

Міністерство освіти і науки України  
Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки

## **ПОЯСНЮВАЛЬНА ЗАПИСКА**

до випускної кваліфікаційної роботи бакалавра  
на тему: «Проект мережної інфраструктури міського Ін-  
тернет-провайдера»

Виконав студент 4-го курсу групи КІ-4  
спеціальності 123 «Комп'ютерна інженерія»

\_\_\_\_\_ В.В. Гузюк

Керівник доцент кафедри комп'ютерної інженерії та кі-  
бербезпеки, кандидат технічних наук, доцент

\_\_\_\_\_ П.П. Топольницький

Рецензент професор кафедри комп'ютерної інженерії та  
кібербезпеки, доктор технічних наук, доцент

\_\_\_\_\_ Воротніков В.В.

Житомир – 2022

Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки  
Спеціальність 123 «Комп'ютерна інженерія»  
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач  
кафедри комп'ютерної  
інженерії та кібербезпеки  
\_\_\_\_\_ Андрій Єфіменко  
1 березня 2022 р.

## ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Гузюк Владислав Віталійович

Тема роботи: **«Проект мережної інфраструктури міського Інтернет-провай-  
дера»**

затверджена Наказом університету від 1 березня 2022 р. № 127/с

Термін здачі студентом закінченої роботи 10 червня 2022 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Топологія мережі
2. Постачальники мережного обладнання
3. Протокол віддаленого доступу SSH, Telnet

Обладнання та програмне забезпечення:

1. Cisco Packet Tracer
2. GNS3
3. Oracle VM VirtualBox

#### 4. VMware Workstation

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

| Розділ | Консультант   | Підпис, дата   |                  |
|--------|---------------|----------------|------------------|
|        |               | Завдання видав | Завдання прийняв |
| 1      | А.А. Єфіменко |                |                  |
| 2      | А.А. Єфіменко |                |                  |
| 3      | А.А. Єфіменко |                |                  |

Студент \_\_\_\_\_ В.В. Гузюк

Керівник \_\_\_\_\_ П.П. Топольницький

### Календарний план

| № з/п | Назви етапів випускної кваліфікаційної роботи                | Термін виконання етапів роботи | Примітка |
|-------|--------------------------------------------------------------|--------------------------------|----------|
| 1     | Постановка завдання                                          | 1 березня                      |          |
| 2     | Розробка плану проекту                                       | 2 березня                      |          |
| 3     | Вибір програмного забезпечення                               | 4 березня                      |          |
| 4     | Пошук теоретичної інформації                                 | 26 березня                     |          |
| 5     | Розробка проекту                                             | 20 квітня                      |          |
| 6     | Вибір обладнання                                             | 30 квітня                      |          |
| 7     | Створення в програмному додатку проекту                      | 15 травня                      |          |
| 8     | Створення в програмному додатку схеми для тестування захисту | 22 травня                      |          |
| 9     | Тестування проекту                                           | 28 травня                      |          |
| 10    | Оформлення пояснювальної записки                             | 10 червня                      |          |

Студент \_\_\_\_\_ В.В. Гузюк

Керівник \_\_\_\_\_ П.П. Топольницький

## АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи бакалавра на тему «Проект мережної інфраструктури міського Інтернет-провайдера» складається з вступу, трьох розділів, висновків, списку використаної літератури та додатку.

Текстова частина викладена на 80 сторінках друкованого тексту.

Пояснювальна записка має 12 сторінок додатків. Список використаних джерел містить 36 найменування і займає 3 сторінки. В роботі наведено 42 рисунків. Загальний обсяг роботи – 103 сторінок.

У першому розділі було розглянуто основи мережної архітектури, теоретичну інформацію про протоколи та технології.

У другому розділі розглянуто основні етапи та особливості. Розроблено фізичну та логічну топологію, систему адресації, допоміжну інфраструктуру, підсистеми захисту.

У третьому розділі вибрано обладнання. Проведено налагодження обладнання. Проведено тестування складових елементів.

Висновок містить в собі результати виконаної роботи проектування мережної інфраструктури міського Інтернет-провайдера.

У додатках представлено схему мережі, конфігураційні файли обладнання.

Ключові слова: МЕРЕЖА, ІНФРАСТРУКТУРА, ІНТЕРНЕТ-ПРОВАЙДЕР.

|           |      |                    |        |      |                                                                                |                |      |         |
|-----------|------|--------------------|--------|------|--------------------------------------------------------------------------------|----------------|------|---------|
|           |      |                    |        |      | КІК.КР.Б – 123 – 10 – ПЗ                                                       |                |      |         |
|           |      |                    |        |      |                                                                                |                |      |         |
| Змн.      | Арк. | № докум.           | Підпис | Дата |                                                                                |                |      |         |
| Розроб.   |      | Гузюк В.В.         |        |      | Проект мережі (мережної інфра-<br>структури) міського Інтернет-про-<br>вайдера | Літ.           | Арк. | Аркушів |
| Керівник  |      | П.П. Топольницький |        |      |                                                                                |                |      |         |
| Реценз.   |      | Воротніков В.В.    |        |      |                                                                                |                |      |         |
| Н. контр. |      | П.П. Топольницький |        |      |                                                                                | ФІКТ, Гр. КІ-4 |      |         |
| Затверд.  |      | Єфіменко А.А.      |        |      |                                                                                |                |      |         |

## ANNOTATION

The explanatory note to the bachelor's qualification work on the topic "City Internet Service Provider Network Infrastructure Project" consists of an introduction, three sections, conclusions, a list of references and an appendix.

The text is set out on 80 pages of printed text.

The explanatory note has 12 pages of appendices. The list of used sources contains 36 names and occupies 3 pages. The paper presents 42 figures. Total volume of work - 103 pages.

The first section discusses the basics of network architecture, theoretical information on protocols and technologies.

The second section discusses the main stages and features. Physical and logical topology, addressing system, auxiliary infrastructure, protection subsystems have been developed.

In the third section, the equipment is selected. Equipment adjustment was carried out. Testing of constituent elements was carried out.

The conclusion contains the results of the work performed by designing the network infrastructure of the city Internet provider.

The appendices present the network diagram, equipment configuration files.

Keywords: NETWORK, INFRASTRUCTURE, INTERNET PROVIDER.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 5    |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

## ЗМІСТ

|                                                                                                              |    |
|--------------------------------------------------------------------------------------------------------------|----|
| ВСТУП .....                                                                                                  | 8  |
| РОЗДІЛ 1 ТЕОРИТИЧНІ ЗАСАДИ ПОБУДОВИ МІСЬКОЇ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ .....                                    | 9  |
| 1.1 Основні мережні архітектури.....                                                                         | 9  |
| 1.2 Моделі побудови міських мережних інфраструктури інтернет-провайдера .....                                | 14 |
| 1.3 Технології та протоколи побудови міських мереж.....                                                      | 16 |
| РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ МІСЬКОГО ІНТЕРНЕТ-ПРОВАЙДЕРА.....                          | 51 |
| 2.1 Особливості та етапи проектування мережної інфраструктури міського інтернет-провайдера.....              | 51 |
| 2.2 Розробка фізичної та логічної топології мережі .....                                                     | 53 |
| 2.3 Розробка схеми адресації.....                                                                            | 58 |
| 2.4 Розробка допоміжної сервісної інфраструктури та підсистем захисту .....                                  | 60 |
| РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ПРАЦЕЗДАТНОСТІ МІСЬКОЇ МЕРЕЖІ ІНТЕРНЕТ-ПРОВАЙДЕРА ..... | 61 |
| 3.1 Вибір обладнання та програмного забезпечення для розробки проекту мережної інфраструктури.....           | 61 |
| 3.2 Базове налагодження мережних пристроїв.....                                                              | 68 |
| 3.3 Налagodження засобів підсистем захисту.....                                                              | 71 |
| 3.4 Тестування складових елементів мережної інфраструктури.....                                              | 77 |
| ВИСНОВКИ.....                                                                                                | 85 |
| СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ .....                                                                         | 86 |
| ДОДАТКИ.....                                                                                                 | 89 |

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 6    |

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

FE – Fast Ethernet

GE – Gigabit Ethernet

OSPF – OpenShortestPathFirst

PON – PassiveOpticalNetwork

VLAN – Virtual Local Area Network

SSH – Secure SHell

AAA – authentication, authorization, accounting

DHCP – Dynamic Host Configuration Protocol

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 7    |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

## ВСТУП

Актуальність теми зумовлена швидким розвитком технологій що веде за собою збільшення кількості користувачів мережі а також пристроїв які потребують інтернет підключення. Розгортання швидких, стабільних і безпечних мереж це попит на які росте через збільшення кількості інтернет сервісів.

Метою кваліфікаційної роботи є проектування мережі міського інтернет провайдер

Визначена мета обумовлює наступні завдання:

- аналіз необхідних технологій та протоколів які використовуються бля побудови інтернет мереж;
- Розбір обладнання та компаній що його виробляють
- Проектування мережі інтернет провайдер в емуляторах та симуляторах
- Тестування роботи створених мереж

**Об'єктом дослідження** є процес проектування комп'ютерних мереж та захист інформації в них, технології що використовуються при побудові та компанії що надають обладнання.

**Предметом дослідження** є мережі міського інтернет провайдер, технології FastEthernet та GigabitEthernet, OSPF, RSTP, PON, протоколи захисту обладнання та мережне обладнання таких компанії Cisco, Huawei, Juniper, BDCOM.

У процесі виконання кваліфікаційної роботи було розроблено проект міської мережі інтернет провайдер у програмному додатку Cisco Packet Tracer. Було використано наявне в програмі мережне обладнання компанії Cisco. Реалізація підсистем захисту буде реалізована в програмному додатку GNS 3.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 8    |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

# РОЗДІЛ 1 ТЕОРИТИЧНІ ЗАСАДИ ПОБУДОВИ МІСЬКОЇ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

## 1.1 Основні мережні архітектури

Мережева архітектура - досить широке поняття, яке включає в себе досить багато розділів і визначень. Воно може мати відношення, як до побудови мереж, так і до їх проектування. Але найкраще його описує таке слово як Framework. У різних словниках наводиться багато різних тлумачень цього слова, але, найчастіше, воно означає «каркас, що несе або підтримуюча конструкція, яка виступає в ролі основи будь-якої побудови».

Мережева архітектура завжди лежить в основі і є фундаментом для повноцінної роботи мережі. Найчастіше, вона складається з декількох важливих складових:

- топологія локальної мережі;
- лінійно-кабельна інфраструктура;
- активне мережеве обладнання.

При проектуванні мережі необхідно з особливою увагою вибирати всі ці компоненти мережі для оптимізації продуктивності, спрощення управління всім устаткуванням і надання можливості подальшого зростання і розвитку мережі.

Кабельно-лінійна інфраструктура - один з найважливіших ділянок всієї мережі. Неякісно спроектована або погано змонтована кабельна система може викликати багато проблем, значно ускладнити своєчасне усунення несправностей за рахунок чого можуть виникнути тривалі простої. У старих системах (таких як, наприклад, ранні стандарти Ethernet), що не бралася до уваги необхідність усунення можливих неполадок. Сучасні системи з топологією «зірка» набагато зручніші в плані експлуатації і управління.

При прокладці та монтажі кабелів необхідно строго дотримуватися існуючих стандартів, які описують зіркообразну топологію мережі. Ділянка, на якому кабелі з'єднують робочі області з телекомунікаційними розподільними шафами, назива-

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 9    |

ється розподільним. Розподільні шафи також можуть з'єднуватися між собою. Ділянка кабельної інфраструктури, що з'єднує телекомунікаційні шафи, називається магістральною.

Найчастіше, для передачі даних, застосовується мідна звита пара UTP. Існує сім категорій даного типу кабелю.

Сьогодні, найчастіше, застосовуються лише чотири категорії: 5, 5е, 6, 6а. Кабель категорії 5 являє собою 4-х парний кабель. Він застосовується в наступних типах мереж:

- 10BASE-T;
- 100BASE-TX;
- 1000BASE-T;
- в телефонних лініях.

При використанні всього 2-х пар, можна добитися швидкості передачі 100 Мбіт/с, а при використанні всіх 4-х пар - до 1000 Мбіт/с. Кабель категорії 5е найчастіше застосовується при побудові мереж через його низьку собівартість і маленького діаметру. Кабелі категорії 6 і 6а застосовуються тільки в мережах Fast Ethernet і Gigabit Ethernet.

Волоконно-оптичні мережі зараз досить широко поширені і використовуються повсюдно. Деякі оператори зв'язку стверджують, що установка оптичної лінії обходиться дешевше установки лінії побудованої на мідному кабелі UTP. Але, на жаль, все мережеве обладнання, що використовується в оптичній мережі, значно дорожче своїх аналогів, що працюють в мережах, побудованих на мідній звитій парі. Але, незважаючи на ціну, волоконно-оптична мережа має безліч переваг перед мідними кабелями. У порівнянні з витою парою вона може передавати дані на великі відстані зі значно більшою швидкістю, при цьому не вносячи в сам сигнал додаткових перешкод.

Але яке б середовище передачі даних не було б обране, потрібно не забувати про можливе зростання і розширення мережі. При створенні мережі потрібно закладати кабелі з невеликим запасом, а діаметри монтажних отворів і кабельних каналів повинні бути зроблені свідомо більше необхідного.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 10   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

Це дозволить без особливих проблем і труднощів прокласти додаткові кабелі при необхідності.

Крім кабельно-лінійної системи, важливим і обов'язковим компонентом будь-якої мережі є активне мережеве обладнання. Мости, комутатори і маршрутизатори дозволяють збільшити кількість підключених пристроїв і розділяти на сегменти трафік для підвищення продуктивності. Розуміючи відмінності між пристроями, їх особливості та специфіку відповідної архітектури мережі, можна легко визначити коли і на якій саме ділянці встановлювати те чи інше обладнання.

Мости використовуються коли необхідно об'єднати дві або більше однотипних мереж. Дані пристрої повністю прозорі для всіх мережевих протоколів. Дві мережі, які з'єднані бриджем, фізично розділені, але логічно вони утворюють одну єдину мережу. Це означає, що правила монтажу кабелів застосовні до кожної мережі окремо, а не для всіх одночасно. Мережевими протоколами, якими з'єднані кілька мереж, розглядаються як одна єдина мережа.

Мости поділяють весь потік даних на сегменти: вони пропускають тільки той трафік, який адресований пристроям, що знаходяться по інший бік мосту. Так як бриджі не пропускають локальний трафік, вони дозволяють значно знизити навантаження на мережу, що складається з декількох однотипних сегментів.

Але в мостах також є і недоліки. Один з основних недоліків полягає в тому, що вони налаштовані на передачу пакетів по широкому каналу. При деякому збігу обставин (несправності або помилки в ПЗ) це загрожує виникненню суцільного потоку ширококомовних пакетів, який призводить до стану ширококомовного шторму (Broadcast storm). Це стан, коли ширококомовні пакети заповнюють всю мережу цілком і серйозно знижують її продуктивність.

Колись мости були найбільш популярним методом з'єднання мереж. Сьогодні ж, в результаті технічного прогресу, маршрутизатори стали значно дешевше і доступніше. Багато виробників стали випускати маршрутизатори з функціями бриджів. Цей пристрій працює для підтримуваних протоколів як маршрутизатор і як бридж для інших.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 11   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

Маршрутизатор - це, найчастіше, спеціалізовані комп'ютери або ПЗ, встановлене на мережевому сервері. Вузькоспеціалізовані маршрутизатори забезпечують високу продуктивність і гнучке управління в порівнянні з програмними маршрутизаторами. Однак, ціна на останні набагато нижче і, як правило, їх продуктивності цілком вистачає для невеликих мереж.

Бриджі застосовуються для з'єднання однотипних локальних мереж, а маршрутизатори - і для однотипних, і для різнотипних. Як і мости, маршрутизатори так само фізично розділяють мережу, відмінність полягає лише в тому, що при застосуванні маршрутизаторів мережа розділяється і на логічному рівні. Маршрутизатор залишають поза передачею пакети по широкомовному каналу і дозволяють сегментувати весь трафік, що проходить через них.

Крім сегментації трафіку, маршрутизатори дозволяють створювати резервні канали між мережами. Резервні канали підвищують надійність мережі. Наприклад, коли один маршрутизатор відмовив, його функції бере на себе інший маршрутизатор. Багато маршрутизаторів мають також вбудований фільтр. Він фільтрує дані по заголовкам пакетів і інформації в ньому. Як і бриджі, маршрутизатори пропускають тільки той трафік, який адресований пристроям на іншій стороні. Це також дозволяє обмежити вплив трафіку з однієї мережі на іншу.

Для вирішення проблеми низької продуктивності мережі при нестачі пропускної здатності були розроблені комутатори. Однак, всупереч загальній думці, вони не є порятунком від усіх насущних проблем з низькою продуктивністю і забезпеченням безперебійного зв'язку в мережі.

Комутатор розділяє мережу на менші домени, в результаті чого кожен кінцевий вузол отримує більшу частку всієї сумарної пропускної спроможності. По суті, це міст з великою кількістю портів. Подібно мостам, комутатори направляють весь трафік з однієї мережі в іншу.

Існують комутатори, які передають пакет тільки після того, як приймуть його цілком. Такі комутатори використовують вид комутації іменованій «проміжна буферизація». Принцип його роботи наступний: пакет, що приймається записується в

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 12   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

пам'ять комутатора, перевіряється на помилки за допомогою спеціальних алгоритмів і тільки після цього він відправляється далі по мережі до місця адресації.

Існують також комутатори, що використовують наскрізний метод комутації. Даний вид комутації відрізняється від проміжної буферизації тим, що комутатор пересилає пакет даних в той момент, коли отримує адресу одержувача. Такий метод дає набагато менші затримки, якщо порівнювати з проміжною буферизацією, але зростає ризик того, що адресат прийме пошкоджений пакет.

Існують комутатори гібридного типу. Цей пристрій, приймаючи пакет, спочатку перевіряє його на помилки і стежить за їх кількістю. Коли загальне число помилок перевищує певний поріг, включається буферизація, яка залишається включеною до того моменту, поки кількість помилок знову не стане допустимим. Після цього, комутатори знову починають працювати як наскрізні.

У комутаторів є і кілька недоліків. Подібно мостам, вони пересилають пакети по широкомовних каналах і не забезпечують належним чином захист від стану, коли широкомовні пакети повністю заповнюють всю мережу. Крім цього, при наскрізній комутації, адресат може отримувати пошкоджений або неповний пакет даних, а при проміжній буферизації істотно знижується швидкість роботи самого пристрою[4]

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 13   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

## 1.2 Моделі побудови міських мережних інфраструктури інтернет-провай- дера

В умовах ринкової економіки суб'єктами підприємницької діяльності у галузі телекомунікацій виступають мережеві оператори та сервіс-провайдери (постачальники послуг). Вони забезпечують побудову мереж зв'язку загального користування, так званих публічних мереж (Public Network). Ці мережі призначені постачати послуги зв'язку широкому колу користувачів різних категорій.

В залежності від масштабу мережі провайдери діляться на три рівні: місцевого рівня, регіонального рівня та національного рівня.

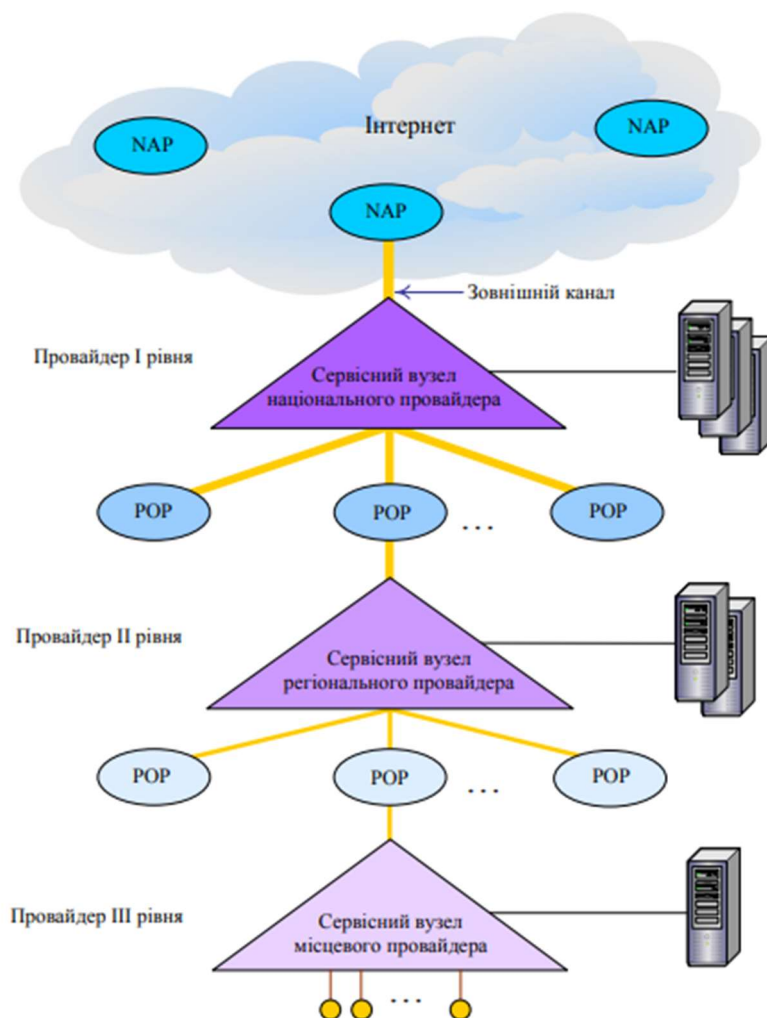


Рисунок 1.1 - Інтернет-сервіс-провайдинг

В даному проекті ми будемо розглядати провайдера місцевого рівня, однак це не означає що провайдер не може поєднувати всі рівні для збільшення прибутку.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 14   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

Оскільки даний проекти передбачає проектування мережі міської то нехай наш провайдер буде розглядатись як провайдер місцевого рівня.

На рівні найбільш узагальненого уявлення, будь-яка мережа складається з сукупності пунктів і з'єднуючих їх ліній, взаємне розташування яких характеризує зв'язність мережі та здатність забезпечувати інформаційний обмін між різними адресатами. Така відокремлена структура мережі має назву «топология».

Для побудови мережі можуть використовуватись такі топології як:

- «точка - точка»;
- Дерево подібна;
- «кільце»;
- Коміркова;
- Змішані.

Най доцільніше при побудові використовувати змішаний тип топології, це може додати зручності при побудові мережах району чи іншої територіальної одиниці, але може ускладнить обслуговування самої мережі.

Також важливою частиною є логічна топология мережі. Від неї залежить яким чином буде рухатись інформація в межах мережі від джерела до одержувача. Типи логічних топологій:

- логічну шину;
- логічне кільце;
- комутовану топологию;

Слід зазначити що фізична та логічна топология можуть як збігатися так і не збігатися.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 15   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

### 1.3 Технології та протоколи побудови міських мереж

Для побудови міських мережі необхідно використовувати велику кількість протоколів та технологій для забезпечення передачі інформації, такими є:

- FastEthernet та GigabitEthernet;
- Протоколи IPv4 і IPv6;
- Протокол OSPF;
- Протоколи STP та RSTP;
- Технологія PON.

FastEthernet — термін, що описує набір стандартів Ethernet для пакетної передачі даних з номінальною швидкістю 100 Мбіт/с, що в 10 разів швидше за початкову для Ethernet швидкість у 10 Мбіт/с. Класичний 10-мегабитний Ethernet влаштував більшість користувачів на протязі близько 15 років. Проте на початку 90-х років почала відчуватися його недостатня пропускна спроможність. Для комп'ютерів на процесорах Intel 80286 або 80386 з шинами ISA (8 Мбайт/с) або EISA (32 Мбайт/с) пропускна спроможність сегменту Ethernet складала 1/8 або 1/32 каналу “пам'ять-диск”, і це добре узгоджувалося із співвідношенням об'ємів даних, що обробляються локально, і даних, передаваних по мережі. Для могутніших клієнтських станцій з шиною PCI (133 Мбайт/с) ця частка впала до 1/133, що було явно недостатньо. Тому багато сегментів 10-мегабитного Ethernet стали переобтяженими, реакція серверів в них значно впала, а частота виникнення колізій істотно зросла, ще більш знижуючи корисну пропускну спроможність.[10]

Назріла необхідність в розробці Ethernet, тобто технології, яка була б такою ж ефективною по співвідношенню ціна/якість при продуктивності 100 Мбіт/с. В результаті пошуків і досліджень фахівці розділилися на два табори, що врешті-решт привило до появи двох нових технологій – FastEthernet і 100VGAnyLAN. Вони відрізняються ступенем спадкоємності з класичним Ethernet.

Осіною 1995 року комітет IEEE 802.3 прийняв специфікацію FastEthernet як стандарт 802.3и. який не є самостійним стандартом, а є доповненням до існуючого стандарту 802.3 у вигляді розділів з 21 по 30.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 16   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

Fast Ethernet повністю сумісна з класичним Ethernet, зміни відбулися лише на фізичному рівні, описана в стандартах 802.3, 802.4.

Мережі Fast Ethernet орієнтуються на зіркоподібну та ієрархічну фізичні топології. Логічна топологія залишається шинною для випадку використання концентраторів, коли ж застосовуються комутатори, мережі називаються комутованими.

FastEthernet – це набір стандартів передачі даних в комп’ютерних мережах зі швидкістю до 100 Мб/с. Описаний в стандарті IEEE 802.3u як доповнення до стандарту IEEE 802.3 з 21 по 33 розділ.

Встановлено три різні специфікації для фізичного рівня для підтримки наступних етапів кабельних систем на витій парі:

- 100Base-TX;
- 100Base-T4;
- 100Base-T2.

Як середовище Fast Ethernet може використовувати звиту пару 3-ї категорії (4 пари провідників), 5-ї категорії (2 пари провідників) та волоконно-оптичний кабель (2 волокна). Вони представлені на рисунках 1.2 та 1.3.

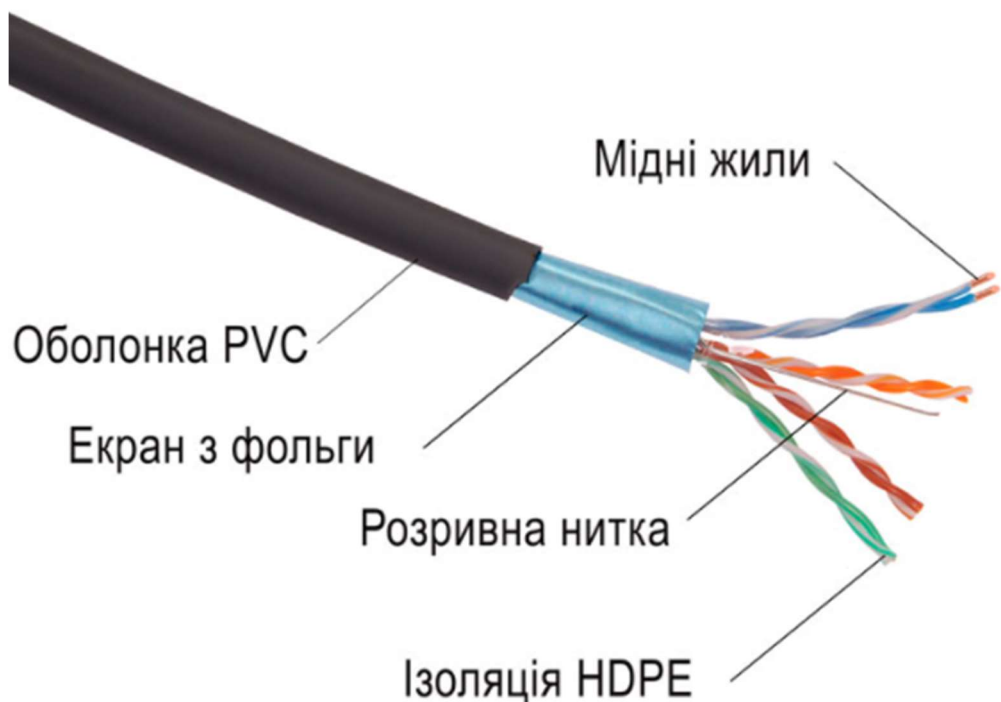


Рисунок 1.2 – Конструкція звитої пари

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 17   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

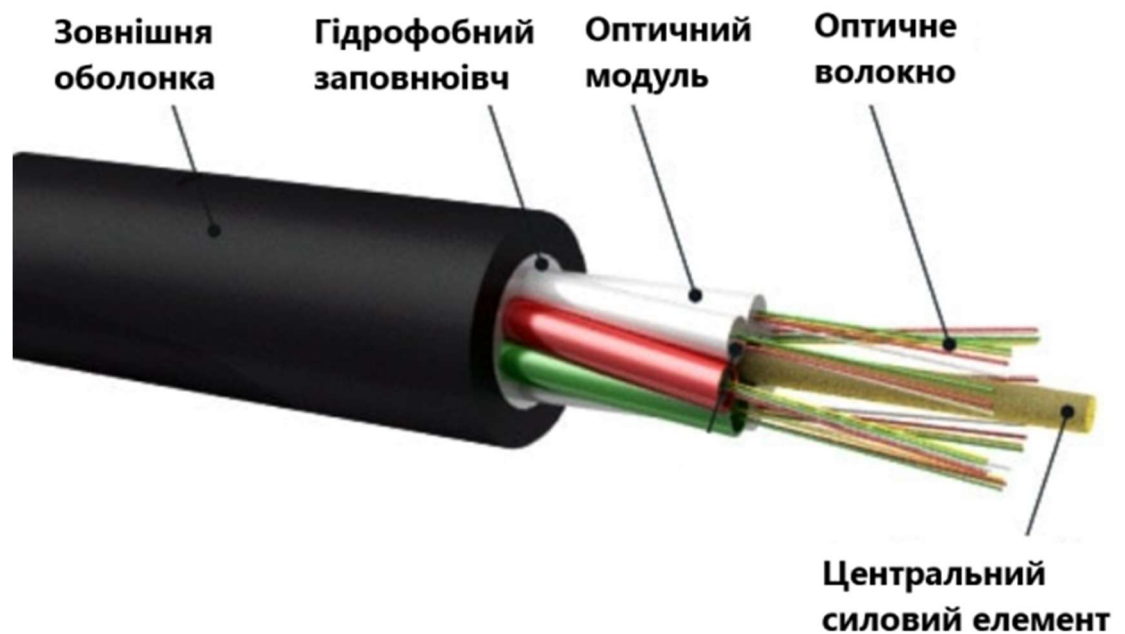


Рисунок 1.3 – Конструкція волоконно-оптичного кабеля

Основною відмінністю Fast Ethernet від Ethernet є зменшення бітового інтервалу (в 10 разів) до 0,01 мкс, що вплинуло на складність фізичного рівня і довжину мережі.

Правила коректної побудови сегментів мереж Fast Ethernet включають:

- обмеження на максимальні довжини сегментів, що з'єднують DTE з DTE;
- обмеження на максимальні довжини сегментів, що з'єднують DTE з портом повторювача;
- обмеження на максимальний діаметр мережі;
- обмеження на максимальне число повторювачів і максимальну довжину сегмента, що з'єднує повторювачі.

Структуру фізичного рівня Fast Ethernet представлено на рисунку 1.4, де:

- Узгодження – підрівень рівень узгодження;
- МПІ – незалежний від середовища інтерфейс;
- PCS – підрівень кодування;
- PMD – підрівень залежності фізичного середовища;

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 18   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

- Автопереговори – підрівень автопереговорів про швидкість передачі;
- MDI – роз’єм;
- PHY – пристрій фізичного рівня (трансивер).
- PCS – підрівень логічного кодування даних, який перетворює байти, отримані від рівня MAC в символи коду 4В/5В або 8В/6В.

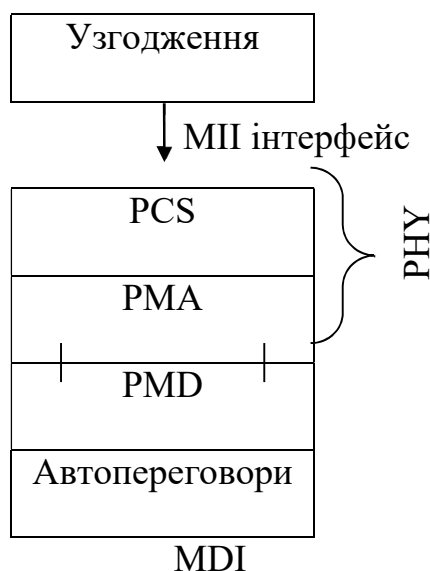


Рисунок 1.4 – Структура фізичного рівня Fast Ethernet

Рівень узгодження необхідний для того, щоб рівень MAC розрахований на інтерфейс АVІ міг працювати з фізичним рівнем через інтерфейс МІІ.

Підрівні фізичного під’єднання РМА та РМД забезпечують формування сигналів у відповідності з методом фізичного кодування (MLT-3, NRZI, рисунок 1.5).

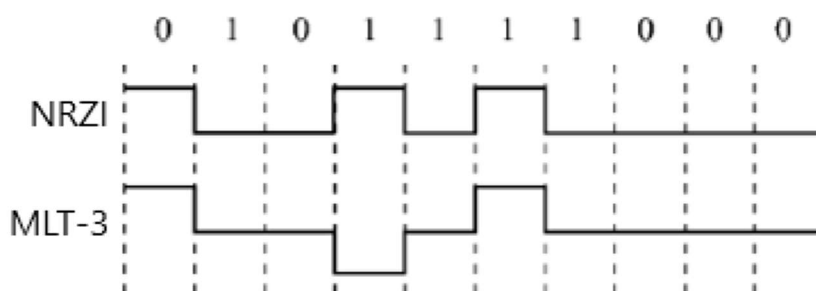


Рисунок 1.5 – Методи фізичного кодування MLT-3, NRZI

Підрівень автопереговорів служить для автоматичного визначення швидкості і методу передачі. Переговорний процес відбувається при включенні пристроїв (на-явності живлення).

В Fast Ethernet на відміну від класичного Ethernet ознакою вільного середовища є наявність символу простого джерела Idle. Для виділення початку і кінця кадру використовуються значущі символи (рисунк 1.6).

|                |    |           |     |    |    |     |      |     |   |                |
|----------------|----|-----------|-----|----|----|-----|------|-----|---|----------------|
| Преамбула Idle | JK | Преамбула | SFD | DA | SA | L/T | Дані | CRC | T | Преамбула Idle |
|----------------|----|-----------|-----|----|----|-----|------|-----|---|----------------|

Рисунок 1.6 – Формат кадру Fast Ethernet

- SFD (Start of Frame Delimiter) – Роздільник початку кадру;
- DA (Destination Address) – Адреса призначення;
- Дані – Поле даних;
- SA – Адреса відправника (тільки унікальна);
- Тип – Тип протоколу вищого рівня.

Основні специфікації технології Fast Ethernet представлено у таблиці 2.1.

Таблиця 1.1 – Основні технології Fast Ethernet

| Специфікація | Середовище              | Кількість провідників, роз'єм | Допустима довжина сегменту, м | Логічне кодування | Фізичне кодування |
|--------------|-------------------------|-------------------------------|-------------------------------|-------------------|-------------------|
| 100Base-TX   | UTP cat.5<br>STP Type 1 | 2 пари,<br>RJ-45              | 100                           | 4B/5B             | MLT-3             |
| 100Base-T4   | UTP cat.3 і вище        | 4 пари,<br>RJ-45              | 100                           | 8B/6B             | NRZI              |
| 100Base-SX   | MMF (світлодіод)        | 1 пара,<br>Duplex SC          | 300                           | 4B/5B             | NRZI              |
| 100Base-LX   | SMF                     | 1 пара,<br>Duplex SC          | 15 км<br>(Duplex)             | 4B/5B             | NRZI              |
| 100Base-FX   | MMF (лазер)             | 1 пара,<br>Duplex SC          | 412, 2000<br>(Duplex)         | 4B/5B             | NRZI              |
|              | SMF (лазер)             |                               | 100 км                        |                   |                   |

Fast Ethernet слід застосовувати в організаціях і частинах мереж, де до цього широко застосовувався простий Ethernet, але сьогоdnішні умови або ж найближчі перспективи вимагають у цих частинах мереж більш високої пропускної здатності.

Проте технологія Fast Ethernet крім позитивних властивостей, успадкувала і недоліки технології Ethernet:

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 20   |

- великі затримки доступу до середовища при коефіцієнті використання середовища вище 30 ...40%, Що є наслідком застосування алгоритму доступу CSMA / CD;
- невеликі відстані між вузлами навіть при використанні оптоволокна внаслідок методу виявлення колізій;
- відсутність визначення надлишкових зв'язків у стандарті і відсутність підтримки пріоритетного трафіку додатків реального часу.

Досить швидко після появи на ринку продуктів Fast Ethernet мережеві інтегратори й адміністратори відчули певні обмеження при побудові корпоративних мереж. У багатьох випадках сервери, підключені по 100-мегабітного каналу, переважали магістралі мереж, що працюють також на швидкості 100 Мбіт/с — магістралі FDDI і Fast Ethernet. Відчувалася потреба в наступному рівні ієрархії швидкостей.

Перша версія стандарту була розглянута в січні 1997 року, а остаточно стандарт 802.3z був прийнятий 29 червня 1998 року на засіданні комітету IEEE 802.3. Роботи з реалізації Gigabit Ethernet на кручений парі категорії 5 були передані спеціальному комітету 802.3ab, що вже розглянув кілька варіантів проекту цього стандарту, причому з липня 1998 року проект придбав досить стабільний характер.

Не чекаючи прийняття стандарту, деякі компанії випустили перше устаткування Gigabit Ethernet на оптоволоконому кабелі вже до літа 1997 року.

Основна ідея розробників стандарту Gigabit Ethernet складається в максимальному збереженні ідей класичної технології Ethernet при досягненні бітової швидкості в 1000 Мбіт/с.

Тому що при розробці нової технології природно очікувати деяких технічних новинок, що йдуть у загальному руслі розвитку мережних технологій, те важливо відзначити, що Gigabit Ethernet, так само як і його менш швидкісні побратими, на рівні протоколу не буде підтримувати:

- якість обслуговування;
- надлишкові зв'язки;

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузок В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 21   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

— тестування працездатності вузлів і устаткування (в останньому випадку — за виключенням тестування зв'язку порт — порт, як це робиться для Ethernet 10Base-T і 10Base-F і Fast Ethernet).

Головна ідея розробників технології Gigabit Ethernet полягає в тому, що існує і буде існувати дуже багато мереж, у яких висока швидкість магістралі і можливість призначення пакетам пріоритетів у комутаторах будуть цілком достатні для забезпечення якісного транспортного обслуговування всіх клієнтів мережі. І тільки в тих рідких випадках, коли і магістраль досить завантажена, і вимоги до якості обслуговування дуже тверді, потрібно застосовувати технологію АТМ, що дійсно за рахунок високої технічної складності дає гарантії якості обслуговування для всіх основних видів трафіка.

Gigabit Ethernet на рівні протоколу не підтримує:

- якість обслуговування;
- надлишкові зв'язку;
- тестування працездатності вузлів і устаткування (в останньому випадку - за винятком тестування зв'язку порт-порт, як це робиться в Ethernet 10Base-T і 10Base-F і FastEthernet).

У технології GigabitEthernet в порівнянні з технологіями Ethernet і FastEthernet:

- зберігаються всі формати кадрів Ethernet;
  - зберігається напівдуплексна версія протоколу, що підтримує метод доступу CSMA / CD, і повнодуплексна версія, що працює з комутаторами;
- підтримуються всі основні види кабелів, використовуваних в Ethernet і FastEthernet: волоконно-оптичний, вита пара категорії 5 і коаксіальний кабель.

Існують чотири різних фізичних стандартів для Gigabit Ethernet, використовуючи оптоволокні (1000Base-X) кабель, вита пара (1000Base-T), або збалансований мідний кабель (1000Base-CX).

В IEEE 802.3z стандарт включає 1000Base-SX для передачі багатоходового волокна, 1000Base-LX для передачі одномодового волокна, і майже застарілих

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 22   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

1000Base-CX для передачі збалансованим мідним кабелем. Ці стандарти використовують 8b/10b кодування, який розширює канал на 25%, з 1000 Мбіт / с до 1250 Мбіт / с для забезпечення DC збалансованого сигналу. Символи надіслано з допомогою NRZ.

Особливо складним була реалізація технології Gigabit Ethernet для звитої пари, оскільки накладалося обмеження на середовища (cat-5e 125 МГц, 4 пари провідників). Обмеження були обійдені за рахунок використання сучасних цифрових сигнальних процесорів та методу кодування PAM-5 (рисунок 1.7).

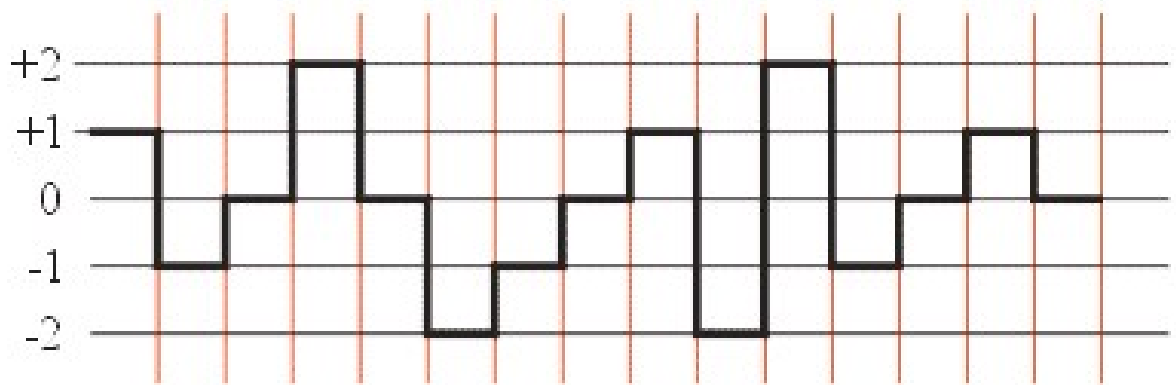


Рисунок 1.7 – Кодування п'ятирівневним сигналом PAM-5

PAM-5 має 5 рівнів і дозволяє передавати на одному рівні 2 біти.

Основні специфікації технології Gigabit Ethernet представлені у табл. 1.2.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 23   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

Таблиця 1.2 - Основні технології Gigabit Ethernet

| Специфікація | Середовище                               | Довжина хвилі | Кабель   | Допустима довжина |
|--------------|------------------------------------------|---------------|----------|-------------------|
| 1000Base-SX  | MMF                                      | 850 нм        | 62,5/125 | 2-220 м           |
|              |                                          |               | 50/125   | 2-500 м           |
| 1000Base-LX  | SMF                                      | 1300 нм       | 9/125    | 2-5000 м          |
|              | MMF                                      | 1300 нм       | 62,5/125 | 2-550 м           |
|              |                                          |               | 50/125   |                   |
| 1000Base-LN  | SMF                                      | 1300 нм       | 9/125    | 1-49 км           |
|              |                                          | 1550 нм       |          | 50-100 км         |
| 1000Base-CX  | Твіаксіальний кабель                     | —             | —        | 25 км             |
| 1000Base-T   | Звита пара (cat-5, cat-5e, cat-6, cat-7) | —             | 4 пари   | 100 м             |

1000Base-T, IEEE 802.3ab — стандарт, що використовує виту пару категорій 5е. У передачі даних беруть участь 4 пари. Швидкість передачі даних — 250 Мбіт/с по одній парі. Використовується метод кодування РАМ5, частота основної гармоніки 62,5 МГц. Відстань до 100 метрів. На рисунку 1.8 показана структура рівнів Gigabit Ethernet. Як і в стандарті Fast Ethernet, в Gigabit Ethernet не існує універсальної схеми кодування сигналу, яка була б ідеальною для всіх фізичних інтерфейсів - так, з одного боку, для стандартів 1000Base-LX/SX/CX використовується кодування 8В/10В, а з іншого боку, для стандарту 1000Base-T використовується спеціальний розширений лінійний код ТХ/Т2. Функцію кодування виконує підрівень кодування PCS, розміщений нижче за середовищенезалежного інтерфейса GМІІ.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 24   |

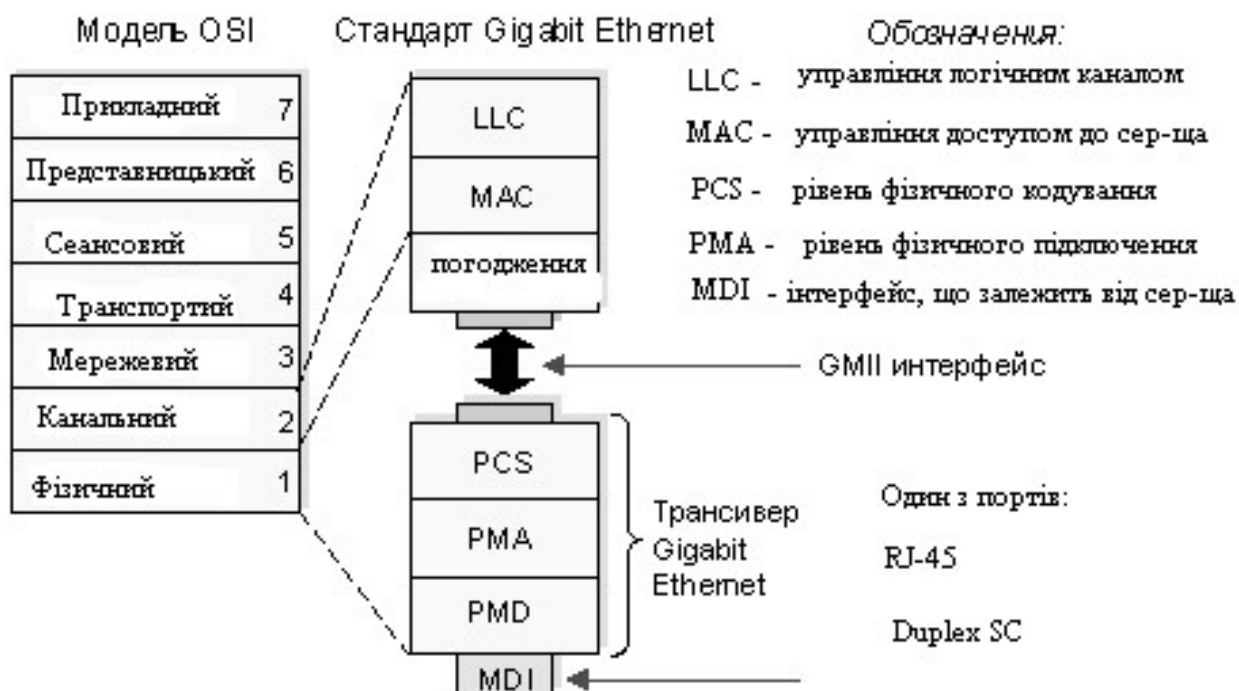


Рисунок 1.8 - Структура рівнів стандарту Gigabit Ethernet

Фізичний рівень Gigabit Ethernet використовує декілька інтерфейсів, включаючи традиційну виту пару категорії 5, а також багатомодове і одномодове волокно. Підрівень PMD визначає оптичні/електричні характеристики фізичних сигналів для різних середовищ. Всього визначаються 4 різних типи фізичних інтерфейсів середовища.

Формат кадру Gigabit Ethernet представлено на рисунку 1.9.

| Преамбула SFD | Адреса призначення | Адреса відправника | L/T | Дані           | FCS     | Розширення носія |
|---------------|--------------------|--------------------|-----|----------------|---------|------------------|
| 8 + 1 байт    | 6 байт             | 6 байт             | 2   | 46 - 1500 байт | 4 байти |                  |

Рисунок 1.9 – Формат кадру Gigabit Ethernet

L/T – довжина поля даних / тип поля даних.

Gigabit Ethernet на рівні протоколу не підтримує:

- якість обслуговування;
- надлишкові зв'язку;
- тестування працездатності вузлів і устаткування (в останньому випадку

- За винятком тестування зв'язку порт-порт, як це робиться в Ethernet 10Base-T і 10Base-F і FastEthernet).

Якщо порівнювати Gigabit Ethernet та його попередників, то в них збереглися наступні спільні риси:

- збережені всі формати кадрів Ethernet;
- існують напівдуплексна та дуплексна версії;
- підтримуються основні середовища (звита пара, волоконно-оптичний кабель).

Відмінності:

- бітові інтервали становлять 0,001 мкс (1 нс);
- мінімальний розмір кадру збільшений з 64 до 512 байтів;
- дозволяється передача кількох кадрів підряд (сумарною довжиною до 8192 байти) без передачі середовища іншим станціям.[11]

Протоколи IPv4 і IPv6. Оригінальна версія Internet Protocol була вперше розгорнута в 1983 році в ARPANET, тобто Internet Protocol версії 4 (IPv4). IPv4 - четверта версія IP-адреси з обмеженням 4 мільярди IP-адрес. IPv4-адреса виражається у 32-бітному цілому значенні та записується у крапково-десяткові позначення, що складається з чотирьох груп октетів восьми значущих адрес, виражених незалежно у десяткових нотах. і розлучається крапками. Діапазони можуть бути від 0 до 255.

Приклад: IP-адреса 105.249.119.16 представляє 32-розрядне десяткове число, а в двійковій - 01101001.11111001.01110111.00010000.

Далі наведено схематичне пояснення заголовка дейтаграми:

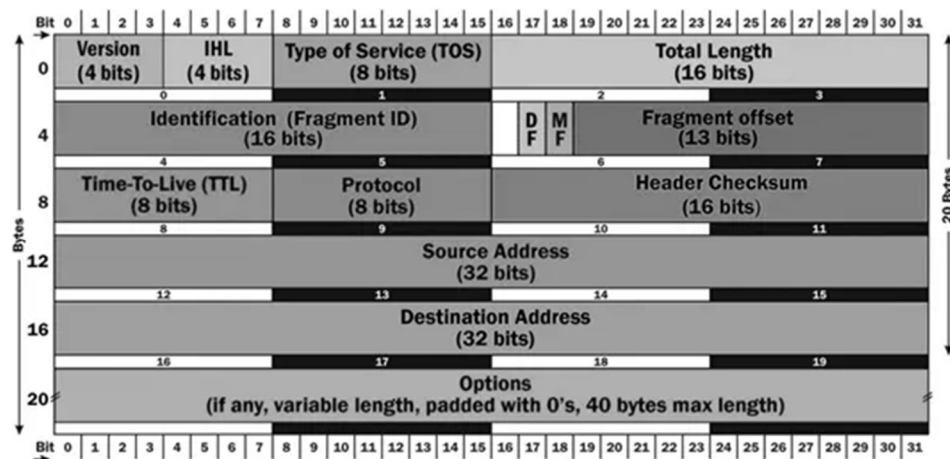


Рисунок 1.10 – Заголовок дейтаграми ipv4

Заголовок дейтаграми ipv4 у табличному форматі нижче:

Таблиця 1.3 - Заголовок дейтаграми ipv4

|                                                |                                                                                                                                                                                                                                                        |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Версія</b>                                  | Це 4-бітове поле, і воно говорить про версію IP, яку ми використовуємо.                                                                                                                                                                                |
| <b>HLen</b>                                    | Це дає довжину заголовка. Мінімальна довжина заголовка повинна становити 20 байт, оскільки максимальний розмір заголовка у 4 біти дорівнює 15. Якщо ми будемо використовувати поле параметрів, максимальною довжиною заголовка буде 60 байт (20 + 40). |
| <b>Тип послуги</b>                             | Перші 3 біти вказують на пріоритет, а наступні 4 біти вказують на тип послуги, а останні біти не використовуються. 4 біти послуг визначають затримку, пропускну здатність, надійність, вартість.                                                       |
| <b>Загальна довжина</b>                        | Поле загальної довжини визначає загальну довжину дейтаграми, включаючи заголовок. загальна довжина може бути обчислена як довжина даних + довжина заголовка або довжина даних = загальна довжина - довжина заголовка 16 біт                            |
| <b>Ідентифікація (ідентифікатор фрагмента)</b> | Оскільки IPv4 - послуга дейтаграми, ці біти допомагають однозначно ідентифікувати, коли фрагментація закінчується на пакети дейтаграм.                                                                                                                 |
| <b>Прапори</b>                                 | Прапор вказує на фрагментацію за допомогою ідентифікаційного поля, в основному вказує, чи може бути фрагментований чи поточний - остаточним.                                                                                                           |
| <b>Зсув фрагмента</b>                          | Положення сусіда кожного фрагмента вимірюється від початку вихідних даних одиницями у 8 байт.                                                                                                                                                          |

### Продовження таблиці 1.3

|                                   |                                                                                                                                                                                                                                                    |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Час жити</b>                   | Це допомагає неправильно керувати транзакціями дейтаграм. Він вимірює кількість файлів no.of.routers, через які може пройти дейтаграма. Він перевіряє, зменшуючи значення до 1, поки не досягає 0. Даніграма відміняється, коли вона досягає нуля. |
| <b>Протокол</b>                   | IPv4 містить дані з різних протоколів. Це поле допомагає мережевому шару зрозуміти, які дані належать до якого протоколу.                                                                                                                          |
| <b>Заголовок контрольної суми</b> | Це поле використовується для виявлення помилок у пакетах чи повідомленнях.                                                                                                                                                                         |
| <b>IP-адреса джерела</b>          | 32-розрядна адреса хоста, що відправляє.                                                                                                                                                                                                           |
| <b>Ip адреса призначення</b>      | 32-розрядна адреса приймаючого хоста.                                                                                                                                                                                                              |
| <b>Параметри</b>                  | Кожна датаграма не вказує поле опцій. Саме перелік специфікацій містить обмеження безпеки, маршрутизацію тощо.                                                                                                                                     |

#### Обмеження IPv4:

- Нестача адресного простору: адресний простір швидко вичерпується, оскільки кількість пристроїв, підключених до Інтернету, швидко зростає.
- Слабка розширюваність протоколу: недостатній розмір заголовка IPv4, не вміщує необхідні додаткові параметри no.of.
- Проблема з обмеженням безпеки для комунікацій: Інформація не має обмеженого доступу, який розміщується в мережі. Спочатку розроблений для ізолюваних військових мереж. Потім адаптували до мережі громадської освіти та досліджень.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 28   |

– Відсутність якісної підтримки в сервісі: затримка пропускну здатності інформації та певних мереж не підтримує цю причину.

– Географічні обмеження: Оскільки він створений у США, він передбачає розповсюдження IP-адреси, і майже 50% зарезервовано для Сполучених Штатів.

#### Переваги IPv4:

– Надійна безпека: цей пакет адрес має шифрування даних для підтримання конфіденційності та безпеки під час комунікації із загальнодоступними засобами масової інформації.

– Великі завдання щодо маршрутизації: велика кількість функціональних маршрутизаторів робить це Інтернет-ланкою, і, таким чином, він має життєво важливу мережу, інфраструктура залежить від ієрархічної та плоскої маршрутизації, також стає легко підключати кілька пристроїв у великій мережі без NAT.

– Відео бібліотеки та конференції: Збільшення кількості користувачів Інтернету сповільнює онлайн-передачу даних. Ця модель зв'язку забезпечує якісне обслуговування та ефективну передачу даних. Послуги TCP & UDP використовуються в більшості випадків; незважаючи на обмежений функціонал, адреси IPv4 переосмислюються і дозволяє шифрувати дані.

– Гнучкість: маршрутизація IPv4 є більш масштабованою та ефективною, оскільки адресація об'єднується. Зокрема, добре працює для передачі даних та передачі даних між мережами в організації.[1]

Інтернет-протокол версії 6 – це нова версія протоколу мережевого рівня, що дозволяє здійснювати передачу інформації через мережу. Незважаючи на те, що його розробка розпочалася ще в 1998 році, він почав заміщати протокол IPv4 лише в 2017 році.

Очікувалось, що до 2010 року всі варіанти унікальних IPv4-адрес будуть вичерпані та використовуватимуться користувачами.

Для вирішення цієї проблеми був створений новий протокол мережевого рівня, щоб уможливити надання додаткових унікальних адрес, саме це і стало початком протоколу IPv6.

Існує три класи IPv6-адрес:

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 29   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

– Unicast – індивідуальна адреса, використовується для передачі пакета до конкретного інтерфейсу хоста.

– Multicast – групова адреса, використовується для одночасної передачі пакетів від одного відправника до багатьох хостів-отримувачів, які мають однакову групову адресу.

– Anycast – альтернативна адреса, принцип роботи якої схожий до групової адреси, проте, пакет даних доставляється до найближчого від відправника інтерфейсу

Відмінності IPv4 і IPv6:

– 128 біт в IPv6-адреси є вісім 16-бітових шістнадцяткових блоків, розділених двокрапкою. Наприклад, 2dfc: 0: 0: 0: 0217: cbff: fe8c: 0. Традиційною формою запису IPv4 адреси є запис у вигляді чотирьох десяткових чисел (від 0 до 255), розділених крапками. Через дріб вказується довжина маски підмережі. Наприклад, 192.168.0.0/16.

– У IPv4 для мультимовлення зарезервована підмережа 224.0.0.0/4. IPv6 для цієї мети використовує вбудований адресний простір FF00 :: / 8;

– IPv4 використовує широкомовні адреси для передачі широкомовних пакетів, IPv6 - багатоадресні групи;

– IPv4 використовує 0.0.0.0 як невизначену адресу, а 127.0.0.1 для створення адреси зворотного зв'язку (loopback). В IPv6 використовуються :: і :: 1 відповідно;

– IPv4 використовує глобально унікальні публічні адреси для трафіку і «приватні» адреси, IPv6 - глобально унікальні юнікаст-адреси і локальні адреси (FD00 :: / 8).

Переваги IPv6 перед IPv4:

– Більш ефективна маршрутизація без фрагментації пакетів;

– Вбудована технологія Quality of Service (QoS), яка визначає чутливі до затримки пакети;

– Усунення NAT для розширення адресного простору з 32 до 128 біт;

– Вбудована підтримка IPsec (використання IPsec опціонально);

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузіук В.В.        |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 30   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

- Автоконфігурація адрес для спрощення адміністрування мережі;
- Покращена структура заголовка з меншими витратами на обробку.

Після запуску IPv6 з'явилася вбудована можливість шифрувати інтернет-трафік за допомогою поширеного стандарту шифрування IPSec, який не дає прочитати вміст трафіку при його перехопленні. Однак шифрування і розшифрування даних вимагає обладнання, яке коштує грошей. До того ж IPSec можна реалізувати і на IPv4, що в теорії означає, що IPv4 і IPv6 однаково безпечні.

Деякі експерти стверджують, що поки перехід не завершений, користувачі шостої версії знаходяться в більшій небезпеці, ніж користувачі четвертої. Провайдери можуть використовувати IPv6-тунелі для надання користувачам IPv4 доступу до IPv6-контенту. Зловмисники можуть використовувати ці тунелі для проведення своїх атак.

Ще одна потенційна проблема пов'язана з автоконфігурацією - новою функцією IPv6. Вона дає їм змогу самостійно призначати собі IP-адресу на основі MAC-адреси, що може бути використано сторонніми особами для відстеження певних користувачів. Проте на пристроях під управлінням популярних операційних систем вже встановлені розширення конфіденційності, тому для більшості людей це не буде проблемою.

Основною причиною відсутності повного переходу на IPv6 є вартість обладнання. Щоб оновити всі сервери, маршрутизатори і комутатори, які весь цей час залежали тільки від IPv4, потрібно безліч грошей і часу.

Крім того, щоб впоратися з нестачею адрес, провайдери призначають користувачам динамічну адресу, яка може змінюватися при підключенні до іншої мережі. Після відключення від мережі пристрої звільняють свою адресу, роблячи його доступним для інших пристроїв. По суті ви орендуєте, але не володієте адресою. Це сильно уповільнює перехід з IPv4 на IPv6.[2]

Протокол динамічної маршрутизації OSPF на основі технології відстежування стану каналу та використання алгоритму Дейкстри для знаходження найкращого маршруту.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 31   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

OSPF включає в себе великий список можливостей для налаштування.

OSPF є:

- Відкритим;
- Динамічним;
- Протоколом з врахуванням стану каналу;
- Внутрішньо шлюзовим протоколом;
- Ієрархічним;
- Наявна можливість забезпечити розподіл навантаження по каналам передачі з однаковою вартістю (метрикою);
- Має засоби захисту;
- Підтримує мереж різних типів;
- Підтримка VLSM та CIDR.
- Підтримка інкапсуляції IP.
- Підтримка передачі по всіх фізичних середовищах.
- Передача між маршрутизаторами не всієї таблиці, а лише її зміни.
- Потребує меншого об'єму трафіку.
- Велика масштабованість.

Поділяючись на зони протокол покращує роботу мережі зменшуючи навантаження на ЦП, зменшує розмір таблиць маршрутизації та кількість пакетів повідомлень про стан каналу.

Зони:

- Магістральна зона – є центральною частиною мережу яка об'єднує між собою інші зони;
- Стандартна зона – звичайна зона, яка створюється за умовчанням;
- Тупикова зона – приймає маршрутну інформацію тільки з інших зон, а якщо необхідно передавати інформацію за кордон автономної системи користується маршрутом за умовчанням;
- Totally stubby area – схожа на тупикову але взагалі маршрутні інформацію не приймає.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 32   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

Метрика протоколу OSPF за замовчуванням метрика маршруту розраховується за стандартною формулою:

$$M = \sum_{i=1}^N \left[ \frac{RefBW}{BW_i} \right]$$

де  $M$  – метрика певного маршруту;

$N$  – кількість ділянок маршруту;

$RefBW$  – еталона пропускна здатність за замовчуванням  $10^8$  біт/с, може змінюватися адміністративно;

$BW_i$  – значення пропускної здатності  $i$ -ї ділянки, може змінюватися адміністративно.

Таким чином 1000 Мбіт/с це 1, 100 Мбіт /с це 10, 10 Мбіт /с це 100, 1 Мбіт /с це 1000.

Повідомлення протоколу OSPF необхідні для роботи маршрутизації. А саме такі:

- Hello – регулярні повідомлення для пошуку сусідніх приладів;
- Database Description DBD – перевірка синхронізації LSDB у сусідніх маршрутизаторів;
- Link state request LSR – запит LSA у сусіднього маршрутизатора. Використовується тільки увімкнутими маршрутизаторами або коли був втрачений маршрут до якоїсь мережі;
- Link state update LSU – стан зв'язків маршрутизатора.

Link State Acknowledgment LSAck – пакет-підтвердження використовується для відповіді на інші пакети.[9]

Spanning Tree Protocol (STP) (протокол кістякового дерева) — мережевий протокол, що працює на другому рівні моделі OSI. Заснований на однойменному алгоритмі, розробником якого є Радья Перлман.

Протокол був створений для запобігання петель в комутаторах.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 33   |

Принцип роботи даного протоколу оснований на тому, щоб всі надлишкові канали між комутаторами логічно блокувались і трафік по них не передавався. Для цього будується топологія у вигляді дерева(математичного графу). Для побудови протокол використовує повідомлення двох типів: BPDU – інформація про комутатори і TCN – і повідомлення про зміни топології. При ввімкненні протоколу STP, комутатори починають передавати BPDU повідомлення. Після відбувається вибір кореневого комутатора, для цього використовується інформація із BPDU повідомлень:

- Ідентифікатор відправника (Bridge ID);
- Ідентифікатор кореневого маршрутизатора (Root Bridge ID);
- Ідентифікатор інтерфейсу (Port ID);
- Вартість маршруту до кореневого маршрутизатора (Root Path Cost).

Після порівняння інформації, комутатор з найменшим пріоритетом стає кореневим комутатором. У випадку коли пріоритети збігаються порівнюються MAC-адреса.

Після вибору кореневого комутатора, він починає розсилати BPDU повідомлення для формування топології. Також під час формування топології інтерфейсам комутатора встановлюються певні стани, а саме такі як:

- Blocking — блокування. Вданому стані через інтерфейс не передаються ніякі повідомлення. Використовується для запобігання петель.
- Listening — слухання. Використовується під час вибору кореневого комутатора, передаються лише BPDU. В даному стані інтерфейс буде перебувати поки не пройде Forward delay timer, який становить 15 секунд та не буде обраний кореневий комутатор. Після чого переходить в стани — Learning.
- Learning — навчання. Приймає BPDU повідомлення, але нічого не відправляє. Вся інформація що приходить заноситься в MAC-адресів комутатора. Перехід в наступний стан відбувається також через Forward delay timer.
- Forwarding — пересилання. Основний стан інтерфейсу під час якого відбувається пересилання звичайних та службових пакетів інформації.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 34   |

Для перевірки стану мережі кореневий комутатор відправляє BPDU повідомлення кожні 2 секунди, за замовчуванням. Цей таймер називається Hello Timer. Інші комутатори отримавши це повідомлення пересилають його далі. У випадку коли комутатор не отримує це повідомлення за таймером Max Age(20 секунд за замовчуванням), це трактується як втрата зв'язку з кореневим комутатором. Після чого відбувається повторний вибір головного комутатора.

У випадках коли не кореневий комутатор помічає зміни в топології, такі як ввімкнення чи вимкнення підключення, використовуються TCN повідомлення. TCN повідомлення несуть тільки інформацію про те що в топології щось змінилось і ці повідомлення пересилаються на кореневий комутатор. TCN пересилаються тільки звичайними комутаторами для зв'язку з кореневим комутатором.[5]

RSTP більш сучасний варіант протоколу STP. Даний протокол не базується на таймерах і дозволяє всім комутаторам передавати BPDU повідомлення. Для моніторингу стану перевіряється кількість втрачених повідомлень, а механізм Proposal/Agreement використовується для переходу інтерфейсів в стан роботи без таймерів. Але в випадку коли до мережі підключено пристрій що не підтримує RSTP доводиться проходити всі етапи протоколу STP.

Для використання оптичних мереж існує технологія FTTx що є збіркою назвою для багатьох варіантів архітектури, різниця між якими відстань до кінцевої точки, куди доходить оптична лінія.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 35   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

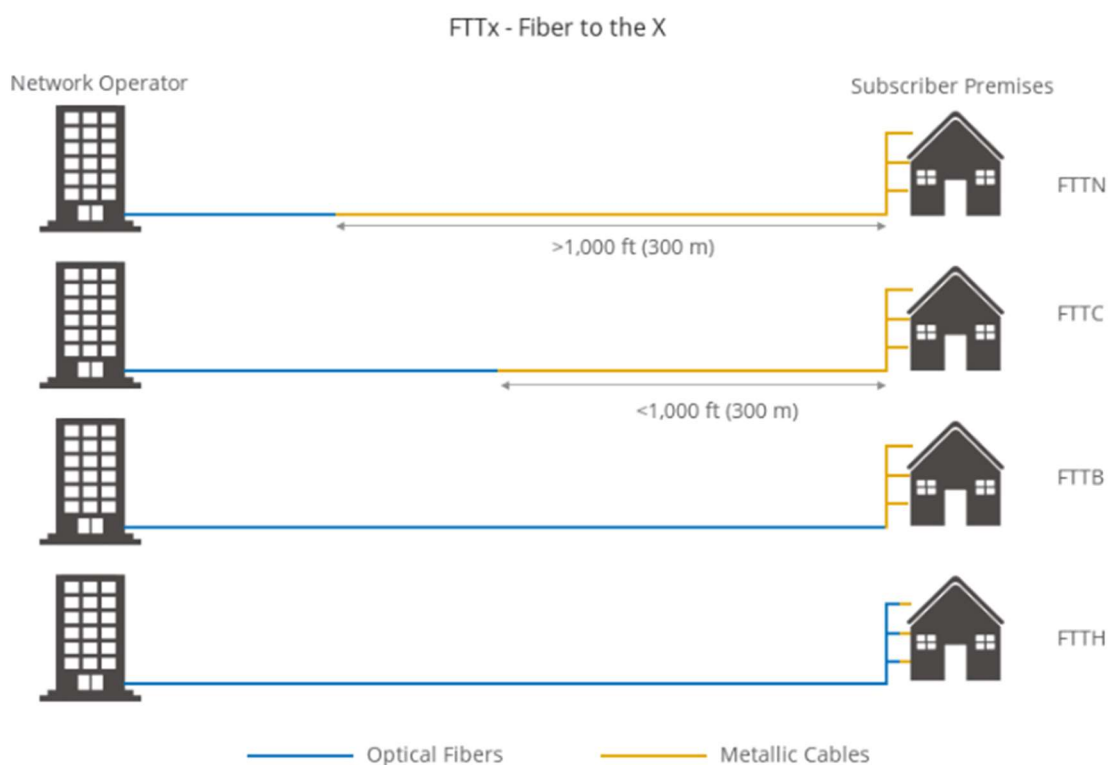


Рисунок 1.11 – Технології FTTx

Fibre to the Home (FTTH) це мережева архітектура при якій оптичний кабель доходить до житлового будинку. Мережна структура буває домашньою (Home Run), активною мережею типу зірка та пасивними оптичними мережами (PON).

FTTH – Home Run це архітектура при якій оптичне волокно напряму із офісу доходить до клієнту. Кількість клієнтів при такій побудові не велика оскільки не кожному потрібно мати найкоротший шлях до світової мережі. При побудові користувачу заводять два кабелі: один для інтернету, другий для кабельного телебачення.

FTTH – Активна зірка це архітектура при якій використовуються локальні активні вузли. Дана архітектура зменшує кількість кабелів що необхідно прокласти між користувачами та офісом провайдера однак додає активні вузли типу комутаторів що за умов використання з оптичними інтерфейсами може значно підвищити ціну мережі.

Fibre to the Antenna (FTTA) це архітектура при якій оптичне волокно під'єднують до віддаленої RRH в верхній частині вежі мобільного зв'язку.

|      |      |                    |        |      |                                 |      |
|------|------|--------------------|--------|------|---------------------------------|------|
|      |      | Гузюк В.В.         |        |      | <b>КІК.КР.Б – 123 – 10 – ПЗ</b> | Арк. |
|      |      | П.П. Топольницький |        |      |                                 | 36   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                                 |      |

Fibre to the Node (FTTN) це архітектура при якій оптичний кабель ведуть до мережного вузлу. Відстань між клієнтом і вузлом при такій побудові складає декілька кілометрів.

Fibre to the Building (FTTB) Це архітектура при якій оптичний кабель доводиться до будинку. Дана архітектура зручна у випадку підключення багато квартирних будинків. Це схоже на архітектуру FTTN, однак при побудові між користувачем є вузол від якого використовується вже мідний кабель.[35]

PON (PassiveOpticalNetwork – пасивна оптична мережа) пропонує створення розгалуженої мережі (переважно деревоподібної топології) без активних компонентів – на пасивних оптичних розгалужувачах.

Технологія PON ідеально підходить для покриття великої території з різною щільністю забудови: від багатоповерхових районів до котеджних містечків, де переваги технології розкриваються в повній мірі.

Передача та прийом в обох напрямках здійснюється, я правило, по одному оптичному волокну, але на різних довжинах хвиль (1310 та 1490 нм).

Інформація для всіх користувачів передається одночасно з часовим розподіленням каналів від головної станції – оптичного лінійного термінулу (OLT, Optical Line Terminal) - до кінцевих оптичних мережесих блоків (ONU, Optical Network Unit).

Оптична потужність з виходу OLT у вузлах мережі ділиться (рівномірно або нерівномірно) таким чином, щоб рівень сигналу на вході всіх ONU був приблизно однаковий.

Переваги технології PON:

- Економія волокон в оптичних кабелях;
- Значна економія оптичних випромінювачів на головній станції;
- Можливість надання трьох видів інформації (згідно концепції Triple Play) – голосу, відео та даних;
- Відсутність необхідності електроживлення мережесих елементів (крім кінцевих);
- Невеликі витрати на обслуговування;

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 37   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

- Проста можливість підключення абонентів;
- Подальше збільшення швидкості передачі (до 10 Гбіт/с та вище) без заміни обладнання лінійного тракту (оптичні кабелі, розгалужувачі, з'єднувачі).

GPON (Gigabit-capable Passive Optical Network) – один із широко використовуваних стандартів PON, забезпечуючий передачу даних на швидкостях прямого потоку до 2,488 Гб / с, а в зворотному - 1,244 Гб/с, з максимальним коефіцієнтом ділення 1:128.

Дана технологія використовує наступні довжини хвиль:

- 1490 нм в сторону абонента;
- 1310 нм зі сторони абонента;
- 1550 нм зарезервована для кабельного телебачення.

Основою в технології GPON є GFP (GenericFramingProtocol), а також використовується TDMA, SDH, Ethernet, ATM.

Технологія дозволяє за допомогою внутрішніх інструментів достатньо гнучкою налаштувати широкий спектр послуг, з різним пріоритетом та швидкостями.

GEPON (Gigabit Ethernet Passive Optical Network) один з різновидів технології пасивних оптичних мереж PON, що дозволяє передавати і приймати дані на швидкості (до 1,2 Гбіт / с), з максимальним коефіцієнтом ділення 1:64

Також, як і в технології GPON, дана технологія використовує 1490нм для передачі інформації, 1310нм для прийому та 1550нм також зарезервована для кабельного ТБ.

Формування кадру в GEAPON відбувається шляхом «додавання» заголовка в ETHERNET фрейм інформації, що містить в собі дані про тимчасовий слот ONU, її мак адресу і способі коригування помилок.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 38   |

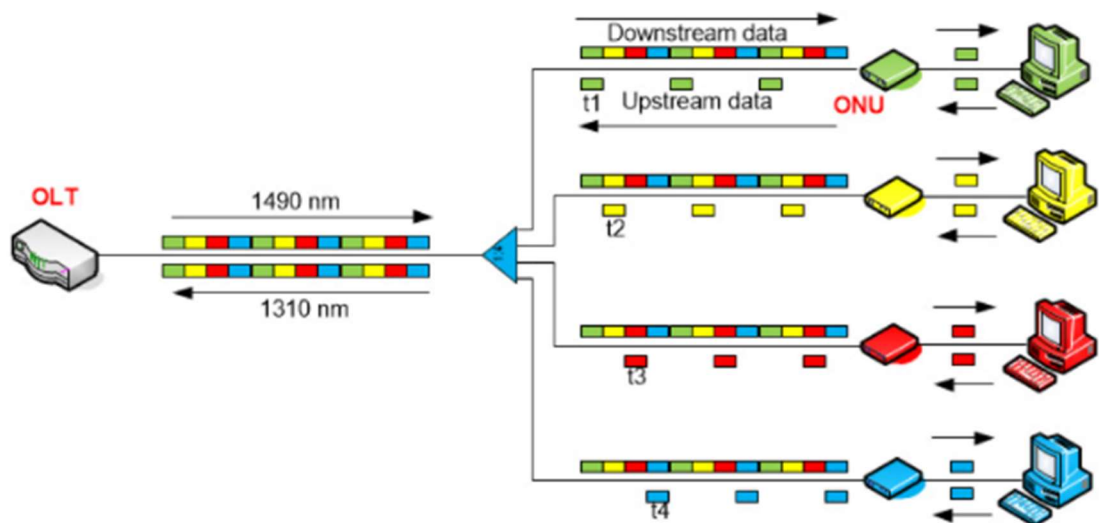


Рисунок 1.12 – Ілюстрація роботи PON

За допомогою даних двох технологій можливо побудувати широкосмгову мережу передачі даних з урахуванням потреби в певній кількості потенційно можливих клієнтів. Саме після вивчення географічних особливостей і кількість потенційних клієнтів, можна вибрати ту чи іншу технологію, так як немає необхідності використовувати в локації з кількістю Потенційних Абонентів менше 200 технологію GPON через те що мінімальна ємність GPON тисячу двадцять чотири абонента проти 256 абонентів на пристрій, в разі застосування GEPON, так само має кінцевою метою побудови мережі і тип клієнта.

У разі, якщо мережа буде використовуватися в основному для «корпоративників», то слід віддати переваги GPON через гнучкості конфігурації виходячи з вимог замовника до рівня послуг, що надаються.[7]

Розібратися також необхідно з основними допоміжними протоколами, такими як:

- Технологія VLAN;
- Протоколи SSH та Telnet;
- Протокол LACP;
- Протокол HSRP;
- Технологія RADIUS.

VLAN це мережа віртуального типу, налаштовується вона на комутаторі другого рівня. Також неї називають широкомовним доменом.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 39   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

VLAN являє собою мітку в кадрі передану мережею. У неї є ID. Під нього відводиться 12 біт, тобто мітка може мати нумерацію від 0 до 4095.

VLAN налаштовується на комутаторах. На портах таких пристроїв налаштовується значення, яке відповідає віртуальній мережі в якій знаходиться. Весь трафік, що входить через цей порт, буде відзначений міткою – VLAN. Завдяки цьому він надалі зможе йти та через інші інтерфейси свитчей, що працюють під цією позначкою. При цьому інші порти цей трафік приймати не будуть.

Таким чином, створюється окрема підмережа, яка не може вступати у взаємодію з іншими підмережами без використання комутатора або роутера.

VLAN дозволяє робити:

- Побудувати мережу з незалежною логічною структурою. Побудова її топології не буде залежити від того, де фізично знаходяться компоненти мережі;
- Розбити один такий домен на кілька: трафік широкомовного типу, який належить одному домену, не буде проходити через інший. Це дозволяє менше навантажувати мережеве обладнання;
- Розбити один такий домен на кілька: трафік широкомовного типу, який належить одному домену, не буде проходити через інший. Це дозволяє менше навантажувати мережеве обладнання;
- Групувати ПК, які входять в одну підмережу, і застосовувати політики на всю групу;
- Здійснювати маршрутизацію за допомогою використання віртуальних портів.

Щоб забезпечити можливість відправки й приймання трафіку, який належить іншій підмережі, портом, його необхідно перевести в стан транка або тегування. У першому випадку роз'єм пропускає трафік всіх VLAN, а в другому — працює з трафіком тільки деяких VLAN.

Варто відзначити, що різному обладнанню можуть знадобитися різні налаштування. Так, деякі пристрої вимагають, щоб на фізичному інтерфейсі було зазначено стан конкретного порту. Для іншого ж обладнання може знадобитися вказати, що певний роз'єм належить тому чи іншому вілану. Якщо ж буде потрібно, щоб

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 40   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

кілька VLAN йшли через один порт, то в кожному з них необхідно вказати інтерфейс з тегом.

Маршрутизація між VLAN є класичною маршрутизацією підмереж. Але є відмінність: в нашому випадку кожної з підмереж відповідає конкретний віртуальний LAN на другому рівні.

Як це працює? Наприклад, у вас — пара віланів: ID = 40 і ID = 50. На рівні 2 одна мережа з їх допомогою розбивається на дві підмережі: їх хости один одного не виявляють. Щоб вони розпізнавали один одного і була можливість взаємодії між ними, потрібна маршрутизація трафіку обох віртуальних підмереж. З цієї причини кожному VLAN потрібен власний IP. Це можна зробити на девайсі третього рівня. Адреси будуть виконувати функції шлюзів, які потрібні для забезпечення виходу в інші підмережі. Це дає можливість:

- Налаштувати безпечний клієнтський доступ: члени однієї підмережі не зможуть потрапити в іншу;
- Використовувати один VLAN для декількох фізичних портів свитча. Виходить, на комутаторі рівня 3 можна відразу налаштувати маршрутизацію, не використовуючи зовнішній роутер. Або ж можна роутер, з'єднаний зі свитчем 2-го рівня з налаштованими VLAN, використовувати для створення віртуальних інтерфейсів в необхідній кількості;
- Використовувати другий рівень у вигляді VLAN між 1 і 3 рівнями. Підмережі можна позначати як вілани, які призначені на певні інтерфейси. Також є можливість налаштувати один VLAN і розмістити в ньому кілька портів свитча.

Подібні мітки створюють для об'єднання девайсів, приєднаних до різних свитчів в одну мережу. Можна частину комп'ютерів згрупувати в один вілан, а частину — в другий. Завдяки цьому ПК в різних доменах будуть функціонувати таким чином, ніби вони під'єднані до одного комутатора. Як ми вже говорили, обладнання, яке входить в різні вілани, розпізнавати один одного не зможе. Це також дає можливість створення гостьової мережі.

Виходячи з усього вищесказаного, можна виділити чотири головні плюси застосування Virtual LAN:

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 41   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

– Можливість гнучкого угруповання девайсів (в тому числі й комп'ютерів, які підключені до різних комутаторів) і створення таким чином ізольованої підмережі;

– Зниження обсягу широкомовного трафіку: він просто не транслюється між різними підмережами;

– Підвищення рівня безпеки та можливостей управління. Для кожної віртуальної підмережі можна застосовувати різні налаштування безпеки та доступу.

Можливість знизити кількість мережевих пристроїв і кабелів для використання, адже для створення нової віртуальної підмережі не потрібно купувати комутатор і прокласти кабель живлення.[3]

SSH – універсальний протокол. Його структура та функції безпеки дозволяють використовувати його різними способами, наприклад, для віддаленого доступу, переадресації портів, тунелювання та безпечної передачі файлів

Віддалений доступ дає користувачам можливість увійти на інший комп'ютер або сервер з власної машини. Він використовується для доступу до локальних файлів цільової машини або для виконання служб на ній, не потребуючи фізичного перебування там.

Заходи шифрування та аутентифікації, що беруть участь у SSH, дозволяють користувачам захищати підключення до іншого сервера чи комп'ютера навіть через потенційно небезпечну проміжну мережу.

Віддалений доступ із SSH зазвичай реалізується для того, щоб працівники могли працювати віддалено або дозволити ІТ-відділу виконувати завдання, не потребуючи фізичного підходу до машини. Його можна використовувати для віддаленого адміністрування, управління мережевою інфраструктурою, для налаштування автоматизації, створення резервних копій тощо.

SSH-1 є першою версією протоколу, яка спочатку була випущена у версії ліцензія з відкритим кодом. Це вважається незахищеним, і його не слід застосовувати.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 42   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

SSH-2 і OpenSSH по суті однакові, що стосується їх архітектури та способів роботи. Основна відмінність полягає в тому, що фірмова версія оснащена різноманітними варіантами підтримки, тоді як ті, що використовують OpenSSH, повинні покладатися на ресурси, створені громадою.

SSH-2 та OpenSSH, які складаються з трьох окремих протоколів:

- Транспортний протокол – Це встановлює зв'язок і забезпечує основну безпеку;
- Протокол аутентифікації – Цей шар використовується для аутентифікації клієнта;
- Протокол з'єднання – Цей протокол обробляє канали, по яких передаються дані.

Кожен з цих протоколів виконує унікальну роль, яка працює на встановлення та забезпечення зв'язку, автентифікацію іншої сторони та передачу даних. Типовий порт з'єднання TCP – 22, а з'єднання встановлюються між клієнтом SSH та сервером SSH уздовж модель клієнт-сервер.

Процес віддаленого входу в SSH протікає відповідно до наступної основної структури (з варіаціями залежно від конфігурації), про яку ми розповімо докладніше пізніше:

- Клієнт зв'язується з сервером SSH, щоб розпочати з'єднання.
- Потім сервер надсилає клієнту свій відкритий ключ для підтвердження його ідентичності.
- Дві сторони узгоджують параметри з'єднання, а потім встановлюють захищений канал по цих лініях.

Потім користувач увійде в операційну систему хоста сервера і тепер може віддалено керувати своїми завданнями.[6]

Telnet (*TELEtype NETwork*)— мережевий протокол для реалізації текстового інтерфейсу по мережі.

Призначення протоколу TELNET у наданні достатньо спільного, двонаправленого, восьмибітового байт-орієнтованого засобу зв'язку. Його основне завдання полягає в тому, щоб дозволити термінальним пристроям і термінальним процесам

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 43   |

взаємодіяти один з одним. Передбачається, що цей протокол може бути використаний для зв'язку виду термінал-термінал («зв'язування») або для зв'язку процес-процес («розподілені обчислення»).

Хоча у сесії Telnet виділяють клієнтську і серверну сторону, протокол насправді повністю симетричний. Після встановлення транспортного з'єднання (як правило, TCP) обидва його кінця грають роль «мережевих віртуальних терміналів» (Network Virtual Terminal, NVT), які обмінюються двома типами даних:

- Прикладними даними (тобто даними, які йдуть від користувача до текстового додатка на стороні сервера і назад);
- Командами протоколу Telnet, окремим випадком яких є *опції*, службовці для з'ясування можливостей і переваг сторін.

Хоча Telnet-сесії, що виконується по TCP, властивий повний дуплекс, NVT повинен розглядатися як напівдуплексний пристрій, що працює за замовчуванням у буферизованому рядковому режимі.

Прикладні дані проходять через протокол без змін. Дані можуть зазнавати змін (наприклад може бути скинутий старший біт) у разі, якщо на вхід одного терміналу надійшли дані, допустимість приймання яких не була підтверджена другим. Тобто на виході другого віртуального терміналу ми бачимо саме те, що було введено на вхід першого. З точки зору протоколу дані представляють просто послідовність байтів, за замовчуванням належать набору ASCII, але при включеній опції *Binary* - будь-яких. Хоча були запропоновані розширення для ідентифікації набору символів Telnet Charset Option, але на практиці ними не користуються. Всі значення октетів прикладних даних крім \ 377 (десятькове 255) передаються з транспорту як є. Октет \ 377 передається послідовністю \ 377 \ 377 із двох октетів. Це пов'язано з тим, що октет \ 377 використовується на транспортному рівні для кодування опцій.

Протокол контролю агрегації посилянь (LACP) - це протокол для колективної обробки декількох фізичних портів, який може розглядатися як єдиний канал для цілей мережевого трафіку. Це служить загальному принципу агрегації зв'язків,

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 44   |

який описує зусилля зі створення паралельних мережевих структур для забезпечення надмірності або для підвищення продуктивності.

Інститут інженерів електротехніки та електроніки (IEEE) має власний стандарт LACP 802.3ad, але існують також фірмові типи LACP, розроблені такими компаніями, як Cisco. LACP розроблявся протягом 90-х років, а початковий випуск стандартів IEEE стався в 2000 році. Експерти вважають, що LACP має переваги перед деякими іншими типами резервного копіювання, як звичайні системи відмовлення.

З точки зору фактичної методології, агрегація може здійснюватися на шарах два та три моделі OSI, і пристрої можуть спільно використовувати один логічний IP або MAC-адресу. Агрегація посилань може допомогти з обмеженнями пропускної здатності в кабельних мережах. В цілому ці системи допомагають підтримувати більш потужні та ефективні мережі, де технологія компаній у великій кількості дала змогу пропонувати все більш здатні мережеві системи, побудовані докорінно різними способами.

HSRP це протокол із сімейства протоколів резервування шлюзу FHRP (First Hop Redundancy Protocol). Суть усіх протоколів сімейства FHRP полягає в наданні можливості декільком пристроям третього рівня (комутаторам третього рівня або маршрутизаторам) використовувати одну IP-адресу, яка для кінцевих пристроїв буде IP-адресою шлюзу.

Даний протокол був створений для запобігання відсутності шлюзу. Підвищення надійності шлюзу досягається шляхом застосування декількох, найчастіше двох, фізично окремих пристроїв третього рівня. Протокол HSRP надає можливість утворити одну або декілька груп фізичних чи віртуальних інтерфейсів третього рівня, що належать різним пристроям (комутаторам третього рівня або маршрутизаторам), і присвоїти кожній з груп інтерфейсів спільну MAC-адресу та IP-адресу (які можна вважати віртуальними). При цьому тільки один з інтерфейсів третього рівня, з найвищим серед інших інтерфейсів у групі пріоритетом, буде знаходитися в активному стані Active (активний інтерфейс), і тільки один інтерфейс з найвищим після активного інтерфейсу пріоритетом – у стані резерву Standby (резервний інтерфейс). Якщо в HSRP групі більше двох інтерфейсів, то інші інтерфейси будуть

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 45   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

знаходиться в стані прослуховування Listen, оскільки ці інтерфейси мають пріоритети менші, ніж в інтерфейсів, що перейшли в стан Active та Standby.

Пріоритет маршрутизатора може мати значення від 1 до 255, за замовчуванням значення пріоритету становить 100. Чим вище значення, тим вище пріоритет маршрутизатора бути активним. Якщо значення пріоритету декількох інтерфейсів є однаковим, то більший пріоритет має інтерфейс з більшим значенням IP-адреси. Також існує можливість застосування динамічної зміни пріоритету за допомогою відстеження стану певного інтерфейсу.

Маршрутизація IP-пакетів виконується тільки через інтерфейс третього рівня, який знаходиться в активному стані. Активний інтерфейс на запит протоколу ARP, що містить віртуальну IP-адресу відповідної HSRP групи, відправляє ARP відповідь, до якої поміщає віртуальну MAC-адресу цієї HSRP групи, що призводить до наступної передачі кадрів Ethernet на активний інтерфейс.

Активний і резервний інтерфейси з інтервалом часу 3 с (за замовчуванням) відсилають повідомлення Hello на широкомовну IP-адресу 224.0.0.102. Передача повідомлень Hello здійснюється за допомогою протоколу UDP на порт UDP з номером 1985

Якщо резервний інтерфейс не отримує повідомлення Hello протягом 10 с (за замовчуванням), то вважається, що активний інтерфейс став недоступним, що призводить до переходу інтерфейсу з резервного в активний стан і виконання функції маршрутизації IP-пакетів. У цей момент усі інші інтерфейси HSRP групи переходять у стан розмови Speak, у якому починають періодичне розсилання повідомлень Hello та бере участь у виборах резервного інтерфейсу за критерієм найбільшого пріоритету після активного інтерфейсу. Таким чином, перехід інтерфейсу в стан резервного Standby можливий тільки зі стану розмови Speak після проведення виборів.

Протокол HSRP реалізує функцію пріоритетного переривання обслуговування, яка дозволяє інтерфейсу з найвищим пріоритетом негайно ставати активним. У першу чергу пріоритет визначається за встановленим користувачем значенням пріоритету, а потім за IP-адресою. В обох випадках, чим більше значення, тим вище

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 46   |

пріоритет. При перериванні обслуговування інтерфейс з більш високим пріоритетом відправляє повідомлення *Coup*. Коли активний інтерфейс з меншим пріоритетом одержує повідомлення *Coup* від інтерфейсу з більш високим пріоритетом, він переходить у стан розмови *Speak*, у якому відбуваються вибори активного та резервного інтерфейсів за критерієм найбільшого пріоритету.

Функція затримки пріоритетного переривання обслуговування протоколу HSRP дозволяє відкласти переривання на зазначений у налаштуваннях час, що дає пристрою третього рівня можливість заповнити таблицю маршрутизації перед переходом в активний стан. Відлік часу затримки починається з першої спроби пріоритетного переривання обслуговування.

Протокол HSRP у якості віртуальних використовує такі MAC-адреси:

0000.0c9f.fXXX,

де XXX – відповідає номеру HSRP групи (довжина становить 12 бітів).

Таким чином, HSRP групі може бути присвоєний номер від 0 до 4095, але більшість пристроїв не можуть підтримати більше 16 HSRP груп.

Кожний інтерфейс третього рівня може одночасно входити до складу декількох HSRP груп. При цьому, будучи активним інтерфейсом в одній із груп, в інших групах цей же інтерфейс може перебувати або в стані резерву *Standby*, або в стані прослуховування *Listen*.

Використання одного інтерфейсу третього рівня в декількох HSRP групах дозволяє реалізувати балансування (розділення) навантаження між маршрутизаторами за рахунок установаження на кінцевих пристроях різних IP-адрес шлюзів, у якості яких використовуються віртуальні IP-адреси HSRP груп. При цьому активні інтерфейси з різних груп будуть здійснювати маршрутизацію IP-пакетів, на відміну від випадку використання однієї HSRP групи, коли для маршрутизації може бути використаний тільки один активний інтерфейс.

Розглянемо структуру пакета протоколу HSRP (рисунок 2.12).

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 47   |

|                     |          |       |           |    |
|---------------------|----------|-------|-----------|----|
| 0                   | 7 8      | 15 16 | 23 24     | 31 |
| Version             | Op Code  | State | Hellotime |    |
| Holdtime            | Priority | Group | Reserved  |    |
| Authentication Data |          |       |           |    |
| Authentication Data |          |       |           |    |
| Virtual IP Address  |          |       |           |    |

Рисунок 1.13 – Структура пакета протоколу HSRP

Коротко наведемо призначення полів пакета протоколу HSRP:

Version (1 байт) – версія протоколу HSRP.

Op Code (1 байт) – тип повідомлення, що міститься в пакеті протоколу HSRP.

Можливі такі значення поля Op Code:

- повідомлення Hello (періодично відправляється, щоб вказати, що інтерфейс працює і здатний стати активним або резервним);
- повідомлення Coup (відправляється інтерфейсом з найвищим пріоритетом, коли цей інтерфейс хоче стати активним, з метою реалізації функції пріоритетного переривання обслуговування);
- повідомлення Resign (відправляється, коли інтерфейс більше не хоче бути активним);

State (1 байт) – поточний стан інтерфейсу. Для різних версій протоколу HSRP коди станів різні.

Hellotime (1 байт) – період привітання. Період повторення повідомлень привітання Hello (у секундах). Значення за замовчуванням – 3 с.

Holdtime (1 байт) – час утримання. Час, протягом якого зберігається коректність поточного привітання Hello (у секундах). Значення за замовчуванням – 10 с.

Priority (1 байт) – пріоритет інтерфейсу. Використовується для вибору активного й резервного інтерфейсів. При порівнянні пріоритетів двох різних інтерфейсів активним призначається той, у якого значення пріоритету вище. При рівних пріоритетах вибирається інтерфейс із більшою IP-адресою.

Group (1 байт) – номер HSRP групи.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 48   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

Reserved (1 байт) – зарезервовано для застосування в майбутньому, у поточній версії протоколу HSRP не використовується.

Authentication Data (8 байтів) – дані аутентифікації. Поле містить пароль для аутентифікації. Якщо аутентифікація не настроєна, використовується значення за замовчуванням.

Virtual IP Address (4 байти) – віртуальна IP-адреса HSRP групи.

Таблиця 1.4 – Стани протоколу HSRP

| Стан    | Визначення                                                                                                                                                                                                                                                                                                   |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Initial | Початковий стан. Протокол HSRP не активний. Цей стан під час зміни конфігурації або під час первинного настроювання інтерфейсу третього рівня                                                                                                                                                                |
| Learn   | У цьому стані інтерфейс третього рівня ще не визначив віртуальну IP-адресу й не побачив аутентифікованого повідомлення привітання від активного інтерфейсу. У цьому стані інтерфейс третього рівня, як і раніше, очікує команду від активного інтерфейсу                                                     |
| Listen  | Інтерфейсу третього рівня відома віртуальна IP-адреса, але він не є ні активним, ні резервним. Він слухає (тільки ухвалює й аналізує) привітальні повідомлення від цих інтерфейсів                                                                                                                           |
| Speak   | Інтерфейс третього рівня спрямовує періодичні привітальні повідомлення й бере активну участь у процесі вибору активного та/або резервного інтерфейсу. Інтерфейс третього рівня не може перейти в стан Speak, якщо в нього нема віртуальної IP-адреси                                                         |
| Standby | Інтерфейс третього рівня може стати наступним активним інтерфейсом і періодично посилає повідомлення привітання. За винятком перехідних станів, у кожній групі необхідна наявність не більше одного інтерфейсу третього рівня в режимі Standby                                                               |
| Active  | Інтерфейс третього рівня в цей час пересилає пакети, відправлені на віртуальну MAC-адресу HSRP групи. Інтерфейс третього рівня періодично посилає повідомлення привітання. За винятком перехідних станів, у кожній HSRP групі необхідна наявність не більше одного інтерфейсу третього рівня в режимі Active |

Висновками з цього розділу є визначання теоретичної інформації про правила та принципи побудови мережі. Розглянуто протоколи та технології які використовуються при побудові мереж. При розгляді були визначені переваги і недоліки їх використання.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 50   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

## РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ МІСЬКОГО ІНТЕРНЕТ-ПРОВАЙДЕРА

### 2.1 Особливості та етапи проектування мережної інфраструктури міського інтернет-провайдера

Оскільки це проект мережної інфраструктури провайдера то першою особливістю має бути отримання прибутку якій залежить від кількості потенційних користувачів. Тому мережа повинна проектуватися з урахуванням потенційної кількості користувачів з можливістю масштабування. Для цього на етапі ядра та рівня розподілу має закладатись можливість масштабування у вигляді можливості встановлення додаткових інтерфейсів.

Наступною особливістю є вибір доступних точок виходу в зовнішній інтернет, це у нашому випадку має надавати провайдер регіонального рівня. Даних точок доступу може бути не одна а декілька для забезпечення надійності зв'язку та балансування навантаження.

Для роботи провайдера необхідно мати офіс який буде місцем базування персоналу та центрального обладнання. Для обладнання що розміщується за межами офісу необхідно забезпечити безпеку, це можна зробити за допомогою встановлення обладнання в захищені шафи які будуть знаходитись під охороною охоронної фірми.



Рисунок 2.1 – Захищена шафка

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 51   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

Дане обладнання зазвичай встановлюється в багатоквартирних будинках та живиться від місцевої мережі. Однак у випадках коли це приватний сектор встановлення обладнання відбувається в приватному будинку.

Після розрахунку кількості потенційних користувачів та отримання доступу до точки чи точок доступу в зовнішню мережу можна переходити до розгортання ядра мережі та точок доступу користувачів. Даний етап повинен супроводжуватись рекламною компанією яка має забезпечити перших користувачів.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 52   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

## 2.2 Розробка фізичної та логічної топології мережі

Мережа спроектована з використанням трьох рівнів, а саме:

- Рівень ядра. Центральна частина мережі яка займається розподілом інтернет трафіку між мережами. Ядро складається переважно з маршрутизаторів, які з'єднані між собою за допомогою Gigabit Ethernet. Також в пбудову повино закладатись можливість розширення мережі.
- Рівень розподілу. Сполучає ядро та кінцеві мережі з рівня доступу. Будується маршрутизаторами та комутаторами які поєднуються зо допомогою Gigabit Ethernet.
- Рівень доступу. Кінцеве устаткування користувачів мережі та комутаційного обладнання.

Почнемо з фізичної топології мережі.

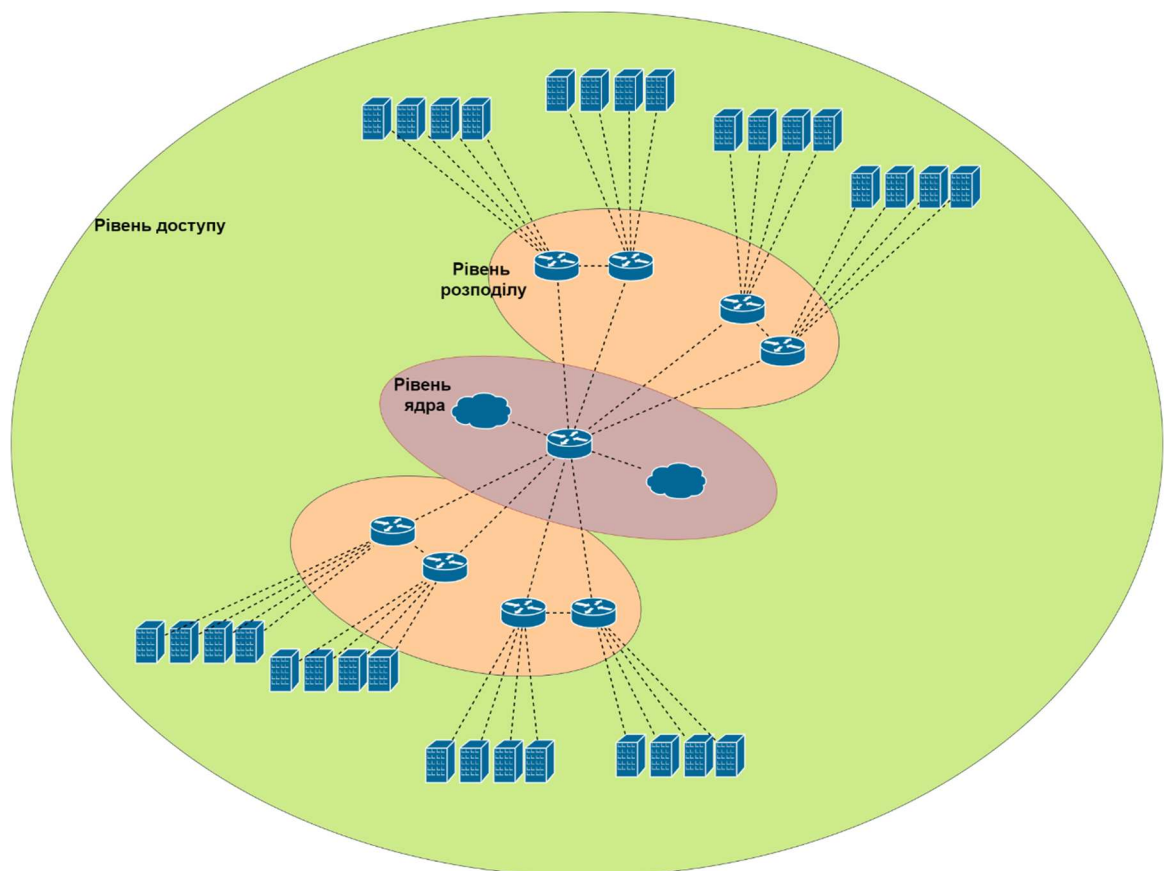


Рисунок 2.2 – Топологія мережі

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузіук В.В.        |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 53   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

Між користувачами та рівнем розподілу встановлено комутаційне обладнання з можливостями розширення.

Для забезпечення високої швидкості передачі інформації між рівнем доступу та розподілу використовується з'єднання Gigabit Ethernet. Кінцеві вузли в рівні доступу підключені до комутатора з використанням лінії Fast Ethernet або Gigabit Ethernet в залежності від тарифу користувача.

Загалом в прикладі мережі використовується 9 маршрутизаторів та мінімум 48 комутаторів. Кількість підмереж 35 включаючи мережі між маршрутизаторами.

В залежності від району доцільно використовувати різні типи топології.

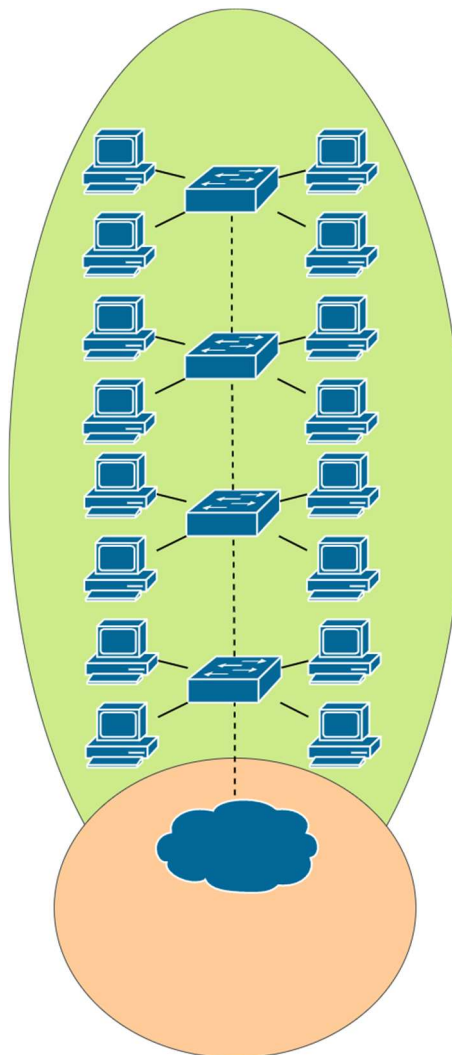


Рисунок 2.3 – Послідовне з'єднання

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 54   |

Подібна побудова рівня доступу доцільна і має такі переваги як простота встановлення, налаштування та обслуговування. Однак у випадку відмови частина або вся топологія втратить доступ до інтернету.

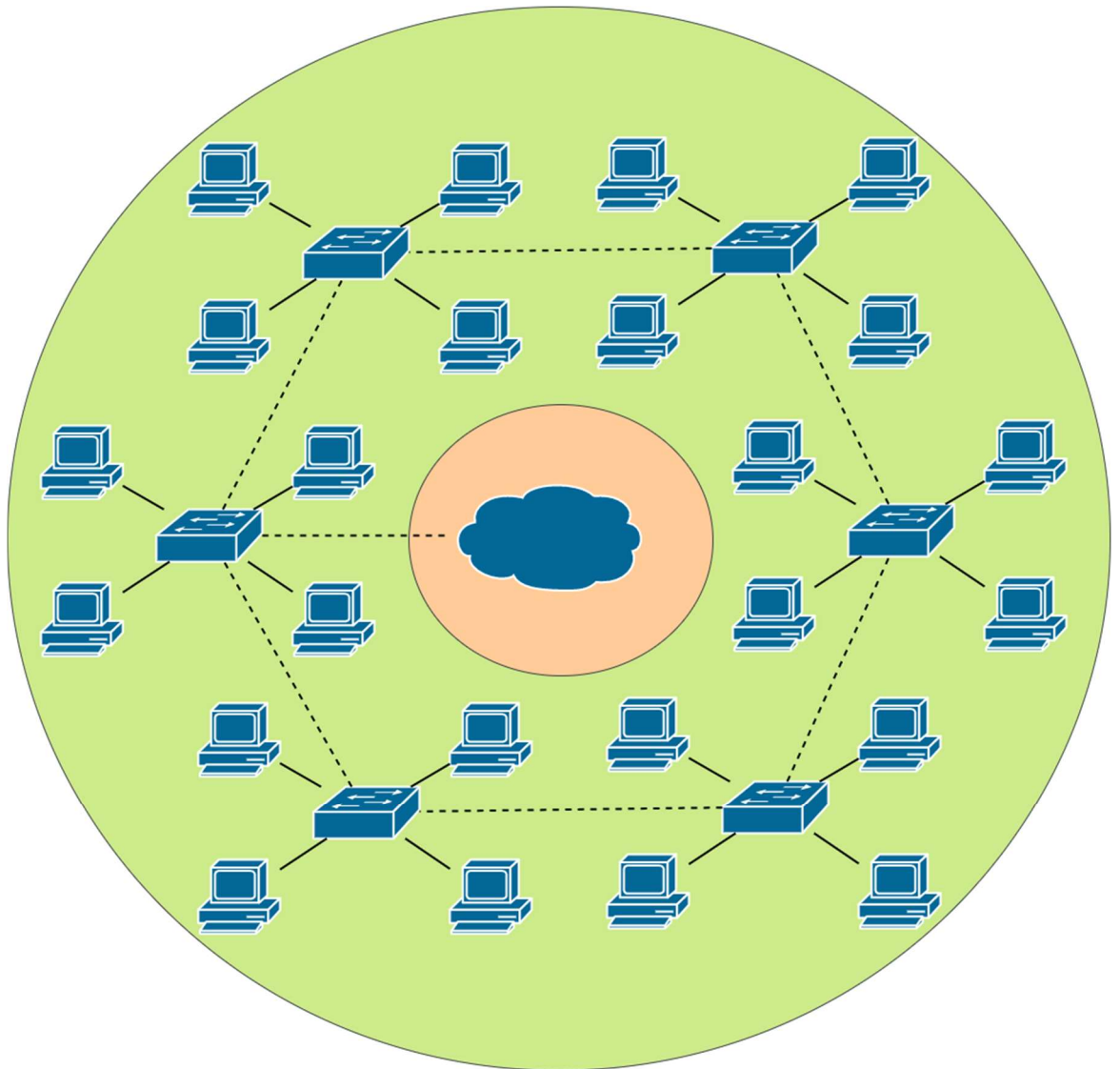


Рисунок 2.4 – Кільцеве з'єднання

Кільцева побудова рівня доступу є більш надійний чим послідовне і також має такі переваги як простота встановлення та обслуговування.

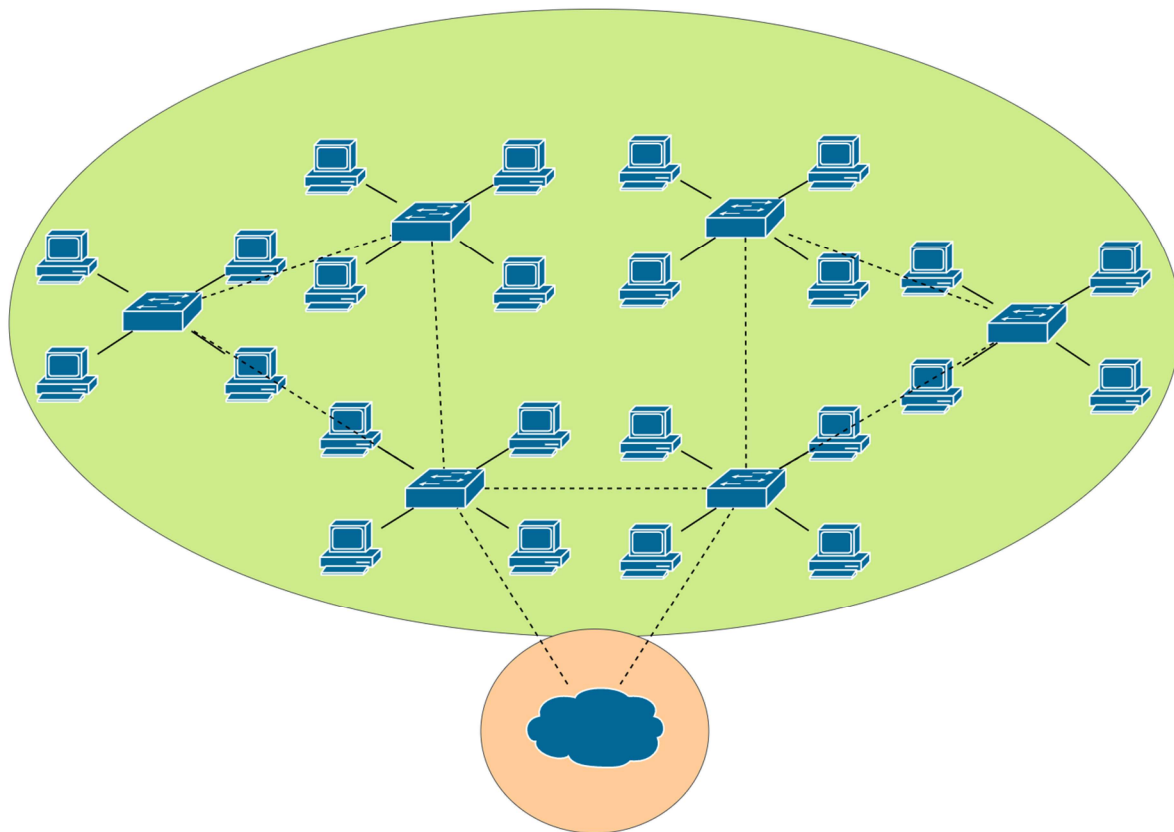


Рисунок 2.5 – Дерево подібне з'єднання

Дерево подібне з'єднання має серед переваг високу надійність. Однак за таку перевагу збільшується складність встановлення та обслуговування обладнання в порівнянні з послідовним і кільцевим з'єднанням.

Зв'язок між маршрутизаторами та OLT буде виконуватись за допомогою дво-точкових мережних з'єднань.

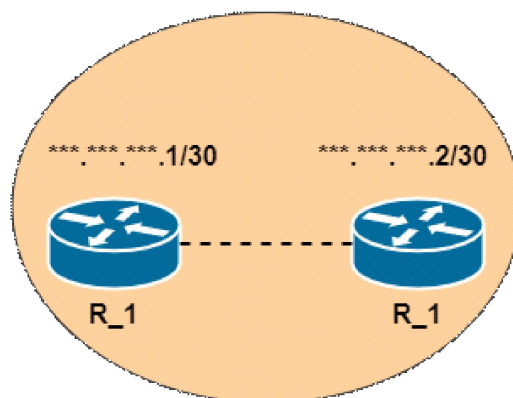


Рисунок 2.6 – Дво-точкове з'єднання

На комутаційному обладнанні буде налаштовано робота двох різних мереж за допомогою протоколу VLAN.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 56   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

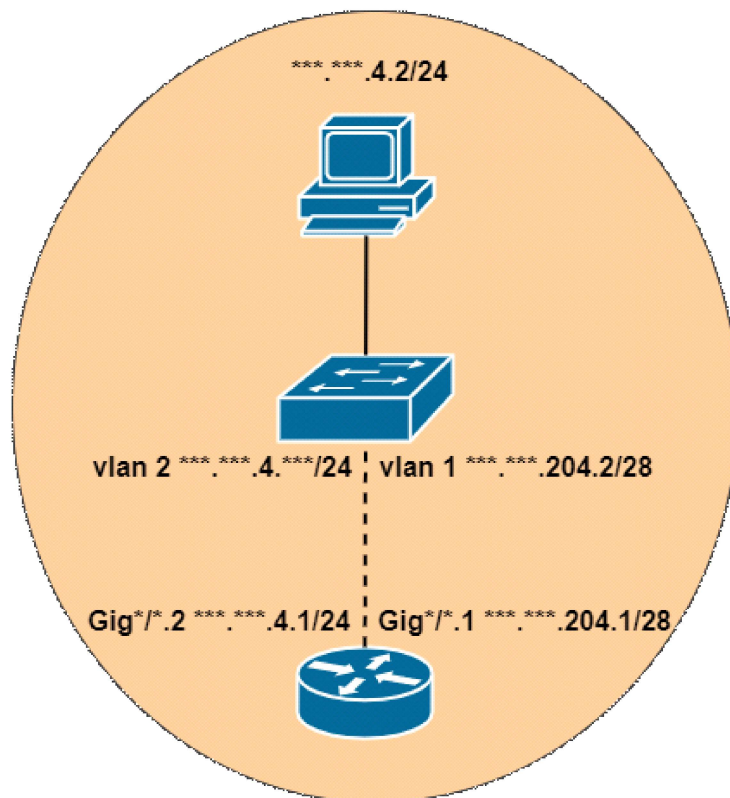


Рисунок 2.7 – Розподіл мереж

Дане налаштування забезпечить нас більш надійною безпекою оскільки відділить користувачів від комутаційного обладнання та при правильному використанні спростить масштабування мереж.

В більшості випадків логічна топологія буде використовуватись логічна шина та комутувана. Подібна логічна топологія виходить з побудованих вище фізичних топології як відрізняються в залежності від зручності використання.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 57   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

## 2.3 Розробка схеми адресації

Почати слід з розподілу адрес мережам. Розподіл підключень між маршрутизаторами та OLT описано в таблиці 2.1.

Таблиця 2.1 – Адреса мереж між маршрутизаторами та OLT

| Назва мережі | Призначення | Адреса мережі | Маска           | Префікс |
|--------------|-------------|---------------|-----------------|---------|
| A            | CoreR - R_1 | 200.4.210.0   | 255.255.255.252 | /30     |
| B            | CoreR - R_2 | 200.4.210.4   | 255.255.255.252 | /30     |
| C            | CoreR - R_3 | 200.4.210.8   | 255.255.255.252 | /30     |
| D            | CoreR - R_4 | 200.4.210.12  | 255.255.255.252 | /30     |
| E            | CoreR - R_5 | 200.4.210.16  | 255.255.255.252 | /30     |
| F            | CoreR - R_6 | 200.4.210.20  | 255.255.255.252 | /30     |
| G            | CoreR - R_7 | 200.4.210.24  | 255.255.255.252 | /30     |
| I            | CoreR - R_8 | 200.4.210.32  | 255.255.255.252 | /30     |
| J            | R_1 - R_2   | 200.4.210.36  | 255.255.255.252 | /30     |
| K            | R_3 - R_4   | 200.4.210.40  | 255.255.255.252 | /30     |
| L            | R_5 - R_6   | 200.4.210.44  | 255.255.255.252 | /30     |

Далі необхідно зайнятись розподілом адрес для користувачів і комутаторів. Розділення мереж для комутаторів і користувачів збільшить безпеку мережі. Однак слід зазначити що для районів де використовується технологія передачі PON необхідності в додатковій технічній підмережі відсутня.

Таблиця 2.2 – Адрес підмереж

| Назва мережі | Адреса мережі | Маска           | Префікс |
|--------------|---------------|-----------------|---------|
| D1_C         | 200.4.1.0     | 255.255.255.0   | /24     |
| D1_M         | 200.204.1.0   | 255.255.255.240 | /28     |
| D2_C         | 200.4.2.0     | 255.255.255.0   | /24     |
| D2_M         | 200.204.2.0   | 255.255.255.240 | /28     |
| D3_C         | 200.4.3.0     | 255.255.255.0   | /24     |
| D3_M         | 200.204.3.0   | 255.255.255.240 | /28     |
| D4_C         | 200.4.4.0     | 255.255.255.0   | /24     |
| D4_M         | 200.204.4.0   | 255.255.255.240 | /28     |
| D5_C         | 200.4.5.0     | 255.255.255.0   | /24     |
| D5_M         | 200.204.5.0   | 255.255.255.240 | /28     |

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 58   |

Продовження таблиці 2.2

|        |              |                 |     |
|--------|--------------|-----------------|-----|
| D6_C   | 200.4.6.0    | 255.255.255.0   | /24 |
| D6_M   | 200.204.6.0  | 255.255.255.240 | /28 |
| D7_C   | 200.4.7.0    | 255.255.255.0   | /24 |
| D7_M   | 200.204.7.0  | 255.255.255.240 | /28 |
| D8_C   | 200.4.8.0    | 255.255.255.0   | /24 |
| D8_M   | 200.204.8.0  | 255.255.255.240 | /28 |
| D9_C   | 200.4.9.0    | 255.255.255.0   | /24 |
| D9_M   | 200.204.9.0  | 255.255.255.240 | /28 |
| D10_C  | 200.4.10.0   | 255.255.255.0   | /24 |
| D10_M  | 200.204.10.0 | 255.255.255.240 | /28 |
| D11_C  | 200.4.11.0   | 255.255.255.0   | /24 |
| D12_C  | 200.4.12.0   | 255.255.255.0   | /24 |
| D13_C  | 200.4.13.0   | 255.255.255.0   | /24 |
| Office | 200.204.0.0  | 255.255.255.240 | /28 |

Після визначення адрес підмереж варто розподілити адреси маршрутизаторів рівня ядра і розподілу для спрощення реалізації проекту(додаток Ж).

Комутаційне обладнання буде отримувати статичну адресу для VLAN що відповідає за доступ до цього обладнання для можливості віддаленого контролю, а користувачі за допомогою протоколу DHCP будуть динамічно отримувати власні адреси.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 59   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

## 2.4 Розробка допоміжної сервісної інфраструктури та підсистем захисту

Для роботи мережі важливо розробити допоміжна інфраструктуру яка має відповідати за різний допоміжний функціонал, по типу DHCP, систем аутентифікації AAA. В даному проекті в допоміжній інфраструктурі буде тільки аутентифікація AAA за допомогою RADIUS сервера.

Допоміжна сервісна інфраструктура як було написано вище буде мати пряме підключення до ядра мережі та надавати доступ до інтернету пристроям в офісу.

До підсистем захисту треба віднести налаштування інтерфейсів рівня доступу на маршрутизаторах що забезпечує від ділення користувачів від адресного простору комутаторів. Налаштування віддаленого доступу до пристроїв за допомогою RADIUS сервера та налаштування що обмежує доступ до пристроїв мережею офісу.

Далі повинні бути налаштовані комутатори для захисту від MAC-Flooding, MAC-Spoofing, атак на протоколи STP/PVST+, ARP, DHCP. Дане налаштування забезпечить безпеку мережі від най частіших методів атак на неї.

В даному розділі було розглянуто особливості та етапи проектування мережі. Розроблено фізичну та логічну топологію мережі. Розроблено систему адресацій з урахуванням подальшої можливості захисту. Розроблено допоміжну інфраструктуру та розглянуто необхідні підсистеми захисту.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 60   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

## РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ПРАЦЕЗДАТНОСТІ МІСЬКОЇ МЕРЕЖІ ІНТЕРНЕТ-ПРОВАЙДЕРА

### 3.1 Вибір обладнання та програмного забезпечення для розробки проекту мережної інфраструктури

Вибір обладнання слід почати з загального огляду спектру обладнання, які надається такі провідні світові компаній, як:

- Cisco Systems
- Juniper Networks
- Huawei Technologies
- D-Link Systems, Inc.
- Mikrotiks Ltd. (MikroTik)
- Shanghai Baud Data Communication Co., Ltd. (BDCOM)

Компанія Cisco – це світовий лідер в області мережевих технологій. Діяльність компанії направлена на п'ять основних технологічних напрямки:

- Магістральна маршрутизація, комутація і послуги;
- Рішення для спільної роботи;
- віртуалізація центрів обробки даних та хмарні обчислення;
- відеотехнології;
- архітектури для трансформації бізнесу.

На сьогоднішній день Cisco надає найбільш якісні послуги в своїй галузі ринку. Продукція компанії продається практично у всіх країнах світу як рядовим споживачам, так і великим корпораціям.[8]

Компанія Juniper Networks - один з лідерів в сфері виробництва телекомунікаційного обладнання. Організація розробляє високопродуктивне і високоякісні маршрутизатори, комутатори, міжмережеві екрани, магістральний обладнання, яке може бути використане як ядра для дата-центрів.

Крім того, Juniper здійснює цілодобову технічну підтримку і сервісне обслуговування своїх пристроїв. У числі клієнтів організації присутні 130 провідних міжнародних постачальників мережевих послуг.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузіук В.В.        |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 61   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

Основні сфери застосування обладнання компанії – провайдери послуг зв'язку, центри обробки даних, фінансові корпорації та державний сектор.

Мережеве обладнання Juniper Networks базується на принципах безпеки, надійності, масштабованості і відкритості.

Мережеві рішення Juniper управляються власної ОС. Вона базується на FreeBSD і застосовує розроблені компанією процесори. Організація випустила власну революційну IP платформу, яка пропонує користувачам використовувати більш широкий асортимент сервісів з можливістю масштабування.[14]

Huawei Technologies — світовий лідер в області рішень для мереж зв'язку наступного покоління. Huawei Technologies прагне забезпечити клієнтам максимальний прибуток і потенціал розвитку, надаючи їм нові рішення, створені за індивідуальними вимогами.

Huawei Technologies світовий лідер з постачання телекомунікаційних мереж нового покоління, зараз обслуговує 45 з 50 провідних світових операторів, поряд з одним мільярдом користувачів по всьому світу.[15]

D-Link є всесвітньо відомим розробником і виробником мережевого і телекомунікаційного обладнання і пропонує широкий набір рішень для домашніх користувачів, корпоративного сегмента і провайдерів інтернет-послуг.

D-Link пропонує закінчені мережеві і комунікаційні рішення для побудови «цифрового дому», підприємств малого та середнього бізнесу, мереж масштабу робочих груп і підприємств і провайдерів послуг Інтернет.

Застосування інноваційних методик і високі вимоги до якості дозволяють компанії випускати високопродуктивні пристрої, що базуються на сучасних стандартах.[16]

MikroTik — великий латвійський виробник мережевого обладнання. Основна перевага продукції MikroTik — впроваджена операційна система Mikrotik RouterOS розроблена самою компанією яка відкриває нові можливості і потужний функціонал для обладнання. Майже всі маршрутизатори та точки доступу підтримують технологію живлення POE. У порівнянні зі своїми аналогами ціна MikroTik

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 62   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

на порядок дешевше, а функціонал ні трохи не поступається своїм дорогим конкурентам. [36]

Компанія Shanghai Baud Data Communication Co., Ltd. (BDCOM). Компанія спеціалізується на розробці, виробництві, реалізації та обслуговуванні мережевого обладнання та є постачальником економічних рішень для побудови мереж зв'язку.[17]

Основними замовниками є провайдери зв'язку, великі підприємства та держструктури.

Вибір обладнання потрібно робити з врахуванням необхідних параметрів і задач які необхідно виконати. Достатня кількість портів, підтримка необхідних технологій та протоколів які не обхідні для побудови мережі.

На рівні ядра необхідно мати маршрутизатор з можливість використання протоколу OSPF, підтримувати використання технології GigabitEthernet. Маршрутизатор Cisco 7606[19](Рисунок 3.1) має необхідні параметри для роботи.



Рисунок 3.1 – Маршрутизатор Cisco 7606

Даний маршрутизатор один із 7600 серії маршрутизаторів провайдерського класу. Має можливість розширення кількості портів за рахунок модулів.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 63   |

Також під подібні задачі підходить Juniper J-4350-JB[21](Рисунок 3.2) це також маршрутизатор провайдерського класу зможливістю розширення кількості інтерфейсів.



Рисунок 3.2 – Маршрутизатор Juniper J-4350-JB

Маршрутизатором для рівня розподілу можна вибрати простіший. Такім може бути ISR4331/K9[20](Рисунок 3.3). Дана модель має достатню потужність щоб бути ядром у мережі компаній та граничним маршрутизатором в провайдерських компаніях.



Рисунок 3.3 – Маршрутизатор Cisco ISR4331/K9

Також під подібні задачі підходить Juniper J2320-JB-SC[22](Рисунок 3.4) це також маршрутизатор провайдерського класу.



Рисунок 3.4 – Маршрутизатор Juniper J2320-JB-SC

Для рівня доступу доцільно використати комутатор з великою кількістю портів технології FastEthernet та декількома портами технології GigabitEthernet для під'єднання до маршрутизатора чи підключення ще одного комутатора. Підходить для цього комутатор Cisco WS-C2960+24LC-L[18](Рисунок 3.5).



Рисунок 3.5 – Комутатор Cisco WS-C2960+24LC-L

Даний комутатор має 24 порти технології FastEthernet, 2 порти технології GigabitEthernet та можливість до встановити ще два порти технології GigabitEthernet, що повністю задовольняє задані параметри.

Аналогом буде Huawei S1700-28GFR-4P-AC(Рисунок 3.6).



Рисунок 3.6 – Комутатор Huawei S1700-28GFR-4P-AC

Дана модель схожа за характеристиками.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 65   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

Однак слід зазначити, що будувати мережу використовуючи обладнання різних компаній може призвести до зниження ефективності роботи та затримок. Але якщо розподіляти обладнання правильно то можна поєднувати його.

Також необхідно розглянути обладнання для технології PON. Розглянемо на прикладі обладнання компанії BDCOM.

Спочатку розглянемо технологію GPON на прикладі BDCOM P3310C[24](Рисунок 3.7). Він відповідає вимогам стандартів IEEE 802.3ah, YD/T 1475-2006 та STC2.0/2.1. Підтримує автоматичне виявлення і роботу з абонентськими терміналами (ONU) різних виробників.



Рисунок 3.7 – Концентратор BDCOM P3310C

P3310C підтримує симетричну швидкість передачі даних 1,25 Гбіт/с в низхідному та висхідному напрямках, а також ефективне управління смугою пропускання. Максимальний коефіцієнт ділення 1:64.

Технологія GPON буде розглянути на прикладі BDCOM GP3600[23](Рисунок 3.8) відповідає стандарту ITU-T G.984 / G.988. Повністю підтримують стандарт STC2.0, для автоматичної синхронізації та підключення абонентських терміналів різних виробників.

BDCOM GP3600 підтримує асиметричний аплінк 1.25Gbps / даунлік 2.5Gbps для передачі даних в пасивної оптичної мережі, завдяки ефективному використанню смуги пропускання даний продукт дає можливість надавати якісні послуги на найвищому рівні.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 66   |



Рисунок 3.8 – Концентратор BDCOM GP3600

Дане обладнання дозволяє використовувати коефіцієнт розподілу до 128 абонентів на гілку, що дає можливість мінімізувати фінансові вкладення при побудові мережі.

Основна мережа буде спроектована в програмі Cisco Packet Tracer. Ця програма надає можливість навчитись налаштуванню обладнання, але обмежена встановленим обладнанням. Маршрутизатори 4331 моделі та універсальний PT-Empty, комутатори 2960 моделі та універсальний PT-Empty будуть використовуватись як аналоги обладнання яке було обрано вище. Слід зазначити що, обладнання з найменуванням PT-Empty це не реальне а віртуальне обладнання яке доводиться використовувати для імітації необхідних моделей.

Для реалізації підсистем захисту буде використовуватись набір програми головною із яких є GNS 3 яка здатна проводити емуляцію реального обладнання. Дана програма теж має свої обмеження в плані доступних пристроїв оскільки потребує образи реального обладнання. Також для роботи програми необхідно використовувати віртуальну машину де будуть встановлюватись образи обладнання, для цього буде використовуватись програма VMware Workstation. Оскільки ми будемо реалізовувати системи захисту нам потрібно буде перевірити їх роботу спроможність для цього буде використовуватись Oracle VM VirtualBox куди буде встановлено образ Kali Linux. Дана операційна система спеціально створена для проведення атак на мережеві пристрої тому має все необхідне програмне забезпечення для цього.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 67   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

### 3.2 Базове налагодження мережних пристроїв

Базове налагодження пристроїв це налагодження основних протоколів та технології обладнання для забезпечення передачі інформації у мережі.

Почати слід з налагодження адрес інтерфейсів маршрутизаторів. Розглянуто буде маршрутизаторі R\_1.

```
R_1(config)#interface gigabitEthernet 0/0
R_1(config-if)#no sh
R_1(config-if)#ex
R_1(config)#interface gigabitEthernet 0/0.1
R_1(config-subif)#description Link_to_D1_M
R_1(config-subif)#encapsulation dot1Q 1
R_1(config-subif)#ip address 200.204.1.1 255.255.255.240
R_1(config-subif)#no sh
R_1(config-subif)#ex
R_1(config)#interface gigabitEthernet 0/0.2
R_1(config-subif)#description Link_to_D1_C
R_1(config-subif)#encapsulation dot1Q 2
R_1(config-subif)#ip address 200.4.1.1 255.255.255.0
R_1(config-subif)#no sh
R_1(config-subif)#ex
R_1(config)#interface gigabitEthernet 0/5
R_1(config-subif)#description Link_to_CoreR
R_1(config-if)#ip address 200.4.210.2 255.255.255.252
R_1(config-if)#no sh
R_1(config-if)#ex
```

Як видно з налаштування інтерфейс що веде до рівня доступу розділений на два під інтерфейси для забезпечення розділення мережі користувачів та мережі доступу до комутаційного обладнання.

Налаштування маршрутизації OSPF.

```
R_1>en
R_1#conf t
R_1(config)#route ospf 10
R_1(config-router)# network 200.4.210.128 255.255.255.240 area 0
```

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузьок В.В.        |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 68   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```
R_1(config-router)# network 200.4.210.40 255.255.255.252 area 0
R_1(config-router)# network 200.4.210.4 255.255.255.252 area 0
R_1(config-router)# network 200.4.210.16 255.255.255.252 area 0
```

Налаштування маршрутизації дозволить передавати пакети між підмережами різних маршрутизаторів.

Налаштування комутаторів рівня доступу адреси:

```
SW>en
SW#conf t
SW(config)#vlan 2
SW(config-vlan)#ex
SW(config)#interface vlan 1
SW(config-if)#ip address 200.204.1.2 255.255.255.240
SW(config-if)#no sh
SW(config-if)#ex
SW(config)#ip default-gateway 200.204.1.1
SW(config)#interface range g1/0-1
SW(config-if-range)#switchport trunk encapsulation dot1q
SW(config-if-range)#switchport mode trunk
SW(config-if-range)#ex
SW(config)#interface range f0/0-23
SW(config-if-range)#switchport mode access
SW(config-if-range)#switchport access vlan 2
SW(config-if-range)#ex
```

На комутаторах було проведено розділення інтерфейсів для різних vlan.

Після базового налаштування обладнання налаштуємо додаткові протоколи та технології.

Маршрутизатори рівня розподілу налаштовуються як DHCP-сервери.

```
R_1>en
R_1#conf t
R_1(config)#ip dhcp excluded-address 200.4.1.254
R_1(config)#ip dhcp pool Lan_P
R_1(dhcp-config)#network 200.4.1.0 255.255.255.0
```

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузіук В.В.        |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 69   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```
R_1(dhcp-config)#default-router 200.4.1.254
R_1(dhcp-config)#domain-name myP.net
```

DHCP спростить підключення користувачів до мережі.

Налаштування віддаленого доступу:

```
CoreR(config)#aaa new-model
CoreR(config)#username badmin secret badmin
CoreR(config)#aaa authentication login default group radius local
CoreR(config)#aaa authentication enable default group radius local
CoreR(config)#radius server 200.204.0.10
CoreR(config-radius-server)#key cisco123
CoreR(config-radius-server)#address ipv4 200.204.0.10
ex
CoreR(config)#ip domain-name cisco.com
CoreR(config)#ip ssh version 2
CoreR(config)#crypto key generate rsa
1024
CoreR(config)#line vty 0 4
CoreR(config-line)#transport input ssh
CoreR(config-line)#login authentication default
CoreR(config-line)#end
```

Віддалений доступ відбуватиметься за допомогою RADIUS сервера щоб спростити масштабування мережі.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 70   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

### 3.3 Налаштування засобів підсистем захисту

В даному підрозділі буде продовжено налаштування обладнання мережі. Продовжимо налаштування внесенням правил обмежуючих доступ до віддаленого налаштування обладнання і для цього будемо використовувати списки доступу які будуть обмежувати доступ до обладнання однією мережею офісу. Налаштування буде виглядати так для маршрутизаторів:

```
R_5(config)#access-list 1 permit 200.204.0.0 255.255.255.240
R_5(config)#line vty 0 4
R_5(config-if)#access-group 1 out
R_5(config-if)#access-group 1 in
R_5(config-if)#ex
R_5(config)#interface g0/0.1
R_5(config-if)#ip access-group 1 out
R_5(config-if)#ip access-group 1 in
```

Дане налаштування відкине можливість доступу до маршрутизатора та комутаторів із зовнішньої мережі. Однак для забезпечення більшої надійності подібне потрібно налаштувати на комутаторах також:

```
SW_D1_1(config)#access-list 1 permit 200.204.0.0 255.255.255.240
SW_D1_1(config)#line vty 0 4
SW_D1_1(config-if)#access-group 1 out
SW_D1_1(config-if)#access-group 1 in
```

Для подальшого проектування захисту нам знадобиться створити проект в програмному додатку GNS 3, оскільки для перевірки роботи спроможності захисту необхідно проводити атаки на це обладнання. Також для роботи програми знадобиться VMware Workstation для запуску віртуальної машини GNS 3 та Oracle VM VirtualBox для запуску віртуальної машини Kali Linux для проведення атак на пристрої.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 71   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

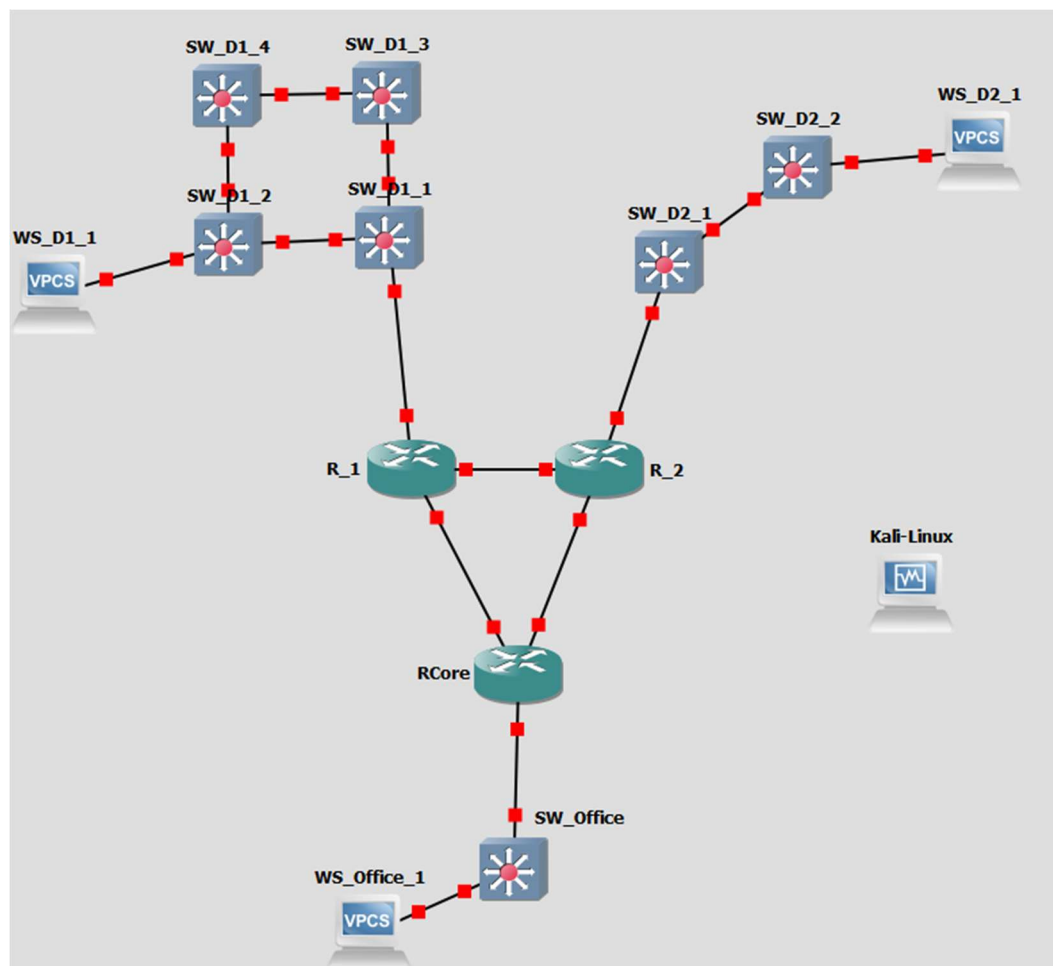


Рисунок 3.9 – Схема для налагодження захисту

Налаштування захисту важлива частина оскільки від нього залежить працездатність мережі в певних випадках.

Налаштування захисту від MAC-Flooding та MAC-Spoofing атак:

```
SW(config)# interface fastethernet0/1
SW(config-if)# switchport mode access
SW(config-if)# switchport port-security
SW(config-if)# switchport port-security violation shutdown
SW(config-if)# switchport port-security mac-address sticky
SW(config)#errdisable recovery cause psecure-violation
SW(config)#errdisable recovery interval 500
```

Також варіант налаштування:

```
SW(config)# interface fastethernet0/1
SW(config-if)# switchport mode access
SW(config-if)# switchport port-security
```

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузіук В.В.        |        |      | KIK.KP.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 72   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```
SW(config-if)# switchport port-security violation restrict
SW(config-if)# switchport port-security mac-address aaaa.aaaa.aaaa
SW(config)#errdisable recovery cause psecure-violation
SW(config)#errdisable recovery interval 500
```

Дане налаштування в обох варіантах активує та встановлює інтервал відновлення. В першому варіанті дією на порушення буде вимкнення інтерфейсу та мак-адреса інтерфейсу буде триматися певний час. В другому реакцією на порушення буде обмеження та мак-адреса буде статична. Треба зазначити що краще буде використовувати статичну адресу та вимкнення інтерфейсу хоч це і може викликати проблеми при зміні пристрою користувача.

Далі розглядається захист від атак на протоколи STP/PVST+. Приклад налаштування необхідно розглядати на декількох пристроях для наглядності налаштування:

```
SW_1#config terminal
SW_1(config)#interface FastEthernet 0/1
SW_1(config-if)#spanning-tree guard root
SW_1(config)#interface range FastEthernet 0/3-24
SW_1(config-if-range)#spanning-tree portfast
SW_1(config-if-range)#spanning-tree bpduguard enable
SW_1(config-if-range)#exit
```

Перший комутатор налаштований як кореневий для захисту від можливості зміни кореневого пристрою та налаштовується захист інтерфейсів користувачів.

```
SW_2#config terminal
SW_2(config)#spanning-tree portfast default
SW_2(config)#spanning-tree portfast bpduguard default
SW_2(config)#errdisable recovery cause bpduguard
SW_2(config)#errdisable recovery interval 60
SW_2(config)#interface range FastEthernet 0/1-2
SW_2(config-if)#spanning-tree portfast disable
SW_2(config-if)#spanning-tree bpduguard disable
SW_2(config-if)#exit
SW_2(config)#interface range FastEthernet 0/3-24
```

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 73   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```
SW_2(config-if-range)#spanning-tree portfast
SW_2(config-if-range)#spanning-tree bpduguard enable
SW_2(config-if-range)#exit
SW_2(config-if)#exit
```

На другому комутаторі продемонстровано команди що відповідають за виведення повідомлень про помилки, команди що відповідають за час відновлення роботи порту та команди що активують та деактивують захист портів. Відповідно порти між комутаторами без налаштувань захисту, а порти користувачі із захистом.

Захист від атак на протокол ARP. Налаштовується за допомогою функції DAI. Приклад налаштування при використанні DHCP:

```
SW_1#configure terminal
SW_1(config)#ip dhcp snooping vlan 1
SW_1(config)#ip dhcp snooping database flash:/dhcp-snoop.db
SW_1(config)#ip dhcp snooping
SW_1(config)#interface FastEthernet 0/24
SW_1(config-if)#ip dhcp snooping trust
SW_1(config-if)#exit
SW_1(config)#ip arp inspection vlan 1
SW_1(config)#interface FastEthernet 0/24
SW_1(config-if)#ip arp inspection trust
SW_1(config-if)#exit
SW_1(config)#errdisable recovery cause arp-inspection
SW_1(config)#errdisable recovery interval 120
```

Дане налаштування виконується на інтерфейсі що веде до маршрутизатору. Далі буде розглянуто приклад налаштування для статичної адресації.

```
SW_1>enable
SW_1#configure terminal
SW_1(config)#arp access-list SW-ARP-Defend
SW_1(config-arp-nacl)#permit ip host 200.4.1.1 mac host 0C54.A514.2EE4
SW_1(config-arp-nacl)#permit ip host 200.4.1.2 mac host 00AA.0075.6865
SW_1(config-arp-nacl)#permit ip host 200.4.1.250 mac host 00E0.F76B.D0A1
SW_1(config-arp-nacl)#permit ip host 200.4.1.254 mac host 001D.4641.02B4
SW_1(config-arp-nacl)#exit
```

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 74   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```
SW_1(config)#ip arp inspection filter SW-ARP-Defend vlan 1 static
SW_1(config)#errdisable recovery cause arp-inspection
SW_1(config)#errdisable recovery interval 120
```

Оскільки в проєкті мережі користувачі отримують адресу за допомогою DHCP нам необхідно використовувати перший варіант налаштування.

В проєкті як було сказано вище використовується DHCP тоді нам необхідно захистити цей протокол від атак. Для захисту існує також два методи перший з використанням мак-адрес пристроїв мережі:

```
R_1#configure terminal
R_1(config)#ip dhcp excluded-address 195.1.1.1
R_1(config)#ip dhcp excluded-address 195.1.1.250
R_1(config)#ip dhcp pool WS_1
R_1(dhcp-config)#host 195.1.1.101 255.255.255.0
R_1(dhcp-config)#default-router 195.1.1.1
R_1(dhcp-config)#dns-server 195.1.1.1
R_1(dhcp-config)#client-identifier 0108.0027.C9C8.30
R_1(dhcp-config)#client-name WS_A
R_1(dhcp-config)#domain-name my.net
R_1(dhcp-config)#exit
R_1(config)#ip dhcp pool WS_2
R_1(dhcp-config)#host 195.1.1.102 255.255.255.0
R_1(dhcp-config)#default-router 195.1.1.1
R_1(dhcp-config)#dns-server 195.1.1.1
R_1(dhcp-config)#client-identifier 0108.0027.7F91.0A
R_1(dhcp-config)#client-name WS_B
R_1(dhcp-config)#domain-name my.net
R_1(dhcp-config)#exit
```

При подібному методі необхідно буде виконувати це для кожного підключеного пристрою, однак варто зауважити що таке налаштування дозволяє видавати одну й ту саму адресу пристрою що може знадобитись при розміщені серверу чи тому подібного обладнання.

Для роботи з динамічними адресами використовують функцію DHCP-Snooping, налаштування захисту буде виконано на комутаторі:

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 75   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```

SW_1#configure terminal
SW_1(config)# ip dhcp snooping
SW_1(config)#interface GigabitEthernet 0/1
SW_1(config-if)#ip dhcp snooping trust
SW_1(config-if)#ip dhcp snooping limit rate 256
SW_1(config-if)#exit
SW_1(config)#exit

```

Дане налаштування набагато простіше та виконується на комутаторі що дозволяє зменшити навантаження на маршрутизатор чи сервер. Захист встановлює обмеження на кількість пакетів запиту для протоколу DHCP.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 76   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

### 3.4 Тестування складових елементів мережної інфраструктури

Ще під час налаштування адрес пристрої в протрібно перевіряти зв'язок між ними.

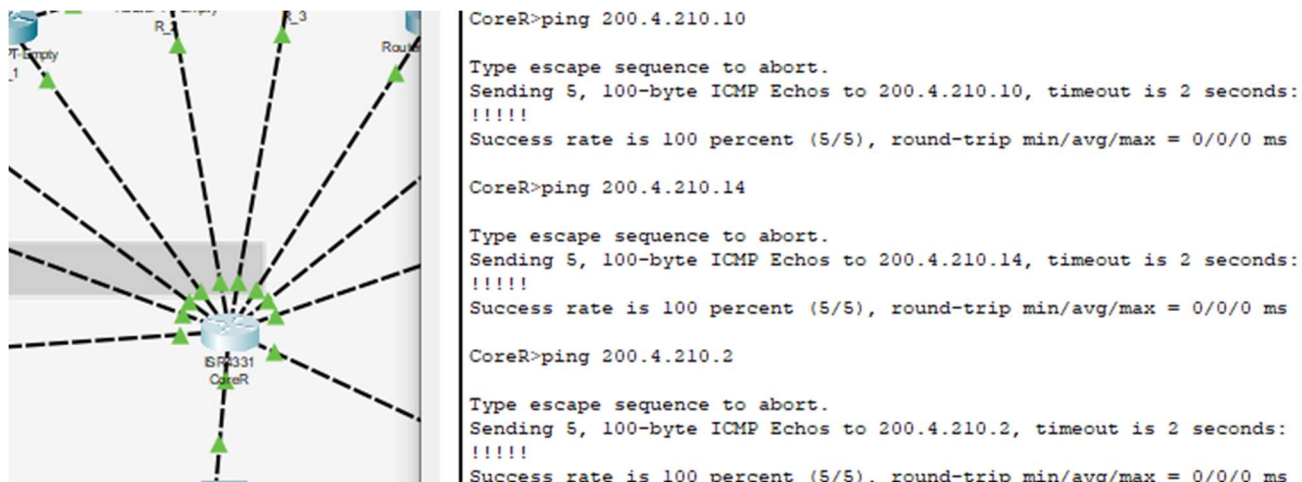


Рисунок 3.10 – Перевірка зв'язку між маршрутизаторами

Перевірка роботи маршрутизації. Слід зазначити що подібна перевірка можлива лише коли користувачам надали відкриту IP адресу.

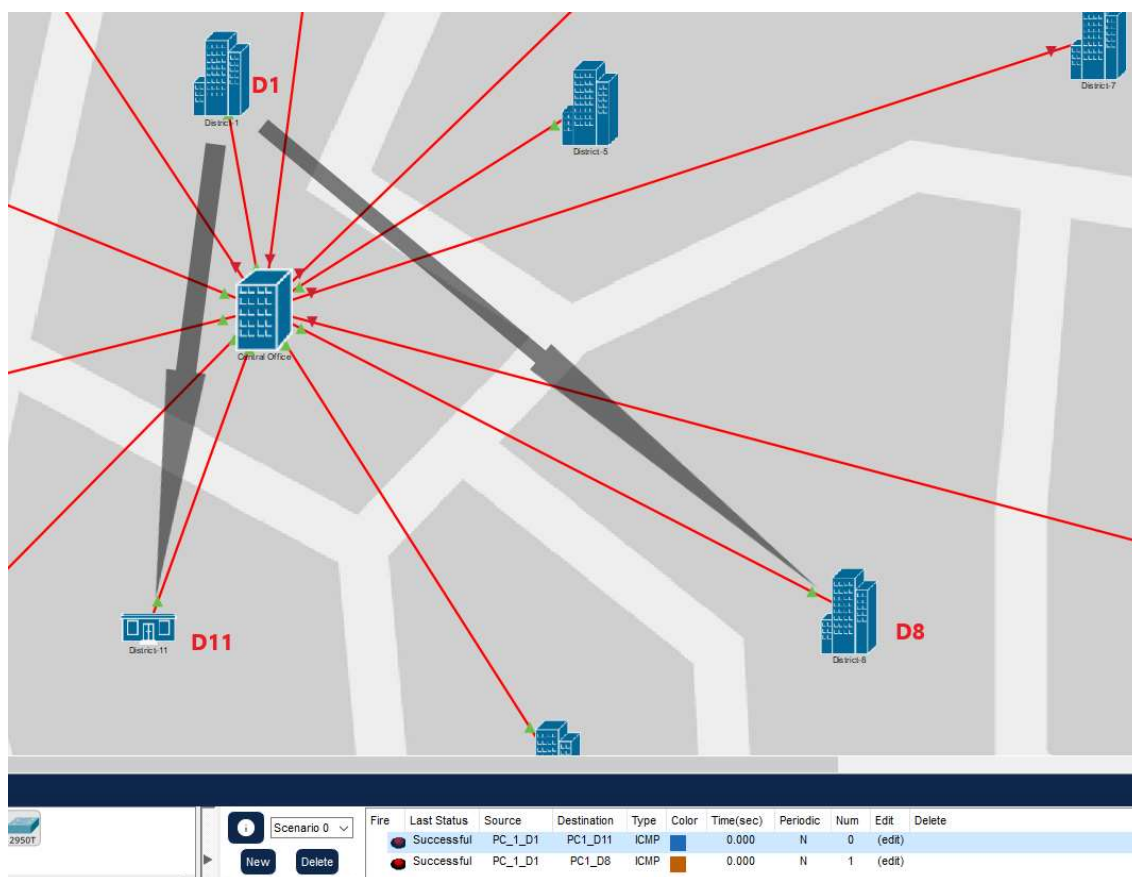


Рисунок 3.11 – Перевірка роботи маршрутизації

Тепер слід перевірити можливість віддаленого контролю.

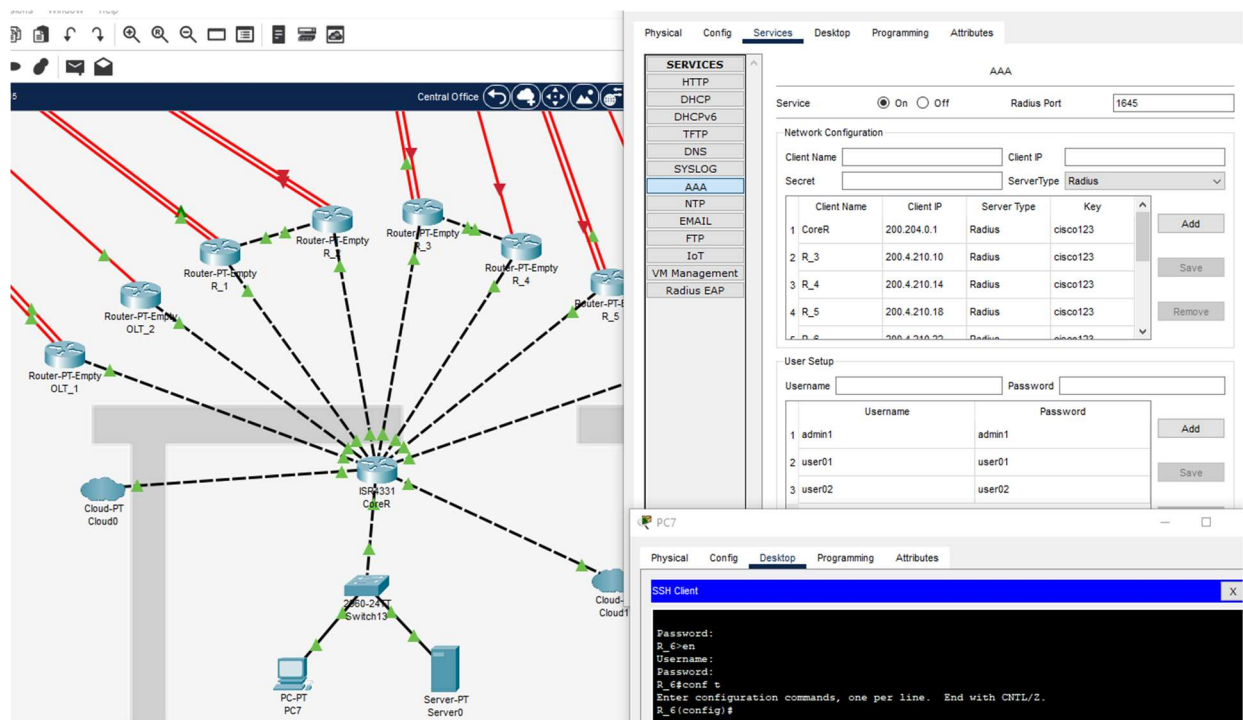


Рисунок 3.12 – Перевірка роботи віддаленого доступу

Далі буде проводитись тестування підсистем захисту. Почнемо з обмеження доступу до віддаленого контролю.

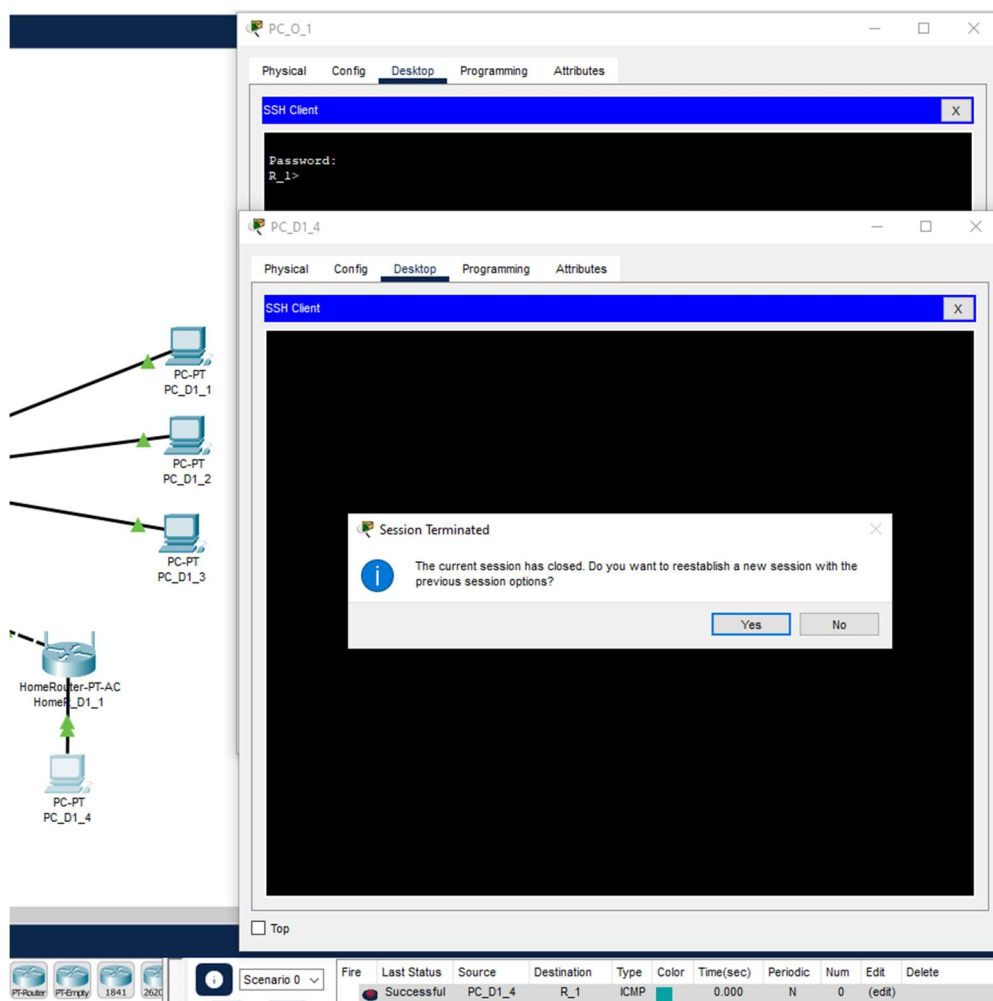


Рисунок 3.13 – Перевірка обмеження доступу

Як видно з рис. 3.13 комп'ютер що розміщений в офісі зміг провести підключення до маршрутизатора. Однак комп'ютер користувача хоч і має зв'язок з маршрутизатором проте підключити віддалений доступ не може.

Перевірка захисту від атак MAC-Flooding та MAC-Spoofing. Почнемо з перевірки чи мережа пропускає пакети даних після налаштування.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 79   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

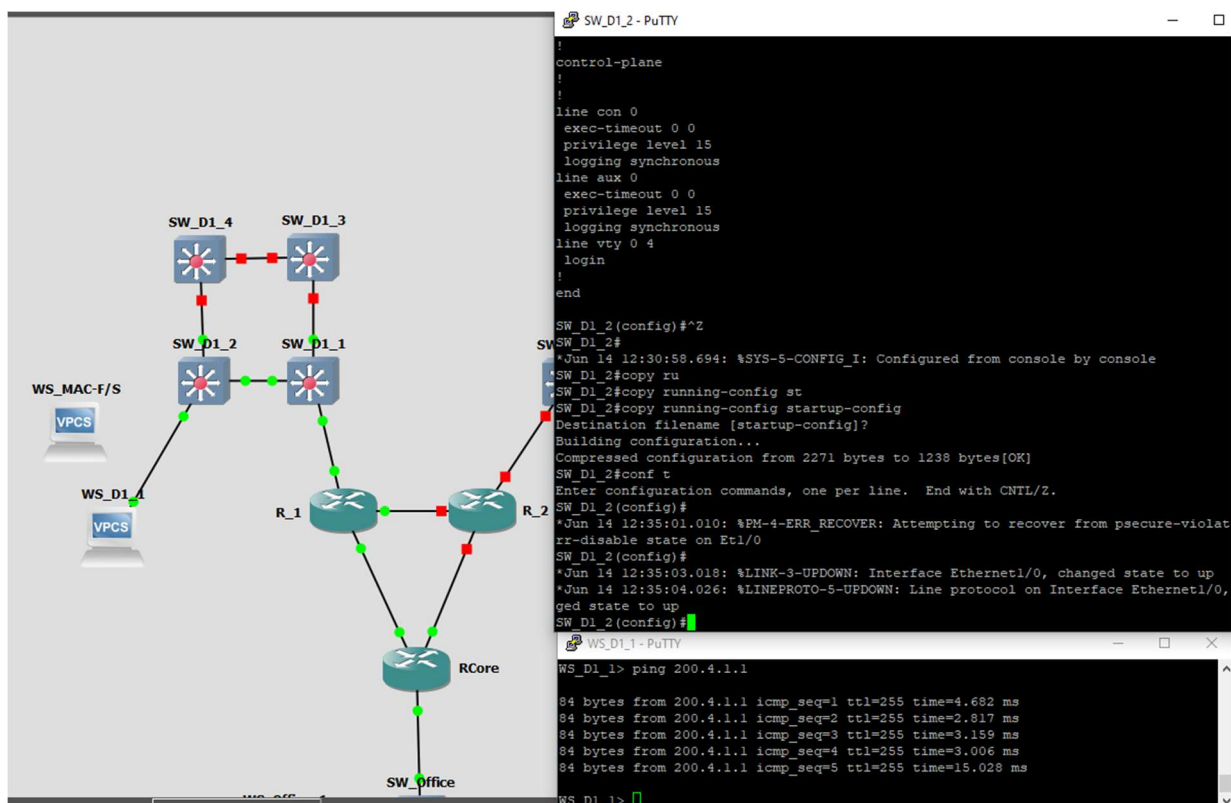


Рисунок 3.14 – Перевірка роботи

Як бачимо пакети проходять, тепер підключимо пристрій зловмисника за-  
мість станції користувача.

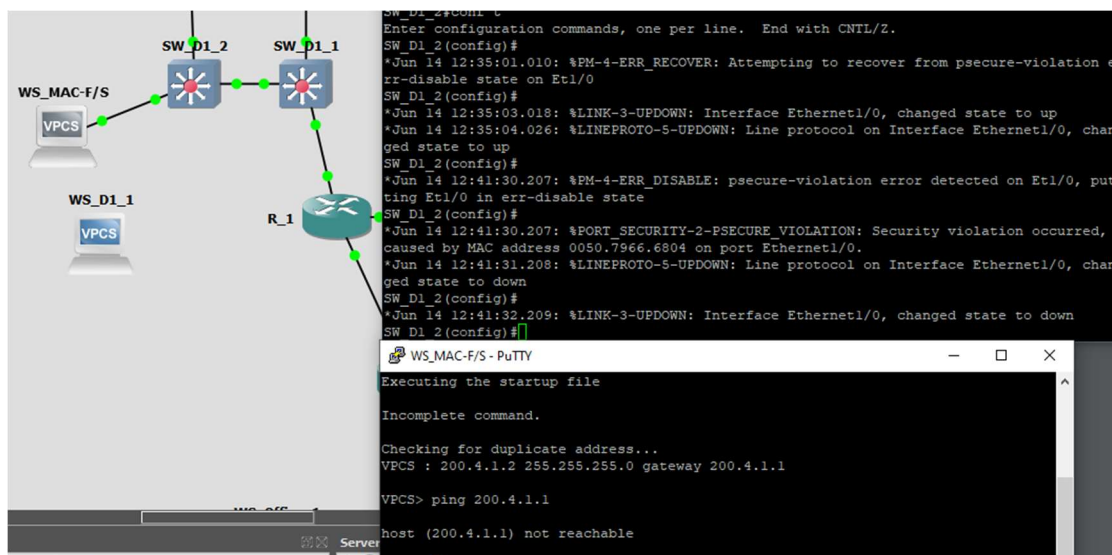


Рисунок 3.15 – Підключення станції зловмисника

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 80   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

В результаті після підключення і спроби перевірити зв'язок комутатор вивів повідомлення про відключення інтерфейсу і згідно налаштувань він увімкнеться через певний час.

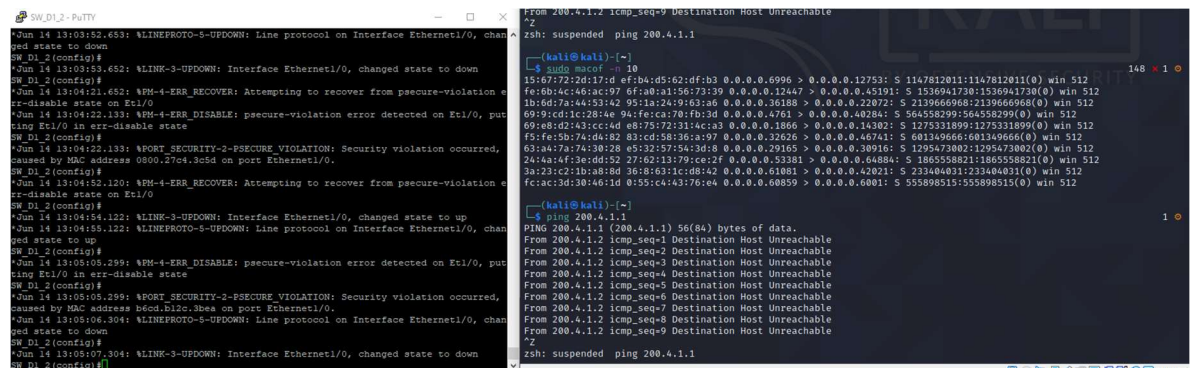


Рисунок 3.16 – Захист від MAC-Flooding

Як видно із рис. 3.16 підчас проведення атаки MAC-Flooding інтерфейс відключається так само як і при атаці MAC-Spoofing.

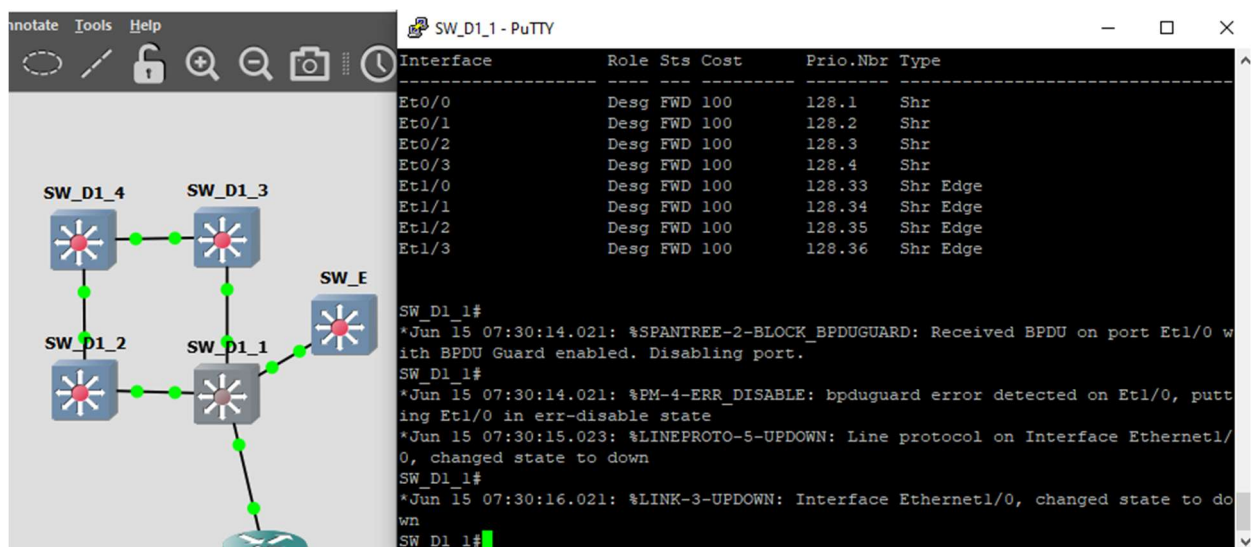


Рисунок 3.17 – Атака зловмисним комутатором

Як видно з терміналу на рис. 3.17 при підключенні зловмисного комутатора порт був відключений для забезпечення безпеки мережі.

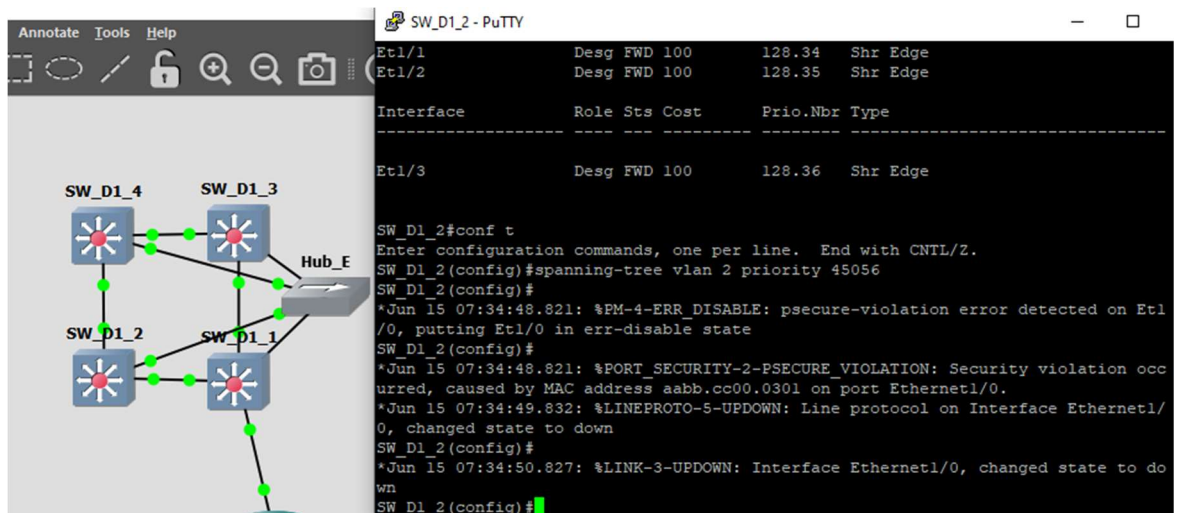


Рисунок 3.18 – Створення петель

За допомогою концентратора була спроба створити петлю, однак як видно з терміналу на рисунку 3.18 поти підключення до концентратора були відключені.

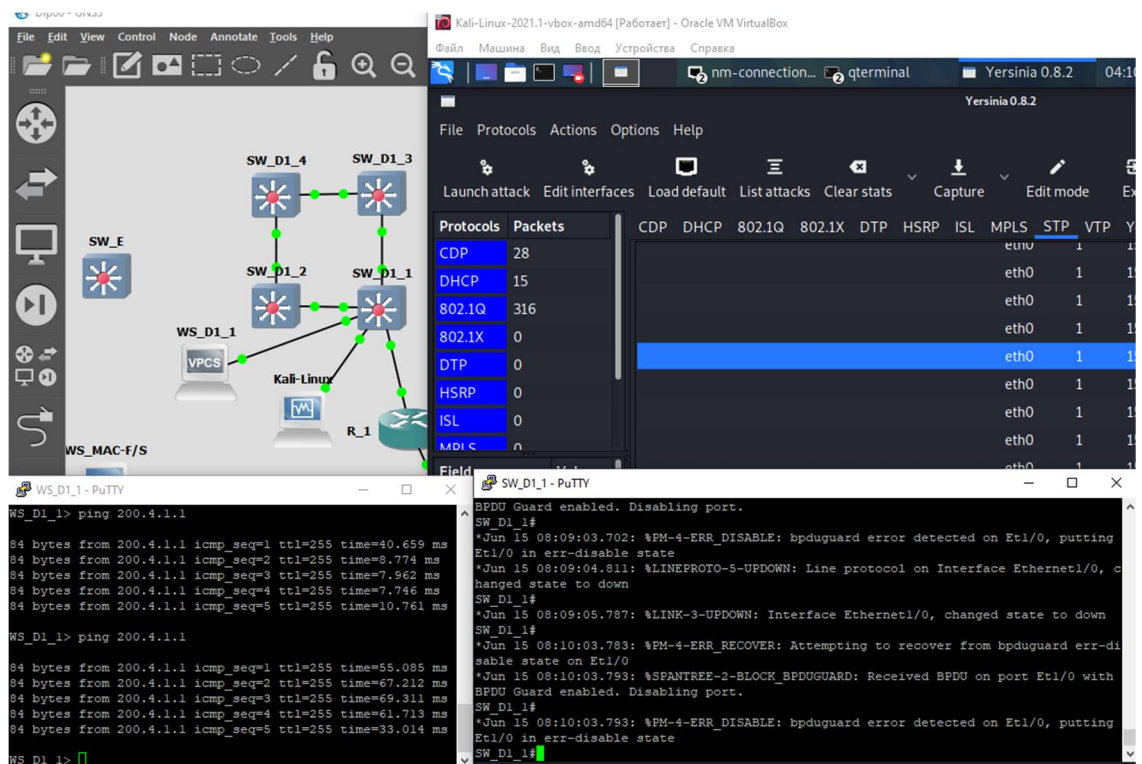


Рисунок 3.19 – DoS атака на протокол STP

DoS атака не вдалась оскільки підсистема захисту вимкнула порт через який велась атака та продовжуватиме його перевіряти поки атака не зупиниться.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 82   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

Далі буде перевірено захист від атак на протокол ARP.

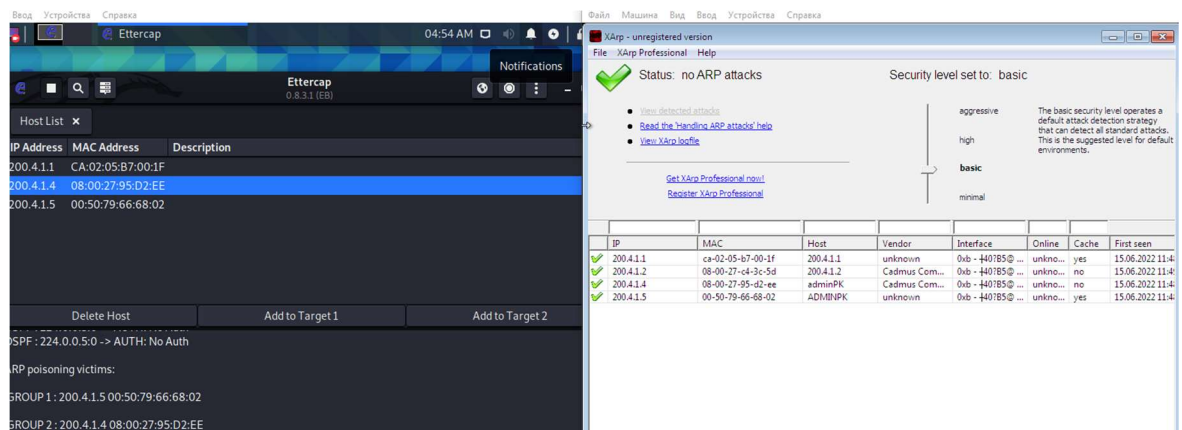


Рисунок 3.20 – Спроба атаки на протокол ARP

Програма що перевіряє атаки на протокол ARP атаки не виявила, а отже захист працює.

Атака на протокол DHCP це підміна сервера та DoS атаки.

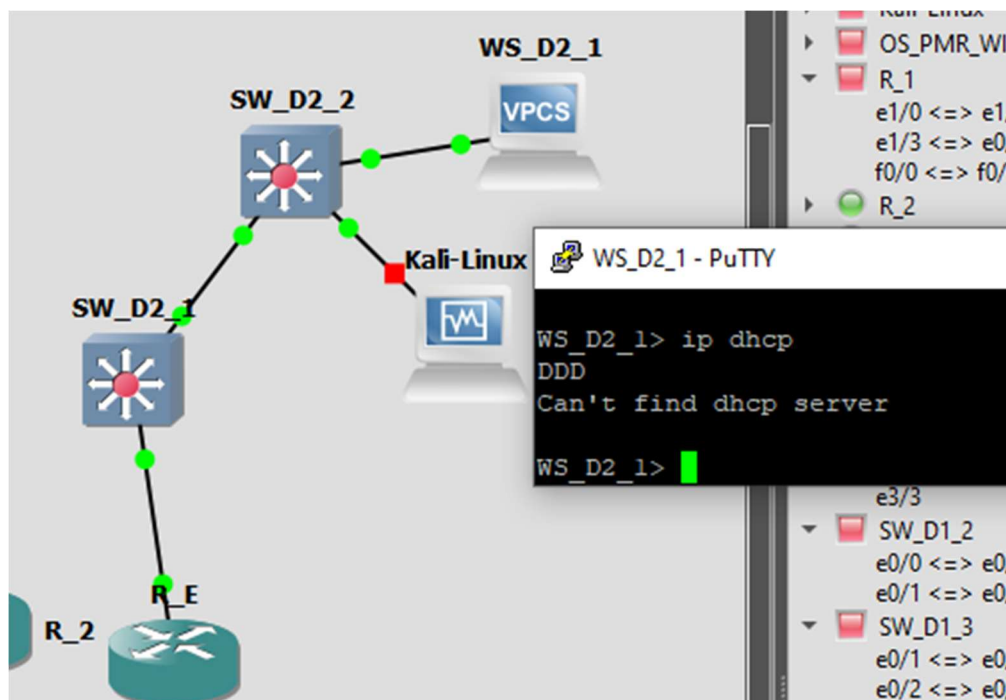


Рисунок 3.21 – Атака підміною серверу

При спробі підмінити сервер пристрої не можуть отримати адреси зловмисника які дозволили прослуховувати всі дані користувача.

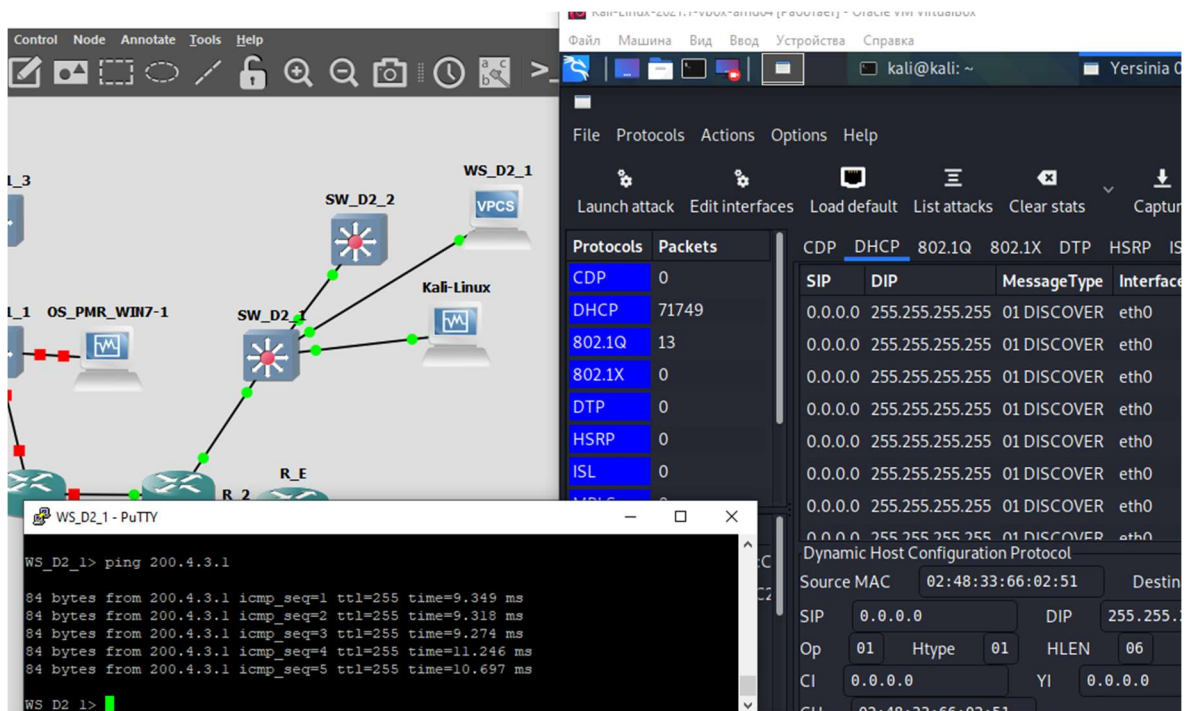


Рисунок 3.22 – DoS атака на протокол DHCP

Під час проведення DoS атаки можливе невелике початкове просідання мережі після чого зв'язок відновлюється.

В даному розділі було розглянуто найбільші компанії постачальники мережевого обладнання. Також було розглянуто обладнання цих компаній для використання в побудові мережі із чого можна визначити що це залежить в основному від бюджетних можливостей компанії та технічної підготовки персоналу, оскільки обладнання кожної компанії налаштовується по різному та може погано поєднуватись якщо використовувати обладнання різних виробників в одній мережі. Вибрано програмне забезпечення з обґрунтуванням їхнього вибору. Далі було проведено базове налаштування обладнання та налаштовано підсистеми захисту. Наприкінці проведено тестування складових елементів мережі.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          |      |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          | 84   |

## ВИСНОВКИ

Висновками з першого розділу є визначення теоретичної інформації про правила та принципи побудови мережі. Розглянуто протоколи та технології які використовуються при побудові мереж. При розгляді були визначені переваги і недоліки їх використання.

Далі було розглянуто особливості та етапи проектування мережі. Розроблено фізичну та логічну топологію мережі. Розроблено систему адресацій з урахуванням подальшої можливості захисту. Розроблено допоміжну інфраструктуру та розглянуто необхідні підсистеми захисту.

В третьому розділі було розглянуто найбільші компанії постачальники мережевого обладнання. Також було розглянуто обладнання цих компаній для використання в побудові мережі із чого можна визначити що це залежить в основному від бюджетних можливостей компанії та технічної підготовки персоналу, оскільки обладнання кожної компанії налаштовується по різному та може погано поєднуватись якщо використовувати обладнання різних виробників в одній мережі. Вибрано програмне забезпечення з обґрунтуванням їхнього вибору. Далі було проведено базове налаштування обладнання та налаштовано підсистеми захисту. Наприкінці проведено тестування складових елементів мережі.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 85   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке IPv4? [Електронний ресурс] – Режим доступу: <https://uk.education-wiki.com/6575994-what-is-ipv4>.
2. Що таке протокол IPv6 [Електронний ресурс] – Режим доступу: <https://uk.wizcase.com/blog/що-таке-протокол-ipv6-i-чому-ви-повинні-звє/>.
3. Що таке VLAN: логіка, технологія і налаштування. Реалізація VLAN в пристроях CISCO [Електронний ресурс] – Режим доступу: <https://e-server.com.ua/uk/poradi/shho-take-vlan-logika-tehnologija-i-nalashtuvannja-realizacija-vlan-v-pristrojah-cisco>.
4. Архітектура мережі або мережева архітектура [Електронний ресурс] – Режим доступу: <https://nettech.ua/news/arxitektura-seti-ili-setevaja-arxitektura>.
5. Rapid STP [Електронний ресурс] – Режим доступу: <https://habr.com/ru/company/cbs/blog/330358/>.
6. Що таке SSH і як він працює? [Електронний ресурс] – Режим доступу: <https://instagalleryapp.com/informacijna-bezpeka/shho-take-ssh-i-jak-vin-pracjue/>.
7. Технологія PON [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/knowegable-base/reference-information/66122.html>.
8. Cisco URL: <https://dovidnyk.info/index.php/Brand/115>.
9. OSPF Protocol [Електронний ресурс] – Режим доступу: <https://www.javatpoint.com/ospf-protocol>.
10. Опис технології Fast Ethernet [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/knowegable-base/reference-information/opisanie-tehnologii-fast-ethernet.html>.
11. Мережа Gigabit Ethernet [Електронний ресурс] – Режим доступу: <https://ua5.org/lan/141-merezha-gigabit-ethernet.html>.
12. Побудова мереж GPON на базі обладнання ТМ BDcom (семінар по обладнанню BDcom) [Електронний ресурс] – Режим доступу:

|      |      |                    |        |      |                                 |      |
|------|------|--------------------|--------|------|---------------------------------|------|
|      |      | Гузюк В.В.         |        |      | <i>КІК.КР.Б – 123 – 10 – ПЗ</i> | Арк. |
|      |      | П.П. Топольницький |        |      |                                 | 86   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                                 |      |

<https://deps.ua/ua/knownegable-base/reference-information/ua-equipment-gpon-bdcom-seminar-1.html>.

13. Побудова мереж GPON на базі обладнання ТМ BDcom (практична частина) (семинар по обладнанню BDcom) [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/knownegable-base/reference-information/ua-equipment-gpon-bdcom-seminar-3.html>.
14. Juniper Networks [Електронний ресурс] – Режим доступу: <https://omnilink.ua/juniper/>.
15. Huawei [Електронний ресурс] – Режим доступу: <https://omnilink.ua/huawei/>.
16. D-link [Електронний ресурс] – Режим доступу: <https://omnilink.ua/d-link/>.
17. BDCOM [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/brands/bdcom.html>.
18. Коммутатор Cisco WS-C2960 [Електронний ресурс] – Режим доступу: <https://stack-systems.com.ua/kommutator-cisco-ws-c2960-24lc-1>.
19. Маршрутизатор Cisco 7606 [Електронний ресурс] – Режим доступу: <https://stack-systems.com.ua/marshrutizator-cisco-7606>.
20. Маршрутизатор ISR4331/K9 [Електронний ресурс] – Режим доступу: <https://stack-systems.com.ua/marshrutizator-cisco-isr4331-k9>.
21. Маршрутизатор J-4350-JB [Електронний ресурс] – Режим доступу: <https://stack-systems.com.ua/marshrutizator-juniper-j-4350-jb>.
22. Маршрутизатор Juniper J2320-JB-SC [Електронний ресурс] – Режим доступу: <https://stack-systems.com.ua/marshrutizator-juniper-j2320-jb-sc>.
23. GPON-концентратор BDCOM GP3600-08 [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/katalog/concentrators-olt/bdcom-gp3600-08.html>.
24. GERON концентратор BDCOM P3310C [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/katalog/concentrators-olt/bdcom-p3310c.html>.
25. Навчальний курс CCNA Routing and Switching: Introduction to Networks [Електронний ресурс] – Режим доступу: [www.netacad.com](http://www.netacad.com).

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 87   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

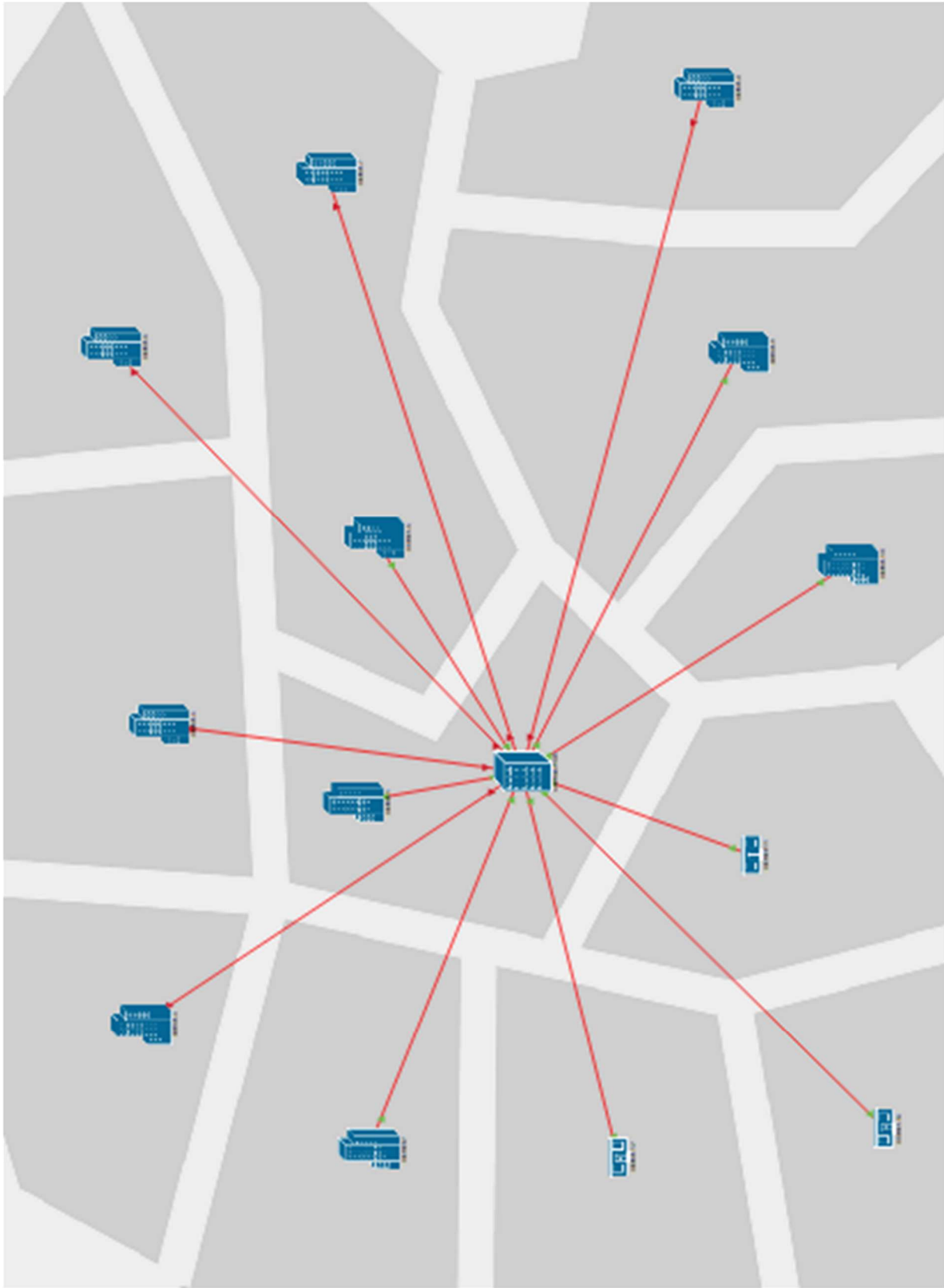
26. Навчальний курс CCNA Routing and Switching: Routing and Switching Essentials [Електронний ресурс] – Режим доступу: [www.netacad.com](http://www.netacad.com).
27. Навчальний курс CCNA Routing and Switching: Scaling Networks [Електронний ресурс] – Режим доступу: [www.netacad.com](http://www.netacad.com).
28. Навчальний курс CCNA Routing and Switching: Connecting Networks [Електронний ресурс] – Режим доступу: [www.netacad.com](http://www.netacad.com).
29. Навчальний курс CCNAv7: Introduction to Networks [Електронний ресурс] – Режим доступу: [www.netacad.com](http://www.netacad.com).
30. Навчальний курс CCNAv7: Switching, Routing, and Wireless Essentials [Електронний ресурс] – Режим доступу: [www.netacad.com](http://www.netacad.com).
31. Навчальний курс CCNAv7: Enterprise Networking, Security, and Automation [Електронний ресурс] – Режим доступу: [www.netacad.com](http://www.netacad.com).
32. Навчальний курс CCNA Security [Електронний ресурс] – Режим доступу: [www.netacad.com](http://www.netacad.com).
33. Навчальний курс CCNA Cybersecurity Operations [Електронний ресурс] – Режим доступу: [www.netacad.com](http://www.netacad.com).
34. Навчальний курс CCNP Enterprise: Core Networking [Електронний ресурс] – Режим доступу: [www.netacad.com](http://www.netacad.com).
35. FTTx [Електронний ресурс] – Режим доступу: <https://lanmarket.ua/entsiklopediya/telekommunikatsionnye-tehnologii/ftth.html>.
36. MikroTik [Електронний ресурс] – Режим доступу: <https://omni-link.ua/mikrotik/>.

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 88   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

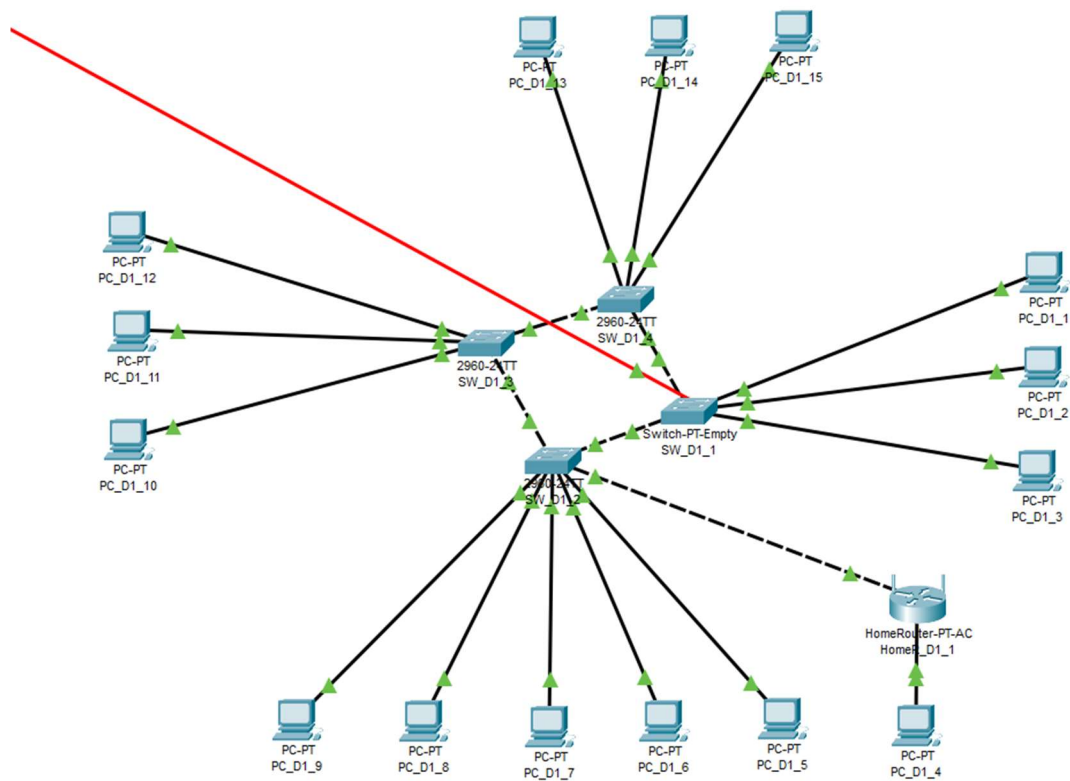
# ДОДАТКИ

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 89   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

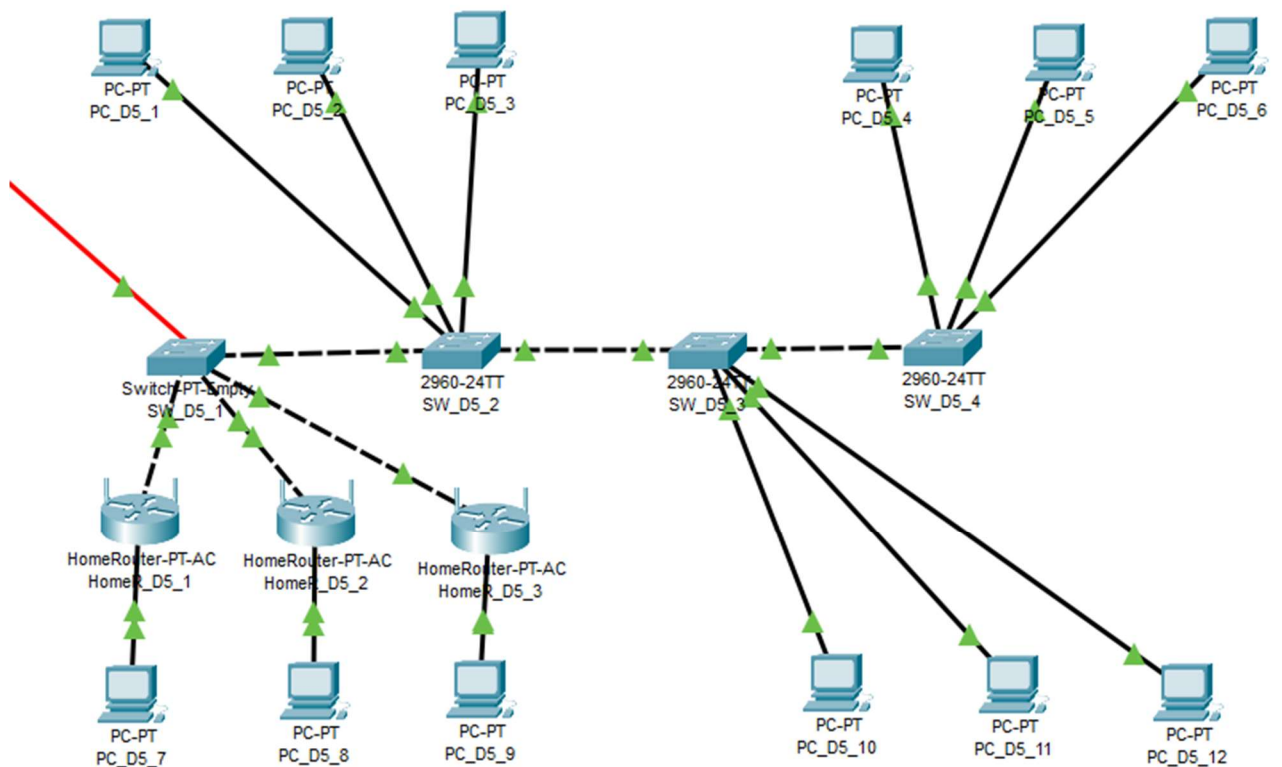
Додаток А – Загальна схема мережі



## Додаток Б – Схема «кільце»

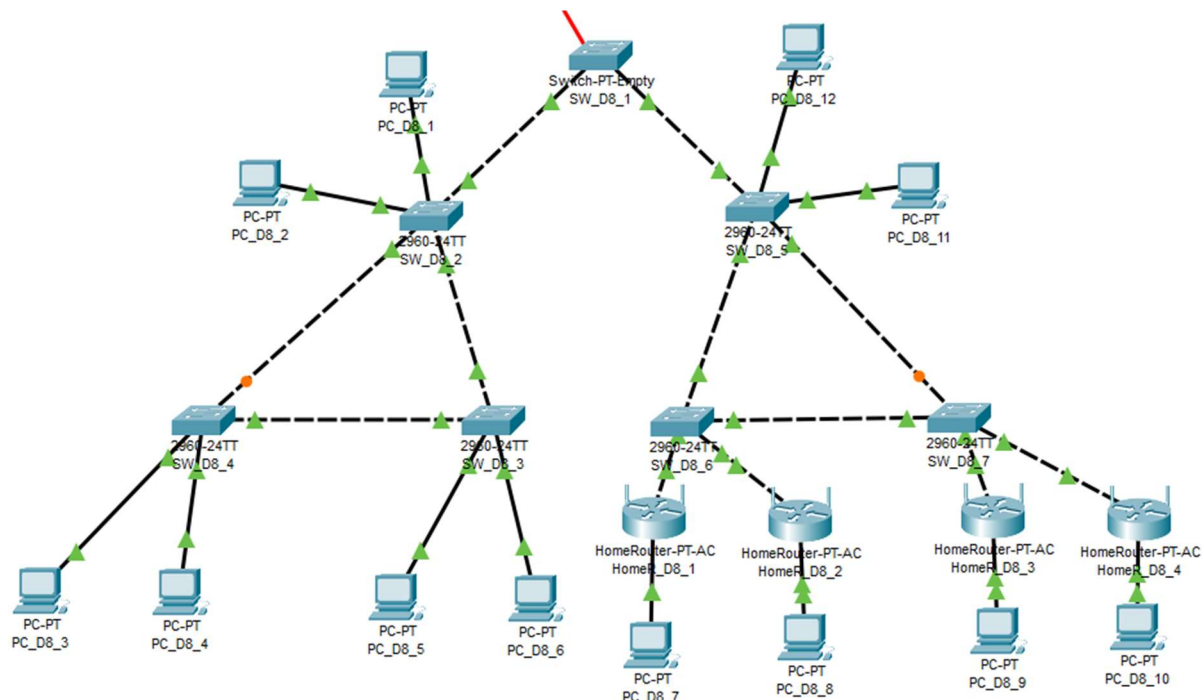


## Додаток В – Схема «послідовне»

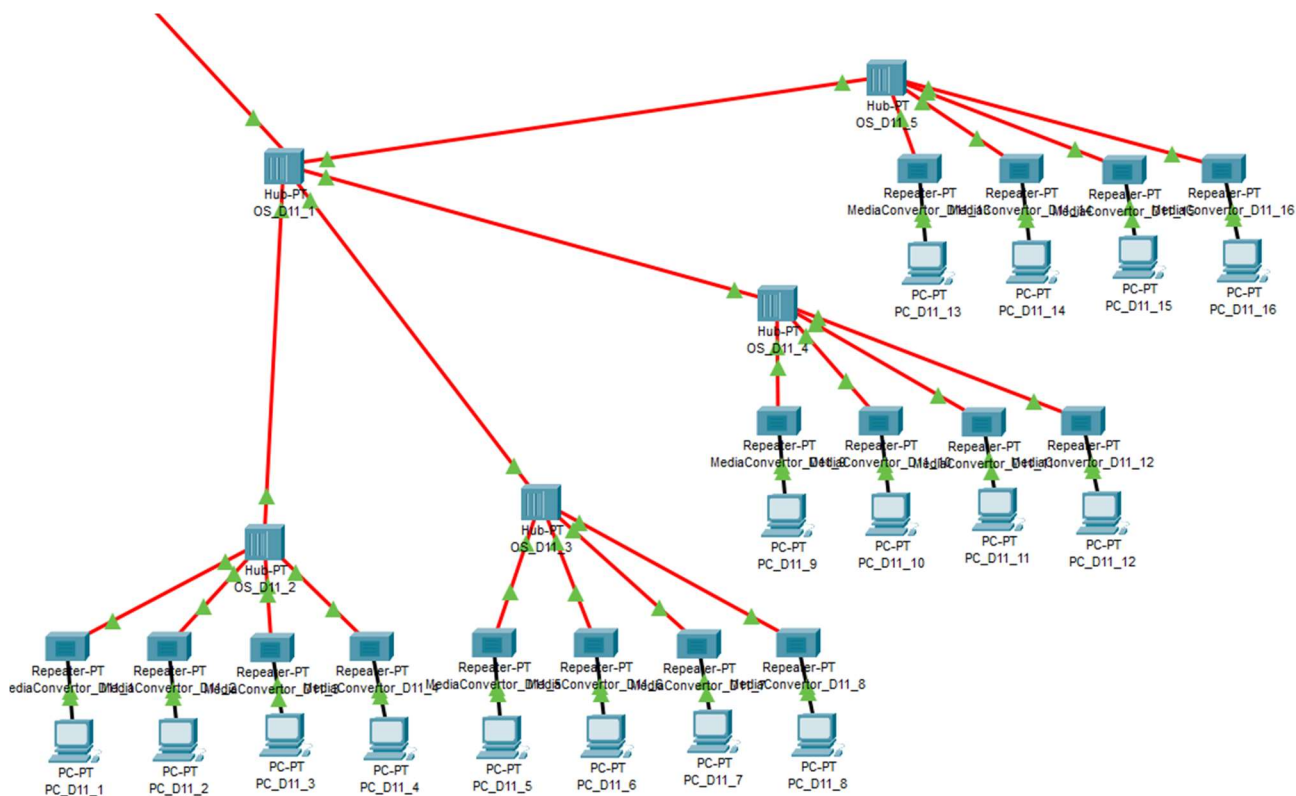


|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | KIK.KP.B – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 91   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

## Додаток Г – Схема «дерево подібна»



## Додаток Г – Схема «PON»



## Додаток Д – Файл конфігурації маршрутизатора ядра

```
CoreR#show run
Building configuration...

Current configuration : 2829 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname CoreR
!
aaa new-model
!
aaa authentication login default group radius local
aaa authentication enable default group radius local
!
no ip cef
no ipv6 cef
!
username badmin secret 5 $1$mERr$0YnMc/8gMTWcOkZcvNTJc/
!
ip ssh version 2
ip domain-name cisco.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
ip address 200.4.210.33 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/0/1
ip address 200.4.210.5 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/0/2
media-type sfp
ip address 200.4.210.9 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1/0
switchport access vlan 4
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet0/1/1
switchport access vlan 5
switchport mode access
```

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 93   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```

switchport nonegotiate
!
interface GigabitEthernet0/1/2
switchport access vlan 6
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet0/1/3
switchport access vlan 7
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet0/2/0
switchport access vlan 8
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet0/2/1
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet0/2/2
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet0/2/3
switchport access vlan 9
switchport mode access
switchport nonegotiate
!
interface Vlan1
no ip address
shutdown
!
interface Vlan4
mac-address 00e0.a307.5201
ip address 200.4.210.21 255.255.255.252
!
interface Vlan5
mac-address 00e0.a307.5202
ip address 200.4.210.1 255.255.255.252
!
interface Vlan6
mac-address 00e0.a307.5203
ip address 200.4.210.25 255.255.255.252
!
interface Vlan7
mac-address 00e0.a307.5204
ip address 200.4.210.17 255.255.255.252
!
interface Vlan8
mac-address 00e0.a307.5205
ip address 200.4.210.13 255.255.255.252

```

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 94   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```

!
interface Vlan9
  mac-address 00e0.a307.5206
  ip address 200.204.0.1 255.255.255.240
!
router ospf 10
  log-adjacency-changes
  network 200.204.0.0 0.0.0.15 area 0
  network 200.4.210.0 0.0.0.3 area 0
  network 200.4.210.4 0.0.0.3 area 0
  network 200.4.210.8 0.0.0.3 area 0
  network 200.4.210.12 0.0.0.3 area 0
  network 200.4.210.16 0.0.0.3 area 0
  network 200.4.210.20 0.0.0.3 area 0
  network 200.4.210.24 0.0.0.3 area 0
  network 200.4.210.28 0.0.0.3 area 0
  network 200.4.210.32 0.0.0.3 area 0
!
router rip
!
ip classless
!
ip flow-export version 9
!
no cdp run
!
radius server 200.204.0.10
  address ipv4 200.204.0.10 auth-port 1645
  key cisco123
!
line con 0
!
line aux 0
!
line vty 0 4
  login authentication default
  transport input ssh
!
end

```

## Додаток Е – Файл конфігурації маршрутизатора розподілу

```

R_1#show run
Building configuration...

Current configuration : 2316 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R_1
!

```

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузіук В.В.        |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 95   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```

aaa new-model
!
aaa authentication login default group radius local
aaa authentication enable default group radius local
!
no ip cef
no ipv6 cef
!
username badmin secret 5 $1$mERr$0YnMc/8gMTWcOkZcvNTJc/
!
ip ssh version 2
ip domain-name cisco.com
!
interface GigabitEthernet0/0
no ip address
!
interface GigabitEthernet0/0.1
description Link_to_D1_M
encapsulation dot1Q 1 native
ip address 200.204.1.1 255.255.255.240
!
interface GigabitEthernet0/0.2
description Link_to_D1_C
encapsulation dot1Q 2
ip address 200.4.1.1 255.255.255.0
!
interface GigabitEthernet1/0
no ip address
!
interface GigabitEthernet1/0.1
description Link_to_D2_M
encapsulation dot1Q 1 native
ip address 200.204.2.1 255.255.255.240
!
interface GigabitEthernet1/0.2
description Link_to_D2_C
encapsulation dot1Q 2
ip address 200.4.2.1 255.255.255.0
!
interface GigabitEthernet2/0
no ip address
shutdown
!
interface GigabitEthernet3/0
no ip address
shutdown
!
interface GigabitEthernet4/0
no ip address
shutdown
!
interface GigabitEthernet5/0
ip address 200.4.210.2 255.255.255.252

```

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 96   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```

duplex auto
speed auto
!
interface GigabitEthernet6/0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet7/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet8/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet9/0
no ip address
duplex auto
speed auto
shutdown
!
router ospf 10
log-adjacency-changes
passive-interface GigabitEthernet0/0
passive-interface GigabitEthernet1/0
network 200.4.1.0 0.0.0.255 area 0
network 200.4.2.0 0.0.0.255 area 0
network 200.204.1.0 0.0.0.15 area 0
network 200.204.2.0 0.0.0.15 area 0
network 200.4.210.0 0.0.0.3 area 0
network 200.4.210.36 0.0.0.3 area 0
!
router rip
!
ip classless
!
ip flow-export version 9
!
access-list 1 permit 0.0.0.0 255.255.255.240
access-list 1 permit host 200.204.0.2
!
no cdp run
!
radius-server host 200.204.0.10 auth-port 1645 key cisco123
!
line con 0
!
line aux 0

```

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 97   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```

!
line vty 0 4
access-class 1 in
access-class 1 out
login authentication default
transport input ssh
!
end

```

## Додаток Є – Файл конфігурації комутатора

```

SW_D1_2#show run
Building configuration...

```

```

Current configuration : 2133 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_D1_2
!
aaa new-model
!
aaa authentication login default group radius local
aaa authentication enable default group radius local
!
ip ssh version 2
ip domain-name cisco.com
!
username badmin secret 5 $1$mERr$0YnMc/8gMTWcOkZcvNTJc/
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 2
!
interface FastEthernet0/2
switchport access vlan 2
!
interface FastEthernet0/3
switchport access vlan 2
!
interface FastEthernet0/4
switchport access vlan 2
!
interface FastEthernet0/5
switchport access vlan 2
!
interface FastEthernet0/6
switchport access vlan 2
!

```

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 98   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```

interface FastEthernet0/7
switchport access vlan 2
!
interface FastEthernet0/8
switchport access vlan 2
!
interface FastEthernet0/9
switchport access vlan 2
!
interface FastEthernet0/10
switchport access vlan 2
!
interface FastEthernet0/11
switchport access vlan 2
!
interface FastEthernet0/12
switchport access vlan 2
!
interface FastEthernet0/13
switchport access vlan 2
!
interface FastEthernet0/14
switchport access vlan 2
!
interface FastEthernet0/15
switchport access vlan 2
!
interface FastEthernet0/16
switchport access vlan 2
!
interface FastEthernet0/17
switchport access vlan 2
!
interface FastEthernet0/18
switchport access vlan 2
!
interface FastEthernet0/19
switchport access vlan 2
!
interface FastEthernet0/20
switchport access vlan 2
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
switchport mode trunk
!

```

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 99   |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

```

interface GigabitEthernet0/2
!
interface Vlan1
ip address 200.204.1.3 255.255.255.240
!
ip default-gateway 200.204.1.1
!
radius-server host 200.204.0.10 auth-port 1645 key cisco123
!
access-list 1 permit 0.0.0.0 255.255.255.240
access-list 1 permit host 200.204.0.2
line con 0
login
!
line vty 0 4
access-class 1 in
access-class 1 out
login authentication default
transport input ssh
line vty 5 15
!
!
!
!
end

```

Додаток Ж – таблиця адрес маршрутизаторів

| Назва при-строю | Інтерфейс | Ме-режа | Адреса       | Маска           | Пре-фікс |
|-----------------|-----------|---------|--------------|-----------------|----------|
| CoreR           | GigE0/1/1 | A       | 200.4.210.1  | 255.255.255.252 | /30      |
|                 | GigE0/0/1 | B       | 200.4.210.5  | 255.255.255.252 | /30      |
|                 | GigE0/0/2 | C       | 200.4.210.9  | 255.255.255.252 | /30      |
|                 | GigE0/2/0 | D       | 200.4.210.13 | 255.255.255.252 | /30      |
|                 | GigE0/1/3 | E       | 200.4.210.17 | 255.255.255.252 | /30      |
|                 | GigE0/1/0 | F       | 200.4.210.21 | 255.255.255.252 | /30      |
|                 | GigE0/1/2 | G       | 200.4.210.25 | 255.255.255.252 | /30      |
|                 | GigE0/0/0 | I       | 200.4.210.33 | 255.255.255.252 | /30      |
|                 | GigE0/2/3 | Office  | 200.204.0.1  | 255.255.255.240 | /28      |
| R_1             | GigE5/0   | A       | 200.4.210.2  | 255.255.255.252 | /30      |
|                 | GigE6/0   | J       | 200.4.210.37 | 255.255.255.252 | /30      |

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 100  |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |

|            |           |      |              |                 |     |
|------------|-----------|------|--------------|-----------------|-----|
|            | GigE0/0.2 | D1_C | 200.4.1.1    | 255.255.255.0   | /24 |
|            | GigE0/0.1 | D1_M | 200.204.1.1  | 255.255.255.240 | /28 |
|            | GigE1/0.2 | D2_C | 200.4.2.1    | 255.255.255.0   | /24 |
|            | GigE1/0.1 | D2_M | 200.204.2.1  | 255.255.255.240 | /28 |
| <b>R_2</b> | GigE5/0   | B    | 200.4.210.6  | 255.255.255.252 | /30 |
|            | GigE6/0   | J    | 200.4.210.38 | 255.255.255.252 | /30 |
|            | GigE0/0.2 | D3_C | 200.4.3.1    | 255.255.255.0   | /24 |
|            | GigE0/0.1 | D3_M | 200.204.3.1  | 255.255.255.240 | /28 |
|            | GigE1/0.2 | D4_C | 200.4.4.1    | 255.255.255.0   | /24 |
|            | GigE1/0.1 | D4_M | 200.204.4.1  | 255.255.255.240 | /28 |
| <b>R_3</b> | GigE5/0   | C    | 200.4.210.10 | 255.255.255.252 | /30 |
|            | GigE6/0   | K    | 200.4.210.41 | 255.255.255.252 | /30 |
|            | GigE0/0.2 | D5_C | 200.4.5.1    | 255.255.255.0   | /24 |
|            | GigE0/0.1 | D5_M | 200.204.5.1  | 255.255.255.240 | /28 |
|            | GigE1/0.2 | D6_C | 200.4.6.1    | 255.255.255.0   | /24 |
|            | GigE1/0.1 | D6_M | 200.204.6.1  | 255.255.255.240 | /28 |
| <b>R_4</b> | GigE5/0   | D    | 200.4.210.14 | 255.255.255.252 | /30 |
|            | GigE6/0   | K    | 200.4.210.42 | 255.255.255.252 | /30 |
|            | GigE0/0.2 | D7_C | 200.4.7.1    | 255.255.255.0   | /24 |
|            | GigE0/0.1 | D7_M | 200.204.7.1  | 255.255.255.240 | /28 |
| <b>R_5</b> | GigE5/0   | E    | 200.4.210.18 | 255.255.255.252 | /30 |
|            | GigE6/0   | L    | 200.4.210.45 | 255.255.255.252 | /30 |
|            | GigE0/0.2 | D8_C | 200.4.8.1    | 255.255.255.0   | /24 |
|            | GigE0/0.1 | D8_M | 200.204.8.1  | 255.255.255.240 | /28 |
|            | GigE1/0.2 | D9_C | 200.4.9.1    | 255.255.255.0   | /24 |
|            | GigE1/0.1 | D9_M | 200.204.9.1  | 255.255.255.240 | /28 |
| <b>R_6</b> | GigE5/0   | F    | 200.4.210.22 | 255.255.255.252 | /30 |

|      |      |                    |        |      |                                 |      |
|------|------|--------------------|--------|------|---------------------------------|------|
|      |      | Гузюк В.В.         |        |      | <b>KIK.KP.B – 123 – 10 – ПЗ</b> | Арк. |
|      |      | П.П. Топольницький |        |      |                                 | 101  |
| Змн. | Арк. | № докум.           | Підпис | Дата |                                 |      |

|     |           |       |              |                 |     |
|-----|-----------|-------|--------------|-----------------|-----|
|     | GigE6/0   | L     | 200.4.210.46 | 255.255.255.252 | /30 |
|     | GigE0/0.2 | D10_C | 200.4.10.1   | 255.255.255.0   | /24 |
|     | GigE0/0.1 | D10_M | 200.204.10.1 | 255.255.255.240 | /28 |
| R_7 | GigE5/0   | G     | 200.4.210.26 | 255.255.255.252 | /30 |
|     | GigE0/    | D11_C | 200.4.11.1   | 255.255.255.0   | /24 |
|     | GigE0/    | D12_C | 200.4.12.1   | 255.255.255.0   | /24 |
| R_8 | GigE5/0   | A     | 200.4.210.2  | 255.255.255.252 | /30 |
|     | GigE0/    | D13_C | 200.4.13.1   | 255.255.255.0   | /24 |

|      |      |                    |        |      |                          |      |
|------|------|--------------------|--------|------|--------------------------|------|
|      |      | Гузюк В.В.         |        |      | КІК.КР.Б – 123 – 10 – ПЗ | Арк. |
|      |      | П.П. Топольницький |        |      |                          | 102  |
| Змн. | Арк. | № докум.           | Підпис | Дата |                          |      |