

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 магістра
на тему: «Методи, технології та інструменти
побудови мережної інфраструктури
міського Інтернет-провайдера»

Виконав студент 2-го курсу групи КІм-22-1
спеціальності 123 «Комп'ютерна інженерія»

 В.В. Гузюк

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

 В.В. Воротніков

Рецензент, завідувач кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

 А.А. Єфіменко

Житомир – 2023

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

13 жовтня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу мігістра

Студент: Гузюк Владислав Віталійович

Тема роботи: «Методи, технології та інструменти побудови мережної інфраструктури міського Інтернет-провайдера»

затверджена Наказом університету від 13 жовтня 2023 р. № 571/с

Термін здачі студентом закінченої роботи 11 грудня 2023 р.

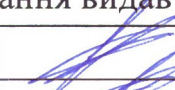
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

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	Я.Т. Кручинський	13.10.23 	13.10.23 
2	Я.Т. Кручинський	13.10.23 	13.10.23 
3	Я.Т. Кручинський	13.10.23 	13.10.23 

Студент  В.В. Гузюк

Керівник  В.В. Воротніков

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	1 вересня	
2	Розробка плану проекту	2 вересня	
3	Вибір програмного забезпечення	4 вересня	
4	Пошук теоретичної інформації	26 вересня	
5	Розробка проекту	20 жовтня	
6	Вибір обладнання	30 жовтня	
7	Створення в програмному додатку проекту	15 листопада	
8	Створення в програмному додатку схеми для тестування захисту	22 листопада	
9	Тестування проекту	28 листопада	
10	Оформлення пояснювальної записки	12 грудня	

Студент  В.В. Гузюк

Керівник  В.В. Воротніков

АНОТАЦІЯ

Пояснювальна записка до випускної кваліфікаційної роботи магістра на тему «Методи, технології та інструменти побудови мережної інфраструктури міського Інтернет-провайдера» складається з вступу, трьох розділів, висновків, списку використаної літератури та додатку.

Текстова частина викладена на 78 сторінках друкованого тексту.

Пояснювальна записка має 12 сторінок додатків. Список використаних джерел містить 44 найменування і займає 4 сторінки. В роботі наведено 39 рисунки. Загальний обсяг роботи – 102 сторінок.

У першому розділі було розглянуто основи мережної архітектури, теоретичну інформацію про протоколи та технології, що застосовують для побудови мереж інтернет-провайдерів .

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

У третьому розділі виконано вибір обладнання для побудови мережі. 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.

ANNOTATION

The explanatory note to the magister's qualification work on the topic "Methods, technologies and tools for building the network infrastructure of a city Internet provider" consists of an introduction, three sections, conclusions, a list of references and an appendix.

The text is set out on 78 pages of printed text.

The explanatory note has 12 pages of appendices. The list of used sources contains 44 names and occupies 4 pages. The paper presents 39 figures. Total volume of work - 102 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.

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ МІСЬКОГО ІНТЕРНЕТ-ПРОВАЙДЕРА.....	10
1.1 Аналіз основних мережних архітектур.....	10
1.2 Моделі побудови мережних інфраструктур міських інтернет- провайдерів.....	14
1.3 Технології та протоколи побудови міських мереж	16
РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ МІСЬКОГО ІНТЕРНЕТ-ПРОВАЙДЕРА.....	47
2.1 Проектування мережної інфраструктури міського інтернет- провайдера	47
2.2 Розробка фізичної та логічної топології мережі.....	49
2.3 Проектування схеми адресації.....	55
2.4 Проектування допоміжної сервісної інфраструктури та підсистеми захисту мережі.....	57
РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ПРАЦЕЗДАТНОСТІ МІСЬКОЇ МЕРЕЖІ ІНТЕРНЕТ-ПРОВАЙДЕРА	58
3.1 Вибір обладнання та програмного забезпечення для проекту мережної інфраструктури	58
3.2 Базове налагодження мережних пристроїв	65
3.3 Налagodження засобів підсистеми захисту мережі	69
3.4 Тестування складових елементів мережної інфраструктури та підсистеми захисту мережі	75
ВИСНОВКИ.....	83
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	84
ДОДАТКИ.....	88

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

ВСТУП

Актуальність даної теми обумовлена стрімким розвитком технологій, що призводить до зростання числа користувачів мережі та розширення попиту на інтернет-підключення для різноманітних пристроїв. Зокрема, швидке, стабільне і безпечне розгортання мереж стає важливим завданням, оскільки збільшується число інтернет-сервісів.

Мета даної кваліфікаційної роботи полягає у визначенні методів побудови мережі міського інтернет-провайдера. Це визначає ряд конкретних завдань, таких як:

- Аналіз необхідних технологій та протоколів для побудови інтернет-мереж.
- Розгляд обладнання та компаній, які його виробляють, що доступні на ринку.
- Проектування мережі інтернет-провайдера в емуляторах та симуляторах.
- Тестування роботи створених мереж.

Об'єктом дослідження є процес проектування комп'ютерних мереж інтернет-провайдерів та захист інформації в них, а також технології, що використовуються при їхній побудові, та компанії, які надають відповідне обладнання. Предметом дослідження є мережі міського інтернет-провайдера, технології FastEthernet та GigabitEthernet, OSPF, RSTP, PON, а також протоколи захисту обладнання та мережного обладнання від таких компаній, як Cisco, Huawei, Juniper, BDCOM.

У процесі виконання роботи було розроблено проект міської мережі інтернет-провайдера за допомогою програмного додатку Cisco Packet Tracer, використовуючи доступне мережне обладнання від компанії Cisco. Реалізація підсистем захисту буде виконана у програмному додатку GNS 3.

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ МІСЬКОГО ІНТЕРНЕТ-ПРОВАЙДЕРА

1.1 Аналіз основних мережних архітектур

Мережева архітектура - широке поняття, яке охоплює багато розділів і означень. Краще за все його можна описати як "каркас, що несе або підтримує будь-яку побудову". Мережева архітектура завжди є основою і фундаментом для роботи мережі. Вона складається з таких елементів, як топологія локальної мережі, кабельна інфраструктура та активне мережеве обладнання. Важливо ретельно вибирати ці компоненти для оптимізації продуктивності, спрощення управління та забезпечення можливості подальшого зростання і розвитку мережі. Кабельна інфраструктура є однією з найважливіших складових мережі, і погано спроектована або встановлена система може призвести до проблем і значно ускладнити усунення несправностей. При монтажі кабелів важливо дотримуватися стандартів, які описують зіркообразну топологію мережі. Це включає розподільні шафи, які з'єднані кабелями, та магістральну ділянку, що з'єднує ці шафи.

Зазвичай для передачі даних використовується мідна звита пара (UTP). Існує сім категорій цього типу кабелю. На сьогоднішній день найбільш поширені лише чотири категорії: 5, 5e, 6, 6a, 7 та вище. Кабель категорії 5 і вище є 4-парним і використовується для таких типів мереж:

- 100 BASE-TX;
- 1000 BASE-T;
- 10G Base-T та вище.

З використанням лише 2 пар можна досягти швидкості передачі 100 Мбіт/с, а при використанні всіх 4 пар - до 1000 Мбіт/с і вище. Кабель категорії 5e застосовується частіше через свою низьку собівартість і малий діаметр. Кабелі категорії 6 і 6a використовуються лише в мережах Gigabit Ethernet та 10 GE.

Волоконно-оптичні мережі стали широко поширеними і використовуються всюди. Деякі оператори зв'язку стверджують, що встановлення оптичної лінії обходиться дешевше, ніж лінії, побудовані на мідному кабелі UTP. Однак обладнання для оптичної мережі є значно дорожчим порівняно з аналогами для мереж, побудованих на мідній зв'язній парі.

Незважаючи на ціну, волоконно-оптична мережа має безліч переваг перед мідними кабелями. В порівнянні зі звитою парою вона може передавати дані на великі відстані з великою швидкістю, при цьому не вносячи додаткових перешкод у сигнал.

Але незалежно від того, яке середовище передачі даних обрано, важливо враховувати можливе зростання та розширення мережі. При створенні мережі необхідно враховувати запас кабелів і збільшувати діаметри монтажних отворів і кабельних каналів свідомо більше, ніж необхідно. Це сприятиме прокладанню додаткових кабелів без зайвих труднощів, якщо це буде потрібно.

Крім кабельно-лінійної системи, активне мережеве обладнання є важливим компонентом будь-якої мережі. Мости, комутатори і маршрутизатори дозволяють збільшити кількість підключених пристроїв і ефективно розділяти трафік для підвищення продуктивності. Розуміння відмінностей між пристроями і їхніми особливостями дозволяє легко визначити момент та місце для встановлення конкретного обладнання.

Мости використовуються для об'єднання двох чи більше однотипних мереж, зберігаючи прозорість для всіх мережевих протоколів. Вони фізично розділяють дві мережі, але логічно утворюють одну єдину мережу. Мости дозволяють поділити весь трафік на сегменти, пропускаючи лише той, який призначений для пристроїв по іншу сторону мосту. Важливо враховувати можливі недоліки, такі як виникнення широкомовного шторму внаслідок передачі пакетів по широкомовному каналу.

Хоча колись мости були популярним методом з'єднання мереж, сучасні маршрутизатори стали більш доступними і ефективними завдяки технічному прогресу.

Багато виробників пропонують маршрутизатори з функціями мостів, що дозволяє їм працювати як маршрутизатори і мости одночасно.

Маршрутизатори, встановлені як на спеціалізованих пристроях, так і на мережевих серверах, забезпечують високу продуктивність і гнучке управління. Вони дозволяють фізично і логічно розділити мережу, а також створювати резервні канали для підвищення надійності мережі. Незважаючи на це, важливо урахувати вартість та продуктивність для конкретного випадку мережі. 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 розбиває мережу на менші домени, що дозволяє кожному кінцевому вузлу отримати більшу частку загальної пропускної спроможності. Фактично, це подібно до мостів, комутатори направляють весь трафік з однієї мережі в іншу.

Існують комутатори, які передають пакет лише після його повного отримання. Такі комутатори використовують метод комутації, відомий як "проміжна буферизація". Його принцип полягає в тому, що прийнятий пакет записується в пам'ять комутатора, перевіряється на помилки за допомогою спеціальних алгоритмів, і лише після цього відправляється далі по мережі до призначення.

Також існують комутатори, які використовують метод "наскрізної комутації". Цей метод відрізняється від проміжної буферизації тим, що комутатор пересилає пакет даних в той самий момент, коли отримує адресу отримувача. Цей підхід дозволяє зменшити затримки порівняно із проміжною буферизацією, але збільшує ризик того, що адресат отримає пошкоджений пакет.

Існують також комутатори гібридного типу, які, приймаючи пакет, спочатку перевіряють його на помилки і ведуть облік їх кількості. Якщо загальна кількість помилок перевищує певний поріг, активується буферизація, яка залишається активною до тих пір, поки кількість помилок не стане допустимою. Після цього комутатори знову переходять до режиму наскрізної комутації.

У комутаторів існують деякі недоліки. Подібно до мостів, вони передають пакети по широкомовних каналах і не забезпечують належного захисту від стану, коли широкомовні пакети повністю заповнюють всю мережу. Крім того, при наскрізній комутації, адресат може отримати пошкоджений або неповний пакет даних, а при проміжній буферизації істотно знижується швидкість роботи самого пристрою. [10]

1.2 Моделі побудови мережних інфраструктур міських інтернет-провайдерів

В умовах ринкової економіки суб'єктами підприємницької діяльності у галузі телекомунікацій виступають мережеві оператори та сервіс-провайдери (постачальники послуг). Вони відповідають за розбудову мереж зв'язку для загального використання, відомих як публічні мережі (Public Network). Ці мережі призначені для надання послуг зв'язку різним категоріям користувачів.

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

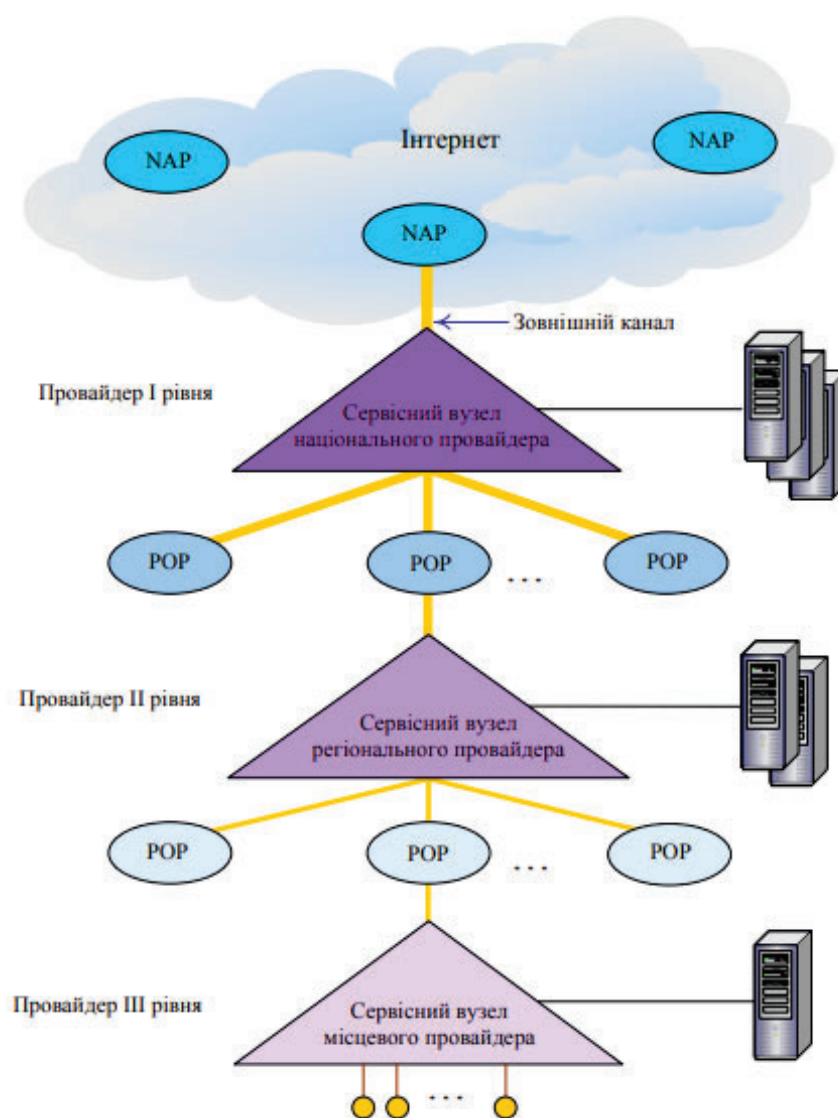


Рисунок 1.1 – Інтернет-сервіс-провайдинг

У цьому проекті ми розглядатимемо провайдера на місцевому рівні, проте це не виключає можливості провайдера поєднувати різні рівні для збільшення прибутку. Оскільки цей проект передбачає дослідження методів побудови міської мережі, наш провайдер буде вважатися провайдером на місцевому рівні.

На найбільш узагальненому рівні, будь-яка мережа складається з набору точок і з'єднуючих їх ліній, розташування яких визначає зв'язність мережі і її здатність забезпечувати інформаційний обмін між різними адресатами. Така структура мережі відома як "топологія".

При побудові мережі можуть використовуватися різні типи топологій, такі як:

- "точка-точка";
- деревоподібна;
- "кільце";
- коміркова;
- змішані.

Найбільш доцільним при побудові є використання змішаного типу топології, що може полегшити побудову мереж у конкретному районі чи іншій територіальній одиниці, але водночас може ускладнити обслуговування самої мережі.

Логічна топологія мережі є також важливою частиною, і вона визначає, як рухатиметься інформація в межах мережі від джерела до отримувача. Типи логічних топологій включають:

- логічну шину;
- логічне кільце;
- комутовану топологію.

Важливо відзначити, що фізична та логічна топологія можуть збігатися або не збігатися.

1.3 Технології та протоколи побудови міських мереж

Для розгортання міських мереж необхідно використовувати різноманітні протоколи та технології для забезпечення ефективної передачі інформації, зокрема:

- FastEthernet, GigabitEthernet та 10 GE;
- Протоколи IPv4 і IPv6;
- Протокол OSPF;
- Протоколи STP та RSTP;
- Технологія PON.

Термін "FastEthernet" вказує на набір стандартів Ethernet для передачі даних зі швидкістю 100 Мбіт/с, що в 10 разів перевищує початкову швидкість Ethernet у 10 Мбіт/с. Класичний 10-мегабітний Ethernet використовувався протягом багатьох років, але його обмежена пропускна здатність стала помітною проблемою. У зв'язку з цим виникла необхідність у розробці більш продуктивної технології, яка б забезпечувала швидкість 100 Мбіт/с.

FastEthernet і 100VGAnyLAN стали результатом досліджень та розділили експертів на дві групи. У 1995 році комітет IEEE 802.3 прийняв специфікацію FastEthernet як доповнення до існуючого стандарту 802.3. Мережі Fast Ethernet орієнтовані на зіркові та ієрархічні фізичні топології, і при використанні комутаторів називаються комутованими.

FastEthernet використовує різні специфікації фізичного рівня для підтримки кабельних систем на витій парі, такі як 100Base-TX, 100Base-T4 та 100Base-T2. Можливість використання волоконно-оптичного кабелю також розглядається. Вони представлені на рисунках 1.2 та 1.3.

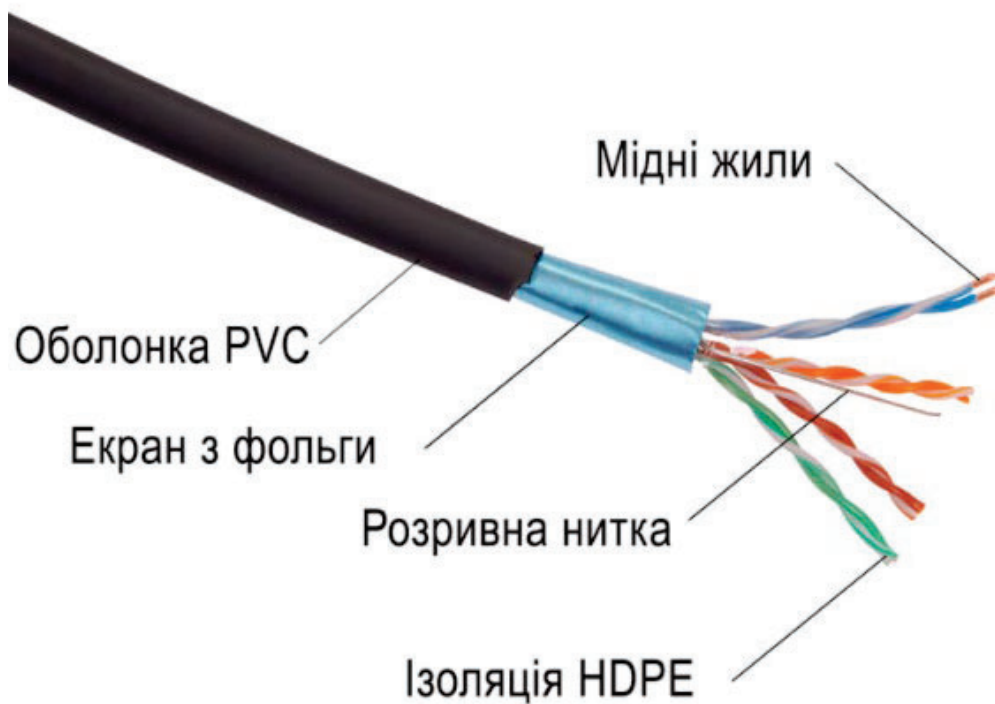


Рисунок 1.2 – Конструкція звитої пари

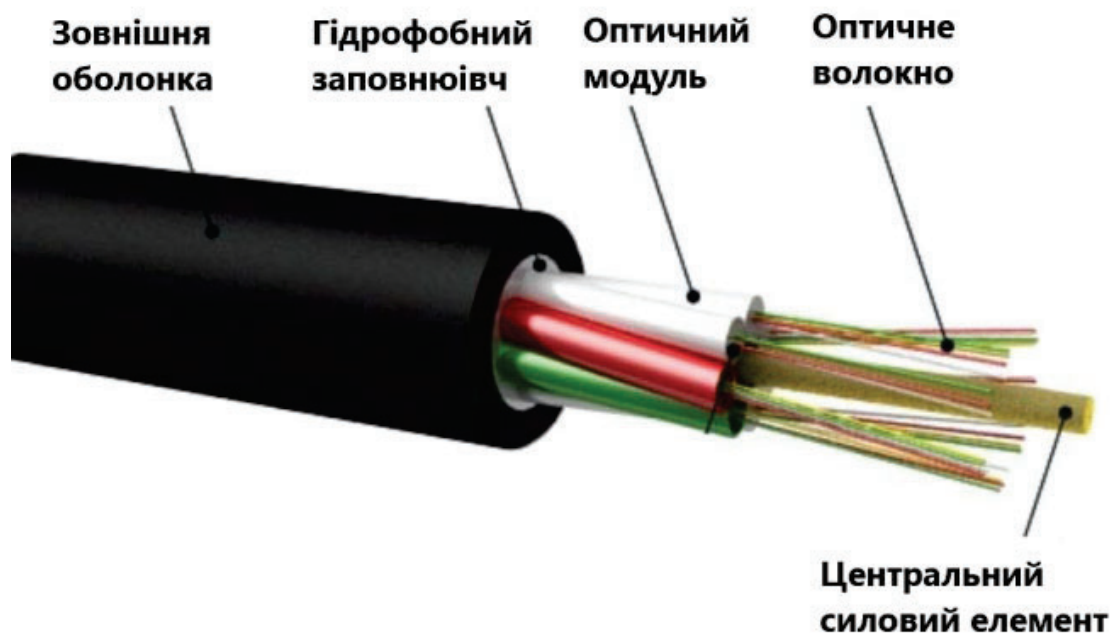


Рисунок 1.3 – Конструкція волоконно-оптичного кабелю

Після введення продуктів Fast Ethernet мережеві інтегратори та адміністратори швидко виявили певні обмеження при створенні корпоративних мереж. У ба-

гатьох випадках сервери, підключені за допомогою 100-мегабітних каналів, перевантажували магістралі мереж, які також працюють на швидкості 100 Мбіт/с — магістралі FDDI і Fast Ethernet. Виникла необхідність в наступному рівні ієрархії швидкостей.

У січні 1997 року було розглянуто першу версію стандарту, а остаточне затвердження стандарту 802.3z відбулося 29 червня 1998 року на засіданні комітету IEEE 802.3. Завдання з реалізації Gigabit Ethernet на крученому кабелі категорії 5 були передані спеціальному комітету 802.3ab, який вже відмітив кілька варіантів проекту цього стандарту, і з липня 1998 року проект набув стабільності.

Деякі компанії, не чекаючи на офіційне затвердження стандарту, випустили перше обладнання Gigabit Ethernet на оптоволоконному кабелі ще до літа 1997 року. Основна концепція розробників стандарту Gigabit Ethernet полягає в максимальному збереженні основних принципів класичної технології Ethernet при досягненні бітової швидкості в 1000 Мбіт/с.

Важливо відзначити, що на рівні протоколу Gigabit Ethernet, так само як і його менш швидкісні варіанти, не підтримує:

- якість обслуговування;
- надлишкові зв'язки;
- тестування працездатності вузлів і обладнання (за винятком тестування зв'язку порт-порт, як це робиться для Ethernet 10Base-T і 10Base-F, а також Fast Ethernet).

Основна ідея технології Gigabit Ethernet полягає в тому, що в багатьох мережах висока швидкість магістралі та можливість надання пакетам пріоритету в комутаторах є достатніми для забезпечення якісного транспортного обслуговування усіх користувачів мережі. Тільки у виняткових ситуаціях, коли магістраль значно завантажена, і вимоги до якості обслуговування високі, застосування технології АТМ може стати необхідним. Ця технологія, завдяки своїй високій технічній складності, надає гарантії якості обслуговування для різних видів трафіку.

У порівнянні з технологіями Ethernet і Fast Ethernet у Gigabit Ethernet:

- зберігаються всі формати кадрів Ethernet;
- підтримується як напівдуплексна версія протоколу, що використовує метод доступу CSMA/CD, так і повнодуплексна версія, яка працює з комутаторами;
- підтримуються всі основні види кабелів, що використовуються в Ethernet і Fast Ethernet, такі як волоконно-оптичний, вита пара категорії 5 і коаксіальний кабель.

Існують чотири різні фізичні стандарти для Gigabit Ethernet, які використовують оптоволокно (1000Base-X), виту пару (1000Base-T) або збалансований мідний кабель (1000Base-CX).

Стандарт IEEE 802.3z включає в себе 1000Base-SX для передачі по багатомодовому волокну, 1000Base-LX для передачі по одномодовому волокну, а також практично застарілий 1000Base-CX для передачі по збалансованому мідному кабелю. Ці стандарти використовують 8b/10b кодування, яке розширює пропускну здатність каналу на 25%, з 1000 Мбіт/с до 1250 Мбіт/с для забезпечення симетричного сигналу з постійною складовою. Символи передаються за допомогою методу NRZ.

Реалізація технології Gigabit Ethernet для звитої пари була особливо складною через обмеження середовища (cat-5e 125 МГц, 4 пари провідників). Ці обмеження були подолані за допомогою сучасних цифрових сигнальних процесорів та методу кодування PAM-5. (рисунок 1.7).

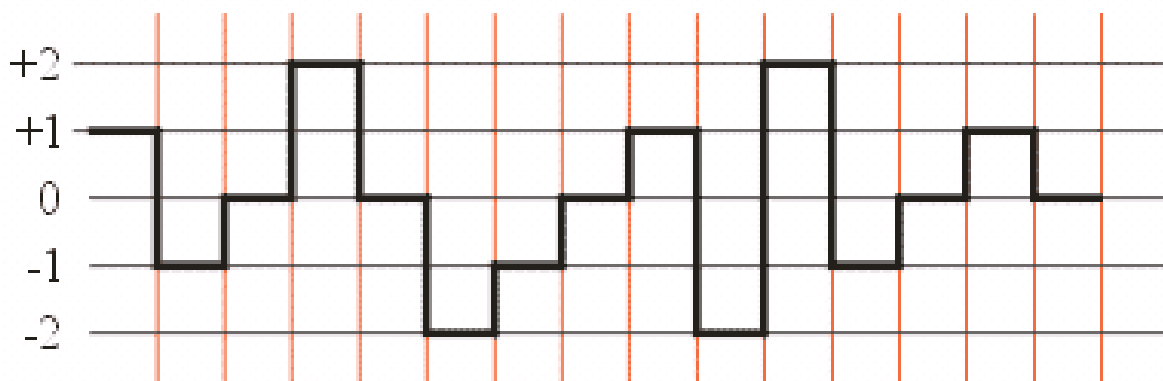


Рисунок 1.4 – Кодування п'ятирівневним сигналом PAM-5

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

Основні специфікації технології Gigabit Ethernet представлені у табл. 1.2.

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

Стандарт 1000Base-T, відомий як IEEE 802.3ab, використовує виту пару категорії 5е для передачі даних за участь у 4 парах. Швидкість передачі даних становить 250 Мбіт/с для кожної пари, використовуючи метод кодування РАМ5 та основну частоту 62,5 МГц. Максимальна допустима відстань становить 100 метрів. На рисунку 1.8 представлена структура рівнів Gigabit Ethernet. Як і у стандарті Fast Ethernet, в Gigabit Ethernet не існує універсальної схеми кодування сигналу, що б підходила для всіх фізичних інтерфейсів. Наприклад, для стандартів 1000Base-LX/SX/CX використовується кодування 8В/10В, тоді як для стандарту 1000Base-T застосовується

спеціальний розширений лінійний код TX/T2. Функцію кодування виконує підрівень кодування PCS, який розташований нижче за середовищенезалежний інтерфейс GMII.

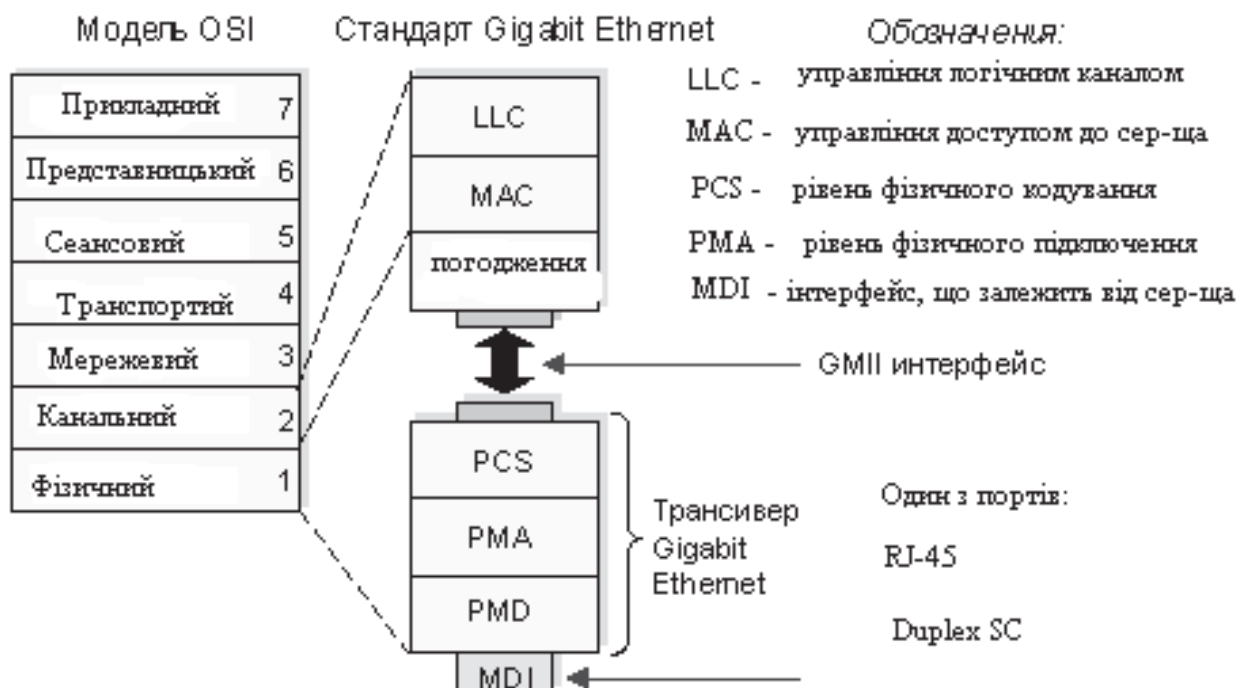


Рисунок 1.5 – Структура рівнів стандарту Gigabit Ethernet

Фізичний рівень Gigabit Ethernet має кілька інтерфейсів, що охоплюють різні технології, включаючи традиційну використання витой пари категорії 5, а також багатомодове і одномодове волокно. Підрівень PMD визначає оптичні та електричні характеристики фізичних сигналів для різних типів середовищ. Загалом існують чотири різних типи фізичних інтерфейсів середовища.

Формат кадру Gigabit Ethernet представлено на рисунку 1.9.

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

Рисунок 1.6 – Формат кадру Gigabit Ethernet

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

Якщо порівнювати Gigabit Ethernet і його попередників, вони мають наступні загальні риси:

- Збережені всі формати кадрів Ethernet.

- Існують напівдуплексна та дуплексна версії.
- Підтримуються основні середовища (звита пара, волоконно-оптичний кабель).

Відмінності включають:

- 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.

На заміну стандарту Gigabit Ethernet прийшов 10 Gigabit Ethernet. Стандарт 10 Gigabit Ethernet був розроблений і вперше опублікований у вересні 2002 року в документі з ідентифікатором IEEE 802.3ae. Однак перед тим декілька років (у 1999 році) була визначена робоча група для розробки стандарту 10 Gigabit Ethernet, і вона активно працювала над його стандартизацією до офіційного прийняття в 2002 році.

Основною перевагою 10 Gigabit Ethernet є здатність передавати дані із швидкістю 10 гігабіт на секунду. Це робить його ідеальним для великих обсягів даних, великих корпоративних мереж, дата-центрів та інших високопродуктивних застосувань.

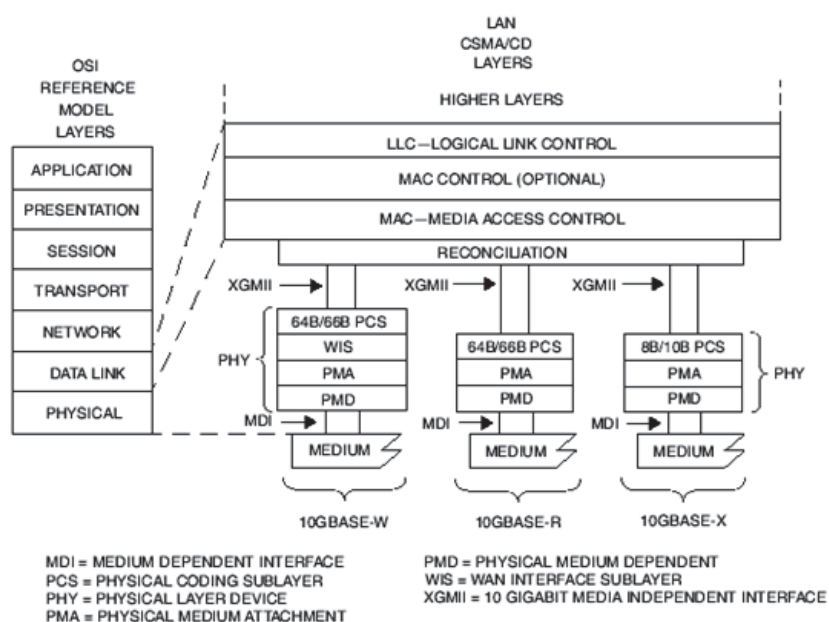


Рисунок 1.7 – Структура рівнів стандарту 10 Gigabit Ethernet

10GE може бути реалізовано на різних типах медіа, таких як оптичні волокна, мідні кабелі, або ж мідно-оптичні гібриди, що надає більше гнучкості при проектуванні мережі. 10GE підтримує різні режими передачі, включаючи половинну та повну дуплексну передачу даних. Повна дуплексна передача дозволяє відсутність конфліктів при передачі і отриманні даних одночасно.

10GE широко використовується в великих корпоративних мережах, дата-центрах, провайдерських мережах і інших областях, де вимагається велика пропускна здатність.

Один з варіантів реалізації 10GE використовує мідні кабелі (10GBase-T), що дозволяє використовувати існуючі інфраструктури мідних кабелів для впровадження швидкої мережі без необхідності прокладання нових оптичних волокон.

Для використання оптичних мереж існує технологія FTTx, яка є загальною назвою для різних варіантів архітектури, відмінності між якими полягають у відстані до кінцевої точки, до якої доходить оптичний сигнал.

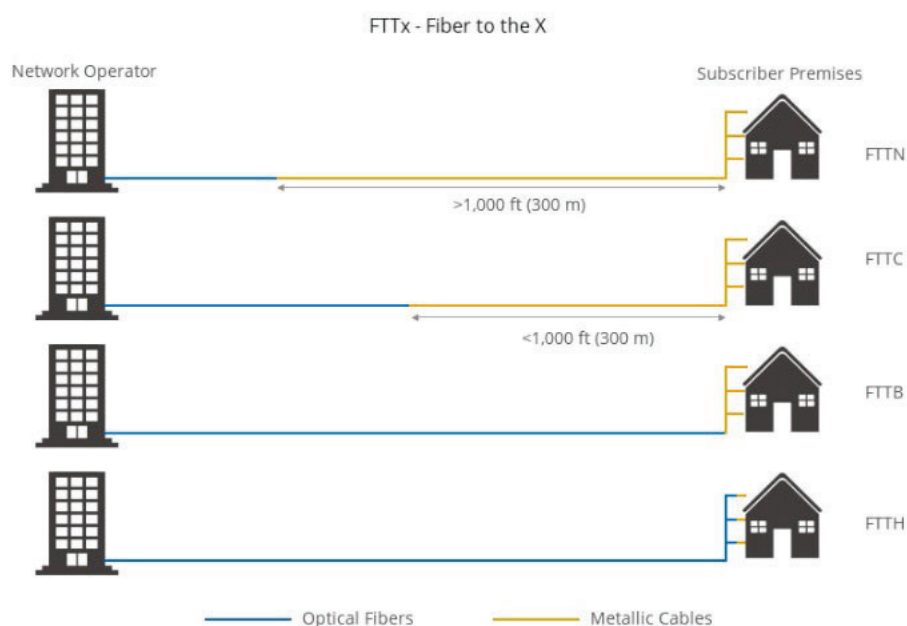


Рисунок 1.8 – Технології FTTx

Fibre to the Home (FTTH) представляє собою мережеву архітектуру, в якій оптичний кабель доходить безпосередньо до житлового будинку. Ця архітектура може використовувати різні мережеві структури, такі як домашня (Home Run), активна мережа типу "зірка" або пасивні оптичні мережі (PON).

У випадку FTTH – Home Run, оптичне волокно прокладається безпосередньо з офісу до клієнта. Ця архітектура призначена для обмеженої кількості клієнтів, оскільки не кожному потрібно мати найкоротший шлях до глобальної мережі. Кожному користувачеві прокладається два кабелі: один для інтернету і другий для кабельного телебачення.

FTTH – Активна зірка використовує локальні активні вузли, що дозволяє зменшити кількість кабелів між користувачами та офісом провайдера. Однак вона включає активні вузли, такі як комутатори, що може підвищити вартість мережі при використанні оптичних інтерфейсів.

Fibre to the Antenna (FTTA) передбачає підключення оптичного волокна до віддаленої RRH в верхній частині вежі мобільного зв'язку.

Fibre to the Node (FTTN) включає оптичний кабель, що веде до мережного вузла. Відстань між клієнтом і вузлом складає кілька кілометрів.

Fibre to the Building (FTTB) передбачає прокладання оптичного кабелю до будинку. Ця архітектура зручна для підключення багатьох квартирних будинків і схожа на FTTH, за винятком того, що використовується мідний кабель від вузла до користувача.[41]

Технологія PON (пасивна оптична мережа або Passive Optical Network) розглядає можливість створення розгалуженої мережі, переважно з деревоподібною топологією, без використання активних компонентів, а замість цього використовує пасивні оптичні розгалужувачі. PON ідеально підходить для покриття обширних територій з різною щільністю забудови, включаючи багатоповерхові райони і котеджні містечка, де переваги цієї технології виявляються в повній мірі.

Зазвичай передача та прийом інформації в PON відбувається по одному оптичному волокні, але на різних довжинах хвиль (1310 та 1490 нм). Інформація для всіх користувачів передається одночасно з використанням каналів, розділених за часом, від головної станції, яка також називається оптичним лінійним терміналом (OLT), до кінцевих оптичних мережевих блоків (ONU).

Оптична потужність, яка виходить з OLT у вузлах мережі, розподіляється (рівномірно або нерівномірно) так, щоб рівень сигналу на вході всіх ONU був приблизно однаковий.

Переваги технології PON включають:

- Економію волокон у оптичних кабелях;
- Значну економію оптичних випромінювачів на головній станції;
- Можливість передачі трьох видів інформації (згідно концепції Triple Play) - голосу, відео та даних;
- Відсутність потреби в електроживленні для мережевих елементів (за винятком кінцевих);
- Невеликі витрати на обслуговування;
- Просте підключення абонентів;
- Можливість подальшого збільшення швидкості передачі (до 10 Гбіт/с та вище) без заміни обладнання лінійного тракту (оптичні кабелі, розгалужувачі, з'єднувачі).

Стандарт GPON (Gigabit-capable Passive Optical Network) є одним із широко використовуваних стандартів PON, який забезпечує передачу даних на швидкостях до 2,488 Гб/с у прямому потоці та 1,244 Гб/с у зворотньому, з максимальним коефіцієнтом ділення 1:128.

Ця технологія використовує наступні довжини хвиль:

- 1490 нм для передачі сигналу в напрямку абонента;
- 1310 нм для прийому сигналу від абонента;
- 1550 нм зарезервовано для кабельного телебачення.

Основою для технології GPON є GFP (Generic Framing Protocol), і вона використовує також TDMA, SDH, Ethernet та ATM.

Ця технологія дозволяє гнучко налаштовувати широкий спектр послуг за допомогою внутрішніх інструментів з різними пріоритетами та швидкостями.

GEPON (Gigabit Ethernet Passive Optical Network) є одним з різновидів технології пасивних оптичних мереж PON, яка дозволяє передавати і приймати дані на швидкості до 1,2 Гбіт/с, з максимальним коефіцієнтом ділення 1:64. Також, аналогічно до технології GPON, GEAPON використовує 1490 нм для передачі інформації, 1310 нм для прийому, і 1550 нм зарезервовано для кабельного телебачення.

Формування кадру в GEAPON відбувається шляхом "додавання" заголовка в ETHERNET фрейм інформації, яка містить дані про тимчасовий слот ONU, її MAC-адресу і засоби коригування помилок.

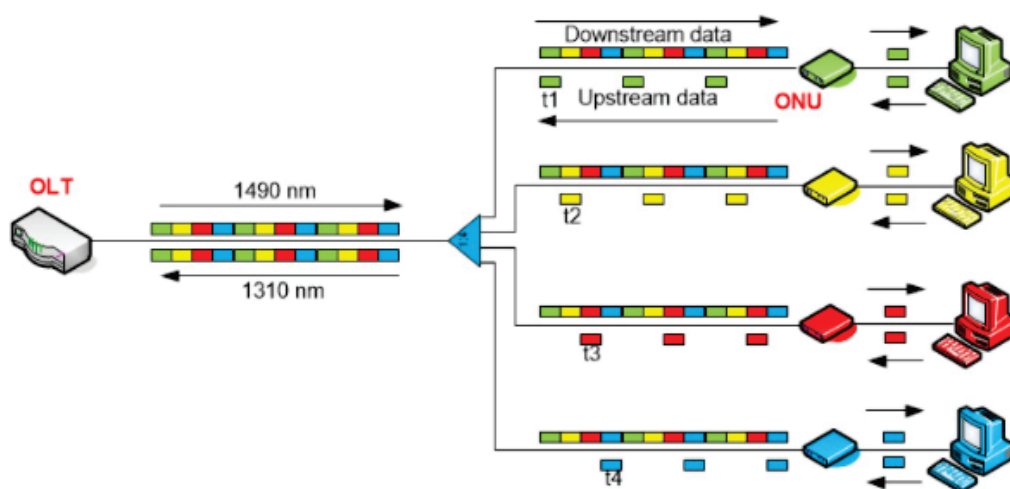


Рисунок 1.9 – Ілюстрація роботи PON

Використовуючи обидві технології, можна створити широкомасштабну мережу передачі даних, враховуючи потреби у певній кількості потенційних клієнтів. Після аналізу географічних особливостей та потенційної кількості клієнтів можна визначити, яку технологію варто використовувати. Наприклад, в локаціях з менше ніж 200 потенційними абонентами можна обрати GEAPON або GPON, оскільки GPON має мінімальну ємність на тисячу двадцять чотири абоненти, порівняно з 256 абонентами на пристрій для GEAPON. Вибір між цими технологіями також залежить від цілей побудови мережі та вимог до типу клієнтів.

Якщо мережа головним чином використовується для корпоративних клієнтів, рекомендується обрати GPON через його гнучкість конфігурації, щоб відповідати вимогам замовника до рівня послуг, наданих.[13]

Щодо протоколів IPv4 і IPv6, оригінальна версія Internet Protocol, IPv4, була вперше розгорнута в ARPANET у 1983 році. IPv4 є четвертою версією IP-адреси з обмеженням у 4 мільярди IP-адрес. Адреса IPv4 виражається у 32-бітному цілому значенні та записується у крапково-десяткових позначеннях, що складаються з чотирьох груп октетів восьми значущих адрес, виражених незалежно у десятичних нотах і розрізняються крапками. Діапазон може бути від 0 до 255.

Наприклад, IP-адреса 105.249.119.16 представляє 32-розрядне десяткове число, а в двійковій системі – 01101001.11111001.01110111.00010000.

Далі наведено схематичне пояснення заголовка дейтаграми:

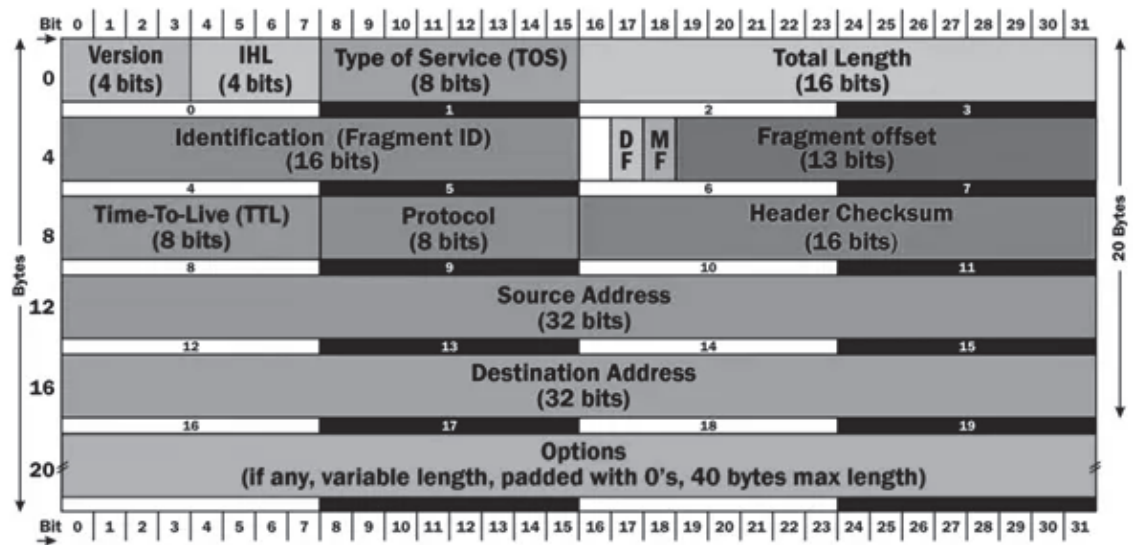


Рисунок 1.10 – Заголовок дейтаграми ipv4

Заголовок дейтаграми ipv4 у табличному форматі нижче:

Таблиця 1.3 – Заголовок дейтаграми ipv4

Версія	Це 4-бітове поле, і воно говорить про версію IP, яку ми використовуємо.
IHL	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).

Продовження таблиці 1.3

Тип послуги	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.
Загальна довжина	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
Ідентифікація (ідентифікатор фрагмента)	Оскільки IPv4 - послуга дейтаграми, ці біти допомагають однозначно ідентифікувати, коли фрагментація закінчується на пакети дейтаграм.
Прапори	Прапор вказує на фрагментацію за допомогою ідентифікаційного поля, в основному вказує, чи може бути фрагментований чи поточний - остаточним.
Зсув фрагмента	Положення сусіда кожного фрагмента вимірюється від початку вихідних даних одиницями у 8 байт.
Час жити	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.
Протокол	IPv4 містить дані з різних протоколів. Це поле допомагає мережевому шару зрозуміти, які дані належать до якого протоколу.

Продовження таблиці 1.3

Заголовок контрольної суми	Це поле використовується для виявлення помилок у пакетах чи повідомленнях.
IP-адреса джерела	32-розрядна адреса хоста, що відправляє.
Ip адреса призначення	32-розрядна адреса приймаючого хоста.
Параметри	Кожна датаграма не вказує поле опцій. Саме перелік специфікацій містить обмеження безпеки, маршрутизацію тощо.

Недоліки IPv4 включають:

- Нестача адресного простору, оскільки кількість підключених пристроїв до Інтернету стрімко зростає.
- Слабка розширюваність протоколу через недостатній розмір заголовка IPv4, який не може вмістити необхідні додаткові параметри.
- Проблеми з обмеженням безпеки комунікацій, оскільки інформація може мати необмежений доступ, що початково було розроблено для ізольованих військових мереж і потім адаптовано для громадських та дослідницьких мереж.
- Відсутність якісної підтримки в сервісі затримки пропускної здатності і те, що деякі мережі не підтримують це.

Переваги IPv4 включають:

- Надійна безпека завдяки шифруванню даних для забезпечення конфіденційності та безпеки під час комунікації.

- Великі можливості маршрутизації через велику кількість функціональних маршрутизаторів, що робить його важливим зв'язком для Інтернету та забезпечує легке підключення багатьох пристроїв у великих мережах без NAT.
- Відмінна ефективність для відео бібліотек та конференцій, надаючи якісне обслуговування та ефективну передачу даних за участю служб TCP і UDP.
- Гнучкість маршрутизації, яка є більш масштабованою та ефективною, зокрема для передачі та обміну даними між мережами в організаціях.[7]

Протокол Інтернету версії 6 (IPv6) представляє собою нову ітерацію протоколу мережевого рівня, яка забезпечує передачу інформації у мережі. Хоча розробка його почалася у 1998 році, його широке впровадження і заміна протоколу IPv4 на початковому етапі відбулися лише у 2017 році.

Очікувалося, що до 2010 року всі доступні унікальні IPv4-адреси будуть вичерпані, і користувачам буде потрібно шукати альтернативи. З цією метою був розроблений новий протокол мережевого рівня, що дозволяє надавати додаткові унікальні адреси, і саме це послужило виникненню протоколу IPv6.

IPv6 має три класи адрес:

- Unicast – індивідуальна адреса, яка використовується для направлення пакета до конкретного інтерфейсу хоста.
- Multicast – групова адреса, застосовується для одночасної передачі пакетів від одного відправника до багатьох хостів-отримувачів з однаковою груповою адресою.
- Anycast – альтернативна адреса, яка працює за принципом схожим до групової адреси, але пакети доставляються до найближчого інтерфейсу від відправника.

Різниця між IPv4 і IPv6:

- У IPv6 адреси складаються з 128 біт, представлених восьми 16-бітовими шістнадцятковими блоками, розділеними двокрапкою. Наприклад, 2dfc:0:0:0:0217:cbff:fe8c:0. IPv4 використовує запис у вигляді чотирьох десяткових чисел (від 0 до 255), розділених крапками, і вказує довжину маски підмережі, наприклад, 192.168.0.0/16.

- У IPv4 для мультікастингу використовується підмережа 224.0.0.0/4, тоді як IPv6 використовує вбудований адресний простір FF00::/8.

- IPv4 використовує широкомовні адреси для передачі широкомовних пакетів, тоді як IPv6 використовує адреси багатоканальних груп.

- IPv4 використовує 0.0.0.0 як невизначену адресу і 127.0.0.1 для адреси зворотного зв'язку (loopback). У IPv6 використовуються :: і ::1 відповідно.

- IPv4 має глобально унікальні публічні адреси та "приватні" адреси, в той час як IPv6 використовує глобально унікальні унікаст-адреси та локальні адреси (FD00::/8).

Переваги IPv6 перед IPv4:

- Ефективніша маршрутизація без фрагментації пакетів.
- Вбудована технологія Quality of Service (QoS), яка визначає чутливі до затримки пакети.
- Усунення необхідності використання NAT для розширення адресного простору з 32 до 128 біт.
- Вбудована підтримка IPsec (використання IPsec є необов'язковим).
- Автоматична конфігурація адрес для спрощення адміністрування мережі.
- Покращена структура заголовка з меншими витратами на обробку.

Після впровадження IPv6 з'явилася можливість шифрувати інтернет-трафік за допомогою стандарту шифрування IPSec, що забезпечує конфіденційність і безпеку під час комунікації. Однак для реалізації шифрування потрібне відповідне обладнання, і це є стандартною практикою як для IPv4, так і для IPv6.

Деякі фахівці висловлюють думку, що наразі користувачі, які використовують шосту версію, знаходяться в більшій небезпеці, ніж ті, які використовують четверту. Постачальники послуг можуть використовувати тунелі IPv6 для надання користувачам доступу до IPv6-контенту через IPv4. Однак зловмисники можуть скористатися цими тунелями для проведення своїх атак.

Ще однією потенційною проблемою є автоконфігурація, нова функція IPv6. Ця функція надає можливість пристроям самостійно призначати IP-адресу на основі MAC-адреси, що може стати об'єктом відстеження соціальними мережами та іншими сторонніми особами. Однак багато операційних систем вже мають розширення конфіденційності, які захищають більшість користувачів від цього виду проблем.

Головною причиною відсутності повного переходу до IPv6 є вартість оновлення обладнання. Для того щоб адаптувати всі сервери, маршрутизатори і комутатори, які традиційно використовували IPv4, необхідно вкласти значні фінансові та часові ресурси.

Крім того, для подолання дефіциту адрес постачальники надають користувачам динамічні IP-адреси, які можуть змінюватися при підключенні до інших мереж. При відключенні пристрою від мережі його IP-адреса звільняється і стає доступною для інших пристроїв. Фактично, ви отримуєте адресу в оренду, а не володієте нею. Це суттєво уповільнює перехід з IPv4 на IPv6.[8]

Протокол OSPF для динамічної маршрутизації ґрунтується на технології відстеження стану каналу і використовує алгоритм Дейкстри для пошуку оптимального маршруту. OSPF надає розширені можливості для конфігурації, і його характеристики включають:

- Відкритий характер;
- Динамічний протокол;
- Протокол із врахуванням стану каналу;
- Внутрішньо-шлюзовий протокол;
- Ієрархічна структура;
- Можливість розподілу трафіку за каналами із однаковою метрикою;
- Засоби захисту вбудовані в протокол;
- Підтримка мереж різних типів;
- Підтримка VLSM (Змінюване довжина адреси підмережі) та CIDR (Зведена адресація без втрати префіксів);
- Підтримка інкапсуляції IP;
- Робота по всіх фізичних середовищах;
- Передача лише змін у таблицях маршрутизації між маршрутизаторами, замість повного пересилання всієї таблиці;
- Ефективне використання мережевого трафіку;
- Висока масштабованість.

Розділяючись на зони, OSPF покращує продуктивність мережі, зменшуючи навантаження на центральний процесор, обмежуючи розмір таблиць маршрутизації та кількість повідомлень про стан каналу.

Розглянемо характеристики різних типів зон у протоколі OSPF:

- Магістральна зона: Це центральна частина мережі, яка об'єднує інші зони.
- Стандартна зона: Це зона, що створюється за умовчанням, і є звичайною частиною мережі.
- Тупикова зона: Ця зона приймає маршрутну інформацію тільки з інших зон. Якщо потрібно передати інформацію за межі автономної системи, вона користується маршрутом за замовчуванням.

- Totally stubby area: Схожа на тупикову зону, але взагалі не приймає маршрутну інформацію.

Метрика протоколу OSPF розраховується за стандартною формулою, яка є метрикою за умовчанням для маршрутів.:

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

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 1000Мбіт/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.[15]

Протокол кістякового дерева (STP) є мережевим протоколом, який діє на другому рівні моделі OSI та був розроблений Радьєю Перлманом для уникнення виникнення петель в комутаторах. Його принцип роботи ґрунтується на блокуванні всіх надлишкових каналів між комутаторами, логічно створюючи топологію у вигляді дерева (математичного графа).

Для досягнення цієї мети протокол використовує два типи повідомлень: BPDU, яке містить інформацію про комутатори, і TCN, що передає повідомлення про зміни у топології. Після активації протоколу STP комутатори починають відправляти повідомлення BPDU. Під час цього процесу обирається кореневий комутатор на основі інформації з BPDU-повідомлень, такої як ідентифікатор відправника, ідентифікатор кореневого маршрутизатора, ідентифікатор інтерфейсу та вартість маршруту до кореневого маршрутизатора.

Після вибору кореневого комутатора він починає відсилати BPDU-повідомлення для створення топології. Під час цього процесу інтерфейсам комутатора надаються різні стани, такі як:

- Blocking (блокування): Інтерфейс не передає жодних повідомлень і використовується для запобігання петлям.
- Listening (слухання): Інтерфейс передає лише BPDU-повідомлення під час вибору кореневого комутатора.
- Learning (навчання): Інтерфейс приймає BPDU-повідомлення, але не відправляє нічого, зберігаючи отриману інформацію про MAC-адреси комутатора.
- Forwarding (пересилання): Основний стан інтерфейсу, під час якого відбувається пересилання інформаційних пакетів.

Для моніторингу стану мережі, кореневий комутатор періодично висилає BPDU повідомлення кожні 2 секунди за промовчанням, і цей таймер відомий як Hello Timer. Інші комутатори, прийнявши ці повідомлення, пересилають їх далі. У випадку, коли комутатор не отримує це повідомлення протягом таймера Max Age

(20 секунд за замовчуванням), це розглядається як втрата зв'язку з кореневим комутатором, що спричиняє повторний вибір головного комутатора.

Коли не кореневий комутатор помічає зміни в топології, такі як включення або виключення підключення, використовуються повідомлення TCN. TCN повідомлення містять інформацію про зміни в топології, і ці повідомлення пересилаються на кореневий комутатор. Звичайні комутатори єдині, хто пересилає TCN повідомлення для спілкування з кореневим комутатором.

RSTP представляє сучасний варіант протоколу STP, який не використовує таймери і дозволяє всім комутаторам передавати BPDU повідомлення. Для моніторингу стану, використовується перевірка кількості втрачених повідомлень, і механізм Proposal/Agreement використовується для переведення інтерфейсів в робочий стан без використання таймерів. Але, у випадку підключення пристрою, що не підтримує RSTP, необхідно пройти всі етапи протоколу STP.

Також слід ознайомитися з основними допоміжними протоколами, такими як:

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

Технологія VLAN, яка представляє собою віртуальну мережу, що налаштовується на комутаторах другого рівня та також відома як широкомовний домен. Кожна VLAN отримує ідентифікатор (ID) у 12 біт, що дозволяє нумерувати їх від 0 до 4095. На портах комутаторів налаштовується значення, відповідне віртуальній мережі. Трафік, що входить через цей порт, відзначається міткою VLAN, що дозволяє йому проходити тільки через відповідні інтерфейси інших комутаторів.

Ця технологія надає можливість:

- Побудувати мережу з незалежною логічною структурою, що не залежить від фізичного розташування компонентів мережі.

- Розділити широкомовний трафік, який належить одній VLAN, від іншого, зменшуючи навантаження на мережеве обладнання.
- Групувати ПК в одній підмережі та застосовувати політики для всієї групи.
- Здійснювати маршрутизацію за допомогою віртуальних портів.

Для забезпечення відправки та прийому трафіку між різними VLAN, порт потрібно перевести в режим транка або тегування. У першому випадку роз'єм пропускає трафік всіх VLAN, в другому - працює тільки з трафіком певних VLAN.

Важливо відзначити, що різному обладнанню можуть бути необхідні різні налаштування. Деякі пристрої, наприклад, можуть вимагати, щоб стан конкретного порту був вказаний на фізичному інтерфейсі. Для іншого обладнання може бути важливим вказати, що певний роз'єм належить конкретному VLAN. Якщо, наприклад, необхідно, щоб кілька VLAN проходили через один порт, то в кожному з них потрібно вказати інтерфейс з тегом.

Маршрутизація між VLAN є типовою маршрутизацією підмереж, але з істотною відмінністю: кожній підмережі відповідає конкретна віртуальна LAN на другому рівні.

Як це працює? Наприклад, у вас є два VLAN: ID = 40 і ID = 50. На рівні 2 мережа розбивається на дві підмережі, ID яких — 40 та 50, відокремлюючи хости один від одного. Для того щоб ці хости взаємодіяли, потрібна маршрутизація трафіку обох віртуальних підмереж. Кожному VLAN слід призначити власний IP-адресу на пристрої третього рівня. Ці IP-адреси виконуватимуть функції шлюзів, необхідних для направлення трафіку між різними підмережами. Це дає можливість:

- Налаштувати безпечний доступ для клієнтів: члени однієї підмережі не матимуть можливості потрапити в іншу;
- Використовувати один VLAN для декількох фізичних портів на комутаторі. Це означає, що на комутаторі рівня 3 можна налаштувати мар-

шрутизацію без необхідності використання зовнішнього маршрутизатора. Також можна використовувати роутер, який з'єднаний із світчем другого рівня і налаштований з VLAN, для створення віртуальних інтерфейсів в необхідній кількості;

- Використовувати другий рівень у вигляді VLAN між 1 і 3 рівнями. Підмережі можна позначати як віртуальні лани, призначаючи їм певні інтерфейси. Також існує можливість налаштувати один VLAN і розмістити в ньому кілька портів на світчі.

Подібні мітки створюють для об'єднання пристроїв, підключених до різних світчів, в одну мережу. Це дозволяє групувати деякі комп'ютери в один віртуальний лан, а інші - в інший. Це призводить до того, що ПК в різних ланах працюватимуть, ніби вони підключені до одного і того ж світча. Як було зазначено раніше, обладнання в різних ланах не може взаємодіяти одне з одним. Це також відкриває можливість створення гостьової мережі.

З усього сказаного можна виділити чотири основні переваги використання віртуальних LAN:

- Можливість гнучкого групування пристроїв, включаючи комп'ютери, підключені до різних світчів, для створення ізольованих підмереж;
- 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, оскільки для створення нової віртуальної підмережі не потрібно придбати новий світч і прокласти додатковий кабель.[9]

SSH - універсальний протокол, з властивостями та заходами безпеки, які дозволяють його використовувати в різноманітних контекстах, таких як віддалений

доступ, переадресація портів, тунелювання та захищена передача файлів. Віддалений доступ через SSH дозволяє користувачам здійснювати вхід на інший комп'ютер або сервер зі своєї власної машини. Це використовується для доступу до локальних файлів цільової машини або виконання служб на ній, уникаючи фізичного присутності.

Шифрування та аутентифікаційні заходи, вбудовані в SSH, забезпечують захист підключення до іншого сервера чи комп'ютера, навіть через потенційно небезпечну проміжну мережу. Використання віддаленого доступу через SSH часто використовується для роботи з віддалених місць або для дозволу ІТ-відділу виконувати завдання без фізичного доступу до машини. Його можна використовувати для віддаленого адміністрування, управління мережевою інфраструктурою, автоматизації налаштувань, створення резервних копій та інших завдань.

SSH-1, як перша версія протоколу з ліцензією з відкритим кодом, вважається незахищеною і не рекомендується для використання. У порівнянні з цим, SSH-2 та OpenSSH фактично ідентичні в архітектурі та способах роботи, з різницею у тому, що фірмова версія має різноманітні варіанти підтримки, тоді як OpenSSH покладається на ресурси, створені громадою.

SSH-2 та OpenSSH складаються із трьох окремих протоколів, які виконують унікальні ролі у встановленні та забезпеченні зв'язку, аутентифікації клієнта та передачі даних:

- Транспортний протокол: Цей протокол встановлює зв'язок і забезпечує основну безпеку.
- Протокол аутентифікації: Цей шар використовується для аутентифікації клієнта.
- Протокол з'єднання: Цей протокол обробляє канали, через які передаються дані.

Кожен із цих протоколів виконує свою функцію в установленні та забезпеченні зв'язку, аутентифікації іншої сторони та передачі даних. Типовий порт для

з'єднання TCP - 22, а саме з'єднання встановлюється між клієнтом SSH та сервером SSH відповідно до моделі клієнт-сервер.

Процес віддаленого входу в SSH включає такі етапи, які мають основну структуру (з варіаціями в залежності від конфігурації), про яку буде надано докладніші пояснення пізніше:

- Клієнт встановлює з'єднання з сервером SSH для ініціювання взаємодії.
- Сервер надсилає клієнту свій відкритий ключ для підтвердження ідентичності.
- Обидві сторони узгоджують параметри з'єднання і потім створюють захищений канал для передачі даних.
- Користувач входить в операційну систему сервера та може віддалено керувати своїми завданнями.[12]

Telnet (TELEtype NETwork) - це мережевий протокол, призначений для забезпечення текстового інтерфейсу через мережу.

Основна мета протоколу Telnet полягає в створенні спільного, двонаправленого, восьмибітового байт-орієнтованого засобу зв'язку. Цей протокол призначений для того, щоб термінальні пристрої та термінальні процеси могли взаємодіяти один з одним. Він може використовуватися для зв'язку як між терміналами (процес "зв'язування"), так і між процесами (процес "розподілені обчислення").

Хоча сесії Telnet визначають клієнтську та серверну сторони, протокол насправді є повністю симетричним. Після встановлення транспортного з'єднання (зазвичай, через TCP) обидва кінці взаємодіють як "мережеві віртуальні термінали" (Network Virtual Terminal, NVT), обмінюючись двома видами даних:

- Прикладні дані: Це дані, які передаються від користувача до текстового додатка на стороні сервера та навпаки.
- Команди протоколу Telnet: Це включає опції та службові команди для визначення можливостей та переваг сторін.

Незважаючи на те, що Telnet-сесії по TCP володіють повним дуплексом, NVT, за замовчуванням, розглядається як напівдуплексний пристрій, що функціонує у буферизованому рядковому режимі.

Прикладні дані проходять через протокол без внесення змін. Випадкові зміни даних, такі як скидання старшого біта, можуть виникнути, якщо на вхід одного терміналу подаються дані, прийняття яких не підтверджено іншим терміналом. Іншими словами, вихід другого віртуального терміналу відображає те, що було введено на вхід першого.

З погляду протоколу, дані представляють собою просто послідовність байтів, які за замовчуванням належать набору ASCII. Однак при увімкненні опції Binary вони можуть бути будь-якими. Хоча були запропоновані розширення для ідентифікації набору символів, таких як Telnet Charset Option, на практиці вони рідко використовуються. Всі значення октетів прикладних даних, крім \ 377 (десятькове 255), передаються з транспорту як є. Октет \ 377 передається послідовністю \ 377 \ 377 з двох октетів через використання його на транспортному рівні для кодування опцій.

Протокол контролю агрегації посилянь (LACP) - це протокол для колективної обробки декількох фізичних портів, розгляду як єдиний канал для мережевого трафіку. Це відображає загальний принцип агрегації зв'язків, який полягає в створенні паралельних мережевих структур для надійності та підвищення продуктивності.

Інститут інженерів електротехніки та електроніки (IEEE) має свій стандарт LACP 802.3ad, але існують і фірмові реалізації LACP, створені компаніями, такими як Cisco. Розробка LACP відбувалася протягом 90-х років, і стандарт IEEE був випущений в 2000 році. Експерти вважають, що LACP має переваги перед деякими іншими методами резервного копіювання, такими як звичайні системи відмов.

З погляду фактичної методології, агрегація може відбуватися на рівнях два та три моделі OSI, дозволяючи пристроям спільно використовувати одну логічну IP або MAC-адресу. Здійснення агрегації посилянь може вирішити проблеми обмеже-

ної пропускної здатності в кабельних мережах. Загалом, ці системи сприяють створенню потужних та ефективних мереж, враховуючи різноманітні технології компаній.

HSRP є частиною сімейства протоколів резервування шлюзу FHRP (First Hop Redundancy Protocol). Засновані на загальному принципі FHRP, ці протоколи дозволяють кільком пристроям третього рівня (комутаторам або маршрутизаторам) використовувати одну IP-адресу як шлюз для кінцевих пристроїв.

HSRP був розроблений для уникнення відсутності шлюзу, забезпечуючи надійність за рахунок двох окремих пристроїв третього рівня. Цей протокол дозволяє утворювати групи фізичних чи віртуальних інтерфейсів, що належать різним пристроям, і надавати їм спільні MAC-адреси та IP-адреси (віртуальні). Тільки один інтерфейс з найвищим пріоритетом буде активним, а інший - у стані резерву, забезпечуючи надійність шлюзу. Якщо в групі HSRP є більше двох інтерфейсів, інші будуть у стані прослуховування, оскільки їх пріоритети менші.

Пріоритет маршрутизатора може приймати значення від 1 до 255, і за замовчуванням встановлено значення 100. Чим вище значення пріоритету, тим вищий пріоритет маршрутизатора для стану активного. У випадку однакового значення пріоритету для різних інтерфейсів, визначається той інтерфейс, у якого IP-адреса має більше значення.

Маршрутизація IP-пакетів виконується тільки через активний інтерфейс третього рівня. Активний інтерфейс, на запит протоколу ARP, який містить віртуальну IP-адресу відповідної групи HSRP, відправляє ARP-відповідь, що містить віртуальну MAC-адресу цієї групи, і призводить до наступного відправлення кадрів Ethernet на активний інтерфейс.

Активний та резервний інтерфейси періодично висилають повідомлення Hello на широкомовну IP-адресу 224.0.0.102 і порт UDP 1985 з інтервалом часу 3 секунди (за замовчуванням). Якщо резервний інтерфейс не отримує повідомлення Hello протягом 10 секунд (за замовчуванням), він вважається недоступним, і відбу-

вається перехід інтерфейсу з резервного в активний стан. У цей момент інші інтерфейси HSRP групи переходять у стан розмови Speak, розсилаючи періодичні повідомлення Hello та беручи участь у виборах резервного інтерфейсу, з орієнтацією на пріоритет після активного інтерфейсу. Перехід інтерфейсу в стан резервного Standby можливий лише зі стану розмови Speak після проведення виборів.

Протокол HSRP впроваджує функцію пріоритетного переривання обслуговування, що дозволяє негайно активувати інтерфейс з найвищим пріоритетом. Пріоритет визначається спочатку встановленим користувачем значенням, а потім за IP-адресою. У обох випадках вище значення вказаного параметру вказує на вищий пріоритет. Під час пріоритетного переривання обслуговування інтерфейс з вищим пріоритетом висилає повідомлення Coor. Якщо активний інтерфейс з меншим пріоритетом отримує Coor від інтерфейсу з вищим пріоритетом, він переходить у стан розмови Speak, де відбуваються вибори активного та резервного інтерфейсів за пріоритетом.

Функція затримки пріоритетного переривання обслуговування протоколу HSRP дозволяє встановити затримку перед перериванням на певний в налаштуваннях час. Це надає пристрою третього рівня можливість оновити таблицю маршрутизації перед переходом у стан активного. Час затримки починає відраховуватися 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).

Отже, номер HSRP групи може знаходитися в межах від 0 до 4095, хоча більшість пристроїв не можуть підтримувати більше 16 груп HSRP.

Кожен інтерфейс третього рівня може одночасно бути частиною кількох груп HSRP. Таким чином, коли цей інтерфейс є активним в одній групі, в інших групах він може знаходитися або в стані резерву (Standby), або в режимі прослуховування (Listen).

Використання одного і того ж інтерфейсу третього рівня в різних групах HSRP дозволяє реалізувати балансування навантаження між маршрутизаторами, розподіляючи різні IP-адреси шлюзів на кінцевих пристроях. У цьому випадку активні інтерфейси з різних груп здійснюватимуть маршрутизацію IP-пакетів, навіпаки до використання однієї HSRP групи, де тільки один активний інтерфейс може використовуватися для маршрутизації.

Розглянемо структуру пакета протоколу HSRP (рисунок 1.13).

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 1.11 – 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 опції для поля Op Code включають:

- Повідомлення Hello, яке відсилається періодично, підтверджуючи, що інтерфейс працює і може стати активним або резервним.
- Повідомлення Coup, яке інтерфейс з найвищим пріоритетом відсилає, коли він бажає стати активним, реалізуючи функцію пріоритетного переривання обслуговування.
- Повідомлення Resign, яке відсилається, коли інтерфейс вже не бажає залишатися активним.

Поле State (1 байт) вказує на поточний стан інтерфейсу, і коди станів можуть відрізнитися для різних версій протоколу HSRP.

Hellotime (1 байт) представляє періодичність відсилення повідомлень Hello у секундах (за замовчуванням - 3 с).

Holdtime (1 байт) визначає час утримання, тобто тривалість коректності поточного Hello (за замовчуванням - 10 с).

Priority (1 байт) вказує пріоритет інтерфейсу для визначення активного та резервного інтерфейсів. У випадку рівних пріоритетів активним визначається інтерфейс з вищою значенням пріоритету, а при рівних пріоритетах - інтерфейс з більшою IP-адресою.

Group (1 байт) представляє номер HSRP групи.

Reserved (1 байт) - зарезервовано для майбутнього використання і наразі не використовується в поточній версії протоколу HSRP.

Authentication Data (8 байтів) містить дані аутентифікації, такі як пароль. 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 налаштування 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

Продовження таблиці 1.4

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

У цьому розділі ми здійснили аналіз теоретичної інформації, що стосується засад і правил конструювання мереж. Докладно розглянуті різноманітні протоколи та технології, які застосовуються при розробці мережних структур. Під час огляду були визначені як переваги, так і недоліки використання цих протоколів та технологій.

РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ МІСЬКОГО ІНТЕРНЕТ-ПРОВАЙДЕРА

2.1 Проектування мережної інфраструктури міського інтернет-провайдера

Проектування мережної інфраструктури міського інтернет-провайдера є складним завданням, яке вимагає уважного розгляду різних аспектів, таких як пропускна здатність, масштабованість, безпека і ефективність. Розглянемо важливі аспекти враховувати при проектуванні мережі міського інтернет-провайдера.

Все починається з аналізу вимог які включають в себе визначення масштабів мережі та потреб у пропускній здатності та врахування попиту на різні послуги, такі як широкосмуговий доступ до Інтернету, IP-телефонія, віртуальні приватні мережі (VPN) і т. д.

Вибір відповідної топології мережі, такої як зірка, кільце або комбінована. Розгляд мережі забезпечення доступу, мережі передачі та мережі ядра. Вибір технологій передачі даних, таких як Ethernet, оптичні волокна, бездротові технології і т. д. Врахування маршрутизації, комутації, безпеки, управління трафіком і інших технічних параметрів.

Розгляд заходів забезпечення безпеки, виявлення вторгнень, шифрування даних, шафики для захисту обладнання поза офісом і т. д. Захист мережі від зовнішніх загроз і внутрішніх атак.

Врахування можливості розширення мережі для відповіді на зростаючий попит. Забезпечення достатньої гнучкості для впровадження нових технологій і сервісів. Врахування планів забезпечення бекапів і відновлення в разі аварій. Розгляд систем управління для моніторингу та управління мережею.

Визначення стратегій управління трафіком для забезпечення якості обслуговування важливих послуг. Встановлення механізмів пріоритетів для різних видів трафіку.

Дотримання відповідних стандартів та регуляцій, які стосуються мережі міського інтернет-провайдера.

Проектування мережі міського інтернет-провайдера вимагає комплексного підходу, а також підтримки відгуків від користувачів і актуалізації відповідно до змін у технологічному середовищі та вимогах користувачів.

2.2 Розробка фізичної та логічної топології мережі

Проектування мережної інфраструктури передбачає формування фізичної та логічної її топології. Традиційно для проектування застосовується рівневий підхід на основі однієї з загальноприйнятих моделей. Основною моделлю при проектуванні сучасних мереж є трирівнева ієрархічна модель, розроблена компанією Cisco. Ця модель передбачає формування трьох мережі, а саме рівня ядра, рівня розподілу, рівня доступу.

Рівень ядра – це центральна частина мережі, що відповідає за розподіл інтернет-трафіку між різними мережами. Ядро складається переважно з маршрутизаторів, які взаємодіють між собою за допомогою Gigabit Ethernet. При проектуванні також передбачається можливість розширення мережі.

Рівень розподілу – рівень, на якому виконується функція з'єднання ядра і кінцевих мереж з рівня доступу. Для його створення використовуються маршрутизатори та комутатори, які взаємодіють між собою за допомогою Gigabit Ethernet.

Рівень доступу – це кінцеве обладнання користувачів мережі та комутаційне обладнання.

Бвають випадки, коли через розмір мережі виділяти три рівні недоцільно, тоді проводиться об'єднання певних рівнів, як правило рівня ядра і рівня доступу. Таке поєднання рівнів отримало назву згорнуте ядро. Варто зазначити, що у випадках дуже малих мереж, наприклад локальної мережі на основі одного комутатора, або домашнього маршрутизатора з інтеграцією послуг, застосування моделі Cisco недоцільне.

Проектування мережі міського інтернет—провайдера через її великий розмір буде ефективним при застосуванні моделі Cisco саме з використанням трьох рівнів.

Давайте розглянемо фізичну топологію мережі.

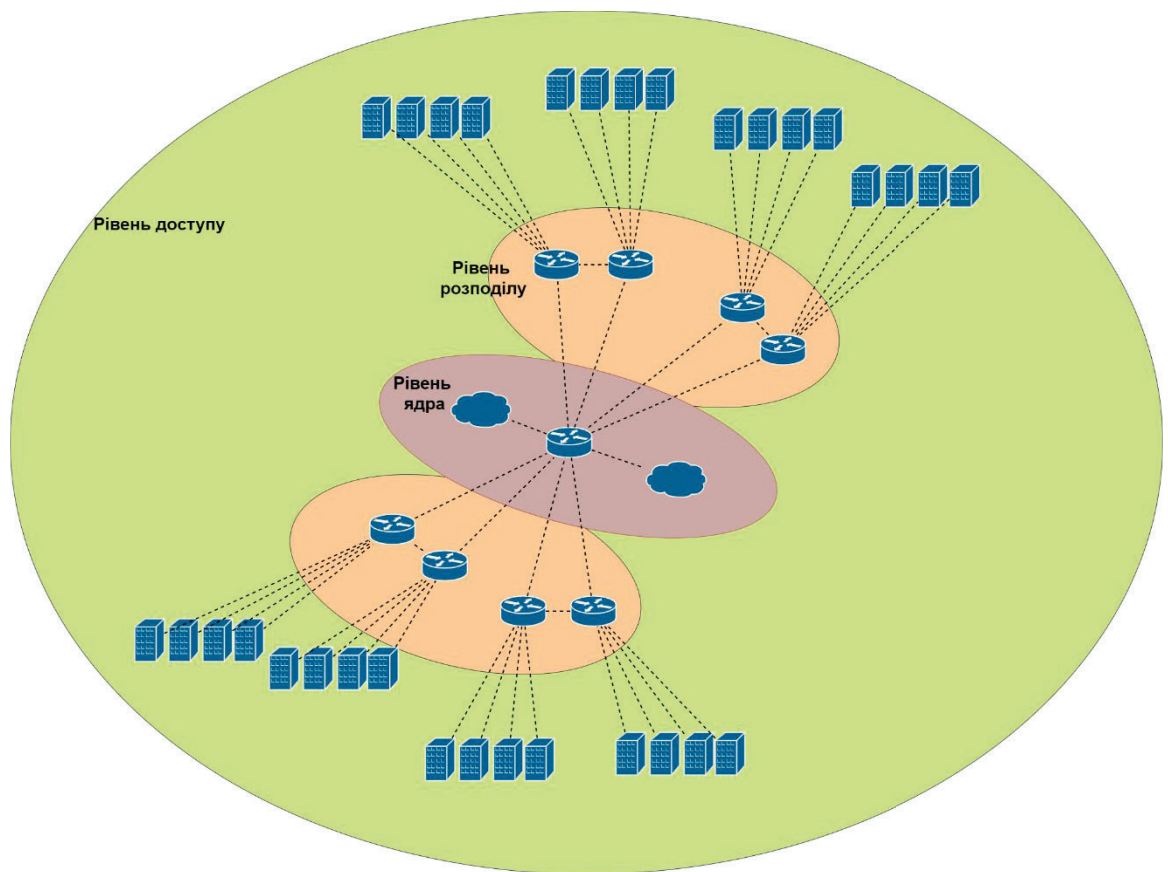


Рисунок 2.1 – Топологія мережі

Між користувачами та рівнем розподілу встановлено комутаційне обладнання з можливістю розширення. Для забезпечення високої швидкості передачі інформації між рівнями доступу та розподілу використовується з'єднання Gigabit Ethernet. Кінцеві вузли в рівні доступу підключені до комутатора за допомогою ліній Fast Ethernet або Gigabit Ethernet, залежно від обраного тарифного плану користувача.

У цьому прикладі мережі використовується 9 маршрутизаторів та мінімум 48 комутаторів. Кількість підмереж складає 35, включаючи мережі між маршрутизаторами.

Враховуючи місцеві особливості, розумно використовувати різні типи топологій.

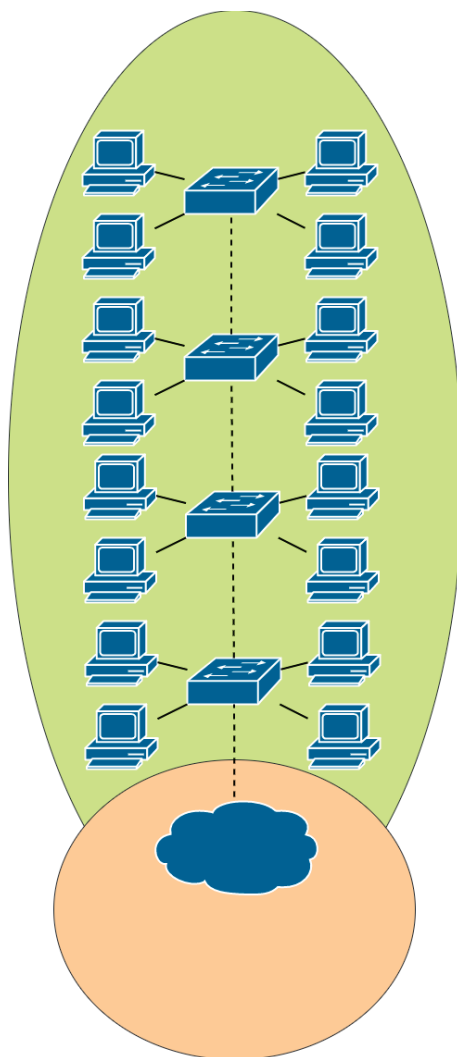


Рисунок 2.2 – Послідовне з'єднання

Побудова рівня доступу за подібною схемою є доцільною і володіє такими перевагами, як легкість встановлення, налаштування та обслуговування. Однак у випадку виникнення проблем часткова або повна відмова може призвести до втрати доступу до Інтернету в певній частині або взагалі в усій топології.

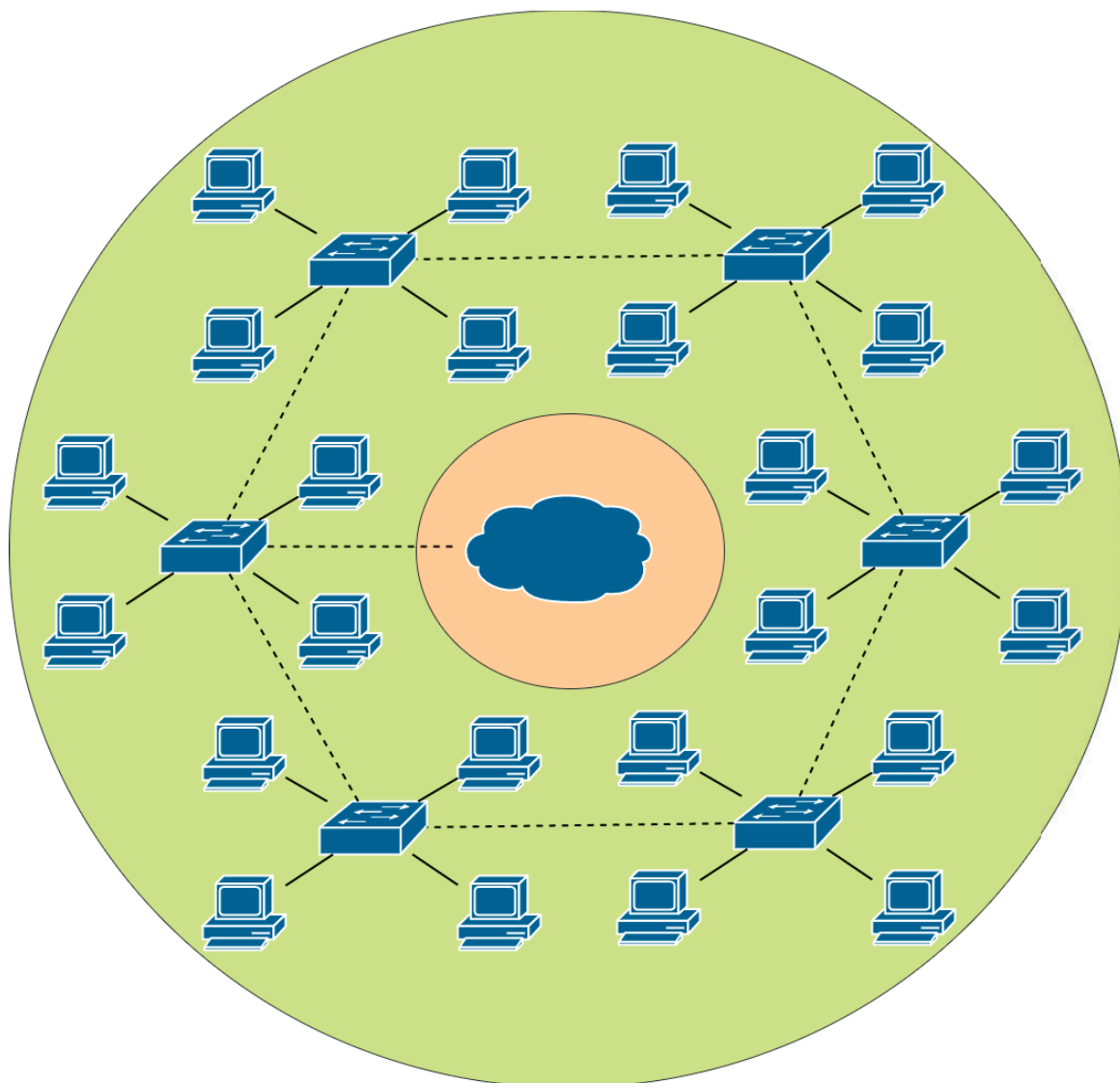


Рисунок 2.3 – Кільцеве з'єднання

Структура рівня доступу у формі кільця є більш надійною, ніж послідовна, і також володіє перевагами у вигляді легкості встановлення та обслуговування.

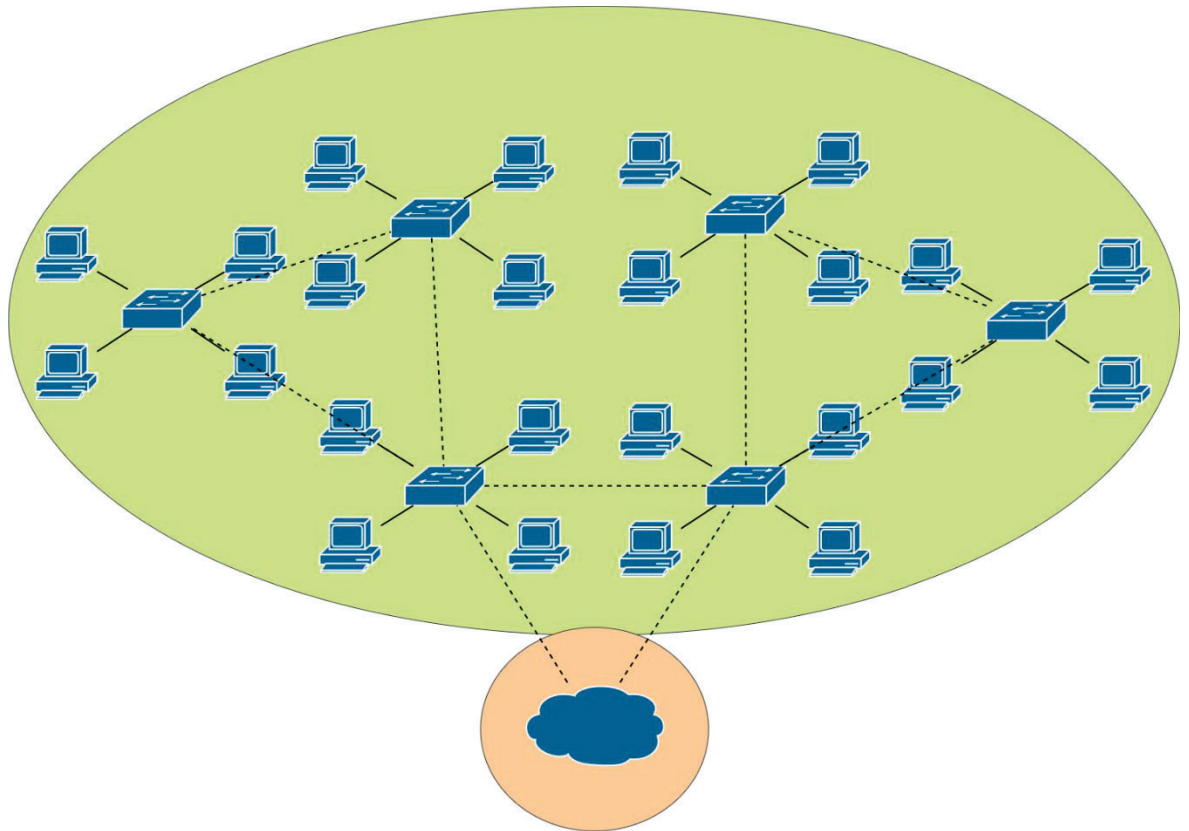


Рисунок 2.4 – Дерево подібне з'єднання

Підключення у формі деревоподібної структури відзначається високою надійністю серед своїх переваг. Проте, в разі вибору цієї переваги, ускладнюється процес встановлення та обслуговування обладнання порівняно з послідовним та кільцевим з'єднанням.

Взаємодія між маршрутизаторами та OLT буде здійснюватись за допомогою дво-точкових мережних з'єднань.

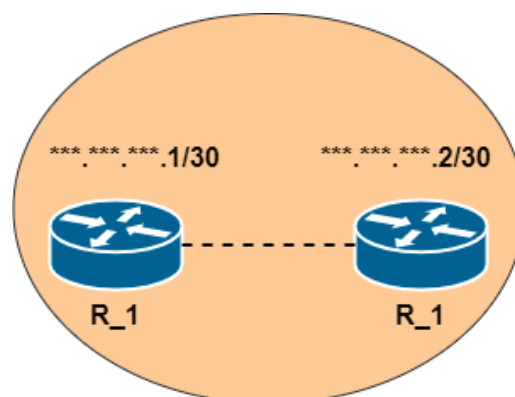


Рисунок 2.5 – Дво-точкове з'єднання

Комутаційне обладнання буде налаштовано для роботи з двома відмінними мережами за допомогою протоколу VLAN.

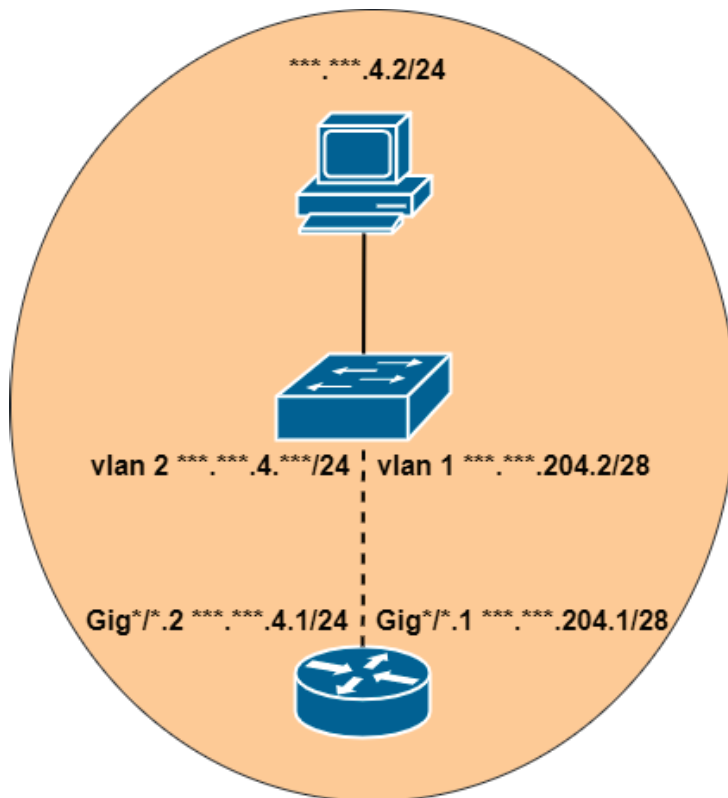


Рисунок 2.6 – Розподіл мереж

Це налаштування забезпечить нам більш високий рівень безпеки, оскільки відокремить користувачів від комутаційного обладнання і, при правильному використанні, спростить масштабування мережі.

У більшості випадків логічна топологія буде використовувати логічну шину та комутовану структуру. Ця логічна топологія базується на вищезазначених фізичних топологіях і може відрізнятися в залежності від зручності використання.

2.3 Проектування схеми адресації

Почнемо з призначення адрес для мереж. Процес розподілу підключень між маршрутизаторами та OLT подано 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

Наступним етапом є розподіл адрес для користувачів і комутаторів. Розділення мережі для комутаторів і користувачів сприятиме підвищенню безпеки. Проте важливо зауважити, що для областей, де використовується технологія передачі PON, немає потреби в додатковій технічній підмережі.

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

Продовження таблиці 2.2

D5_M	200.204.5.0	255.255.255.240	/28
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 рекомендується розподілити адреси для маршрутизаторів рівня ядра і розподілу, щоб спростити впровадження проекту (див. Додаток Ж).

Комутаційне обладнання отримає статичні адреси для VLAN, що відповідають за доступ до цього обладнання і дозволяють віддалений контроль. Користувачі отримають свої адреси динамічно за допомогою протоколу DHCP.

2.4 Проектування допоміжної сервісної інфраструктури та підсистеми захисту мережі

Для ефективної роботи мережі важливо створити допоміжну інфраструктуру, яка відповідатиме за різноманітні допоміжні функції, такі як DHCP, система аутентифікації, авторизації та обліку (AAA). У даному проекті допоміжною інфраструктурою буде лише аутентифікаційна система AAA, реалізована за допомогою RADIUS-сервера.

Допоміжна сервісна інфраструктура, як описано вище, буде прямо підключена до ядра мережі та забезпечувати доступ до Інтернету для пристроїв в офісі.

До підсистем захисту слід віднести налаштування інтерфейсів рівня доступу на маршрутизаторах, яке забезпечить відокремлення користувачів від адресного простору комутаторів. Також важливим є налаштування віддаленого доступу до пристроїв за допомогою RADIUS-сервера та обмеження доступу до пристроїв мережі офісу.

Далі необхідно налаштувати комутатори для захисту від таких атак, як MAC-Flooding, MAC-Spoofing, атаки на протоколи STP/PVST+, ARP, DHCP. Ці налаштування гарантують безпеку мережі від найпоширеніших методів атак на неї.

У цьому розділі були розглянуті особливості та етапи проектування мережі, розроблена фізична та логічна топологія мережі, а також розроблена система адресації з урахуванням можливостей забезпечення захисту. Також розглянута створена допоміжна інфраструктура та визначені необхідні підсистеми захисту.

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

3.1 Вибір обладнання та програмного забезпечення для проекту мережної інфраструктури

Вибір обладнання слід розпочати з аналізу широкого спектру пропозицій від провідних світових виробників, таких як Cisco Systems, Juniper Networks, Huawei Technologies, D-Link Systems, Inc., Mikrotiks Ltd. (MikroTik), Shanghai Baud Data Communication Co., Ltd. (BDCOM).

Компанія Cisco, яка є світовим лідером у сфері мережевих технологій, пропонує рішення в п'яти ключових технологічних напрямках:

- 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 найвищу якість послуг у своєму сегменті ринку. Їхні продукти успішно продаються як серед кінцевих споживачів, так і великих корпорацій у практично всіх країнах світу.[14]

Juniper Networks виступає як один із лідерів у виробництві телекомунікаційного обладнання, спеціалізуючись у розробці високопродуктивних та високоякісних маршрутизаторів, комутаторів, міжмережевих екранів і магістрального обладнання, яке може служити ядром для дата-центрів.

Компанія також надає цілодобову технічну підтримку та сервісне обслуговування своїх пристроїв, маючи серед своїх клієнтів 130 провідних міжнародних постачальників мережевих послуг.

Основними сферами використання обладнання компанії є провайдери послуг зв'язку, центри обробки даних, фінансові корпорації та державний сектор. Мережеве обладнання Juniper Networks спирається на принципи безпеки, надійності, масштабованості і відкритості.

Рішення Juniper здійснюють управління власною операційною системою, що базується на FreeBSD і використовує розроблені компанією процесори. Компанія також випустила власну революційну IP-платформу, що дозволяє користувачам використовувати різноманітні сервіси з можливістю масштабування.[20]

Huawei Technologies, як глобальний лідер у сфері розробки рішень для мереж наступного покоління, визначається своїм прагненням забезпечити клієнтам максимальний прибуток та потенціал розвитку. Компанія надає нові індивідуально розроблені рішення, спрямовані на задоволення унікальних потреб клієнтів.

Huawei Technologies також є світовим лідером у сфері постачання телекомунікаційних мереж нового покоління, обслуговуючи наразі 45 з 50 провідних світових операторів і налічуючи понад мільярд користувачів по всьому світу.[21]

D-Link є відомим у всьому світі розробником та виробником мережевого та телекомунікаційного обладнання, пропонуючи різноманітні рішення для домашніх користувачів, корпоративного сектора та постачальників послуг Інтернету.

Компанія D-Link надає комплексні мережеві та комунікаційні рішення для створення "цифрового дому", задовольняє потреби підприємств малого та середнього бізнесу, вирішує завдання масштабування робочих груп та корпорацій, а також обслуговує провайдерів послуг Інтернету.

Інноваційні підходи та високі стандарти якості дозволяють компанії виготовляти високопродуктивні пристрої, що відповідають сучасним стандартам.[22]

MikroTik є великим латвійським виробником мережевого обладнання. Головною перевагою продукції MikroTik є використання власної операційної системи MikroTik RouterOS, розробленої самою компанією. Ця система надає нові можливості та потужний функціонал обладнанню. Практично всі маршрутизатори та то-

чки доступу MikroTik підтримують технологію живлення через Ethernet (POE). Порівняно з конкурентами, ціни на продукцію MikroTik значно більш доступні, а функціонал їхнього обладнання не поступається дорогим конкурентам. [42]

Shanghai Baud Data Communication Co., Ltd. (BDCOM) – це компанія, яка спеціалізується на розробці, виробництві, впровадженні та обслуговуванні мережевого обладнання. Вона виступає постачальником ефективних рішень для створення комунікаційних мереж.[23]

Основними клієнтами постачальники зв'язку, великі підприємства та установи державного сектору. При виборі обладнання важливо враховувати необхідні параметри та завдання, які має бути виконано. Це включає достатню кількість портів, підтримку необхідних технологій та протоколів, необхідних для побудови мережі.

Для кращої наглядності для проектування мережі було обрано обладнання що наявне на ринку.

На рівні ядра необхідно мати маршрутизатор, який підтримує використання протоколу OSPF та може використовувати технологію 10 GigabitEthernet. Маршрутизатор Cisco ISR4461/K9 [25] (Рисунок 3.1) володіє необхідними параметрами для ефективної роботи в таких умовах.



Рисунок 3.1 – Маршрутизатор Cisco ISR4461/K9

Цей конкретний маршрутизатор представляє собою один з маршрутизаторів серії ISR4000, які використовуються в провайдерських мережах. Він має можливість збільшення кількості портів шляхом встановлення модулів.

Також для вирішення схожих завдань може бути використаний маршрутизатор Juniper CHAS-BP-MX240-S[27] (Рисунок 3.2), який також є маршрутизатором провайдерського класу і має можливість розширення кількості інтерфейсів.



Рисунок 3.2 – Маршрутизатор Juniper CHAS-BP-MX240-S

В якості маршрутизатора для рівня розподілу можна вибрати менш складний варіант. Один із таких прикладів — Cisco ISR4321-AX/K9[26] (Рисунок 3.3). Ця модель має достатню потужність, щоб виконувати роль ядра в корпоративних мережах та виступати як граничний маршрутизатор у провайдерських компаніях.



Рисунок 3.3 – Маршрутизатор Cisco ISR4321-AX/K9

Для вирішення аналогічних завдань можна взяти у розгляд маршрутизатор Juniper J2320-JB-SC-TAA[28] (Рисунок 3.4), що є також маршрутизатором провайдерського класу.



Рисунок 3.4 – Маршрутизатор Juniper J2320-JB-SC-TAA

Для рівня доступу рекомендовано використовувати комутатор із значною кількістю портів технології FastEthernet чи GigabitEthernet та кількома портами технології GigabitEthernet чи 10 GE відповідно для підключення до маршрутизатора або для з'єднання з іншим комутатором. Для цього можна використати, наприклад, комутатор Cisco WS-C2960X-24TS-LL[24] (Рисунок 3.5).



Рисунок 3.5 – Комутатор Cisco WS-C2960X-24TS-LL

Цей комутатор обладнаний 24 портами технології GigabitEthernet, 2 SFP порти, які підтримують встановлення модулів технології 10 GigabitEthernet, та можливістю додатково встановити два порти технології GigabitEthernet, що в повній мірі відповідає вказаним вимогам. Альтернативним варіантом є Juniper EX2200-24T-4G (Рисунок 3.6).



Рисунок 3.6 – Комутатор Juniper EX2200-24T-4G

Характеристики даної моделі подібні. Однак слід відзначити, що створення мережі з використанням обладнання різних виробників може впливати на ефективності та викликати затримки. Але з правильним розподілом обладнання можна ефективно його поєднувати.

Також важливо розглянути обладнання для технології PON. Розглянемо приклад обладнання від компанії BDCOM. Спочатку оцінимо технологію GEPON на

прикладі BDCOM P3600-08E[30] (Рисунок 3.7). Цей пристрій відповідає стандартам IEEE 802.3ah, YD/T 1475-2006 та CTC2.1/3.0. Він підтримує автоматичне виявлення і взаємодію з абонентськими терміналами (ONU) різних виробників.



Рисунок 3.7 – Оптичний лінійний термінал BDCOM P3600-08E

P3600-08E забезпечує симетричну передачу даних зі швидкістю 1,25 Гбіт/с у вниз та вгору, а також ефективне управління пропускнуою здатністю. Максимальний коефіцієнт розділення складає 1:64.

Технологію GPON можна розглянути за прикладом BDCOM GP3600-16B [29] (Рисунок 3.8), який відповідає стандартам ITU-T G.984 / G.988. Повністю сумісний зі стандартом CTC2.0, цей пристрій забезпечує автоматичну синхронізацію та підключення абонентських терміналів від різних виробників.

BDCOM GP3600-16B підтримує асиметричний потік даних uplink 1,25 Гбіт/с та downlink 2,5 Гбіт/с для передачі даних у пасивних оптичних мережах. Завдяки ефективному використанню пропускнуої здатності, цей продукт надає можливість надавати високоякісні послуги.



Рисунок 3.8 – Оптичний лінійний термінал BDCOM GP3600-16B

Це обладнання дозволяє використовувати розподіл до 128 абонентів на одну гілку, що дозволяє зменшити фінансові витрати при розгортанні мережі.

Основна мережа буде розроблена за допомогою програми Cisco Packet Tracer. Це дозволить навчитися конфігуруванню обладнання, але з обмеженою кількістю доступного обладнання. Маршрутизатори моделі 4331 та універсальний RT-Empty, а також комутатори моделі 2960 та універсальний RT-Empty будуть використовуватись як аналоги вже обраного обладнання. Важливо відзначити, що обладнання з позначенням RT-Empty є віртуальним, а не реальним, і використовується для імітації вибраних моделей.

Для впровадження систем захисту буде використано набір програм, головною з яких є GNS3, що здатна емулювати реальне обладнання. Однак ця програма обмежена у доступних пристроях, оскільки потребує образів реального обладнання. Для її роботи необхідно також використовувати віртуальну машину, де будуть встановлюватись образи обладнання; для цього використовується програма VMware Workstation. Оскільки ми будемо реалізовувати системи захисту, нам доведеться перевірити їх ефективність, для чого буде використано Oracle VM VirtualBox, де буде встановлено образ Kali Linux. Ця операційна система спеціально створена для проведення атак на мережеві пристрої і має всі необхідні програмні засоби для цього.

3.2 Базове налагодження мережних пристроїв

Базова конфігурація пристроїв означає налаштування основних протоколів та технологій обладнання для забезпечення передачі інформації у мережі. Перший крок у цьому процесі - налаштування адрес інтерфейсів маршрутизаторів. Для ілюстрації цього підходу розглянемо маршрутизатор 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 можна помітити з конфігурації, інтерфейс, який веде до рівня доступу, розділений на два підінтерфейси для забезпечення відокремлення мережі користувачів від мережі доступу до комутаційного обладнання. Далі буде проведена конфігурація протоколу 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
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

```

Конфігурація протоколу маршрутизації дозволить пересилати пакети між підмережами різних маршрутизаторів.

Конфігурація адрес комутаторів рівня доступу:

```

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
```

Було виконано розділення інтерфейсів на комутаторах для різних VLAN. Після завершення основної конфігурації обладнання ми перейдемо до налаштування додаткових протоколів та технологій.

Маршрутизатори рівня розподілу будуть сконфігуровані 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
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.

3.3 Налаштування засобів підсистеми захисту мережі

У цьому розділі ми продовжимо конфігурування обладнання мережі. Додамо обмежувальні правила для віддаленого доступу, використовуючи списки доступу, які обмежать з'єднання до обладнання лише з однієї мережі офісу. Налаштування для маршрутизаторів буде виглядати наступним чином:

```
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
```

Це налаштування виключить можливість доступу до маршрутизатора та комутаторів з зовнішньої мережі. Однак для забезпечення вищої надійності, схожі параметри також слід налаштувати на комутаторах.

```
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 розроблення системи захисту, ми повинні створити проект у програмному забезпеченні GNS 3. Це необхідно, оскільки для перевірки ефективності захисту потрібно виконувати атаки на це обладнання. Для коректної роботи програми також необхідно використовувати VMware Workstation для запуску віртуальної машини GNS 3 та Oracle VM VirtualBox для використання віртуальної машини Kali Linux для проведення атак на пристрої.

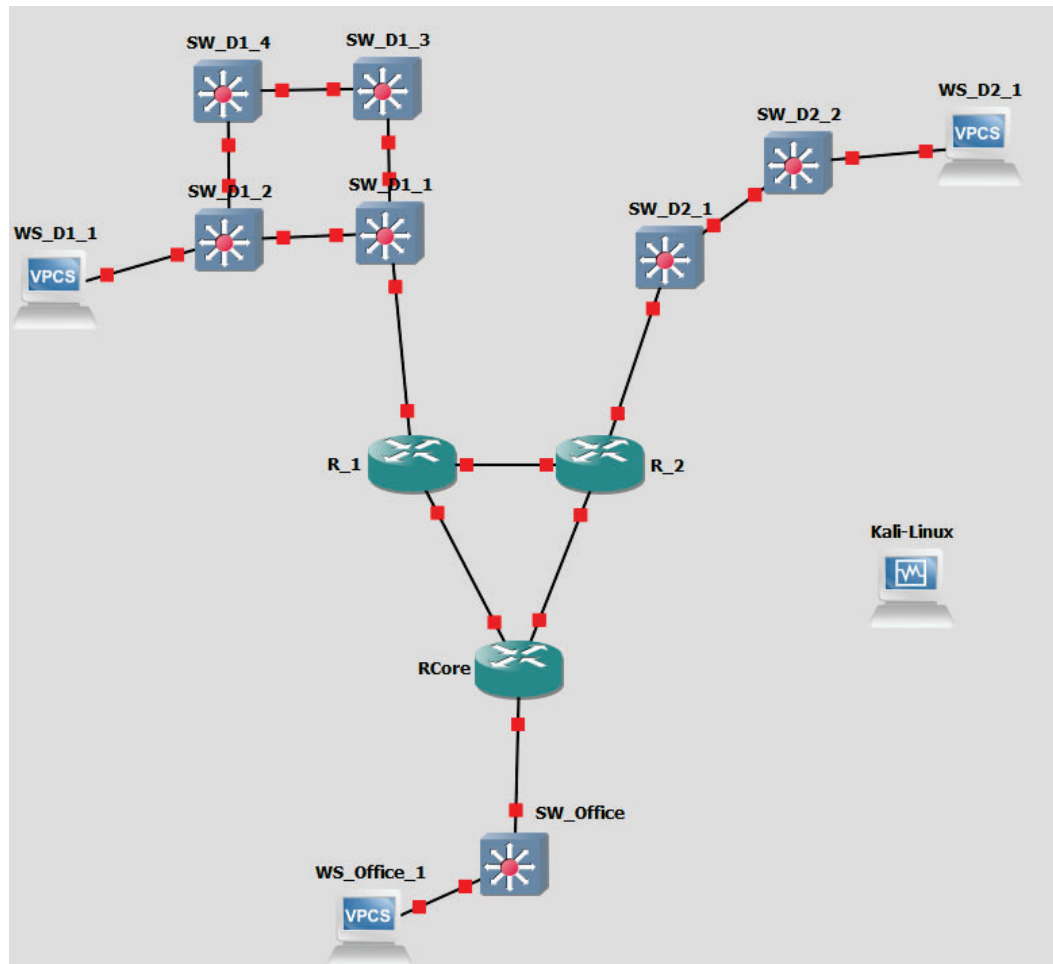


Рисунок 3.9 – Схема для налагодження захисту

Налаштування захисту відіграє важливу роль, оскільки від нього залежить надійність роботи мережі у конкретних ситуаціях.

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
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
```

Це налаштування в обох випадках активує та встановлює інтервал відновлення. У першому варіанті на випадок порушення виконується вимкнення інтерфейсу, а мак-адреса інтерфейсу залишається непридатною протягом певного часу. У другому варіанті відгуком на порушення буде обмеження, а мак-адреса залишиться статичною. Важливо відзначити, що бажано використовувати статичну адресу та вимкнення інтерфейсу, хоча це може викликати проблеми при зміні пристрою користувача.

Наступним етапом є розгляд захисту від атак на протоколи STP/PVST+. Приклад конфігурації буде розглянуто на декількох пристроях для більшої ілюстративності:

```
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
```

На першому комутаторі встановлено конфігурацію так, щоб він виконував роль кореневого комутатора. Це зроблено для уникнення можливості зміни кореневого пристрою, і також налаштовано 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
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 представлені команди, які відповідають за виведення повідомлень про помилки, налаштування часу відновлення роботи порту і активацію/деактивацію захисту портів. При цьому порти між комутаторами не мають налаштувань захисту, тоді як порти для користувачів мають активний захист.

Також проведено захист від атак на протокол ARP, налаштований за допомогою функції DAI, і подано приклади налаштування в разі використання 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
```

Ця конфігурація здійснюється на інтерфейсі, який направлений до маршрутизатора. Тепер розглянемо 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
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 у проекті мережі користувачі отримують адресу за допомогою DHCP, нам слід використовувати перший варіант налаштування.

В даному проекті використовується DHCP, тому ми також повинні захистити цей протокол від атак. Для забезпечення безпеки існують два методи, перший з яких використовує мак-адреси 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 такому підході потрібно буде виконати це налаштування для кожного підключеного пристрою. Тим не менше, важливо зауважити, що такі налаштування дозволяють видавати одну і ту саму адресу пристрою, що може бути корисним для розташування сервера чи подібного обладнання. Для роботи з динамічними адресами використовується функція DHCP-Snooping, і заходи забезпечення будуть налаштовані на комутаторі.

```
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
```

Це конфігурування набагато більш просте і виконується на комутаторі, що сприяє зменшенню навантаження на маршрутизатор або сервер. Захист встановлює обмеження на кількість пакетів запиту для протоколу DHCP.

3.4 Тестування складових елементів мережної інфраструктури та підсистеми захисту мережі

Під час конфігурації адрес пристроїв важливо відслідковувати зв'язок між ними.

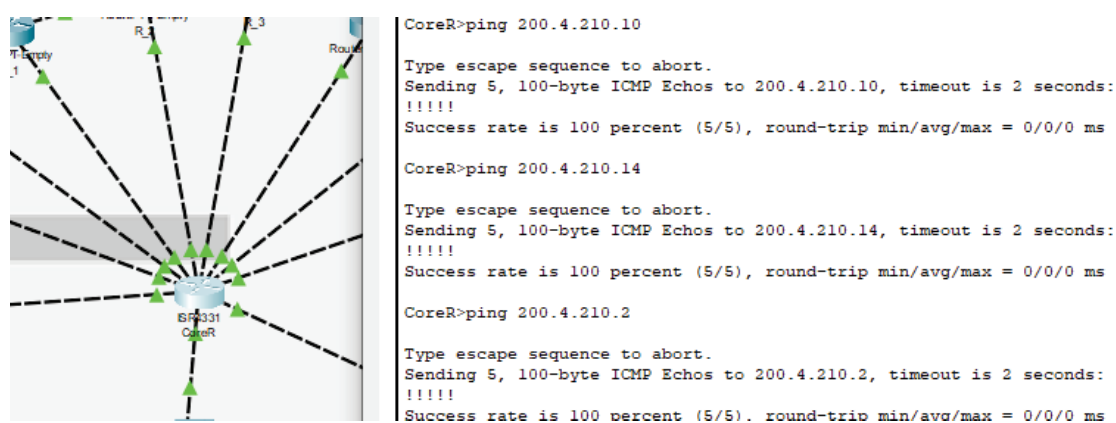


Рисунок 3.10 – Перевірка зв'язку між маршрутизаторами

Перевірка ефективності маршрутизації можлива лише у випадку, коли користувачам було надано відкритий IP-адресу.

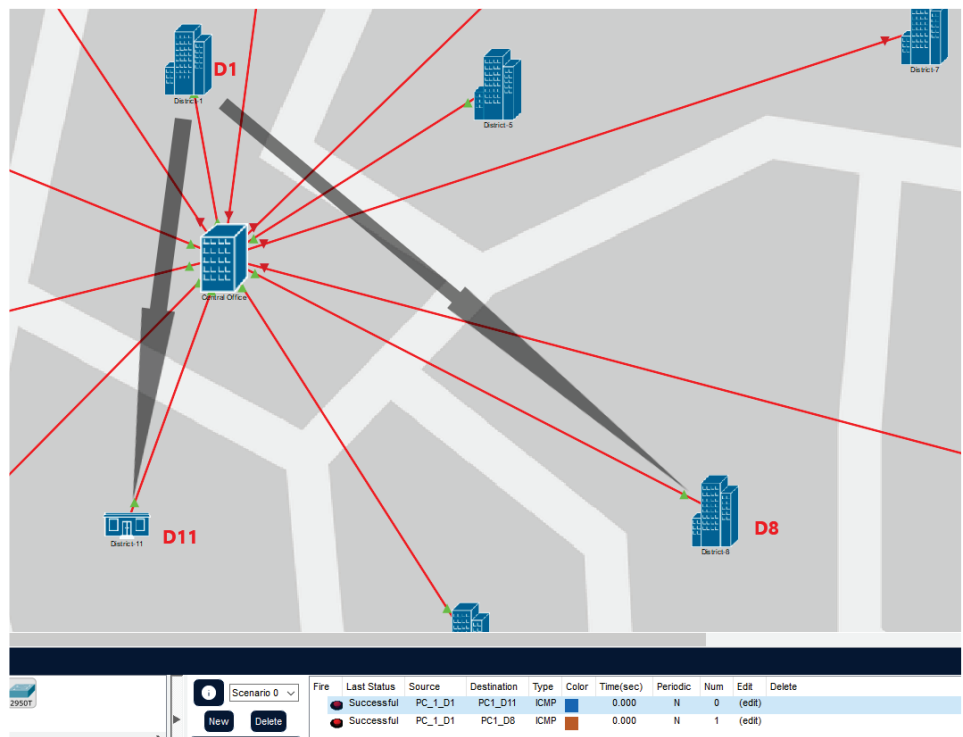


Рисунок 3.11 – Перевірка роботи маршрутизації

Тепер необхідно перевірити можливість віддаленого управління.

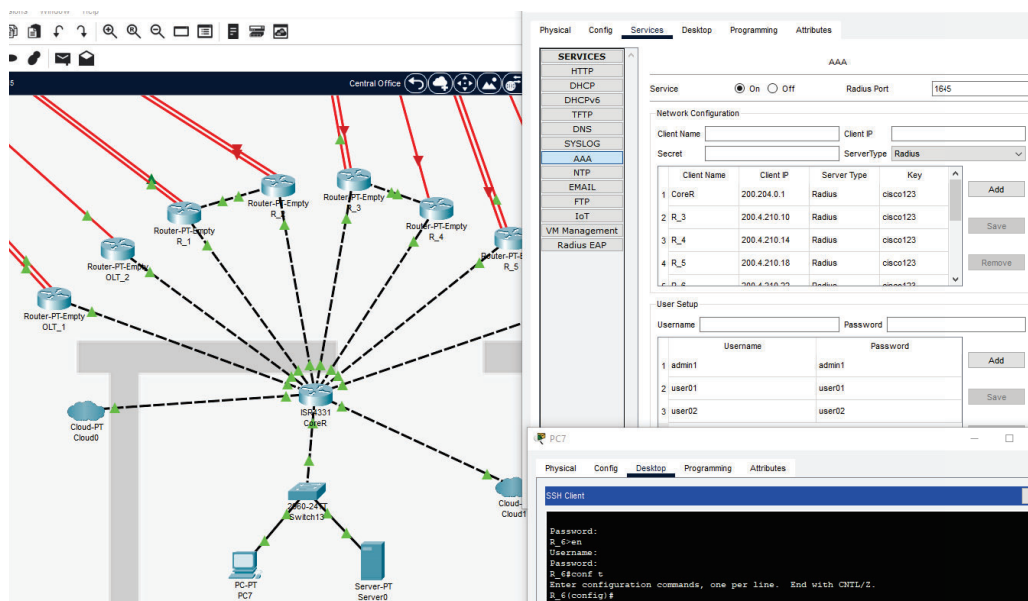


Рисунок 3.12 – Перевірка роботи віддаленого доступу

Наступним етапом буде проведено тестування підсистем захисту, починаючи з обмеження доступу до віддаленого управління.

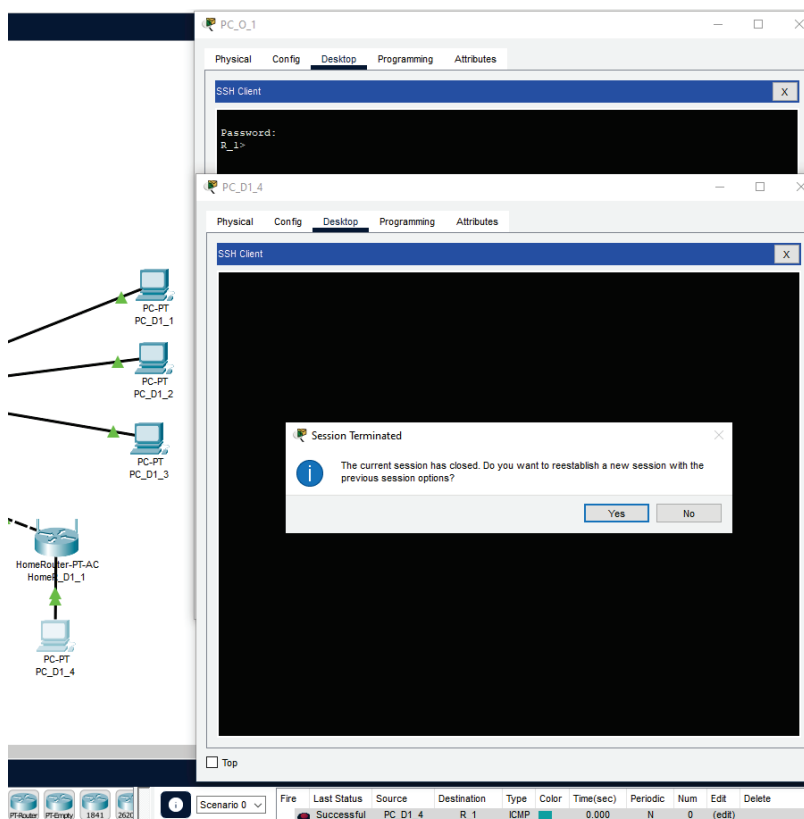


Рисунок 3.13 – Перевірка обмеження доступу

Як видно на рис. 3.13, комп'ютер, розташований в офісі, успішно встановив підключення до маршрутизатора. Однак комп'ютер користувача, хоч і має зв'язок з маршрутизатором, не може підключитися до віддаленого доступу.

Тепер проведемо перевірку захисту від атак MAC-Flooding та MAC-Spoofing, розпочавши з перевірки, чи мережа передає пакети даних після відповідного налаштування.

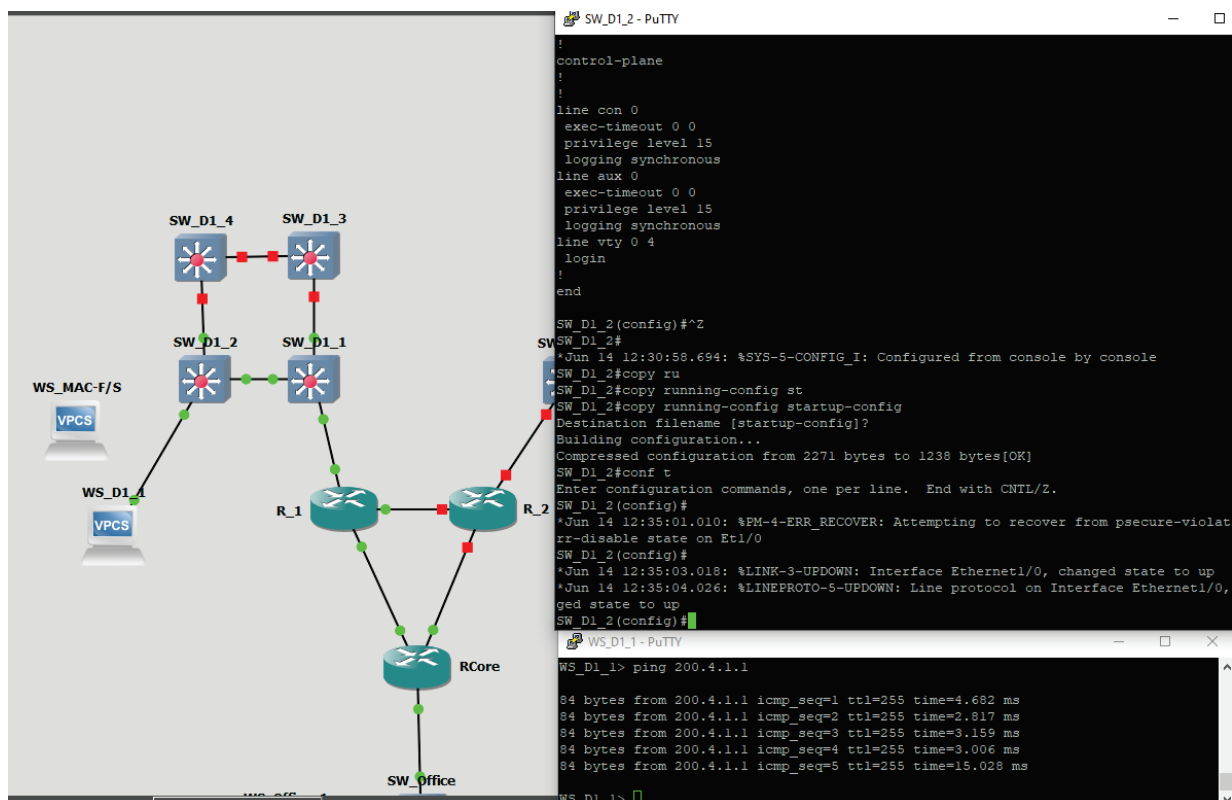


Рисунок 3.14 – Перевірка роботи

Як можна спостерігати, пакети успішно проходять. Тепер спробуємо підключити пристрій зломисника замість станції користувача.

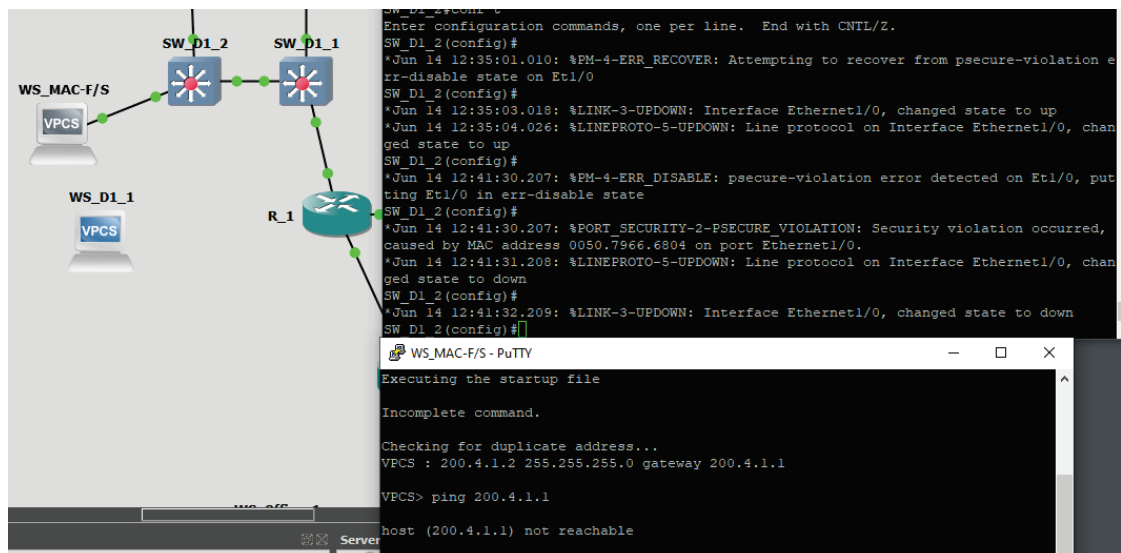


Рисунок 3.15 – Підключення станції зловмисника

Внаслідок підключення та спроби перевірити зв'язок, комутатор висунув повідомлення про відключення інтерфейсу, а відповідно до налаштувань, цей інтерфейс буде активований через визначений період часу.

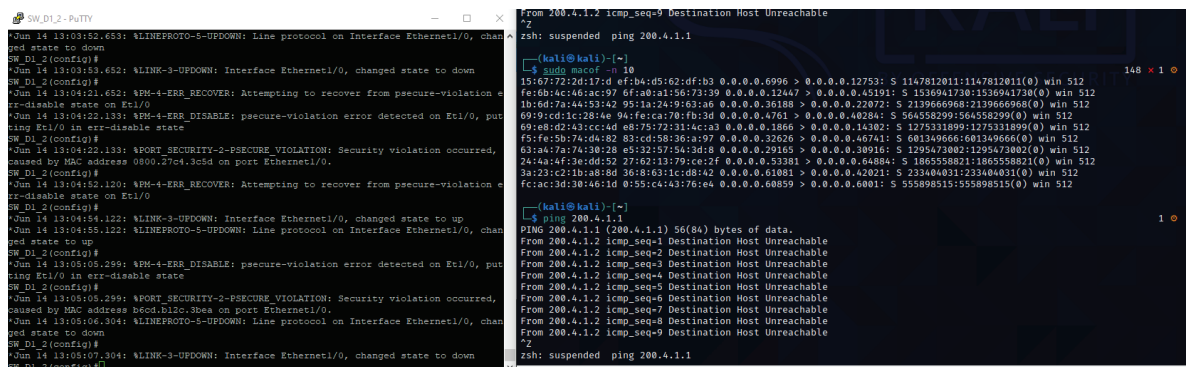


Рисунок 3.16 – Захист від MAC-Flooding

Як можна бачити на зображенні 3.16, під час здійснення атаки MAC-Flooding інтерфейс відключається так само, як і при атакі MAC-Spoofing.

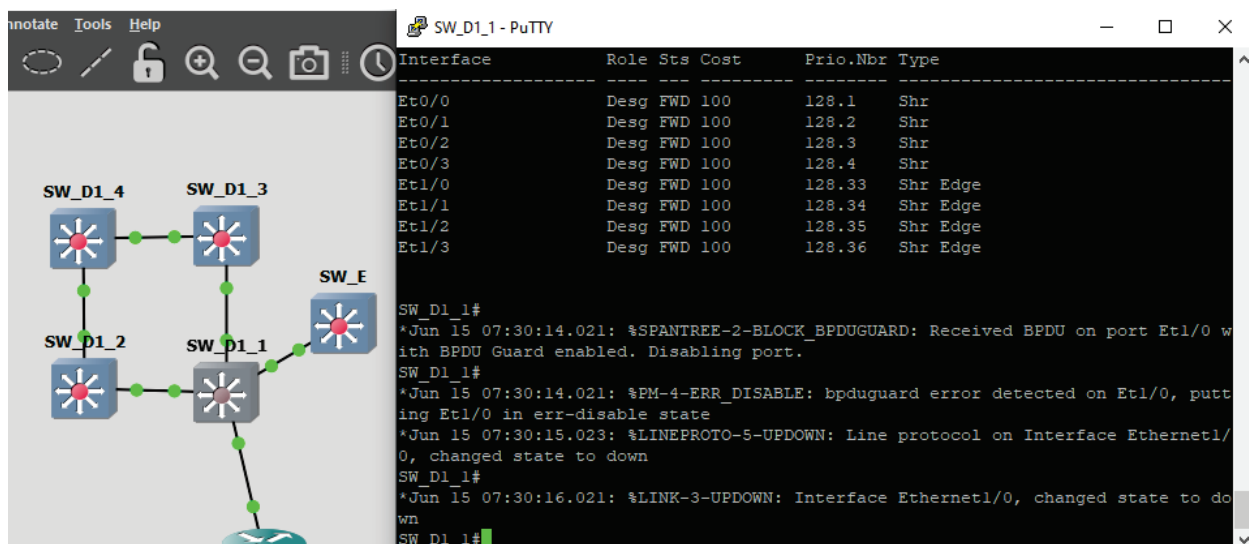


Рисунок 3.17 – Атака зловмисним комутатором

Як можна зауважити на терміналі, зловмисний комутатор був відключений для забезпечення безпеки мережі, як показано на рис. 3.17.

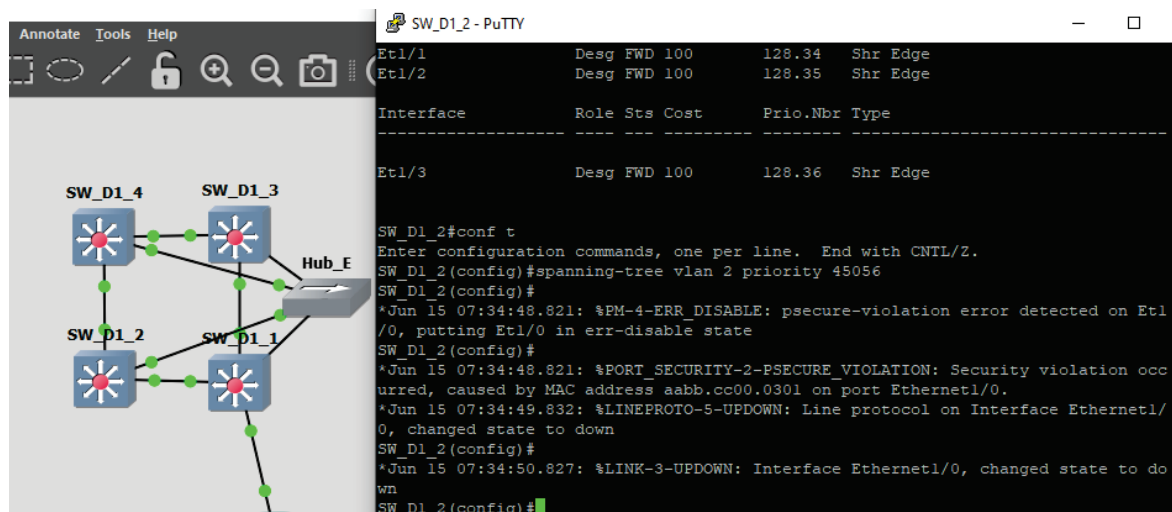


Рисунок 3.18 – Створення петель

Використовуючи концентратор, намагалися створити петлю. Проте, як можна спостерігати на терміналі, на рисунку 3.18, порти, підключені до концентратора, були відключені.

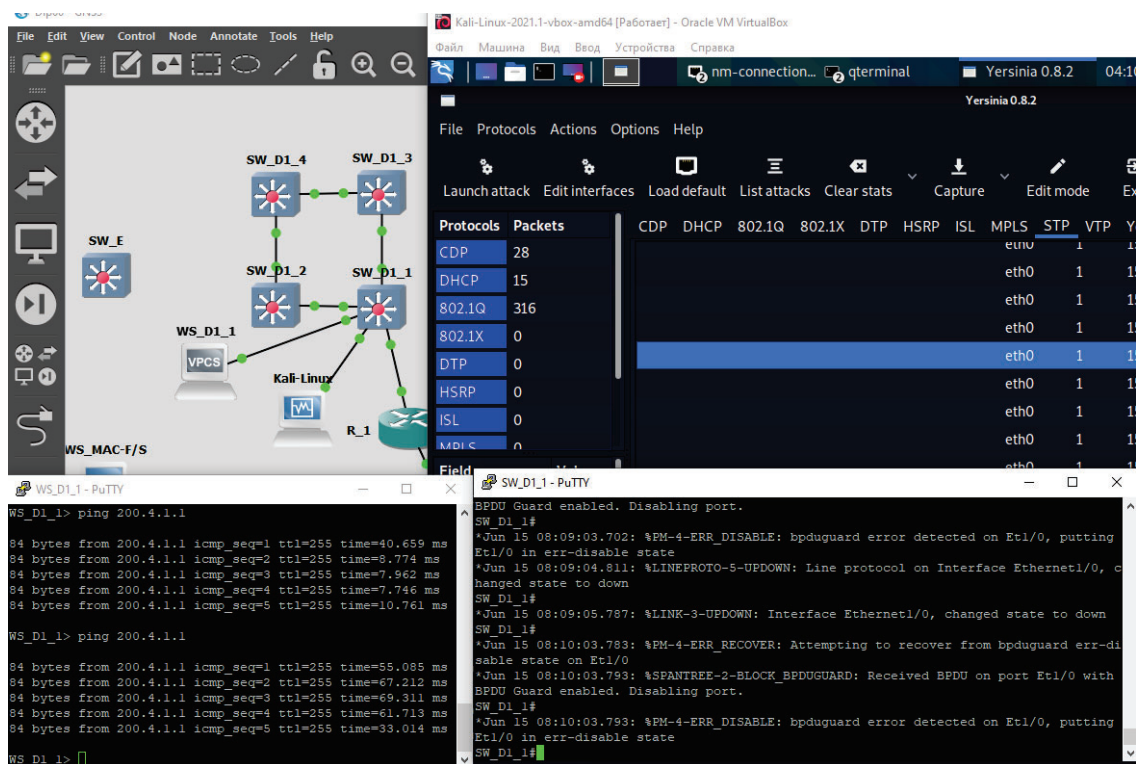


Рисунок 3.19 – DoS атака на протокол STP

Атака типу DoS не була успішною, оскільки система захисту вимкнула порт, через який відбувалася атака, і продовжує його моніторити до моменту зупинки атаки.

Далі буде перевірено захист від атак на протокол ARP.

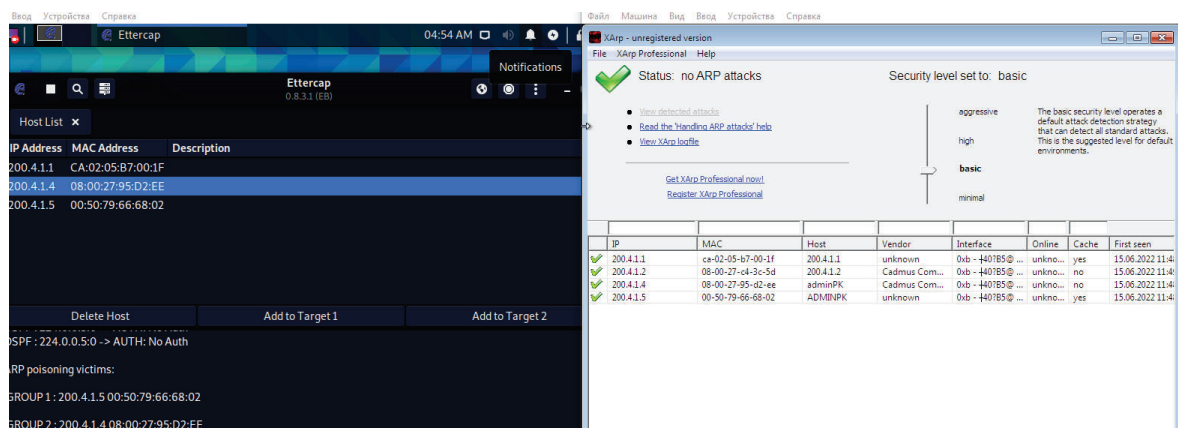


Рисунок 3.20 – Спроба атаки на протокол ARP

Програма, яка моніторить атаки на протокол ARP, не зафіксувала жодної атаки, що свідчить про ефективність захисту.

Атака на протокол DHCP включає підміну сервера і атаки DoS.

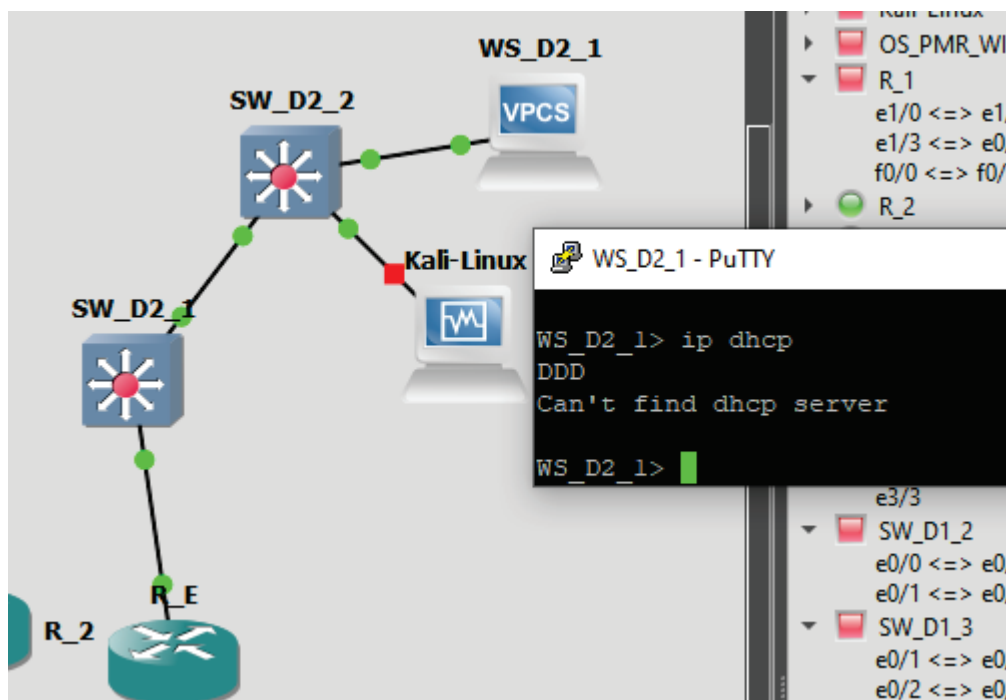


Рисунок 3.21 – Атака підміною серверу

При намаганні здійснити підміну сервера, пристрої не можуть отримати адреси від зловмисника, що убезпечує їхні дані від прослуховування.

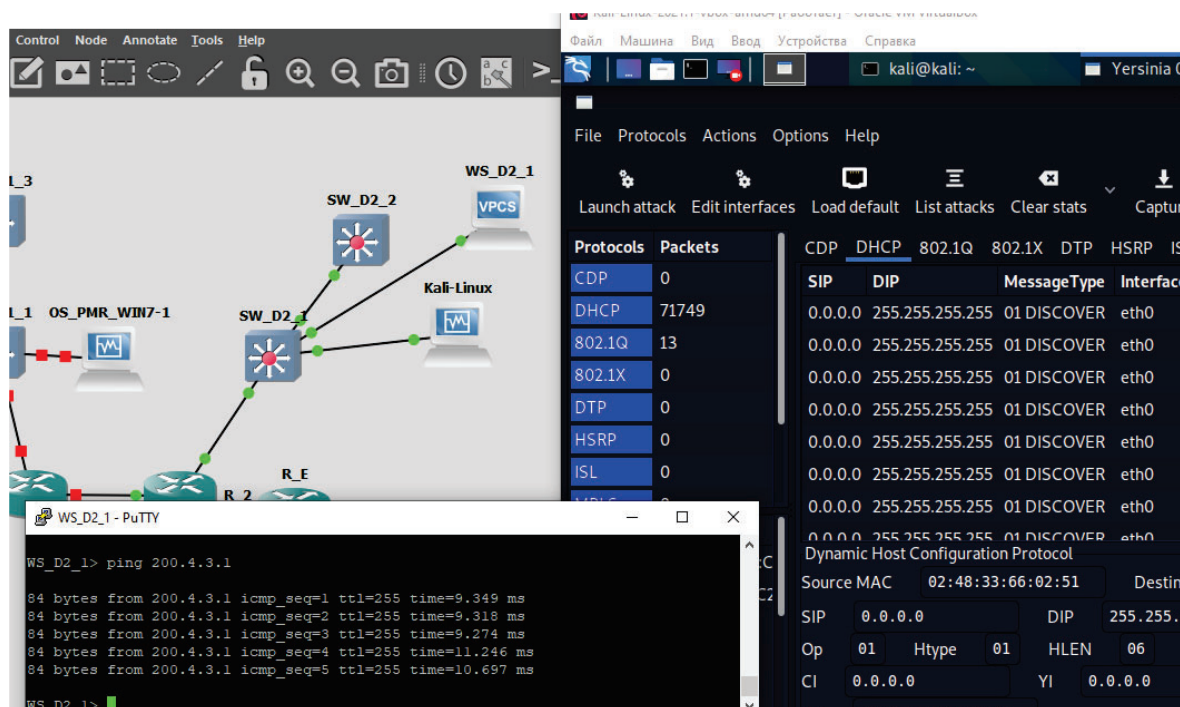


Рисунок 3.22 – DoS атака на протокол DHCP

Під час здійснення DoS атаки може виникнути невелике початкове зниження продуктивності мережі, проте зв'язок відновлюється з часом.

У третьому розділі детально проаналізовані провідні компанії, які постачають мережеве обладнання наявні на ринку. Також розглянуте обладнання цих компаній з огляду на використання в мережевих проектах. Зазначено, що вибір обладнання в значній мірі залежить від бюджетних можливостей компанії та рівня технічної підготовки персоналу. Також обрано програмне забезпечення з обґрунтуванням вибору. Проведено базове налаштування обладнання та підсистем захисту, після чого було виконано тестування окремих компонентів мережі та підсистем її захисту.

ВИСНОВКИ

У роботі розглянуто теоретичні відомості про правила та принципи побудови мережі. Визначено моделі побудови мережних інфраструктур міського інтернет-провайдера. Вивчено протоколи та технології, які застосовуються при розробці мереж. Під час обговорення були визначені переваги та недоліки їхнього використання.

Далі було розглянуто особливості та етапи проектування мережі міського інтернет-провайдера. Було розроблено фізичну та логічну топології, систему адресації з урахуванням можливості подальшого масштабування. Створено допоміжну інфраструктуру та розглянуто підсистеми захисту.

Проведено аналіз провідні компанії наявні на ринку, які постачають мережеве обладнання. Також розглянуте обладнання цих компаній з огляду на використання в мережевих проектах. Зазначено, що вибір обладнання в значній мірі залежить від бюджетних можливостей компанії та рівня технічної підготовки персоналу. Також обрано програмне забезпечення з обґрунтуванням вибору. Проведено базове налаштування обладнання та підсистем захисту, після чого було виконано тестування окремих компонентів мережі та підсистем її захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

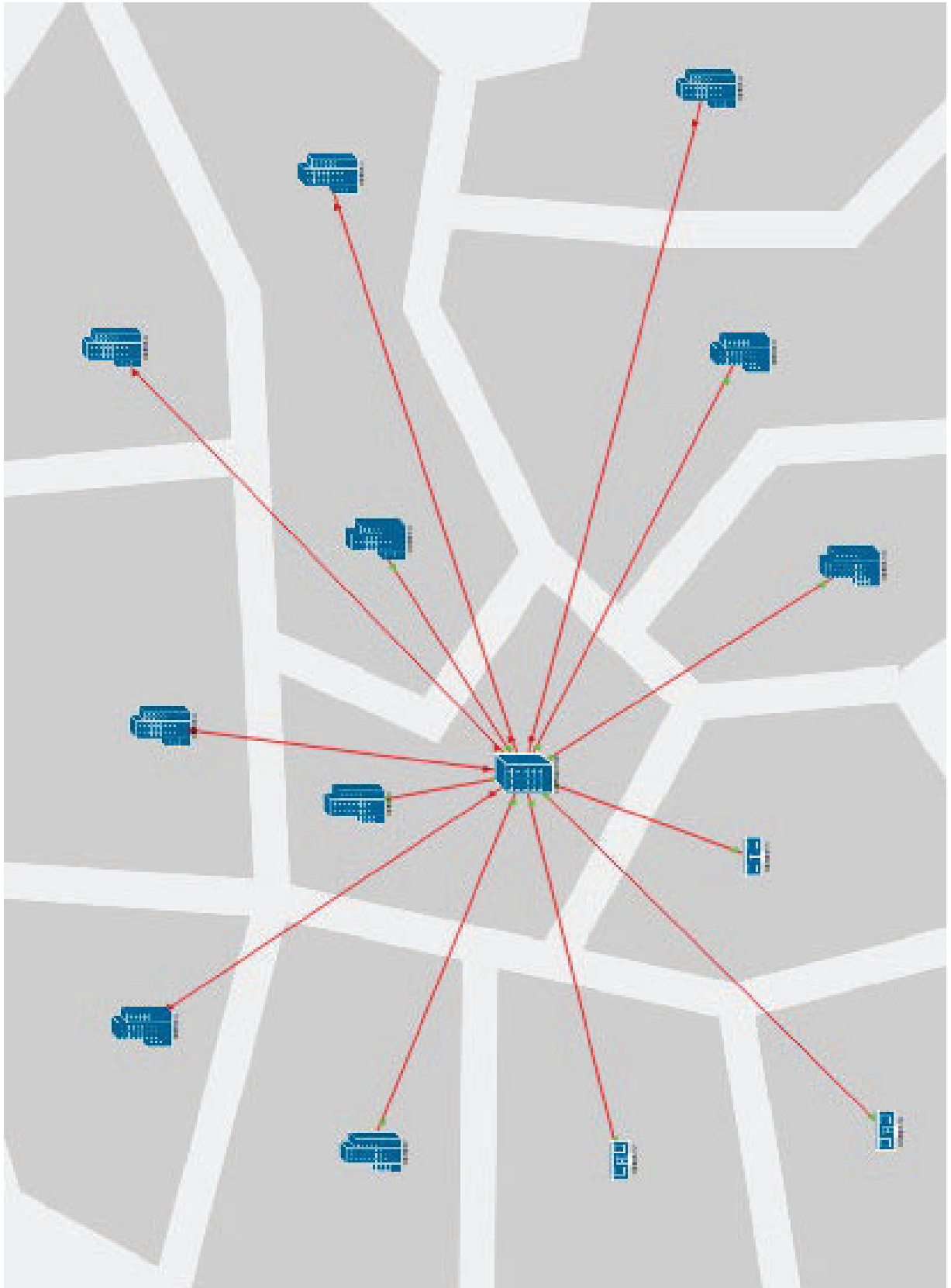
1. Lammle T. CCNA Routing and Switching Complete Study Guide. Sybex; 2nd edition, 2016. 1136 с.
2. Stallings W. Network Security Essentials: Applications and Standards 6th Edition. Pearson; 6th edition, 2016. 464 с.
3. Edelman J., Lowe S., Oswalt M. Network Programmability and Automation: Skills for the Next-Generation Network Engineer 1st Edition. O'Reilly Media; 1st edition, 2018. 581 с.
4. Chappell L. Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide. Laura Chappell University; 2nd Revised ed. edition, 2012. 986 с.
5. Stallings W. Cryptography and Network Security: Principles and Practice, 7Th Edition. PEARSON INDIA; 7th edition, 2017. 768 с.
6. Gray K., D. Nadeau T. Network Function Virtualization 1st Edition. Morgan Kaufmann; 1st edition, 2016. 270 с.
7. Що таке IPv4? [Електронний ресурс] – Режим доступу: <https://uk.education-wiki.com/6575994-what-is-ipv4>.
8. Що таке протокол IPv6 [Електронний ресурс] – Режим доступу: <https://uk.wizcase.com/blog/що-таке-протокол-ipv6-і-чому-ви-повинні-звє/>.
9. 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>.
10. Архітектура мережі або мережева архітектура [Електронний ресурс] – Режим доступу: <https://nettech.ua/news/arxitektura-seti-ili-setevaja-arxitektura>.
11. Rapid STP [Електронний ресурс] – Режим доступу: <https://habr.com/ru/company/cbs/blog/330358/>.

- 12.Що таке SSH і як він працює? [Електронний ресурс] – Режим доступу: <https://instagalleryapp.com/informacijna-bezpeka/shho-take-ssh-i-jak-vin-pracjue/>.
- 13.Технологія PON [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/knowegable-base/reference-information/66122.html>.
- 14.Cisco URL: <https://dovidnyk.info/index.php/Brand/115>.
- 15.OSPF Protocol [Електронний ресурс] – Режим доступу: <https://www.javatpoint.com/ospf-protocol>.
- 16.Опис технології Fast Ethernet [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/knowegable-base/reference-information/opisanie-tehnologii-fast-ethernet.html>.
- 17.Мережа Gigabit Ethernet [Електронний ресурс] – Режим доступу: <https://ua5.org/lan/141-merezha-gigabit-ethernet.html>.
18. Побудова мереж GPON на базі обладнання ТМ BDcom (семінар по обладнанню BDcom) [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/knowegable-base/reference-information/ua-equipment-gpon-bdcom-seminar-1.html>.
19. Побудова мереж GPON на базі обладнання ТМ BDcom (практична частина) (семінар по обладнанню BDcom) [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/knowegable-base/reference-information/ua-equipment-gpon-bdcom-seminar-3.html>.
20. Juniper Networks [Електронний ресурс] – Режим доступу: <https://omnilink.ua/juniper/>.
21. Huawei [Електронний ресурс] – Режим доступу: <https://omnilink.ua/huawei/>.
22. D-link [Електронний ресурс] – Режим доступу: <https://omnilink.ua/d-link/>.
23. BDCOM [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/brands/bdcom.html>.

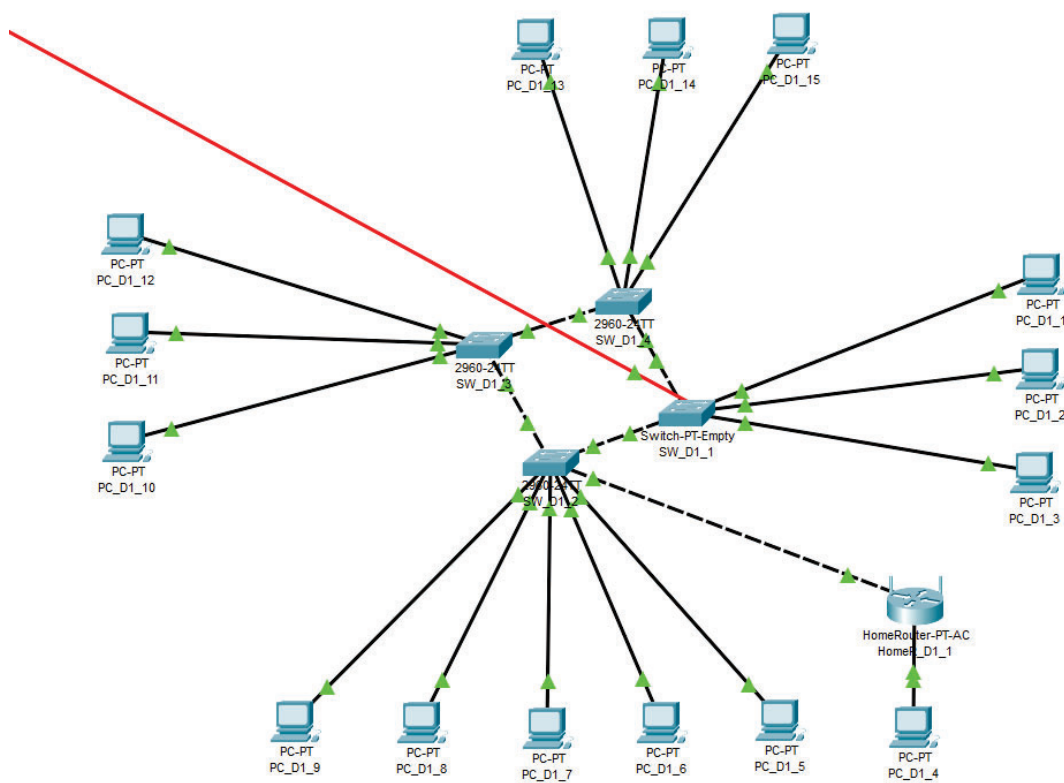
24. Коммутатор Cisco WS-C2960X-24TS-LL [Електронний ресурс] – Режим доступу: <https://stack-systems.com.ua/kommutator-cisco-ws-c2960x-24ts-ll>.
25. Маршрутизатор Cisco ISR4461/K9 [Електронний ресурс] – Режим доступу: <https://stack-systems.com.ua/marshrutizator-cisco-isr4461-k9>.
26. Маршрутизатор Cisco ISR4321-AX/K9 [Електронний ресурс] – Режим доступу: <https://stack-systems.com.ua/marshrutizator-cisco-isr4321-ax-k9>.
27. Маршрутизатор Juniper CHAS-BP-MX240-S [Електронний ресурс] – Режим доступу: <https://stack-systems.com.ua/marshrutizator-juniper-chas-bp-mx240-s>.
28. Маршрутизатор Juniper J2320-JB-SC-TAA [Електронний ресурс] – Режим доступу: <https://stack-systems.com.ua/marshrutizator-juniper-j2320-jb-sc-taa>.
29. Оптичний лінійний термінал BDCOM GP3600-16B [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/katalog/concentrators-olt/46394.html>.
30. Оптичний лінійний термінал BDCOM P3600-08E [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/katalog/concentrators-olt/47186.html>.
31. Навчальний курс CCNA Routing and Switching: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.
32. Навчальний курс CCNA Routing and Switching: Routing and Switching Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.
33. Навчальний курс CCNA Routing and Switching: Scaling Networks [Електронний ресурс] – Режим доступу: www.netacad.com.
34. Навчальний курс CCNA Routing and Switching: Connecting Networks [Електронний ресурс] – Режим доступу: www.netacad.com.
35. Навчальний курс CCNAv7: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.
36. Навчальний курс CCNAv7: Switching, Routing, and Wireless Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.
37. Навчальний курс CCNAv7: Enterprise Networking, Security, and Automation [Електронний ресурс] – Режим доступу: www.netacad.com.

38. Навчальний курс CCNA Security [Електронний ресурс] – Режим доступу: www.netacad.com.
39. Навчальний курс CCNA Cybersecurity Operations [Електронний ресурс] – Режим доступу: www.netacad.com.
40. Навчальний курс CCNP Enterprise: Core Networking [Електронний ресурс] – Режим доступу: www.netacad.com.
41. FTTx [Електронний ресурс] – Режим доступу: <https://lanmarket.ua/entsiklopediya/telekommunikatsionnye-tekhnologii/ftth.html>.
42. MikroTik [Електронний ресурс] – Режим доступу: <https://omnilink.ua/mikrotik/>.
43. Гузюк В. Оптично-волоконні мережі, якими підключають користувачів / Владислав Гузюк // Комп'ютерні технології: інновації, проблеми, рішення : Всеукр. науково-техн. конф., Житомир, 1–2 груд. 2022 р. – Житомир, 2022.
44. Гузюк В. Оптичні–волокна / Владислав Гузюк // III Всеукраїнській науково-практичній Інтернет-конференції «СУЧАСНІ КОМП'ЮТЕРНІ ТА ІНФОРМАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ», Запоріжжя, 12-19 груд. 2022 р. – Запоріжжя, 2022.

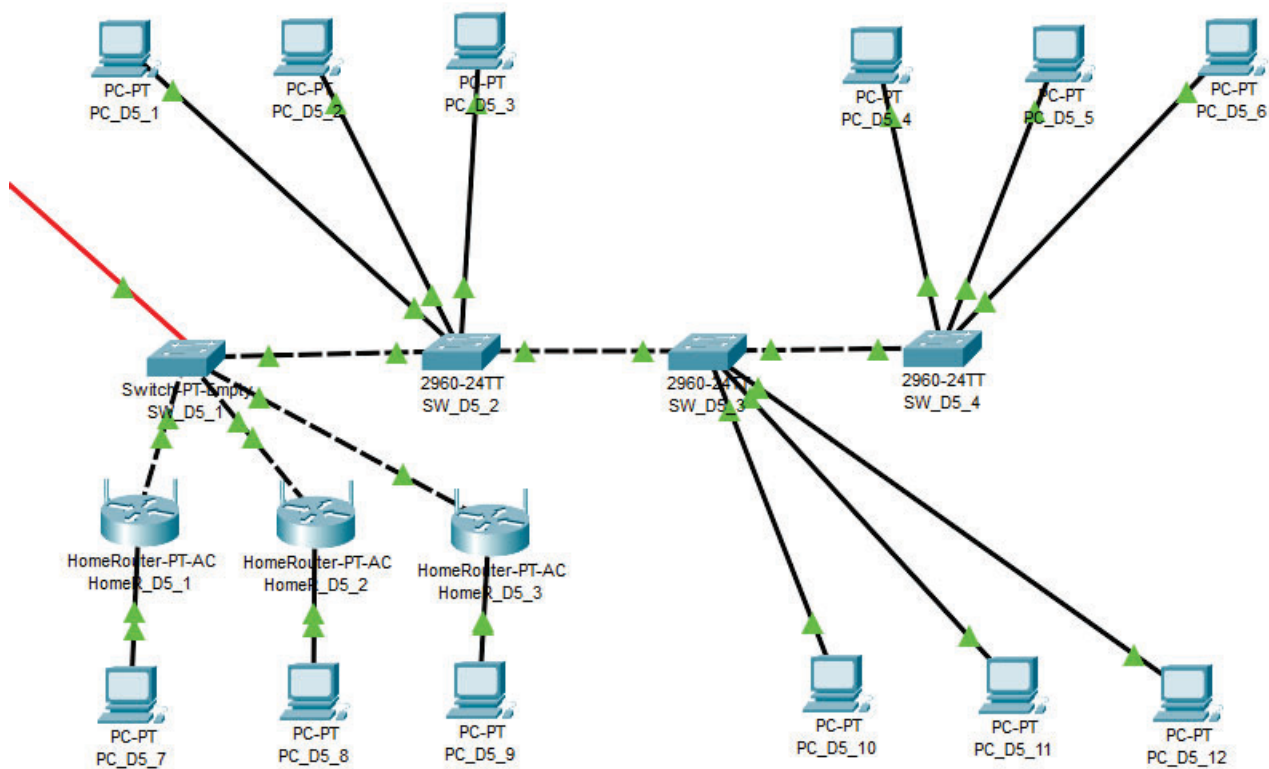
ДОДАТКИ



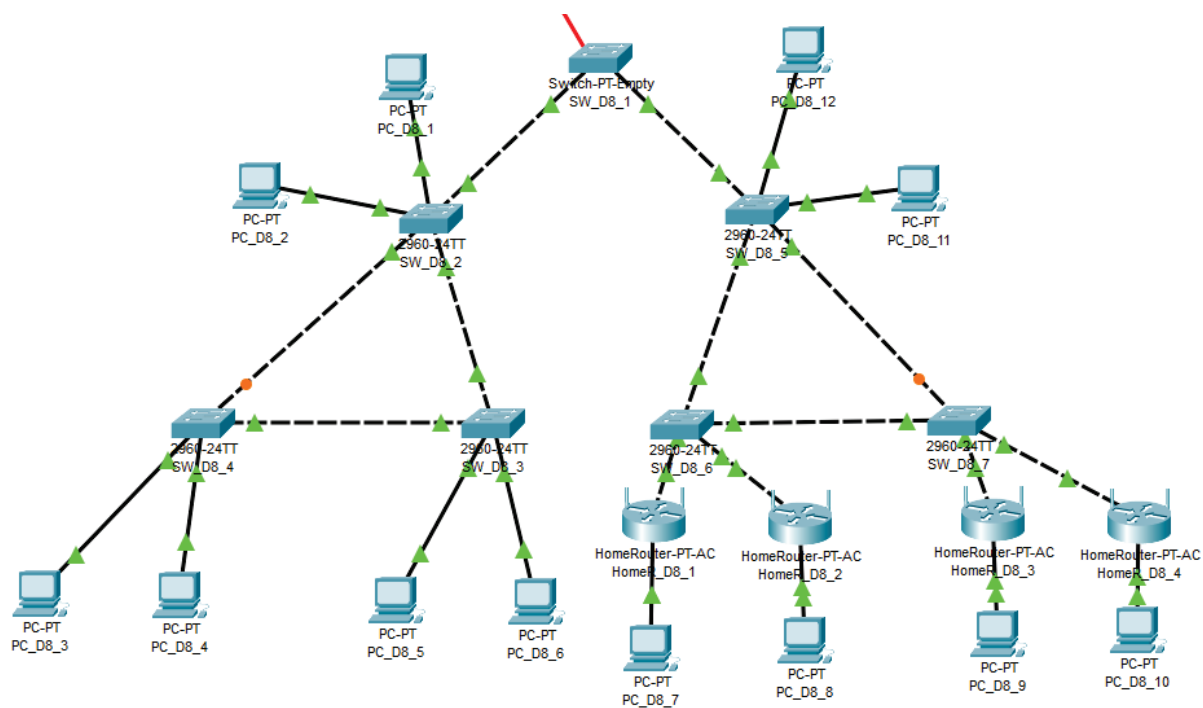
Додаток Б – Схема «кільце»



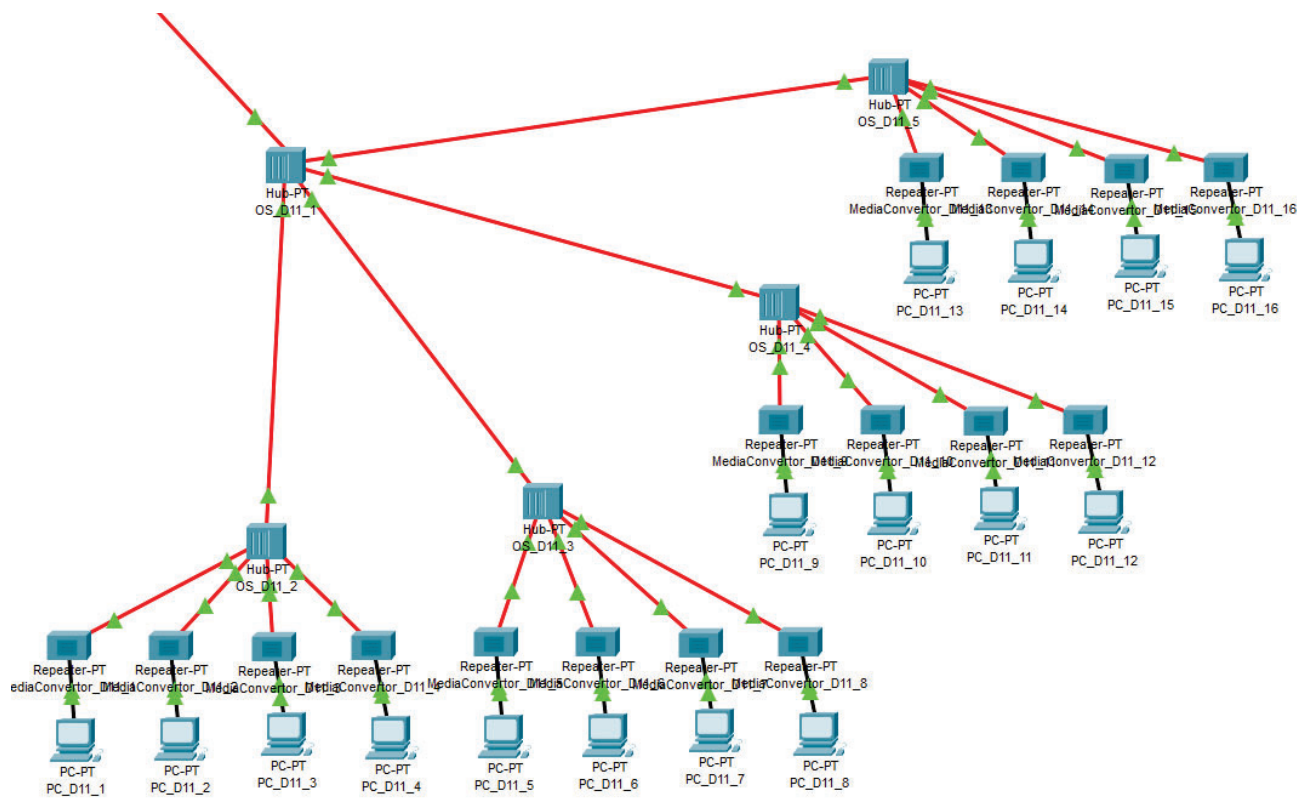
Додаток В – Схема «послідовне»



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$oS0YnMc/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
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
!
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
!
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
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
!
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
!
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
!
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
	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
R_2	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
R_3	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
R_4	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
R_5	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
R_6	GigE5/0	F	200.4.210.22	255.255.255.252	/30
	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
--	--------	-------	------------	---------------	-----