ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «**СТВОРЕННЯ ТА ЗАСТОСУВАННЯ МЕТОДИКИ МОДЕЛЮВАННЯ ТРАФІКУ ІНТЕРНЕТ ЛОКАЛЬНИХ МЕРЕЖ**»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Денис БУРБА

_____ _____

(*підпис*)

Виконав: Здобувачка вищої освіти гр.ТСДМ-61

Денис БУРБА

Керівник: Віктор ЗАЇКА
ДТН, професор
науковий ступінь, вчене звання

Рецензент:
КТН, доцент
науковий ступінь, вчене звання

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

Кафедра Телекомунікаційних систем та мереж
Ступінь вищої освіти Магістр
Спеціальність 172 Електронні комунікації та радіотехніка
Освітньо-професійна програма Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Телекомунікаційних систем та мереж
_____Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бурбі Денису Вікторовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: **: «Створення та застосування методики моделювання трафіку інтернет локальних мереж»**

керівник кваліфікаційної роботи Віктор ЗАЇКА, ДТН, професор
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467.

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.
3. Вихідні дані до кваліфікаційної роботи:

1. Види інтернет локальних мереж
2. Особливості та безпека інтернет локальних мереж
3. Створення інтернет локальної мережі
4. Науково-технічна література

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Види та структура інтернет локальних мереж
2. Дослідження методів та устаткування створення інтернет локальних мереж
3. Практичне налаштування

Перелік ілюстративного матеріалу: ***презентація***

6. Дата видачі завдання «___» _____ 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	10.10.2025	Викон.
2	Види та структура інтернет локальних мереж	20.10.2025	Викон.
3	Дослідження методів та устаткування створення інтернет локальних мереж	31.10.2025	Викон.
4	Практичне налаштування	20.11.2025	Викон.
5	Висновки, вступ, реферат	30.11.2025	Викон.
6	Розробка презентації	15.12.2025	Викон.

Здобувач вищої освіти _____ Денис БУРБА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної
роботи _____ Віктор ЗАЇКА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Бурба Д.В. до захисту кваліфікаційної роботи

(прізвище та ініціали)

за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Створення та застосування методики моделювання трафіку інтернет локальних мереж».

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника магістерської роботи

Здобувач Бурба Денис Вікторович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до наукової роботи.
Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Бурби Дениса Вікторовича на оцінку «добре» та присвоїти йому кваліфікацію Магістр з Електронних комунікацій та радіотехніки.

Керівник
:валіфікаційної роботи Віктор ЗАЇКА
(підпис) *Ім'я ,ПРІЗВИЩЕ)*

«____» _____ 2025 року

Висновок кафедри про магістерську роботу

Кваліфікаційна робота розглянута. Здобувач Бурба Д.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою Телекомунікаційних систем та мереж Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

Здобувача вищої освіти Бурби Дениса Вікторовича
(прізвище, ім'я, по батькові)
на тему «Створення та застосування методики моделювання трафіку інтернет локальних мереж»

Актуальність: На даний день мережа Інтернет використовується майже повсюди. Нові технології та стандарти розвиваються кожний день з неймовірною швидкістю. Завдяки цьому ми можемо використовувати мережу Інтернет в будь-яких цілях для власного користування, в будь-якій точці світу при наявності телефонного зв'язку. Це дає можливість нам задіювати різну інформацію та дані, корегувати їх та обмінюватися ними з іншими користувачами для ефективних цілей.

Позитивні сторони:

В практичній частині роботи описано, як побудувати власну домашню інтернет локальну мережу, які використовуються для цього засоби та інструменти, методи, яке апаратне програмне забезпечення лежить в основі побудови та практичне використання та налаштування. Наведено всі фактори для створення якісної та ефективної LAN, які мають практичне застосування та реалізацію технічних та програмних рішень у вигляді мережі власного користування в житловому будинку.

Недоліки: 1. Слід було більше уваги приділити технічним засобам, їх технічним характеристикам, та виконати порівняльний аналіз.

2. У роботі слід було більш ширше розглянути питання розвитку технології п'ятого покоління в майбутньому.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної магістерської роботи

Висновок: *кваліфікаційна магістерська робота заслуговує оцінку "***добре***", а здобувач* Бурба Денис Вікторович *заслуговує присвоєння кваліфікації:* Магістр з електронних комунікацій та радіотехніки.

Рецензент: _____ _____
науковий ступінь, вчене звання *підпис* *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра : ____стор., ___ рис., ___табл., ___джерел.

Мета роботи – розглянути та проаналізувати особливості інтернет локальних мереж.

Об'єкт дослідження – інтернет локальні мережі.

Предмет дослідження – різновиди та організація інтернет локальних мереж.

В даній роботі приведено особливості та організація інтернет локальних мереж. Простежено історію виникнення та створення інтернет локальних мереж. Проаналізовано роботу основних технологій в інтернет локальних мережах. Окреслено засоби безпеки та захисту інформації в інтернет локальних мережах. Визначено головні переваги та недоліки в LANмережах. Виявлено подальша тенденція розвитку інтернет локальних мереж в найближчому майбутньому. Розглянуто практичне налаштування та застосування інтернет локальних мереж для послуг користувача.

КЛЮЧОВІ СЛОВА:

Технологія Ethernet, Технологія Wi-Fi, Інтернет локальна мережа, CiscoPacketTrace

ABSTRACT

Text part of the master's work: _____stories, ___ drawings, ___ tables, ___ dzherel. Meta robots - look at and analyze the features of Internet local networks.

The object of investigation is Internet local networks.

The subject of research is various types of Internet organization of local networks.

This work describes the specifics and organization of Internet local networks. The history of guilt and the creation of the Internet of local networks has been covered. The work of basic technologies in Internet local networks has been analyzed. The security and protection of information on the Internet in local areas has been christened. Major advantages and shortcomings in LAN boundaries were identified. A further trend has been identified for the development of Internet local networks in the near future. The practical setup and installation of the Internet of local measures for the services of a koristuvach is examined.

KEY WORDS:

Ethernet technology, Wi-Fi technology, Local network Internet, CiscoPacketTrace

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ……9

ВСТУП……10

РОЗДІЛ 1 ВИДИ ТА СТРУКТУРА ІНТЕРНЕТ ЛОКАЛЬНИХ МЕРЕЖ… ….12
1.1 Аналіз та особливості інтернет локальних мереж……..12
1.2 Історія створення інтернет локальних мереж…….……19
1.3 Мережева модель OSI…….21
1.4 Технологія Ethernetта її різновиди……...26
1.5 Технологія Wi-Fiта її особливості……31
РОЗДІЛ 2 ОРГАНІЗАЦІЯ ІНТЕРНЕТ ЛОКАЛЬНИХ МЕРЕЖ…… …36
2.1Переваги та недоліки інтернет локальних мереж……...36
2.2 Безпека та захист в інтернет локальних мережах…….....40
2.3 Майбутній розвиток інтернет локальних мереж…….51
РОЗДІЛ 3 ПРАКТИЧНЕ НАЛАШТУВАННЯ ІНТЕРНЕТ
ЛОКАЛЬНОЇ МЕРЕЖІ……..55
3.1 Налаштування та застосування інтернет локальної мережі……...55
3.2 Технологія NAT……...74
3.3 Устаткування та інструменти для побудови інтернет
3.4 локальної мережі…… 80

ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ …….....84

ВИСНОВКИ…….....86

ПЕРЕЛІК ПОСИЛАНЬ…….....……... . 88

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ ……89

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

«OSI» The Open Systems Interconnection model – модель, яка здійснює передачу даних в мережі.

«CSMA/CD» Carrier Sense Multiple Access with Collision Detection – протокол, який здійснює множинний доступ та виявляє колізії.

«LLC» Logical Link Control – підрівень логічної передачі даних.

«WEP» Wired Equivalent Privacy – протокол, який забезпечує безпеку стандартів Wi-Fi.

«WPA»Wi-Fi Protected Access – спосіб шифрування для захисту безпровідних мереж.

«IEEE» Institute of Electrical and Electronic Engineers – Інститут інженерів порадіоелектроніці.

«PDU» Protocol Data Unit – протокольний блок даних.

«ARP» Address Resolution Protocol – протокол визначення адрес.

«TCP» Transmission Control Protocol – протокол управління передачею.

«UDP»User Datagram Protocol – протокол користувальницьких датаграм.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ……6

ВСТУП……..7

1 ВИДИ ТА СТРУКТУРА ІНТЕРНЕТ ЛОКАЛЬНИХ МЕРЕЖ……...9
1.1 Аналіз та особливості інтернет локальних мереж……...9
1.2 Історія створення інтернет локальних мереж……..…16
1.3 Мережева модель OSI……...18
1.4 Технологія Ethernetta її різновиди……..23
1.5 Технологія Wi-Fita її особливості……..28
2 ОРГАНІЗАЦІЯ ІНТЕРНЕТ ЛОКАЛЬНИХ МЕРЕЖ……33
2.1 Переваги та недоліки інтернет локальних мереж……..33
2.2 Безпека та захист в інтернет локальних мережах…….....37
2.3 Майбутній розвиток інтернет локальних мереж……48
3 ПРАКТИЧНЕ НАЛАШТУВАННЯ ІНТЕРНЕТ ЛОКАЛЬНОЇ МЕРЕЖІ……...52
3.1 Налаштування та застосування інтернет локальної мережі……..52
3.2 Технологія NAT……71
3.3 Устаткування та інструменти для побудови інтернет локальної мережі…… 77

ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ …….....82

ВИСНОВКИ…….....84

ПЕРЕЛІК ПОСИЛАНЬ…….....86

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

«OSI» TheOpenSystemsInterconnectionmodel – модель, яка здійснює передачу даних в мережі.

«CSMA/CD» Carrier Sense Multiple Access with Collision Detection – протокол, який здійснює множинний доступ та виявляє колізії.

«LLC» LogicalLinkControl – підрівень логічної передачі даних.

«WEP» WiredEquivalentPrivacy – протокол, який забезпечує безпеку стандартів Wi-Fi.

«WPA»Wi-FiProtectedAccess – спосіб шифрування для захисту безпровідних мереж.

«IEEE» Institute of Electrical and Electronic Engineers – Інститут інженерів порадіоелектроніці.

«PDU» ProtocolDataUnit – протокольний блок даних.

«ARP» Address Resolution Protocol – протокол визначення адрес.

«TCP» Transmission Control Protocol – протокол управління передачею.

«UDP»UserDatagramProtocol – протокол користувальницьких датаграм.

ВСТУП

На даний день мережа Інтернет використовується майже повсюди. Нові технології та стандарти розвиваються кожний день з неймовірною швидкістю. Завдяки цьому ми можемо використовувати мережу Інтернет в будь-яких цілях для власного користування, в будь-якій точці світу при наявності телефонного зв'язку. Це дає можливість нам задіювати різну інформацію та дані, корегувати їх та обмінюватися ними з іншими користувачами для ефективних цілей.

Саме через такі інноваційні впровадження виникає питання використання технічного обладнання на певній обмеженій території та передачі телекомунікаційних технологій, для вирішення таких питань приходять інтернет локальні мережі, які можуть задовольнити велику кількість користувачів завдяки своїм специфікаціям.

У даній роботі розглядаємо саме інтернет локальні мережі. На даний час ці мережі використовує велика частина людства. Їх роль дуже важлива у сучасному технологічному світі. Багатофункціональність та гнучкість локальних мереж заставляє користувачам обирати саме їх.

Зазвичай LAN використовує невелику зону покриття, наприклад, це мережі в рамках лабораторій, офісах, фірмах, тощо. Це дає можливість передавати інтернет інформацію та потоки великих обсягів на невеликих межах підприємств, домах, в залежності від задачі використання. Саме даним сферам діяльності буде приділена дана бакалаврська робота.

Локальні мережі дуже допомагають у сучасних реаліях, коли в нашому світі виникають проблеми, такі як пандемія коронавірусної хвороби, які можуть завадити багатьом людям з розвитком бізнесу, технологій та іншим, але завдяки LAN це не є перешкодою, а навпаки полегшує наше життя від вирішення таких завад.

Дана робота висвітлює в основній та теоретичній частині загальні специфікації та особливості, переваги та недоліки, питання щодо безпеки та захисту, історію і розвиток інтернет локальних мереж.

В практичній частині роботи описано, як побудувати власну домашню інтернет локальну мережу, які використовуються для цього засоби та інструменти, методи, яке апаратне програмне забезпечення лежить в основі побудови та практичне використання та налаштування. Наведено всі фактори для створення якісної та ефективної LAN, які мають практичне застосування та реалізацію технічних та програмних рішень у вигляді мережі власного користування в житловому будинку.

Всі гідності інтернет локальних мереж користувач може реалізувати тільки при грамотній побудові, виборі моделі, топології, типу з’єднання, апаратних та програмних засобів, методів безпеки та захисту. Щоб побудувати свою локальну мережу або вибрати потрібний вам варіант, ви можете спокійно використовувати інформацію та знання, які застосовані в даній дипломній роботі.

1 ВИДИ ТА СТРУКТУРА ІНТЕРНЕТ ЛОКАЛЬНИХ МЕРЕЖ

1.1Аналіз та особливості інтернет локальних мереж

Інтернет локальні мережі (LocalAreaNetwork, LAN) - мережі, в яких об’єднуються комп’ютери та інші периферійні пристрої, такі як мобільні телефони, сервери, принтери та інше обладнання в мережі Інтернет, робота яких обмежена на певній ділянці або площі, прикладом можуть слугувати локальна мережа в межах школи, будинку або офісу. Але не зважаючи на розмір або географічне охоплення, головною особливістю локальної мережі є те, що вона охоплює технічні прилади, які розташовуються в лімітованій області.

Якщо дані пристрої об’єднали в одну локальну мережу, то це дає можливість користувачам обмінюватися інформацією та даними один з одним, мати допуск до однакового з'єднання по інтернету, використовувати загальні ресурси технічних пристроїв, які підключені до мережі.

Одною із основних головних задач будь-якої комп’ютерної мережі є надання інформаційних та обчислювальних ресурсів підключеним до неї користувачам.

Отже, з цього може випливати, що інтернет локальну мережу можна розглядати як сукупність серверів та робочих станцій.

Сервер – комп’ютер, який підключений до мережі та забезпечує своїх користувачів певними послугами. У серверів є багато функцій, основні з яких це зберігання даних, управління БД (бази даних), віддалена обробка різних завдань, друк завдань та багатий перелік інших функцій, потреба в яких може виникнути у користувачів мережі. Сервер можна вважити джерелом ресурсів мережі.

Робоча станція –персональний комп’ютер, який підключений до мережі за допомогою якого користувач отримує доступ до до її ресурсів.Робоча станція може функціонувати, як в мережевому, так і в локальному режимі. Дана станція оснащена власною операційною системою (наприклад, MSDOS, Windowsta ін.),

може забезпечувати користувача усіма необхідними інструментами для вирішення прикладних завдань, які стоять перед ним.

Комп'ютерні мережі реалізують розподілену обробку даних. Обробка даних у даному випадку розподілена між двома об'єктами : клієнт та сервер.

Клієнт – задача, робоча станція, персональний комп'ютер або користувач комп'ютерної мережі. Під час процесу обробки даних клієнт може сформувати запит на сервер для виконання складних процедур, читання файлів, пошук інформації у базі даних тощо.

Сервер, який підключений до мережі, виконує запит, який надіслав клієнт. Результати щодо виконання даного запиту надсилаються назад клієнту. Сервер дає та забезпечує зберігання даних загального користування, може організувати доступ до цих даних і передати дані клієнту.

Клієнт оброблює отримані дані та представляє результат обробки даних у вигляді, зручному для користувача. Для таких систем загально прийнято терміни – системи чи архітектура клієнт-сервер.

Архітектура клієнт-сервер може використовуватись як в однорангових мережах (тимчасова мережа), так і в мережі з виділеним сервером.

Існують різні варіанти та класифікації інтернет локальних мереж, все залежить від параметрів, які входять в основу мережі. В залежності від типа їх поділяють на два види : тимчасова мережа (однорангова) та мережа на основі клієнт-сервер.

Перший тип - **тимчасова мережа**, в якій всі користувачі мають однакові права та доступ на використання файлів та даних. Мережева операційна система розподілена по робочим станціям. Кожна із таких станцій у мережі може виконувати функції як клієнта, так і сервера. Користувач такої мережі має доступ до всіх пристроїв, які підключені до інших робочих станцій. Даний тип зазвичай

використовується для невеликих офісів, які не потребують серйозного захисту інформації від стороннього втручання.

Переваги тимчасової мережі :

- Низька вартість
- Висока надійність

Недоліки тимчасової мережі :

- Складність керування мережею
- Залежність ефективності роботи мережі від кількості робочих станцій
- Складність забезпечення захисту
- Проблеми з оновленням та зміною ПО підключених робочих станцій

Найбільш популярні тимчасові мережі використовуються на базі операційних систем LANtastic, NetwareLite.

Другий тип - **мережа на основі клієнт-сервер**, в якій передача інформації, даних та управління цілою мережею здійснюється за допомогою одного головного комп'ютеру – сервера. Дані локальні мережі мають більш надійний рівень захисту інформації, яка передається, і забезпечують високу продуктивність. Такий тип мереж використовують для компаній та офісів, які мають значну кількість технічних пристроїв, підключених до мережі.На головному комп'ютері встановлюється мережева операційна система, також до нього можуть підключатися всі зовнішні пристрої, що розділяються – жорсткі диски, принтери і модеми.

Переваги мережі на основі клієнт-сервер :

- Надійна система захисту інформації
- Висока швидкодія
- Відсутність на обмеження кількості робочих станцій
- Простота в управлінні у порівнянні з одноранговими мережами

Недоліки мережі на основі клієнт-сервер :

- Висока вартість із-за виділення одного комп’ютеру на сервер
- Залежність швидкодії та надійності від сервера
- Менша гнучкість у діях порівняно з одноранговими мережами

Мережі на основі клієнт-сервер є більш поширені у використанні користувачем комп’ютерних мереж. Мережі операційні системи для таких мереж – LanServer (IBM), WindowsNTServerта NetWare (Novell).

Дляз’єднання мережі є два варіанта : **дротове** та **бездротове**.

В дротових мережах передача даних здійснюється по провідним лініям зв’язку, а саме вита пара або оптичний кабель, які під’єднуються до ПК та застосовують технологію Ethernet.

Бездротове з’єднання дає змогу передавати дані без допомоги дротів. В бездротових мережах передача інформації здійснюється за допомогою радіосигналу, такі як Wi-FI, Bluetooth або подібних інтернет-протоколів.

Bluetooth – одна з технологій бездротової передачі зв'язку, яка надає користувачам обмін інформацією та даними між комп’ютерами, мобільними телефонами, периферійними пристроями, клавіатурами та іншими на невеликому радіусі, приблизно до 10 метрів.

Wi-Fi – технологія бездротової передачі даних та інформації за допомогою радіорелейних пристроїв. Зв'язок Wi-Fізазвичай діє на відстані до кілька десятків метрів.

Топологія – фізична структура розташування технічних пристроїв та способи їх з’єднання за допомогою ліній передач.

Мережева топологія визначає стандарти для обладнання, тип кабелю, який використовується, який метод використовується для обміну інформацією та надійність роботи мережі.

Виділяють три основних топології мережі :

- Топологія шина(bus)
- Топологія зірка (start)
- Топологія кільце (ring)

Топологія «Шина»

В цій топології існує одна єдина лінія зв’язку, інформація передається по черзі між з’єднаними комп’ютерами, якщо дана умова не виконується, то це призводить до виникнення колізій. В даній мережі всі абоненти рівноправні. Отже, у шині відбувається напівдуплексна передача даних (рисунок 1.1).

Переваги :

- Простота побудови мережі
- Мережа легко розширюється
- Пропускна спроможність каналу ефективно використовується
- Надійність вище, якщо вийде з ладу один із окремих комп’ютерів, то це не порушить працездатність мережі загалом

Недоліки :

- Обмежена довжина шини
- Відсутнє автоматичне підтвердження прийому повідомлень
- Низький рівень захисту даних
- Можливість виникнення зіткнень (колізій) на шині, при умові, що інформація передається декількома станціями
- Проблема знаходження місця обриву
- Вихід із ладу будь-якого відрізку кабелю веде до порушення працездатності мережі



Рис. 1.1 Мережева топологія «Шина»

Топологія «Зірка»

В основі даної топології є центральний комп’ютер до якого під’єднані інші абонентські станції, кожна з них використовує свою окрему лінію передачі.Головний елементявляється не комп’ютер , а хаб (hub), що відновлює сигнали, які надходять та пересилає до інших ліній зв’язку (рисунок 1.2).

Переваги :

- Простота перефирійного обладнання
- Високий рівень захисту даних
- Легке виявлення несправностей у кабельній мережі
- Кожен користувач може працювати незалежно від інших користувачів

Недоліки :

- Якщо центральний пристрій вийде з ладу, то вся мережа буде призупинена
- Велика вартість центрального пристрою
- Зменшення продуктивності мережі із збільшенням кількості комп’ютерів, які підключені до мережі

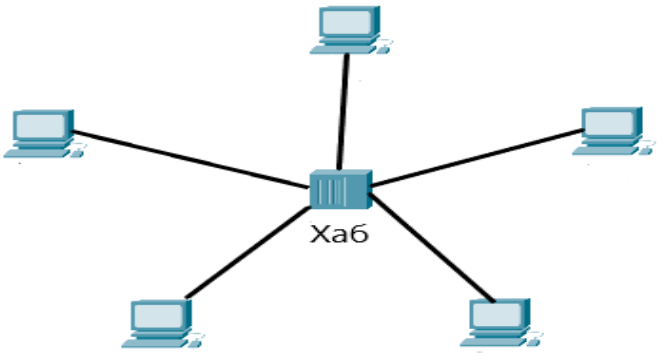


Рис. 1.2 Мережева топологія «Зірка»

Топологія «Кільце»

Топологія в якій кожний комп’ютер передає інформацію наступному абоненту в ланцюжку, а отримує дані від попереднього в ланцюжку. Даний ланцюжок замкнутий схему «кільце». Головний абонент у цій технології відсутній, усі комп’ютери мають можливість бути однаковими. В цій топології може бути велика кількість абонентів (рисунок 1.3).

Переваги :

- Відсутня проблема маршрутизації
- Відсутність дорогого центрального пристрою
- Легкий пошук несправних вузлів
- Простота контролю помилок
- Пропускна спроможність мережі розділяється між всіма користувачами, отже, означає, що всі користувачі гарантовано послідовно отримають свій доступ до мережі

Недоліки :

- Важко підключити до мережі нові комп’ютери

- Кожний комп’ютер в мережі має брати активну участь у передаванні інформації, для цього потрібні ресурси, щоб не було затримок в основній роботі цих комп’ютерів
- Якщо виходить з ладу один із комп’ютерів мережі або певний відрізок кабелю, то вся мережа повністю паралізується

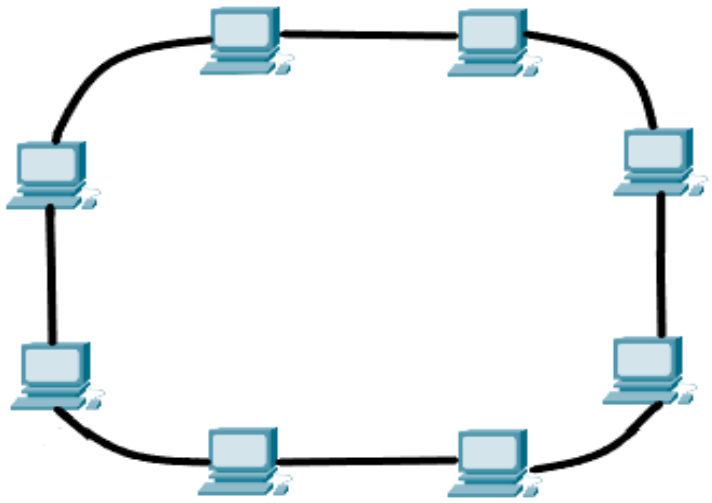


Рис. 1.3 Мережева топологія «Кільце»

1.2 Історія створення та розвитку інтернет локальних мереж

Перед початком створення інтернет локальних мереж з’явилась самеВсесвітня мережа Інтернет.

Лоуренс Робертс, який займав посаду дослідника Лінкольнскої лабораторії у структурі Массачусетського технологічного інституту, самим першим запропонував ідею передачу цифрових даних між двома ПК. У 1969 р. цю ідею вирішили реалізувати в проект та побудували комп’ютерну мережу ARPANet (Advanced Research Projects Agency Network). З кожнимроком мережа становилася більш модернізованою та популярною. У січні 1983 р. мережа ARPANet стала використовувати стек протоколів TCP/IP. Пізніше у 1985 р. було створено нову мережу NFSNet, яка також використовувала протокол TCP/IP, вона

використовувалася для обміну даних в наукових цілях.NFSNet стала більш удосконаленою та розгалуженою мережею, ніж ARPANet. Все це дало поштовх для розвитку глобальної мережі Інтернет.

TCP/IP – міжмережевий протокол, який керує з'єднання та здійснює обмін інформацією і даними між системами.

З розвитком мережі Internetпочали розвиватися локальні мережі. Початком створення локальних мереж можна вважати 1973 р, коли компанія Xerohрозробила проект експериментальної мережі під назвою «Ethernet», призначенням даної мережі було об'єднання пристроїв, таких як комп'ютери, сервери та лазерні принтери. Назва мережі пішла від слова «ether» ,в перекладі означає «ефір» , що означало передачу бітової інформації між усіма користувачами мережі у фізичному середовищі.Почаласьстандартизація технології Ethernetта офіційно визнали стандартом у 1985 р. за допомогою IEEE (інститут інженерів електрики та електроніки). Стандарт динамічно формувався за допомогою оновлень, покращень і це дало використовувати технологіюEthernetв усіх сферах LAN. На даний день стандарти Ethernet зовсім не схожі, на ті які були на початку свого створення. Середою передачі даних є вита пара або оптоволокно.

Бездротове з'єднання комп'ютерів у локальних мережах, а саме Wi-Fi, зародився як спосіб широкосмугового доступу в мережу Internet, що використовує радіосигнал для передачі даних. Дату народження Wi-Fi можна вважити у 1997 р. , коли був створений набір стандартів IEEE 802.11 , який використовується для сполучення в безпровідних мережах. В наступних роках технологія Wi-Fi почала дуже активно розвиватися в різних сферах, де використовуються інтернет локальні мережі.

Позитивний наслідок роботи в технологіях мереж дало різним компаніям шанс створити свої стандарти, технічні пристрої та апаратне забезпечення. За допомогою звершень та досягнень у даній сфері почалось різке поширення

локальних мереж, що призвело до популяризації LAN у значної кількості людства. Розвиток локальних мереж дуже вплинув на технологічний світ і зараз LAN займають провідні позиції у Всесвітній мережі Інтернет.

1.3 Мережева модель OSI

Мережева модель OSIмає в своїй будові сім рівнів, які ієрархічнорозташовані від більшого до меншого. Модель OSI почала розроблюватися ще у 1970-х роках, призначенням було описати архітектуру та принцип роботи мереж передачі даних. Хочу нагадати, що дані передаються не тільки через загальну мережу Інтернет, але у й локальних мережах, як за допомогою дротових так і бездротових з’єднань

У процесі передачі інформацією завжди беруть участь пристрій, який є відправником, пристрій, який є одержувачем, а також самі дані, які мають бути передані та отримані. Для звичайного юзера задача дуже проста – потрібно взяти та надіслати ці дані. Отже, дана семирівнева модель OSI детально описує все, що відбувається при надсиланні та прийому даних (рисунок 1.4).

На останньому рівні інформація представляється у вигляді даних, на першому у вигляді бітів. Процес, коли інформація йде на відправку і переходить із даних у біти, має назву інкапсуляція. Процес зворотній цьому, коли інформація, яка була отримана в бітах на першому рівні, переходить у дані на сьомому, називається декапсуляцією. На кожному рівні моделі OSIінформація подається у вигляді блоків даних протоколу – PDU.

Модель OSI

Дані	7 прикладний application	Доступ до мережевих служб
	6 представлень presentation	Представлення і кодування даних
	5 сеансовий session	Управління сеансом зв'язку
Сегменти	4 транспортний transport	Прямий зв'язок між кінцевими пунктами і надійність
Пакети	3 мережевий network	Визначення маршруту і логічна адресація
Кадри	2 канальний data link	Фізична адресація
Біти	1 фізичний physical	Робота з середовищем передачі , сигналами і двійковими даними

Рис. 1.4 Мережева модель OSI

Фізичний рівень

Даний рівень відповідає за обмін фізичними сигналами між фізичними пристроями користувачів. Пристрої розуміють тільки вигляд набору нулів та одиниць – біт. В цьому випадку біт є блоком даних протоколу.

На фізичному рівні пристрої оперують бітами. Вони передаються проводами (оптоволокно, вита пара і т.д) або без проводів (наприклад, через Bluetooth, Wi-Fi, GSM, 4G або інші).

Канальний рівень

На другому рівні вирішується питання та адресації інформації. Канальний рівень отримує біти та перетворює їх у кадри (frame, також «фрейми»). Головна задача даного рівня – створити кадри з адресою відправника та отримувача, після чого відправити їх по мережі.

Даний рівень має два підрівні – MACта LLC. Задачею MACє присвоєння фізичних MAC-адресів, а LLC займається перевіркою та виправленням даних, а також керує їх передачею.

Основні пристрої, які працюють на другому рівні – комутатори, вони відповідають за передачу сформованих кадрів від одного пристрою до іншого, використовуючи у вигляді адрес тільки фізичні MAC-адреси.

Мережевий рівень

На цьому рівні працює таке поняття, як маршрутизація. Цю задачу виконують пристрої третього рівня – маршрутизатори (роутери). Маршрутизатори отримують MAC-адреси від комутаторів, які працюють на минулому рівні. Після отримання MAC-адреси вони займаються побудовою маршруту від одного пристрою до іншого, враховуючи усі потенційні несправності, які можуть бути у мережі.

На мережевому рівні використовується такий протокол, як ARP. Даний протокол перетворює 64-бітні MAC-адреси в 32-бітні IP-адреси та навпаки, завдяки чому забезпечується інкапсуляція та декапсуляція даних.

Транспортний рівень

Мережеву модель OSIумовно можна розділити на дві групи :

- Media Layers (рівні середовища),
- Host Layers (рівні хосту).

Рівні MediaLayers (фізичний, канальний та мережевий рівень) займаються передачею даних (по кабелю або безпровідній мережі), використовують мережеві пристрої, як маршрутизатори, комутатори і т.д.

Рівні HostLayers (транспортний, сеансовий, рівень представлення та прикладний рівень) використовуються вже безпосередньо на пристроях користувачів, як стаціонарні ПК чи портативні мобільні пристрої.

Транспортний рівень є посередником між MediaLayersta HostLayers, який скоріш за все, більше відноситься до перших рівнів, ніж до останніх. Головною задачею даного рівня є транспортування пакетів.

При передачі даних, які є найбільш чутливими до втрат на цьому рівні використовується протокол TCP, який контролює цілісність доставленої інформації.

Для мультимедійних файлів найбільш критичною є затримка, ніж втрата даних. Для передачі даних, які є найбільш чутливими до затримок використовується протокол UDP, який дозволяє організовувати зв'язок без встановлення з'єднання.

В протоколі TCP під час передачі дані діляться на сегменти. Сегмент – частина пакету. Якщо приходить пакет з даними, який перевищує пропускну спроможність мережі, то пакет ділиться на сегменти допустимого розміру. Сегментація пакетів також може використовуватись в ненадійних мережах, коли може статися велика ймовірність, що великий пакет буде втрачено або буде відправлений не тому адресату.

При передачі даних за протоколом UDP пакети даних діляться на датаграми. Датаграма – також частина пакету. Але в залежності від сегменту, найбільша різниця датаграм в автономності. Кожна датаграма містить в собі всі необхідні заголовки, щоб пройти шлях до кінцевого адресата, тому вони не залежать від мережі, можуть взагалі доставлятися різними маршрутами та напрямками у різному порядку.

Датаграма та сегмент – два PDUтранспортного рівня мережевої моделі OSI.

Сеансовий рівень

На цьому рівні йде оперування чистими даними, так як на шостому і на сьомому рівні. Головною задачею п'ятого рівня є підтримка сеансу або сесію

зв’язку. Йде керування взаємодією між програмами, відкривається можливість синхронізації різних завдань, завершення сеансу та обмін інформацією.

Служби, які працюють на сеансовому рівні більш за все застосовуються серед додатків, які мають потребу віддаленого виклику процедур, щоб вимагати виконання дій на віддалених комп’ютерах або незалежних системах на одному пристрої (при умові наявності кількох ОС).

Одним з головних прикладів п’ятого рівня може бути відеодзвінок по мережі. На час відеозв’язку необхідно, щоб два потоки даних (аудіо та відео) йшли синхронно. У випадку, якщо до розмови додається третя людина, то створюється конференція. Задача сеансового рівня – зробити так, щоб співрозмовники могли зрозуміти, хто на поточний момент розмови говорить.

Рівень представлення

Задачею шостого рівня є представлення даних (які все ще є PDU)у зрозумілій формі та вигляді для людини та машині. Одним із прикладів може служити, що коли один пристрій вміє відображати текст у вигляді кодування ASCII, а інший тільки у UTF-8, то переклад тексту з одного кодування в інший відбувається на даному рівні.

Також рівень представлення даних займається представленням картинок (в JPEG, GIFта ін.), а також відео-аудіо (в MPEG, QuickTime). Ще одна з функцій шостого рівня є шифрування даних, коли при передачі їх необхідно захистити.

Прикладний рівень

Останній рівень ще можуть називати рівень додатків. Даний рівень – те з чим взаємодіють користувачі, по своїй суті, як графічний інтерфейс усієї мережевої моделі OSI, але з іншими він взаємодіє найменше.

Всі сервіси, які сьомий рівень отримує від інших, використовуються для доставки даних для користувача. Протоколи, які працюють на даному рівні, їм не

потрібно займатися маршрутизацією та гарантувати доставку даних, тому що за це відповідають минулі шість рівнів. Головна задача прикладного рівня – використовувати свої власні протоколи, щоб користувач зміг побачити дані в зрозумілому для нього вигляді.

Використовуються такі протоколи як UDP (наприклад, DHCP) або TCP (HTTP, HTTPS, SFTP, DNS). Сьомий рівень є самим верхнім по ієрархії.

1.4 Технологія Ethernet та її різновиди

Ethernet – технологія, яка з'єднує провідні локальні мережі за допомогою пакетної передачі даних. Ethernet в основному використовує стандарти IEEE групи 802.3. На фізичному рівні моделі OSI стандарт Ethernet використовує дротове з'єднання(саме коаксіальний кабель, вита пара, оптоволокно) та електричні сигнали, на канальному рівні – формат кадрів та протоколи, які керують управлінням доступу до середовища. На початку створення стандарту для середовища передачі даних використовувався коаксіальний кабель, але згодом до цього списку додались вита пара та оптоволокно.

Різновиди фізичного середовища передачі даних в технології Ethernet :

- 10Base-5 – коаксіальний кабель, який має діаметр 0,5 дюйма, має назву «товстий» коаксіальний кабель (рисунок 1.5).
- 10Base-2 – коаксіальний кабель, який має діаметр 0,25 дюйма, має назву «тонкий»коаксіальний кабель (рисунок 1.5).
- 10Base-T – кабель, який має основу витої пари (рисунок 1.6).
- 10Base-F – кабель на основі оптоволокна (рисунок 1.7).

Цифра «10»позначає швидкість передачі інформації – 10 Мбіт/с , а слово «Base» – метод передачі на одній базовій частоті, а саме 10 МГц.



Рис. 1.5 Різниця між «тонким» та«товстим» коаксіальним кабелем

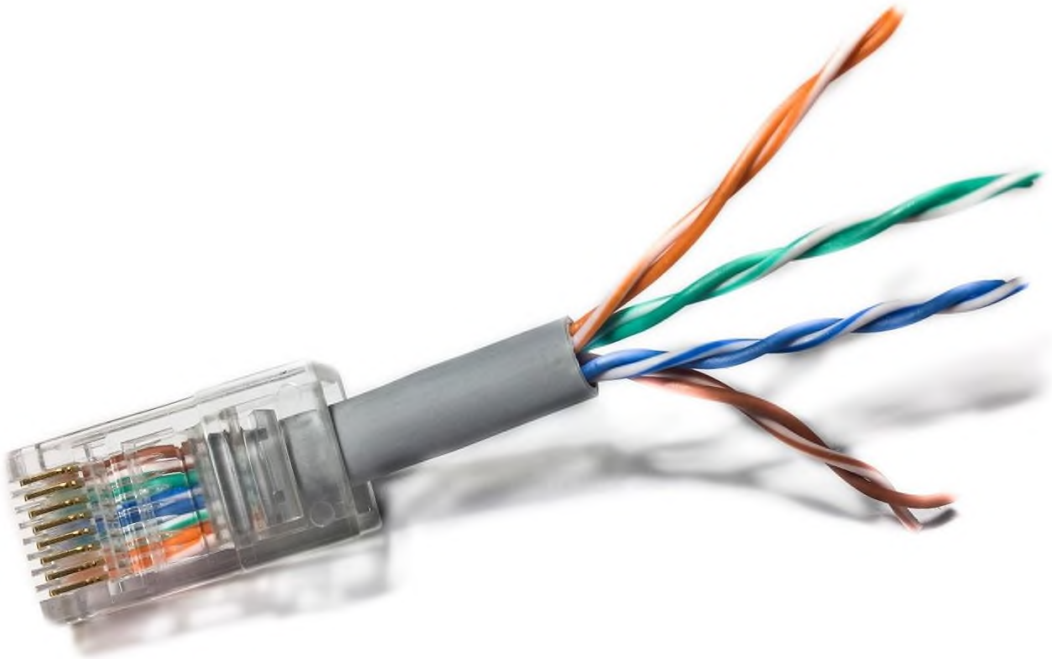


Рис. 1.6 Вита пара



Рис. 1.7 Оптоволокно

Принцип роботи

Метод, який використовує Ethernet для управління доступом - CSMA/CD. Перед відправленням даних в мережу інформація «нарізується»на сегменти, які мають розмір від 72 до 1526 байт. Після цього до протоколу додається заголовок, який містить в собі адресу відправника та отримувача даних. Також є «кінцевик» , який містить в собі контрольну суму, що використовується для контролювання виникнення помилок. Якщо протокол, який приймається, має різницю від того, який передається, це означає, що сталась колізія. Усі передачі відкладаються, в яких виникли помилки, та через деякий випадковий час, процес повторюється. Саме технологія управлінням доступу CSMA/CD зроблена для контролю колізій та вже враховує їх виникнення.

Таблиця 1.1

Різновиди Ethernet

Назва	Швидкість	Кабель	Стандарт
Ethernet	10 Мбіт/с	Тонкий та товстий коаксіальний кабель, вита пара, оптоволокно, оптика	802.3
Fast Ethernet	100 Мбіт/с	Оптоволокно, вита пара, оптика	802.3u
Gigabit Ethernet	1 Гбіт/с	Оптоволокно, вита пара, оптика	802.3z та 802.3ab
10G Ethernet	10 Гбіт/с	Вита пара, оптика	802.3ae та 802.3an

Технологія Ethernet має два підрівні, а саме LLC та MAC. MAC-адреса це особливий ідентифікатор технічного приладу, який приєднаний до мережі Ethernet. Це саме унікальний номер мережевої карти, а не загального комп’ютера.

Типи MAC-адреси :

- Індивідуальні (виділені комп’ютери)

- Групові (для певної кількості комп’ютерів)
- Широкомовні (для усіх комп’ютерів мережі)

Адреса може присвоюватися як і централізовано, так і локально. Централізовано, у випадку, якщо назначає постачальник технічного оснащення, а локально, коли назначає адміністратор мережі.

FastEthernet

Дана технологія була реалізована у 1995 р. та працює на основі стандарту 802.3u. Швидкість передачі даних – 100 Мбіт/с, що в 10 разів більше, ніж в класичній технології. Відмінність від Ethernetв тому, що змінились деякі компоненти конфігурації засобів, які знаходяться на фізичному рівні, це допомогло посилити пропускну здатність, а саме типи кабелю, які застосовуються, кількість хабів та розмір сегментів.На фізичному рівні використовується більш складна структура на відміну від Ethernet. Є три види FastEthernet :

- 100Base-Fx – багатомодове оптоволокно, яке включає два волокна

- 100Base-Tx – двухпарна вита пара, яка відноситься до 5 категорії

- 100Base-T4 – чотирьохпарний кабель, на основі витої пари, який відноситься до 3 категорії

GigabitEthernet

GigabitEthernet був розроблений у 1998 р. Дана технологія працює за стандартом 802.3z або 802.3ab. Продуктивність в даній технології – 1 Гбіт/с (1000Мбіт/с). Цей стандарт налічує в собі 5 стандартів фізичного рівня, для яких використовується оптоволокно(1000Base-X), вита пара(1000Base-T), а також екранований збалансований мідний кабель(1000Base-CX). Також стандарт 1000Base-T підтримує функцію автоузгодження між технічними пристроями, які працюють на швидкостях 100 або 1000 Мбіт/с, це дає змогу користувачам

використовувати стандарт FastEthernet і при необхідності перейти на гігабітну технологію. На самому початку створення в стандарті описувались напівдуплексні гігабітні з’єднання з використанням мережевих хабів, але більше дана особливість не оновлюється, зараз використовується тільки повнодуплексний режим із з’єднанням через світч.

Отже, GigabitEthernet гарантує дуже швидкий обмін інформацією між користувачами інтернет локальних мереж та зазвичай його використовують для побудови корпоративних мережах, наприклад, в офісі або житловому будинку.

1.5 Технологія Wi-Fi та її особливості для локальних мереж

Wi-Fi – набір стандартів IEEE 802.11, які використовуються для передачі цифрових потоків по радіоканалам. Стандарти безпровідних мереж було створено Інститутом інженерів з електротехніки та електроніки – IEEE.

Безпровідні мережі умовно можна поділити на декілька типів : персональні (WPAN) , локальні (WLAN), міські (WMAN) та глобальні (WWAN). В локальних мережах найбільшої популярності та розповсюдженості набув стандарт Wi-Fi. Дані мережі мають різні стандарти (рисунок 1.8).

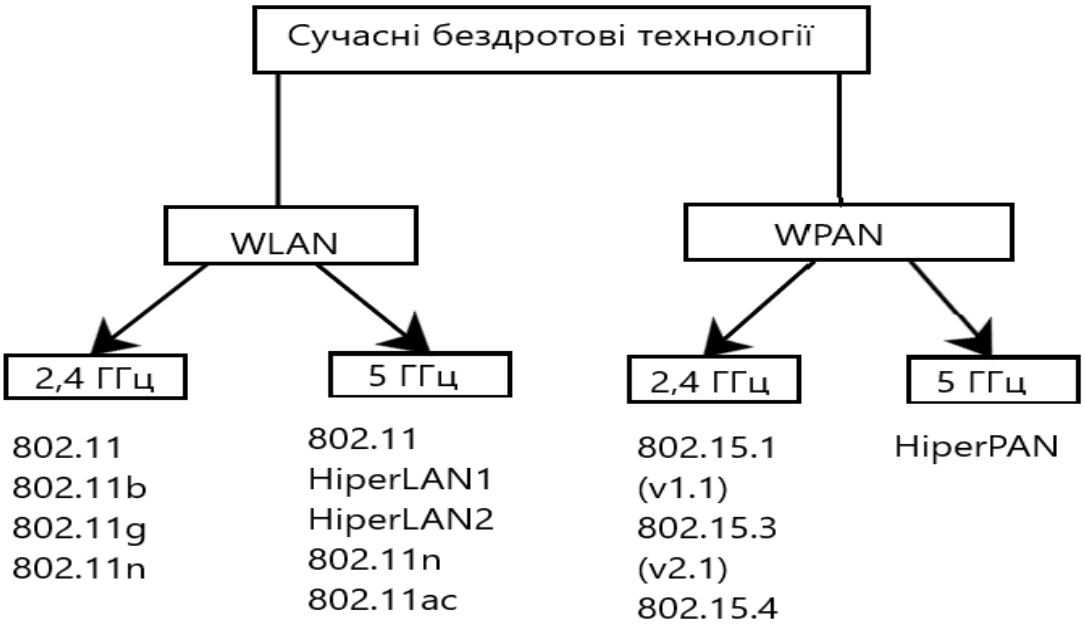


Рис. 1.8 Стандарти безпровідних мереж

На даний момент розроблені самі основні стандарти Wi-Fi мережей :

- IEEE 802.11 – основний стандарт, який має низьку швидкість передачі даних
- IEEE 802.11b – передає інформацію на частоті 2,4 ГГЦ зі швидкістю 11 Мбіт/с
- IEEE 802.11a – дозволяє працювати на частоті 5 ГГЦ , де швидкість становить 54 Мбіт/с
- IEEE 802.11g – має аналогію з минулим стандартом, але має сумісність зі стандартом 802.11bта використовує частоту 2.4 ГГц
- IEEE 802.11n – працює в спектрах 20 та 40 Мгц , максимальна кількість передавачів – 4
- IEEE 802.11ac – самий новий стандарт, який працює на частотах 2,4 та 5 ГГЦ. На даний день він має саму максимально можливу швидкість передачі даних, а саме 1,3 Гбіт/с

Принцип роботи

Wi-Fівикористовує радіохвилі для передачі даних. Даний стандарт працює через радіочастоти для передачі інформації від роутера, який являє собою джерело сигналу до обладнання або одержувача. Доступом до інтернету в цьому стандарті є технологія пакетної передачі даних Ethernet. Радіочастоти вимірюються в гігагерцах.

Wi-Fi працює у двох діапазонах частот : 2,4 ГГц (стандарт 802.11b) та 5 ГГц (стандарт 802.11a). Маршрутизатори з частотою 2,4 ГГц мають більшу зону покриття, але меншу швидкість передачі даних (рисунок 1.9).

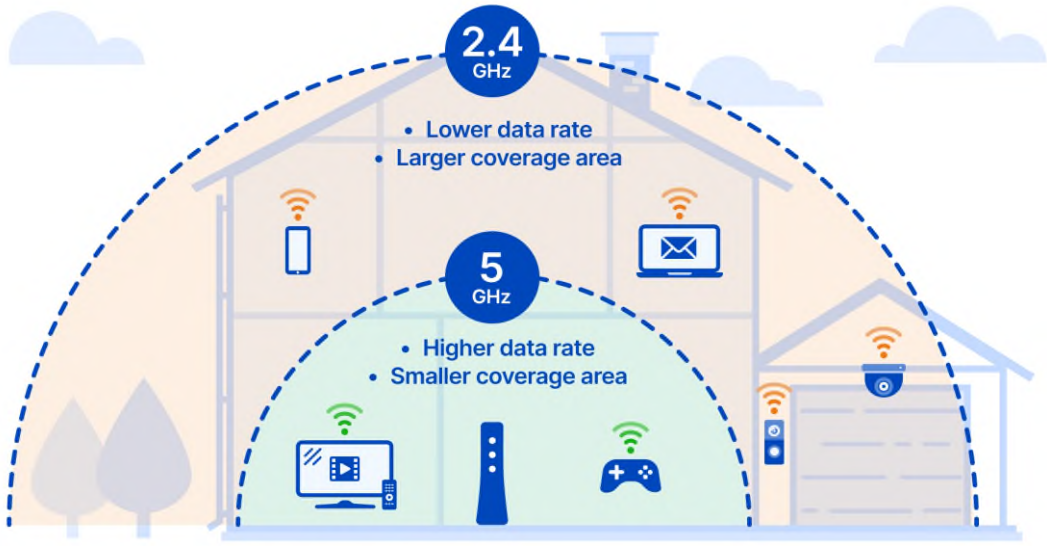


Рис. 1.9 Різниця покриття Wi-Fi на 2,4 ГГц та 5 ГГц

Роутер (маршрутизатор) – спеціалізований технічний пристрій, який дозволяє перенаправляти пакети даних. До роутера потрібно підключити кабель провайдера і до маршрутизатора можна підключити необхідну кількість обладнання, таких як : комп’ютери, смартфони для роботи в мережі Інтернет.Звичайний роутер працює на відстані 30 метрів в любу сторону, але погіршити або заблокувати передачу даних може предмет, який проводить електрику.

Безпека у Wi-Fiмережах

Також Wi-Fi має свої основні рівні безпеки :

WEP – цей режим вже вийшов з моди, він має самий найменший рівень захисту.

WPA – має більш надійний рівень захисту від минулого режиму та за використанням буває приватним та корпоративним. Даний режим містить багатоступеневу систему захисту. Забезпечує швидку і безпечну передачу інформації від однієї точки доступу до іншої, безпечне припинення сеансу.

WPA2 – більш новітня, оновлена та вдосконалена версія режиму WPA.

Топологія Wi-Fiмережі

Архітектура Wi-Fi має 3 основні типи :

- Режим Ad-Hoc (Independent Basic Service Set (IBSS) або Peer-to-Peer)
- Режим BSS (Basic Service Set)
- Режим ESS (Extended Service Set)

Ad-Hoc

Безпровідна мережа, яка не має постійної структури та сама найлегша за побудовою. Клієнтські станції, зазвичай комп’ютери або ноутбуки та інші пристрої, взаємодіють між собою та створюють мережу (рисунок 1.10).

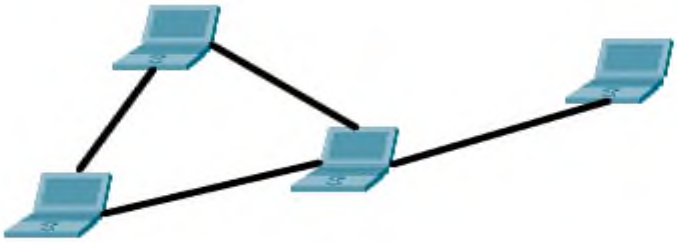


Рис 1.10 Схема роботи обладнання у режимі Ad-Hoc

Для створення даної мережі мінімальна конфігурація та мала кількість обладнання.Допомагає швидко та терміново розгорнути мережу.

BSS

У даному режимі всі абонентські станції взаємодіють один з одним не напряму, а за допомогою точки доступу (AccessPoint).

Точка доступу може бути в ролі моста, який матиме підключення до зовнішньої кабельної мережі (рисунок 1.11).



Рис. 1.11 Схема роботи обладнання у режимі BSS

ESS

Режим ESS дозволяє об’єднати декілька точок доступу, це означає, що ця мережа об’єднує кілька мереж BSS. В даному випадку точки доступу можуть взаємодіяти між собою. Даний режим краще всього застосовувати тоді, коли необхідно об’єднати в єдину мережу декілька користувачів або з’єднати кілька дротових та бездротових мереж (рисунок 1.12).

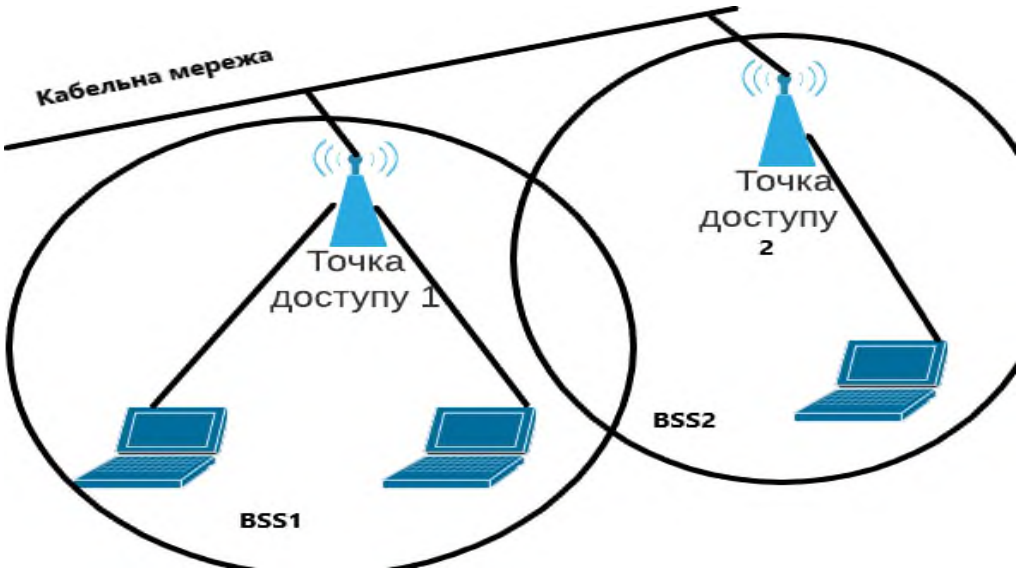


Рис. 1.12 Схема роботи обладнання у режимі ESS

Отже, Wi-Fi – універсальний спосіб передачі даних, який використовує значна кількість людства тому, що він відрізняється легкою зручністю, гарною швидкістю передачі даних та безпекою.

2 ОРГАНІЗАЦІЯ ІНТЕРНЕТ ЛОКАЛЬНИХ МЕРЕЖ

2.1 Недоліки та переваги інтернет локальних мереж

Переваги

На даний момент спостерігається велика кількість користувачів, які використовують глобальну мережу інтернет для власних задач або для робочої сфери, локальні мережи полегшують велику частину завдань, які ставить перед собою клієнт мережі, адже LANмає значні переваги для використання. На відміну від інших мереж, саме в локальній відсутня необхідність використання запозиченої телекомунікаційної лінії передачі.

Найбільш суттєвим аспектом даних мереж є доступ до інтернету. Якщо доступ до мережі Інтернет відсутній, то мережа не функціонує, поки знову не з’явиться з’єднання з Інтернетом.

Локальна мережа може використовуватися для передачі цифрових даних : зображень, документів, фотографій, музикальних файлів, відеофайлів. На кожному комп’ютері мережі користувач може корегувати, відновлювати та переглядати їх.

Також важливою перевагою локальних мереж є швидкість передачі даних. В залежності від цілі та конфігурування інтернет локальної мережі швидкість може бути різна, як досить швидка, так і досить низька. Але кожен користувач може налаштувати оптимальну швидкість для своєї конкретної задачі. При передачі даних відбувається мінімальна кількість помилок, що не наносить шкоду для використання. Це дає змогу ефективно працювати та не відчувати зв’язок, під цим можна розуміти, що висока швидкість передачі інформації між додатками та швидкість доступу майже незамітна для користувача. Але швидкість передачі даних повинна відповідати приросту та конфігурації до сучасних комп’ютерів, адже в іншому випадку це приведе до сповільнення інтернет локальної мережі та буде зниження доступу до мережевих ресурсів.

Локальна мережа використовується у різних сферах діяльності, наприклад, офіси, банки, лікарні, школи, магазини та інші. LANнадає таким сферам розділювати дані, вони можуть зберігатись на головному комп'ютері – сервері та бути доступними для кожної абонентської станції, яка підключена до мережі. Розподіл ресурсів надає доступ всім користувачам мережі використовувати периферійні пристрої, такі як принтери, сканери або факс. Розподіл програм дає доступ користувачам до відповідних робочих програм, які були єдиний раз встановлені централізовано.

Якщо мережа має тип на основі клієнт-сервер, де вся інформація та дані передаються за допомогою одного головного комп'ютера – сервера, то це дає можливість економно розподіляти пам'ять, тобто дані будуть зберігатися на головному ПК, але будуть доступні для будь-якого ПК.

Крім того, локальна мережа на основі головного серверу дає змогу вести роботу з файлами та інформацією, які мають великий обсяг та велике навантаження тому, що мережі даного типу використовуються для робочої сфери в якій в наявності є велика кількість обладнання, це призводить до накопичення та передачі великої кількості даних.

Якщо використовується рівноправна мережа, де немає загально виділеного центрального ПК, то це дає додаткові переваги над мережу типу клієнт-сервер, а саме це не дуже великі затрати на апаратне та програмне забезпечення та високу надійність, якщо вийшла з ладу одна абонентська станція, то це призводить до втрати доступу лише деякої інформації, а не цілих даних всієї мережі. Також перевагами такого типу мережі є :

- Просто налаштування та встановлення мережі
- Мала вартість і простота в експлуатації
- Не потрібно наймати додатковий персонал для наглядом за мережею
- Відсутня залежність комп'ютерів від сервера

- Кожний користувач самостійно керує доступом ресурсами власного ПК
- Простота побудови

За допомогою локальних мереж можна вирішувати такі задачі :

- Можна з’єднати фізично або за допомогою радіосигналу комп’ютери та усі пристрої, які підключені до мережі на невеликому радіусі
- Зазвичай вже визначена обмежена кількість комп’ютерів, які будуть підключені до мережі
- Локальна мережа має велику пропускну здатність
- Висока якість каналів зв'язку передачі

Недоліки

У інтернет локальних мережах є багато переваг, які дають абонентам змогу вести свої завдання максимально ефективно та полегшити роботу всередині компанії або власної приватної домашньої мережі, це дає можливість користувачу зробити вибір саме в сторону LAN , а не будь-яких інших, але при наявності такої великої кількості гарних аспектів в локальних мережах існують також свої недоліки.

Одним з головних недоліків інтернет локальних мереж можна вважати їх не дуже велику географічну зону покриття, тобто залежність від відстані, зазвичай вони займають територію школи, офісу та не дуже великих компаній, на відміну від інших типів мереж, які можуть покривати набагато більшу зону, таку як село, місто, окремі країни або взагалі континенти.

Зазвичай більше недоліків виникає, якщо локальна мережа вибрана у варіанті клієнт-сервер, так як в даному типі потрібні додаткові матеріальні витрати, щоб купити апаратне устаткування, програмне забезпечення для головного ПК та підключених до нього автономних станцій. На відміну від

тимчасової мережі (або ще рівноправної), мережа з виділеним головним сервером менш гнучка, а також більш дорожча ніж окремий комп’ютер.

Якщо з’єднання в мережі дротове, то потрібно забезпечити додаткову вартість на прокладку сполучних кабелів для роботи цілої мережі, це перешкоджає можливості переміщувати комп’ютери. Дане з’єднання являється дуже чутливим до пошкоджень, які можуть виникнути в кабельній системі, що може призвести до погіршення або зовсім до припинення роботи в цілій мережі.

Також мережа вимагає додаткового часу та грошей на навчання нового персоналу, а саме адміністратора мережі, який повинен займатися керування роботи усієї мережі, її оновленням, контролюванням доступу до розподілу ресурсів для користувачів, виявленням та усуненням помилок, а також резервним копіюванням. Якщо це велика офісна мережа або для компанії, то одного адміністратора може не вистачити, а потрібен буде штат з декількох адміністраторів.

Якщо до мережі підключено багато клієнтських станцій це може дати малу продуктивність та повільну швидкість передачі даних, але це залежить від специфікації комп’ютерів, яке в них устаткування та забезпечення, це може дати погані результати для роботи та витрачений час. Із-за цього можуть виникнути труднощі під час оновлення та зміни програмного забезпечення на клієнтських станціях, які підключені до мережі. Тобто є дуже велика залежність між швидкодією роботи та працездатністю центрального ПК та усієї мережі.

Зазвичай в роботі з інтернет локальними мережами виникають проблеми з питанням ефективної взаємодії управління між абонентськими станціями та забезпеченням безпеки і секретної інформації. Адже такі віртуальні місця представляють в собі середовище в якому є дуже велика ймовірність для поширення комп’ютерних вірусів. Так як комп'ютери об’єднані в одну загальну локальну мережу та кожен має доступ до файлів та ресурсів, що дає можливість хакерам або недосвідченим користувачам занести вірус або троян, це в свою чергу

поширитися на всі технічні пристрої та призведе до глобальних проблем в роботі цілої мережі та витоку важливої, а може і секретної інформації, яка потратить до рук шахраїв та злодіїв.

При використанні рівноправної локальної мережі є також свої недоліки, а саме : використовується невелика кількість комп'ютерів (приблизно до 10), відсутнє централізоване керування інформацією та можливість для пошуку даних. В такому типі мережі необхідно використовувати велику кількість пароль тому, що вони забезпечують доступ до ресурсів мережі, а також зменшується ефективність комп'ютерів, якщо їх ресурси інтенсивно застосовуються.

Є ще додаткові недоліки в локальних мережах :

- Відсутня загальна інформаційна база
- Інформація мережі залежить від стану ПК (якщо комп'ютер буде вимкнений, то інформація буде недоступна для користувача)
- Зазвичай низька безпека

Отже, інтернет локальні мережі мають свій ряд переваг та недоліків, вони мають усі специфікації, щоб задовольнити потреби максимально ефективної та продуктивної роботи, але це залежить від цілей та задач, які користувач ставить перед собою, яке в нього програмне та апаратне забезпечення, який тип мережі вибрано для побудови та інші класифікації, все це впливає на структура та роботу локальної мережі.

2.2 Безпека та захист інформації в інтернет локальних мережах

Безпека інформації та захист даних є дуже гострим та одним із найголовніших питань при побудові та роботі інтернет локальної мережі тому, що однією з функцій локальної мережі є доступ до загальних даних та обладнання, в свою чергу це може призвести до втрати інформації або несанкціонованого доступу. Щоб запобігти атакам хакерів та злочинців, які хочуть заподіяти шкоди або викрасти важливі дані, потрібен ефективний спеціаліст, а саме адміністратор

мережі, який матиме знання основ захисту даних у цій сфері, але наявність знань це лише мала частина, потрібно їх ефективно використовувати, розуміти функціонування та знати проблемні місця в локальних мережах.

Несанкціонований доступ – отримання доступу до даних шляхом втручання в програмне забезпечення та обладнання за допомогою різних злочинних махінацій, які перевищують службові та робочі цілі.

Щоб вирішити питання щодо проблем з безпекою та захистом інформації в локальних мережах використовують три основних метода: технічні, програмні та організаційні засоби.

Технічні засоби

До технічних засобів відносяться пристрої електричного, електронного та інших типів технічного характеру. Технічні засоби діляться на:

- Апаратні типи пристроїв, вони сполучаються з апаратним забезпеченням локальних мереж та вбудовані вже в апаратуру, зазвичай це захисні регістри, різні схеми для контролю та захисту інформації в апаратному забезпеченні
- Фізичні засоби, це електро-мехачні апарати та системи захисту, наприклад, охорона, сигналізація, відеоспостереження, двері під замком

Перевагами такого методу захисту є : надійність, висока адаптивність до оновлень. Недоліки : великі затрати, важка маса пристроїв.

Програмні засоби

Це програми, функції яких призначені та спеціалізовані для захисту інформації. До таких програм входять шифрування інформації, антивірусні програми, біометричний захист інформації, архівація даних.

Шифрування інформації (криптографічний захист) – виконує перетворення даних з метою забезпечення захисту інформацію. Шифрування відбувається за

допомогою криптографічного ключа. Цей ключ складається з послідовності бітів, які використовуються для шифрування та розшифрування інформації. Повідомлення передаються вільним чином, але приховується зміст інформації, яка передається, щоб упевнитися в її достовірності та правдивості.

Антивірусні програми (антивірус) – спеціалізована програма для захисту операційної системи комп’ютера від вірусів та його різновидів. Антивірус виконує наступні задачі для безпеки :

- Проводить сканування на наявність вірусів у мережі
- Блокує проникнення вірусів до комп’ютерів
- Мінімізує пошкодження системи від функціонування вірусу
- Можливість відновити пошкоджені файли

Біометричний захист інформації – метод, який використовує для перевірки особливі фізіологічні характеристики індивідуальності. Змістом цього процесу є визначення, чи справді людина є тією особистістю, якою вона себе кличе. Біометричну перевірку можна вважити найбільш точною, так як параметри, які надаються на перевірку дуже важко підмінити або майже неможливо (рисунок 2.1).



Рис. 2.1 Види біометричного захисту інформації

Види фізичних характеристик, які можуть перевірятися:

- Відбиток пальця
- Голосове розпізнавання
- Розпізнавання по обличчю
- Сканування сітківки ока
- Аналіз динаміки напису
- Геометрія обличчя

Архівація даних – стиснення певної кількості файлів в один єдиний файл (архів) з метою зменшення загального розміру вихідних файлів, можуть бути стиснені без втрат.

Також є додаткові спеціалізовані програмні засоби : брандмауер та proxy-сервер.

Брандмауер (firewall) – функціонально апаратна або програмна частина, що фільтрує інформацію, яка надходить від локальної мережі до глобальної. Можна вважати захисною стінкою між користувачем локальної мережі та виходом до глобальної інтернет мережі (рисунок 2.2).



Рис. 2.2 Брандмауер

Налаштування брандмауера(рисунок 2.3)**:**

- Натиснути кнопку Пуск Windowsта вибрати Параметри >Оновлення та безпека > Безпека Windows>Брандмауер та захист мережі
- Вибрати профіль мережі : Доменна мережа, Приватна мережа або Загальнодоступна мережа
- У розділі Брандмауер MicrosoftDefenderвстановити для параметра значення Увімк.
- Щоб вимкнути, потрібно перемкнути цей параметр у положення Вимк. Відключення Брандмауера MicrosoftDefender може зробити пристрій користувача більш вразливим для несанкціонованого доступу. Якщо потрібно використовувати додаток, що блокується, можна дозволити його використання через брандмауер замість відключення самого брандмауера

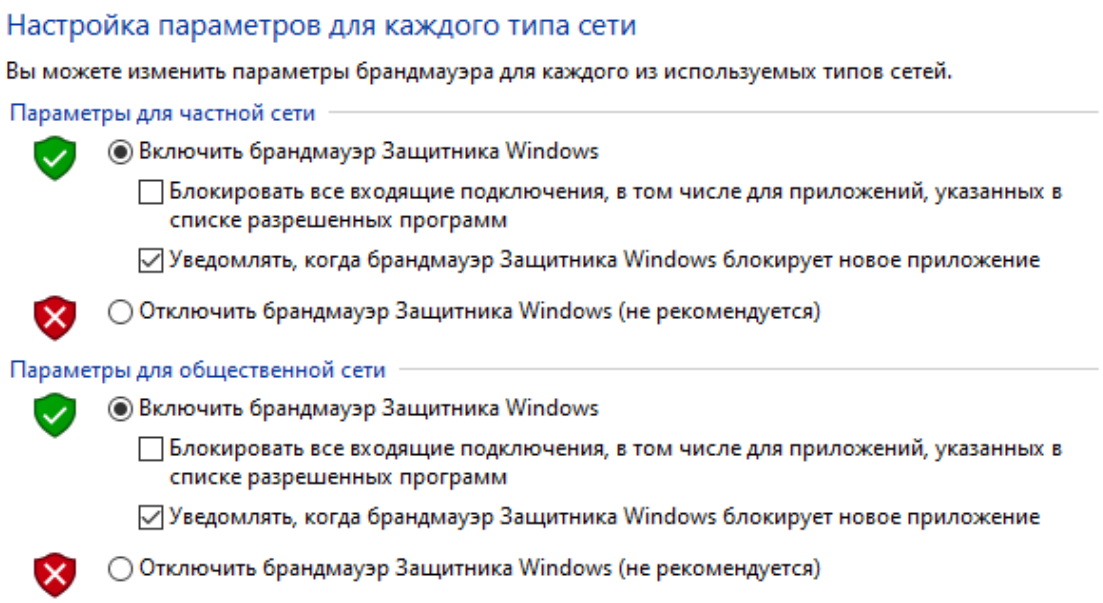


Рис. 2.3 Налаштування брандмауера

Функції брандмауера :

- Допомагає захистити комп’ютер від зловмисників або шкідливих програм у локальній мережі і в Інтернеті.

- Блокує підключення до додатків, яких немає в списку дозволених програм.
- Контролює доступ користувача до ресурсів мережі.
- Може дозволити підключення, лише якщо воно пройшло перевірку підлинності або якщо джерело є авторизованим користувачем, групою або комп'ютером.

Proxy-сервер – сервер-посередник, який здійснює контроль над виходом до Інтернету користувача, проміжний сервер, який знаходиться між користувачем та цілевим сервером, який дозволяє клієнтам виконувати непрямі запити (приймати та передавати їх через проксі-сервер) до інших мережних служб, так і отримувати відповіді і надсилати назад до користувача.А також створює умови при яких сайт думає, що проксі – це і є реальна людина (рисунок 2.4).

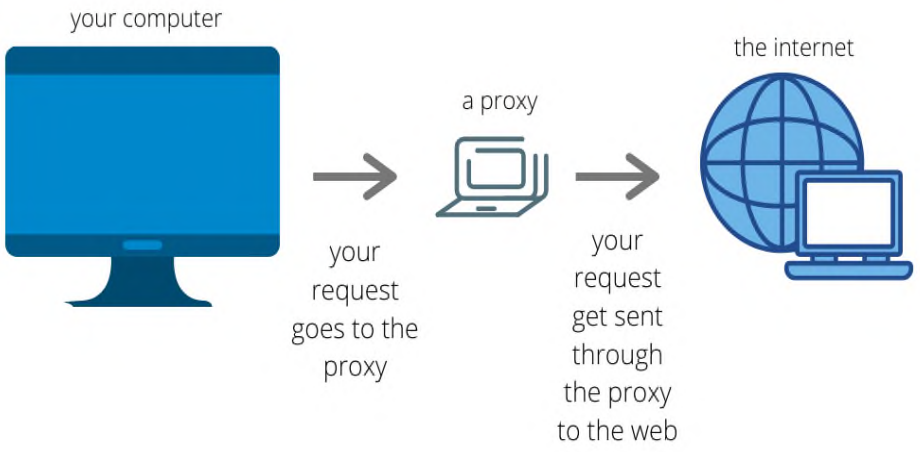


Рис. 2.4 Проксі-сервер

Завдання, які виконує proxy-сервер :

- Забезпечення конфіденційності
- Підвищує рівень безпеки, коли користувач виходить до мережі, атаки будуть направлені саме на проксі.

- Допомагає отримати доступ до заблокованих сторінок (сайтів, мессенджерів і т.д.).
- Приховує адресу внутрішньої мережі.
- Прискорення роботи інтернету (зберігається кешовані копії веб-сайтів).
- Стиснення даних.

Налаштування проксі-серверу

Для прикладу буде вибрана операційна система – Windows 10.

Щоб зробити проксі-сервер у Windows 10 потрібно зробити наступне :

- Відкрити основні налаштування мережі
- Вибрати пункт налаштувань «Мережа та інтернет»
- Далі перейти в підпункт «Проксі-сервер» (рисунок 2.5)

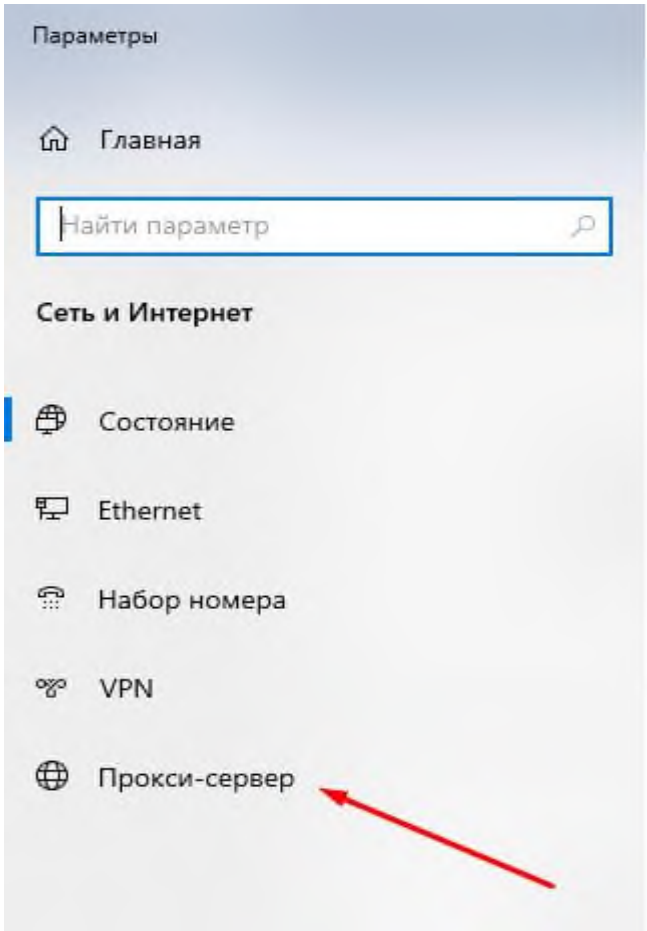


Рис. 2.5 Підпункт «Проксі-сервер»

- Спуститися до блоку налаштувань «Налаштування проксі вручну»
- Перевести тумблер «Використовувати проксі-сервер в положення «Вкл.».
- Ввести адресу проксі-серверу та порту у відповідні поля (рисунок 2.6).
- Зберегти налаштування

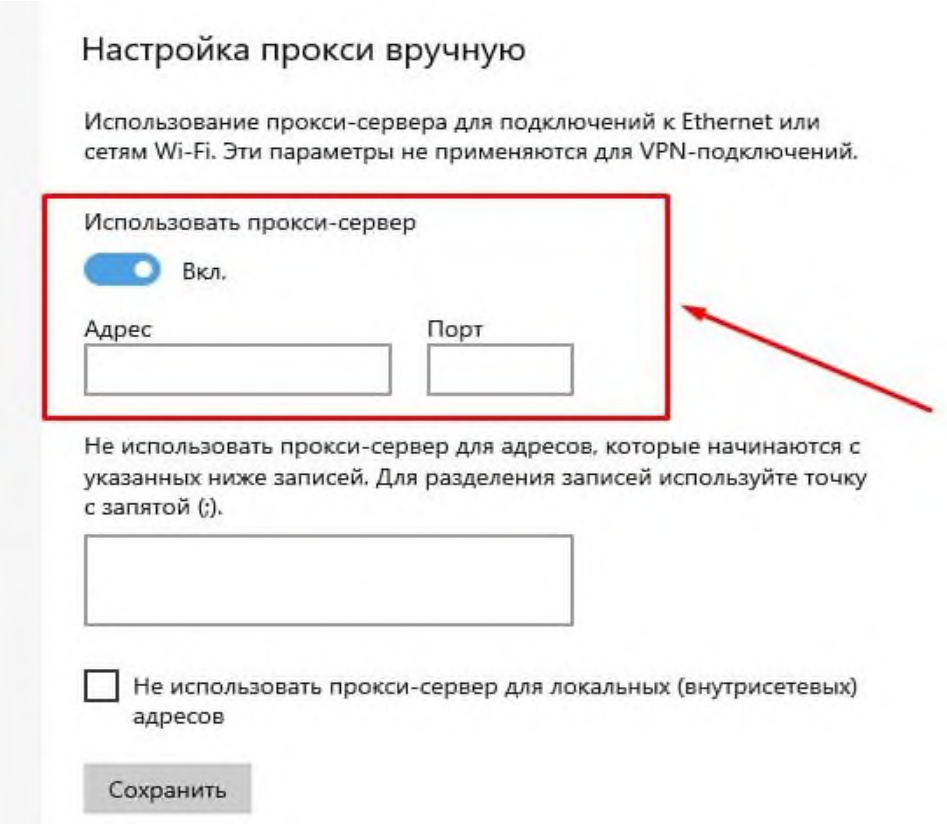


Рис. 2.6 Налаштування проксі-серверу вручну

Перевагами програмних засобів є : висока надійність, стабільність, простота встановлення, а недоліками : зменшує та обмежує здатність функцій мережі, використання ресурсів апаратного забезпечення.

Організаційні засоби

Даний метод займається організаційно-технічними питаннями. Можуть виникнути проблеми, які не залежать від дії людини або мережі, наприклад, труднощі в системах електропостачання, стихійні лиха, налаштування кабельної систем і тд.

Щоб не допустити втрати важливої інформації під час незапланованого відключення електроенергії компанія може використовувати дубльовані системи електроживлення для абонентських станцій, встановити резервні електрогенератори, мати електропровідники, які відповідають навантаженню.

Захист від стихійних лих (пожежа, гроза, повінь, землетрус і т.д) залежить від вибору розміщення апаратного забезпечення, це повинні бути захищенні приміщення та зберігання резервних копій даних.

Для налаштування кабельної системи організація повинна мати просторе приміщення, прокладати кабельну системи згідно умов та правил доступу до неї користувачем.

Переваги цього методу являються : допомагають налаштувати локальну мережу для ефективної роботи, постійний розвиток та оновлення. Недоліки : залежність від подій та чинників, які людина не передбачає.

Віртуальна приватна мережа

Ще одним вирішенням питання щодо безпеки в локальних мережах може бути використання віртуальної приватної мережі, а саме VPN.

VPN (VirtualPrivateNetwork) – приватна мережа, яка дозволяє користувачу використовувати Інтернет безпечним доступом. Цей метод створює віртуальні лінії зв'язку, які мають назву «VPN-тунелі». Інформація, яка проходить через дані тунелі приховується. Технологія VPN шифрує усі дії користувача в Інтернеті, все що він відправляє та отримує. Якщо абонент входить тільки через віртуальну приватну мережу, видно не його справжнє джерело підключення, а один із багатьох VPN-маршрутизаторів.

Для створення безпечної та захищеної системи безпеки можна використовувати саме VPN, оскільки вони забезпечують інкапсуляцію, аутентифікацію і повне шифрування даних в інтернет локальних мережах.

Перевагами даної технології є : доступ до заблокованих веб-сайтів, конфіденційність, можна позбутися від стеження. Недоліки : уповільнення роботи, блокування VPN.

Налаштування VPN

Для налаштування приватної мережі також оберемо для прикладу операційну систему Windows 10.

- Відкрити параметри мережі
- Обрати пункт налаштувань «Параметри мережі та Інтернет»
- Далі обрати підпункт «VPN» (рисунок 2.7)
- Натиснути на іконку «Додати VPN-підключення» (рисунок 2.7)

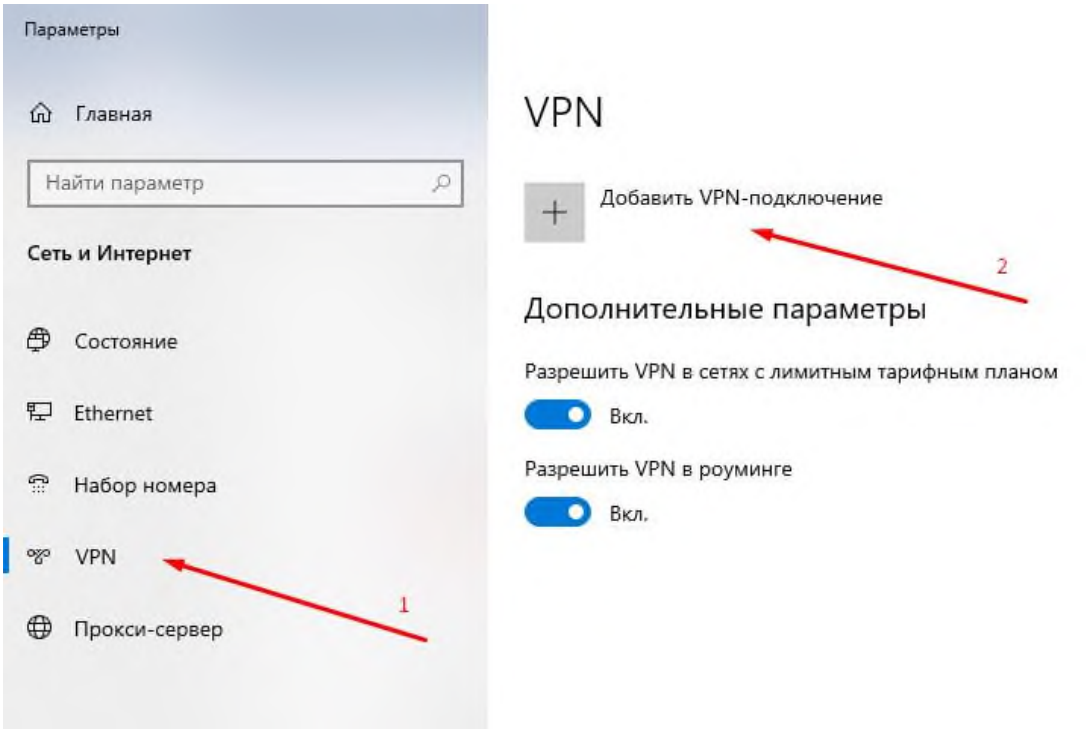


Рис. 2.7 Налаштування VPN

У розділі «Додати VPN-підключення» зробити наступне (рисунок 2.8):

- У полі «Постачальник послуг VPN»вибрати Windows (вбудований)
- У полі ім’я підключення ввести зрозуміле вам ім’я. Це ім’я підключення VPN, яке потрібно буде шукати для підключення

- У полі «Ім’я або адрес серверу» ввести адресу для серверу VPN
- Вибрати «Тип VPN-підключення», яке необхідно створити. Потрібно знати, який тип VPN-підключення або служба VPN використовується
- У полі «Тип даних для входу» вибрати тип даних для входу, які необхідно використовувати. Це може бути ім’я користувача та пароль, одноразовий пароль, сертифікат або сім-карта. Ввести свої ім’я користувача та пароль у відповідні поля (при необхідності)
- Зберегти налаштування

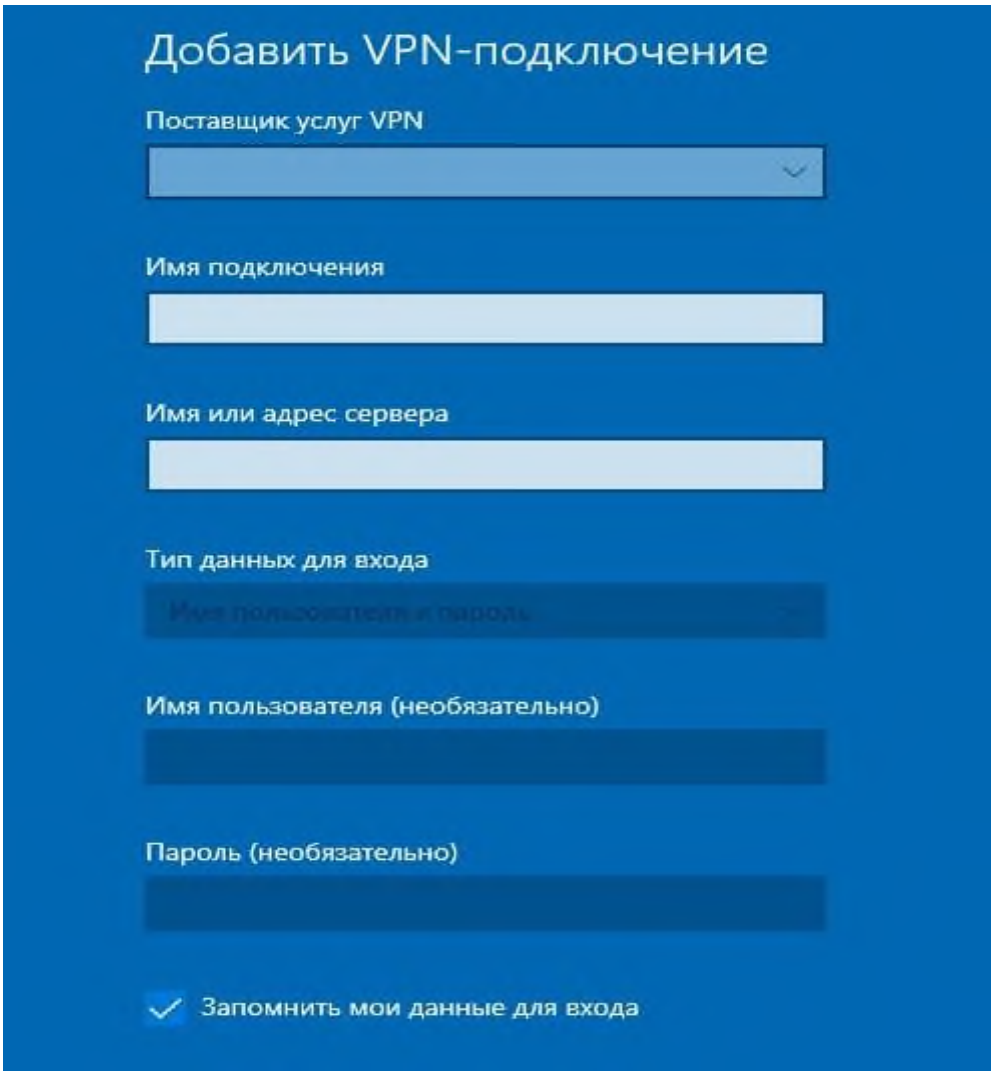


Рис. 2.8 Додавання VPN-підключення

Отже, існує багато різновидів та засобів для забезпечення та захисту інформації в локальних мережах, але треба розуміти, що дані рішення не можуть дати повну та абсолютну безпеку. Щоб добитися мінімального ризику втрати

важливої інформації потрібно комплексно та ефективно підходити до питань захисту та безпеки в LAN.

2.3 Майбутній розвиток інтернет локальних мереж

Сучасний технологічний світ не стоїть на місці, кожен день з'являються та модифікуються нові технології, обладнання. Не є винятком і інтернет локальні мережі, які продовжують бурхливо розвиватися, причому досить швидко. Теперішня тенденція, яка спрямована на застосування комутації впливає на всі фактори виконання мережевої передачі інформації, включаючи тип приладів, який ми купуємо, і виробників, у яких купуємо, та закінчуючи вибором налаштування наших локальних мереж.

Замість пасивного кабелю, який з'єднує комп’ютери, в значній кількості з’являється сучасне та ефективне комунікаційне обладнання – комутатори, маршрутизатори та шлюзи. Саме ці технічні пристрої можуть дати можливість побудови великих інтернет локальних мереж, які зможуть нараховувати до тисячі комп’ютерів та мати складну структуру.

Розвивається і одна з головних технологій, яка належить до одного з варіантів побудови інтернет локальних мереж, а саме Ethernet. Першим рішенням для покращення даної технології є заміна застарілих хабів на сучасні Ethernetсвітчі. Вони схожі за виглядом на хаби, але Switchмає різні характеристики многопортового бриджу.EthernetSwitch, який існує на даний час має досить гарні специфікації для користувача : 16 портів і робить передачу пакетів між будь-якими двома незалежно від них. Пропускна спроможність такого світча досягає до 80 Мбіт/с.

Наступним рішенням також може стати – повнодуплексний Ethernet, для його використання в наявності має бути новий світч і новий мережевий адаптер. Це дасть можливість одночасно пересилати два пакети, якщо вони йдуть в різних напрямках. Дане рішення може збільшити пропускну здатність майже в два рази, але знаходиться тільки на стадії затвердження. Стандарти Ethernet стрімко

розвиваються, вже існують 40 GigabitEthernet та 100 GigabitEthernet і це далеко не межа.

На даний час розробникам на вибір є чотири можливості модернізації Ethernet :

- GigabitEthernetдля корпоративних користувачів
- Бездротовий Ethernet, який можна буде використовувати вдома та офісі
- Мережеві засоби зберігання даних
- 10 GigabitEthernetв міських мережах, що дасть змогу розширити ще більше інтернет локальні мережі

У разі затвердження нових видів та модифікацій Etherneti появи нового та відповідного апаратного забезпечення, зміни більшою мірою торкнуться частини в якій вони передаються між собою, це хаби, світчі та інтерфейси, а частина, якою вони представлені до комп’ютера та користувача може не зазнати великих змін або взагалі не змінитися, що дозволить абонентам використовувати наявне програмне забезпечення та засоби. Модифікація Ethernet з кожним роком буде все більше поширюватися та надасть своїм користувачам такі особливості : продуктивність та ефективність масштабного характеру, збільшення радіусі дії, низька вартість, гнучкість і сумісність, простота у використанні з керованим адмініструванням.

З'явилась ще тенденція, яка тільки набирає своїх обертів та популярності і зачіпає інтернет локальні мережі, а саме, що в них стали оброблятися інформація, яка раніше була невластива обчислювальним мережам, це голосові повідомлення, відеозображення, відеоконфернції, малюнки і т.д. Такий різкий напрям поширення інформації змусив внести зміну в роботу протоколів, комунікаційного обладнання та мережеві операційні системи. Це призводить до покращення апаратного та програмного забезпечення локальних мереж, їх модифікацій, що покращує ефективність роботи для користувача.

Різні спостереження та статистики дають змогу побачити, що в найближчому майбутньому кількість технічних інновацій та підключень буде тільки зростати, приблизно на 25% щорічно. Інтернет технології будуть впроваджуватися з кожним разом все швидше та активніше, і чим далі, тим більше простих або складних пристроїв знадобиться підключати.

У відповідності з такими темпами розвитку технологій в інтернет локальних мережах будуть формуватися нові вимоги – низькі витрати на енергоресурси, більш тривалий час автономної роботи, покращення покриття мережі, збільшення кількості пристроїв та загального обладнання. Спрощення мережних модулів і ефективна модель дозволять досягти максимально автономної роботи, яка може бути розрахована до 10 років. Таким чином інтернет локальні мережі будуть споживати дуже малу кількість електроенергії. Але реалізація даних вимог буде відрізнятися в залежності від того, до якої технології це буде застосовано.

Також дуже активно розвивається один із головних варіантів бездротового з'єднання в інтернет локальних мережах – Wi-Fi, він постійно знаходиться в стадії оновлення. Останньою версією є 802.11ac.

На даний момент існує декілька варіантів для розвитку стандарту 802.11, а саме :

- 802.11af – версіяWi-Fiв білих смугах телевізійного діапазону (від 54 до 695 МГц). Інформація передається в локальних смугах пропускання 6 або 8 МГц. Максимальна можлива швидкість передачі до 26 Мбіт/с. Радіус дії цього стандарту може охопити багато кілометрів, але при роботі на низьких частотах. Він ще не використовується, але може стати дуже затребуваним в майбутньому.
- 802.11ah – один із варіантів Wi-Fi, який використовує неліцензований діапазон ISMв 902-928 Мгц. Також використовує низькі частоти, але на відстань до кілометра.

- 802.11ax – оновлена версія стандарту 802.11ac. Використовується в діапазонах 2,4 і 5 ГГц, але скоріш за все буде працювати в смузі частов 5 ГГц виключно для використання смуги пропускання 80 або 160 Мгц. Можлива максимальна швидкість передачі даних до 10 Гбіт/с.
- 802.11ay – розширення стандарту 802.11ad. В планах на цей стандарт використання його на смузі частот в 60 ГГц, а головною цілю являється зростання швидкості до 20 Гбіт/с. В планах розширити радіус дії до 100 метрів.

Саме через ці причини бездротові види з’єднання мереж стали дуже вигідним та ефективним рішенням для мобільних та комп’ютерних користувачів, а також виступили в якості механізму до швидкого доступу для дуже широкого кола клієнтів, які використовують LAN.

Отже, можна зробити висновок, що інтернет локальні мережі мають дуже велику кількість користувачів, яка з кожним все більше та більше зростає, це в свій час дає розробникам покращувати та удосконалювати усі критерії (програмне та апаратне забезпечення, стандарти та технології, швидкість і безпеку) згідно вимог абонентів, які їх використовують. На даний час локальні мережі займають важливі та навіть провідні позиції у своєму використанні в Інтернеті, але на мою думку, саме подальший розвиток Інтернету буде дуже впливати на розвиток мережі LAN.

3 ПРАКТИЧНЕ НАЛАШТУВАННЯ ІНТЕРНЕТ ЛОКАЛЬНОЇ МЕРЕЖІ

3.1 Налаштування та застосування інтернет локальної мережі

В даному розділі буде описано практичне налаштування домашньої інтернет локальної мережі, її схематичне моделювання та тестування за допомогою стандартного програмного забезпечення.

Інтернет-провайдер

Для того щоб у користувача був доступ до ресурсів та мережі всесвітньої глобальної мережі у нього повинен бути постачальник послуг Інтернет (провайдер).

Провайдер – організація, яка забезпечує абоненту доступ до використання мережі Інтернет.

Кожне підключення до Інтернету, без різниці від типу з’єднання, це підключення устаткування користувача до функціоналу провайдера. Комп'ютер отримує доступ до ресурсів серверу провайдера, який має постійну лінію зв’язку з мережею Інтернет.

Сервер інтернет-провайдеру описує швидкість передачі, якість наданої послуги для користувача та яку одночасну кількість абонентів він може обслуговувати. В залежності від тарифу, який обрав користувач, компанії-провайдери виділяють для абонента деяку частину від загальної пропускної здатності власної лінії виходу до мережі Інтернет. Ідентифікація споживача послугами інтернет-провайдера відбувається за допомогою логіна та пароля.

Контакт провайдера з мережею Інтернет відбувається наступним чином:

- Користувач відправляє запит до серверу провайдера
- Діє обробка даного запиту та перенаправлення на потрібний сервер в Інтернеті.
- Реакція Інтернет-сервера на устаткування провайдера.

- Йде передача інформації на обладнання користувача.

Даний рисунок показує роботу інтернет-провайдера за допомогою якого відбувається доступ до ресурсів Інтернету обладнанням абонента (рисунок 3.1).

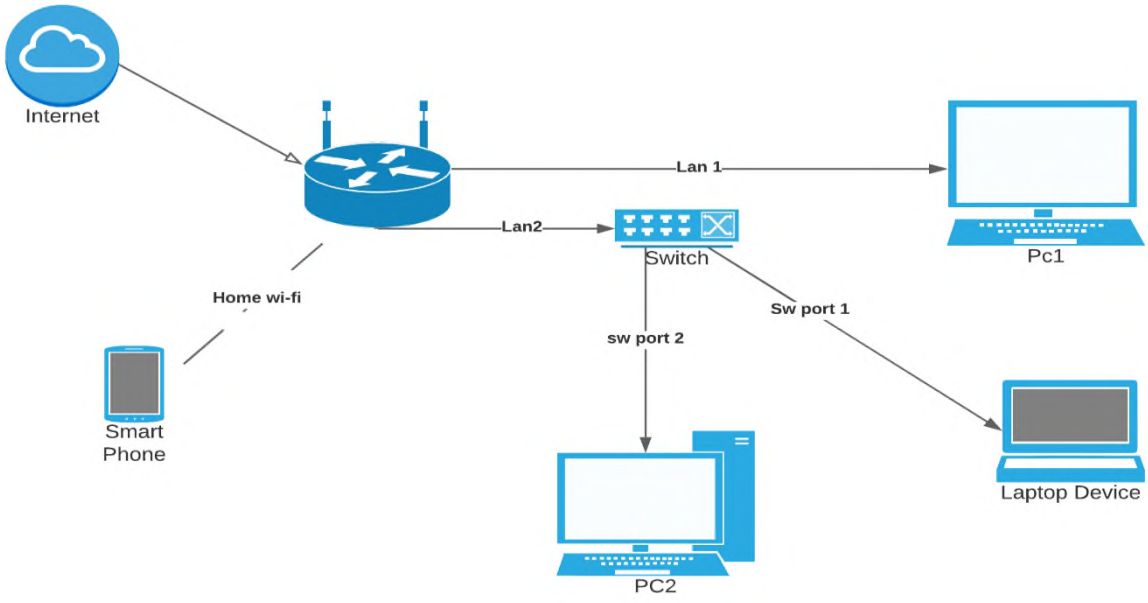


Рис. 3.1 Робота інтернет-провайдера

DHCP

DHCP (DynamicHostConfigurationProtocol) – мережевий протокол, який керує IP-адресами в локальних мережах та автоматично привласнює динамічну IP-адресу для кожного нового пристрою. За допомогою цього методу можна відмовитись від ручного налаштування комп'ютерів в мережі та дозволяє зменшити кількість помилок.

Адресація в даній мережі виведена за допомогою методу DHCP, сервером в мережі виступає – роутер. Всі сучасні роутери мають вже вбудований функціонал служби DHCP. Якщо дана функція налаштована і включена на роутері, то не потрібно буде налаштовувати мережеве підключення на абонентських пристроях. Для бездротових пристроїв потрібно лише включити Wi-Fi, вибрати потрібну мережу та ввести пароль при необхідності. Якщо з'єднання відбувається за

допомогою кабелю, потрібно, щоб він був підключений до мережевої карти комп’ютера.

При появі нового пристрою в мережі, служба DHCPперевіряє список вільних IP-адрес і привласнює йому один з них. Дублювання IP-адреси виключено.

Налаштування DHCP в мережі

- Підключити кабель інтернет-провайдеру до роутера
- Відкрити будь-який браузер та перейти за стандартними адресами 192.168.0.1/192.168.1.1 або можна знайти посилання на конкретний веб-інтерфейс сайту роутера на зворотньому боці роутера - наліпка знизу самого роутера (рисунок 3.2).

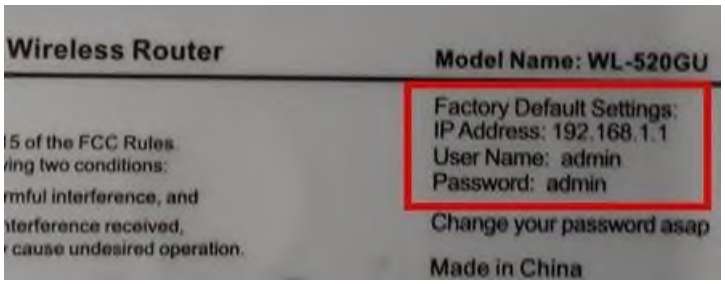


Рис. 3.2 Адреса та дані для входу в налаштування роутеру

- З’явиться запит імені користувача та пароля. Стандартні дані для входу (логін та пароль) зазвичай – adminта admin
- Здійснився вхід в налаштування роутера

На моєму прикладі, у веб-інтерфейсі роутера TP-Linkперейти до розділу Базових налаштувань (Basic) та в типі підключень (Connectiontype) вибрати пункт DynamicIPабо DHCP, в залежності від назви та зберегти налаштування (рисунок 3.3).

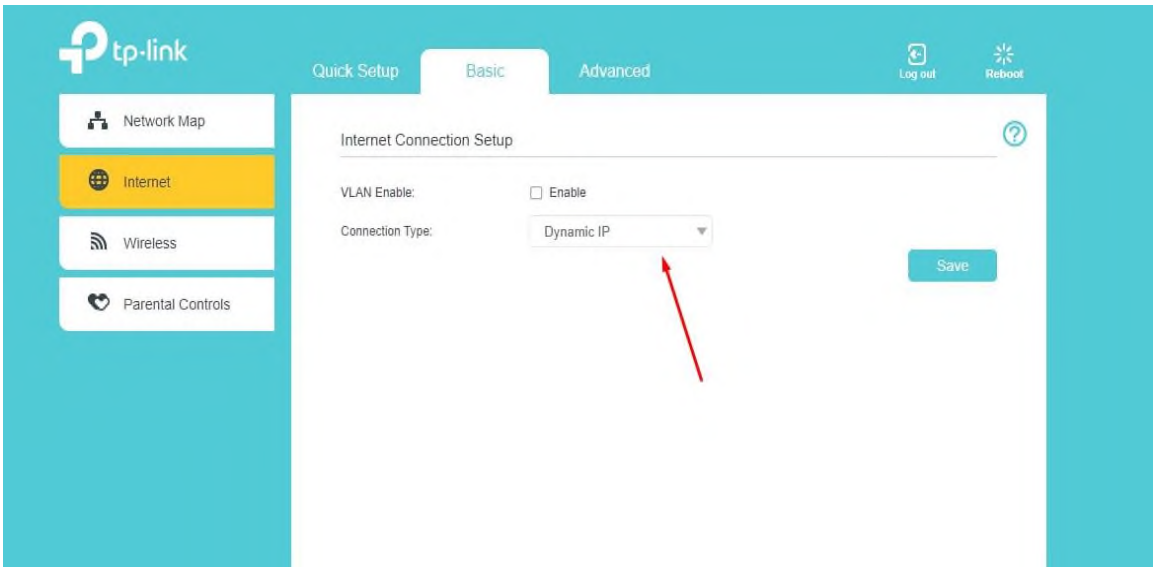


Рис. 3.3 Налаштування серверу DHCP

Для служби DHCPповинен бути заданий діапазон IP-адрес, які можна використовувати та вписати у відповідні поля. Поле «Адреса початку IP-пулу» – перша адреса діапазону, а «Адреса кінця IP-пулу» – відповідно остання. Отже, IP-пул адресів тільки один на роутері (рисунок 3.4).

Також обов'язковим параметром є поле «Строк оренди» – термін дії адреси, який рахується в хвилинах. Це час, на який конкретна IP-адреса може присвоюватися до конкретного пристрою. Після його закінчення IP-адреса може бути змінена або присвоєна до іншого пристрою. Зазвичай це поле вказано автоматично в налаштуваннях та його не потрібно змінювати (рисунок 3.4).



Рисунок 3.4 IP-пул адресів та строк оренди IP-адреси

IP-адреса – унікальний цифровий номер, який ідентифікує кожен пристрій в мережі та побудований на основі протоколу TCP/IP.

IP-пул адресів – набір із доступних IP-адресів, з якого назначаються IP-адреси користувачам при створенні користувачів.

Налаштування мережі

Схема підключення моєї мережі йде за технологією GPON. Домашня інтернет локальна мережа буде розділена на 2 кімнати, в першій – роутер, який відповідає за передачу інтернета до першої та другої кімнати, комп'ютер, принтер та декілька смартфонів. Перед роутером встановлений ONU-термінал, до якого йде передача сигналу по оптоволокну, а вже від ONU-термінала по витій парі під'єднаний роутер.В другій кімнаті – Ethernet світч, який під'єднаний до роутеру в першій кімнаті по витій парі, підключений до світча комп'ютер, а також ноутбук та мобільні телефони (рисунок 3.5).

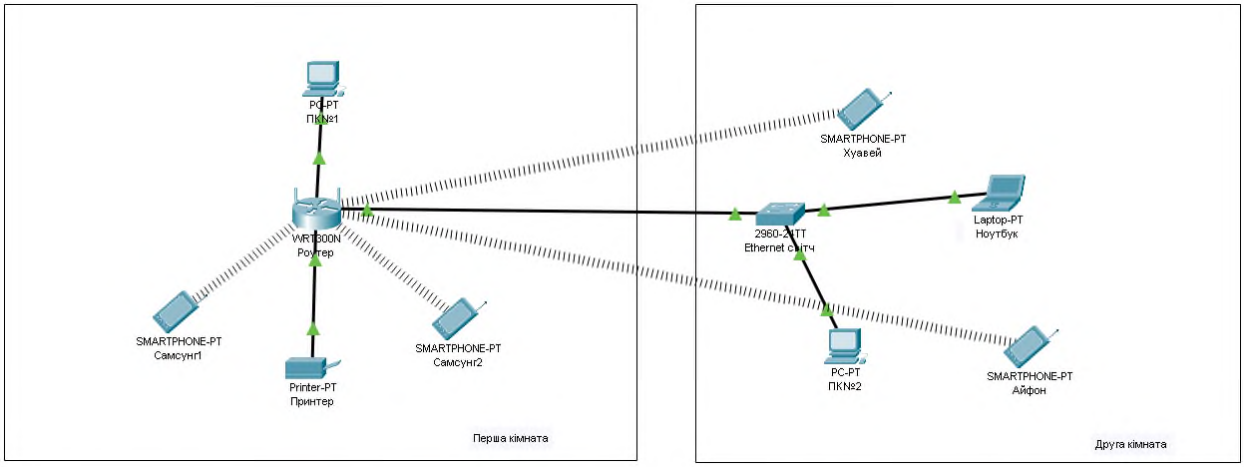


Рис. 3.5 Схема першої та другої кімнати в домашній інтернет локальній мережі

PON/GPON

У сучасних реаліях та проблемах з доволі частим та довгостроковим зниканням електроживлення постає питання про надання провайдерами Інтернету без світла, так як від цього залежить дуже багато. Одним із таких рішень стала

дана технологія, яка гарантує на певний період часу надання Інтернету без електроживлення, провайдер може встановити в себе на обладнанні ДБЖ, генератори, акумулятори та інші речі для підтримання енергії до обладнання.

Так як зазвичай, стандартна побудова відбувається в установці світча в кожному будинку і не кожен провайдер може встановити ДБЖ на кожен будинок, а також на шлюзи, сервера і т.д, які знаходяться перед світчами 2-го рівня. Оптична мережа означає заживлення базової станції, голови (OLT-а) з боку провайдера та підтримці його живленням для більшого часу споживання, а з боку користувача заживити ONU-термінал та роутер (через Powerbank, генератор, зарядну станцію, безперебійник та ін.) або ж підключити необхідній пристрій напряму та живити тільки ONU-термінал, щоб витрачати менше споживання енергії, таке рішення допоможе для вирішення певних задач користувача, для роботи або мінімально для оцінки поточної ситуації, щоб прочитати новини.

PON (PassiveOpticalNetwork) – пасивна оптична мережа. Це, по суті, технологія абонентського множинного доступу за допомогою одного волокна із застосуванням тимчасового мультиплексування (TDM) та поділу частотного тракту прийому/передачі (WDM).GPON, приставка G – означає Gigabit.

Основна ідея PON – використання всього одного прийомопередавального модулю в OLT (opticallineterminal) для передачі інформації безлічі абонентських пристроїв ONT (opticalnetworkterminal), також, які звуться ONU (opticalnetworkunit) в термінології IEEE і прийому інформації від них.

Схема підключення (рисунок 3.6)

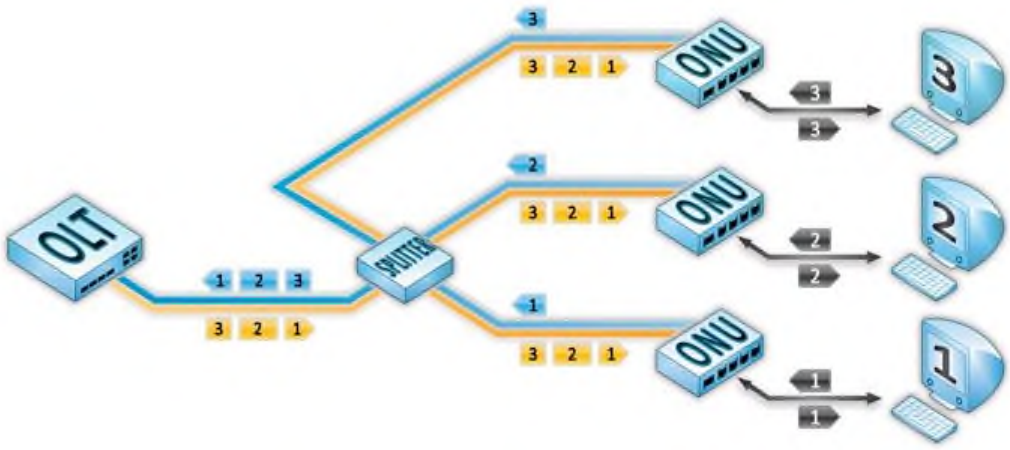


Рис. 3.6 Схема підключення PON

OLT – світч L2, який оснащений Uplinkпортами (щоб підключатися до обладнання L3 «шлюз») і Downlink портами (для створення мережі PON) (рисунок 3.7).



Рис. 3.7 OLT (opticallineterminal)

Модуль SFPOLT–промисловий стандарт модульних компактних прийопередатчиків (трансиверів), які використовуються для передачі та прийому даних, використовуються для приєднання плати мережевого пристрою (комутатору, маршрутизатору або подібного пристрою) до оптичного волокна (рисунок 3.8).



Рис 3.8 Модуль SFPOLT

Сплітер (Розгалужувач) – пристрій, який працює у розгалужувальному режимі в напрямку «провайдер-клієнт» і у змішувальному режимі у зворотньому напрямку (рисунок 3.9).



Рис. 3.9 Сплітер

ONU – оптичний модем, який підключається до термінальної точки за допомогою оптичного кабелю. Він використовується в приміщенні кінцевого користувача для підключення мережі PON з одного боку та взаємодії з користувачем з іншого боку (рисунок 3.10).



Рис. 3.10 ONU (opticalnetworkunit)

Налаштування роутеру

Роутер з'єднаний через порт WAN до загальної мережі інтернет, LAN порти відведені для комп’ютера в першій кімнаті та для кабельного з’єднання з Ethernet світчем в другій кімнаті. Смартфони працюють за допомогою бездротового з’єднання Wi-Fi.

Налаштування роутеру:

- Під’єднати кабель до WAN порту для підключення до мережі провайдера з цілью отримати доступ до Інтернету
- Включити та налаштувати DHCP
- Налаштувати Wi-Fi в веб-інтерфейсі роутера та шифрування
- Зберегти налаштування та перезавантажити роутер
- З’єднати через LANпорт кабелем Ethernetсвітч в другій кімнаті

WAN порт на роутері зазвичай виділений окремий кольором – синій колір, в цей порт потрібно конкретно під’єднувати кабель інтернет-провайдеру, а не будь-який інший, так як не буде працювати, а усі інші (4 однакових порти) зазвичай жовтого кольору це йдуть LANпорти, які створені для підключення пристроїв користувача – ноутбуків, комп’ютерів,Ethernetсвічів та інших (рисунок 3.11).

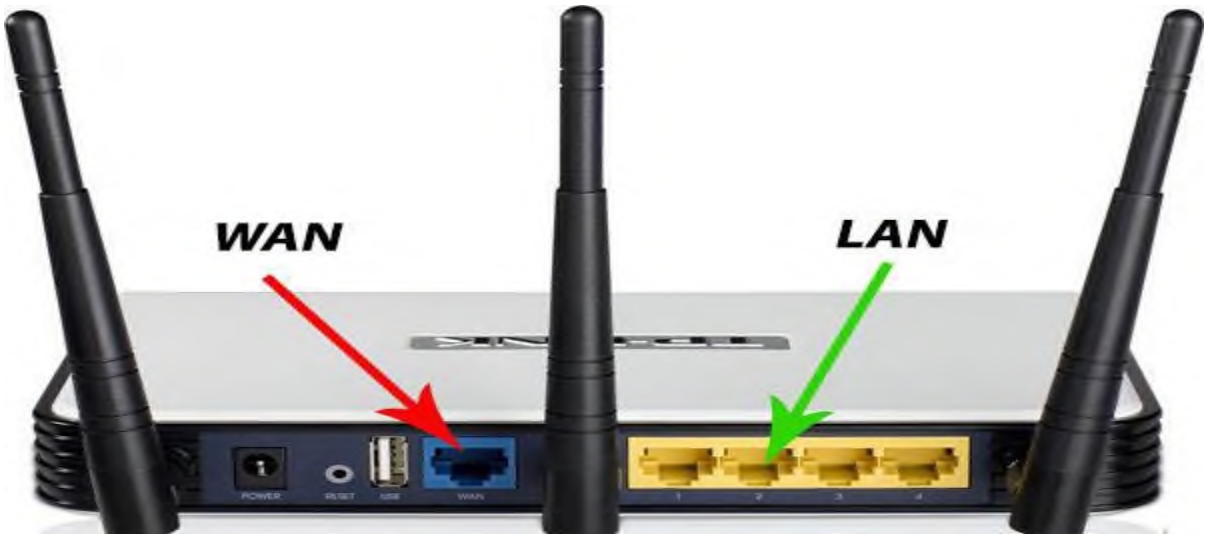


Рис. 3.11 Роз’єми роутера

Включаючи метод DHCPIP-адреса автоматично присвоюється від інтернет-провайдера на роутер, далі мережевий протокол DHCP передає IP-пул адресів на Ethernetсвітч.

Можливо, у деяких провайдерів є прив’язка за MAC-адресою при підключенні нового пристрою до мережі і поки його не прив’язати з боку інтернет-провайдеру, то інтернет не запрацює, в такому випадку потрібно зателефонувати/звернутися до вашого провайдеру і уточнити дану інформацію.

Налаштування Wi-Fi

Щоб під’єднатися до Wi-Fi потрібно зайти в налаштування абонентського пристрою, знайти в списку пункт «Wi-Fi» та в пошуку доступних мереж знайти потрібну, ввести пароль та буде автоматичне з’єднання з технологію бездротової передачі інформації.

У веб-інтерфейсі роутера зайти до розділу Wi-Fi, там можна вказати за бажанням власну назву мережі (SSID), пароль (PIN/Password) або залишити стандартні дані, які вказані на самому роутері, ключ захисту та інші дані (рисунок 3.12).

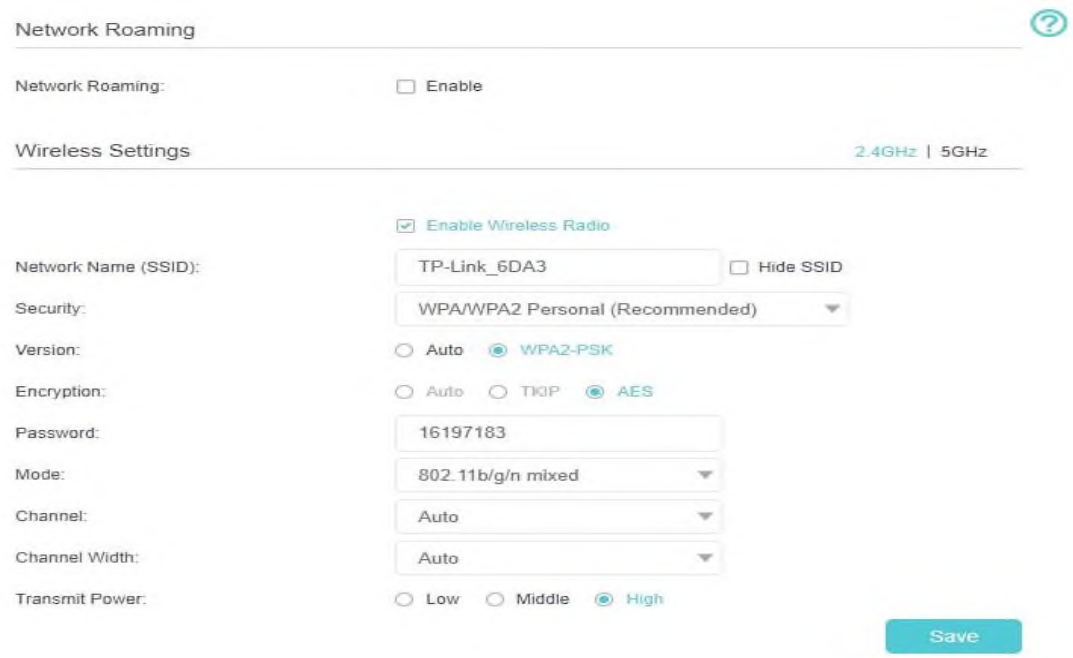


Рис. 3.12 Налаштування Wi-Fiта шифрування

Перевірка мережі

Потрібно перевірити з’єднання між комп’ютерами, які знаходяться в різних кімнатах, для цього необхідно зробити пінг між ними. Заходимо в командну строку, за допомогою комбінацій клавіш Win+R, вводимо в полі, що з’явилося «cmd» та прописуємо команду «ping та IP-адресу іншого комп’ютера», так як обмін пакетами йде, то мережа між комп’ютерами є (рисунок 3.13).

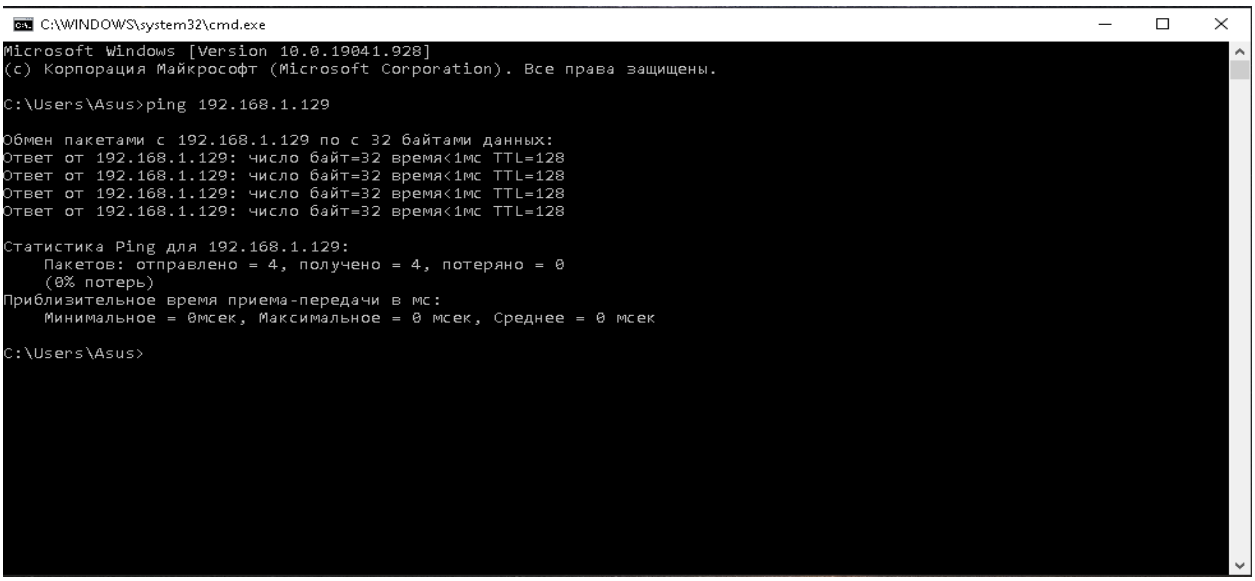


Рис. 3.13 Перевірка фізичного зв’язку між комп’ютерами

EthernetSwitch

Комутатор (це ж Ethernetswitchабо просто «світч») – відокремлений вузол, який відповідає за об’єднання декількох пристроїв в локальній мережі.

Різниця між маршрутизатором – підключення пристроїв через комутатор відбувається тільки через кабель, пристрій не забезпечує розгортання безпровідної мережі.

Ethernetсвітч під’єднаний через кабель типу вита пара до LANпорту роутера. Далі вже у вільні порти світча під’єднати кабелі від пристроїв в мережі – комп’ютера, ноутбука та інших при необхідності, пристрої мають автоматично під’єднатися, зазвичай світч не потребує ніяких налаштувань, лише під’єднати кабель живлення та кабель, який отримує сигнал від роутера. Вибір на користь світча полягає в тому, що це дасть більшу швидкість передачі даних в мережі через кабельне з’єднання ніж через бездротове, так як обладнання в другій кімнаті потрібно для енергоресурсних та ємних задач.

Також світч надає безпеку передачі інформації, ніхто з абонентів мережі, підключених до світча, не зможе використовувати та перехоплювати трафік інших абонентів.

Від Ethernet світча трафік буде комутуватися через відповідні Ethernet порти на абонентські пристрої, які знаходяться в другій кімнаті та підключені через кабельне з’єднання, а саме до комп’ютера та ноутбуката при необхідності підключення ще додаткових пристроїв, так як будуть ще вільні порти для підключення. Кожному Ethernet порту буде відповідати окрема IP-адреса, яка видається метод DHCP з IP-пулу адресів від роутера, який знаходиться в першій кімнаті. Для цього потрібно з’єднати вільні LAN порти на Ethernet світчі з LAN портами на комп’ютері та ноутбуці, які знаходяться в другій кімнаті.

Види Ethernet світчів

Кількість світчів на поточний час дуже багато, але більшість ключових характеристик даного пристрою діляться на кілька груп.

За керованістю:

- Некеровані – працюють у повному автоматичному режимі без необхідності та можливості впливу з боку користувача. Більше підходять для невеликих мереж, адже при підключені великої кількості пристроїв користувачів може обмежуватись пропускна здатність
- Керовані – підтримка управління користувачем через власний мережевий інтерфейс. Оптимальніше підходять для великих компаній

По класифікації відповідно до мережевої моделі OSI :

- 2-го рівня – працюють тільки в одному сегменті локальної мережі та тільки з MAC-адресою
- 3-го рівня – забезпечення більших можливостей підключення за допомогою підтримки мережевих протоколів IPv4, IPv6, IPX, PPTP, PPPoE, VPNта інші
- 4-го рівня – йдуть продуктивні та потужні пристрої, які автоматично аналізують дані, що передаються, і пізнають IP-адреси, протоколи TCP/UDP та інші різні параметри

За типом комутації :

- Store-and-Forward– кадр, що отримується, виходить повністю, перевіряючись на помилки та передається далі
- Cut-through – наскрізна передача даних. Йде зчитка лише адреси призначення, файл не перевіряється на помилки, отже, швидкість передачі набагато вища
- Fragment-free – змішаний/гібридний режим, при якому зчитується адреса і лише (64 байти) кадру для перевірки

За шириною пропускання кожного порту :

- Симетричні – всі порти мають однакову полосу пропускання (наприклад, суворо 100Mbpsабо 1Gb)
- Асиметричні – моделі, які комбінують відразу кілька портів з різною пропускною здатністю

Принцип роботи Ethernetсвітча

Комутатор (світч) проводить аналіз заголовку кадру 2 рівня мережевої моделі OSI. Кожний Ethernet кадр має 2 адреси : MAC-адреса джерела та MAC-адреса призначення.

MAC-адрес (MediaAccessControl) – унікальна адреса обладнання, яка встановлена виробником та присвоюється мережевій карті пристрою.

Світч отримує інформацію від пристроїв, які звернулися до нього та заповнює таблицю комутації їх MAC-адресами навпроти номеру порта. При наступних передачах інформації комутатор шукає адресу обладнання, яке відправило дані, аналізує таблицю та за допомогою неї вирішує на який пристрій потрібно пересилати інформацію.Інші комп'ютери не знають про цю передачу даних (рисунок 3.14)

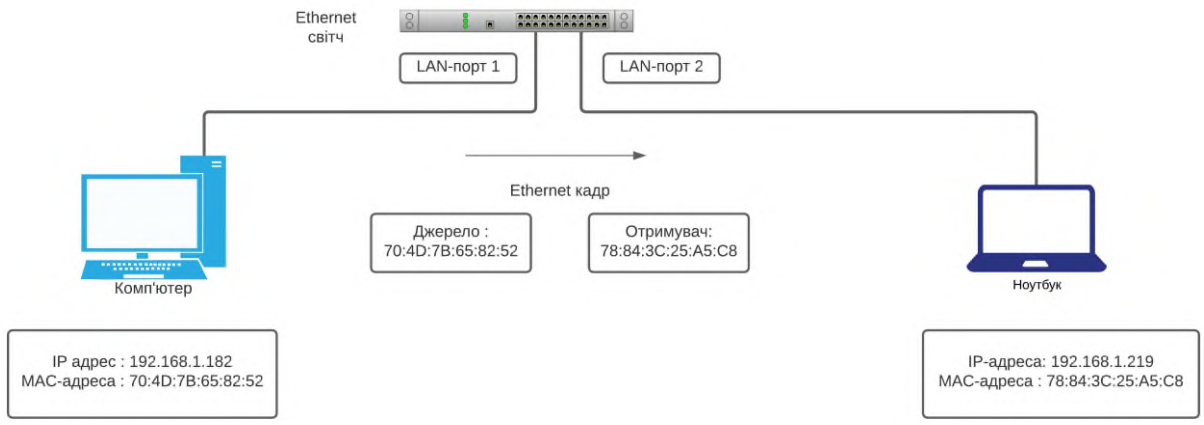


Рис. 3.14 Схема роботи Ethernet світча

Якщо це новий комутатор, який знаходиться на етапі «навчання» та не знаходить даних по MAC-адресі отримувача, то світч розсилає дані на всі підключені до нього пристрої в мережі крім відправника. Отримувач, у якого сходяться всі дані, відповідає комутатору, який в свою чергу робить новий запис в таблиці комутації. Якщо дані збережені, то в майбутньому світч, приймаючи інформацію з тією ж MAC-адресою, вже відправляє інформацію на конкретну адресу, а не всім пристроям в мережі.

Таблиця комутації має в собі повний список MAC-адреси усіх пристроїв мережі, IP-адресу та тип підключення до мережі (рисунок 3.15).

ID	Client Name	MAC Address	Assigned IP	Leased Time
1	OnePlus-9-Pro-5G	A6-C7-A0-66-8F-B8	192.168.0.100	23:23:32
2	OnePlus-9-Pro-5G	32-16-76-C7-F5-88	192.168.0.101	20:21:11
3	A50-pol-zovatela-Lena	66-24-3D-D3-2C-96	192.168.0.107	20:26:02
4	Unknown	90-0E-B3-2E-9C-06	192.168.0.102	23:46:12
5	Unknown	00-1E-B8-15-B3-21	192.168.0.103	23:33:04

Рис. 3.15Таблиця комутації в Ethernetсвітчі

Налаштування інтернет локальної мережі через систему Windows

Налаштування даної домашньої інтернет локальної мережі відбувається в останній версії системі Windows 10, що дає змогу використовувати найсучасніші параметри та технології для реалізації проекту.

Спочатку потрібно, щоб у кожного пристрою в мережі було однакове ім’я робочої групи.Для цього використовуємо комбінацію клавіш Win+R та у вікні, яке з’явилось вводимо команду «sysdm.cpl» та нажимаємо Ок.

Якщо потрібно змінити ім’я, то потрібно натиснути на кнопку «Змінити» та змінити ім’я робочої групи (рисунок 3.16).

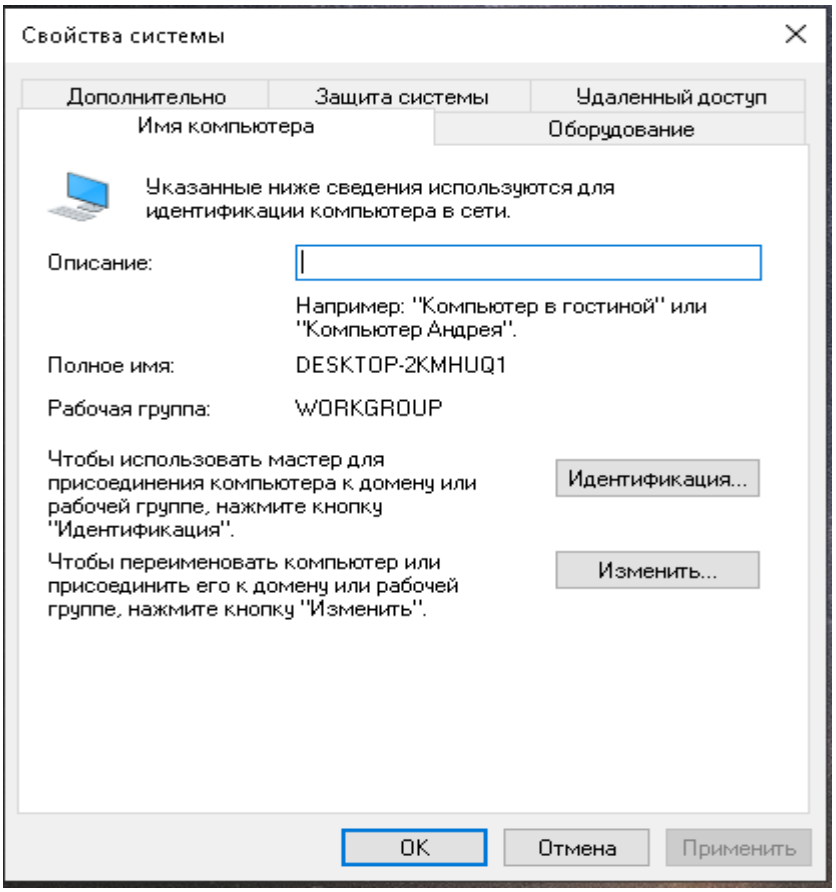


Рис. 3.16 Налаштування ім’я робочої групи

Далі потрібно налаштувати настройки загального доступу.Для цього натискаємо на пуск Windows, переходимо в Параметри та заходимо в пункт «Мережа та Інтернет» та вибираємо «Центр управління мережами та загальним доступом». Далі переходимо у вкладку «Змінити додаткові параметри загального доступу» (рисунок 3.17). Або іншим спобом на панелі завдань правою кнопкою комп’ютерної миші натиснути на значок підлючення до інтернету та вибрати параметр Відкрити «Параметри мережі та інтернет», далі перейти на вкладку Ethernet і також натиснути на параметр «Центр управління мережами та загальним доступом».

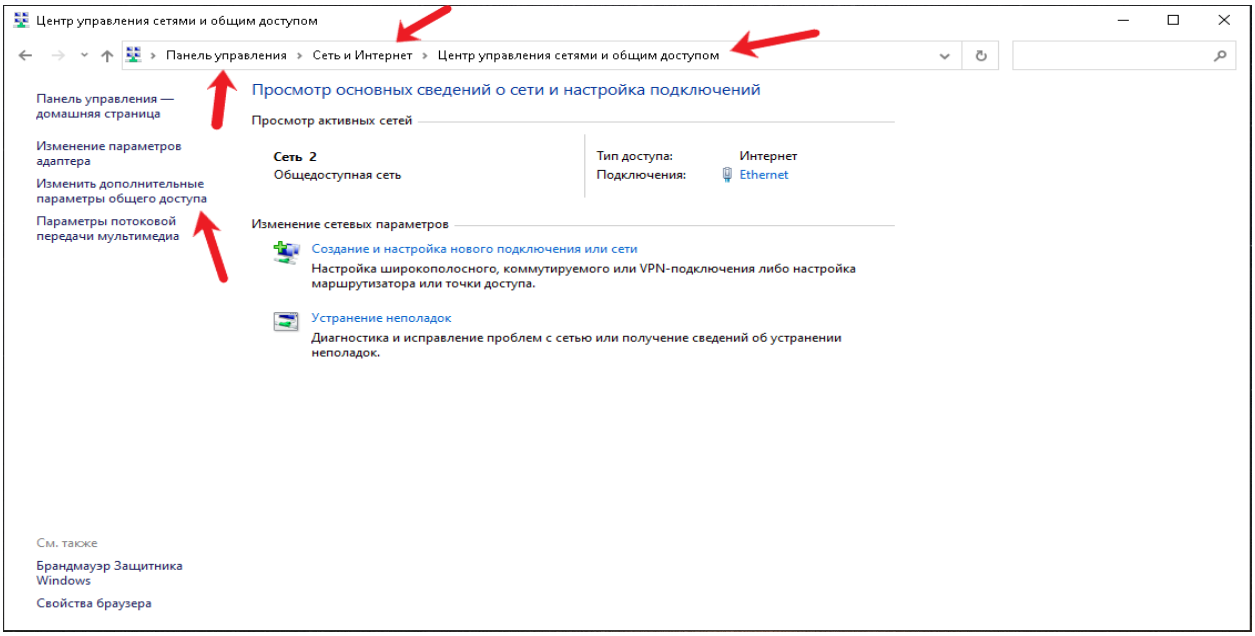


Рис. 3.17 Налаштування параметрів загального доступу

Потрібно поставити перемикач біля кнопки «Включити мережеве виявлення»у підпункту «Приватна мережа», також включити загальний доступ до файлів та принтеру та включити загальний доступ до папок у у підпункту «Усі мережі» (рисунок 3.18).

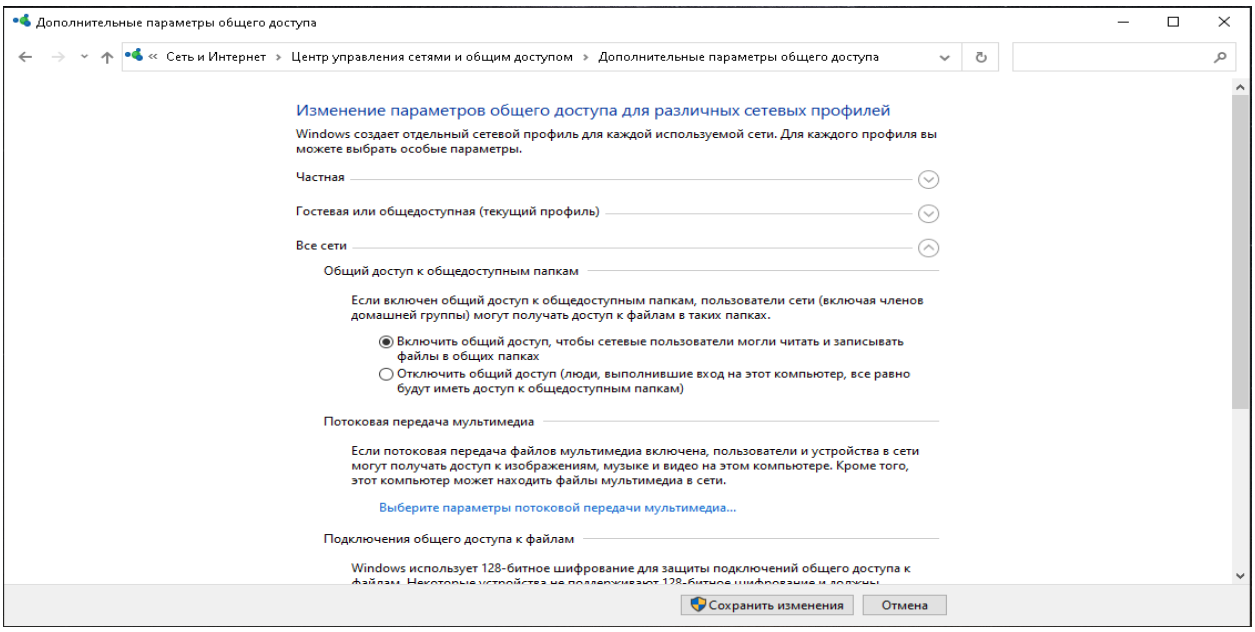


Рис. 3.18 Налаштування параметрів для мережевих профілів

У вкладці «Усі мережі»обов'язково відключити перемикач «Загальний доступ з методом парольного захисту» (рисунок 3.19).

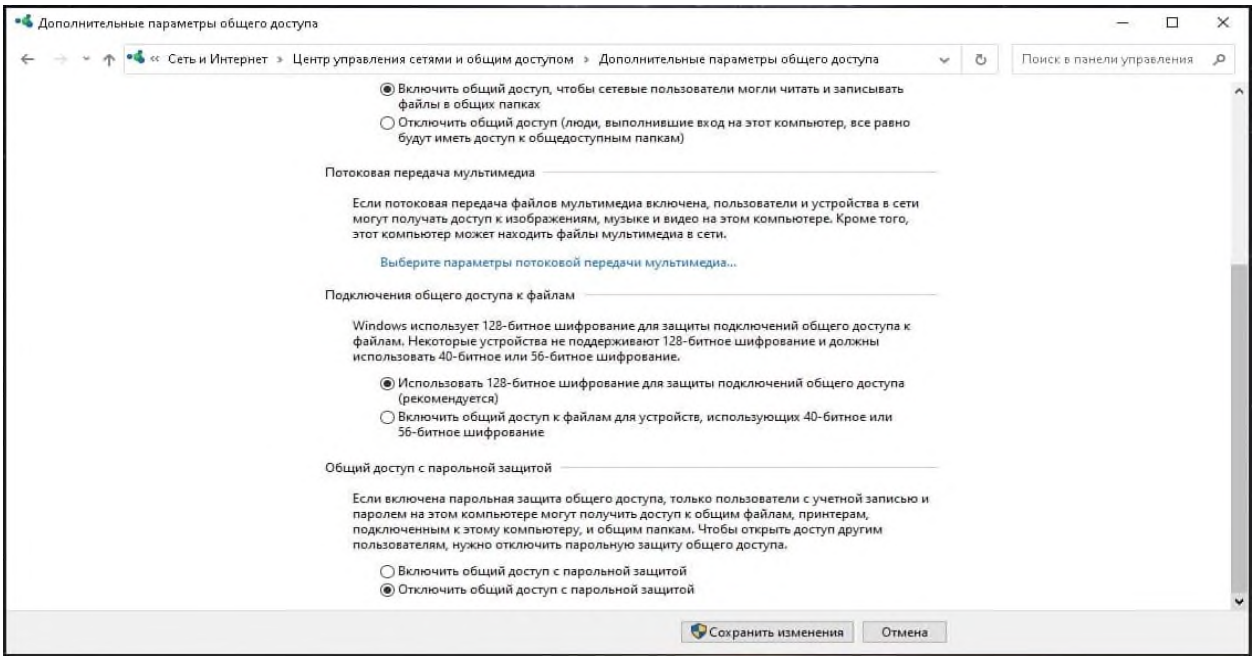


Рис. 3.19 Зміна параметрів для загального доступу

Тепер за допомогою програмного забезпечення проведемо схематичне моделювання та тестування повної схеми домашньої інтернет локальної мережі (рисунок 3.20).

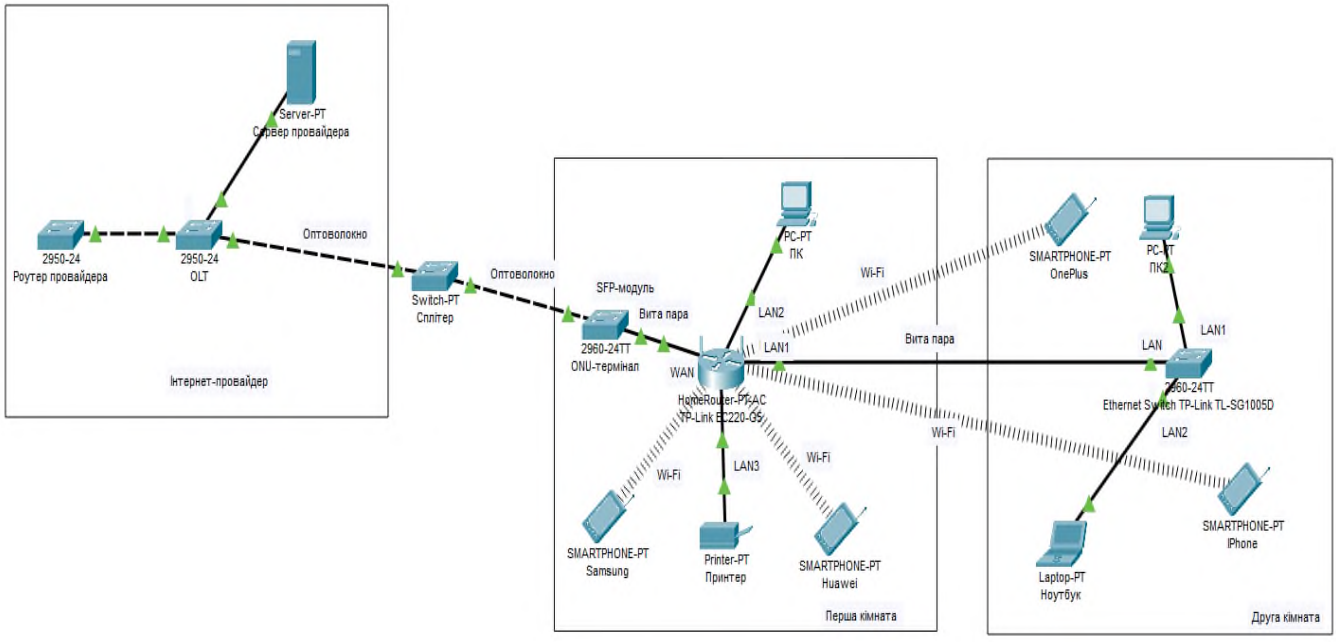


Рис. 3.20 Загальна схема домашньої інтернет локальної мережі

Перевіримо віртуалізацію роботи мережі (рисунок 3.21).

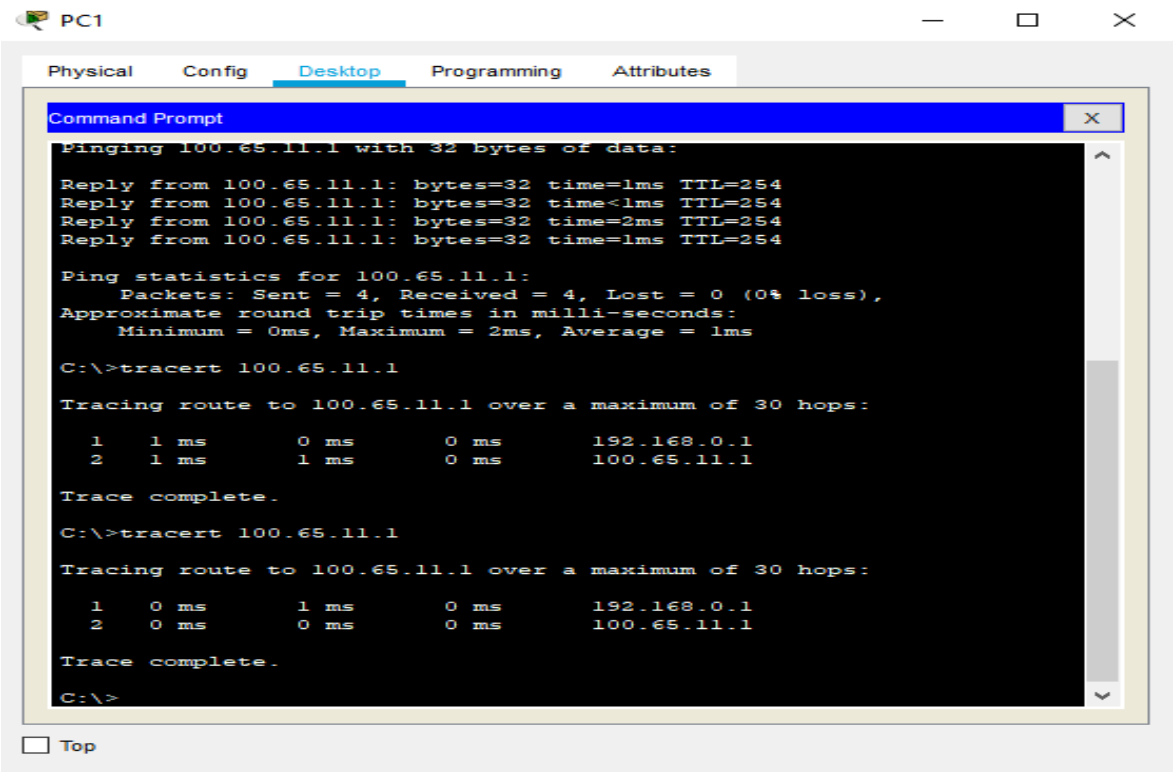


Рис. 3.21 Віртуальна перевірка роботи мережі

На даному рисунку йде перевірка трасування маршруту, яка показує взаємодію домашньої локальної мережі із зовнішньою мережею (провайдера), а також взаємодію з іншими хостами, які розташовані у внутрішній мережі.

Трасування (команда tracert) – утиліта командного рядка, за допомогою якої можна простежити шлях, який проходить пакет Інтернет-протоколу до місця призначення.

Хост – будь-який пристрій, що має підключення до локальної мережі або до всесвітньої мережі Інтернет та є складовою частиною цієї мережі.

Отже, домашню інтернет локальну мережу можна вважити створеною, на всіх абонентських пристроях мережі є загальний доступ до ресурсів (папки, зображення, музики, відео та файлів), який дає змогу обмінюватися ними та використовувати в робочій сфері, також є доступ до загального використання принтеру, який знаходиться в першій кімнаті, всіма пристроями цієї мережі. Це значно полегшує та оптимізує роботу в межах дому для власних цілей абонентів.

3.2 Технологія NAT

У 80-х роках 20-го століття в основу заклали IPv4, яка дозволяє створювати понад 4.3 млрд адресів, але ніхто не підозрював, що цей запас так швидко закінчиться. З кожним роком кількість абонентів зростає все більше і більше і вже у 2019 році в Європі офіційно закінчилися IP-адреси. Ліміт було вичерпано.

Щоб вирішити дану проблему було розроблено декілька варіантів :

Перший спосіб – полягає у посиленні за контролем IP-адрес.

Може існувати деякий сайт Хз IPv4, і його хост вирішив припинити підтримку даного сайту. Сайт вважається покинутим, але IP-адреса продовжує вважатися зайнятою і таких випадків може бути дуже багато. Тобто потрібно пройти «ревізію» IP-адрес та вилучити, які не використовуються.

Другий спосіб – масове використання системи IPv6.

Протокол IPv6 розроблений на зміну, як наступник протоколу IPv4. Найбільш основними перевагами IPv6 над IPv4 є збільшення адресного простору (IPv4 мав 32 біти, що дорівнювало 2^{32} адресам, а IPv6 має 128 біт, що дорівнює 2^{128} адресам). 6 версія протоколу стала більш безпечнішою, ніж у попередника.

Можна вважити, що проблема вирішена, але перейти з протоколу IPv4 на IPv6 визиває складнощі, так як дані протоколі несумісні. Також причиною важкого переходу на 6 версію протоколу є грошова вартість. Більшість компаній поки, що не готові вкласти достатню кількість коштів на перехід, хоча на поточний час процес переходу з 4 на 6 версію поступово просувається.

Третій спосіб – використання технології трансляції мережевих адрес NAT.

Згідно документу RFC 1918, IANAзарезервувала 3 блоки адресів для приватних IP-адрес (сірих) (рисунок 3.22), усі інші IP-адреси мають назву публічних IP-адрес (білих).

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Рис. 3.22 Блоки приватних IP-адрес (сірих)

NAT (Network Address Translation) –перетворення мережевих адрес. Створений для спрощення та збереження IP-адрес. Він дозволяє приватним IP-мережам, які використовують незареєстровані IP-адреси, підключатися до Інтернету. Дана технологія працює на маршрутизаторі, який зазвичає з'єднує дві мережі та перетворює приватні (не глобально унікальні) адреси у внутрішній, локальній мережі на дійсні, унікальні адреси перед відправкою пакетів у іншу мережу.

Приймаючи пакет від локального комп'ютера, маршрутизатор проводить аналіз IP-адреси призначення. Якщо це локальна адреса, то пакет трафіку пересилається іншому локальному комп'ютеру, якщо ні, то пакет потрібно надіслати назовні в Інтернет.

Маршрутизатор підмінює зі свого боку зворотну IP-адресу пакета на свою зовнішню (яка видима з Інтернету) IP-адресу та змінює номер порту (щоб розрізняти пакети у відповідь, адресовані різним локальним комп'ютерам). Дана комбінація зберігається в тимчасовій таблиці. Через певний період часу, як клієнт і сервер завершать обмін пакетами, то маршрутизатор зітре у себе в таблиці запис про n-ий порт за терміном давності.

Призначення NAT

- Виведення в Інтернет внутрішньої локальної мережі через певний пул зовнішніх адрес, одна зовнішня адреса
- Для заміни зовнішньої IP-адреси іншим (перенаправлення трафіку)

- Для балансування навантаження між однаковими серверами з різними IP-адресами
- Для об’єднання двох локальних мереж з внутрішньою адресацією, що перетинається

Типи технології NAT

Статичний NAT – відображення незареєстрованої IP-адреси на зареєстровану IP-адресу на основі один до одного (рисунок 3.23).

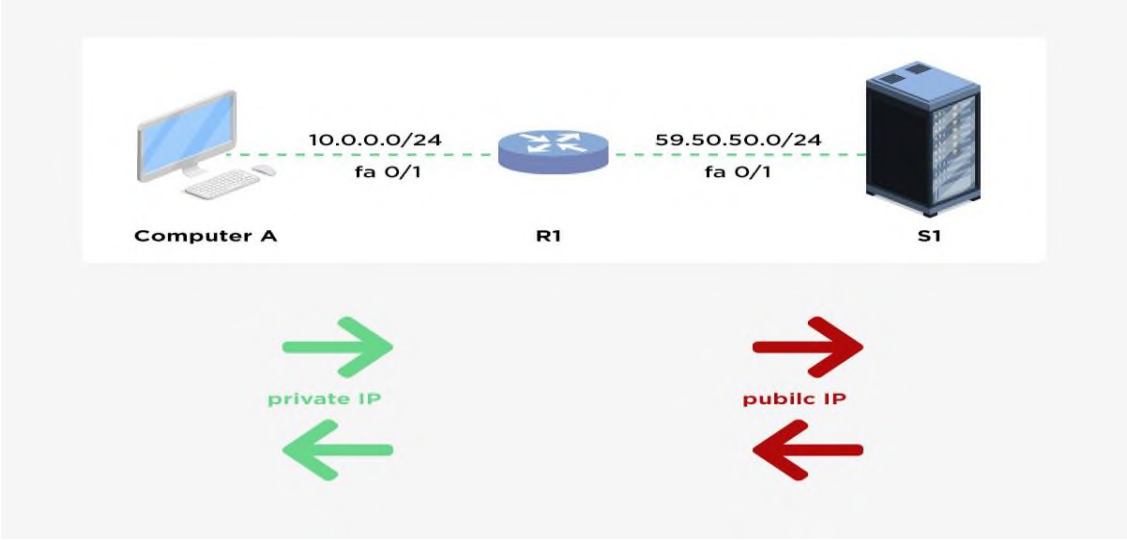


Рис. 3.23 Статичний NAT

Динамічний NAT–відображення незареєстрованої IP-адреси на зареєстровану адресу із групи зареєстрованих IP-адресів. Також динамічний NATвстановлює відображення між незареєстрованою та зареєстрованою адресою, але відображення може змінюватись залежно зареєстрованої адреси, доступної в пулі адрес, під час комунікації (рисунок 3.24).

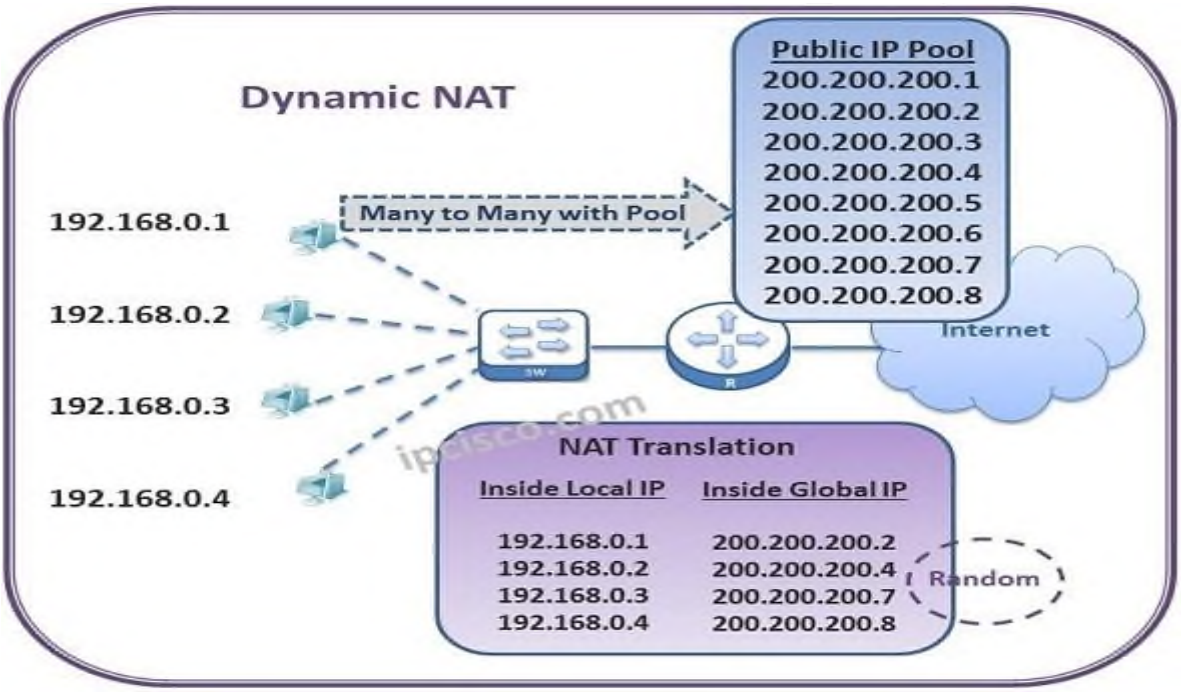


Рис. 3.24 Динамічний NAT

Перевантажений NAT – форма динамічного NAT, який відображає декілька незареєстрованих адрес в єдину зареєстровану IP-адресу, при цьому використовуючи різні порти. При перевантаженні кожний комп'ютер у приватній локальній мережі транслюється на ту саму адресу, але з різним номером порту (рисунок 3.25).

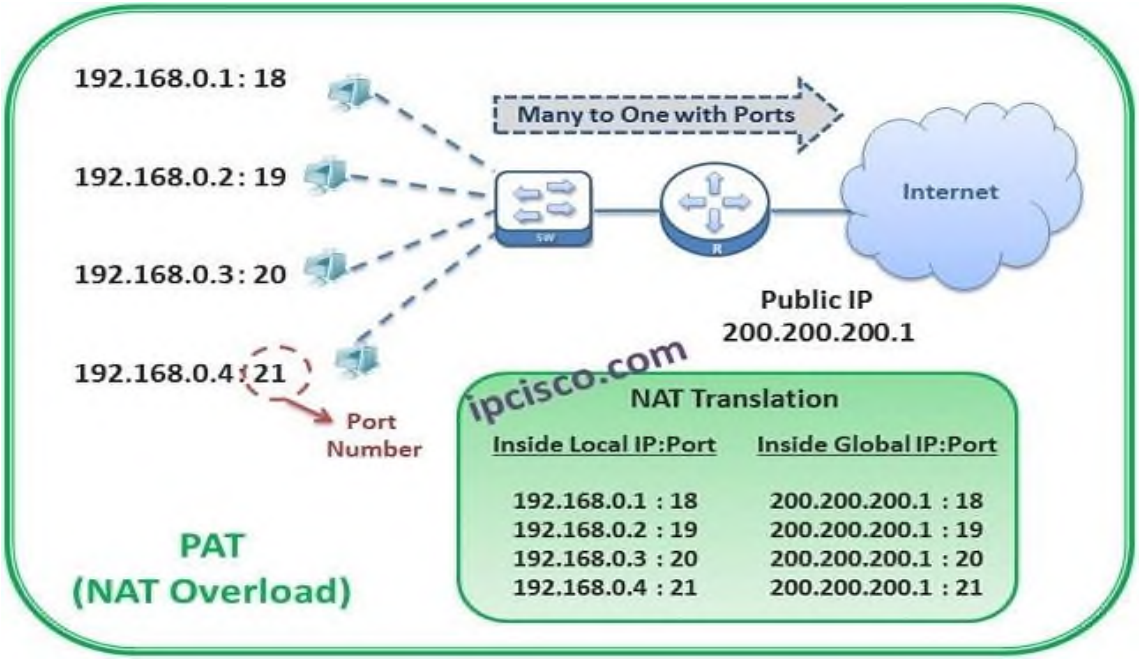


Рис. 3.25 Перевантажений NAT

Налаштування NAT

Зазвичай у всіх стандартних маршрутизаторах NATвстановлений та налаштований автоматично, так як без цієї функції з локальної мережі користувач не матиме доступ до ресурсу глобальної мережі Інтернет.

Але якщо технологія NAT все таки не налаштована автоматично в роутері, то можна скористатися даною інструкцією, яка буде наведена нижче на моєму прикладі через веб-інтерфейс маршрутизатора TP-Link(рисунок 3.26) :

- Відкрити будь-який браузер та перейти за стандартними адресами 192.168.0.1/192.168.1.1у веб-інтерфейс роутера
- Ввести стандартні дані admin/admin у логін та пароль або які користувач встановив самостійно
- Перейти на сторінку Advanced (Додаткові налаштування) >SystemTools (Системні інструменти) >SystemParameters (Системні параметри)
- В підрозділі NAT поставити індикатор/увімкнути галочку в пункті «EnableNAT (включити NAT)»

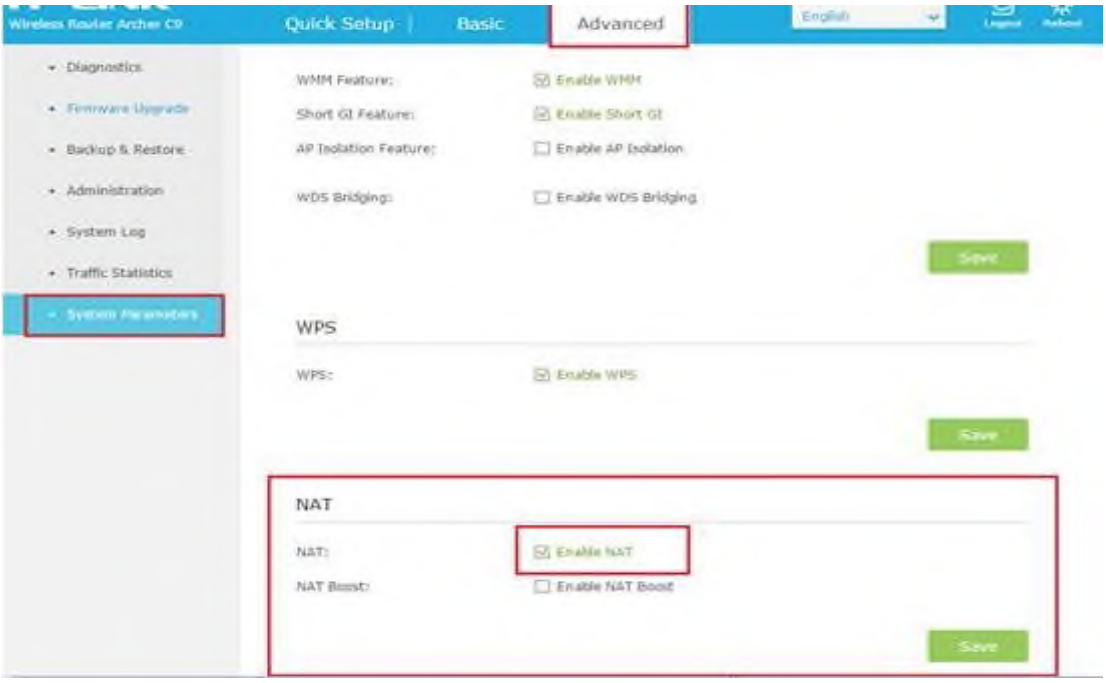


Рис. 3.26 Налаштування NAT у веб-інтерфейсі роутера

Таблиця 3.1

Переваги та недоліки NAT

Переваги	Недоліки
Дозволяє заощадити IP-адреси, транслюючи кілька внутрішніх IP-адрес в одну зовнішню IP-адресу.	Старі протоколи. Протоколи, які були розроблені до масового впровадження NAT, не в змозі працювати, якщо на шляху між хостами, що взаємодіють, є трансляція адрес.
Дозволяє запобігти чи обмежити звернення зовні до внутрішніх хостів, залишаючи можливість звернення зсередини назовні.	Ідентифікація користувачів. Через трансляцію адрес «багато в одну» з’являються складнощі з ідентифікацією користувачів та необхідністю зберігати повні логи трансляцій.
Дозволяє приховати певні внутрішні послуги внутрішніх хостів/серверів. Виконується та ж сама трансляція на певний порт, але можливо підмінити внутрішній порт офіційно зареєстрованої служби. Підвищення безпеки та приховування «непублічних» ресурсів.	Ілюзія DoS-атаки. Якщо NAT використовується для підключення багатьох користувачів до одного і того ж самого сервісу, це може викликати ілюзію DoS-атаки на сервіс.

Продовження таблиці 3.1

	Пірингові мережі. У NAT-пристроях, які не підтримують технологію UniversalPlug&Play, в деяких випадках необхідне додаткове налаштування при роботі з піринговими мережами та деякими іншими програмами, в яких необхідно не тільки ініціювати вихідні з'єднання, але також приймати вхідні.

3.3 Устаткування та інструменти для побудови інтернет локальної мережі

В даному підрозділі буде описано основне устаткування, яке використовувалося для побудови домашньої інтернет локальної мережи, а саме роутер, Ethernet світч та програмне забезпечення (інструменти) за допомогою якого проводилось схематичне моделювання та побудова домашньої LAN.

Роутер

Модель роутера для домашньої інтернет локальної мережі була вибрана – TP-LinkEC220-G5.

Це високошвидкісний двухдіапазоний роутер, який працює в діапазонах 2.4 ГГц та 5 ГГц і підтримує безпровідний зв'язок до 1.2 Гбіт/с. Чотири добре розташованих антени роблять підключення більш ефективним та стабільним. Удосконалена антена технологія збільшує чутливість прийому для збільшення покриття зони Wi-Fi. Підтримує всі стандартні ОС(рисунок 3.27).



Рис. 3.27 Роутер TP-LinkEC220-G5

Кнопка WPS (Wi-FiProtectedSetup) – технологія, яка дозволяє швидко та безпечно з’єднати між собою два Wi-Fi пристрої між собою, а також дає можливість підключитися до маршрутизатора різними абонентськими пристроями, як мобільний телефон, планшет, ноутбук без вводу пароля.

Кнопка Reset–може бути виконана як у вигляді кнопки, так і у вигляді захованої мембрани (отвір), зазвичай її можна натиснути гострим предметом (голкою або зубочисткою). Якщо затиснути цю кнопку на 5-10 секунд, то налаштування роутера скинуться до заводських.

Індикатором успішності процедури стане блимання індикаторів роутера. Уточнити наскільки довго затискати цю кнопку можна в інструкції до роутера. Затримка при натисканні додана для страховки від випадкового натискання та мимовільного скидання налаштувань роутера.

Інтерфейси, який підтримує роутер :

- 3 порти LAN 10/100/1000 Мбіт/с
- 1 порт WAN 10/100/1000 Мбіт/с

Функції безпеки :

- Міжмереже
- вий екран SPI
- Батьківський контроль

Підтримка таких протоколів, як : DHCP, IPsec, IPv4, IPv6, L2TP, PPPoE, PPTP, UPnP.

Типи шифрування :

- WPA2-PSK
- WPA3
- WPA-PSK

Інші функції : статистика безпровідної мережі, контроль доступу, локальне управління, віддалене управління, локальний контроль управління, список хостів, розклад доступу, управління правилами, міст WDS, WMM.

Ethernet світч

В якості комутатора була вибрана модель –TP-LinkTL-SG1005D.

Дана модель являє собою 5-портовий гігабітний комутатор для високошвидкісних мереж Ethernet, за допомогою його економічності, простоті у використанні та високій продуктивності, можна провести модернізацію мережі та здійснити перехід на рівень 1000 Мбіт/с без додаткових витрат та додаткових налаштувань (рисунок 3.28).



Рис. 3.28 Ethernet світч TP-LinkTL-SG1005D

Світч відноситься до типу некерованих, що означає простий спосіб підключення пристроїв Ethernet із фіксованою конфігурацією, до яких не можна вносити жодних змін, зазвичай такий тип використовується для невеликих інтернет локальних мереж.

Шляхом підключення пристроїв користувача до гігабітної мережі на основі даного пристрою можна збільшити швидкість роботи мережевого сервера та з'єднань, що примикають.

Комутатор TP-LinkTL-SG1005D підтримує функцію контролю потоку IEEE 802.3хдля повнодуплексного режиму та функцію Backpressurey напівдуплексному режимі. Функція Backpressure означає, що приймаючий пристрій (порт комутатора) у разі переповнення буфера відправляє штучно створений сигнал виявлення колізії або відправляє назад пристрою-відправнику його кадри.

Додаткові можливості :

- Порти RJ45 10/100/1000 Мбіт/сз підтримкою Auto MDI/MDIX
- Неблокуюча архітектура комутації
- GreenEthernettехнологія (до 70% економії енергії)

CiscoPacketTracer

За допомогою цього інструмента моделювалися та тестувалися схеми домашньої інтернет локальної мережі в даній бакалаврській роботі.Це програмний інструмент, створений компанією Cisco. Цей інструмент забезпечує мережеве моделювання для відпрацювання мереж.

Основною метою CiscoPacketTracer є допомога користувачам із засвоєнням принципів роботи побудованої мережі з використанням практичного досвіду. За допомогою нього можна демонструвати технічні концепції та мережеві системи.

Даний інструмент ділиться на 2 робочі області:

– Логічна область показує логічну топологію мережі, яка створена користувачем. Представляє розміщення та підключення віртуальних мережевих пристроїв.

– Фізична область показує графічний фізичний вимір логічної мережі. Ця область робить зображення того, як мережі пристрої (маршрутизатори, комутатори та інші) будуть виглядати в реальному середовищі. Також забезпечує географічне представлення мереж.

Основними характеристиками CiscoPacketTracerє:

- Необмежена кількість пристроїв
- Візуалізація мереж
- Режим реального часу та режим імітації
- Підтримує більшість мережевих протоколів

ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

В даному пункті буде розглянута цінова політика побудови домашньої інтернет локальної, її устаткування, інструменти та технічні особливості цих рішень.

Основною метою створення інтернет локальних мереж є об’єднання абонентських пристроїв, які можуть мати різне географічне положення, в одну мережу. Головним питанням, яке є для вартості створення таких мереж це забезпечення швидкої передачі даних, безпечне передавання інформації та з'єднання обладнання і підмереж в одну.

Перелік, який входить до вартості складається з:

- Роутера
- Ethernet світча
- Прокладка кабеля типу вита пара
- Ціна тарифу інтернет-провайдера

Роутер, який використовується в побудові домашньої інтернет локальної мережі, а саме TP-LinkEC220-G5, має ціну на технічному ринку приблизно 900-1300 грн. Даний роутер був вибраний тому, що він володіє швидкою передачею інформації, гарну функціональністю, має просте налаштування та стабільність в роботі.

Ethernet світч, TP-LinkTL-SG1005D, на різних інтернет-сервісах має ціну від 400 до 600 грн. Обрав саме цей світч тому, що він недорогий, надійний в плані безпеки та захисту інформації, простий в налаштуванні та підходить для домашнього користування та невеликих локальних мереж.

Ціна тарифа інтернет-провайдера на місяць становить 200 грн. В даний тариф входить :

- Швидкість до 1000 Мбіт/с

- Безлімітний трафік

На сучасному ринку прокладання фізичної лінії для з’єднання обладнання в домашній інтернет локальній мережі типу вита пара коштує приблизно 30-40 доларів (840-1120грн) на 100 метрів довжини, цієї довжини достатньо для прокладки кабелю в домашній інтернет локальній мережі, яка описана в даній дипломній роботі. Прокладка оптоволокна до квартири та встановлення ONU-терміналу була безкоштовна з боку Інтернет-провайдера.

Не враховано вартість абонентських станцій (комп’ютери, ноутбуки, смартфони, принтер), так як домашнє обладнання було вже встановлено до створення локальної мережі. Також не додано вартість за ремонтні роботи під час прокладки фізичної лінії.

ВИСНОВКИ

В даній магістерській роботі було наведено один із способів розробки моделі трафіка інтернет локальних мереж.

Розглянуто особливості інтернет локальних мереж, а саме їх типи, основні топології, варіанти з'єднання , а також дві основні технології в локальних мережах – Ethernet та Wi-Fi.

Наведена історія створення інтернет локальних мереж, а також подальший розвиток та їх вплив на технологічний світ.

Описана побудова, налаштування та застосування такої мережі за допомогою мережевого устаткування і стандартного програмного забезпечення та інструментів.

Моделювання та логічна структура мережі була побудована за допомогою інструмента CiscoPacketTracer. Даний інструмент надає користувачу зобразити логічну та фізичну структуру мережі в реальному часі та побачити її візуалізацію.

Основне налаштування мережі відбувається змінами стандартних параметрів роутера та Ethernetсвітча. Реалізація обладнання використовується в середовищі Windows 10.

Також було описано схематична фізична робота мережі та функціонування LAN з глобальною мережею Інтернет, а саме поділення домашньої інтернет локальної мережі на дві кімнати, як відбувається передача інформація між ними та з інтернет-провайдером.

Для передачі трафіку використовується кабель типу вита пара. Технологія, яка лежить в основі даної мережі – FastEthernet, що підходить для оптимального функціонування та відповідає усім потребам.

Застосовано мережеве устаткування у вигляді:

- Роутера
- Ethernet світча
- Абонентських станцій (комп’ютери, ноутбук, смартфони та принтер).

Був проведений аналіз особливостей сучасних технологій інтернет локальних мереж, розібрано основні переваги та недоліки таких мереж, які

методи використовуються для безпеки та захисту інформації та яке майбутнє та розвиток чекає на LAN.

Інтернет локальні мережі зручно використовувати для полегшення роботи користувача, також для об’єднання обладнання, щоб використовувати його для загального використання.

Результати практичної частини даної дипломної роботи з налаштування домашньої інтернет локальної мережі можуть бути використані для потреб користувача, що бажають отримати доступ до всесвітньої мережі Інтернет, а також знання, які використані.

Отже, можна вважати, що завдання дипломної роботи виконано, є всі необхідні дані для реалізації розробки моделі трафіка інтернет локальних мереж

ПЕРЕЛІК ПОСИЛАНЬ

1. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П.Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013ю — 256 с. ISBN 978-617-574-087-3
2. БуровЄ. В. Комп'ютерні мережі: підручник / Євген Вікторович Буров. — Львів: «Магнолія 2006», 2010. — 262 с. ISBN 966-8340-69-8
3. Галіцин В. К., Левченко Ф. А. Багатокористувацькі системи та мережі: Посібник. – 1998 р. – 360с.
4. Буров Є. Комп‘ютерні мережі. 2-ге оновлене і доповн. – Львів: БаК, 2003. – 584 с
5. Миллер Д. Рождение Internet/ Д.Миллер // PCWORLDUKRAINE. — 1999. — № 11-12. — С. 89
6. Симонович С.В., Євсєєв Г.А. Практична інформатика: Навчальний посібник для середньої школи. Універсальний курс. - М.: АСТ-ПРЕСС, 2002.
7. *Валецька Т. М.* Комп'ютерні мережі: .— Чернівці: Зелена Буковина, 2001.— 138 с. ISBN 966-7123-63-4
8. Стаття «Мережі для початківця ІТ-фахівця. Обов’язкова база»[Веб-ресурс] –https://habr.com/ru/post/491540/
9. Стаття «Налаштування локальної мережі в Windows» [Веб-ресурс] - https://siniy-ekran.ru/poleznoe/nastrojka-lokalnoj-seti-v-windows/
10. Відеоматеріали «Основи комп’ютерних мереж – принцип роботи та обладнання» [Веб-ресурс] – https://www.youtube.com/watch?v=2NjjmwMT4nY
11. Мельник Ю.В., Заїка В.Ф., Перепелиця Н.Л., Гринкевич Г.О. Методичні рекомендації для виконання бакалаврської роботи на ступінь вищої освіти «бакалавр» для студентів денної та заочної форм навчання спеціальності 172 «Телекомунікації та радіотехніка». – К.: ДУТ, 2019. – 37с.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **СТВОРЕННЯ ТА ЗАСТОСУВАННЯ МЕТОДИКИ МОДЕЛЮВАННЯ ТРАФІКУ ІНТЕРНЕТ ЛОКАЛЬНИХ МЕРЕЖ**

Виконав: студент гр. ТСДМ-61
Бурба Д.В..
Керавник: ДТН, професор Заїка В.Ф.

КИЇВ-2025

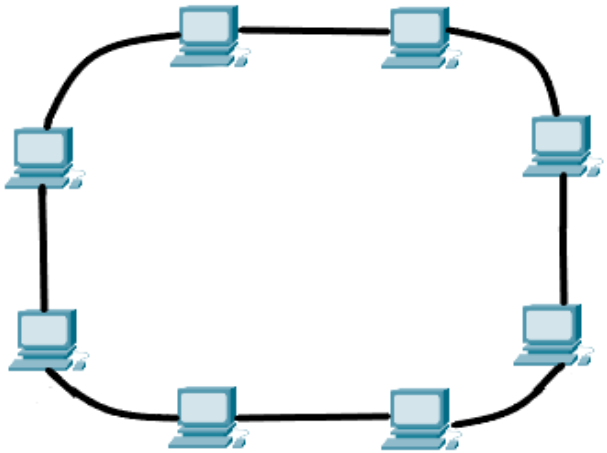
Мета роботи – розглянути та проаналізувати особливості інтернет локальних мереж.

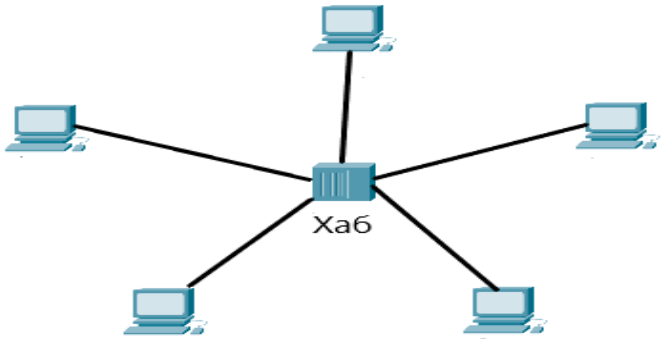
Об'єкт дослідження – інтернет локальні мережі.

Предмет дослідження – різновиди та організація інтернет локальних мереж.

В даній роботі приведено особливості та організація інтернет локальних мереж. Простежено історію виникнення та створення інтернет локальних мереж. Проаналізовано роботу основних ехнологій в інтернет локальних мережах. Окреслено засоби безпеки та захисту інформації в інтернет локальних мережах. Визначено головні переваги та недоліки в LANмережах. Виявлено подальша тенденція розвитку інтернет локальних мереж в найближчому майбутньому. Розглянуто практичне налаштування та застосування інтернет локальних мереж для послуг користувача.







Мережеві топології

Мережева модель OSI

Модель OSI

Дані	7 прикладний application	Доступ до мережевих служб
	6 представлень presentation	Представлення і кодування даних
	5 сеансовий session	Управління сеансом зв'язку
Сегменти	4 транспортний transport	Прямий зв'язок між кінцевими пунктами і надійність
Пакети	3 мережевий network	Визначення маршруту і логічна адресація
Кадри	2 канальний data link	Фізична адресація
Біти	1 фізичний physical	Робота з середовищем передачі , сигналами і двійковими даними

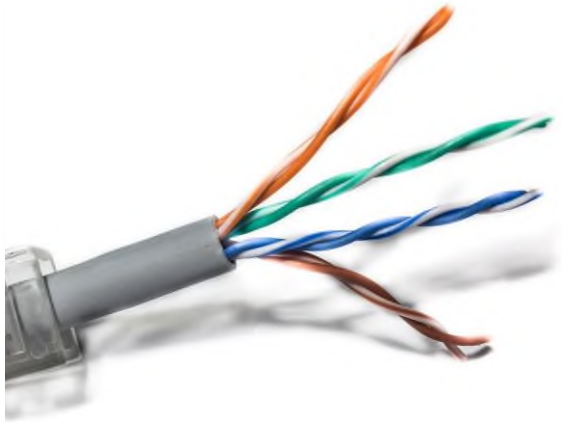


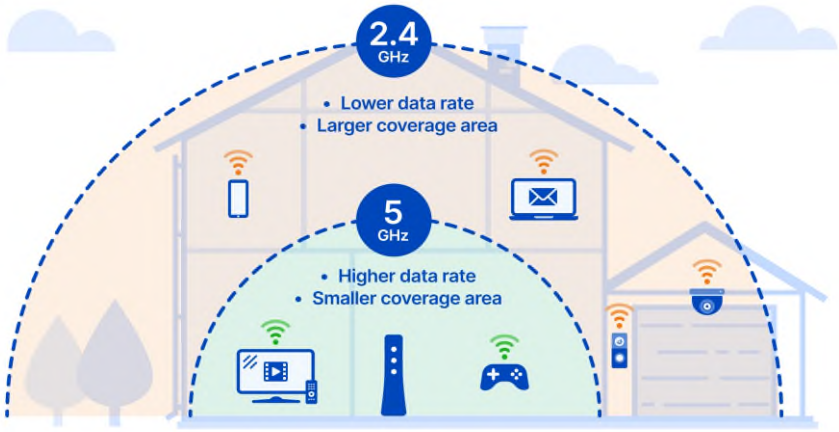
Різниця між «тонким» та«товстим» коаксіальним кабелем



Оптоволокно

Вита пара





Різниця покриття Wi-Fi на 2,4 ГГц та 5 ГГц



BSS



Схема роботи
обладнання у режимі Ad-Hoc

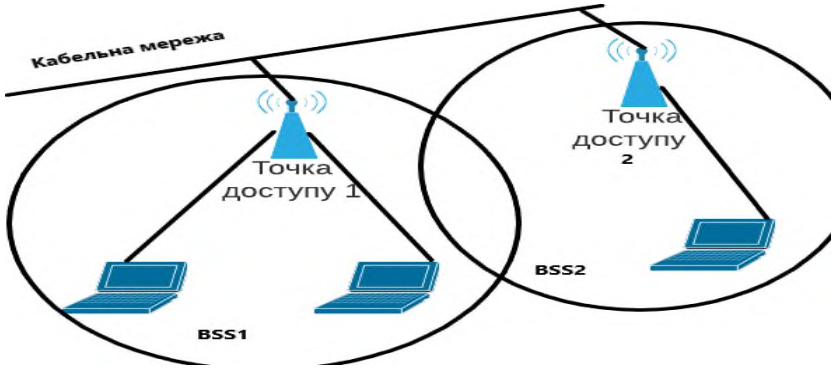


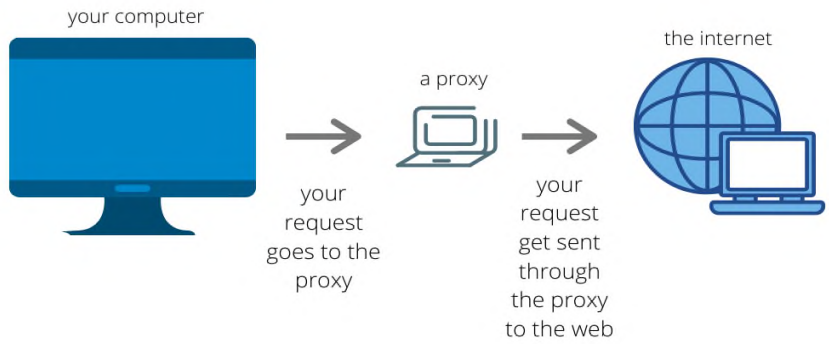
Схема роботи обладнання у режимі ESS



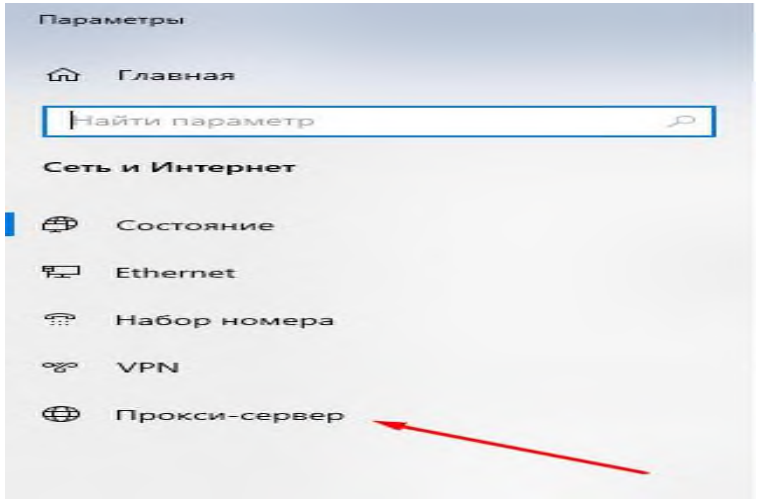
Види біометричного захисту інформації



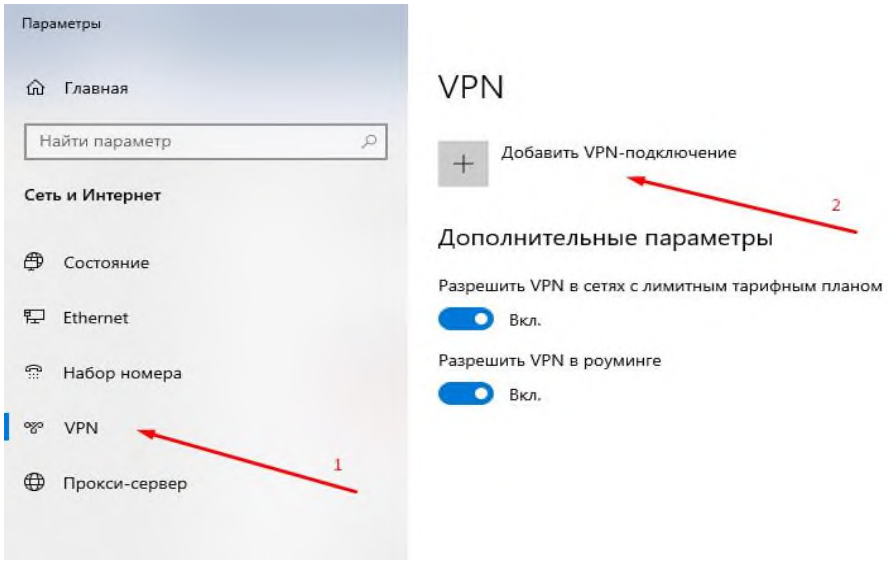
Брандмауер



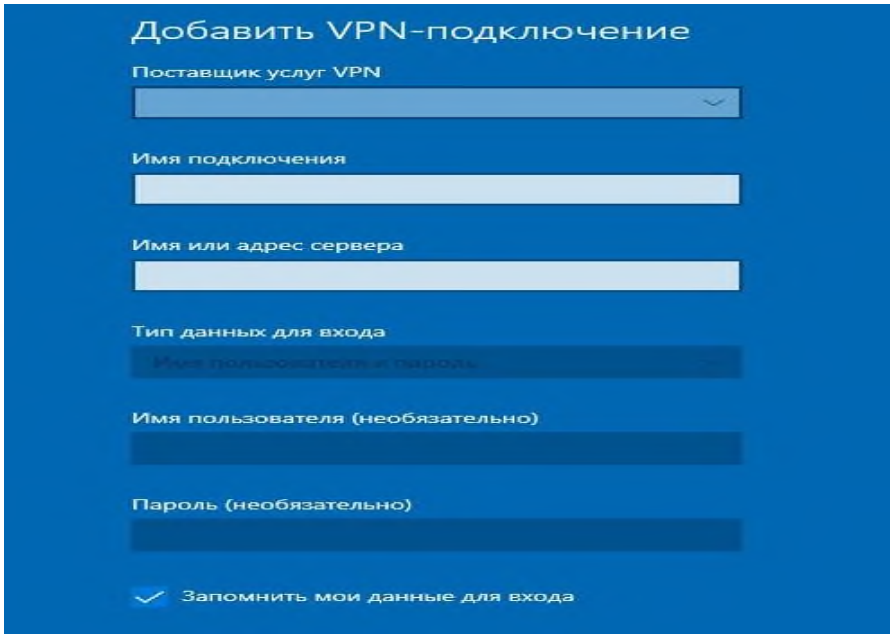
Проксі-сервер



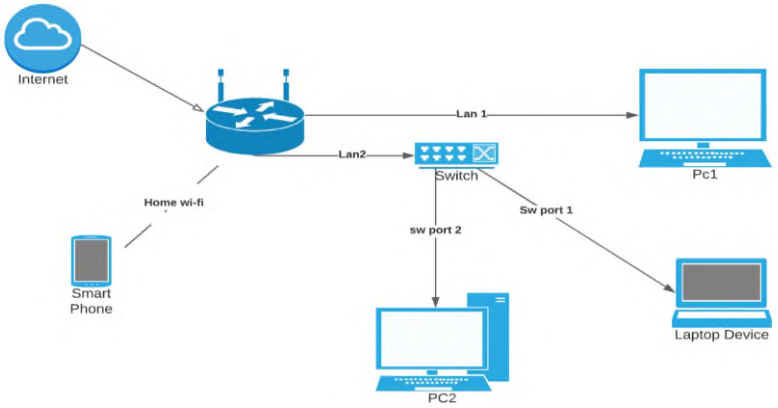
Підпункт «Проксі-сервер»



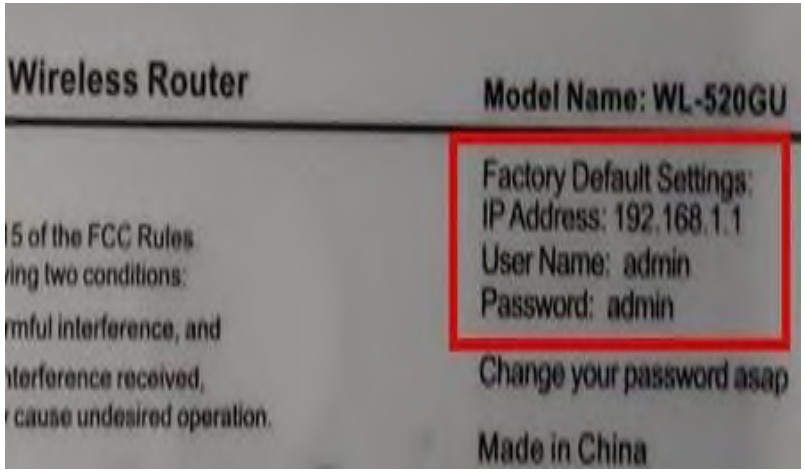
Налаштування VPN



Додавання VPN-підключення



Робота інтернет-провайдера
DHCP



Адреса та дані для входу в налаштування роутеру

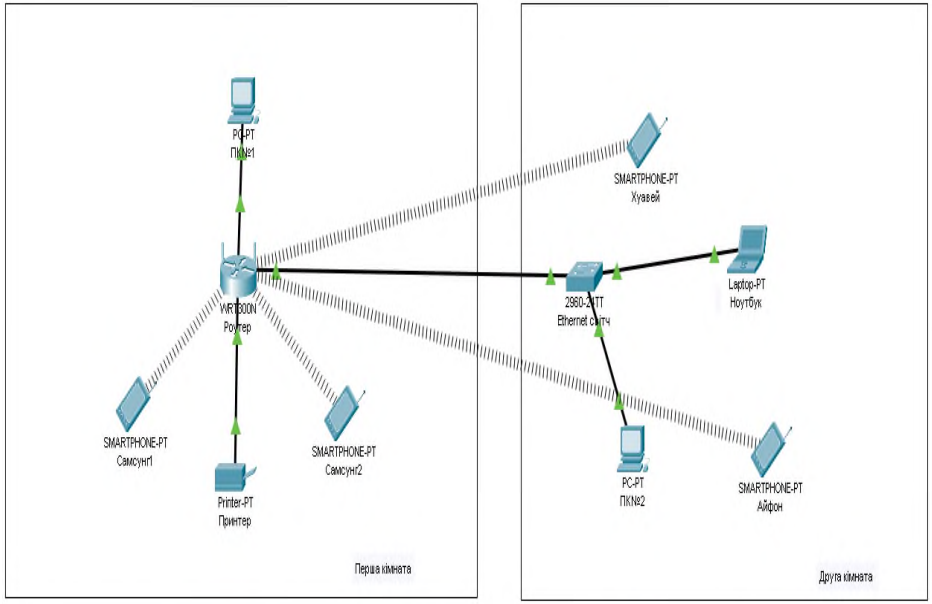


Схема першої та другої кімнати в домашній інтернет локальній мережі **PON/GPON**

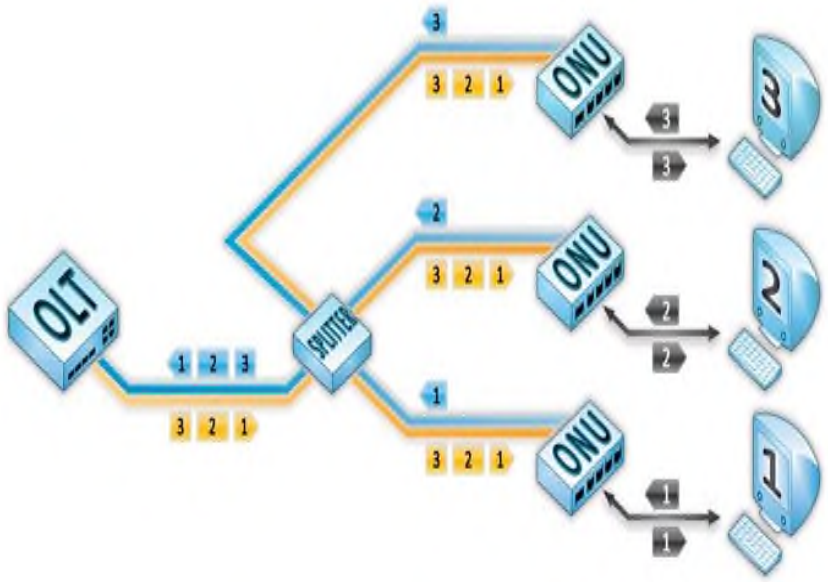


Схема підключення PON



OLT (opticallineterminal)



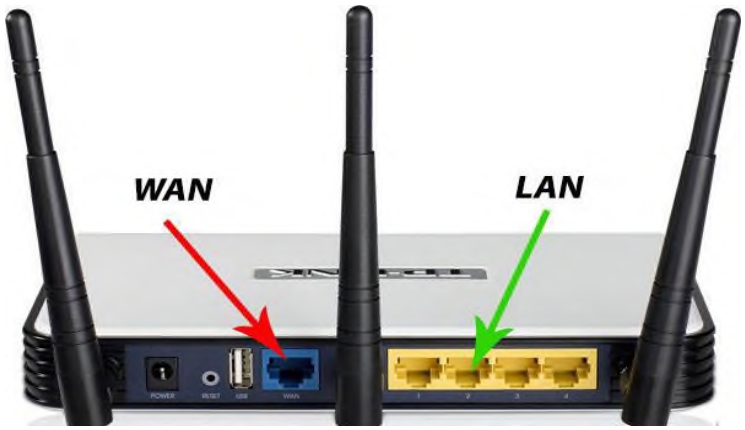
ONU (opticalnetworkunit)

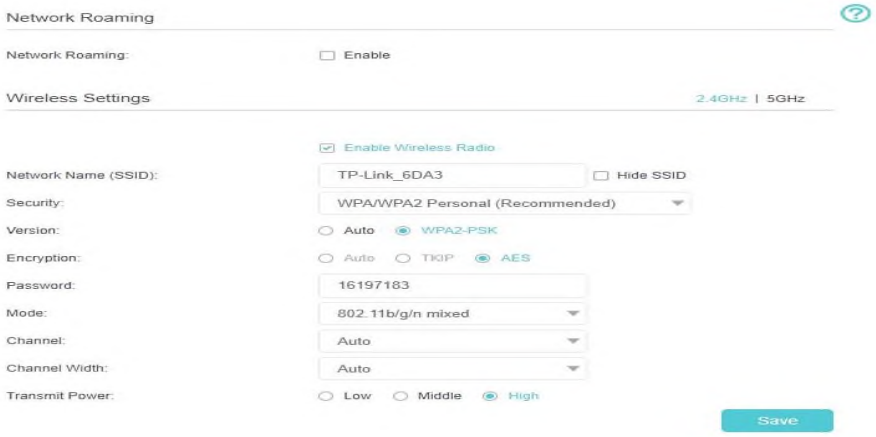


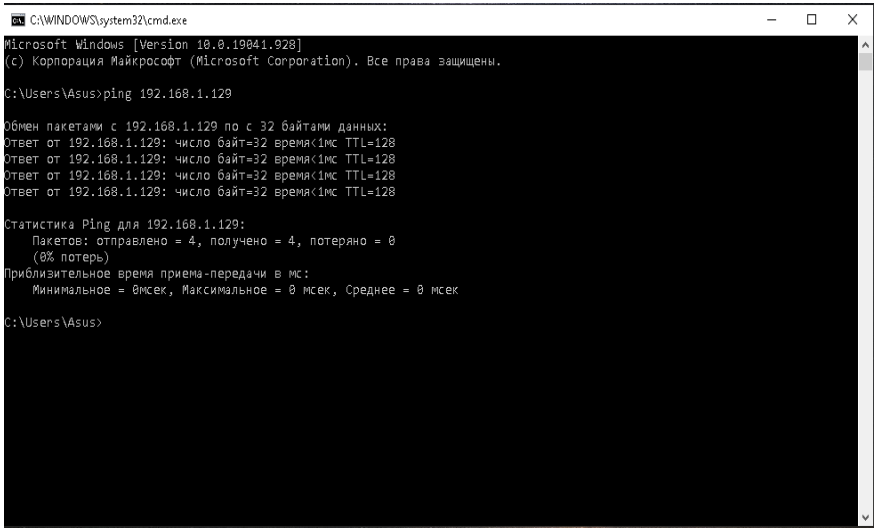
Модуль SFPOLT



Сплітер







Перевірка фізичного зв’язку між комп’ютерами

EthernetSwitch

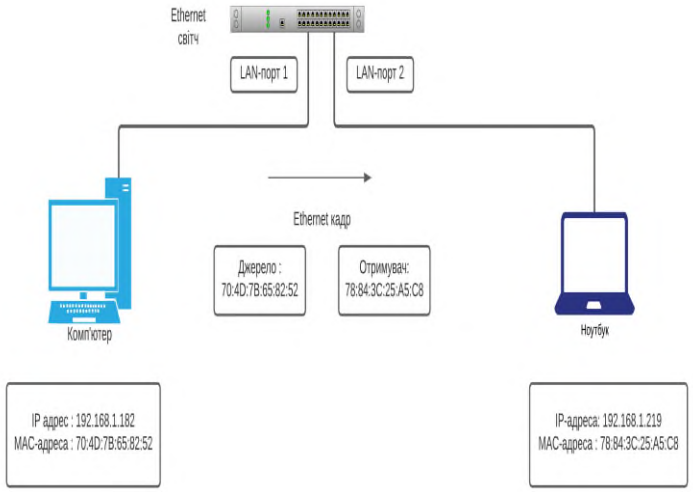
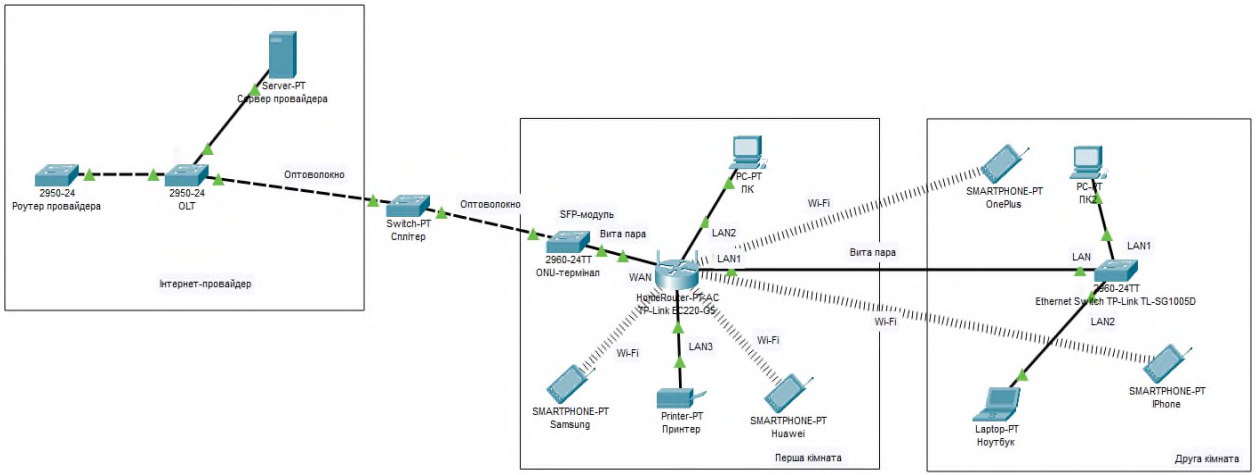
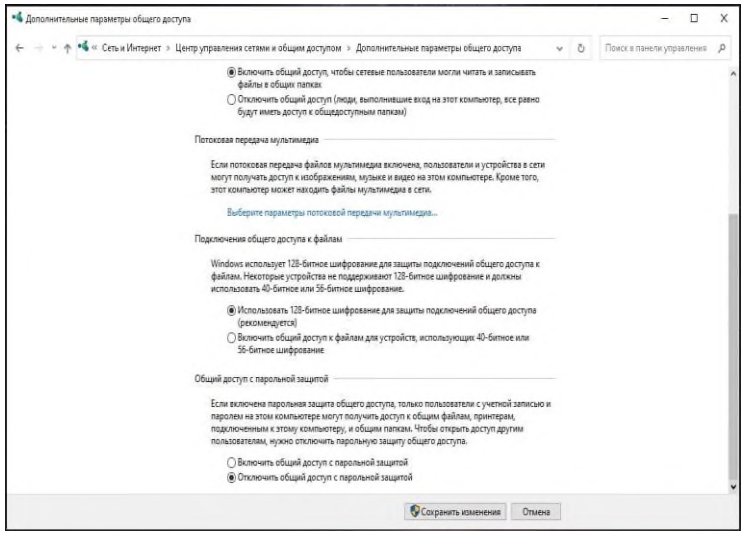


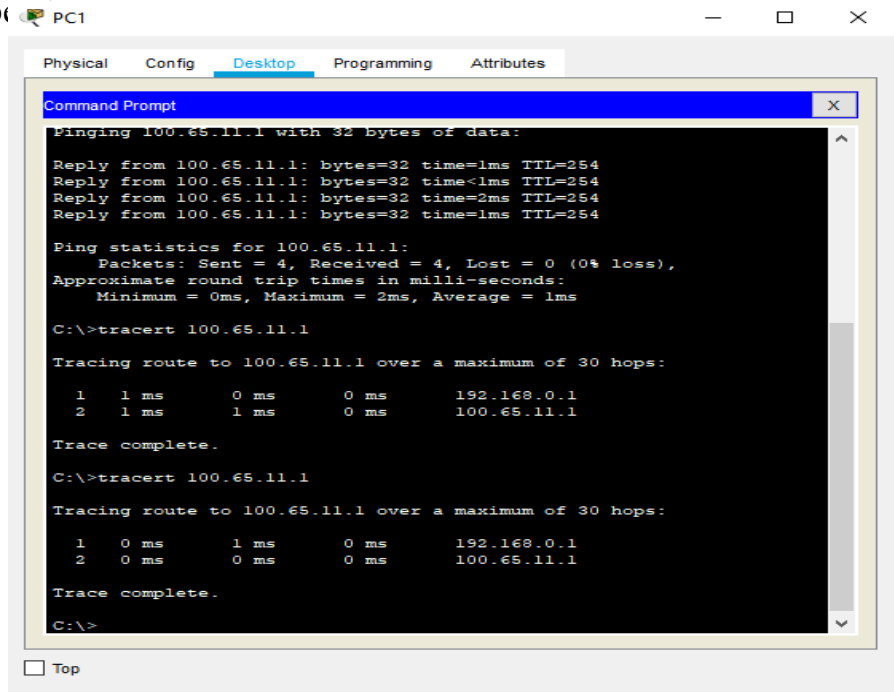
Схема роботи Ethernet світча



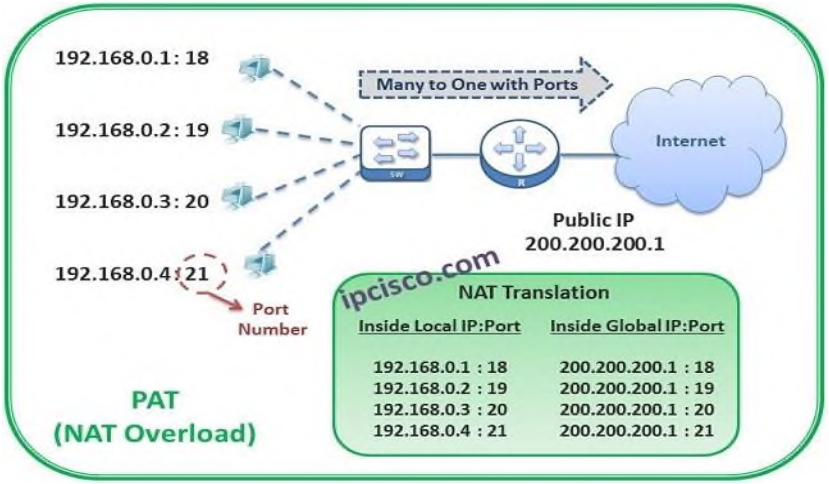
Загальна схема домашньої інтернет локальної мере



Зміна параметрів для загального доступу



Віртуальна перевірка роботи мережі



Перевантажений NAT



Налаштування NAT у веб-інтерфейсі роутера

ВИСНОВКИ

В даній магістерській роботі було наведено один із способів розробки моделі трафіка інтернет локальних мереж.

Розглянуто особливості інтернет локальних мереж, а саме їх типи, основні топології, варіанти з'єднання , а також дві основні технології в локальних мережах – Ethernet та Wi-Fi.

Наведена історія створення інтернет локальних мереж, а також подальший розвиток та їх вплив на техноло гічний світ.

Описана побудова, налаштування та застосування такої мережі за допомогою мережевого устаткування і стандартного програмного забезпечення та інструментів.

Моделювання та логічна структура мережі була побудована за допомогою інструмента CiscoPacketTracer. Даний інструмент надає користувачу зобразити логічну та фізичну структуру мережі в реальному часі та побачити її візуалізацію.

Основне налаштування мережі відбувається змінами стандартних параметрів роутера та Ethernetсвітча. Реалізація обладнання використовується в середовищі Windows 10.

Також було описано схематична фізична робота мережі та функціонування LAN з глобальною мережею Інтернет, а саме поділення домашньої інтернет локальної мережі на дві кімнати, як відбувається передача інформація між ними та з інтернет-провайдером.

Для передачі трафіку використовується кабель типу вита пара. Технологія, яка лежить в основі даної мережі – FastEthernet, що підходить для оптимального функціонування та відповідає усім потребам.

Був проведений аналіз особливостей сучасних технологій інтернет локальних мереж, розібрано основні переваги та недоліки таких мереж, які методи використовуються для безпеки та захисту інформації та яке майбутнє та розвиток чекає на LAN.

Інтернет локальні мережі зручно використовувати для полегшення роботи користувача, також для об’єднання обладнання, щоб використовувати його для загального використання.

Результати практичної частини даної дипломної роботи з налаштування домашньої інтернет локальної мережі можуть бути використані для потреб користувача, що бажають отримати доступ до всесвітньої мережі Інтернет, а також знання, які використані.

Отже, можна вважати, що завдання дипломної роботи виконано, є всі необхідні дані для реалізації розробки моделі трафіка інтернет локальних мереж

ДОПОВІДЬ ЗАКІНЧИD

ДЯКУЮ ЗА УВАГУ