Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ З НАВЧАЛЬНИХ ДИСЦИПЛІН “Системи електронних комунікацій”, “Спеціальні системи електронних комунікацій”

Лабораторний практикум

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів першого (бакалаврського) рівня освіти за освітніми програмами «Безпека державних інформаційних ресурсів» спеціальності 125 Кібербезпека та захист інформації та «Комп’ютерні системи і технології спеціального зв’язку» спеціальності 122 Комп’ютерні науки

Укладачі: Д.І. Могилевич, Р.Ю. Сбоєв, М.С. Ірха

Електронне мережеве навчальне видання

Київ
КПІ ім. Ігоря Сікорського
2024

УДК 621.39
М74

Укладачі: Могилевич Дмитро Ісакович
Сбоєв Роман Юрійович
Ірха Максим Сергійович

Рецензент *Кононова І.В.*, кандидат технічних наук, доцент
завідувач Спеціальної кафедри № 4 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"

Відповідальний редактор *Погребняк Л.М.,* кандидат технічних наук.

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол № 6 від 10.04.2025 р.)
за поданням вченої ради ІСЗЗІ КПІ ім. Ігоря Сікорського
(протокол № 5 від 26.12.2024 р.)

М74 Методичні рекомендації до виконання лабораторних робіт із навчальних дисциплін "Системи електронних комунікацій", "Спеціальні системи електронних комунікацій", [Електронний ресурс] : лаб. практикум : навч. посіб. для здобувачів першого (бакалаврського) рівня освіти за освіт. програмою «Безпека державних інформаційних ресурсів» спец. 125 Кібербезпека та захист інформації, «Комп'ютерні системи і технології спеціального зв'язку» спец. 122 Комп'ютерні науки / КПІ ім. Ігоря Сікорського ; уклад.: Д. І. Могилевич, Р. Ю. Сбоєв, М. С. Ірха. Електрон. текст. дані (1 файл). Київ : КПІ ім. Ігоря Сікорського, 2024. 110 с.

Методичні рекомендації призначені для здобувачів вищої освіти ступеня "бакалавр", які вивчають навчальні дисципліни "Системи електронних комунікацій", "Спеціальні системи електронних комунікацій". Вони складені відповідно до освітньо-професійних програм підготовки здобувачів вищої освіти бакалавр за спеціальностями 125 Кібербезпека та захист інформації, 122 Комп'ютерні науки. Методичні рекомендації призначені для використання на лабораторних заняттях, практичних заняттях і при самостійній роботі.

УДК 621.39

Реєстр. № НП 24/25-418. Обсяг 4,9 авт. арк.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Берестейський, 37, м. Київ, 03056
https://kpi.ua
Свідоцтво про внесення до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

CHR (Cloud Hosted Router) – маршрутизатор для хмарних рішень;

CLI (Command Line Interface) – інтерфейс командного рядка;

CPS (Customer Programming Software) – клієнтське програмувальне забезпечення;

DHCP (Dynamic Host Configuration Protocol) – протокол динамічного налаштування вузла;

LAN (Local Area Network) – локальна мережа;

MAC (Media Access Control) – контроль доступу до середовища;

MNDP (Mikrotik Neighbor Discovery Protocol) – протокол виявлення сусідів від MikroTik;

NAT (Network Address Translation) – трансляція мережевих адрес;

ROS (Router Operation System) – операційна система маршрутизатора;

SIP (Session Initiation Protocol) – протокол ініціації сесії;

SSID (Service Set Identifier) – унікальне найменування бездротової мереж;

WAN (Wide Area Network) – глобальна мережа;

АТС – автоматична телефонна станція;

ВМ – віртуальна машина;

ПК – персональний комп’ютер;

РС – радіостанція;

СРШ – станція радіорелейна широкосмугова.

ЛАБОРАТОРНА РОБОТА №1
ПІДКЛЮЧЕННЯ ДО МАРШРУТИЗАТОРА MIKROTIK

Мета:

1) ознайомити користувача з інтерфейсом програми Winbox;

2) навчитися підключати пристрої MikroTik до персонального комп'ютера для подальшого налаштування.

Теоретичні відомості

Налаштування маршрутизатора MikroTik можливе декількома основними способами:

- За допомогою графічого інтерфейсу (GUI) – через утиліту **Winbox**, через браузер ПК (WebBox).
- За допомогою командного рядка (CLI) – Telnet, SSH, Serial консоль.
- За допомогою інтерфейсу програмування застосунків (API) – для програмування утиліт.

Набільш поширеним і зручним є використання утиліти WinBox.

Winbox – це невелика утиліта, яка дозволяє адмініструвати MikroTik RouterOS за допомогою швидкого та простого графічного інтерфейсу. Це двійковий файл Win32 (зроблено під OS Windows), але його можна запускати в Linux і MacOS (OSX) за допомогою емулятора Wine. Усі функції інтерфейсу Winbox максимально віддзеркалюють функції консолі. Деякі розширені та критичні для системи налаштування неможливі з Winbox, наприклад зміна MAC-адреси в журналі змін інтерфейсу Winbox.

Починаючи з Winbox версії 3.14, використовуються такі функції безпеки:

- Winbox.exe підписаний сертифікатом розширеної перевірки, виданим SIA Mikrotikls (MikroTik).
- Обидві сторони перевіряють, чи знає інша сторона пароль (неможлива атака посередині (**man in the middle**).
- Winbox у режимі RoMON вимагає, щоб агент мав останню версію (для можливості підключатися до маршрутизаторів останньої версії).
- Winbox використовує AES128-CBC-SHA як алгоритм шифрування (потрібна версія Winbox 3.14 або вище).

Winbox працює за логічним портом ***8291/tcp***. Для знаходження пристрою Winbox використовує протоколи **Neighbor Discovery**. RouterOS версії до 6.38 працює на різних рівнях моделі OSI і містить у собі два шляхи оголошення та отримання інформації: на рівні L4 працює транспорт UDP, на рівні L2 інформацію приймає та передає протокол сімейства MNDP/VDP/CDP. Отримана з обох джерел інформація об'єднується та відображається у списку виявлених сусідів **"/ip neighbors"**.

У версію 6.38 вже додана підтримка відкритого протоколу LLDP. Тепер у списку сусідів відображається і будь-яке LLDP-сумісне обладнання за умови, що до нього також додано підтримку оголошення LLDP.

Опис кнопок і полів екрана завантажувача Winbox в простому режимі:

Кнопки/прапорці:

- "**Connect**" – підключення до маршрутизатора.
- "**Connect To RoMON**" – підключитися до RoMON Agent.
- "**Add/set**" – зберегти/редагувати будь-які збережені записи маршрутизатора на вкладці "Managed".

- “**Open In New Window**” – залишає завантажувач відкритим у фоновому режимі та відкриває нові вікна для кожного пристрою, до якого встановлено підключення.

Поля:

- **“Connect To:”** – цільова IP- або MAC-адреса маршрутизатора.
- **“Login”** – ім'я користувача, яке використовується для аутентифікації.
- **“Password”** – пароль, який використовується для аутентифікації.
- **“Keep Password”** – якщо не позначено, пароль не буде збережено в списку.

Опис кнопок і полів екрана завантажувача Winbox в розширеному режимі:

Кнопки/прапорці:

- **“Browse”** – перегляд каталогу файлів для певного сеансу.
- **“Keep Password”** – якщо не позначено, пароль не буде збережено в списку.
- **“Secure Mode”** – якщо позначено, Winbox використовуватиме DH-1984 для обміну ключами та модифіковане q посилене шифрування RC4-drop3072 для захисту сеансу.
- **“Autosave session”** – автоматично зберігає сеанси для пристроїв, до яких встановлено підключення.

Поля:

- **“Session”** – збережений сеанс маршрутизатора.
- **“Note”** – примітка, яка призначена для збереження запису маршрутизатора.
- **“Group”** – група, якій призначено збережений запис маршрутизатора.

- **“RoMON Agent”** – Виберіть RoMON Agent зі списку доступних пристроїв.

Опис пунктів меню, що випадає на екрані завантажувача:

File:

- **“New”** – створити новий список керованих маршрутизаторів у вказаному місці.
- **“Open”** – відкрити файл списку керованих маршрутизаторів.
- **“Save as”** – зберегти поточний список керованих маршрутизаторів у файл.
- **“Exit”** – вихід із завантажувача Winbox.

Tools:

- **“Advanced Mode”** – вмикає/вимикає розширений режим перегляду.
- **“Import”** – імпортує збережений файл сеансу.
- **“Export”** – експорт збереженого файлу сеансу.
- **“Move Session Folder”** – змінити шлях, де зберігаються файли сеансу.
- **“Clear cache”** – очистити кеш Winbox.
- **“Check For Upda**tes” – перевірити наявність оновлень для завантажувача winbox.

Хід роботи

1. Перед початком роботи зберіть схему підключення за зразком (для початкового налаштування кабель від провайдера під’єднувати необов’язково), як на рисунку 1.1.

2. Winbox можна завантажити зі сторінки завантаження MikroTik. Перейдіть на сторінку https://mikrotik.com/download у вашому браузері та завантажте останню версію Winbox, як наведено на рисунку 1.2.

Краще обирайте версію, що за розрядністю відповідає вашому ПК. Але якщо ви завантажите 32-розрядну програму, вона також буде працювати на 64-розрядному ПК.

Рисунок 1.1. Схема підключення ПК до маршрутизатора

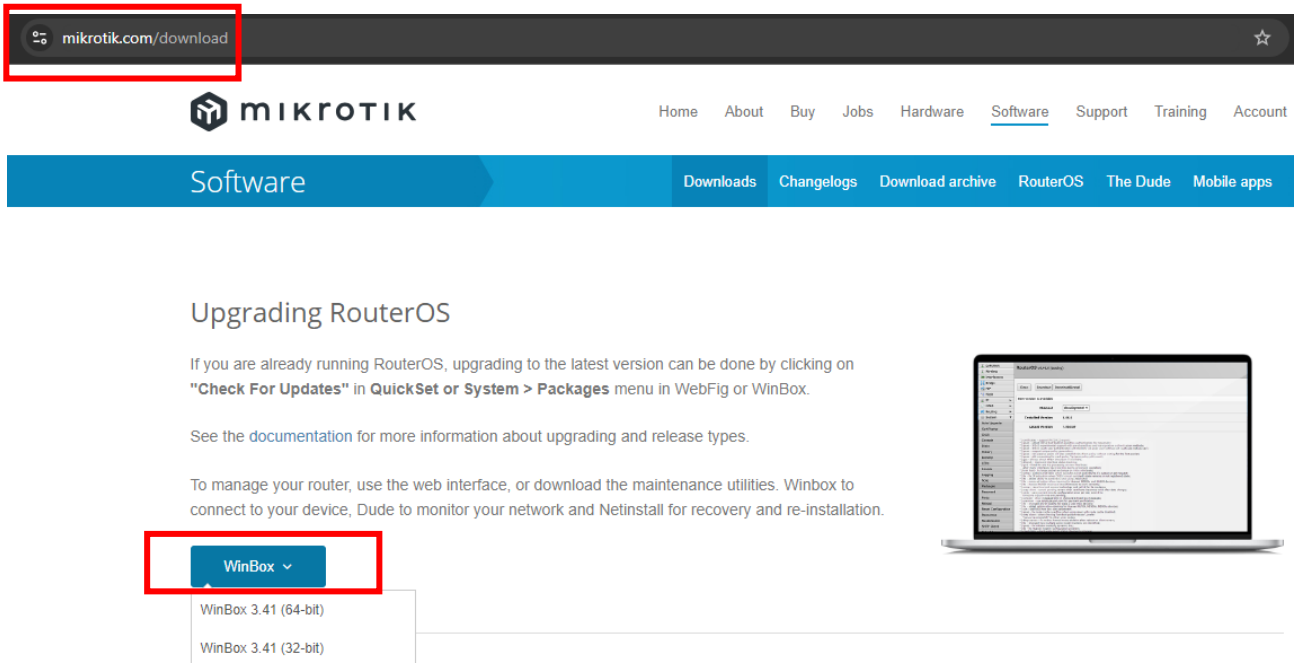

Рисунок 1.2. Сторінка завантаження Winbox

3. Коли файл winbox.exe буде завантажено, двічі клікніть його, і з’явиться вікно Winbox. Скористайтесь **“Neighbor Discovery”** (виявлення сусідів), щоб отримати список доступних маршрутизаторів на вкладці **“Neighbors”**, як на рисунку 1.3 (натисніть кнопку **“Refresh”**). Зробіть скріншот.

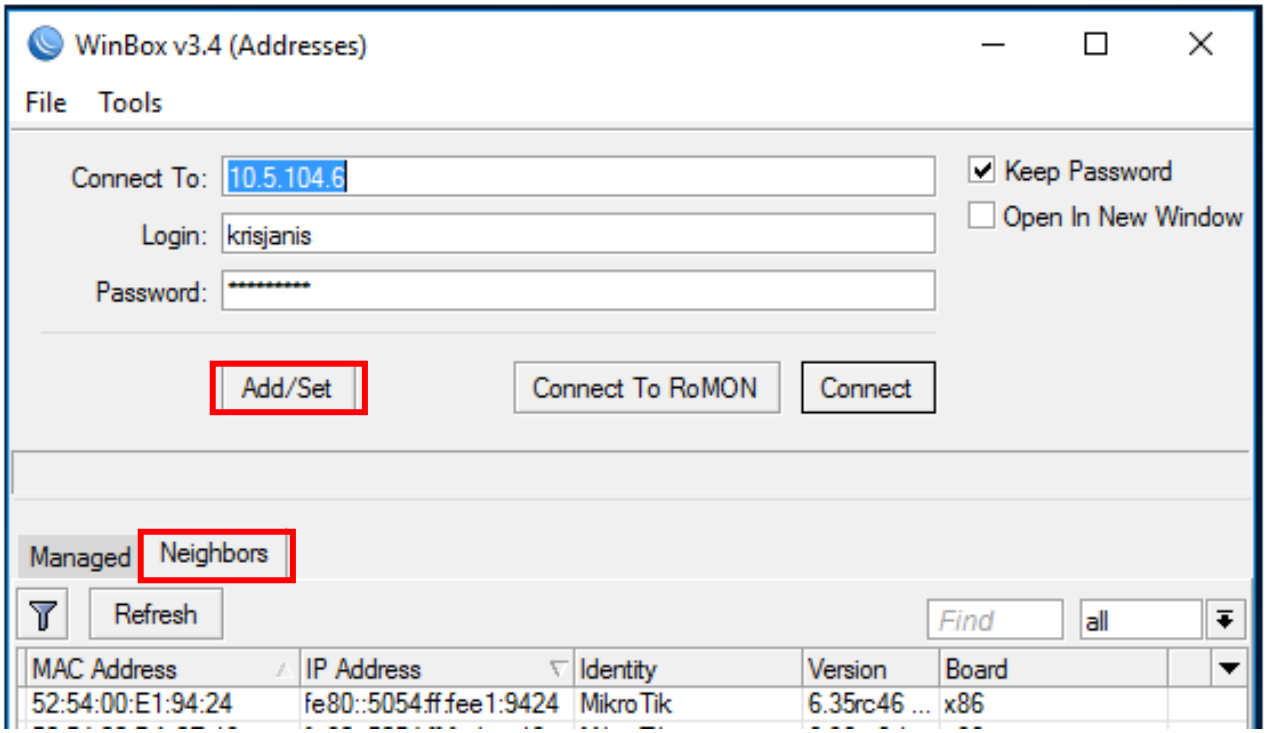

Рисунок 1.3. Пошук доступних пристроїв у winbox

Примітка. *Якщо у вас є фізичне підключення ПК до маршрутизатора, але в списку сусідів не відображається жодного пристрою, то в мережевих налаштуваннях ПК вимкніть всі мережеві з’єднання крім того, що наразі є активним і використовується для підключення маршрутизатора MikroTik.*

4. За замовчуванням ви перебуваєте в простому режимі **(“Simple Mode”)** Winbox, як на рисунку 1.4.

5. Щоб перейти до розширеного режиму, поставте галочку у випадаючому меню **“Tools”** навпроти рядка **“Advanced Mode”**, як наведено на рисунку 1.5.

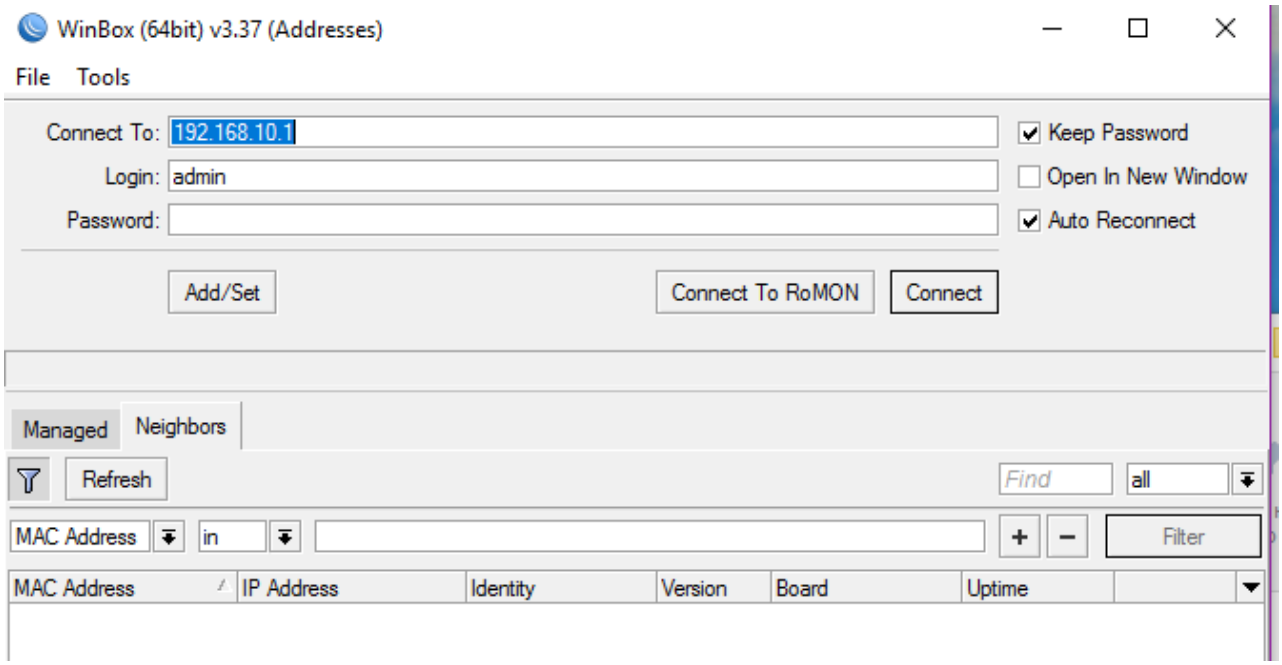

Рисунок 1.4. Простий режим вікна Winbox

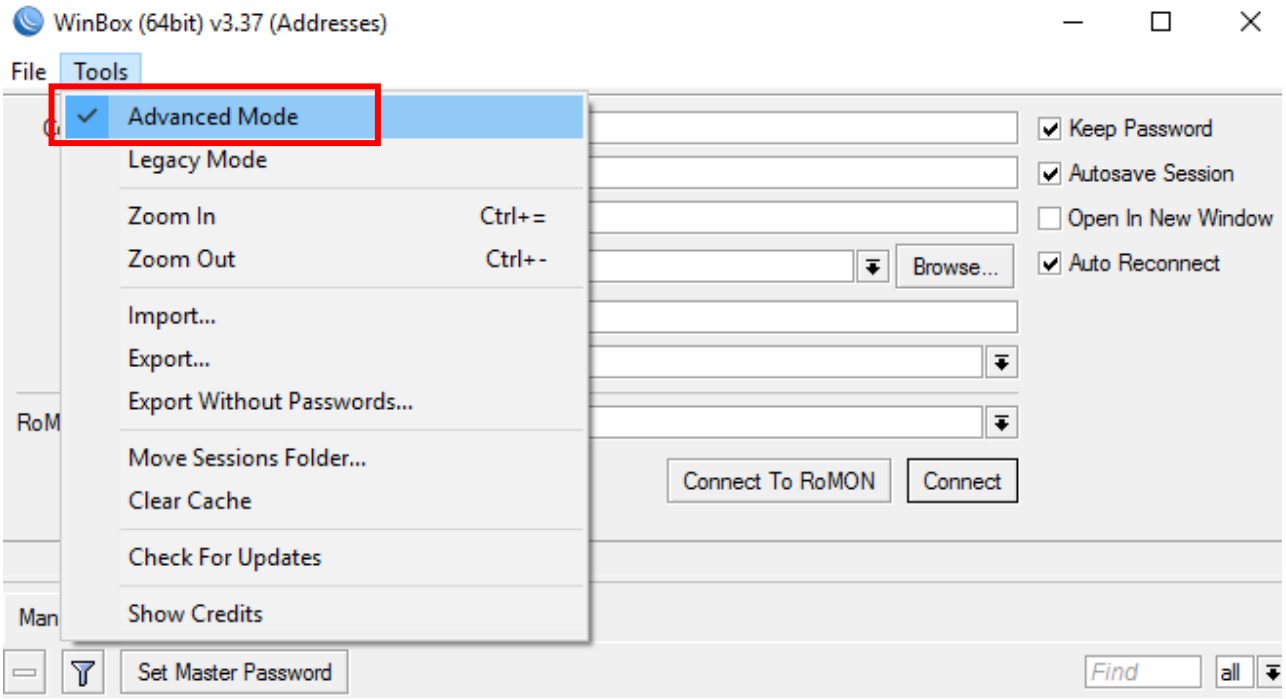

Рисунок 1.5. Перехід до розширеного режиму Winbox

6. Після цього вікно програми набуде вигляду, як на рисунку 1.6.

7. Поверніться до простого режиму. Щоб підключитися до маршрутизатора, введіть IP або MAC-адресу маршрутизатора в полі “**Connect To**”. Або натисніть на MAC-адресу вкладки “**Neighbors**”, як наведено на рисунку 1.7.

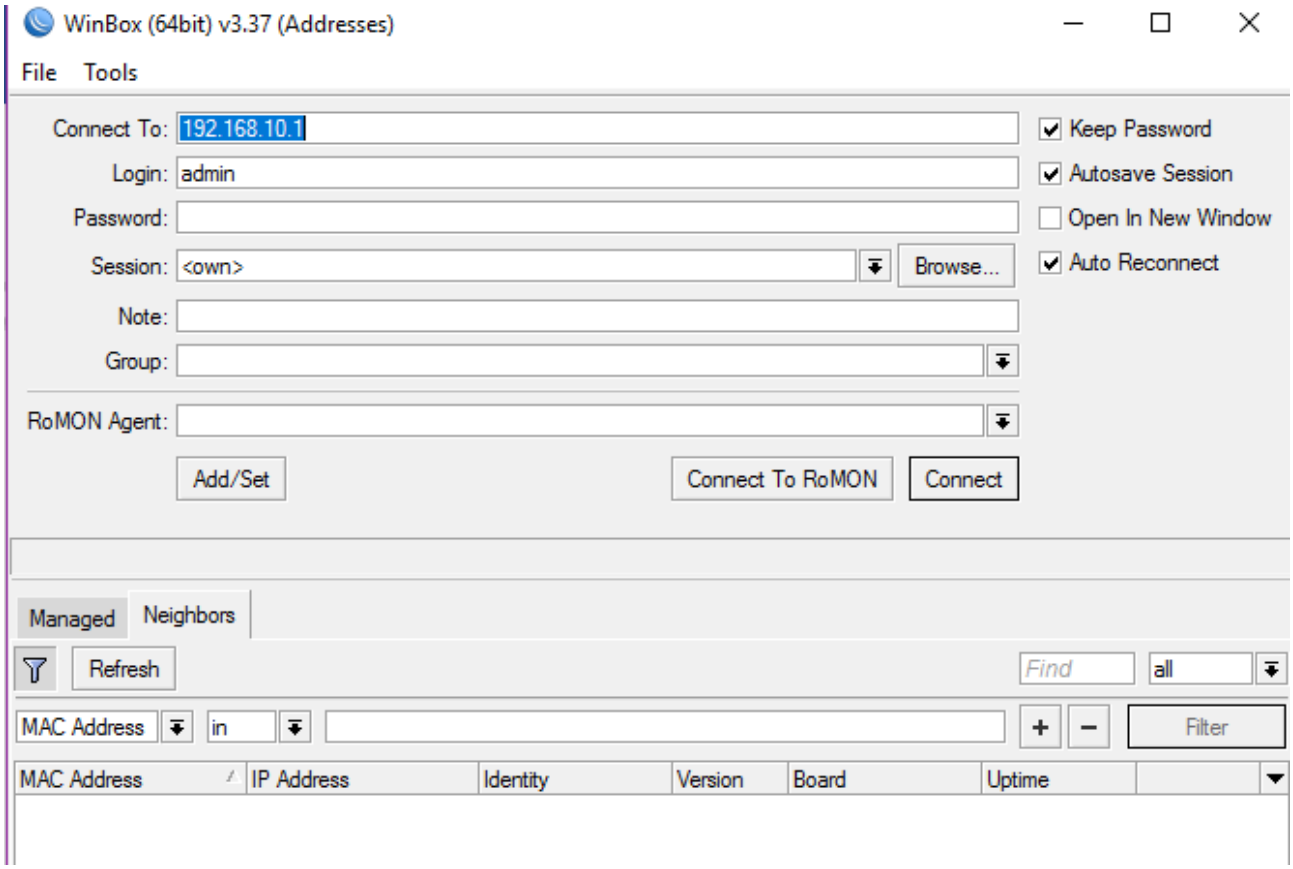

Рисунок 1.6. Вікно Winbox у розширеному режимі

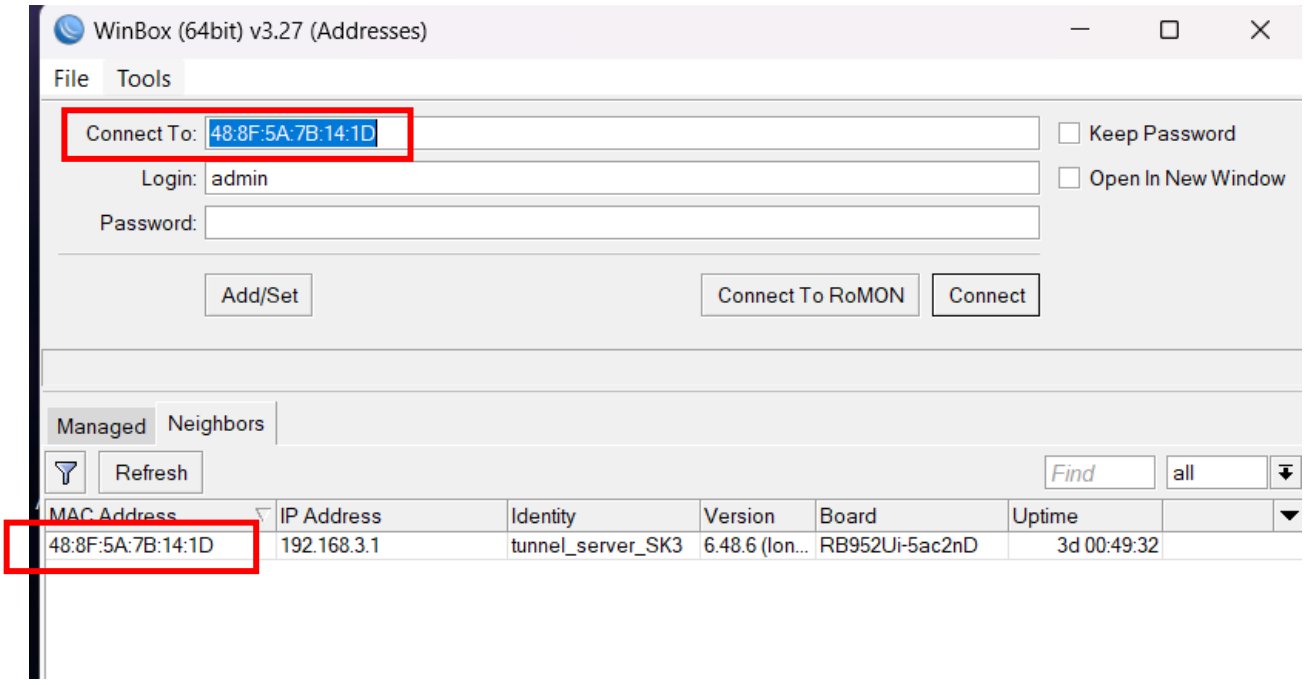

Рисунок 1.7. Вибір пристрою для входу

8. Вкажіть ім’я користувача та пароль (за замовчуванням логін – “admin”, а пароль відсутній) і натисніть кнопку **“Connect”**, як наведено на рисунку 1.8. Ви

також можете ввести номер порту після IP-адреси, розділивши їх двокрапкою, наприклад: 192.168.88.1:9999. За замовчування IP-адреса MikroTik в локальній мережі 192.168.88.1. Порт потім можна змінити в меню сервісів RouterOS.

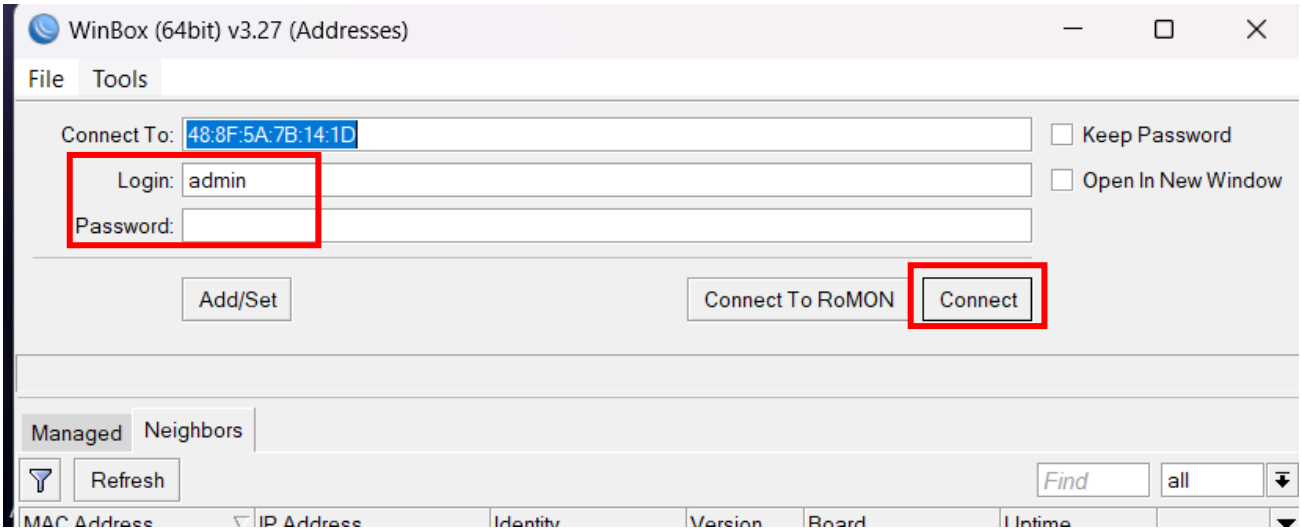

Рисунок 1.8. Введення авторизаційних даних

9. Після цього відкриється вікно конфігурування маршрутизатора (рис.1.9).

10. Налаштування через командний рядок також можна здійснювати у вікні Winbox. Для цього натисніть **“New Terminal”**, як наведено на рисунку 1.10.

При першому вході в командний рядок навіть з графічного інтерфейсу Winbox, маршрутизатор може запитати у вас ті самі логін і пароль, як і при вході в графічний інтерфейс. Після цього введіть в терміналі команду **“*export*”** – вона виведе на екран всі поточні налаштування маршрутизатора. Зробіть ***скріншот***.

Пам’ятайте, що весь функціонал MikroTik ROS доступний саме з командного рядка. Графічний інтерфейс за структурою подібний до командного рядка, але його можливості дещо обмежені.

11. Ви можете закрити поточне вікно Winbox повністю (“**Exit**”) або закрити сесію з поточним пристроєм, але лишитися у вікні програми (“**Disconnect**”) щоб повернутися до попереднього вікна входу, як на рисунку 1.11.

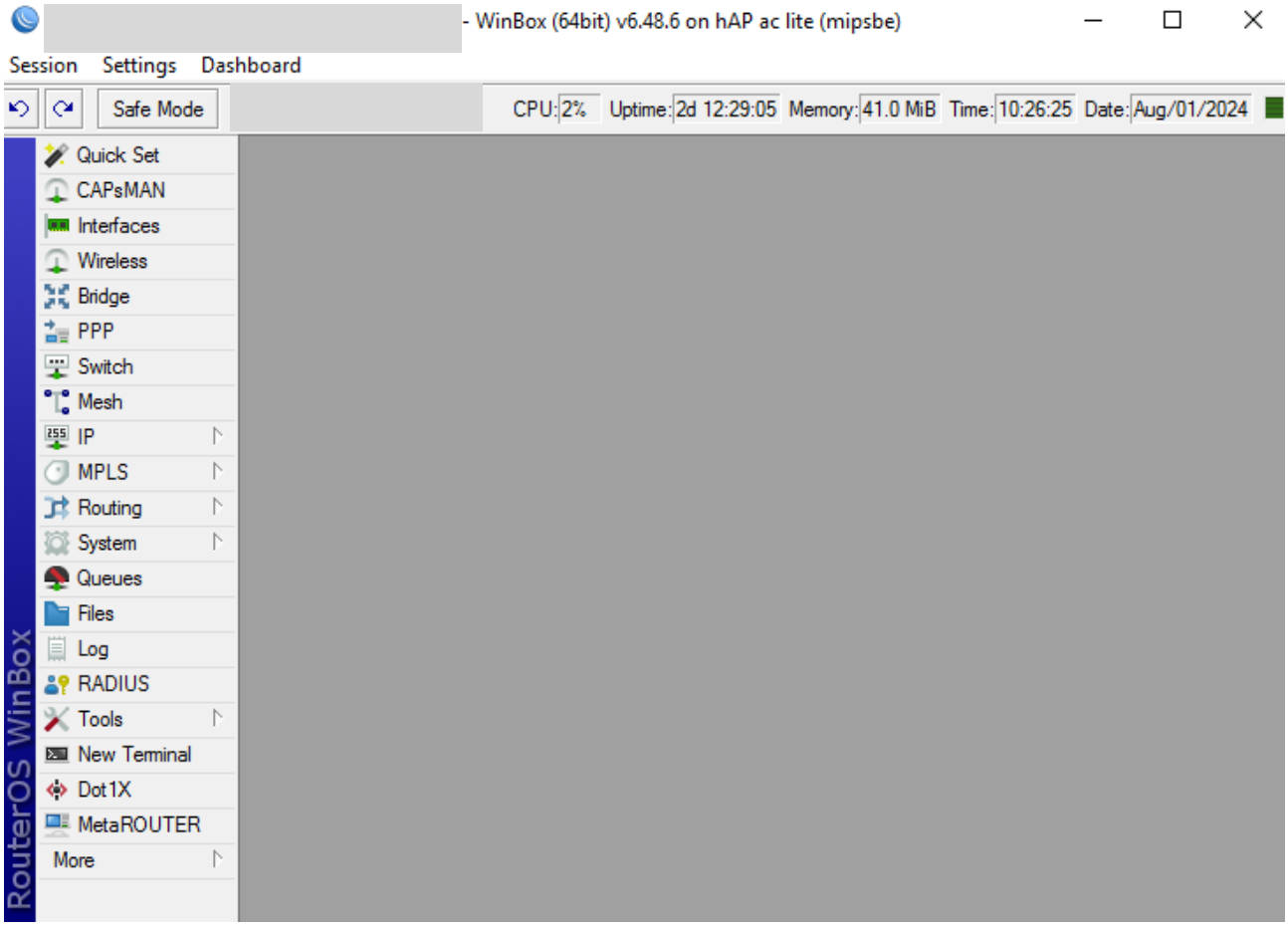

Рисунок 1.9. Початкове вікно конфігурації MikroTik у Winbox

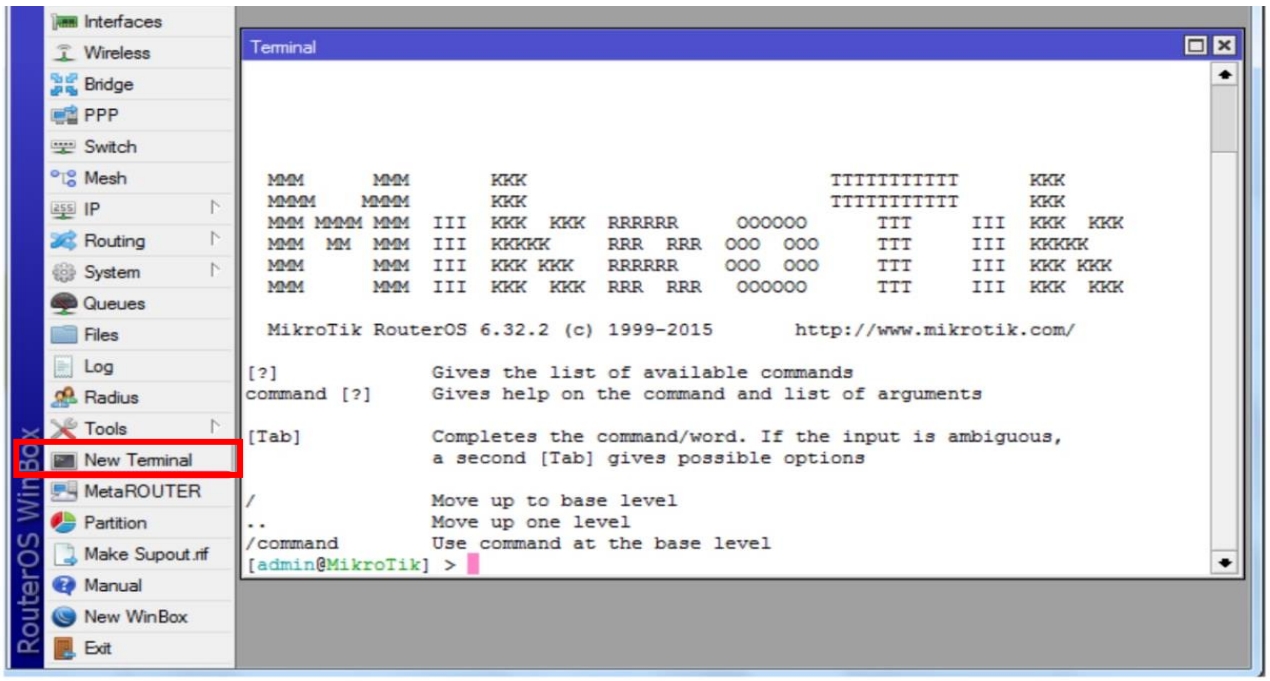

Рисунок 1.10. Вхід в інтерфейс командного рядка

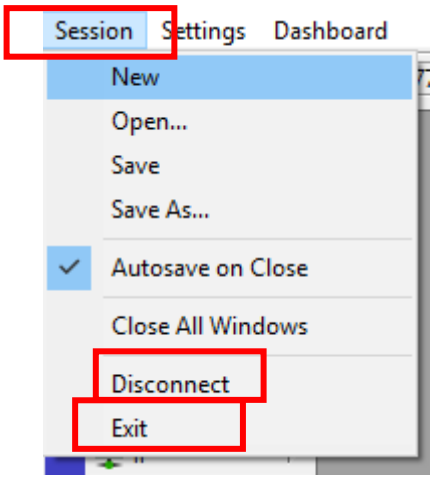

Рисунок 1.11. Закриття сесії між ПК і маршрутизатором

Контрольні питання

1. Які способи налаштування пристроїв MikroTik ви знаєте?
2. Який порт використовується для підключення по Winbox?
3. За яким протоколом працює виявлення сусідів у Winbox?
4. Які команди CLI MikroTik ви вже знаєте?
5. Що це за режим “Advanced Mode”?

ЛАБОРАТОРНА РОБОТА № 2
СКИДАННЯ НАЛАШТУВАНЬ МАРШРУТИЗАТОРА MIKROTIK

Мета:

1) ознайомитися з варіантами скидання налаштувань пристроїв MikroTik та різницею між ними;

2) отримати практичні навички зі скидання налаштувань різних пристроїв MikroTik.

Теоретичні відомості

Існують випадки, коли постає необхідність скинути налаштування маршрутизатора MikroTik, наприклад:

- неправильно встановлено пароль адміністратора;
- пристрій зламано;
- пароль втрачений.

Важливо !!! Скинути тільки пароль в Router OS – неможливо !!!

Скинути налаштування можливо двома такими способами:

- через кнопку “Reset”;
- через Router OS:
  - через GUI (наприклад, Winbox);
  - через командний рядок.

Хід роботи

2.1. Скидання через кнопку “RESet”

1. Вимкніть живлення маршутизатора.

2. Затисніть кнопку **“RESet”** (рис. 2.1) та увімкніть живлення маршрутизатора.

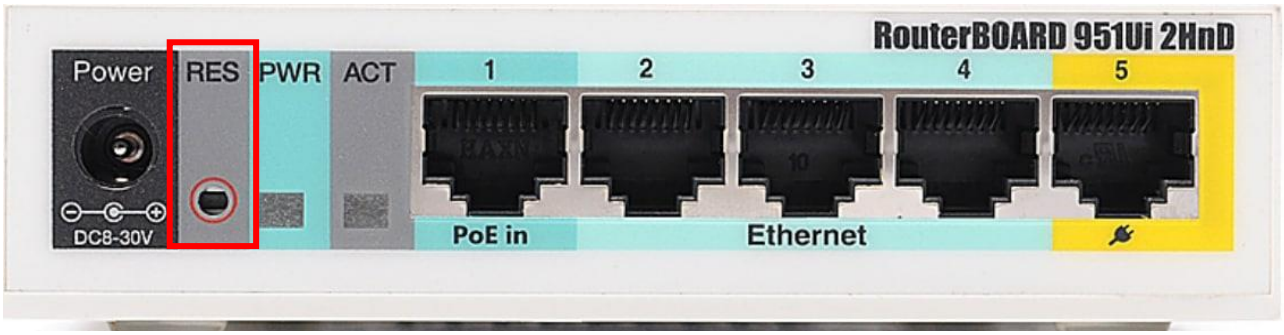

Рисунок 2.1. Розташування “RESet” на маршрутизаторі

3. Очікуйте моменту, коли індикатор **“ACTive”** почне блимати (приблизно через 5 с) і відпустіть **“RES”**.

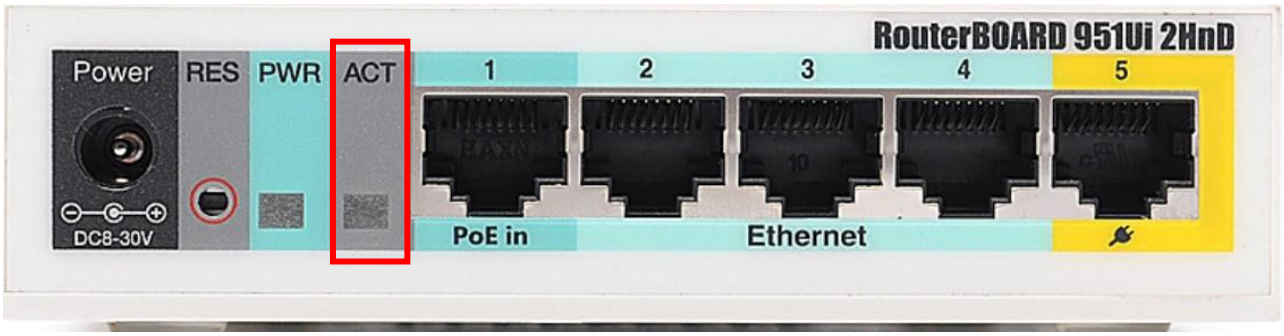

Рисунок 2.2. Розташування індикатора ACT на маршрутизаторі

4. Після скидання налаштувань маршрутизатора зазначеним способом він перейде до заводських налаштувань **(Default Configuration)**. Тобто після перезавантаження пристрою його IP-адреса стане **192.168.88.1**, а логін і пароль – стандартними. Після скидання налаштувань при першому вході на маршрутизатор

через Winbox перед dами з’явиться вікно, у якому буде відображена поточна конфігурація, а також можливість зробити повне скидання налаштувань, натиснувши кнопку **“Remove Configuration”**.

Примітка. *Старіші моделі RouterBOARD оснащені отвором для перемички скидання (замість кнопки). Для деяких пристроїв може знадобитися відкрити корпус. Закрийте перемичку металевою викруткою та завантажте плату, доки конфігурація не буде очищена за тим же алгоритмом, що був наведений вище. Зразки таких плат наведені на рис.2.3.*

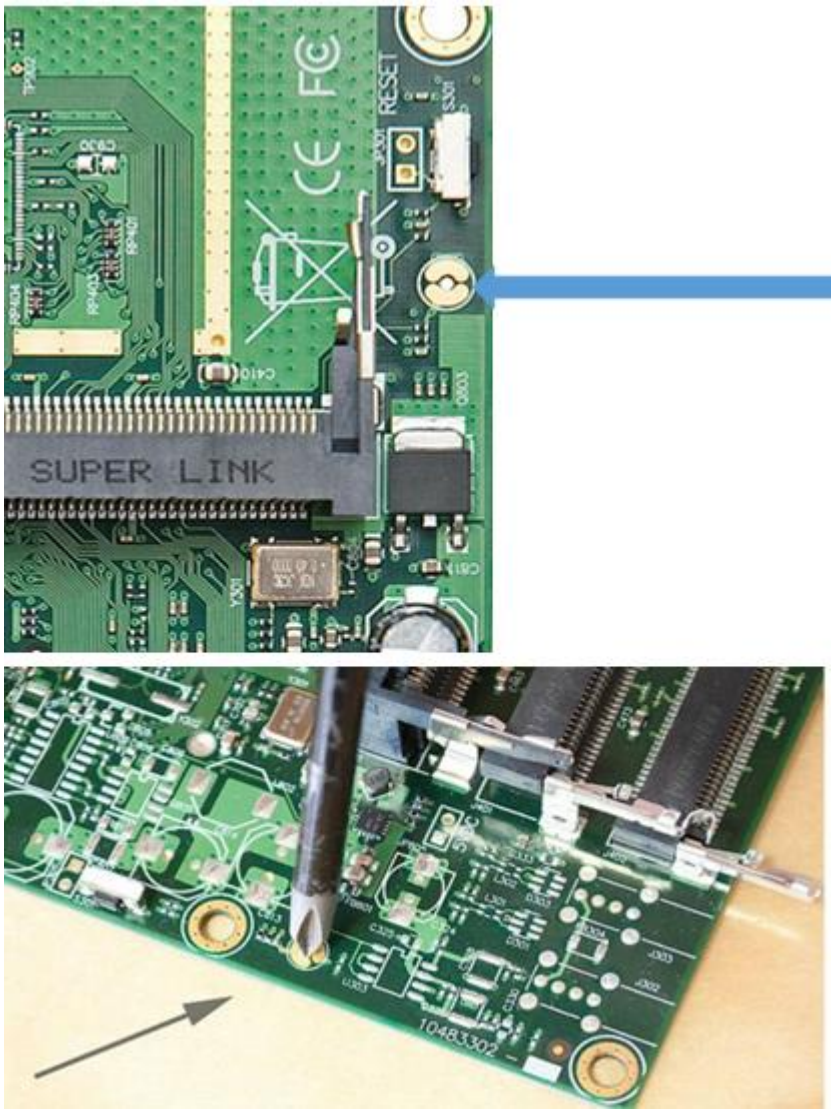

Рисунок 2.3. Розташування контактів для скидання налаштувань маршрутизатора на платі

2.2. Скидання засобами Router OS

1. Для того, щоб скинути налаштування маршрутизатора за допомогою вбудованих засобів, необхідно знати логін та пароль, або перед цим скинути до заводських налаштувань через кнопку чи отвір **“RESet”** і зайти зі стандартними логіном та паролем. Далі ввійдіть через Winbox в налаштування маршрутизатора, перейдіть на вкладку **“System”** та оберіть **“RESet Configuration”**, як наведено на рисунку 2.4:

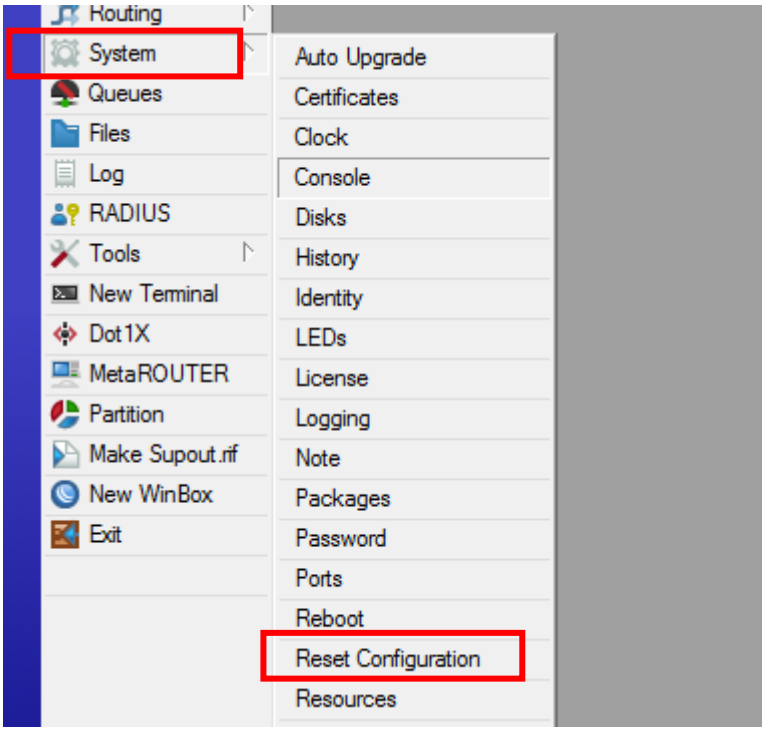

Рисунок 2.4. Скидання налаштувань через графічний інтерфейс

2. Для повного скидання налаштувань без створення резервної копії існуючої конфігурації у наступному вікні поставте відповідні галочки та натисніть **“RESet Configuration”** (рис.2.5):

3. Після цього програма вас “викине” з налаштувань, маршрутизатор перезавантажиться, і можна проводити налаштування “з нуля”. При цьому IP-адреса маршрутизатора буде **0.0.0.0**. Логін буде “admin”, а пароль – відсутнім, або скористайтесь наведеним на зворотній стороні маршрутизатора на етикетці поряд зі штрих-кодом.

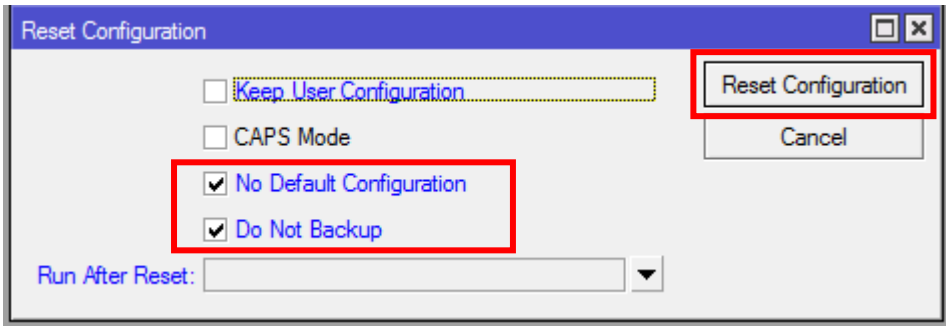

Рисунок 2.5. Повне скидання налаштувань через графічний інтерфейс

4. Альтернативним способом можна скинути маршрутизатор через CLI, для цього необхідно зайти в **New Terminal** і прописати команду:

/system reset-configuration no-defaults=yes skip-backup=yes

Після цього маршрутизатор перезавантажиться і буде мати повністю пусту конфігурацію.

Контрольні питання

1. Які способи скидання налаштувань пристроїв MikroTik ви знаєте?
2. Чи можна скинути лише пароль маршрутизатора MikroTik?
3. Чи можна скинути налаштування вибірково?
4. Яка IP-адреса за замовчуванням у пристроїв MikroTik після скидання налаштувань до заводських?
5. Чи можна скинути маршрутизатор через CLI?

ЛАБОРАТОРНА РОБОТА №3
ВСТАНОВЛЕННЯ CLOUD HOSTED ROUTER VIRTUAL BOX

Мета:

1) ознайомитися з можливостями та характеристиками Cloud Hosted Router MikroTik;

2) отримати практичні навички зі встановлення на гіпервізор Cloud Hosted Router MikroTik.

Теоретичні відомості

Cloud Hosted Router (CHR) – це версія RouterOS, призначена для роботи на віртуальній машині. Він підтримує 64-розрядну архітектуру і може використовуватися на більшості популярних гіпервізорів, таких як VMWare, Hyper-V, VirtualBox, KVM та інші. CHR має всі функції RouterOS, увімкнені за замовчуванням, але модель ліцензування відрізняється від інших версій RouterOS.

Мінімальні вимоги для встановлення CHR:

- версія пакетів: RouterOS v6.34 або новіша;
- центральний процесор: 64-розрядний з підтримкою віртуалізації;
- оперативна пам'ять: не менше 128 МБ;
- Диск: 128 МБ дискового простору для віртуального жорсткого диска CHR (макс.: 16 ГБ).

Варіанти безкоштовного використання та випробування CHR:

- **Безкоштовна версія.** Рівень безкоштовної ліцензії дозволяє CHR працювати необмежений час. Швидкість завантаження на інтерфейсі обмежена 1 Мбіт/с. Усі інші функції, які надає CHR, доступні без обмежень. Щоб

скористатися цим, все, що вам потрібно зробити, це завантажити файл образу диска з офіційної сторінки завантаження та створити віртуальну машину.

- **60-денна пробна версія**. Окрім обмеженої безкоштовної інсталяції, ви також можете перевірити підвищену швидкість ліцензій P1/P10/PU за допомогою пробної версії 60.

Для цього ви повинні мати обліковий запис на MikroTik.com. Потім ви можете надіслати запит на потрібний рівень ліцензії для пробної версії маршрутизатора, який призначить ідентифікатор вашого маршрутизатора вашому обліковому запису та дозволить придбати ліцензію з вашого облікового запису. Усі еквіваленти платної ліцензії доступні для пробної версії. Пробний період становить 60 днів з дня придбання, після закінчення цього часу в меню вашої ліцензії почне відображатися «Обмежені оновлення», що означає, що RouterOS більше не можна оновити.

Якщо ви плануєте придбати вибрану ліцензію, ви повинні зробити це протягом 60 днів після закінчення пробної версії. Якщо ваш пробний період закінчився, і протягом 2 місяців після його закінчення не було жодних покупок, пристрій більше не відображатиметься у вашому обліковому записі MikroTik. Щоб здійснити покупку протягом необхідного періоду часу, вам доведеться зробити заново встановити CHR.

Щоб надіслати запит на пробну ліцензію, потрібно виконати команду *“/system license renew”* із командного рядка пристрою CHR. Вам буде запропоновано ввести ім’я користувача та пароль вашого облікового запису Mikrotik.com.

Хід роботи

1. Завантажте VirtualBox: установіть останню версію VirtualBox з офіційного сайту: https://www.virtualbox.org/wiki/Downloads/.

2. Завантажте образ CHR: завантажте та розпакуйте останню стабільну або тестову версію образу CHR VDI з веб-сайту MikroTik: https://mikrotik.com/download, як наведено на рисунку 3.1.

***Примітка**: краще всього завантажувати Long-Term версію.*

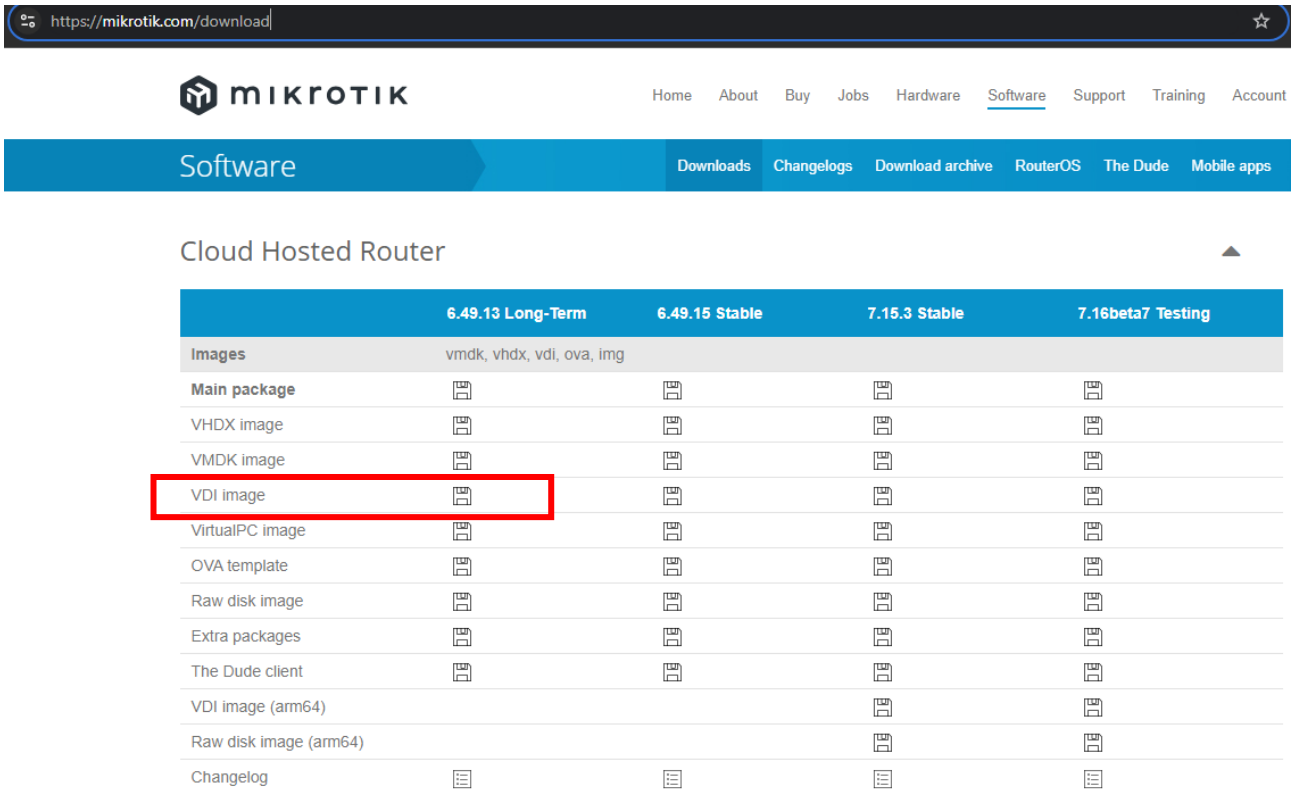

Рисунок 3.1. Образ CHR на сайті MikroTik

3. Запустіть програму VirtualBox. Створіть нову віртуальну машину (натисніть «**New**»), як наведено на рисунку 3.2.

4. Придумайте назву для вашої віртуальної машини, оберіть тип **“Linux”** та версію, як на рисунку 3.3, зробіть ***скріншот***, натисніть **“Next”**.

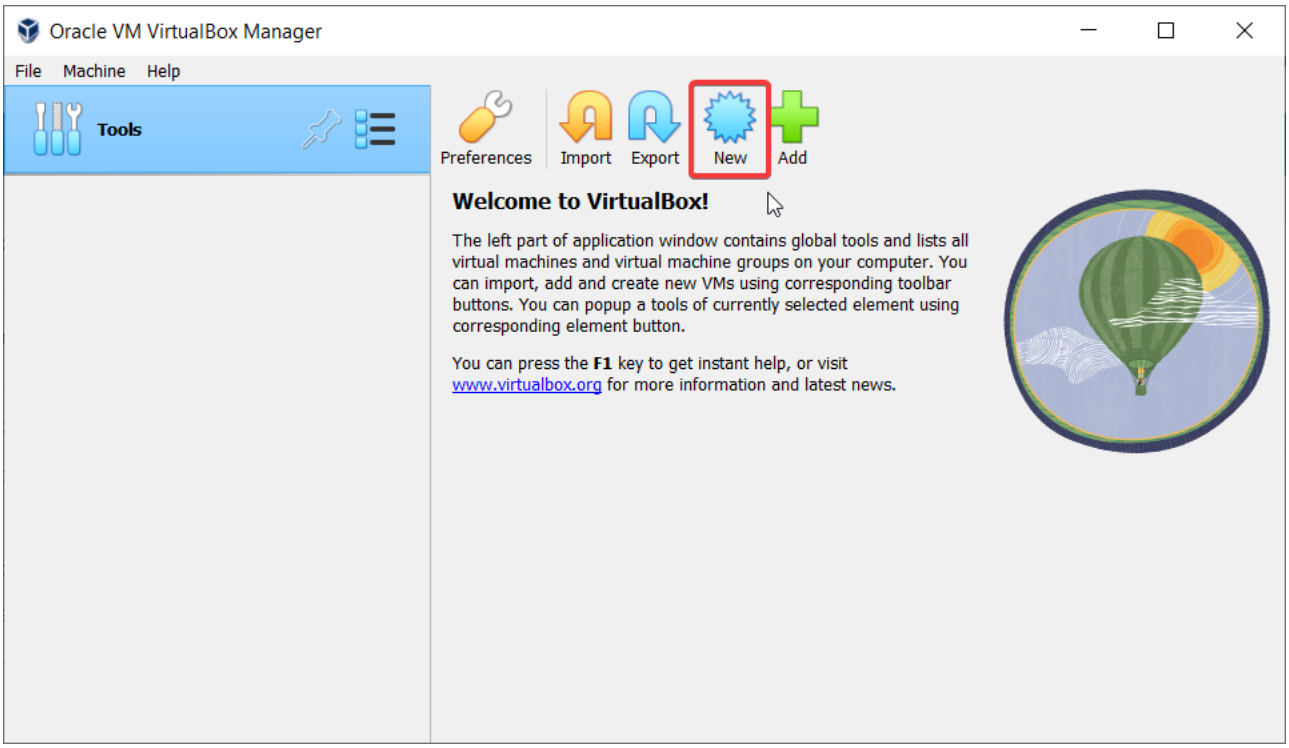

Рисунок 3.2. Створення нової віртуальної машини в VirtualBox

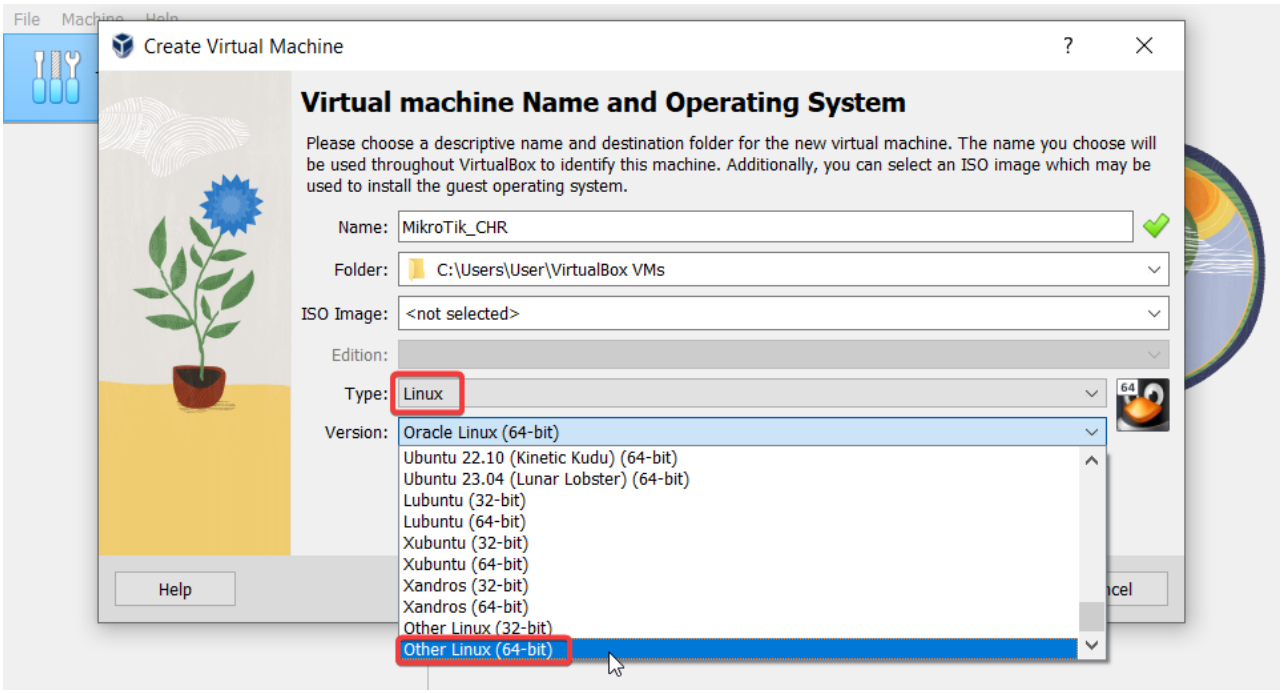

Рисунок 3.3. Вибір типу ОС

5. Виділіть пам’ять для віртуальної машини. Рекомендується виділити не менше 256 МБ оперативної пам’яті, як на наведено на рисунку 3.4. Також оберіть кількість процесорів, натисніть **“Next”**.

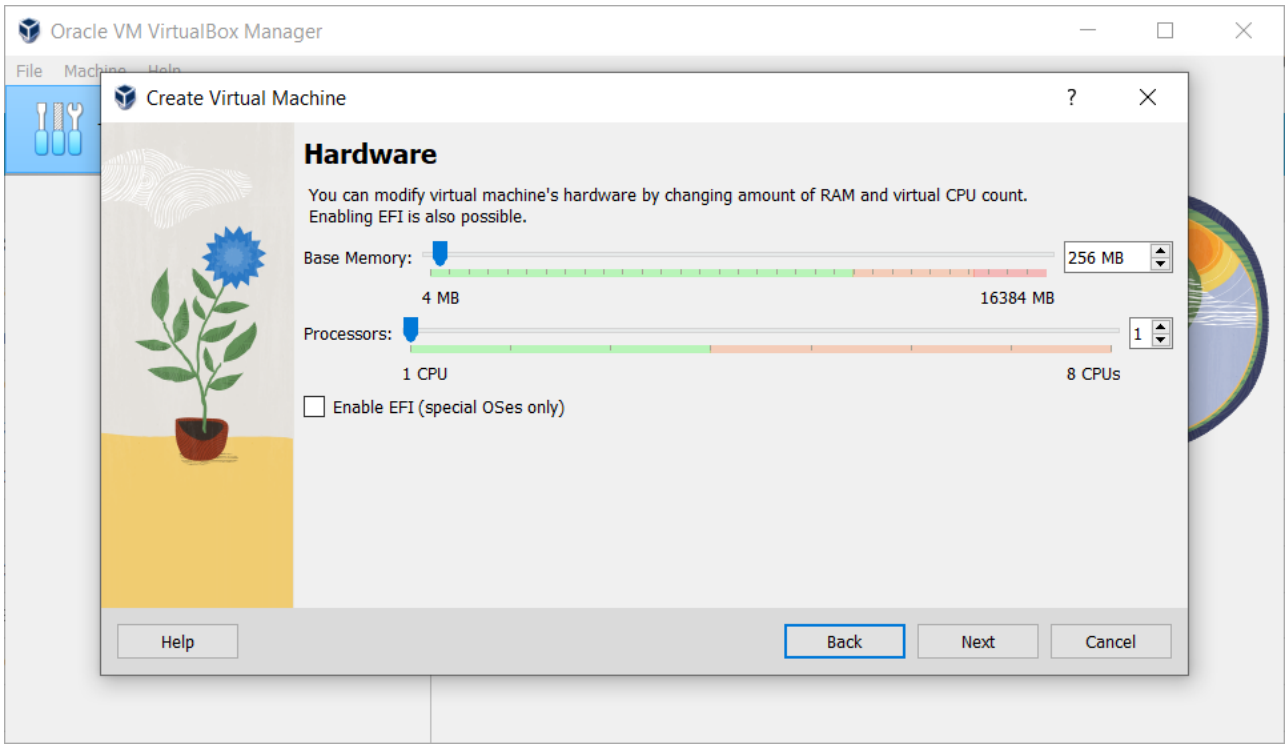

Рисунок 3.4. Виділення пам’яті під ВМ

6. Віртуальний жорсткий диск: Виберіть **“Використовувати наявний файл жорсткого диска”**, додайте завантажений файл образу VDI, натисніть **“Next”**, як наведено на рисунку 3.5.

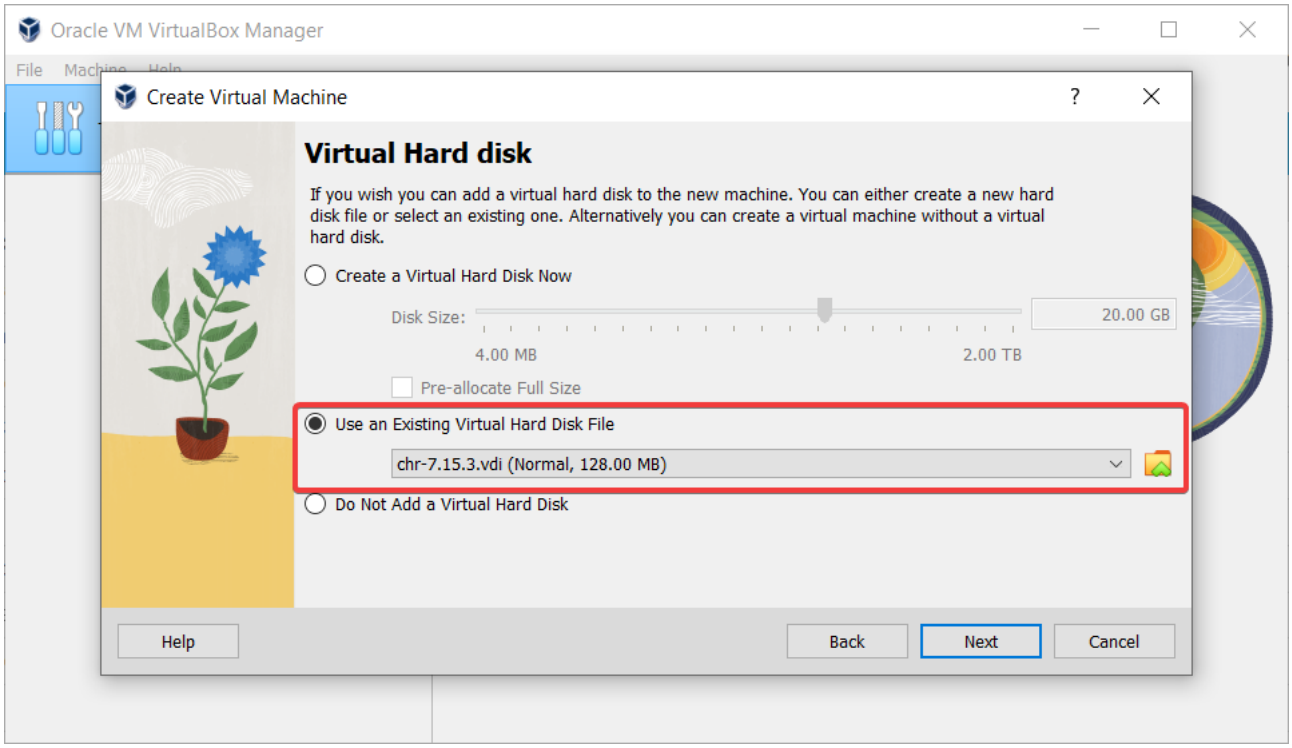

Рисунок 3.5. Вибір віртуального диска

7. Перевірте налаштування, зробіть ***скріншот*** та натисніть **“Finish”**, як наведено на рисунку 3.6.

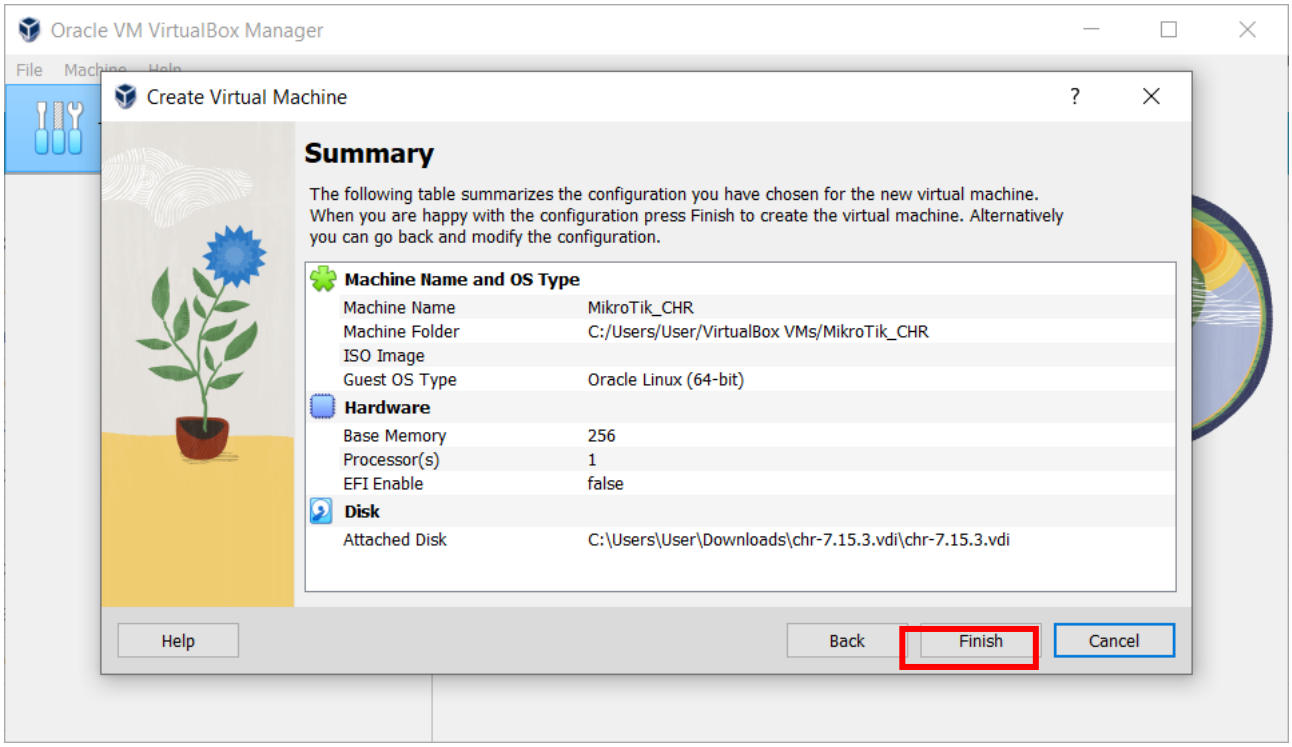

Рисунок 3.6. Завершення створення ВМ

8. Виберіть вашу нову віртуальну машину та натисніть **“Settings”**, як наведено на рисунку 3.7.

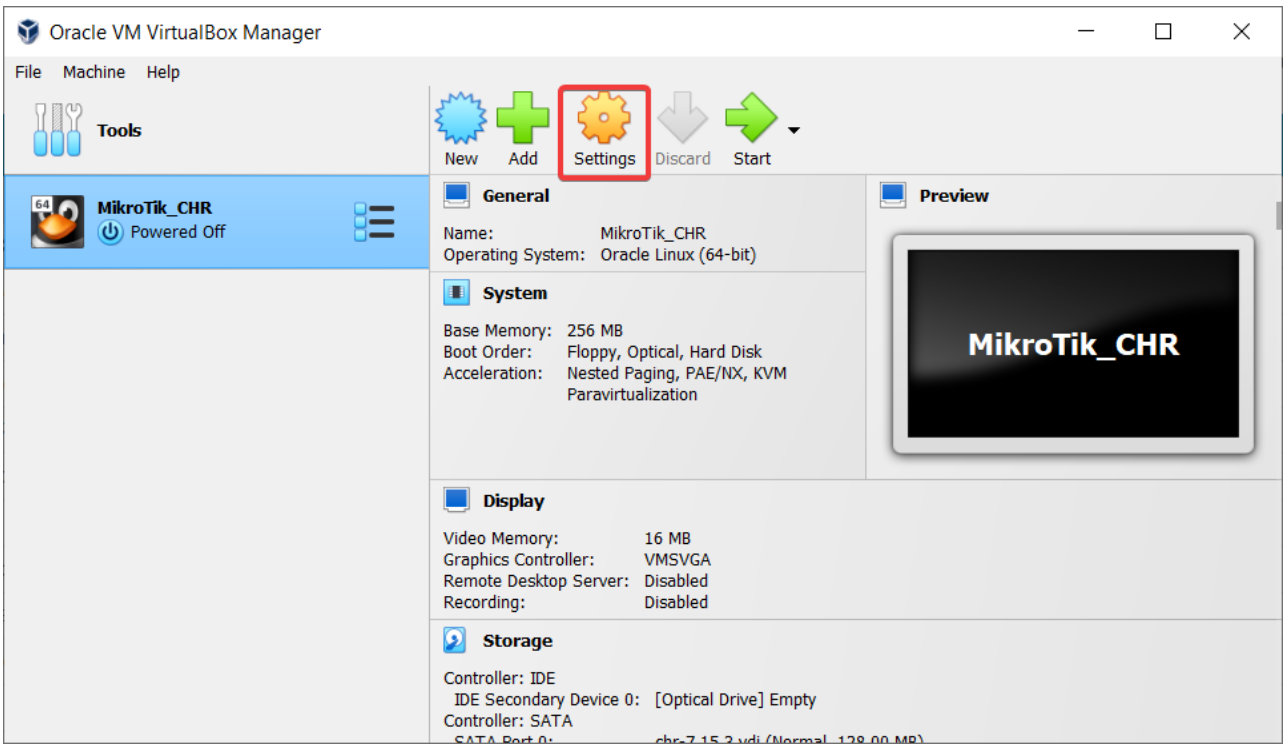

Рисунок 3.7. Додаткові налаштування ВМ

9. Перейдіть на вкладку **“Network”** та виберіть налаштування мережевого адаптера **“Bridged”**, як наведено на рисунку 3.8 або **“NAT”**.

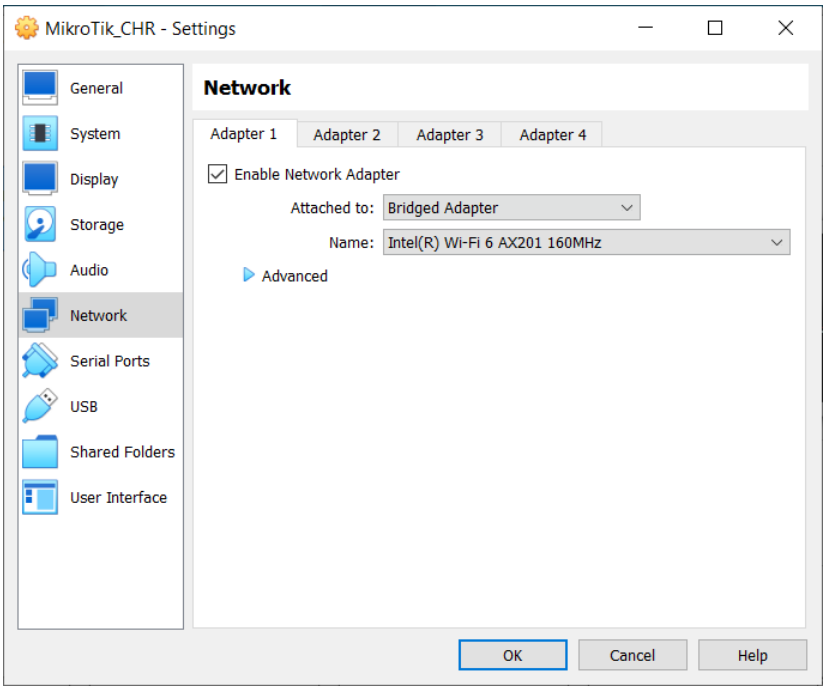

Рисунок 3.8. Мережеві налаштування ВМ

10. Запустіть віртуальну машину, як наведено на рисунку 3.9.

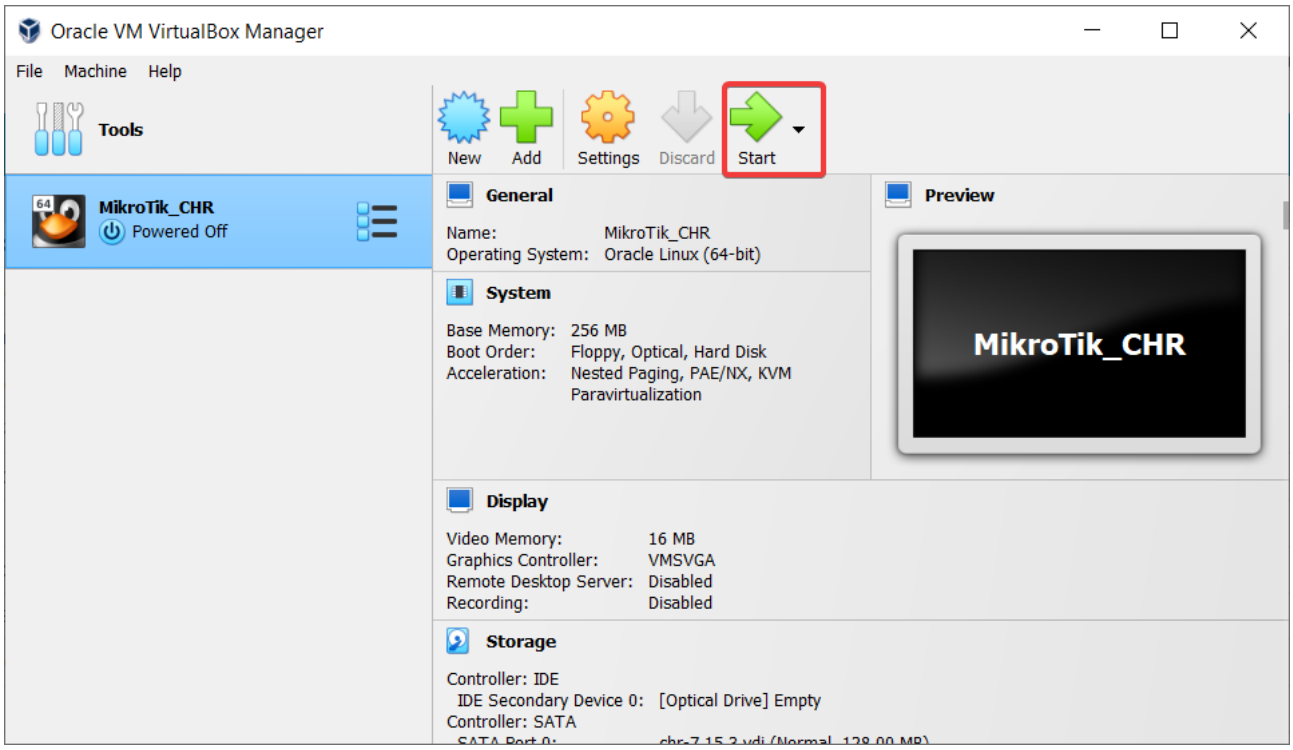

Рисунок 3.9. Запуск новоствореної ВМ

11. Після завантаження віртуальної машини ви побачите запит на вхід до CLI CHR, як на рисунку 3.10, зробіть ***скріншот***.

Стандартні облікові дані для входу:

- ім'я користувача: ***admin***;
- пароль відсутній.

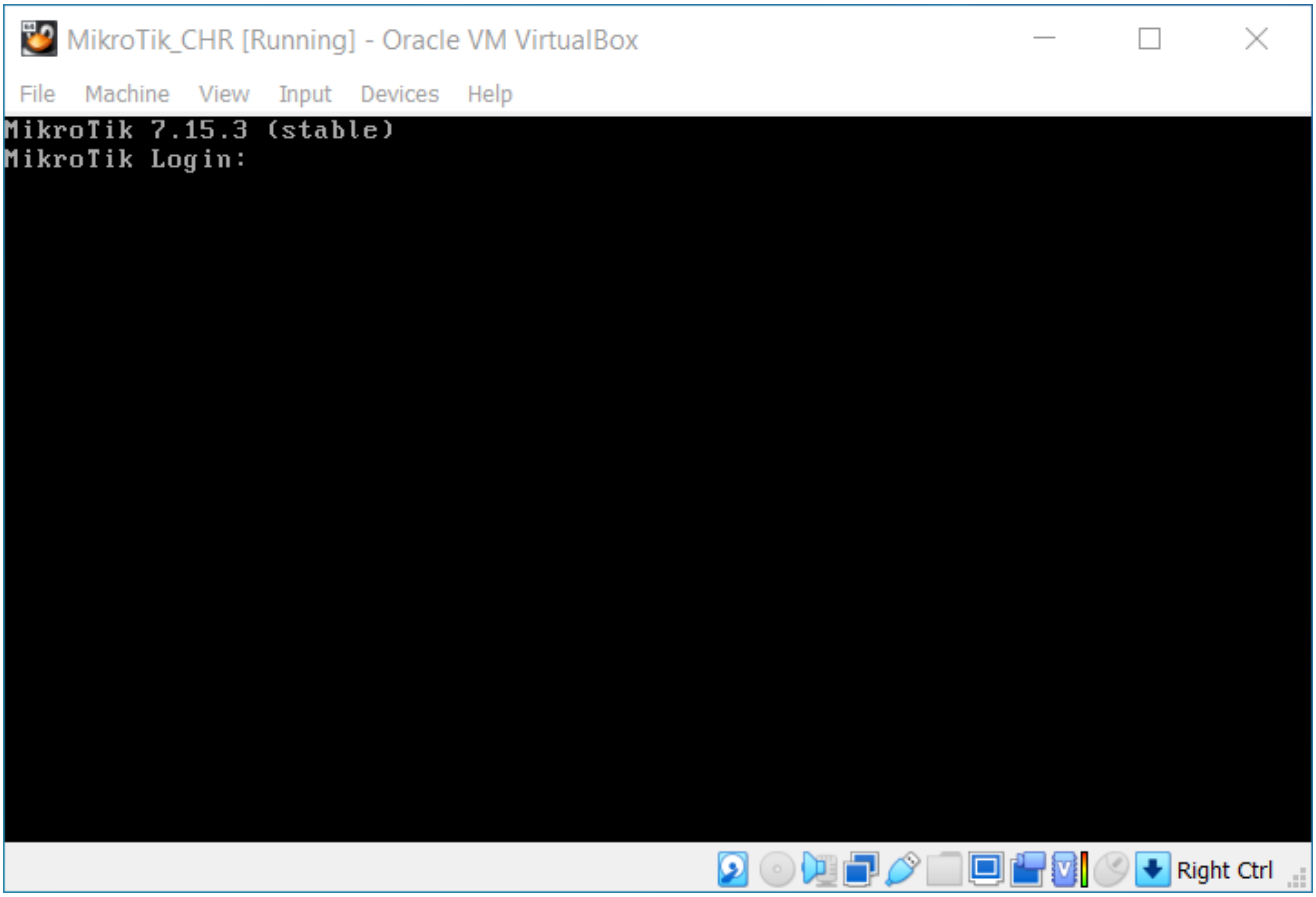

Рисунок 3.10. Вхід до CLI CHR

Також тепер ви можете підключитись до CHR за допомогою Winbox, використовуючи його MAC-адресу або IP-адресу, як було наведено в лабораторній роботі № 1. Для цього запустіть Winbox та перегляньте список доступних пристроїв.

12. Ви успішно встановили MikroTik CHR на VirtualBox. Тепер ви можете продовжити мережеві налаштування і використовувати всі функції MikroTik RouterOS. Використовуйте та налаштовуйте CHR відповідно до вимог мережі за допомогою MikroTik CLI або Winbox.

Контрольні питання

1. Що таке MikroTik CHR?

2. Які обмеження на безкоштовну версію CHR?

3. Звідки можливо завантажити образ CHR?

4. Чи правильно при завантаженні віртуального жорсткого диску “Використовувати наявний файл жорсткого диска”?

5. Чи можливо виділити менше 256 МБ оперативної пам’яті для віртуальної машини?

ЛАБОРАТОРНА РОБОТА №4
РЕАЛІЗАЦІЯ РЕЗЕРВНИХ КОПІЙ

Мета:

1) ознайомитися з видами резервних копій та порядком їх створення для пристроїв MikroTik;

2) отримати практичні навички з виконання та відновлення резервних копій пристроїв MikroTik.

Теоретичні відомості

Функція резервного копіювання RouterOS дозволяє клонувати конфігурацію маршрутизатора в двійковому форматі, який потім можна повторно застосувати на тому самому пристрої, або використати для повного чи вибіркового перенесення налаштувань на інший пристрій (залежно від виду резервної копії). Файл повної резервної копії системи містить MAC-адреси пристрою, які відновлюються під час завантаження файлу. **Тому рекомендовано відновлювати резервну копію на тій же версії RouterOS !!!**

4.1 Збереження повної резервної копії ОС (.backup)

- .backup файл не редагується (бінарний).
- Містить всі налаштування, включно з системними обліковими даними.
- Якщо явно не задати ім’я файлу, то воно буде складатися з ідентифікації маршрутизатора, дати і часу його створення.

1. Для реалізації резервної копії перейдіть на вкладку **“Files”** та натисніть кнопку **“Backup”**, задайте ім’я (прізвище_дата), пароль, та натисніть кнопку

“Backup” у вікні, що з’явилось, як наведено на рисунку 4.1. Ця дія призведе до створення повної резервної копії ROS з розширенням *.backup*.

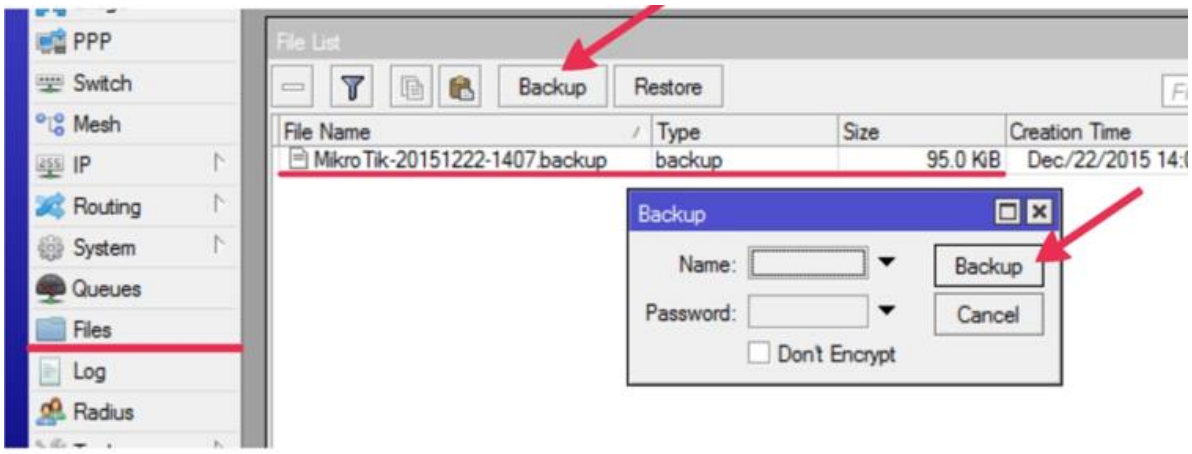

Рисунок 4.1. Виконання повної резервної копії MikroTik ROS

***Примітка**: якщо стоїть галочка **Don’t-encrypt** (так|ні; за замовчуванням: ні), це дає можливість вимкнути шифрування файлу резервної копії. Зауважте, що з RouterOS v6.43 без наданого пароля файл резервної копії незашифрований. З точки зору безпеки рекомендовано завжди шифрувати файл резервної копії та створювати надійний пароль.*

2. На деяких маршрутизаторах є папка **“flash”** (рис.4.2), і за замовчуванням копія створюється поза нею. У випадку зникнення живлення, вона зітреться з пам’яті. Аби цьому запобігти, необхідно перетягнути копію в цю папку.

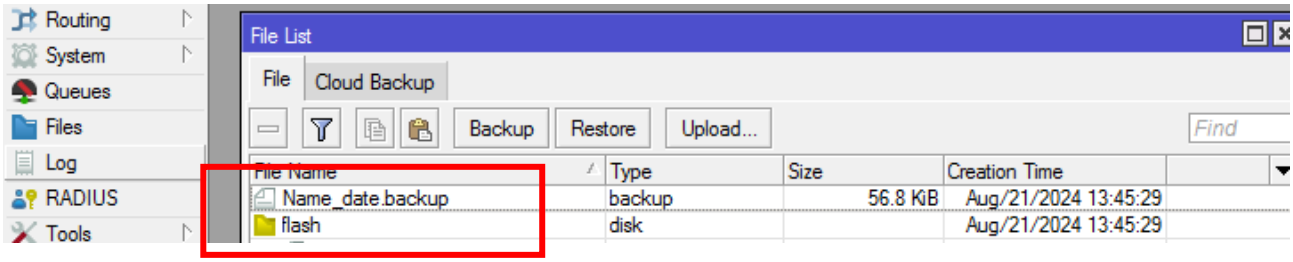

Рисунок 4.2. Папка flash

3. Зменшіть вікно Winbox та перетягніть резервну копію собі на робочий стіл за допомогою миші, результат повинен виглядати, як наведено на рисунку 4.3. Або скористайтесь кнопкою **“Upload”.** Зробіть ***скріншот.***

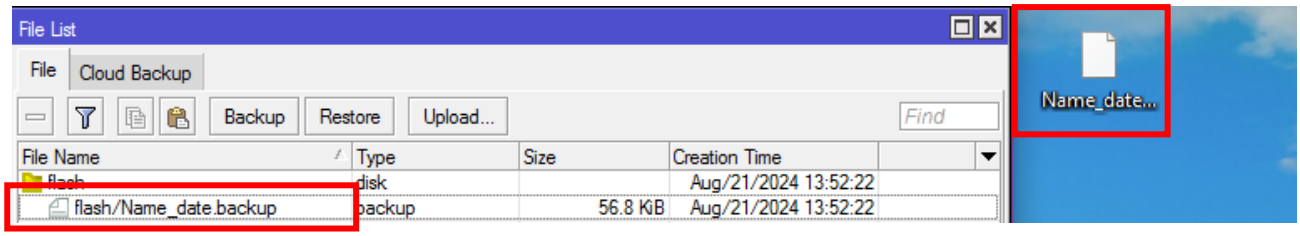

Рисунок 4.3. Перетягування резервної копії на робочий стіл

4. Відкрийте файл резервної копії на робочому столі ПК з допомогою блокнота. Що ви можете прочитати? Зробіть ***скріншот***.

5. Для завантаження (відновлення з) резервної копії перейдіть на вкладку **“Files”**, виберіть потрібний файл та натисніть **“Restore”**. У вікні, що з’явилося, уведіть пароль і також натисніть кнопку **“Restore”**, як наведено на рисунку 4.4.

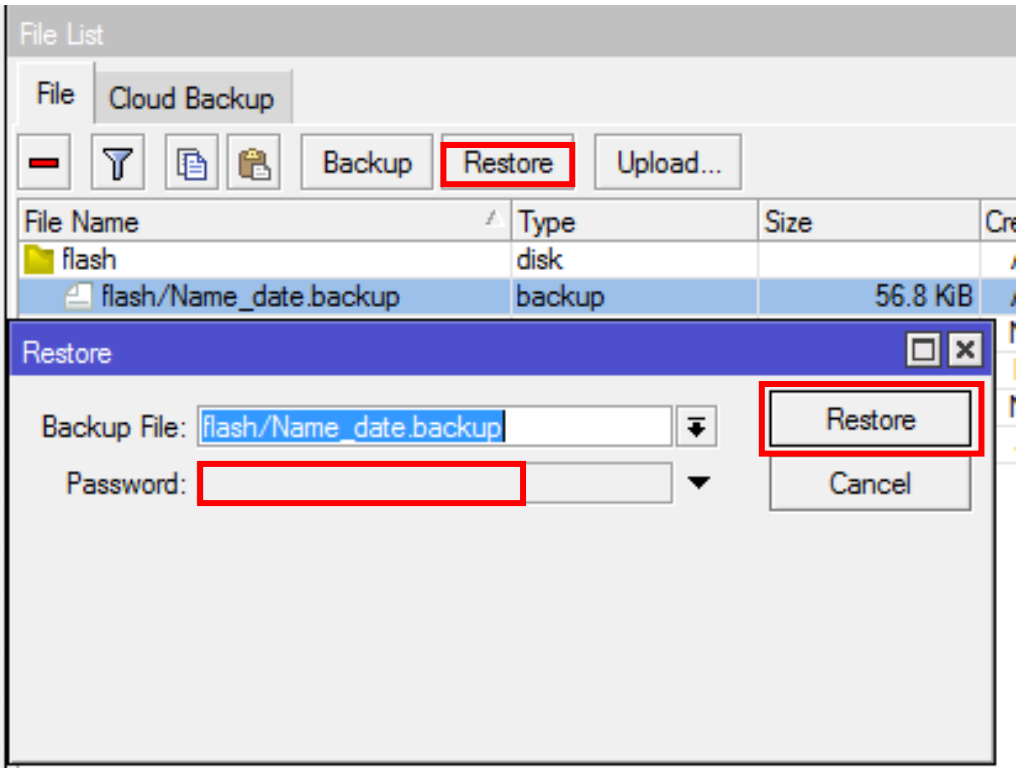

Рисунок 4.4. Відновлення ROS з файлу резервної копії

4.2 Збереження часткової резервної копії ОС (.rsc)

- Команда ***"export"*** друкує сценарій, який можна застосовувати для відновлення конфігурації, якщо використовувати виведення команди в файл (він отримає розширення ***.rsc***). Загалом, ця команда виводить поточну конфігурацію маршрутизатора на певному рівні в інтерфейсі CLI. Цю команду можна викликати на будь-якому рівні меню, і вона діє нього та всіх рівнів меню нижче (можна зберігати часткові налаштування маршрутизатора). Результати можна зберегти у файлі, доступному для завантаження за допомогою FTP.
- Export/import доступний лише з CLI.
- Export файл редагується (скрипт).
- Містить налаштування без системних облікових даних (не містить паролі користувачів).

1. Для виконання резервної копії за допомогою команди ***"export"***, перейдіть в термінал (командний рядок) маршрутизатора. Виконайте команду, та зробіть скріншот CLI:

[admin@MikroTik] > export file = Name_date

Примітка. *Name_date – ім'я файлу який ви створите командою. Може бути будь-яке.*

2. Перейдіть на вкладку **"Files"**, та знайдіть новий створений файл з розширенням **".rsc"**. Зменшіть вікно Winbox та перетягніть цей файл на свій робочий стіл за допомогою миші, як в 4.1 цієї лабораторної роботи. Відкрийте файл резервної копії за допомогою блокнота. Зробіть ***скріншот***. Що ви можете прочитати?

3. Для завантаження конфігурації такого формату виконайте команду в CLI:

[admin@MikroTik] > import file-name = Name_date

Контрольні питання

1. Які види резервних копій у Router OS існують? Чим відрізняються?
2. У яких ситуаціях краще обирати той чи інший вид резервної копії ROS?
3. Що означає наявність галочки “Don’t-encrypt”
4. Для чого потрібна команда “export”?
5. Чи редагуються .backup файли?

ЛАБОРАТОРНА РОБОТА № 5
НАЛАШТУВАННЯ ДОСТУПУ З ЛОКАЛЬНОЇ МЕРЕЖІ В ГЛОБАЛЬНУ МЕРЕЖУ ІНТЕРНЕТ НА MIKROTIK ROS

Мета:

1) ознайомитися з порядком налаштування доступу з локальної мережі в глобальну мережу інтернет на Mikrotik ROS;

2) отримати практичні навички з виконання налаштувань пристроїв MikroTik.

Хід роботи

1. Перед початком роботи зберіть схему підключення за зразком, як наведено на рисунку 5.1, (комп'ютер або ноутбук можна підключати до будь-якого інтерфейсу маршрутизатора крім того, який буде працювати як WAN).

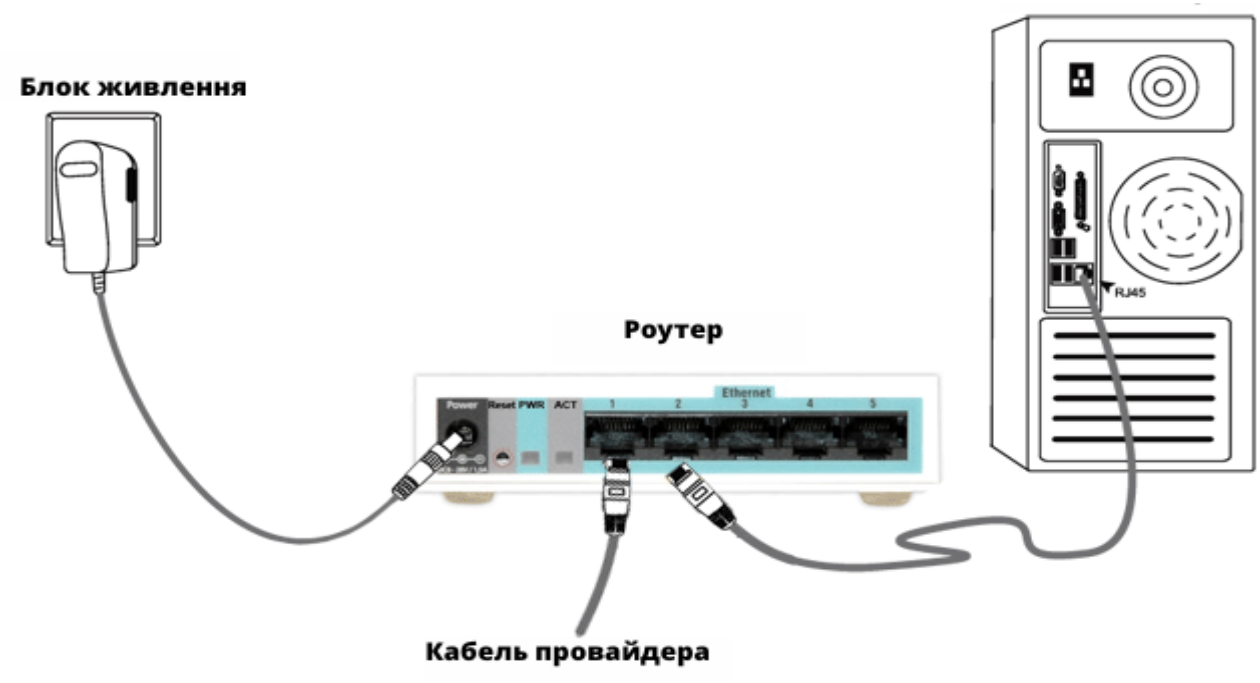

Рисунок 5.1. Схема підключення ПК та провайдера до маршрутизатора

2. Зайдіть через Winbox на маршрутизатор та скиньте його налаштування, як наведено на рисунку 5.2.

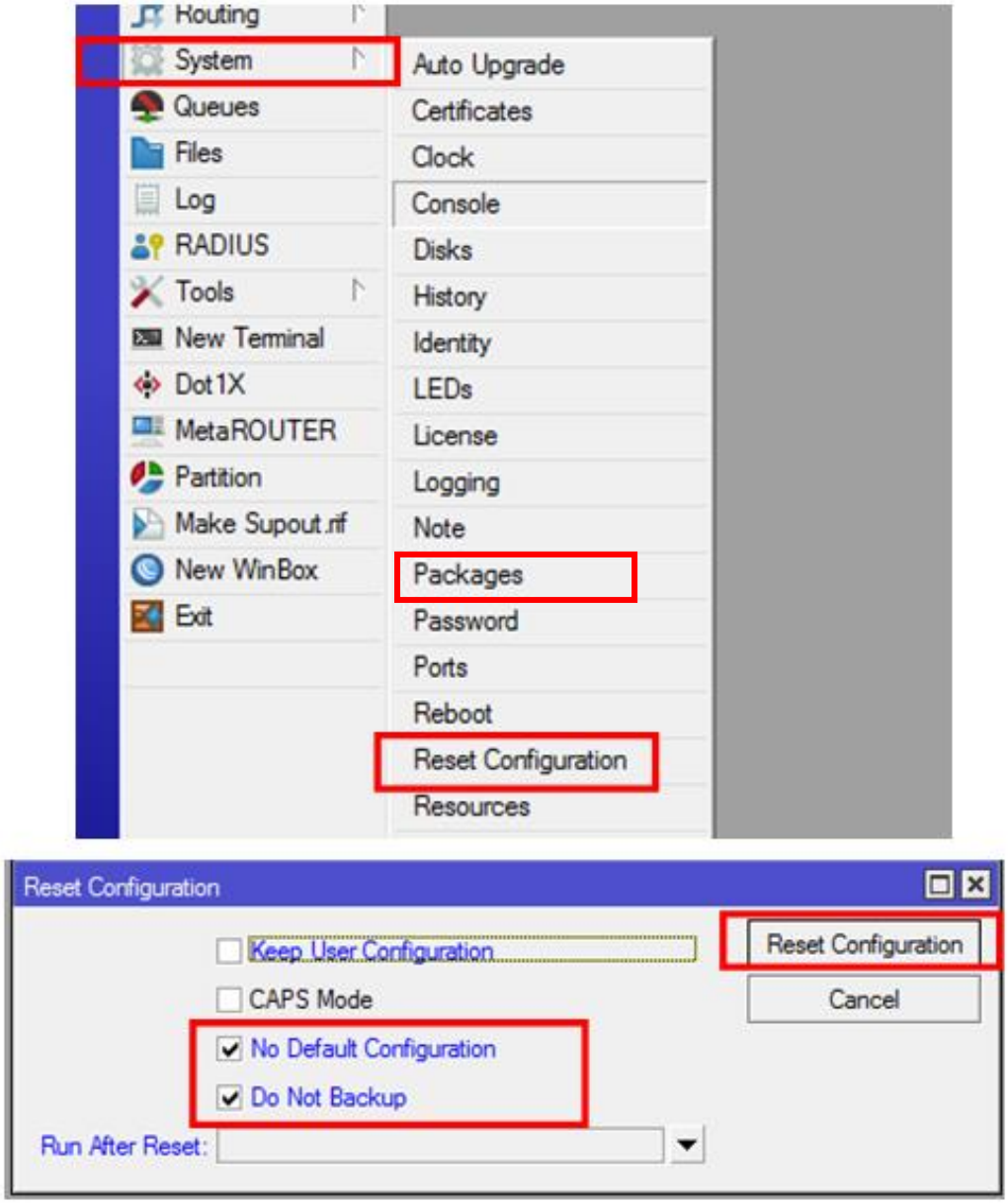

Рисунок 5.2. Скидання налаштувань маршрутизатора

3. Задайте ім’я маршрутизатору **(*name_X*) (тут і далі *X* – номер за журналом)**, як наведено на рисунку 5.3. Зробіть ***скріншот***.

4. Створіть нового користувача з правами адміністратора, задайте йому пароль **“1”**, усі подальші дії виконуйте від його імені **(*admin_name_X*)**, як наведено на рисунку 5.4. Зробіть ***скріншот*.**

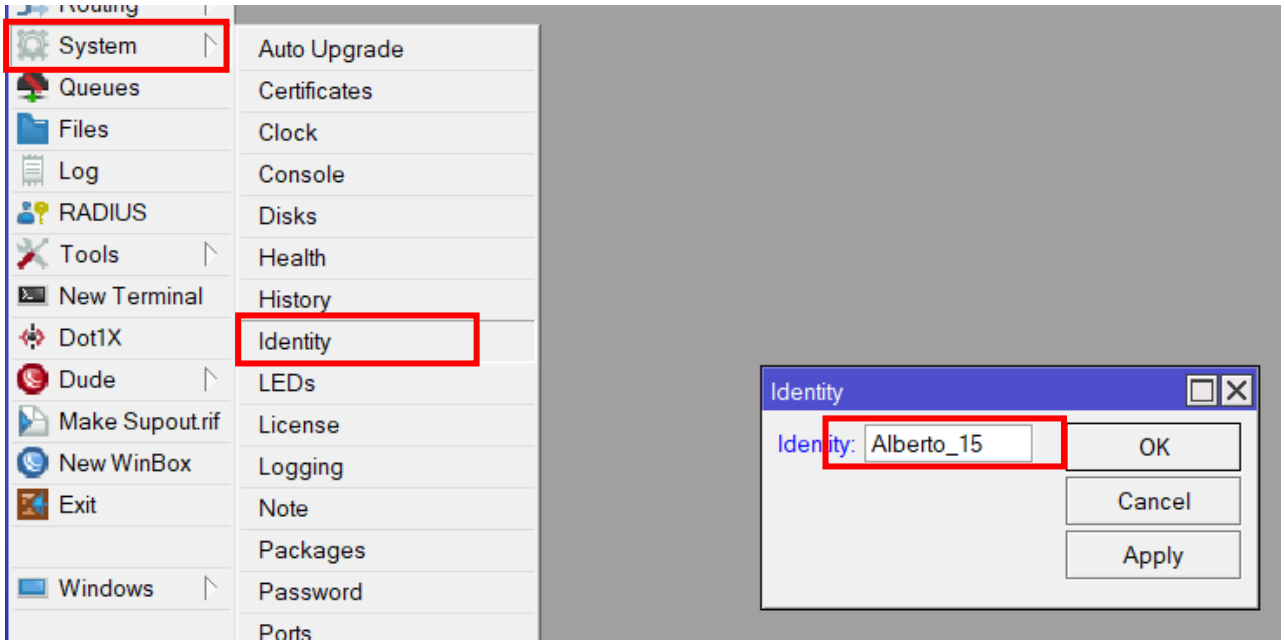

Рисунок 5.3. Ідентифікація маршрутизатора

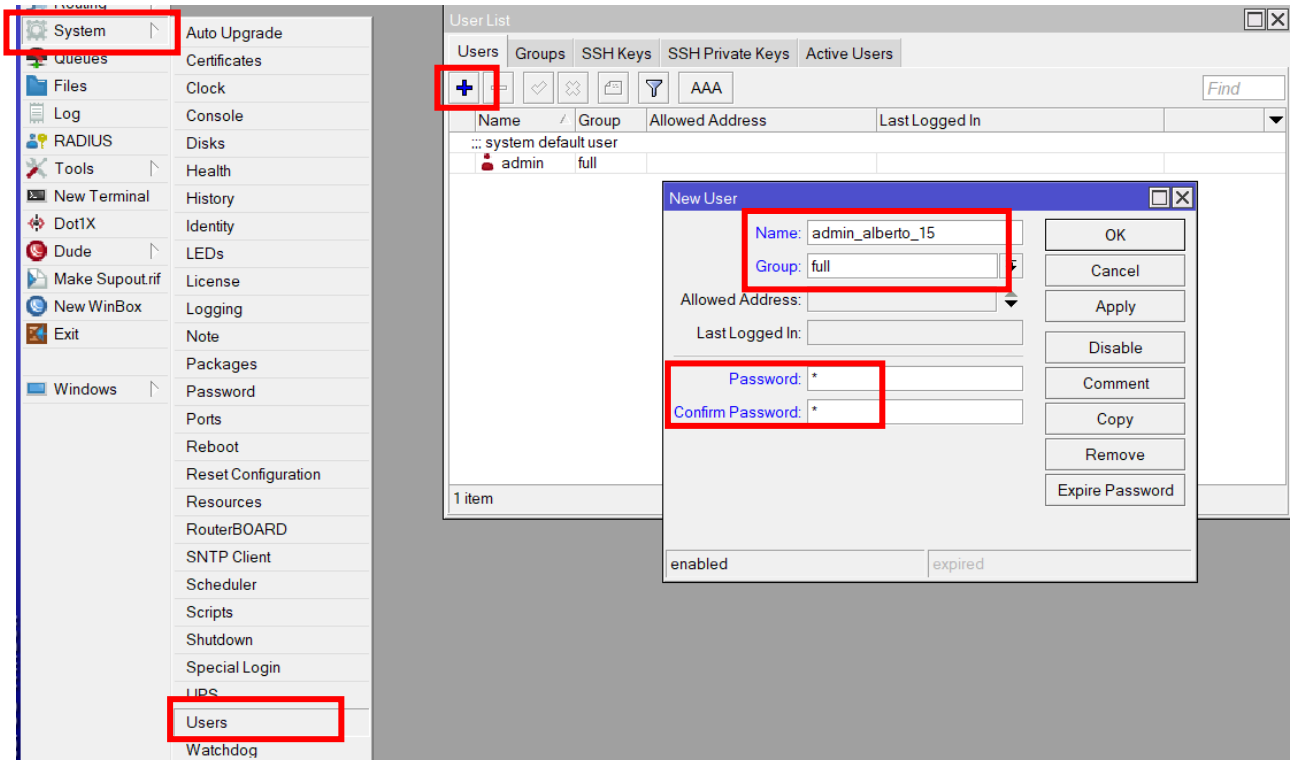

Рисунок 5.4. Ідентифікація маршрутизатора

5. Об’єднайте всі, крім одного, проводові інтерфейси в локальну мережу (пул адрес: 172.30.X.0/24), як наведено на рисунках 5.5-5.7. Зробіть ***скріншот.***

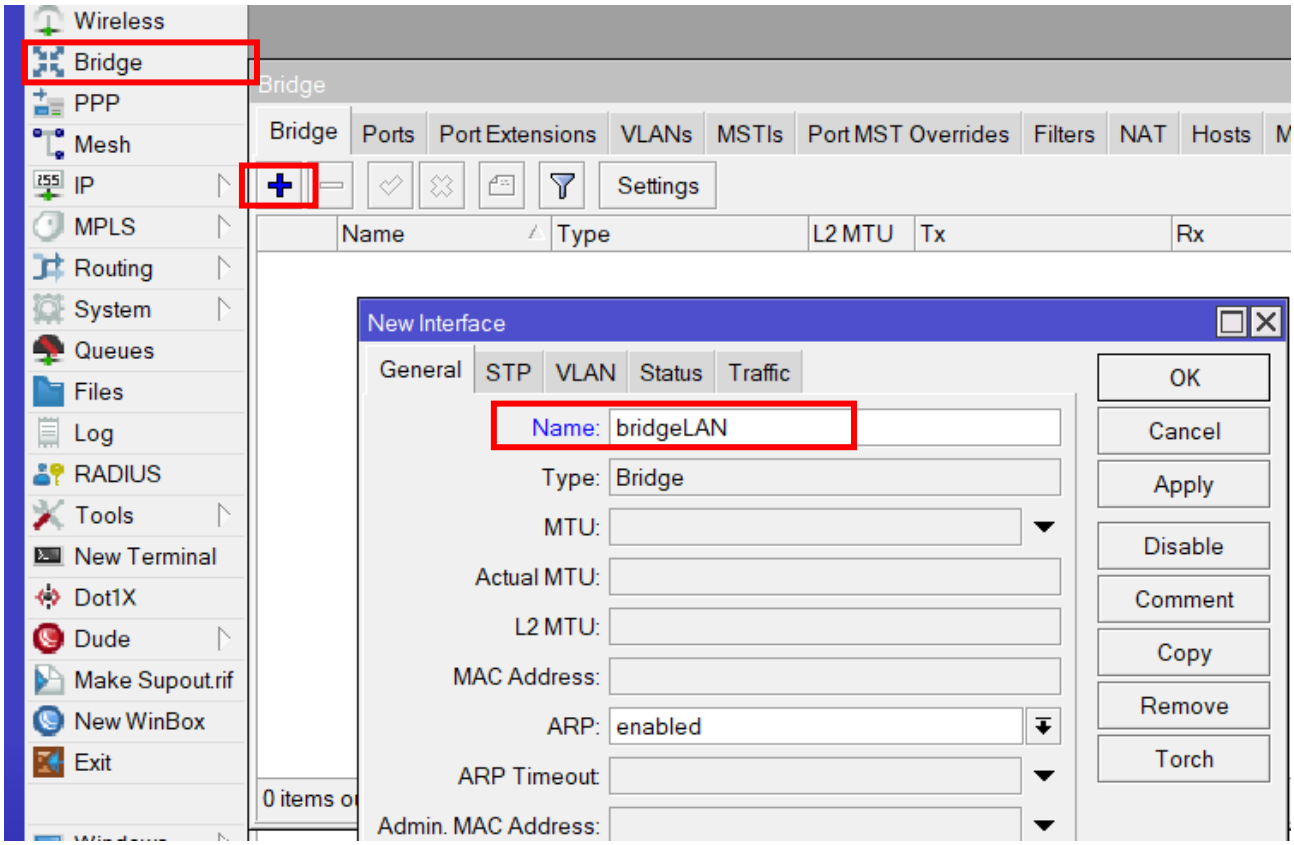

Рисунок 5.5. Створення bridge

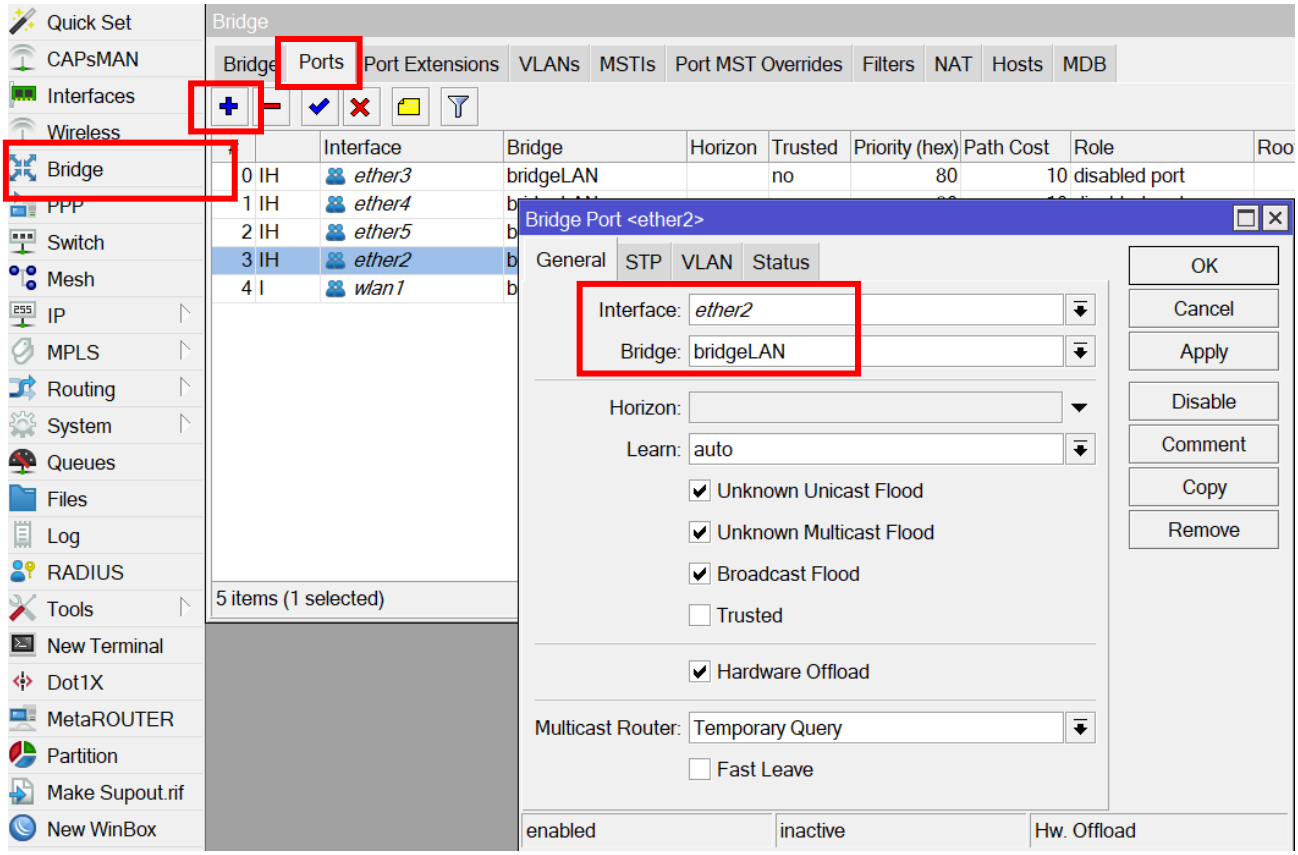

Рисунок 5.6. Почергове додавання портів до bridge

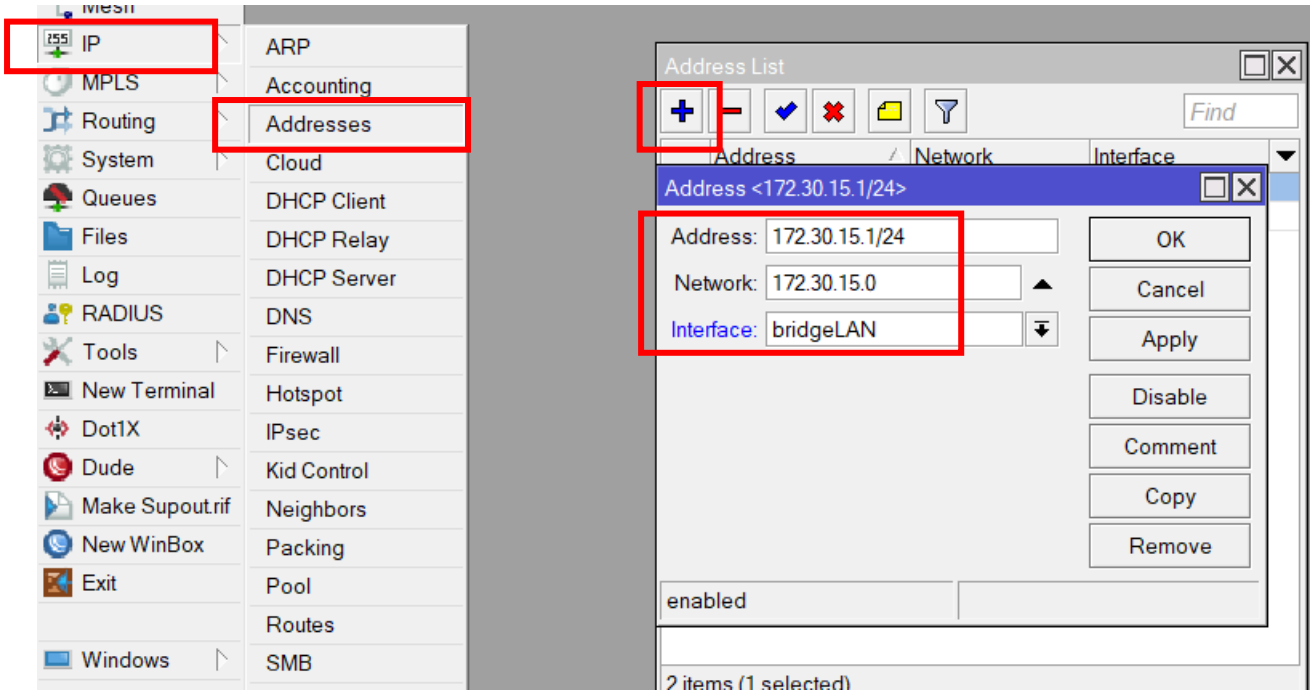

Рисунок 5.7. Присвоєння IP-адреси на bridge

6. Налаштуйте IP-адресу одному з інтерфейсів для виходу в глобальну мережу (адреса: 192.168.3.1X/24), як наведено на рисунку 5.8. Зробіть ***скріншот.***

Примітка. *Це може змінюватись залежно від налаштувань провайдера.*

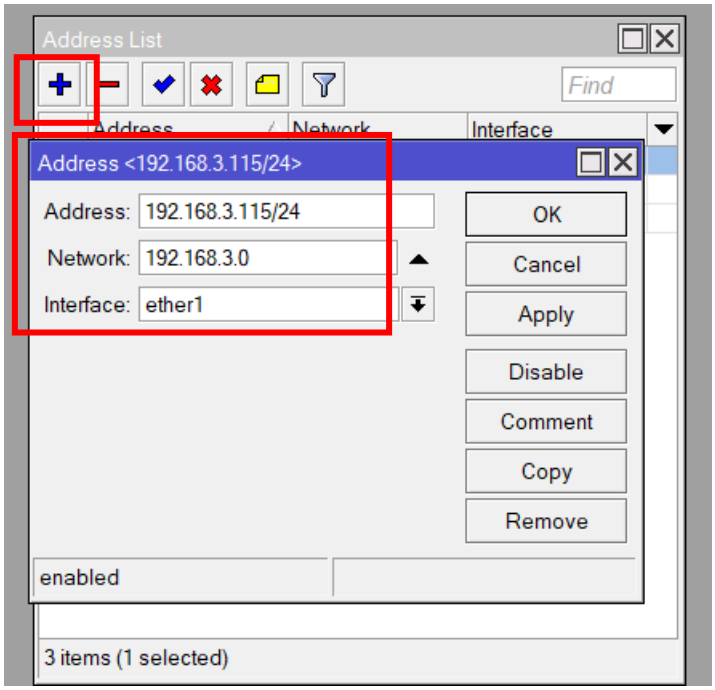

Рисунок 5.8. Присвоєння IP-адреси на bridge

7. Налаштуйте DNS. ***192.168.3.1*** як сервер для Вашого маршрутизатора. Це залежить від провайдера. Також ваш маршрутизатор повинен виконувати функції DNS-сервера для локальної мереж, як наведено на рисунку 5.9. Зробіть ***скріншот.***

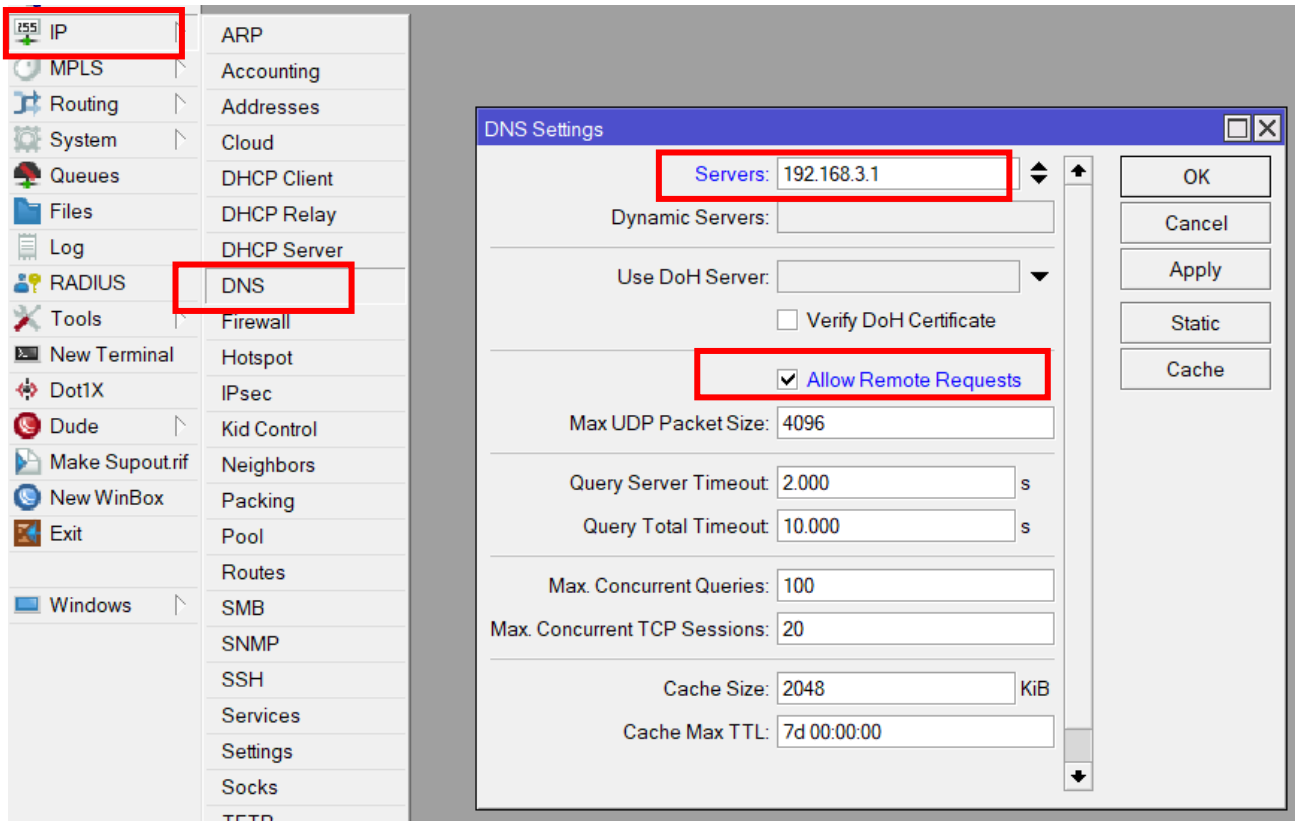

Рисунок 5.9. Налаштування DNS

8. Налаштуйте DHCP-сервер для локальної мережі, як наведено на рисунку 5.10, перевірте його роботу (на маршрутизаторі в **“*Leases*”** (зробіть ***скріншот***) та на ПК через ***ipconfig***, зробіть ***скріншот).***

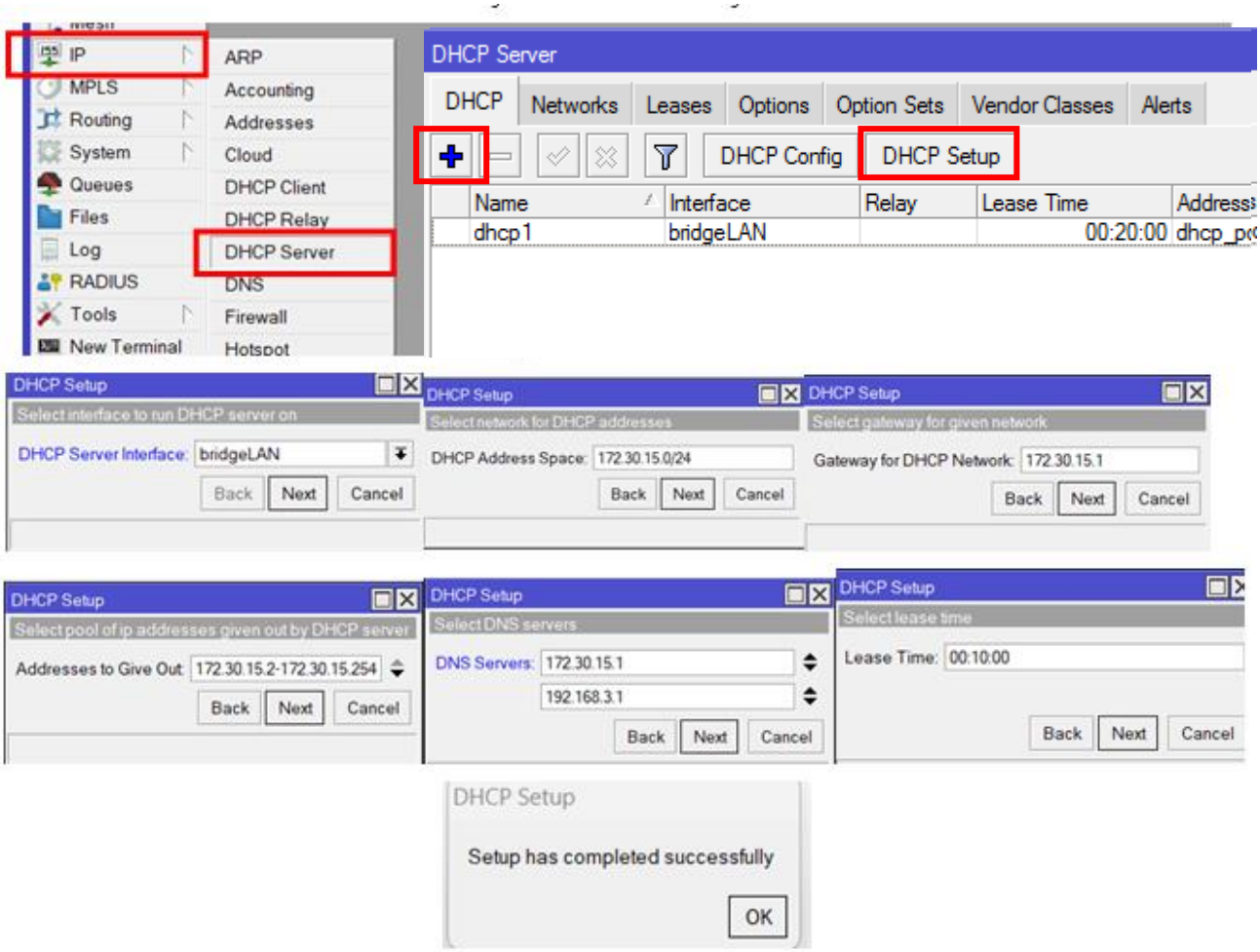

Рисунок 5.10. Налаштування DHCP

9. Вкажіть маршрут за замовчуванням (*default-gateway:192.168.3.1*), як наведено на рисунку 5.11. Залежить від провайдера. Зробіть ***скріншот.***

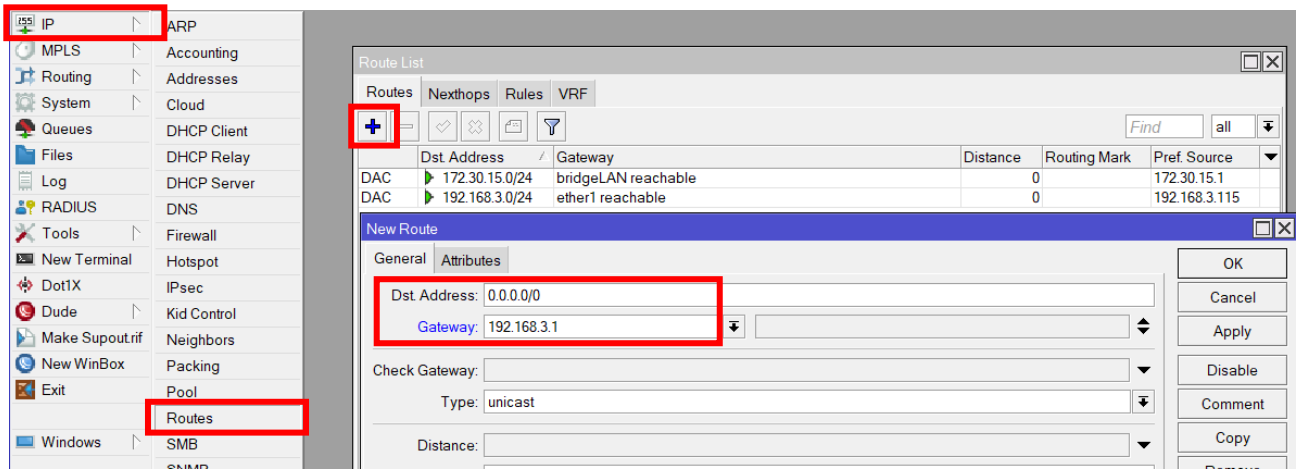

Рисунок 5.11. Налаштування маршруту за замовчуванням

10. Налаштуйте NAT, як наведено на рисунку 5.12, перевірте й покажіть наявне інтернет-з'єднання з маршрутизатора та з ПК, зробіть ***скріншоти***.

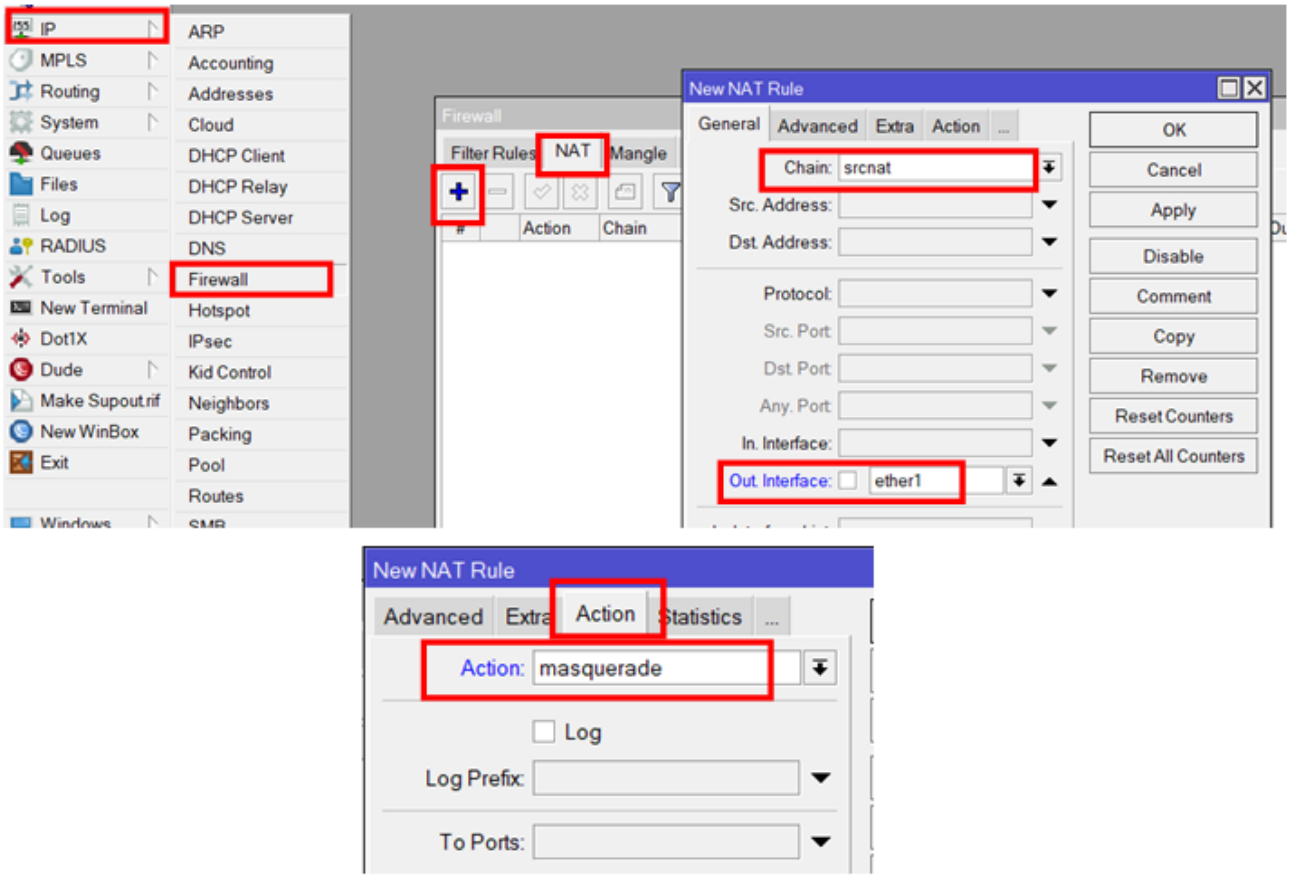

Рисунок 5.12. Налаштування правила NAT

11. Під час виконання лабораторної роботи до кожного пункту зробіть необхідні скріншоти повного вікна Winbox чи CLI ПК та/або маршрутизатора. Зробіть звіт, надішліть викладачу.

Контрольні питання

1. Що таке DNS? Його роль в маршрутизаторах MikroTik.
2. Що таке DHCP? Його роль в маршрутизаторах MikroTik.
3. Що таке default-gateway?
4. Поясніть, що таке bridge-інтерфейс в MikroTik.
5. Що таке NAT? Його роль в маршрутизаторах MikroTik.
6. Як перевірити наявність виходу в мережу інтернет на маршрутизаторі та на ПК ?

ЛАБОРАТОРНА РОБОТА №6
НАЛАШТУВАННЯ VPN-З'ЄДНАННЯ (L2TP)

Мета:

1) ознайомитися з видами VPN-з'єднань (тунелів), їх можливостями та порядком створення на пристроях MikroTik;

2) отримати практичні навички з налаштування L2TP на пристроях MikroTik.

Для виконання цієї лабораторної роботи вам необхідно мати два налаштованих маршрутизатори з підключенням до інтернету (рис. 6.1). Схема зв'язку буде подібною до наведеної на рисунку нижче. У вас можуть відрізнятися IP-адреси на реальному обладнанні, головна вимога – один з маршрутизаторів, який буде виступати в ролі сервера, повинен мати «білу» IP-адресу. Під час виконання роботи на реальному обладнанні білу IP-адресу L2TP-сервера дізнайтесь у викладача. Якщо ви виконуєте схему в емуляторах GNS3 або EVE – зберіть таку саму схему, білу IP-адресу призначте самостійно довільно. LAN-мережу лівого маршрутизатора задайте у форматі: 172.30.X.0/24 (де *X* – ваш номер за списком.)

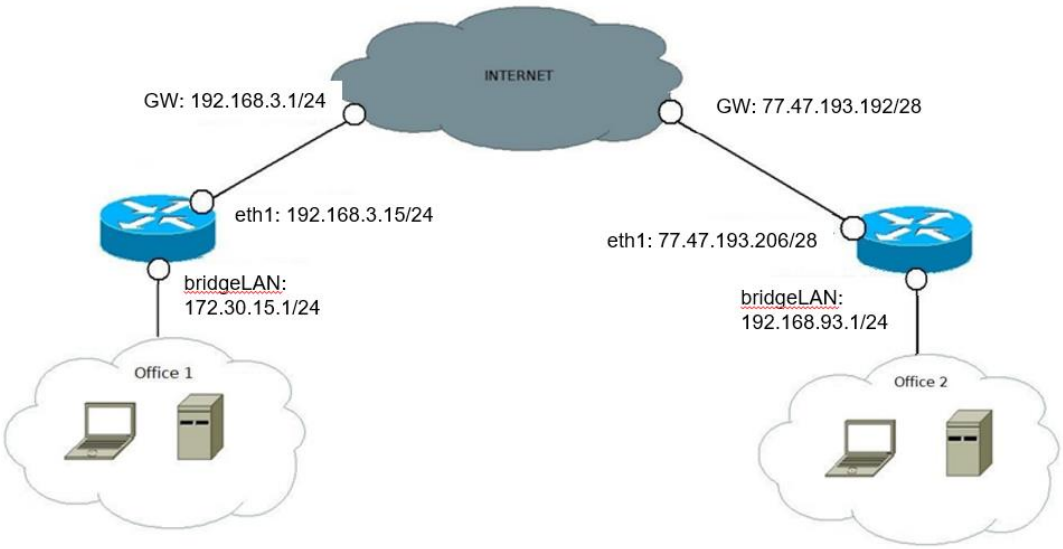

Рисунок 6.1. Схема з'єднань маршрутизаторів для побудови VPN

Хід роботи

5.1 Налаштування L2TP-сервера

1. На маршрутизаторі, що виступає сервером та має **“білу”** IP-адресу (на рисунку справа) перейдіть на вкладку **“PPP”** та додайте нового користувача (рис. 6.2). Зверніть увагу на **“Local”** та **“Remote”** адреси, вони мають 32-бітну маску та будуть використовуватись для маршрутизації через L2TP тунель. І запам’ятайте пароль, який буде використано на клієнті для автентифікації. Зробіть ***скріншот***.

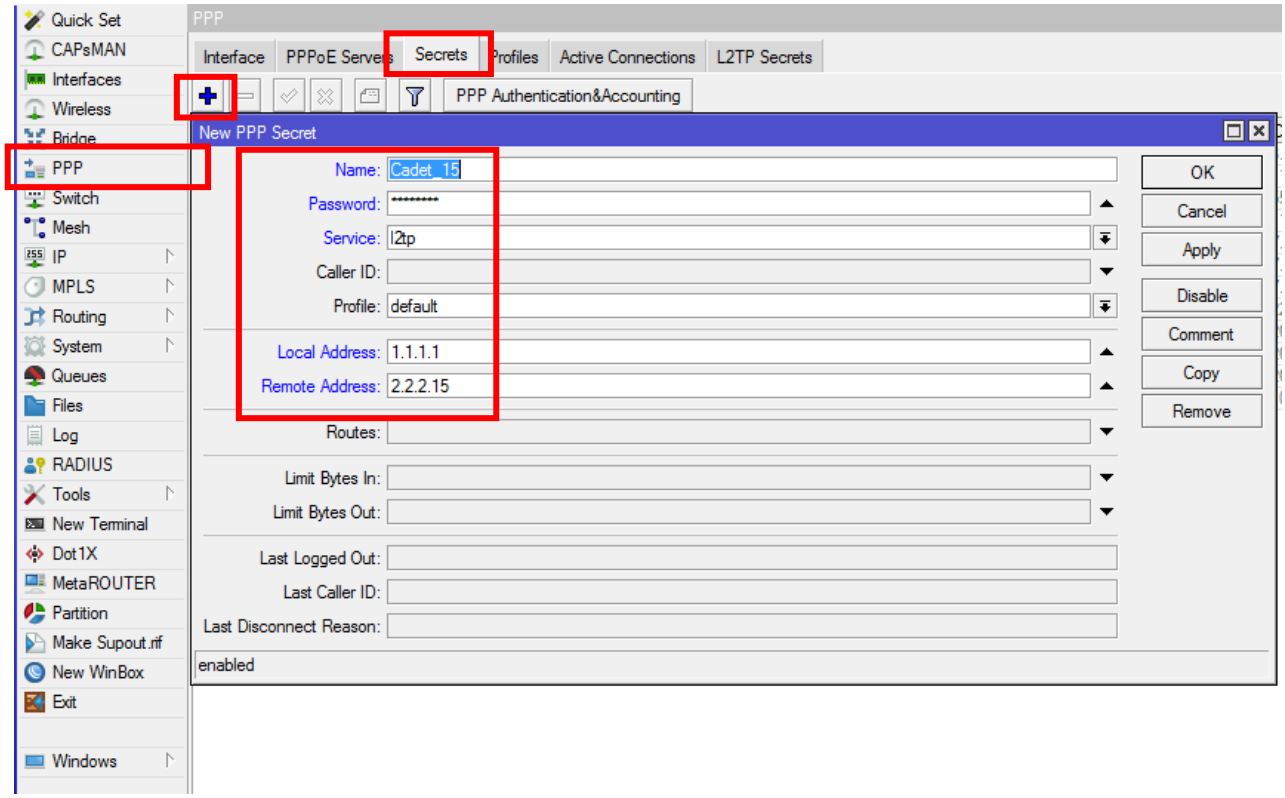

Рисунок 6.2. Налаштування користувача на L2TP-сервері

2. На тій самій вкладці **“PPP”** оберіть **“L2TP Server”** та виставте налаштування, як наведено на рисунку 6.3. Обов’язково виберіть профіль з шифруванням **(“default-encryption”)** або створіть новий. Зробіть ***скріншот***.

3. Перейдіть на вкладку **“IP”** > **“Routes”** та пропишіть новий маршрут із сервера в мережу L2TP-клієнта (як шлюз використовуйте **“Remote Address”** з

пункту 1 цієї лабораторної роботи), як наведено на рисунку 6.4. Шлюз не стане доступним, а маршрут – активним, поки не буде проведено відповідних налаштувань на клієнті. Зробіть ***скріншот***.

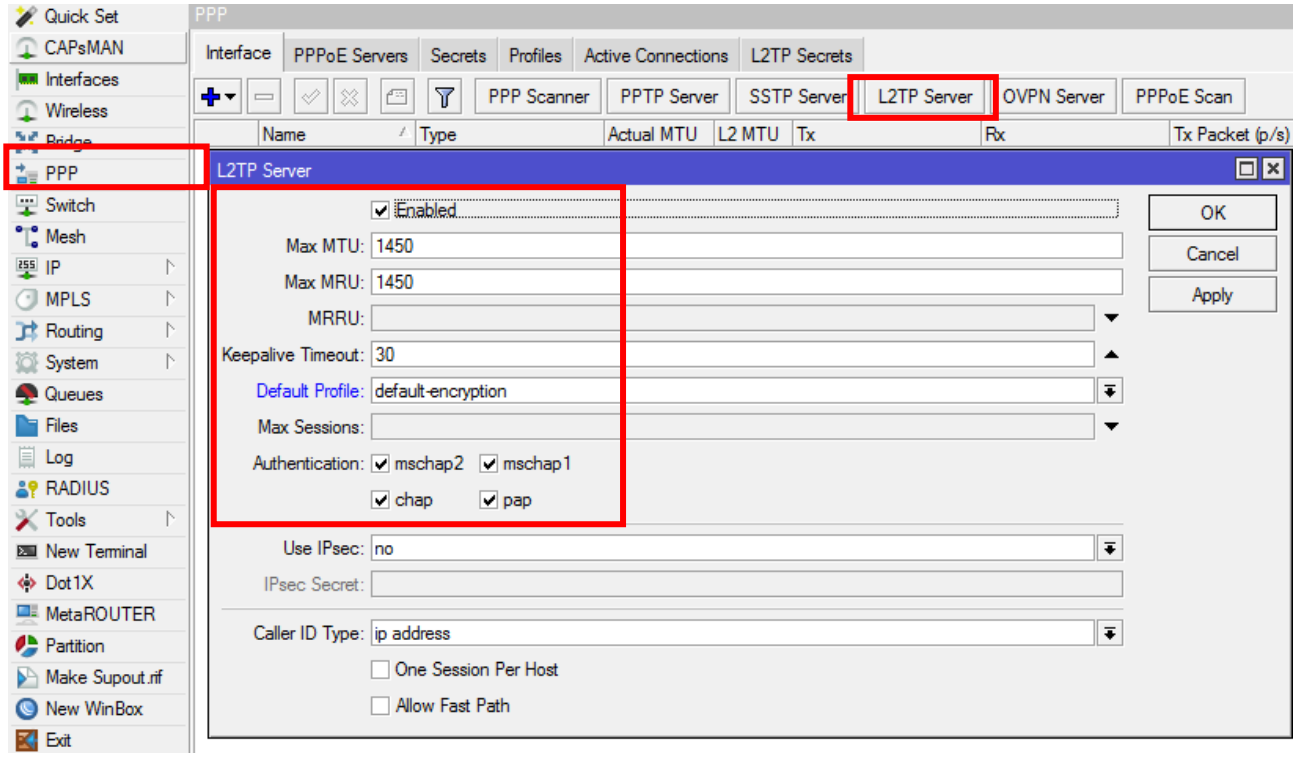

Рисунок 6.3. Налаштування користувача на L2TP-сервері

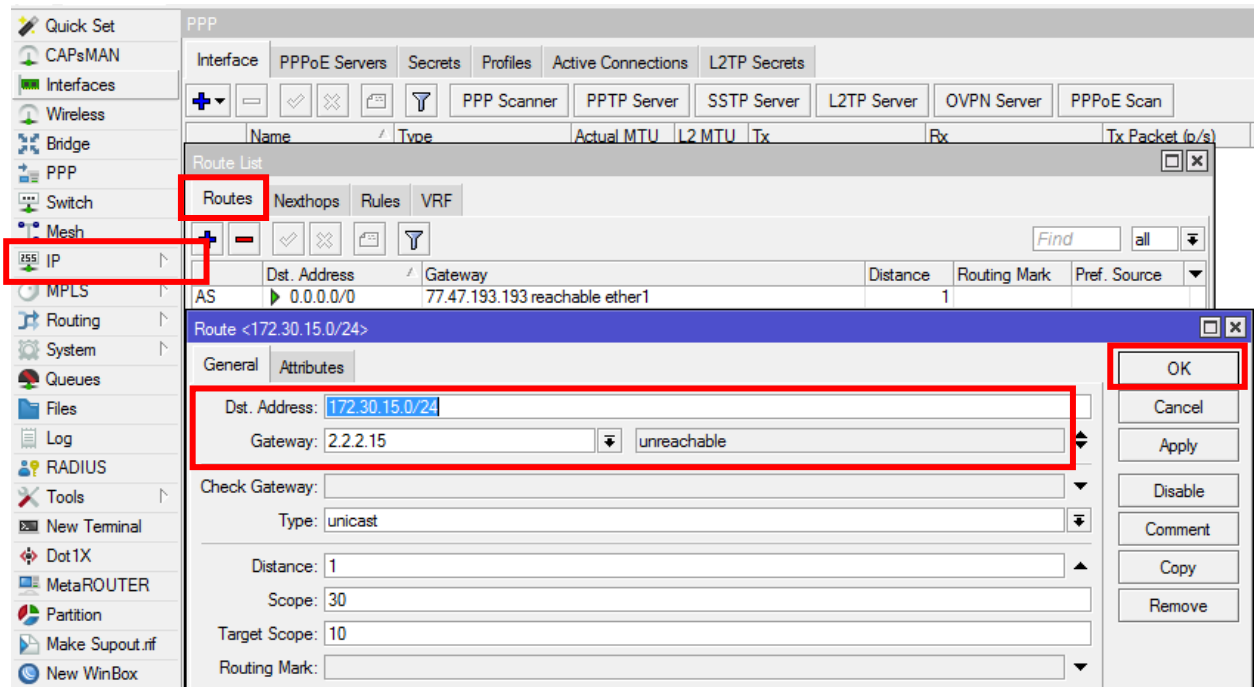

Рисунок 6.4. Налаштування маршруту на L2TP-сервері

5.2 Налаштування L2TP-клієнта

1. На маршрутизаторі, що виступає клієнтом (на рис. 6.1 – зліва) перейдіть на вкладку **“PPP”** та додайте новий інтерфейс **“L2TP Client”**. Далі на вкладці **“Dial Out”** (рис. 6.5) вкажіть **«білу»** IP-адресу сервера, у полі **“User:”** – ім’я користувача, створеного на сервері, і в полі **“Password:”** – відповідний пароль, **“Profile: default-encryption”**. Зробіть ***скріншот***.

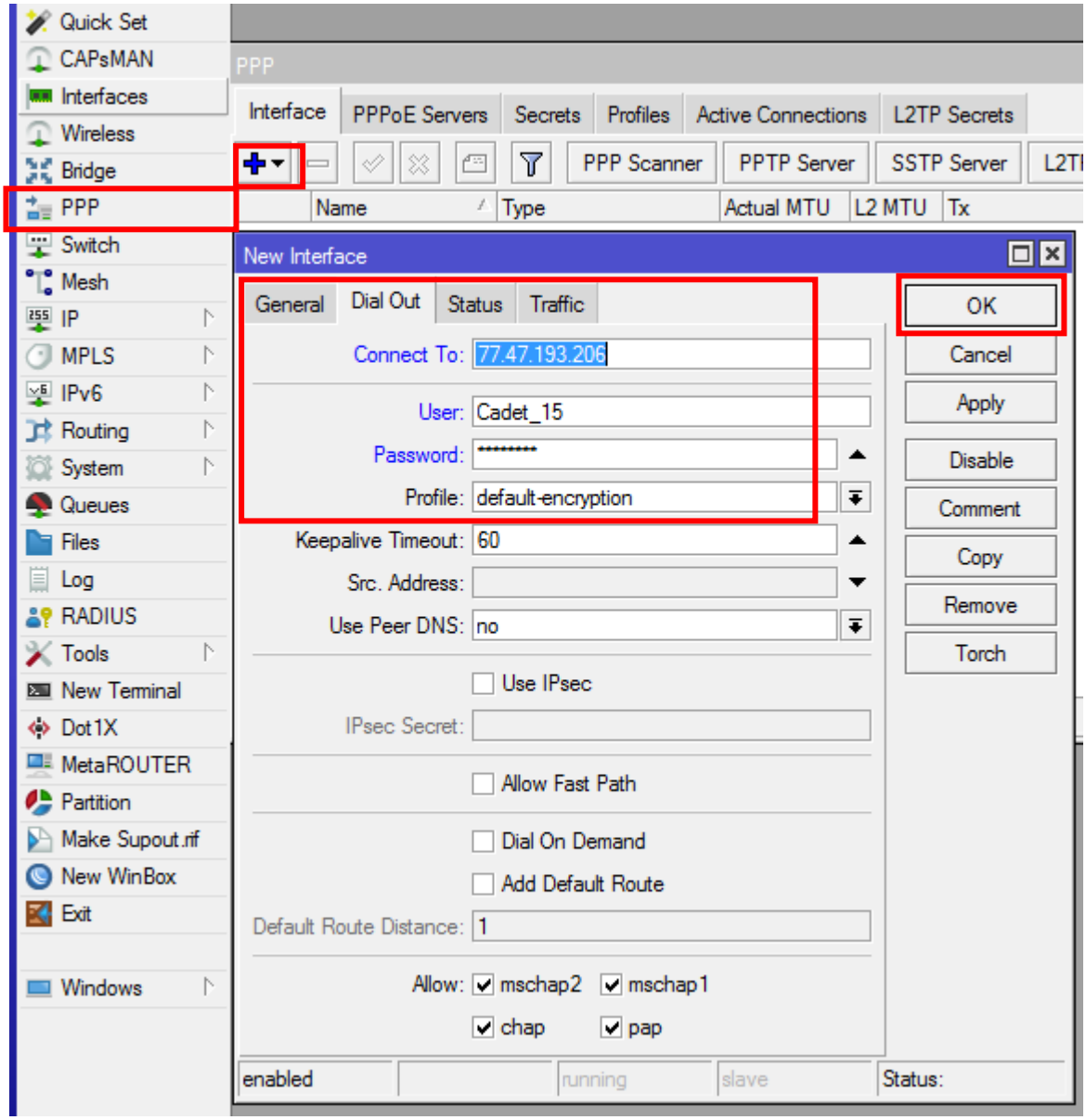

Рисунок 6.5. Налаштування підключення на L2TP-клієнті

2. Переконайтесь, що ваше з'єднання встановлено на вкладці **"PPP-Interfaces"** (з'явиться інтерфейс з прапорцем **"R"**). Зробіть ***скріншот***. Ви можете перейменувати свій інтерфейс або закоментувати, як наведено на рисунку 6.6:

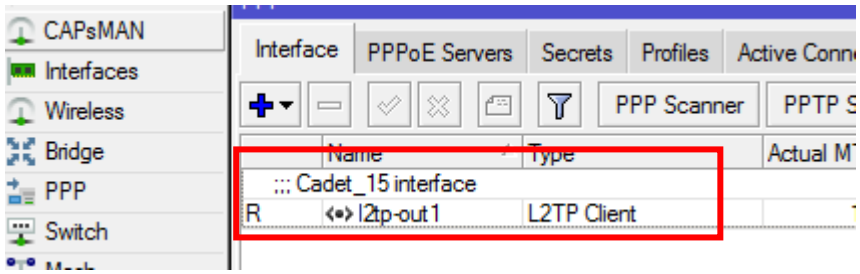

Рисунок 6.6. Активний динамічний L2TP-інтерфейс на L2TP-клієнті

3. Перейдіть на вкладку **"IP"** > **"Routes"** та пропишіть новий маршрут із клієнта в локальну мережу L2TP-сервера (шлюз – Local Address із сервера), як наведено на рисунку 6.7. Якщо все зроблено правильно, то після натиснення **"Apply"** шлюз стане доступним. Зробіть ***скріншот***. Натисніть **"ОК"**.

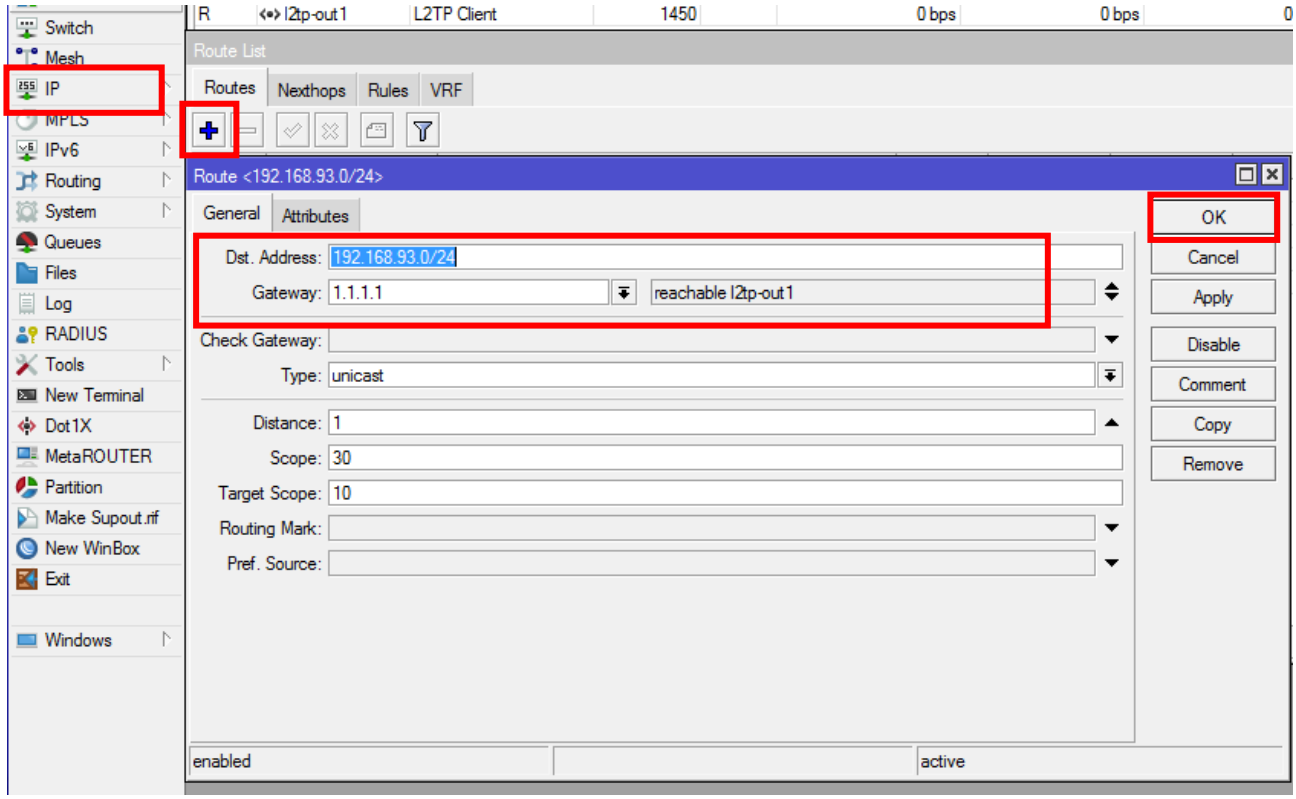

Рисунок 6.7. Налаштування маршруту на L2TP-клієнті

4. У списку маршрутів з’явився новий активний статичний маршрут в локальну мережу сервера. Прокоментуйте його (за допомогою жовтого аркуша), подібно до того, як наведено на рисунку 6.8. Зробіть ***скріншот***.

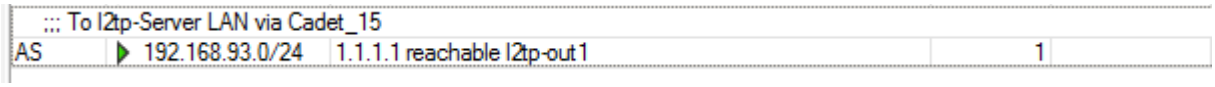

Рисунок 6.8. Налаштування маршруту на l2tp-клієнті

5. Перевірте доступність локальної мережі сервера з клієнта за допомогою **“ping”** з терміналу (рис. 6.9) та через утиліту **“ping”** графічного інтерфейсу (рис. 6.10). Зробіть ***скріншоти***.

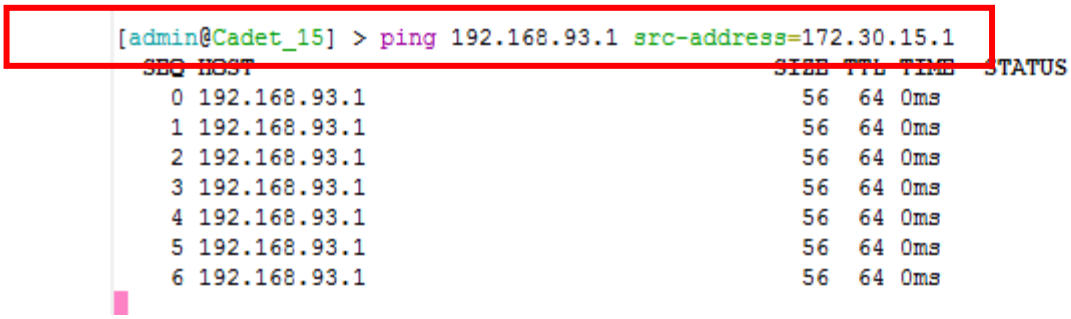

Рисунок 6.9. Ping через CLI

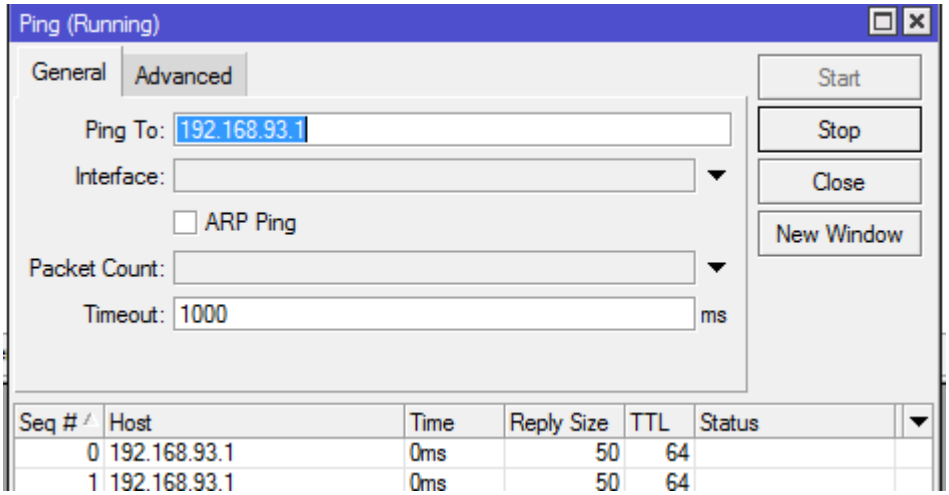

Рисунок 6.10. Ping через Tools>Ping

6. Аналогічно попередньому пункту, перевірте доступність локальної мережі клієнта з сервера за допомогою **“ping”** з терміналу та через утиліту **“ping”** графічного інтерфейсу. Зробіть ***скріншоти***.

Контрольні питання

1. Що таке VPN? На якому логічному порту він працює?
2. Які варіанти застосування VPN?
3. Які принципи роботи L2TP?
4. Який порядок налаштування L2TP-тунелю?
5. Яким чином можливо закоментувати маршрут?

ЛАБОРАТОРНА РОБОТА № 7
НАЛАШТУВАННЯ МАРШРУТИЗАТОРА MIKROTIK У РЕЖИМІ БЕЗПРОВОДОВОЇ ТОЧКИ ДОСТУПУ

Мета:

1) ознайомитися з режимами роботи безпроводових інтерфейсів на пристроях MikroTik;

2) отримати практичні навички з налаштування безпроводової мережі на пристроях MikroTik.

Для виконання цієї лабораторної роботи вам необхідно мати налаштований маршрутизатор з підключенням до інтернету (виконана лабораторна робота № 5).

Хід роботи

1. Для створення безпечного безпроводового з'єднання спочатку створіть профіль безпеки. Для цього перейдіть на вкладку **"Wireless" > "Security Profiles"**. Задайте назву профілю, пароль, оберіть динамічні ключі та тип аутентифікації, як наведено на рисунку 7.1. Зробіть ***скріншот***. Натисніть **"ОК"**.

2. Перейдіть на вкладку **"Wireless" > "Wi-Fi Interfaces"** та відкрийте налаштування першого безпроводового інтерфейсу подвійним натисканням миші. Натисніть кнопку **"Advanced Mode"**, щоб відкрити більше налаштувань, як наведено на рисунку 7.2.

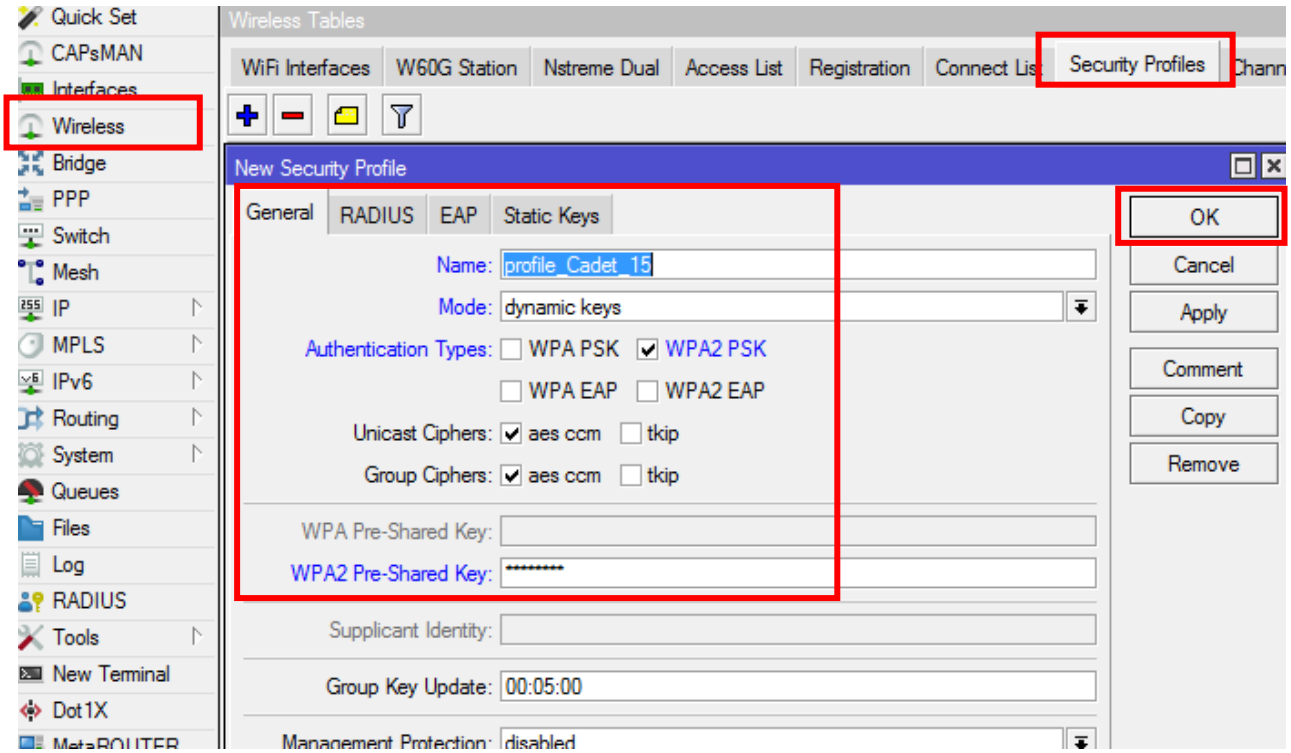

Рисунок 7.1. Створення профілю безпеки

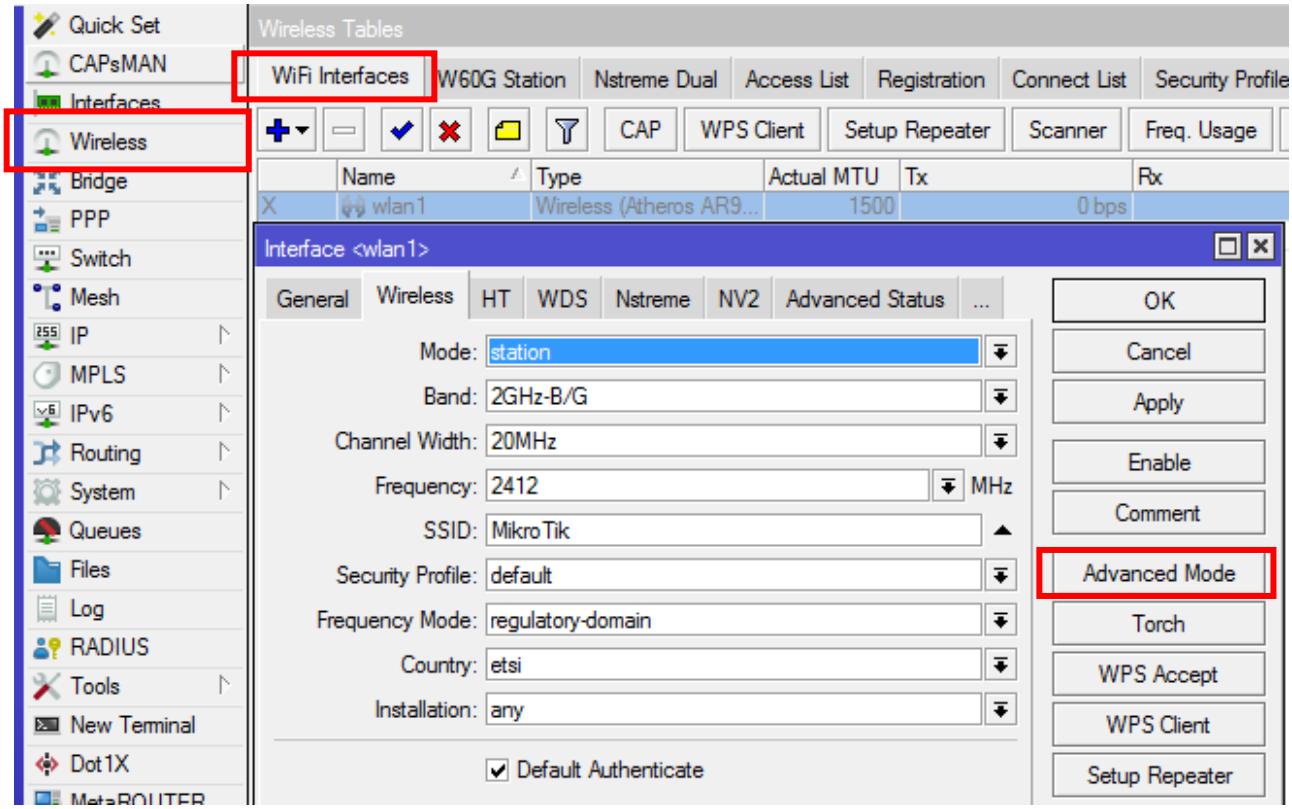

Рисунок 7.2. Перехід до розширених налаштувань безпроводового інтерфейсу

3. Натисніть кнопку **“Freq. Usage”**, потім **“Start”** та оберіть найменш зайняту частоту для подальшої роботи, наприклад, 2447, (рис. 7.3). Зробіть ***скріншот***. Після цього зупиніть сканер кнопкою **“Stop”**.

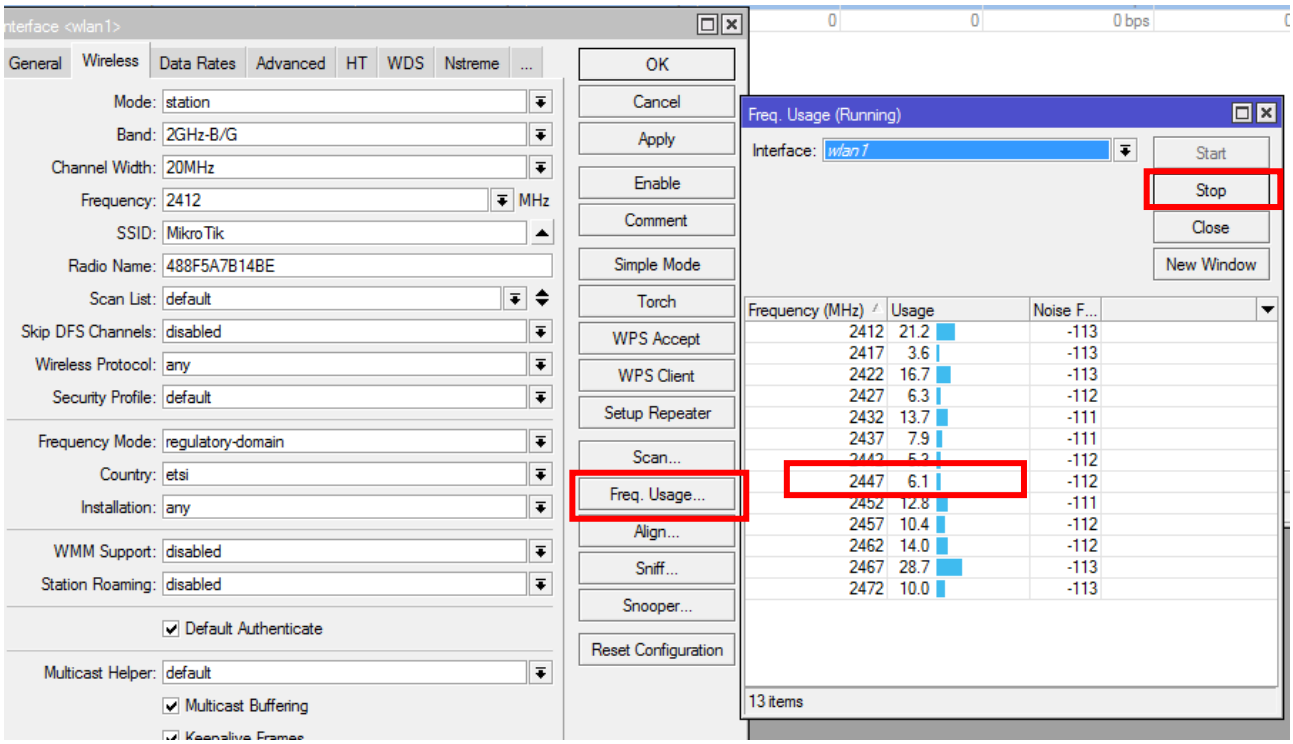

Рисунок 7.3. Вибір частоти

4. Перейдіть на вкладку **“Wireless” > “Wi-Fi Interfaces” > “Wireless”** та вкажіть наступні параметри: **“Mode: ap bridge”, “Frequency:** (з попереднього пункту)”, **“SSID: Cadet_X”, “Radio Name: Cadet_X”**, де X – ваш номер за списком, **“Wireless Protocol: 802.11”**, “**Secutiry Profile:** (оберіть зі списку створений вами профіль)”, **“Country: Ukraine”.** Натисніть **“Apply”** і після цього увімкніть інтерфейс кнопкою **“Enabled”,** як наведено на рисунку 7.4. Зробіть ***скріншот*.**

5. Спробуйте знайти вашу точку доступу зі смартфона чи ноутбука (за SSID), спробуйте підключитись. Чи вийшло? Як ви думаєте чому?

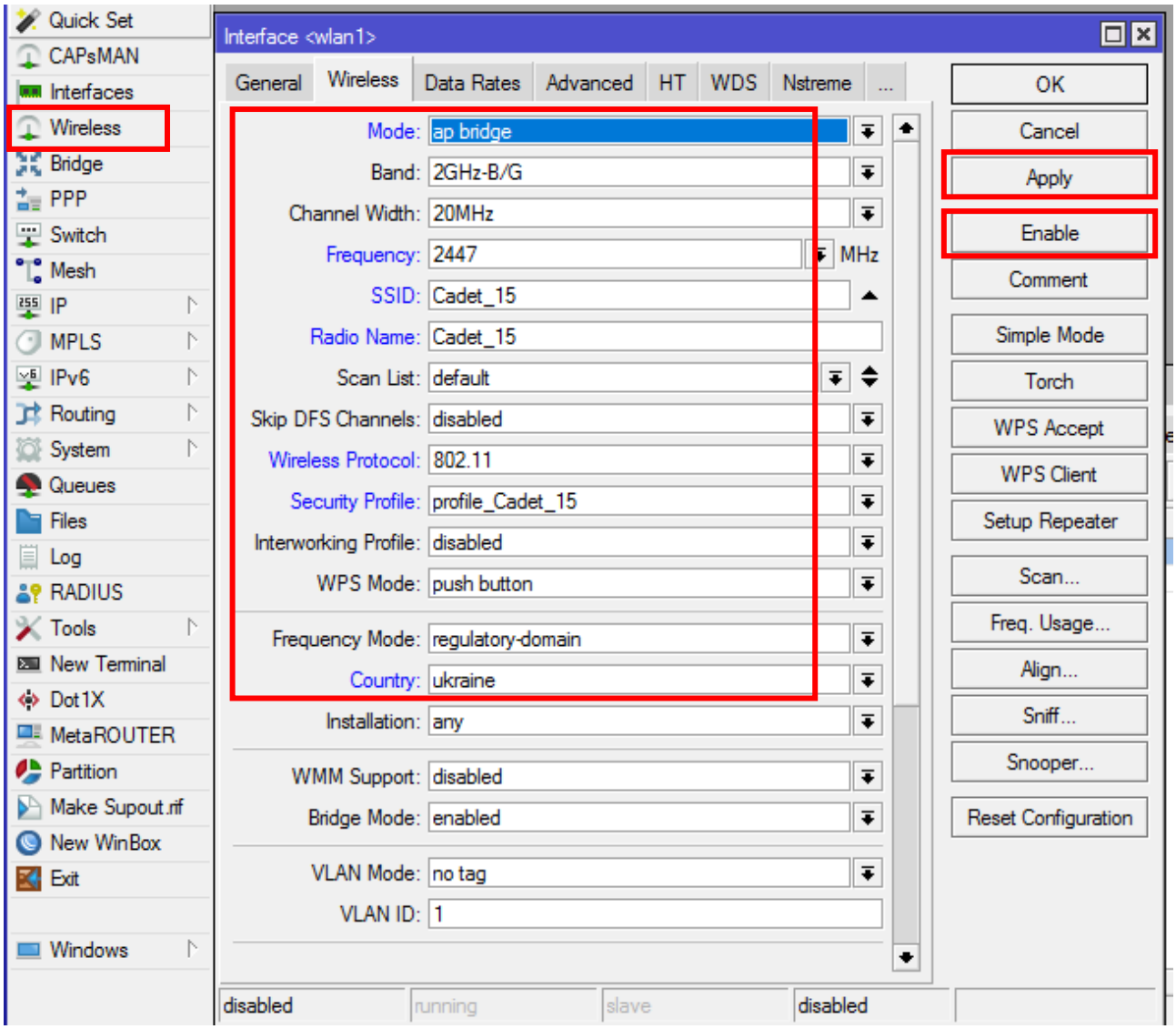

Рисунок 7.4. Налаштування безпроводового інтерфейсу в режимі точки доступу

6. Перейдіть на вкладку **“Bridge” > “Ports”** та додайте ваш налаштований безпроводовий інтерфейс до BridgeLAN, як наведено на рисунку 7.5. Натисніть **“ОК”**.

7. Спробуйте знайти вашу точку доступу зі смартфона чи ноутбука (за SSID), спробуйте підключитись. Чи вийшло цього разу? Перейдіть на вкладку **“Wireless” > “Wi-Fi Interfaces” > “wlan1” > “Traffic”.** Що ви тут бачите? Зробіть ***скріншот,*** як наведено на рисунку 7.6. *Як ви думаєте, що це означає?* Закрийте **“wlan1”**.

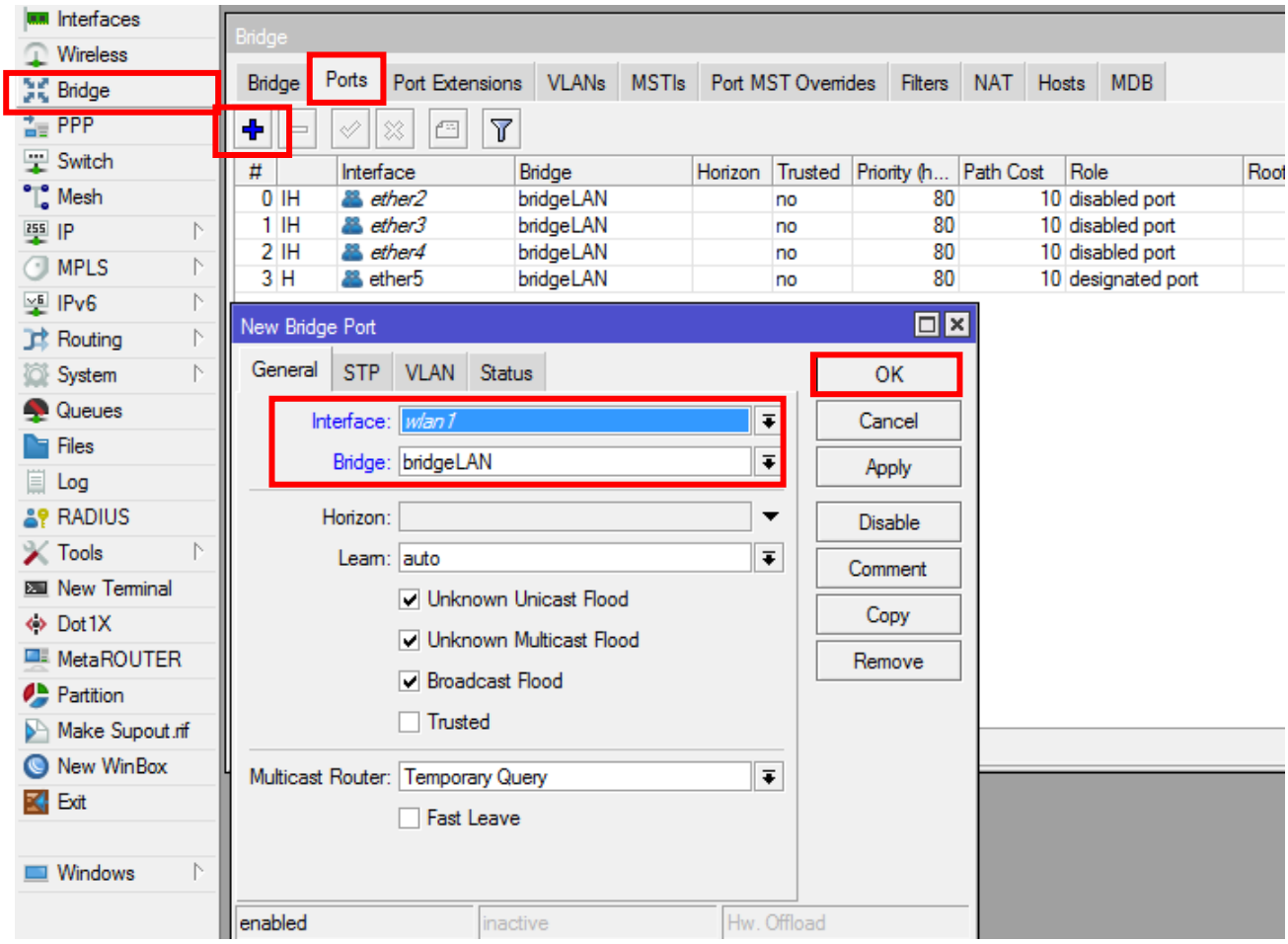

Рисунок 7.5. Додавання безпроводоводо інтерфейсу до “bridge”

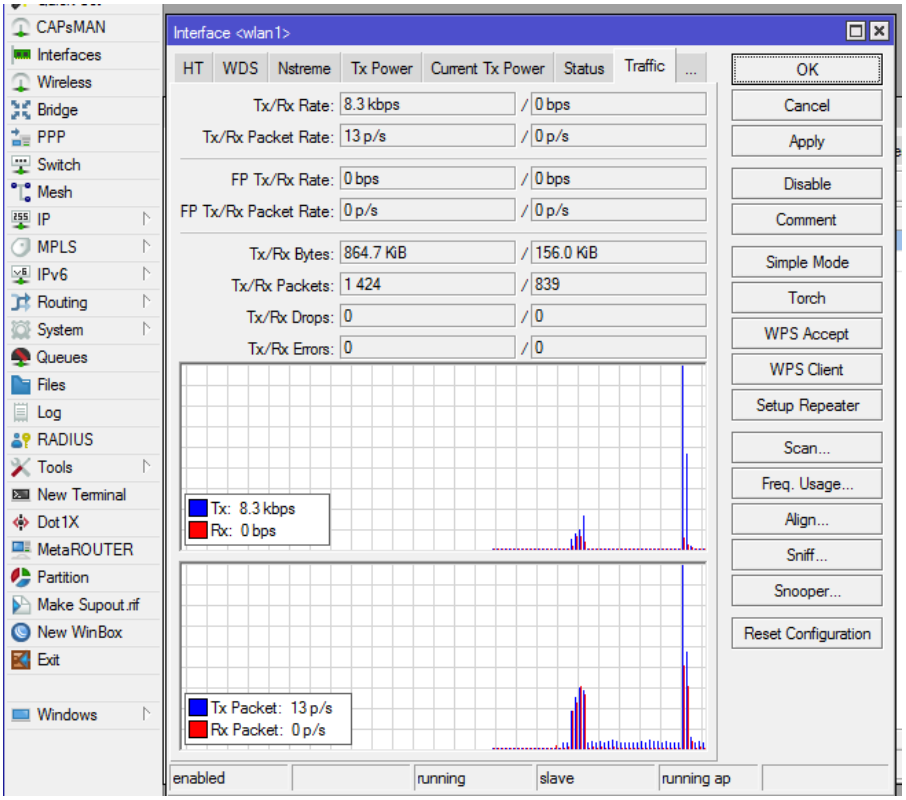

Рисунок 7.6. Вкладка “Traffic” на “wlan1”

8. Перейдіть на вкладку **“Wireless” > “Wi-Fi Interfaces” > “Registration”**, як наведено на рисунку 7.7. Скільки пристроїв підключено до точки доступу? Які в них MAC-адреси? Як довго вони підключені? Зробіть ***скріншот***.

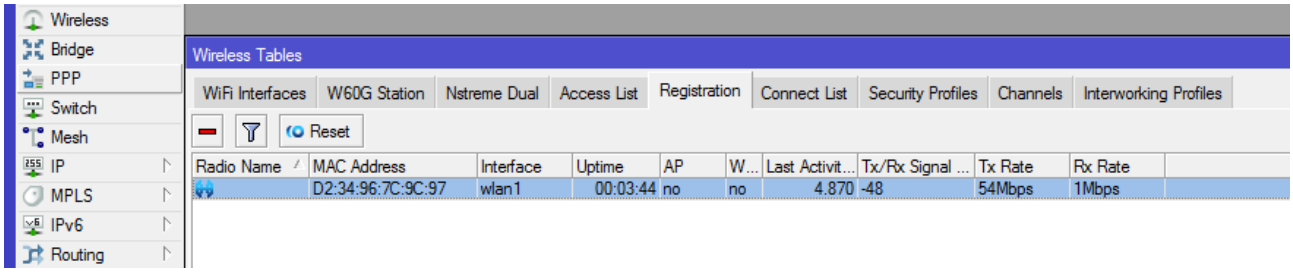

Рисунок 7.7. Вкладка “Registration”

9. Подвійним кліком миші відкрийте детальну інформацію про перший за списком підключений пристрій, як наведено на рисунку 7.8. Натисніть кнопку **“Copy to Access List”**, потім “**ОК**”.

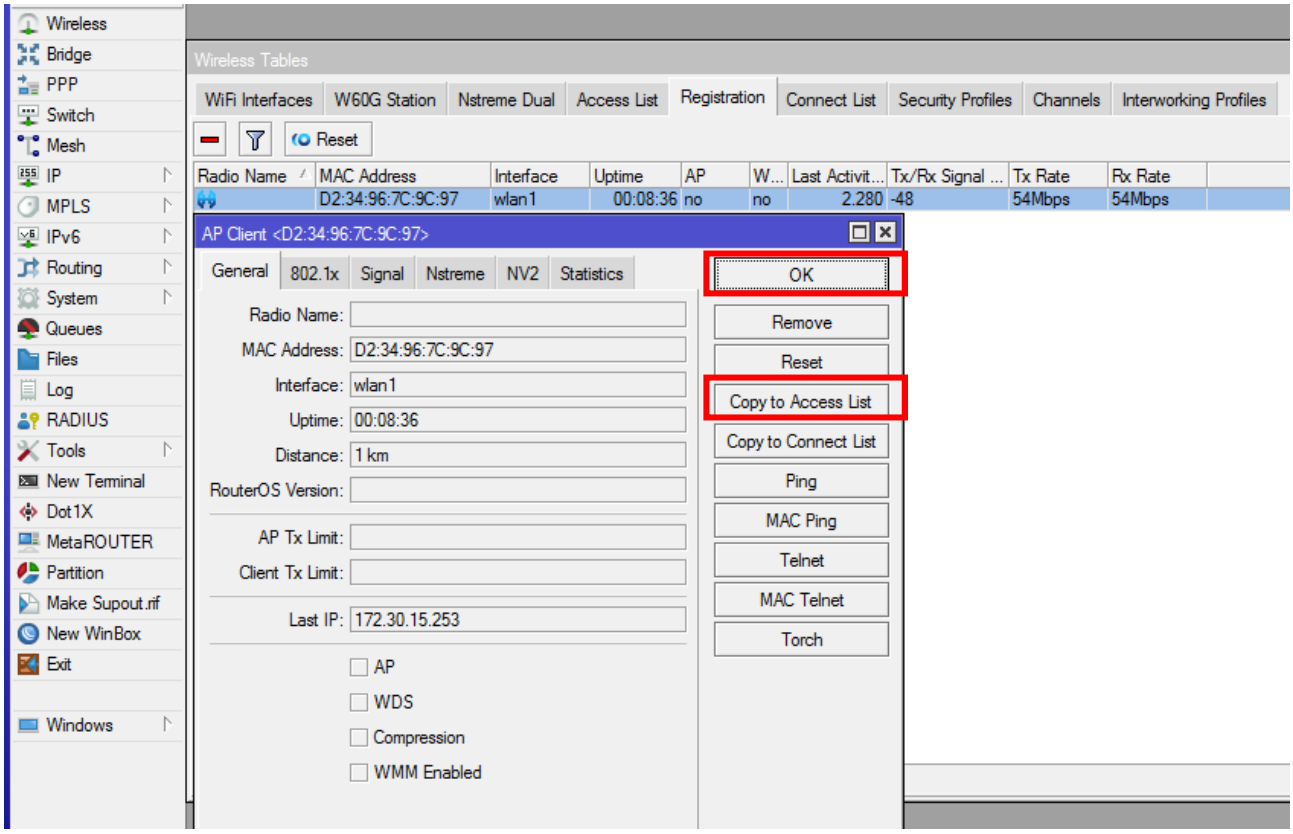

Рисунок 7.8. Детальна інформація про підключений пристрій

10. Перейдіть на вкладку **“Wireless” > “Access List”.** Перевірте, чи з’явився тут новий пристрій (рис. 7.9). Чим інформація на цій вкладці відрізняється від інформації на вкладці **“Registration”**?

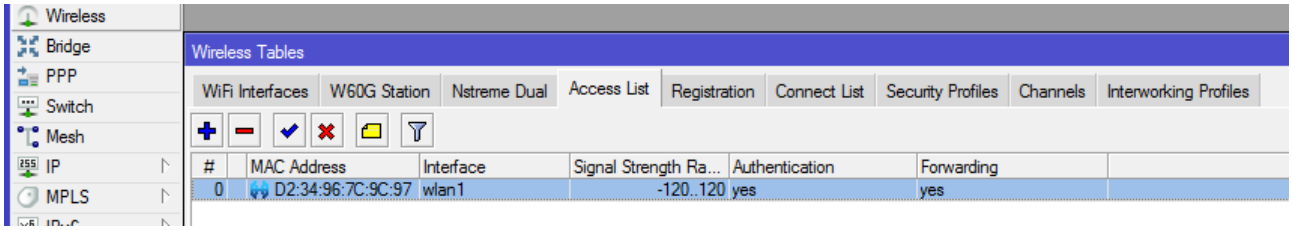

Рисунок 7.9. “Access List” безпроводового інтерфейсу

11. Перейдіть на **“Wireless” > “Wi-Fi Interfaces” > “wlan1”.** Знизу поставте галочку в полі **“Hide SSID”**, як наведено на рисунку 7.10. Зробіть ***скріншот***. Натисніть **“OK”**.

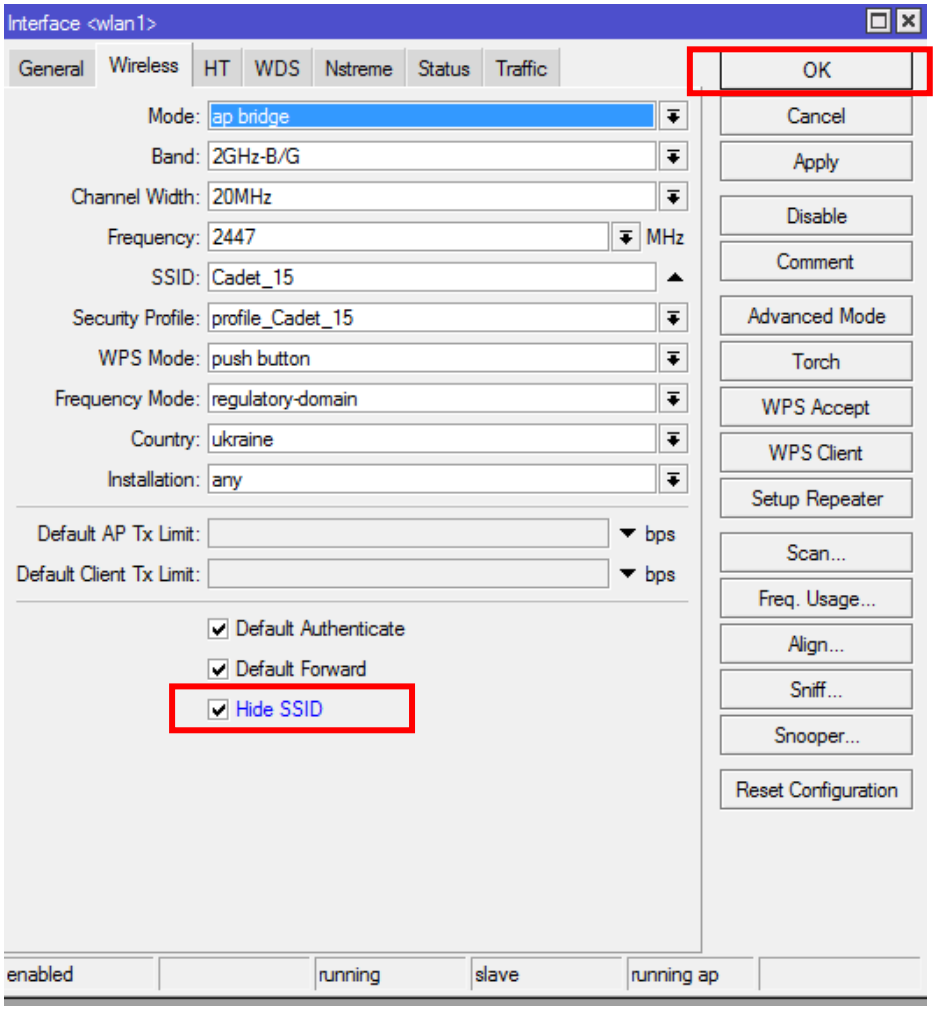

Рисунок 7.10. Hide SSID

11. Спробуйте відкрити перелік доступних безпроводових мереж іншим пристроєм (крім доданого до “Access List”) та знайти вашу точку доступу. Який результат? Чому? Приберіть галочку з поля **“Hide SSID”**. Натисніть **“OK”.**

12. Перейдіть на **“Wireless” > “Wi-Fi Interfaces” > “wlan1”.** Знизу приберіть галочку в полі **“Default Authenticate”**. Зробіть ***скріншот***, як наведено на рисунку 7.11. Натисніть **“OK”**.

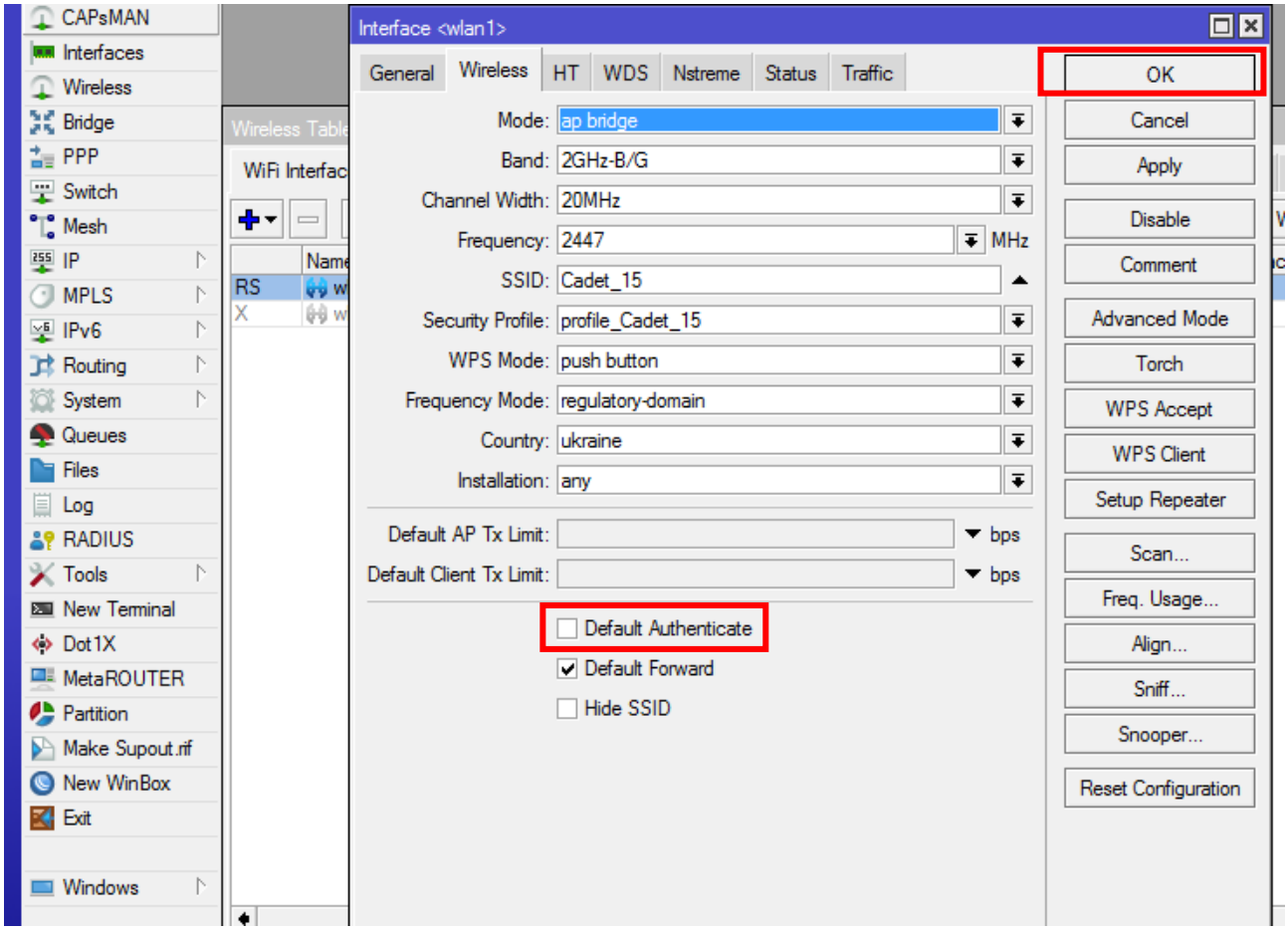

Рисунок 7.11. Default Authenticate

13. Спробуйте підключитись за вашим SSID іншим пристроєм (крім доданого до “Access List”). І знову тим пристроєм, який доданий до списку. Який результат? Чому?

14. Поверніть галочку з п.12 та повторіть п.13.

15. Вимкніть безпроводовий інтерфейс. Яким чином ви це зробили?

16. Зробіть звіт зі скріншотами й відповідями та надішліть викладачу.

Контрольні питання

1. Що таке Wi-Fi?
2. Діапазони роботи Wi-Fi.
3. Які стандарти Wi-Fi вам відомі?
4. Як забезпечити підключення з паролем до безпроводової точки доступу MikroTik?
5. Що таке Access-list у безпроводової точки доступу?
6. Які режими роботи безпроводового інтерфейсу MikroTik ви знаєте?
7. Як приховати SSID вашої точки доступу?

ЛАБОРАТОРНА РОБОТА № 8
НАЛАШТУВАННЯ ФАЄРВОЛА В MIKROTIK ROS

Мета:

1) ознайомитися з принципами функціонування фаєрволів на пристроях MikroTik;

2) отримати практичні навички з налаштування фаєрволів мережі на пристроях MikroTik.

Для виконання цієї лабораторної роботи вам необхідно мати налаштований маршрутизатор з підключенням до інтернету (виконана лабораторна роботи №5).

У цій роботі ви налаштуєте й перевірите працездатність декількох правил firewall (брандмауера) MiktoTik. Перед початком роботи підключіть за допомогою витої пари комп'ютер до інтерфейсу MikroTik, що входить у BridgeLAN.

Хід виконання

1. Створіть правило firewall: закрийте доступ на маршрутизатор від зовнішнього інтерфейсу (ether1) по *Winbox*. Який ланцюг треба обрати? Який порт?

1.1. Для цього перейдіть на **"IP" > "Firewall" > "Filter Rules" > "General".** Натисніть **"+"** та виставте значення полів, як наведено на рисунку 8.1. Зробіть ***скріншот***.

1.2 У цьому ж вікні перейдіть на вкладку **"Action"** та оберіть потрібну дію **"drop",** як наведено на рисунку 8.2. Що вона означає? Зробіть ***скріншот***. Натисніть **"ОК"**.

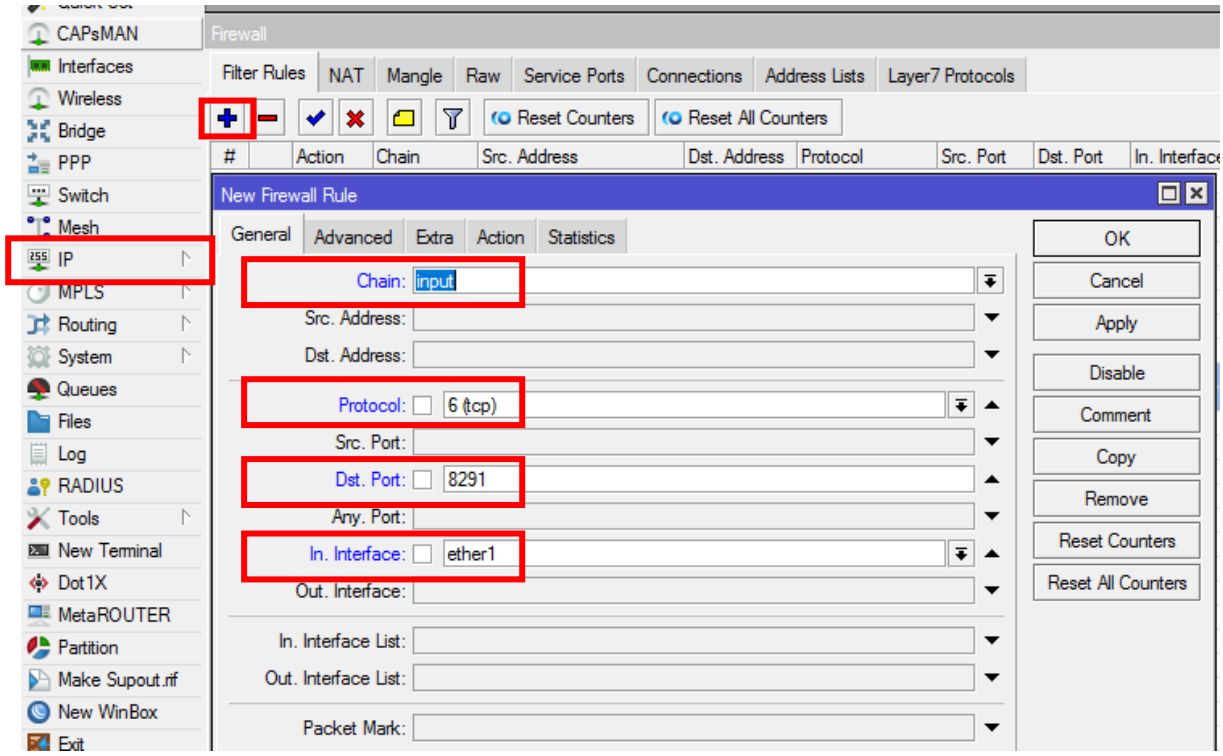

Рисунок 8.1. Створення правила для закриття доступу через Winbox з WAN

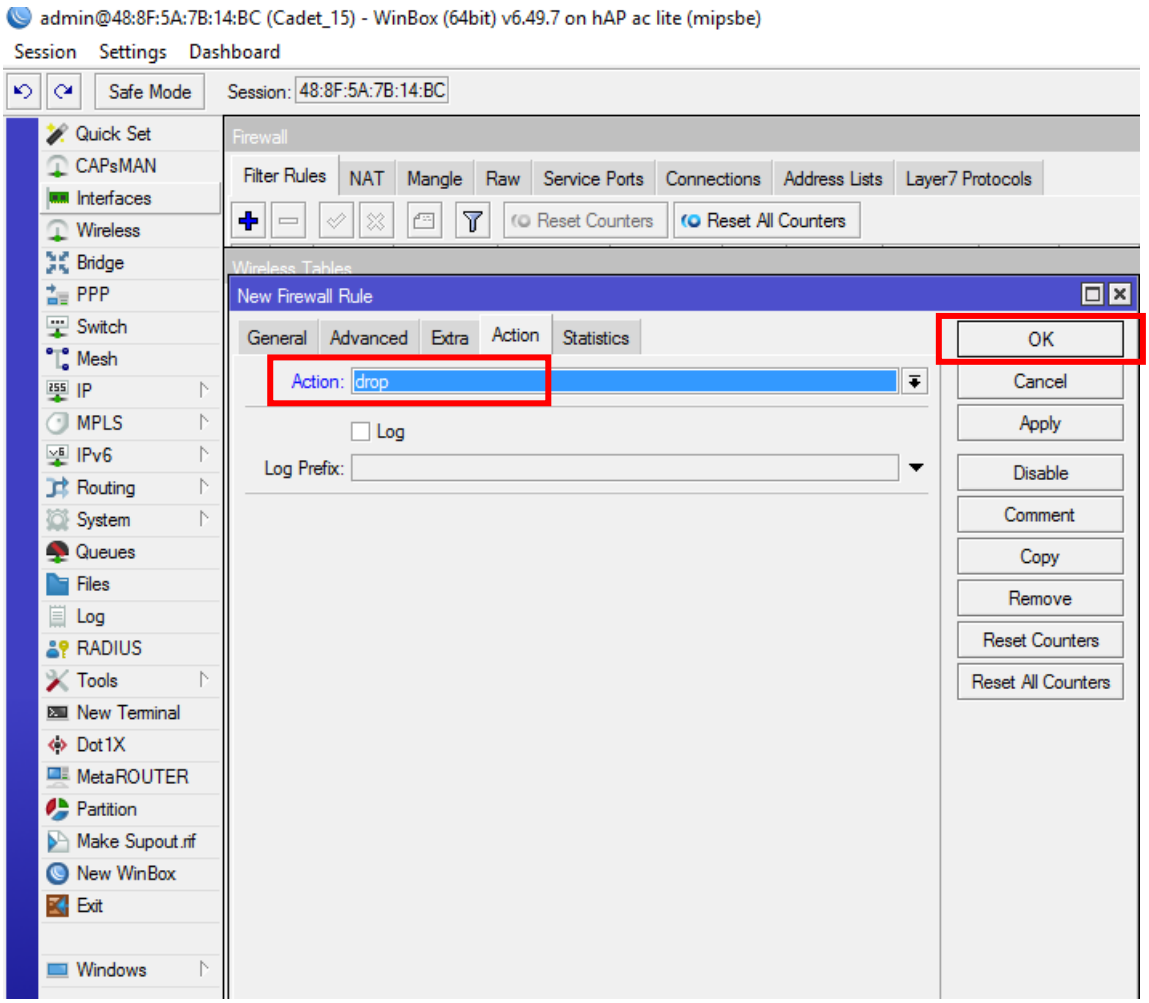

Рисунок 8.2. Вибір дії для забороняючого правила

1.3 У вікні **“IP” > “Firewall” > “Filter Rules”** перевірте, чи з’явилось нове правило, як наведено на рисунку 8.3. Зробіть ***скріншот***.

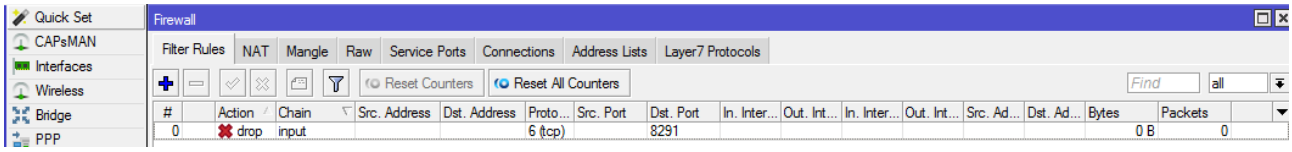

Рисунок 8.3. Перегляд нового правила

1.4 Від’єднайте кабель виту пару від маршрутизатора та увімкніть його в *ether1*. Спробуйте підключитись **за IP-адресою** на маршрутизатор через *Winbox*. Зробіть ***скріншот***. Поверніть виту пару від ПК у попереднє положення, а на *ether1* підключіть інтернет.

2. Створіть правило firewall: закрийте доступ в інтернет деяким “поганим” користувачам за IP-адресами (172.30.X.34, 172.30.X.54; 172.30.X.65 – 89, де *X* – ваш номер за списком). Яким чином вказати одразу декілька IP-адрес в правилах фаєрвола MikroTik ROS?

2.1. Для початку необхідно створити список IP-адрес. Перейдіть на **“IP” > “Firewall” > “Address Lists”.** Натисніть **“+”** , придумайте назву списку та внесіть першу IP-адресу, як наведено на рисунку 8.4 (тільки використовуйте IP-адресу з вашої підмережі). Зробіть ***скріншот***. Натисніть **“ОК”**.

2.2. При внесенні першої IP-адреси список створюється, далі його вже можна буде вибрати зі списку створених. Додавання інших IP-адрес відбувається за тим же принципом. Повторіть крок 2.1 у для інших адрес згідно вашої IP-адресації, як наведено на рисунку 8.5.

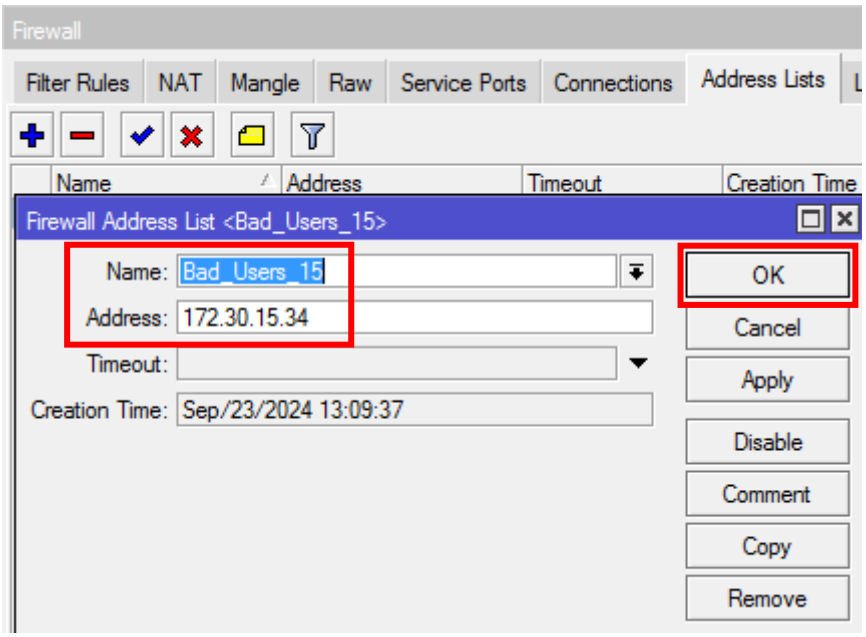

Рисунок 8.4. Створення списку IP-адрес для firewall

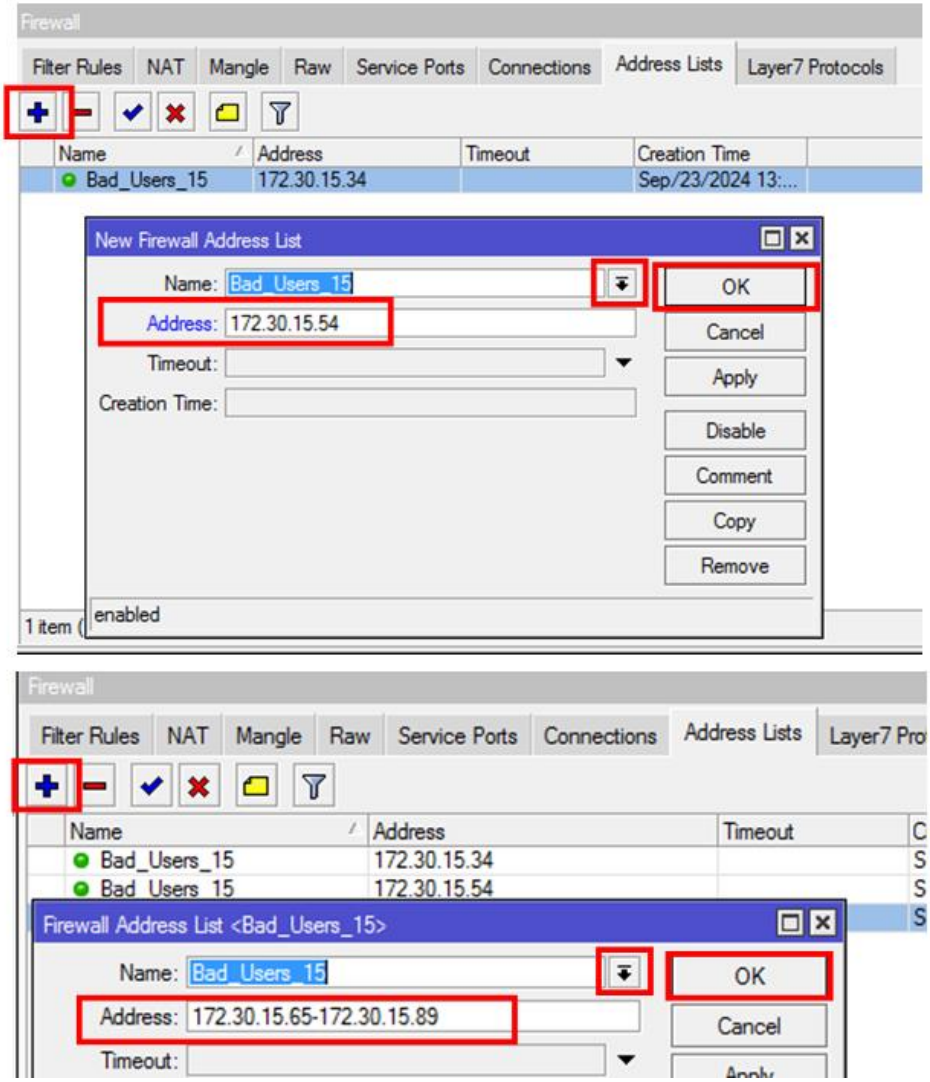

Рисунок 8.5. Додавання інших IP-адрес до списку

2.3 Зробіть ***скріншот*** повного списку доданих IP-адрес, як наведено на рисунку 8.6.

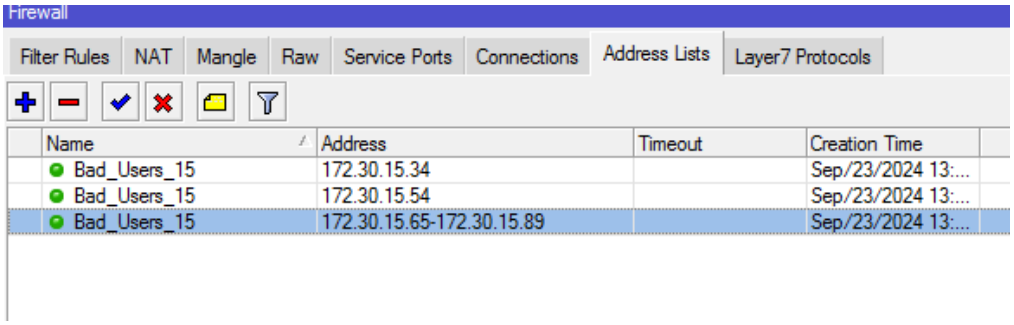

Рисунок 8.6. Повний список IP-адрес для firewall

2.4 Далі перейдіть на **“IP” > “Firewall” > “Filter Rules” > “General”** та додайте нове правило, як наведено на рисунку 8.7. Який ланцюг ви обрали? Чому?

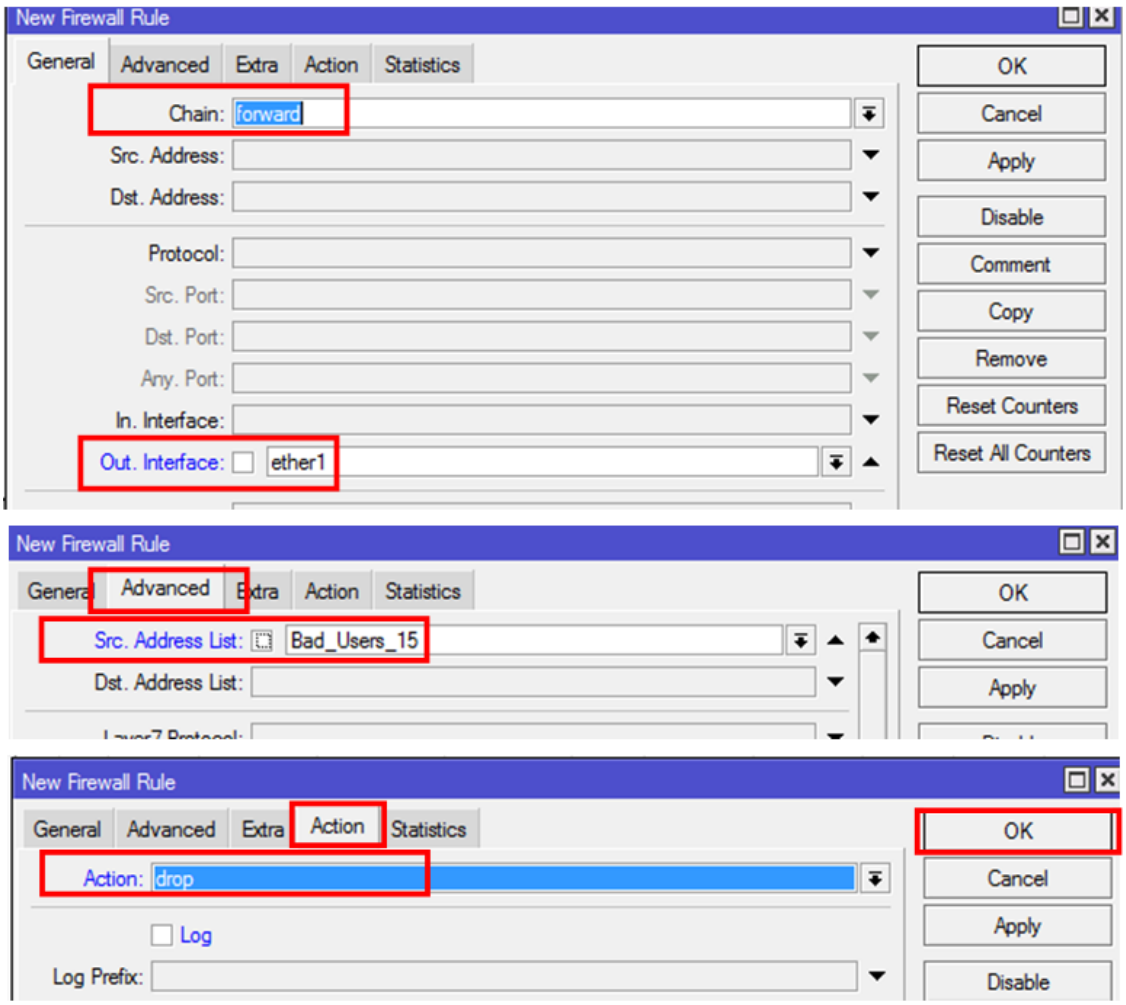

Рисунок 8.7. Правило фаєрвола з використанням списку IP-адрес

2.5. У вікні **“IP” > “Firewall” > “Filter Rules”** перевірте, чи з’явилось нове правило. Зробіть ***скріншот***.

2.6. Задайте на своєму ПК будь-яку статичну IP-адресу зі створеного списку “***Bad_Users_15”***. Перевірте з командного рядка ПК нові мережеві налаштування через *ipconfig*. Спробуйте запустити пінг на відомий вам сервер в Інтернеті, наприклад, *ping 8.8.8.8*. Який отримали результат? Зробіть ***скріншот***.

2.7 Поверніть мережеві налаштування ПК до попереднього стану (отримання IP-адреси по dhcp).

3. Створіть правило firewall: ваш маршрутизатор повинен виконувати функції VPN-клієнта, тому потрібно відкрити певні порти для доступу до нього (UDP 1701, TCP 1723). Які VPN-тунелі використовують ці порти? Який ланцюг firewall ви оберете? Зазвичай, таке завдання постає, коли зверху є забороняюче правило.

3.1. Для відкриття двох портів необхідно створити два окремих правила. Перейдіть на вкладку **“IP” > “Firewall” > “Filter Rules” > “General”** та створіть правила, як наведено на рисунках 8.8-8.9. Зробіть ***скріншоти***.

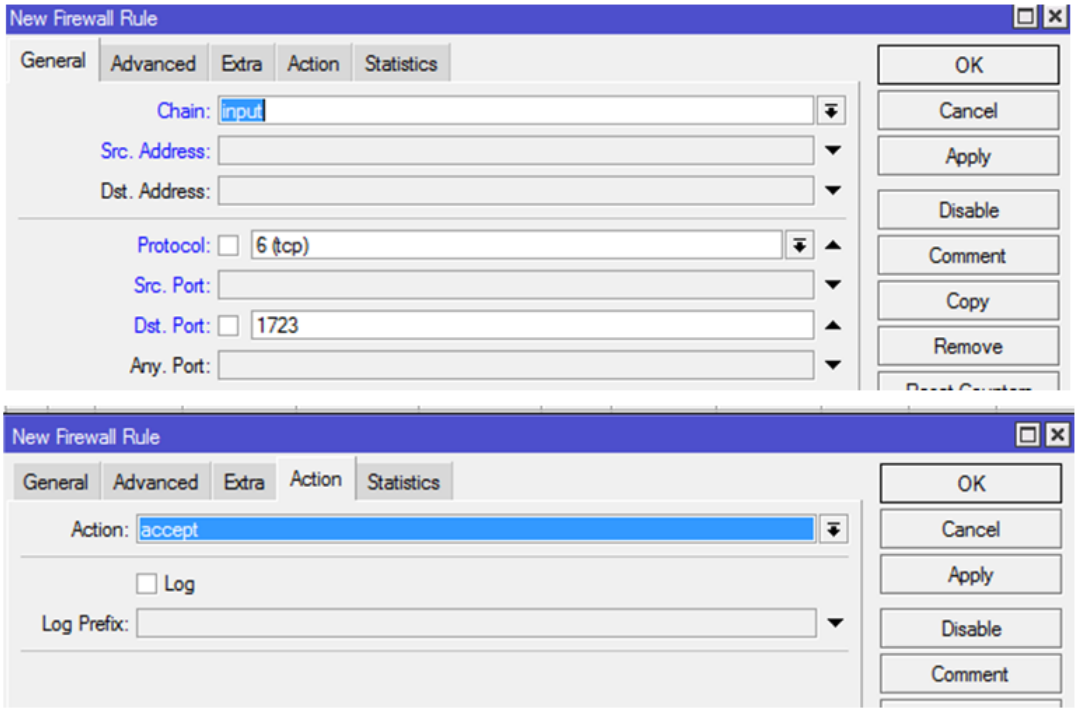

Рисунок 8.8. Створення дозволяючого правила для першого VPN

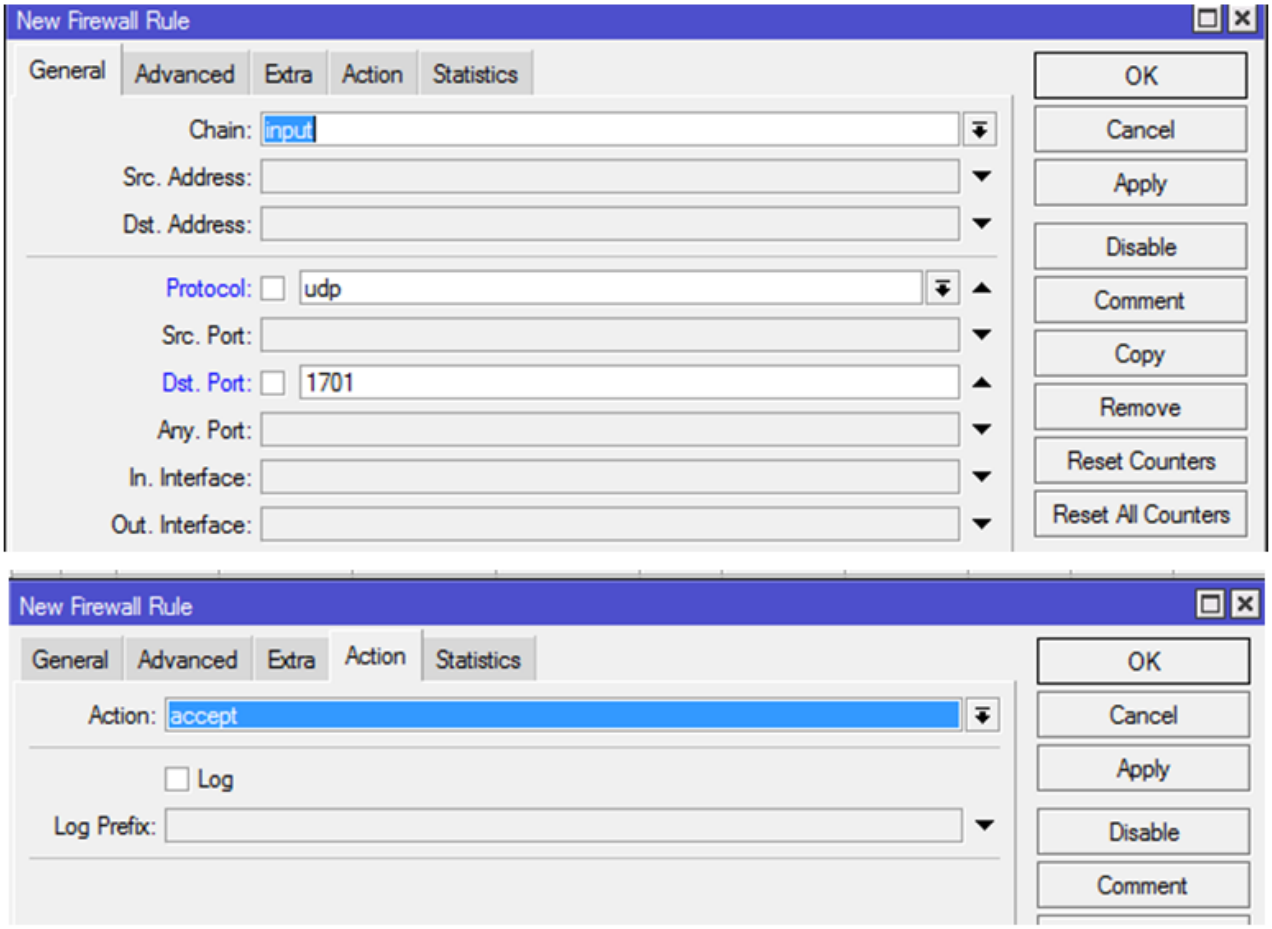

Рисунок 8.9. Створення дозволяючого правила для другого VPN

4. Створіть правило firewall: закрийте користувачам *ping* (ICMP-трафік) для 8.8.8.8. Який ланцюг ви оберете? Чому?

4.1 Перейдіть на **“IP” > “Firewall” > “Filter Rules”** та додайте нове правило, як наведено на рисунку 8.10. Потім натисніть **“OK”**.

4.2 Перевірте працездатність цього правила. Що для цього треба зробити? Зробіть ***скріншот***.

5. ДЛЯ САМОСТІЙНОГО ВИКОНАННЯ !!!

Заблокуйте порт telnet (TCP-23) на маршрутизаторі, оскільки це небезпечно. Який ланцюг ви оберете? Чому? Зробіть ***скріншот*** правила.

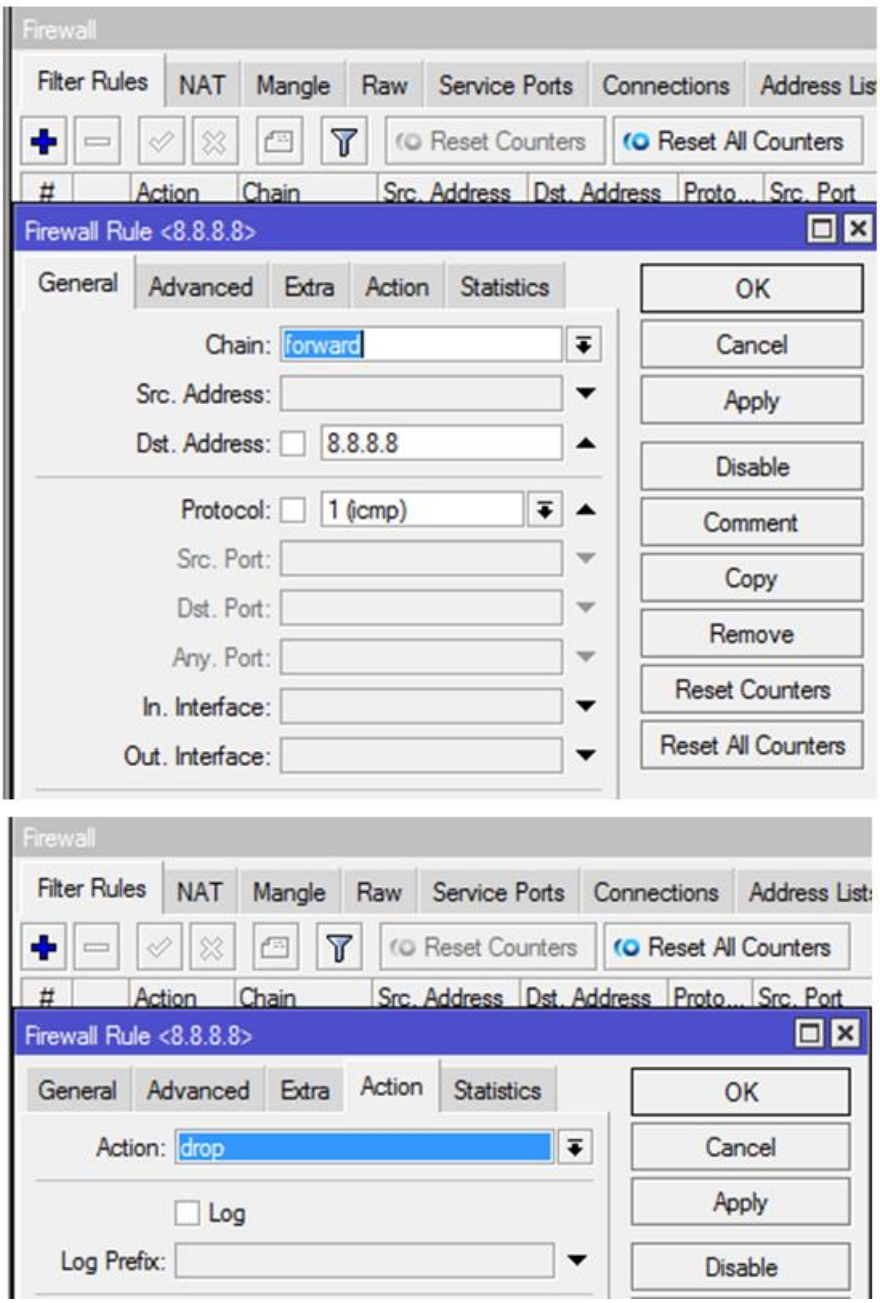

Рисунок 8.10. Правило для заборони *icmp*-трафіка

6. ДЛЯ САМОСТІЙНОГО ВИКОНАННЯ !!!

Забороніть маршрутизатору пінгувати 8.8.4.4.

Який ланцюг ви оберете? Чому? Зробіть ***скріншот*** правила. Перевірте його працездатність (***скріншот***).

7. За допомогою команди *export* перегляньте усі ваші правила брандмауера. Скільки їх? Зробіть ***скріншот***, як наведено на рисунку 8.11.

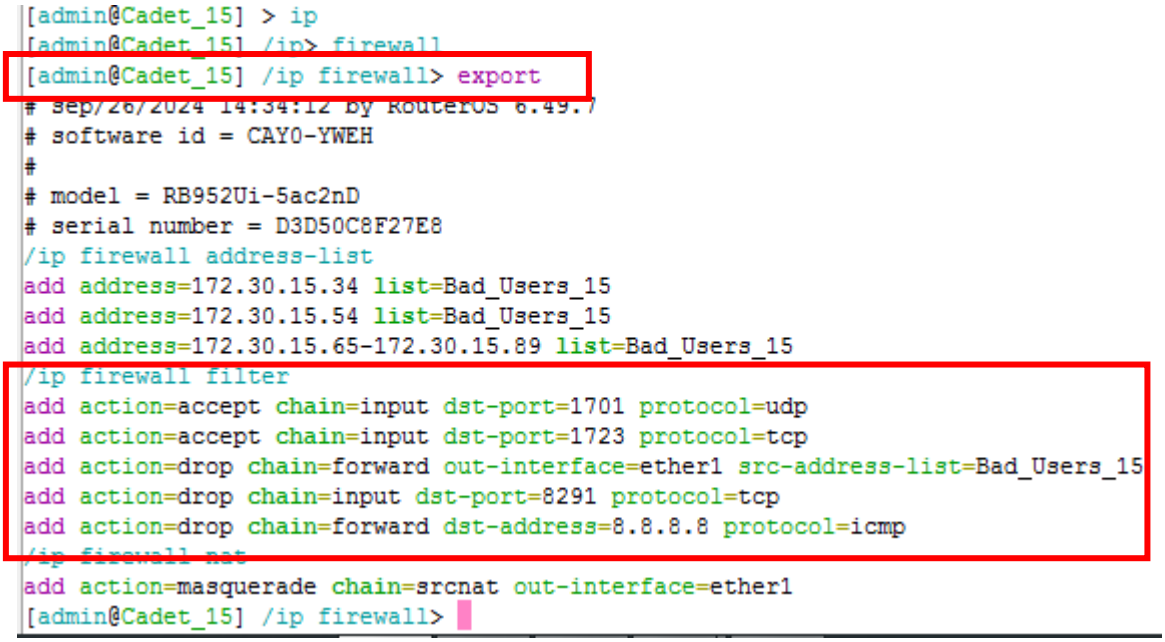

Рисунок 8.11. Перелік всіх правил firewall через CLI

8. Зробіть звіт зі скріншотами й відповідями та надішліть викладачу.

Контрольні питання

1. Які є види ланцюгів брандмауера у MikroTik?

2. Які основні дії (actions) можете обрати при побудові правил брандмауера?

3. Як створити список адрес для використання брандмауером у MikroTik?

4. Які порти потрібно відкрити, щоб ваш маршрутизатор виконував функції VPN-клієнта?

5. Чи можливо закрити доступ в інтернет деяким «поганим» користувачам за IP-адресами?

ЛАБОРАТОРНА РОБОТА № 9
ПОБУДОВА МЕРЕЖІ IP-ТЕЛЕФОНІЇ НА ОСНОВІ ОБЛАДНАННЯ GRANDSTREAM

Мета:

1) ознайомитися з принципами функціонування та порядком налаштування АТС Grandstream та IP-телефонів Grandstream;

2) отримати практичні навички з налаштування АТС Grandstream та IP-телефонів Grandstream.

Початкові дані

Типова схема організації сегменту мережі IP-телефонії зображена на рисунку 9.1.

Рисунок 9.1. Схема організації сегменту мережі IP-телефонії

Номери абонентів:

- $10X$, $10(X+1)$, де X – номер за списком у форматі двозначного числа.

Дані для створених користувачів:

- Extension: 10XX.
- Caller ID Number: 10XX.
- Authenticate ID: 10XX.
- Password: Sk312345678@.

Паролі на АТС:

- UCM6202: Sk312345678_.
- UCM6302: Sk312345678_.

Хід роботи

9.1. Налаштування АТС Grandstream.

1. Скиньте налаштування АТС до заводських через дисплей на корпусі АТС за допомогою кнопок, як наведено на рисунку 9.2 (необхідно знайти в меню пункт **“Factory Reset”**):

Рисунок 9.2. Кнопки для налаштування АТС через меню вбудованого дисплея

2. Переконайтесь, що ПК і АТС знаходяться в одній підмережі (за IP-адресою). За допомогою браузера перейдіть на IP-адресу, вказану на дисплеї АТС, як наведено на рисунку 9.3 (логін для входу через вебінтерфейс: ***admin***; пароль: на звороті біля штрихкоду).

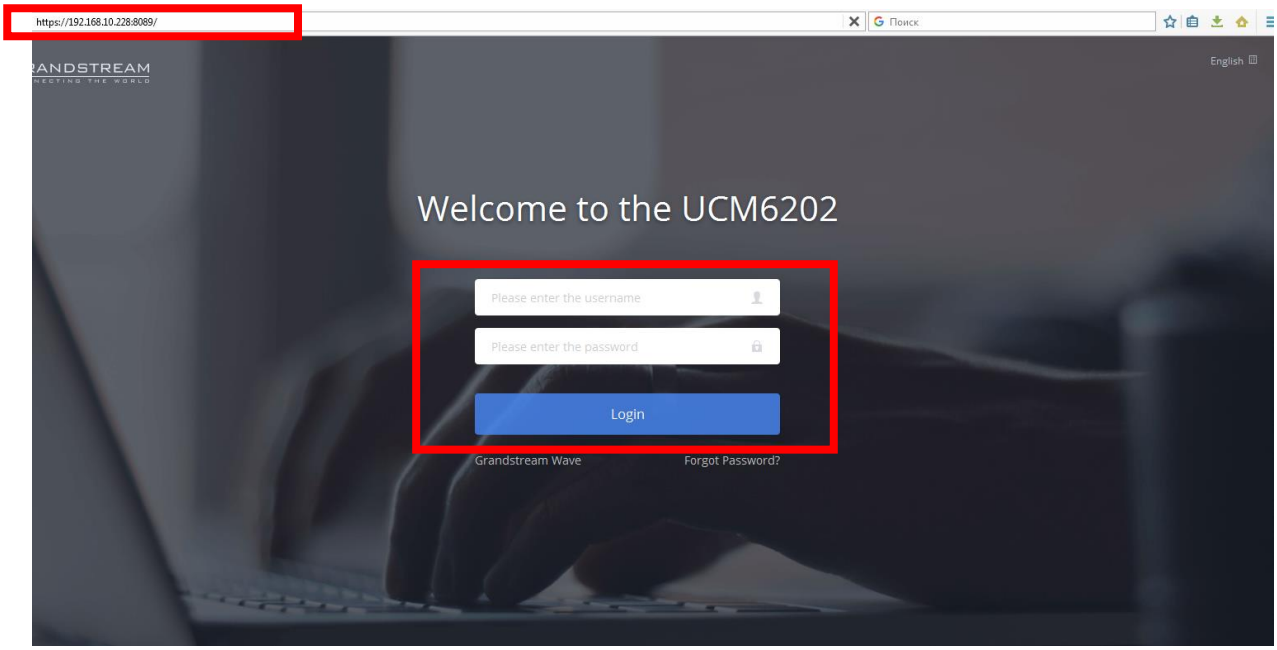

Рисунок 9.3. Вхід на веб-інтерфейч АТС

3. Пропустіть налаштування **“Setup Wizard (Quit)”**.

4. Перейдіть на відповідну вкладку меню (рис. 9.4) та встановіть новий пароль: ***Sk312345678_***. Натисніть **“Save”**. Після цього АТС вас викине з налаштувань і запропонує заново пройти авторизацію, але вже з новим паролем.

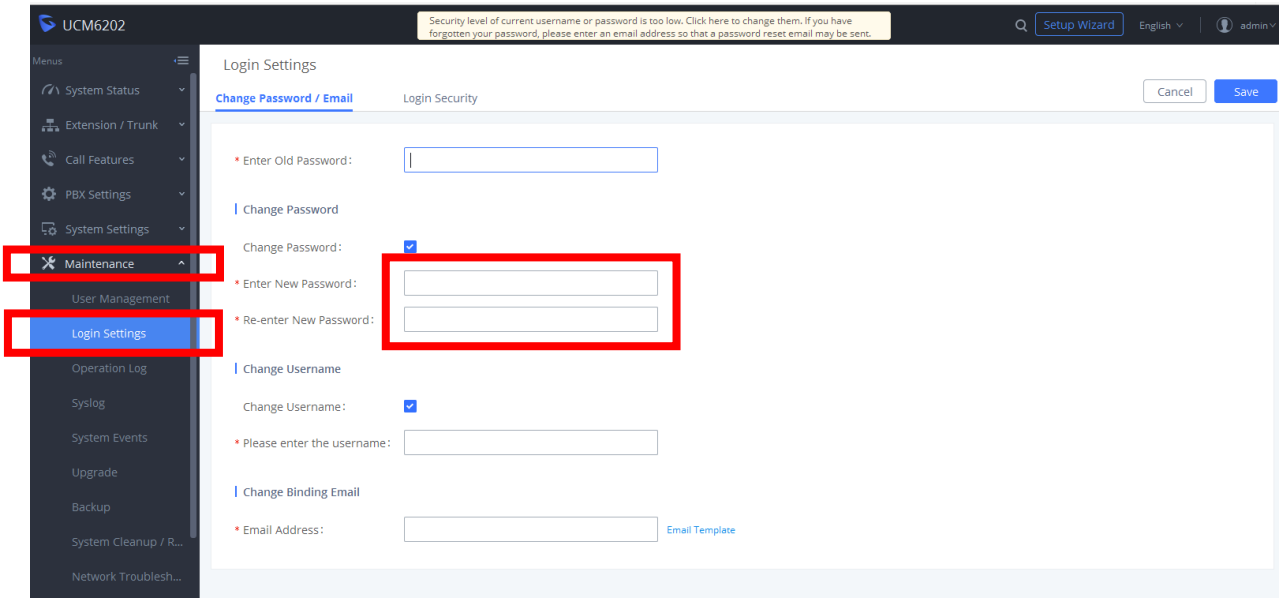

Рисунок 9.4. Створення нового пароля на вхід в АТС

5. Перейдіть до мережевих налаштувань, задайте режим роботи **“Switch”**, статичну адресу на LAN та шлюз згідно з адресацію вашої підмережі, як наведено

на рисунку 9.5. Після внесення нової IP-адреси та мережевого режиму роботи АТС перезавантажиться. Після цього зайдіть на її вебінтерфейс вже за новою IP-адресою.

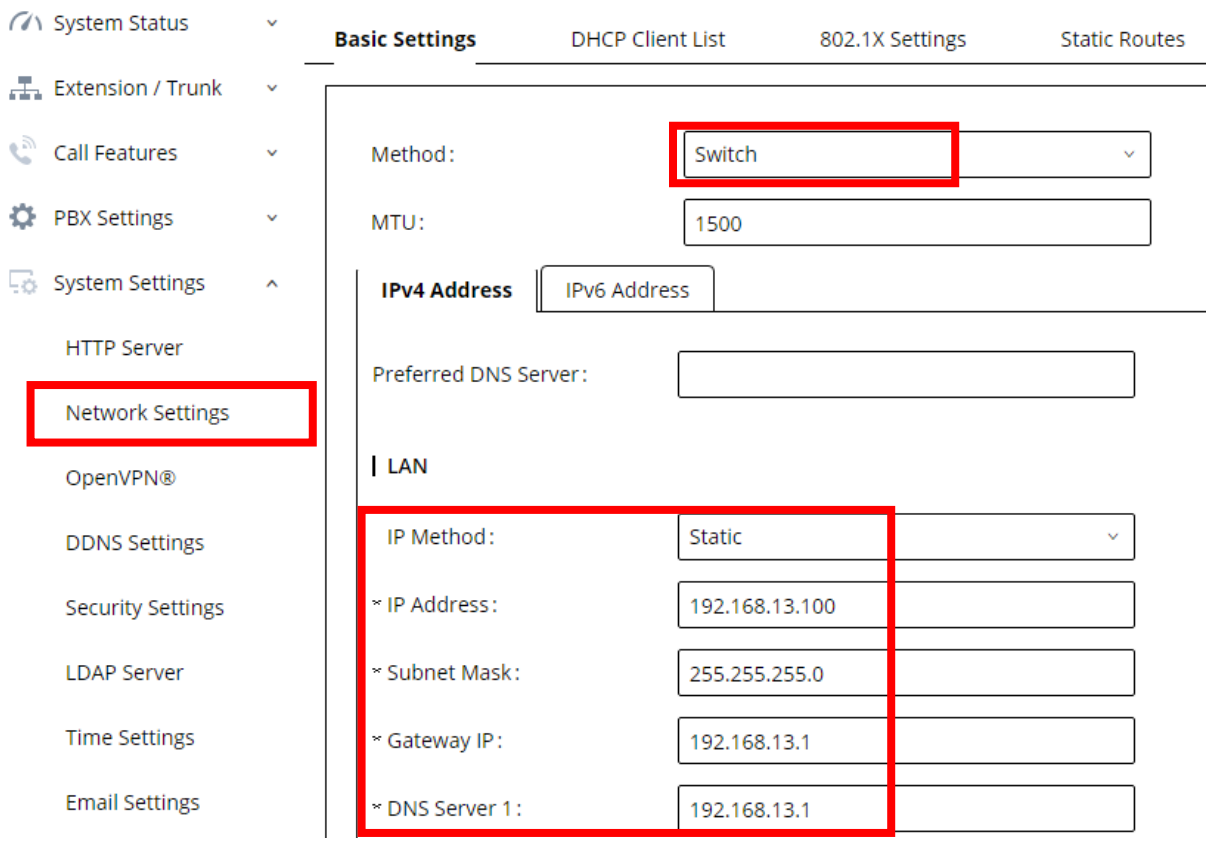

Рисунок 9.5. Створення нової IP-адреси в режимі Switch

6. Для створення абонентів та відповідних їм ліній перейдіть на вкладку **“Extensions”** та натисність **“Add”**. Таким чином створіть двох нових абонентів згідно з умовами, заданими на початку заняття (для прикладу на рисунку 9.6 створено абонентів з номерами 1300, 1301).

Задайте абоненту необхідні ідентифікатори (також вказані у початкових даних) та пароль, який потім буде використаний на кінцевому обладнанні для ідентифікації, та натисніть **“Save”**:

7. Після внесення будь-яких змін у конфігурацію абонентів або з’єднувальних ліній між АТС (транків) необхідно підтвердити свої дії, натиснувши кнопку **“Apply Changes”,** як наведено на рисунку 9.7. Після цього АТС почне виконувати внесені зміни.

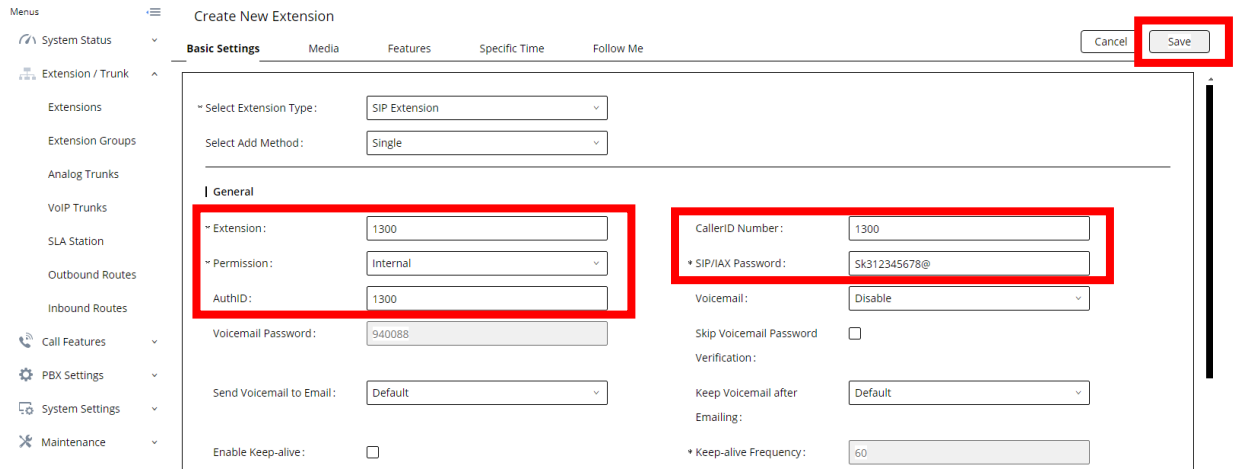

Рисунок 9.6. Створення нового абонента на АТС

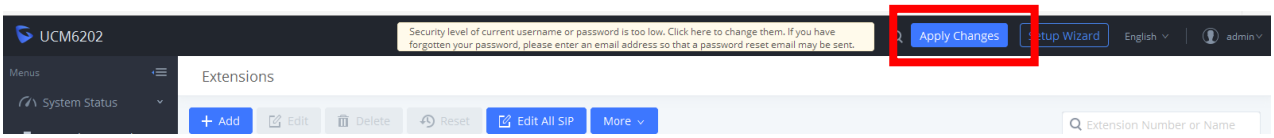

Рисунок 9.7. Підтвердження конфігурації на АТС

8. Після створення абонентів ви можете подивитися їх статус на вкладці **“Extensions”**. Успішно підключені абоненти будуть позначені **Idle.** Вони стануть такими після налаштування IP-телефонів.

9.2. Налаштування IP-телефонів

1. Скиньте налаштування IP-телефонів до заводських через дисплей на корпусі телефону за допомогою кнопок, як наведено на рисунку 9.8 (необхідно знайти в меню пункт **“Factory Reset”**):

Рисунок 9.8. Кнопки для налаштування IP-телефонів через меню вбудованого дисплея

2. Після скидання й перезавантаження телефону необхідно зайти на його IP-адресу. Переконайтесь, що ПК і IP-телефон знаходяться в одній підмережі. За допомогою браузера перейдіть на IP-адресу, вказану на дисплеї телефону, як наведено на рисунку 9.9 (логін для входу через вебінтерфейс: ***admin***; пароль на звороті біля штрихкоду).

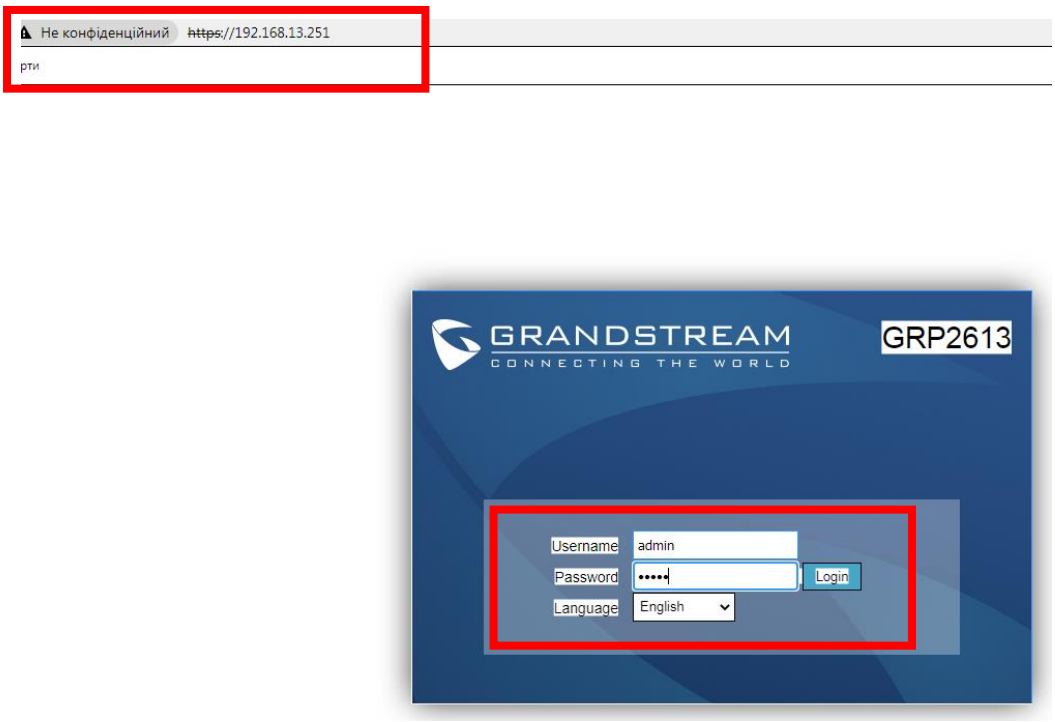

Рисунок 9.9. Вхід на вебінтерфейс управління телефоном

3. При першому вході відбувається запит на зміну пароля – задайте новий пароль: **1.**

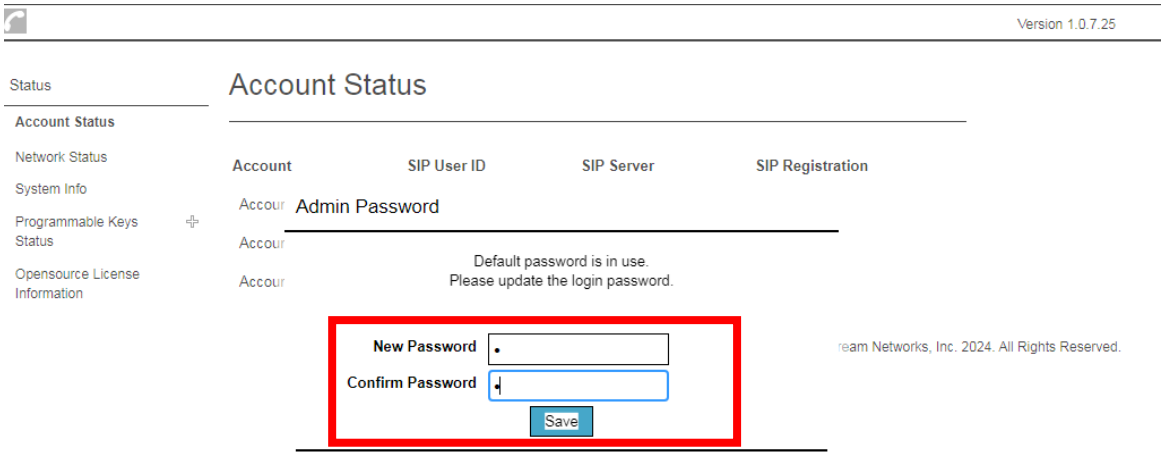

Рисунок 9.10. Зміна паролю при 1 вході

4. Перейдіть на вкладу **“Accounts” > “Account” > “General Settings”** та налаштуйте обліковий запис абонента згідно зі створеним записом в АТС, як наведено на рисунку 9.11. Натисніть **“Save and Apply”**.

5. Якщо все налаштовано правильно, то обліковий запис стане активним (перевірити на вкладці **“Account Status”** телефону, а також на вкладці **“Extensions”** в АТС). Налаштуйте другий телефон, спробуйте дзвонити в межах однієї АТС.

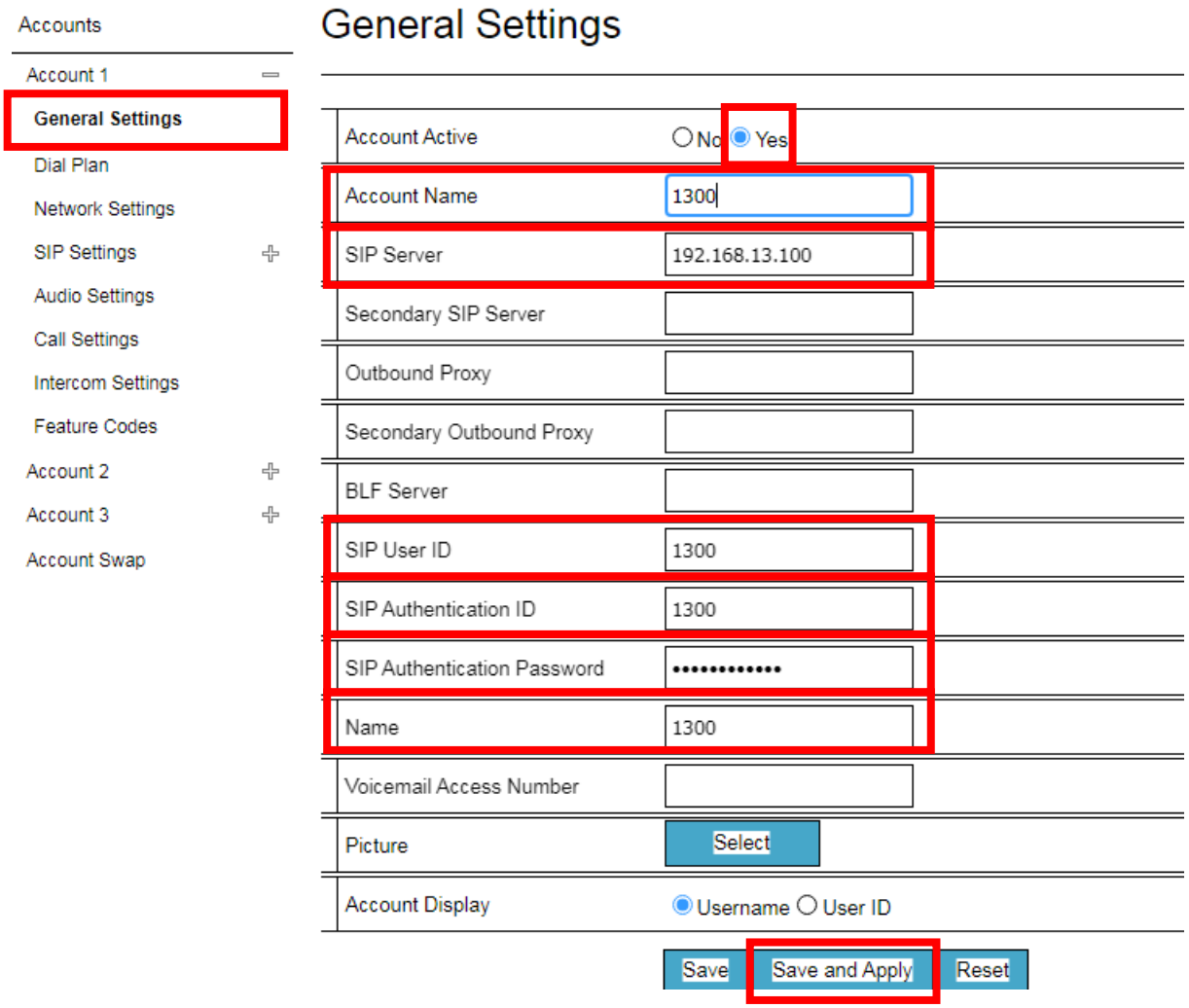

Рисунок 9.11. Налаштування облікового запису на IP-телефоні

9.3. Додаткові можливості та налаштування АТС

1. Ви можете налаштувати АТС в режимі маршрутизатора. WAN-адресу можна налаштувати статично, як наведено на рисунку 9.12, або отримати від DHCP-сервера.

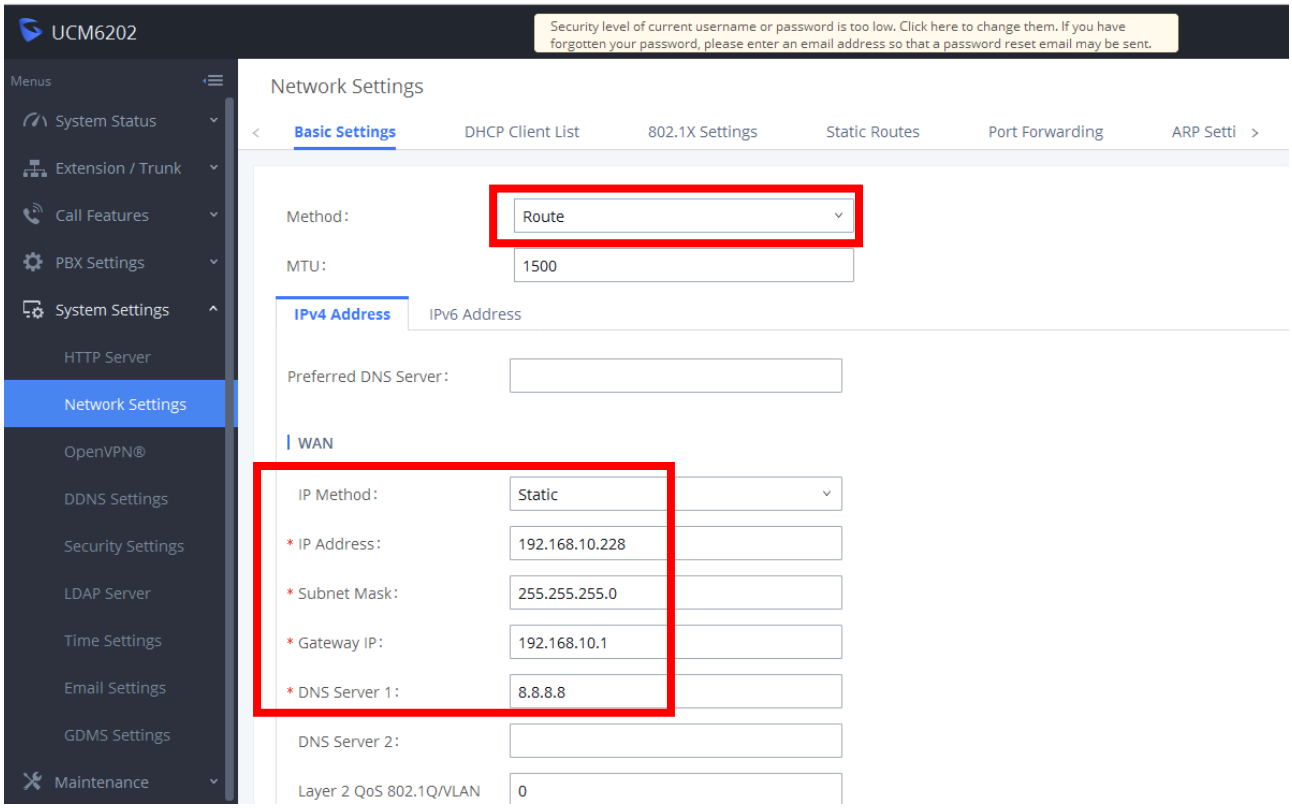

Рисунок 9.12. Налаштування WAN-адресації АТС в режимі маршрутизатора

2. Далі необхідно налаштувати LAN-мережу окремо від WAN. У такому випадку АТС може виконувати функції DHCP-сервера. Приклад налаштування LAN-мережі наведено на рисунку 9.13.

3. Якщо ваша АТС вже виконує функції DHCP-сервера, і телефони вже отримали IP-адресу від нього, то є можливість статично закріпити IP-адреси за конкретними MAC-адресами, як наведено на рисунку 9.14.

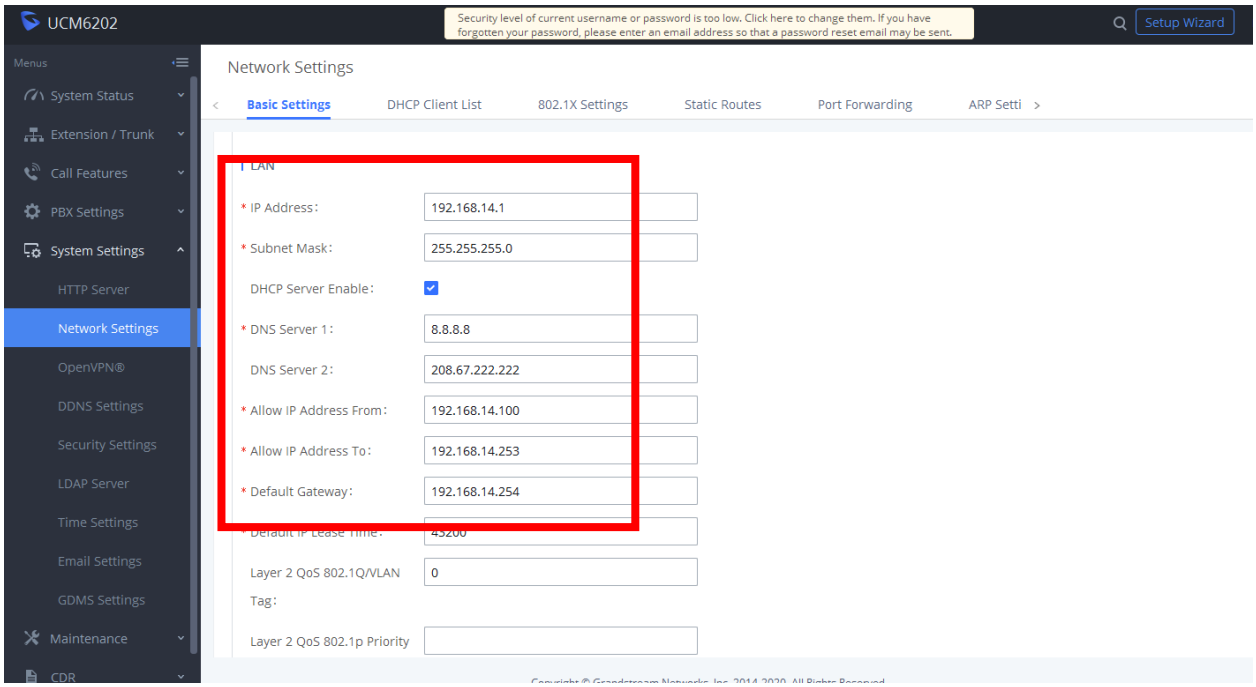

Рисунок 9.13. Налаштування LAN ATC в режимі маршрутизатора

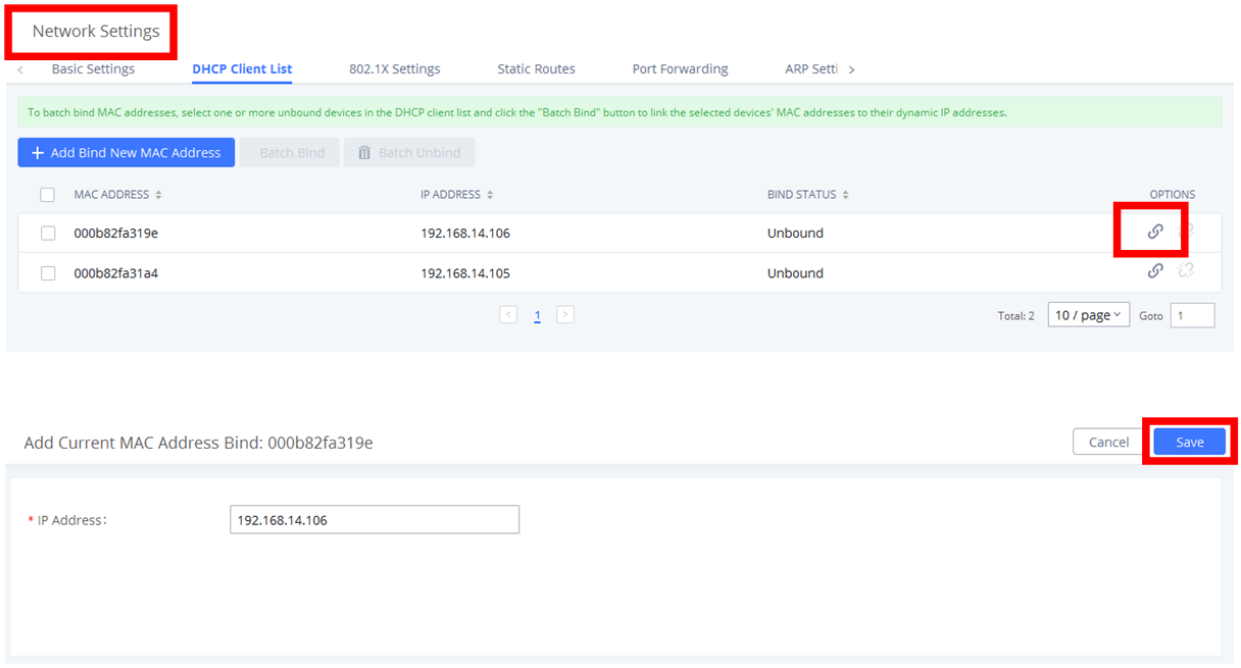

Рисунок 9.14. Закріплення IP-адреси за MAC-адресою пристрою в LAN ATC

4. Результат представлено на рисунку 9.15:

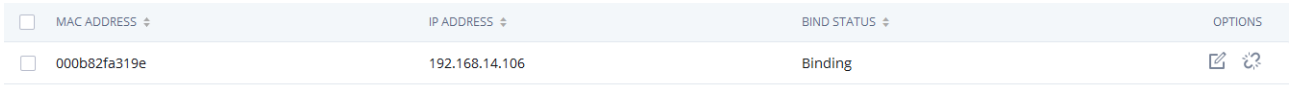

Рисунок 9.15. Результат закріплення IP-адреси за MAC-адресою пристрою в LAN ATC

5. Також після вказання нової IP-адреси в налаштуваннях LAN АТС, можна прив’язати цю ж адресу АТС в налаштуваннях SIP. Для цього потрібно перейди на вкладку **“PBX Settings” > “SIP settings”** та вписати IP-адресу в поле **“Bind IPv4 address”**. У такому випадку АТС буде відповідати на SIP-запити лише за цією адресою, як наведено на рисунку 9.16.

Якщо в цьому полі буде записано значення **“0.0.0.0”** – АТС буде відповідати на SIP-запити за будь-якою зі своїх IP-адрес, навіть, якщо вони зміняться, наприклад, внаслідок отримання нової адреси по DHCP або загальної зміни схеми мережі.

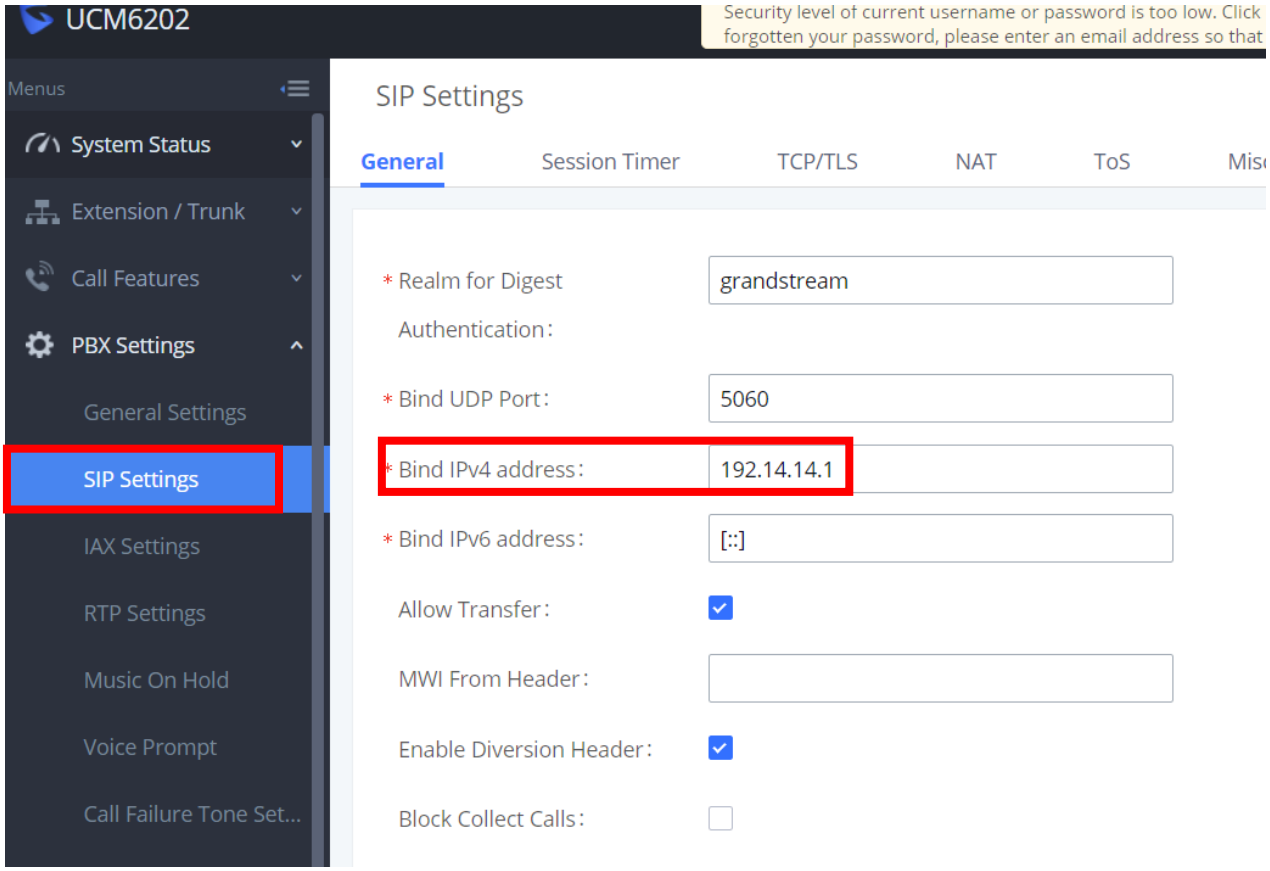

Рисунок 9.16. Закріплення SIP за конкретною IP-адресою АТС

Контрольні питання

1. Призначення та можливості АТС Grandstream 6202 та 6302.
2. Принцип роботи протоколу SIP.
3. Порядок мережевих налаштувань АТС Grandstream 6202 та 6302.
4. Порядок створення та налаштування абонентів на АТС Grandstream 6202 та 6302.
5. Порядок налаштування IP-телефонів Grandstream.
6. Які голосові кодеки вам відомі?
7. Що таке VoIP-шлюз, для чого призначений?

ЛАБОРАТОРНА РОБОТА № 10
НАЛАШТУВАННЯ РАДІОРЕЛЕЙНОЇ СТАНЦІЇ СРШ-5000

Мета:

1) ознайомитися з технічними характеристиками, можливостями та порядком налаштування СРШ-5000;

2) отримати практичні навички з налаштування СРШ-5000.

Хід роботи

1. На ПК, що підключається до СРШ, запустіть програму Winbox. У діалоговому вікні, що з'явилось, перейдіть на вкладку **"Neighbors"** та натисніть кнопку **"Refresh"**.

Після закінчення пошуку СРШ обрати станцію за MAC-адресою, ввести потрібні логін (***admin***) та пароль (***1***), після чого натиснути кнопку **"Connect"** (рис. 10.1).

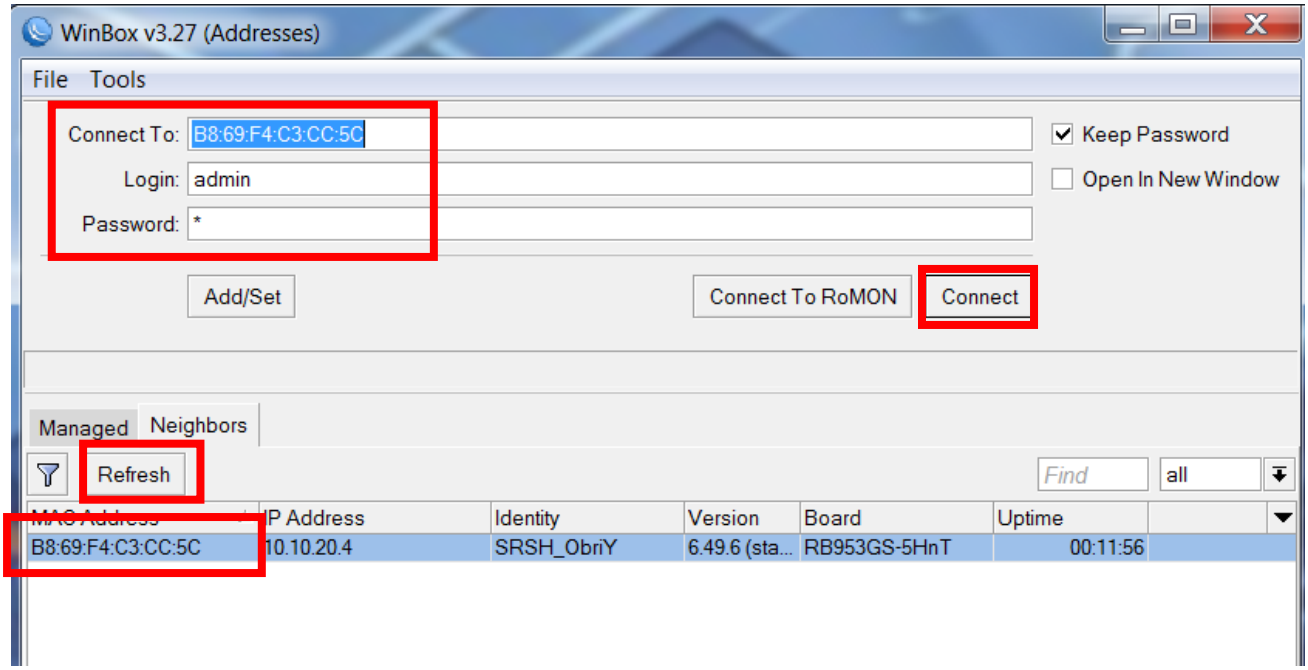

Рисунок 10.1. Підключення до СРШ

2. Створіть інтерфейс *Bridge*, та додайте до нього *Ethernet-інтерфейси* та *wlan-інтерфейс*. Для цього перейдіть на вкладку **“Bridge”**, як наведено на рисунку 10.2.

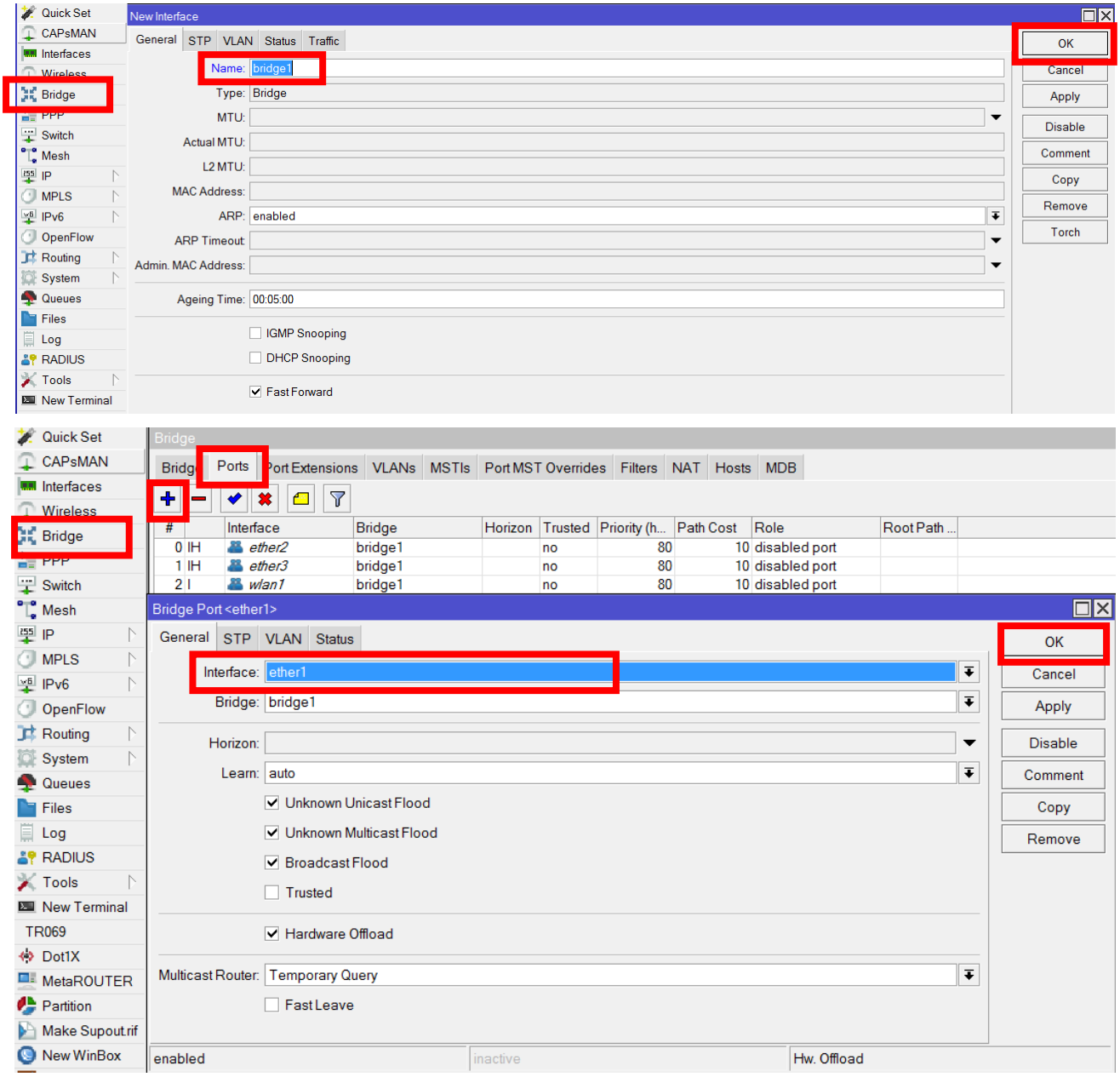

Рисунок 10.2. Створення інтерфейсу Bridge та додавання інтерфейсів до нього на СРШ

3. Для перегляду IP-адрес, що призначені інтерфейсам СРШ, перейдіть на вкладку **“IP-Addresses”**. Для додавання нової адреси, натисніть кнопку . Уведіть наступні параметри, як наведено на рисунку 10.3:

Address – IP-адреса (вказується у форматі xxx.xxx.xxx.xxx/yy);

Network – мережа інтерфейсу (вказувати необов'язково, бо якщо правильно вказана IP-адреса та маска підмережі, то мережа буде заповнена автоматично);

Interface – інтерфейс, якому буде призначено адресу.

Натисніть кнопку **"Apply"**, потім **"OK"**.

Якщо є необхідність видалення адреси, оберіть необхідний рядок та натисніть кнопку .

На обох СРШ для правильної роботи мають бути різні IP-адреси одної підмережі !!!

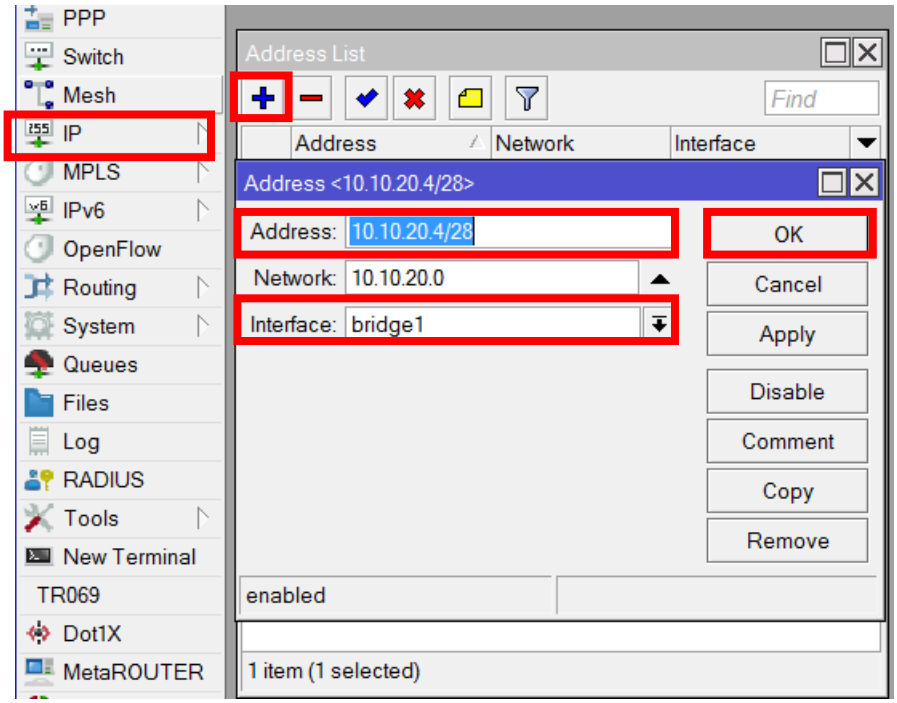

Рисунок 10.3. Додавання IP-адреси

4. Для забезпечення шифрування радіоданих між радіостанціями та для підключення до зашифрованої радіомережі необхідно використовувати профілі безпеки бездротового інтерфейсу з різними типами ключів доступу.

Налаштування профілів безпеки виконується через меню **"Wireless"**, вкладка **"Security Profiles"**, як наведено на рисунку 10.4.

Тут присутній стандартний профіль, який неможливо видалити. За бажанням, можна виконати його налаштування.

Для додавання нового профілю натисніть кнопку (рис. 10.4).

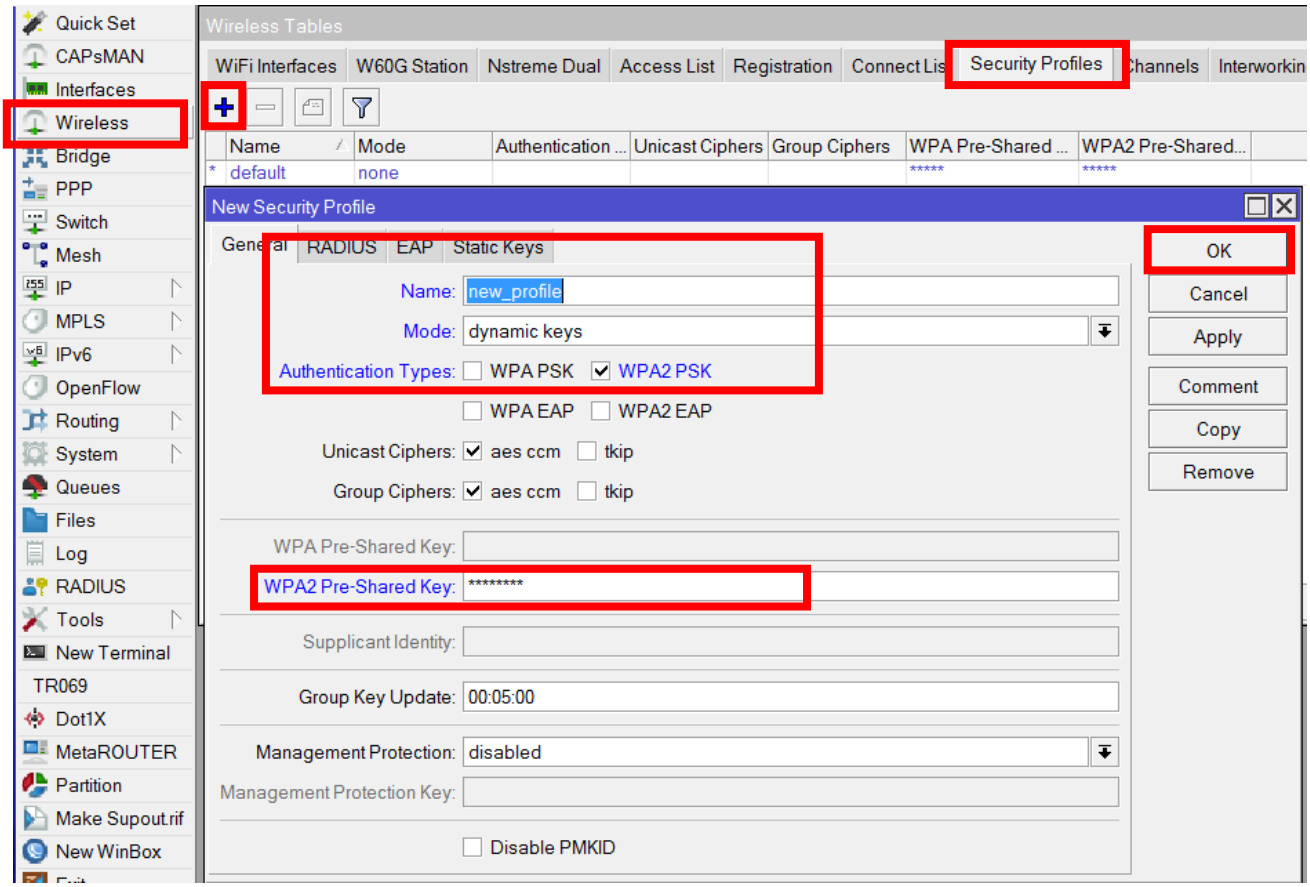

Рисунок 10.4. Налаштування профілю безпеки бездротового зв'язку

Для увімкнення шифрування із динамічними ключами необхідно встановити параметр **“Mode»** в режим **“dynamic keys”**.

Після чого необхідно вказати режим аутентифікації **“WPA2 PSK”** для параметру **“Authentication Types”**.

Уведіть пароль доступу до радіомережі з довжиною щонайменше 8 символів (символи паролю можуть містити латинські літери, знаки пунктуації та цифри). На обох радіостанціях паролі повинні бути однаковими. Для навчальних цілей використовуйте пароль **“12345678”**.

Натисніть кнопку **“Apply”**, потім **“OK”**.

5. При налаштуванні радіоканалу між СРШ, треба враховувати структуру мережі, яка будується за принципом **“головна станція (AP-bridge) – підлегла станція (station-bridge)”**. Тобто одна із СРШ повинна бути в мережі базовою станцією (БС), інші – абонентськими станціями (АС).

Вибеіть протокол радіозв'язку **“nstreme”** – гібридний протокол бездротового зв'язку, який використовує технології TDD/TDMA з фіксованим періодом передачі/прийому фреймів. У порівнянні з 802.11 має більший час встановлення зв'язку, але може бути використаний на великих відстанях. Ефективний у роботі на складних інтервалах (без оптичної видимості) за умови використання вузької ширини каналу. Має високу стабільність джитеру.

Налаштування станцій, які планується додати до однієї радіомережі, виконується однаково. Різниця між налаштуваннями БС та АС складається тільки в декількох параметрах.

Для налаштування СРШ як базової станції, виконайте наступні дії:

- У головному вікні утиліти Winbox обрати меню **“Wireless”** та виконати налаштування інтерфейсу **“wlan1”** СРШ як точки доступу;
- Ввійти до діалогового вікна редагування параметрів обраного інтерфейсу, двічі натиснувши лівою кнопкою миші, потім перейти на вкладку **“Wireless**” та натиснути кнопку **“Advanced Mode”**;
- Встановити наступні параметри інтерфейсу **“wlan1”**» (рис. 10.5):

Frequency mode: superchannel (встановіть цей параметр першим);

Mode: ap bridge;

Band: 5GHz-only-N;

Channel Width: 20/40MHz Ce, ширину каналу необхідно підбирати залежно від характеристик профілю радіорелейної лінії для стійкого з’єднання між СРШ;

Frequency: 5300 MHz, частота може бути іншою, вона вводиться відповідно до наданих дозволів, також можливе додавання всіх дозволених частот, що надасть змогу у разі погіршення сигналу автоматично здійснити перехід на іншу частоту;

SSID: StudyRRL, це назва мережі, повинна бути однаковою для обох станцій;

Radio name: Basic, це унікальний ідентифікатор станції в радіомережі, кожна станція має власний Radio Name;

Wireless protocol: nstreme (він також повинен бути включеним на відповідній вкладці **“Nstreme”**);

Security Profile відповідно до налаштованого в попередньому пункті.

- Прийняти зміни, натиснувши кнопку «**Apply**»;
- Перейти на вкладку «***HT***» та впевнитися, що параметри «Tx/Rx Chains» встановлено тільки для chain0 (що відповідає антенному роз’єму 1), як наведено на рисунку 10.6.

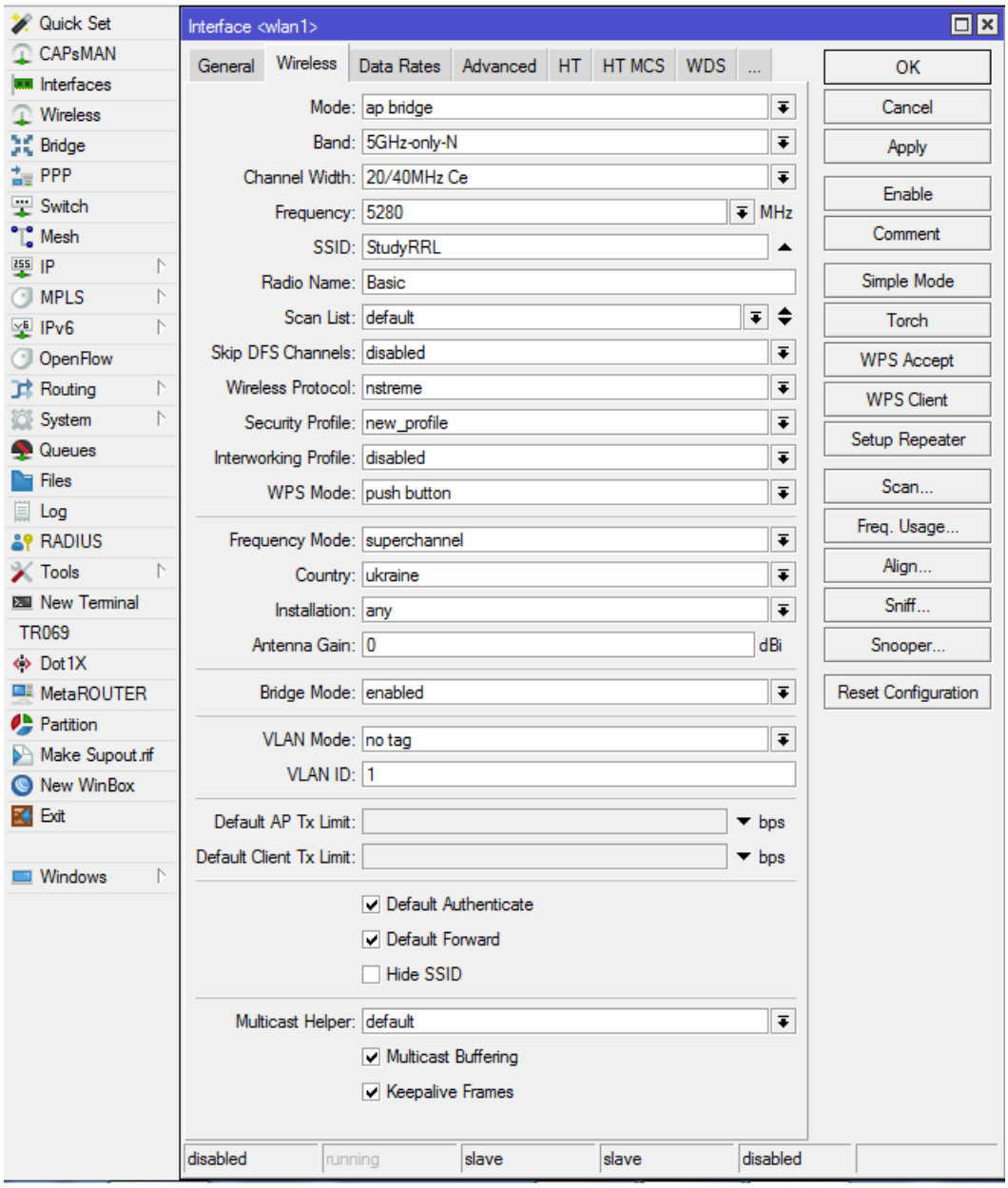

Рисунок 10.5. Налаштування параметрів безпроводового інтерфейсу на головній станції

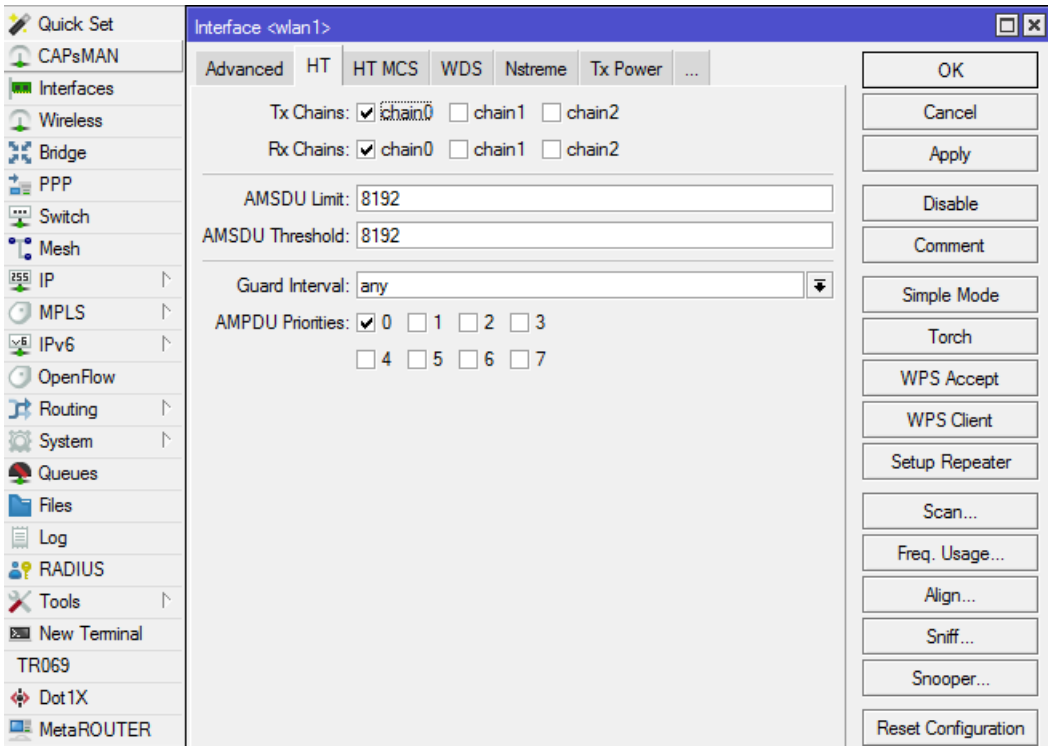

Рисунок 10.6. Приклад налаштування параметрів на вкладці HT

- Перейти на вкладку **“Tx Power”** та впевнитися, що параметр **“Tx Power Mode”** встановлено у режим **“default”**, як наведено на рисунку 10.7.

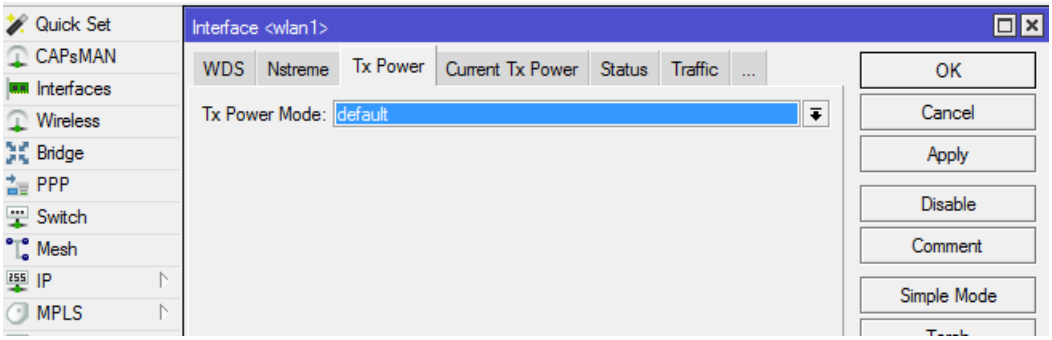

Рисунок 10.7. Приклад налаштування параметрів на вкладці “Tx Power”

- Після встановлення всіх параметрів увімкніть інтерфейс кнопкою **“Enable”**, як наведено на рисунку 10.8, або галочкою.

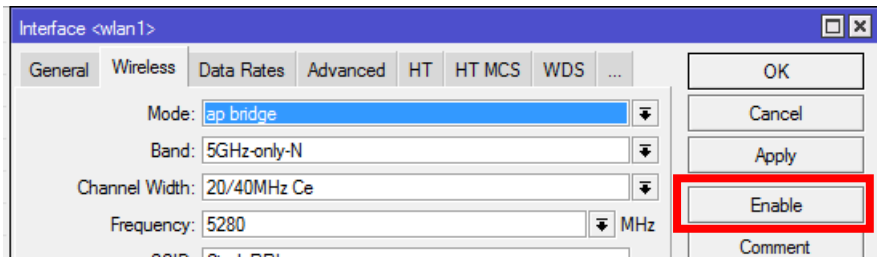

Рисунок 10.8. Увімкнення безпроводового інтерфейсу

6. При налаштуванні абонентської СРШ також створіть bridge та додайте в нього відповідні порти (рис. 10.9), задайте відповідну IP-адресацію в підмережі з БС (рис. 10.10) і вкажіть всі параметри безпроводового інтерфейсу (рис. 10.11), аналогічні БС. Різниця в параметрах радіоінтерфейсів БС і АС буде полягати в такому: *Mode*: station bridge; *Radio name*: Abonent;

Натисніть кнопку **“Apply”**. Включіть інтерфейс кнопкою **“Enable”** або галочкою.

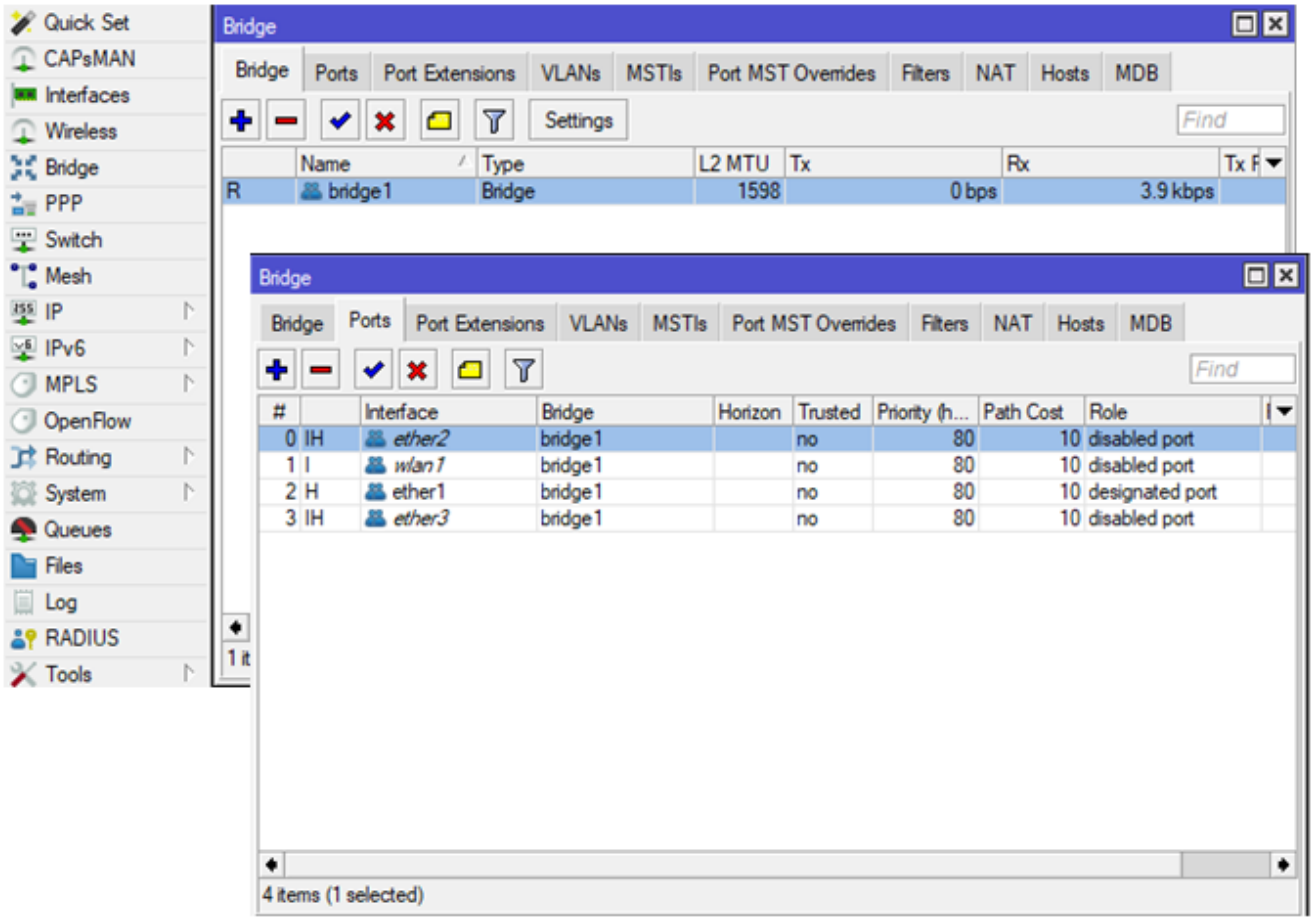

Рисунок 10.9. Налаштування bridge на підлеглій станції

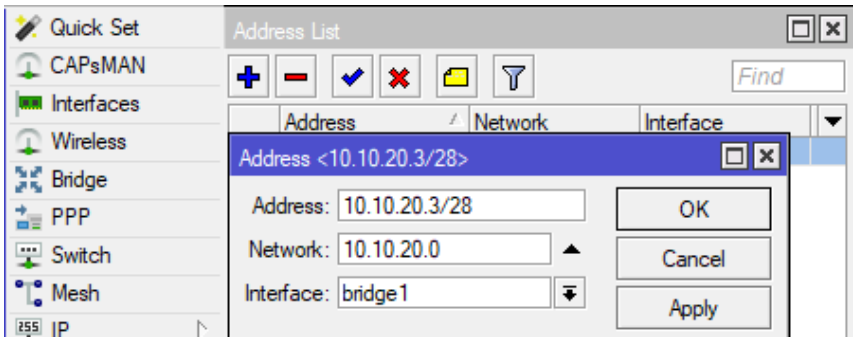

Рисунок 10.10. IP-адресація на підлеглій станції

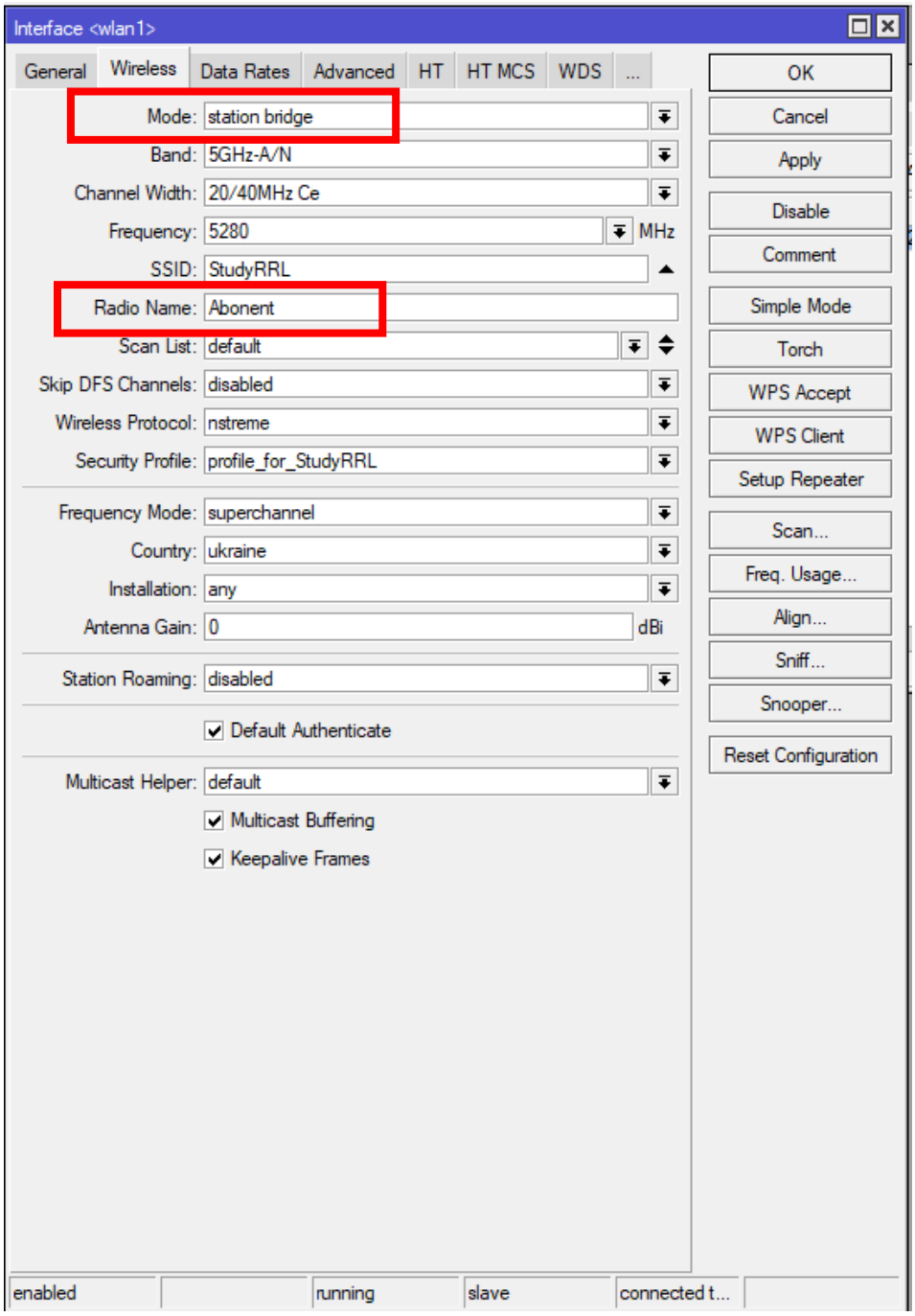

Рисунок 10.11. Налаштування параметрів безпроводового інтерфейсу на підлеглій станції

7. У вікні налаштування інтерфейсу “**wlan1”** як БС, так і АС, на вкладці **“Status”** будуть відображені значення параметрів з’єднання (рис. 10.12 – показники на АС), після його встановлення між СРШ.

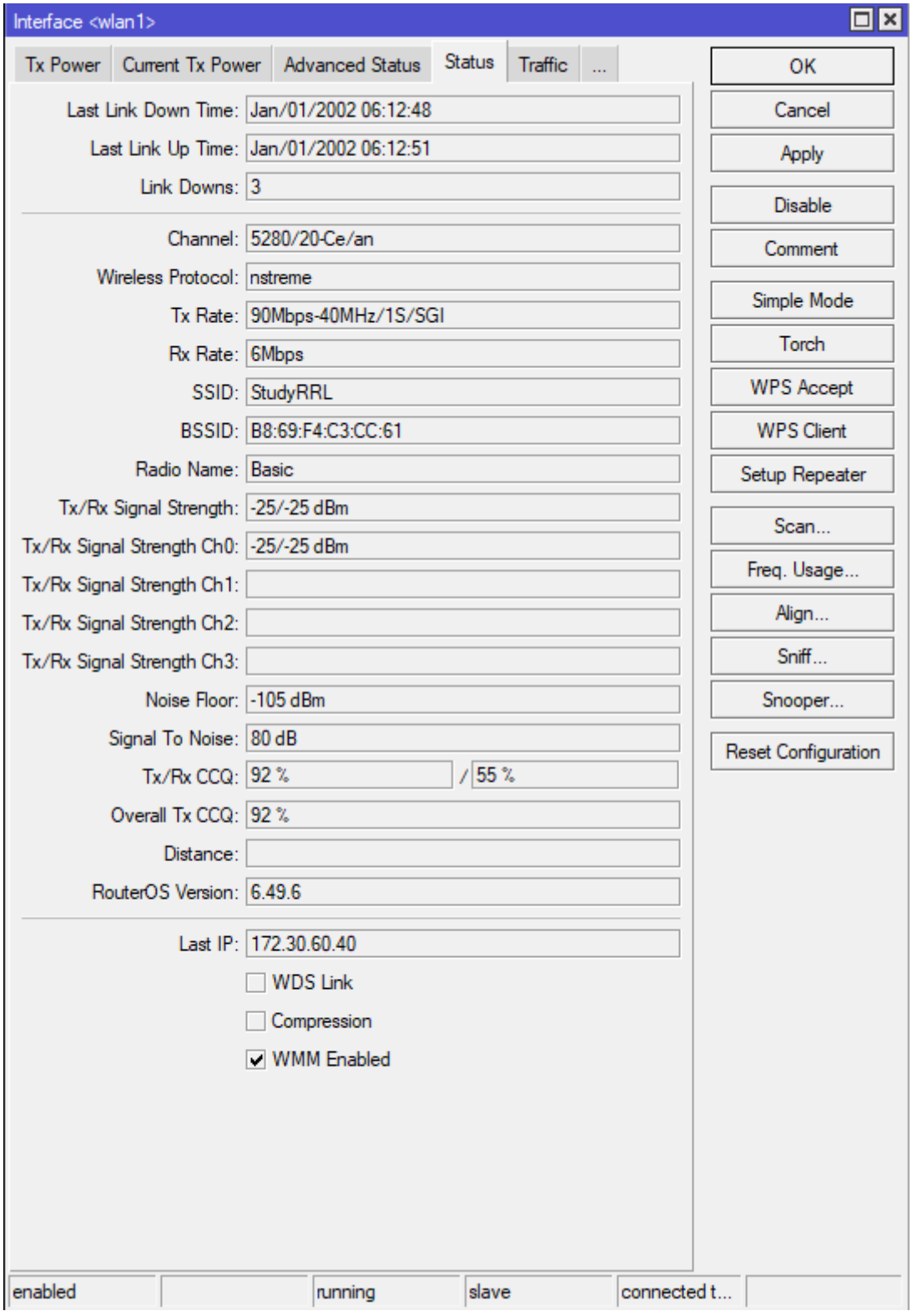

Рисунок 10.12. Приклад параметрів з’єднання на вкладці Status

8. Також на вкладці ***Traffic*** можна побачити ряд параметрів та візуальне підтвердження наявності зв'язку між радіорелейними станціями (рис. 10.13).

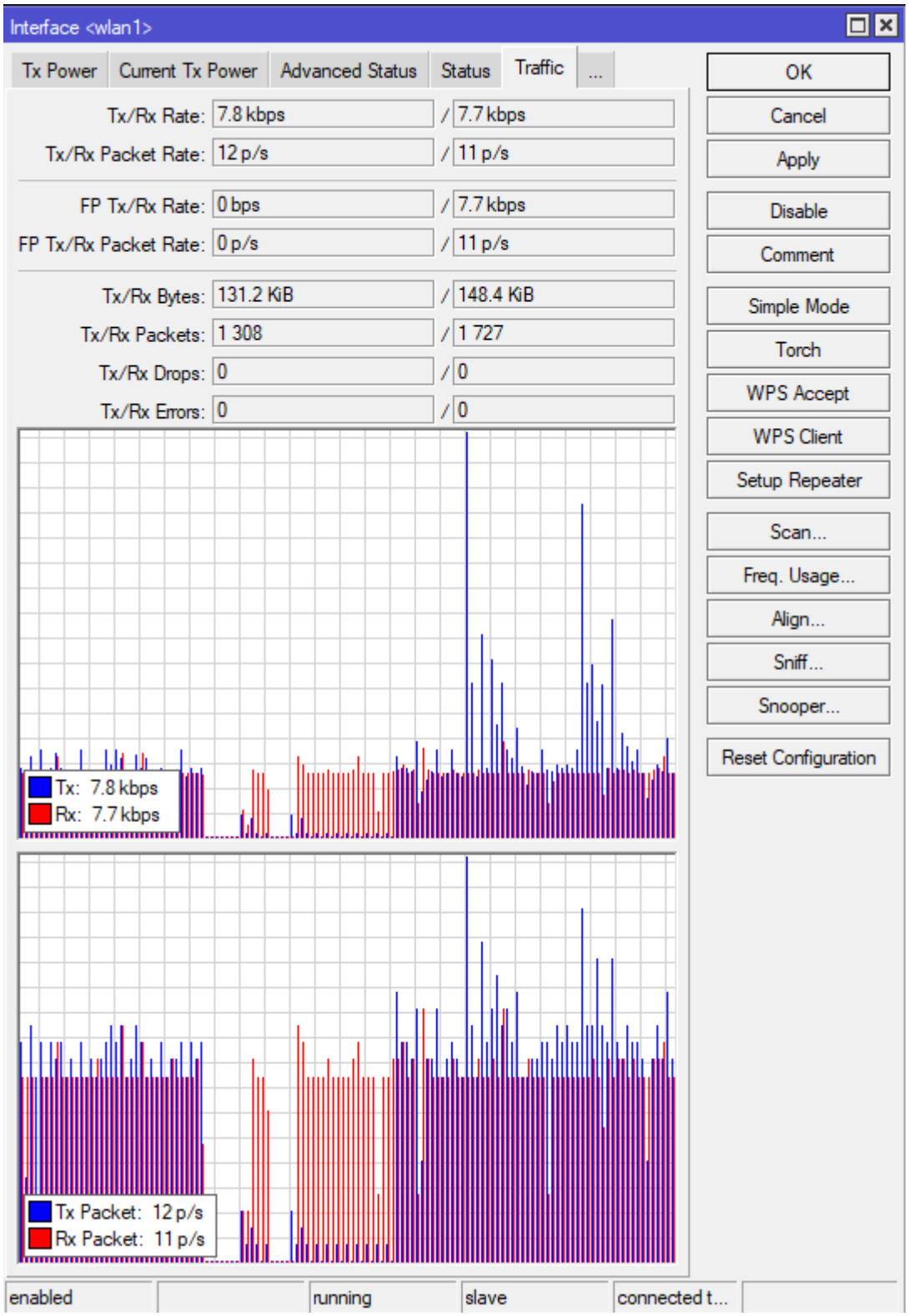

Рисунок 10.13. Приклад параметрів з'єднання на вкладці Traffic

9. Для збільшення максимальної пропускної спроможності з'єднання між СРШ та зниження затримок в радіоканалі необхідно виконати додаткове, почергове юстування антен як для базової, так і для абонентської СРШ. При цьому, необхідно спостерігати за змінами значень параметрів "**Tx/Rx Signal Strength"** та **"Signal To Noise"**.

При показниках Tx/Rx Signal Strength менше за мінус 87 дБм та/або Signal To Noise менше за 20 дБ присутні розриви з'єднання. Таким чином, встановити з'єднання неможливо. Рекомендується зменшити ширину каналу.

10. Виконайте фіксацію антен при досягненні максимальних значень цих параметрів.

11. Переконайтесь у проходженні пакетів між СРШ за допомогою утиліти **"ping".**

12. З'єднайте патчкордом RJ-45 роз'єм **"Data"** та роз'єм відповідного обладнання локальної мережі (наприклад один з інтерфейсів маршрутизатора MikroTik). Переконайтесь у проходженні пакетів між локальними мережами, до яких підключені СРШ.

13. Для вимкнення СРШ після закінчення роботи (зв'язку) спочатку вимкніть безпроводовий інтерфейс кнопкою "**Disable**", як наведено на рисунку 10.14, потім перейдіть на вкладку **"System" > "Shutdown"**, як наведено на рисунку 10.15.

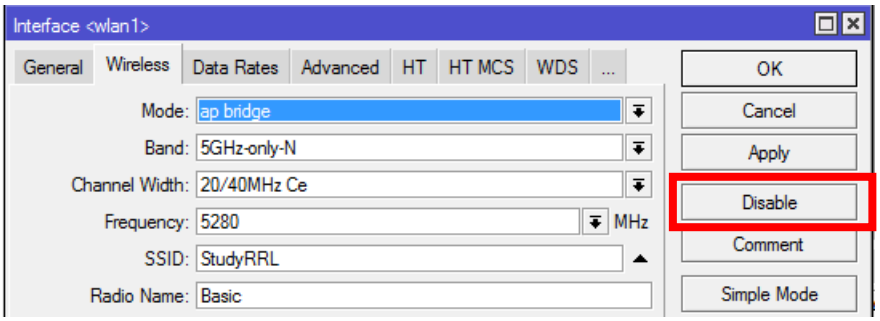

Рисунок 10.14. Вимкнення безпроводового інтерфейсу

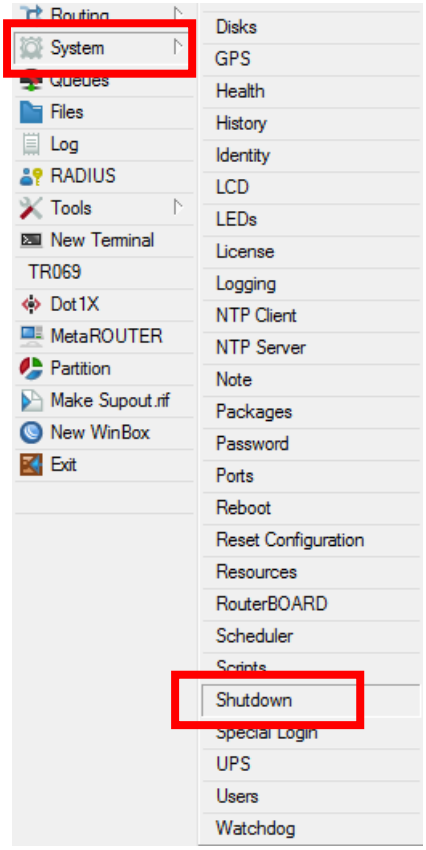

Рисунок 10.15. Вимкнення СРШ

14. Після цього можете від’єднати живлення від радіостанцій.

Контрольні питання

1. Призначення та характеристики СРШ-5000.
2. Режими роботи СРШ-5000.
3. Порядок налаштування головної станції СРШ-5000.
4. Порядок налаштування підлеглої станції СРШ-5000.
5. Безпроводові протоколи роботи СРШ-5000.

ЛАБОРАТОРНА РОБОТА № 11
НАЛАШТУВАННЯ РАДІОСТАНЦІЙ HYTERA

Мета:

1) ознайомитися з технічними характеристиками, можливостями та порядком налаштування радіостанцій Hytera HP 705;

2) отримати практичні навички з налаштування радіостанцій Hytera HP 705.

Початкові дані

У цій лабораторній роботі буде побудовано найпростішу схему (рис. 11.1) взаємодії транкінгових радіостанцій Hytera «кожен з кожним» у режимі групових викликів через канал прямого зв’язку (без ретранслятора).

Рисунок 11.1. Схема взаємодії радіостанцій Hytera HP 705 в радіомережі

Перелік мінімально необхідного обладнання та програмного забезпечення:

1) Мобільна радіостанція Hytera HP 705 – 2 шт. (це необхідний мінімум для перевірки працездатності радіоканалу).

2) Кабель для програмування (прошивки) радіостанцій Hytera HP 705 – 1 шт. (рис. 11.2).

Рисунок 11.2. Кабель для програмування радіостанцій Hytera HP705

3) Ноутбук або персональний комп'ютер (далі – ПК) із встановленим спеціалізованим програмним забезпеченням Hytera – 1 шт. (Customer Programming Software (далі – CPS), краще обирати найновішу версію, приклади зовнішнього вигляду ярликів – рис. 11.3).

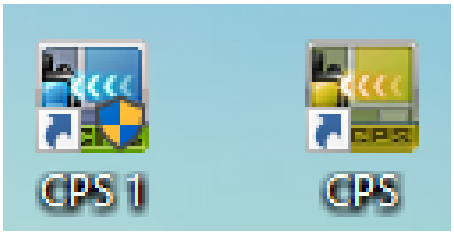

Рисунок 11.3. Зовнішній вигляд виконуваних файлів програмного забезпечення CPS

Хід роботи

1. Підключіть кабель для програмування до радіостанції Hytera (далі – PC), а також до одного з USB-портів до ПК.

2. Увімкніть PC.

3. Запустіть програму CPS.

3. Оберіть на верхній панелі **“Program-“ > “Read from Radio”** або натисніть **“Read”,** як наведено на рисунку 11.4):

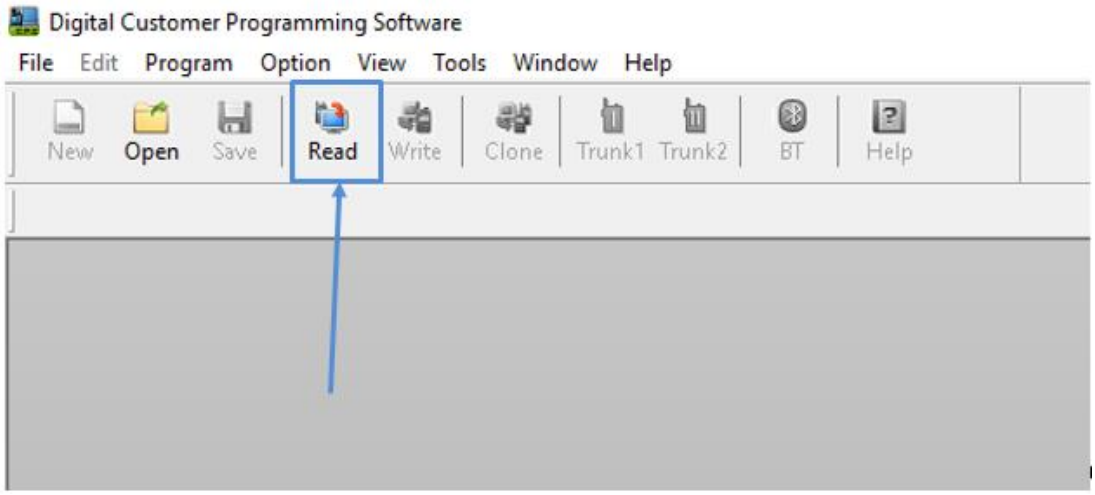

Рисунок 11.4. Зчитування конфігурації з радіостанції

4. У спливаючому вікні оберіть порт, до якого підключена PC, та натисніть **“OK”** (рис. 11.5).

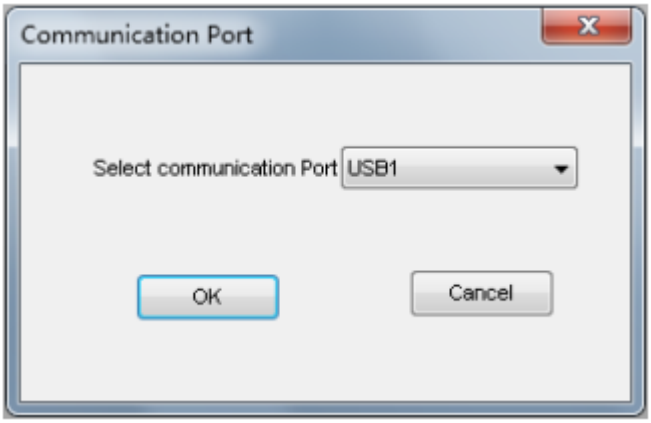

Рисунок 11.5. Меню обрання порта USB, до якого підключена PC

5. Далі натисніть **“ОК”** у вікні зчитування конфігурації (рис. 11.6).

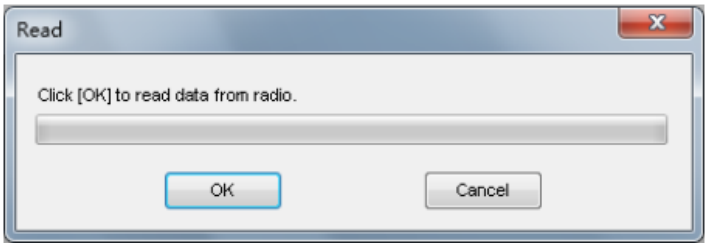

Рисунок 11.6. Спливаюче меню зчитування

6. Після зчитування конфігурації будуть доступні всі налаштування РС. **Змініть назву РС та її ID у відповідному меню, як наведено на рисунку 11.7,** для забезпечення можливості її обліку та розрізнення в радіомережі.

Примітка. *Після зчитування конфігурації РС можна від’єднати від ПК, зберегти конфігурацію в окремий файл і вносити правки в нього.*

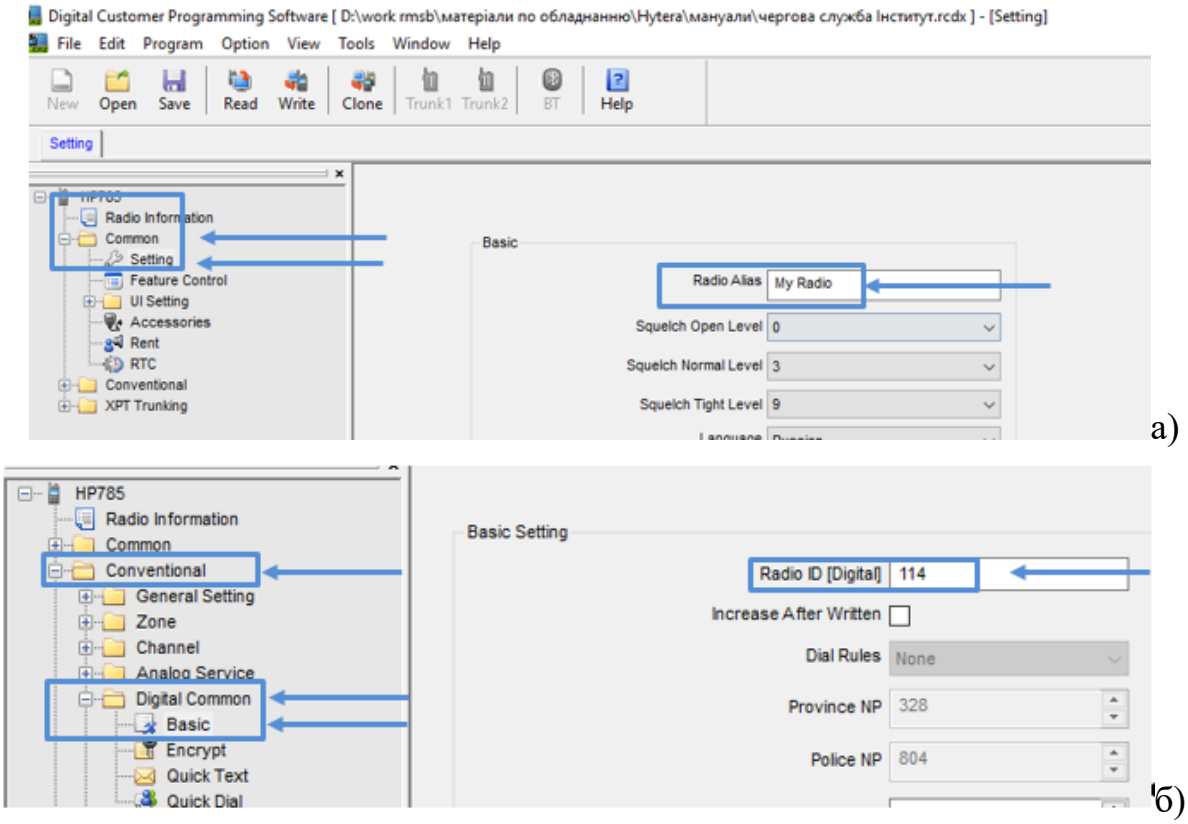

Рисунок 11.7. (а) – зміна імені РС; (б) – зміна ID РС

7. **Створення ключів шифрування** (рис. 11.8). Необхідно додати значення ключів шифрування для каналу, адже за замовчуванням ключі вимкнені. Довжину ключа можна змінити у полі **“Encrypt Key Length”**. Оберіть значення **“10 Characters”**, що відповідає 40-бітному ключу шифрування, який буде використаний далі. Ключ необхідно задавати максимально «рандомізованими» символами, які можна використовувати: 0-9, A-F.

<u>Важливо:</u> для зв’язку РС в межах однієї радіомережі ключ повинен бути однаковим на всіх РС.

Ім’я (*Key Alias*) та ID ключа (*Key ID*) використовуються винятково для ідентифікації ключів в межах конфігурації РС, тому варто їх називати так, щоб було зрозуміло безпосередньо користувачу.

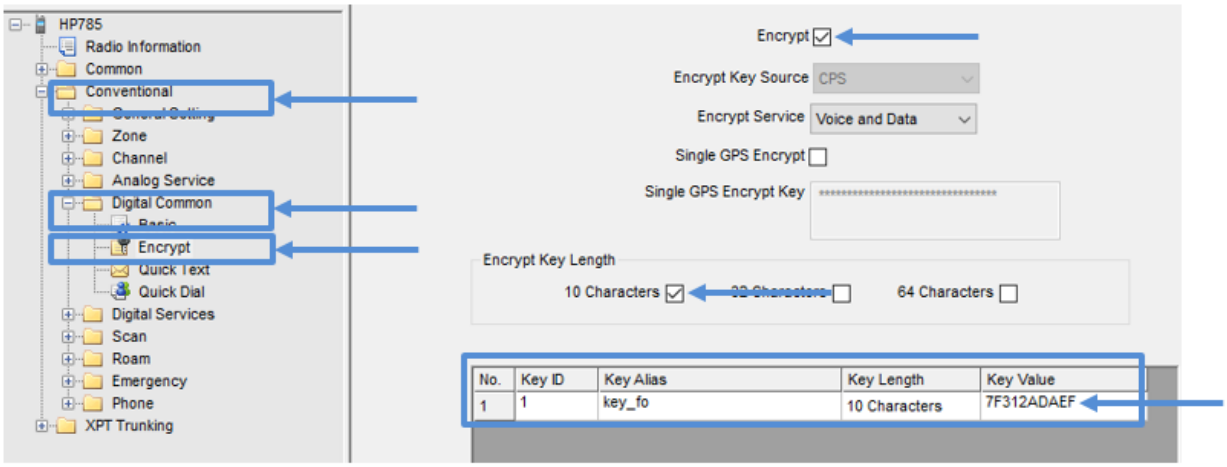

Рисунок 11.8. Створення ключа шифрування

8. **Створення контактів** (рис. 11.9). Після створення ключів треба налаштувати контакти, з якими буде працювати РС, групові та індивідуальні виклики. За схемою (рис. 11.1) буде створено один контакт в режимі групового виклику (*Call Alias* використовується винятково для ідентифікації контактів у межах конфігурації РС, тому варто їх називати так, щоб було зрозуміло безпосередньо користувачу).

<u>Важливо:</u> «Call ID» в режимі групового виклику повинен бути однаковим в межах однієї радіомережі.

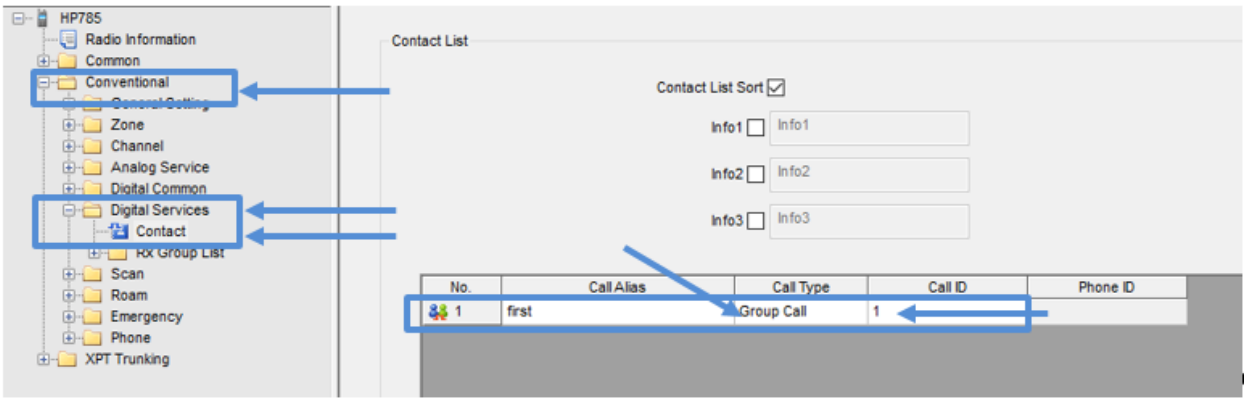

Рисунок 11.9. Створення контакту для групового виклику

9. **Створення груп прийому** (рис. 11.10). Після налаштування контактів, переходимо до цифрових груп прийому та додаємо до них контакти які будуть використовуватися (створені вище). Додавання та видалення контактів в групу здійснюється кнопками **“Add”** і **“Remove”** зі списку **“Available”** у список **“Members”** обраної групи прийому. На даному етапі необхідно залишити одну групу прийому з доданим одним контактом (створеним вище). Назва групи прийому (*Rx Group List Alias*) використовується також винятково для ідентифікації груп в межах конфігурації РС, тому варто їх називати так, щоб було зрозуміло безпосередньо користувачу.

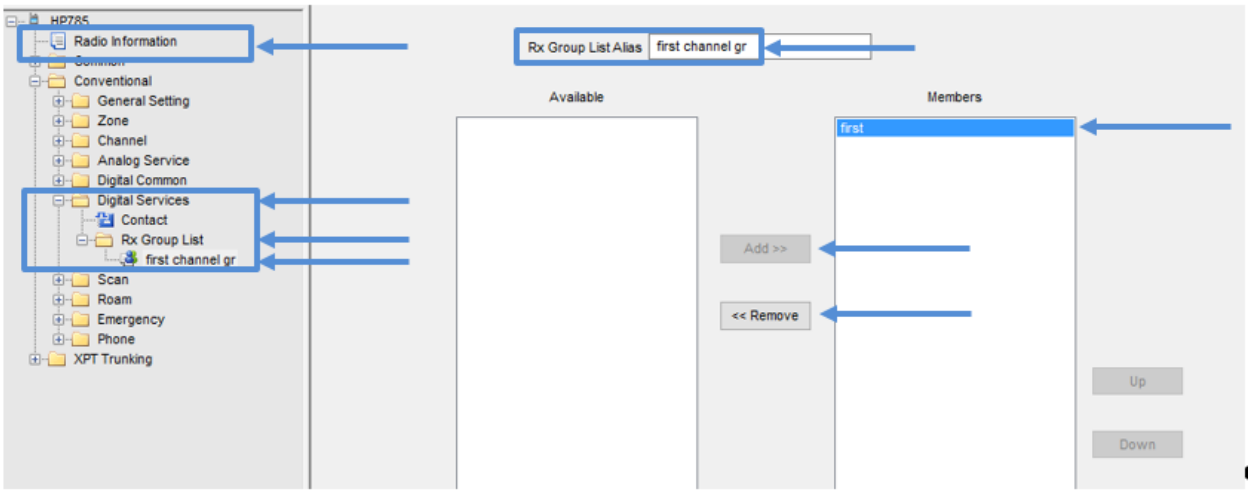

Рисунок 11.10. Створення груп прийому

10. **Налаштування цифрових каналів** (рис. 11.11). Спочатку залишіть один цифровий канал, усі інші цифрові канали – видалити кнопкою **“Remove”**.

Далі:

- введіть назву каналу в полі **“Channel Alias”** (ідентифікація в межах РС);
- введіть значення **“Color Code”** (має бути однаковим в межах радіомережі);
- виберіть **“Slot 1”** в полі **“Slot Operation”** (має бути однаковим в межах радіомережі);
- уведіть частоту прийому в полі **“Receive Frequency”** та групу прийому, створену раніше (дозволені частоти вказує викладач);
- уведіть частоту передачі в полі **“Transmit Frequency”** та контакт, створений раніше (дозволені частоти надає викладач);
- виберіть потужність передавача в полі **“Power Level”**;
- відмітьте галочкою **“Encrypt”**, оберіть **“Type encrypt”** – Full (відповідає алгоритму ARC4 при використанні 10-символьного ключа) та створений раніше ключ шифрування;
- інші параметри залишіть за замовчуванням.

11. **Налаштування зони** (рис 11.12):

- створити зону (залишити одну, усі інші видалити кнопкою “**Remove**”);
- ввести назву зони в полі “**Zone Alias**” (довільна назва, вона буде використана ідентифікацію в межах РС);
- кнопками “***Add***” і “***Remove***” додати до списку “**Members**” потрібні канали (у даному випадку один налаштований на попередньому етапі канал).

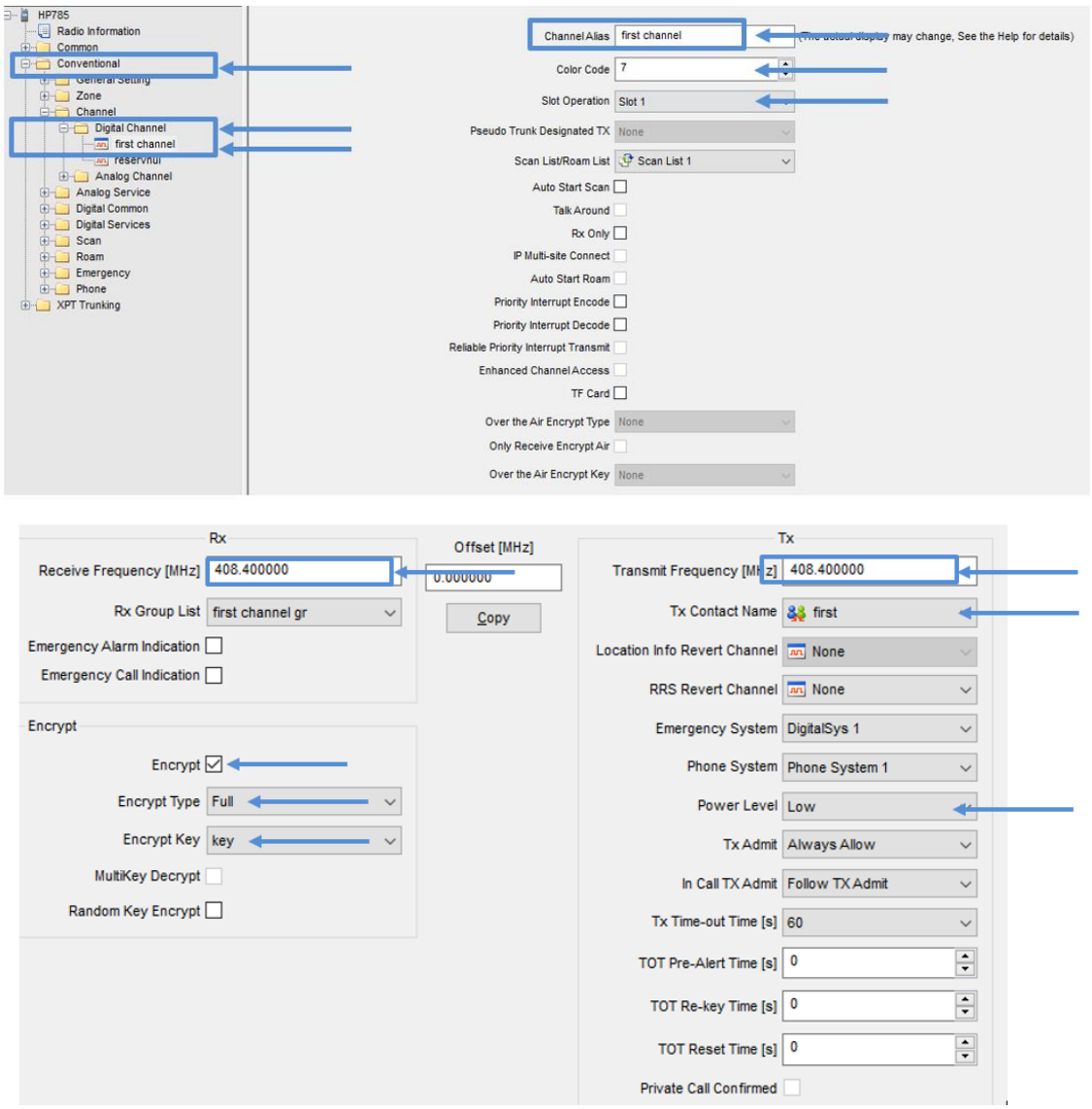

Рисунок 11.11. Налаштування цифрових каналів

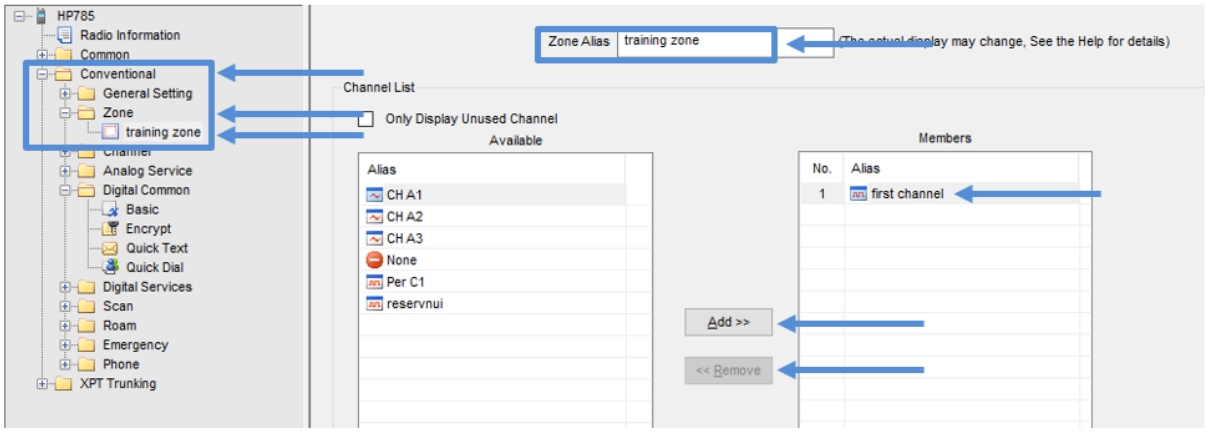

Рисунок 11.12. Налаштування зони

12. **Збережіть конфігурацію** собі на ПК для можливості подальшої конфігурації РС вашої радіомережі (рис. 11.13). Тобто ви можете багаторазово

використовувати один і той самий файл для запису налаштувань на однотипні радіостанції.

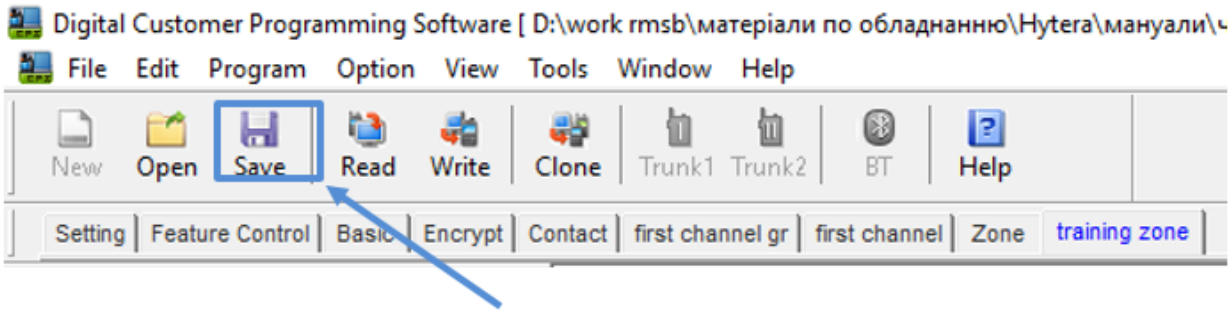

Рисунок 11.13. Збереження конфігурації

13. **Запишіть конфігурацію на радіостанцію** (**“Write”** – це функція використовується для запису на ту ж станцію, з якої була зчитана конфігурація, або в разі неспрацювання – **“Clone”**) (рис. 11.14).

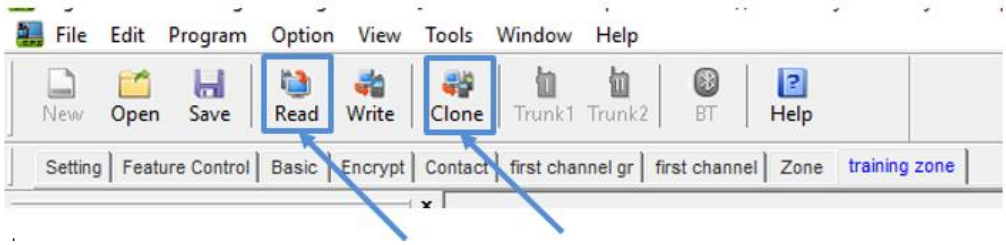

Рисунок 11.14. Запис конфігурації на PC

14. Після успішного запису конфігурації (повідомлення “**Successful”**) радіостанція перезавантажиться та буде готова до перевірки та експлуатації.

15. Підключіть іншу PC, повторіть вищезазначений п. 13 та перевірте працездатність радіомережі шляхом радіообміну.

Контрольні запитання

1. Яке призначення та особливості застосування радіостанцій Hytera HP705 та Hytera HM785?
2. Назвіть основні технічні характеристики радіостанцій Hytera HP705 та Hytera HM785.
3. Назвіть призначення органів управління радіостанцій Hytera HP705 та Hytera HM785.
4. Назвіть статус світлодіодної індикації радіостанцій та блока живлення.
5. Які особливості монтажу на транспортному засобі радіостанцій Hytera HM785?
6. Як здійснити базові операції на радіостанціях Hytera HP705 та Hytera HM785?
7. Наведіть алгоритм програмування радіостанцій Hytera HP705 та Hytera HM785.
8. Які символи можна використовувати при створенні ключа шифрування?
9. Які можливості розділення логічних каналів на одній частоті?
10. Як зчитати налаштування з радіостанції?
11. Що таке «прихований режим»? Як його включити?
12. Які параметри повинні співпадати, щоб зв’язати декілька радіостанцій в одну мережу, захищену ключем шифрування?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Офіційна документація MikroTik. [Електронний ресурс]: https://wiki.mikrotik.com/Main_Page.

2. Zen Vittore. Theory, laboratories and exercises for Mikrotik RouterOS. *Independently published*, 2021. 186 p.

3. Maher Haddad. MikroTik MTCNA – Student Guide: Prepare for the MikroTik MTCNA certification exam with step-by-step LABS on RouterOS v7. *Independently published*, 2022. 370 p.

4. Maher Haddad. MikroTik MTCSE – Student Guide: Prepare for the MikroTik MTCSE certification exam with step-by-step LABS on RouterOS v7. *Independently published*, 2023. 277 p.

5. Maher Haddad. MikroTik Switching with LABS: Master Switching on MikroTik – All Topics in the MTCSWE Certification Exam Are Covered. *Amazon Digital Services LLC – Kdp*, 2021. 219 p.

6. Maher Haddad. Multicast on MikroTik with LABS: Master Multicast on RouterOS using step-by-step LABS. *Independently published*, 2021. 117 p.

7. Головін Ю. О., Ніколаєнко Б. А., Бойко В. В., Сбоєв Р. Ю. Системи мобільного зв’язку. Застосування засобів мобільного зв’язку [Електронний ресурс] : навч. посіб. для здобувачів ступеня бакалавра за освіт. програмою «Спеціальні системи електронних комунікацій» спец. 172 «Електронні комунікації та радіотехніка» / КПІ ім. Ігоря Сікорського; Головін Ю. О., Ніколаєнко Б. А., Бойко В. В., Сбоєв Р. Ю. – Електронні текстові дані (1 файл: 8.49 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2023. – 187 с. URL: https://ela.kpi.ua/handle/123456789/63044.

8. Вакуленко О. В., Ніколаєнко Б. А. Станція радіорелейна широкосмугова СРШ-5000 (станція радіорелейна Р-402) [Електронний ресурс] : навчальний посібник для підготовки та проведення навчальних занять для курсантів (слухачів, студентів), які навчаються в Інституті за спеціальностями 172 “Телекомунікації та радіотехніка”, 122 “Комп’ютерні науки”, 125 “Кібербезпека” /

ІСЗЗІ КПІ ім. Ігоря Сікорського ; Вакуленко О. В., Ніколаєнко Б. А. – Електронні текстові данні (1 файл: 3.35 Мбайт). – Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2020. – 85 с. URL: https://ela.kpi.ua/handle/123456789/63044.

ПРИМІТКИ

ПРИМІТКИ