МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний технічний університет

«Харківський політехнічний інститут»

Навчально-науковий інститут комп’ютерного моделювання, прикладної фізики та математики

Кафедра динаміки та міцності машин

Звіт

про виконання

лабораторної роботи № 9

по курсу «Комп’ютерні мережі та розподілені обчислювання»

з теми "Створення та налаштування бездротової мережі.

Бездротова мережа WEP"

                                                    Виконав:

студент групи ІКМ-220Б

Пономаренко О.В.

Викладач:

доцент кафедри ДММ

Трубаєв О.І.

Харків 2022

**Завдання лабораторної роботи**

**Завдання №1.** Створення нової бездротової мережі

**Завдання №2.** Налаштування бездротової мережі WPA

**Завдання №3.** Бездротова мережа з точкою доступу

**Завдання №4.** Бездротова мережа між офісами

**Завдання №5.** Налаштування комутуючого WI-FI з’єднання

**Завдання №6.** Бездротова мережа в Packet Tracer з бездротовим роутером

**Теоретичні відомості**

Створення нової бездротової мережі починається безпосередньо з конфігурації точки доступу - бездротового маршрутизатора (роутера) підключення до неї комп'ютерів та іншого бездротового обладнання.

**Класичний спосіб налаштування такий:**

спочатку проводиться підключення до точки доступу обладнання, а потім потрібно задати вручну ім'я бездротової мережі і ключ безпеки. У цій лабораторній роботі далі ми розглянемо різні варіанти бездротових мереж і способи їх налаштування в програмі CPT. Ключ безпеки бездротової мережі - унікальний код (пароль), який закриває доступ до вашої мережі. При цьому важливим є не стільки сам ключ, скільки тип шифрування. Справа в тому, що вся інформація, яка протікає між роутером і ПК шифрується. Якщо введено неправильний ключ, то пристрій просто не зможе розкодувати її. Це зроблено для підвищення безпеки. Варто зазначити, що на сьогоднішній день існує три типи шифрування Wi-Fi підключень: **WPA, WPA2, WEP.**

**WEP (Wired Equivalent Privacy)** — алгоритм для забезпечення безпеки мереж Wi-Fi. Використовується для забезпечення захисту переданих даних.

***Бездротова мережа WPA***

Типи шифрування мережі WPA і WPA2 потребують від абонентів введення

унікального пароля, без нього неможливо виконати підключення. Після перевірки введеного ключа всі дані, які передаються між учасниками мережі, шифруються.

Сучасні роутери підтримують обидві технології. Але, WPA2 все ж надає більш високий захист. Тому по можливості слід обирати саме його.

**WPA (Wi-Fi Protected Access)** — являє собою технологію захисту бездротової

Wi-Fi мережі. Плюсами WPA є посилена безпека даних і посилений контроль доступу до бездротових мереж, а також - сумісність між безліччю бездротових пристроїв як на апаратному рівні, так і на програмному.

Точка доступу в англійській термінології – **Wireless Access Point.** [1]

***Розуміння WEP***

Подібно до того, як будь-хто в зоні дії радіостанції може налаштуватися на частоту станції та прослухати сигнал, будь-який бездротовий мережевий пристрій у зоні дії точки доступу/мосту може приймати радіопередачі точки доступу/мосту. Оскільки WEP є першою лінією захисту від зловмисників, Cisco рекомендує використовувати повне шифрування у бездротовій мережі.

Шифрування WEP шифрує радіозв’язок між точками доступу/мостами, щоб зберегти конфіденційність зв’язку. Точки доступу/мости зв’язку використовують той самий ключ WEP для шифрування та розшифрування радіосигналів. Ключі WEP шифрують як одноадресні, так і групові повідомлення. Одноадресні повідомлення адресуються лише одному пристрою в мережі. Багатоадресні повідомлення адресуються багатьом пристроям у мережі.

**Автентифікація протоколу розширюваної автентифікації (EAP)** надає динамічні ключі WEP для бездротових пристроїв. Динамічні ключі WEP більш безпечні, ніж статичні або незмінні ключі WEP. Якщо зловмисник пасивно отримує достатньо пакетів, зашифрованих тим самим ключем WEP, зловмисник може виконати обчислення, щоб дізнатися ключ і використати його для приєднання до вашої мережі. Оскільки динамічні ключі WEP часто змінюються, вони не дозволяють зловмисникам виконати обчислення та дізнатися ключ. Див. «Налаштування типів автентифікації», щоб отримати детальну інформацію про EAP та інші типи автентифікації.

**Комплекти шифрів** — це набори алгоритмів шифрування та цілісності, розроблені для захисту радіозв’язку у бездротовій локальній мережі. Ви повинні використовувати набір шифрів, щоб увімкнути **Wi-Fi Protected Access (WPA)** або **Cisco Centralized Key Management (CCKM)**. Оскільки набори шифрів забезпечують захист WEP, а також дозволяють використання автентифікованого керування ключами, Cisco рекомендує вам увімкнути WEP за допомогою команди шифрування режиму шифрування в CLI або за допомогою розкривного меню шифрування в інтерфейсі веб-браузера. Комплекти шифрів, які містять TKIP, забезпечують найкращий захист для вашої бездротової локальної мережі, а набори шифрів, які містять лише WEP, є найменш безпечними.

Ці функції безпеки захищають трафік даних у бездротовій локальній мережі:

•**WEP** (Wired Equivalent Privacy) — WEP — це стандартний алгоритм шифрування 802.11, спочатку розроблений для забезпечення бездротової локальної мережі такого ж рівня конфіденційності, який доступний для дротової локальної мережі. Однак базова конструкція WEP має недоліки, і зловмисник може порушити конфіденційність, доклавши розумних зусиль.

•**TKIP** (протокол цілісності тимчасового ключа) — TKIP — це набір алгоритмів, що оточують WEP, розроблений для досягнення найкращої можливої ​​безпеки на застарілому обладнанні, створеному для роботи з WEP. TKIP додає чотири вдосконалення до WEP:

– Функція змішування ключів для кожного пакета для подолання атак зі слабким ключем

– Нова дисципліна секвенування IV для виявлення атак повтору

– Криптографічна перевірка цілісності повідомлень (MIC), яка називається Michael, для виявлення підробок, таких як перевертання бітів і зміна джерела та призначення пакетів

– Розширення IV простору, щоб практично усунути необхідність повторного введення ключа

• **CKIP** (протокол цілісності ключа Cisco) — техніка перестановки ключа WEP від ​​Cisco на основі раннього алгоритму, представленого групою завдань безпеки IEEE 802.11i.

• **CMIC** (перевірка цілісності повідомлень Cisco) — як і Майкл TKIP, механізм перевірки цілісності повідомлень Cisco розроблений для виявлення атак підробки. [2]

**Хід роботи**

**Завдання №1.**

Для першого завдання створимо таку мережу (рис. 1)

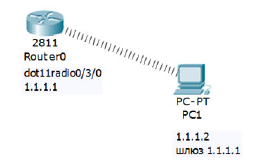


Рисунок 1 - Постановка задачі

Оснастимо маршрутизатор радіоточкою доступу HWIC-AP-AG-B

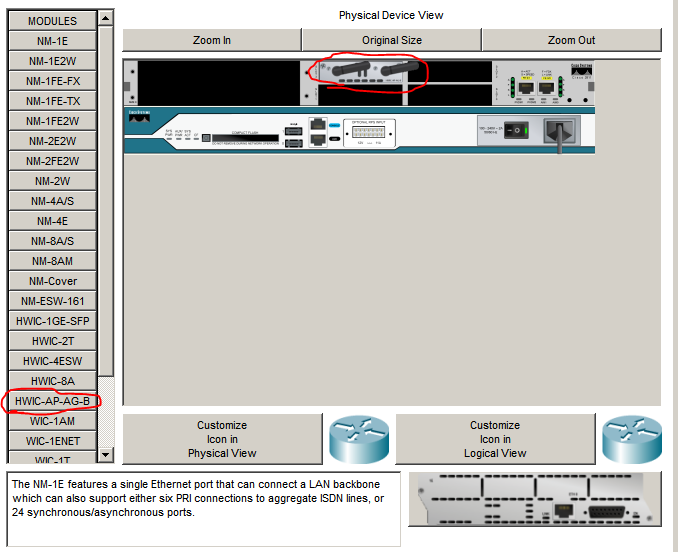


Рисунок 2 – встановлення модуля для роутера

Вставимо в ПК бездротовий адаптер WMP300N (рис. 3)

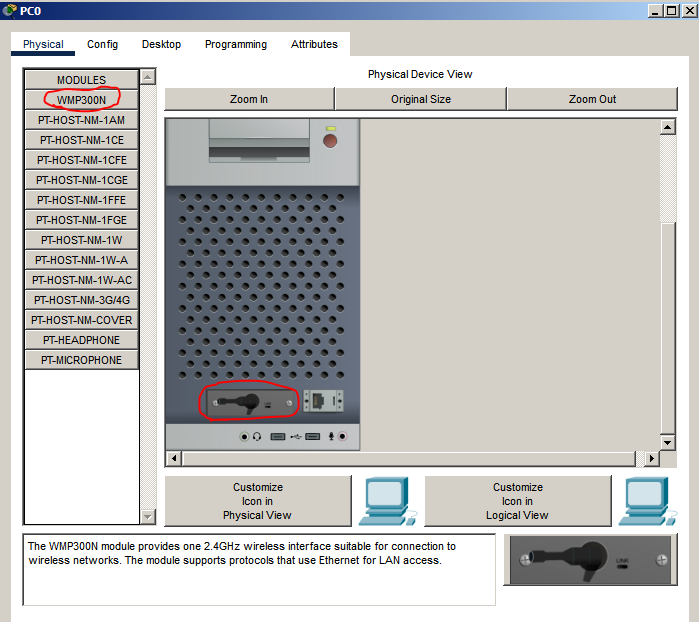


Рисунок 3 – встановлення адаптера на ПК

Налаштуємо бездротовий адаптер на PC1 (рис. 4)

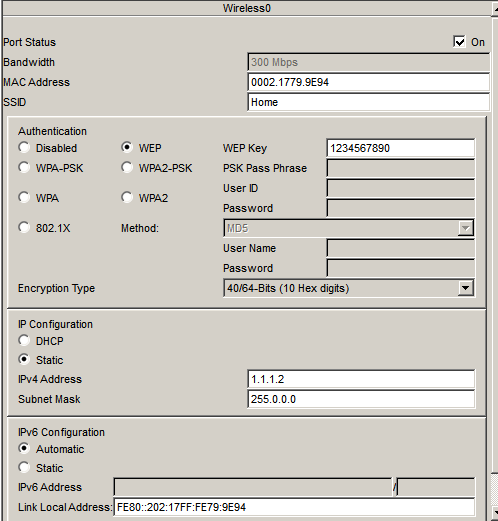


Рисунок 4 - налаштування адаптера на комп'ютері

Тепер налаштуємо наш роутер, встановимо ім’я Home та WEP пароль 123456790 (рис. 5)

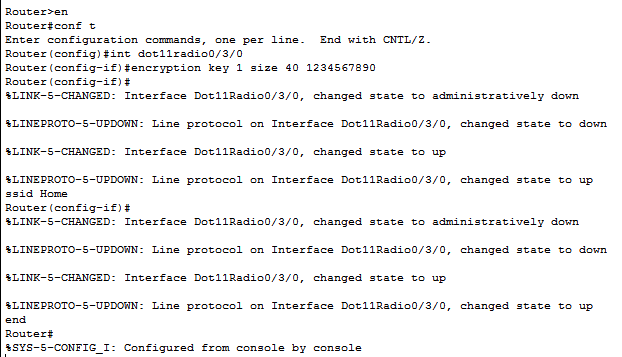


Рисунок 5 - налаштування інтерфейсу для адаптера

Підключимось до нашого роутера з комп'ютера (рис. 6)

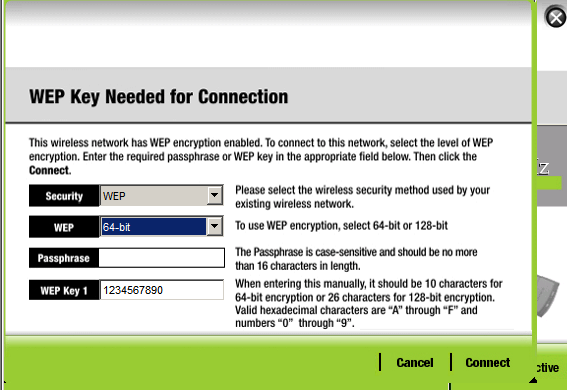


Рисунок 6 - підключення до мережі

Спробуємо пінганути наш роутер з комп’ютера (рис. 7)

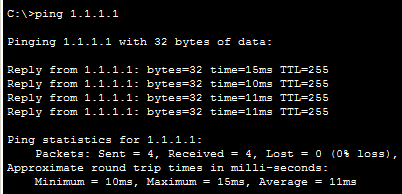


Рисунок 7 - пінг сервера

Як ми бачимо все працює справно.

**Завдання №2.**

Для другого завдання створимо таку мережу (рис. 8)

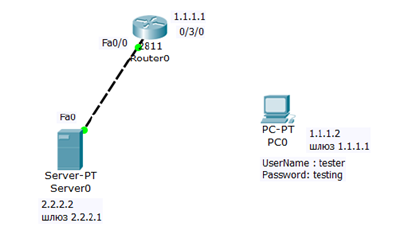


Рисунок 8 - схема мережі

Проводимо налаштування адаптера ПК (рис. 9)

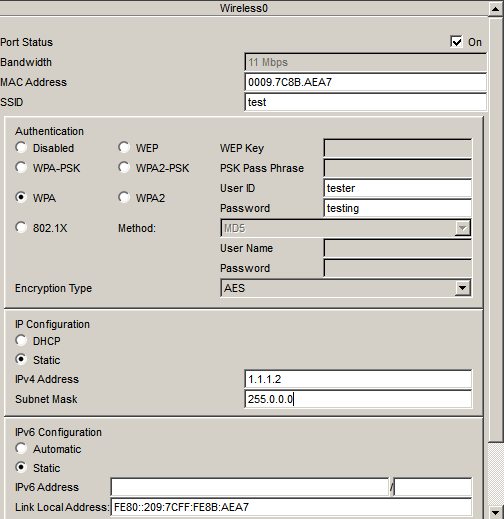


Рисунок 9 - конфігурація ПК

Знайдемо наш роутер у списку та підключимось до нього (рис. 10)

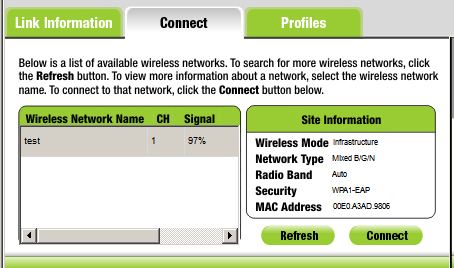


Рисунок 10 - список WAN мереж

Тепер спробуємо пінганути сервер та роутер (рис. 11)

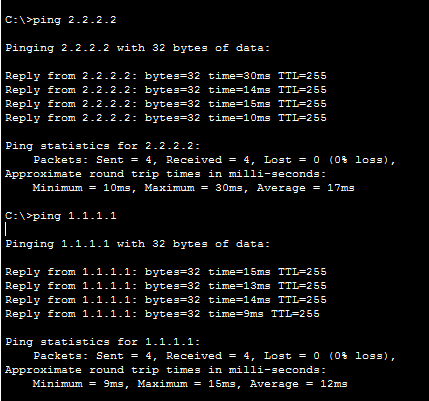


Рисунок 11 - пінг маршрутизатора та сервера

**Завдання №3.**

Для другого завдання створимо таку мережу (рис. 12)

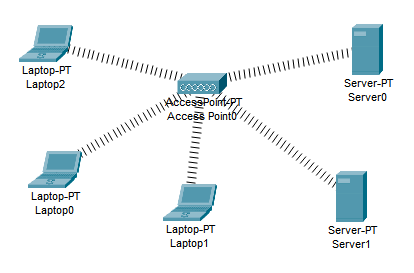


Рисунок 12 - мережа третього завдання

Розглянемо налаштування точки доступу, вони відповідають налаштуванням за замовчуванням (рис. 13)

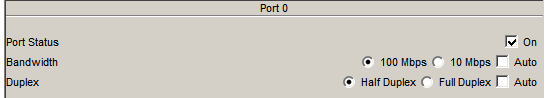


Рисунок 13 - налаштування AP

Статичне налаштування ноутбуку (рис. 14)

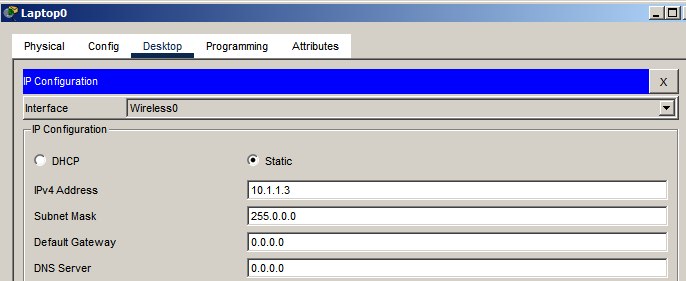


Рисунок 14 – статичне налаштування ноутбуку

Динамічне налаштування ноутбуку (рис. 15)

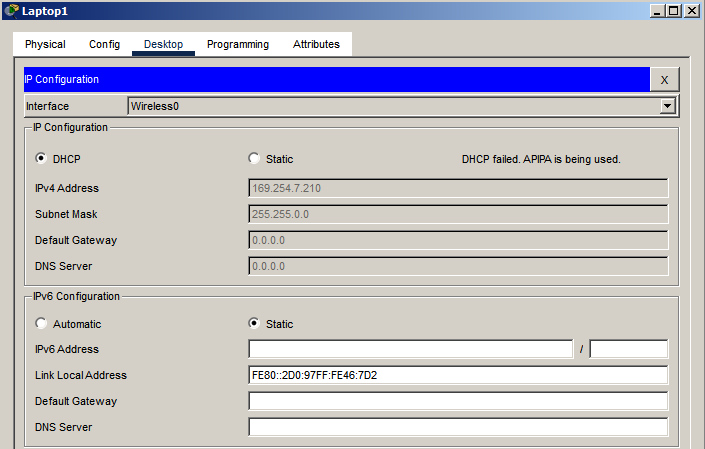


Рисунок 15 - динамічне налаштування ноутбуку

Налаштування серверів (рис. 16-17)

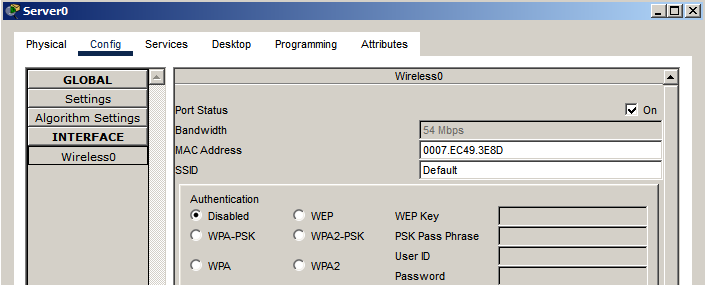


Рисунок 16 - налаштування 1 сервера

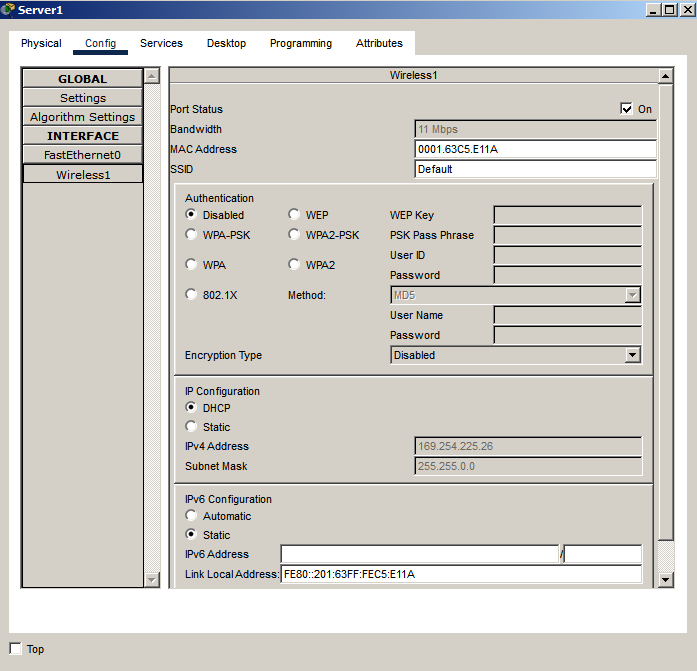


Рисунок 17 - налаштування 2 сервера

Давайте пінганемо з другого ноутбуку другий сервер (рис. 18)

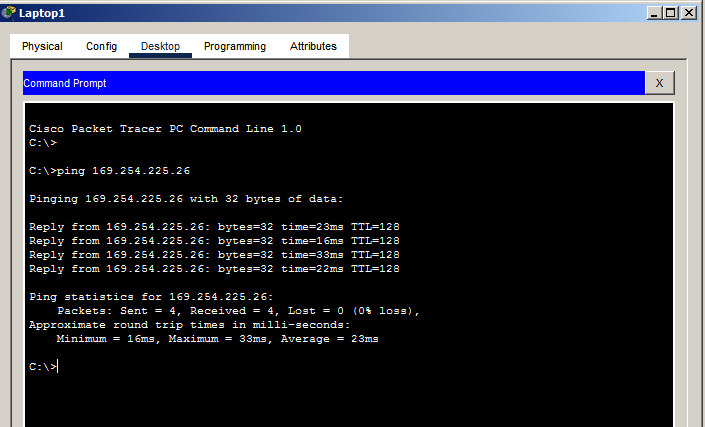


Рисунок 18 - пінг сервера з ноута

Як ми бачимо, все чудово налаштовано і працює справно.

**Завдання №4.**

Налаштуємо наступну бездротову мережу (рис. 19)

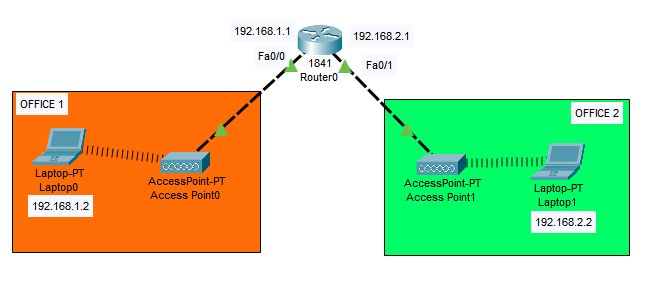


Рисунок 19 - мережа 4 завдання

Пропишемо ip адреси нашим ноутбукам (рис. 20)

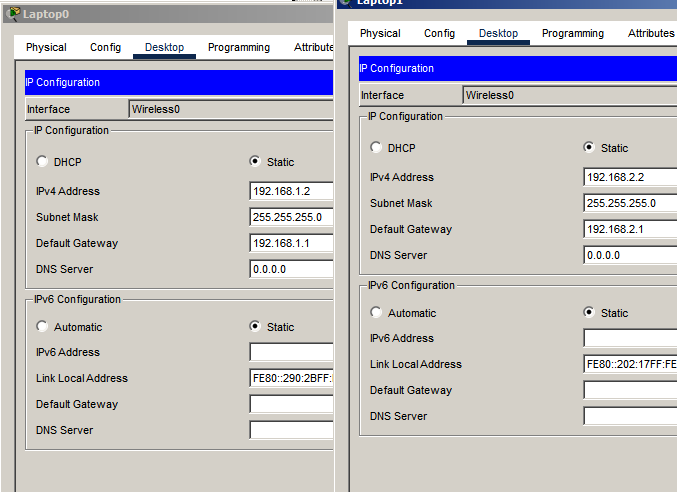


Рисунок 20 - На Laptop0 і Laptop1 вказуємо адресу шлюзу

SSID за даємо на обох точках доступу (рис. 21)

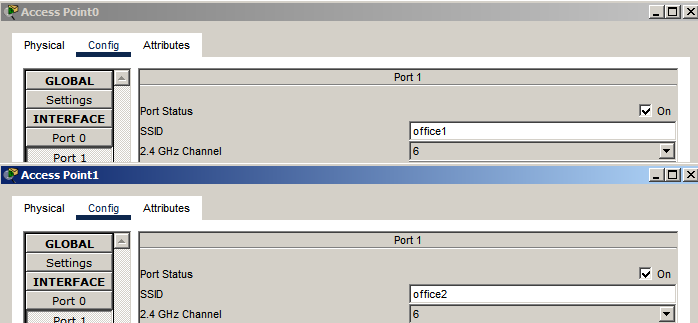


Рисунок 21 - SSID на точках доступу

Перевіряємо зв’язок ПК з різних офісів (рис. 22)

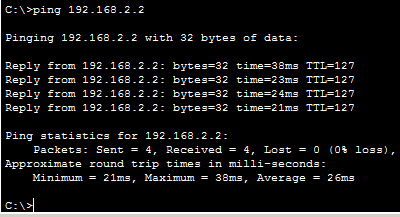


Рисунок 22 - Перевіряємо зв’язок ПК з різних офісів

**Завдання №5.**

Зберемо і налаштуємо мережу, зображену на рис. 23

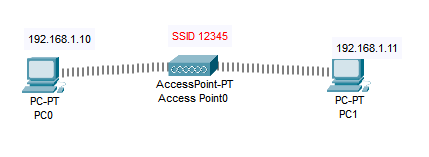


Рисунок 23 - мережа п'ятого завдання

Спочатку задаємо ім'я мережі (SSID) на точці доступу (рис. 24)

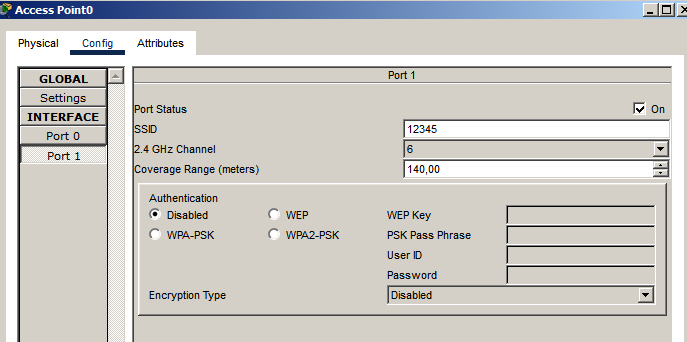


Рисунок 24 - налаштування точки доступу

В обидва ПК вставляємо бездротовий адаптер Linksys-WPM-300N (рис. 25)

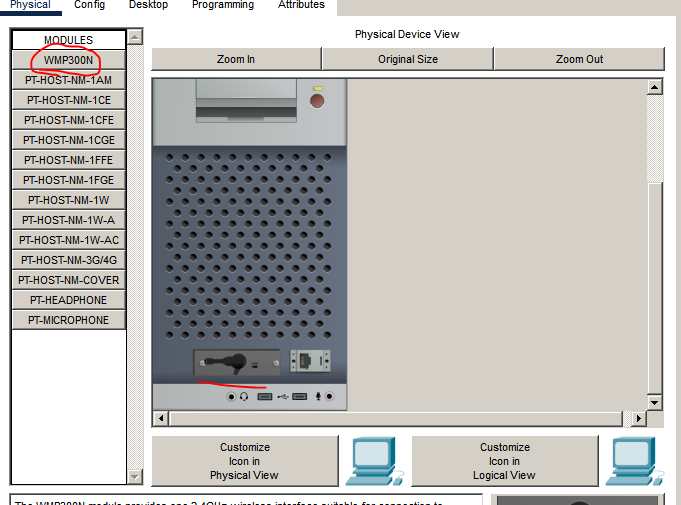


Рисунок 25 - втавляємо адаптер в ПК

Установлюємо зв'язок точки доступу і PC0, для цього натискаємо на кнопку PC Wireless (рис. 26)

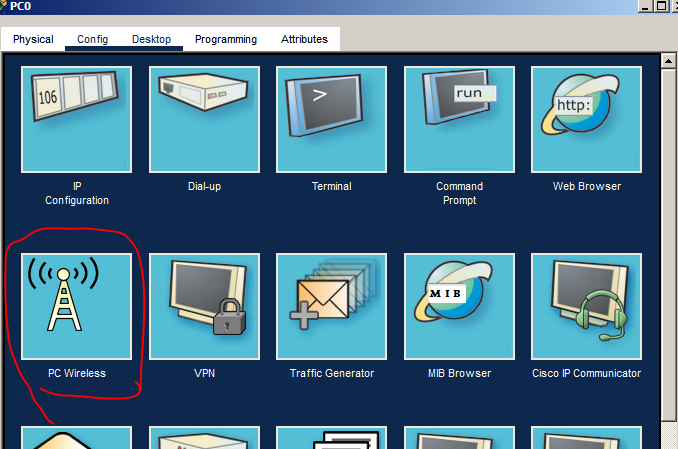


Рисунок 26 - вибираємо программку для встановлення зв'язку

Відкриваємо вкладку Connect і натискаємо на кнопку Connect (рис. 27)



Рисунок 27 - під'єднуємость до точки доступу

У результаті вийде динамічний зв’язок PC0 і Access Point-PT (рис. 28)

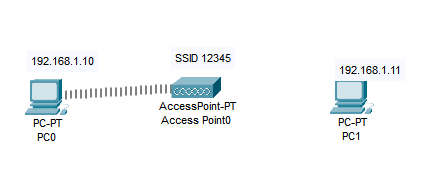


Рисунок 28 - поточний результат

Змінюємо динамічну адресу на статичну (рис. 29)

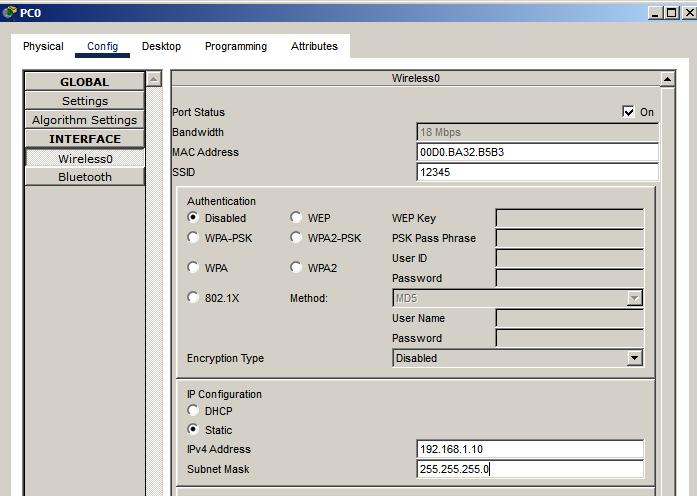


Рисунок 29 - встановлюємо статичну адресу для 1 ПК

Аналогічно налаштовуємо PC1 і перевіряємо зв’язок між ПК (рис. 30)

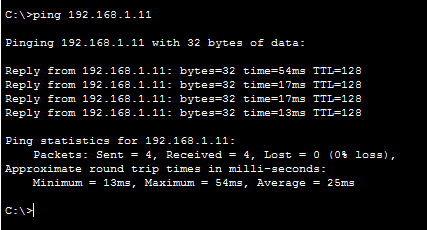


Рисунок 30 - пінгуємо другий ПК з першого

**Завдання №6.**

На рис. 31 приведена схема мережі з бездротовим роутером.



Рисунок 31 - схема мережі з бездротовим роутером

Якщо забезпечимо обидва ПК бездротовим модулем, то в даній мережі можна спостерігати появу WI-FI зв'язку (рис. 32)

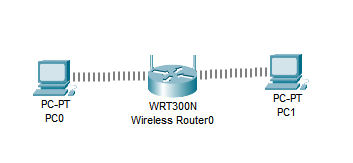


Рисунок 32 - поява WIFI зв'язку

Зайдемо на роутер і подивимося на його IР-адресу. Як бачимо, включений DHCP-service і роутер отримує IP-адресу автоматично (рис. 33)

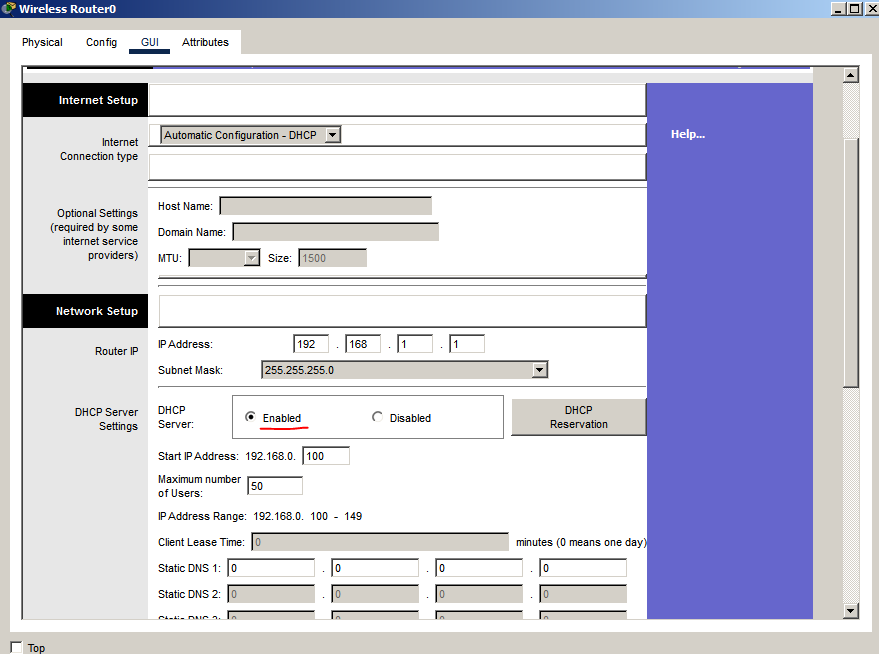


Рисунок 33 - автоматичне конфігурування роутера

На вкладці Config налаштуємо аутентифікацію роутера (рис. 34)

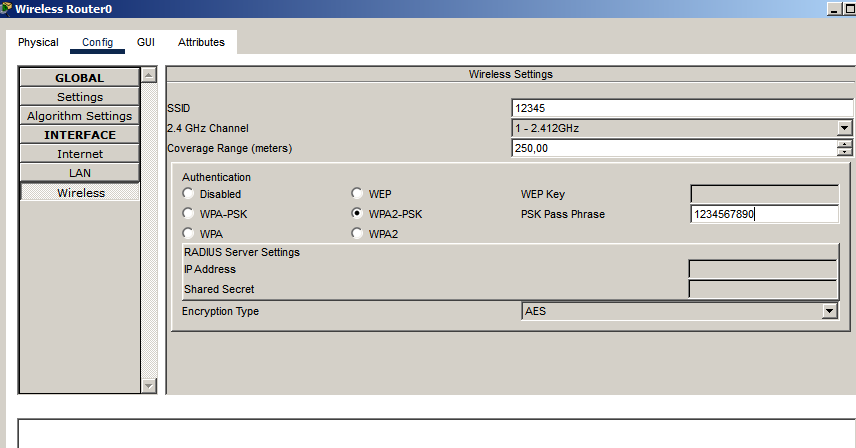


Рисунок 34 - вводимо SSID та WPA2-PSK

Для PC0 заходимо в меню PC Wireless (рис. 35)

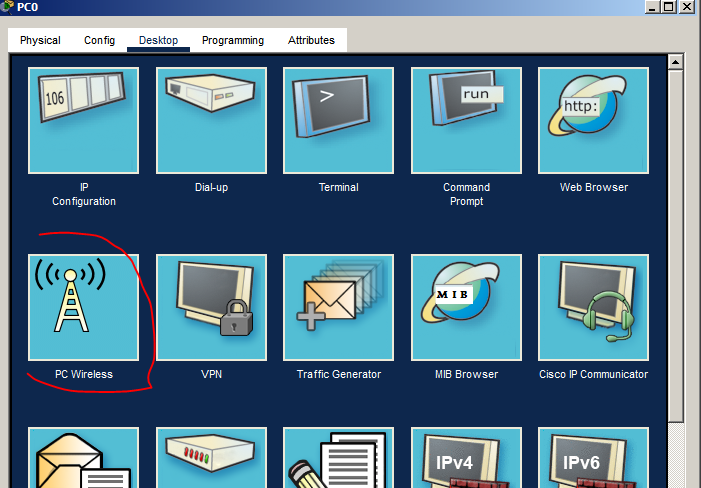


Рисунок 35 - знаходимо PC Wireless

Встановлюємо з’єднання PC0 і роутера (рис. 36)

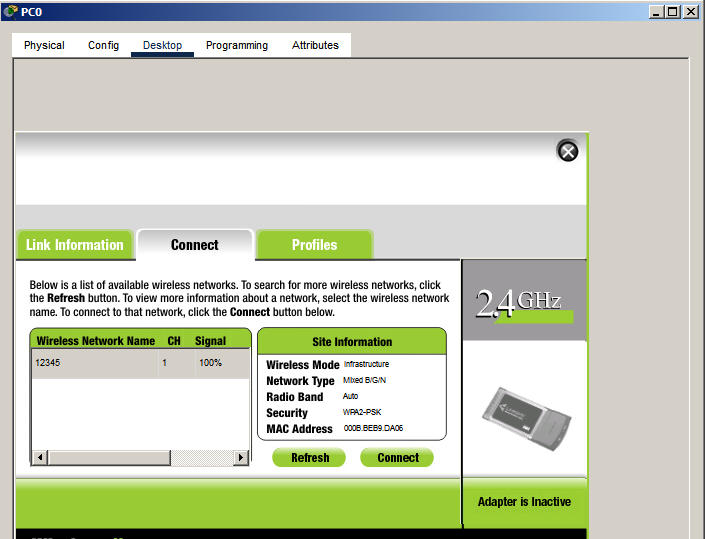


Рисунок 36 - на вкладці Connect натискаємо на кнопку Connect

Для аутентифікації необхідний WPA2-PSK пароль, тобто 1234567890 (рис. 37)

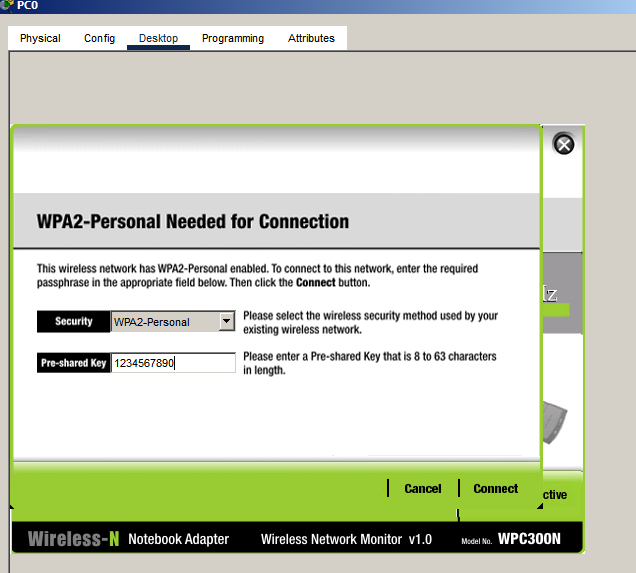


Рисунок 37 - вводимо пароль і натискаємо кнопку Connect

"Пропуск" на вхід користувача в мережу пред’явлено і зв'язок пристроїв встановлений, так само робимо з другим комп’ютером (рис. 38)

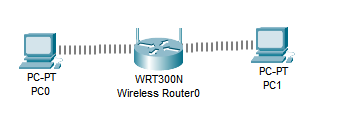


Рисунок 38 - обидва комп'ютери з'єднані з роутером

Дізнаємось динамічну IP адресу для PC1 і пінгуємо її з PC0 (рис. 39)

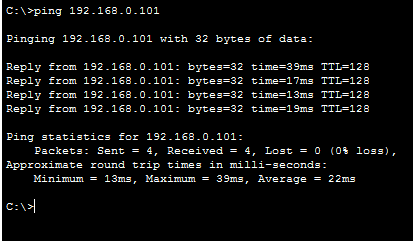


Рисунок 39 - пінгуємо другий комп'ютер

**Висновки**

Отже, виконуючи дану лабораторну роботу я навчився поєднувати комп’ютери у WAN за допомогою адаптерів. Також, тепер я вмію налаштовувати комутуючі WI-FI з’єднання, навчився захищати мережі завдяки встановленню авторизації на роутери, більш того, я тепер вмію встановлювати wifi адаптери на ПК, для спілкування комп’ютерів по Wifi, а не по кабелю, на випадок, якщо в ньому немає вбудованого такого адаптера.

**Список джерел**

1. Комп’ютерний практикум № 9.
2. https://www.cisco.com/c/en/us/td/docs/wireless/access\_point/1300/12-2\_15\_JA/configuration/guide/o13wep.html