

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ
до виконання лабораторних робіт з дисципліни
"Бездротові технології"
для бакалаврів спеціальності 123 "Комп'ютерна інженерія",
усіх форм навчання.
Моделювання Wi-Fi мереж. Частина 2

Методичні вказівки до виконання лабораторних робіт з дисципліни "Бездротові технології" для бакалаврів спеціальності 123 "Комп'ютерна інженерія", усіх форм навчання. Моделювання Wi-Fi мереж. Частина 2 / Укл. Г.Г. Киричек. – Запоріжжя: Національний університет «Запорізька політехніка», 2023. – 30 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.

Рецензент:

М.Ю. Тягунова, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 8 від 27.04.2023

Рекомендовано до видання
НМК КНТ
Протокол № 9 від 28.04.2023

ЗМІСТ

1 ЛАБОРАТОРНА РОБОТА.....	4
1.1 Загальні відомості.....	4
1.2 Налаштування бездротової точки доступу	9
1.3 Конфігурування обладнання мережі	11
1.4 Індивідуальне завдання	13
1.5 Зміст письмового звіту	15
1.6 Контрольні питання.....	15
2 ЛАБОРАТОРНА РОБОТА.....	16
2.1 Загальні відомості.....	16
2.2 Захист комп'ютера.....	18
2.3 Конфігурування обладнання мережі	21
2.4 Індивідуальне завдання	27
2.5 Зміст письмового звіту	29
2.6 Контрольні питання.....	29
Рекомендована література.....	30

1 ЛАБОРАТОРНА РОБОТА.

Моделювання бездротової мережі з точками доступу в режимі wds bridge mode

Мета роботи: ознайомитися з режимом роботи точок доступу WDS Bridge mode, які утворюють мостове з'єднання.

1.1 Загальні відомості

Термін WDS (Wireless Distribution System) розшифровується як «розподілена бездротова система». У цьому режимі точки доступу з'єднуються тільки між собою, утворюючи мостове з'єднання.

Всі точки в режимі Wireless Distribution System використовують один канал, тому їх кількість не повинна бути великою. Підключення клієнтів здійснюється тільки за допомогою провідної мережі через uplink-порти точок (рис. 1.1).

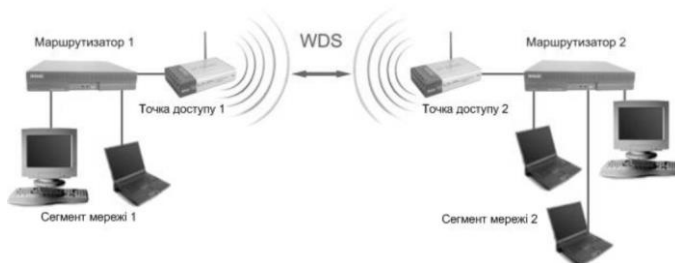


Рисунок 1.1 – Мостовий режим

Режим бездротового моста, аналогічно дротовим мостам, служить для об'єднання підмереж, або сегментів мереж в загальну мережу. За допомогою бездротових мостів можна об'єднувати дротові LAN, що знаходяться як в сусідніх будівлях, так і на відстані до декількох кілометрів. Це дозволяє об'єднати в мережу центральний офіс і філіали та підключити клієнтів до мережі провайдера (рис. 1.2).

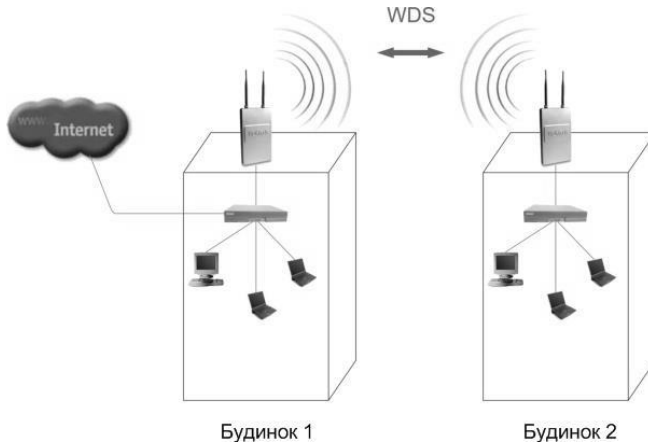


Рисунок 1.2 – Мостовий режим між будівлями

Бездротовий міст може використовуватися там, де прокладка кабелю між будівлями небажана або неможлива. Дане рішення дозволяє досягти значної економії коштів та забезпечує простоту настройки і гнучкість конфігурації при переміщенні офісів.

До точки доступу, що працює в режимі моста, підключення бездротових клієнтів неможливо. Бездротовий зв'язок здійснюється тільки між парою точок, що реалізують міст.

Термін WDS with AP (WDS with Access Point) означає "розподілена бездротова система, яка включає точку доступу", тобто за допомогою цього режиму можна не тільки організувати мостовий зв'язок між точками доступу, але й одночасно підключити клієнтські комп'ютери (рис.1.3). Це дозволяє досягти істотної економії обладнання та спростити топологію мережі. Дана технологія підтримується більшістю сучасних точок доступу.

Тим не менш, необхідно пам'ятати, що всі пристрої в складі однієї WDS with AP працюють на одній частоті і створюють взаємні перешкоди, що обмежує кількість клієнтів до 15-20 вузлів.

Для збільшення кількості клієнтів, які підключаються можна використовувати декілька WDS-мереж (WDS with AP-мереж), налаштованих на різні канали не перекриті та з'єднані проводами через uplink-порти.

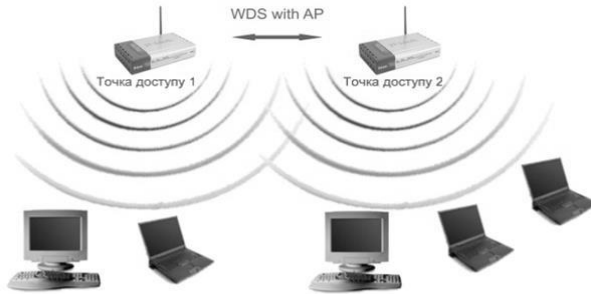


Рисунок 1.3 – Режим WDS with AP

Топологія організації бездротових мереж в режимі WDS (WDS with AP) аналогічна звичайним провідним топологіям.

Топологія типу "шина" за своєю структурою допускає ідентичність мережного устаткування комп'ютерів, а також рівноправність всіх абонентів (рис. 1.4).

Тут відсутній центральний абонент, через який передається вся інформація, і це збільшує її надійність (адже при відмові будь-якого центра перестає функціонувати вся керована цим центром система).



Рисунок 1.4 – Топологія типу "шина"

Додати нових абонентів у шину досить просто. Треба ввести параметри нової точки доступу, що призведе лише до короткочасного перезавантаження останньої точки. Шині не страшні відмови окремих точок, так як всі інші комп'ютери мережі зможуть нормально продовжувати обмін між собою, але при цьому решта комп'ютерів не зможе отримати доступ в Інтернет.

Топологія типу "кільце" – це топологія, у якій кожна точка доступу з'єднана тільки з двома іншими (рис. 1.5). Чітко виділеного центру в даному випадку немає, всі точки є однаковими. Підключити нових абонентів у "кільце" просто, хоча це вимагає обов'язкової зупинки роботи двох крайніх точок від нової точки доступу.

У той же час основна перевага кільця полягає в тому, що ретрансляція сигналів кожним абонентом дозволяє істотно збільшити розміри всієї мережі в цілому (часом до кількох десятків кілометрів). Кільце в цьому відношенні істотно перевершує будь-які інші топології.

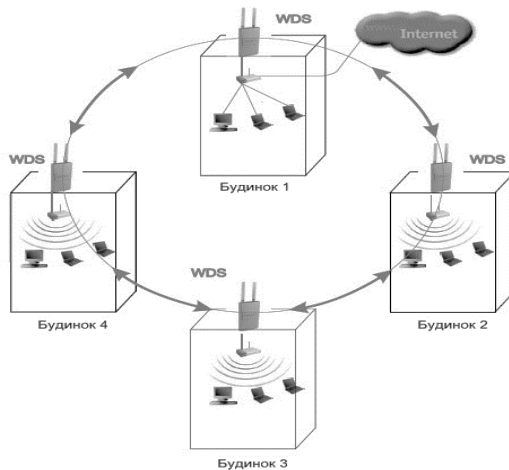


Рисунок 1.5 – Топологія типу "кільце"

Топологія зв'язків між точками в цьому режимі являє собою ациклічний граф типу "дерево", тобто дані з Інтернет від точки 4 до точки 2 проходять по двох напрямках - через точку 1 і 3. Для усунення зайвих зв'язків, здатних призводити до появи циклів в графі, реалізується алгоритм Spanning tree.

Топологія типу «зірка» - це топологія з явно виділеним центром, до якого підключаються всі інші абоненти (рис. 1.6). Весь обмін інформацією йде виключно через центральну точку доступу, на яку в результаті лягає дуже велике навантаження. Якщо говорити про стійкість зірки до відмов точок, то вихід з ладу звичайної точки доступу

ніяк не відбивається на функціонуванні решти мережі, зате будь-яка відмова центральної точки робить мережу повністю непрацездатною.

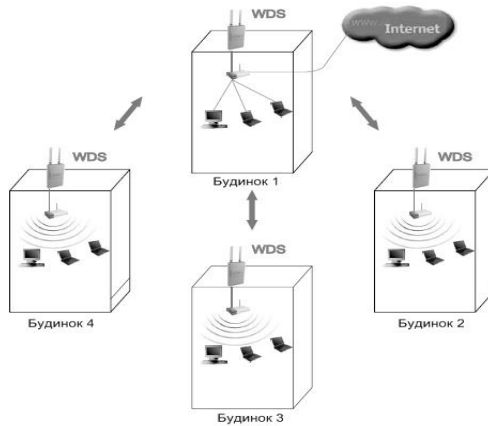


Рисунок 1.6 – Топологія типу "зірка"

Істотний недолік топології "зірка" полягає в жорсткому обмеженні кількості абонентів. Так як всі точки працюють на одному каналі, зазвичай центральний абонент може обслуговувати не більше 10 периферійних абонентів через падіння швидкості.

У більшості випадків, наприклад для об'єднання кількох районів у місті, використовують комбіновані топології. Далі в роботі описується процес створення моста типу "точка - точка" (рис. 1.7).

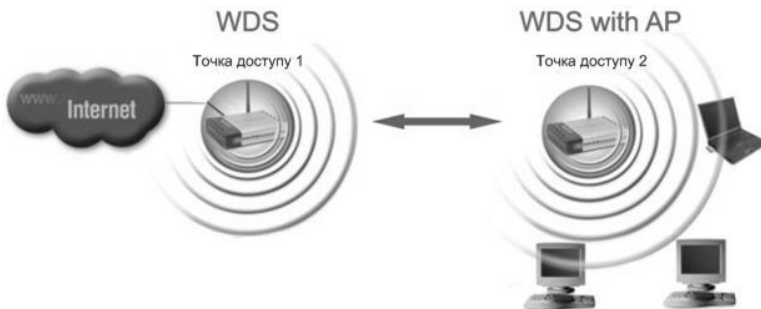


Рисунок 1.7 – Міст типу "точка – точка"

1.2 Налаштування бездротової точки доступу

Рекомендації з налаштування бездротової точки доступу реалізуємо для моделі мережі, представленої на рисунку 1.8. Для цього виконайте наступні дії:

- в робочу область перенесіть AccessPoint-PT (для зручності краще перейменувати його у AP-1);
- в робочу область перенесіть 2 HomeRouter-PT-AC (для зручності краще перейменувати його у WR-A1 та WR-B1);
- в робочу область перенесіть 2 робочі станції PC-PT та (для зручності краще перейменувати його у PC-A1 та PC-B1);
- в робочу область перенесіть 4 ноутбука Laptop (для зручності краще перейменувати його LAP-A2, LAP-A3 та LAP-B2, LAP-B3).

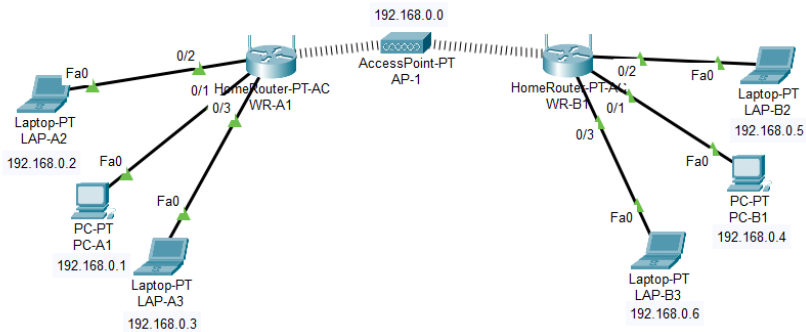


Рисунок 1.8 – Модель мережі

Таблиця 1.1 – Параметри інтерфейсів

Device (Hostname)	IP address	Subnet Mask
PC-A1	192.168.0.1	255.255.255.0
LAP-A2	192.168.0.2	255.255.255.0
LAP-A3	192.168.0.3	255.255.255.0
PC-B1	192.168.0.4	255.255.255.0
LAP-B2	192.168.0.5	255.255.255.0
LAP-B3	192.168.0.6	255.255.255.0

Для установки Wi-Fi роутера необхідно перейти на закладку Wireless Devices (рис. 1.9) і перетягти HomeRouter (підкреслений) елемент у робочу область.

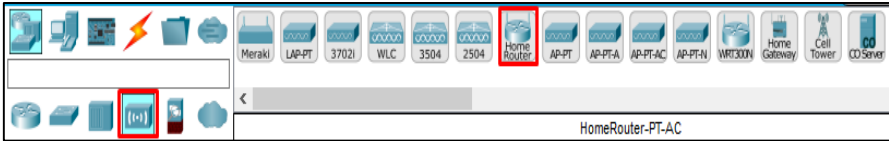


Рисунок 1.9 – Вибір Wi-Fi

Для установки точки доступу необхідно перейти на закладку Wireless Devices (рис. 1.10) і перетягти AP-PT (підкреслений) елемент у робочу область.

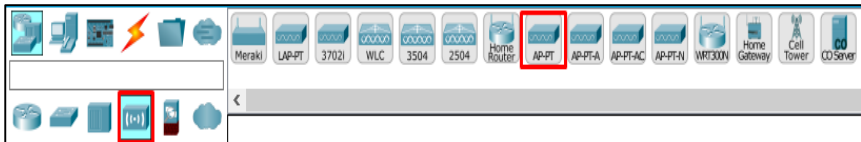


Рисунок 1.10 – Вибір точки доступу

Наступним кроком є з'єднання між собою елементів мережі. Для усіх з'єднань будемо використовувати кабель вита пара (рис. 1.11).



Рисунок 1.11 – Вибір типу з'єднання елементів мережі

Для того, щоб з'єднати 2 інтерфейси різних пристроїв виконайте наступне:

- виберіть відповідний кабель, після чого покажчик миші зміниться;
- далі клікнути лівою кнопкою по першому пристрою, який ви хочете підключити;

- у спливаючому вікні клікніть по порту, до якого буде підключено кабель;
- задайте кінцеву точку підключення кабелю: вибираємо наступний пристрій і аналогічно підключаємо порт (рис. 1.12).

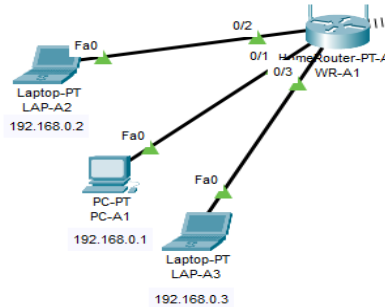


Рисунок 1.12 – Підключення кабелю

1.3 Конфігурування обладнання мережі

Відкрити налаштування AccessPoint-PT та перейти у вкладку «Config → Port 1» та вписати в поле «SSID» найменування Wi-Fi мережі (рис. 1.13).

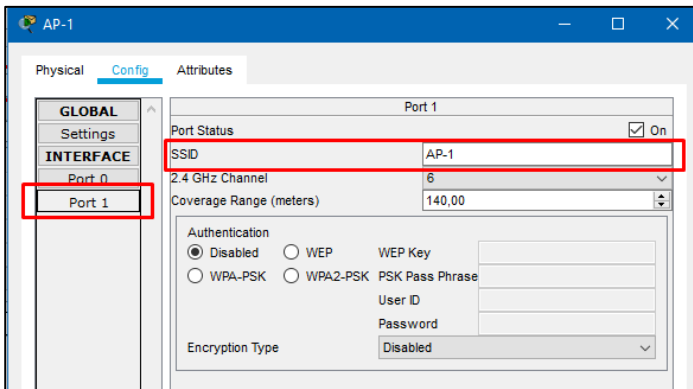


Рисунок 1.13 – Налаштування точки доступу

Відкрити налаштування Wi-Fi router HomeRouter-PT-AC(WR-A1) перейти у вкладку «Config → Internet» та вибрати параметр «Media Bridge» (рис. 1.14).

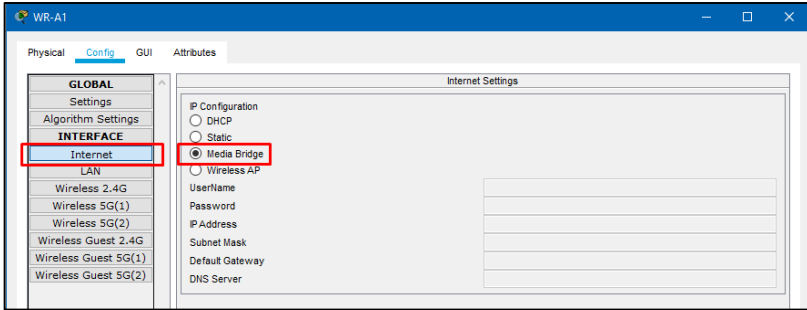


Рисунок 1.14 – Налаштування Wi-Fi роутера

Далі необхідно перейти у вкладку «GUI → Wireless → Wireless Security» та вказати SSID точки доступу AP-1 (рис. 1.15). Після введення назви мережі обов'язково натиснути «SAVE SETTINGS». Аналогічно зробити для WR-B1.

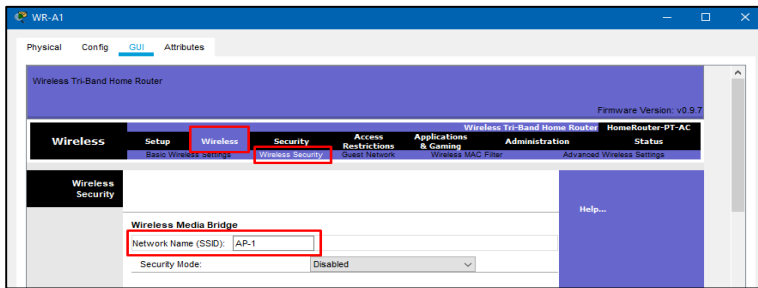


Рисунок 1.15 – Налаштування Wi-Fi роутера

Наступним кроком необхідно налаштувати IP адреси на всіх PC та Laptop для з'єднання AccessPoint-PT. Відкрити налаштування PC перейти у вкладку «Desktop → IP Configuration → Static», потім потрібно ввести необхідні параметри (рис. 1.16). Параметри інтерфейсів наведені у таблиці 1.2.

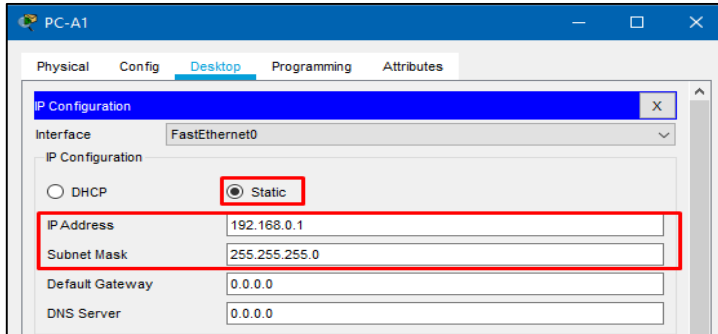


Рисунок 1.16 – Додавання IP адреси

Далі перевірте з'єднання всіх пристроїв в мережі та зробіть відповідні висновки. Прослідкуйте, які протоколи працюють при обміні інформацією та що змінюється у структурі даних під час проходження кадрів та пакетів через різні пристрої мережі (за допомогою режиму Simulation).

1.4 Індивідуальне завдання

Доповніть мережу додавши до пристрою, вказаного в таблиці 1.2, додаткове обладнання згідно варіанту. IP адреса залежить від номера студента наприклад студент під номером 6 має такий адрес:

PC-C1 → 192.168.(6).1;

PC-C2 → 192.168.(6+1).1.

Таблиця 1.2 – Варіанти до самостійної роботи

1	Додати Wi-Fi роутер WR-C1 (з'єднання бездротове) до точки доступу AP-PT, 2 PC до нового роутера (отримують статичні IP)
2	Додати 2 Laptop (отримують статичні IP) до Wi-Fi роутера WR-A1 та 2 PC (отримують статичні IP) до Wi-Fi роутера WR-B1
3	Додати Wi-Fi роутер WR-C1 та WR-D1 (з'єднання бездротове) до точки доступу AP-PT, 2 Laptop (отримують статичні IP) до WR-C1 роутера та 2 PC (отримують статичні IP) до WR-D1 роутера

Продовження таблиці 1.2

4	Додати Wi-Fi роутер WR-D1 (з'єднання бездротове) до точки доступу AP-PT, 1 Laptop (отримують статичні IP) до нового роутера, 1 Laptop (отримують статичні IP) до WR-A1 та 2 PC (отримують статичні IP) до WR-B1
5	Додати Wi-Fi роутер WR-C1 (з'єднання бездротове) до точки доступу AP-PT, 2 Laptop та 1 PC (отримують статичні IP) до нового роутера
6	Додати Wi-Fi роутер WR-D1 (з'єднання бездротове) до точки доступу AP-PT, 2 PC та 1 Laptop (отримують статичні IP) до нового роутера
7	Додати Wi-Fi роутер WR-C1 та WR-D1 (з'єднання бездротове) до точки доступу AP-PT, 1 Laptop (отримують статичні IP) до WR-C1 роутера та 1 PC (отримують статичні IP) до WR-D1 роутера, 1 Laptop (отримують статичні IP) до WR-A1
8	Додати Wi-Fi роутер WR-C1 та WR-D1 (з'єднання бездротове) до точки доступу AP-PT, 3 Laptop (отримують статичні IP) до WR-C1 роутера та 1 PC (отримують статичні IP) до WR-D1 роутера
9	Додати Wi-Fi роутер WR-C1 (з'єднання бездротове) до точки доступу AP-PT, 2 Laptop до нового роутера (отримують статичні IP) та 2 PC (отримують статичні IP) до WR-A1
10	Додати 3 Laptop (отримують статичні IP) до Wi-Fi роутера WR-A1 та 1 PC (отримують статичні IP) до Wi-Fi роутера WR-B1
11	Додати Wi-Fi роутер WR-C1 та WR-D1 (з'єднання бездротове) до точки доступу AP-PT, 2 Laptop (отримують статичні IP) один до WR-C1 та другий до WR-D1 роутера, 2 PC (отримують статичні IP) один до WR-A1 та другий до WR-B2 роутера
12	Додати Wi-Fi роутер WR-C1 (з'єднання бездротове) до точки доступу AP-PT, 1 Laptop та 1 PC (отримують статичні IP) до нового роутера, 1 PC (отримують статичні IP) до WR-A1 та 1 PC (отримують статичні IP) до WR-B1
13	Додати Wi-Fi роутер WR-D1 (з'єднання бездротове) до точки доступу AP-PT, 2 Laptop та 1 PC (отримують статичні IP) до нового роутера
14	Додати Wi-Fi роутер WR-D1 (з'єднання бездротове) до точки доступу AP-PT, 1 PC (отримують статичні IP) до нового роутера, 1 Laptop (отримують статичні IP) до WR-A1 та 1 PC (отримують статичні IP) до WR-B1
15	Додати Wi-Fi роутер WR-C1 (з'єднання бездротове) до точки доступу AP-PT, 2 Laptop (отримують статичні IP) до нового роутера
16	Додати 2 PC (отримують статичні IP) до Wi-Fi роутера WR-A1 та 2 Laptop (отримують статичні IP) до Wi-Fi роутера WR-B1

Продовження таблиці 1.2

17	Додати Wi-Fi роутер WR-C1 (з'єднання бездротове) до точки доступу AP-PT, 2 Laptop до нового роутера (отримують статичні IP) та 1 PC (отримують статичні IP) до WR-B1
18	Додати Wi-Fi роутер WR-C1 та WR-D1 (з'єднання бездротове) до точки доступу AP-PT, 1 Laptop (отримують статичні IP) до WR-C1 та 1 PC (отримують статичні IP) до WR-D, 1 PC (отримують статичні IP) до WR-B1
19	Додати Wi-Fi роутер WR-C1 (з'єднання бездротове) до точки доступу AP-PT, 2 PC до нового роутера (отримують статичні IP) та 2 Laptop (отримують статичні IP) до WR-A1
20	Додати Wi-Fi роутер WR-C1 та WR-D1 (з'єднання бездротове) до точки доступу AP-PT, 1 Laptop (отримують статичні IP) до WR-C1 та 3 PC (отримують статичні IP) до WR-D1

1.5 Зміст письмового звіту

- етапи створення мосту типу "точка–точка";
- відповіді на контрольні питання.

1.6 Контрольні питання

1. Принципи налаштування розподіленої бездротової системи.
2. Топології організації бездротових мереж в режимі WDS.

2 ЛАБОРАТОРНА РОБОТА.

Моделювання безпечної бездротової мережі

Мета: ознайомитись із основними способами побудови бездротових сегментів мережі із урахуванням вимог безпеки.

2.1 Загальні відомості

Бездротовий сегмент мережі завжди має додаткову небезпеку, вимагаючи більшої уваги при установці і налаштування. При налаштування захисту бездротової мережі зазвичай розглядаються декілька методів: зміна пароля адміністратора; відключення трансляції SSID мережі; фільтрація за MAC-адресами; шифрування даних; зниження потужності передавача.

Пристрої випускаються із стандартними (однаковими для всіх подібних пристроїв) паролями. У одному з вікон налаштування користувач повинен ввести новий пароль. Якщо налаштування пристрою забезпечено спеціальним майстром, то зміна пароля є одним з перших пунктів в його роботі.

У нормальному режимі точка доступу повідомляє свій мережевий ідентифікатор (SSID), щоб полегшити пошук і підключення до бездротової мережі. Це повідомлення є широкомовним, його можуть отримати не тільки комп'ютери вашої мережі, але і сторонні, які знаходяться в її зоні дії. У багатьох випадках немає ніякої необхідності демонструвати свою бездротову мережу всім бажаним, тому цей режим можна відключити. Всі пристрої мають встановлений за умовчанням SSID мережі. Якщо змінити SSID і одночасно з цим відключити його трансляцію, то підключитися до мережі зможе тільки той, хто заздалегідь знає SSID.

Якщо створюється та налаштовується невелика бездротова мережа вдома або в офісі, то, як правило, не часто виникає необхідність підключати додаткові комп'ютери. В цьому випадку можливо використовувати фільтрацію за MAC-адресами. Цей режим дозволить підключатися до мережі тільки відомим пристроям з їх унікальними MAC-адресами. Як і паролі, адреси, дозволених для даної мережі MAC-адрес, слід зберігати таємно від сторонніх осіб. Фільтрація за MAC-адресами не може забезпечити стовідсотковий захист. Вона розглядається як один із заходів по забезпеченню безпечної роботи.

Щоб захистити дані під час передачі від одного мережевого пристрою до другого, використовується шифрування даних. При шифруванні даних необхідно на кожному з пристроїв налаштувати протокол шифрування і ключі. Основні типи шифрування:

- WEP-шифрування. Перший та найбільш простий спосіб шифрування - використання протоколу WEP (Wired Equivalence Privacy). На практиці цей метод шифрування вже не є дуже надійним. Використання недостатньо довгих ключів дозволяє дешифрувати повідомлення. При використанні WEP-шифрування необхідно, щоб на всіх підключених точках застосовувались ідентичні ключі. Чим довше ключ, тим складніше дешифрувати повідомлення. Сучасне бездротове устаткування використовує 64-бітні, 128-бітні та 256-бітні ключі. У сучасному мережевому устаткуванні може задаватися до чотирьох ключів WEP. За згодою з клієнтами один з них вибирається в якості активного ключа і використовується для шифрування. Періодично (наприклад, раз на тиждень) можна змінювати активний ключ. Ключі задаються ідентичним способом на всіх пристроях бездротової мережі;

- WPA-шифрування. У пристроях стандарту 802.11g підтримується поліпшений алгоритм шифрування WPA (Wi-Fi Protected Access). Цей стандарт об'єднує два методи: TKIP і MIC. Протокол TKIP (Temporal Key Integrity Protocol) - це реалізація динамічних ключів шифрування. Ключі шифрування мають довжину 128 біт і генеруються при посиланні кожних 10 Кбайт даних за складним алгоритмом. При цьому загальна кількість можливих варіантів ключів обчислюється сотнями мільярдів. Така система дає найвищі гарантії надійності шифрування даних. Протокол MIC (Message Integrity Check) – є протоколом перевірки цілісності пакетів. При його використанні порівнюються відправлені і отримані дані. Це виключає внесення в них змін при передачі. Протокол дозволяє відкидати пакети, які додані в канал третьою особою. Таким чином, хакер не може вбудувати шкідливі коди до даних під час їх передачі.

Для передачі даних в радіоефір кожен бездротовий пристрій забезпечено приймачем і передавачем радіохвиль. Від його потужності залежить радіус дії бездротової мережі, а від чутливості - якість прийому сигналу. Непоганим варіантом захисту мережі є підбір такої потужності передавача, якої достатньо для покриття тільки ваших пристроїв мережі. Цим ви відсікаєте тих, хто може налаштуватися на вашу мережу (з сусіднього будинку або з машини на стоянці). Не

потрібно відразу встановлювати дуже низьку потужність, оскільки цим можна «відключити» зв'язок з віддаленими комп'ютерами. Зменшуйте потужність поступово, але не встановлюйте ту, на якій спостерігається порогова робота пристрою (в певних умовах сигнал може ще більше послабитись), це може привести до відключення віддалених комп'ютерів. Визначити зону покриття бездротової мережі в умовах реального приміщення можна за допомогою ноутбука або іншого пристрою із встановленою програмою Network Stumbler (або WirelessMon). Network Stumbler надає інформацію про MAC-адреси виявлених бездротових пристроїв, значення SSID, імена пристроїв, канали та чи включено шифрування і т.п. Network Stumbler допоможе визначити, чи вірно налаштована бездротова мережа і знайти місця з недостатнім радіопокриттям, встановити наявність і характеристики інших мереж, які можуть заважати роботі вашої мережі.

Якщо точка доступу або маршрутизатор дозволяє налаштовувати даний пристрій по дротовому підключенню при відключенні бездротового налаштування, то доцільно застосувати цей метод. Налаштування точки доступу через Wi-Fi відключається для того, щоб хакер не міг підключитися до неї, навіть знаючи пароль адміністратора. При підключенні по бездротовій мережі до Інтернету за допомогою маршрутизатора можна використовувати його вбудовані засоби захисту. Зазвичай маршрутизатори мають вбудований брандмауер (firewall). Налаштування його параметрів не дуже складне, і не слід їм нехтувати, оскільки в цьому випадку від загроз проникнення хакерів з Інтернету може бути захищена вся мережа.

2.2 Захист комп'ютера

Рекомендації із налаштування захисту бездротової мережі реалізуємо для моделі мережі, наведеної на рисунку 1.1. Для цього виконайте наступні дії:

- 1) з панелі приладів в робочу область перенесіть маршрутизатор 2811 (або будь який із підтримкою Fast Ethernet та вільними слотами) (для зручності краще перейменувати його у R-1);

- 2) в робочу область перенесіть комутатори 2950-24 (для зручності краще перейменувати його у S-1);

3) в робочу область перенесіть 3 робочі станції PC-PT та 2 ноутбука Laptop (для зручності краще перейменувати їх у PC-B1, PC-B2, PC-A1 та L-A2, L-A3);

4) в робочу область перенесіть 1 сервер Server-PT (для зручності краще перейменувати його SRV-1).

5) в робочу область перенесіть 1 Wi-Fi router Lynksys-WRT300N (для зручності краще перейменувати його WR-1).

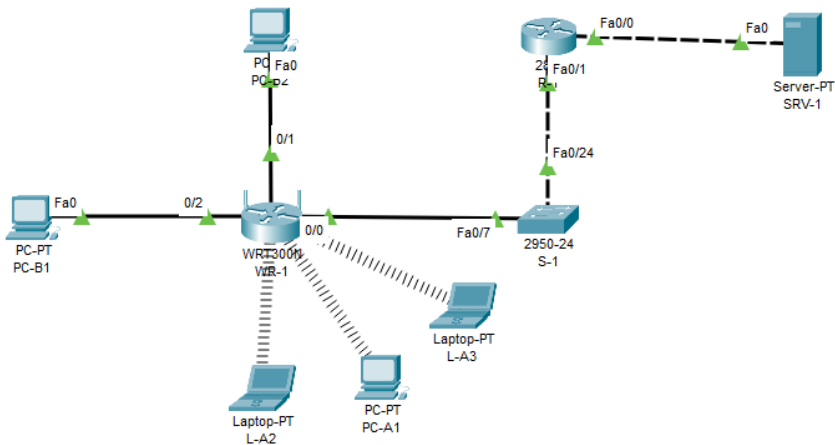


Рисунок 1.1 – Модель мережі

Таблиця 1.1 – Параметри інтерфейсів

	Device (Hostname)	IP address	Default Gateway	DNS
R-1	FEth0/0 (0/0/0)	192.168.0.1\24	-	-
	FEth0/1 (0/0/1)	10.0.0.1\24	-	-
	SRV-1	192.168.0.2\24	192.168.0.1	192.168.0.2

Для установки маршрутизаторів на панелі приладів необхідно вибрати перший елемент – Routers (рис.1.2). З показаних пристроїв треба вибрати 2811 (підкреслений) (або будь який із підтримкою Fast Ethernet та вільними слотами) і перетягти у робочу область.

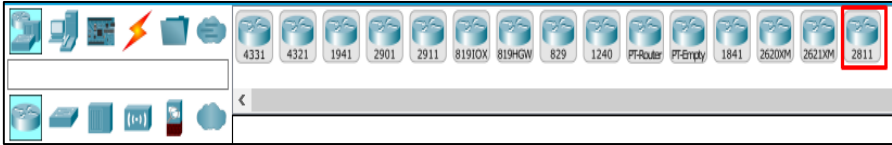


Рисунок 1.2 – Вибір маршрутизаторів

Для установки комутаторів перейдіть на закладку Switches (рис.1.3) і перетягніть 2950-24(підкреслений) елемент у робочу область.

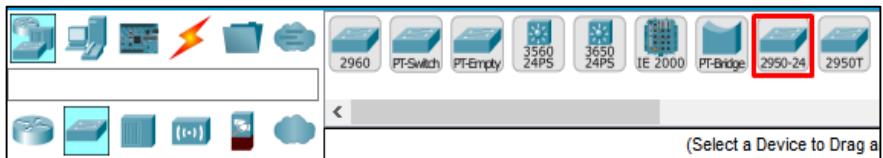


Рисунок 1.3 – Вибір комутаторів

Наступним кроком є з'єднання між собою елементів мережі. Для усіх з'єднань будемо використовувати кабель вита пара (рис. 1.4).

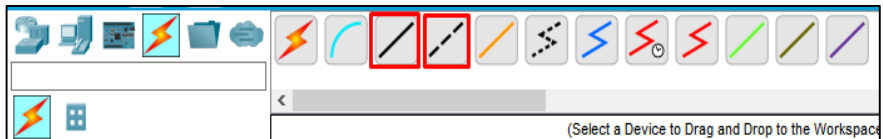


Рисунок 1.4 – Вибір типу з'єднання елементів мережі

Для установки бездротового маршрутизатора з Wireless Devices (рис.1.5) перетягніть WRT300n (підкреслений) у робочу область.

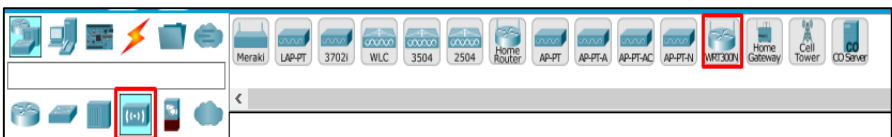


Рисунок 1.5 – Вибір Wi-Fi маршрутизатора

Для того, щоб з'єднати 2 інтерфейси різних пристроїв виконайте наступне:

- виберіть відповідний кабель, після чого покажчик миші зміниться;
- далі клікнути лівою кнопкою по першому пристрою, який ви хочете підключити;
- у спливаючому вікні клікніть по порту, до якого підключаєте кабель;
- задайте кінцеву точку підключення кабелю: виберіть наступний пристрій і аналогічно підключіть порт (рис. 1.6).

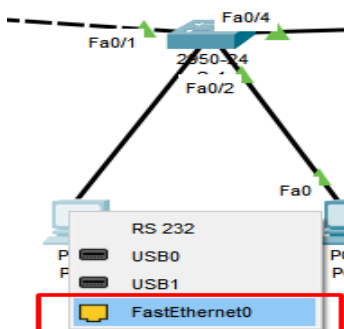


Рисунок 1.6 – Підключення кабелю

Для спрощення налаштувань необхідно кабель підключати на ті порти, які вказані у таблиці 1.1.

2.3 Конфігурування обладнання мережі

Відкрити налаштування Wi-Fi router Linksys-WRT300N та перейти у вкладку «GUI» (рис. 1.7). Здійснити наступні налаштування:

Internet setup:

Static IP;

Internet IP - 10.0.0.4

Subnet mask - 255.255.255.0;

Default gateway - 10.0.0.1

DNS1 - 192.168.0.2

Network setup (локальні мережеві інтерфейси):

Router IP-1 - 172.16.0.1/24;

DHCP Server – Enabled;

Start IP - 172.16.0.2;

Max number users - 5;

Static DNS - 192.168.0.2

(Після введення параметрів **ОБОВ'ЯЗКОВО** натиснути **SAVE SETTINGS**). У Wireless змінити SSID на cisco_network (рис. 1.8).

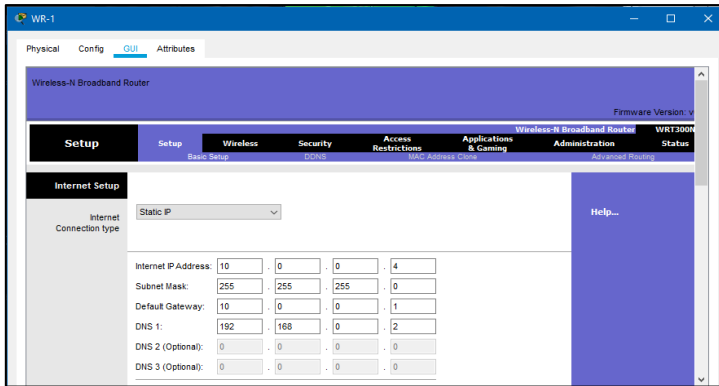


Рисунок 1.7 – Налаштування Linksys-WRT300N

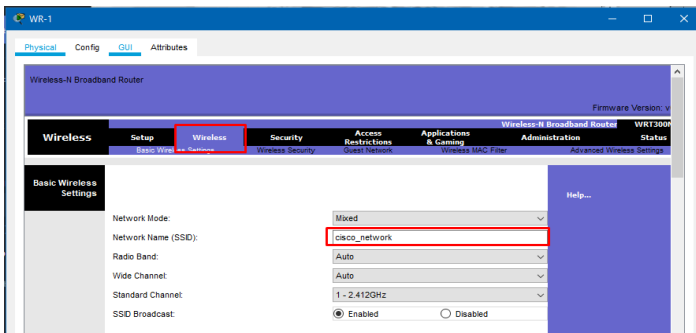


Рисунок 1.8 – Налаштування SSID

Налаштуйте для всіх PC та Laptop з'єднання по бездротовій мережі. Відкрийте налаштування PC або Laptop, вимикаємо пристрій,

беремо модуль з портом Ethernet та на його місце з лівої панелі монтуємо модуль Linksys-WMP300N до нашого пристрою (рис. 1.9-1.10). Після цього треба не забути ввімкнути пристрій.

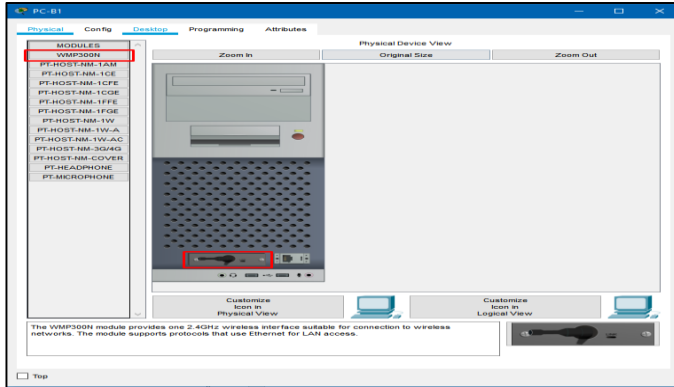


Рисунок 1.9 – Додавання бездротового обладнання PC

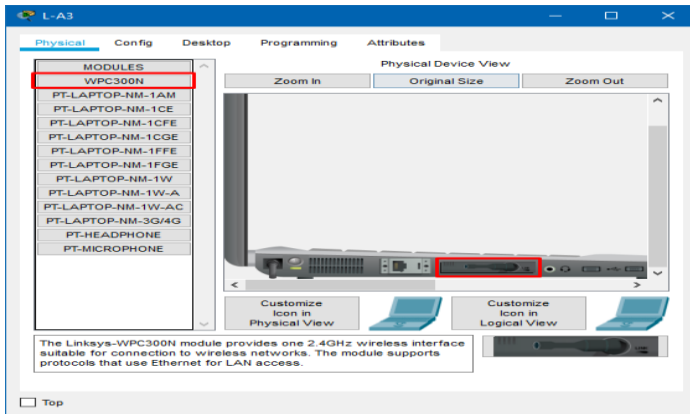


Рисунок 1.10 – Додавання бездротового обладнання Laptop

Налаштуйте PC та Laptop для з'єднання Wi-Fi router Linksys-WRT300N. Відкрити налаштування WR-1 та перейти у вкладку «GUI» та натиснути на кнопку «DHCP Reservation». Потім потрібно ввести «ім'я», «IP-address» та «Mac Address» PC або Laptop (рис. 1.11).

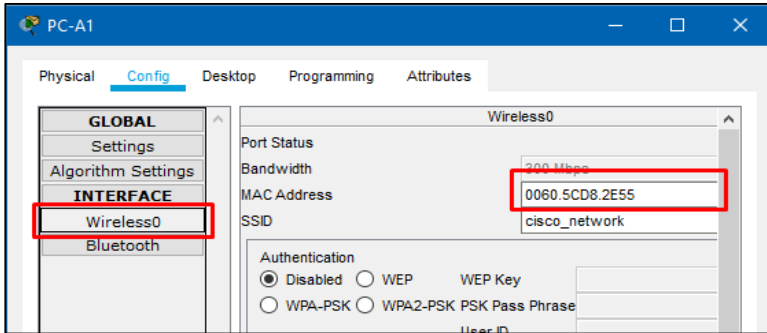


Рисунок 1.11 – Mac Address PC

Після введення параметрів обов'язково натиснути «SAVE SETTINGS». Для того щоб дізнатися «Mac Address» PC або Laptop потрібно відкрити вкладку «Config» та перейти в «Wireless» (рис. 1.12).

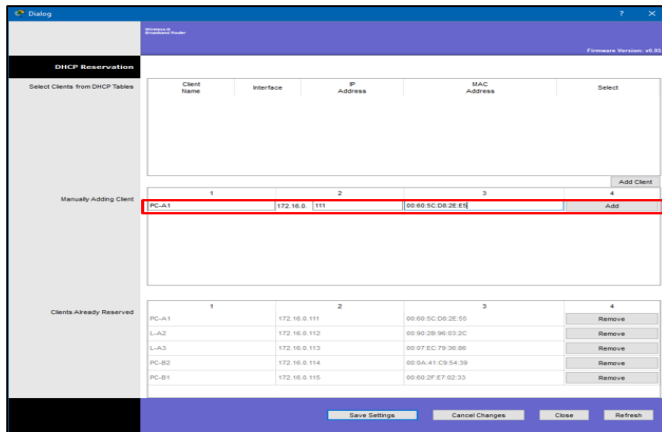


Рисунок 1.12 – DHCP Reservation

Для налаштування безпеки бездротового зв'язку потрібно:

- вибрати Wireless > Wireless Security. змініть режим захисту на WPA2 Personal. На даний момент AES є найсильнішим доступним протоколом шифрування. Залиште це вибраним (рис. 1.13);

– ввести парольну фразу наприклад «aCompWiFi» та прокрутити сторінку вниз і натиснути «Save Settings».

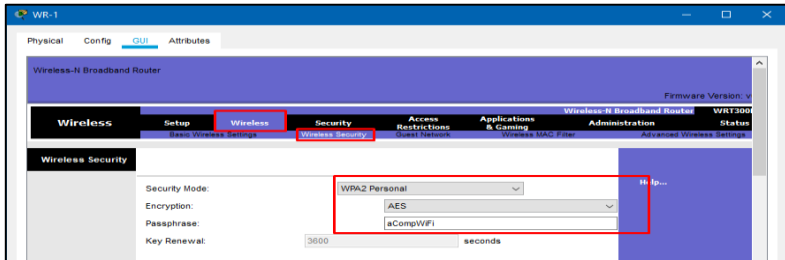


Рисунок 1.13 – Налаштування безпеки Wi-Fi

Далі необхідно перейти у вкладку Desktop і відкрити PC Wireless. Перейти у вкладку Connect, натиснути кнопку Refresh підключитися до мережі «cicso_network» та ввести пароль (рис. 1.14).

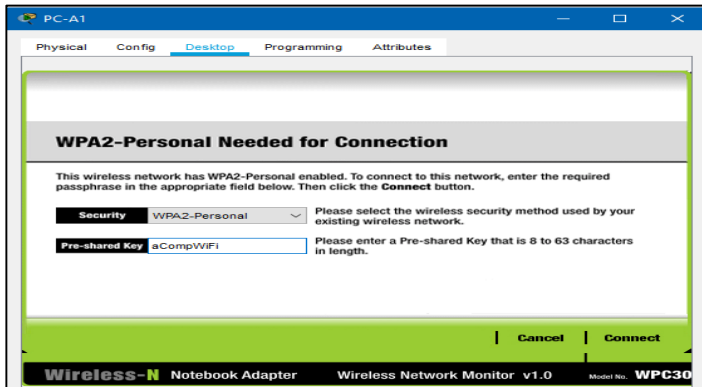


Рисунок 1.14 – Підключення до мережі Wi-Fi

Для пристроїв, які з'єднанні кабелем, потрібно в конфігуруванні вибрати параметр DHCP (рис. 1.15).

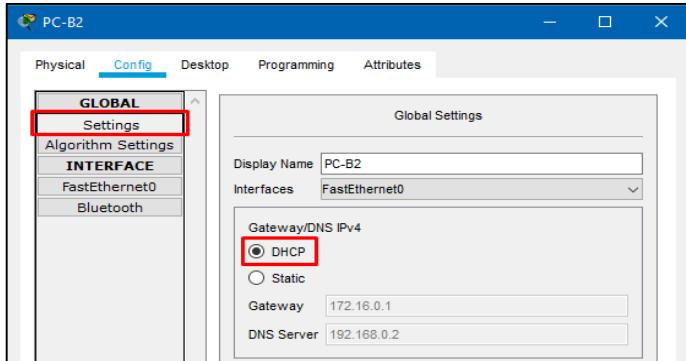


Рисунок 1.15 – Налаштування по DHCP

Далі переходимо до налаштування маршрутизатору R-1 (2811 або той, що обрано). Даний пристрій конфігуруємо через CLI інтерфейс (рис. 1.16). Для цього необхідно по чергово вводити команди у терміналі (після кожної команди натискати ENTER):

```
Router>enable
Router#configure terminal (config t)
(Enter configuration commands, one per line. End with CNTL/Z.)
Router(config)#interface FastEthernet 0/0
Router(config-subif)#ip address 192.168.0.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface FastEthernet 0/1
Router(config-subif)#ip address 10.0.0.1 255.255.255.0
Router(config-subif)#exit
Router(config)#router eigrp 100
Router(config-subif)#network 192.168.0.0
Router(config-subif)#network 10.0.0.0
Router(config-subif)#network 172.16.0.0
Router(config-subif)#exit
Router(config)#ip route 192.168.0.0 255.255.255.0
FastEthernet0/0
Router(config)#ip route 10.0.0.0 255.255.255.0 FastEthernet0/1
Router(config)#ip route 172.16.0.0 255.255.255.0 FastEthernet0/1
Router(config)#exit
Router(config)#write memory
```

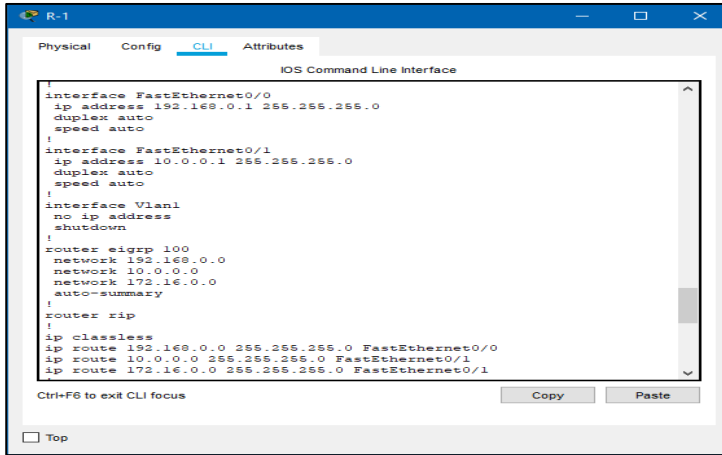


Рисунок 1.16 – CLI інтерфейс маршрутизатора

Далі перевірте з'єднання всіх пристроїв в мережі та зробить відповідні висновки. Прослідкуйте, які протоколи працюють при обміні інформацією та що змінюється у структурі даних під час проходженні кадрів та пакетів через різні пристрої мережі (за допомогою режиму Simulation).

2.4 Індивідуальне завдання

Доповніть мережу, додавши до пристрою вказаного в таблиці 2.2, додаткове обладнання згідно варіанту. IP адреса залежить від номера студента в групі, наприклад студент під номером 6 задає таку адресу:

PC-C1 -> 192.168.(6).1;

PC-C2 -> 192.168.(6+1).1.

Таблиця 2.2 – Варіанти до самостійної роботи

1	Додати Wi-Fi роутер WR-2 (з'єднання за кабелем) до комутатора, 2 PC до нового роутера (1 отримує динамічний IP через DHCP та 1 отримує статичний IP за MAC)
2	Додати 2 Wi-Fi роутер WR-2(3) (з'єднання за кабелем) до комутатора, 2 PC до WR-2 (отримує статичний IP за MAC), 2 Laptop до WR-3 (отримує динамічний IP за DHCP)

Продовження таблиці 2.2

3	Додати 2 Wi-Fi роутер WR-2(3) (з'єднання за кабелем) до комутатора, 2 PC до WR-2 (1 отримує динамічний IP через DHCP та 1 отримує статичний IP за MAC), 2 PC до WR-3 (1 отримує динамічний IP через DHCP та 1 отримує статичний IP за MAC)
4	Додати Wi-Fi роутер WR-2 (з'єднання за кабелем) до комутатора, 3 PC до нового роутера (1 отримує динамічний IP через DHCP за кабелем, 1 отримує динамічний IP через DHCP через Wi-Fi та 1 отримує статичний IP за MAC)
5	Додати Wi-Fi роутер WR-2 (з'єднання за кабелем) до комутатора, 4 PC до нового роутера (2 отримують динамічні IP через DHCP за кабелем, 2 отримують динамічні IP через DHCP через Wi-Fi)
6	Додати Wi-Fi роутер WR-2 (з'єднання за кабелем) до комутатора, 4 PC до нового роутера (2 отримують динамічні IP через DHCP за кабелем, 2 отримують статичні IP за MAC за Wi-Fi)
7	Додати 2 Laptop (отримують статичні IP), 2 PC (1 отримує динамічний IP через DHCP та 1 отримує статичний IP за MAC) до Wi-Fi роутера WR-1
8	Додати Wi-Fi роутер WR-2 (з'єднання за кабелем) до комутатора, 4 PC до нового роутера (1 отримує динамічний IP через DHCP та 1 отримує статичний IP за MAC, 2 отримують статичні IP)
9	Додати 2 Wi-Fi роутер WR-2(3) (з'єднання за кабелем) до комутатора, 2 Laptop до WR-2 (1 отримує динамічний IP через DHCP та 1 отримує статичний IP за MAC), 2 Laptop до WR-3 (отримують статичні IP)
10	Додати Wi-Fi роутер WR-2 (з'єднання за кабелем) до комутатора, 3 PC до нового роутера (1 отримує статичний IP за кабелем, 1 отримує динамічний IP через DHCP через Wi-Fi та 1 отримує статичний IP за MAC)
11	Додати Wi-Fi роутер WR-2 (з'єднання за кабелем) до комутатора, 2 PC до нового роутера (1 отримує динамічний IP через DHCP та 1 отримує статичний IP за MAC), 1 Laptop (отримує статичний IP)
12	Додати 2 Wi-Fi роутер WR-2(3) (з'єднання за кабелем) до комутатора, 3 PC до WR-2 (1 отримує динамічний IP через DHCP та 2 отримують статичні IP через MAC), 3 PC до WR-3 (2 отримують динамічні IP через DHCP та 1 отримує статичний IP за MAC)
13	Додати 2 Wi-Fi роутер WR-2(3) (з'єднання за кабелем) до комутатора, 2 PC до WR-2 (отримують динамічні IP через DHCP), 2 Laptop до WR-3 (2 отримують статичні IP за MAC)
14	Додати Wi-Fi роутер WR-2 (з'єднання за кабелем) до комутатора, 2 PC до нового роутера (з'єднання DHCP, MAC), 1 Laptop (з'єднання кабелем)

Продовження таблиці 2.2

15	Додати Wi-Fi роутер WR-2 (з'єднання за кабелем) до комутатора, 2 Laptop до нового роутера (1 отримує динамічний IP через DHCP та 1 отримує статичний IP за MAC), 1 PC (отримує статичний IP)
16	Додати Wi-Fi роутер WR-2 (з'єднання за кабелем) до комутатора, 4 PC до нового роутера (2 отримують динамічні IP через DHCP та 2 отримують статичні IP за MAC)
17	Додати Wi-Fi роутер WR-2 (з'єднання за кабелем) до комутатора, 4 Laptop до нового роутера (1 отримує динамічний IP через DHCP за кабелем, 1 отримує динамічний IP через DHCP через Wi-Fi, 1 отримує статичний IP за MAC за кабелем та 1 отримує статичний IP за MAC через Wi-Fi)
18	Додати 2 PC (отримують статичні IP), 2 Laptop (1 отримує динамічний IP через DHCP та 1 отримує статичний IP за MAC) до Wi-Fi роутера WR-1
19	Додати 2 Wi-Fi роутер WR-2(3) (з'єднання за кабелем) до комутатора, 2 PC до WR-2 (отримують статичні IP за MAC), 2 PC до WR-3 (отримують динамічні IP через DHCP)
20	Додати Wi-Fi роутер WR-2 (з'єднання за кабелем) до комутатора, 4 PC до нового роутера (2 отримують статичні IP за MAC та 2 отримують динамічні IP через DHCP)

2.5 Зміст письмового звіту

- хід роботи та етапи налаштування точки доступу з підтримки бездротових сегментів мережі з урахуванням вимог безпеки;
- відповіді на контрольні питання.

2.6 Контрольні питання

1. Які заходи безпеки слід здійснити при налаштування захисту бездротової мережі?
2. Які протоколи шифрування даних застосовуються в бездротових мережах?
3. Які режими є у WPA-шифрування?
4. За допомогою яких програм можна досліджувати зону покриття бездротової мережі в умовах реального приміщення?
5. За допомогою яких програмних засобів можна настроїти параметри точки доступу?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Шапорін Р.О. Моделі та методи проектування комунікаційних систем комп'ютерних мереж масштабу підприємства [Текст]: автореф. дис... канд. техн. наук: 05.13.12 / Р.О.Шапорін ; Одеський національний політехнічний ун-т. - О., 2007. - 22 с.
2. Santitoro, R. Metro Ethernet Services—A Technical Overview. In Metro Ethernet Forum (Vol. 2006). 2003.
3. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide / D. Hucaby. – 2nd Edition. – USA: Cisco Press, 2015. – 578 p.
4. Киричек Г. Г. Курсовий проект для бакалаврів з проектування комп'ютерних мереж. Запоріжжя: Національний університет «Запорізька політехніка», 2020.
5. Odom, W. Cisco CCENT/CCNA ICND1 100-101. Indianapolis: Cisco Press. 2013.
6. Odom, W. CCNA Routing and Switching ICND2 200-101 Official Cert Guide. Cisco Press. 2013.
7. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 1. Навчальний посібник. 2020.
8. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 2. Навчальний посібник. 2020.
9. Odom, W. CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. 2019.
10. Odom, W. CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press. 2019.
11. Блозва А.І.. Комп'ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька. К.: Компрінт, 2017.