Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та кібербезпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

ЛОКАЛЬНА ОПТОВОЛОКОННА ДОМАШНЯ МЕРЕЖА

LOCAL FIBER OPTIC HOME NETWORK

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІс-21
Герасимчук Тарас Сергійович

(підпис)

Керівник:
к.т.н., доцент
Христинець Наталія Анатоліївна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« _____ » червня 2023 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2023 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та кібербезпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ проф. Н.Чернящук
«_____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Герасимчуку Тарасу Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Локальна оптоволоконна домашня мережа

Керівник роботи к.т.н., доцент Христинець Наталія Анатоліївна

затверджені наказом закладу вищої освіти від «28» грудня 2022 року № 982/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 01.06.2023р.

3. Вихідні дані до роботи методичні та літературні джерела з мереж, наукові статті інтернет-ресурси з різних джерел на тему дослідження оптоволоконних мереж, Нормативні стандарти та ДСТУ, ПЗ Cisco Packet Tracer

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
1. Огляд досліджень з впровадження оптоволоконних мереж, структур каналів зв'язку.
2. Розробити алгоритм побудови домашньої локальної мережі.
3. Побудувати план будівлі з урахуванням її конструкційних особливостей.
4. Дослідити протокол DHCP, VLAN, NAT, OSPF. Провести налаштування DHCP Servera
5. Спроектувати локально оптоволоконну домашню мережу. Із урахуванням захисту мережі за допомогою Access-List (ACL).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Розділ 1. Аналітичний огляд з дослідження оптоволоконних мереж	Христинець Н.А.		
Розділ 2. Методи побудови і адміністрування мережі	Христинець Н.А.		
Розділ 3. Розробка локальної мережі	Христинець Н.А.		
Висновки	Христинець Н.А.		

7. Дата видачі завдання 01.11.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Аналітичний огляд з дослідження оптоволоконних мереж	25.01.2023 р.	Виконано
2.	Огляд методи побудови каналів звязку та типів оптичних волокон	05.02.2023 р.	Виконано
3.	Методика побудування та конструювання мережі	25.02.2023 р.	Виконано
4.	Адміністрування мережі та безпека	15.03.2023 р.	Виконано
5.	Розроблення плану будівлі, її IP адресації та захисту мережі	20.04.2023 р.	Виконано
6.	Проектування мережі за зазначеним планом	25.05.2023 р.	Виконано
7.	Представлення матеріалів роботи на кафедру	01.06.2023 р.	Виконано

Здобувач вищої освіти _____ (Герасимчук Т.С.)
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ (Христинець Н.А.)
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Герасимчук Т. С. Локальна оптоволоконна домашня мережа. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2023.

Кваліфікаційна робота обсягом 66 сторінки містить 55 ілюстрацій, 4 таблиці, 1 формулу , та 20 джерел за переліком посилань.

У першому розділі проведено аналітичний огляд з дослідження оптоволоконних мереж, огляд досліджень із впровадженням оптоволоконних мереж, структур каналів зв'язку та типи поділу оптичних мереж за їхніми фізичними властивостями.

У другому розділі розглянуто методи побудови і адміністрування мережі, проведено огляд послідовності побудови мережі із дотриманням усіх стандартів. Розглянуто способи адміністрування мережі, дослідження протоколів DHCP, OFPS, NAT, VLAN, дослідження Access-List (ACL), протоколів ACL, дослідження безпеки мережі.

Третій розділ присвячено опису розробки та реалізації локальної оптоволоконної домашньої мережі. Розроблено послідовність виконання роботи, конструювання плану будівлі із застосуванням програми Microsoft Visio. Здійснено налаштування IP адресації, параметрів безпеки мережі. Спроектовано та земулювано локальну оптоволоконну домашню мережу в середовищі Cisco Packet Tracer.

Об'єкт дослідження – локально оптоволоконна домашня мережа.

Предмет дослідження – технології та інструменти для розробки локальної оптоволоконної домашньої мережі.

Ключові слова: оптоволоконна мережа, протоколи IP адміністрування, router, svitch, access-list (ACL), vlan, dhcp, nat, ofps, cisco pasket traiser, ip address.

ANNOTATION

Gerasimchuk T. S. Local fiber-optic home network. Manuscript.

Bachelor's qualifying thesis of the OP «Computer Engineering» specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2023.

The qualification work of 66 pages contains 55 illustrations, 4 tables, 1 formula and 20 sources according to the list of references.

In the first chapter, an analytical review of the research of optical fiber networks, an overview of researches with the implementation of optical fiber networks, the structures of communication channels and the types of division of optical networks according to their physical properties is carried out.

In the second section, the methods of network construction and administration are considered, and the sequence of network construction in compliance with all standards is reviewed. Methods of network administration, study of DHCP protocols, OFPS, NAT, VLAN, study of Access-List (ACL), ACL protocols, study of network security are considered.

The third chapter is devoted to the description of the development and implementation of a local fiber-optic home network. The sequence of work execution, construction of the building plan using the Microsoft Visio program has been developed. IP addressing, network security parameters have been configured. A local fiber-optic home network was designed and laid out in the Cisco Packet Tracer environment.

The object of the research is a local fiber-optic home network.

The subject of research is technologies and tools for the development of a local fiber-optic home network.

Keywords: fiber optic network, IP administration protocols, router, svitch, access-list (ACL), vlan, dhcp, nat, ofps, cisco pasket tracer, ip address.

ВСТУП

Актуальність теми даної роботи полягає в тому, що в наш час на ділянці доступу використовуються переважно мідні кабелі (звиті пари). Пропускна здатність та канальна ємність цих кабелів не дозволяє повною мірою реалізувати сучасні мультисервісні послуги, наприклад: передача мови, даних, трафіку мультимедійного формату, а також відеодані. Таким чином, потрібно забезпечити канал певною смугою пропускання, яка повинна бути ширшою за ту, яку можуть покривати існуючі технології в мідно-кабельній інфраструктурі.

Метою кваліфікаційної роботи є розробка локальної оптоволоконної домашньої мережі.

Для досягнення мети поставлено наступні завдання:

- провести огляд досліджень з впровадження оптоволоконних мереж дослідити структуру каналів зв’язку;
- розробити алгоритм побудови домашньої локальної мережі;
- побудувати план будівлі з урахуванням її конструкційних особливостей;
- дослідити та застосувати на практиці протоколи DHSP, VLAN, NAT, OSPF;
- провести налаштування DHCP SERVER та побудувати таблицю IP-адресацій;
- земулювати локальну домашню мережу у середовищі Cisco Packet Tracer;
- продемонструвати роботу мережі і спроектувати захист на основі протоколу Access-List та NAT;
- спроектувати локальну домашню мережу;

Об’єктом дослідження є локальна оптоволоконна мережа. У цій роботі буде зосереджено увагу на проектуванні та реалізації створення локальних мереж в середині приміщення, надання доступу до інтернет мережі та надання захисту. Розробка цієї мережі дозволить створити ефективний та функціонуючий мережевий канал з врахуванням потреб користувачів.

Предметом дослідження є технології та інструменти для розробки локальної оптоволоконної домашньої мережі. В рамках роботи будуть розглянуті протоколи адміністрування мережі та їх порівняння.

Завдяки поєднанню теоретичних джерел та практичних навиків, ця робота пропонує комплексний підхід до розробки локальної мережі, що враховує сучасні вимоги та технології.

РОЗДІЛ 1
АНАЛІТИЧНИЙ ОГЛЯД З ДОСЛІДЖЕННЯ ОПТОВОЛОКОННИХ МЕРЕЖ

1.1 Огляд досліджень з впровадження оптоволоконних мереж

Питання впровадження дротового під'єднання для організації комунікації між певною к-стю комп'ютерів у локальних мережах досліджувались багатьма вченими. Роберту Меткалфу приписують винахід Ethernet, найбільш поширеної технології локальної мережі (LAN). Він відіграв вирішальну роль у розробці стандарту Ethernet і його подальшому прийнятті, що зробило революцію в проектуванні та управлінні локальними мережами. Радіа Перлман відома своїм внеском у розробку протоколу охоплюючого дерева (STP) і розробку протоколу прозорого з'єднання безлічі посилань (TRILL). Її робота значно вплинула на проектування та управління великомасштабними локальними мережами. Дональд Девіс визнаний однією з ключових фігур у розробці мереж з комутацією пакетів. Він ввів термін «комутація пакетів» і зробив значний внесок у розробку та управління першими локальними мережами.

Також предметом дослідження локальних мереж були організації, університети та виробники обладнання для мереж. Вони активно займаються дослідженнями в галузі впровадження оптоволоконних мереж.

Corning Incorporated є американською міжнародною компанією, яка спеціалізується на розробці, виробництві та постачанні різноманітних високотехнологічних матеріалів, включаючи скло і кераміку. Компанія має багато галузей діяльності, але однією з її ключових областей є оптоволоконна технологія. Основні напрямки діяльності Corning Incorporated у сфері оптоволокна включають, розробку і виробництво оптоволоконних кабелів Corning виробляє різні типи оптоволоконних кабелів, які використовуються для передачі великого обсягу даних на великі відстані. Ці кабелі володіють високою пропускною здатністю та низькими втратами сигналу.

Corning виробляє оптоволоконні прутки і пластини, які використовуються для виготовлення компонентів оптоволоконних мереж, таких як роз'єми, розподільчі плати та спліттери. Крім пасивних компонентів, Corning також займається розробкою активних компонентів для оптоволоконних мереж, включаючи лазерні діоди, фотодетектори та інші елементи, які використовуються для генерації та прийому оптичних сигналів.

Постійно працює над дослідженнями і розробкою нових технологій в галузі оптоволокна. Вони ставлять перед собою завдання покращення характеристик оптоволоконних систем, таких як пропускна здатність, якість передачі та надійність. Corning Incorporated є визнаним лідером у галузі оптоволокна і забезпечує своїми інноваціями розвиток телекомунікаційної індустрії та інших галузей, що використовують оптоволокно.

Інститут оптоволоконних комунікацій (Optical Fiber Communications, OFC) є однією з провідних організацій, яка займається дослідженнями і розробкою в галузі оптоволоконних комунікацій. OFC проводить широкий спектр досліджень, що стосуються різних аспектів оптоволоконних систем і мереж. Вони досліджують нові модуляційні формати, алгоритми управління сигналом та інші інновації, що дозволяють передавати дані на високих швидкостях через оптоволокно.

OFC проводить дослідження з використанням нових матеріалів для виробництва оптоволоконних кабелів. Активно співпрацює зі стандартизаційними організаціями для розробки нових протоколів та стандартів, що стосуються оптоволоконних комунікацій. Це включає такі аспекти, як передавання даних, керування мережами, безпека та інші аспекти оптоволоконних систем.

Виробники обладнання: Компанії, такі як Cisco Systems, Huawei Technologies, Juniper Networks та інші, складають значні зусилля в дослідженні та розробці нових рішень для оптоволоконних мереж. Вони займаються

впровадженням нових технологій, розширенням пропускної здатності мережі, вдосконаленням управління та безпеки оптоволоконних мереж.

Згідно з досліджень [1], [7], дослідження в галузі впровадження оптоволоконних мереж, містить актуальність на сьогоднішній час.

1.2 Структура каналів зв'язку

Оптичний світловод – це циліндричний діелектричний хвилевід, що передає світло від одного до другого кінця усієї своєї довжини завдяки фізичному явищу повного внутрішнього відбиття. Світловод складається із серцевинного та оболонкового шару, які виготовленні із матеріалів, що забезпечують утримування світла всередині кабелю. Для забезпечення функціонування даної системи діелектриків, необхідно мати показник заломлення серцевини більший, ніж оболонки. А також, границя двох середовищ може бути обривчастою, як у волокон зі сходинковим профілем серцевини, чи згладженою, як у волокон з градієнтним профілем серцевини. Структура типового одномодового волокна зазначена на рисунку 1.1.

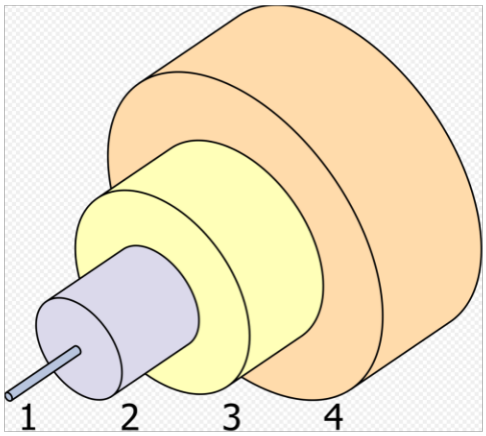


Рисунок 1.1 – Структура одномодового волокна (1 – серцевина 8 μm діаметр; 2 – Оболонка 125 μm діаметр; 3 – Буфер 250 μm діаметр; 4 – Обшивка 400 μm діаметр), [16]

Структура може містити екран, силові елементи та інші конструктивні елементи. Також це фізичний медіум, що складається з певної кількості оптичних волокон, оточених спільною захисною оболонкою, та використовується для передачі світлового потоку, що зображена на рисунку 1.2.

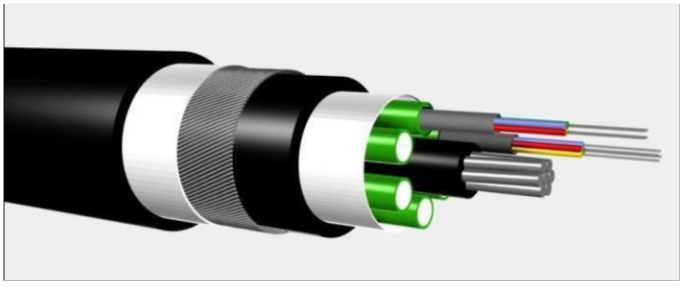


Рисунок 1.2 – Багато волоконний оптичний кабель, [20]

Лінія оптичних сигналів складається з одного або декількох паралельних кабелів із з'єднувальними, стопорними та кінцевими муфтами (ущільненнями) та кріпильними деталями. Розрізняють одномодове і багатомодове волокно. Одномодове волокно (SM) найпоширеніших розмірів, буває: 8/125 і 9/125 мкм (це означає: діаметр серцевини – 8 мкм, діаметр волокна – 125 мкм тощо). Багатомодове (ММ) найпоширеніших розмірів, буває: 50/125 і 62/125 мкм. Одномодове волокно дешевше за багатомодове, дозволяє передавати оптичний імпульс на великі відстані, з меншим розходженням сигналу на виході, але в той же час прямо передавальне устаткування для нього значно дорожче. Існує також багатомодове волокно з градієнтним профілем у якого зменшені ці недоліки.

Оптичні волокна перед їх використанням мають бути покриті захисною оболонкою. Кабельна оболонка – зовнішня захисна структура, що оточує одне або більше волокон. За призначенням оболонка схожа з ізоляцією, що застосовується в мідних кабелях. Кабельна оболонка захищає мідні провідники і волокна від зовнішніх агресивних і механічних впливів, здатних призвести до ушкоджень або погіршення їхніх характеристик. У порівнянні з мідними

кабелями, діелектричні волокна не вимагають додаткових видів захисту від електричних розрядів, замикань і полум’я.

Для будь-якого кабелю важливими характеристиками є межа його міцності на розрив, твердість, термін служби, гнучкість, захищеність від зовнішніх впливів, діапазон робочих температур і, навіть, зовнішній вигляд.

Згідно з досліджень [2-6], межі міцності, оптоволоконних кабелів обчислюються стандартами до прикладу у США стандарти, що регулюють межі міцності оптоволоконних кабелів, розробляються та встановлюються різними організаціями та стандартизаційними органами. Основні стандарти, які впливають на межі міцності оптоволоконних кабелів у США, включають:

TIA/EIA-568: Цей стандарт, розроблений Американською асоціацією телекомунікаційної промисловості (TIA) та Американським інститутом електротехніки (EIA), встановлює стандарти для структурованих кабельних систем, включаючи оптоволоконні кабелі. Він містить вимоги до міцності, захисту та інших параметрів кабелів. ANSI/TIA-568-C.3: Цей стандарт, також розроблений Американською асоціацією телекомунікаційної промисловості (TIA), специфікує вимоги до проектування та інсталяції оптоволоконних кабельних систем. Він включає вимоги до міцності кабелю на розрив, гнучкості, терміну служби та інших параметрів.

National Electric Safety Code (NESC): Цей код, розроблений Інститутом електротехнічної та електронної інженерії (IEEE), встановлює стандарти безпеки для електричних систем, включаючи оптоволоконні кабельні системи. Він містить вимоги до міцності та захисту кабелів у відношенні до зовнішніх впливів, таких як механічні навантаження, погодні умови та інші. National Fire Protection Association (NFPA) 70: Цей стандарт, також відомий як Національний електроустановчий код (NEC), містить правила щодо електричної безпеки. Він включає вимоги до монтажу та охорони оптоволоконних кабелів від пожежі та інших небезпечних ситуацій.

Ці стандарти встановлюють вимоги до різних аспектів міцності оптоволоконних кабелів, забезпечуючи їхню надійність та безпеку при використанні. Оцінка цих характеристик залежить від конкретного застосування.

1.3 Типи оптоволокна. Фізичні властивості

Оптичні волокна поділяють на декілька типів до прикладу одномодове волокно це оптичний світловод із діаметром серцевини розміром приблизно одної десятої довжини несучої світлової хвилі, не можуть бути змодельованими використовуючи теорію геометричної оптики, зразок зображено на рисунку 1.3.

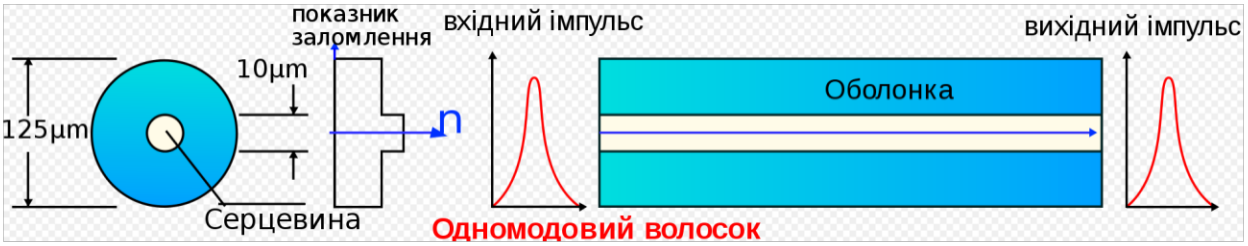


Рисунок 1.3 – Розповсюдження світлових променів через одномодові оптичні світловоди, [16]

На зразок оптичного хвилевода, світловод підтримує один чи декілька локалізованих поперечних мод, у границях яких світло просувається вздовж. Волокно, що працює тільки в одному режимі, називається одномодовим, чи мономодовим. Поведінка оптичних світловодів із значним розміром серцевини теж може бути змодельована за допомогою хвильових рівнянь, що у результаті демонструє їх здатність до пропускання світла у кількох режимах, або модах. Звідси походить і назва типів оптоволокна. Найбільш розповсюджений тип одномодового волокна має діаметр серцевини 8-10 мікрометрів та спроектований для використання світла близького до інфрачервоного діапазону спектру.

Структура моди залежить від довжини хвилі світла, яке задіяне у процесі роботи, таким чином світловод фактично підтримує незначну кількість додаткових мод у видимій частині спектру світла. Багатомодове оптоволокно, для порівняння, виготовлено із діаметром центральної жили поперечного розміру щонайменше ніж 50 мікрометрів, та що найбільше сотні мікрометрів. Нормалізована частота V для волоска має бути не більше ніж нульовий член степеневого ряду функції Бесселя J0 (приблизно 2.405).

Оптичне волокно із великим діаметром серцевини (більше 10 мікрон) може бути розраховане за допомогою методів геометричної оптики, зображено на рисунку 1.4.

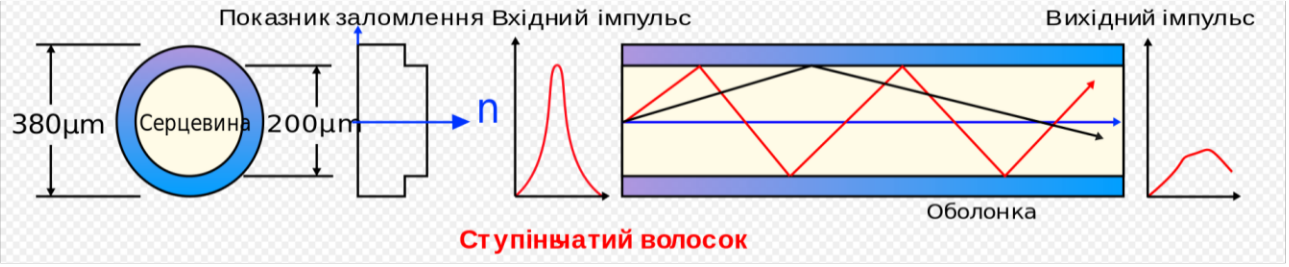


Рисунок 1.4 – Розповсюдження світлових променів через багатомодові оптичні світловоди, [16]

Сходинкове багатомодове волокно проводить промені світла вздовж серцевини завдяки ефекту повного внутрішнього відбиття. Промені, що падають на межу розділу компонентів волосини під стрімким кутом, більшим ніж кут повного внутрішнього відбиття, зазнають цілковитого відображення. Промені що стикаються із границею під малим кутом заломлюються у напрямку від серцевини до оболонки, а далі поглинаються і не передають інформацію. У градієнтному волокні показник заломлення у серцевині зменшується поступово від осі до зовнішньої стінки волокна, рисунок 1.5.

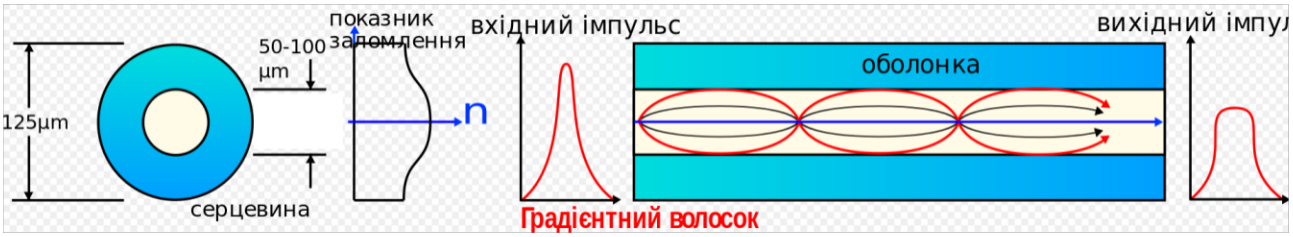


Рисунок 1.5 – Розповсюдження світлових променів через градієнтні оптичні світловоди, [16]

Це змушує промені світла вигинатися дугою при наближенні до оболонки, на відміну від несподіваного відображення на межі розділу компонентів волокна.

Як наслідок, дугоподібний шлях просування зменшує багатовекторну дисперсію розповсюдження, тому що промені під значними кутами проходять через ділянку серцевини із малим показником заломлення швидше, ніж під великим. Ідеальний профіль градієнту заломлення є дуже близький до параболічного при співвідношенні самої величини та відстані до осі. Поляризаційно-стабільне волокно або pm-волокно – це волокно, яке утримує лінійно поляризоване світло, заживлене в його середовище із малим або зовсім відсутнім перерозподілом енергії між поляризованими модами. Існує декілька різних способів створення подвійного променезаломлення в оптоволокні.

Світлопровід може бути геометрично асиметричним, з елементом еліптичної оболонки, або мати асиметричний профіль показника заломлення в іншому випадку, перманентна механічна напруга, прикладена до волокна викликає подвійне променезаломлення деформації. До такої функції придатні стрижні іншого матеріалу, що вкладаються в оболонку. Звідси походить декілька різновидів pm-волокна, що називаються «панда» та «метелик», рисунок 1.6.

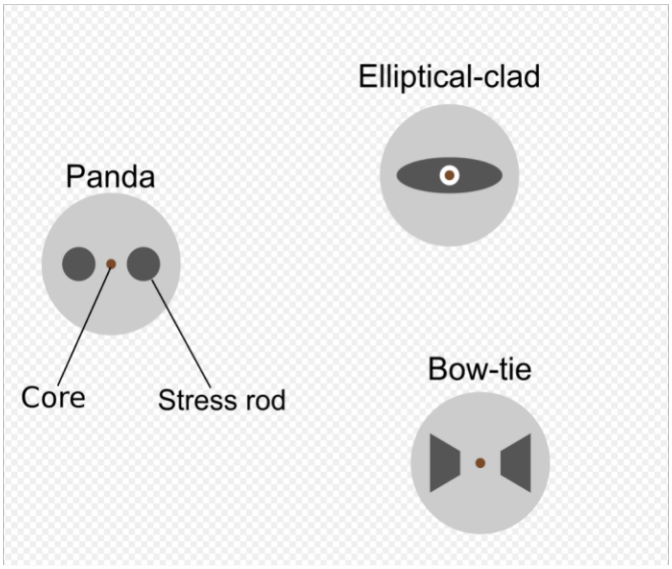


Рисунок 1.6 – Розріз поляризаційно стабільного оптоволоска, [19]

Ще один способом відтворення подвійного променезаломлення є скручування мономодового оптоволокна, викликаючи внутрішню деформацію скручування. Така дія призводить до виникнення кругового подвійного променезаломлення. Отримавши значну різницю у кутових швидкостях правосторонньої та лівосторонньої поляризації, перехресна взаємодія двох мод світлового променю за таких умов є дріб'язкова.

Поляризаційно-стабільні волокна мають спеціальні застосування, як оптоволоконе зондування, інтерферометрія та розповсюдження квантових кодів. Проте, для зв'язку на довгих відстанях поляризаційно-стабільні волокна не експлуатуються, через підвищений рівень загасання сигналу в порівнянні із одномодовими волокнами.

Поляризаційно-стабільне оптоволокно не поляризує світло на зразок поляризатора. Скоріше, воно утримує існуючу поляризацію лінійно поляризованого світлового променю, що вводиться у волокно за умови правильної орієнтації. Якщо поляризація вхідного світлового потоку не налаштована до ладу із добре вираженим пропускним напрямком в самому світловоді, то вихідний сигнал буде визначатися в межах лінійної та кругової поляризації.

Фотонно-кристалічне оптоволокно – новий клас оптичних світловодів, які працюють завдяки властивостям фотонних кристалів. Через неможливість локалізування світла в порожнині пустотілої серцевини та відсутність будь-яких схожих властивостей в традиційному оптоволокні, фотонно-кристалічні світловоди зараз набувають широкого застосування в оптичних комунікаціях, волоконних лазерах, нелінійних оптичних пристроях, трансляції високої потужності, надчутливих газових датчиках та інших пристроях, рисунок 1.7.

Фотонно-кристалічні волокна поділяються на дві категорії згідно з механізмом взаємодії зі світлом. Ті, що мають суцільну серцевину, чи серцевину із показником заломлення вищим, ніж мікроструктурна оболонка, можуть оперувати згідно з тим самим принципом, що і звичайне оптоволокно.

Проте, вони матимуть значнішу різницю показників заломлення серцевини та оболонки, що сприятиме ефективнішій локалізації випромінювання у випадку нелінійних оптичних пристроїв. Інша категорія – це волокно із фотонно-спектральним зазором, в якому світло утримується завдяки мікроструктурній оболонці. Якщо спектральний зазор підібраний правильно, то світловим потоком можна керувати в частині серцевини із низьким показником заломлення, або навіть цілковито пустотілій, заповненій повітрям.

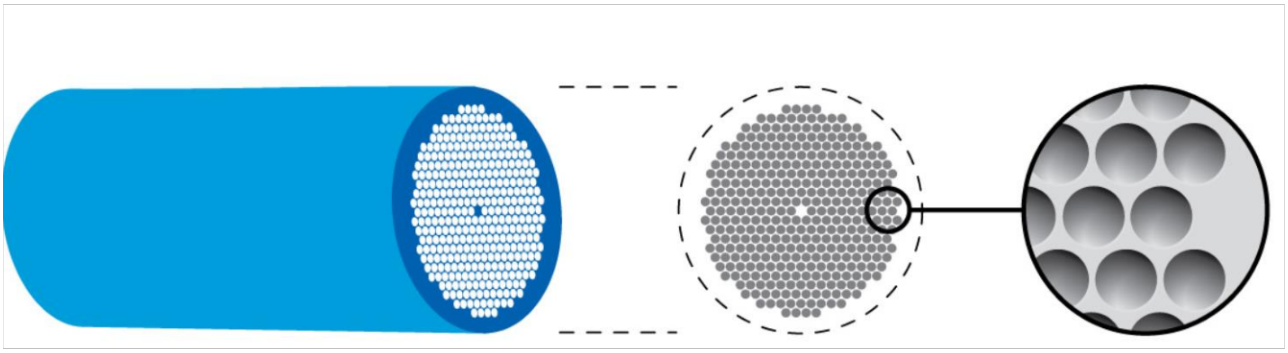


Рисунок 1.7 – Приклад фотонно-кристалічного волокна, [18]

Спектрально-зазорні волокна із відсутньою серцевиною потенційно можуть вирішити проблему, створену обмеженнями доступності необхідних

матеріалів для виготовлення світловоду. Для прикладу, можна створити волокно, що проводить світло із довжиною хвилі, для якої прозорі матеріали відсутні.

Показник заломлення – це відношення швидкостей світла у вакуумі та матеріалі, до якого належить даний показник. Чим більший показник заломлення в речовині – тим швидкість променю в ній нижча. Коли промінь що подорожує в оптично густому матеріалі, натикається на перешкоду під кутом падіння, більшим ніж критичний для даного матеріалу, то світло буде повністю відбите, зразок зображено на рисунку 1.8.

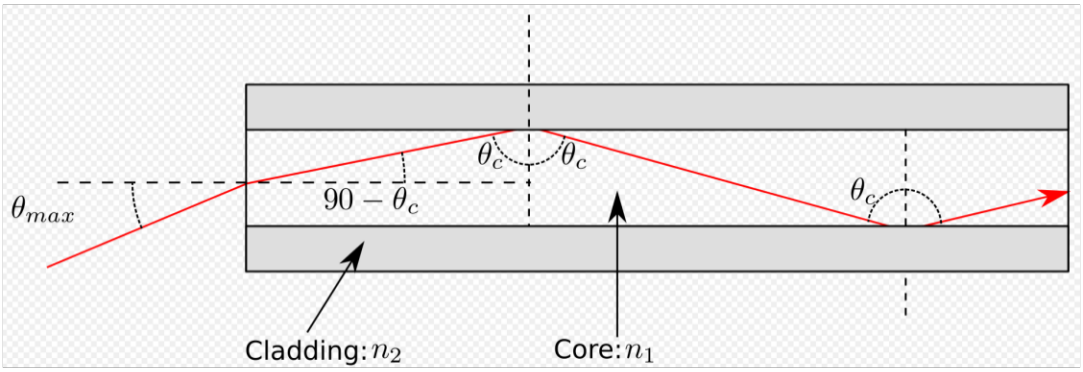


Рисунок 1.8 – Траєкторія світлового променя в оптичній волосині [16]

Цей ефект використовується в оптичному волокні для утримування світлового випромінення у межах його серцевини. Воно поширюється вздовж волоска, відбиваючись вперед та назад від границі розділу двох складових кабелю. По причині того, що промінь повинен впасти на межу розділу під певним нахилом, що є більшим за критичний кут, то тільки світло, яке увійшло у систему у межах певного діапазону напрямків, може пройти через все волокно без просочування за його межі.

У волоконно-оптичних лініях зв’язку (ВОЛЗ) існують хвилі трьох типів, що направляються, що випливають і випромінюються. Хвилі, що випромінюються виникають при введенні світла в хвилевід. Тут певна частина енергії вже випромінюється в навколишній простір і не поширюється вздовж

світловода. Причини що призводять до випромінювання світлових сигналів в навколишній простір, призводить до загасання, або втрати, корисного сигналу в волоконно-оптичних лініях зв'язку (ВОЛЗ).

Загасання – це зменшення інтенсивності світлових променів у волосках відносно відстані перетнутої ними у середовищі передачі, рисунок 1.9. Коефіцієнт загасання в оптоволокні зазвичай використовується в одиницях dB/km, завдячуючи відносно високій прозорості сучасного оптичного медіуму. Як правило, ним виступає кварцовий скляний світловод, що утримує захоплене проміння у границях свого фізичного тіла.

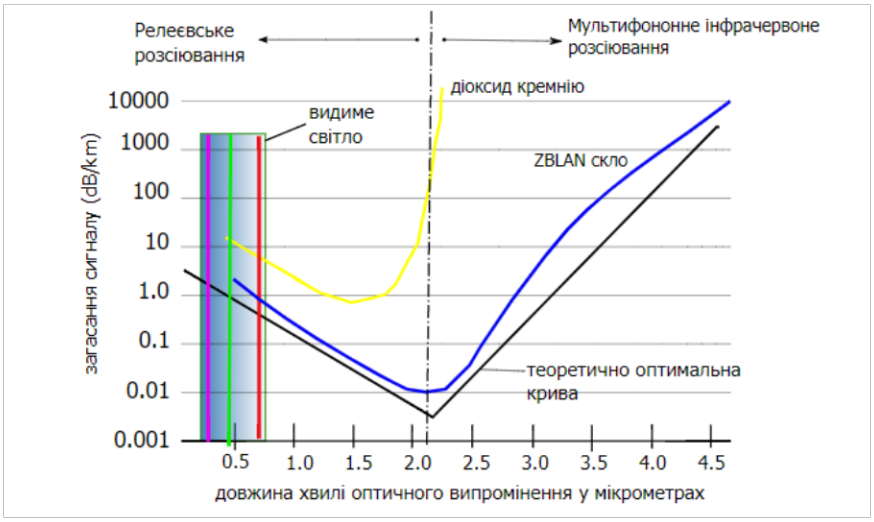


Рисунок 1.9 – Загасання світла через ZBLAN та діоксид кремнієве оптоволокно, [16]

Фактором, що обмежує просування цифрового сигналу на великі відстані. Не дивно, основна маса досліджень була проведена у зв'язку з намаганнями зменшити його вплив, та посилити оптичний сигнал. Емпіричний аналіз показав, що загасання у волосках виникає через розсіювання та поглинання. Загасання ОС за рахунок фізичних особливостей ОВ обумовлено існуванням втрат при передачі інформації.

При поширенні оптичного імпульсу вздовж однорідного волокна потужність P і енергія W імпульсу зменшуються через втрати енергії,

викликаних розсіюванням і поглинанням за експоненціальним законом Бугера, і визначається за формулою 1.1.

$$P(L) = P(0)\, e(-\alpha L),\ W(L) = W(0)\, e(-\alpha L), \qquad (1.1)$$

де P (L) - потужність випромінювання на відстані L;

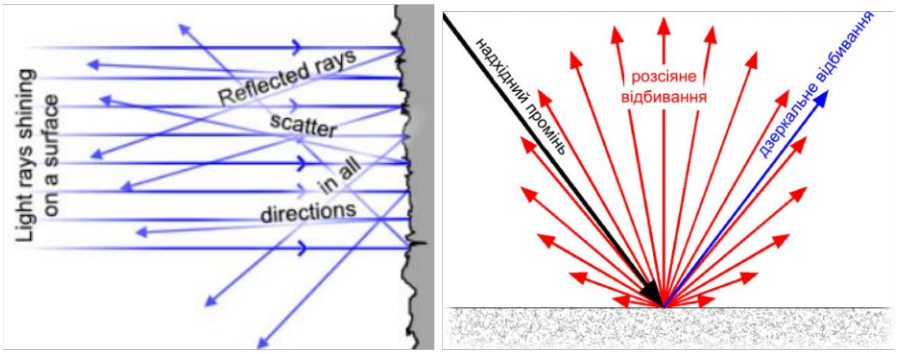
P(0) - потужність випромінювання в початковій точці;

α - коефіцієнт загасання,

α - коефіцієнт загасання, який визначається виразом: α = ln.

Розсіювання світла залежить від довжини світлової хвилі. Таким чином, виникають зони видимості на шкалі просторових координат відліку, що залежать від частоти падаючого променю та фізичних розмірів агенту розсіювання, який зазвичай предстає у вигляді якоїсь мікроструктури. Оскільки видиме світло має розміри довжини хвилі в сотнях нанометрів, то центр дифузного відбиття повинен мати розміри співставимої величини.

Дифузне або розсіяне відбиття світла – явище відбиття світла поверхнею, при якому світлові промені відбиваються в різних напрямках, що зображено на рисунку 1.10 (а, б).



а) б)

Рисунок 1.10 – Способи відбиття: а) дифузне відбиття світла; б) ілюстрація розсіяного та дзеркального відбивання, [16], [17]

Дифузне відбиття пояснюється розсіянням світла на нерівностях поверхні, і є протилежним процесом до дзеркального відбиття. Поверхні, для яких властиве дифузне відбиття, називаються матовими. Поверхня, яка розсіює світло рівномірно у всі напрямки називається абсолютно матовою. Концепція дифузного відбиття світла використовується у тривимірній графіці для створення враження просторовості об’єкта. На відміну від дзеркального, дифузне відбивання відбиває промені не прямолінійно (як при дзеркальному), а розсіяного. Отже, причина загасання – це розсіювання світла, створеного внутрішніми поверхнями та границями розділу речовин. У кристалічних матеріалах, таких як метали та кераміка, на додаток до пор на внутрішніх поверхнях та границях розділу, існують також нерегулярності у вигляді гранул. Будова будь-якого оптично прозорого пристрою потребує вибору матеріалів, обґрунтованого на основі знань їх потенційних обмежень. Вони є результатом інтерактивного співвідношення руху термічно збудженої множини атомів чи молекул тіла та падаючого світлового випромінювання.

Звідси, всі матеріали обмежені поглинанням спричиненим атомними та молекулярними коливаннями. Таким чином, мультифононне розсіювання проявляється, коли два чи більше фонони одночасно діють, продукуючи електричний дипольний момент, який взаємодіє із падаючою променистою радіацією.

З аналітичного огляду можна зробити висновки, що для організації оптоволоконної мережі варто використати наступне обладнання, що впорядковується стандартам TIA/EIA-568. Вибіркове поглинання інфрачервоного світла певним матеріалом проявляється завдяки збігу деякої складової частоти загальної спектральної смуги світла із частотою коливань елементів кристалічної решітки чи молекулярної структури тіла. Оскільки їм притаманна розмаїта природна частота коливань, то звідси походить селективна здатність поглинати різну променисту енергію, або фрагмент спектра.

РОЗДІЛ 2
МЕТОДИ ПОБУДОВИ І АДМІНІСТРУВАННЯ МЕРЕЖІ

2.1 Послідовність побудови мережі

Послідовність і структура побудови локальної мережі може змінюватися в залежності від конкретних вимог і масштабу мережі. Однак ось загальний опис кроків, пов’язаних зі створенням локальної мережі:

Планування та дизайн. Визначивши вимоги до мережі, відзначу цілі та вимоги локальної мережі, такі як кількість користувачів, типи пристроїв, очікуваний обсяг трафіку та бажані мережеві послуги. Здійснивши вибір топології мережі, до прикладу як топологія зірки (поширена в невеликих мережах) або комбінація топології зірки та шини. Перейшовши до планування та створення таблиці IP-адресації, включаючи підмережі та діапазони адресації для різних сегментів мережі.

Вибір апаратного та програмного забезпечення припадає на необхідні мережеві пристрої (маршрутизатор, комутатор, модем, бездротова точка доступу) і програмні рішення (операційні системи, засоби керування мережею), які відповідають вимогам мережі. Встановлюю мережеві кабелі, наприклад кабелі Ethernet або оптоволоконні кабелі, для підключення мережевих пристроїв. Продумавши розташування приладів і планування приміщень.

Встановлення мережевого обладнання фізично встановивши пристрої у відповідних місцях у приміщеннях, наприклад у серверних кімнатах, мережевих шафах або настінних кріпленнях. Конфігурація пристрою полягає в налаштуванні з відповідними параметрами, включаючи IP-адреси, маски підмережі, шлюзи за замовчуванням і параметри безпеки.

Підключення до мережеві пристрої за допомогою відповідного кабелю та налаштуйте їх для підключення до мережі. Це включає налаштування VLAN, транкінгу та маршрутизації, якщо необхідно.

У разі розгортання бездротової мережі налаштуймо точки бездротового доступу (WAP) за допомогою SSID, параметрів безпеки (WPA2, шифрування) і відповідних каналів.

Налаштування серверу DHCP для динамічного призначення IP-адрес пристроям у мережі, забезпечуючи ефективне керування адресами. А також DNS-сервер, щоб увімкнути розпізнавання імен і надавати служби доменних імен для пристроїв у мережі. Налагодження служби спільного доступу до файлів і принтера, щоб забезпечити легкий обмін файлами та ресурсами друку в мережі.

Щодо реалізації безпеки, то тут можливі такі етапи. Контроль доступу. На цьому етапі запроваджуються заходи безпеки, такі як списки контролю доступу (ACL), правила брандмауера та сегментація мережі, щоб контролювати доступ до мережі та захистити від несанкціонованого доступу. Для цього потрібно налаштувати механізми шифрування (WPA2, VPN) та автентифікації (паролі, сертифікати) для захисту бездротового та віддаленого доступу до мережі. Моніторинг мережі. Впроваджує в себе інструменти, щоб виявляти загрози безпеці та реагувати на них, контролювати продуктивність мережі та виявляти будь-які аномалії чи проблеми. Тестування мережі включає в себе ретельне тестування мережі, щоб переконатися в з’єднанні, належній конфігурації та продуктивності. Це включає перевірку з’єднання між пристроями, тестування мережевих служб і імітацію навантаження на трафік. Оптимізація та точне налаштування аналізує продуктивність мережі, виявляйте та вирішуйте будь-які вузькі місця та оптимізуйте конфігурацію мережі для підвищення ефективності та надійності. Мережева документація: створює детальну документацію про проект мережі, параметри конфігурації, схему IP-адресації, мережеві служби та будь-які конкретні мережеві політики чи процедури. Поточне технічне обслуговування регулярно відстежує та обслуговуйте мережеву інфраструктуру, застосовуйте оновлення та виправлення, а також виконуйте періодичні перевірки безпеки та оцінки продуктивності мережі.

Це включає керування призначенням IP-адрес, дотримання гарантій на обладнання та забезпечення резервного копіювання критично важливих мережевих ресурсів. Пам’ятаймо, що фактична реалізація може відрізнятися залежно від таких факторів, як розмір мережі, складність необхідних мережевих служб і конкретне обладнання та програмне забезпечення, що використовується.

Проаналізувавши дослідження [8-11], можна дійти висновку що співпраця з мережевими професіоналами та дотримання найкращих практик можуть допомогти забезпечити успішний проект побудови локальної мережі.

2.2 Адміністрування мережі. Протоколи DHCP, OSPF

Мережне адміністрування передбачає управління та експлуатацію комп’ютерних мереж в організації. Він включає в себе широкий спектр завдань і обов’язків для забезпечення ефективного і безпечного функціонування мережі. Адміністратори мережі відповідають за проектування та планування мережевої інфраструктури організації. Це включає визначення топології мережі, вибір апаратних і програмних компонентів і врахування таких факторів, як масштабованість, надійність і безпека. Контролюють встановлення та налаштування мережевих пристроїв, таких як маршрутизатори, комутатори, брандмауери та точки бездротового доступу. Вони гарантують, що пристрої правильно підключені, адресують IP-адреси та підмережі, налаштовують мережеві протоколи та встановлюють мережеві служби.

До адміністрування також можна віднести продуктивність мережі, виявляючи та вирішуючи проблеми, які можуть вплинути на її роботу. Адміністратори використовують інструменти моніторингу мережі для відстеження мережевого трафіку, використання пропускної здатності, затримки та інших показників продуктивності. Безпека мережі відіграє вирішальну роль у підтримці безпеки мережі. Заходи безпеки, як брандмауери, списки контролю

доступу, системи виявлення та запобігання вторгненням, а також віртуальні приватні мережі (VPN). Встановлення політики безпеки, виконуючи оцінку вразливості та проведення регулярних аудитів безпеки, щоб захистити мережу від несанкціонованого доступу, витоку даних та інших загроз безпеці.

Ось деякі з ключових протоколів, які використовуються в адмініструванні мережі. SNMP є широко використовуваним протоколом для керування та моніторингу мережі.

Це дозволяє збирати та керувати інформацією з мережевих пристроїв, таких як маршрутизатори, комутатори та сервери. SNMP дозволяє контролювати продуктивність пристрою, керувати конфігурацією та віддалене адміністрування пристрою. SSH – це криптографічний мережевий протокол, який забезпечує безпечний віддалений доступ до мережевих пристроїв. Це дозволяє встановлювати зашифровані з'єднання з такими пристроями, як маршрутизатори, комутатори та сервери. SSH забезпечує безпечний віддалений вхід, віддалене виконання команд і безпечну передачу файлів. Telnet – це протокол, який забезпечує віддалений доступ до пристроїв через мережу. Це дозволяє встановлювати текстовий сеанс із пристроями для конфігурації та керування. Однак Telnet не є безпечним, оскільки він передає дані у відкритому вигляді, тому замість нього рекомендується використовувати SSH. Протокол віддаленого робочого стола RDP – це власний протокол, розроблений корпорацією Майкрософт, який забезпечує віддалений доступ і керування системами на базі Windows. Це дозволяє дистанційно керувати та виправляти неполадки серверів і робочих столів Windows, надаючи графічний інтерфейс користувача (GUI) для віддаленого адміністрування. FTP – це стандартний мережевий протокол, який використовується для передачі файлів між системами через мережу. Він зазвичай використовується для оновлення програмного забезпечення, мікропрограми та передачі конфігураційних файлів. TFTP – це спрощена версія FTP, яка використовується для передачі легких файлів.

Він часто використовується для таких завдань, як оновлення мікропрограми на мережевих пристроях або передача конфігураційних файлів на мережеві пристрої під час початкового процесу налаштування. HTTP і HTTPS – це протоколи, які використовуються для веб-адміністрування та керування мережевими пристроями. Багато мережевих пристроїв мають вбудовані веб-сервери, які забезпечують графічний інтерфейс користувача (GUI) для налаштування та керування. HTTPS додає до HTTP функції шифрування та безпеки, що робить його більш безпечним варіантом для віддаленого керування.

VLAN означає віртуальну локальну мережу. Це спосіб логічного поділу однієї фізичної мережі на кілька віртуальних мереж. VLAN надають кілька переваг, зокрема покращену продуктивність мережі, покращену безпеку та спрощене керування мережею. Пристрої в одній VLAN можуть обмінюватися даними один з одним, якщо б вони були підключені до одного комутатора, навіть якщо вони фізично розташовані на різних комутаторах або сегментах мережі. Така сегментація підвищує безпеку та ефективність мережі. Розділивши мережу на VLAN, ви можете зменшити обсяг широкомовного трафіку, який повинен обробляти кожен пристрій. Трансляції обмежуються відповідними мережами VLAN, що запобігає переповненню всієї мережі та споживанню непотрібної пропускної здатності. VLAN забезпечують певний рівень безпеки мережі шляхом ізоляції різних груп користувачів або пристроїв один від одного. Списки контролю доступу (ACL) можна застосовувати до VLAN, дозволяючи адміністраторам мережі контролювати, які пристрої або користувачі можуть спілкуватися один з одним. Це допомагає запобігти несанкціонованому доступу та стримувати порушення безпеки.

VLAN часто асоціюються з тегами VLAN, які включають додавання ідентифікатора VLAN (VLAN ID) до кадрів Ethernet. Теги VLAN дозволяють комутаторам і мережевим пристроям визначати, до якої VLAN належить кадр,

навіть коли він переміщується різними сегментами мережі. Теги VLAN зазвичай реалізуються за допомогою таких стандартів, як IEEE 802.1Q.

Транкінг VLAN використовується для передачі кількох VLAN через одне мережеве з'єднання, як правило, між комутаторами або маршрутизаторами. Магістральні канали можуть транспортувати кадри з тегами VLAN, дозволяючи пристроям на різних комутаторах спілкуватися з пристроями в кількох VLAN.

VLAN зазвичай впроваджуються в корпоративних мережах, центрах обробки даних і великих мережевих інфраструктурах, де важливі сегментація, безпека та ефективне використання ресурсів також створення локальних мереж малопотужних підприємств, освітніх закладів, приватних користувачів є актуальним питанням навіть у наш час. Вони забезпечують гнучкість і масштабованість для проектування та адміністрування мережі, спрощуючи керування та покращуючи продуктивність мережі.

DHCP, що розшифровується як Dynamic Host Configuration Protocol, – це мережевий протокол, який використовується для автоматичного призначення IP-адрес і параметрів конфігурації мережі пристроям у мережі. Це спрощує процес керування IP-адресами шляхом динамічного розподілу IP-адрес, коли пристрої приєднуються до мережі або залишають її. DHCP Discover коли пристрій (відомий як клієнт DHCP) підключається до мережі, він надсилає повідомлення DHCP Discover, шукаючи IP-адресу. Сервер DHCP у мережі отримує повідомлення DHCP Discover і відповідає пропозицією DHCP. Пропозиція включає доступну IP-адресу з пулу адрес, а також іншу інформацію про конфігурацію мережі, таку як маска підмережі, шлюз за замовчуванням, DNS-сервер і тривалість оренди. Запит DHCP клієнт отримує кілька пропозицій DHCP (якщо в мережі є кілька серверів DHCP) і вибирає одну з них. Він надсилає повідомлення DHCP Request на вибраний сервер DHCP, приймаючи запропоновану IP-адресу. Підтвердження DHCP: після отримання запиту DHCP сервер DHCP резервує IP-адресу для клієнта та надсилає повідомлення підтвердження DHCP, підтверджуючи оренду IP-адреси та надаючи клієнту

інформацію про погоджену конфігурацію мережі. DHCP спрощує адміністрування мережі шляхом автоматизації призначення IP-адрес і параметрів конфігурації мережі. Це зменшує ймовірність конфліктів IP-адрес і полегшує ручне налаштування параметрів мережі на окремих пристроях.

Провівши дослідження [11], зроблено висновок, що DHCP, широко використовується в локальних мережах (LAN) і особливо цінний у великих мережах, де керування IP-адресами вручну було б недоцільним.

OSPF (Open Shortest Path First) – це протокол маршрутизації, який використовується в комп'ютерних мережах для визначення найбільш ефективних шляхів для переміщення пакетів даних між маршрутизаторами. Це протокол внутрішнього шлюзу (IGP), який працює в автономній системі (AS) для полегшення маршрутизації в межах однієї мережі чи організації. OSPF – це протокол стану зв'язку, який означає, що маршрутизатори обмінюються інформацією про свої безпосередньо під'єднані канали зв'язку, відомі як оголошення про стан зв'язку (LSA). Ця інформація містить відомості про стан і вартість посилань. OSPF використовує алгоритм Дейкстри для обчислення найкоротшого шляху до пункту призначення на основі інформації про стан зв'язку, отриманої від сусідніх маршрутизаторів. Щоб визначити найкращий шлях, він враховує такі фактори, як вартість зв'язку, перевантаження мережі та доступну пропускну здатність. OSPF дозволяє диференціювати трафік на основі вимог до типу послуги. Він підтримує використання значень Differentiated Services Code Point (DSCP) для визначення пріоритетів певних типів трафіку, забезпечуючи якість обслуговування (QoS) для додатків із певними вимогами.

OSPF розроблено для швидкої адаптації до змін у топології мережі, таких як збоїв зв'язку або доповнення. Він досягає швидкої конвергенції за допомогою таких методів, як поступове оновлення, активовані оновлення та мережева ієрархія, мінімізуючи вплив мережевих змін на передачу даних. Забезпечує механізми автентифікації для забезпечення цілісності та безпеки інформації про маршрутизацію.

Методи автентифікації включають просту автентифікацію на основі пароля та більш безпечні методи, такі як криптографічна автентифікація за допомогою цифрових сертифікатів.

OSPF широко використовується в корпоративних мережах, мережах інтернет-провайдерів (ISP) і великих мережах, де ефективна та надійна маршрутизація має вирішальне значення. Його особливості, такі як швидка конвергенція, масштабованість і підтримка QoS, роблять OSPF надійним і гнучким протоколом маршрутизації для ефективного управління мережевим трафіком.

2.3 Access-List та безпека мережі

Списки контролю доступу (ACL) використовуються для визначення набору правил, які визначають, чи дозволяти чи забороняти мережевий трафік на основі різних критеріїв. Корпоративні мережі адміністратори мереж звертаються до списку правил для керування доступом користувачів та груп до ресурсів мережі. Вони можуть обмежувати доступи до файлів, каталогів, регулювати можливість використання принтерів, електронної пошти, відвідувати веб-сайти тощо. ACL використовуються для керування доступом до різних частин баз даних, як-от таблиці, уявлення, процедури та тригери.

Застосовуються в маршрутизаторах, комутаторах та іншому мережному обладнанні для керування доступом до мережевих ресурсів, таких як порти, протоколи та сервіси. ACL, є потужною функцією Cisco Packet Tracer, яка дозволяє контролювати мережевий трафік шляхом фільтрації пакетів на основі певних критеріїв. Ось кілька поширених застосувань списків доступу в Cisco Packet Tracer.

Списки доступу можна використовувати для фільтрації мережевого трафіку на основі IP-адрес джерела та призначення, протоколів, номерів портів

або інших критеріїв. Розглянемо застосування списків доступу для керування трафіком SSH, HTTP та FTP у Cisco Packet Tracer:

Щоб дозволити SSH-трафік із певної вихідної IP-адреси, ми можемо створити правило списку доступу, яке дозволяє вхідний трафік на TCP-порт 22 (порт за замовчуванням для SSH) із потрібної вихідної IP-адреси.

Застосувавши цей список доступу до інтерфейсу, через який трафік SSH надходить у мережу. Відмова SSH, якщо плануємо заблокувати доступ SSH з певної IP-адреси, можемо створити правило списку доступу, яке забороняє вхідний трафік на TCP-порт 22 із цієї конкретної IP-адреси джерела. Застосувавши цей список доступу до інтерфейсу, ми запобігли підключенню SSH.

Щоб дозволити трафік HTTP, ми створимо правило списку доступу, яке дозволяє вхідний трафік на порт TCP 80 (порт за замовчуванням для HTTP). Після застосування даного списку доступу до інтерфейсу, через який HTTP-трафік надходить у мережу. Якщо бажаємо заблокувати доступ HTTP, тоді ми створимо правило списку доступу, яке забороняє вхідний трафік на порт TCP 80. Застосувавши цей список доступу до відповідного інтерфейсу, щоб запобігти з’єднанням HTTP.

Дозвіл FTP -трафік, потрібно враховувати як з’єднання для керування, так і для передачі даних. Створивши правила списку доступу, які дозволять вхідний трафік на TCP-порт 21 (порт контрольного з’єднання за замовчуванням) і динамічні порти (зазвичай у діапазоні 1024-65535) для з’єднань даних. Застосуймо ці списки доступу до відповідних інтерфейсів. Щоб заблокувати доступ до FTP, створимо правила списку доступу, які забороняють вхідний трафік на TCP-порт 21 (контрольне з’єднання) і динамічні порти для з’єднань даних. Застосуємо дані списки доступу до відповідних інтерфейсів, щоб запобігти підключенню FTP.

Списки доступу часто використовуються для забезпечення виконання політик безпеки в мережі. Це допомагає запобігти несанкціонованому доступу,

захистити конфіденційні дані та пом’якшити мережеві атаки. Списки доступу можна використовувати для класифікації та визначення пріоритетів мережевого трафіку для цілей QoS. Трансляція мережевих адрес (NAT) дозволяє кільком пристроям у приватній мережі спільно використовувати одну публічну IP-адресу. Списки доступу можна використовувати, щоб контролювати, яким пристроям або мережам дозволено використовувати NAT.

Списки доступу також можна використовувати для контролю рішень щодо маршрутизації. Фільтруючи оновлення маршрутизації за допомогою ACL, ми можемо визначити, які маршрути оголошуються або приймаються маршрутизаторами в мережі. Списки контролю доступу (ACL) можна класифікувати на два основні типи: стандартні ACL і розширені ACL. Дослідимо кожен тип докладніше.

Стандартні ACL фільтрують трафік лише на основі IP-адреси джерела. Вони не враховують IP-адресу призначення, протоколи чи порти. Стандартні ACL зазвичай використовуються, коли потрібно дозволити або заборонити трафік із певних джерел IP-адрес. Вони пронумеровані від 1 до 99 або від 1300 до 1999, залежно від платформи, приклад стандартного ACL зображено на рисунку 2.1. Це правило дозволяє весь трафік із вихідної мережі 192.168.1.0/24.

```
access-list 10 permit 192.168.1.0 0.0.0.255
```

Рисунок 2.1 – Приклад стандартного ACL

Розширені ACL забезпечують більш детальний контроль над мережевим трафіком, враховуючи численні фактори, такі як IP-адреси джерела та призначення, протоколи та номери портів. Вони забезпечують більш точну фільтрацію та зазвичай використовуються з метою безпеки. Розширені ACL мають номери від 100 до 199 або від 2000 до 2699, залежно від платформи приклад розширеного ACL зображено на рисунку 2.2.

Це правило дозволяє TCP-трафік із вихідної мережі 192.168.1.0/24 на будь-яку IP-адресу призначення на порту 80 (HTTP).

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80
```

Рисунок 2.2 – Приклад розширеного ACL

Важливо зауважити, що існують також іменовані списки керування доступом, які дозволяють призначати значущу назву списку керування доступом замість використання числового ідентифікатора. Іменовані ACL забезпечують легше керування та читабельність порівняно з пронумерованими ACL. Крім того, деякі мережеві пристрої підтримують ACL на основі часу, які дозволяють визначати правила доступу на основі певних часових діапазонів або розкладів.

Загалом, мережеве адміністрування включає нагляд за всіма аспектами роботи мережі, від проектування та впровадження до технічного обслуговування, безпеки та підтримки. Це вимагає глибокого розуміння мережевих принципів, протоколів і технологій, а також навичок вирішення проблем і спілкування.

РОЗДІЛ 3
РОЗРОБКА ЛОКАЛЬНОЇ МЕРЕЖІ
3.1 Конструювання плану будівлі в програмі Microsoft Visio

Побудову локальної мережі було розпочато з врахуванням конструктивних особливостей будівлі. Зокрема, враховано, що будинок склад з 2 поверхів, та 4-х кімнат., котрі застосовуються для мережевого користування. У процесі створення плану використано пакет ПЗ Microsoft Visio і спроектовано мережу. за рисунком 3.3. Розглянемо перший поверх згідно рисунка 3.1.

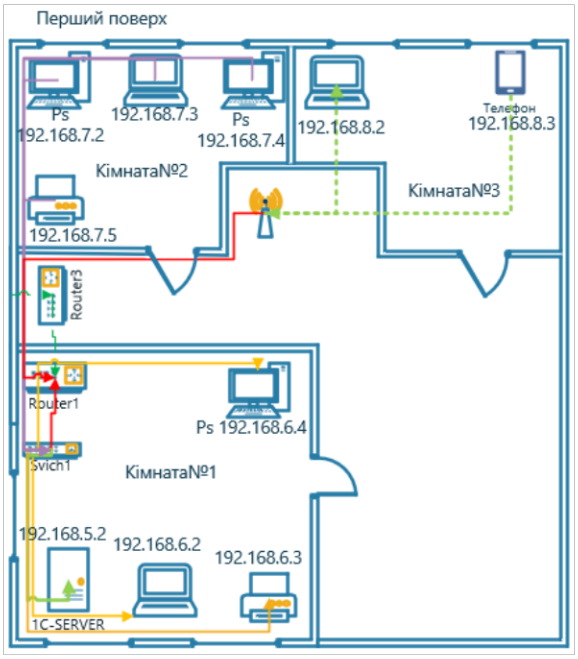


Рисунок 3.1 – План мережі першого поверху

Перший поверх включає у себе три кімнати .В першій та в другій кімнаті користувачі поділені на VLAN на окремі локальні мережі. А саме один VLAN на сервер, також VLAN на кімнату№1 та кімнату№2. А також для окремої групи користувачів, у кімнаті№3 для WiFi користуванням.Таким чином кімната№1 містить в собі дві робочі станції, принтер та окремо власний сервер баз даних. Кімната№2 містить три робочі станції, а також принтер.

Третя кімната розрахована на гостьових користувачів, котрі мають можливість під єднатися до безпровідної мережі. Розглянемо планування другого поверху за рисунком 3.2.

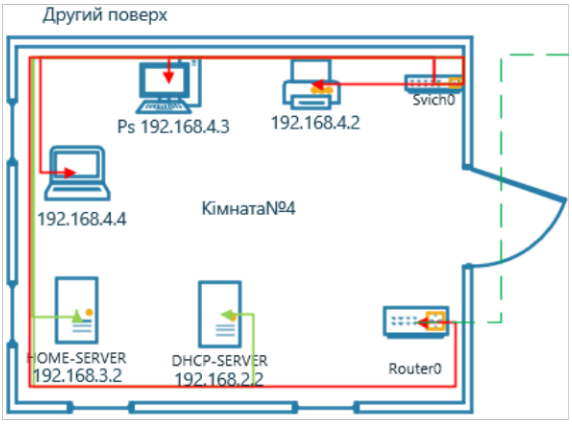


Рисунок 3.2 – план мережі другого поверху

Другий поверх (Рис. 3.3) включає у себе кімнату№4, у якій міститься дві робочі станції, один принтер, а також сервер для спільного користування HOME і сервер IP адресації DHCP, котрий надаватиме IP адресацію нашим локальним мережам.

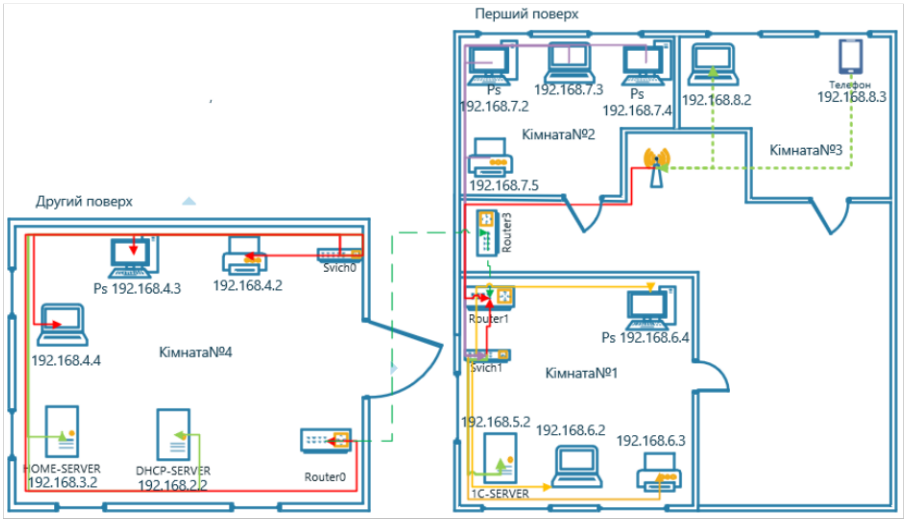


Рисунок 3.3 – План розміщення усієї мережі

Microsoft Visio використовується для створення діаграм, блок-схем, організаційних діаграм, мережевих діаграм, діаграм процесів та інших візуальних представлень інформації, а також для побудови мережних IT-схем.

Згідно з досліджень [12-15] при проектуванні та монтажі мережевих карт (Network Interface Cards, NICs) часто використовуються стандарти та рекомендації, які визначають правила та специфікації для цих пристроїв. Одним з основних стандартів для мережевих карт є Ethernet, який визначає методи передачі даних у локальних мережах. Найпоширеніші стандарти Ethernet включають 10BASE-T, 100BASE-TX, 1000BASE-T (Gigabit Ethernet) та 10GBASE-T (10 Gigabit Ethernet). Ці стандарти визначають характеристики фізичного підключення, швидкість передачі даних та інші технічні параметри.

Україна також має свої національні стандарти, включаючи Державні будівельні норми та правила (ДБН) та Державні стандарти України (ДСТУ), які регулюють проектування та монтаж мережевих систем, включаючи мережеві карти. Зокрема, ДСТУ 4093:2002 «Системи передачі та обробки інформації. Кабельні мережі зв’язку» містить вимоги та рекомендації щодо проектування кабельних мереж зв’язку, включаючи правила вибору та монтажу мережевих компонентів.

3.2 Налаштування IP адресації та параметрів безпеки мережі

Для налагодження безпеки мережі та налаштувань IP адресації була застосована програма для емуляцій та конструювань мереж Cisco Packet Tracer. В якій за допомогою проведених досліджень [8], були задіяні Access-List (ACL)та протоколи безпеки мережі NAT,OSPF. Дані протоколи були досліджені [9] та застосовані на практиці в проектуванні локальної мережі. Для безпеки локальної мережі, застосуємо поділ мережі на підмережі VLAN, завдяки поділу на підмережі надання IP адресації буде проведено набагато зручніше та точніше, дані IP адресів зазначено у таблиці 3.1.

Таблиця 3.1 – IP адресація першого поверху

Перший поверх	LAN	Інтерфейс	Pool / IP-адрес	Маска підмережі	Шлюз за замовчуванням
Кімната № 1	VLAN2	Fa 0/1.2	192.168.5.2	255.255.255.0	192.168.5.1 / 24
Кімната № 1	VLAN3	Fa 0/1.3	DHCP 192.168.6.0	255.255.255.0	192.168.6.1 / 24
Кімната № 2	VLAN4	Fa 0/1.4	DHCP 192.168.7.0	255.255.255.0	192.168.7.1 / 24
Кімната № 3	VLAN5	Fa 0/1.5	DHCP 192.168.8.0	255.255.255.0	192.168.8.1 / 24
Router1	-	Fa 0/0	192.168.10.2	255.255.255.252	-
Router1	-	Fa 0/1	192.168.10.2	255.255.255.252	-
Router3	-	Gi 0/1	192.168.10.1	255.255.255.252	-
Router3	-	Gi 0/2	192.168.20.1	255.255.255.252	-
Router3	-	Gi 0/0	210.214.1.2	255.255.255.252	-
Provider	-	Fa 0/0	210.214.1.1	255.255.255.252	-
Provider	-	Fa 0/1	210.214.2.1	255.255.255.252	-

Налаштувавши VLAN, а також DHCP SERVER, котрий генерував та видавав робочим станціям їхні IP адреси приклад наведено в рисунку 3.4. Застосовано протокол NAT, котрий надав змогу локальній мережі вихід у мережу Internet. В свою чергу було застосовано ACL для безпеки даної мережі.

Щоб захистити від зовнішнього вторгнення до локальної мережі, здійснено обмеження доступ на кінцевому шлюзі на Router3 . Тобто якщо Router буде атакований, він не змозі буде надати зловмиснику інформацію про присутні будь які мережі.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
VLAN7	192.168.7.1	8.8.8.8	192.168.7.0	255.255.255.0	255	0.0.0.0	0.0.0.0
VLAN6	192.168.6.1	8.8.8.8	192.168.6.0	255.255.255.0	255	0.0.0.0	0.0.0.0
VLAN4	192.168.4.1	8.8.8.8	192.168.4.0	255.255.255.0	255	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.2.0	255.255.255.0	255	0.0.0.0	0.0.0.0

Рисунок 3.4 – DHSP pool, адресація мереж на VLAN

Застосувавши ACL а саме стандартні протоколи адміністрування, обмежено доступ до DHSP, 1С серверів, для надійної безпеки мережі. Доступ до сервера 1С що розміщений на першому поверсі має дозвіл лише кімната№1, а

власне до DHCP серверу увесь другий поверх. IP адресація другого поверху зазначена в таблиці 3.2.

Таблиця 3.2 – IP адресація другого поверху

Другий поверх	LAN	Інтерфейс	Pool / IP-адрес	Маска підмережі	Шлюз за замовчуванням
Кімната № 4	VLAN2	Fa 0/1.2	192.168.2.2	255.255.255.0	192.168.2.1 / 24
Кімната № 4	VLAN3	Fa 0/1.3	192.168.3.2	255.255.255.0	192.168.3.1 / 24
Кімната № 4	VLAN4	Fa 0/1.4	DHSP 192.168.4.0	255.255.255.0	192.168.4.1 / 24
Router0	-	Fa 0/0	192.168.20.2	255.255.255.252	-
Router0	-	Fa 0/1	192.168.20.2	255.255.255.252	-

Симуляція пристроїв, надає широкий спектр мережевих пристроїв Cisco, які можна імітувати, включаючи маршрутизатори, комутатори, бездротові точки доступу, сервери та пристрої IoT. Протоколи та технології що були впроваджувані з різними мережевими протоколами та технологіями, такими як TCP/IP, протоколи маршрутизації (наприклад, OSPF, EIGRP), VLAN, NAT, DHCP, VPN тощо.

3.3 Проектування мережі в Cisco Packet Tracer

За спроектованою схемою будівлі у програмному забезпеченні Microsoft Visio, земулюємо розміщення кімнат, та поверхів мережі у Cisco Packet Tracer (рис. 3.5). Будівля містить в собі два поверхи: на першому розміщений інтернет провайдер, Swich, котрий підключає між собою дві кімнати, із окремими локальними мережами а саме кімнату№1 та кімнату№2. В яких розміщені принтери, станції обміну файловими пакетами, маршрутизатор, та сервер.

Додатково під’єднана точка доступу котра розміщена у кімнаті №3, для зручності гостьового користування.

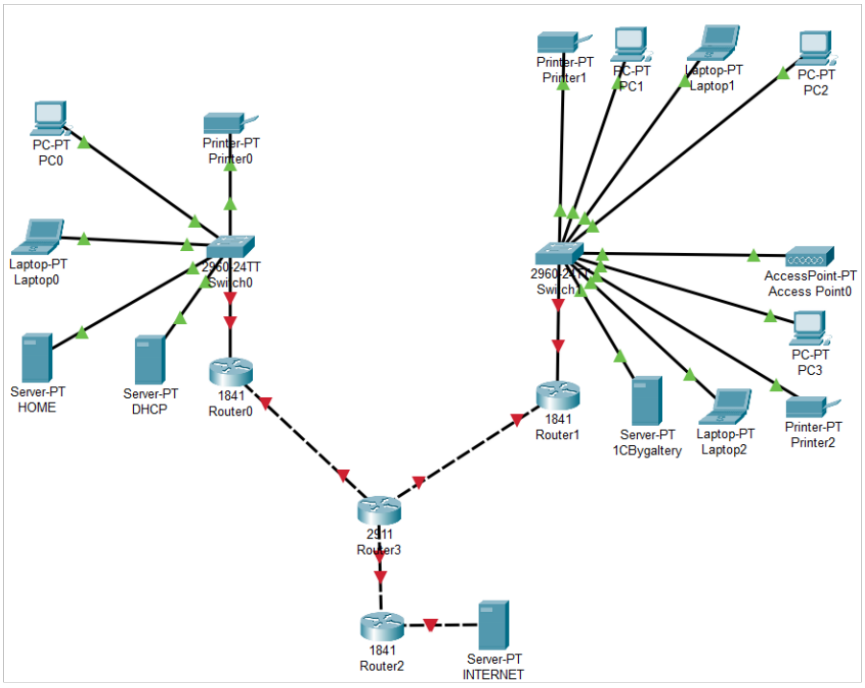


Рисунок 3.5 – Емуляція мережі будинку

Поділимо мережу на під мережі VLAN (рис. 3.6), здійснимо це за допомогою Swich, перейшовши в режим налаштування у терміналі.

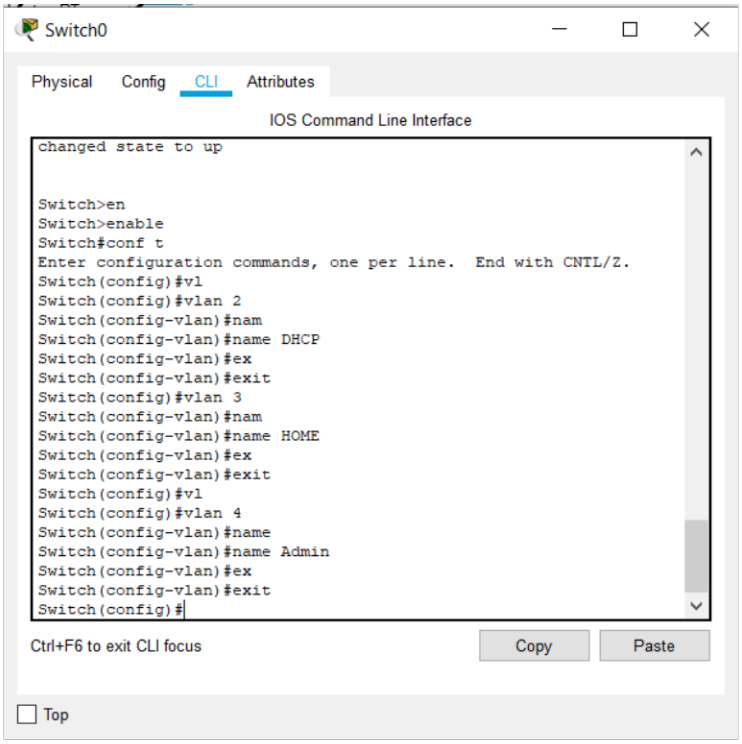


Рисунок 3.6 – Поділи мережі на VLAN

Задаємо налаштування командою *#vlan*, фіксуємо локальні підмережі та їх назви, і вслід за цим підключмо їхні порти адресації, наведено у лістингу 3.1.

Початок Лістинг 3.1

#interface fastEthernet 0/0

#switchport mode access

#switchport access vlan …

#no shutdown

Кінець Лістинг 3.1

За необхідності необхідно виділити декілька портів застосуємо команду, *#interface range fastEthernet 0/0-0.*

Тепер локальні мережі створені та підключені до своїх портів, створимо транковий порт для того, щоб маршрутизатор міг обмінювати інформацію а також файлові пакети між локальними мережами . За допомогою команди *#trung* налаштуємо Swich (рис. 3.7).

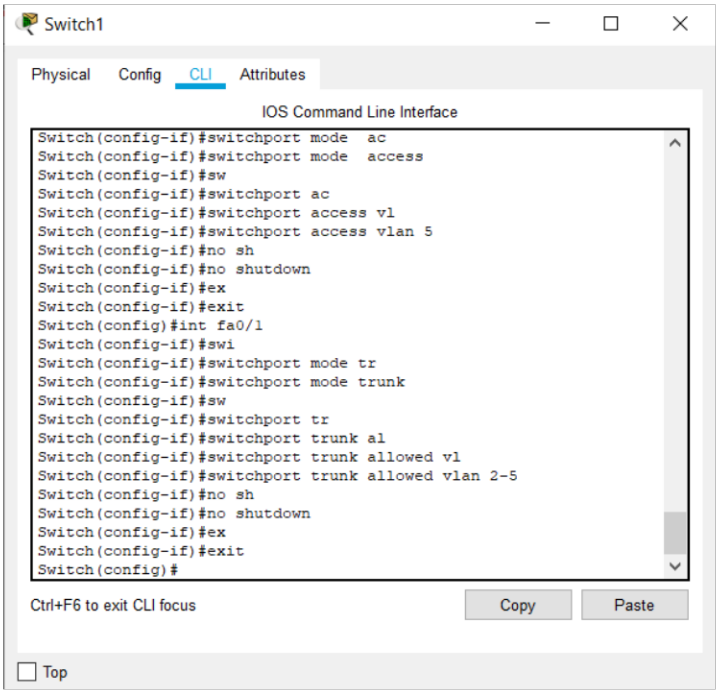


Рисунок 3.7 – Створення транкового порту

Тепер створимо на маршрутизаторах (в подальшому Router0/3) CAP інтерфейс для VLAN, застосуємо команду *#encapsulation dot1Q* та наддамо IP address для усіх VLAN. Для перевірки застосуємо команду *#show run* (рис. 3.8).

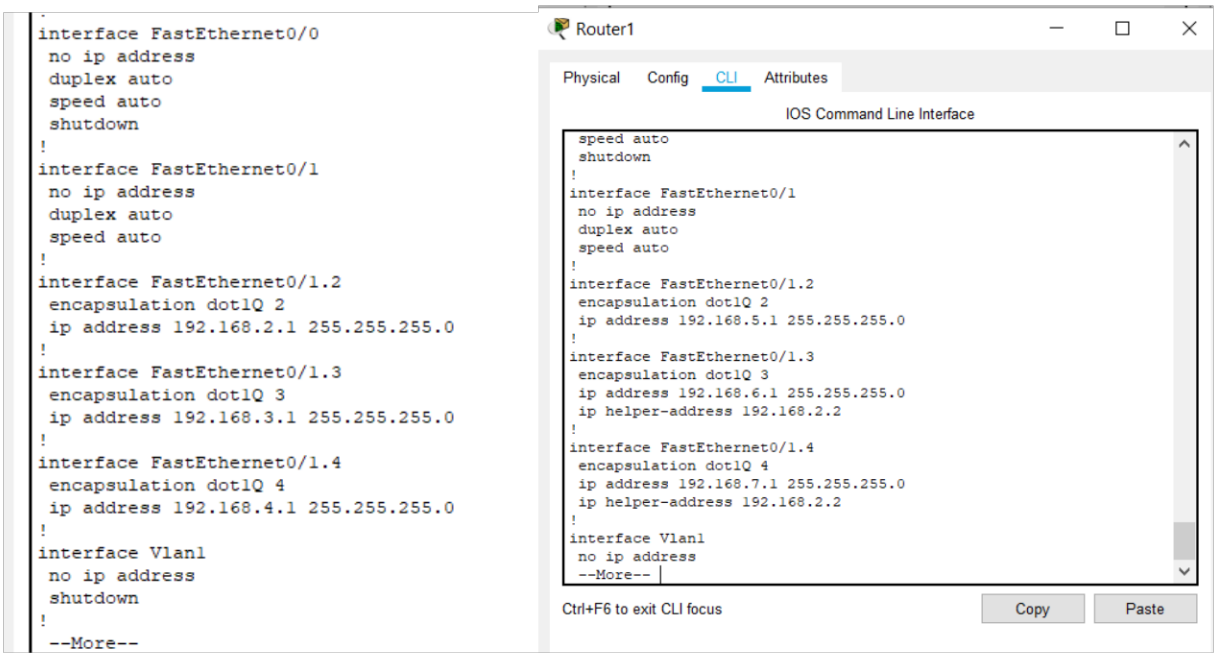


Рисунок 3.8 – Налаштування IP адресації для VLAN

Створено CAP Інтерфейси на обох поверхах. Створимо DHCP сервер, а саме присвоїмо статичну мережу за IP address 192.168.2.2. Відразу перевіримо ,чи DHCP сервер бачить Router0 .Для цього застосуємо команду *#ping* (рис. 3.9).

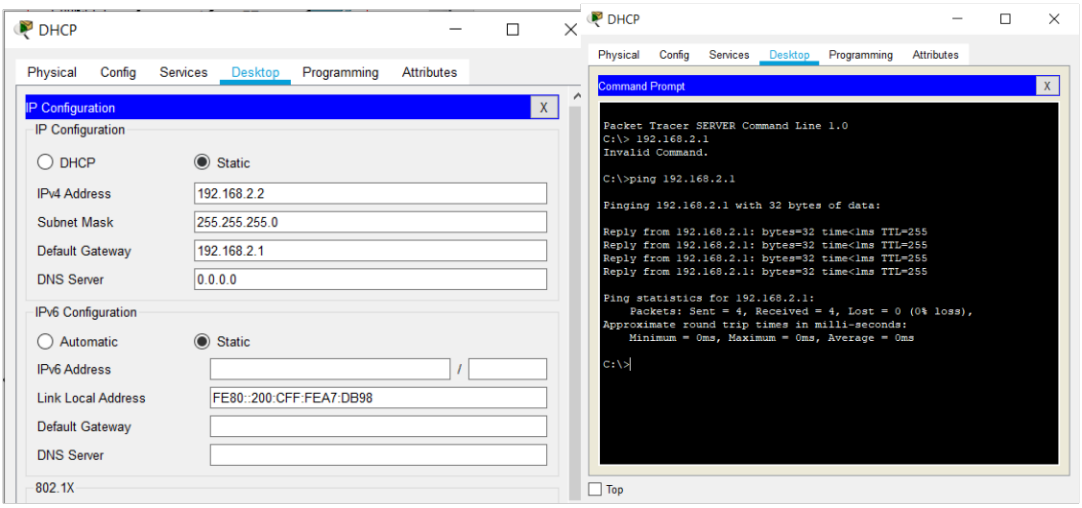


Рисунок 3.9 – Пінгування мережі

Створимо DHCP POOL для VLAN. Коли комп'ютер звертатиметься до DHCP серверу про надання йому IP address, DHCP POOL буде його видавати.

Для цього перейдімо в сам сервер в розділ Services та відкриємо розділ DHCP (рис. 3.10).

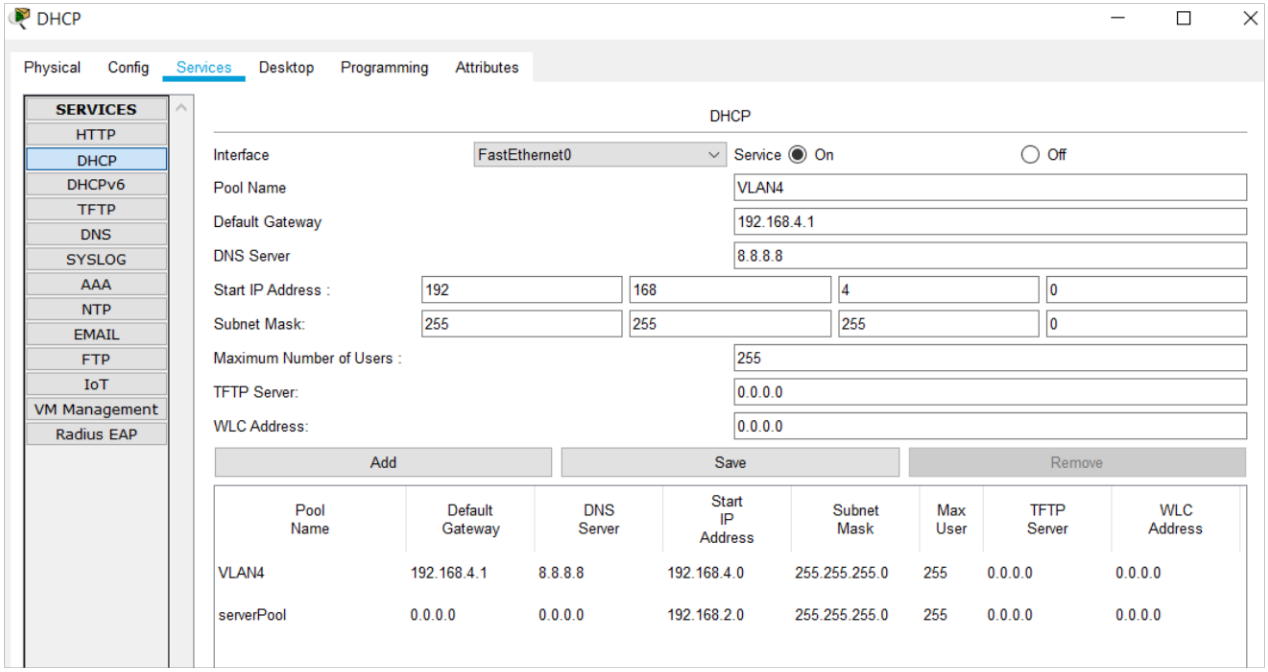


Рисунок 3.10 – Створення DHCP POOL

DHCP POOL готовий, але сервер підключаний у окремому сегменті, і станції його просто не будуть бачити, вони відправлятимуть запит на Router1 і не отримуватимуть відповіді. Тому, здійснимо перенаправлення DHCP запитів за допомогою команди *#Ip helper-addres* та вказуватимемо CAP інтерфейси (рис. 3.11).

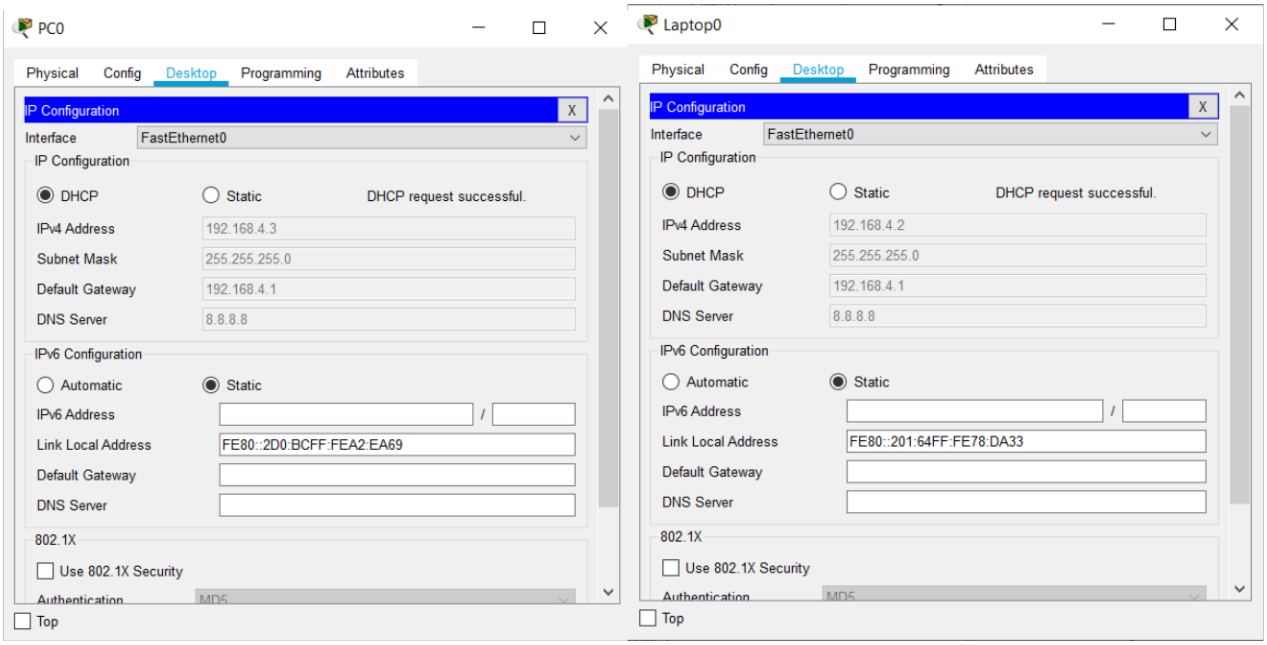


Рисунок 3.11 – Здійснення перенаправлення запитівDHCP

Другий поверх а саме кімната№4 отримала IP address, перейдемо до налагодження першого поверху будинку. Для цього створимо ще два DHCP POOL (рис. 3.12), а також відразу застосуємо перенаправлення запитів у Router1 командою *#Ip helper-addres* та зазначимо CAP інтерфейси.

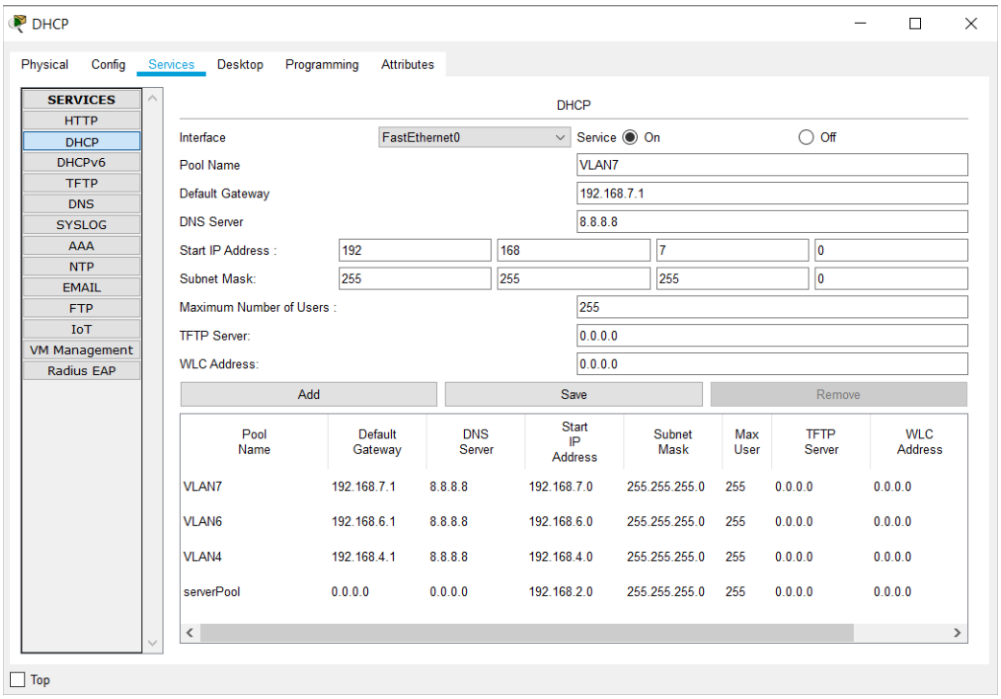


Рисунок 3.12 – Створення DHCP POOL

Створивши DHCP POOL та замінивши переадресацію у Router1, не дасть можливості під’єднання до DHCP POOL (рис. 3.13). Це пов’язано з відсутністю прямого під’єднання до Swich, DHCP сервер знаходиться на другому поверсі

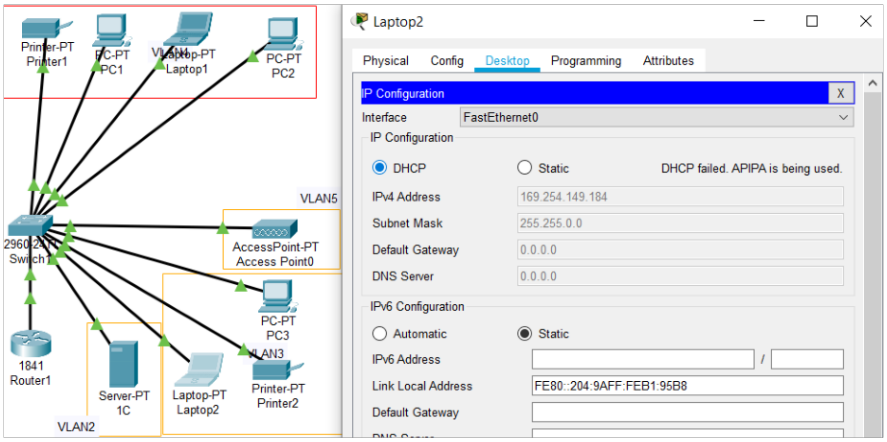


Рисунок 3.13 – Відсутність DHCP POOL

Для вирішення даної проблеми застосуємо протокол OSPF (рис. 3.14), даний протокол дасть можливість об’єднати між собою Router0/Router1, а маршрутизатори в свою чергу отримають доступити до обміну пакетів інформації, а також до комп’ютерів і серверів.

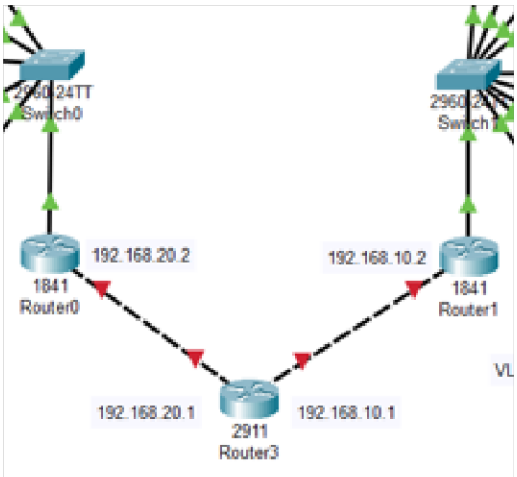


Рисунок 3.14 – Застосування протоколу OSPF

Для застосування протоколу OSPF потрібно задати IP address на Router0/Router3 (рис. 3.15), лістинг 3.2.

Початок Лістинг 3.2

Router1

#Int fa0/0

#ip add 192.168.10.2 255.255.255.255

#No shotdown

Router0

#Int fa0/0

#ip add 192.168.20.2 255.255.255.255

#No shotdown

Router3

#Int gi0/1

#ip add 192.168.10.1 255.255.255.255

#No shotdown

Кінець Лістинг 3.2

```
interface FastEthernet0/0
 ip address 192.168.10.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.12.1 255.255.255.0
!
interface FastEthernet0/1.3
 encapsulation dot1Q 3
 ip address 192.168.13.1 255.255.255.0
 ip helper-address 192.168.2.2
!
interface FastEthernet0/1.4
 encapsulation dot1Q 4
 ip address 192.168.14.1 255.255.255.0
 ip helper-address 192.168.2.2
!
```

```
interface FastEthernet0/0
 ip address 192.168.20.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/1.3
 encapsulation dot1Q 3
 ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/1.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
 ip helper-address 192.168.2.2
!
interface Vlan1
 --More--
```

Рисунок 3.15 – Надання Ip адресації для Router

Застосуємо протокол OSPF для початку налаштуємо Router0 (рис. 3.16), завдяки Loopback інтерфейсам, лістинг 3.3 з послідовністю команд.

Початок Лістинг 3.3

#int loopback 0

#ip add 192.168.100.1 255.255.255.255

#no shotdown

#exit

Кінець Лістинг 3.3

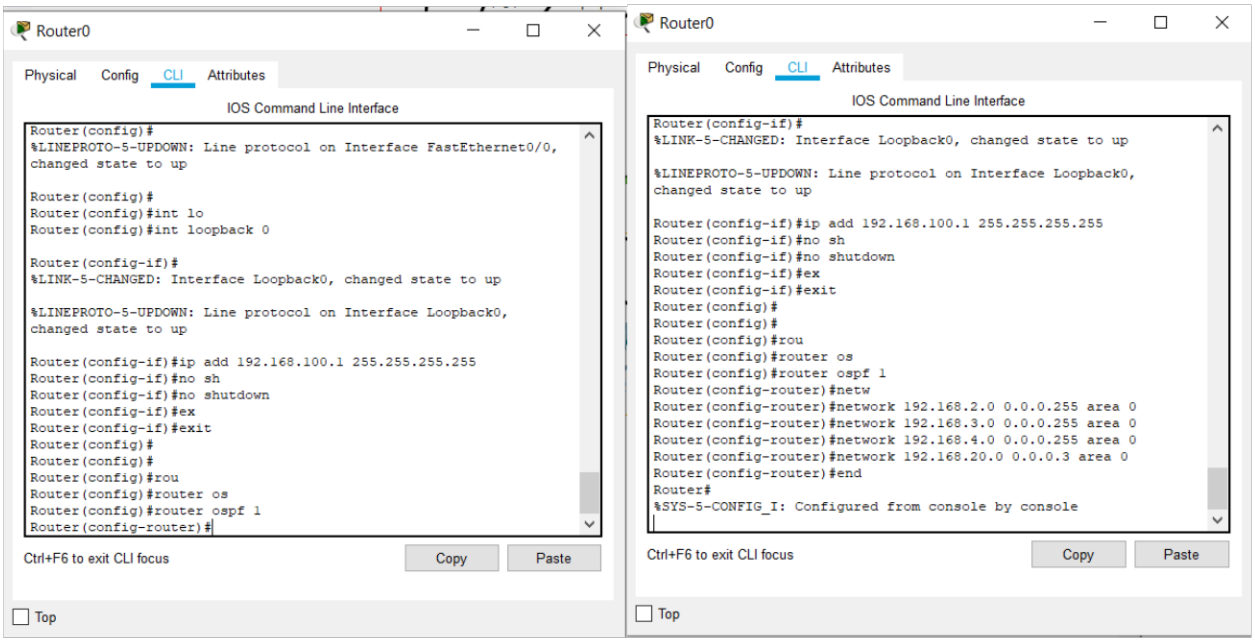


Рисунок 3.16 – Налаштування Loopback інтерфейсів

За допомогою команди *#network* (рис. 3.17), застосуймо анонсування мереж, це створить можливість розсилати оновлюючі пакети інформації. Підчас добавляння мереж не забуваймо про Wildcard mask (зеркальна маска Ip адресації). Налаштування наведенні у лістингу 3.4.

Початок Лістинг 3.4

Router0

#router ospf 1

#network 192.168.2.0 0.0.0.255 area 0

#network 192.168.3.0 0.0.0.255 area 0

#network 192.168.4.0 0.0.0.255 area 0

#network 192.168.20.0 0.0.0.3 area 0

#end

Router1

#router ospf 1

#network 192.168.5.0 0.0.0.255 area 0

#network 192.168.6.0 0.0.0.255 area 0

#network 192.168.7.0 0.0.0.255 area 0

#network 192.168.10.0 0.0.0.3 area 0

#end

Кінець Лістинг 3.4

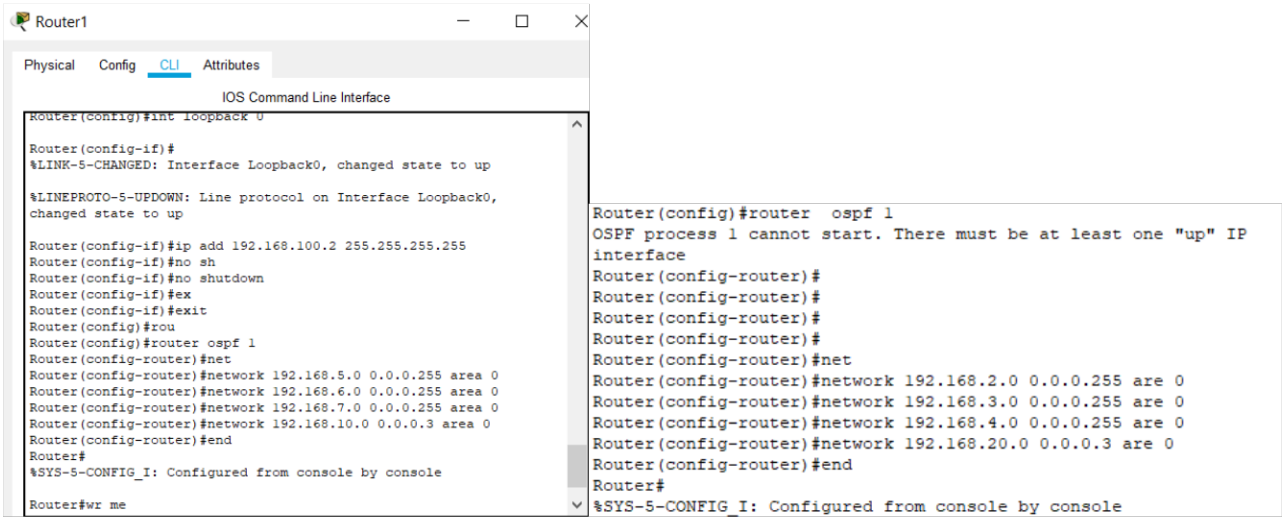


Рисунок 3.17 – Здійснення анонсування мережі

Завершимо налаштування OSPF інтерфейсу, а саме за допомогою Router3 (рис. 3.18), пов’яжемо між собою Router0, Router1, та Router3 в одну мережу, лістинг 3.5.

Початок Лістинг 3.5

Router3

#int loopback 0

#ip add 192.168.100.3 255.255.255.255

#no shotdown

#exit

#router ospf 1

#netwotk 192.168.10.0 0.0.0.3 area 0

#netwotk 192.168.20.0 0.0.0.3 area 0

#end

Кінець Лістинг 3.5

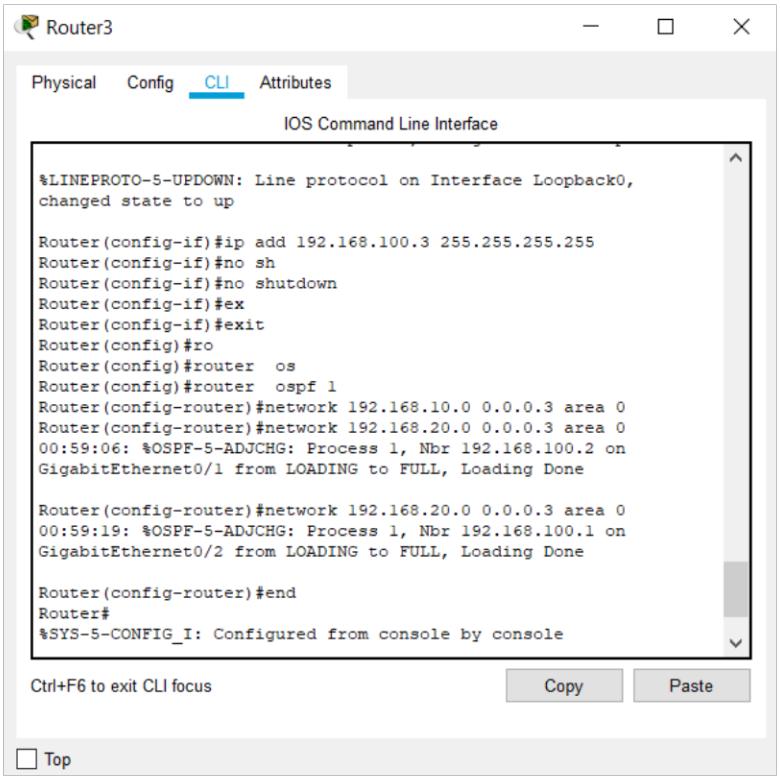


Рисунок 3.18 – Створення OSPF інтерфейсу

Здійснимо перевірку Router3, чи відображає сусідні Router0, Router1, котрі розміщені на різних поверхах будинку. Задля перевірки застосуємо команду : *#Show ip osof neighbor* (рис. 3.19).

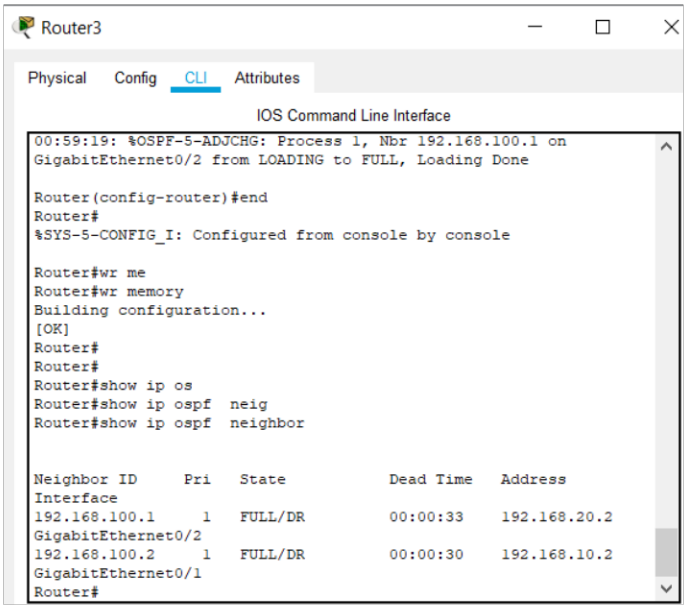


Рисунок 3.19 – Перевірка створення суцільної мережі OSPF

Здійснимо перевірку таблиці маршрутизації IP адресів Router3: *#Show ip route* (рис. 3.20).

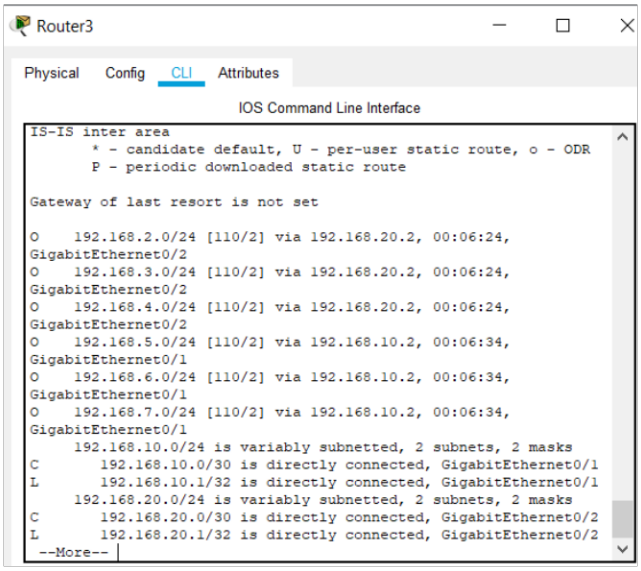


Рисунок 3.20 – Перевірка таблиць маршрутизації IP адресів Router3

Результат таблиці IP адресації показав, що наявні усі мережі будинку. Здійснимо аналогічну перевірку таблиць маршрутизації IP адресів для Router0, Router1 (рис. 3.21).

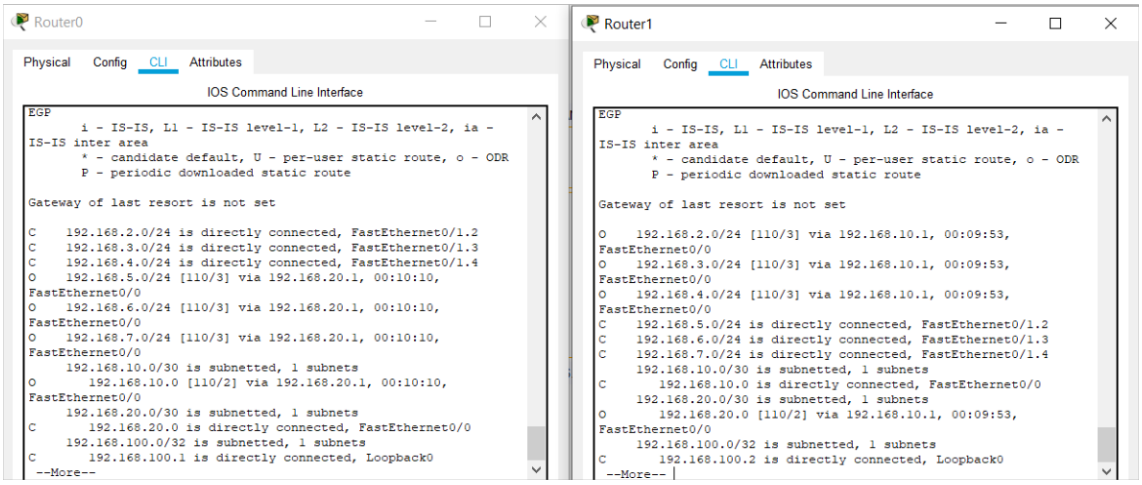


Рисунок 3.21 – Перевірка таблиць маршрутизації IP адресів Route0/Router1

Перевіримо під’єднання першого поверху, а саме кімнату№1, та кімнату№2 на отримання Ip адресу від DHCP POOL (рис. 3.22). Станції отримали власні Ip адреса, тепер вони пов’язані між собою в одній мережі.

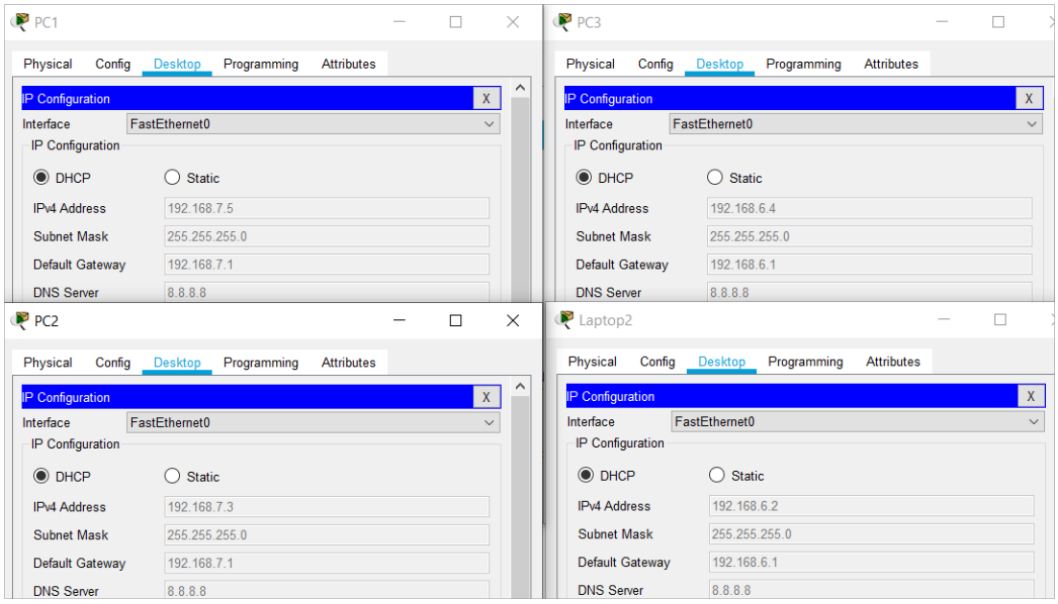


Рисунок 3.22 – Перевірка під’єднання DHCP

Перейдімо до налаштувань серверів, а саме Home, 1C (рис. 3.23). Надамо статичні IP адреси для них.

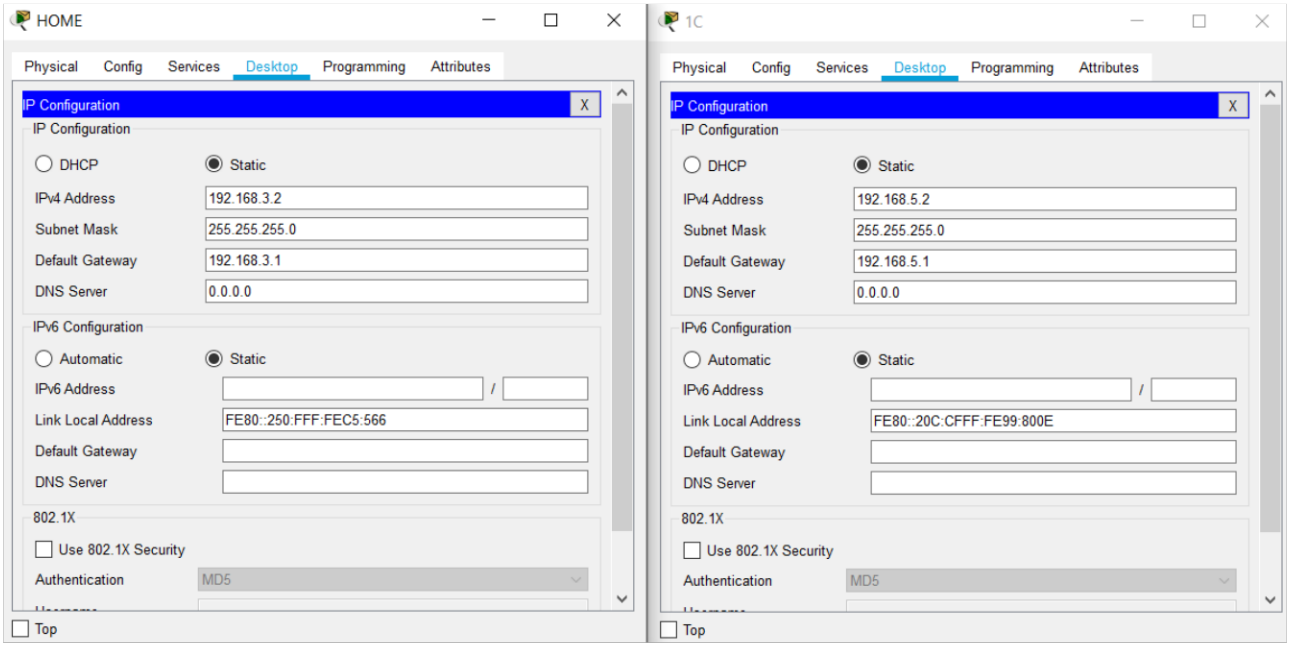


Рисунок 3.23 – Надання Ip адресації серверам

Здійснимо перевірку обміну файлових пакетів із серверами Home, 1C(рис. 3.24), задіявши команду: *#ping*.

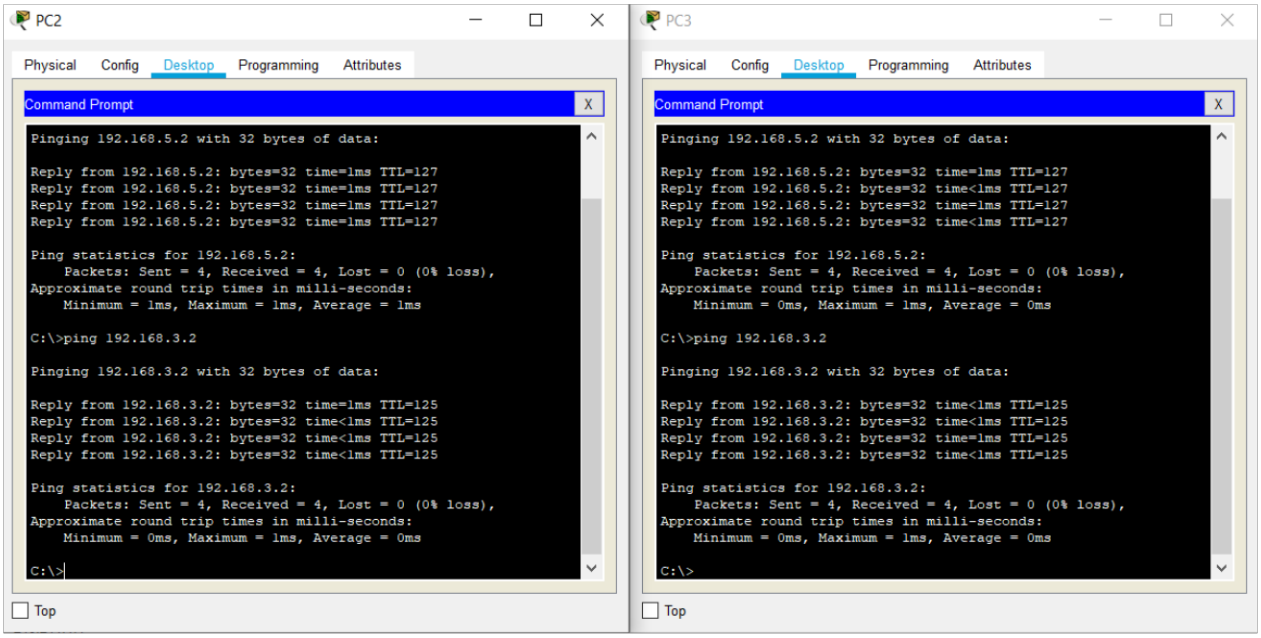


Рисунок 3.24 – Обмін пакетів інформації із серверам

Застосуємо досліджений протокол NAT. А саме налаштуємо підключення нашої локальної мережі до провайдера інтернету (рис. 3.25).

Даний протокол переадресовує сірі адреса у білі для можливості виходу у інтернет. Наддамо IP address для сервера інтернету, та маршрутизатора провайдера(В подальшому Provider), для них будуть білі IP адреса. Здійснимо з'єднання із Router3.

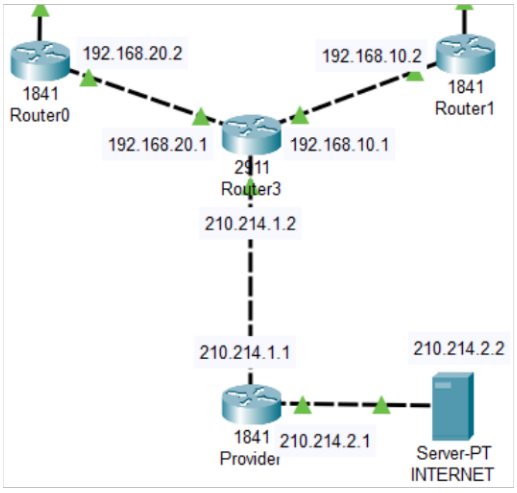


Рисунок 3.25 – З'єднання із провайдером інтернету

Здійсним налаштування шлюзу за замовчуванням або *Default gateway*. Задаймо кінцевий маршрут командою: *#ip route 0.0.0.0 0.0.0.0 210.214.1.1*, на Router3 (рис. 3.26).

```
Router>en
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#ip rou
Router(config)#ip rout
Router(config)#ip ro
Router(config)#ip r
Router(config)#ip r?
route  routing
Router(config)#ip r?
route  routing
Router(config)#ip route 0.0.0.0 0.0.0.0 210.214.1.1
Router(config)#
```

Рисунок 3.26 – Налаштування шлюзу

Повідомимо маршрутизатори про створення ,шлюзу кінцевого маршруту (рис. 3.27).

```
Router(config)#router  os
Router(config)#router  ospf 1
Router(config-router)#
Router(config-router)#dea
Router(config-router)#de
Router(config-router)#default-information or
Router(config-router)#default-information originate
Router(config-router)#
Router(config-router)#
Router(config-router)#
Router(config-router)#
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.27 – Повідомлення створення шлюзу

Створивши та сповістивши про наявність Default маршруту, перейдемо до налагодження NAT. А саме визначимо *inside* (внутрішній) та *outside* (зовнішний) інтерфейси ,на які буде здійснюватися вхід та вихід в мережу Internet (рис. 3.28).

Physical Config CLI Attributes

IOS Command Line Interface

```
% Invalid input detected at '^' marker.

Router(config)#
Router(config)#ip nat
Router(config)#ip nat ou
Router(config)#ip nat outside
% Incomplete command.
Router(config)#int gi0/0
Router(config-if)#ip na
Router(config-if)#ip nat o
Router(config-if)#ip nat outside
Router(config-if)#ex
Router(config-if)#exit
Router(config)#int gi 0/1
Router(config-if)#ip nat
Router(config-if)#ip nat in
Router(config-if)#ip nat inside
Router(config-if)#ex
Router(config-if)#exit
Router(config)#int gi0/2
Router(config-if)#ip na
Router(config-if)#ip nat in
Router(config-if)#ip nat inside
Router(config-if)#ex
```

Рисунок 3.28 – Налаштування інтерфейсів

Створимо стандартний Access-list, та використаєм команду *#permit* яка надає доступ до перелічених мереж (рис. 3.29).

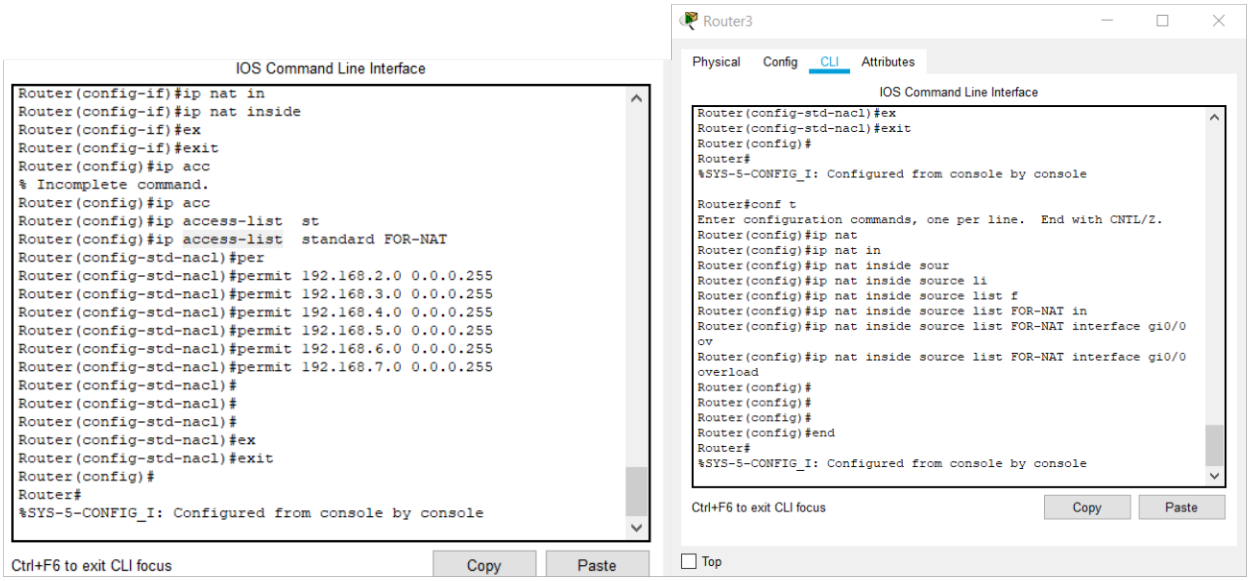


Рисунок 3.29 – Створення стандартного ACL list

Здійсним перевірку з’єднання із сервером інтернет провайдера застосувавши команду *#ping* (рис. 3.31).

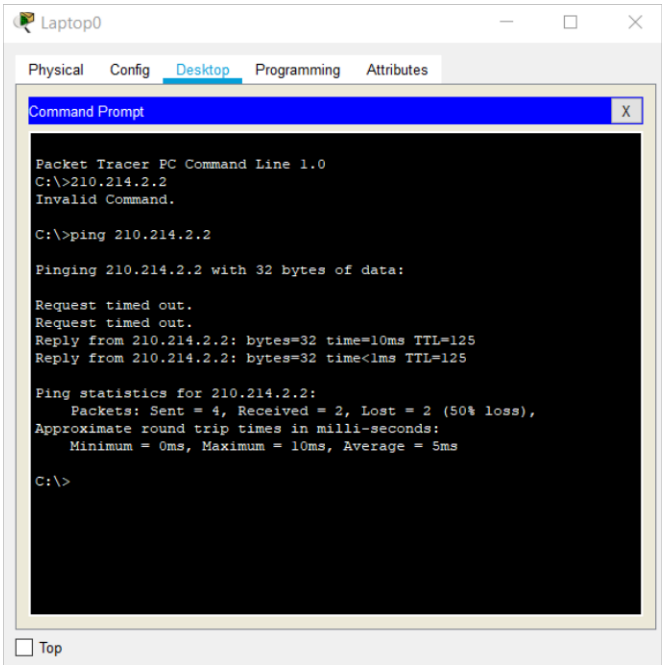


Рисунок 3.30 – Пінгування Internet

Застосуємо Access-List, для захисту мережі від атак через інтернет провайдера, для цього налаштуємо Access-List на Router3 (рис. 3.31). Дамо йому назву FROM-OUTSIDE в даному Access-List перелічимо всі локальні мережі крім, мережі 1С, та DHCP, задля кращої безпеки. Командою *#Router(config) #ip access-list extended – задамо розширений Access-List*.

```
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip acc
Router(config)#ip access-list  ex
Router(config)#ip access-list  extended FROM-OUTSIDE
Router(config-ext-nacl)#den
Router(config-ext-nacl)#deny ip any 192.168.3.0 0.0.0.255
Router(config-ext-nacl)#deny ip any 192.168.4.0 0.0.0.255
Router(config-ext-nacl)#deny ip any 192.168.6.0 0.0.0.255
Router(config-ext-nacl)#deny ip any 192.168.7.0 0.0.0.255
Router(config-ext-nacl)#
```

Рисунок 3.31 – Створення розширеного ACL list для безпеки

Створивши розширений ACL, якій містить команду *#deny ip any.* Тепер даний Access-List потрібно прив’язати до внутрішнього інтерфейсу на вхідний трафік командою: *#ip access-group FROM- OUTSIDE in* (рис. 3.32).

```
Router(config-ext-nacl)#exit
Router(config)#int gi0/0
Router(config-if)#ip acc
Router(config-if)#ip access-group FROM-OUTSIDE in
Router(config-if)#
Router(config-if)#
Router(config-if)#
```

Рисунок 3.32 – Прив’язання до інтерфейсу ACL list

Перевіримо даний трафік чи можемо з Provider, пропінгувати внутрішню мережу застосувавши команду: *#ping* (рис. 3.33).

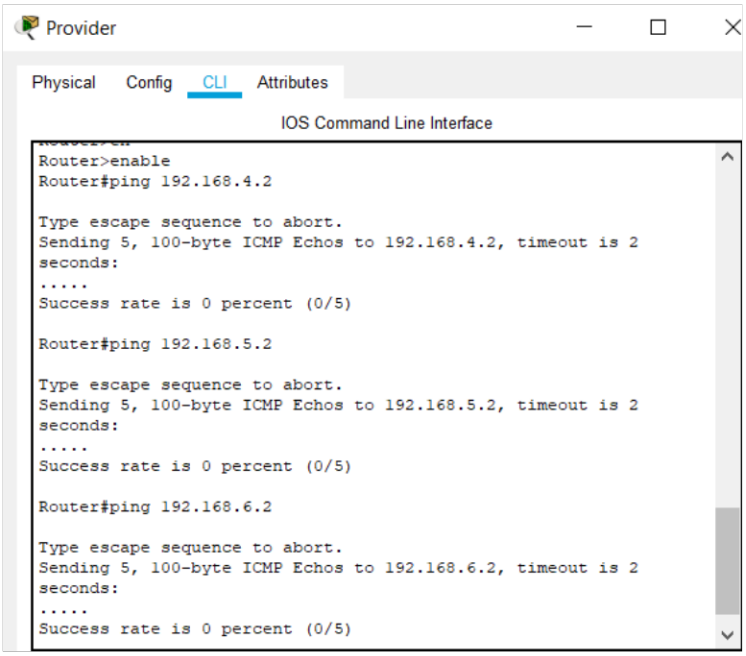


Рисунок 3.33 – Пінгування локальної мережі

Зовні не можемо побачити користувачів локальної мережі. Перевіримо доступ у саму мережу Internet через наші станції (рис. 3.34).

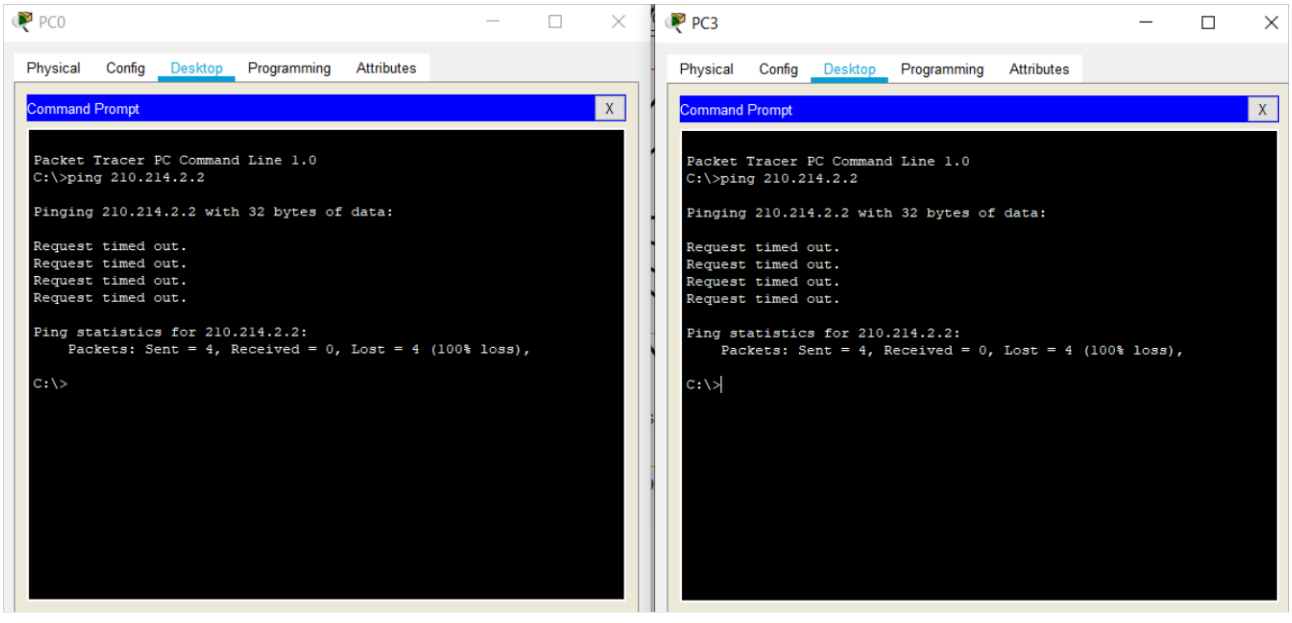


Рисунок 3.34 – Пінгування Internet

Користувачі будинку не бачать доступу до інтернету. А це пояснюється тим, що за замовчуванням у кінці любого ACL стоїть правило *#Deny ip any any*.

Дане правило увесь трафік мережі, відкриємо доступ до Internet для користувачів будинку (рис. 3.35), застосувавши команду: *#permit ip any host* .

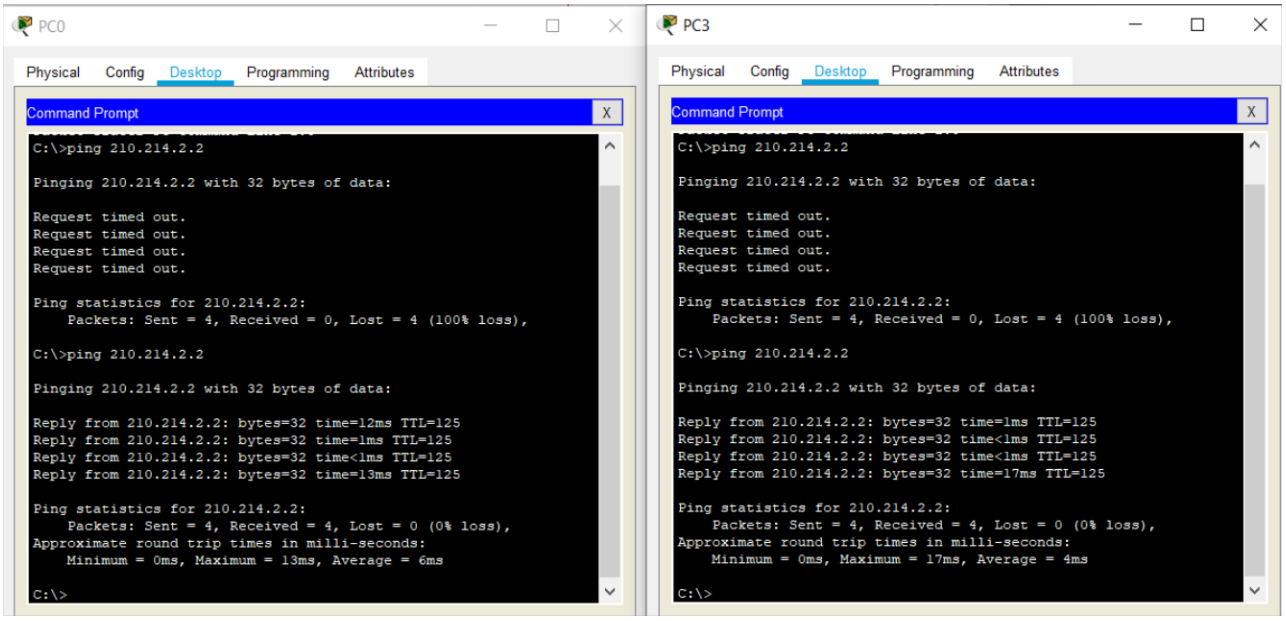


Рисунок 3.35 – Надання доступу до Internet

Переглянувши ACL, то зазначимо що вони створені недоречно, тому що пам’ятаємо що в кінці кожного Access-List присутнє правило *#Deny ip any any*, яке забороняє увесь трафік. Набагато простіше заборонити один ACL, а решта, буде заборонена за замовчуванням . Здійснимо спрощення ACL (рис. 3.36).

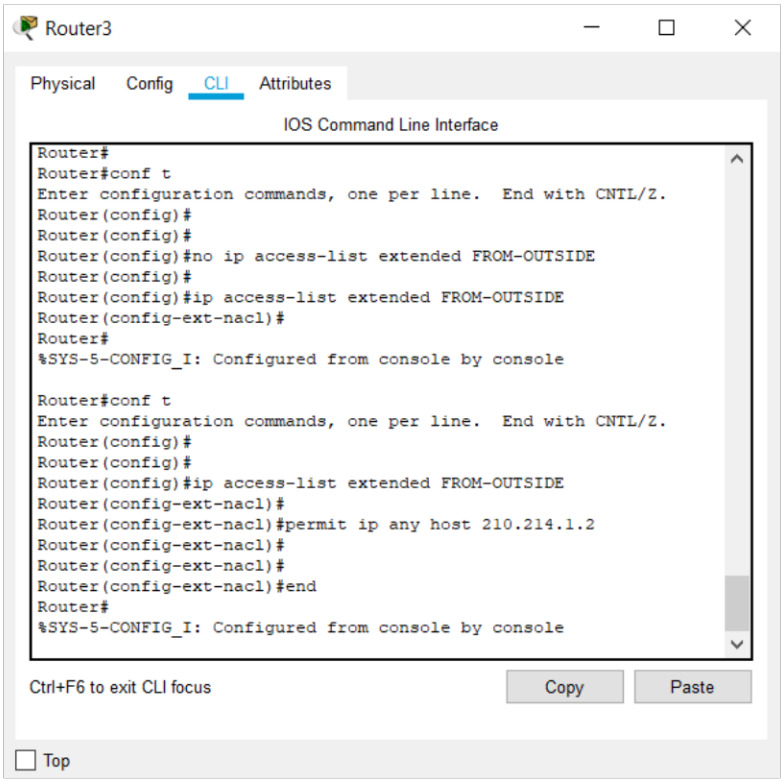


Рисунок 3.36 – Спрощення ACL list

Налаштуємо стандартні ACL, а саме наддамо доступ до сервера 1С, лише кімнаті№1 (рис. 3.37). Та прив’яжемо даний ACL до інтерфейсу Router1.

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip acc
Router(config)#ip access-list st
Router(config)#ip access-list standard TO-1C
Router(config-std-nacl)#per
Router(config-std-nacl)#permit 192.168.6.0 0.0.0.255
Router(config-std-nacl)#ex
Router(config-std-nacl)#exit
Router(config)#int fa0/1.2
Router(config-subif)#ip acc
Router(config-subif)#ip access-group TO-1C ou
Router(config-subif)#ip access-group TO-1C out
Router(config-subif)#ex
Router(config-subif)#exit
Router(config)#ex
Router(config)#exit
Router#
```

Рисунок 3.37 – Створено стандартний ACL для 1С

Аналогічно налаштуємо ACL для DHCP-SRVER (рис. 3.38).

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip acc
Router(config)#ip access-list st
Router(config)#ip access-list standard TO-DHCP
Router(config-std-nacl)#per
Router(config-std-nacl)#permit ip 192.168.4.0 0.0.0.255
                               ^
% Invalid input detected at '^' marker.

Router(config-std-nacl)#permit 192.168.4.0 0.0.0.255
Router(config-std-nacl)#ex
Router(config-std-nacl)#exit
Router(config)#int fa0/1.2
Router(config-subif)#ip acc
Router(config-subif)#ip access-group TO-DHCP ou
Router(config-subif)#ip access-group TO-DHCP out
Router(config-subif)#exit
Router(config-subif)#exit
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.38 – Створено стандартний ACL для DHSP

Налаштуємо безпровідну мережу WiFi. Під’єднаємо її до Swich, підключимо до інтерфейсів (рис. 3.39).

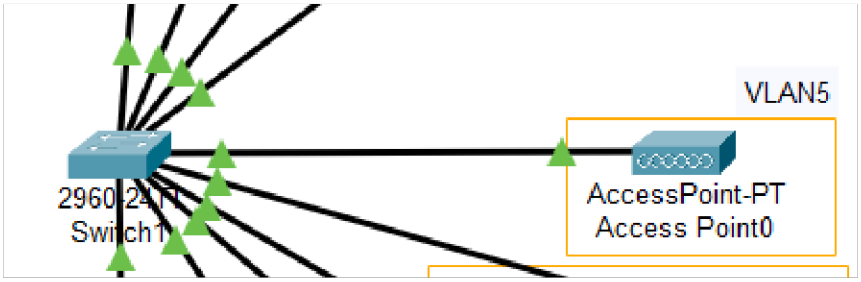


Рисунок 3.39 – Підключення WiFi

Налаштуємо точку доступу, задаймо ім’я нашої безпровідної мережі, тип безпечної передачі мережі, та пароль *ciskocisko*. Створимо CAP Interfaise на Router1 (рис. 3.40), для нашої точки доступу, наддамо IP addres 192.168.8.1 /24.

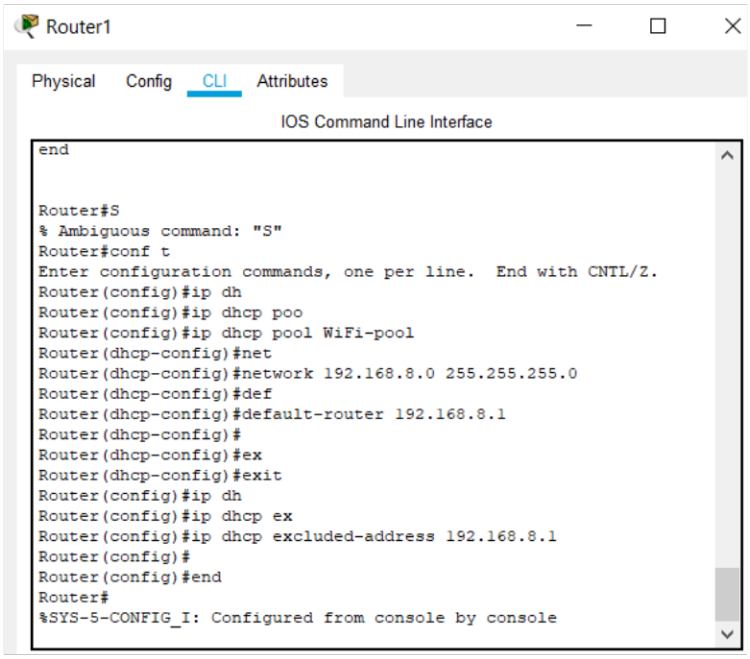


Рисунок 3.40 – Надання Ip адреси WiFi

Далі за допомогою Router1 створимо DHCP Pool, для точки доступу та перевіримо, підключивши 1телефон та 1 ноутбук (рис. 3.41). Дані користувачі отримали Ip addres від нашої точки доступу.

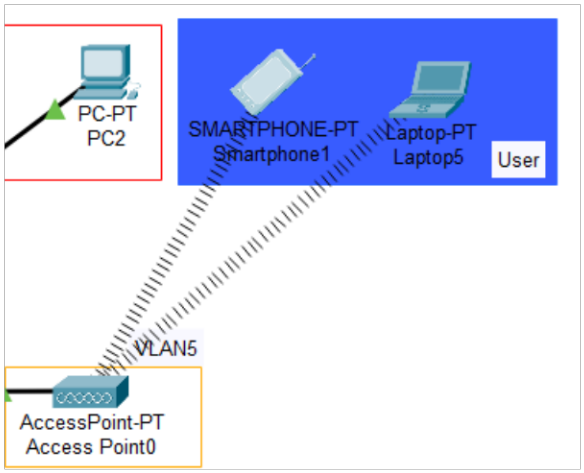


Рисунок 3.41 – Підключення до WiFi

Перевіримо чи користувачі отримали Ip адреса через DHCP POOL (рис. 3.42).

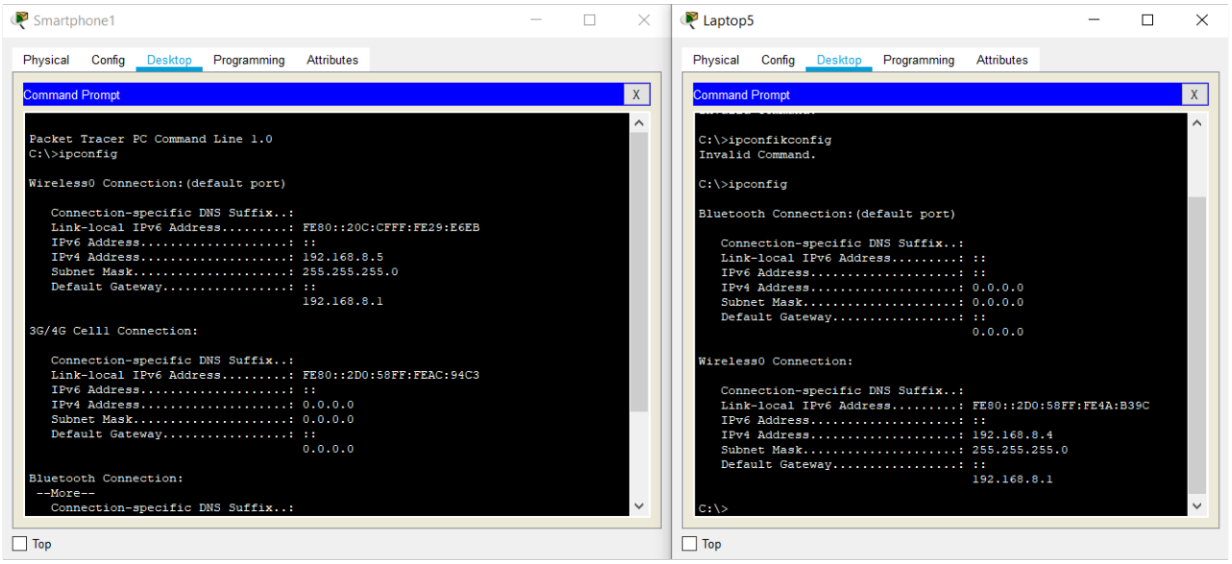


Рисунок 3.42 – Перегляд Ip адресів

Оглянемо доступ до серверів, 1С, DHCP, чи нові користувачі мають доступ до мережі та серверів (рис. 3.43). Командою *#ping*.

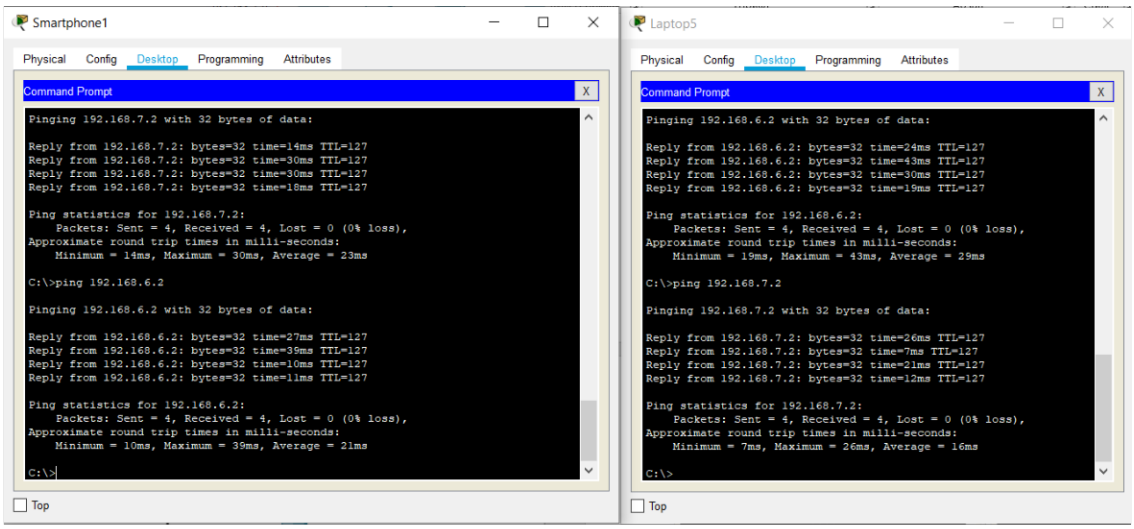


Рисунок 3.43 – Перегляд доступу до серверів

Нові користувачі не мають доступу до серверів, вони можуть лише обмінюватися файловими пакетами із користувачами будинку, на цьому їхні права обмежуються. Отже спроектована мережа володіє системою захисту.

ВИСНОВОК

Домашня оптоволоконна мережа може мати деякі особливості порівняно з іншими типами підключення до Інтернету. Серед них швидкість передачі даних оскільки оптоволоконні мережі зазвичай забезпечують надзвичайно швидку передачу даних, стабільність з'єднання, відсутність електричного струму (оптоволоконна мережа не передає електричний струм, що означає, що вона не піддається електричним перешкодам або не впливає на електроніку в домі). Ця надає ряд переваг щодо створення власної домашньої мережі в приватному будинку.

В результаті виконання кваліфікаційної роботи:

– проведено огляд досліджень з впровадження оптоволоконних мереж, досліджено структуру каналів зв'язку, типи оптоволокна та виявлено, що для організації оптоволоконної мережі варто використати обладнання, що підпорядковується стандартам TIA/EIA-568;

– розроблено алгоритм побудови домашньої локальної мережі та зазначено, що до обов'язкових етапів проектування належить: план будівлі та визначення потреб і вимог користувачів, вибір топології і мережевого обладнання, планування IP-адресації та організація безпеки мережі;

– побудовано план будівлі з урахуванням її конструкційних особливостей та зазначено приміщення для мережевого користування;

– досліджено та застосовано на практиці протоколи DHSP, VLAN, NAT, OSPF, проведено налаштування DHCP SERVER та побудована таблиця IP-адресацій для можливості розширення мережі в майбутньому, збільшення кількості підключених пристроїв, додавання нових підмереж або впровадження нових технологій у існуючій мережі;

– земульовано локальну домашню мережу у середовищі Cisco Packet Tracer, розробку успішно протестовано;

– продемонстровано роботу мережі і спроектовано захист на основі протоколу Access-List та NAT та практично протестовано використання Access-List для обмеження доступу до ресурсів мережі, що дозволяє захистити внутрішні ресурси мережі від прямого доступу з мережі Інтернет і зменшує ризик зловживання або атак зовнішніх користувачів.

Спроектована локальна домашня мережа слугує для обміну даними і комунікації між різними пристроями, які знаходяться в домашньому середовищі. В результаті виконання кваліфікаційної роботи усі поставлені завдання виконано. Тому, можна стверджувати, що мету роботи досягнуто.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конференція волоконно – оптичних комунікацій веб – сайт URL:https://opg.optica.org/conference.cfm?meetingid=5&yr=2022 (дата звернення: 01.04.2023).
2. Структура оптоволоконного кабелю веб-сайт URL:https://comp-net.at.ua/index/optovolokonnij_kabel/0-18 (дата звернення: 01.04.2023).
3. TIA/EIA-568-B визначає такі стандарти структурованого кабелювання веб-сайт URL:https://www.wikiwand.com/uk/TIA/EIA-568-B (дата звернення: 05.04.2023).
4. Стандарти випробувань на мережевий кабель веб-сайт URL:https://ua.scsikabel.com/info/test-standards-for-the-category-6-network-wire-30404398.html (дата звернення: 05.04.2023).
5. NFPA 70, National Electrical Code веб сайт URL:https://www.nfpa.org/News-and-Research/Publications-and-media/Blogs-Landing-Page/NFPA-Today/Blog-Posts/2022/11/21/NFPA-70-National-Electric-Code-Now-Used-in-All-50-States (дата звернення: 05.04.2023).
6. Institute of Electrical and Electronics Engineers, IEEE веб-сайт URL:https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%82_%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D0%B2_%D0%B7_%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D1%82%D0%B5%D1%85%D0%BD%D1%96%D0%BA%D0%B8_%D1%82%D0%B0_%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D1%96%D0%BA%D0%B8 (дата звернення: 10.04.2023).
7. Оптичні комунікації веб сайт URL:https://www.corning.com/optical-communications/worldwide/en/home.html (дата звернення: 10.04.2023).
8. ACL (Access Control List) веб сайт URL:https://highload.today/uk/acl-access-control-list/ (дата звернення : 15.05.2023).

9. Адміністрування мережі – це що таке? веб сайт URL:https://hi-news.pp.ua/internet/10013-admnstruvannya-merezh-ce-scho-take.html (дата звернення: 25.04.2023).
10. Побудова мережевої та локальної системи безпеки веб сайт URL:http://www.telesphera.net/blog/network-and-local-security-system.html (дата звернення: 15.05.2023).
11. Як працює DHCP веб сайт URL:https://uk.wikipedia.org/wiki/DHCP (дата звернення: 15.05.2023).
12. Категорії СКС і їх основні особливості веб сайт URL:https://shop.hypernet.com.ua/kategorii-sks/ (дата звернення: 15.05.2023).
13. Настанова з проектування, монтування та експлуатації автоматизованих систем моніторингу та управління будівлями і спорудами ДСТУ-Н 37:2008 URL :https://antifire.ua/ua/dbn/91.pdf (дата звернення: 25.05.23).
14. ДСТУ EN 41003:2014 веб сайт URL:http://online.budstandart.com/ua/catalog/doc-page?id_doc=74802 (дата звернення: 25.05.2023).
15. IEEE 802.3 веб ресурс URL: https://uk.wikipedia.org/wiki/IEEE_802.3 (дата звернення: 25.05.2023).
16. Оптоволокно веб сайт URL:https://uk.wikipedia.org/wiki/%D0%9E%D0%BF%D1%82%D0%BE%D0%B2%D0%BE%D0%BB%D0%BE%D0%BA%D0%BD%D0%BE (дата звернення: 05.02.2023).
17. Дифузне відбиття світла веб сайт URL:https://uk.wikipedia.org/wiki/%D0%94%D0%B8%D1%84%D1%83%D0%B7%D0%BD%D0%B5_%D0%B2%D1%96%D0%B4%D0%B1%D0%B8%D1%82%D1%82%D1%8F_%D1%81%D0%B2%D1%96%D1%82%D0%BB%D0%B0 (дата звернення: 15.01.2023).
18. Фотонно – кристалічне оптичнне волокно веб сайт URL: https://ua.wikipedia.org/wiki/%D0%A4%D0%BE%D1%82%D0%BE%D0%BD%D0%BD%D0%BE-%D0%BA%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BB%D0%BB%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5_%D0

%BE%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5_%D0%B2%D0%BE%D0%BB%D0%BE%D0%BA%D0%BD%D0%BE (дата звернення: 18.01.2023).

19. Поляризаційно стабільне оптоволокно веб сайт URL:https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%8F%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE_%D1%81%D1%82%D0%B0%D0%B1%D1%96%D0%BB%D1%8C%D0%BD%D0%B5_%D0%BE%D0%BF%D1%82%D0%BE%D0%B2%D0%BE%D0%BB%D0%BE%D0%BA%D0%BD%D0%BE (дата звернення: 20.01.2023).
20. Оптоволоконний кабель веб сайт URL:https://uk.wikipedia.org/wiki/%D0%9E%D0%BF%D1%82%D0%BE%D0%B2%D0%BE%D0%BB%D0%BE%D0%BA%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9_%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C (дата звернення: 18.01.2023).