**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**

**БАНКІВСЬКИХ ТЕХНОЛОГІЙ ТА БІЗНЕСУ**

**КАФЕДРА КІБЕРБЕЗПЕКИ**

**КУРСОВА РОБОТА**

з дисципліни

**КОМП’ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ (РІВЕНЬ D - БЕЗПЕКА КОМП`ЮТЕРНИХ СИСТЕМ).**

(назва дисципліни)

на тему: **ПРОЕКТУВАННЯ КООПЕРАТИВНОЇ МЕРЕЖІ.**

Студента(ки) 3 курсу 303 групи

спеціальності «Кібербезпека»

Хомічак М.О.   
 (прізвище та ініціали)

Керівник

доцент кафедри

(посада, вчене звання, науковий ступінь,

Гордєєв О.О.

(прізвище та ініціали)

Національна шкала \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кількість балів: \_\_\_\_

Оцінка: ECTS \_\_\_\_

Члени комісії

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (прізвище та ініціали)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (прізвище та ініціали)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (прізвище та ініціали)

Київ - 2020 рік

**ТЕХНІЧНЕ ЗАВДАННЯ**

Варіант 7

На розробку і конфігурування комп’ютерної мережі

1. Область застосування — комп’ютерні мережі.

2. Основа розробки — робочий навчальний план дисципліни.

3. Мета та експлуатаційне призначення:

3.1. Мета – отримання практичних навичок проектування та конфігурування комп’ютерних мереж;

3.2. призначення розробки — навчальна курсова робота із дисципліни «Комп’ютерні системи та мережі (Рівень D - Безпека комп`ютерних систем)»;

4. Джерела розробки — індивідуальне завдання на курсовий проект із дисципліни, технічні рекомендації щодо проектування локальних та розподілених мереж та інші технічні матеріали для налаштування окремих компонентів мережі.

5. Технічні вимоги

5.1. Мережа складається з трьох окремих LAN, що об’єднуються WAN мережею, побудованою на основі технології віртуальних каналів.

5.2. Вимоги для проектування LAN1

5.2.1. Адреса мережі 192.168.7.0

5.2.2. Складається з п’яти сегментів, кількість робочих станцій в кожному з яких становить: 28, 26, 60, 10, 4.

5.2.3. Розподіл адресного простору має бути оптимальним;

5.2.4. Для об’єднання окремих сегментів використовуються 4 маршрутизатори;

5.2.5. З’єднання між маршрутизаторами здійснюються за допомогою скрученої пари;

5.2.6. Для обмеження проходження трафіку з одного сегменту в інший мають бути застосовані стандартні і розширені ACL. Стандартні списки мають заборонити проходження трафіку з мереж NET4, NET1 та NET5 відповідно до мереж NET4, NET1 та NET2. Розширені ACL мають заборонити проходження трафіку протоколів NETBIOS, PING та POP3 з NET2 до NET1 та HTTP HTTPS та ICMP з NET4 до NET3. ACL необхідно розмістити в найбільш вдалому місці.

5.2.7. У середині мережі використовується статична маршрутизація.

5.2.8. На маршрутизаторах Rt2-Rt4 налаштувати DHCP-сервіс і забезпечити динамічне призначення адрес хостам в мережах Net1-Net5.

5.2.9. На маршрутизаторі Rt1 налаштовано сервіс трансляції адрес NAT.

5.3. Вимоги для проектування LAN2

5.3.1. Адреса мережі 10.2.7.0/24

5.3.2. Складається з 5 сегментів, в яких розташовані ПК користувачів.

5.3.3. Розподілити адресний простір таким чином: в мережах, що з’єднують маршрутизатори, використовувати префікс 30 (маска 255.255.255.252), весь вільний простір, що залишається, рівномірно поділити між мережами, в яких розташовані Switch1- Switch5.

5.3.4. З’єднання між маршрутизаторами Rt2-Rt3 та Rt1-Rt2 здійснюється за допомогою послідовних інтерфейсів з використанням протоколів канального рівня HDLC та РРР відповідно. Інші з’єднання виконуються за допомогою скрученої пари.

5.3.5. Під’єднання мережі LAN2 до мережі WAN виконується через маршрутизатор Rt4.

5.3.6. В середині мережі використовується динамічна маршрутизація на основі протоколу EIGRP.

5.3.7. На маршрутизаторі Rt4 налаштовано сервіс трансляції адрес NAT.

5.4. Вимоги для проектування LAN3

5.4.1. Реалізована на основі комутаторів Catalyst 2960 з підтримкою технології віртуальних мереж.

5.4.2. Поділена на три віртуальні сегменти, кожний з яких містить по два сервери.

5.4.3. На комутаторах Sw1, Sw2 до Vlan 2 належать порти FastEtherne13-FastEthernet15 та FastEthernet21-FastEthernet22 відповідно, до Vlan 3 FastEthernet3-FastEthernet7 та FastEthernet7-FastEthernet11 відповідно.

5.4.4. З’єднання між комутаторами здійснюються за допомогою скрученої пари і технології Gigabit Ethernet.

5.4.5. В віртуальних мережах VLAN1, VLAN2 та VLAN3 використовуються адреси 134.87.0.0, 220.57.154.0 та 138.1.0.0 відповідно.

5.5. Вимоги для проектування WAN

5.5.1. Об’єднання локальних мереж здійснюється за допомогою Frame Relay комутатора з використанням топології Full Mesh.

5.5.2. Адреси інтерфейсів маршрутизаторів, що під’єднані до Frame Relay мережі, належать до мережі з адресою 15.0.0.0/8

5.5.3. З’єднання між локальними мережами здійснюється за допомогою послідовних інтерфейсів.

5.6. Загальні вимоги до налаштувань маршрутизаторів

5.6.1. Встановити на всіх маршрутизаторах паролі на консольне з’єднання та на привілейований режим.

5.6.2. Налаштувати доступ через протокол SSH до шлюзових маршрутизаторів.

6. Апаратні вимоги - використання обладнання фірми Cisco

7. Текстова документація розробленої мережі повинна відповідати діючим стандартам України.

8. Стадії та етапи розробки мережі включать розробку та відлагодження окремих LAN та об’єднання LAN1-4 за допомогою WAN мережі.

Розробив студент групи 303-Кб Хомічак Микола Остапович

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**

**БАНКІВСЬКИХ ТЕХНОЛОГІЙ ТА БІЗНЕСУ**

**КАФЕДРА КІБЕРБЕЗПЕКИ**

Спеціальність: «Кібербезпека»

Курс 3 Група 303-Кб Семестр 5

Дисципліна Комп’ютерні системи та мережі (Рівень D - Безпека комп`ютерних систем)

**ЗАВДАННЯ**

**на курсову роботу студента/студентки**

**Хомічака Миколи Остаповича**

(прізвище, ім’я, по батькові)

1. **Тема курсової роботи**: Розробка комп’ютерної мережі та конфігурування мережевого обладнання

2. **Термін здачі студентом закінченої роботи**  18.12.2020

**3. Постановка задачі.**

1. Розробити комп’ютерну мережу

2. Розрахувати адресний простір для мереж LAN1-LAN3

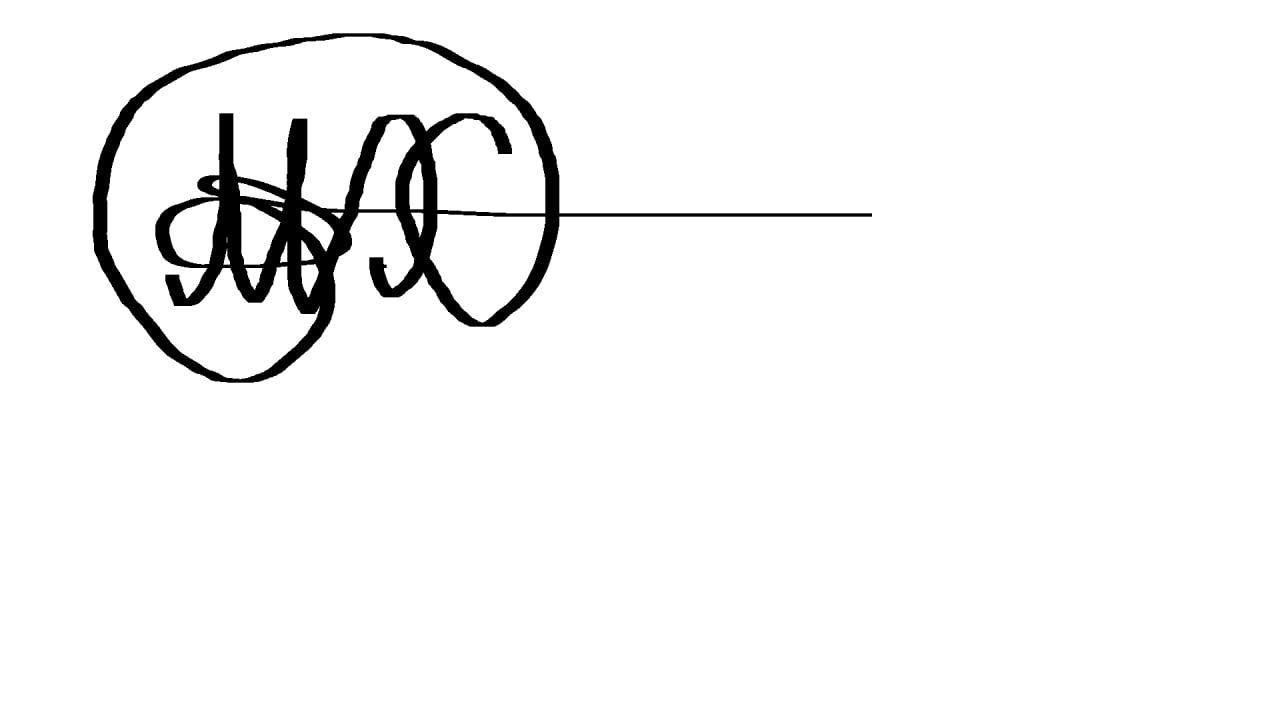
3. Створити конфігураційні файли для всіх мережевих пристроїв.

4. Виконати моделювання мережі засобами GNS3.

Вихідні дані:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| LAN №1 | підмережі | | ІР-адреса | | Кількість хостів | | | | | | | | | | | | |
| Net1 | | | Net2 | | | Net3 | | Net4 | | | | Net5 |
| 192.168.7.0 | | 28 | | | 26 | | | 60 | | 10 | | | | 4 |
| ст. ACL | | відпр. | | отр. | | | відпр. | | | отр. | | відпр. | | | | отр. |
| Net5 | | Net4 | | | Net3 | | | Net1 | | Net2 | | | | Net5 |
| розш. ACL | | відпр. | | отр. | | | відпр. | | | отр. | | відпр. | | | | отр. |
| Net3 | | Net6 | | | 3, 4, 12 | | | Net5 | | Net3 | | | | 8, 9, 11 |
| LAN №2 | № сх. | | | ІР-адреса | | Serial HDLC | | | Serial PPP | | | Шлюз | | | Тип маршрутизації | | |
| 7 | | | 10.2.7.0/24 | | Rt2-Rt3 | | | Rt1-Rt2 | | | Rt4 | | | EIGRP | | |
| LAN №3 | Net1 | Net2 | | | Net3 | | Switch1 | | | | | | | Switch3 | | | |
| Vlan 2 | | | Vlan 3 | | | | Vlan 2 | | Vlan 3 | |
| 134.87.0.0 | 220.57.154.0 | | | 138.1.0.0 | | 7-11 | | | 13-15 | | | | 21-22 | | 3-7 | |

6. Дата видачі завдання “ 16.09 ” 20 20 р



**КАЛЕНДАРНИЙ ПЛАН**

|  |  |  |
| --- | --- | --- |
| № з/п | Назва етапу роботи | Термін виконання |
| 1 | Отримання завдання | 16.09 |
| 2 | Аналіз технічної задачі | 26.09 |
| 3 | Розробка структурної схеми | 03.10 |
| 4 | Встановлення IР-адрес мережевих інтерфейсів | 10.10 |
| 5 | Налагодження серверів | 17.10 |
| 6 | Планування дозволу імен | 31.10 |
| 7 | З’єднання частин мережі за допомогою маршрутизаторів | 14.11 |
| 8 | Моделювання потоків трафіку в мережі | 21.11 |
| 9 | Розрахунок PDV | 28.11 |
| 10 | Оформлення пояснювальної записки | 12.12 |
| 11 | Захист курсової роботи | 18.12 |

Студент Хомічак М.О. (підпис)

Керівник Гордєєв О.О. (підпис)

АНОТАЦІЯ

Курсова робота складається з пояснювальної записки, що містить 3 розділи та файлу топології Packet Tracer в якому був розроблений сам курсовий проект.

Для виконання даного курсового проекту була побудована модель кооперативної мережі у програмі Cisco Packet Tracer з урахуванням всіх вимог, вказаних в технічному завданні.

Курсова робота складається з 3 розділів, 42 сторінок, 16 рисунків (з урахуванням додатків), 1 таблиці, 8 використаних джерел та 1 додатку.

**ЗМІСТ**

[ВСТУП 10](#_Toc62663971)

[РОЗДІЛ 1 ТЕНХІЧНА ЧАСТИНА ПРОЕКТУ 11](#_Toc62663972)

[1.1 Аналіз сучасних технологій локальних та глобальних мереж 11](#_Toc62663973)

[1.2 Розрахунок адресного простору 18](#_Toc62663974)

[1.3. Вибір та налаштування способу маршрутизації 23](#_Toc62663975)

[РОЗДІЛ 2 НАЛАШТУВАННЯ ПРИСТРОЇВ 27](#_Toc62663976)

[2.1 Конфігурування базових функцій маршрутизаторів 27](#_Toc62663977)

[2.2 Проектування віртуальних мереж (VLAN) 28](#_Toc62663978)

[2.3 Конфігурування базових функцій комутаторів LAN 30](#_Toc62663979)

[РОЗДІЛ 3 ДЕТАЛЬНА КОНФІГУРАЦІЯ ОБЛАДНАННЯ ТА ТЕСТУВАННЯ РОЗОБЛЕНОЇ МЕРЕЖІ 33](#_Toc62663980)

[3.1 Конфігурування додаткових функцій маршрутизаторів 33](#_Toc62663981)

[3.2 Налаштування захисту та конфігурування функцій безпеки 36](#_Toc62663982)

[3.3 Налаштування віддаленого доступу до активного обладнання 37](#_Toc62663983)

[3.4 Моделювання та тестування роботи розробленої межі 38](#_Toc62663984)

[ВИСНОВКИ 40](#_Toc62663985)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 41](#_Toc62663986)

[ДОДАТОК А 42](#_Toc62663987)

# ВСТУП

Сучасний світ нерозривно пов'язаний з інформатизацією. Комп'ютери грають величезну роль в житті нашого суспільства. Для більш ефективного використання їх об'єднують в комп'ютерні мережі, які дозволяють одним комп'ютерам мережі використовувати ресурси як інших комп'ютерів, так і спеціально виділених сервером і мережевого устаткування.

При проектуванні комп'ютерних мереж постає питання їх безпеки та надійності. В окремих випадках, таких як домашні мережі – цими питаннями можна знехтувати, однак комп'ютерна мережа організації, особливо фінансової – повинна відповідати всім вимогам по надійності та безпеки. Це означає, що вона повинна забезпечувати роботу мережевих пристроїв навіть в разі виходу з ладу обладнання, та регламентувати доступ до елементів комп'ютерної мережі, як ззовні її, так і всередині.

Створення ефективної та безпечної комп'ютерної мережі – складне завдання, яке не може бути вирішено без попереднього проектування та розробки. Для вирішення завдань безпеки та надійності існує багато рішень, як апаратних, так і програмних. Деякі такі рішення будуть розглянуті в даній роботі.

Актуальність даної роботи полягає в тому, що в ній буде спроектована спеціальна комп'ютерна мережа, що складається з трьох окремих локальних мереж, що взаємодіють один з одним. При проектуванні будуть враховані різні аспекти безпеки комп'ютерних мереж, проведено налаштування обладнання, що забезпечує захист від несанкціонованого доступу. Також будуть розглянуті аспекти відмовостійкості комп'ютерних мереж, на прикладі мережі ЦОД.

# РОЗДІЛ 1 ТЕНХІЧНА ЧАСТИНА ПРОЕКТУ

## 1.1 Аналіз сучасних технологій локальних та глобальних мереж

Локальні комп’ютерні мережі - це системи розподіленої обробки даних і, на відміну від глобальних та регіональних комп’ютерних мереж, охоплюють невеликі території (діаметром 5-10 км) всередині окремих контор, банків, бірж, вузів, установ, науково-дослідних організацій і т.д. При допомозі загального каналу зв’язку локальна мережа може об’єднувати від десятків до сотень абонентських вузлів, що включають персональні комп’ютери, зовнішні запам’ятовуючі пристрої, дисплеї, друкуючі і копіюючі пристрої, касові і банківські апарати, інтерфейсні схеми та інші. Локальні мережі можуть під’єднуватися до інших локальних і великих (регіональних або глобальних) мереж ЕОМ за допомогою спеціальних шлюзів, мостів і маршрутизаторів, які реалізуються на спеціалізованих пристроях або на персональних комп’ютерах з відповідним програмним забезпеченням.

На базі економічної та високопродуктивної електронної техніки у 80-х роках визначилась нова тенденція розвитку інформаційно-обчислювальної техніки - створення локальних обчислювальних мереж LAN (Local Area Network) різноманітного призначення. Локальна обчислювальна мережа - це комунікаційна мережа, яка забезпечує в межах деякої обмеженої території взаємозв’язок для широкого кола програмних продуктів. Вона підтримує зв’язок між ЕОМ, терміналами, обладнанням, забезпечує сумісне використання ресурсів.

Спочатку локальні обчислювальні мережі створювалися для наукових цілей з метою сумісного використання загальних ресурсів. Це пояснювалось тим, що в багатьох випадках широко розповсюджені персональні комп’ютери не забезпечували створення та функціонування достатньо потужних автоматизованих інформаційних систем через недостатність власних ресурсів. Для таких автоматизованих інформаційних систем необхідно було застосовувати потужніші комп’ютери - сервери, які дозволяли б концентрувати мережні ресурси і були б розраховані на ефективну роботу в мережі для сумісного використання користувачами. Сьогодні найпоширенішими стають локальні обчислювальні мережі комерційного призначення.

Широка і постійно зростаюча номенклатура локальних обчислювальних мереж, мережні програмні продукти і технології покладають на потенційного користувача складну задачу вибору потрібної системи з великої кількості існуючих. Сьогодні в світі нараховується десятки тисяч різних локальних обчислювальних мереж і для їх розгляду корисно мати систему класифікації. Усталеної класифікації локальних мереж поки що не існує, але для них можна виявити певні класифікаційні ознаки за:

* призначенням;
* типом використовуваних ЕОМ;
* організацією управління;
* організації передачі інформації;
* топологією;
* методах теледоступу;
* фізичних носіях сигналів;

Класифікація за призначенням. За призначенню локальні обчислювальні мережі можна розділити на: керуючі, інформаційні (інформаційно- пошукові), розрахункові, інформаційно-розрахункові, обробки документальної інформації і т.д.

Класифікація за типом використовуваних в мережі ЕОМ. За типом використовуваних в мережі ЕОМ локальні мережі можна розділити на однорідні і неоднорідні. Прикладом однорідної локальної обчислювальної мережі може служити мережа DECNET, в яку входять ЕОМ тільки фірми DEC. Часто однорідні локальні обчислювальні мережі характеризуються і однотиповим складом абонентських засобів, наприклад, тільки комплексами машинної графіки або тільки дисплеями. Неоднорідні локальні обчислювальні мережі містять різні класи ЕОМ (мікро-, міні-, великі) і різні моделі всередині класів ЕОМ, а також різне абонентське обладнання.

Класифікація за організацією управління. За організацією управління однорідні локальні обчислювальні мережі в залежності від наявності (або відсутності) центральної абонентської системи діляться на дві групи. До першої групи відносяться мережі з централізованим управлінням. Для таких мереж характерні велика кількість службової інформації і пріоритетність під’єднаних до моноканалу станцій (по розміщенню або прийнятому пріоритету). В загальному випадку локальна обчислювальна мережа з централізованим управлінням (не обов’язково на основі моноканалу) має централізовану систему (ЕОМ), яка керує роботою мережі. Прикладний процес центральної системи організовує проведення сеансів, зв’язаних з передачею даних, здійснює діагностику мережі, веде статистику і облік роботи. В локальній обчислювальній мережі з моноканалом центральна система реалізовує, також, загальну ступінь захисту від конфліктів. При виході із ладу центральної системи вся локальна обчислювальна мережа зупиняє роботу. Мережі з централізованим управлінням відрізняється простотою забезпечення функцій взаємодії між ЕОМ в локальній мережі і, як правило, характеризуються тим, що більша частина інформаційно-обчислювальних ресурсів концентрується в центральній системі. Застосування локальної мережі з централізованим управлінням доцільне при невеликому числі абонентських систем. У тому випадку, коли інформаційно-обчислювальні ресурси локальної мережі рівномірно розподілені по великому числу абонентських систем, централізоване управління малопридатне, оскільки не забезпечує потрібну надійність мережі і призводить до різкого збільшення службової (управлінської) інформації. В цьому випадку доцільно застосовувати локальні мережі з децентралізованим або розподіленим управлінням. В цих мережах всі функції управління розподілені між системами мережі. Однак, для проведення діагностики, збору статистики і проведення інших адміністративних функцій, в мережі використовується спеціально виділена абонентська система або прикладний процес в такій системі. В децентралізованих локальних обчислювальних мережах на основі моноканалу у порівнянні з централізованими ускладнюються проблеми захисту від конфліктів, для чого застосовуються багаточисленні тракти, що враховують суперечливі вимоги надійності і максимального завантаження моноканалу. Одна із найрозповсюдженіших децентралізованих форм управління передбачає два рівні захисту від конфліктів. На першому рівні сконцентровані функції, що визначають активність моноканалу і блокування передачі у випадку виявлення будь-якої активності. На другому рівні виконуються складніші функції аналізу системних затримок, які управляють моментами початку передачі інформації якійсь із підсистем локальної мережі.

Класифікація за формуванням передачі інформації. По формуванню передачі інформації локальні мережі поділяються на мережі з маршрутизацією інформації і селекцією інформації. Взаємодія абонентських систем з маршрутизацією інформації забезпечується визначенням шляхів передачі блоків даних по адресах їх призначення. Цей процес виконується всіма комунікаційними системами, що знаходяться в мережі. При цьому абонентські системи можуть взаємодіяти по різних шляхах (маршрутах) передачі блоків даних, а для скорочення часу передачі здійснюється пошук найкоротшого по часу маршруту.

Класифікація за топологією мережі. Топологія, тобто конфігурація з’єднання елементів в локальних мережах, притягує до себе увагу більше, ніж інші характеристики мережі. Це пов’язано з тим, що саме топологія багато в чому визначає основні властивості мережі, наприклад, такі, як надійність (живучість), продуктивність та інші. Механізм передачі даних, допустимий в тій чи іншій локальній мережі, багато в чому визначається топологією мережі. По топологічних ознаках локальні мережі поділяються на мережі з довільною, кільцевою, деревовидною конфігурацією, мережі типу “загальна шина” (моноканал), “зірка” та інші. Найбільш поширені топології «рис. 1.1 - 1.5»:

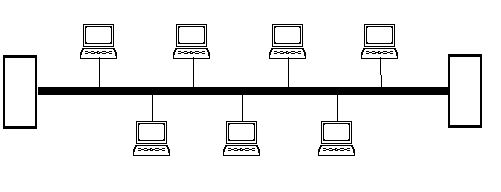


Рисунок 1.1 Топологія «Шина»

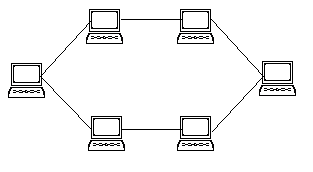


Рисунок 1.2 Топологія «Кільце»

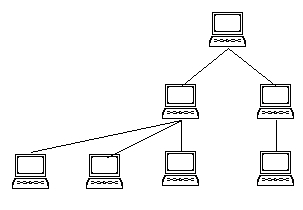


Рисунок 1.3 Топологія «Ієрархія»

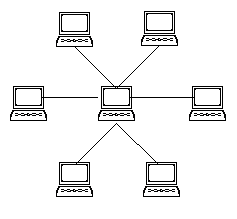


Рисунок 1.4 Топологія «Зірка»

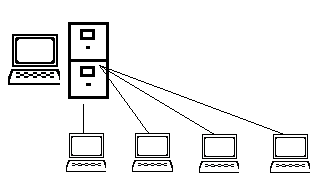


Рисунок 1.5 Топологія «Клієнт-сервер»

Важливою характеристикою локальної мережі є швидкість передачі інформації. В ідеальному варіанті при відсиланні і отриманні даних через мережу час відгуку повинен бути таким же, як і при роботі з особистим персональним комп’ютером користувача, а не з якогось місця поза ним у мережі. Це вимагає швидкості передачі даних від 1 до10 Мбіт/с і більше.

Поряд з цим локальні мережі повинні не тільки швидко передавати інформацію, але і легко адаптуватися до нових умов, мати гнучку архітектуру, яка дозволяла б розташовувати автоматизовані робочі місця (або робочі станції) там, де це потрібно. Користувач повинен мати можливість встановлювати нові або переносити існуючі робочі місця або інші пристрої мережі, а також, від’єднувати їх у випадку необхідності без переривань роботи мережі. Задоволення перерахованих вимог досягається модульною побудовою локальної мережі, яка дозволяє будувати комп’ютерні мережі різної конфігурації і з різними можливостями. Основними фізичними компонентами локальних комп’ютерних мереж є: кабелі, робочі станції, інтерфейсні плати мережі, сервери мережі.

Кожен пристрій локальної мережі під’єднується до кабелю передачі даних, що дозволяє їм взаємодіяти. Під’єднуючі кабелі можуть бути різноманітними: від найпростіших двожильних телефонних до дорогих волоконно-оптичних. Пристрої мережі з’єднуються кабелями за допомогою інтерфейсних плат. Специфічними компонентами локальної обчислювальної мережі є сервери. Вони виконують функції управління розподілом мережних ресурсів загального доступу. Сервери - це апаратно-програмні системи. Апаратним засобом, звичайно, є достатньо потужній персональний комп’ютер, міні-ЕОМ, велика ЕОМ або комп’ютер, спеціально спроектований як сервер. Локальна мережа може мати декілька серверів для управління мережними ресурсами, але завжди повинен бути один або більше файл - серверів чи серверів баз даних. Сервер управляє зовнішніми запам’ятовуючими пристроями загального доступу і дозволяє формувати потрібні бази даних. У випадку файл - серверу кожній під’єднаній робочій станції забезпечується доступ до цілого файлу баз даних. Це зокрема означає, що робота відбувається із всіма записами в конкретній базі даних, а не тільки з потрібними. Тобто по мережі на конкретну робочу станцію передається повна база даних, хоча цьому користувачу був потрібний лише один чи декілька записів з багатьох. Все це може призвести до непотрібного перевантаження локальної обчислювальної мережі. Сервер баз даних працює в таких випадках набагато продуктивніше, тому що він обробляє лише ті записи, з якими працює користувач в даний момент часу.

## 1.2 Розрахунок адресного простору

На відміну від фізичних MAC–адрес, формат яких залежить від конкретної мережної архітектури, IP–адреса будь–якого вузла мережі є чотирибайтовим числом. Записуються IP–адреси чотирма числами в діапазоні від 0 до 255, які представляються в двійковій, вісімковій, десятковій або шістнадцятковій системах числення та розділяються крапками (наприклад 192.168.40.250). Для більш ефективного використання єдиного адресного простору Internet введено класи мереж:

* Мережі класу A ( 1–126) мають 0 в старшому біті адрес. На мережну адресу відводиться 7 молодших бітів першого байта, на гост–частину – 3 байти. Таких мереж може бути 126 з 16 мільйонами вузлів у кожній.
* Мережі класу B (128–191) мають 10 у двох старших бітах адрес. На мережну адресу відводиться 6 молодших бітів першого байта та другий байт, на гост–частину – 2 байти. Таких мереж може бути близько 16 тисяч з 65 тисячами вузлів в кожній.
* Мережі класу C (192–223) мають 110 у трьох старших бітах адрес. На мережну адресу відводиться 5 молодших бітів першого байта та другий і третій байт, на гост–частину – 1 байт. Таких мереж може бути близько 2 мільйонів з 254 вузлами в кожній.
* Мережі класу D (224–239) мають 1110 у чотирьох старших бітах адрес. Решта біт є спеціальною груповою адресою. Адреси класу D використовуються у процесі звернення до груп комп'ютерів.
* Мережі класу E (240–255) зарезервовані на майбутнє.

Для зменшення трафіка в мережах з великою кількістю вузлів застосовується розділення вузлів за підмережами потрібного розміру. Адреса підмережі використовує кілька старших бітів гост–частини IP–адреси, решта молодших бітів – нульові. В цілому IP–адреса складається з адреси мережі, підмережі та локальної гост–адреси, яка є унікальною для кожного вузла. Для виділення номерів мережі, підмережі та госта (вузла) використовується маска підмережі – бітовий шаблон, в якому бітам, що використовуються для адреси підмережі, присвоюються значення 1, а бітам адреси вузла – значення 0. Розглянемо адресу 192.168.40.252 та значення маски 255.255.255.0. У цьому випадку маємо адресу підмережі 192.168.40 та адресу госта – 252. При цьому всі гости підмережі 192.168.40 мають встановити ту ж саму маску підмережі. Отже, мережа 192.168 може мати 256 підмереж з 254 вузлами в кожній. Використання ж маски 255.255.255.192 дасть змогу мати 1024 підмережі з 60 вузлами в кожній.

Комбінації всіх нулів або всіх одиниць у мережній, підмережній або гост–частині зарезервовані для загальних (broadcast) повідомлень та службових цілей. Наприклад, адреса 192.168.40.255 використовується для загального повідомлення всім вузлам підмережі 192.168.40.

Кожен гост може мати не тільки IP–адресу, але й ім'я (Host name). Як і цифрові IP–адреси, імена вузлів діляться на частини, що розділяються крапками. Починають запис від імені комп'ютера, далі йдуть імена локальних доменів (груп комп'ютерів) і закінчується ім'я вказанням імен вищих доменів (організаційних та територіальних). Список цих імен зберігається в спеціальній базі даних доменів служби імен DNS (Domain Name System). Наприклад, ім'я blues.franko.lviv.ua відповідає серверу з іменем Blues у домені franko.lviv.ua комп'ютерів кампусної мережі Львівського державного університету ім. І. Франка. Звертаючись до вузла, з однаковим успіхом можна використати як IP–адресу, так і його ім'я.

Розподіл адрес в мережі Інтернет організовано на основі централізованої ієрархічної системи. Головним органом цієї системи є неурядова некомерційна організація ICANN (Internet Corporation for Assigned Numbers). ICANN координує регіональні відділення – ARIN (Америка), RIPE (Європа), APNIC (Азія і Тихоокеанський регіон). Регіональні відділення видають блоки адрес великим провайдерам послуг Інтернет. Провайдери в свою чергу видають блоки адрес своїм клієнтам. Для отримання українським провайдером блоку адрес, провайдер повинен стати членом RIPE NCC та отримати статус Локального Інтернет-Реєстру (LIR). Відповідно до RFC 1518, 1519 блоки адрес виділяються на основі однакового префікса, виділення блоків на основі класів адрес вважається застарілим і в даний час не використовується.

Адреси з першими розрядами рівними 11110 зарезервовані для майбутніх застосувань. Пакет з адресою 255.255.255.255 повинен розсилатися всім вузлам, що знаходяться в тій же підмережі, що і джерело пакету. Такий спосіб розсилки називається обмеженим широкомовлення (limited broadcast). Якщо розряди адреси, яка відповідає номеру вузла, містять тільки одиниці, то пакет розсилається всім вузлам мережі з заданим номером. Такий спосіб розсилки називається широкомовним (broadcast).

192.168.7.255 – широкомовна адреса для мережі 192.168.7.0 з маскою підмережі 255.255.255.0

213.1.18.127 – широкомовна адреса для мережі 213.1.18.64 з маскою підмережі 255.255.255.192

Якщо у адресі одержувача в полі номера мережі містяться тільки нулі, то вузол-одержувач належить тій же підмережі, що і вузол, який відправив пакет. Блок адрес 127.0.0.0/8 використовується для тестування і взаємодії мережевих процесів в межах окремого комп'ютера. Наприклад, при передачі пакетів на адресу 127.0.0.1, пакети не передаються по мережі, а повертаються модулям верхнього рівня як тільки що прийняті. Інакше кажучи, передача пакетів на адресу 127.0.0.1 означає зв'язок з самим собою. Адреса 127.0.0.1 відповідає віртуальному петлевий (loopback) мережному інтерфейсу, який реалізується програмно і не пов'язаний з фізичними інтерфейсами (RFC 3330). Наприклад, цей інтерфейс може бути використаний клієнтськими мережевими процесами для взаємодії з серверним процесом, що виконується на тому ж комп'ютері.

Згідно з технічним завданням був розподілений адресний простір мережі центрального офісу. Задана адреса всієї мережі – 192.168.7.0 з кількістю хостів на підмережу 28, 26, 60, 10, 4. Розподіл та призначення адрес відбувався за описаним вище алгоритмом та описаний в таблиці «табл. 1.1»:

Таблиця 1.1

Розподіл IP-адрес в мережі LAN1

|  |  |  |  |
| --- | --- | --- | --- |
| Мережа | Адреса мережі | Адреси хостів | Широкомовна адреса |
| NET 1 | 192.168.7.0/27 | 192.168.7.1 – 192.168.7.30 | 192.168.7.31 |
| NET 2 | 192.168.7.32/27 | 192.168.7.33 – 192.168.7.62 | 192.168.7.63 |
| NET 3 | 192.168.7.64/26 | 192.168.7.65 – 192.168.7.126 | 192.168.7.127 |
| NET 4 | 192.168.7.128/28 | 192.168.7.129 – 192.168.7.142 | 192.168.7.143 |
| NET 5 | 192.168.7.144/29 | 192.168.7.145 – 192.168.7.190 | 192.168.7.191 |

Після виконаних дій з адресним простором мережа LAN1 має вигляд, зображений на рисунку «рис. 1.6»:

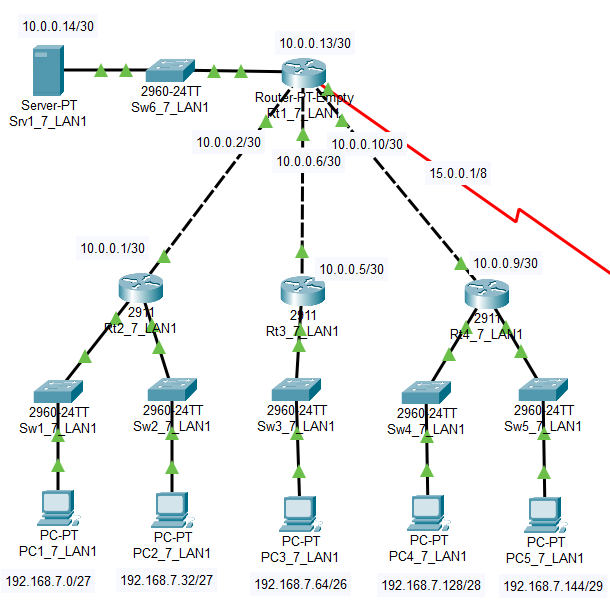


Рисунок 1.6 Загальний вигляд мережі LAN1

Адресний простір в мережі LAN2 був розподілений за тим же алгоритмом, що був описаний вище з умовою зміни внутрішніх адрес мережі з урахуванням визначених в технічному завданні префіксів, масок підмережі та з’єднань. Загальний вигляд мережі зображено на рисунку «рис. 1.7.»:

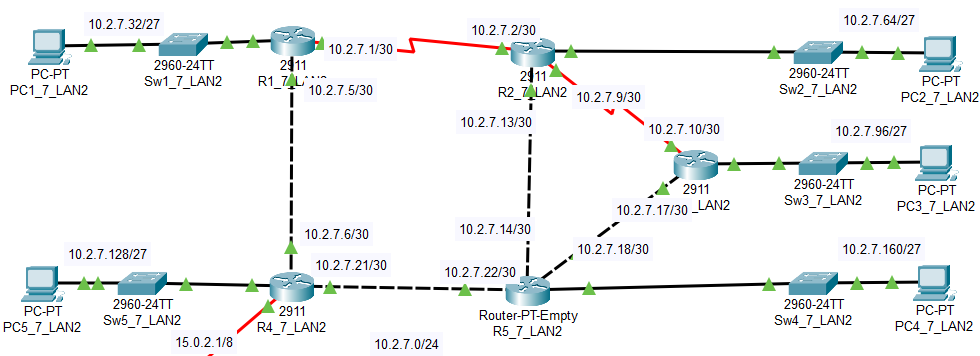


Рисунок 1.7 Загальний вигляд топології LAN2

Мережа LAN3 поділена на три підмережі, що містять по два сервера і кожна пара серверів має різні адреси підмережі. Було обрано розбиття на пари Sv1-Sv2, Sv3-Sv4, Sv5-Sv6 та адресами 134.87.0.0, 220.57.154.0 та 138.1.0.0 відповідно. Вони були присвоєні з вибором оптимальної маски підмережі за уже визначеним алгоритмом. Загальний вигляд зображено на рисунку «рис. 1.8»:

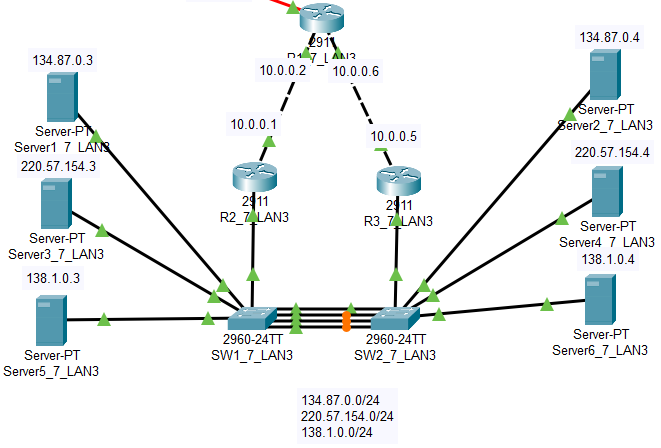


Рисунок 1.8 Загальний вигляд топології мережі LAN3

Також частиною адресного простору є симуляція глобальної мережі – Cloud PT. Згідно технічного завдання адреси з’єднань з глобальною адресою мають вигляд 15.0.1.0, 15.0.2.0 та 15.0.3.0 відповідно до номеру локальної мережі.

## 1.3. Вибір та налаштування способу маршрутизації

У загальнодоступному значенні слова маршрутизація означає пересування інформації від джерела до пункту призначення через об’єднану мережу. При цьому, як правило, на шляху зустрічається принаймні один вузол. Маршрутизація часто протиставляється об’єднанню мереж за допомогою моста, що, у популярному розумінні цього способу, виконує точно такої ж функції. Основне розходження між ними полягає в тім, що об'єднання за допомогою моста має місце на Рівні 2 еталонні моделі ISO, у той час як маршрутизація зустрічається на Рівні 3. Цією різницею поясняється те, що маршрутизація й об'єднання за мостовою схемою використовують різну інформацію в процесі її переміщення від джерела до місця призначення. Результатом цього є те, що маршрутизація й об'єднання за допомогою моста виконують свої задачі різними способами; фактично, мається кілька різних видів маршрутизації й об’єднання за допомогою мостів.

Тема маршрутизації висвітлювалася в науковій літературі про комп'ютери більш 2-х десятиліть, однак з комерційної точки зору маршрутизація придбала популярність тільки в 1970 р. Протягом цього періоду мережі були досить простими, гомогенними оточеннями. Великомасштабне об'єднання мереж стало популярно тільки останнім часом.

Алгоритми маршрутизації можна диференціювати, ґрунтуючись на декількох ключових характеристиках. По-перше, на роботу результуючого протоколу маршрутизації впливають конкретні задачі, що вирішує розроблювач алгоритму. По-друге, існують різні типи алгоритмів маршрутизації, і кожний з них по-різному впливає на мережу і ресурси маршрутизації. І нарешті, алгоритми маршрутизації використовують різноманітні показники, що впливають на розрахунок оптимальних маршрутів. У наступних розділах аналізуються ці атрибути алгоритмів маршрутизації.

При розробці алгоритмів маршрутизації часто переслідують одну чи трохи з перерахованих нижче цілей:

* Оптимальність
* Простота і низькі непродуктивні витрати
* Живучість і стабільність
* Швидка збіжність
* Гнучкість

Оптимальність, імовірно, є самою загальною метою розробки. Вона характеризує здатність алгоритму маршрутизації вибирати "найкращий" маршрут. Найкращий маршрут залежить від показників і від "ваги" цих показників, використовуваних при проведенні розрахунку. Наприклад, алгоритм маршрутизації міг би використовувати кілька пересилань з визначеною затримкою, але при розрахунку "вага" затримки може бути їм оцінений як дуже значний. Природно, що протоколи маршрутизації повинні строго визначати свої алгоритми розрахунку показників.

Алгоритми маршрутизації розробляються як можна більш простими. Іншими словами, алгоритм маршрутизації повинний ефективно забезпечувати свої функціональні можливості, з мінімальними витратами програмного забезпечення і коефіцієнтом використання. Особливо важлива ефективність у тому випадку, коли програма, що реалізує алгоритм маршрутизації, повинна працювати в комп'ютері з обмеженими фізичними ресурсами.

Алгоритми маршрутизації повинні мати живучість. Іншими словами, вони повинні чітко функціонувати у випадку неординарних чи непередбачених обставин, таких як відмовлення апаратури, умови високого навантаження і некоректні реалізації. Маршрутизатори розташовані у вузлових крапках мережі, їхнє відмовлення може викликати значні проблеми.  
Часто найкращими алгоритмами маршрутизації виявляються ті, котрі витримали іспит часом і довели свою надійність у різних умовах роботи мережі.

Алгоритми маршрутизації повинні швидко сходитися. Збіжність – це процес угоди між усіма маршрутизаторами по оптимальних маршрутах. Коли яка-небудь подія в мережі приводить до того, що чи маршрути відкидаються, чи стають доступними, маршрутизатори розсилають повідомлення про відновлення маршрутизації. Повідомлення про відновлення маршрутизації пронизують мережі, стимулюючи перерахування оптимальних маршрутів і, в остаточному підсумку, змушуючи всі маршрутизатори прийти до угоди по цих маршрутах. Алгоритми маршрутизації, що сходяться повільно, можуть привести до утворення петель чи маршрутизації виходам з ладу мережі.

Згідно технічного завдання був обраний тип маршрутизації EIGRP.

EIGRP – дистанційно-векторний протокол маршрутизації, що був оптимізований для зменшення нестабільності протоколу після змін топології мережі, уникнення проблеми зациклення маршруту та більш ефективного і економного використання потужностей маршрутизатора. Алгоритм визначення маршруту базується на алгоритмі Дейкстрі пошуку в глибину на графі. EIGRP обчислює і враховує 5 параметрів для кожної ділянки маршруту між вузлами мережі: − Total Delay — Загальна затримка передачі (з точністю до мікросекунди) − Minimum Bandwidth — Мінімальна пропускна спроможність (в Кб/с – кілобіт/секунду) − Reliability – Надійність (оцінка від 1 до 255; 255 найбільш надійно) − Load – Завантаження (оцінка від 1 до 255; 255 найбільш завантажено) − Maximum Transmission Unit (MTU) (не враховується при обчисленні оптимального маршруту, береться до уваги окремо) – максимальний розмір блоку, що можливо передати по ділянці маршруту. Протокол маршрутизації EIGRP має чотири базових складових: виявлення сусіда; надійний транспортний протокол; алгоритм DUAL; модуль, що залежить від протоколу. Кожен маршрутизатор зберігає інформацію про сусідні маршрутизатори. Якщо з'являється новий сусід, інформація про нього записується в таблицю маршрутизації. Для кожного модуля, залежного від протоколу, підтримується своя таблиця маршрутизації. Записи в таблиці сусідів містять інформацію, потрібну для надійної доставки, наприклад номер повідомлення. Цей номер використовується для перевірки того, що повідомлення від сусіда прийшли у тому порядку, в якому він їх відправив. Протокол EIGRP забезпечує швидке підключення завдяки застосуванню моделі «запит-відповідь», при якій повідомлення посилаються тільки тим маршрутизаторам, на роботу яких може вплинути зміни в мережевій топології. Для гарантії отримання відправлених повідомлень EIGRP використовує фірмовий протокол гарантії доставки – RTP, який забезпечує гарантовану доставку пакетів. Для цього використовується пропріетарний алгоритм Cisco, reliable multicast.

# РОЗДІЛ 2 НАЛАШТУВАННЯ ПРИСТРОЇВ

## 2.1 Конфігурування базових функцій маршрутизаторів

Маршрутизатор являє собою пристрій, що має один або кілька мережних інтерфейсів для підключення локальних мереж або віддалених з’єднань. Кожному фізичному інтерфейсу ставиться у відповідність одна чи кілька ІР-підмереж, що мають з ним безпосередній зв’язок. Маршрутизатор виконує міжмережну передачі пакетів між вузлами доступних йому підмереж. До однієї з функцій маршрутизатора входить зменшення полю TTL (Time tо Live, час життя) на одиницю при приході пакету, а потім кожну секунду його перебування в маршрутизаторі.

У своїй роботі маршрутизатор використовує таблицю маршрутизації, в якій міститься інформація про ІР-адреси і маски підмереж, підключених до його портів мереж, а також список сусідніх маршрутизаторів.

Особливим маршрутом, що має бути присутнім в будь якій таблиці маршрутизації є «Маршрут за замовчуванням», він також може мати назви «Основний шлюз», «Основний маршрут». Такий запис говорить про те на який мережний інтерфейс необхідно відправляти дейтаграми, у випадку коли адреса призначення дейтаграми жодна з підмереж підключених до маршрутизатору, ІР-адреса основного маршруту – 0.0.0.0 маска підмережі 0.0.0.0.

Рішення на відправлення дейтаграми на відповідний порт виробляється на основі аналізу зазначеної в заголовку пакету ІР-адреси вузла-одержувача, та таблиці маршрутизації. Спочатку визначається до якої мережі належить вузол-одержувач, якщо відомості про таку мережу є в таблиці маршрутизації, то пакет відправляється на мережний інтерфейс, до якого підключена мережа призначення, якщо такі відомості відсутні то пакет відправляється на мережний інтерфейс, який в таблиці маршрутизації зазначено, як «Основний маршрут».

Заповнення таблиць маршрутизації може виконуватись динамічно або статично.

Крім цього на маршрутизатори може покладатися задача фільтрації, за певними правилами, пакетів, які циркулюють між підмережами підключеними до маршрутизатору.

Настроювання робочої станції для використання маршрутизатора полягає в задані основного маршруту (шлюзу за замовчуванням), який є ІР-адресою локального інтерфейсу маршрутизатора.

Основні налаштування маршрутизаторів – ІР-адресація та маршрутизація, що описані вище. Всі ці функції були налаштовані згідно технічного завдання.

## 2.2 Проектування віртуальних мереж (VLAN)

Безпека телекомунікаційних мереж багато в чому визначається розмірами широкомовних доменів, усередині яких може відбуватися несанкціонований доступ до конфіденційної інформації. У традиційних мережах розподіл на широкомовні домени реалізується маршрутизатором. Віртуальні мережі створені, щоб реалізувати сегментацію мережі на комутаторах. Таким чином, створення віртуальних локальних мереж (Virtual Local Area Networks – VLAN), які являють собою логічне об'єднання груп станцій мережі «рис. 2.1», є одним з основних методів захисту інформації в мережах на комутаторах.

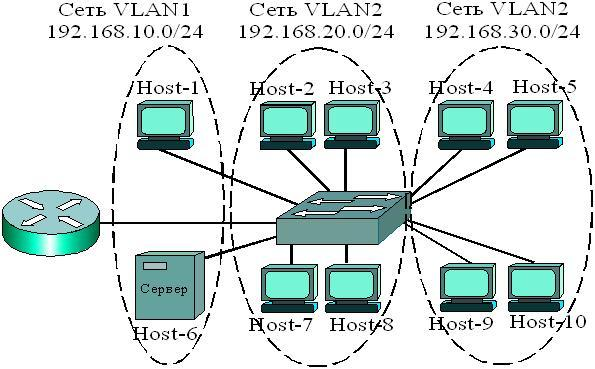


Рисунок 2.1 Приклад мережі VLAN

VLAN, які створені, щоб забезпечити послуги сегментації, зазвичай надаються маршрутизаторами в конфігурації локальної мережі. VLAN, розглядають такі питання, як масштабованість, безпека та управління мережею. Маршрутизатори в топологіях VLAN забезпечують фільтрацію, безпеку, узагальнення адрес та управління трафіком. За визначенням, вимикачі не можуть з’єднувати IP-трафік між мережами VLAN, так як це буде порушенням цілісності широкомовного домену VLAN.

+Це також корисно, якщо хтось хоче створити кілька мереж 3-го рівня на тому ж комутаторі 2 рівня. Наприклад, якщо сервер DHCP (який буде перевіряти його наявність) підключений до комутатора він буде обслуговувати будь-який хост, який налаштований на отримання свого IP від сервера DHCP. За допомогою віртуальних локальних мереж можна легко розділити мережу так, щоб вузли не використовували цей сервер DHCP і отримували локальні адреси, або отримували адресу з іншого серверу DHCP.Віртуальні локальні мережі 2-го рівня конструкції є важливими, порівняно з IP-підмережами, які є конструкціями 3-го рівня При використанні VLAN, можна управляти пакетами трафіку і швидко реагувати на переміщення. Мережі VLAN забезпечують гнучкість, щоб адаптуватися до змін у мережі вимогам і дозволяють спрощене адміністрування.

В мережі LAN3 топологія серверів була поділена на три віртуальні мережі. Кожна така мережа має свою унікальну ІР-адресу. Оскільки сервери з однієї віртуальної мережі з’єднані різними комутаторами, відповідні порти комутаторів були налаштовані на Trunk режим «рис. 2.2»:

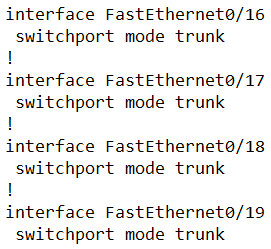


Рисунок 2.2 Конфігурація портів комутатора у Trunk режимі

Віртуальні мережі були налаштовані за допомогою відповідних команд у привілейованому режимі Cisco IOS. На обох комутаторах були створені три віртуальні мережі, куди були внесені порти, в які підключені відповідні обраній VLAN сервери, та за допомогою Trunk режиму віртуальні мережі двох комутаторів були об’єднані.

## 2.3 Конфігурування базових функцій комутаторів LAN

Мережевий комутатор – пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента.

На відміну від концентратора, що поширює трафік від одного під'єднаного пристрою до всіх інших, комутатор передає дані лише безпосередньо отримувачу. Це підвищує продуктивність і безпеку мережі, рятуючи інші сегменти мережі від необхідності (і можливості) обробляти дані, які їм не призначалися.

Комутатор працює на канальному рівні моделі OSI, і тому в загальному випадку може тільки поєднувати вузли однієї мережі по їхніх MAC-адресах. Для з'єднання декількох мереж на основі мережного рівня служать маршрутизатори.

Комутатор зберігає в пам'яті таблицю, у якій вказуються відповідні MAC-адреси вузла порту комутатора. При включенні комутатора ця таблиця порожня, і він працює в режимі навчання. У цьому режимі дані, що поступають на який-небудь порт передаються на всі інші порти комутатора. При цьому комутатор аналізує кадри й, визначивши MAC-адресу хоста-відправника, заносить його в таблицю. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, MAC-адреса якого вже є в таблиці, то цей кадр буде переданий тільки через порт, зазначений у таблиці. Якщо MAC-адреса хоста-отримувача ще не відома, то кадр буде продубльований на всі інтерфейси. Згодом комутатор будує повну таблицю для всіх своїх портів, і в результаті трафік локалізується.

Принцип роботи комутатора подібний до роботи мосту. Він базується на алгоритмі прозорого моста ІЕЕЕ 802.1D. Для того, щоб передавати кадри, комутатор (світч) використовує таблицю комутації. До включення комутатора, записи в таблиці відсутні. Комутатор здійснює автоматичне заповнення таблиці, при отриманні кадрів від вузлів. Після отримання кадру комутатором, він спочатку передає його відповідно до своїх правил, а потім запам'ятовує фізичну адресу відправника, вказану у кадрі і ставить її у відповідність порту на якому він був отриманий.

Коли комутатор заповнює таблицю, він знає відповідність вузла порту та передає кадри на відповідні порти. Кадр, що адресований лише одному абоненту, фізичної адреси якого немає в таблиці комутації, називається кадром з невідомою адресою.

В мережах LAN1 та LAN2 комутатори виконують функцію посередника між маршрутизатором та комп’ютером і не потребують особливого налаштування окрім забезпечення безпеки за допомогою паролю до привілейованого режиму та конфігурації SSH для можливості вирішити проблеми та несправності у роботі пристрою дистанційно.

У мережі LAN3 обидва комутатори виконують роль пристроїв, що розділяють топологію на віртуальні мережі, що було описано вище. Для надійності роботи цього з’єднуючого механізму вони з’єднані між собою за допомогою чотирьох RJ-45 кабелів на випадок, якщо основний буде несправний, тому для коректної роботи такої системи на Trunk режим, описаний раніше, були налаштовані всі чотири відповідні порти.

# РОЗДІЛ 3 ДЕТАЛЬНА КОНФІГУРАЦІЯ ОБЛАДНАННЯ ТА ТЕСТУВАННЯ РОЗОБЛЕНОЇ МЕРЕЖІ

## 3.1 Конфігурування додаткових функцій маршрутизаторів

На деяких маршрутизаторах був налаштований протокол динамічного присвоєння адрес DHCP для уникнення конфліктів адрес у випадку присвоєння їх власноруч.

DHCP – це мережевий протокол, що дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі TCP / IP. Даний протокол працює по моделі «клієнт-сервер». Для автоматичної конфігурації комп'ютер-клієнт на етапі конфігурації мережевого пристрою звертається до так званого сервера DHCP, і отримує від нього потрібні параметри. Адміністратор може задати діапазон адрес, що розподіляються сервером серед комп'ютерів. Це дозволяє уникнути ручного налаштування комп'ютерів мережі і зменшує кількість помилок. Протокол DHCP використовується в більшості великих (і не дуже) мереж TCP / IP.

DHCP є розширенням протоколу BOOTP, що використовувався раніше для забезпечення бездискових робочих станцій IP-адресами при їх завантаженні. DHCP зберігає зворотну сумісність з BOOTP.

Були налаштовані допустимі при динамічному присвоєнні адреси та ті, що будуть присвоюватись у разі якоїсь помилки в роботі протоколу за замовчуванням «рис. 3.1».

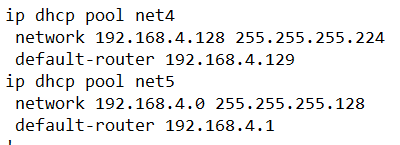


Рисунок 3.1 Конфігурація DHCP

Також на маршрутизаторах був налаштований механізм маскування ІР-адреси відправника пакету – NAT.

NAT– це механізм у мережах TCP/IP, котрий дозволяє змінювати IP-адресу у заголовку пакунку, котрий проходить через пристрій маршрутизації трафіку.

Важливим для роботи NAT-пристрої є правило поширення маршрутних оголошень через кордони приватних мереж. Оголошення протоколів маршрутизації про зовнішні мережах «пропускаються» прикордонними маршрутизаторами у внутрішні мережі і обробляються внутрішніми маршрутизаторами. Протилежне твердження невірно – маршрутизатори зовнішніх мереж не отримують оголошень про внутрішні мережах, оголошення про них фільтруються при передачі на зовнішні інтерфейси. Тому внутрішні маршрутизатори «знають» маршрути до всіх зовнішніх мереж, а зовнішнім маршрутизаторів нічого не відомо про існування приватних мереж.

Традиційна технологія NAT підрозділяється на технології базовоїтрансляції мережевих адрес (Basic Network Address Translation, Basic NAT) і трансляції мережевих адрес і портів (Network Address Port Translation, NAPT). В технології Basic NAT для відображення використовуються тільки IP-адреси, а в технології NAPT - ще й так звані транспортні ідентифікатори, в якості яких найчастіше виступають TCP- і UDP-порти.

Існує 3 базових концепції трансляції адрес: статична, динамічна, перевантажена.

**Статичний NAT** – відображення незареєстрованої IP-адреси на зареєстровану IP-адресу на основі один до одного. Особливо корисно, коли пристрій повинен бути доступним зовні мережі.

**Динамічний NAT** – відображує незареєстровану IP-адресу на зареєстровану адресу з групи зареєстрованих IP-адрес. Динамічний NAT також встановлює безпосереднє відображення між незареєстрованими і зареєстрованими адресами, але відображення може мінятись в залежності від зареєстрованої адреси, доступної у купі адрес, під час комунікації.

**Перевантажений NAT** – форма динамічного NAT, котрий перетворює декілька незареєстрованих адрес у єдину зареєстровану IP-адресу, використовуючи різноманітні порти. Відомий також як PAT. При перевантаженні кожен комп'ютер у приватній мережі транслюється у ту ж саму адресу, але з різним номером порту.

Для можливості коректно та безпечно передавати пакети даних на шлюзових маршрутизаторах був налаштований саме зовнішній динамічний NAT.

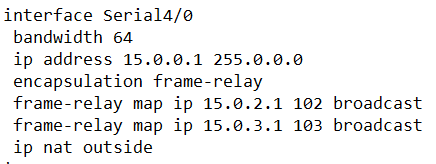


Рисунок 3.2 Конфігурація NAT на шлюзовому маршрутизаторі

На інших маршрутизаторах всередині був налаштований внутрішній NAT «рис. 3.3».

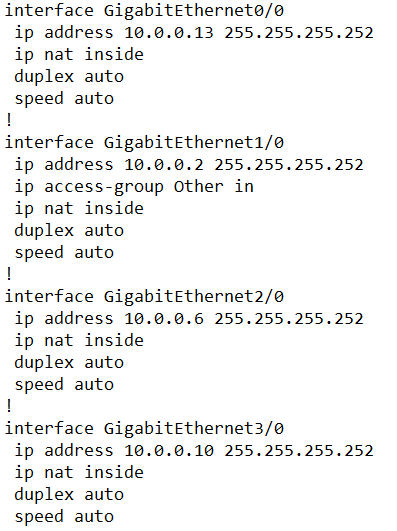


Рисунок 3.3 Конфігурація NAT на маршрутизаторі

Подібна конфігураціє встановлена на кожному маршрутизаторі кооперативної мережі.

## 3.2 Налаштування захисту та конфігурування функцій безпеки

Основними методами забезпечення безпеки мережі було встановлення паролів на привілейований режим до кожного мережевого пристрою та генерація ACL.

Access Control List або ACL – список управління доступом, який визначає, хто або що може отримувати доступ до об'єкта (програми, процесу чи файлу), і які саме операції дозволено або заборонено виконувати суб'єкту (користувачеві, групі користувачів). У файлових системах для реалізації ACL використовується ідентифікатор користувача процесу (UID в термінах POSIX).

Лист доступу являє собою структуру даних, що містить записи, що визначають права індивідуального користувача або групи на спеціальні системні об'єкти, такі як програми, процеси або файли. Ці записи також відомі як ACE (англ. Access Control Entries) в операційних системах Microsoft Windows і OpenVMS. В операційній системі Linux і Mac OS X більшість файлових систем мають розширені атрибути, які виконують роль ACL. Кожен об'єкт в системі містить покажчик на свій ACL. Привілеї (або повноваження) визначають спеціальні права доступу, які дозволяють користувачеві читати з, писати в, або виконувати об'єкт. У деяких реалізаціях ACE (Access Control Entries) можуть визначати право користувача або групи на зміну ACL об'єкта.

Концепції ACL в різних операційних системах розрізняються, незважаючи на існуючий «стандарт» POSIX. (Проекти безпеки POSIX, .1e і .2c, були відкликані, коли стало ясно що вони зачіпають занадто велику область і робота не може бути завершена, але добре опрацьовані частини, що визначають ACL, були широко реалізовані і відомі як «POSIX ACLs».)

У мережах ACL представляють список правил, що визначають порти служб або імена доменів, доступних на вузлі або іншому пристрої третього рівня OSI, кожен зі списком вузлів і / або мереж, яким дозволений доступ до сервісу. Мережеві ACL можуть бути налаштовані як на звичайному сервері, так і на маршрутизаторі і можуть керувати як входять, так і вихідний трафік, як брандмауера.

## 3.3 Налаштування віддаленого доступу до активного обладнання

Для вирішення проблем та несправностей на мережевих пристроях дистанційно на кожному з них був встановлений протокол віддаленого доступу SSH, що дозволяє відкрити інтерфейс Cisco IOS на комп’ютері.

SSH – мережевий протокол сеансового рівня, який дозволяє забезпечувати віддалене управління операційною системою. Мережевий протокол сеансового рівня SSH дає можливість проводити віддалене управління ОС і тунелювання TCP-з'єднань. За своєю функціональністю схожий з протоколами Telnet і rlogin. SSH шифрує трафік і паролі, які передаються.

## 3.4 Моделювання та тестування роботи розробленої межі

Для перевірки роботоспроможності розробленої мережі були виконані команди ping з кінцевих пристроїв. Успішність таких команд свідчить про те, що пакети даних безперешкодно можуть бути передані з одного кінцевого пристрою на інший.

Для перевірки успішності передачі пакетів даних між мережами були виконані тестові команди ping на пристроях з різних мереж «рис. 3.4».

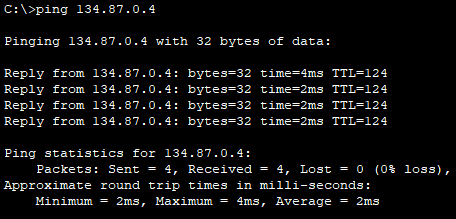


Рисунок 3.4 Відправка пакетів даних з комп’ютера в мережі LAN1 на сервер в мережі LAN3

Був також здійснений тест на коректність передачі пакетів даних в межах однієї мережі «рис. 3.5».

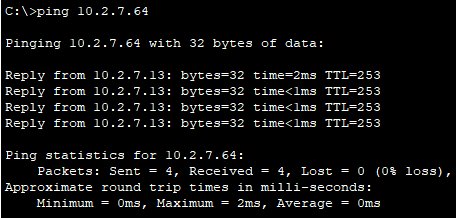


Рисунок 3.5 Відправка пакетів даних з комп’ютера в мережі LAN2 на інший комп’ютер в тій же мережі

Результати тестування роботи розробленої мережі показали її повну роботоспроможність та коректність виконання поставлених завдань.

# ВИСНОВКИ

В рамках даного курсового проекту була розроблена та сконфігурована модель кооперативної мережі, що максимально наближена до реальної мережі та виконує всі визначені функції.

Робота виконувалась виключно згідно технічного завдання та методичних вказівок. Були також застосовані знання та навички, отримані по ходу вивчення курсу з безпеки комп’ютерних мереж та попереднього курсу з основ мереж та маршрутизації.

Також по ходу виконання роботи були набуті нові знання та практичні навички роботи з мережевим обладнанням та операційною системою Cisco IOS.

Основними засобами для отримання інформації були онлайн ресурси, зазначена література та доступні по ходу семестру курси Cisco.

Всі основні вимоги до працездатності та конфігурації розробленої мережі були виконані.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кульгін М. Комп'ютерні мережі, практика побудови / Максим Кульгін. Санкт-Петербург: СПб, 2003. – 464 с.
2. Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. Комп’ютерні мережі : навчальний посібник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.] Вінниця : ВНТУ, 2013. – 371 с.
3. Оліфер В. Г. Комп'ютерні мережі. Принципи, технологї, протоколи. Підручник для вузів / В. Г. Оліфер, Н. А. Оліфер. Санкт-Петербург: СПб, 2007. – 960 с
4. Біляєв А. В. Методи та засоби захисту інформації [Електронний ресурс] / А. В. Біляєв. 2000. – Режим доступу до ресурсу: http:// www.citforum.ru/internet/infsecure/its2000\_01.shtml.
5. Колбін Р. В. Глобальні та локальні мережі: створення, налаштування та використання / Р. В. Колбін. М.: Біном. Лабораторія знань, 2008. – 55 с.
6. Платонов В. В. Програмно-апаратні засоби забезпечення інформаційної безпеки обчислювальних мереж / В. В. Платонов. М.: Академія, 2006. – 240 с.
7. Алгоритми: побудова та створення / Т.Корман, Ч. Лейзерсон, Р. Рівест, К. Штайн. М.: Видавничий дім "Вільямс", 2007. – 1296 с. – (2).
8. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп’ютерні мережі [навчальний посібник] – Львів, «Магнолія 2006», 2013. – 256 с.

# ДОДАТОК А

**ІЛЮСТРАЦІЇ СКОНФІГУРОВАНОЇ МЕРЕЖІ**

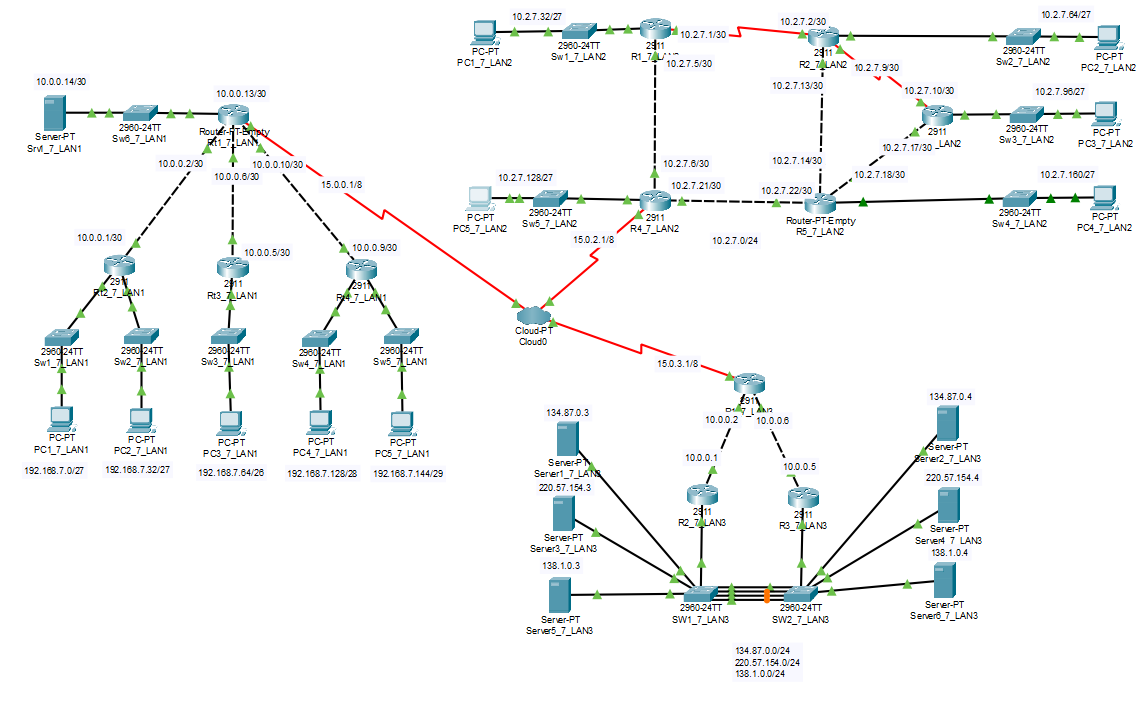


Рисунок А.1 Загальний вигляд розробленої мережі