

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Комп'ютерних наук та технологій

(повне найменування факультету)

Комп'ютерних систем та мереж

(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту(роботи)

магістра

(ступінь вищої освіти)

на тему: СИСТЕМА ІНФОРМАЦІЙНОГО ОБМІНУ В ТОРГОВО-
ЛОГІСТИЧНОМУ ЦЕНТРІ

Виконав: студент 2 курсу, групи КНТ-612м

Спеціальності 123 «Комп'ютерна інженерія»

(код і найменування спеціальності)

Освітня програма (спеціалізація)

«Спеціалізовані комп'ютерні системи»

РЕНГЕВИЧ Д.С.

(ПРИЗВИЩЕ та ініціали)

Керівник МР

ЗЕЛЕНЬОВА І.Я.

(ПРИЗВИЩЕ та ініціали)

Рецензент від закладу вищої освіти

СТЕПАНЕНКО О.О.

(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет Комп'ютерних наук і технологій
Кафедра «Комп'ютерні системи та мережі»
Ступінь вищої освіти магістерський
Спеціальність 123 Комп'ютерна інженерія
(код і найменування)
Освітня програма (спеціалізація) «Спеціалізовані комп'ютерні системи»
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ
Зав. кафедри Кудерметов Р.К.

“ ” 2023 року

**ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА**

РЕНГЕВИЧУ Данилу Сергійовичу

1. Тема проєкту (роботи) Система інформаційного обміну в торгово-логістичному центрі
керівник проєкту (роботи) Зеленьова І. Я. к.т.н., доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від «24» жовтня 2023 року № 400

2. Строк подання студентом проєкту (роботи) 13 грудня 2023 року

3. Вихідні дані до проєкту (роботи) дротові мережі, бездротові мережі, вита пара, оптоволоконна мережа, WI-FI 5, WI-FI 6

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1) Використання оптоволоконної мереж

2) Використання бездротової мережі

3) Заходи з підвищення надійності мереж підприємства

4) Дослідження дротових та бездротових мереж

5) Практичні рекомендації щодо організації і використанню підмереж у складі систем інформаційного обміну

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

6. Консультанти розділів проєкту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видала	прийняла виконане завдання
1-4	ЗЕЛЕНЬОВА І.Я., доцент		
нормоконтроль	ЩЕРБАК Н.В., ст. викл.		

7. Дата видачі завдання 01.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз наявних методів та алгоритмів пошуку об'єктів, перегляд отриманих результатів, виділення недоліків та переваг	05.09.2023 р.	
2	Розробка структури мережі	08.10.2023 р.	
3	Розробка алгоритму роботи мережі	04.10.2023 р.	
4	Використання роботи мережі	01.11.2023 р.	
5	Дослідження роботи мережі	09.11.2023 р.	
6	Оформлення отриманих результатів у ПЗ	10.11.2023 р.	
7	Оформлення графічного матеріалу	15.11.2023 р.	
8	Оформлення допоміжного матеріалу	20.11.2023 р.	

Студент

Керівник проєкту(роботи)



Данило РЕНГЕВИЧ

Ірина ЗЕЛЕНЬОВА

РЕФЕРАТ

ПЗ: 58 с., 13 рис., 5 табл., 8 посилань.

БЕЗДРОТОВА МЕРЕЖА, ВИТА ПАРА, ДРОТОВА МЕРЕЖА, ОПТОВОЛОКОННА МЕРЕЖА, WI-FI 5, WI-FI 6

Об'єктом дослідження є система інформаційного обміну в торгово - логістичному центрі.

Предметом дослідження є дротові та бездротові операційні мережі, які служать для обміну інформацією в торгово-логістичному центрі.

Основною метою цього дослідження є огляд дротових та бездротових технологій, розробка дротових та бездротових підмереж та заходи з підвищення загальної надійності мережі підприємства.

В першому розділі був зроблен огляд дротових та бездротових мереж, розглянута структура підприємства та розглянуті задачі для забезпечення умов стійкості на підприємстві.

В другому розділі була проведена розробка складових загальної мережі інформаційного обміну, були зроблені заходи з підвищення надійності мережі підприємства.

В третьому розділі було проведено тестування і дослідження складових загальної мережі підприємства, також були дані практичні рекомендації щодо організації і використання підмереж у складових системи інформаційного обміну.

ABSTRACT

Explanatory note to the master's work: 58 p., 13 figures, 5 tables, 8 sources.

FIBER NETWORK, TWISTED PAIR, WI-FI 5, WI-FI 6, WIRED NETWORK, WIRELESS NETWORK,

The object of the study is the system of information exchange in the trade and logistics center.

The subject of the study is wired and wireless operational networks that serve to exchange information in a trade and logistics center.

The main purpose of this study is to review wired and wireless technologies, the development of wired and wireless subnets, and measures to improve the overall reliability of an enterprise network.

In the first chapter, an overview of wired and wireless networks was made, the structure of the enterprise was considered, and the tasks to ensure the conditions of stability at the enterprise were considered.

In the second section, the components of the general network of information exchange were developed, measures were taken to increase the reliability of the company's network.

In the third section, testing and research of the components of the general network of the enterprise was carried out, as well as practical recommendations were given for the organization and use of subnetworks in the components of the information exchange system.

ЗМІСТ

Перелік скорочень та умовних позначок.....	7
Вступ	9
1 Огляд сучасних технологій інформаційного обміну.....	10
1.1 Огляд дротових мереж.....	10
1.2 Огляд бездротових мереж.....	12
1.3 Аналіз умов організації інформаційного обміну на підприємстві.....	13
1.3.1 Структура підприємства	14
1.3.2 Аналіз вимог до різних типів мереж на підприємстві.....	15
1.3.3 Постановка задачі розробки та стійкості на підприємстві.....	16
1.4 Аналіз технічних характеристик та вибір апаратних пристроїв	18
1.5 Вибір системи моделювання мережі.....	22
2 Розробка складових загальної мережі інформаційного обміну	23
2.1 Розробка дротових підмереж.....	23
2.1.1 Підмережа на основі витой пари	24
2.1.2 Підмережа на основі оптоволоконна.....	26
2.2 Розробка бездротових підмереж.....	28
2.2.1 Підмережа на основі технології WI-FI 5	28
2.2.2 Підмережа на основі технології WI-FI 6.....	29
2.3 Заходи з підвищення надійності загальної мережі підприємства.....	30
3 Тестування і дослідження складових загальної мережі підприємства.....	32
3.1 Дослідження дротових і бездротових підмереж.....	32
3.1.1 Вибір принципу адресації та маршрутизації для LAN і WAN сегментів.....	33
3.1.2 Програмне налаштування всього мережного обладнання	35
3.1.3 Адміністрування мережі	45
3.1.4 Практичні рекомендації щодо організації і використання підмереж у.....	48
складі інформаційного обміну.....	48
Висновки	57
Перелік джерел посилання	58

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАК

IP – Internet Protocol;

LAN – Local Area Network WAN – Wide Area Network ПЗ – програмне забезпечення;

ПК – персональний комп'ютер ЦОД – центр обробки даних МЗ – мережа зв'язку;

IoT – Internet of Things;

АТ – Акціонерне Товариство;

FDDI – Fiber Distributed Data Interface VPN – Virtual Private Network;

VLAN – Virtual Local Area Network OSPF – Open Shortest Path First;

DHCP – Dynamic Host Configuration Protocol OSI – Open Systems Interconnection;

PDU – Power Distribution Unit;

GRE – Generic Routing Encapsulation PC – Personal Computer;

LACP – Link Aggregation Control Protocol MLT – Multi-link trunking;

PAgP – Port Aggregation Protocol;

IEEE – Institute of Electrical and Electronics Engineers VRRP – Virtual Router Redundancy Protocol;

HSRP – Hot Standby Router Protocol PPP – Point-to-Point Protocol;

HDLC – High-Level Data Link Control МШ – мінімальні шляхи; МП – мінімальні перетини;

CSMA/CA – Carrier-Sense Multiple Access with Collision Detection UTP – Unshielded Twisted Pair;

NIC – Network Interface Card;

MDI – Medium Dependent Interface;

ANSI – American National Standards Institute;

ASNI TP-PMD – Twisted Pair Physical layer Medium Dependent RJ45 – Registered jack-45;

MLT-3 – Multi-Level Transmit-3 NRZI – NonReturn to Zero Inverted STP – Spanning Tree Protocol;

USB – Universal Serial Bus;

Cisco IOS – Cisco Internetwork Operating System IPS – in-plane switching; IPSEC – Internet Protocol Security SSL – Secure Sockets Layer;

DSP – Digital Signal Processor PVC – Permanent Virtual Circuit LSZH – LowSmoke Zero Halogen;

S/FTP – Secure File Transfer Protocol IPv4/ IPv6 – Internet Protocol version 4/6GNS3 – Graphical Network Simulator-3;

EVE-NG – Emulated Virtual Environment - Next Generation VIRL – VirtualInternet Routing Lab;

UNetLab – Unified Networking Lab.

ВСТУП

Швидкий розвиток інформаційних технологій створює необхідність постійно оновлювати та вдосконалювати системи інформаційного обміну на підприємстві. Основні аспекти актуальності включають:

- швидкість передачі даних: у сучасному світі, де інформація швидко змінюється і дуже цінна, швидкість передачі даних має вирішальне значення для прийняття рішень в реальному часі та забезпечення конкурентоспроможності;
- стабільність та надійність: важливо, щоб системи інформаційного обміну працювали без збоїв та перебоїв, оскільки вони є основою для функціонування всього підприємства;
- вибір найсучасніших технологій: забезпечення використання передових технологій у системі інформаційного обміну дозволяє збільшити продуктивність та зменшити витрати;
- захист від кіберзагроз: сучасні технології обміну даними повинні бути захищені від кіберзагроз та забезпечувати конфіденційність і цілісність інформації;
- вимоги споживачів: клієнти та споживачі вимагають якісних та швидких послуг, тому необхідно вдосконалювати системи інформаційного обміну для задоволення їхніх потреб;
- ефективність та продуктивність: забезпечення ефективної роботи підприємства та оптимізація логістичних процесів допомагають знизити витрати та підвищити продуктивність.

Отже, актуальність цієї роботи полягає в пошуку та впровадженні найсучасніших технологій для забезпечення швидкого обміну даними та стабільної роботи підприємства в умовах швидкозмінюючогося інформаційного середовища.

1 ОГЛЯД СУЧАСНИХ ТЕХНОЛОГІЙ ІНФОРМАЦІЙНОГО ОБМІНУ

1.1 Огляд дротових мереж

Дротові мережі є важливою складовою сучасних інформаційних систем, які використовуються на підприємствах та в офісних середовищах для забезпечення зв'язку та обміну даними. Огляд дротових мереж допомагає визначити їхні можливості, переваги та недоліки в контексті конкретного підприємства.

Типи дротових мереж: дротові мережі можуть бути різних типів, включаючи:

– мережі на основі витої пари: вони використовуються для передачі даних за допомогою витої пари кабелів, таких як Ethernet-кабелі. Цей тип мережі добре підходить для офісів та підприємств, оскільки забезпечує високу швидкість передачі даних.

На рисунку 1.1 показана вита пара.

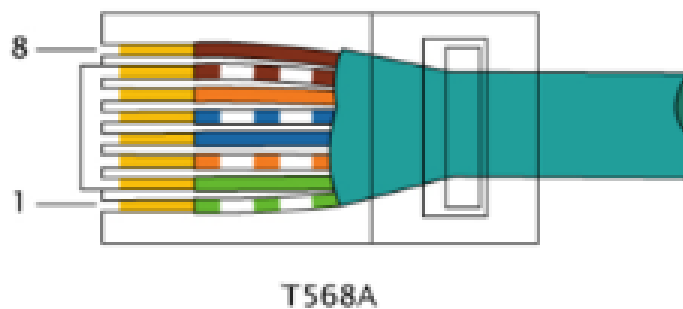


Рисунок 1.1 – Вита пара

– оптоволоконні мережі: оптоволоконні кабелі використовуються для передачі даних у вигляді світлових сигналів. Вони забезпечують високу швидкість та надійність передачі даних та відмінно підходять для підприємств з великим обсягом інформації.

На рисунку 1.2 показан оптоволоконний кабель.



Рисунок 1.2 – Оптоволоконный кабель

Переваги дротових мереж:

- надійність: дротові мережі зазвичай володіють високою стабільністю та надійністю зв'язку;
- швидкість: дротові технології можуть забезпечувати високу швидкість передачі даних;
- безпека: дротові мережі зазвичай менше вразливі до зовнішніх атак, оскільки фізичний доступ до кабелю зазвичай складніше отримати.

Недоліки дротових мереж:

- обмеженість: дротові мережі можуть бути обмежені в термінах фізичної інфраструктури, і це може вимагати додаткових витрат на прокладку кабелю;
- можлива складність розширення: додавання нових вузлів або підключення нових користувачів може бути витратним і часомкрадучим процесом.

Огляд дротових мереж є важливим кроком у процесі розробки інфраструктури зв'язку на підприємстві. Враховуючи потреби та вимоги конкретного підприємства, можна визначити найкращий тип дротової мережі,

яка забезпечить оптимальну продуктивність та надійність інфраструктури зв'язку.

1.2 Огляд бездротових мереж

Бездротові мережі є важливою частиною сучасних інформаційних систем та відіграють значну роль в організації зв'язку та обміну даними на підприємствах та в інших середовищах. Огляд бездротових мереж допомагає розібратися у їхніх характеристиках, перевагах та недоліках.

Типи бездротових мереж:

- Wi-Fi: технологія Wi-Fi є однією з найпоширеніших форм бездротових мереж і використовується для підключення різних пристроїв до мережі через бездротовий зв'язок. Wi-Fi має велику популярність в домашніх та офісних середовищах.

- Bluetooth: технологія Bluetooth зазвичай використовується для бездротового підключення малопотужних пристроїв, таких як гарнітури, клавіатури та миші.

- Zigbee: Zigbee використовується для створення мереж малопотужних пристроїв для "розумного дому" та промислових застосувань.

Переваги бездротових мереж:

- мобільність: бездротові мережі надають користувачам можливість рухатися і залишати підключену зону без втрати зв'язку;

- швидкість встановлення: встановлення бездротового зв'язку зазвичай більш швидке та просте, порівняно з дротовими аналогами;

- ефективність в складних середовищах: бездротові мережі дозволяють підключати пристрої в складних фізичних умовах, де проводи були б недосяжні.

Недоліки бездротових мереж:

- обмежена швидкість передачі даних: незважаючи на те, що бездротові технології постійно розвиваються, їхні швидкості в передачі даних зазвичай менші, ніж у дротових мережах;

- обмежена дальність дії: досягнення стабільного бездротового зв'язку може бути складним у великих відстанях або в обмежених просторах;

- безпека: бездротові мережі можуть бути більш вразливими до несанкціонованого доступу та атак ззовні, що вимагає додаткових заходів для захисту.

Огляд бездротових мереж є важливим кроком у виборі оптимальної інфраструктури зв'язку для конкретного підприємства. Розуміння переваг та обмежень бездротових технологій допомагає бізнесам забезпечити надійну та продуктивну мережу, яка відповідає їхнім потребам.

1.3 Аналіз умов організації інформаційного обміну на підприємстві

Аналіз умов організації інформаційного обміну на підприємстві є ключовим етапом у створенні надійної та ефективної інфраструктури зв'язку. Для досягнення успіху в цьому аналізі, важливо враховувати різні аспекти, включаючи структуру підприємства, вимоги до мережі, завдання забезпечення стійкості та економічний аспект.

- структура підприємства: розуміння структури підприємства є важливим аспектом при аналізі умов організації інформаційного обміну. Важливо визначити, які відділи, підрозділи та локації підприємства потребують зв'язку та обміну даними. Це допомагає визначити необхідну мережеву інфраструктуру та встановити, як взаємодіяти з різними частинами організації;

- аналіз вимог до різних типів мереж на підприємстві: різні відділи та функціональні області підприємства можуть мати різні вимоги до типів мереж. Наприклад, відділ маркетингу може потребувати великої швидкості для передачі

медіаконтенту, тоді як відділ обліку може бути більш зацікавлений у безпеці та надійності. Аналіз цих вимог допомагає визначити, які технології та типи мереж краще підходять для кожного відділу чи процесу на підприємстві;

– задача забезпечення умов стійкості на підприємстві: забезпечення стійкості мережі на підприємстві є критично важливою задачею. Визначення вимог до надійності та доступності мережі є необхідним для запобігання можливим перебоям у роботі та втраті даних.

Загальний аналіз умов організації інформаційного обміну на підприємстві допомагає визначити найкращий підхід до розробки і підтримки мережі, яка відповідає потребам та цілям бізнесу. Враховуючи всі вказані аспекти, підприємство може побудувати інфраструктуру зв'язку, яка сприяє ефективності та успішності його операцій.

1.3.1 Структура підприємства

Проектована мережа забезпечує з'єднання всіх комп'ютерів, периферійних пристроїв між собою за допомогою комбінованої системи з'єднання за участі використання бездротових и дротових технологій.

Для підключення робочих комп'ютерів використовується дротовий спосіб з'єднання за допомогою оптоволоконна та вітої пари.

Для підключення інших пристроїв використовується бездротовий спосіб підключення за допомогою Wi-Fi.

Ця комбінація гарантує надійну, безпечну та швидку передачу даних.

Підприємство розташоване в м.Запоріжжя. Одне велике приміщення.

В ньому працюють такий персонал:

- директор;
- заступник директора;
- товаровознавець;
- сервісз-менеджер;
- ІТ –експерт;
- комірник;

- продавець непродовольчих товарів;
- прибиральниця;
- охоронець.

Директор відповідає за всі процеси на підприємстві.

Заступник Директора відповідальний також за всі процеси, права рука директора коли его немає на робочому місці.

Товарознавець відповідає за товар на підприємстві.

Сервіс-менеджер вирішує всі проблеми клієнтів.

ІТ-експерт займається налаштуванням апаратного та програмного забезпечення на підприємстві, також вирішує програмні проблеми клієнтів.

Комірник займається розподілом товару по залу, також загрузкою та вивантаженням товару з машини.

Продавець непродовольчих товарів займається своєю зоною відповідальності, також продажею товарів підприємства.

Прибиральниця слідкує за чистотою на підприємстві.

Охоронець займається безпекою та порядком на підприємстві.

1.3.2 Аналіз вимог до різних типів мереж на підприємстві

Аналіз вимог до різних типів мереж на підприємстві допомагає визначити, які конкретні технології та типи мереж відповідають потребам та цілям бізнесу. Вимоги можуть варіюватися в залежності від функціональних областей та відділів на підприємстві. Ось кілька загальних кроків для аналізу вимог:

- збір вимог: почніть зі збору інформації від різних відділів та функціональних областей вашого підприємства. Питайте співробітників про їхні потреби в зв'язку та обміні даними;
- визначення типів даних: розгляньте, які типи даних передаються та обробляються на підприємстві. Це може включати текстові дані, мультимедійні файли, фінансову інформацію, дані клієнтів тощо;
- визначення обсягів даних: визначте, які обсяги даних потрібно передавати і обробляти в різних відділах та процесах підприємства. Це допоможе визначити потреби у пропускній здатності мережі;

– вимоги до швидкості передачі даних: визначте, наскільки швидким повинен бути зв'язок для задоволення потреб в різних відділах. Наприклад, відділ маркетингу може вимагати великої швидкості для завантаження великих мультимедійних файлів, тоді як фінансовий відділ може вимагати високої безпеки та надійності;

– вимоги до безпеки: визначте рівень безпеки, необхідний для захисту конфіденційних даних підприємства. Це може включати шифрування даних, ідентифікацію та автентифікацію користувачів;

– потреби у мобільності: розгляньте, чи потрібно працівникам мати можливість доступу до мережі з різних місць та пристроїв. Це може включати вимоги до бездротових мереж (Wi-Fi, мобільний доступ тощо);

– перспективи розвитку: розгляньте майбутні потреби підприємства та можливий ріст обсягів даних та користувачів. Враховуйте плани на майбутнє.

1.3.3 Постановка задачі розробки та стійкості на підприємстві

Забезпечення умов стійкості на підприємстві є однією з ключових завдань в галузі інформаційної безпеки та інфраструктури зв'язку. Стійкість мережі та інформаційної системи важлива для забезпечення безперебійності бізнес-процесів та захисту від можливих загроз. Ось кілька аспектів та завдань, пов'язаних із забезпеченням стійкості на підприємстві:

Захист від кіберзагроз:

– визначення потенційних кіберзагроз та вразливостей в мережі та інформаційних системах;

– впровадження систем захисту від кіберзагроз, таких як брандмауери, антивіруси та системи виявлення вторгнень;

– проведення регулярних аудитів безпеки та оновлення заходів захисту.

Резервне копіювання та відновлення:

– створення регулярних резервних копій даних та засобів зв'язку;

- розробка плану відновлення після аварії (Disaster Recovery Plan), який включає процедури відновлення після виникнення аварій, таких як відключення енергії чи відновлення даних після кібератаки.

Моніторинг та аналіз:

- встановлення систем моніторингу, які надають інформацію про стан мережі та інформаційних систем;
- аналіз логів та відповідь на можливі інциденти, що можуть підірвати стійкість системи.

Фізична безпека:

- забезпечення фізичної безпеки обладнання, яким користуються мережа та інформаційні системи;
- обмеження доступу до центрів обробки даних та інших критичних пунктів.

Тести на стійкість:

- проведення регулярних тестів на стійкість для перевірки реакції системи на навантаження та вразливості.

Плани надзвичайних ситуацій:

- розробка планів надзвичайних ситуацій, які включають в себе дії під час природних катастроф, терористичних актів та інших небезпек.

Організаційна готовність:

- навчання персоналу стосовно правил безпеки та дій в надзвичайних ситуаціях;
- розробка комунікаційних планів для взаємодії з владними структурами та іншими організаціями під час надзвичайних ситуацій.

Забезпечення стійкості на підприємстві є багатогранним завданням, і вимагає постійного оновлення та адаптації до змінюючогося оточення. Важливо ретельно аналізувати потенційні загрози та вживати відповідні заходи для захисту мережі та інформаційних ресурсів.

1.4 Аналіз технічних характеристик та вибір апаратних пристроїв

Інтеграція ефективної мережі починається з вибору оптимальних роутерів та комутаторів, які визначатимуть ефективність локальної мережі.

Це обладнання відіграє ключову роль у забезпеченні стабільності та функціональності мережі в цілому, зокрема, важливо, щоб обрані комутатори та роутери дозволяли користувачам передавати інформацію без зайвих ускладнень відповідно до стандартів.

Один із передових модульних мережних маршрутизаторів сучасності - Cisco 2901, розроблений для оптимального функціонування в умовах конвергентних мереж. Це обладнання гарантує безпечне підключення до Інтернету та є ідеальною платформою для розгортання різноманітних мережових програм.

Особливості цього маршрутизатора вражають своєю високою надійністю, винятковою продуктивністю та гнучкою апаратною платформою, яка підтримує масштабування та можливість встановлення додаткових інтерфейсних модулів. Застосована оновлена операційна система включає в себе широкий набір функціональних інструментів, підтримку всіх необхідних мережових протоколів, а також функції аналізу мережного трафіку і засоби моніторингу та контролю роботиобладнання.

Маршрутизатор Cisco 2901 базується на високопродуктивній архітектурі, що забезпечує найкраще у своєму класі співвідношення між продуктивністю та вартістю мережевого обладнання. Завдяки цим характеристикам, він стає надійним фундаментом для будь-якої сучасної мережі, де ефективність та безпека є високопріоритетними завданнями.

Спрощене управління. Для зручного керування модульними маршрутизаторами використовується інтерфейс mini-USB, що значно полегшує процес інсталяції та подальшого обслуговування мережного обладнання. При

встановленні SEC-ліцензії користувачеві стають доступні функції апаратно підтримуваної технології IPSEC VPN.

Маршрутизатор Cisco 2901 операційною системою Cisco IOS забезпечує всі необхідні функції для виконання всіх завдань. У комплекті з обладнанням йде повноцінний безкоштовний пакет ліцензій для Firewall, системи захисту від вторгнень IPS, IPSEC VPN, IP-телефонії, дійсний протягом 90 днів з моменту активації.

Високий рівень безпеки. Маршрутизатори Cisco 2901 використовують технологію IPS для ефективного захисту від вторгнень, мають вбудовану апаратну підтримку протоколів шифрування SSL і IPSEC, а також підтримують DSP. Потужний багатоядерний процесор допомагає успішно впоратися з завданнями безпеки інформаційного трафіку. Завдяки модульній платформі, маршрутизатори стають ідеальним рішенням для підтримки IPSEC VPN доступу та розгортання безпечної IP-телефонії та WI-FI зв'язку.

Cisco Catalyst 2950-24: Ефективна Інфраструктура Комутації. У серії Cisco Catalyst 2950, виробник презентує комутатор, який відрізняється автономною функціональністю, роблячи його ідеальним вибором для будь-якого середовища. Ці моделі ефективно функціонують в Ethernet інфраструктурах незалежно від використовуваного протоколу (Fast або Gigabit), дозволяючи користувачам зафіксувати необхідну конфігурацію та отримувати продуктивність відповідно до потреб мережі передачі даних.

Особливості обладнання:

- користувачам серії Cisco Catalyst 2950 доступна зручна панель адміністрування, що забезпечує легке використання та моніторинг мережевих неполадок;
- гнучкість комутаторів дозволяє швидко інтегрувати їх у діючі інфраструктури, уникаючи додаткових витрат на обладнання;
- всі моделі комутаторів у лінійці є надійними, і вони уникають раптових зупинок роботи портів чи інших вузлів на каналі;
- обладнання демонструє високий потенціал масштабування, дозволяючи

збільшувати кількість каналів за потребою та використовувати резервні джерела живлення.

Опис: Комутатор Cisco Catalyst 2950-24 може бути легко встановлений у стійку та має 24 LAN-порти із базовою швидкістю передачі даних 100 Мбіт/с. Він підтримує мережеві стандарти, такі як IEEE 802.1q (VLAN), IEEE 802.3ad (Link Aggregation Control Protocol), IEEE 802.1p (Priority tags), IEEE 802.1d (Spanning Tree), автовизначення MDI/MDIX, IEEE 802.1s (Multiple Spanning Tree). Управління комутатором відбувається на рівні 2 і включає особливості підтримки роботи в стеку, роблячи його відмінним вибором для комерційних організацій, віддалених об'єктів та промислових середовищ.

В таблицях 1.1-1.3 приведені детальні та додаткові характеристики пристрою.

Таблиця 1.1 – Детальні характеристики:

Тип пристрою	комутатор
Можливість встановлення у стійку	є
Моніторинг та конфігурування	Web-інтерфейс

Таблиця 1.2 – Комутатор:

Кількість LAN-портів	24
Базова швидкість передачі даних	100 Мбіт/с
Внутрішня пропускна здатність	13.6 Гбіт/сек
Розмір таблиці MAC адрес	8192
Тип керування комутатора	рівень 2

Таблиця 1.3 – Додаткові характеристики:

Об'єм оперативної пам'яті	32 МБ
Об'єм флеш-пам'яті	16 МБ
Особливості	підтримка роботи у стеку

Мережеві стандарти - IEEE 802.1q (VLAN), IEEE 802.3ad (Link Aggregation Control Protocol), IEEE 802.1p (Priority tags), IEEE 802.1d (Spanning Tree), автовизначення MDI/MDIX, IEEE 802.1s (Multiple Spanning Tree).

Вита пара — вид кабелю зв'язку. Є однією або кількома парами ізолюваних провідників, скручених між собою (з невеликим числом витків на одиницю довжини), покритих пластиковою оболонкою.

Звивання провідників проводиться з метою підвищення ступеня зв'язку між собою провідників однієї пари (електромагнітні перешкоди однаково впливають на обидва дроти пари) та подальшого зменшення електромагнітних перешкод від зовнішніх джерел, а також взаємних наведень під час передачі диференціальних сигналів. Для зниження зв'язку окремих пар кабелю (періодичного зближення провідників різних пар) у кабелях UTP категорії 5 та вище дроти пари звиваються зрізним кроком. Вита пара - один із компонентів сучасних структурованих кабельних систем. Використовується в телекомунікаціях та комп'ютерних мережах як фізичне середовище передачі сигналу в багатьох технологіях, таких як Ethernet, Arcnet, Token ring, USB. В даний час, завдяки своїй дешевизні та легкості монтажу, є найпоширенішим рішенням для побудови провідних (кабельних) локальних мереж. Кабель підключається до мережевих пристроїв за допомогою роз'єму 8P8C (який помилково називають RJ45).

Переваги кабелю вита пара:

- добре продумана конструкція. Завдяки посиленню взаємодії між кожною парою провідників, в результаті користувачі гарантовано отримують високий рівень ефективності передачі даних;
- універсальність та широке поширення. За допомогою кабелів кручений пари можна підключити майже будь-який пристрій. Оскільки ринок наповнюється різновидами кабелів, кожен користувач може підібрати те, що йому потрібно;
- простота монтажу. Основна якість кабелю — гнучкість. Його легко можна розмістити в недоступних для погляду або фізичного впливу місцях. При цьому

кабель чудово підходить під передачу різних сигналів як офісних локальних мережах, так і в глобальних міських;

– щодо низька вартість товару.

1.5 Вибір системи моделювання мережі

Cisco Packet Tracer - це популярний інструмент для моделювання, налагодження та аналізу мереж Cisco. Він є досить потужним інструментом для навчання та вивчення мережевих технологій. Ось кілька переваг, які роблять PacketTracer привабливим:

– простота використання: Packet Tracer має інтуїтивний інтерфейс, що дозволяє швидко створювати та налаштовувати мережі без глибоких технічних знань;

– моделювання різних типів мереж: Він дозволяє створювати й тестувати різні типи мереж, від простих домашніх до складних корпоративних;

– підтримка пристроїв Cisco: Packet Tracer включає в себе широкий спектр пристроїв Cisco, таких як маршрутизатори, комутатори, VoIP-пристрої та інші;

– симуляція роботи мережі: Ви можете виконувати симуляцію роботи мережі, перевіряти конфігурації та переглядати трафік для аналізу;

– навчальний інструмент: Packet Tracer широко використовується в освітніх закладах для вивчення мережевих технологій, оскільки він надає можливість практичного досвіду без потреби фізичних пристроїв.

2 РОЗРОБКА СКЛАДОВИХ ЗАГАЛЬНОЇ МЕРЕЖІ ІНФОРМАЦІЙНОГО ОБМІНУ

2.1 Розробка дротових підмереж

Розробка дротових підмереж є важливою частиною структури мережі підприємства та може бути налаштована для відповідності конкретним потребам та вимогам вашого бізнесу. Ось загальний процес розробки дротових підмереж:

Визначення потреб:

- визначення, які частини підприємства потребують окремих дротових підмереж для забезпечення ефективності та безпеки;
- визначення типів даних та послуг, які будуть передаватися через дротові підмережі.

Вибір технологій:

- вибір типів кабелів (наприклад, вита пара, оптоволокно) та активного обладнання (комутатори, маршрутизатори);
- розгляд можливостей для використання технологій PoE (Power over Ethernet), які дозволяють живлення пристроїв через мережевий кабель.

Проектування мережевої топології:

- розробка схеми підмереж та фізичної розмітки кабелів та обладнання;
- визначення кількості комутаторів та їх розташування;
- розгляд запасних маршрутів для забезпечення надійності.

Налаштування IP-адресації:

- надання IP-адрес для кожного з підмереж;
- розробка плану маршрутизації для забезпечення зв'язку між різними підмережами.

Безпека та керування доступом:

- встановлення механізмів безпеки, таких як відфільтрування пакетів, файрволи, VPN для захисту даних на дротових підмережах;

- налаштування системи керування доступом для обмеження доступу до мережі.

Тестування та впровадження:

- проведення тестів на стійкість та продуктивність підмережі перед впровадженням;

- поступове впровадження дротових підмереж та перевірка їх правильності та працездатності.

Моніторинг та підтримка:

- постійний моніторинг дротових підмереж для виявлення проблем та відновлення стійкості;

- внесення змін та оновлень за необхідності.

Розробка дротових підмереж важлива для забезпечення ефективного обміну даними та забезпечення безпеки в межах підприємства. Вона вимагає компетентності в галузі мережевого проектування та технічної експертизи для досягнення оптимальних результатів.

2.1.1 Підмережа на основі виті пари

Підмережа на основі виті пари - це один із типів дротових підмереж, який використовується для передачі даних у мережі. Вита пара - це кабель, який містить провідники, навколо яких виконують спеціальний захист у вигляді "пари" провідників. Вита пара використовується для підключення комп'ютерів, телефонів, мережевого обладнання та інших пристроїв до локальної мережі (LAN).

Ось кілька ключових аспектів підмережі на основі виті пари:

- категорії кабелів: Вита пара класифікується за категоріями (наприклад, Cat5e, Cat6, Cat6a, Cat7 і т. д.), кожна з яких має свої характеристики щодо пропускної здатності та дальності передачі сигналу. Вибір категорії кабелю залежить від потреб мережі та типу передачі даних.

На рисунку 2.1: Показана категорії кабелів Cat.

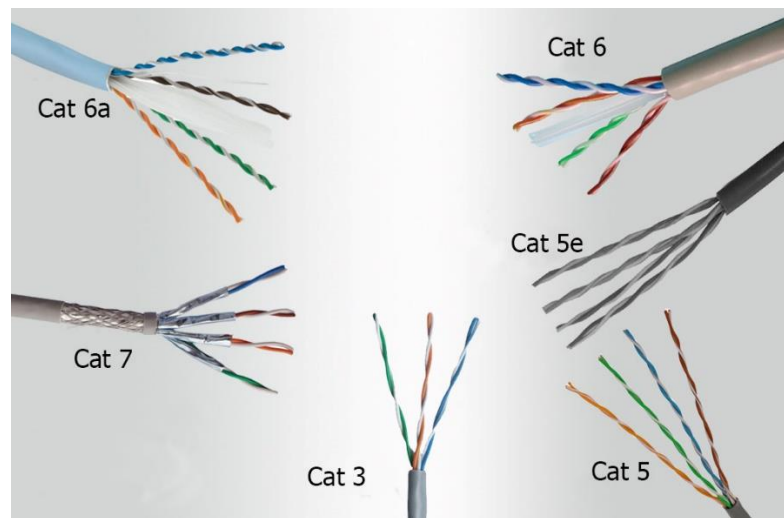


Рисунок 2.1 – Категорії кабелів Cat

– роз'єми: Для підключення витої пари використовуються стандартні роз'єми RJ-45, які забезпечують з'єднання між кабелем і мережевими пристроями, такими як комутатори та маршрутизатори.

На рисунку 2.2: Показан роз'єм RJ-45.



Рисунок 2.2 – Роз'єм RJ-45.

– поширеність: вита пара є одним із найпоширеніших типів кабелю для побудови LAN на робочих місцях, в офісах та домах. Вона підходить для передачі даних, голосу та відео;

- застосування: вита пара може використовуватися для різних цілей, включаючи підключення комп'ютерів до мережі, створення телефонних ліній, підключення камер відеоспостереження та інших пристроїв;

- поширені стандарти: кабелі на основі витої пари повинні відповідати різним мережевим стандартам, таким як Ethernet. Вони можуть підтримувати різні швидкості передачі даних, від 10/100 Мбіт/с до 1 Гбіт/с та більше.

Підмережі на основі витої пари залишаються популярними завдяки своїй доступності та універсальності. Вони є важливою складовою будь-якої LAN та використовуються для забезпечення зв'язку та обміну даними у бізнесі та домогосподарствах.

2.1.2 Підмережа на основі оптоволоконна

Підмережа на основі оптоволоконного кабелю використовується для передачі даних в мережі за допомогою світлового сигналу, який пропускається через волоконний кабель. Оптоволоконні підмережі мають ряд переваг, таких як висока пропускна здатність, низька затрата на передачу, висока стійкість до електромагнітних перешкод і велика дальність передачі сигналу. Ось ключові аспекти підмережі на основі оптоволоконна:

- волоконний кабель: оптоволоконний кабель складається з одного або кількох волокон, виготовлених з скловолокна або пластику. Ці волокна мають здатність передавати світловий сигнал на великі відстані;

- роз'єми: для підключення оптоволоконних кабелів використовуються спеціальні роз'єми, такі як SC, LC, MTP/MPO та інші. Вони забезпечують точне з'єднання між кабелем та мережевим обладнанням.

На рисунку 2.3: Показан LAN порт.

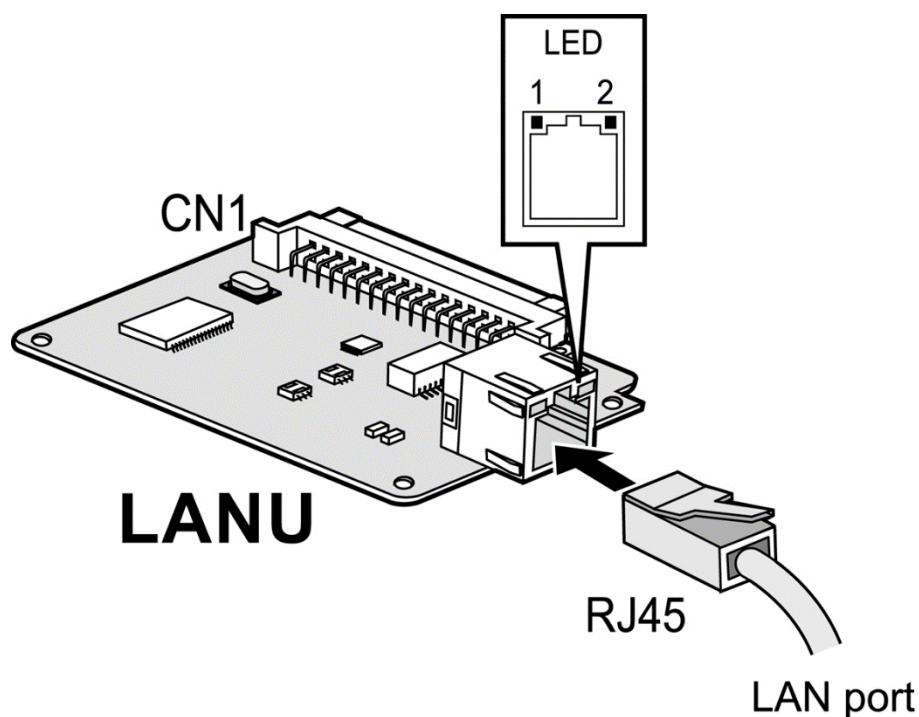


Рисунок 2.3 – LAN порт

Види оптоволоконних кабелів: існують різні види оптоволоконних кабелів, включаючи одномодові та багатомодові кабелі. Одномодові кабелі зазвичай використовуються для передачі сигналів на великі відстані та мають вищу пропускну здатність;

- пропускну здатність: оптоволоконні підмережі можуть підтримувати високі швидкості передачі даних, включаючи 1 Гбіт/с, 10 Гбіт/с, 40 Гбіт/с і більше. Це робить їх ідеальними для великих обсягів даних та вимог до високої пропускну здатності;

- висока стійкість: оптоволоконні кабелі мають високу стійкість до електромагнітних перешкод, інтерференції та шуму, що може бути важливим на заводах та в об'єктах з великими електричними навантаженнями;

- відстань передачі: оптоволоконні підмережі можуть передавати сигнал на значні відстані без втрати якості сигналу. Дальність залежить від типу оптоволоконного кабелю та активного обладнання;

– застосування: оптоволоконні підмережі використовуються у великих дата-центрах, підприємствах з великим обсягом даних, телекомунікаційних мережах, мережах високої швидкості та в інших сферах.

Підключення до оптоволоконної мережі може значно підвищити продуктивність та надійність мережі на вашому підприємстві, забезпечуючи високу швидкість передачі даних та мінімізуючи електромагнітні перешкоди.

2.2 Розробка бездротових підмереж

2.2.1 Підмережа на основі технології Wi-Fi 5

Підмережа на основі технології Wi-Fi 5, також відомої як 802.11ac, є бездротовою підмережею, яка використовує стандарт Wi-Fi для передачі даних. Wi-Fi 5 пропонує високу швидкість передачі даних і може бути використана для забезпечення бездротового підключення до мережі на підприємстві. Ось ключові аспекти підмережі на основі Wi-Fi 5:

– швидкість передачі даних: Wi-Fi 5 підтримує високу швидкість передачі даних і може досягати швидкостей до 1,3 Гбіт/с на одну точку доступу (AP). Це робить його ідеальним для вимогливих додатків та великих обсягів даних;

– діапазони частот: Wi-Fi 5 працює в діапазоні частот 5 ГГц, що дозволяє уникнути перенасиченості інтерференцією з іншими бездротовими пристроями, які використовують 2,4 ГГц;

– множинний доступ: Wi-Fi 5 використовує технологію множинного доступу (MU-MIMO), яка дозволяє одночасно підключати більше пристроїв до точки доступу без втрати швидкості передачі даних;

– забезпечення безпеки: Wi-Fi 5 підтримує різні механізми безпеки, включаючи шифрування WPA3, щоб захистити мережу від несанкціонованого доступу;

- маршрутизація та комутація: для підключення до проводової мережі та Інтернету може використовуватися маршрутизатор або комутатор з підтримкою Wi-Fi 5;

- застосування: Wi-Fi 5 підходить для бездротового підключення пристроїв в офісах, готелях, установах організованих мереж і будь-де, де потрібен бездротовий доступ до мережі;

- управління та моніторинг: щоб забезпечити ефективне управління та моніторингом Wi-Fi 5, може бути використана спеціалізована система керування Wi-Fi, яка дозволяє відстежувати стан мережі та вчасно виявляти проблеми.

Wi-Fi 5 є добрим рішенням для бездротового зв'язку на підприємстві і може забезпечити високу продуктивність та зручність для користувачів. Також важливо враховувати фактори, такі як щільність пристроїв та особливості середовища, для оптимального розташування точок доступу та забезпечення покриття мережі на всьому підприємстві.

2.2.2 Підмережа на основі технології WI-FI 6

Підмережа на основі технології Wi-Fi 6 (802.11ax) є сучасним і високопродуктивним рішенням для бездротового підключення на підприємстві. Wi-Fi 6 володіє рядом переваг порівняно з попереднім стандартом Wi-Fi 5, включаючи вищу швидкість передачі даних, покращену продуктивність та надійність. Ось деякі ключові аспекти підмережі на основі Wi-Fi 6:

- вища швидкість передачі даних: Wi-Fi 6 забезпечує значно вищу швидкість передачі даних порівняно з попереднім стандартом. Він може підтримувати швидкості до 9,6 Гбіт/с (залежно від конфігурації мережі);

- вища пропускна здатність: Wi-Fi 6 використовує технологію OFDMA (Orthogonal Frequency Division Multiple Access), яка дозволяє одночасно підключати багато пристроїв та забезпечує більш ефективне використання пропускної здатності мережі;

- менше завад: Wi-Fi 6 використовує технологію BSS Coloring, яка допомагає зменшити взаємну інтерференцію між пристроями та підвищити продуктивність мережі в умовах великої щільності пристроїв;

- більша дальність передачі сигналу: Wi-Fi 6 має покращену систему керування маршрутизацією, що дозволяє працювати на більших відстанях, забезпечуючи стабільний зв'язок;

- покращена безпека: Wi-Fi 6 підтримує більші кількості шифрування WPA3, що забезпечує високий рівень безпеки для мережі;

- маршрутизація та комутація: Wi-Fi 6 може використовувати сучасні маршрутизатори та комутатори для підключення до проводової мережі та Інтернету;

- застосування: Wi-Fi 6 ідеально підходить для вимогливих додатків і сценаріїв, де потрібна висока швидкість передачі даних та надійність. Він використовується в багатьох підприємствах, установах організованих мереж та інших сферах;

- управління та моніторинг: для ефективного управління мережею Wi-Fi 6 може бути використана спеціалізована система керування Wi-Fi, яка дозволяє відстежувати стан мережі та вчасно виявляти проблеми.

Підключення до мережі Wi-Fi 6 допомагає забезпечити високу продуктивність та якість зв'язку для користувачів підприємства. Важливо правильно спроектувати та розгорнути мережу Wi-Fi 6, враховуючи фактори, такі як щільність пристроїв, обсяги даних та особливості середовища.

2.3 Заходи з підвищення надійності загальної мережі підприємства

Забезпечення надійності загальної мережі підприємства - це критична задача для забезпечення безперебійної роботи бізнес-процесів і забезпечення доступності даних та сервісів. Щоб зробити мережу стійкою та надійною, слід вживати різноманітні заходи та стратегії. Ось кілька таких заходів:

- дублювання компонентів: використання дубльованих (резервних) компонентів, таких як комутатори, маршрутизатори, сервери та канали передачі

даних, дозволяє автоматично переключати трафік на резервний компонент у разі відмови головного;

- резервні джерела живлення: використання резервних джерел живлення, таких як безперебійні джерела живлення (UPS) та генератори, допомагає уникнути втрати живлення в разі відмови основного джерела;

- автоматичне резервування: використання пристроїв і механізмів автоматичного резервування, які дозволяють швидко переключати трафік на резервний шлях або компонент у разі відмови;

- моніторинг та управління: впровадження системи моніторингу та управління, яка дозволяє виявляти проблеми в реальному часі та вживати відповідні заходи;

- захист від кіберзагроз: забезпечення високого рівня кібербезпеки, включаючи використання брандмауерів, систем виявлення вторгнень та різних методів шифрування даних;

- резервне планування: розробка резервних планів та процедур в разі аварій та відмов в роботі, включаючи процедури відновлення даних та систем;

- регулярне оновлення та підтримка: постійне оновлення обладнання та програмного забезпечення для забезпечення сумісності та вирішення вразливостей;

- відмовостійкість: використання технологій та архітектурних рішень, які зменшують ризик відмов та забезпечують автоматичне відновлення;

- забезпечення бекапів: регулярне створення бекапів даних та їх збереження в безпечних місцях для можливості відновлення інформації в разі її втрати або пошкодження;

- тестування та відновлення: регулярне проведення тестувань системи на відновлення та підготовка персоналу до дій в разі аварій;

- оцінка ризиків: виконання оцінки ризиків та ідентифікація потенційних загроз, що дозволяє приймати заходи для їх запобігання;

– планування мережі: осмислене проектування мережі, включаючи оптимізацію топології та розташування компонентів для мінімізації однієї точки відмови.

Ці заходи допоможуть забезпечити надійність мережі підприємства та знизити ризики збоїв та втрати даних. Важливо планувати, впроваджувати та підтримувати ці стратегії на підприємстві для забезпечення безперебійної роботи вашої мережі.

3 ТЕСТУВАННЯ І ДОСЛІДЖЕННЯ СКЛАДОВИХ ЗАГАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

3.1 Дослідження дротових і бездротових підмереж

Мережа містить всього 15 PC, 2 сервери і 6 підмереж, 15 PC рівномірно розподілено на кожен підмережу (у даному випадку одна підмережа - це один офіс або сегмент). 2 сервери розміщені в першій та п'ятій підмережі. А перша, друга, містять по 2 ПК та одному Switch. Третя підмережа містить 2 ПК, один Switch. Четверта по 3 ПК та один Switch. П'ята підмережа містить 1 ПК, один Switch. Шоста підмережа містить 3 ПК, 2 Ноутбука, 1 WI-FI Route. Перша та п'ята підмережа має свій комутатор, на якому налаштований DHCP і VLAN. Кожен офіс містить свій VLAN. Для першого офісу це VLAN 10, для другого – VLAN 20, третього – VLAN 30, четвертого – VLAN 40, п'ятого – VLAN 50. Також налаштовано TRUNK порти.

Кожного комутатора офісів має свій роутер. Налаштовано динамічну маршрутизацію по технології EIGRP на роутерах. Налаштовано на Server 1,2 DNS. Налаштовано тунелі (VPN GRE) з 1 підмережі до 3 та з 4 до 5 підмережі.

Логічну схему мережі зображено на рисунку 3.1.

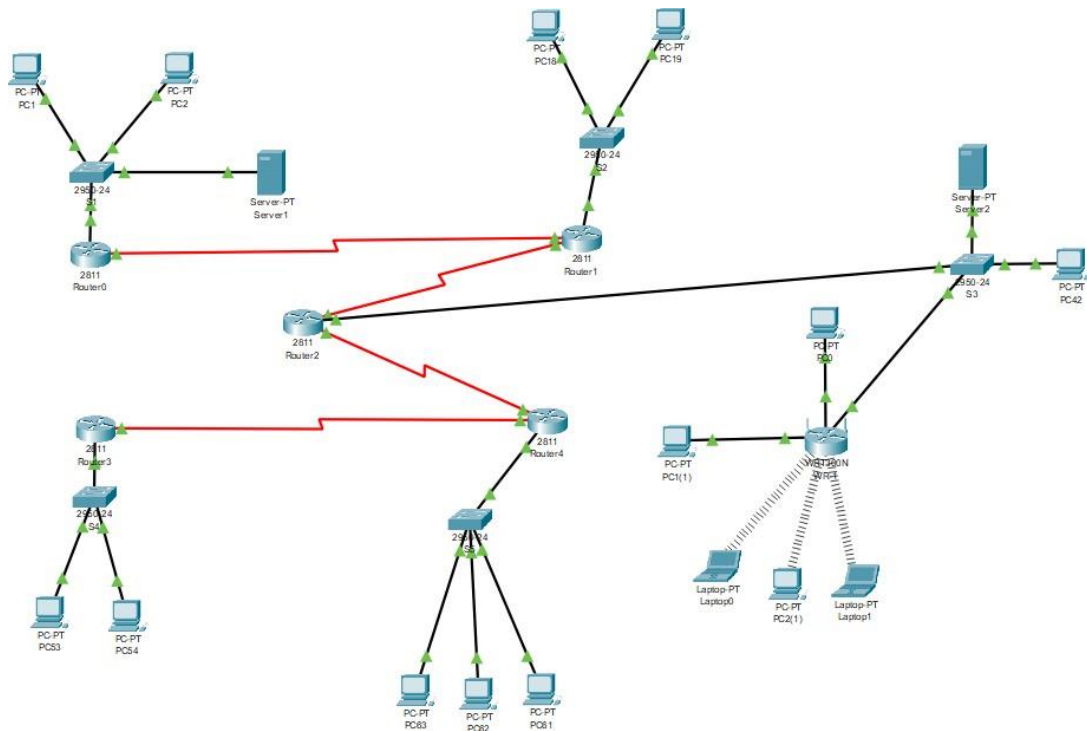


Рисунок 3.1 – Логічна схема мережі

На рисунку 3.2 показано роботу DNS на кожному ПК підмережі.

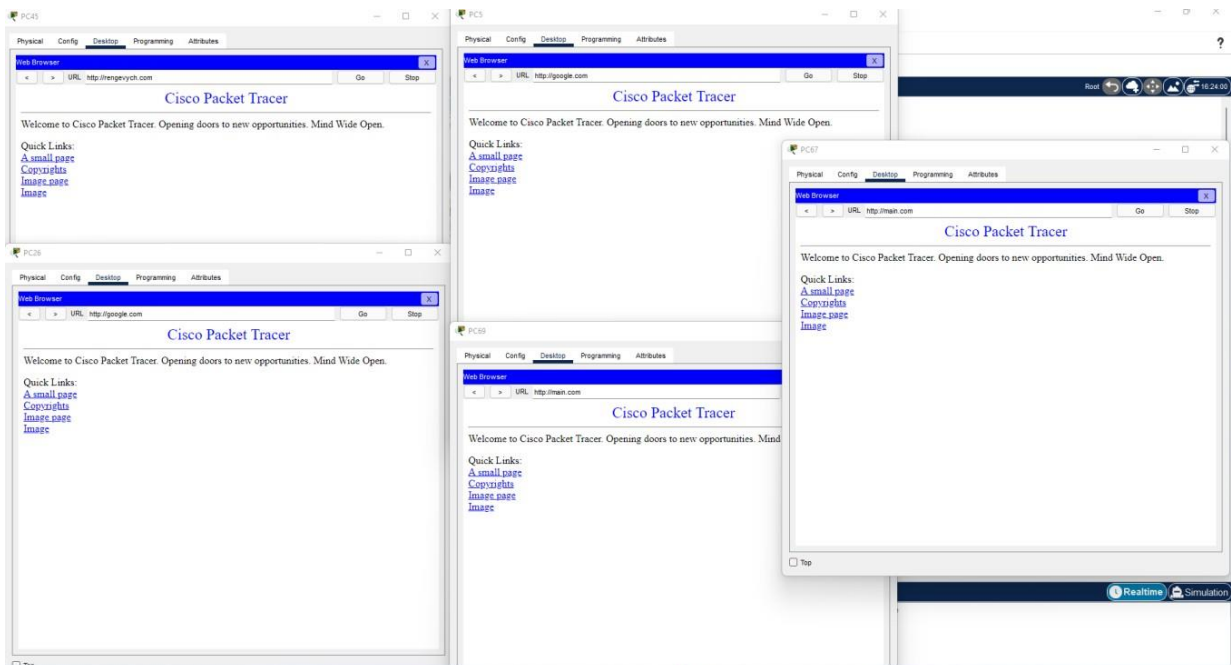


Рисунок 3.2 – робота DNS на різних ПК підмережі

3.1.1 Вибір принципу адресації та маршрутизації для LAN і WAN сегментів

EIGRP (Enhanced Interior Gateway Routing Protocol) - протокол

маршрутизації, розроблений фірмою Cisco на основі протоколу IGRP тієї ж фірми. Реліз протоколу відбувся 1994 року. EIGRP використовує механізм DUAL для вибору найкоротшого маршруту.

Більш ранній протокол IGRP, який практично не використовується нині, був створений як альтернатива протоколу RIP (до того, як був розроблений OSPF). Після появи OSPF Cisco представила EIGRP – перероблений та покращений варіант IGRP, вільний від основного недоліку дистанційно-векторних протоколів – особливих ситуацій із зациклюванням маршрутів – завдяки спеціальному алгоритму поширення інформації про зміни у топології мережі. EIGRP більш простий у реалізації і менш вибагливий до обчислювальних ресурсів маршрутизатора, ніж OSPF. Також EIGRP має більш просунутий алгоритм обчислення метрики DUAL (Diffusing Update ALgorithm), який може використовувати 5 різних компонентів для розрахунку:

- bandwidth (Пропускна спроможність). Мінімальна пропускна спроможність для цього маршруту (а не сума цін (cost) на відміну від OSPF);

- delay (Затримка). Сумарна затримка по всьому шляху маршруту;

- reliability (Надійність). Найгірший показник надійності по всьому шляху маршруту, заснований на keepalive;

- loading (Завантаженість). Найгірший показник завантаженості інтерфейсу по всьому шляху маршруту, заснований на кількості трафіку проходить через інтерфейс і настроєному на ньому параметрі bandwidth;

- MTU Мінімальний розмір MTU по всьому шляху маршруту.

За замовчуванням, EIGRP використовує лише перші два компоненти, оскільки надійність та завантаженість – динамічні величини, які можуть змінюватися до кількох разів на секунду. Відповідно, кожна зміна викликає перерахунок метрики для маршрутів та використання процесорної потужності маршрутизатора до 100%.

MTU не є динамічною величиною, але не використовується через слабкий вплив на метрику маршруту.

Слід зазначити, що ускладнення формули обчислення метрик призводить

до ускладнення розуміння метрики адміністратором. Хоча багато прихильників OSPF і вважають, що, за інших рівних, EIGRP відпрацьовує зміна топології повільніше ніж OSPF, але це швидше помилка, оскільки при малій кількості маршрутизаторів EIGRP відпрацьовує швидше, а при ускладненні схеми дизайн і архітектура протоколу OSPF вимагає більш ретельного впровадження (створення зон та міжзонних відносин), що також уповільнює обмін маршрутами та ускладнює кількість обчислень необхідних для вибору кращого маршруту. В результаті EIGRP працює порівняно однаково, а в деяких найпростіших або навпаки складніших топологіях навіть швидше за інші, що існують на даний момент, протоколи маршрутизації.

Ще одна перевага протоколу EIGRP в тому, що він здатний проводити сумаризацію на будь-якому маршрутизаторі на шляху, оскільки є протоколом класу «вектор відстані» (Distance Vector), інформація передається від сусіда до сусіда, де кожен наступний вибирає лише найкращий маршрут, який віддається сусіду.

Єдиним недоліком протоколу EIGRP зараз є його обмеженість у використанні обладнання тільки компанії Cisco. Хоча у лютому 2013 року Cisco відкрила EIGRP, його впровадження у маршрутизатори інших виробників офіційно не оголошено.

3.1.2 Програмне налаштування всього мережного обладнання

На рисунку 3.3 показано налаштування DNS на Switch. А на рисунку 3.4 показаноналаштування VPN(GRE) тунелю на Route.

```
Switch(config)#dh
Switch(config)#ip dg
Switch(config)#ip dh
Switch(config)#ip dhcp p
Switch(config)#ip dhcp pool vl10
Switch(dhcp-config)#conf t
Switch(dhcp-config)#no dn
Switch(dhcp-config)#no dns-server
Switch(dhcp-config)#dn
Switch(dhcp-config)#dns-server 10.1.10.23
Switch(dhcp-config)#
```

Рисунок 3.3 – Налаштування DNS на Switch

```

GigabitEthernet0/0      unassigned      YES NVRAM  up          up
GigabitEthernet0/0.10  10.1.10.1      YES NVRAM  up          up
GigabitEthernet0/1      unassigned      YES NVRAM  up          down
Serial0/3/0            199.56.0.2      YES NVRAM  up          up
Serial0/3/1            unassigned      YES NVRAM  down        down
Tunnel0                10.10.10.1      YES manual up          up
Vlan1                  unassigned      YES NVRAM  administratively down down
Router#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.10.2 (Tunnel0) is up: new adjacency

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

Gateway of last resort is not set

      8.0.0.0/24 is subnetted, 1 subnets
D       8.8.8.0/24 [90/2681856] via 199.56.0.1, 00:28:45, Serial0/3/0
      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.1.10.0/24 is directly connected, GigabitEthernet0/0.10
L       10.1.10.1/32 is directly connected, GigabitEthernet0/0.10
D       10.1.20.0/24 [90/2684416] via 199.56.0.1, 01:01:45, Serial0/3/0
D       10.1.30.0/24 [90/2684416] via 199.56.0.1, 00:47:39, Serial0/3/0
D       10.1.40.0/24 [90/2684416] via 199.56.0.1, 00:28:40, Serial0/3/0
D       10.1.50.0/24 [90/2684416] via 199.56.0.1, 00:28:36, Serial0/3/0
C       10.10.10.0/24 is directly connected, Tunnel0
L       10.10.10.1/32 is directly connected, Tunnel0
      18.0.0.0/24 is subnetted, 1 subnets
D       18.9.0.0/24 [90/2681856] via 199.56.0.1, 00:28:49, Serial0/3/0
      172.56.0.0/24 is subnetted, 1 subnets
D       172.56.0.0/24 [90/2681856] via 199.56.0.1, 01:03:42, Serial0/3/0
D       192.168.0.0/24 [90/2681856] via 199.56.0.1, 00:47:39, Serial0/3/0
      199.56.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       199.56.0.0/24 is directly connected, Serial0/3/0
L       199.56.0.2/32 is directly connected, Serial0/3/0

Router(config-if)#tunnel destination 199.56.0.2
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.10.1 (Tunnel0) is up: new adjacency

```

Рисунок 3.4 – Налаштування VPN(GRE) тунелю на Route

На рисунку 3.5 показано параметри налаштування динамічної маршрутизації на різних інтерфейсах.

```
Router#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address           Interface           Hold Uptime      SRTT  RTO   Q   Seq
                               (sec)              (ms)          Cnt  Num
0   199.56.0.2         Se0/3/0            13   00:37:47    40   1000   0   26
1   172.56.0.2         Se0/2/1            11   00:36:04    40   1000   0   20
2   192.168.0.2        Se0/3/1            12   00:20:08    40   1000   0   17
3   18.9.0.1           Se0/2/0            14   00:01:10    40   1000   0   17
4   8.8.8.2            Se0/1/0            13   00:01:05    40   1000   0   17
```

Рисунок 3.5 – Параметри настроювання динамічної маршрутизації на різних Інтерфейсах

Після успішного підключення всіх мережевих пристроїв до мережі необхідно провести їх налаштування. Першочерговою задачею є налаштування кожного індивідуального пристрою в мережі та надання йому унікального ідентифікатора (IP). Для даної мережі використовуються динамічні IP (Internet Protocol) адреси. Починаючи з встановлення Gateway і закінчуючи IP адресою самого пристрою та маскою підмережі.

Параметри інтерфейсів мережевого обладнання включають різноманітні налаштування, що регулюють роботу та поведінку конкретного мережевого з'єднання. Основні параметри, які можна налаштовувати на інтерфейсах, включають:

- IP-адреса та маска підмережі;
- MAC-адреса;
- MTU;
- VLAN;
- Trunking та Port Channeling;
- Швидкість та дуплекс;
- QoS (Quality of Service);
- ARP (Address Resolution Protocol).

IP-адреса та маска підмережі (встановлення IP-адреси та маски підмережі для ідентифікації пристрою в мережі та визначення обсягу адресного простору).

IP-адреса - це унікальний ідентифікатор пристрою у мережі. Це числове значення, що складається з чотирьох октетів (зазвичай в десятковій системі

числення), розділених крапками. Наприклад: 192.168.0.1 або 10.0.0.1. IP-адреса дозволяє пристроям спілкуватися та ідентифікувати один одного у мережі Інтернет або локальній мережі. Маска підмережі - це ще одне числове значення, яке визначає, яка частина IP-адреси відноситься до мережі, а яка — до конкретного пристрою в цій мережі. Маска підмережі складається з чотирьох октетів(зазвичай записується так само, як і IP-адреса), але вона представлена не числами, а шляхом задання кількості бітів у мережевій частині адреси. Наприклад, маска підмережі /24 означає, що перші 24 біти адреси відносяться до мережі, а останні 8 бітів — до конкретних пристроїв у цій мережі. Таким чином, IP-адреса 192.168.0.1 з маскою підмережі /24 вказує на те, що цей пристрій знаходиться у мережі 192.168.0.0, а останній октет (1) відноситься до конкретного пристрою в цій мережі. Налаштування IP-адреси та маски підмережі дозволяє пристроям правильно ідентифікувати інші пристрої у мережі та здійснювати обмін даними. Вони є важливими параметрами для налаштування мережевого з'єднання та його коректної роботи;

MAC-адреса (унікальний ідентифікатор пристрою на рівні каналного рівня, який призначається виробником мережевого адаптера). MAC-адреса (Media Access Control) — це унікальний ідентифікатор мережевого пристрою на рівні каналного доступу в мережах Ethernet або Wi-Fi. Він призначений виробником мережевої карти або пристрою ізначається без можливості зміни. Основні характеристики MAC-адреси: унікальність, формат, складеність, розділення на блоки. Кожен пристрій мережі має свій власний MAC-адрес, який гарантує його унікальність в мережі. Це забезпечує ідентифікацію кожного пристрою. MAC-адреса зазвичай відображаються у вигляді шістнадцяткових чисел, розділених двокрапками або тире. Наприклад : 00:1A:2B:3C:4D:5E або 00-1A-2B-3C-4D-5E. MAC-адреса складаються з шістнадцятирічних цифр (0-9, A-F), що представляють унікальний ідентифікатор пристрою. MAC-адреса поділені на два блоки. Перший блок зазвичай вказує на виробника мережевої карти (OUI - Organizationally Unique Identifier), а другий — на конкретний пристрій у цій серії від виробника. MAC-адреса, як правило, залишається постійним протягом

життєвого циклу пристрою. Вона не піддається зміні, за винятком деяких випадків, коли виробник пристрою надає можливість зміни MAC-адреси. MAC-адреса є важливим елементом мережевої ідентифікації, вона використовується для унікального ідентифікування пристроїв у мережах Ethernet та Wi-Fi, а також для керування доступом до мережі;

Статус інтерфейсу (активний/неактивний) -можливість активувати або деактивувати інтерфейс для забезпечення чи припинення передачі даних. Статус інтерфейсу визначається його активністю або неактивністю. Коли інтерфейс активний, він може передавати та приймати дані у мережі. Якщо інтерфейс неактивний, він не здатний взаємодіяти з іншими пристроями у мережі. Керування статусом інтерфейсу має важливе значення для адміністрування мережі і забезпечення безпеки. Адміністратор може активувати або деактивувати певний інтерфейс на мережевому пристрої. Це може бути корисно для виключення певних портів чи інтерфейсів у випадку проблем або для безпеки. Статус інтерфейсу також може відображати фізичний стан підключення. Наприклад, якщо кабель вийнято з порту Ethernet, інтерфейс буде неактивним. Статус інтерфейсу використовується для моніторингу пристроїв у мережі та автоматизації управління, зокрема для автоматичного виявлення проблем і реагування на них. Відключення неактивних інтерфейсів може бути частиною стратегії забезпечення безпеки мережі, щоб уникнути можливих атак або несанкціонованого доступу. Статус інтерфейсу — це важливий аспект управління мережею, який дозволяє адміністраторам контролювати та керувати роботою окремих інтерфейсів для забезпечення ефективності та безпеки мережі;

MTU (Maximum Transmission Unit)- налаштування максимального розміру пакетів даних, які можуть бути передані через інтерфейс без фрагментації. MTU (Maximum Transmission Unit) визначає максимальний розмір пакета даних, який може бути переданий через мережевий інтерфейс без фрагментації. Це один з важливих параметрів налаштування мережевих пристроїв. MTU вимірюється в байтах і визначає максимальний об'єм даних, які можуть бути включені до одного пакета для передачі в мережі без розділення на менші частини. Якщо

розмір пакета перевищує MTU на якому- небудь вузлі мережі, пакет буде розділений на менші частини (фрагменти) для передачі. Фрагментація може призвести до збільшення накладних витрат на мережі та збільшення ймовірності втрати частин пакета.

Адміністратори можуть налаштовувати MTU на різних пристроях мережі відповідно до їхніх потреб.

VLAN (Virtual LAN)- налаштування віртуальних локальних мереж для розділення трафіку на фізичному мережевому обладнанні.

VLAN (Virtual LAN) - це технологія мережі, яка дозволяє розділити одну фізичну мережу на кілька логічних мереж (VLAN) за допомогою програмного засобу.

Кожна VLAN має свою власну адресацію та може функціонувати незалежно від інших VLAN: VLAN дозволяють розділити мережу на окремі логічні сегменти, незалежно від фізичної інфраструктури. Це корисно для керування трафіком, безпеки та організації робочих груп у мережі.

Використання VLAN дозволяє обмежувати доступ до різних частин мережі для підвищення безпеки. Наприклад, можна встановити різні права доступу до ресурсів мережі для різних VLAN. VLAN дозволяють управляти трафіком, що перетинає мережу, зменшуючи витрати на широкомовний трафік. Це дозволяє підвищити продуктивність мережі та зменшити затори. VLAN дозволяють створювати групи пристроїв, які можуть взаємодіяти один з одним, навіть якщо вони фізично розташовані на різних частинах мережі. Управління VLAN зазвичай здійснюється через програмне забезпечення мережевого обладнання, таке як комутатори. Адміністратор мережі може створювати, налаштовувати та керувати VLAN. Використання VLAN може покращити безпеку, ефективність та організацію мережі, дозволяючи адміністраторам легко розділити та управляти різними частинами мережі відповідно до потреб організації;

Trunking та Port Channeling - об'єднання кількох фізичних інтерфейсів в одну логічну групу для збільшення пропускної здатності або забезпечення надійності. Trunking та Port Channeling - це два різних механізми, які

використовуються для підвищення пропускної здатності та надійності в мережесередовищах, зокрема на рівні комутаторів (switches) або інших мережесередовищ. Trunking дозволяє передавати дані різних VLAN через одне фізичне з'єднання між комутаторами або іншими пристроями. За допомогою протоколів, таких як IEEE 802.1Q для Ethernet, утворюються логічні з'єднання, які можуть передавати трафік з кількох VLAN через один порт.

Ефективне використання пропускної здатності, зменшення кількості необхідних фізичних з'єднань між комутаторами. Port Channeling дозволяє об'єднувати кілька фізичних з'єднань між двома пристроями в одну логічну групу для підвищення пропускної здатності та надійності. Декілька фізичних портів об'єднуються в один "канал" (channel), що веде до підвищення швидкості передачі даних та забезпечення резервування (redundancy) в разі відмови одного з'єднання. Підвищення пропускної здатності, збільшення надійності та резервування для уникнення втрати з'єднання. Обидва механізми використовуються для оптимізації мережі, підвищення її ефективності та надійності. Trunking дозволяє передавати різні VLAN через одне з'єднання, тоді як Port Channeling об'єднує кілька фізичних з'єднань для підвищення пропускної здатності та надійності мережі;

Швидкість та дуплекс: налаштування швидкості передачі даних та режиму дуплексного з'єднання (повний дуплекс або напівдуплекс) для взаємодії з іншими пристроями. Параметри швидкості та дуплексу в мережевому зв'язку визначають, як швидко дані можуть бути передані та чи може одночасно відбуватися передача в обидві сторони з'єднання. Це важливі налаштування для оптимізації пропускної здатності та надійності зв'язку між мережевими пристроями. Швидкість визначає максимальну швидкість передачі даних через мережеве з'єднання; зазвичай вимірюється у Mbps (мегабіт в секунду) або Gbps (гігабіт в секунду). Приклади швидкостей: 10/100/1000 Mbps або 1/10 Gbps.

У повному дуплексу (Full Duplex) пристрій може відправляти та приймати дані одночасно, що підвищує продуктивність. У півдуплексу (Half Duplex): пристрій може відправляти або приймати дані, але не одночасно. Це може

призвести до колізій на мережі та зниження продуктивності. Налаштування правильної швидкості та режиму дуплексу між мережевими пристроями є важливим для забезпечення ефективної передачі даних. Неправильні налаштування можуть призвести до погіршення продуктивності та ненадійності зв'язку між пристроями;

QoS (Quality of Service): налаштування пріоритету обробки пакетів на інтерфейсі для підвищення якості обслуговування певних видів трафіку. QoS (Quality of Service) - це набір технологій та механізмів в мережевих пристроях і програмному забезпеченні, які дозволяють керувати та контролювати якість обслуговування різних видів трафіку в мережі. Основна мета QoS - забезпечити пріоритетність передачі певних типів даних перед іншими, що дозволяє оптимізувати використання пропускну здатності мережі та забезпечувати кращу продуктивність та користувацький досвід. QoS дозволяє встановлювати пріоритети для різних видів трафіку в мережі, наприклад, віддавати перевагу голосовому чи відео трафіку перед загальним інтернет-трафіком. QoS дозволяє розподіляти доступну пропускну здатність між різними видами трафіку в мережі, забезпечуючи кращу продуктивність для критичних додатків. Встановлення правил та політик, які регулюють трафік, дозволяє уникнути перевантаження мережі в ситуаціях великої активності. QoS може контролювати затримки та втрати пакетів для забезпечення кращої якості послуг, особливо для чутливого до затримок трафіку, такого як VoIP. Використання QoS дозволяє створювати різні політики, наприклад, обмеження швидкості для певних типів трафіку або встановлення пріоритетів в залежності від важливості. QoS допомагає оптимізувати ефективність мережі, забезпечує кращу якість обслуговування для критичних додатків та знижує вплив навантаження на швидкість та якість мережі в цілому;

ARP (Address Resolution Protocol): Налаштування протоколу резольвінгу адрес, що визначає відповідність IP-адреси та MAC-адреси. ARP (Address Resolution Protocol) — це протокол на рівні мережі в моделі OSI, який використовується для відображення мережевих адрес (IP-адреси) на фізичні

адреси (MAC-адреси) у локальних мережах. Основна функція ARP полягає в тому, щоб дозволити пристроям знаходити MAC-адресу іншого пристрою в мережі на основі його IP-адреси. Коли пристрій в мережі потребує відправити дані на інший пристрій за його IP-адресою, він використовує ARP, щоб отримати відповідну MAC-адресу цього пристрою. Процес розв'язання адрес зазвичай включає ARP- запити, коли пристрій запитує у мережі про MAC-адресу для конкретної IP-адреси, та ARP-відповіді, коли пристрій із відповідною IP-адресою повертає свою MAC-адресу. Пристрої зберігають отримані відповіді ARP у своєму кеші для швидкого доступу до цієї інформації в майбутньому. Це допомагає уникнути постійних ARP-запитів для тих самих пристроїв у мережі. ARP використовується для встановлення відповідності між IP-адресами та MAC-адресами в локальних мережах. Це дозволяє пристроям коректно взаємодіяти та передавати дані від одного пристрою до іншого на фізичному рівні.

Налаштування правил фаєрволу, ACL (Access Control Lists) та інших механізмів безпеки для фільтрації трафіку. Безпека і фільтрація трафіку — це важливі аспекти для забезпечення безпеки мережі та захисту пристроїв від небажаного доступу та атак. Деякі засоби безпеки та фільтрації трафіку включають: Firewalls (брандмауери) , VPN (Virtual Private Network), Intrusion Detection/Prevention Systems, (IDS/IPS), Access Control Lists (ACLs), антивірусне та антималware програмне забезпечення, системи моніторингу мережі. Брандмауери контролюють трафік, який входить та виходить з мережі. Вони можуть блокувати або дозволяти трафік залежно від заданих правил. Stateful firewalls можуть аналізувати пакети на основі стану підключення, що дозволяє керувати доступом більш ефективно. VPN створює зашифрований тунель між пристроями, що дозволяє безпечно передавати дані через небезпечні мережі, наприклад, через Інтернет. Системи виявлення та запобігання вторгненням виявляють потенційні загрози в мережі та намагаються уникнути або заблокувати їх. ACLs встановлюють правила фільтрації трафіку на мережевому рівні, визначаючи, який трафік має бути блокований чи дозволений на основі IP-адрес, портів, протоколів тощо. Антивірусне та антималware програмне забезпечення -

це програми, що шукають, виявляють та блокують шкідливі програми та загрози, які можуть використовувати мережу для вторгнень або поширення. Системи моніторингу мережі дозволяють виявляти та реагувати на виклики безпеки в реальному часі, слідкуючи за трафіком, подіями та аномаліями в мережі.

Ці параметри дозволяють адміністраторам мережі керувати та оптимізувати роботу інтерфейсів мережевого обладнання, забезпечуючи ефективну передачу даних та забезпечення безпеки мережі.

В таблиці 3.1 показані параметри інтерфейсів.

Таблиця 3.1 – Параметри інтерфейсів

Пристрій	Інтерфейс	Assignment	Network
S1	Fa0/15	Vlan10	10.1.1.1
	Fa0/1-Fa0/14	Vlan10	10.1.1.1
	Fa0/24	Trunk	***
S2	Fa0/1-Fa0/14	Vlan20	10.1.2.1
	Fa0/24	Trunk	***
S3	Fa0/1-Fa0/14	Vlan30	10.1.3.1
	Fa0/16	Vlan30	10.1.3.1
	Fa0/24	Trunk	***
S4	Fa0/1-Fa0/14	Vlan40	10.1.4.1
	Fa0/24	Trunk	***
S5	Fa0/1-Fa0/12	Vlan50	10.1.5.1
	Fa0/24	Trunk	***

В таблиці 3.2 приведена адресація пристроїв.

Таблиця 3.2 – Адресація

Пристрій	Інтерфейс	ІР-адреса	Маска	Default Gateway
R0	Fa0/0.10	10.56.8.1	255.255.255.0	***
	Serial0/2/0	199.56.8.1	255.255.255.224	***
	Tunnel0	10.10.10.1	255.255.255.0	***
R1	Fa0/0.20	10.56.7.1	255.255.255.0	***
	Serial0/2/0	199.56.8.2	255.255.255.224	***
	Serial0/2/1	199.56.7.1	255.255.255.224	***
R2	Fa0/0.50	10.56.4.1	255.255.255.0	***
	Serial0/2/1	199.56.7.2	255.255.255.224	***
	Serial0/2/0	199.56.6.1	255.255.255.224	***
R3	Fa0/0.30	10.56.6.1	255.255.255.0	***
	Serial0/2/1	199.56.5.2	255.255.255.224	***
R4	Fa0/0.40	10.56.5.1	255.255.255.0	***
	Serial0/2/0	199.56.6.2	255.255.255.224	***
	Serial0/2/1	199.56.5.1	255.255.255.224	***
WR1	Fa0	192.168.1.1	255.255.255.0	***
	Fa1	192.168.1.2	255.255.255.0	***
Server 1	Fa0	10.56.8.7	255.255.255.0	10.56.8.1
Server 2	Fa0	10.56.4.11	255.255.255.0	10.56.4.1
PC1-PC2	***	DHCP	255.255.255.0	10.56.8.1
PC18-PC19	***	DHCP	255.255.255.0	10.56.7.1
PC53-PC-54	***	DHCP	255.255.255.0	10.56.6.1
PC61-PC-63	***	DHCP	255.255.255.0	10.56.5.1
PC42	***	DHCP	255.255.255.0	10.56.4.1
PC0-PC1(1)	***	DHCP	255.255.255.0	10.56.9.1
Laptop 0-1	***	DHCP	255.255.255.0	10.56.9.1

3.1.3 Адмістрування мережі

Програмна емуляція та тестування працездатності роботи мережі буде проводитись в програмі Cisco Packet Tracer. Емуляція роботи представлена нижче нарисунку 3.5.

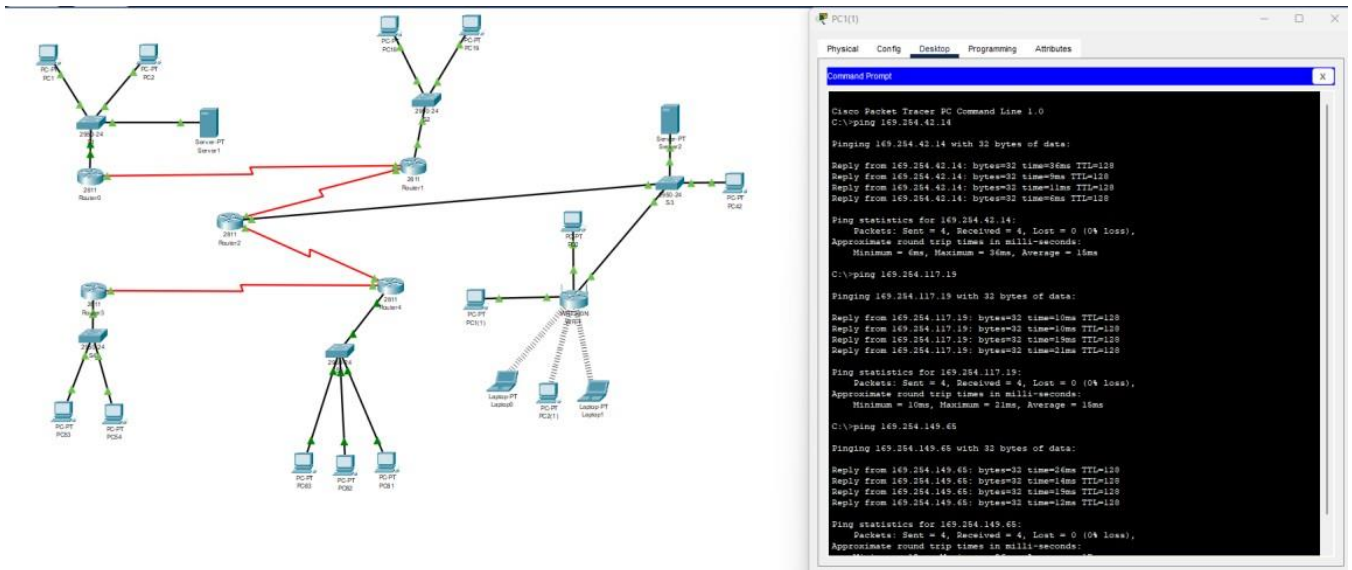


Рисунок 3.5 – Тестування роботи мереж

Як можливо побачити на рисунку 3.5, то мережа працює безвідмовно, персональні комп'ютери пінгуються без втрачання пакетів. Отже, цю мережу можливо використовувати та реалізовувати на підприємстві.

На рисунку 3.6 показано виконання програми ping між першою та другою підмережою.

```
Router#ping 10.1.20.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.20.5, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

Router#ping 10.1.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

Router#ping 10.1.10.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.10.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

Router#ping 10.1.10.23

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.10.23, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Рисунок 3.6 – Виконання програми ping між першою та другою підмережою

На рисунку 3.7 показано виконання програми ping між усіма підмережами.

```

Router#ping 10.1.40.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.40.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/9/20 ms

Router#ping 10.1.50.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.50.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/7/9 ms

Router#ping 10.1.10.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.10.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/8/15 ms

Router#
Router#ping 10.1.30.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.30.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/5/10 ms

Router#ping 10.1.20.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.20.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/8/9 ms

```

Рисунок 3.7 – Виконання програми ping між усіма підмережами

3.1.4 Практичні рекомендації щодо організації і використання підмережу складі системи інформаційного обміну

Коли йдеться про організацію та використання підмереж у системі інформаційного обміну, кілька практичних рекомендацій може значно полегшити процес: розподілення за функціональністю, фізична сегментація мережі, забезпечення безпеки, оптимізація трафіку, масштабованість і управління, моніторинг та аналіз, резервність та надійність, стандартизація та

документація.

Сегментування підмереж за функціональним призначенням (наприклад, окремі підмережі для обробки замовлень, складського управління, фінансів тощо) допоможе забезпечити кращий контроль та управління.

Розподілення за функціональністю в мережевому середовищі може бути організоване з урахуванням різних функцій та завдань, які виконують пристрої та компоненти мережі. Ось деякі типи функціонального розподілення:

- керування мережею (Network Management). Мережеві менеджери (Network Managers) - програми або пристрої, які відповідають за моніторинг, налагодження та управління мережею; елементи управління (Management Devices) - програмне забезпечення або пристрої, що включають в себе системи моніторингу, конфігурації та керування мережею;

- передача даних та комутація (Data Forwarding and Switching). Комутатори (Switches) - пристрої, які забезпечують комутацію кадрів або пакетів даних у мережі для їхньої подальшої передачі; маршрутизатори (Routers) - пристрої, які приймають та направляють пакети даних між різними мережами;

- безпека мережі (Network Security). Брандмауери (Firewalls) - програми або пристрої, які фільтрують трафік мережі для захисту від несанкціонованого доступу та загроз безпеці; системи виявлення та запобігання вторгненням (IDS/IPS) - програмне забезпечення або пристрої, що виявляють та реагують на потенційні загрози в мережі;

- доступ до мережі (Network Access). Мережеві комутатори (Access Switches) - комутатори, які забезпечують прямий доступ пристроїв до мережі на рівні локального підключення; бездротові точки доступу (Wireless Access Points) - пристрої, що надають можливість бездротового підключення до мережі.

Це лише декілька прикладів функціонального розподілення в мережевому середовищі. Кожен тип пристрою або компонента мережі може виконувати певні функції та завдання для забезпечення працездатності та безпеки мережі.

Використання різних підмереж на основі фізичного розташування (наприклад, різні підмережі для різних складів або відділень) дозволить

зменшити навантаження на мережеве обладнання і полегшити моніторинг.

Фізична сегментація мережі передбачає поділ мережі на фізично відокремлені частини або сегменти з метою забезпечення покращеної безпеки, продуктивності та управління. Ось деякі аспекти та приклади фізичної сегментації мережі:

- використання VLAN (Virtual LAN): створення віртуальних локальних мереж (VLAN), які логічно розділяють мережу, незалежно від фізичного розташування пристроїв; VLAN дозволяють групувати пристрої на основі функцій чи відділень, навіть якщо вони підключені до різних фізичних комутаторів;

- фізична ізоляція за допомогою комутаторів: використання окремих комутаторів для різних груп пристроїв чи відділень; це може допомагати уникнути конфліктів, забезпечити кращу пропускну здатність та підвищити безпеку мережі;

- фізичне розділення за допомогою підмереж (Subnets): розділення мережі на підмережі на основі фізичного розташування чи функціональності; кожна підмережа може мати свою власну адресацію IP та бути оброблена окремо;

- використання фізичних мережевих пристроїв: застосування фізичних роз'ємів, комутаторів або маршрутизаторів для розділення мережі; це може включати використання різних комутаторів для різних частин будівлі чи поверху;

- захищені бездротові мережі (WLANs): використання фізичних бар'єрів та різних каналів для розділення бездротових мереж і зменшення можливості перехоплення сигналів;

- ізоляція чутливих даних: введення фізичних бар'єрів та обмежень доступу до чутливих частин мережі для забезпечення високого рівня безпеки; фізична сегментація мережі дозволяє підвищити безпеку, керувати пропускну здатністю та легше управляти мережевим середовищем шляхом фізичного.

Використання підмережі для ізоляції чутливих даних та застосування відповідних заходів безпеки для кожної з них допоможе уникнути несанкціонованого доступу до важливої інформації.

Забезпечення безпеки мережі - це комплексний процес, який включає в себе ряд заходів та стратегій для захисту мережевих ресурсів, даних та пристроїв від потенційних загроз та атак.

Ось деякі ключові аспекти забезпечення безпеки мережі:

- Firewalls та Intrusion Detection/Prevention Systems (IDS/IPS): встановлення брандмауерів, які контролюють трафік мережі для блокування несанкціонованого доступу та запобігання атакам;

- використання систем виявлення та запобігання вторгнення для виявлення та блокування підозрілого трафіку;

- аутентифікація, авторизація та облік (AAA): застосування механізмів аутентифікації, які перевіряють ідентифікацію користувачів перед наданням доступу до мережевих ресурсів; використання авторизації для контролю доступу до різних частин мережі на основі прав доступу;

- шифрування трафіку (Encryption): застосування шифрування для захисту конфіденційної інформації під час передачі через мережу, особливо у відкритих або незахищених мережних середовищах.

Політики безпеки та оновлення програмного забезпечення: встановлення строгих політик безпеки, які включають в себе правила паролів, обмеження доступу та інші заходи для забезпечення безпеки пристроїв та даних; регулярні оновлення програмного забезпечення, включаючи операційні системи, антивірусне програмне забезпечення та інші важливі компоненти;

- фізична безпека та моніторинг: захист фізичного доступу до мережевих пристроїв та інфраструктури, таких як серверні кімнати або комутатори; використання систем моніторингу для виявлення аномалій та вчасного реагування на потенційні загрози;

- свідомість та навчання користувачів: проведення навчань та інформування персоналу про базові правила безпеки, фішинг та інші потенційні

загрози для зменшення ризику соціально-інженерних атак. Забезпечення безпеки мережі - це постійний процес, який вимагає комплексного підходу та постійного оновлення, щоб захистити мережеві ресурси та дані від зростаючих загроз.

Необхідно використовувати підмережі для оптимізації трафіку та розподіляти ресурси так, щоб зменшити затори та збільшити швидкість обміну даними.

Оптимізація трафіку мережі спрямована на покращення продуктивності, зменшення затримок та ефективне використання доступної пропускної здатності. Ось кілька способів оптимізації трафіку:

- Quality of Service (QoS): встановлення пріоритетів для різних типів трафіку, що дозволяє виділити пропускну здатність для критичних застосунків (наприклад, VoIP) та запобігти перевантаженню мережі менш важливим трафіком;

- кешування та компресія даних: використання кешування для збереження копій популярних або часто запитуваних даних на близьких до користувачів серверах або пристроях, що сприяє швидкому доступу до цих даних; використання методів компресії для зменшення обсягу передаваних даних та підвищення продуктивності мережі;

- розподіл навантаження (Load Balancing): використання механізмів розподілу навантаження для рівномірного розподілу трафіку між різними серверами чи маршрутами, що дозволяє покращити швидкодію та стабільність системи;

- керування трафіком та маршрутизація: використання технологій, таких як маршрутизація на основі вмісту (Content-Based Routing), що дозволяє направляти трафік на основі типу даних чи інших параметрів;

- оптимізація пропускної здатності WAN: використання WAN оптимізації для зменшення затримок та оптимізації використання пропускної здатності у великих мережах;

- балансування трафіку між хмарами та локальними серверами: використання гібридних рішень, які дозволяють розподіляти навантаження між

локальними ресурсами та хмаровими сервісами в залежності від вимог застосунків; оптимізація трафіку - це важливий аспект для покращення продуктивності мережі та забезпечення оптимального використання доступних ресурсів, особливо у великих та розподілених мережних середовищах.

Плануйте з урахуванням масштабованості. Системи повинні бути гнучкими для майбутніх розширень, і підмережі допоможуть управляти цим масштабуванням.

Масштабованість та ефективне управління мережею є ключовими аспектами для забезпечення стабільності та розвитку інфраструктури. Ось деякі стратегії:

- горизонтальне масштабування (Horizontal Scaling): додавання нових пристроїв чи ресурсів для збільшення мережевої потужності; використання технологій, які дозволяють автоматично розподіляти навантаження та ресурси між доданими пристроями;

- Software-Defined Networking (SDN): використання програмно-визначеної мережі, де управління мережею розділене від фізичної інфраструктури; SDN дозволяє більш гнучке управління мережею та автоматизацію процесів;

- моніторинг та аналіз даних: застосування систем моніторингу для збору даних та аналізу працездатності мережі; використання цих даних для прийняття рішень щодо масштабування та оптимізації; ці стратегії дозволяють масштабувати мережу та забезпечувати ефективне управління, що є важливими для розвитку мережевої інфраструктури відповідно до змін потреб та технологічних вимог.

Необхідно забезпечити моніторинг кожної підмережі для виявлення можливих проблем, а також для здійснення аналізу швидкості передачі даних та використання ресурсів.

Моніторинг та аналіз мережі є важливими етапами для забезпечення її ефективності, безпеки та відповідності. Ось деякі ключові аспекти моніторингу та аналізу:

- системи моніторингу мережі: встановлення систем, які постійно

відстежують стан мережевих пристроїв, збирають дані про трафік та реагують на аномалії; використання програмних інструментів, таких як Nagios, Zabbix, або SolarWinds, для нагляду за роботою мережі;

- моніторинг безпеки: виявлення та відстеження потенційних загроз безпеці та аномальної активності в мережі; використання систем виявлення вторгнень (IDS) та вірусних сканерів для нагляду за безпекою;

- аналіз трафіку: збір та аналіз даних про мережевий трафік для виявлення паттернів, перевантажень, чи аномальних активностей; використання інструментів, таких як Wireshark або NetFlow Analyzer, для аналізу трафіку

- управління ресурсами та масштабуванням: відстеження використання ресурсів та їх оптимізація для підтримки ефективної роботи мережі; аналіз потреб та масштабування мережевих ресурсів у відповідності до змін в навантаженні;

- моніторинг продуктивності мережі та доступності: постійне відстеження доступності мережевих пристроїв та сервісів для виявлення проблем та усунення їх на ранніх стадіях; аналіз даних про швидкість, пропускну здатність та час відповіді для покращення продуктивності;

- побудова звітності та візуалізація даних: створення звітів та графіків на основі зібраних даних для зручного аналізу та прийняття рішень; використання візуалізації для зрозумілого представлення стану мережі та проблем. Ці процеси допомагають усувати проблеми, виявляти загрози та покращувати продуктивність мережі, забезпечуючи надійність та ефективність її роботи.

Використання підмереж дозволяє створювати резервні шляхи для передачі даних, що забезпечує високу доступність системи в разі відмови основних каналів. Резервність та надійність мережі є критичними аспектами для забезпечення безперебійної роботи інфраструктури. Ось деякі ключові підходи до забезпечення цих характеристик:

- резервні канали та шляхи: використання резервних шляхів та альтернативних каналів зв'язку для забезпечення доступу в разі відмови основних ліній;

- Redundant Hardware (Запасне обладнання): використання резервних

пристроїв (наприклад, дублювання комутаторів або маршрутизаторів) для автоматичного перехоплення роботи в разі відмови основних;

- Protocols & Technologies (Протоколи та технології): використання протоколів, таких як Spanning Tree Protocol (STP) або Rapid Spanning Tree Protocol (RSTP), для уникнення петель у мережі та забезпечення резервних шляхів; використання технологій як Virtual Router Redundancy Protocol (VRRP) або Hot Standby Router Protocol (HSRP) для забезпечення резервності маршрутизаторів;

- Failover та Load Balancing: використання механізмів failover для автоматичного переходу на резервні ресурси або пристрої у разі відмови; load balancing дозволяє рівномірно розподілити навантаження між різними системами чи пристроями, підвищуючи надійність;

- регулярні резервні копії та архіви: здійснення регулярного резервного копіювання даних та конфігурацій для можливості відновлення в разі втрати або пошкодження даних;

- тестування та відновлення: проведення тестів відновлення для перевірки ефективності системи резервного копіювання та відновлення даних у реальному часі;

- плани надзвичайних ситуацій (Disaster Recovery Plans): розробка планів в разі катастрофи для швидкого відновлення роботи мережі в непередбачуваних ситуаціях; ці підходи дозволяють створити мережеву інфраструктуру, яка володіє високим рівнем надійності та здатності до відновлення в разі непередбачених подій чи відмов.

Стандартизація та документація: документація структури підмереж та їхніх параметрів для спрощення майбутнього управління та підтримки.

Стандартизація та документація є важливими складовими для ефективного управління мережевим середовищем і забезпечення його стабільності та розвитку. Ось деякі аспекти стандартизації та документації:

- стандартизація процесів та протоколів: встановлення стандартів щодо використання конкретних протоколів, конфігурацій та процесів у мережі для

забезпечення їхньої єдності та сумісності;

- документування мережі: створення документації, яка описує архітектуру, конфігурації, топологію мережі, а також інші характеристики, що дозволяють розуміти та управляти мережею;

- інвентаризація обладнання та програмного забезпечення: ведення інвентаризації всього мережевого обладнання, включаючи інформацію про моделі, серійні номери, версії програмного забезпечення, конфігурації тощо;

- процедури та політики управління мережею: визначення стандартів, політик безпеки, процедур реагування на інциденти та інших правил управління мережею;

- регулярне оновлення та аудит документації: постійне оновлення документації для відображення змін у мережі та усунення застарілої інформації; проведення аудиту для перевірки актуальності та правильності документації;

- системи управління конфігурацією (Configuration Management): використання систем, які дозволяють ефективно керувати конфігураціями пристроїв та зберігати історію змін; стандартизація та документація мережі допомагають уникнути непорозумінь, забезпечують послідовність у роботі та дозволяють забезпечити ефективне управління та підтримку мережі.

Ці рекомендації можуть допомогти ефективно організувати та використовувати підмережі у складі системи інформаційного обміну, забезпечуючи безпеку, ефективність та масштабованість мережі.

ВИСНОВКИ

У цій роботі я провів огляд сучасних технологій інформаційного обміну та розглянув питання структури підприємства, аналізу вимог до різних типів мереж, задачі забезпечення стійкості та заходів з підвищення надійності загальної мережі підприємства.

Для забезпечення ефективного інформаційного обміну на підприємстві важливо враховувати різні аспекти, включаючи вибір технологій передачі даних, створення структури мережі та забезпечення безперебійної роботи.

Дротові та бездротові мережі надають різні можливості та вимоги, і важливо адаптувати їх до потреб підприємства.

Аналіз структури підприємства, його вимог та завдань допомагає розробити оптимальну мережу для забезпечення задач бізнесу.

Забезпечення стійкості та надійності мережі стає важливим завданням для забезпечення безперебійної роботи бізнес-процесів.

Застосування сучасних технологій, резервування та безпека допомагають знизити ризики та забезпечити стійку роботу мережі.

У цій роботі розглянув різні аспекти організації мережі на підприємстві, і важливо ретельно розробити та підтримувати мережу для забезпечення високої продуктивності та безперебійної роботи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Навчальний матеріал та інформація про мережеві технології URL: <https://learningnetwork.cisco.com/s/> (дата звернення: 21.10.2023).
2. Наукові статі та документи з мережевих технологій URL: <https://ieeexplore.ieee.org/Xplore/home.jsp> (дата звернення: 26.10.2023).
3. Український веб-портал із новинами та ресурсами про інформаційні domain/intech.online?redirected=true (дата звернення: 31.10.2023).
4. Форум для обговорення мережевих технологій та інших ІТ-питань в українській спільноті URL: <https://ua-net.com/> (дата звернення: 11.10.2023).
5. Офіційний веб-сайт Wi-Fi Alliance містить інформацію про різні покоління Wi-Fi URL: <https://www.wi-fi.org/> (дата звернення: 05.10.2023).
6. Це офіційний стандарт IEEE, що описує технологію Wi-Fi 5 (802.11ac) URL: <https://ieeexplore.ieee.org/document/7203543> (дата звернення: 01.11.2023).
7. Офіційний веб-сайт Wi-Fi Alliance містить інформацію про Wi-Fi 6 URL: <https://www.wi-fi.org/> (дата звернення: 12.11.2023).
8. IEEE 802.11ax - Це офіційний стандарт IEEE, що описує технологію Wi-Fi 6 (802.11ax) URL: <https://ieeexplore.ieee.org/document/8275282> (дата звернення: 27.11.2023).