресацію кінцевих пристроїв за протоколом DHCP.

В таблиці 3.1 наведені розраховані адреси підмереж компанії, а в таблиці 3.2 адресація інтерфейсів мережних пристроїв згідно з правилами.

Таблиця 3.1 – Схема адресації мережі

Назва підмережі	Порібна кіл-ть вузлів	Доступна кіль-ть хостів	Адреса підмережі	Маска підмережі	Діапазон допустимих IP-адрес вузлів
LAN1	63	126	172.23.113.128	255.255.255.128	172.23.113.129 - 172.23.113.254
LAN2	77	126	172.23.113.0	255.255.255.128	172.23.113.1 - 172.23.113.126
LAN3	15	30	172.23.114.0	255.255.255.224	172.23.114.1 - 172.23.114.30
LAN4	94	126	172.23.112.0	255.255.255.128	172.23.112.1 - 172.23.112.126
LAN5	85	126	172.23.112.128	255.255.255.128	172.23.112.129 - 172.23.112.254
WAN1	2	2	172.23.114.32	255.255.255.252	172.23.114.33 - 172.23.114.34
WAN2	2	2	172.23.114.36	255.255.255.252	172.23.114.37 - 172.23.114.38
WAN3	2	2	172.23.114.40	255.255.255.252	172.23.114.41 - 172.23.114.42
WAN4	2	2	172.23.114.44	255.255.255.252	172.23.114.45 - 172.23.114.46

Таблиця 3.2 – Схема адресації маршрутизаторів

Пристрій	Інтерфейс	IP-адреса	Маска
KULINICH_R3	F0/0	172.23.113.129	255.255.255.128
	F0/1	172.23.114.33	255.255.255.252
	S0/3/0	172.23.114.46	255.255.255.252
	S0/3/1	172.23.114.50	255.255.255.252
KULINICH_R1	F0/0	172.23.112.129	255.255.255.128
	F0/1	172.23.114.34	255.255.255.252
KULINICH_R4	F0/0	172.23.114.1	255.255.255.224
	F0/1	172.23.114.33	255.255.255.252
	S0/1/0	172.23.114.41	255.255.255.252
	S0/3/0	172.23.114.45	255.255.255.252
	S0/3/1	172.23.114.49	255.255.255.252
KULINICH_Edge	F0/1	172.23.114.37	255.255.255.252
	S0/0/0	209.165.202.1	255.255.255.252
	S0/0/1	172.23.114.42	255.255.255.252
	E0/1/0	172.23.113.1	255.255.255.128
KULINICH_R5	F0/1	172.23.112.1	255.255.255.128
	E0/1/0	64.100.13.2	255.255.255.252
ISP	F0/0	64.100.13.1	255.255.255.252
	S0/0/0	209.165.202.2	255.255.255.252

3.3 Базове налаштування мережних пристроїв

За рекомендацією виробника Cisco базове налаштування мережних пристроїв включає в себе:

– назву пристрою;

– безпечний доступ до інтерфейсу командного рядка (CLI) та порту консолі за допомогою зашифрованих та відкритих паролів;

– повідомлення для користувачів, які входять до системи маршрутизатора;

– IP-адресація інтерфейсів;

– збереження базових налаштувань.

В лістингу 3.1 наведено приклад з базового налаштування маршрутизатора KULINICH_R1.

Лістинг 3.1 – Базове налаштування маршрутизатора

```
en
configure terminal
hostname KULINICH_R1
no ip domain-lookup
banner motd # This is a secure system. Authorized Access
Only!#
enable secret class
line console 0
password cisco
login
line vty 0 4
password cisco
login
service password-encryption
interface FastEthernet0/0
ip address 172.23.112.129 255.255.255.128
interface FastEthernet0/1
no shutdown
ip address 172.23.114.34 255.255.255.252
no shutdown
interface FastEthernet1/0
ip address 172.23.114.38 255.255.255.252
no shutdown
exit
copy run start
```

Можна застосувати цей лістинг на інших маршрутизаторах в підмережах, змінивши відповідно назву пристрою та IP-адреси.

3.4 Налаштування та перевірка маршрутизації

Так як на різних ділянках між маршрутизаторами використовуються різні типи підключень і пропускна здатність, то слід застосовувати протокол маршрутизації, який в якості метрики використовує значення пропускної здатності.

Алгоритм найкоротшого шляху (OSPF) – це протокол маршрутизації для IP-мереж на основі стану каналу. OSPF виявляє зміни у топології, наприклад збій каналу, і швидко сходиться у новій безпетлевій структурі маршрутизації. OSPF розраховує кожен маршрут з допомогою алгоритму Дейкстри, тобто. алгоритму найкоротшого шляху.

В лістингу 3.2 наведено налаштування OSPF на прикладі маршрутизатора KULINICH_R4. Використовується router ospf 9 у режимі глобальної конфігурації, щоб увімкнути протокол. Командою network оголошуються конкретні підмережі із прямим підключенням та ідентифікатор області, рівний 0.

Лістинг 3.2 – Налаштування OSPF на KULINICH_R4

```
router ospf 9
log-adjacency-changes
network 172.23.114.0 0.0.0.31 area 0
network 172.23.114.44 0.0.0.3 area 0
network 172.23.114.40 0.0.0.3 area 0
network 172.23.114.48 0.0.0.3 area 0
```

Можна застосувати цей лістинг на інших маршрутизаторах в підмережах, змінивши відповідно конкретні підмережі із прямим підключенням на кожному маршрутизаторі.

Після налаштування OSPF кожен маршрутизатор в таблиці маршрутизації побудує найкоротші шляхи до всіх відомих йому мереж.

Команда show ip route, введена на маршрутизаторі, відобразить всі мережі в таблиці маршрутизації на всіх маршрутизаторах. На рисунку 3.2 представлено таблиця маршрутизації на KULINICH_R4 після налаштування OSPF на всіх маршрутизаторах.

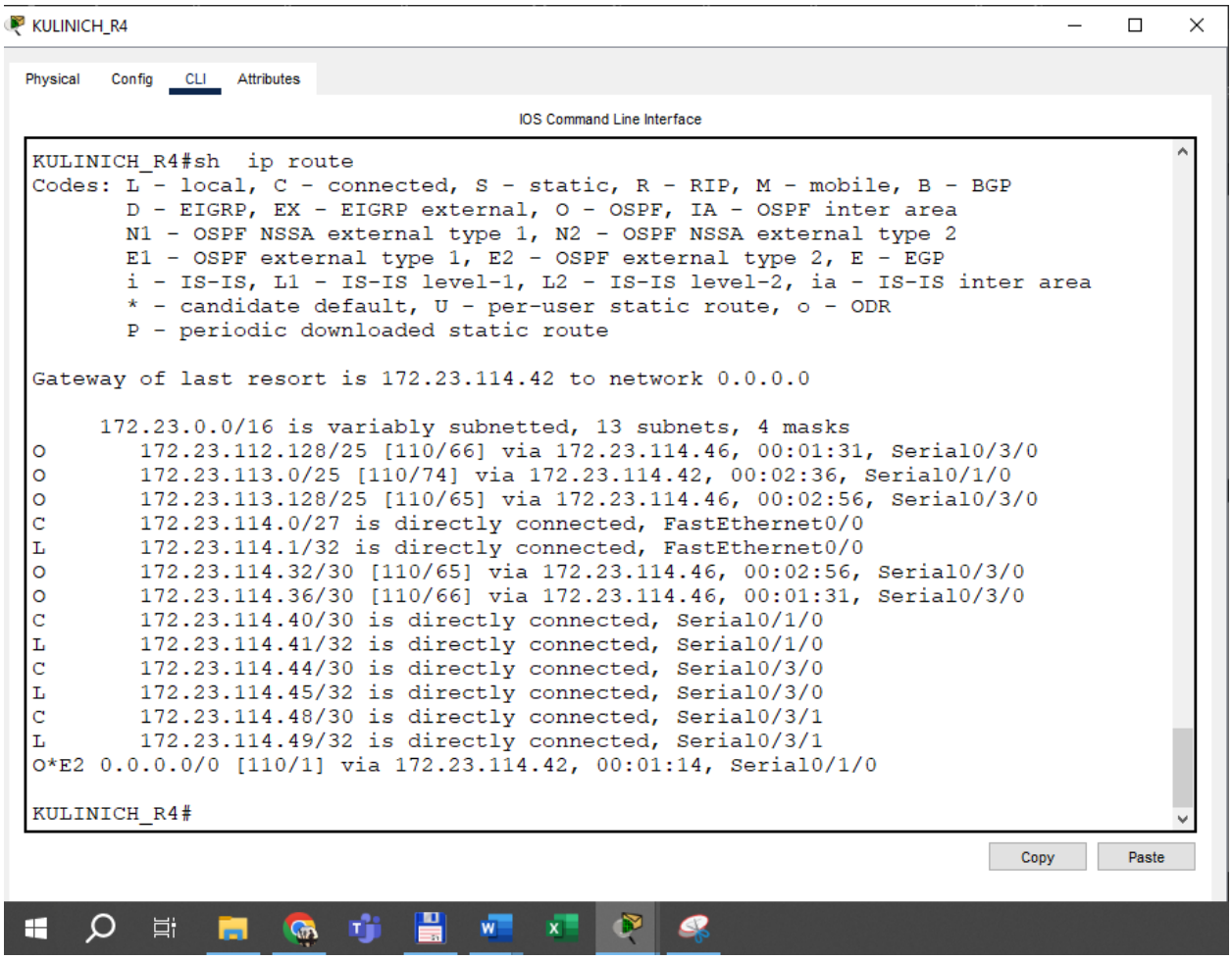

Рисунок 3.2 – Таблиця маршрутизації на KULINICH_R4

Всі комп'ютери повинні успішно відправляти ехо-запити до всіх інших комп'ютерів, зазначених у топології.

3.5 Налаштування та перевірка DHCP

DHCP (Dynamic Host Configuration Protocol) – це мережевий протокол, який дозволяє мережевим адміністраторам керувати та автоматизувати розподіл IP-адрес Без DHCP адміністраторам довелося б призначати та налаштовувати IP-адреси, DNS-сервери, шлюз за замовчуванням потрібно було б призначати і налаштовувати вручну. У міру зростання мереж і переміщення пристроїв з однієї внутрішньої мережі в іншу це стає складною адміністративною задачею.

В мережі LAN2 хости отримуватимуть IP-адреси по DHCP, за винятком серверів та ПК «NetFlow Analyse», який буде виконувати роль колектора протоколу NetFlow.

Для того щоб автоматично призначити адресну інформацію в мережі, необхідно налаштувати маршрутизатор KULINICH_Edge як сервер DHCPv4. На маршрутизаторі KULINICH_Edge необхідно створити пул DHCP-адрес для локальної мережі LAN2. Також потрібно виключити адреси, які не призначатимуться з пулу адрес. Виключати адреси рекомендується в першу чергу, щоб запобігти їхній випадковій оренді для інших пристроїв. В лістингу 3.3 виключаються перші десять адрес, пул DHCP містить стандартний шлюз, сервер DNS (172.23.113.254).

Лістинг 3.3 – налаштування сервера DHCPv4 на маршрутизаторі KULINICH_Edge

```
ip dhcp excluded-address 172.23.113.1 172.23.113.10
ip dhcp pool LAN2
network 172.23.113.0 255.255.255.128
default-router 172.23.113.1
dns-server 172.23.113.254
```

Щоб перевірити роботу DHCP на маршрутизаторі слід виконати команду show ip dhcp binding, щоб переглянути список орендованих DHCP адрес (рис.3.3).

```
KULINICH_Edge#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.23.113.11    0001.C959.B101            --                    Automatic
172.23.113.95    0002.4AA8.C16A            --                    Automatic
172.23.113.99    0001.96D0.84A3            --                    Automatic
172.23.113.97    0060.2F55.2C52            --                    Automatic
KULINICH_Edge#
```

Рисунок 3.3 – Список орендованих DHCP адрес

На рис. 3.4 відображено відомості з мережних налаштувань на ПК в мережі LAN2 з MAC-адресою 0002.4AA8.C16A.

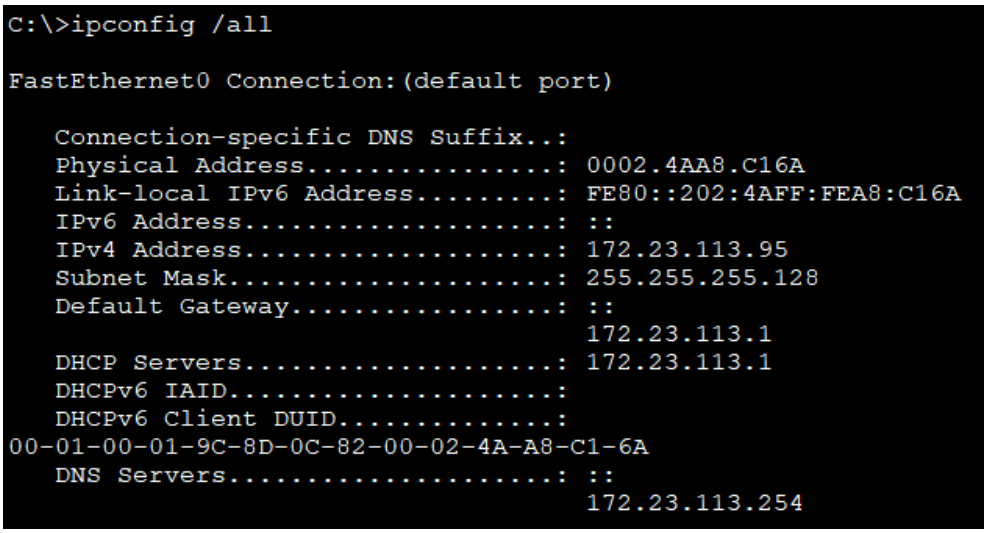

Рисунок 3.4 – Мережні налаштування на ПК u1_lan2

3.6 Налаштування доступу до Інтернет

Маршрут в Інтернет оголошений маршрутом за замовчуванням на пограничному маршрутизаторі KULINICH_Edge і розповсюджено іншим маршрутизаторам в мережі компанії через повідомлення OSPF (лістинг 3.4).

Лістинг 3.4 – Налаштування доступу до Інтернет на граничному маршрутизаторі KULINICH_Edge

```
router ospf 9
  redistribute static
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
```

В організації використовується приватний діапазон для адресації хостів, який зблокований провайдерами для маршрутизації через Інтернет.

Трансляція мережевих адрес (NAT) – це процес, за допомогою якого мережевий пристрій, наприклад, маршрутизатор Cisco, призначає публічні адреси хостам у приватній мережі. Оскільки кількість доступних публічних IPv4-адрес обмежена, NAT використовується для зменшення кількості публічних IP-адрес, що використовуються організацією.

Для доступу ззовні до внутрішніх серверів необхідно резервувати публічні IP-адреси та застосовувати статичний NAT на граничному маршрутизаторі KULINICH_Edge. В таблиці 3.3 наведено дані статичного NAT. В лістингу 3.5 налаштування статичного NAT.

Таблиця 3.3 – Статичний NAT

Сервер	Inside local	Inside global	Тип NAT
DNS server	172.23.113.254	209.165.200.5	статичний
WEB server	172.23.113.126	209.165.200.4	статичний

Лістинг 3.5 – Налаштування статичного NAT на KULINICH_Edge

```
ip nat inside source static  172.23.113.254 209.165.200.5
ip nat inside source static  172.23.113.126 209.165.200.4
```

Для доступу до Інтернет застосовується трансляція на основі інтерфейсу. В результаті IP-адреси внутрішніх хостів до Інтернет будуть замінені на IP-адресу інтерфейсу s0/0/0 граничного маршрутизатора KULINICH_Edge. В лістингу 3.6 налаштування динамічного NAT на пограничному маршрутизаторі KULINICH_Edge.

Лістинг 3.6 – Налаштування динамічного NAT на KULINICH_Edge

```
interface FastEthernet0/1
  ip nat inside
interface Serial0/0/0
  ip nat outside
interface Serial0/0/1
  ip nat inside
 interface Ethernet0/1/0
  ip nat inside
ip nat inside source list NAT interface Serial0/0/0 overload
ip access-list standard NAT
 permit 172.23.112.0 0.0.7.255
```

Після налаштування статичного NAT можна зайти на сторінку веб-сервера за його global-адресою 209.165.200.5 або за доменним ім’ям 123.dnipro.ua з будь-якого комп’ютера в Інтернеті (рис. 3.5).

В динамічному NAT при проходженні через маршрутизатор нова адреса заміняється на адрему вихідного інтерфейсу. Запис про трансляцію зберігається деякий час, щоб відповідні пакети могли бути доставлені адресату (рис. 3.6).

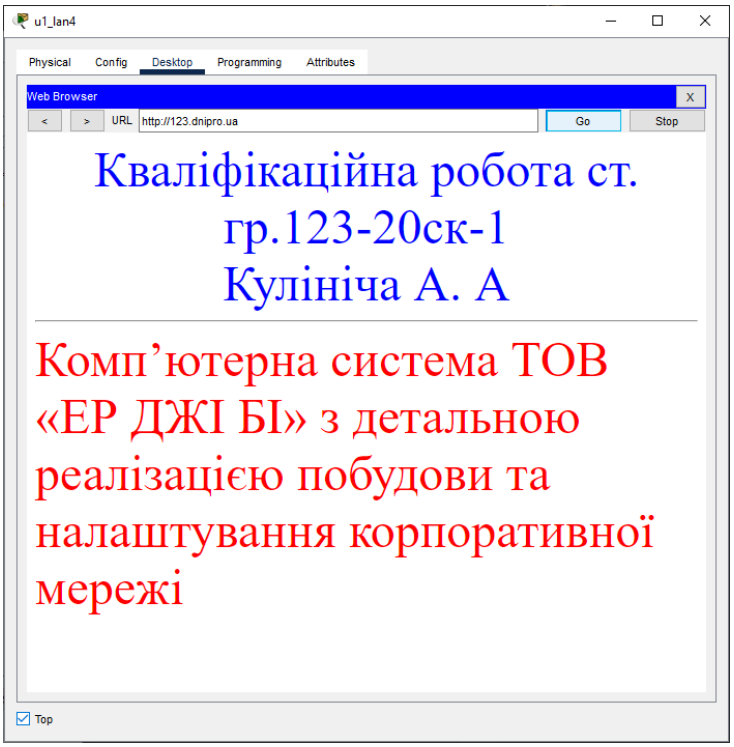

Рисунок 3.5 – Головна сторінка веб-сервера

```
KULINICH_Edge#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.202.1:1024172.23.114.10:4    172.23.112.21:4    172.23.112.21:1024
icmp 209.165.202.1:4   172.23.113.11:4    172.23.112.21:4    172.23.112.21:4
udp 209.165.200.5:53   172.23.113.254:53  172.23.112.22:1030 172.23.112.22:1030
---  209.165.200.4     172.23.113.126     ---                ---
---  209.165.200.5     172.23.113.254     ---                ---
tcp 209.165.200.4:80   172.23.113.126:80  172.23.112.22:1025 172.23.112.22:1025
tcp 209.165.200.4:80   172.23.113.126:80  172.23.112.22:1026 172.23.112.22:1026
tcp 209.165.200.4:80   172.23.113.126:80  172.23.112.22:1027 172.23.112.22:1027
```

Рисунок 3.6 – Таблиця трансляцій NAT

3.7 Захист інформації в комп'ютерній системі від несанкціонованого доступу

3.7.1 Захист локального доступу

За замовчанням, при приєднанні до маршрутизатора по консолі або порту AUX користувач одразу потрапляє до привілейованого режиму без пароля під обліковим записом звичайного користувача. Тому, якщо маршрутизатор не захищений фізично (не знаходиться в окремому приміщенні з обмеженим доступом), то необхідно встановити пароль на роботу в EXEC на цих портах. Навіть якщо маршрутизатор знаходиться в закритому приміщенні,

це також не зашкодить. Пароль слід задавати через локальну базу користувачів, що задається командою username.

Адміністратори мережі можуть відволікатися і випадково залишити сеанс привілейованого режиму EXEC у терміналі відкритим. Це може дозволити суб'єкту внутрішньої загрози отримати доступ до конфігурації пристрою з метою її зміни або видалення. За замовчуванням маршрутизатори Cisco закривають сеанс EXEC після 10 хвилин бездіяльності, тому це значення варто змінити на менше значення командою exec-timeout хвилин секунд. Її можна застосовувати на консольних, допоміжних (AUX) і vty-лініях. В лістингу 3.7 наведено налаштування до обмеженого локального доступу

Лістинг 3.7 – Налаштування локального доступу

```
line console 0
login local
exec-timeout 2
line aux 0
login local
```

Але якщо зловмисник має фізичний доступ до маршрутизатора, то він зможе використовувати для отримання доступу добре відомі методи відновлення паролів.

3.7.2 Обмеження віддаленого доступу

Використання Telnet небезпечно, оскільки текстові дані передаються в незашифрованому вигляді. Можна будь-яким мережним аналізатором перехопити пакети і вирахувати пароль. В лістингу 3.8 наведено налаштування ssh і відключення доступу по telnet. Також з цією конфігурацією контролюється кількість невдалих спроб входу в період часу, тим самим забезпечується захист від атаки підбору пароля. За замовчуванням кількість спроб 5, та час очікування відповіді від клієнта, коли сервер SSH намагається узгодити ключ сеансу та метод шифрування з клієнтом, що підключається, 60 секунд.

Лістинг 3.8 – Налаштування захисту віддаленого доступу

```
ip ssh time-out 60
ip ssh authentication-retries 3
ip domain-name erjib.com
crypto key generate rsa
1024
line vty 0 4
login local
transport input ssh
```

3.7.3 Захист AAA

Основною формою безпеки доступу до мережних пристроїв є створення паролів для ліній консолі, vty та aux. Під час доступу до маршрутизатора користувачеві пропонується лише ввести пароль. Налаштування привілейованого режиму EXEC увімкнення секретного пароля ще більше покращує безпеку, але для кожного режиму доступу потрібен лише базовий пароль.

Окрім основних паролів, у локальній базі даних маршрутизатора можна визначити конкретні імена користувачів або облікові записи з різними рівнями привілеїв, які можуть застосовуватися до маршрутизатора в цілому. Коли лінії консолі, vty або aux налаштовані для посилання на цю локальну базу даних, користувачеві буде запропоновано ввести ім’я користувача та пароль під час використання будь-якого з цих рядків для доступу до маршрутизатора.

Додатковий контроль над процесом входу можна досягти за допомогою автентифікації, авторизації та обліку (AAA). Для базової автентифікації AAA можна налаштувати для доступу до локальної бази даних для входу користувачів, а також можна визначити резервні процедури. Однак цей підхід не дуже масштабований, оскільки його потрібно налаштувати на кожному маршрутизаторі. Щоб повністю скористатися перевагами AAA та досягти максимальної масштабованості, AAA використовується разом із зовнішньою базою даних сервера TACACS+ або RADIUS. Коли користувач намагається увійти, маршрутизатор звертається до бази даних зовнішнього сервера, щоб переконатися, що користувач входить за допомогою дійсного імені користувача та пароля.

AAA (Authentication, Authorization, and Accounting) захищає мережу від несанкціонованого доступу, забезпечує контроль над правами доступу користувачів та забезпечує можливість виявлення та реагування на події в мережі для забезпечення безпеки та надійності.

На маршрутизаторів налаштуємо локальну автентифікацією за допомогою AAA. Налаштуємо RADIUS на сервері та використовуємо AAA для автентифікації користувачів на сервері RADIUS.

На рисунку 3.7 на RADIUS-сервер створено базу даних користувачів. Встановлені правила або політики, які визначають, які користувачі мають доступ до мережевих ресурсів.

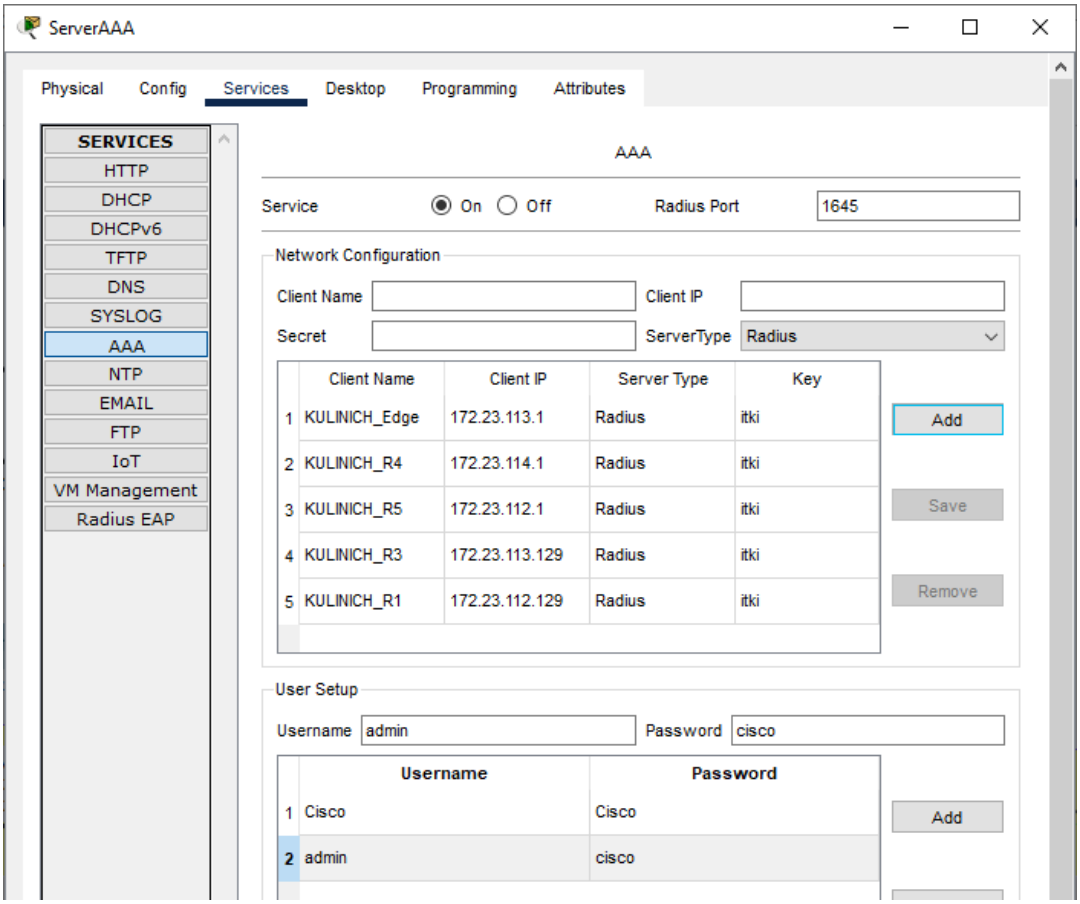

Рисунок 3.7 – Server-AAA захисту

Щоб налаштувати доступ AAA на мережних пристроях, необхідно дотримуватися наступних кроків.

Крок 1. Захист доступу до привілейованого режиму EXEC і конфігурації (enable і enable secret) портів vty, async, aux і tty.

Крок 2. Активувати AAA за допомогою команди aaa new-model.

Крок 3. Встановити конфігурацію профілів автентифікації AAA.

Крок 4. Встановити необхідну конфігурацію засобів авторизації AAA, які використовуються після автентифікації користувача.

Крок 5. Встановити необхідну конфігурацію засобів аудиту AAA щодо форми записів аудиту та їхнього вмісту.

Крок 6. Виконати налагодження та тестування конфігурації.

На листингу 3.9 наведено команди з налаштування служби AAA та доступу до сервера RADIUS за допомогою Cisco IOS. Налаштовано список, щоб спочатку використовувати RADIUS для служби автентифікації, а потім за локальною базою. Якщо сервер RADIUS недоступний і автентифікація не може бути виконана, маршрутизатор буде звертатися до локальної бази. Це запобіжний захід на випадок, якщо маршрутизатор запускається без підключення до активного сервера RADIUS.

Лістинг 3.9 – Налаштування служби aaa та доступу до сервера radius

```
conf t
radius-server host 172.23.112.10
radius-server key itki
aaa new-model
aaa authentication login default group radius local
line console 0
login authentication default
line vty 0 4
login authentication default
```

Вказано IP-адресу сервера RADIUS, ServerAAA (172.23.112.10). Ключ − це секретний пароль, який спільно використовують сервер RADIUS і клієнт RADIUS, який використовується для автентифікації з’єднання між маршрутизатором і сервером перед початком процесу автентифікації користувача.

Тепер можна з будь-якого ПК підєднатися по ssh до маршрутизатора за логіном Cisco, створеним на сервері AAA (рис. 3.8).

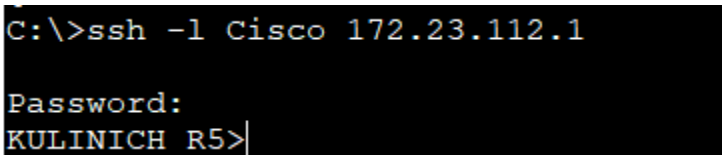

Рисунок 3.8 – Під’єднання по ssh через сервер AAA

Якщо сервер буде недоступний, то авторизація буде за локальним користувачем admin.

3.7.4 Захист від атаки грубої сили або підбору пароля

Зловмисники можуть застосувати до мережного пристрою атаку грубої сили, використовуючи програмне забезпечення для зламу пароля. Ця атака безперервно перебирає усі можливі варіанти пароля, допоки якийсь не спрацює. Для стримування цього типу атаки в лістингу 3.10 наведена команда в режимі глобальної конфігурації на 120 секунд блокуватиме спроби під'єднання до ліній vty, якщо протягом 60 секунд було три невдалих спроби входу.

Лістинг 3.10 – Захист від атаки грубої сили або підбору пароля

```
login block-for 120 attempts 3 within 60
```

3.7.5 Організація безпеки комутаторів

Щоб запобігти атакам переповнення таблиці CAM, необхідно налаштувати безпеку порту, щоб обмежити кількість MAC-адрес, які може вивчати кожен порт комутатора. Якщо кількість MAC-адрес перевищує встановлений ліміт, порт буде вимикатися.

Port Security – це функція канального рівня, яка створена для запобігання несанкціонованої зміни MAC адреси мережевого підключення. Також, дана функція захищає комутатор від атак, які можуть бути спрямовані на переповнення таблиці MAC адрес. В лістингу 3.11 приведено перелік команд для задання захисту на прикладі комутатора SW_LAN4 на порту f0/5, до якого підєднано ServerAAA наведено на рисунку 3.9. Зроблено наступні налаштування:

– налаштувано порт в режимі доступу;

– вімкнено функцію безпеки на порту до якого приєднаний ServerAAA;

– вказано лише 1 пристрій як максимум для доступу до цього порту;

– призначено MAC-адрес ServerAAA статично;

– налаштовано рівень порушення безпеки так, щоб в разі атаки порт залишався включеним, а пакети, що поступають від невідомих джерел відкидались;

– вимкнено всі невикористовувані порти.

Лістинг 3.11 – Налаштувння Port Security

```
interface FastEthernet0/5
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address 0010.112A.124E
switchport port-security violation restrict
interface range f0/15-22
shutdown
```

Перевіримо, чи включено функцію безпеки портів. Відправимо exo-пакет з сервера на шлюз. Як бачимо на рисунку 3.9, він пройшов успішно.

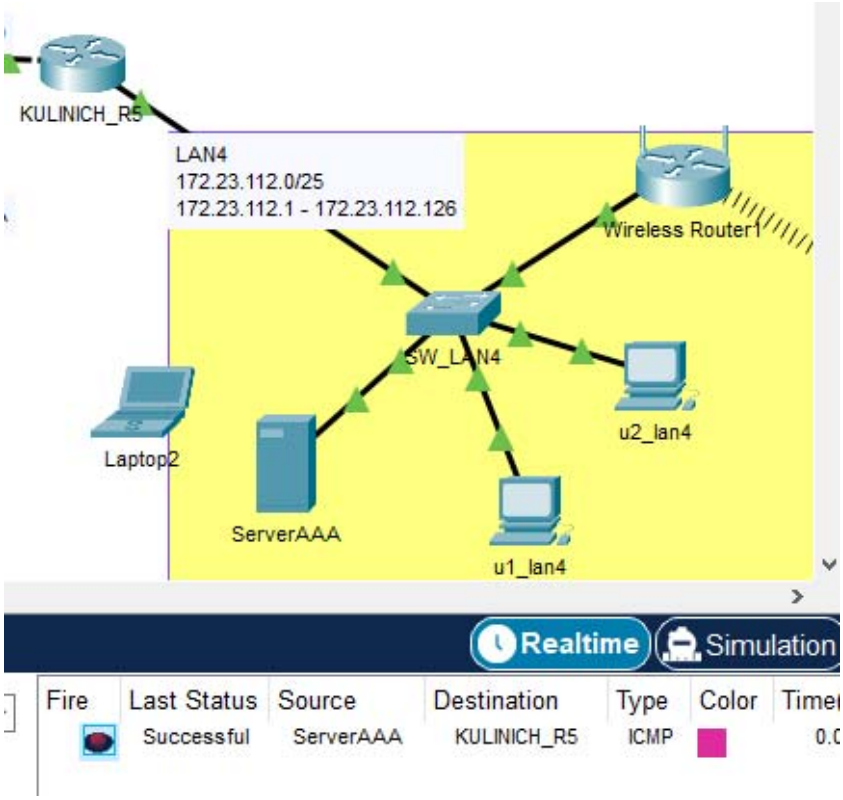

Рисунок 3.9 – Exo-пакет з ServerAAA на KULINICH_R5

Відключмо ServerAAA і підключим сторонній ноутбук, назначаємо йому таку ж IP-адрему, як і на сервері AA та знову відправимо exo-пакет. Як бачимо на рисунку 3.10, пакет відхиллено.

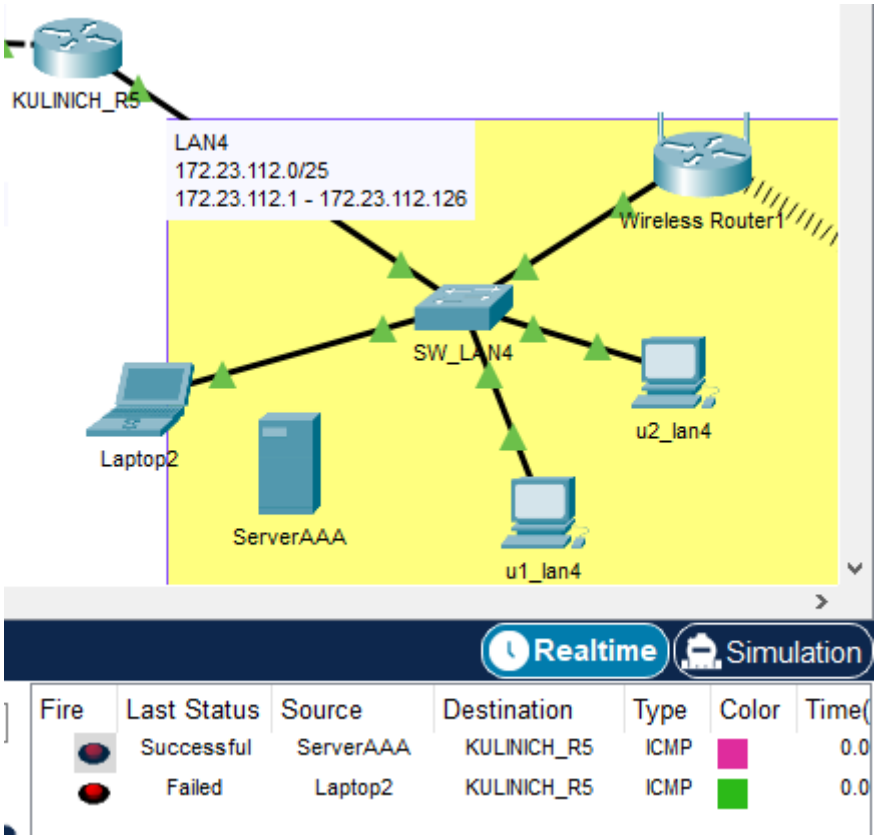

Рисунок 3.10 – Exo-запит з Laptop2

На рис. 3.11 відображено порушення безпеки заблокованого порту.

```
Switch#show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000D.BD95.1A1B:1
Security Violation Count   : 1
```

Рисунок 3.11 – Порушення безпеки заблокованого порту

Відключмо стороннє підключення і знову підключмо ServerAAA. Тепер ServerAAA відправляти exo-запит на вузли в локальній мережі (рис. 3.12).

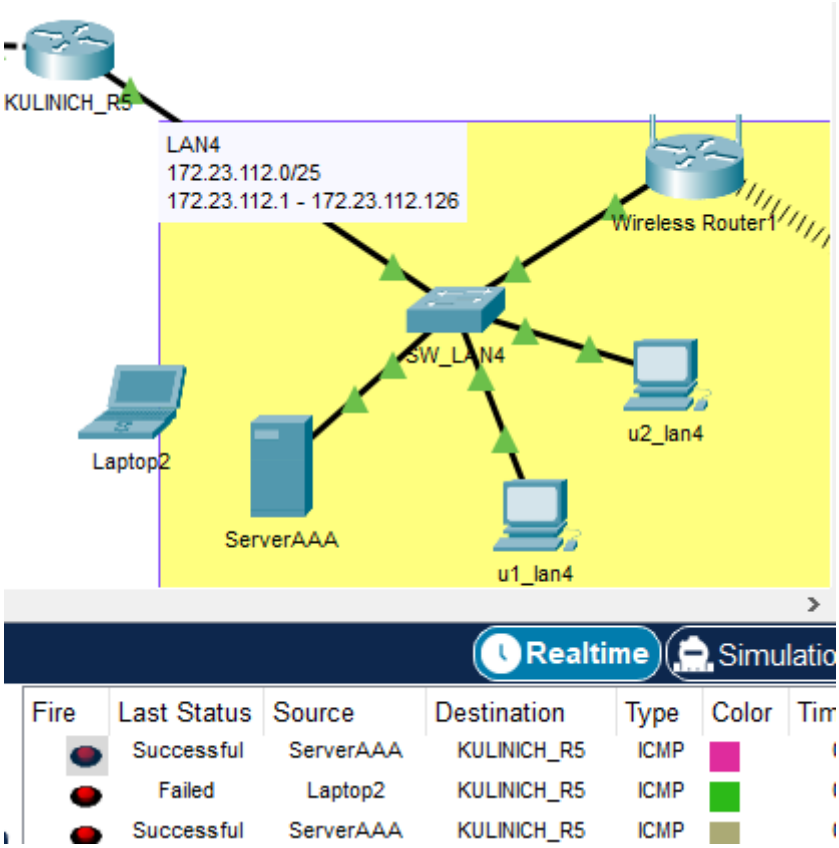

Рисунок 3.12 – Підключено ServerAAA

4 РОЗРОБКА ПІДСИСТЕМИ МОНІТОРИНГУ СТАТИСТИКИ МЕРЕЖНИХ ПОТОКІВ

4.1 Аналіз архітектури протоколу Netflow

Мережний протокол NetFlow – призначений для обліку мережного трафіку, розроблений в 1996 році, він прийшов на заміну CEF, но важливим компонентом залишилась збір статистики. Поняття NetFlow складається з 2-х слів: Net мережа і Flow потік. Відповідно, NetFlow означає мережевий потік. Це поняття застосувала компанія Cisco Systems для своєї технології, використовуваної в операційній системі Cisco IOS. Відповідно до NetFlow протоколом виконується аналіз пакетів, що проходять через певний інтерфейс мережевого пристрою, на основі чого формується інформація в певному форматі про параметри різних мережевих потоків, що проходять через цей інтерфейс, і ця інформація передається по IP мережі спеціальною програмою, NetFlow колектором (NetFlow Collector).

У контексті завдання управління мережею він є незамінним інструментом для моніторингу завантаження каналів передачі даних. Звичайно, протокол NetFlow не може витягувати інформацію безпосередньо з каналу (крученої пари або оптичної лінії) – дані знімаються з пристроїв, підключених до цікавого сегменту. NetFlow підтримується багатьма мережними пристроями: з цього протоколу можуть відправляти інформацію маршрутизатори, комутатори і міжмережні екрани Cisco.

Принцип дії протоколу полягає в наступному. При відкритті чергового сеансу передачі даних на мережевому обладнанні формується інформація про даний сеанс, так званий потік (flow). Відомості про потік включають кількість переданих байтів, вхідний і вихідний інтерфейси для сеансу, IP-адреси відправника/одержувача, порти відправника/одержувача, номер протоколу IP, параметри QoS. Потоки акумулюються на мережевому пристрої і відправляються колектору NetFlow в датаграму UDP. Колектор NetFlow агрегує отриману інформацію, проводить аналіз і формує зручні для

сприйняття звіти і графіки. Один з популярних колекторів NetFlow – NetFlow Analyzer, але існують колектори. Протокол NetFlow дозволяє отримати повну картину трафіку в каналах. Можна переглянути якісний склад трафіку (IP-адреси, порти, додатки) в будь-якому сегменті мережі, а також оцінити, яку частку пропускної здатності каналу (у відсотковому відношенні) займає той чи інший потік.

NetFlow дозволяє пристроям Cisco передавати дані про трафік, що проходить через даний пристрій, на будь-який хост в мережі, де ці дані можуть накопичуватися, зберігатися в певному виді і відповідно відображатися. Таким чином маємо три типи об'єктів, які працюють з NetFlow: сенсор, колектор, аналізатор, що зображено на рис. 4.1.

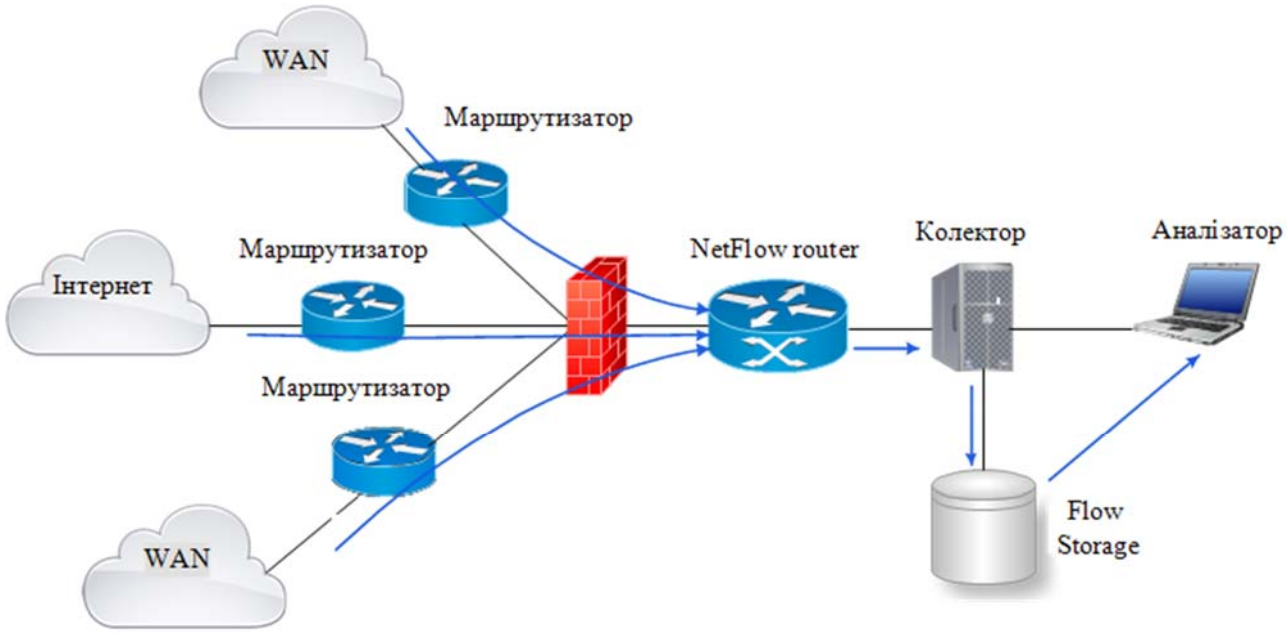

Рисунок 4.1 – Архітектура NetFlow

Для захоплення, передачі та аналізу даних NetFlow слід використовувати наступні компоненти з підтримкою NetFlow:

а) Сенсор (Exporter) збирає статистику трафіка по проходить через нього. Зазвичай це L3 – комутатор або маршрутизатор, хоча можна використовувати і окремі сенсори, які отримують дані шляхом відображення трафіка. Сенсор прослуховує мережу і фіксує дані сеансу. Також як Snort або

будь-яка інша система виявлення вторгнень, сенсор повинен мати можливість підключитися до хабу, переглядати порт комутатора або будь-якого іншого пристрою, для перегляду мережного трафіку. Якщо використовувати систему пакетної фільтрації на базі BSD або Linux, то це чудове місце для сенсора NetFlow, так як весь трафік буде проходити через цю точку. Сенсор буде збирати інформацію про сеанси і скидати її в колектор.

Сенсор, що зображений на рис. 4.2, виділяє з трафіку потоки, які характеризуються наступними параметрами:

– IP адреса джерела даних;

– IP адреса приймача даних;

– порт джерела для UDP і TCP;

– порт призначення для UDP і TCP;

– тип і код повідомлення для ICMP;

– номер протоколу IP;

– мережний інтерфейс (параметр ifindex SNMP);

– IP Type of Service.

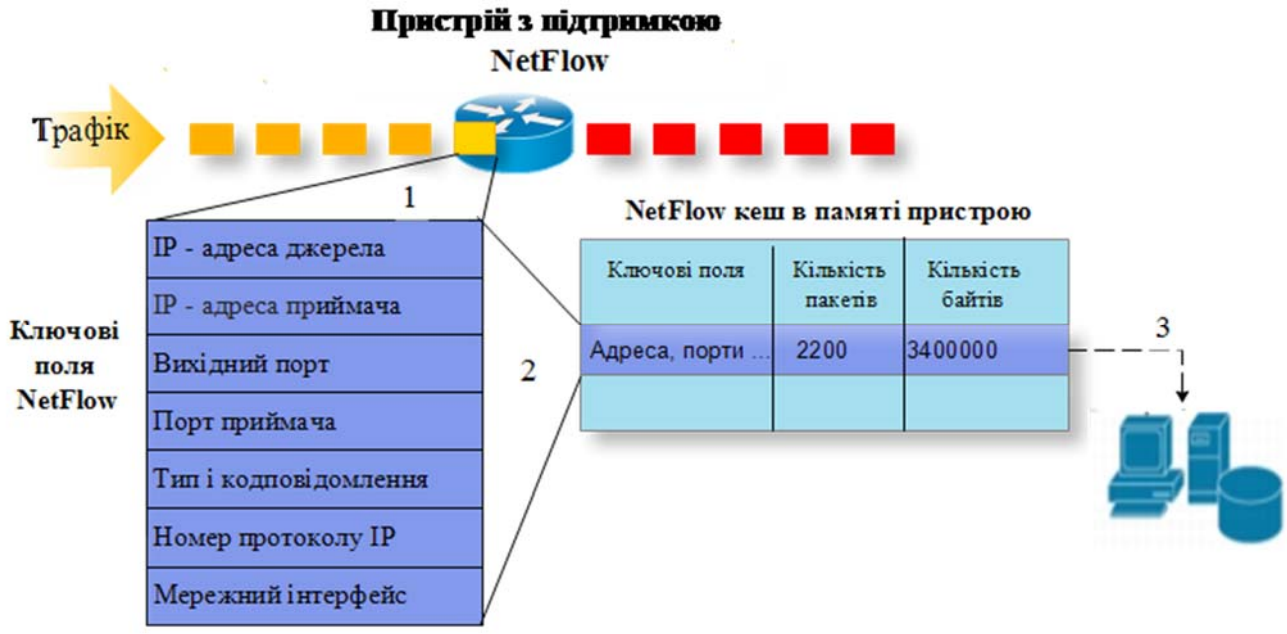

Рисунок 4.2 – Параметри трафіка

Потоком вважається набір пакетів, що проходять в одній області. Коли сенсор визначає, що потік закінчився (за зміною параметрів пакетів), він

відправляє інформацію в колектор. В залежності від налаштувань він також може періодично відправляти в колектор інформацію про все ще поточні потоки.

Перераховані вище поля є ключовими в протоколі NetFlow всіх версій.

б) Колектор відповідальний за збір, фільтрування та зберігання даних. Він включає в себе історію про інформацію про потоки, які були підключені за допомогою інтерфейсу. Зниження обсягу даних також відбувається за допомогою колектора та обраних фільтрів, агрегації. Дані NetFlow періодично надсилаються колектору NetFlow. Колектор – це інший сервер або комп'ютер, на якому запускається програмне забезпечення приймача NetFlow, призначене для збору, запису, фільтрування та аналізу отриманих потоків, таких як PRTG NetFlow Analyzer Paessler. Програмне забезпечення колектора повинно підтримувати ту саму версію NetFlow, що і сервер-експортер. Наприклад, для моніторингу маршрутизатора Cisco з використанням NetFlow v5 потрібно буде використовувати датчик NetFlow v5. Для маршрутизатора, що використовує NetFlow v9, потрібен датчик NetFlow v9. Обидва датчики можуть бути включені на одному комп'ютері одночасно, так що єдиний колектор може отримувати дані з обох версій NetFlow і повідомляти про них. Діаграми NetFlow експортуються за допомогою протоколу обробки користувацьких даних UDP та SCTP. IP-адреса колектора та порт призначення повинні бути налаштовані на маршрутизаторі або самостійно. У деяких випадках SNMP може бути використаний для ввімкнення NetFlow та налаштування IP-адреси колектора для надсилання даних. У Cisco IOS команда ip flow-export може використовуватися для налаштування IP-адреси призначення з командного рядка. Один з найпопулярніших портів, який використовується для експорту NetFlow, становить 2055, але в основному можна використовувати будь – який порт, якщо правильно вказати його в приймачі NetFlow.

в) Аналізатор аналізує зібрані колектором дані і формує придатні для читання людиною звіти (часто у вигляді графіків). NetFlow Analyzer – це просте рішення для адміністраторів, щоб краще розуміти споживання смуги

пропускання, тенденції трафіку, додатки, хости і аномалії трафіку, візуалізувати трафік за допомогою мережевих пристроїв, інтерфейсів і підмереж, сегментів трафіку і кінцевих користувачів. NetFlow Analyzer використовує Cisco NetFlow, IPFIX, sFlow і сумісні NetFlow подібних протоколи, щоб допомогти адміністратором з контролем смуги пропускання, дослідженням мережевого трафіку, аналіз і звітністю. Це дозволяє оптимізувати свої мережі і додатки, планувати розширення мережі, економити час, необхідний для усунення неполадок і діагностики, а також підвищити безпеку – в свою чергу, значно знижуючи операційні витрати і підвищуючи продуктивність мережної команди.

4.2 Налаштування Netflow на мережному пристрої

NetFlow – це технологія Cisco IOS, яка надає статистику пакетів, що проходять через маршрутизатор. NetFlow є стандартом для отримання робочих даних IP з IP-мереж. NetFlow надає дані для моніторингу мережі та безпеки, мережевого планування, аналізу трафіку та обліку IP.

Flexible NetFlow покращує оригінальний NetFlow, додаючи можливість налаштовувати параметри аналізу трафіку відповідно до конкретних вимог. Flexible NetFlow полегшує створення більш складних конфігурацій для аналізу трафіку та експорту даних за допомогою багаторазових компонентів конфігурації.

Граничний маршрутизатор KULINICH_Edge буде виконувати роль експортера потоку NetFlow. KULINICH_Edge для моніторингу потоків, які вийшли з локальної мережі, збиратиме весь вхідний трафік на інтерфейсах во внутрішні мережі (F0/1, s0/0/1 та Eth0/1/0) та з зовнішньої мережі Internet (s0/0/0) і експортуватиме дані на ПК NetFlow Analyse на IP-адресу 172.23.113.9. Для експорту даних на збірник NetFlow буде використовувати версію 9 NetFlow. Записи NetFlow експортуються до збирача Netflow за допомогою протоколу UDP на порт 9996.

Flexible Netflow надає можливість налаштовувати параметри аналізу трафіку. Конфігурація для Flexible Netflow на пристрої Cisco складається з чотирьох кроків:

Крок 1. Створення записів потоку (Flow record).

Крок 2. Налаштування експортера потоку (Flow exporter).

Крок 3. Налаштування монітора потоку (Flow monitor).

Крок 4. Застосування монітора потоку до інтерфейсу (Flow Sampler).

4.2.1 Створення записів потоку

Запис потоку визначає інформацію, яку збирає NetFlow, наприклад пакети в потоці та типи лічильників, зібраних для кожного потоку. Якщо необхідно створити спеціальний запис потоку поза попередньо визначеним netflow-original, налаштовується серія команд match і collect, які повідомляють пристрою, які поля слід включити до вихідного NetFlow PDU. Поля match є ключовими полями. Вони використовуються для визначення унікальності потоку. Поля collect – це лише додаткова інформація, яку додаємо, щоб надати більше деталей Flow Collector для звітів і аналізу.

В Додатку А сім записів match потоку rec1, які рекомендовано завжди включати в конфігурацію. Однак поля збору collect можуть значно відрізнятися залежно від того, скільки інформації надсилається збирачу.

4.2.2 Налаштування експортера потоку

Експортуватимуться інформація про потоки на ПК NetFlow Analyse на IP-адресу 172.23.113.9 за допомогою протоколу UDP на порт 9996.

В Додатку А наведено налаштування відомостей про експортера потоку.

4.2.3 Налаштування монітора потоку

Flow Monitor пов’язує всю конструкцію разом, посилаючись на Flow Exporter і Flow Record.

Монітор потоку (Flow monitor) – компонент, який використовується для забезпечення фактичного моніторингу трафіку на налаштованому інтерфейсі. Коли монітор потоку застосовується до інтерфейсу, створюється кеш монітора потоку, який використовується для збору трафіку на основі ключових (key) та неключових (nonkey) полів у налаштованому записі.

В Додатку А наведено налаштування монітора потоку.

На рис. 4.3 наведено результат перевірки налаштування монітора потоку.

```
KULINICH_Edge#show flow monitor
Flow Monitor FLOWMON
  Description:       User defined
  Flow Record:       rec1
  Flow Exporter:     myFlow
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 163852 bytes
    Inactive Timeout:  15 seconds
    Active Timeout:    1800 seconds
    Update Timeout:    1800 seconds
```

Рисунок 4.3 – Перевірка налаштування монітора потоку

4.2.4 Застосування монітора потоку до інтерфейсу

Останнім кроком необхідно налаштувати відповідні інтерфейси для кешування введення або виведення, пов’язаного з відповідним монітором потоку.

KULINICH_Edge збиратиме весь вхідний трафік на інтерфейсах во внутрішні мережі (F0/1, s0/0/1 та Eth0/1/0) та з зовнішньої мережі Internet (s0/0/0) і експортуватиме дані на ПК NetFlow Analyse на IP-адресу 172.23.113.9.

В Додатку А наведену конфігурацію NetFlow до кожного інтерфейсу, на якому виконується аналіз потоку:

На рис. 4.4 наведено результат перевірки налаштування монітора потоку до інтерфейсів.

```
KULINICH_Edge#show flow interface
Interface Ethernet0/1/0
FNF:  monitor:            FLOWMON
      direction:          Input
      traffic(ip):        on
Interface FastEthernet0/1
FNF:  monitor:            FLOWMON
      direction:          Input
      traffic(ip):        on
Interface Serial0/0/0
FNF:  monitor:            FLOWMON
      direction:          Input
      traffic(ip):        on
Interface Serial0/0/1
FNF:  monitor:            FLOWMON
      direction:          Input
      traffic(ip):        on
KULINICH_Edge#
```

Рисунок 4.4 – Перевірка налаштування монітора потоку до інтерфейсів

4.3 Тестування системи моніторингу статистики мережних потоків

Відкриємо експортер потоку ПК NetFlow Analyse і на вкладці Desktop (Робочий стіл) натиснемо піктограму NetFlow Collector, яку зображено на рисунку 4.5.

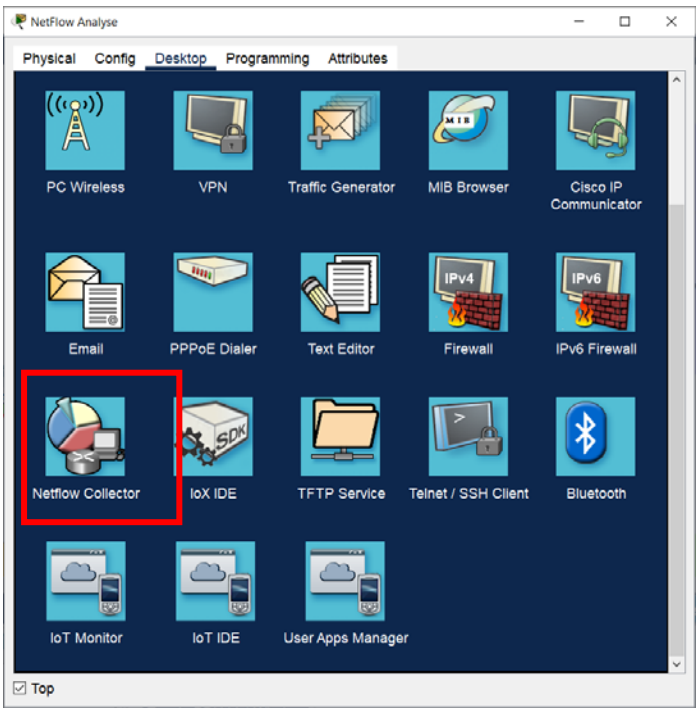

Рисунок 4.5 – Додаток NetFlow Collector

Після активації засобу збору даних на екрані засобу збору даних NetFlow відображається кругова діаграма. У записі потоку будуть поля, представлені у табл. 4.1.

Таблиця 4.1 – Інформація та опис пакетів

Початковий рівень	Опис
Розподіл трафіку	Це частка всього трафіку, представленого цим потоком.
IPv4-адреса джерела	Це IP-адреса джерела пакетів потоку.
IPv4-адреса призначення	Це IP-адреса призначення пакетів потоку.
Порт джерела trns	Це порт джерела транспортного рівня. Значення дорівнює 0, якщо це потік ICMP.
Порт призначення trns	Це порт призначення транспортного рівня. Значення дорівнює 0, якщо це потік ICMP.
IP-protocol	Він визначає службу 4-го рівня, зазвичай це 1 для ICMP, 6 для TCP, 17 для UDP.
Перша мітка часу	Це мітка часу для початку потоку.
Остання мітка часу	Це позначка часу для останнього пакета в потоці.
Флаги tcp	Це значення прапора TCP.
Лічильник байтів	Це кількість байтів у потоці.
Лічильник пакетів	Це кількість пакетів у потоці.
Вхід інтерфейсу	Це інтерфейс експортера потоку, який зібрав потік у вхідному напрямку (вхід до інтерфейсу пристрою моніторингу).
Вихідний інтерфейс	Це інтерфейс експортера потоку, який зібрав потік у вихідному напрямку (вихід із інтерфейсу пристрою моніторингу). Значення Null, оскільки це був ехо-запит на вхідний інтерфейс.

Потік визначається як односпрямований потік пакетів з однаковими IP-адресами та номерами портів джерела та призначення, а також одним IP-протоколом. Створимо сценарії трафіку, який буде поступати на інтерфейси KULINICH_Edge. Кожен сценарій матиме іншу IP-адресу джерела та призначення, тому буде створено новий запис потоку, представлений новим сегментом кругової діаграми з колірним кодуванням.

Сценарій 1: ехо-запити з ПК «u1_lan2» в LAN2 на шлюз за замовчуванням. На час тестування ПК мав IP-адресу 172.23.113.14 по DHCP. В потоці було чотири ехо-пакети. Пакети надійшли на інтерфейс експортера

e0/1/0 (рис. 4.6). Якщо повторно відправити ехо-запит на шлюз, то новий запис не з’явиться, а статистика збільшиться (рис. 4.7).

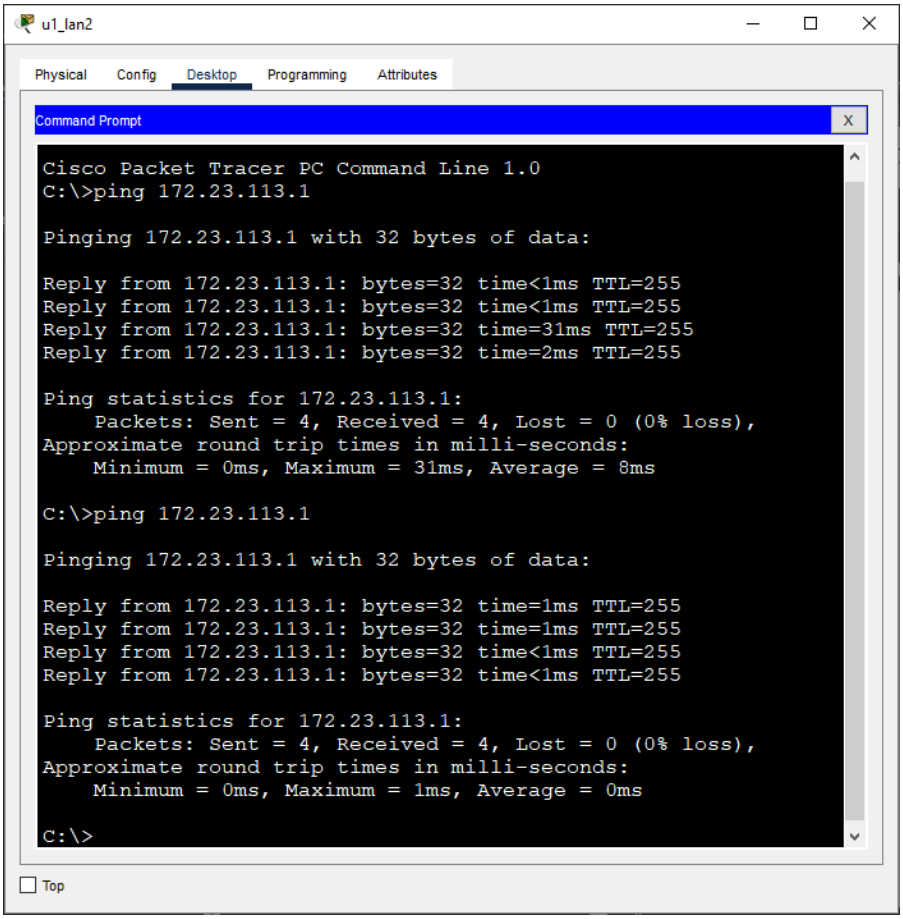

Рисунок 4.6 – Ехо-запити

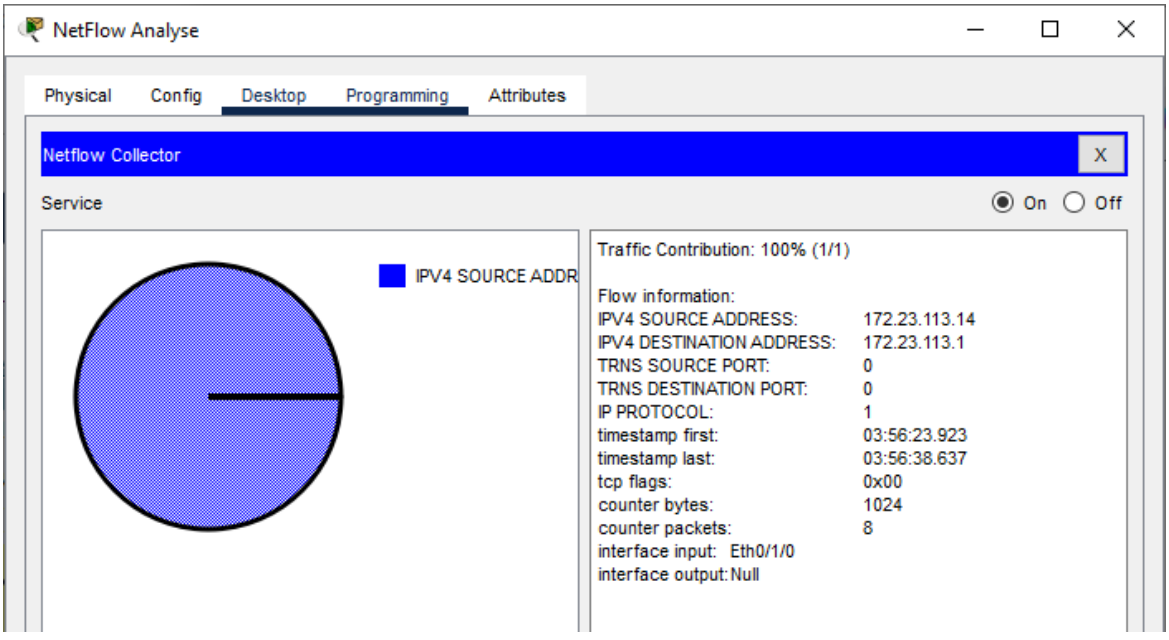

Рисунок 4.7 – Отримані аналізатором ехо-пакети

Сценарій 2: створимо додатковий трафік. Відправімо ехо-пакети з ПК «u2_lan2», який має IP-адресу 172.23.113.11 на шлюз за замовчуванням 172.23.113.1. Потік визначається як одно-направлений потік пакетів з однаковими IP-адресами та номерами портів джерела та призначення, а також одним IP-протоколом. Цей трафік матиме іншу IP-адресу джерела, тому буде створено новий запис потоку, представлений новим сегментом кругової діаграми з кольоровим кодуванням (рис. 4.2).

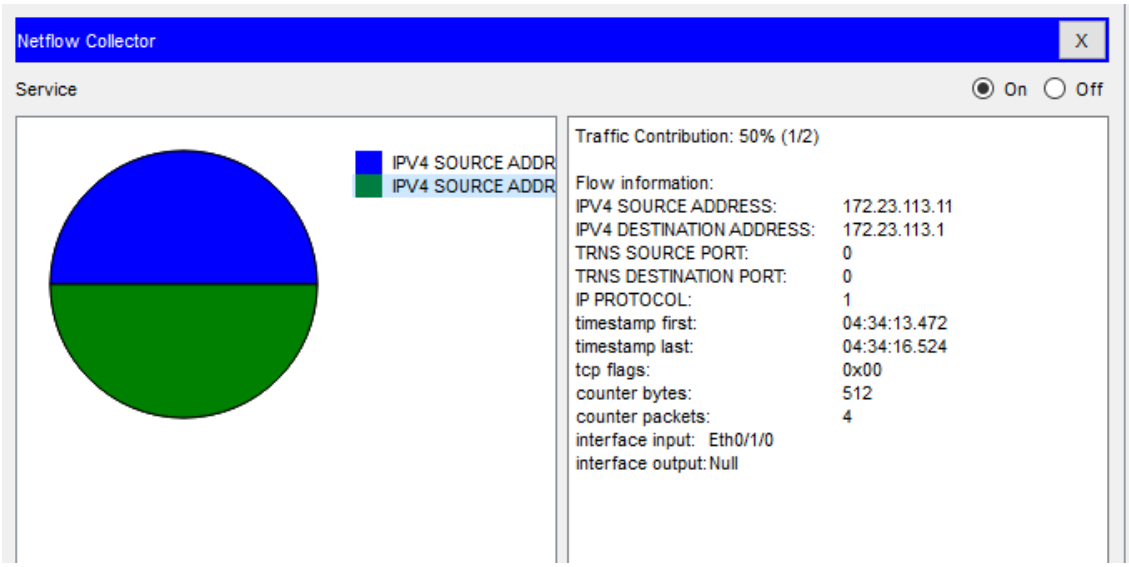

Рисунок 4.8 – Отримані додаткові ехо-пакети

Таблиця 4.2 – Статистика потоків

Початковий рівень	Сценарій 1	Сценарій 2
Розподіл трафіку	50 % (1/2)	50 % (1/2)
IPv4-адреса джерела	172.23.113.14	172.23.113.11
IPv4-адреса призначення	172.23.113.1	172.23.113.1
Порт джерела trns	0	0
Порт призначення trns	0	0
IP-protocol	1	1
Перша мітка часу	04:48:18.289	04:48:28.428
Остання мітка часу	04:48:26.044	04:48:31.437
Флаги tcp	0x00	0x00
Лічильник байтів	1024	512
Лічильник пакетів	8	4
Вхід інтерфейсу	Eth0/1/0	Eth0/1/0
Вихідний інтерфейс	Null	Null

Сценарій 3: створимо новій потік, який буде представляти email-трафік. На ПК u1_lan5, на якому створено користувача з email «user2@erjib.com» відкриємо вкладку Desktop (Робочий стіл), натиснемо піктограму Email, яку зображено на рисунку 4.9 та натиснемо на кнопку «Compose», зображену на рис. 4.10.

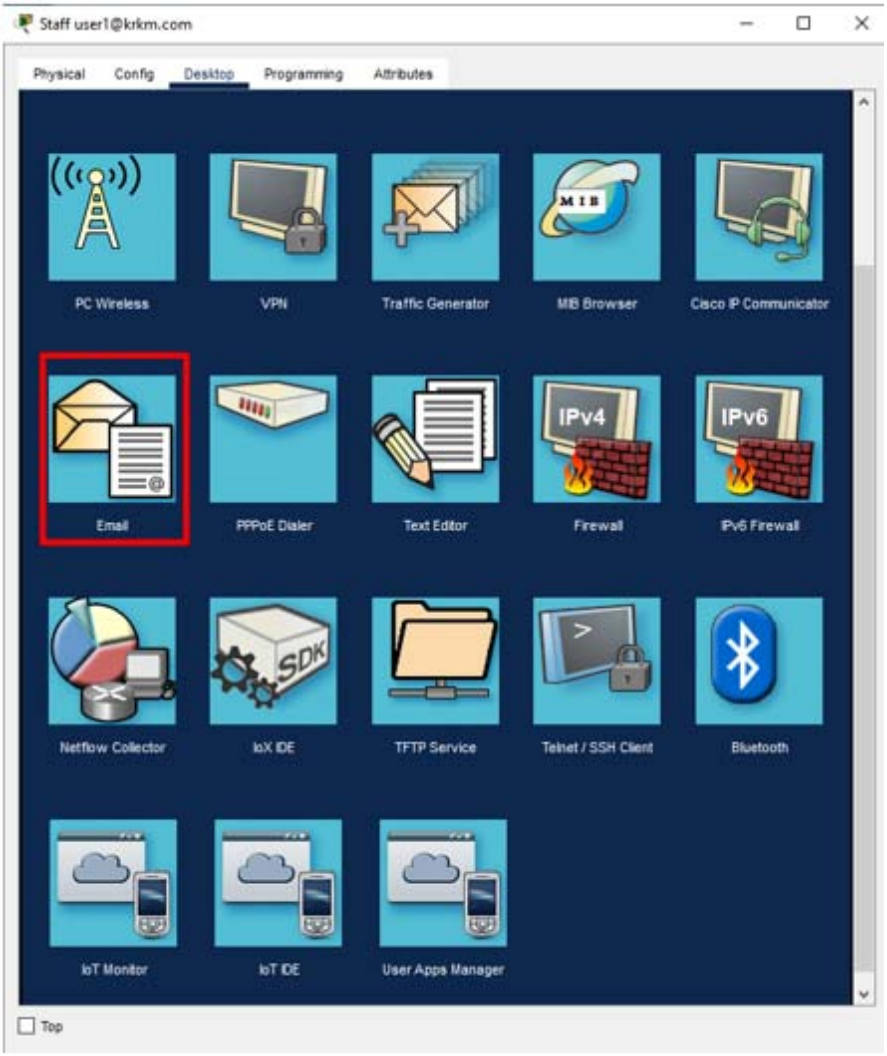

Рисунок 4.9 – Додаток Email

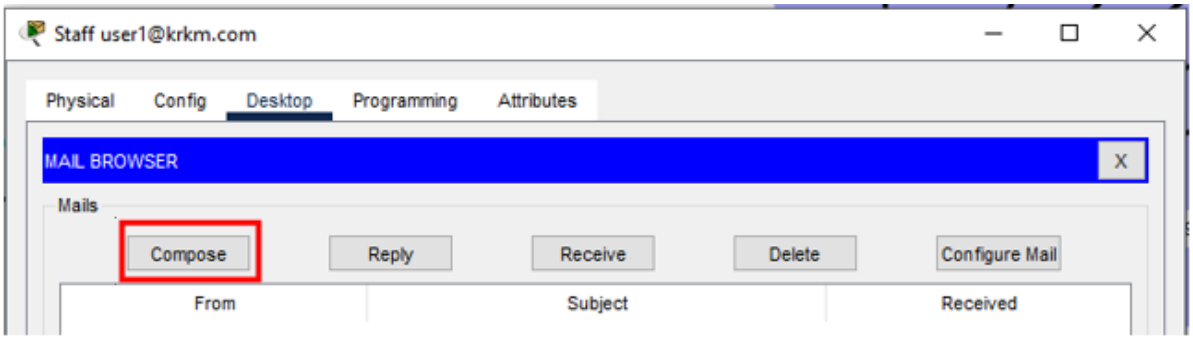

Рисунок 4.10 – Створення нового повідомлення

Створимо Email повідомлення, яке буде надіслано користувачу в LAN1 user1@erjib.com від користувача user2@erjib.com, для цього вводимо отримувача повідомлення у поле «To:» та вводимо бажану тему у поле «Subject» та текст повідомлення у порожнє поле. Для відправки повідомлення натиснемо кнопку «Send», яку зображено на рис. 4.11.

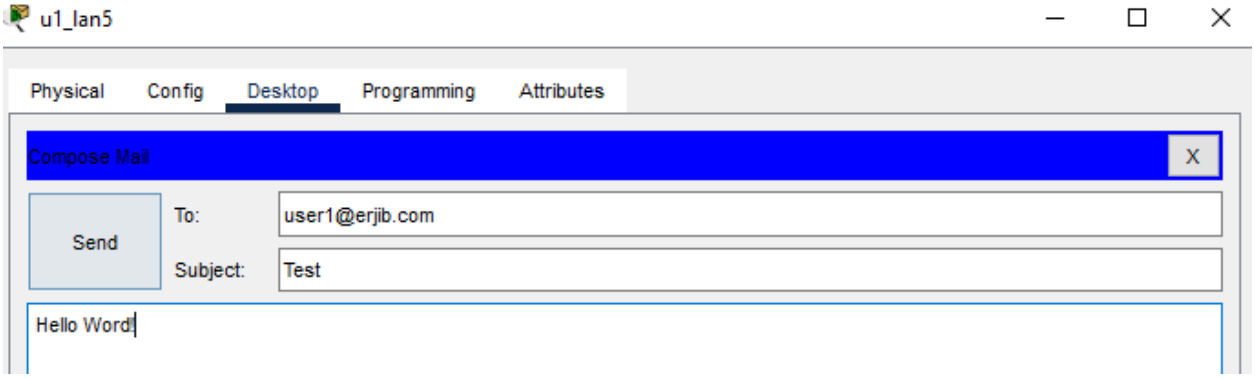

Рисунок 4.11 – Відправлення створеного повідомлення

Для надсилання вихідної пошти використовується порт TCP 25. Цей трафік матиме іншу IP-адресу джерела та призначення, тому буде створено новий запис потоку, представлений новим сегментом кругової діаграми з кольоровим кодуванням (рис.4.12 та рис.4.13)

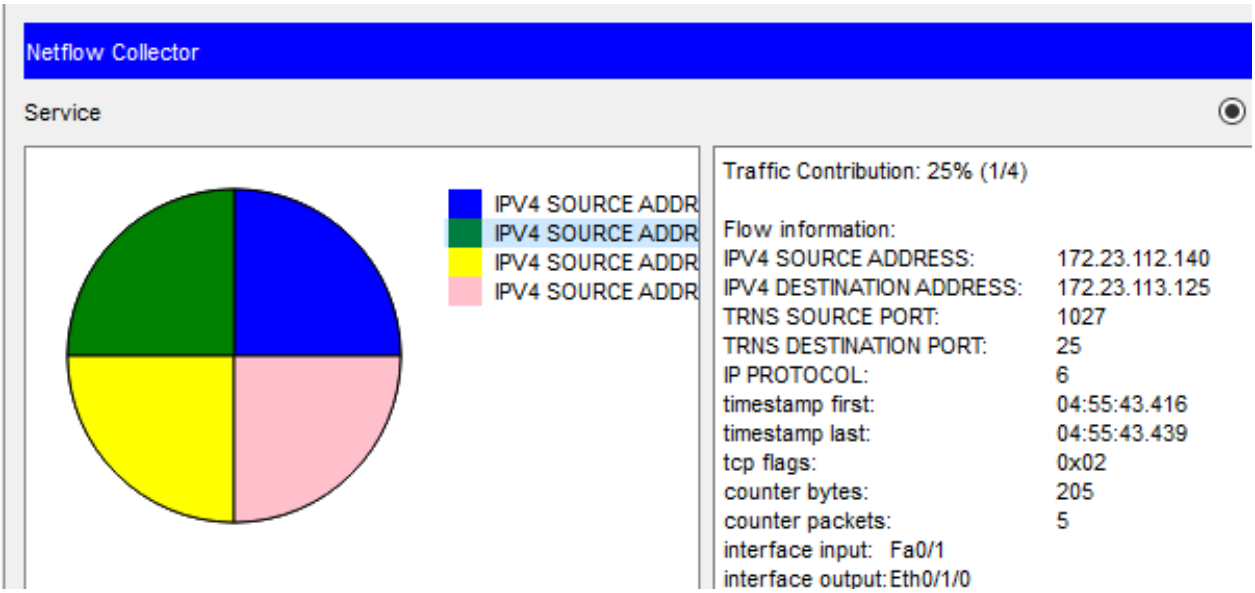

Рисунок 4.12 – Потік трафіку надсилання на SMTP-сервер (порт 25)

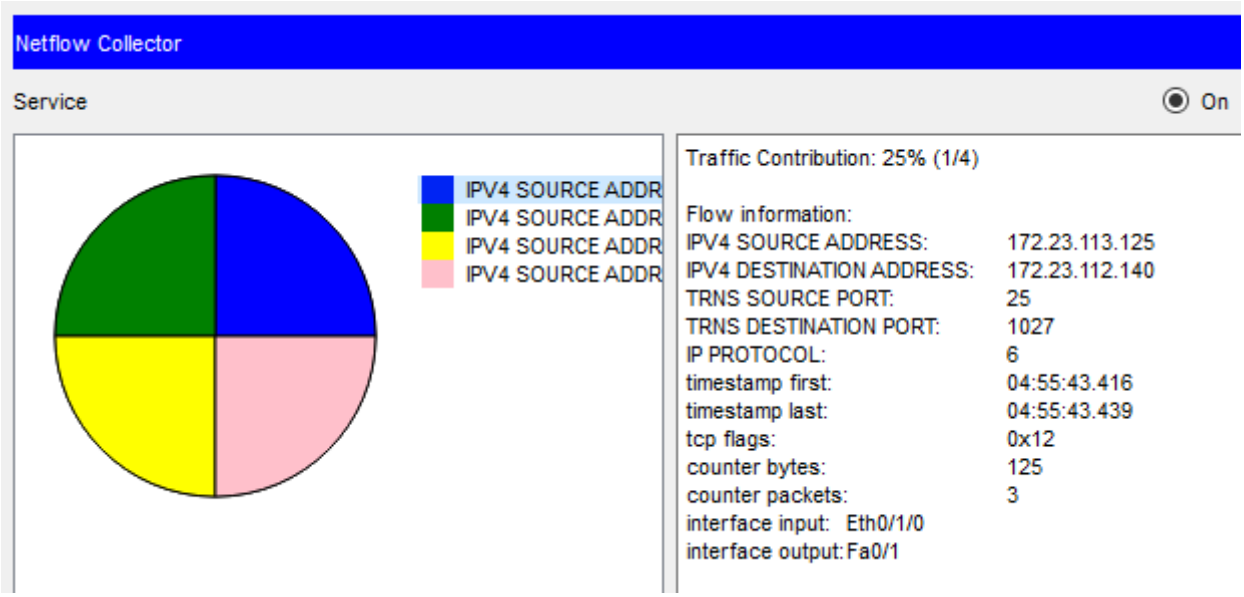

Рисунок 4.13 – Потік трафіку відповіді з SMTP-сервера (порт 25)

Для отримання повідомлення користувачу user1@erjib.com треба вибрати піктограму Email у вкладці Desktop та натиснути «Recieve» (рис. 4.14) для перегляду останніх отриманих повідомлень.

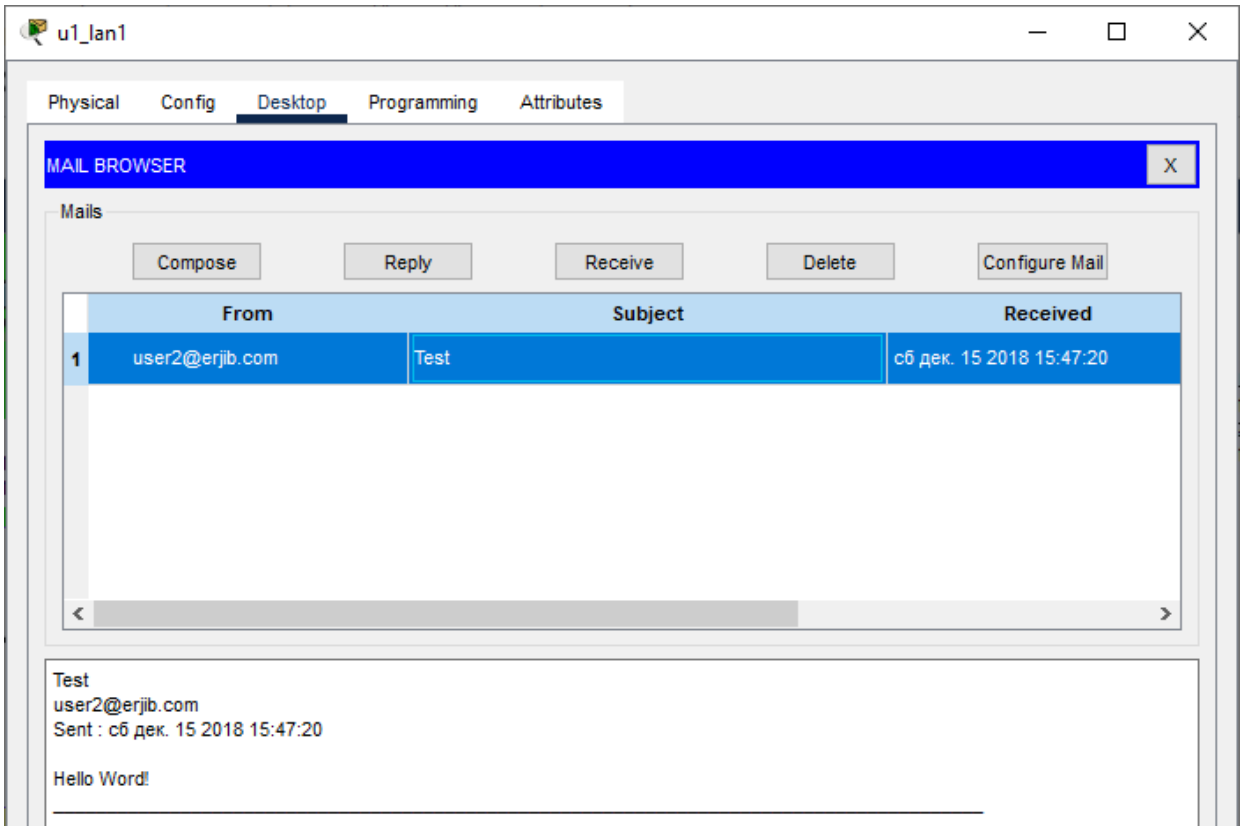

Рисунок 4.14 – Отримання нових повідомлень

У цьому розділі також можна побачити тему повідомлення, адресу відправника, дату відправлення та текст повідомлення.

Відкриємо експортер потоку ПК NetFlow Analyse і на вкладці Desktop (Робочий стіл) натиснемо піктограму NetFlow Collector, яку зображено на рис. 4.15. Діаграма буде оновлена, і на ній з'являться ще два нових пакета трафіку, отриманих аналізатором. Оновлена статистика мережного трафіку можна побачити в табл. 4.3.

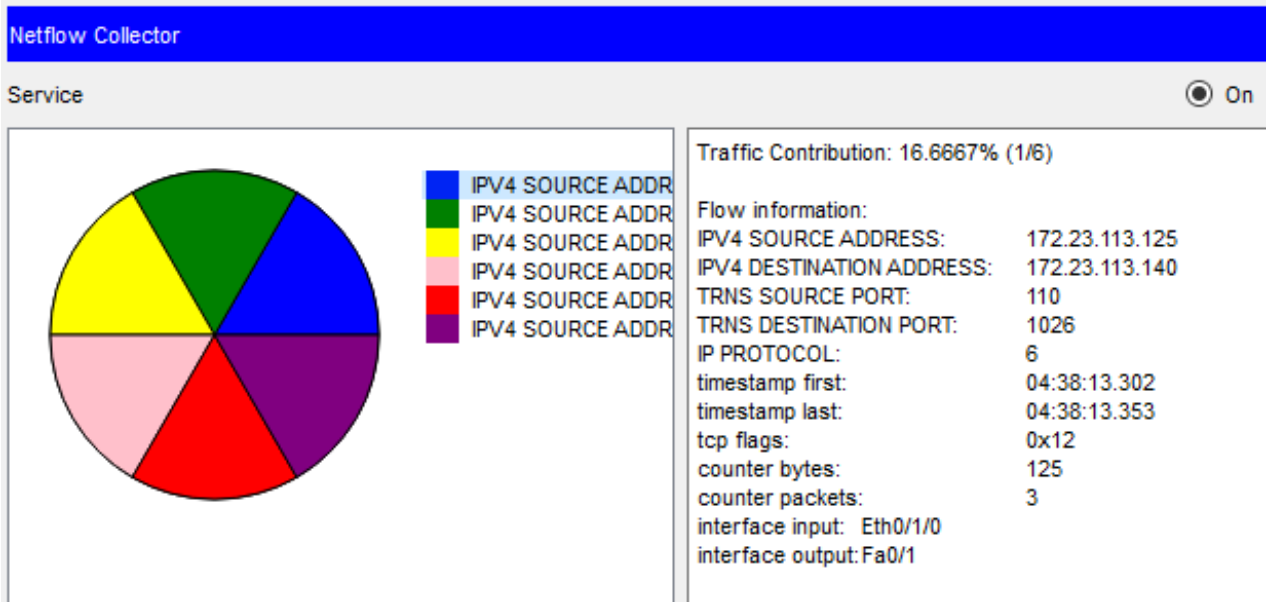

Рисунок 4.15 – Нові пакети трафіку

Використання NetFlow дає змогу застосовувати отриманні дані для подолання типових проблем, з якими стикаються системні адміністратори, зокрема:

– моніторинг основних учасників мережевого трафіку;

– розуміння трафіку програми та його впливу на мережу;

– усунення несправностей і розуміння точок перевантаження мережі;

– виявлення несанкціонованого трафіку WAN;

– DDoS і виявлення аномалій;

– перевірка параметрів QoS.

Таблиця 4.3 – Статистика потоків

Початковий рівень	Сценарій 1	Сценарій 2	Сценарій 3			
Розподіл трафіку	16.6667% (1/6)	16.6667% (1/6)	16.6667% (1/6)	16.6667% (1/6)	16.6667% (1/6)	16.6667% (1/6)
IPv4-адреса джерела	172.23.113.14	172.23.113.11	172.23.113.125	172.23.113.140	172.23.113.125	172.23.112.140
IPv4-адреса призначення	172.23.113.1	172.23.113.1	172.23.113.140	172.23.113.125	172.23.112.140	172.23.113.125
Порт джерела trns	0	0	110	1027	25	1027
Порт призначення trns	0	0	1027	110	1027	25
IP-protocol	1	1	6	6	6	6
Перша мітка часу	04:48:18.289	04:48:28.428	05:02:02.643	05:02:02.643	04:55:43.416	04:55:43.416
Остання мітка часу	04:48:26.044	04:48:31.437	05:02:02.674	05:02:02.674	04:55:43.439	04:55:43.439
Флаги tcp	0x00	0x00	0x12	0x02	0x12	0x12
Лічильник байтів	1024	512	125	205	125	205
Лічильник пакетів	8	4	3	5	3	5
Вхід інтерфейсу	Eth0/1/0	Eth0/1/0	Eth0/1/0	Fa0/1	Eth0/1/0	Fa0/1
Вихідний інтерфейс	Null	Null	Fa0/1	Eth0/1/0	Fa0/1	Eth0/1/0

Консолідований аналіз трафіку NetFlow може зменшити кількість апаратних і програмних технологій, необхідних для керування мережами, знизити витрати на адміністрування мережі та покращити міжорганізаційну співпрацю та комунікації.

ВИСНОВОК

У кваліфікаційній роботі бакалавра за темою «Комп’ютерна система ТОВ «ЕР ДЖІ БІ» з детальною реалізацією побудови та налаштування корпоративної мережі» були розглянуті основні компоненти локальної мережі, а також процес передачі даних в мережі на всіх рівнях (логічному і апаратному).

Локальна комп'ютерна система мережі підприємства ТОВ «ЕР ДЖІ БІ» спроектована з урахуванням вимог майбутньої структури розвитку підприємства. Залежно від розмірів приміщення була підібрана і максимально оптимізована довжина з'єднувального кабелю для всіх компонентів мережі. На сьогоднішній день розробка та впровадження комп'ютерної системи ТОВ «ЕР ДЖІ БІ» є важливим ІТ-завданням підприємства, так як постійно зростає потреба в контролі інформації в режимі реального часу, а мережевий трафік на всіх рівнях постійно і незупинна збільшується, з’являються нові технології передачі інформації в локальній мережі.

В розділі розробки корпоративної мережі було проведено моделювання комп’ютерної мережі в програмі Cisco Packet, виконані базові налаштування, доступ до Інтернет, маршрутизація по протоколу OSPF. Перевірено функціональність впроваджених служб та протоколів. Розроблені конкретні рекомендації та практичні поради щодо захисту комп'ютерних мереж з використанням обладнання Cisco. Ці рекомендації стануть у нагоді організаціям, які прагнуть захистити свої мережі від загроз і зберегти дані в безпеці.

Розроблено комплект документації для програмного забезпечення комп'ютерної мережі для комп’ютерної системи ТОВ «ЕР ДЖІ БІ».

Розроблена система моніторингу статистики мережних потоків по протоколу NetFlow. Це ефективний інструмент для контролю та аналізу трафіку у комп'ютерних мережах. Проведено експерименти з різними сценаріями трафіку для перевірки працездатності системи моніторингу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) ТОВ "ЕР ДЖІ БІ". Режим доступу: https://leadscanner.com.ua/company/44338678

2) Про нас. Режим доступу: https://rgbweb.studio/about/

3) Міжнародний консалтинг в Україні. Режим доступу: https://accounting-outsourcing.com.ua/uk

4) Протокол NetFlow [Електронний ресурс] – Режим доступу до ресурсу: https://the-purple.team/netflow_protocol/.

5) NetFlow, Cisco и мониторинг трафика [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/articles/175359/.

6) Протоколи збору трафіку: SNMP, Netflow, IPFIX, sFlow, JFlow [Електронний ресурс] – Режим доступу до ресурсу: https://the-purple.team/протоколи-збору-трафіку-snmp-netflow-ipfix-sflow-jflow/.

7) Как настроить мониторинг трафика с помощью NetFlow на маршрутизаторе Cisco [Електронний ресурс] – Режим доступу до ресурсу: https://blog.sedicomm.com/2021/08/27/kak-nastroit-monitoring-trafika-s-pomoshhyu-netflow-na-marshrutizatore-cisco/.

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ ПРОТОКОЛУ NETFLOW НА МАРШРУТИЗАТОРІ EDGE

Текст програми

804.02070743.23009-01 12 01

Листів 4

2023

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування експорту даних на збірник Flexible NetFlow версії 9 за допомогою протоколу UDP на порт 9996.

Flexible Netflow надає можливість налаштовувати параметри аналізу трафіку. Конфігурація для Flexible Netflow на пристрої Cisco складається з чотирьох кроків.

Крок 1. Створення записів потоку (Flow record).

Крок 2. Налаштування експортера потоку (Flow exporter).

Крок 3. Налаштування монітора потоку (Flow monitor).

Крок 4. Застосування монітора потоку до інтерфейсу (Flow Sampler).

ЗМІСТ стор**.**

1. Налаштування записів потоку rec1

```
flow record rec1
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match ipv4 protocol
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect transport tcp flags
 collect counter bytes
 collect counter packets
 collect interface input
 collect interface output
```

2. Налаштування експортера потоку

```
flow exporter myFlow
 destination 172.23.113.9
 transport udp 9996
```

3. Налаштування монітора потоку

```
flow monitor FLOWMON
 record rec1
 exporter myFlow
ip flow-export version 9
```

4. Застосування монітора потоку до інтерфейсу

```
interface FastEthernet0/1
 ip flow monitor FLOWMON input
!
interface Serial0/0/1
 ip flow monitor FLOWMON input
!
interface Ethernet0/1/0
 ip flow monitor FLOWMON input
```