Навчально-методична література

Міністерство освіти і науки України
Тернопільський національний технічний університет
ім. Івана Пулюя
Кафедра комп'ютерно-інтегрованих технологій

Методичні вказівки до виконання лабораторних робіт

з дисципліни

«Управління інформаційною безпекою»

для студентів спеціальності 125 «Кібербезпека»

денної та заочної форми навчання

Тернопіль – 2022

Карташов В. В. Методичні вказівки до виконання лабораторних робіт з дисципліни «Управління інформаційною безпекою» для студентів спеціальності 125 «Кібербезпека» денної та заочної форми навчання / В. В. Карташов, Л. А. Романюк. // ТНТУ. – 2022. – С. 79.

Укладачі: к.т.н., Карташов В.В., Романюк Л.А.
Рецензент: д.т.н., проф. Марущак П.О.

Відповідальний за випуск: Карташов В.В.

Методичні вказівки до виконання лабораторних робіт з дисципліни «Управління інформаційною безпекою» для студентів спеціальності 125 «Кібербезпека» денної та заочної форми навчання розглянуто і схвалено на засіданні кафедри комп'ютерно-інтегрованих технологій

Протокол № 9 від " 16 " травня 2022 року.

Методичні вказівки до виконання лабораторних робіт з дисципліни «Управління інформаційною безпекою» для студентів спеціальності 125 «Кібербезпека» денної та заочної форми навчання схвалено та рекомендовано до друку науково-методичною комісією факультету прикладних інформаційних технологій та електроінженерії

Протокол № 9 від « 07 » червня 2022 року

ЗМІСТ

ВСТУП

На сучасному етапі розвитку техніки та промисловості відбувається масове використання інформаційних технологій і створення єдиного інформаційного простору, в рамках якого відбувається накопичення, обробка, зберігання та обмін інформацією. У зв’язку з цим проблеми інформаційної безпеки набувають першорядного значення в усіх сферах суспільної і державної діяльності. Особлива актуальність цих проблем визначається наступними чинниками:

• високими темпами зростання парку засобів обчислювальної техніки і зв'язку, розширенням областей використання ЕОМ, різноманіттям і повсюдним поширенням інформаційно-керуючих систем, які підлягають захисту;

• залученням до процесу інформаційної взаємодії все більшого числа людей і організацій, різким зростанням їх інформаційних потреб;

• підвищенням рівня попиту на автоматизовані системи управління і обробки інформації, використанням їх в критичних ситуаціях;

• ставленням до інформації, як до товару, переходом до ринкових відносин з властивою їм конкуренцією і промисловим шпигунством у сфері створення і надання інформаційних послуг;

• концентрацією великих обсягів інформації різного призначення на електронних носіях, вдосконалення доступу до інформаційних ресурсів;

• наявністю інтенсивного обміну інформацією між учасниками процесу;

• загостренням протиріч між об'єктивно існуючими потребами суспільства в розширенні вільного обміну інформацією і надмірними або навпаки недостатніми обмеженнями на її поширення і використання;

• рівнями втрат (збитків) від знищення, фальсифікації, розголошення або незаконного тиражування інформації;

• різноманіттям видів загроз і можливих каналів несанкціонованого доступу (НСД) до інформації;

• зростанням числа кваліфікованих користувачів обчислювальної техніки і можливостей по створенню ними програмно-математичних впливів на систему;

• відсутністю достатньої кількості кваліфікованих спеціалістів у сфері захисту інформації.

В такій ситуації виникає потреба в захисті комп’ютерних систем захисту інформації від несанкціонованого доступу, запозичення, знищення та інших злочинних і небажаних дій, число яких безперервно зростає. Так за оцінкою фахівців США, збиток від комп'ютерних злочинів щорічно складає близько 35 мільярдів доларів. В середньому збиток від одного комп'ютерного злочину становить близько 500-600 тисяч доларів. При цьому необхідно зазначити, що на сьогоднішній день:

• не існує єдиної теорії захищених систем, в достатній мірі універсальної в різних предметних областях (як в державному, так і в комерційному секторі);

• виробники засобів захисту, в основному, пропонують окремі компоненти для вирішення приватних завдань, залишаючи вирішення питань формування системи захисту і сумісності цих засобів своїм споживачам;

• для забезпечення надійного захисту необхідно вирішити цілий комплекс технічних і організаційних проблем з розробкою відповідної документації.

У методичних вказівках розглядаються тільки деякі з основних питань, зв'язаних із забезпеченням інформаційної безпеки. Матеріал підготовлений на основі робочої навчальної програми з дисципліни "Управління інформаційною безпекою" для студентів освітнього рівня бакалавр зі спеціальності 125 "кібербезпека".

Дисципліна має метою навчити студентів спеціалізованим заходам у сферах інформаційної та комп'ютерної безпеки, які забезпечують захист сучасних інформаційних систем у професійній діяльності, пов'язаної з отриманням, обробкою, накопиченням і захистом особистої та юридичної інформації, а також із захистом доступу.

Лабораторна робота № 1

Тема: Вивчення базових налаштувань пристроїв для організації спільного доступу до інформації

Мета: Навчитись налаштовувати роутер MikroTik

Хід виконання роботи.

Підключення роутера MikroTik

Для налаштування Wi - Fi роутера MikroTik нам знадобляться:

-кабель провайдера інтернету (Triolan, MaxNet, Воля, Airbites, Vega або будь-які інші);

-комп'ютер або ноутбук з Wi - Fi;

-роутер MikroTik. Він роздаватиме Інтернет по кабелю, а також по Wi - Fi на ноутбук, смартфон, телевізор з Wi - Fi або планшет.

Схема підключення роутера MikroTik (рис. 1.1)**:**

-кабель провайдера інтернету підключаємо в перший порт роутера;

-комп'ютер підключаємо до роутеру MikroTik мережевим кабелем у будь-якій LAN порт від 2 до 5;

-ноутбук і інші безпровідні пристрої підключимо по Wi - Fi;

-блок живлення включаємо в роз'єм "Power" роутера MikroTik.

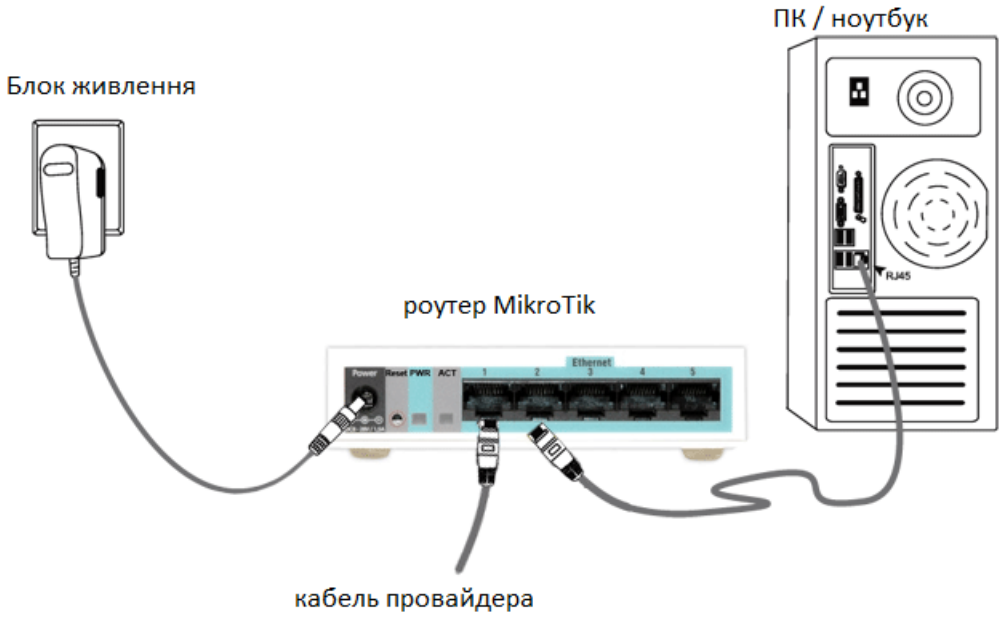


Рис. 1.1 – Схема підключення

Налаштування мережевої карти комп'ютера

Щоб на комп'ютері можна було зайти в налаштування роутера Mikrotik, налаштуємо мережеву карту на отримання автоматичних налаштувань. Відкриваємо "Пуск" → "Панель управління" → "Центр управління мережами і загальним доступом" (рис. 1.2).

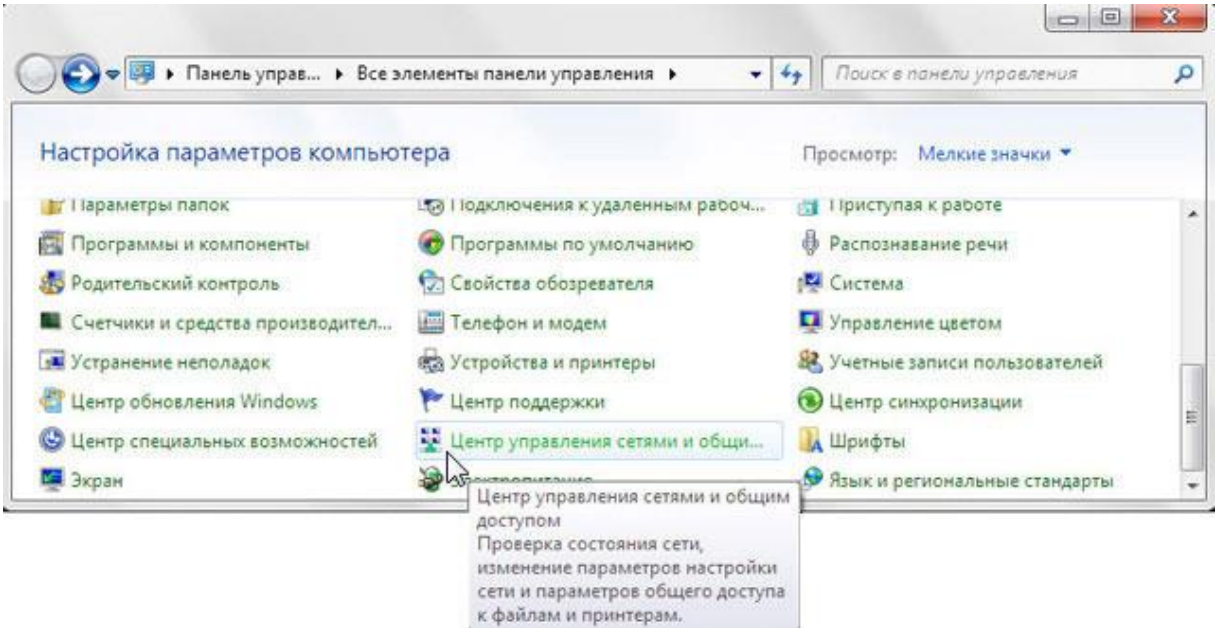


Рис. 1.2 – Панель керування

Перейдемо в "Зміну параметрів адаптера" (рис. 1.3).

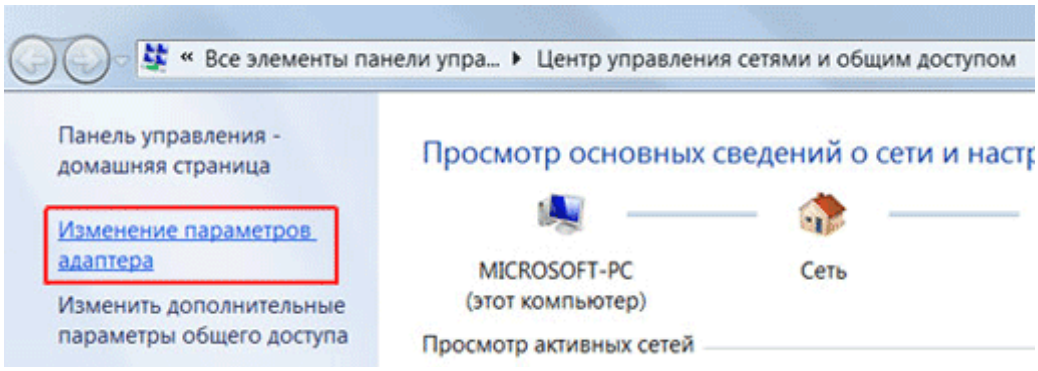


Рис. 1.3 – Перегляд основних відомостей

Натискаємо правою кнопкою миші на "Підключення по локальній мережі" і вибираємо "Властивості" (рис. 1.4):

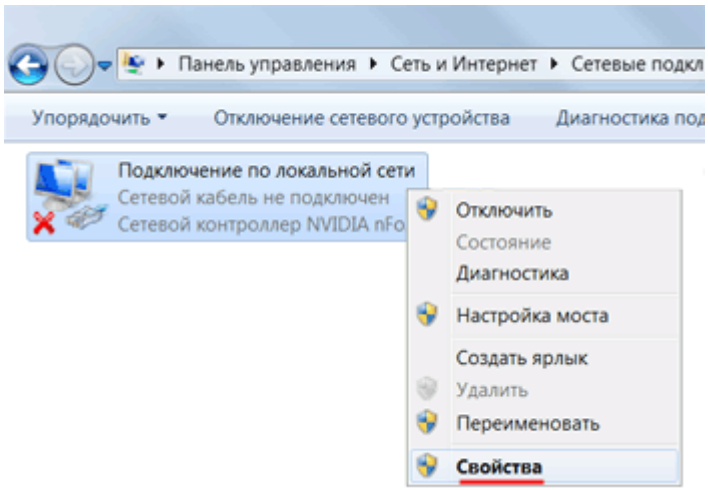


Рис. 1.4 - Властивості

Натискаємо на "Протокол Інтернету версії 4 (TCP/IPv4) " і кнопку "Властивості" (рис. 1.5).

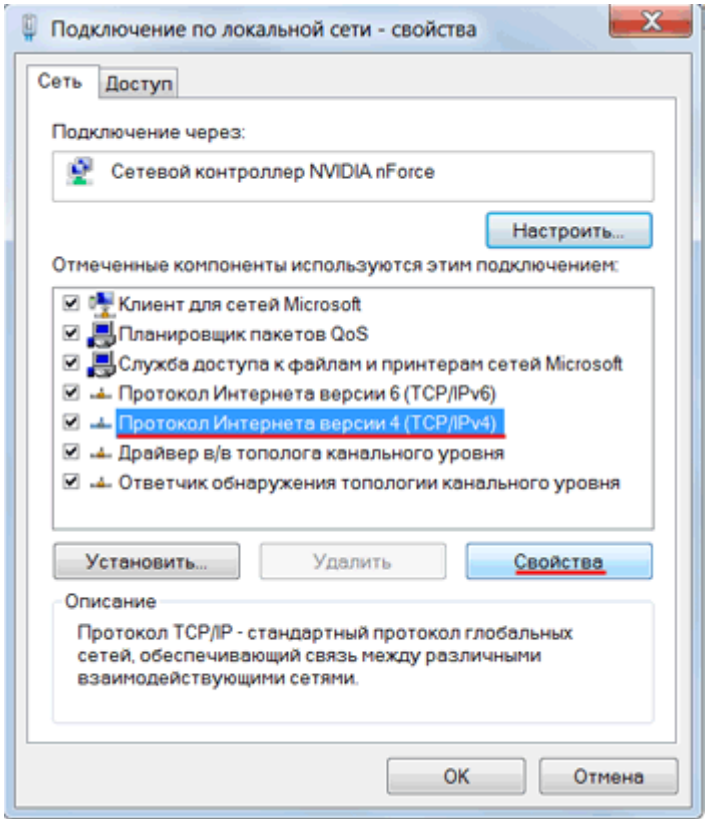


Рис. 1.5 – Протокол TCP/IP

Вибираємо "Отримати IP- адреса автоматично" і натискаєте кнопку "OK" (рис. 1.6).

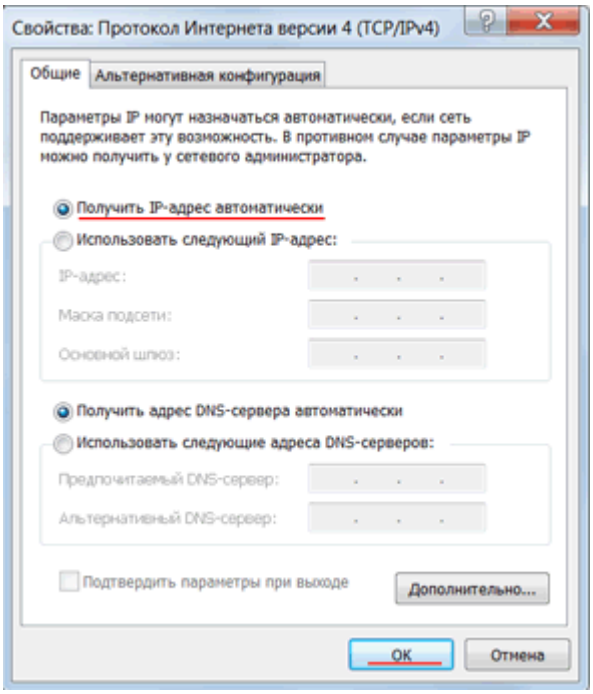


Рис. 1.6 – IP-адреса

Якщо мережева карта не отримує автоматично IP адреса з підмережі 192.168.88.x, спробуйте його вказати вручну(наприклад: 192.168.88.21) або скинути роутер Mikrotik до заводських налаштувань.

Вхід в налаштування роутера MikroTik

Виконати налаштування роутера MikroTik можна різними способами:

- За допомогою спеціальної програми Winbox для ОС Windows. Викачати на офіційному сайті.
- За допомогою браузеру, перейшовши за адресою 192.168.88.1. У налаштуваннях браузеру не має бути вказаний proxy- сервер!
- Налаштування через Telnet.

Ми налаштовуватимемо роутер Mikrotik за допомогою програми Winbox.

Підключаємося до роутеру MikroTik:

1. Запустіть програму Winbox і перейдіть на вкладку Neighbors;
2. У списку відобразиться ваш роутер. Натисніть лівою кнопкою миші на його MAC адреса;
3. Натисніть кнопку Connect.
4. Login за умовчанням admin, пароль порожній (рис. 1.7).

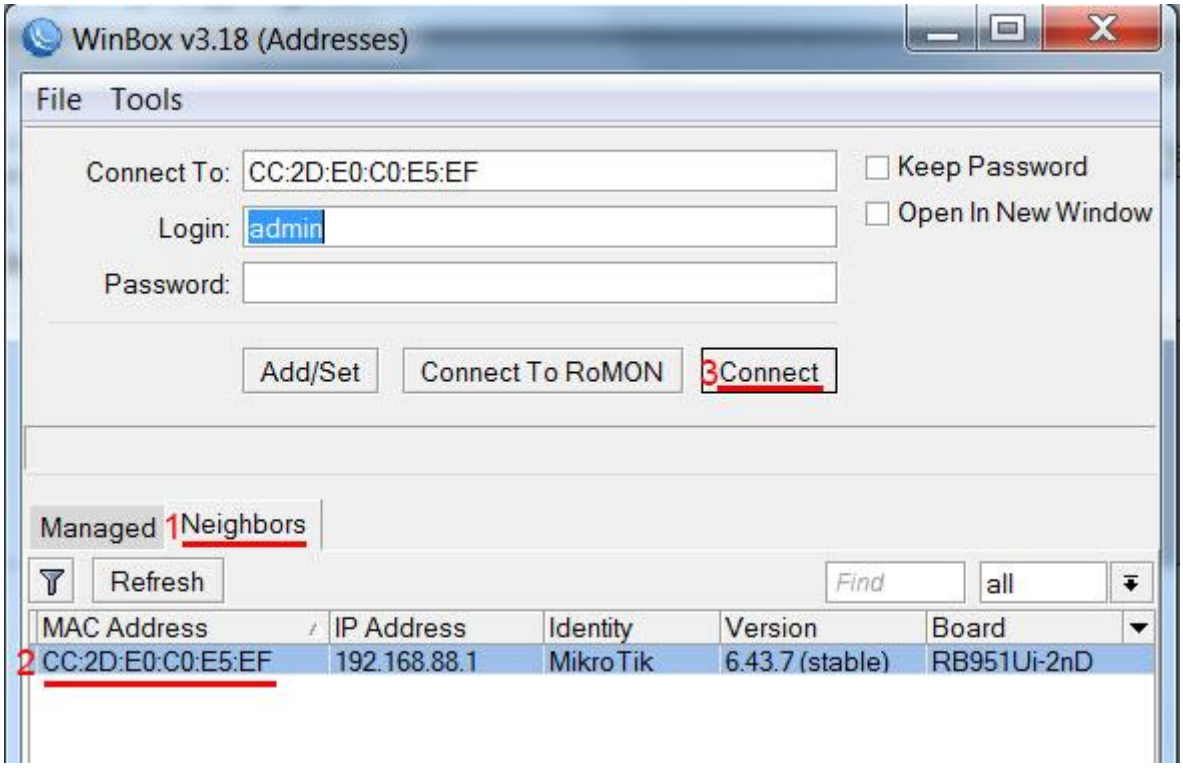


Рис. 1.7 – Підключення до WinBox

Скидання налаштувань роутера

Скинемо усі налаштування роутера MikroTik.

При першому вході у вас з'явиться вікно, як на картинці нижче. Натисніть кнопку Remove Configuration і дочекайтеся перезавантаження пристрою (рис. 1.8).

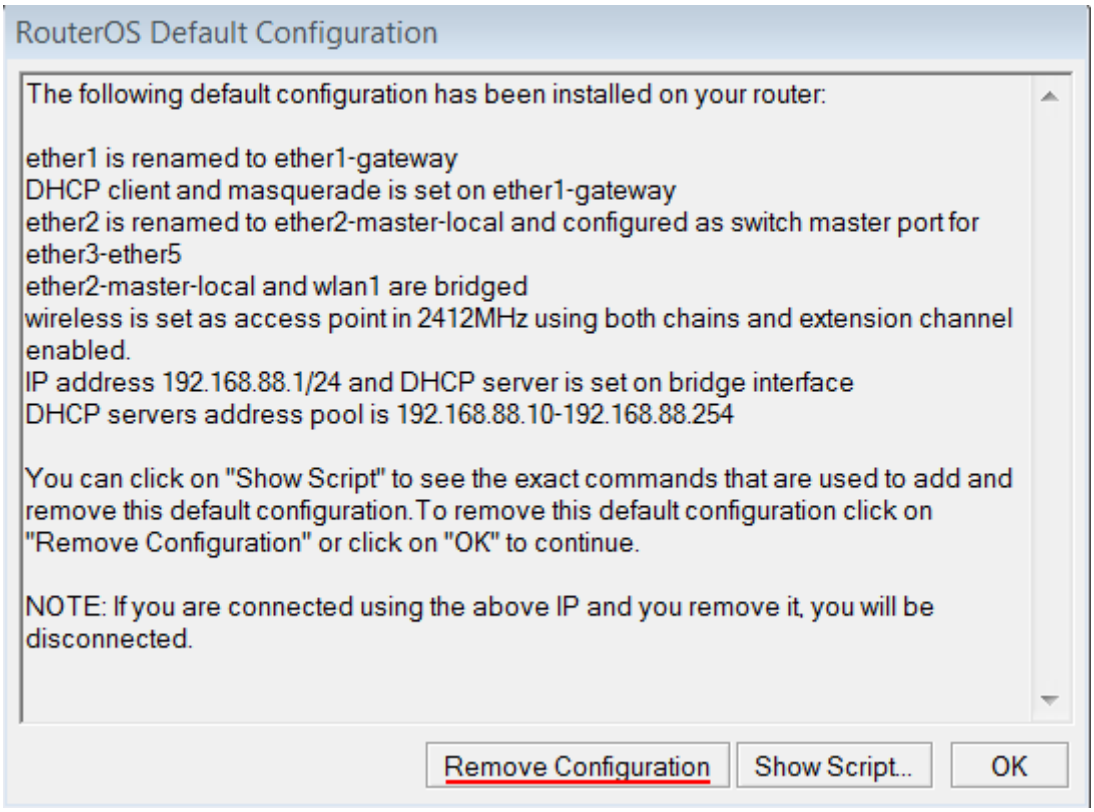


Рис. 1.8 – Скидання налаштувань при першому вході

Якщо у вас не з'явилося це вікно, **скинемо налаштування** через меню:

1. Вибираємо ліворуч меню **System - Reset Configuration**;
2. Поставте галочку **No Default Configuration**;
3. Натисніть кнопку **Reset Configuration**.
4. Натисніть кнопку **Yes** і дочекайтеся перезавантаження пристрою (рис. 1.9).

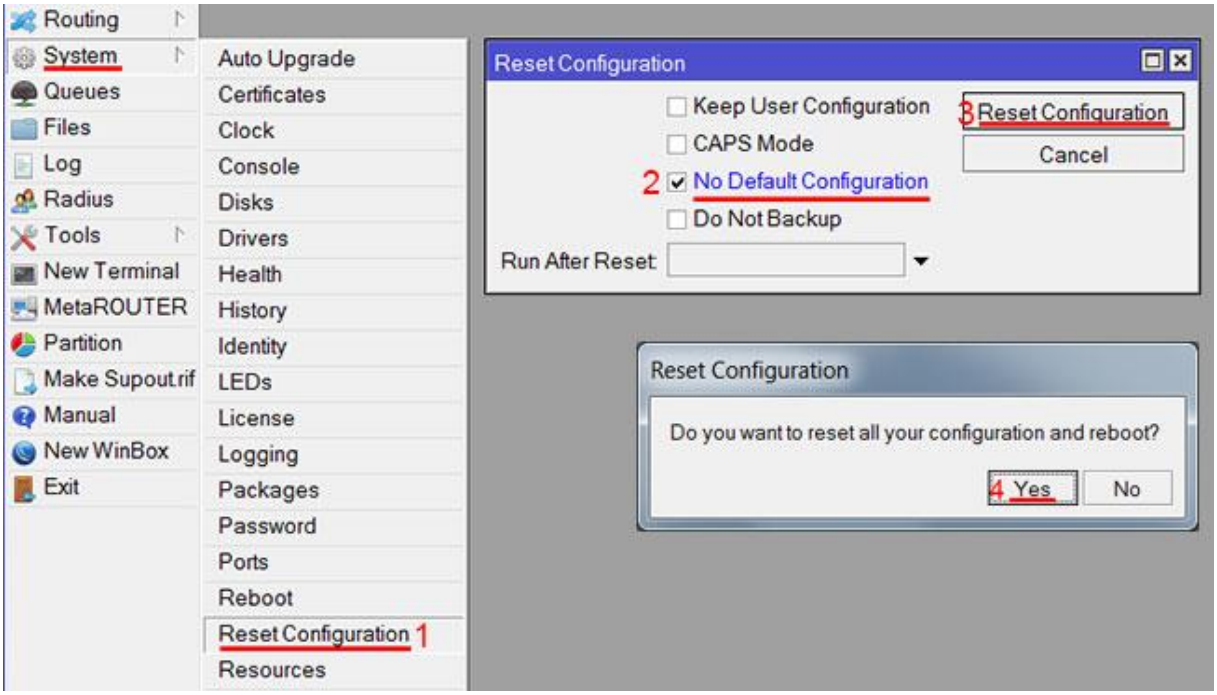


Рис. 1.9 -Скидання налаштувань через меню

Опис мережевих інтерфейсів

Конфігурація мережевих інтерфейсів MikroTik виглядатиме таким чином: перший порт ether1 буде підключений до провайдера(WAN порт), інші порти ether2 - 5 працюватимуть в режимі комутатора для підключення комп'ютерів локальної мережі.

Щоб не плутати мережеві інтерфейси, опишемо їх за допомогою коментарів.

Входимо в **налаштування MikroTik** за допомогою програми Winbox.

Записуємо для першого порту ether1 коментар "WAN" :

1. Відкриваємо меню **Interfaces**;
2. Вибираємо перший інтерфейс **ether1**;
3. Натискаємо жовту кнопку **Comment**;
4. У вікні, що з'явилося, вводимо коментар **"WAN"**;
5. Натискаємо кнопку **OK** (рис. 1.10).

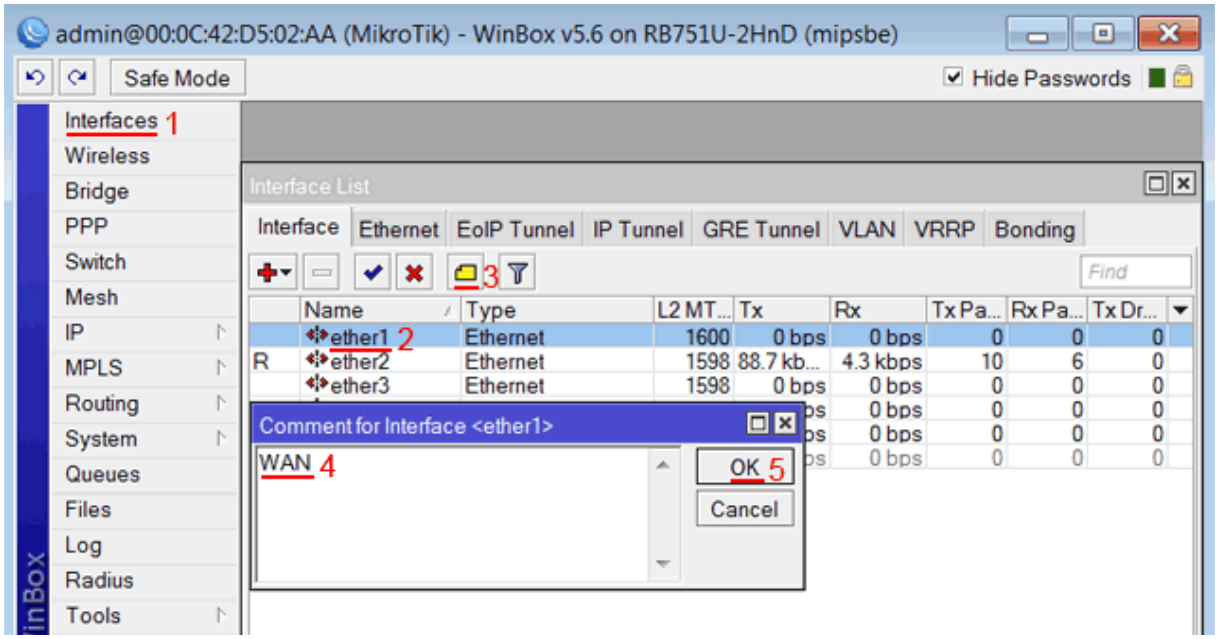


Рис. 1.10 – Коментар першого порту

Записуємо для другого порту ether2 коментар "LAN" :

1. Вибираємо інтерфейс ether2;
2. Натискаємо жовту кнопку Comment;
3. У вікні, що з'явилося, вводимо коментар "LAN";
4. Натискаємо кнопку OK (рис. 1.11).

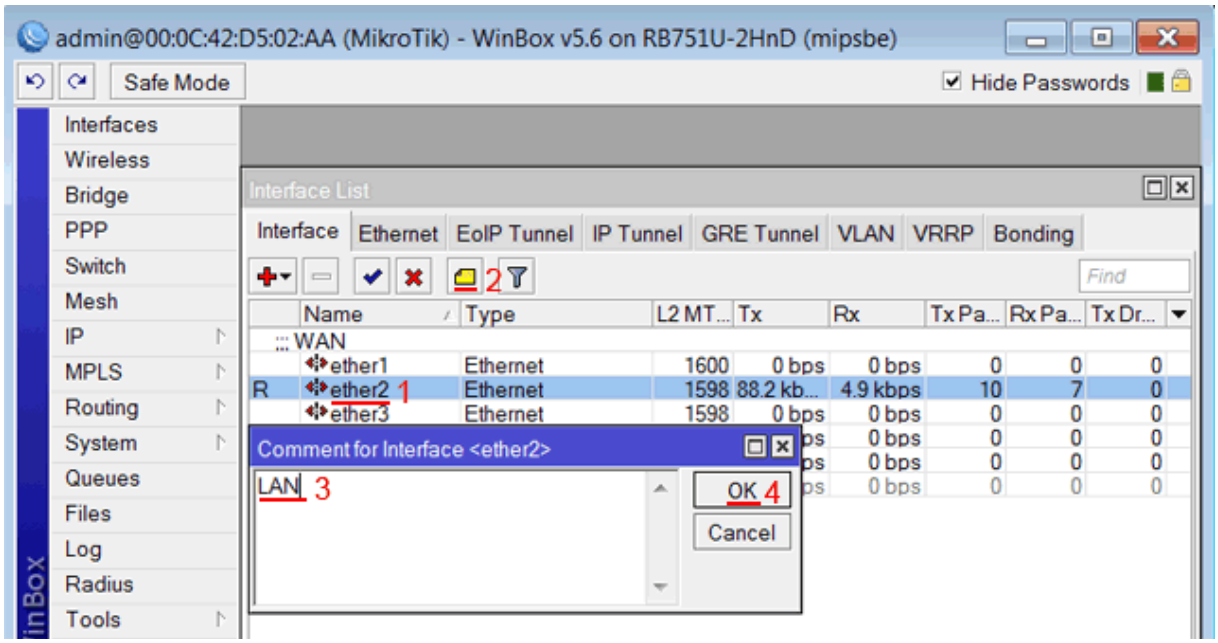


Рис. 1.11 – Коментар другого порту

Тепер в списку інтерфейсів чітко видно їх призначення (рис. 1.12).

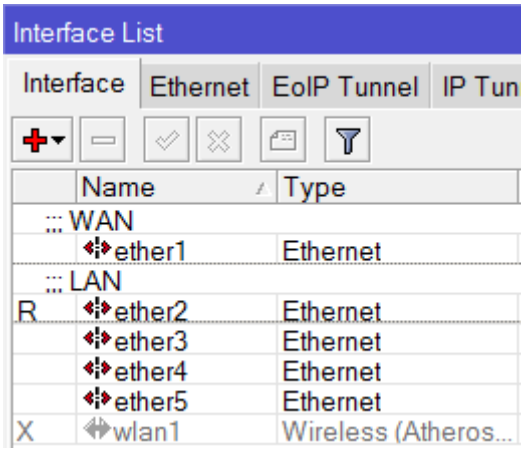


Рис. 1.12 – Список інтерфейсів

Налаштування WAN інтерфейсу MikroTik

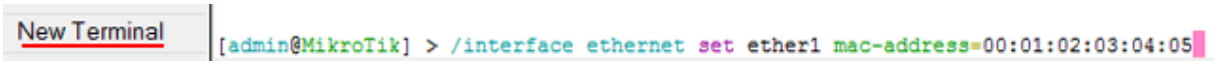
Зміна MAC адреси WAN порту (виключно при потребі)

Якщо Ваш провайдер блокує доступ до мережі по MAC адресі, то необхідно спочатку змінити MAC адреса WAN порту роутера MikroTik. Інакше пропустите цей пункт.

Щоб змінити MAC адреса порту MikroTik, відкриваємо в програмі Winbox меню **New Terminal** і вводимо команду:

/interface ethernet set ether1 mac - address=00 : 01: 02: 03: 04: 05

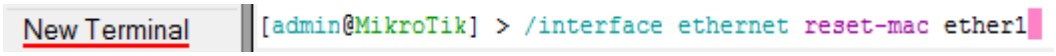
, де **ether1** - ім'я WAN інтерфейсу, **00: 01: 02: 03: 04: 05** - дозволена MAC адреса.



Щоб повернути рідну MAC адресу порту, треба виконати команду:

/interface ethernet reset - mac ether1

, де **ether1** - ім'я інтерфейсу.



Налаштування Dynamic IP

Якщо інтернет провайдер видає Вам мережеві налаштування автоматично, то необхідно настроїти WAN порт роутера MikroTik на отримання налаштувань по DHCP:

1. Відкриваємо меню IP;
2. Вибираємо DHCP Client;
3. У вікні, що з'явилося, натискаємо кнопку Add(плюсик);
4. У новому вікні в списку Interface : вибираємо WAN інтерфейс ether1;

5. Натискаємо кнопку OK для збереження налаштувань (рис. 1.13).

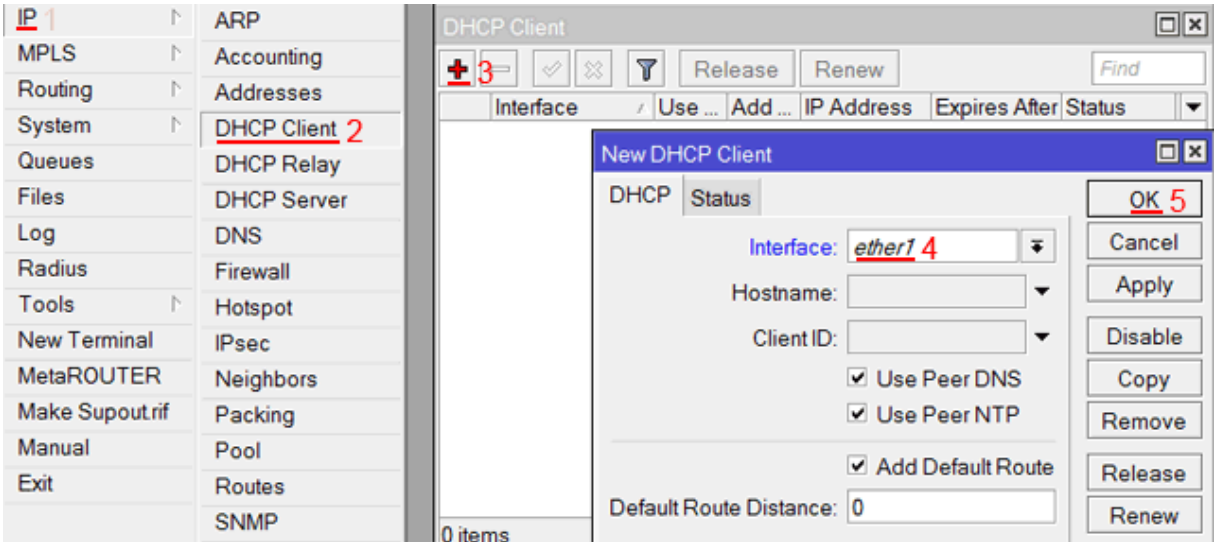


Рис. 1.13 – Налаштування по DHCP

Натискаємо кнопку Enable(синя галочка).

Тепер ми отримали IP адрес від провайдера, який відображається в стовпці IP Adress (рис. 1.14).

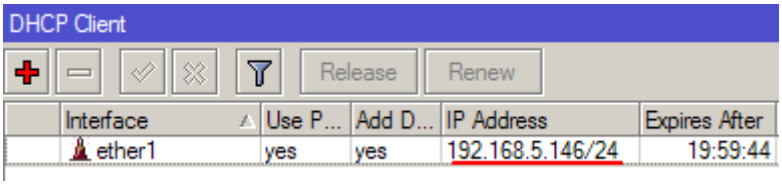


Рис. 1.14 - IP адрес

Перевіримо, що є зв'язок з інтернетом:

1. Відкриваємо меню New Terminal;
2. У терміналі пишемо команду ping www.google.com (пінгуем сайт google) і тиснемо Enter на клавіатурі.

Як бачимо, йдуть пінги по 60 ms, означає інтернет підключений і працює. Зупинити виконання команди можна комбінацією клавіш на клавіатурі Ctrl+C (рис. 1.15).

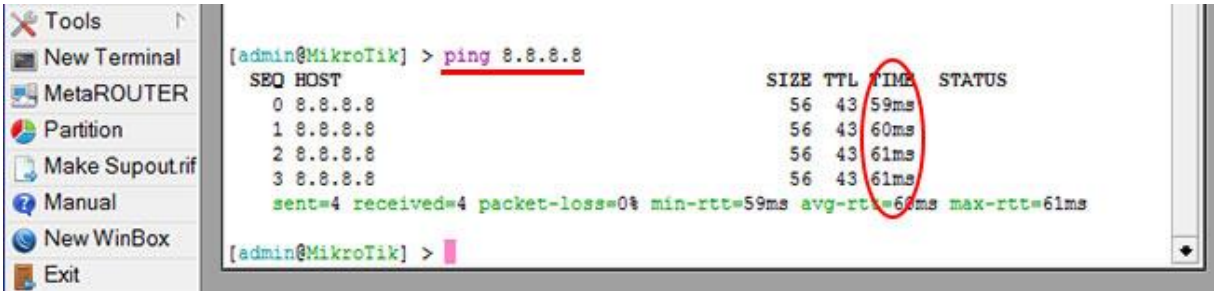


Рис. 1.15 – Перевірка з’єднання з мережею інтернет

На комп'ютерах, підключених до роутеру MikroTik, інтернет не працюватиме, поки ви не настроїте локальну мережу, Firewall і NAT.

Налаштування Static IP (параметри налаштування можуть відрізнятись від даних у методичці, в залежності від параметрів мережі Ethernet).

Якщо ви використовуєте статичні мережеві налаштування, необхідно настроїти WAN порт роутера MikroTik вручну.

Настроїмо статичну IP адресу і маску підмережі WAN порту MikroTik :

1. Відкриваємо меню IP;
2. Вибираємо Addresses;
3. У вікні, що з'явилося, натискаємо кнопку Add (плюсик);
4. У новому вікні в полі Address : прописуємо статичну IP адресу / маску підмережі;
5. У списку Interface : вибираємо WAN інтерфейс ether1;
6. Для збереження налаштувань натискаємо кнопку OK (рис. 1.16).

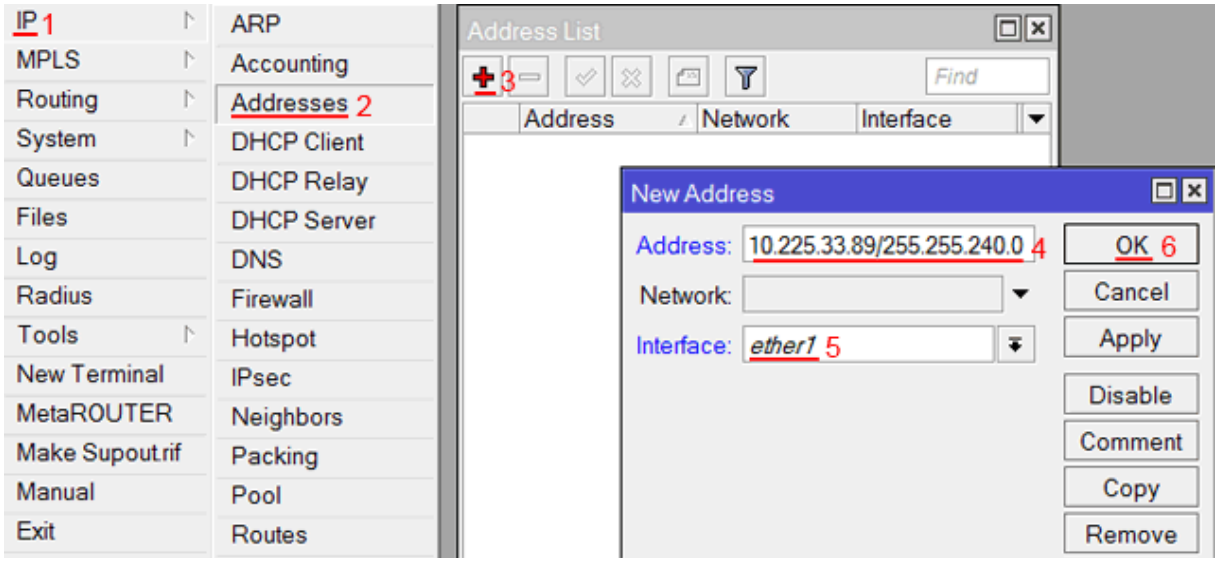


Рис. 1.16 – Статична IP-адреса

Настроїмо адресу інтернет шлюзу MikroTik :

1. Відкриваємо меню IP;
2. Вибираємо Routes;
3. У вікні, що з'явилося, натискаємо кнопку Add(плюсик);
4. У новому вікні в полі Gateway : прописуємо IP адреса шлюзу;
5. Натискаємо кнопку OK для збереження налаштувань (рис. 1.17).

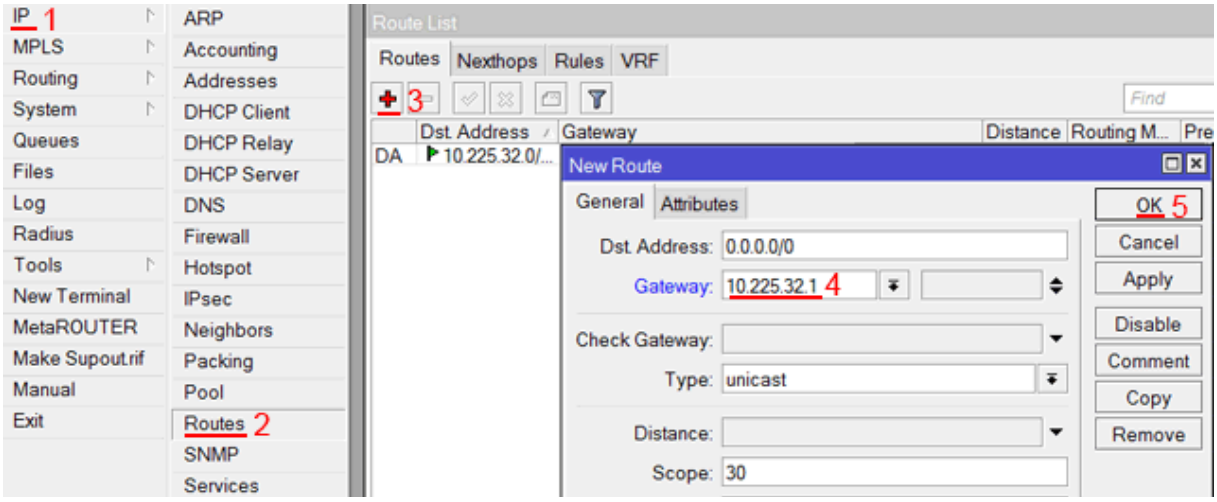


Рис. 1.17 – Адреса шлюзу

Додамо адреси DNS серверів MikroTik :

1. Відкриваємо меню IP;
2. Вибираємо DNS;
3. У вікні, що з'явилося, натискаємо кнопку Settings;
4. У новому вікні в полі Servers : прописуємо IP адреса DNS сервера, що віддається перевага;
5. Натискаємо кнопку "вниз"(чорний трикутник), щоб додати ще одне поле для введення;
6. У новому полі прописуємо IP адреса альтернативного DNS сервера;
7. Ставимо галочку Allow Remote Requests;
8. Натискаємо кнопку OK для збереження налаштувань (рис. 1.18).

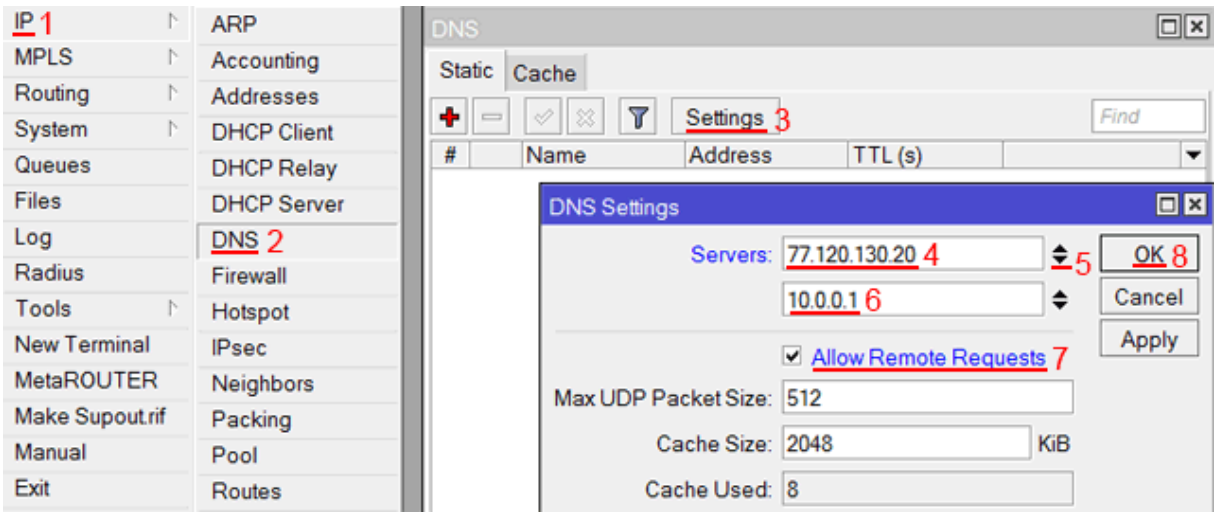


Рис. 1.18 – Адреса DNS-сервера

Перевіримо, що є доступ до інтернету:

1. Відкриваємо меню New Terminal;
2. У терміналі пишемо команду ping www.google.com (пінгуем сайт google) і тиснемо Enter на клавіатурі.

Як бачимо, йдуть пинги по 60ms, означає інтернет підключений і працює. Зупинити виконання команди можна комбінацією клавіш на клавіатурі Ctrl+C (рис. 1.19).

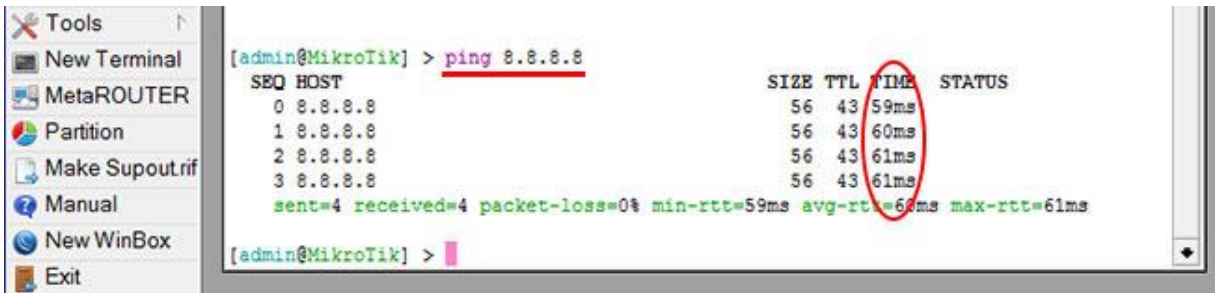


Рис. 1.19 – Повторна перевірка з’єднання

На комп'ютерах, підключених до роутеру MikroTik, інтернет не працюватиме, поки ви не настроїте локальну мережу, Firewall і NAT.

Налаштування PPPoE (при потребі)

Якщо ви використовуєте ADSL модем, до якого по мережевому кабелю підключений роутер MikroTik, спочатку необхідно настроїти ADSL модем в режим Bridge(міст).

Настроїмо клієнтське PPPoE з'єднання на роутере MikroTik:

1. Ліворуч вибираємо меню PPP;
2. Натискаємо кнопку Add(плюсик);
3. Вибираємо PPPoE Client (рис. 1.20).

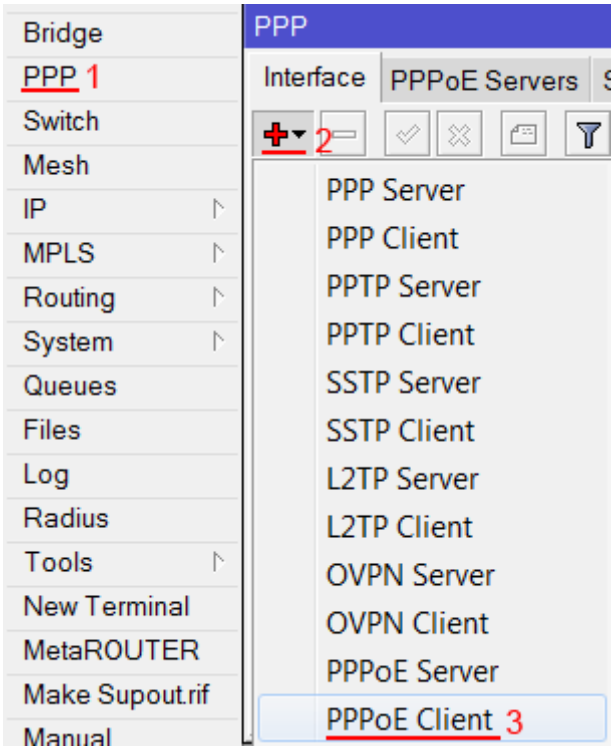


Рис. 1.20 - PPPoE клієнт

Налаштуємо параметри PPPoE з'єднання MikroTik :

1. У полі Name вказуємо ім'я з'єднання;
2. У списку Interfaces вибираємо перший WAN порт ether1, який підключений до провайдера (рис. 1.21);

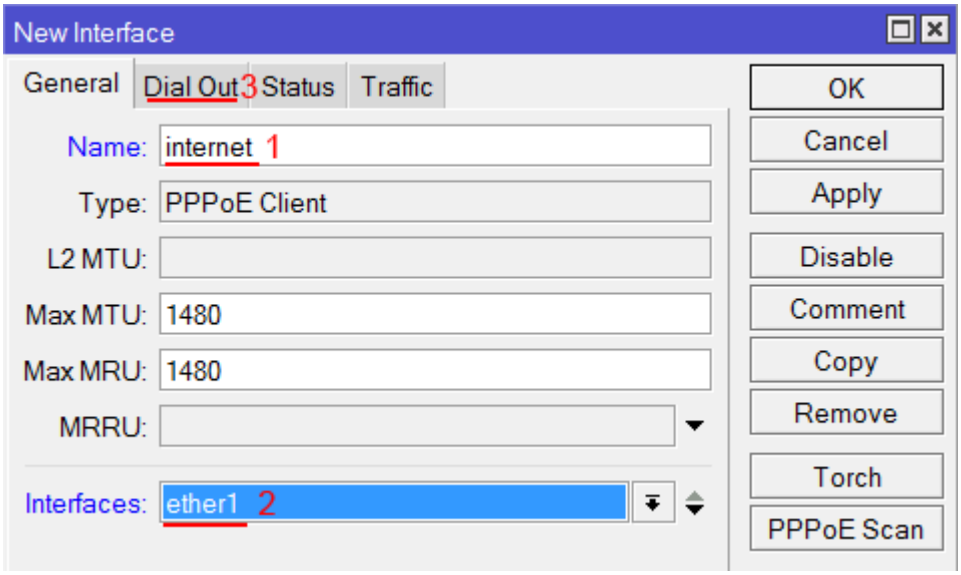


Рис. 1.21 – Загальні налаштування PPPoE з'єднання

3. Переходимо на вкладку Dial Out;
4. У полі User вказуємо ім'я користувача;
5. У полі Password вводимо пароль;

6. Ставимо галочку Use Peer DNS;
7. Натискаємо кнопку OK (рис. 1.22).

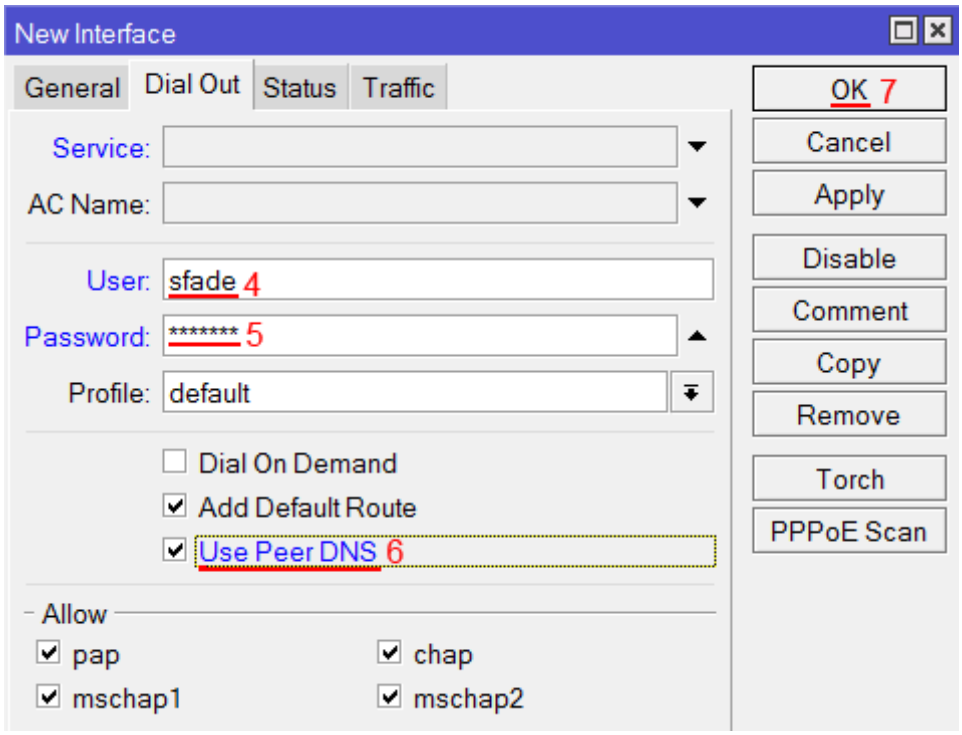


Рис. 1.22 – Новий інтерфейс

Після створення PPPoE з'єднання навпроти нього повинна з'явитися буква R, яка говорить про те, що з'єднання встановлене (рис. 1.23).

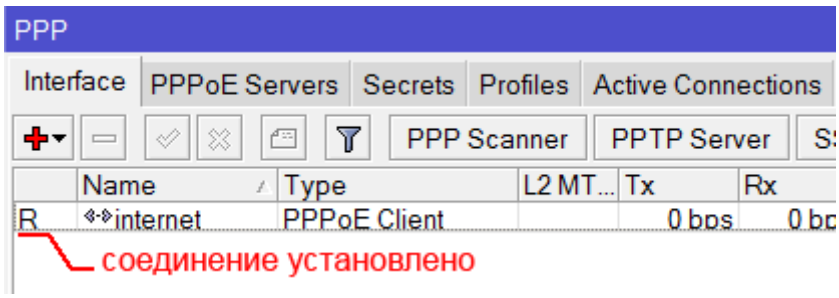


Рис. 1.23 – Інтерфейс PPPoE

Перевіримо, що є зв'язок з інтернетом:

1. Відкриваємо меню New Terminal;
2. У терміналі пишемо команду ping www.google.com (пінгуем сайт google) і тиснемо Enter на клавіатурі.

Як бачимо, йдуть пинги по 60ms, означає інтернет підключений і працює. Зупинити виконання команди можна комбінацією клавіш на клавіатурі Ctrl+C (рис. 1.24).

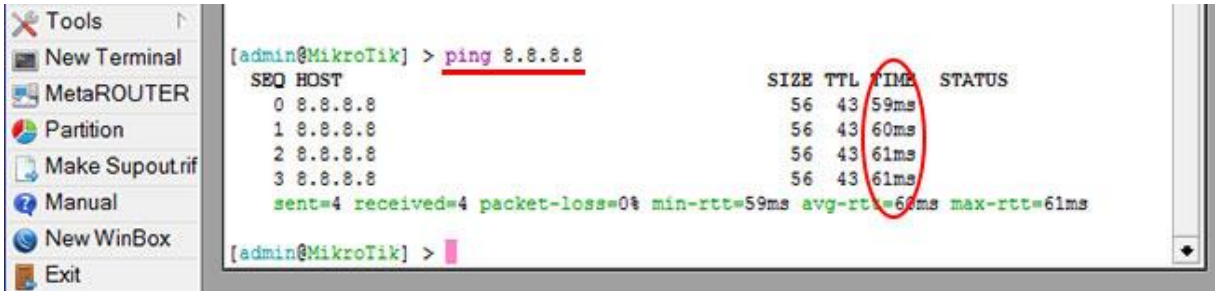


Рис. 1.24 – Перевірка зв’язку

На комп'ютерах, підключених до роутеру MikroTik, інтернет не працюватиме, поки ви не настроїте локальну мережу, Firewall і NAT.

Налаштування локальної мережі MikroTik

Об'єднання Wi - Fi і дротяних інтерфейсів в локальну мережу

Щоб комп'ютери, підключені до роутеру по кабелю і по Wi, - Fi, один одного «бачили», необхідно об'єднати безпровідною і дротяні інтерфейси MikroTik. Якщо у вас роутер без Wi - Fi, то об'єднуєте тільки дротяні інтерфейси.

Створюємо об'єднання bridge - local(міст);

1. Відкриваємо меню Bridge;
2. Натискаємо кнопку Add(плюсик);
3. У полі Name прописуємо ім'я об'єднання bridge - local;
4. Натискаємо кнопку OK (рис. 1.25).

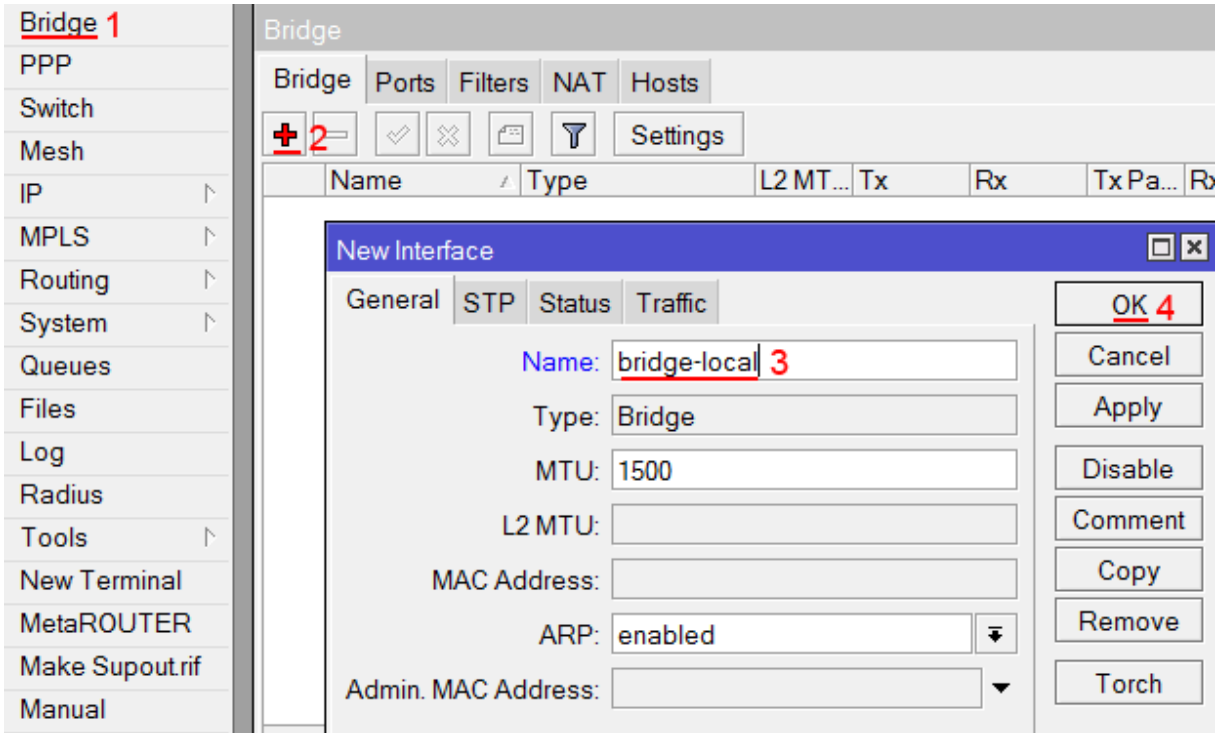


Рис. 1.25 – Інтерфейс вікна Bridge

Додаємо в об'єднання дротяні ethetnet порти 2-5:

1. Переходимо на вкладку Ports;
2. Натискаємо кнопку Add(плюсик);
3. У списку Interface вибираємо ethernet порт ether2;
4. У списку Bridge вибираємо ім'я об'єднання bridge - local;
5. Натискаємо кнопку OK (рис. 1.26);
6. Так само додаємо порти ether3, ether4, ether5.

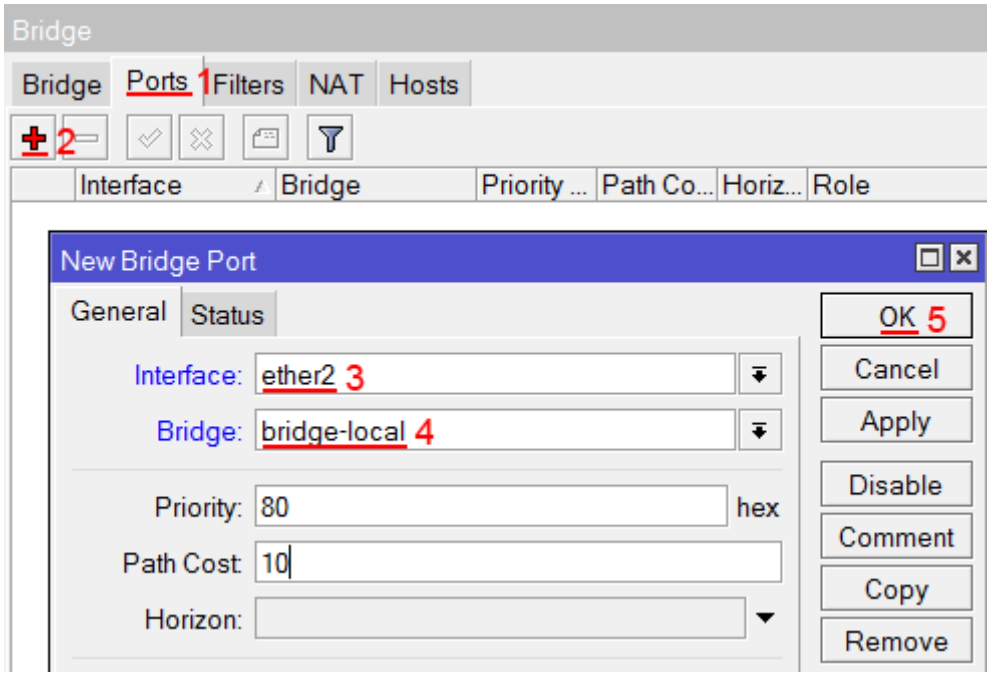


Рис. 1.26 – Параметри порту

Додаємо в об'єднання Wi - Fi інтерфейс.

1. Переходимо на вкладку Ports;
2. Натискаємо кнопку Add(плюсик);
3. У списку Interface вибираємо безпровідний інтерфейс wlan1;
4. У списку Bridge вибираємо ім'я об'єднання bridge - local;
5. Натискаємо кнопку OK (рис. 1.27).

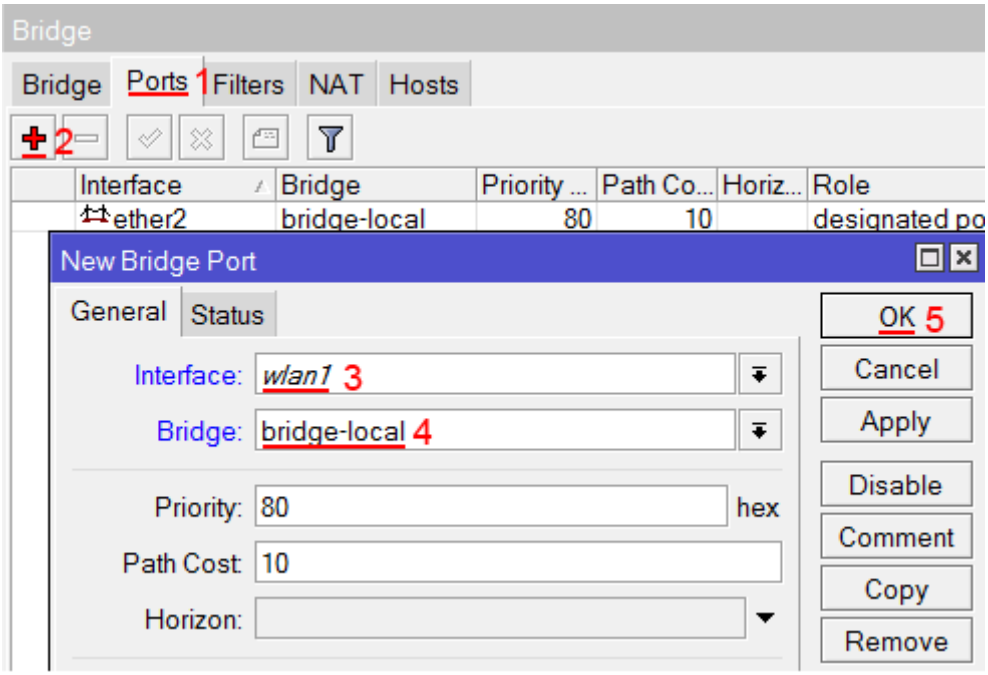


Рис. 1.27 – Параметри порту безпровідного інтерфейсу

Призначення IP адреси локальної мережі

Настроїмо IP адреса локальої мережі MikroTik :

1. Відкриваємо меню IP;
2. Вибираємо Addresses;
3. Натискаємо кнопку Add(плюсик);
4. У полі Address вводимо адресу і маску локальної мережі, наприклад 192.168.66.1/24;
5. У списку Interface вибираємо bridge - local;
6. Натискаємо кнопку OK (рис. 1.28).

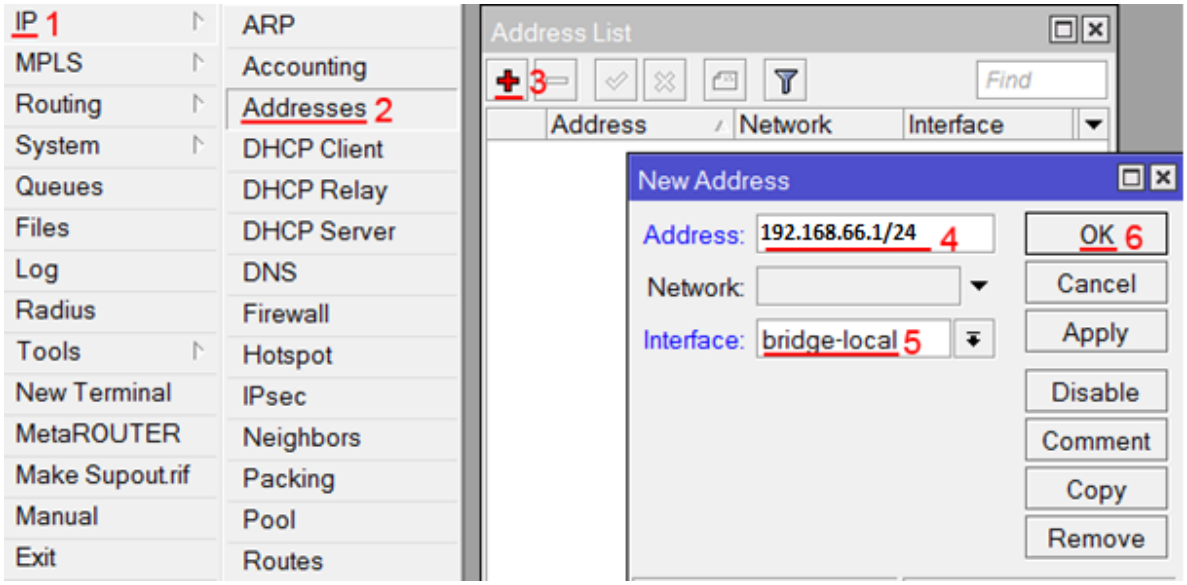


Рис. 1.28 – Адреса локальної мережі

Налаштування DHCP сервера

Щоб комп'ютери, підключені до роутеру, отримували мережеві налаштування автоматично, настроїмо DHCP сервер MikroTik :

1. Відкриваємо меню IP;
2. Вибираємо DHCP Server;
3. Натискаємо кнопку DHCP Setup (рис. 1.29);

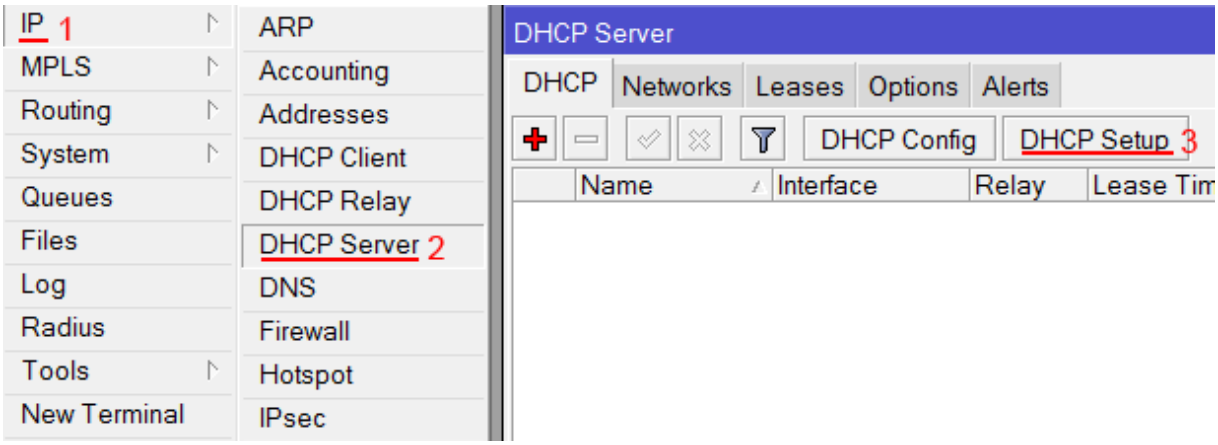


Рис. 1.29 – Вікно DHCP-сервера

4. У списку DHCP Server Interface вибираємо bridge - local;
5. Натискаємо кнопку Next (рис. 1.30);

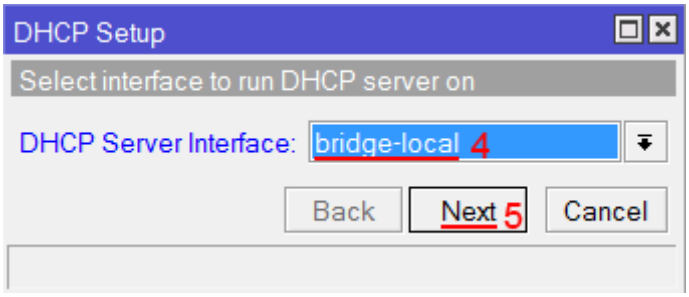


Рис. 1.30 – Інтерфейс DHCP-сервера

6. У цьому вікні вибирається мережа для DHCP. Залишаємо без змін і натискаємо кнопку Next (рис. 1.31);

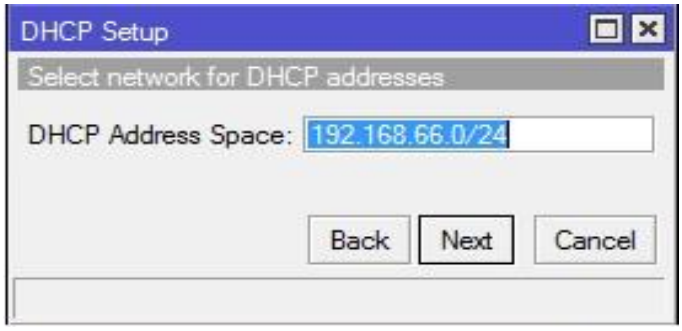


Рис. 1.31 – Адреса DHCP-сервера

7. У наступному вікні вказується адреса шлюзу. Натискаємо кнопку Next;

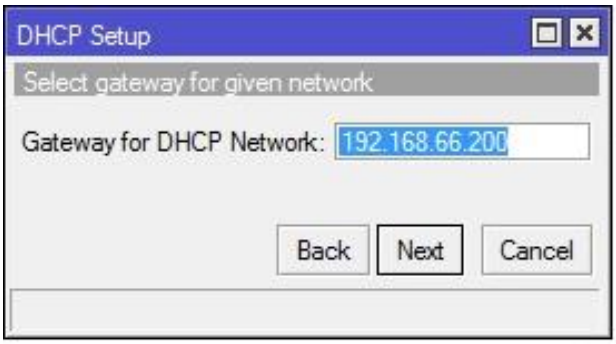


Рис. 1.32 – Адреса шлюзу DHCP-сервера

8. У цьому вікні прописується діапазон IP адрес, які роздаватиме DHCP сервер. Натискаємо кнопку Next (рис. 1.33);

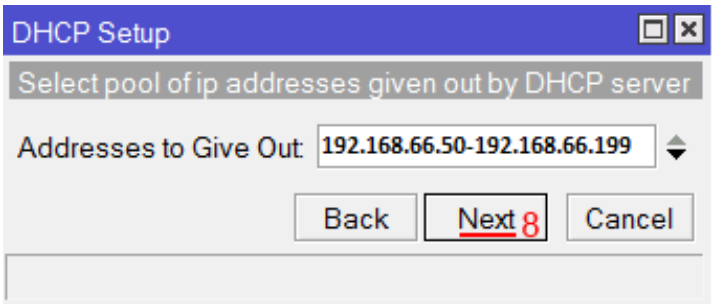


Рис. 1.33 – Діапазон IP-адрес

9. Далі вводяться адреси DNS серверів. Натискаємо кнопку Next (рис. 1.34);

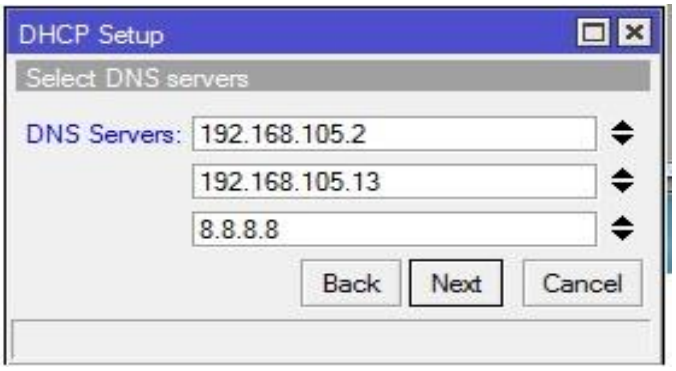


Рис. 1.34 – Адреси DNS-серверів

10. Тут задається час резервування IP адрес. Натискаємо кнопку Next (рис. 1.35);

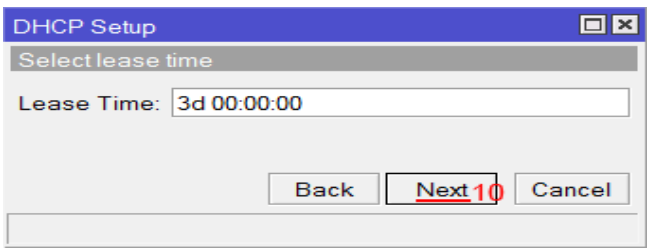


Рис. 1.35 – Налаштування часу

11. Налаштування DHCP сервера успішно завершене. Тиснемо кнопку OK (рис. 1.36).

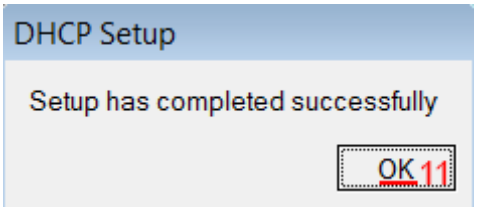


Рис. 1.36 – Завершення налаштування

Тепер мережевий кабель комп'ютера відключаємо від роутера і ще раз підключаємо до нього.

Налаштування Wi - Fi точки доступу MikroTik

Спочатку необхідно включити Wi - Fi модуль:

1. Відкриваємо меню Wireless;
2. Вибираємо Wi - Fi інтерфейс wlan1;
3. Натискаємо кнопку Enable (синя галочка) (рис. 1.37).

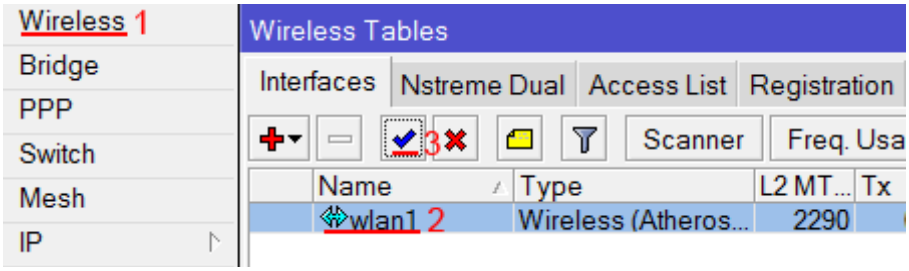


Рис. 1.37 – Інтерфейс бездротового зв’язку

Створюємо пароль для підключення до точки доступу MikroTik :

1. Відкриваємо вкладку Security Profiles;
2. Натискаємо кнопку Add(плюсик);
3. У новому вікні в полі Name : вказуємо ім'я профілю безпеки;
4. Для кращої безпеки залишаємо тільки реєстрацію по протоколу WPA2 PSK;
5. У полі WPA2 Pre - Shared Key вводимо пароль для доступу до Wi - Fi точці;
6. Для збереження налаштувань натискаємо кнопку OK (рис. 1.38).

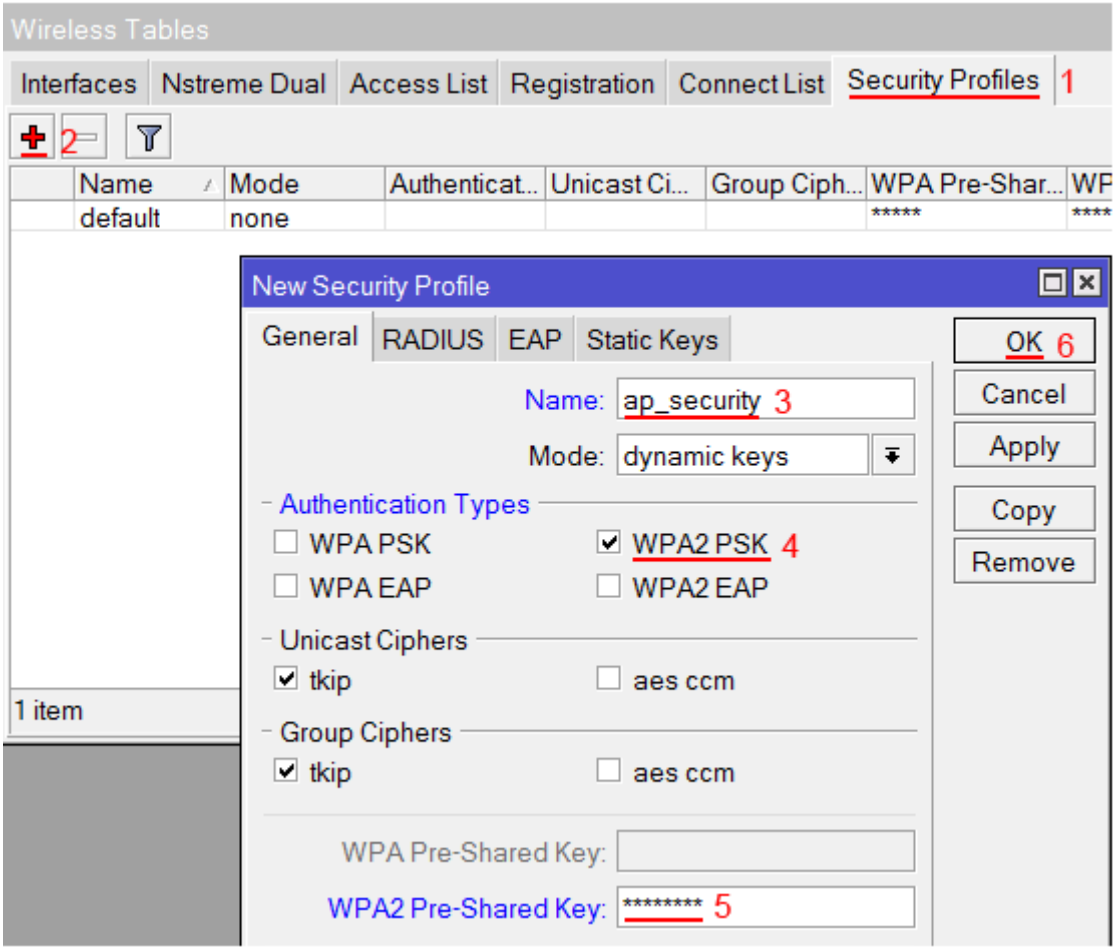


Рис. 1.38 – Налаштування безпеки

Настроюємо параметри Wi - Fi точки MikroTik :

1. Відкриваємо вкладку Interfaces;
2. Робимо подвійний клік кнопкою миші на Wi - Fi інтерфейсі wlan1, щоб зайти в його налаштування;
3. Переходимо на вкладку Wireless;
4. У списку Mode : вибираємо режим роботи ap bridge(точка доступу в режимі моста);
5. У списку Band : вибираємо в яких стандартах працюватиме Wi - Fi точка, ми вибрали B/G/N;
6. У полі SSID : прописуємо ім'я точки доступу;
7. У списку Security Profile вибираємо ім'я профілю безпеки, в якому ми створювали пароль для доступу до Wi, - Fi точці. Якщо поля Security Profile немає у списку, шукаємо і натискаємо кнопку Advanced у правому списку;
8. Натискаємо кнопку OK для збереження налаштувань (рис. 1.39).

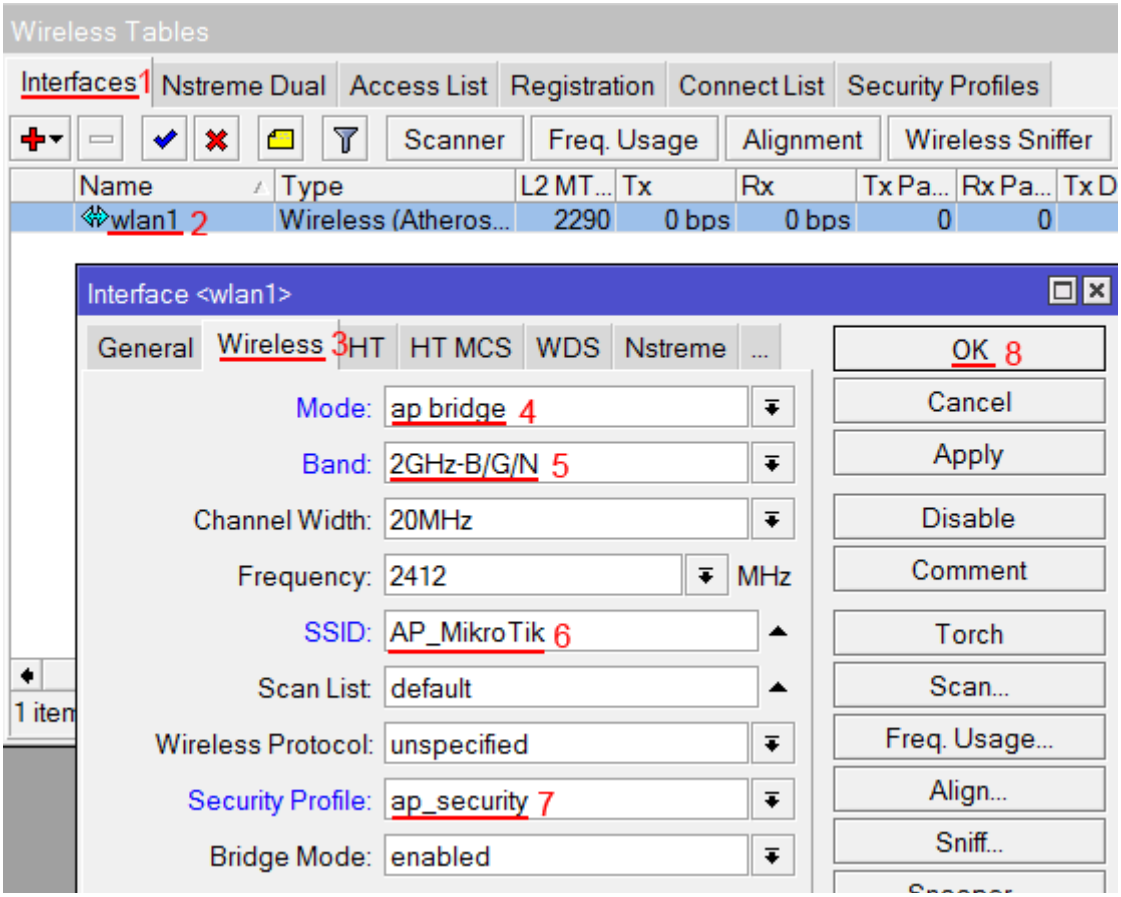


Рис. 1.39 – Налаштування параметрів Wi - Fi точки

Тепер можна підключатися до роутеру по Wi - Fi.

На комп'ютерах, підключених до роутеру MikroTik по Wi, - Fi, інтернет не працюватиме, поки ви не настроїте Firewall і NAT.

Налаштування Firewall і NAT

Щоб комп'ютери діставали доступ до інтернету, необхідно настроїти Firewall і NAT на роутере MikroTik.

Відкрийте меню New Terminal для введення команд.

Налаштування NAT виконується наступними командами:

```
ip firewall nat add chain=srcnat out - interface=ether1 action=masquerade
```

, де ether1 - це інтерфейс, на який приходить інтернет від провайдера. Для PPPoE з'єднань вказується назва PPPoE інтерфейсу.

Налаштування NAT досить, щоб запрацював інтернет.

Опціональний список захисних команд:

Protect router - команди для захисту роутера :

```
ip firewall filter add action=accept chain=input disabled=no protocol=icmp
```

```
ip firewall filter add action=accept chain=input connection - state=established disabled=no in - interface=ether1
ip firewall filter add action=accept chain=input connection - state=related disabled=no in - interface=ether1
ip firewall filter add action=drop chain=input disabled=no in - interface=ether1
```

Protect LAN - захист внутрішньої мережі :

```
ip firewall filter add action=jump chain=forward disabled=no in - interface=ether1 jump - target=customer
ip firewall filter add action=accept chain=customer connection - state=established disabled=no
ip firewall filter add action=accept chain=customer connection - state=related disabled=no
ip firewall filter add action=drop chain=customer disabled=no
```

Призначаємо типи інтерфейсів для захисту внутрішньої мережі(external - зовнішній, internal - внутрішній LAN) :

```
ip upnp interfaces add disabled=no interface=ether1 type=external
ip upnp interfaces add disabled=no interface=ether2 type=internal
ip upnp interfaces add disabled=no interface=ether3 type=internal
ip upnp interfaces add disabled=no interface=ether4 type=internal
ip upnp interfaces add disabled=no interface=ether5 type=internal
ip upnp interfaces add disabled=no interface=bridge - local type=internal
```

Зміна пароля доступу до роутеру MikroTik

Щоб змінити пароль доступу до роутеру MikroTik, виконаєте наступні дії:

Відкриваємо меню System;

Вибираємо Users;

Робимо подвійний клік кнопкою миші на користувачі admin;

Натискаємо кнопку Password...;

У полі New Password вводимо новий пароль;

У полі Confirm Password підтверджуємо новий пароль;

У вікні Change Password натискаємо кнопку OK;

У вікні User натискаємо кнопку OK (рис. 1.40).

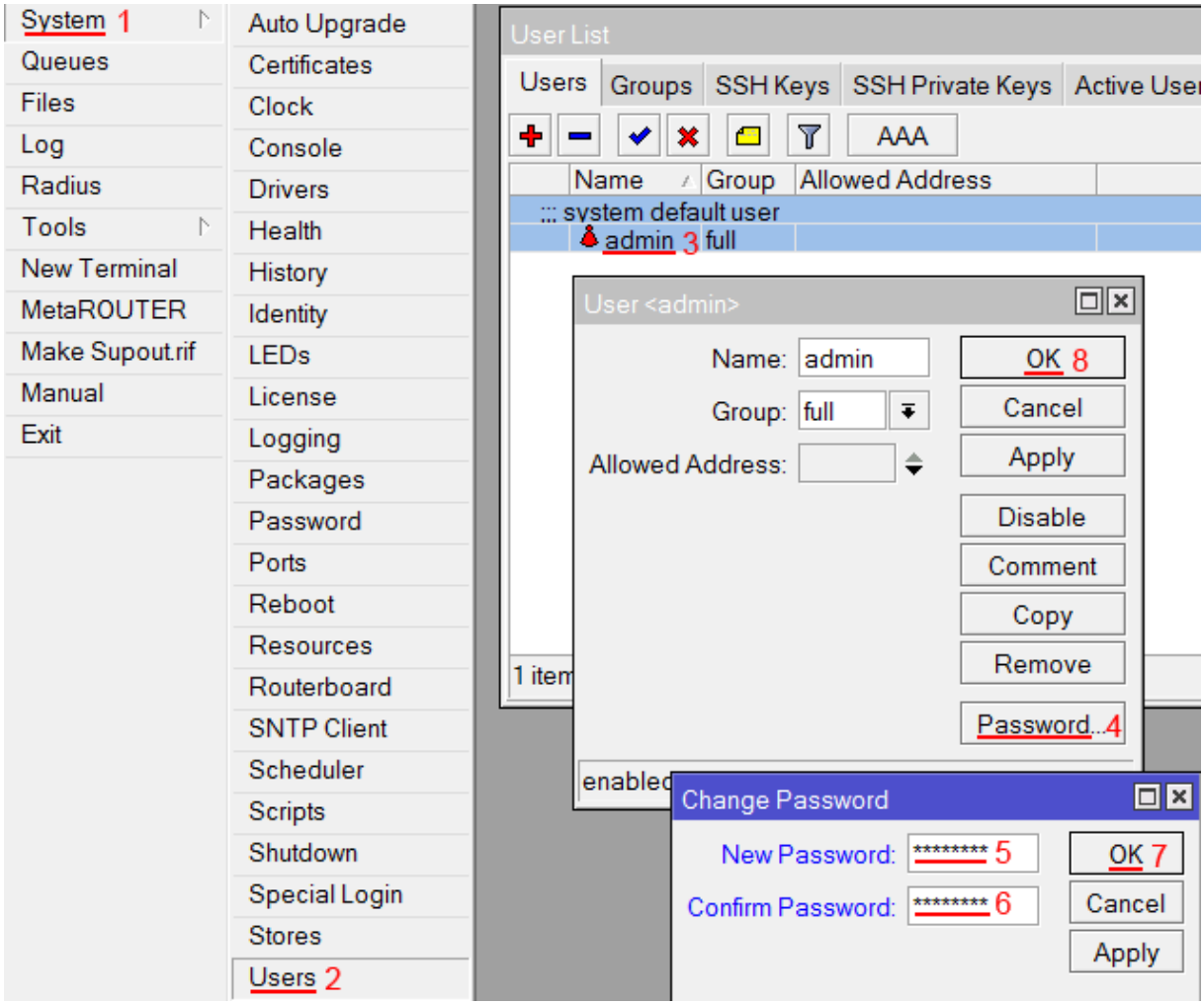


Рис. 1.40 – Налаштування паролю доступу

Перевірити чи є під’єднання до Wi-fi мережі інтернет AP_MikroTik, наприклад, з допомогою смартфону.

Оформити висновки по роботі.

Лабораторна робота № 2

Тема: Реалізація віддаленого vpn доступу до інформаційних ресурсів підприємства.
Мета: Навчитись налаштовувати VPN з аутентифікацією по паролях на роутері MikroTik.

Завдання.

1. Створити на робочих станціях ПК із операційною системою Windows 7 каталог із спільним доступом.
2. В каталозі створити текстовий файл із повідомленням.
3. Налаштувати VPN в роутері MikroTik з аутентифікацією по паролю.
4. Налаштувати VPN з аутентифікацією по паролю в операційній системі робочої станції ПК.
5. Прочитати повідомлення в текстовому файлі Admin_ПК використовуючи ПК Comp1 (папку і текстовий файл створити власноруч).

Теоретичні відомості.

VPN-сервер з аутентифікацією по паролях - це досить зручно, тому що, наприклад, можна на короткий час надати комусь доступ (для віддаленої роботи інженера, приміром), а потім швидко цей доступ зняти, причому не відключаючи користувача, а просто помінявши пароль. Але є і мінуси, як мінімум, безпека. Можливість діставання доступу шляхом перебору паролів - це вразливе місце в системі безпеки - потрібно моніторити логи на предмет спроб входу. Є інший спосіб налаштування VPN сервера Mikrotik - на ключах, IKEv2, але це тема окремої роботи.
Протокол L2TP забезпечує канал передачі даних, тунель.
IPSec забезпечує захист даних від перегляду.
Налаштовувати ми будемо теж по частинах - спочатку тунель, потім - захист даних.
Отже, маємо роутер Mikrotik з LAN 192.168.66.0/24

Хід виконання роботи.

Налаштування туннелювання (L2TP)
1. IP - Pool / Визначаємо діапазон адреса VPN – користувачів (рис. 2.1)

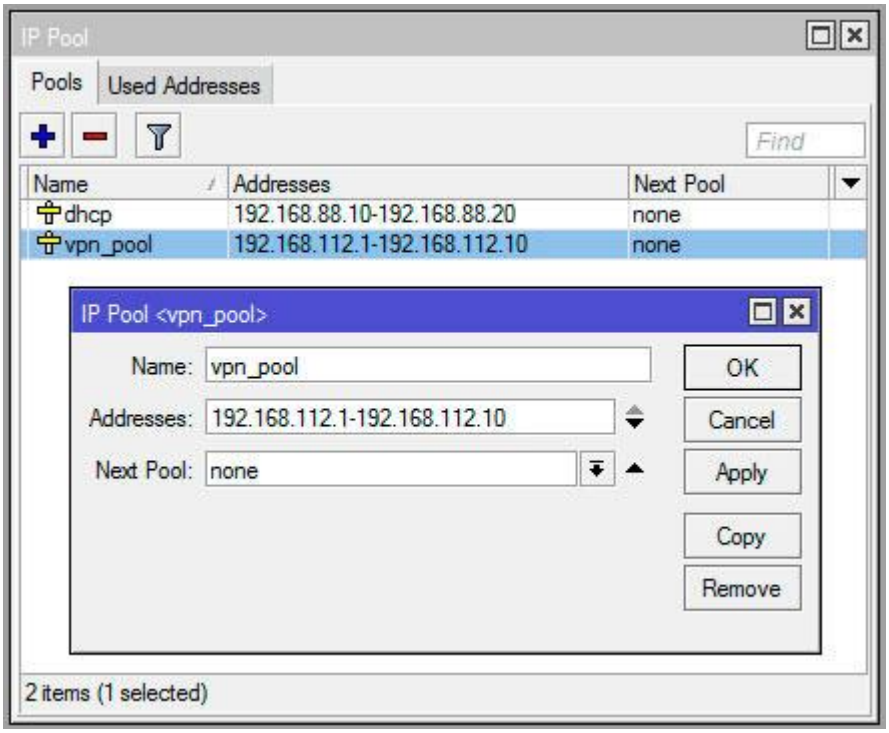


Рис. 2.1 – Діапазон адреси VPN-користувачів

Name: vpn _ pool
Addresses: 192.168.66.1-192.168.66.10
Next pool: none
Краще для клієнтів vpn використати окрему адресацію. Так простіше відділяти одних від інших.

2. PPP - Profiles / Профіль для нашого конкретного тунеля (рис. 2.2)

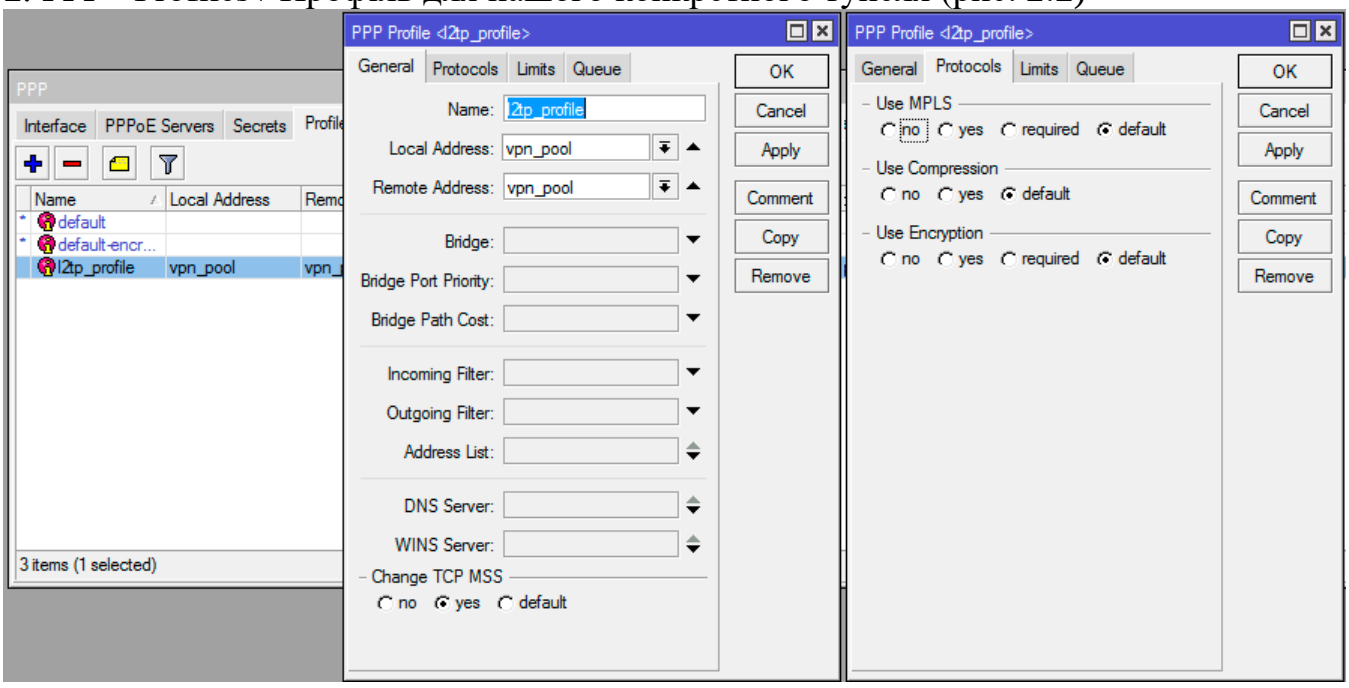


Рис. 2.2 – Налаштування профілю тунеля

General:
Name: l2tp _ profile
Local address: vpn _ pool *(а можна вказати* 192.168.66.1*, самі дивитеся, як вам більше подобається)*

Remote address: vpn _ pool
Change TCP MSS : yes

Protocols:
all to default:
Use MPLS : default
Use compression: default (можна також yes).
Use Encryption : default (можна ставити no, оскільки ppp-шифрування ми використовувати не будемо).
Якщо в мережі, куди ви підключаєтеся, є ресурси по внутрішніх доменних іменах, а не тільки по IP, можете вказати DNS Server цій мережі, наприклад, 192.168.66.1 (чи який вам потрібний).
Limits:
Only one: default
3. PPP - Secrets / Готуємо користувача VPN (рис. 2.3):

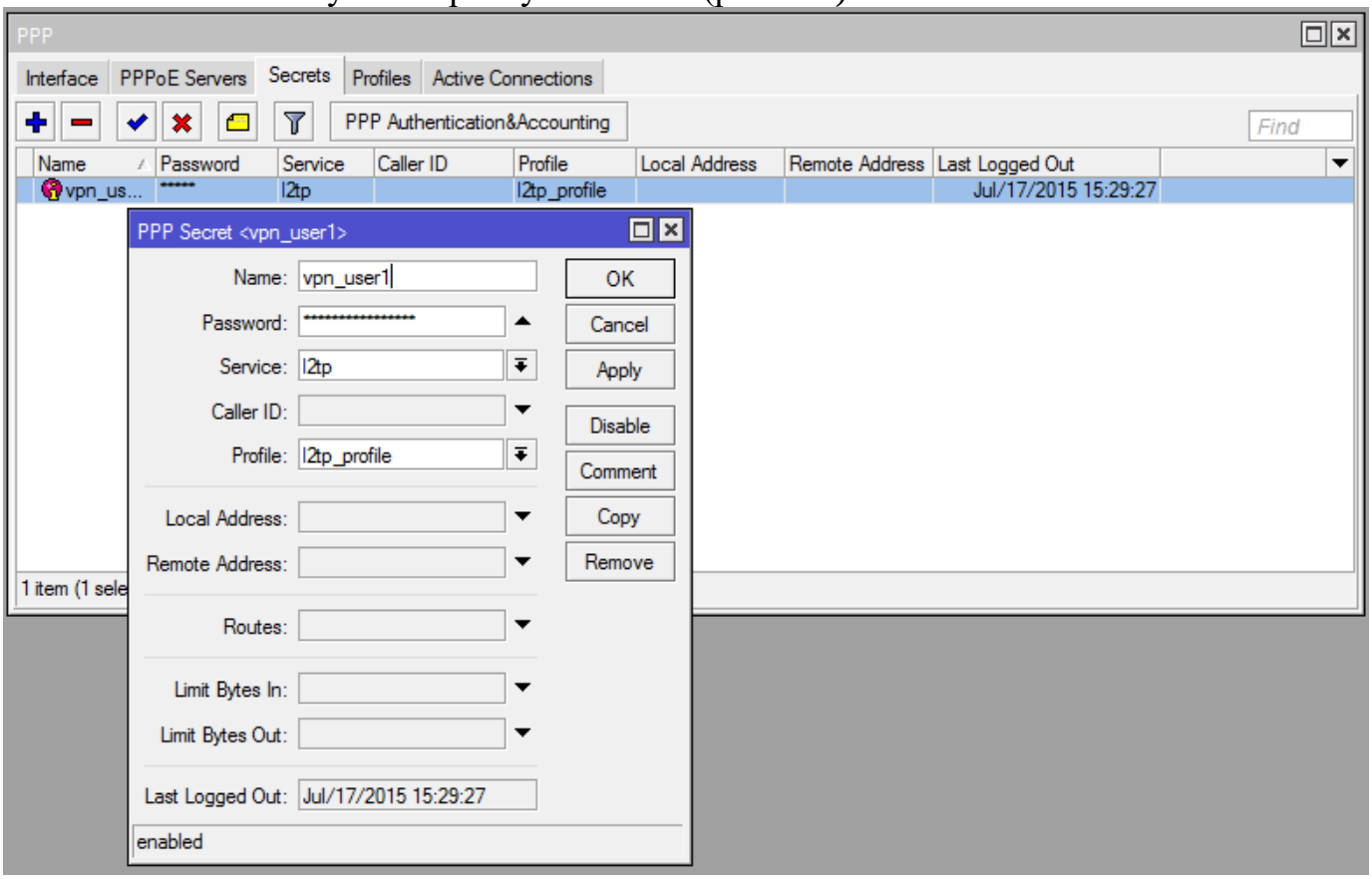


Рис. 2.3 – Налаштування профілю користувача

Name: vpn _ user1
Password: придумати власний
Service: l2tp
Profile: l2tp _ profile

4. PPP - Interface - клік на L2TP Server / Включаємо сервер L2TP (рис. 2.4):

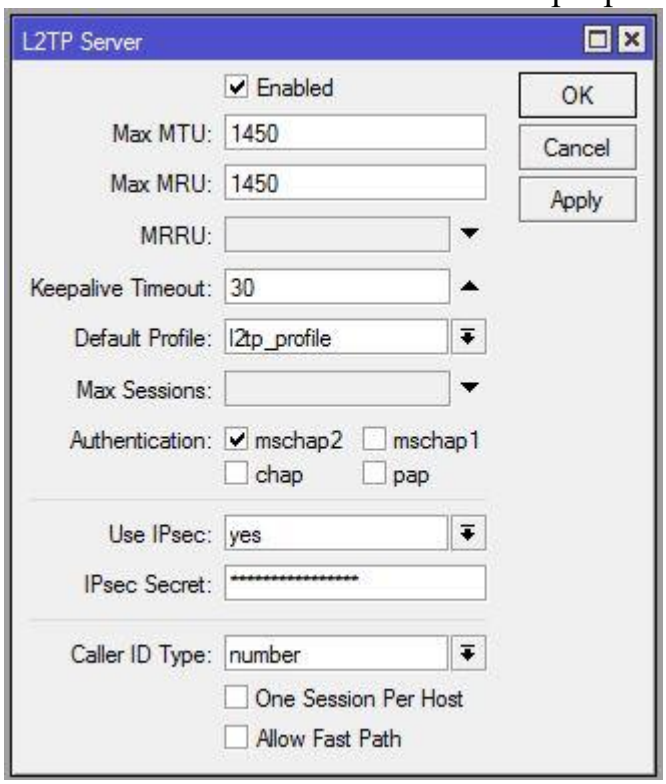


Рис. 2.4 – Параметри L2TP-сервера

Enabled - yes
MTU / MRU - 1450
Keepalive Timeout - 30
Default profile - l2tp _ profile
Authentication - mschap2
Use IPSec - yes
IPSec Secret : придумати власний (це не пароль користувача, а попередній ключ, який потрібно буде вказувати на клієнтах на додаток до логіна/паролю)
При цьому в IP - IPSec - Peers буде створений динамічний пір з ім'ям l2tp - in - server.

Налаштування шифрування даних в "тунелі"(IPSec)
На попередньому етапі ми створили тунель для передачі даних і включили IPSec. У цьому розділі ми налаштуємо параметри IPSec.

7. IP - IPSec - Proposals / "Пропозиції".
Щось подібне до "що ми можемо вам запропонувати". Іншими словами, задаємо опції підключення, які зможуть намагатися використати віддалені клієнти.
Name: default
Auth algorithms: sha1
Enrc. algorithms: 3des, aes - 256 cbc, aes - 256 ctr
Life time: 00: 30: 00
PFS Group : mod 1024

Firewall

Наступні команди можна виконати через термінал:

```
/ip firewall filter
add chain=input action=accept protocol=udp port=1701,500,4500
add chain=input action=accept protocol=ipsec - esp
```

Якщо у вас по-замовчуванні політика forward встановлена в drop (останнє правило для forward "chain=forward action=drop"), вам може бути необхідним дозволити forward з ip- адрес vpn _ pool в локальну мережу:

```
add chain=forward action=accept src - address=192.168.66.0/24 in - interface=!ether1 out - interface=bridge - local comment="allow vpn to lan" log=no log - prefix=""
```

Ось тепер з сервером все.

Proxy ARP.

Proxy ARP – це технологія, яка представляє проксі-сервер для ARP-запитів, дозволяючи зв'язати на канальному рівні різні мережі. Тепер, отримавши від клієнта ARP-запит сервер відповість MAC-адресою, на який клієнт може посилати Ethernet-фрейми.

Існують різні варіанти ARP-проксі, в найпростішому випадку, який реалізований в Mikrotik, роутер відповість на ARP-запит власним MAC-адресою, а отримавши Ethernet-кадр передасть його на інтерфейс, на якому включений Proxy ARP. Таким чином віддалений клієнт і вузли локальної мережі зможуть спілкуватися між собою на канальному рівні без залучення маршрутизатора (як їм здається).

Для того, щоб включити Proxy ARP в роутері Mikrotik перейдіть в налаштування інтерфейсу, що обслуговує вашу локальну мережу, найчастіше це буде мостовий інтерфейс bridge, в нашому випадку це один з ether-портів, і в полі ARP встановіть значення proxy-arp (рис. 2.5).

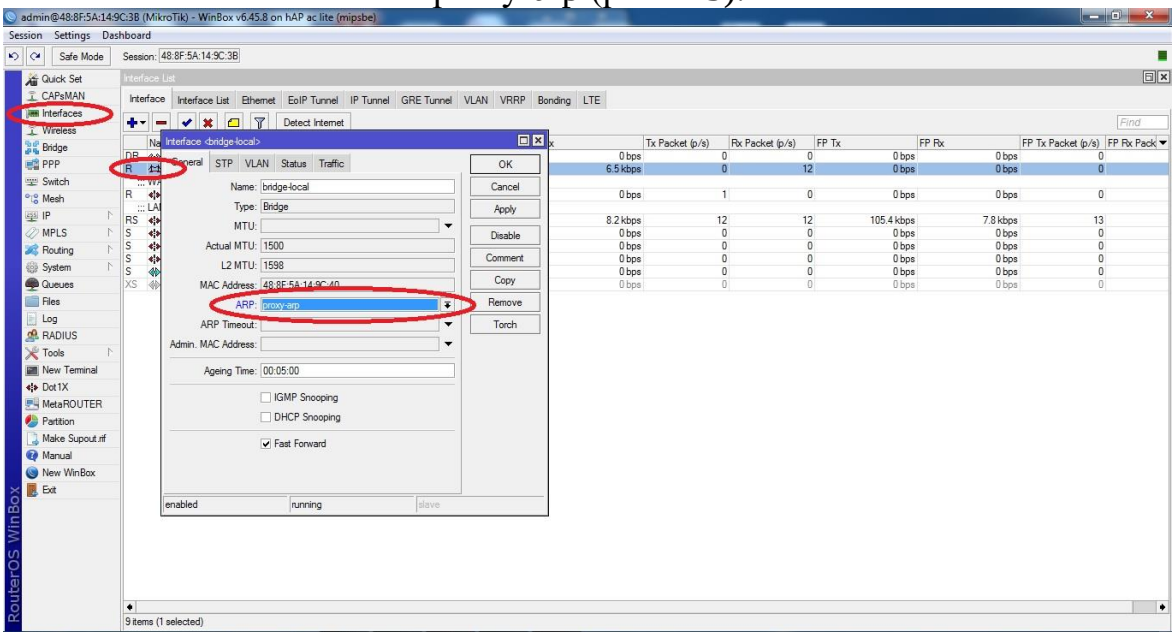


Рис. 2.5 – Налаштування ARP в bridge-local

Підключення відаленого клієнта

Пробуємо підключити Windows 7 :

Панель керування – Мережа та Інтернет - Центр управління мережами і загальним доступом :

Налаштування нового підключення або мережі

Підключення до робочого місця

Створити нове підключення

Використати моє підключення до інтернету (VPN)

Інтернет-адреса: ip або ім'я роутера в мережі

Користувач і пароль з PPP ->Secrets. У нашому випадку це vpn_user1 і його пароль.

Намагаємося підключитися.

Якщо не виходить, або просто потрібно налаштувати створене підключення (рис. 2.6):

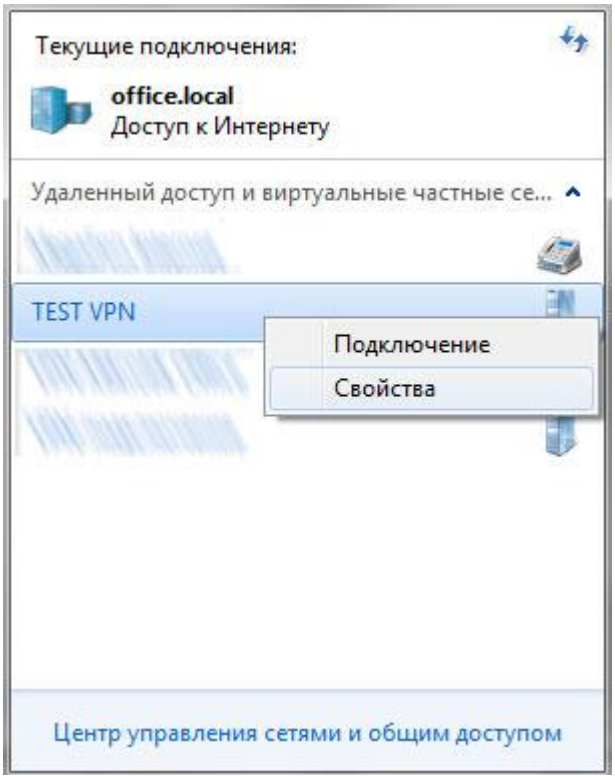


Рис. 2.6 – Поточні підключення

Вкладка Безпека:

Тип VPN : L2TP IPSec VPN

Додаткові параметри: для перевірки достовірності використати попередній ключ (IP - IPSec - Peers) (рис. 2.7):

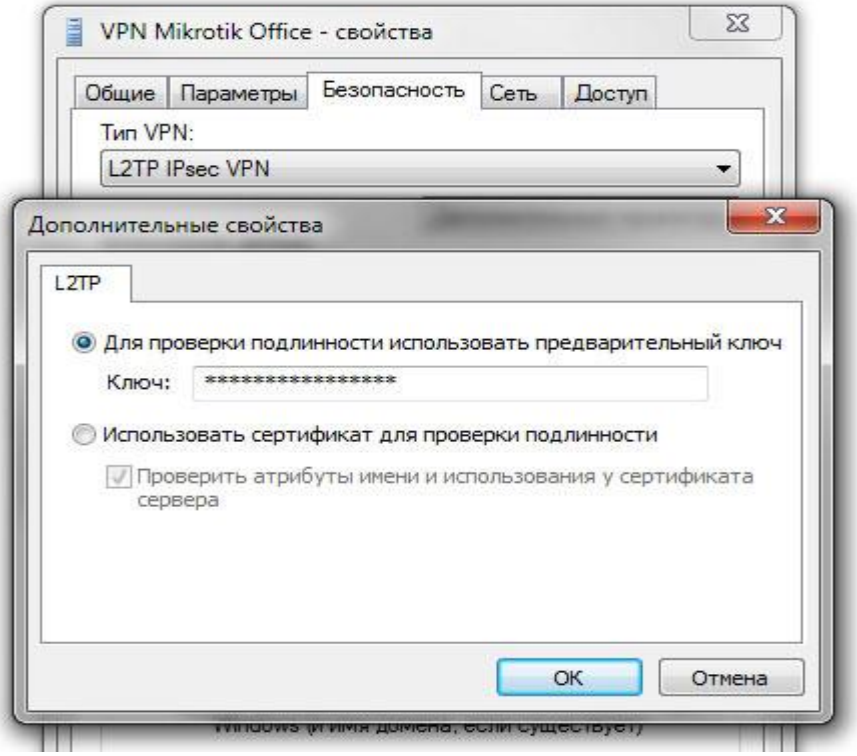


Рис. 2.7 – Вікно введення ключа

Тут же, в групі "Перевірка достовірності", залишаємо тільки CHAP v2:

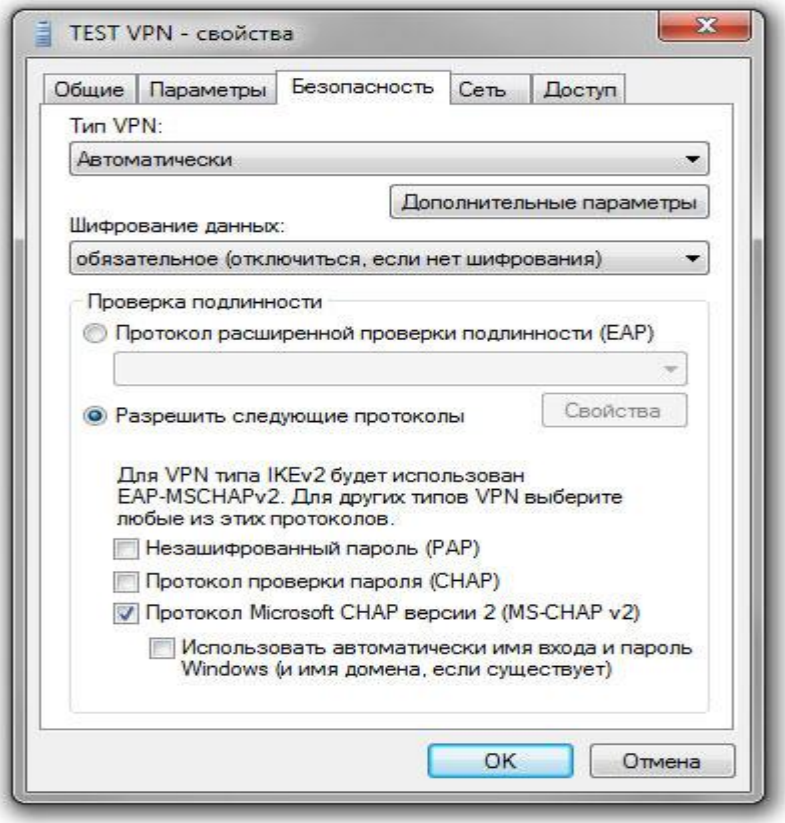


Рис. 2.8 – Вікно властивостей VPN

Тиснемо ОК і намагаємося підключитися.
Пробуємо зайти з ПК COMP1 на Admin_ПК і прочитати текст у файлі.
Оформити висновки по роботі.

Лабораторна робота № 3

Тема: Вивчення базових налаштувань мережевих екранів для забезпечення безпеки підприємства.
Мета: Навчитись налаштовувати FireWall на роутері MikroTik.

Завдання.

1. Налаштувати FireWall на роутері MikroTik таким чином, щоб доступ був лише з певної мережі.
2. Налаштувати FireWall на роутері MikroTik таким чином, щоб доступ в інтернет був заборонений певним користувачам.
3. Налаштувати FireWall на роутері MikroTik для доступу лише до сайтів.

Загальні теоретичні відомості.

Брандмауер реалізує фільтрацію пакетів і тим самим надає функції безпеки, які використовуються для управління потоком даних до, з і через маршрутизатор. Поряд з перекладом мережевої адреси він служить інструментом для запобігання несанкціонованого доступу до безпосередньо підключених мереж і самого маршрутизатора, а також фільтром для вихідного трафіку.

Мережні брандмауери тримають зовнішні загрози подалі від конфіденційних даних, доступних у мережі. Всякий раз, коли різні мережі об'єднані разом, завжди існує загроза того, що хтось з-за меж вашої мережі буде вриватися в вашу локальну мережу. Такі злами можуть призвести до викрадення та передачі приватних даних, зміни або знищення цінних даних або стирання цілих жорстких дисків. Брандмауери використовуються як засіб запобігання або мінімізації ризиків для безпеки, притаманних підключенню до інших мереж. Правильно налаштований брандмауер відіграє ключову роль у ефективному та безпечному розгортанні інфраструктури мережі.

MikroTik RouterOS має дуже потужну реалізацію брандмауера з функціями, включаючи:

- державна перевірка пакетів
- виявлення протоколу Рівня-7
- фільтрування однорангових протоколів
- класифікація трафіку за:
- вихідна MAC-адреса
- IP-адреси (мережа або список) і типи адрес (трансляція, локальна, багатоадресна, одноадресна)
- порт або діапазон портів
- IP-протоколи
- параметри протоколу (поля типу та коду ICMP, позначки TCP, параметри IP та MSS)
- інтерфейс пакет, отриманий з або ліворуч через
- внутрішні позначки потоку та з'єднання

- Байт DSCP
- вміст пакетів
- швидкість надходження пакетів і порядків
- розмір пакета
- час прибуття пакета
- і багато іншого!

Ланцюги

Брандмауер працює за допомогою правил брандмауера. Кожне правило складається з двох частин - матчера, який відповідає потоку трафіку проти заданих умов, і дії, яка визначає, що робити з відповідного пакету.

Правила фільтрації брандмауера згруповані в ланцюжки. Він дозволяє зіставити пакет з одним загальним критерієм в одному ланцюжку, а потім переданий для обробки проти деяких інших загальних критеріїв іншому ланцюжку. Наприклад, пакет повинен зіставити з IP-адресою: port pair. Звичайно, це може бути досягнуто шляхом додавання стільки правил з IP-адресою: port match, скільки потрібно для прямого ланцюжка, але кращим способом може бути додавання одного правила, яке відповідає трафіку з певної IP-адреси, наприклад: /ip фільтр брандмауера додати src-address=1.1.1.2/32 jump-target="mychain" і в разі успішного матчу передає контроль над IP-пакетом якомусь іншому ланцюжку, id est mychain в цьому прикладі. Тоді правила, які виконують відповідність з окремими портами, можуть бути додані в ланцюжок mychain без зазначення IP-адрес.

Існує три попередньо визначені ланцюжки, які не можна видалити:

- **input** - використовується для обробки пакетів, що надходять в маршрутизатор через один з інтерфейсів з IP-адресою призначення, яка є однією з адрес маршрутизатора. Пакети, що проходять через маршрутизатор, не обробляються за правилами вхідного ланцюжка
- **вперед** - використовується для обробки пакетів, що проходять через маршрутизатор
- **output** - використовується для обробки пакетів, що походять з роутера і залишаючи його через один з інтерфейсів. Пакети, що проходять через маршрутизатор, не обробляються за правилами вихідного ланцюжка

Схеми потоків пакетів ілюструють обробку пакетів у RouterOS.

При обробці ланцюжка правила забираються з ланцюжка в тому порядку, в тому порядку, в який вони перераховані там зверху вниз. Якщо пакет відповідає критеріям правила, то на ньому виконується задана дія, і більше в цьому ланцюжку не обробляються правила (виняток - дія проходження). Якщо пакет не відповідав жодному правилу всередині вбудованого ланцюжка, то він приймається.

Властивості

Властивості	Опис
action (*ім'я дії*; Типове значення: **прийняти**)	Дія, яка застосовується, якщо пакет відповідає правилу: • *accept* - прийняти пакет. Пакет не передано до наступного правила брандмауера. • *add-dst-to-address-list* - додати адресу призначення до списку адрес, визначеного параметром `address-list` • *add-src-to-address-list* - додати вихідну адресу до списку адрес, визначеного параметром `address-list` • *drop* - мовчки киньте пакет • *fasttrack-connection* - обробляти пакети з'єднання за допомогою FastPath, вмикаючи FastTrack для з'єднання • *jump* - перейти до визначеного користувачем ланцюжка, заданого значенням параметра `jump-target` • *log* - додати повідомлення до системного журналу, що містить такі дані: in-interface, out-interface, src-mac, protocol, src-ip:port->dst-ip:port та довжина пакета. Після збігу пакета він передається наступному правилу в списку, подібному до `passthrough` • *passthrough* - якщо пакет відповідає правилу, збільште лічильник і перейдіть до наступного правила (корисно для статистики) • *reject* - залиште пакет і надішліть повідомлення про відхилення ICMP • *return* - проходить контроль назад в ланцюжок, звідки відбувся стрибок • *tarpit* - захоплює та утримує TCP-з'єднання (відповідає syn/ACK вхідному пакету TCP SYN)
address-list-timeout (*нединамічний | нестатичний | час;* Типове значення: **нединамічні**)	Проміжок часу, після якого адреса буде видалена зі списку адрес, визначеного параметром. Використовується в поєднанні з діями або `address-listadd-dst-to-address-listadd-src-to-address-list` • Значення () залишить адресу у списку адрес до перезавантаження *none-dynamic* `00:00:00` • Значення залишить адресу у списку адрес назавжди і буде включено до експорту/резервного копіювання конфігурації *none-static*
chain (*ім'я*; За промовчанням:)	Визначає, до якого правила ланцюжка буде додано. Якщо вхідні дані не відповідають назві вже визначеного ланцюжка, буде створено новий ланцюжок.
comment (*рядок*; За промовчанням:)	Описова примітка до правила.
chain (*ім'я*; За промовчанням:)	Визначає, до якого правила ланцюжка буде додано. Якщо вхідні дані не відповідають назві вже визначеного ланцюжка, буде створено новий ланцюжок.
comment (*рядок*; За промовчанням:)	Описова примітка до правила.
connection-bytes (*ціле ціле число*; За промовчанням:)	Зісує пакети, лише якщо певну кількість байтів було передано через певне з'єднання. 0 - означає нескінченність, наприклад, означає, що правило збігається, якщо більше 2MB було передано через відповідне з'єднання `connection-bytes=2000000-0`

connection-limit (*ціле число, сітка;* За промовчанням:)	Повертає з'єднання для кожного блоку адреси або адреси після отримання вказаного значення. Слід використовувати разом з connection-state=new та/або з tcp-flags=syn, оскільки матчер дуже ресурсомісткий.
connection-mark (*рядок без |;* За промовчанням:)	Відповідає пакетам, позначеним за допомогою об'єкта mangle з певним знаком з'єднання. Якщо **позначку не встановлено,** правило відповідатиме будь-якому непозначеного з'єднання.
connection-nat-state (*srcnat | dstnat*; За промовчанням:)	Може збігатися з з'єднаннями, які стисують, задихається або обидва. Зауважте, що connection-state=пов'язані з'єднання connection-nat-стан визначається напрямком першого пакету. і якщо для з' єднання слід використовувати dst-nat для доставки цього з' єднання до тих самих вузлів, що і основне з' єднання, це буде у connection-nat-state=dstnat, навіть якщо правил dst-nat взагалі немає.
connection-rate (*Ціле число 0..4294967295*; За промовчанням:)	Швидкість підключення - це фаєрвол-матчер, який дозволяє фіксувати трафік на основі теперішньої швидкості підключення.
connection-state (*estabilished | недійсні | нові | пов'| з нерекліченими;* За промовчанням:)	Інтерпретує дані аналізу відстеження з'єднань для певного пакета: • *established* - пакет, що належить до існуючого з'єднання • *invalid* - пакет, який не має визначеного стану при відстеженні з'єднання (зазвичай - важкі позазамовні пакети, пакети з неправильним порядком / номером, або в разі надмірного використання ресурсу на маршрутизаторі), з цієї причини недійсний пакет не братиме участі в NAT (як це роблять тільки connection-state=new пакети), і все одно буде містити вихідну IP-адресу при маршруті. Ми настійно рекомендуємо відмовитися від усіх connection-state=недійсних пакетів у фільтрі брандмауера вперед та ланцюжках вводу • *new* - пакет почав нове з'єднання, або іншим чином пов'язане з підключенням, яке не бачив пакетів в обох напрямках. • *related* - пакет, пов'язаний з наявним підключенням, але не є частиною існуючого підключення, наприклад, помилки ICMP або пакет, який починає з'єднання даних FTP • *untracked* - пакет, який був налаштований на обхід відстеження з'єднань у таблицях RAW брандмауера.
connection-type (*ftp | h323 | irc | pptp | quake3 | sip | tftp;* За промовчанням:)	Зісування пакетів із пов'язаних підключень на основі відомостей помічників із відстеження підключень. Відповідний помічник підключення має бути ввімкнуто в /ip-брандмауері service-port
content (*рядок*; За промовчанням:)	Враховувати пакети, які містять указаний текст
dscp (*ціле число: 0..63*; За промовчанням:)	Відповідає полю заголовка DSCP IP.
dst-address (*IP/netmask | Діапазон IP;Діапазон IP-адрес;* За промовчанням:)	Відповідає пакетам, призначення яких дорівнює вказаному IP-адресі або потрапляє до вказаного діапазону IP.
dst-address-list (*ім'я*; За промовчанням:)	Відповідає цільовій адресі пакета зі списком адрес, визначеним користувачем
dst-address-type (*одноадресна | локальна | трансляція | багатоадресна;* За промовчанням:)	Відповідає типу адреси призначення: • *unicast* - IP-адреса, яка використовується для передачі точки в точку • *local* - якщо dst-адреса присвоюється одному з інтерфейсів маршрутизатора • *broadcast* - пакет відправляється на всі пристрої в підмережі • *multicast* - пакет пересилаються на визначену групу пристроїв
dst-limit (*ціле число[/time],ціле число;dst-адреса | dst-port | src-адреса[/time];* За промовчанням:)	Зісує пакети, доки не буде перевищено вказану швидкість. Швидкість визначається як пакети на часовий інтервал. На відміну від матчера, кожен потік має свою власну межу. Потік визначається параметром mode. Параметри записуються в такому форматі: . *limit* `count[/time],burst,mode[/expire]`

- **count** - кількість пакетів за проміжок часу на потік для збігу
- **time** - вказує часовий інтервал, в якому не може бути перевищена кількість пакетів на потік (необов'язково, 1 буде використовуватися, якщо не вказано)
- **burst** - початкова кількість пакетів на потік, що відповідає: це число поповнюється по одному кожні /, до цього числа `timecount`
- **mode** - цей параметр вказує, які унікальні поля визначають потік (src-адреса, dst-адреса, src-and-dst-адреса, dst-address-and-port, адреси-і-dst-порт)
- **expire** - вказує інтервал, після якого потік без пакетів буде дозволено видаляти (необов'язково)

dst-port (*ціле число[-ціле число]: 0..65535*; За промовчанням:) — Список номерів портів призначення або діапазонів номерів портів

fragment (*Так|не;* За промовчанням:) — Відповідає фрагментованим пакетам. Перший (стартовий) фрагмент не рахується. Якщо відстеження з'єднання увімкнено, фрагментів не буде, оскільки система автоматично збирає кожен пакет

hotspot (*автентифікація |-клієнту | http | локального dst |-клієнта;* За промовчанням:) — Пакети матчів, отримані від клієнтів HotSpot, проти різних матчів HotSpot.

- *auth* - відповідає автентичним клієнтським пакетам HotSpot
- *from-client* - відповідає пакетам, які надходять від клієнта HotSpot
- *http* - збігається з HTTP-запитами, надісланими на сервер HotSpot
- *local-dst* - відповідає пакетам, призначеним для сервера HotSpot
- *to-client* - відповідає пакетам, які надсилаються клієнту HotSpot

icmp-options (*ціле число:ціле число*; За промовчанням:) — Відповідає типу ICMP:кодові поля

in-bridge-port (*ім'я*; За промовчанням:) — Фактичний інтерфейс пакет увійшов до маршрутизатора, якщо вхідний інтерфейс є мостом. Працює тільки в тому **випадку, якщо use-ip-firewall** включений в налаштуваннях bridge.

in-bridge-port-list (*ім'я*; За промовчанням:) — Набір інтерфейсів, визначених у списку інтерфейсів. Працює так само, як і *in-bridge-port*

in-interface (*ім'я*; За промовчанням:) — Інтерфейс, в який пакет увійшов до маршрутизатора

in-interface-list (*ім'я*; За промовчанням:) — Набір інтерфейсів, визначених у списку інтерфейсів. Працює так само, як і *in-interface*

ingress-priority (*ціле число: 0..63*; За промовчанням:) — Відповідає пріоритету пакета ingress. Пріоритет може бути отриманий з VLAN, WMM, DSCP або MPLS EXP біт.

ipsec-policy (*в |, ipsec | немає;* За промовчанням:) — Відповідає політиці, яка використовується ipSec. Значення записується в такому форматі: . Напрямок використовується для вибору того, чи слід відповідати політиці, яка використовується для декапсуляції, або політиці, яка буде використовуватися для інкапсуляції. **`direction, policy`**

- *in* - дійсні в ланцюгах ПОПЕРЕДНЬОГО МАРШРУТИЗАЦІЇ, ВВОДУ та ВПЕРЕД
- *out* - дійсні в ланцюгах POSTROUTING, OUTPUT та FORWARD
- *ipsec* - збігається, якщо пакет підлягає обробці IpSec;
- *none* - відповідає пакету, який не підлягає обробці IpSec (наприклад, транспортний пакет IpSec).

Наприклад, якщо маршрутизатор отримує інкапсульований пакет Gre Ipsec, то правило буде відповідати пакету Gre, але правило буде відповідати пакету ESP. `ipsec-policy=in,ipsecipsec-policy=in,none`

ipv4-options (будь-| маршрутизації без джерела | без запису | попередження про відсутність маршрутизатора | маршрутизацію без джерела | без позначки *часу* | *жодного* | *маршруту запису* | *попередження маршрутизатора* | *сувора маршрутизація джерела* | *позначка часу;* За промовчанням:) — Відповідає параметрам заголовка IPv4.

- *any* - відповідність пакета принаймні з одним з варіантів ipv4
- *loose-source-routing* - зіставити пакети з опцією вільної маршрутизації джерела. Цей параметр використовується для маршрутивування інтернет-схеми на основі інформації, наданої джерелом
- *no-record-route* - зіставити пакети без опції маршруту запису. Цей параметр використовується для маршрутивування інтернет-схеми на основі інформації, наданої джерелом
- *no-router-alert* - матч пакетів без маршрутизатора змінити варіант
- *no-source-routing* - зіставити пакети без опції маршрутизації джерела
- *no-timestamp* - матч пакетів без опції часової позначки
- *record-route* - матч пакетів з опцією запису маршруту
- *router-alert* - матч пакетів з маршрутизатором змінити опцію
- *strict-source-routing* - зіставити пакети з строгим варіантом маршрутизації джерела
- *timestamp* - матч пакетів з позначкою часу

jump-target (*ім'я*; За промовчанням:) — Ім'я цільового ланцюжка, щоб перейти до. Застосовується, лише якщо `action=jump`

layer7-protocol (*ім'я*; За промовчанням:) — Ім'я фільтра Layer7, визначене в меню протоколу layer7.

limit (*ціле число,час;ціле число*; За промовчанням:) — Відповідає пакетам з обмеженою швидкістю (швидкість пакетів або швидкість потоку). Правило, яке використовує цей матчер, буде збігатися, доки не буде досягнуто цього обмеження. Параметри записуються в такому форматі: . `count[/time],burst:mode`

- **count** - кількість пакетів або бітів за проміжок часу для збігу
- **time** - вказує часовий інтервал, в якому не можна перевищувати кількість пакетів або бітів (необов'язково, 1 буде використовуватися, якщо не вказано)
- **burst** - початкова кількість пакетів або бітів для збігу: це число перезаряджається кожні 10 мс, тому сплеск повинен бути принаймні 1/100 швидкості в секунду
- **режим** - пакетний або бітовий режим

log-prefix (*рядок*; За промовчанням:) — Додає вказаний текст на початку кожного повідомлення журналу. Застосовується, якщо `action=log`

nth (*ціле число,ціле число*; За промовчанням:) — Відповідає кожному n-му пакету.

out-bridge-port (*ім'я*; За промовчанням:) — Фактичний інтерфейс пакет залишає маршрутизатор, якщо вихідний інтерфейс є bridge. Працює тільки в тому **випадку, якщо use-ip-firewall** включений в налаштуваннях bridge.

out-bridge-port-list (*ім'я*; За промовчанням:) — Набір інтерфейсів, визначених у списку інтерфейсів. Працює так само, як і *out-bridge-port*

out-interface (; За промовчанням:) — Інтерфейс пакета залишає маршрутизатор

out-interface-list (*ім'я*; За промовчанням:) — Набір інтерфейсів, визначених у списку інтерфейсів. Працює так само, як і *out-*

	interface
packet-mark (*рядок без |;* За промовчанням:)	Відповідає пакетам, позначеним за допомогою об'єкта mangle з певною позначкою пакету. Якщо **позначку не встановлено,** правило відповідатиме будь-якому непозначеного пакету.
packet-size (*ціле число[-ціле число]:0.. 65535*; За промовчанням:)	Відповідає пакетам указаного розміру або діапазону розміру в байтах.
per-connection-classifier (*значення:знаменник/залишок*; За промовчанням:)	PcC matcher дозволяє розділити трафік на рівні потоки з можливістю зберігати пакети з певним набором опцій в одному конкретному потоці.
port (*ціле число[-ціле число]: 0..65535*; За промовчанням:)	Відповідає, якщо будь-який (вихідний або кінцевий) порт відповідає вказаному списку портів або діапазонів портів. Застосовується, лише якщо це TCP або UDP `protocol`
priority (*ціле число: 0..63*; Типове значення:)	Відповідає пріоритету пакета після встановлення нового пріоритету. Пріоритет може бути отриманий з біта VLAN, WMM, DSCP, MPLS EXP або від пріоритету, встановленого за допомогою дії.*set-priority*
protocol (*ім'я або ідентифікатор протоколу;* Типове значення: **tcp**)	Відповідає певному IP-протоколу, вказаному іменем або номером протоколу
psd (*ціле число,час;ціле число;ціле число;* За промовчанням:)	Намагається виявити сканування TCP та UDP. Параметри мають такий формат `WeightThreshold, DelayThreshold, LowPortWeight, HighPortWeight` • **WeightThreshold** - загальна вага останніх TCP / UDP пакетів з різними портами призначення, що надходять з одного хоста, який розглядається як послідовність сканування порту • **DelayThreshold** - затримка для пакетів з різними портами призначення, що надходять з одного хоста, щоб розглядатися як можливе підсекреція сканування порту • **LowPortWeight** – вага пакетів із привілейованим (<1024) кінцевим портом • **HighPortWeight** - вага пакету з неважливим портом призначення
random (*integer: 1..99*; Default:)	Випадкове зі збігом пакетів із заданою ймовірністю.
reject-with (*icmp-admin-заборонений | icmp-net заборонений | icmp-protocol-недосяжний | icmp-host заборонений | icmp-network-недосяжний | tcp-reset | icmp-host-недосяжний | icmp-port-недосяжний*; Типове значення: icmp-network- недоступний)	Вказує помилку ICMP, яка надсилається назад, якщо пакет відхилено. Застосовується, якщо `action=reject`
routing-table (*рядок*; За промовчанням:)	Відповідає пакетам, адреси призначення яких розв'януто в певній таблиці маршрутизації. Більш детальну інформацію можна знайти на сторінці відповідність таблиці маршрутизації
routing-mark (*рядок*; За промовчанням:)	Відповідає пакетам, позначеним об'єктом об'єкту mangle з певною позначкою маршрутизації
src-address (*Ip/Netmaks, ip діапазон;* За промовчанням:)	Зісує пакети, джерело яких дорівнює вказаному IP-адресі, або потрапляє до вказаного діапазону IP.
src-address-list (*ім'я*; За промовчанням:)	Збіг вихідної адреси пакета з визначеним користувачем списком адрес
src-address-type (*одноадресна | локальна | трансляція | багатоадресна;* За промовчанням:)	Відповідає типу вихідної адреси: • *unicast* - IP-адреса, яка використовується для передачі точки в точку • *local* - якщо адреса присвоюється одному з інтерфейсів маршрутизатора

- *broadcast* - пакет відправляється на всі пристрої в підмережі
- *multicast* - пакет пересилаються на визначену групу пристроїв

src-port (*ціле число[-ціле число]: 0..65535*; За промовчанням:)	Список вихідних портів і діапазонів вихідних портів. Застосовується, лише якщо протокол Є TCP або UDP.
src-mac-address (*MAC-адреса*; За промовчанням:)	Відповідає вихідній MAC-адресі пакета
tcp-flags (*ack* | *cwr* | *ece* | *плавник* | *psh* | *rst* | | *ург;* За промовчанням:)	Відповідає вказаним позначкам TCP • *ack* - підтвердження даних • *cwr* - вікно перевантаження зменшено • *ece* - Прапор ECN-echo (явне сповіщення про перевантаження) • *fin* - закрити з'єднання • *psh* - функція push • *rst* - падіння з'єднання • *syn* - нове з'єднання • *urg* - термінові дані
tcp-mss (*ціле число[-ціле число]: 0..65535*; За промовчанням:)	Відповідає значенню TCP MSS IP-пакета
time (*час-тайм, сидів* | *пт* | *чт* | *ср* | *вт* | *пн* | *сонце;* За промовчанням:)	Дозволяє створювати фільтр на основі часу прибуття та дати прибуття пакетів або для локально згенерованих пакетів, часу та дати відправлення
tls-host (*рядок*; За промовчанням:)	Дозволяє зіставити https-трафік на основі назви вузла TLS SNI. Приймає синтаксис GLOB для пошуку символів узагальнення. Зауважте, що matcher не зможе зіставити назву вузла, якщо рамка встановлення зв'ї ручок TLS фрагментована на кілька сегментів TCP (пакетів).
ttl (*integer: 0..255*; Default:)	Відповідає значенню TTL пакетів

Теоретичні відомості для роботи

Ланцюжок брандмауерів

Мікротік має наступні ланцюжки

Input - це ланцюжок для обробки пакетів, що надходять до маршрутизатора, які мають IP маршрутизатора як адресу.

Forward - цей ланцюжок обробляє пакети, що проходять через маршрутизатор

Output - це ланцюжок для обробки пакетів, створених маршрутизатором, наприклад, коли ми пінг від маршрутизатора або підключення на telnet

З опису зрозуміло, що для захисту маршрутизатора слід використовувати ланцюжок вводу. А для обробки трафіку від користувачів і користувачів використовуйте ланцюжок вперед. Мені не потрібно було використовувати вивід.

Дія брандмауера

Ось що ви можете зробити в ланцюгах:

Параметр	**Дії**
Accept	Дозволити
add-dst-to-address-list	Додавання IP призначення до списку адрес, переліченого у Address List
add-src-to-address-list	Додавання IP джерела до списку адрес, переліченого у Address List
Drop	Заборонити
fasttrack-connection	Обробляти пакети шляхом включення FastTrack тобто пакети будуть прохожити по найшвидшому маршруті, минаючи інші правила брандмауера та обробку в чергах
Jump	Стрибок, перейти, переключитися на інший ланцюжок, заданий в Jump target
log	Запис в журнал
passthrough	Перейти до наступного правила, нічого не роблячи ніяких дій (корисно для збору статистики)
Reject	Повернути пакек з причиною, вказаною у Reject with

Return	Поверніть пакет в ланцюжок, з якого він прийшов
tarpit	захоплює та підтримує TCP-з'єднання (відповідає за допомогою SYN/ACK на вхідний пакет TCP SYN)

Фільтрування у брандмауері

Фільтрування пакетів, які можуть потрапити в ланцюжки, може бути зроблено

Src.Address - адреса джерела

Dst.Address - адреса призначення

Protocol - Протокол (TCP, UDP і т.д.)

Src.Port - вихідний порт

Dst.Порт – порт призначення

In.Interface - вхідний інтерфейс

Out.Interface - вихідний інтерфейс

Packet.Mark - мітка пакета

Connection.Mark – мітка зєднання

Routing Mark - позначка маршруту

Roting table - адреса одержувача, дозволена в конкретній таблиці маршрутизації

Connection Type – тип підключення

Connection State - стан підключення (встановлений, новий і т.д.)

Connection NAT State - Мережа NAT (srcnat, dstnat)

Хід виконання роботи.

Приклади налаштувань брандмауера

Розглянемо кілька прикладів налаштувань брандмауера на роутері MikroTik.

1. Налаштування безпеки MikroTik

Для початку налаштуємо безпеку на нашому маршрутизаторі, для цього ми зробимо наступне:

1.Давайте заборонимо пінг на наш пристрій

2.Ми відмовляємо в доступі до MikroTik для всіх, крім локальної мережі та дозволених IP-адрес

Щоб налаштувати, підключіться до роутера за допомогою утиліти winbox і перейдіть в меню IP-Firewall. Перейдіть на вкладку " Filter Rules " та натисніть кнопку «додати» (рис. 3.1).

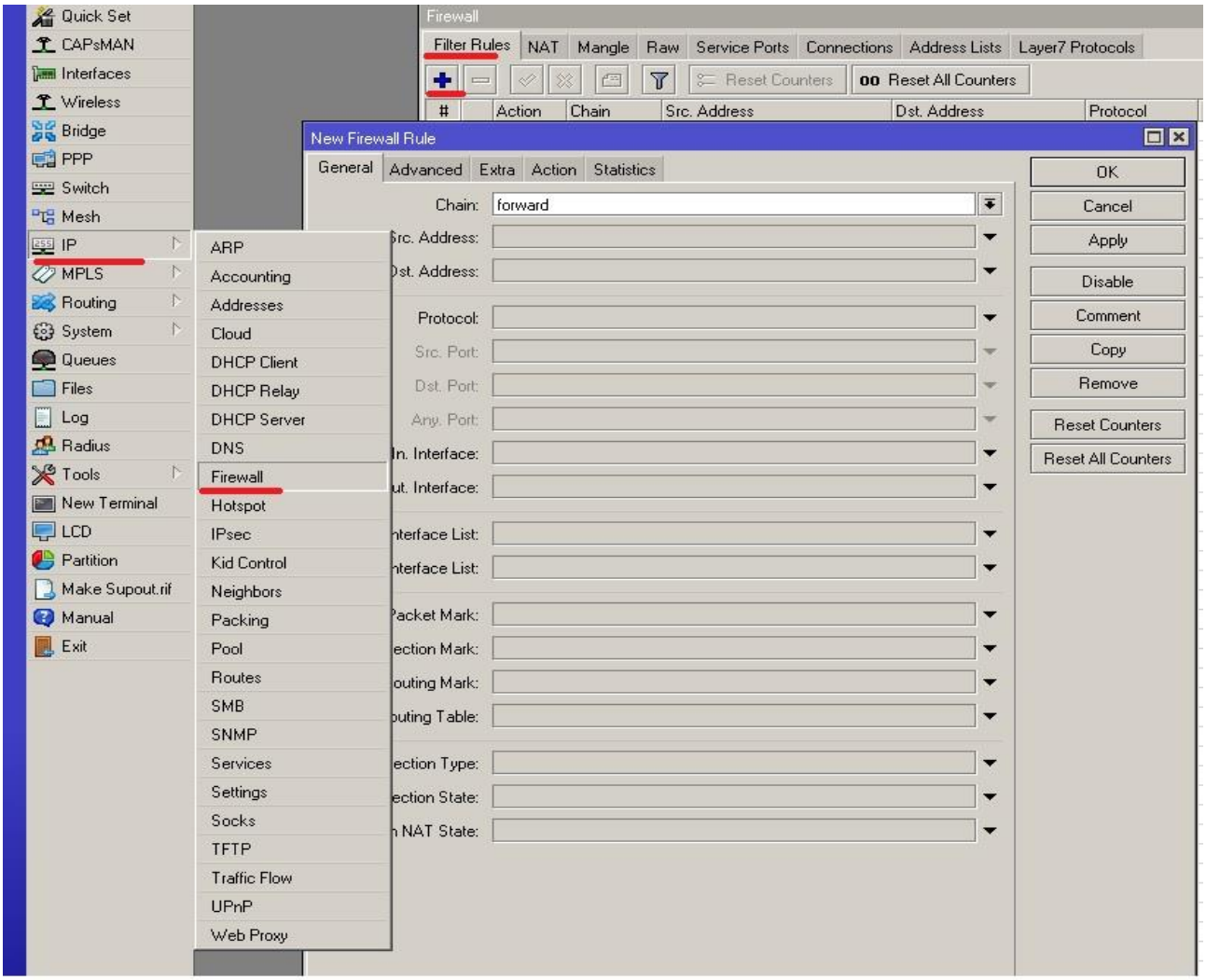


Рис. 3.1 – Розташування вікна нового правила для Firewall

Ми забороняємо пінг на нашому пристрої; для цього, на загальній вкладці **general**, **chain** вибираємо input protocol **icmp** (рис. 3.2):

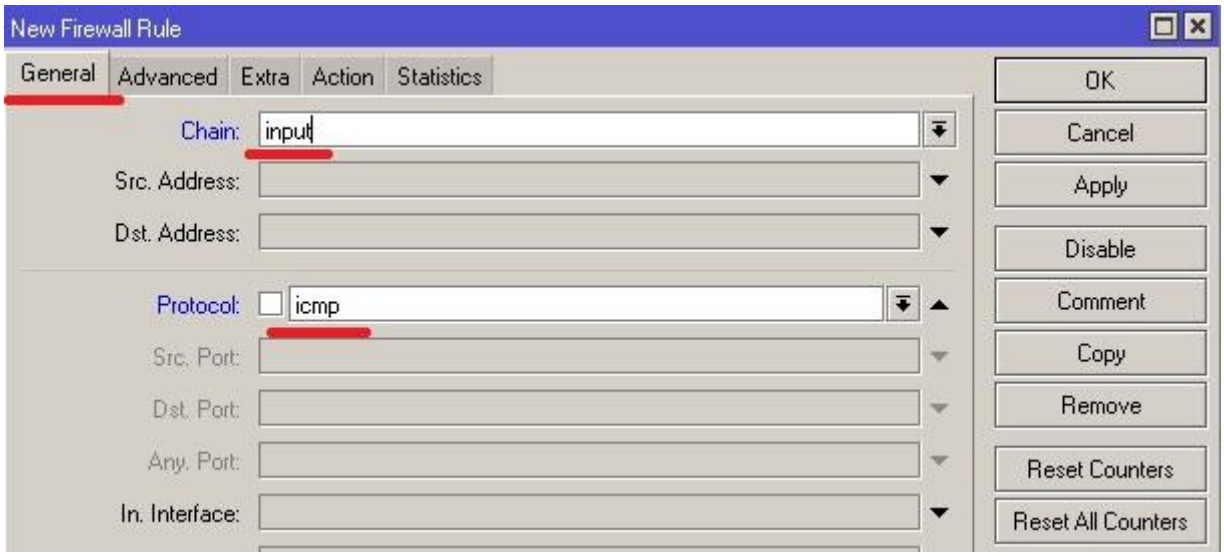


Рис. 3.2 – Загальні налаштування нового правила Firewall

На вкладці **Action** вибираємо **drop** (рис. 3.3):

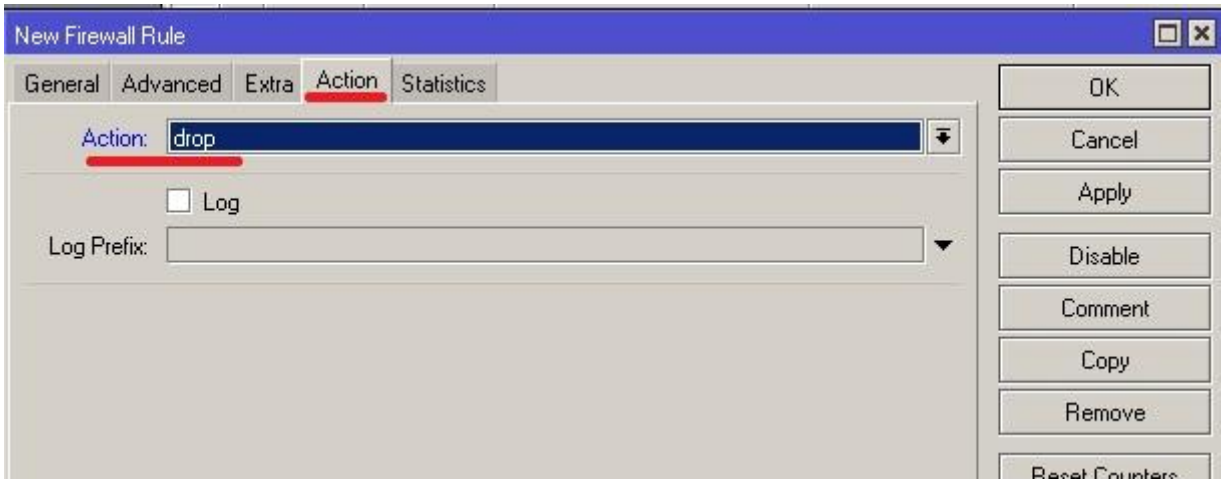


Рис. 3.3 – Вибір дії при виконанні правила

Забороняємо доступ до управління маршрутизатором. Для початку створіть аркуш з нашими дозволеними адресами, перейдіть до IP-Firewall, вкладка Address Lists, додаємо новий аркуш (рис. 3.4):

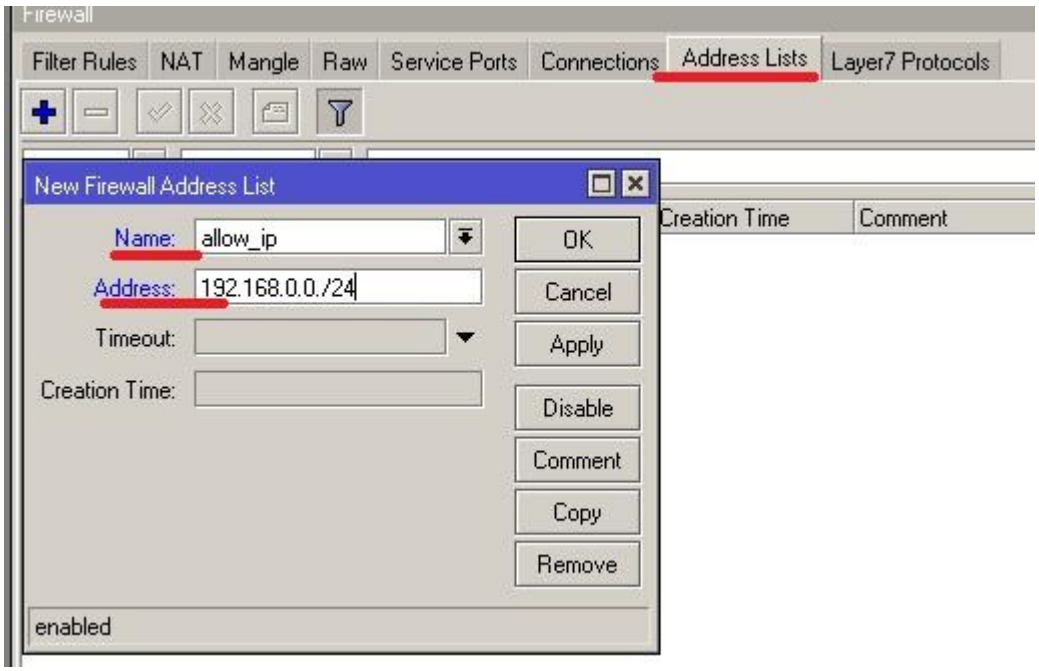


Рис. 3.4 – Вікно дозволених адрес

Name - назва нашого аркуша

Address - адреси, пов'язані з цим аркушем, можна вказати як окремі адреси, так і мережі.

Потім ми створюємо нове правило, повертаємося до Filter rules та додаємо його (рис. 3.5):

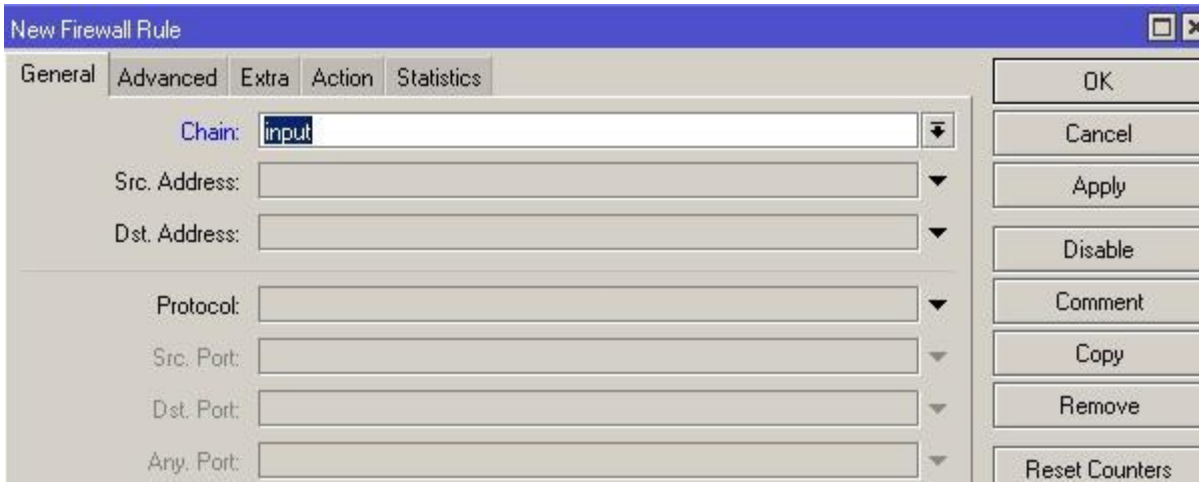


Рис. 3.5 – Нове правило

Потім перейдемо до вкладки Advanced і в якості Src. List вибираємо створений лист (рис. 3.6):

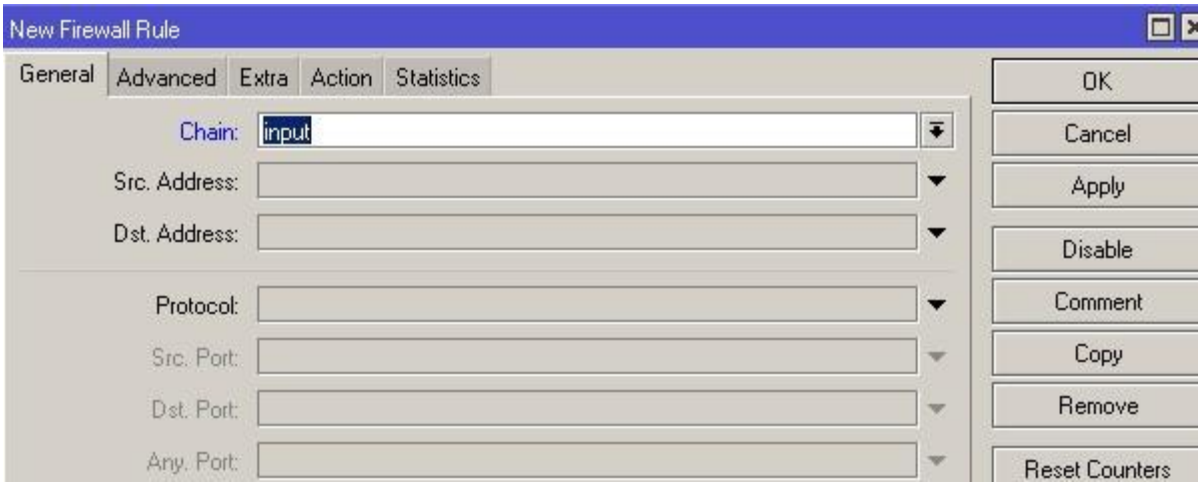


Рис. 3.6 – Нове правило

У дії Action ми вибираємо дозволити accept (рис. 3.7):

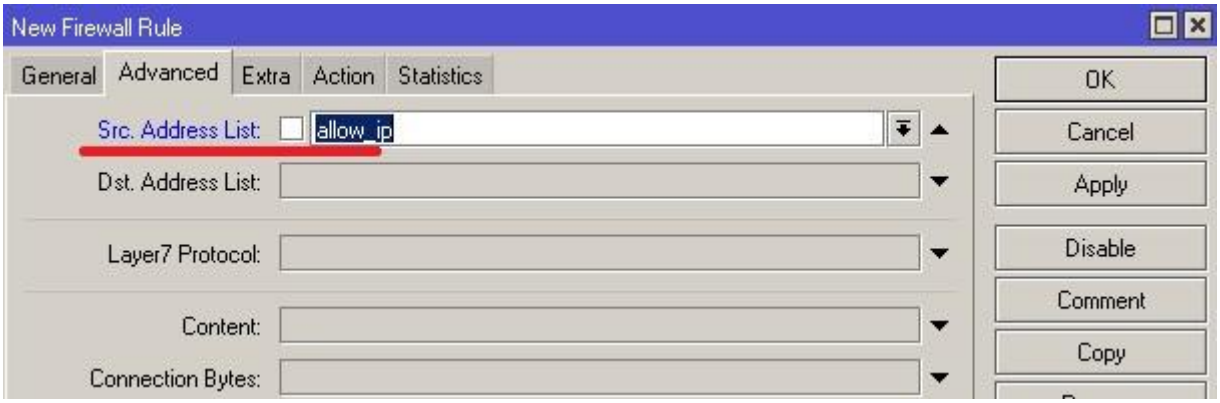


Рис. 3.7 – Додаткові налаштування

Можна було не створювати аркуш, а на вкладці General в параметрі Src. Address прописати нашу мережу, просто нам зручніше працювати зі списками адрес, в подальшому для додавання нового адресу потрібно просто додати його в allow_ip.

Наступний крок - заборона всіх вхідних з'єднань. Додайте правило на chain input, і в дії ставимо drop. Має вийти наступним чином (рис. 3.8).

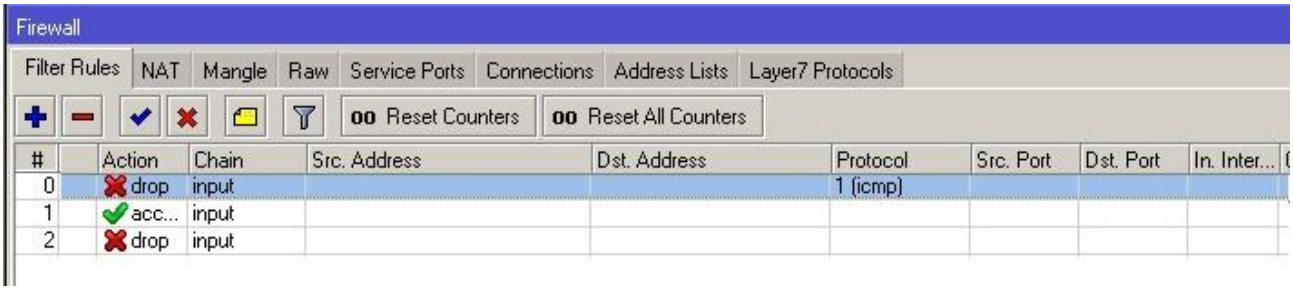


Рис. 3.8 – Дія Drop

Тут слід зазначити, що обробка правил йде зверху вниз, тобто правило, що забороняє всі з'єднання, повинно бути внизу, інакше правила не будуть працювати.

Для того, щоб поміняти місцями правило, потрібно клікнути на стрічку і затиснутою лівою кнопкою миші перетягнути її в потрібне місце. По суті, правило про заборону пінгу можна було не створювати, оскільки останнє правило блокує всі спроби доступу до роутера, включаючи ping.

2. Доступ користувачів до Інтернету

Скажімо, нам потрібно надати доступ до Інтернету тільки для певної мережі. Для цього створіть два дозвільних правила в chain forward. Перше правило дозволяє вихідний трафік з нашої мережі (рис. 3.9):

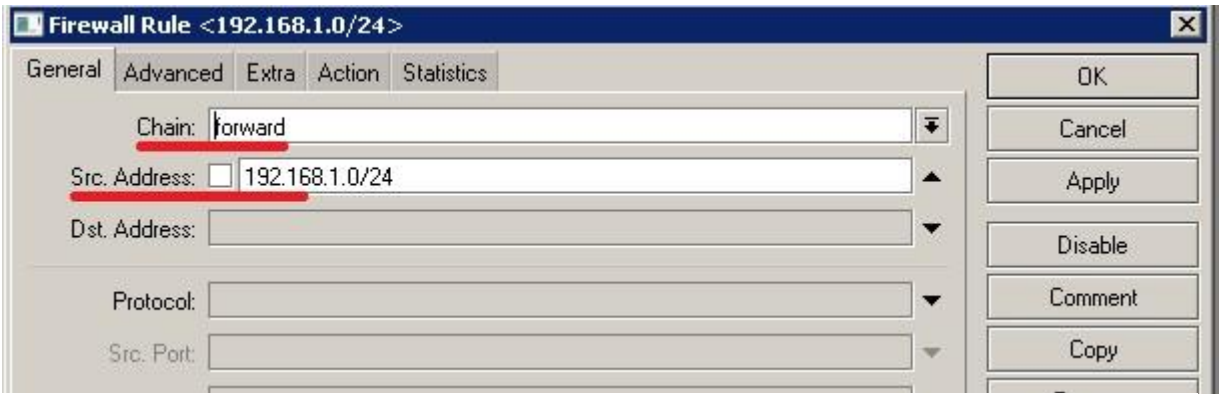


Рис. 3.9 – Нове дозвільне правило

Action ставимо accept. Ви можете як вказати Src. Address, так і використовувати Address Lists, як ми це робили вище. Наступне правило - дозволити проходження пакетів у нашу мережу (рис. 3.10):

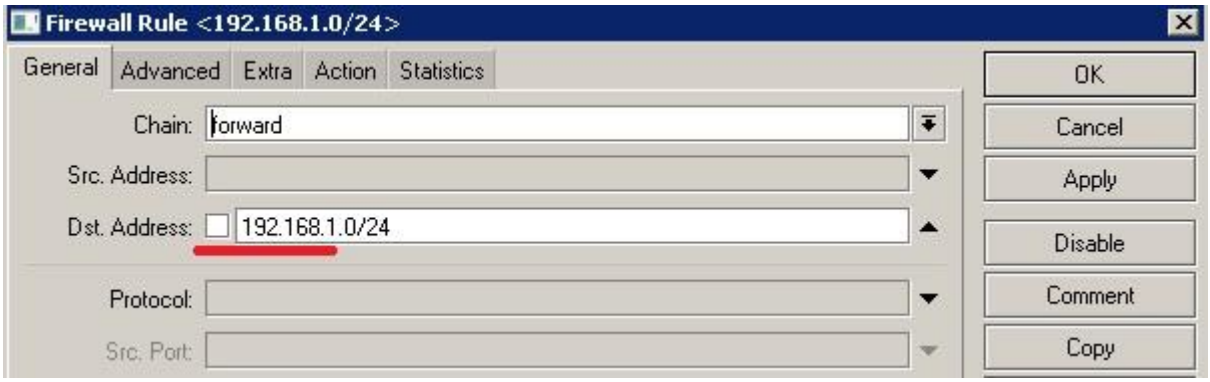


Рис. 3.10 – Адрес призначення

У наступному правилі ми забороняємо всі інші мережі (рис. 3.11):

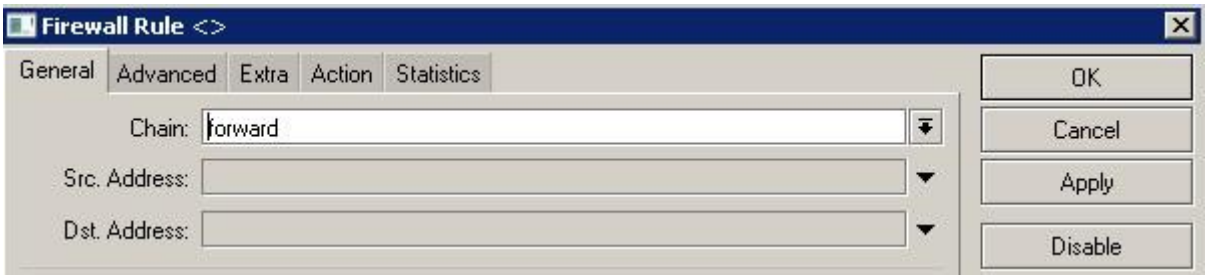


Рис. 3.11 – Заборона інших мереж

Action вибираємо drop. Результатом є наступне (рис. 3.12):

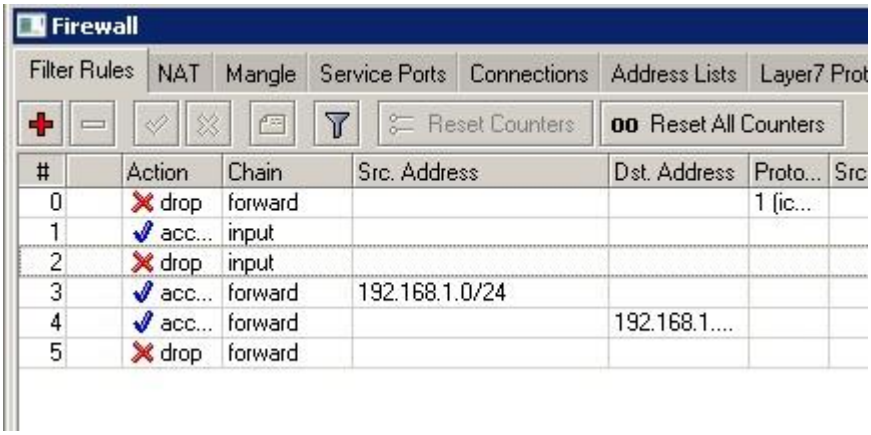


Рис. 3.12 – Дія drop

3. Заборона доступу користувачів до Інтернету

Якщо ми хочемо заборонити доступ до Інтернету певним користувачам, давайте зробимо це за допомогою Address Lists, для полегшення додавання або видалення правил у майбутньому, перейдіть на вкладку Address Lists, і створимо список block, до якого додамо адреси для блокування (рис. 3.13):

Рис. 3.13 – Адреси блокування

Створіть заборонне правило брандмауера в chain forward, в якому на вкладці Advanced в Src. Address List виберіть наш список для блокування (рис. 3.14):

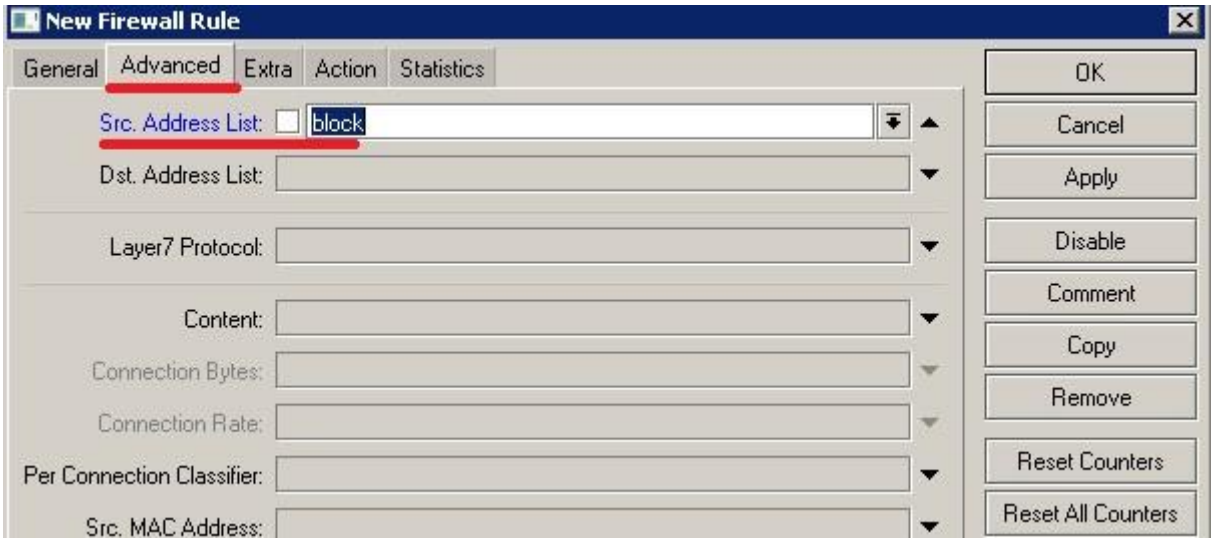


Рис. 3.14 – Блокування адрес

В Action вибираємо Drop. Тепер наше правило потрібно поставити вище дозвільного правила, інакше воно не буде працювати, як я писав вище; результатом є наступна картина (рис. 3.15):

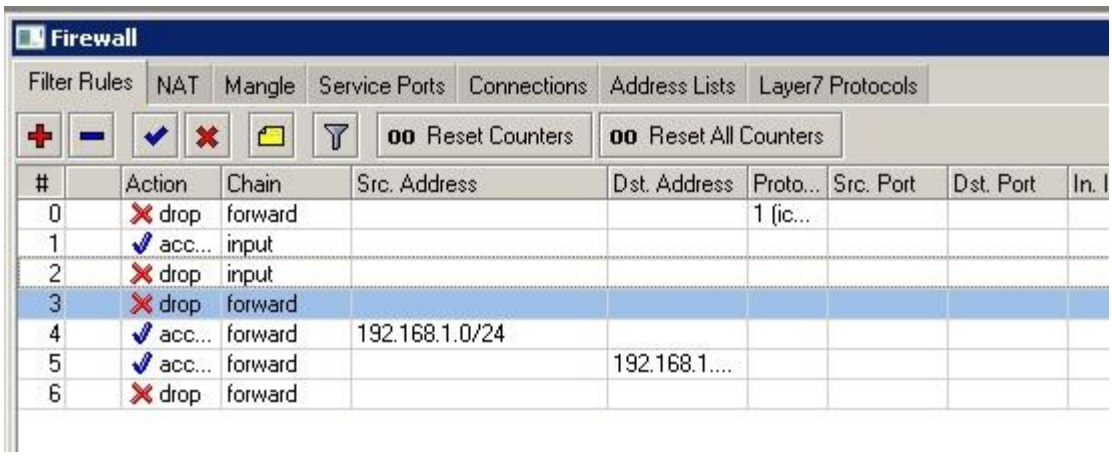


Рис. 3.15 – Послідовність правил

Так само можна заборонити доступ до зовнішніх ресурсів і створити список для блокування, але під час настроювання брандмауера вже вкажіть його як Dst. Address List. Крім IP-адрес, до списку також можна додати доменні імена, наприклад, якщо ми хочемо заборонити користувачам доступ до таких соціальних мереж як однокласники або вконтакті і т.і.

4. Доступ лише до сайтів

У наступному прикладі розглянемо, як дозволити користувачам доступ до Інтернету тільки в портах 80 і 443 і заборонити всі інші, для цього створіть дозвільне правило в chain forward, Protocol выбираємо tcp і в параметрі Dst.Port вказуємо дозволені порти (рис. 3.16):

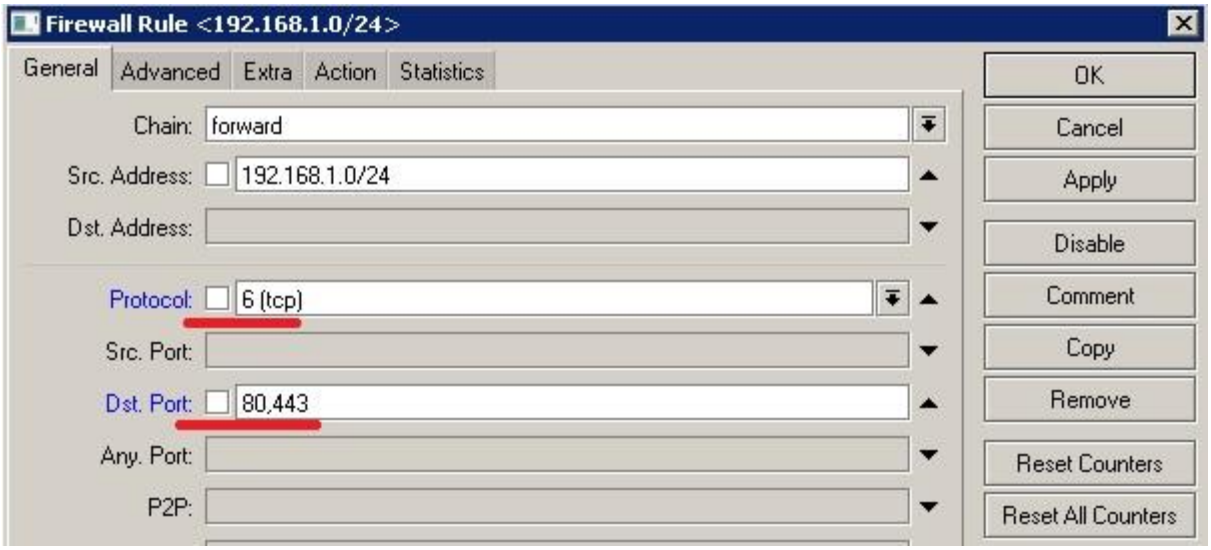


Рис. 3.16 – Дозволені порти

Те ж саме можна зробити і з заборонним правилом з використанням оператора відмови «!», а Action установити drop

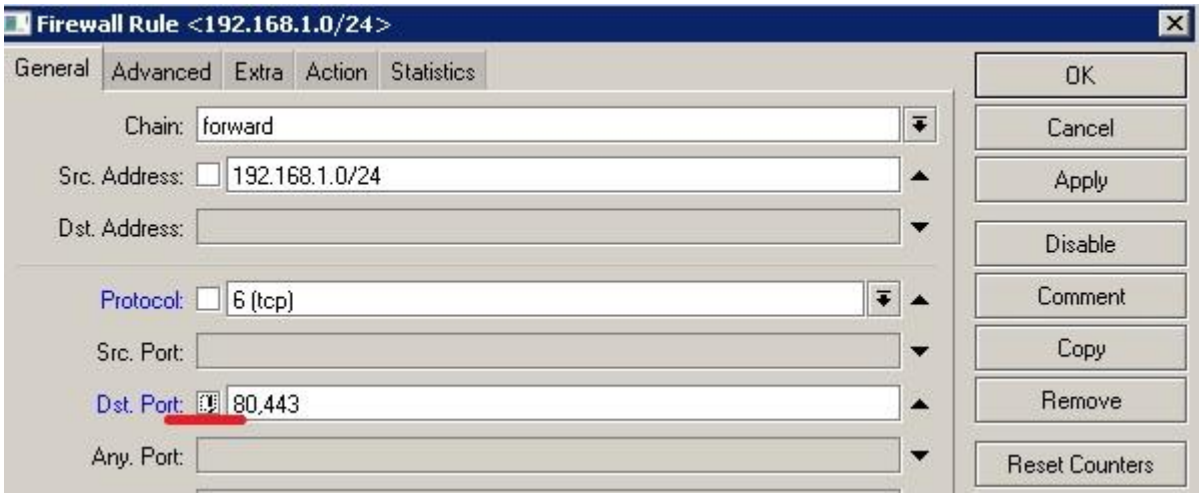


Рис. 3.17 – Оператор відмови

Це означає заборону всіх портів, крім 80 і 443.

Увага! При налаштуванні брандмауера на MikroTIK, рекомендовано проводити всі дії в «Safe Mode», в протилежному випадку ви ризикуєте втратити доступ до маршрутизатора.

Оформити висновки по роботі.

Лабораторна робота №4

Тема: Організація спільного віддаленого захищеного доступу до внутрішніх інформаційних ресурсів через перенаправлення портів.

Мета: Навчитись прокидати порти в роутері MikroTik на прикладі під’єднання камери відеоспостереженя.

Завдання для роботи.

Налаштувати роутер MikroTik використовуючи утиліту WinBox таким чином, щоб отримати доступ до пристроїв відеоспостереження з віддаленої мережі.

Послідовність виконання роботи

Прокидання портів в роутері MikroTik (port forwarding) дозволяє організувати віддалений доступ із інтернету до якого-небудь пристрою всередині вашої локальної мережі (до IP-камери, Web, FTP або ігрового сервера). У даній роботі ми розглянемо приклад, як прокинути порти в роутері MikroTik, щоб отримати доступ до IP-камери в локальній мережі. Ваш роутер обов'язково повинен мати білу IP-адресу, за якою до нього можна підключитися з інтернету.

Перш за все перевіримо чи біла у нас IP-адреса.

У роутері MikroTik перевірити чи білий у вас IP-адрес можна наступним чином:

1. Відкрийте меню **IP - Cloud**
2. Поставте галочку **DDNS Enabled**
3. Натисніть кнопку **Apply**

4. Якщо після цього відобразиться статус "**updated**" без помилок, то у вас білий IP-адрес (рис. 4.1).

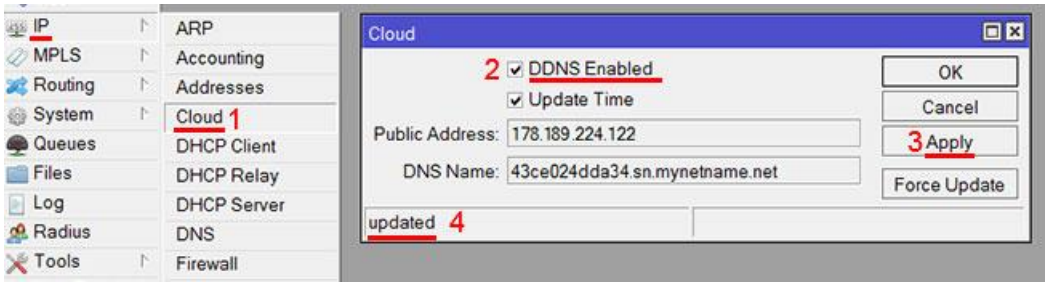


Рис. 4.1 – Перевірка IP-адресу

Якщо в правому нижньому куті екрану відображається помилка типу **"DDNS server received request from IP 67.170.73.47 but your local IP was 104.12.152.1; DDNS service might not work."**, то у вас сірий IP-адрес. В цьому випадку вам потрібно звернутися до провайдера для отримання білої IP-адреси. У деяких провайдерів ця послуга платна (рис. 4.2).

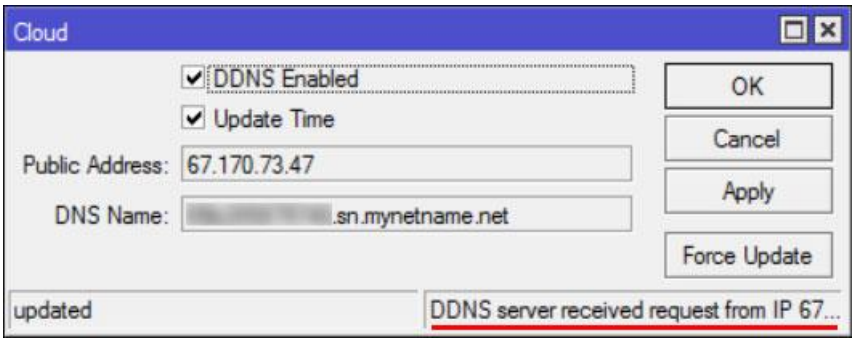


Рис. 4.2 – Помилка при перевірці адреси

Отже, в нас є роутер MikroTik з білим IP-адресом **10.245.42.13**. Він має внутрішню підмережу **192.168.66.0/24**.

Всередині під мережі є IP-камера з адресом **192.168.66.20**, у якої є Web-інтерфейс, що працює на **80** порту. Нам треба забезпечити доступ із інтернету до Web-інтерфейсу IP-камери (рис. 4.3).

Рис. 4.3 – Схема підключення IP-камери

Треба зробити так, щоб при відкриванні в браузері адресу **http://10.245.42.13:10000**, ми потрапляли на Web-інтерфейс IP-камери.

10000 в адресному рядку – це довільний номер порту. Його бажано вказувати в діапазоні від 49152 до 65535. Можна також використовувати діапазон від 1024 до 49151, якщо ви впевнені, що вказаний порт не конфліктуватиме з якоюсь програмою.

Для прокидання портів в роутері MikroTik відкрийте меню **New Terminal** і виконайте команди, описані нижче (рис. 4.4):

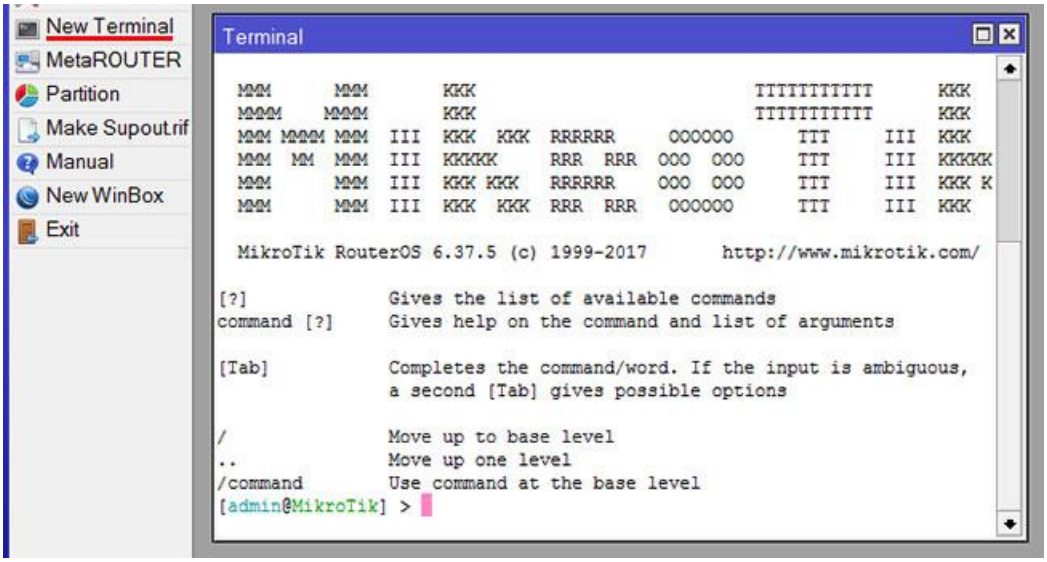


Рис. 4.4 – Команди у меню New Trminal

Насамперед додаємо правило маскарадінгу для підмережі **192.168.66.0/24**

```
/ip firewall nat add action=masquerade chain=srcnat src-address=192.168.66.0/24
```

Далі звернення з інтернету до порту **10000**, перенаправляємо у внутрішню мережу на пристрій **192.168.66.20** і порт **80**.

/ip firewall nat add action=netmap chain=dstnat dst-port=**10000** in-interface=**ether1** protocol=tcp to-addresses=**192.168.66.20** to-ports=**80**

Звернення з локальної мережі до зовнішнього IP-адресу **10.245.42.13** і порту **10000** перенаправляємо в локальну мережу на пристрій **192.168.66.20** і порт **80**, а не в інтернет.

/ip firewall nat add action=netmap chain=dstnat dst-address=**10.245.42.13** dst-port=**10000** in-interface=**bridge** protocol=tcp src-address=**192.168.66.0/24** to-addresses=**192.168.66.20** to-ports=**80**

Створені правила можна подивитися в меню **IP - Firewall** на вкладці **NAT** (рис. 4.5).

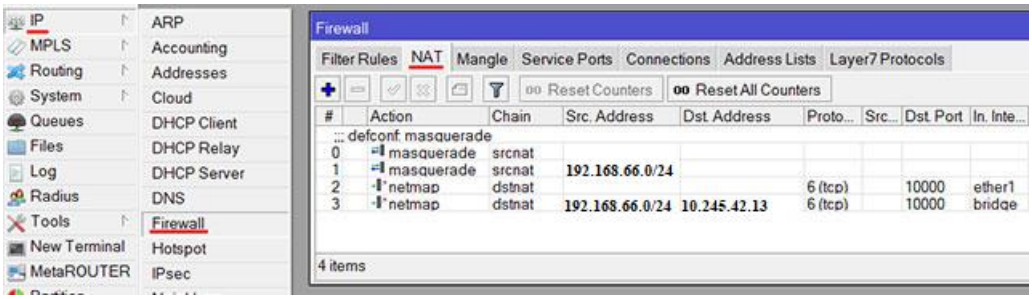


Рис. 4.5 – Меню IP-Firewall

Тепер відкриваємо в браузері адресу **http://10.245.42.13:10000**. З'являється вікно із введенням паролю. Вводимо логін, пароль і потрапляємо на Web-сторінку з відео і налаштуваннями IP-камери (згідно відео інструкції наш логін/пароль Admin / 987654321. При виконанні роботи студент в якості логіна вказує своє прізвище латиницею і у звіті підтверджує скріном) .

Звернення з інтернету до порту **554**, перенаправляємо у внутрішню мережу на пристрій **192.168.66.20** і порт **554**.

/ip firewall nat add action=netmap chain=dstnat dst-port=**554** in-interface=**ether1** protocol=tcp to-addresses=**192.168.66.20** to-ports=**554**

Звернення з локальної мережі до зовнішнього IP-адресу **10.245.42.13** і порту **554** перенаправляємо в локальну мережу на пристрій **192.168.66.20** і порт **554**, а не в інтернет.

/ip firewall nat add action=netmap chain=dstnat dst-address=**10.245.42.13** dst-port=**554** in-interface=**bridge** protocol=tcp src-address=**192.168.66.0/24** to-addresses=**192.168.66.20** to-ports=**554**

Оформити висновки по роботі.

Лабораторна робота № 5

Тема: Вивчення апаратних засобів для реалізації систем контролю доступу.
Мета: Навчитись налаштовувати роутер MikroTik

Хід виконання роботи.

Створіть новий проект (для полегшення збереження виконаної роботи рекомендовано зареєструватися на сайті) (рис. 5.1)

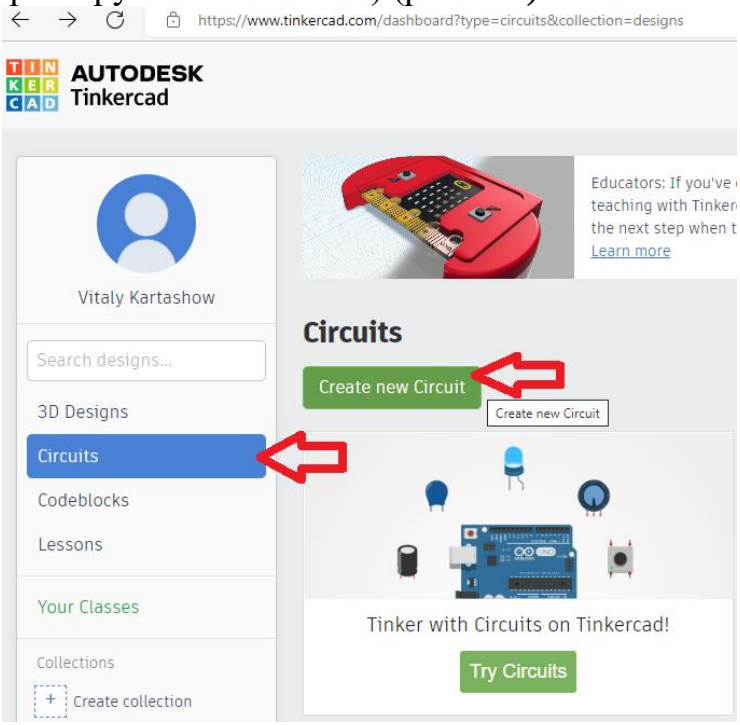


Рис. 5.1 – Головна сторінка

Оберіть у випадаючому списку всі компоненти: Components >> All (рис. 5.2):

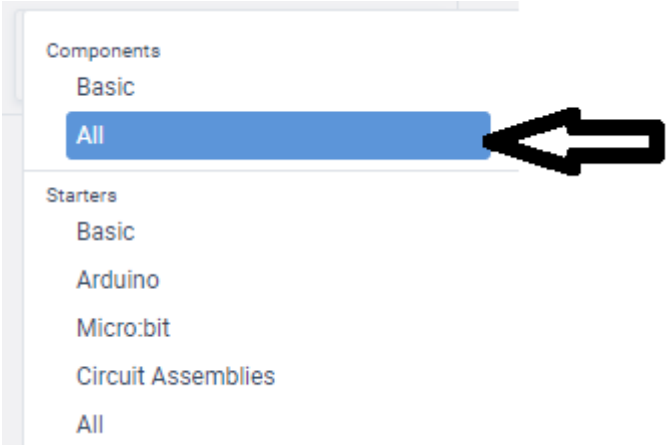


Рис. 5.2 – Компоненти

Перетягніть з інструментальної панелі на робоче поле наступні компоненти: дисплей (LCD 16x2), клавіатура (Keypad 4x4), резистори (Resistor 1kOm) (3шт), сервопривід (Micro Servo), мікроконтролер (Arduino Uno R3) та з'єднувальну панель (Breadboard Small) (рис. 5.3):

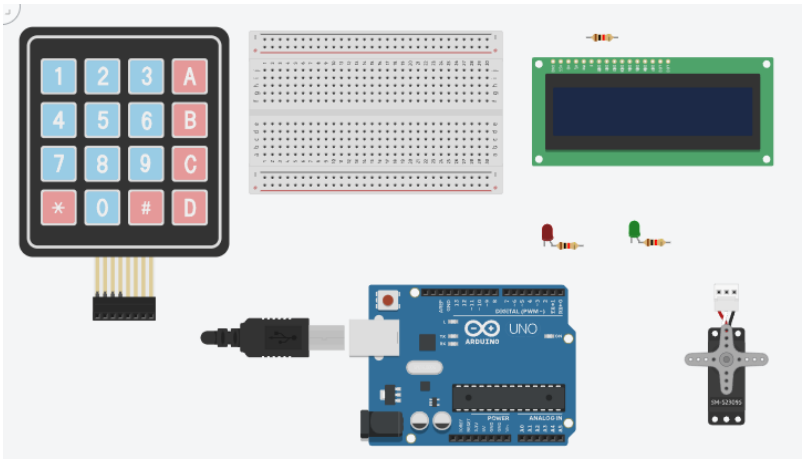


Рис. 5.3 – Компоненти схеми

Подайте живлення +5V з Arduino на макетну плату. Підведіть «–» з макетної плати до клеми GND на Arduino (рис. 5.4). Задайте колір провідників: червоний для «+» і чорний для «–».

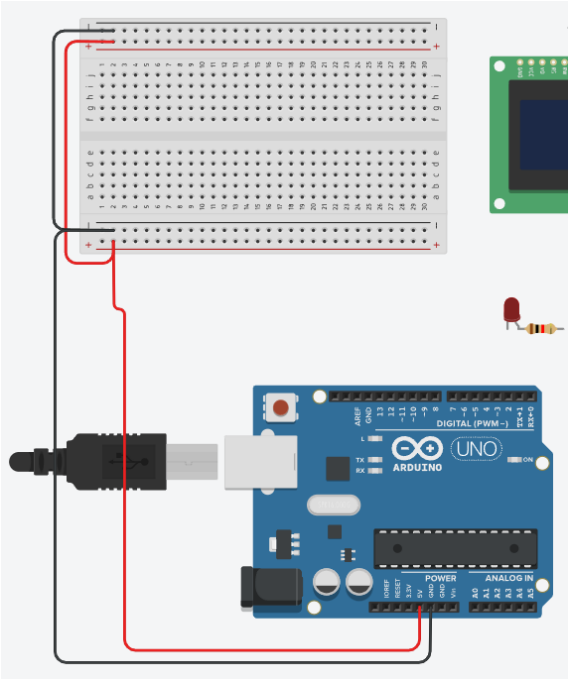


Рис. 5.4 – Під’єднання макетної плати

Здійсніть під’єднання виводів роз’єму клавіатури до клем Arduino: першого виводу на клему «12», а далі послідовно від «9» до «~3» (рис. 5.5). Задайте різний колір для кожного провідника.

Під’єднайте рідкокристалічний дисплей до макетної плати (рис. 5.6). Для цього провідниками чорного кольору подайте «–» на клеми дисплею: GND, V0, RW та LED Cathode. А провідниками червоного кольору подайте «+» на клеми дисплею: VCC та LED Anode. Останній підключіть через резистор 1 кОм.

Сигнальні клеми підключіть провідниками різного кольору до клем з порядковим номером на макетній платі: «DB4» до «20», «DB5» до «21», «DB6» до «22» та «DB7» до «23». Також підключіть клеми «Enable» до «19» та «Register Select» до «18».

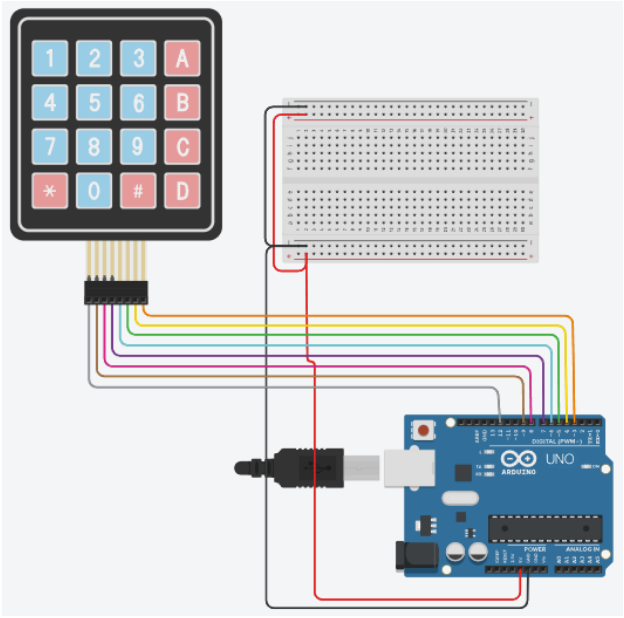


Рис. 5.5 – Під’єднання клавіатури

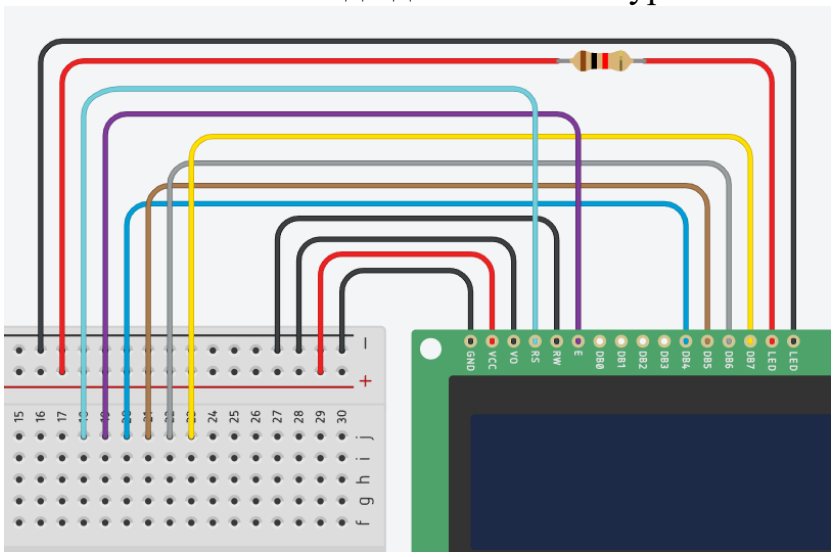


Рис. 5.6 - Під’єднання дисплея

Наступним кроком під’єднайте виводи Arduino до роз’ємів макетної плати, на які підключені виводи дисплея в наступній послідовності:

Arduino	Макетна плата	Arduino	Макетна плата
10	23	A0	20
11	22	A1	19
13	21	A2	18

Щоб не плутатись, використовуйте провідники відповідних кольорів, якими під’єднано виводи дисплея до макетної плати.

Під’єднайте сервопривід до Arduino (рис. 5.7):

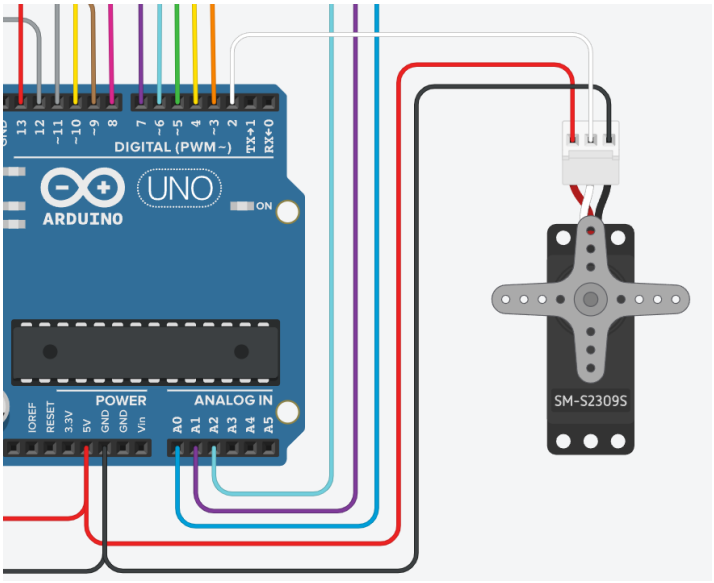


Рис. 5.7 - Під’єднання сервоприводу

Підключіть світлодіоди зеленого та червоного кольору. Катодні ніжки до «–» макетної плати, а «+» через резистори 1 кОм до виводів A4 (для зеленого) та A3 (для червоного).

В готовому вигляді схема підключення виглядає наступним чином (рис. 5.8):

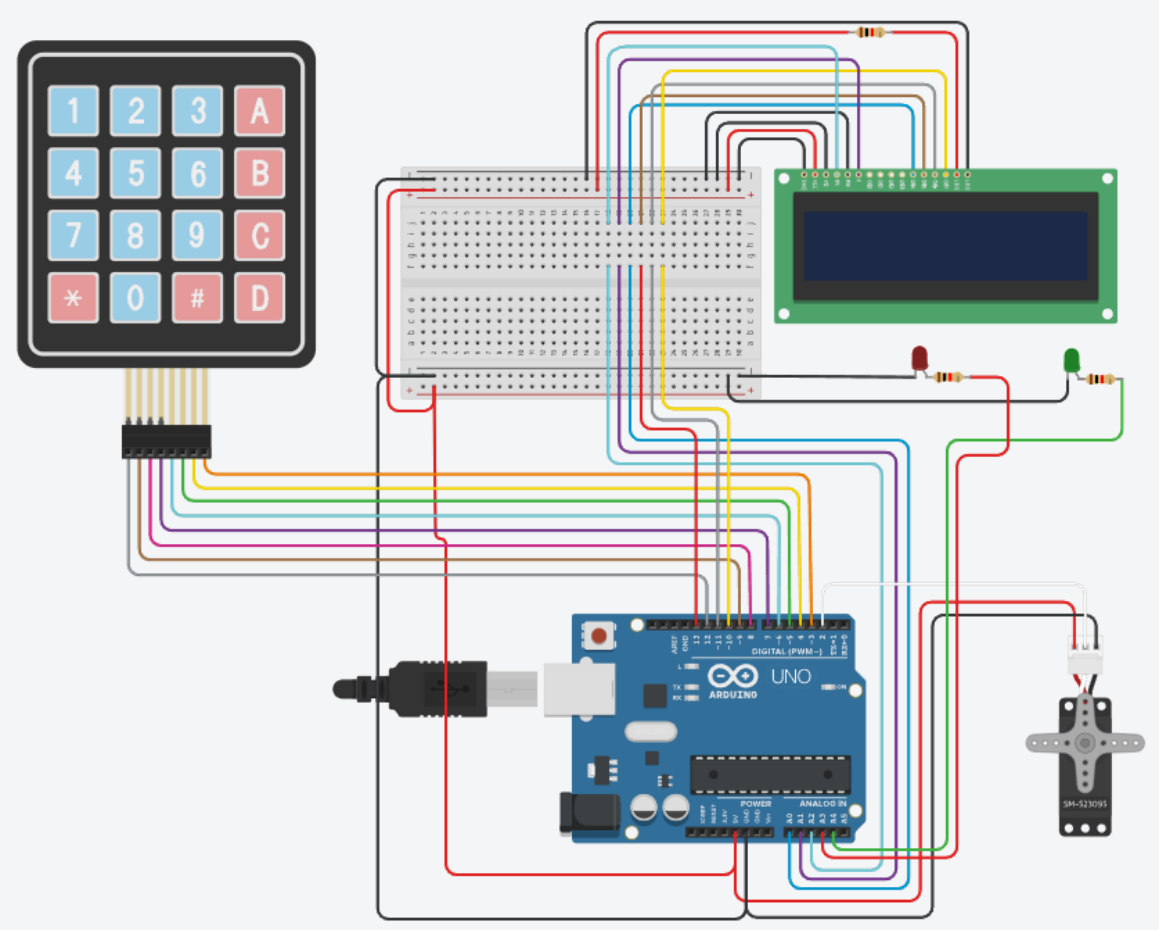


Рис. 5.8 – Схема підключення Arduino

Оформіть висновки по роботі.

Лабораторна робота № 6

Тема: Створення базової системи контролю доступу.

Мета: Навчитись налаштовувати роутер MikroTik

Хід виконання роботи.

Перейдіть в поле написання коду (рис. 6.1):

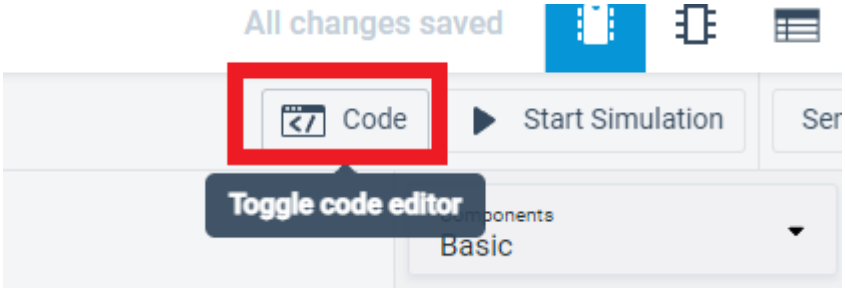


Рис. 6.1 – Перемикач редактора коду

Виберіть режим редагування «текст» (рис. 6.2):

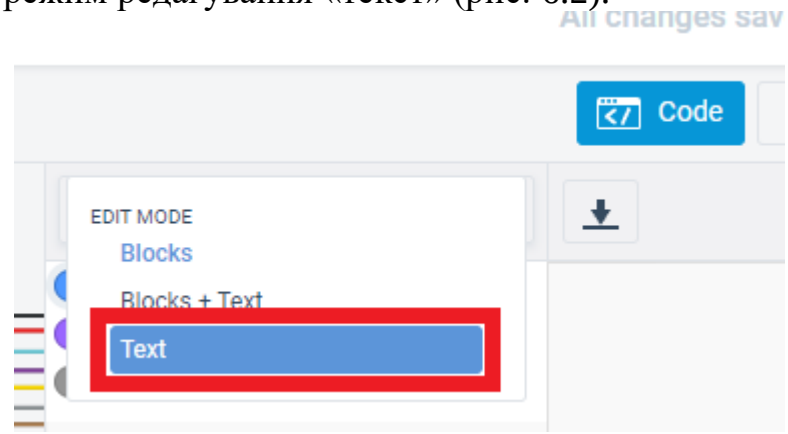


Рис. 6.2 – Вибір варіантів програмування

Пропишіть параметри під'єднання клавіатури (рис.6.3), сервоприводу (рис. 6.4) та дисплею з бібліотекою (рис. 6.5):

```
#include <Keypad.h>
const byte ROWS = 4;
const byte COLS = 4;
char keys [ROWS][COLS] = {
  {'1','2','3','A'},
  {'4','5','6','B'},
  {'7','8','9','C'},
  {'*','0','#','D'},
};
byte rowPins [ROWS] = {12,9,8,7};
byte colPins [COLS] = {6,5,4,3};
Keypad keypad = Keypad (makeKeymap(keys),rowPins,colPins,ROWS,COLS);
```

Рис. 6.3 - Опис модуля клавіатури

```
#include <Servo.h>
Servo servo1;
int ledgreen = 18;
int ledred = 17;
```

Рис. 6.4 - Опис сервоприводу

```
#include <SPI.h>
#include <LiquidCrystal.h>
LiquidCrystal lcd (16,15,14,13,11,10);
```

Рис. 6.5 - Опис дисплею

Переходимо до основної частини коду. Пропишіть під'єднання до виводів Arduino (рис.6.6):

```
void setup ()
{
 Serial.begin (9600);
  pinMode (ledgreen, OUTPUT);
  pinMode (ledred, OUTPUT);
  servo1.attach (2);
  lcd.begin (16,2);
}
```

Рис. 6.6 - Розділ початкового налаштування (виконається 1 раз)

В полі програмування циклу «void loop» запрограмуйте вивід вітального повідомлення «Welcome» (рис. 6.7) та повідомлення «Enter password» при наборі «C» на клавіатурі (рис. 6.8):

```
  lcd.setCursor (0,0);
   lcd.print ("Welcome");
```

Рис. 6.7 – Команда друку на екрані Welcome

```
  char key = keypad.getKey ();
  if (key == 'C')
  {
    lcd.setCursor (0,0);
    lcd.print ("Enter password");
```

Рис. 6.8 – Команда «введіть пароль» при натисканні «C» на клавіатурі

Задайте розмір паролю в 6 символів та відображення їх на дисплеї у вигляді «*» (рис. 6.9). Запрограмуйте зелений світлодіод на сигналізацію введення символів паролю.

```
    lcd.setCursor (0,1);
    char pass[6];
    for (int i = 0; i < 6; i++)
    {
    label: char key = keypad.getKey ();
      if (key != NO_KEY)
      {
      pass [i] = key;
        lcd.print ("*");
        digitalWrite (ledgreen, HIGH);
        digitalWrite (ledgreen, LOW);
      }
    else goto label;
    }
```

Рис. 6.9 – Команда заміни символів на «*» при введені паролю

Вкажіть пароль та пропишіть команду виводу повідомлення на дисплей «доступ дозволено» при вірному введенні паролю (рис. 6.10), та «в доступі відмовлено» при невірному паролі (рис. 6.11). Запрограмуйте зелений світлодіод на постійне свічення при відчинених дверях за умови вірного паролю, та потрійне мигання червоного світлодіоду при невірному паролі. Вкажіть затримку при миганні червоного світлодіода – 500 мсек.

```
54      char rightpass [] = "112233";
55      if (strcmp (pass, rightpass) == 49)
56      {
57      lcd.clear ();
58        lcd.setCursor (0,0);
59        lcd.print ("access is");
60        lcd.setCursor (3,1);
61        lcd.print ("allowed");
62        servo1.write(0);
63        digitalWrite (ledgreen, HIGH);
64        delay (2500);
65      }
```

Рис. 6.10 – Програмування сервоприводу, дисплею та світлодіоду при правильному паролі

```
66      else
67      {
68        lcd.clear ();
69        lcd.setCursor (0,0);
70        lcd.print ("access denied");
71        digitalWrite (ledred, HIGH);
72        delay (500);
73        digitalWrite (ledred, LOW);
74        delay (500);
75        digitalWrite (ledred, HIGH);
76        delay (500);
77        digitalWrite (ledred, LOW);
78        delay (500);
79        digitalWrite (ledred, HIGH);
80        delay (500);
81        digitalWrite (ledred, LOW);
82        }
```

Рис. 6.11 – Програмування сервоприводу, дисплею та світлодіоду при не правильному паролі

Задайте тривалість відчиненого стану дверей 3 сек, та пропишіть команду закриття дверей (рис. 6.12)

```
83    delay (3000);
84    servo1.write(90);
85    digitalWrite (ledgreen, LOW);
86     lcd.clear ();
87      }
88  }
```

Рис. 6.12 – Команда закриття дверей

Запустіть симуляцію роботи проекту (рис. 6.13):

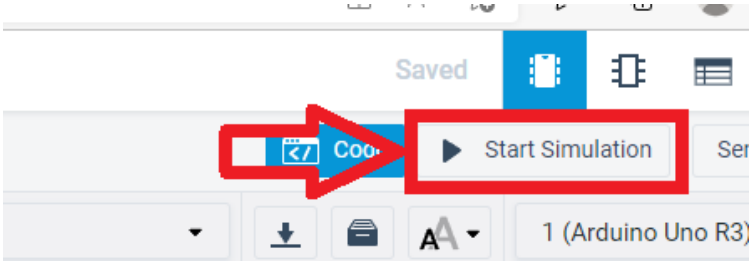


Рис. 6.13 – Кнопка запуску в режимі симуляції

Проект має працювати наступним чином: при натисненні на будь-які символи крім «С» система не реагує і виводить на дисплей вітальне повідомлення (рис. 6.14):

Рис. 6.14 – Вітальне повідомлення

При натисненні на «С» на клавіатурі вітальне повідомлення змінюється на «введіть пароль» (рис. 6.15). При введенні пароль символи відображаються у вигляді «*» (рис. 6.16):

Рис. 6.15 – Повідомлення «Введіть пароль»

Рис. 6.16 – Відображення символів

При введенні невірного паролю виводиться повідомлення «в доступі відмовлено» (рис. 6.17), і тричі мигає червоний світлодіод. Сервопривід не здійснює жодного руху, а при вірному – «доступ дозволено» (рис. 6.18):

Рис. 6.17 – Повідомлення при невірному паролі

Рис. 6.18 – Повідомлення при вірному паролі

При отриманні доступу - сервопривід здійснює рух на 90гр проти годинникової стрілки, при цьому горить зелений світлодіод. Після трьох секундної паузи сервопривід повертається у початкове положення. На екрані знову з’являється напис «Wellcome». Процедуру можна повторити знову.

Оформіть висновки по роботі. Надайте у звіті зафіксовані з допомогою PrintScreen основні етапи роботи.

При виникненні труднощів звірте код із наведеним у додатку А та скористайтесь відеоматеріалами наведеними в ЕНК в системі Atutor.

Лабораторна робота № 7

Тема: Вивчення апаратних засобів контролю доступу біометричного типу.
Мета: Вивчити схему під'єднання сканера відбитку пальця FPM10A до Arduino та його програмування.

1. Порядок виконання роботи.

1.1. Одержати у викладача завдання для розробки програми.
1.2. Ознайомитись з схемами під'єднання сканера відбитку пальця FPM10A та LCD-дисплея до Arduino.
1.3. Під'єднати сканер відбитку пальця FPM10A та LCD-дисплей до Arduino.
1.4. Провести програмування Arduino згідно завдання, виданого викладачем.
1.5. Перевірити правильність роботи Arduino для роботи в системі доступу.
1.6. Оформити звіт по виконаній роботі.

Завдання для роботи

Розробити керуючу програму, для створення бази знімків відбитків пальців. Результатом програми має бути виведення повідомлення на дисплей з інформацією про прізвище користувача та приналежність відбитку до пальців лівої чи правої руки.

Короткі теоретичні відомості

Сканер відбитку пальців / Fingerprint scanner – пристрій, що може зчитувати, зберігати та порівнювати зображення відбитків пальців. У будь-якого сканера відбитків пальців є 2 основні функції: збереження зображення відбитку та порівняння його з іншими, що вже є у базі даних.

Модуль **FPM10A** (рис. 7.1) використовується в різних системах безпеки. В ньому міститься чіп, що опрацьовує зображення, робить необхідні розрахунки для виявлення відповідностей між вже збереженими та поточними даними.

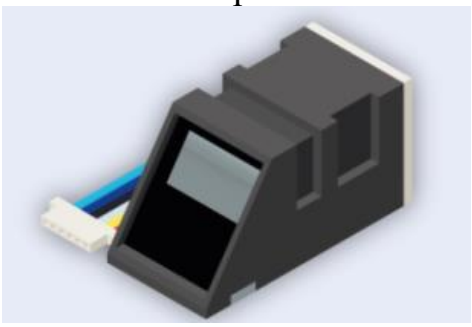


Рис. 7.1 – Загальний вигляд сканера FPM10A

Сканер **FPM10A** працює на швидкості 57600 і має 6 виходів. Для роботи нам потрібні 4: **VCC, GND, RX** та **TX**. VCC підключаємо до виходу 3,3V. RX та TX до 3-го та 2-го виходів цифрового порту відповідно (рис. 7.2):

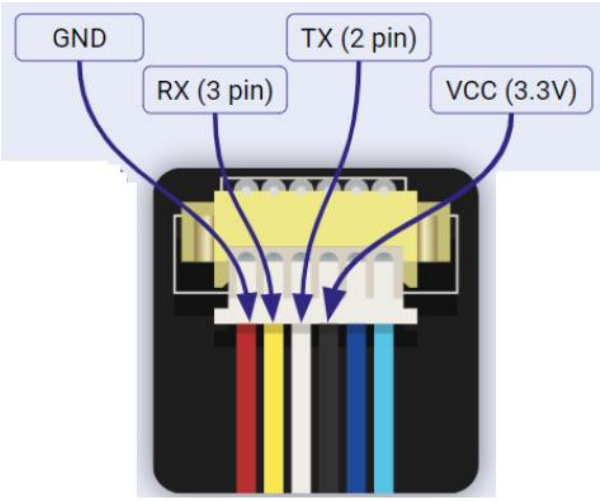


Рис. 7.2 – Схема під’єднання сканера FPM10A

Процес сканування відбувається наступним чином:

При успішному скануванні виводиться повідомлення:

```
00:45:28.220 -> Image taken
00:45:28.641 -> Image converted
00:45:28.641 -> Remove finger
```

Повідомлення свідчить, що сканер отримав зображення пальця, потім перетворив на щось зрозуміле тільки йому і тепер просить прибрати палець. Як тільки ви приберете палець, то отримаєте повідмлення:

```
00:45:30.623 -> ID 3
00:45:30.670 -> Place same finger again
```

Щоб переконатися, що це той палець і немає ніяких помилок, потрібно прикласти палець ще раз.

```
00:48:38.829 -> Image taken
00:48:39.202 -> Image converted
00:48:39.248 -> Creating model for #3
00:48:39.295 -> Prints matched!
00:48:39.295 -> ID 3
00:48:39.342 -> Stored!
00:48:39.342 -> Ready to write a new fingerprint!
00:48:39.388 -> Please type in the ID # (from 1 to 127)
```

Сканер відповів, що відбитки збіглися, і що новий відбиток збережений в базу. Можна додати ще один відбиток, або вийти з програми.

LCD дисплей

Окрім сканера ми використаємо в нашій схемі рідкокристаліччний дисплей LCD 1602 I2C для виводу текстової інформації. Схема його підключення наведена на рис. 7.3.

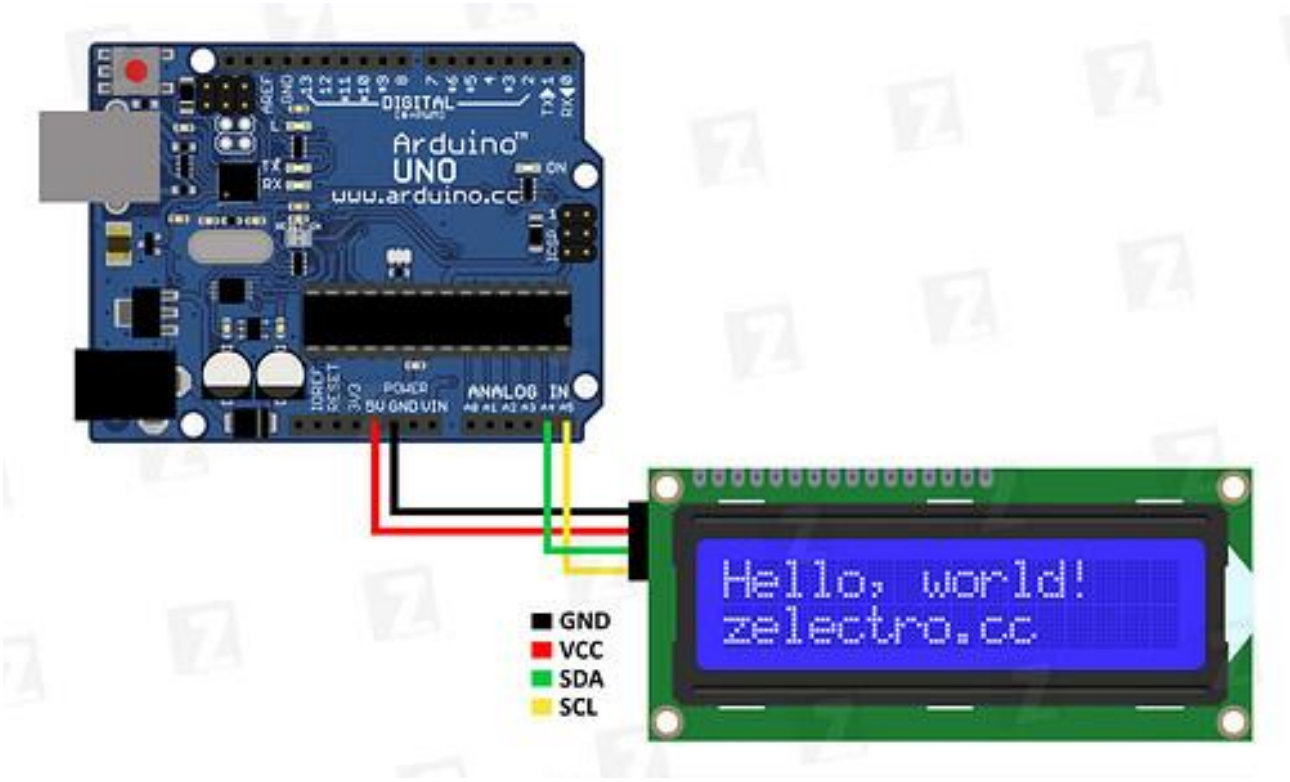


Рис. 7.3 - Схема під’єднання дисплею LCD 1602 I2C до плати ArduinoUno

Хід виконання роботи

Для початку роботи слід виконати наступну послідовність дій:

1. Скачати і встановити Arduino IDE (рис 7.4):

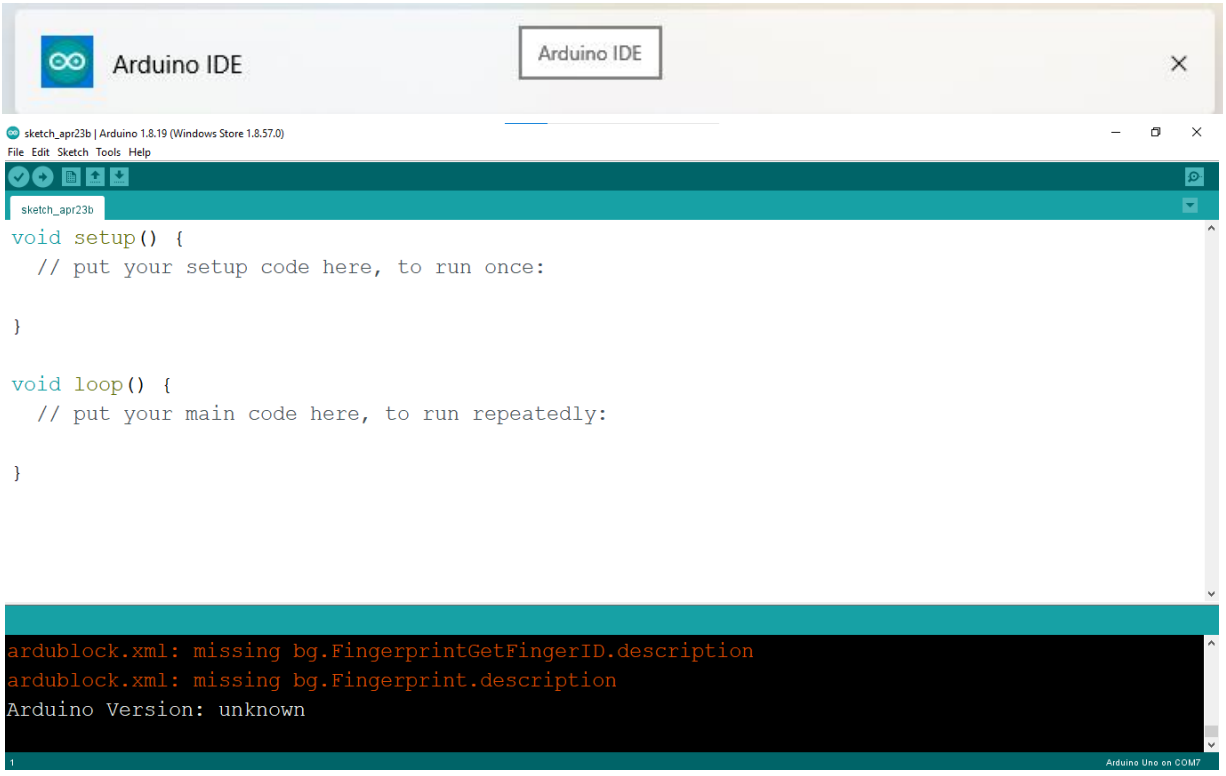
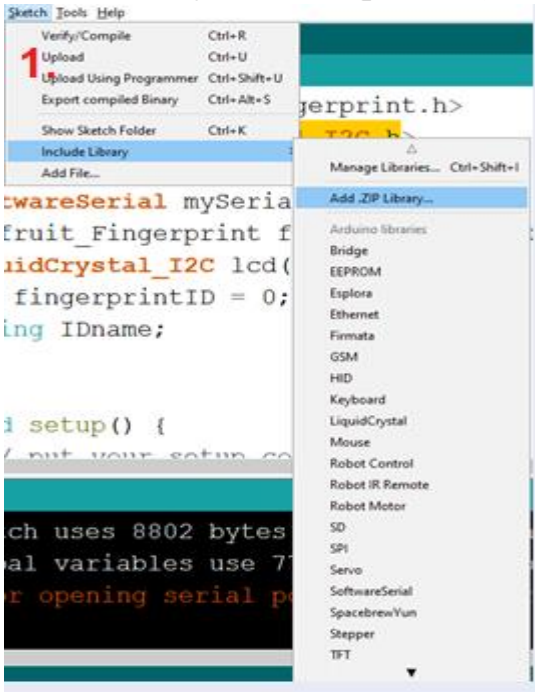


Рис. 7.4 – Загальний вигляд Arduino IDE

2. Завантажити і під’єднати бібліотеку Adafruit_fingerprint.h (рис. 7.5);
3. Завантажити і під’єднати бібліотеку LiquidCrystal_I2C.h (рис. 7.6);
4. Завантажити приклад з меню File>>Examples>> Adafruit Fingerprint Sensor Library>>enroll (рис. 7.7):



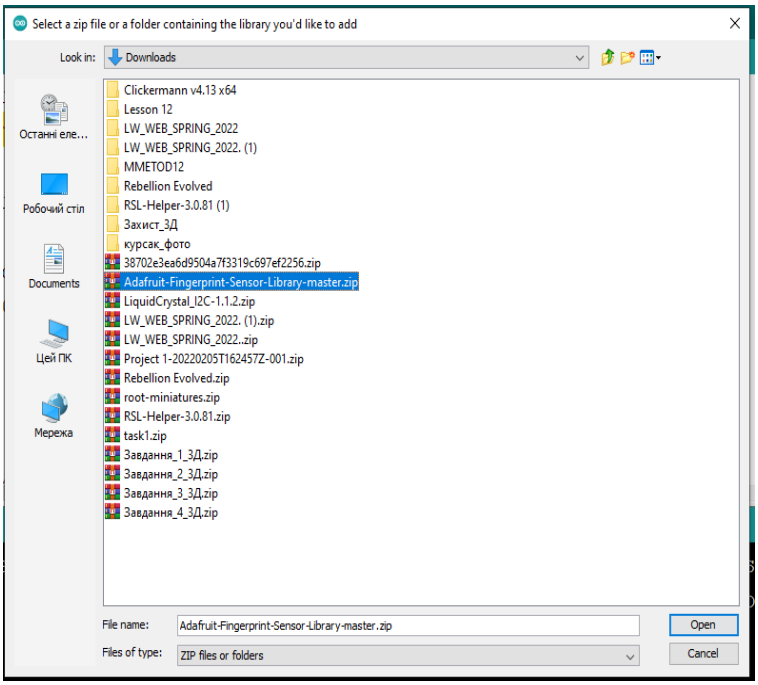


Рис. 7.5 – Бібліотека сканера

Рис. 7.6 – Бібліотека дисплея

Рис. 7.7 – Завантаження прикладу

5. Під’єднати датчик відбитку пальця та дисплей (див. рис. 7.2 та 7.3);
6. Вибрати платформу (в нашому випадку ArduinoUno) (рис. 7.8);
7. Вибрати порт, до якого підключено контролер (рис. 7.9);
8. Завантажити enroll в контролер (рис. 7.10);

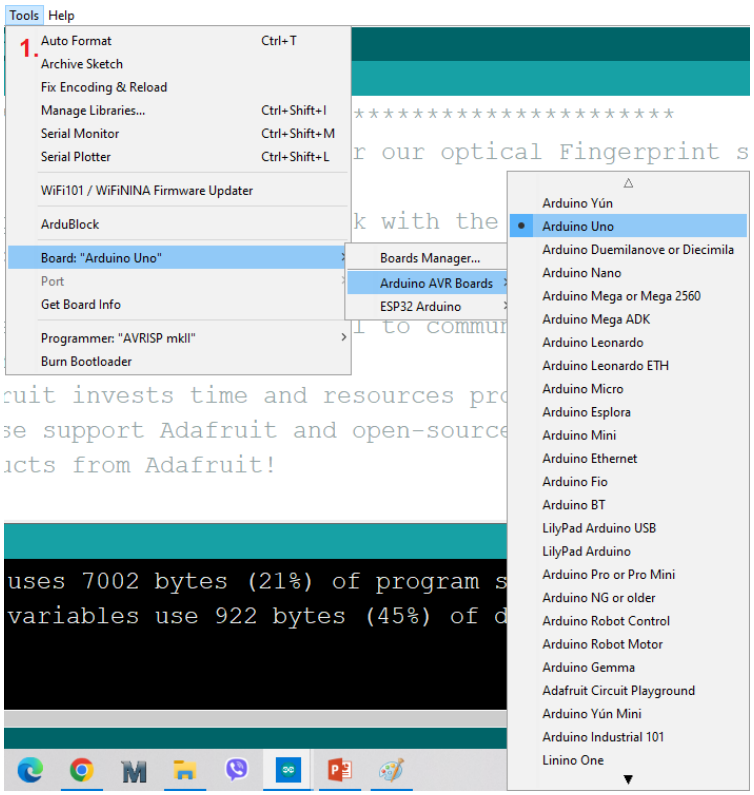


Рис. 7.8 – Вибір платформи

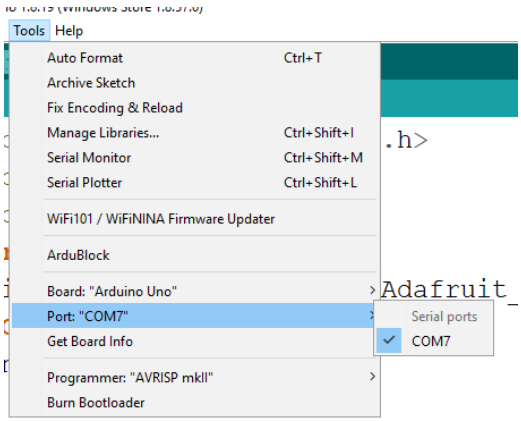


Рис. 7.9 – Вибір порту

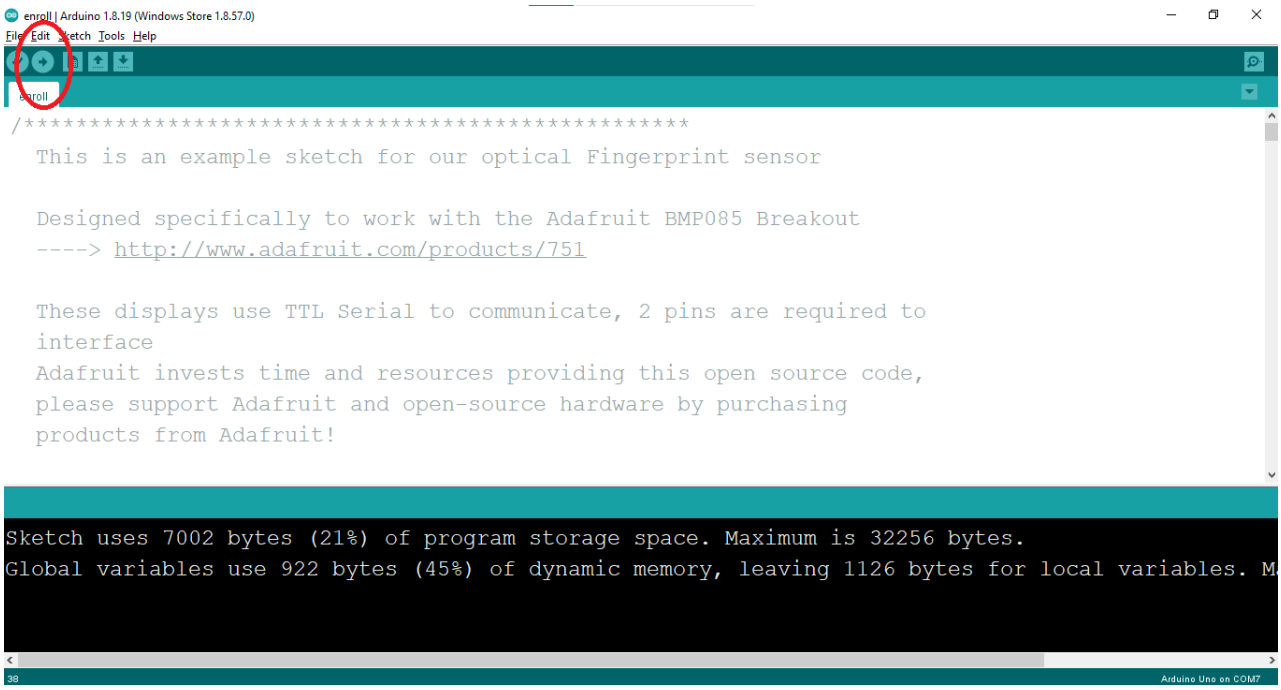


Рис. 7.10 – Завантаження enroll

9. Відкрити монітор порту (рис. 7.11);
10. Вибрати швидкість 9600 (рис. 7.12);

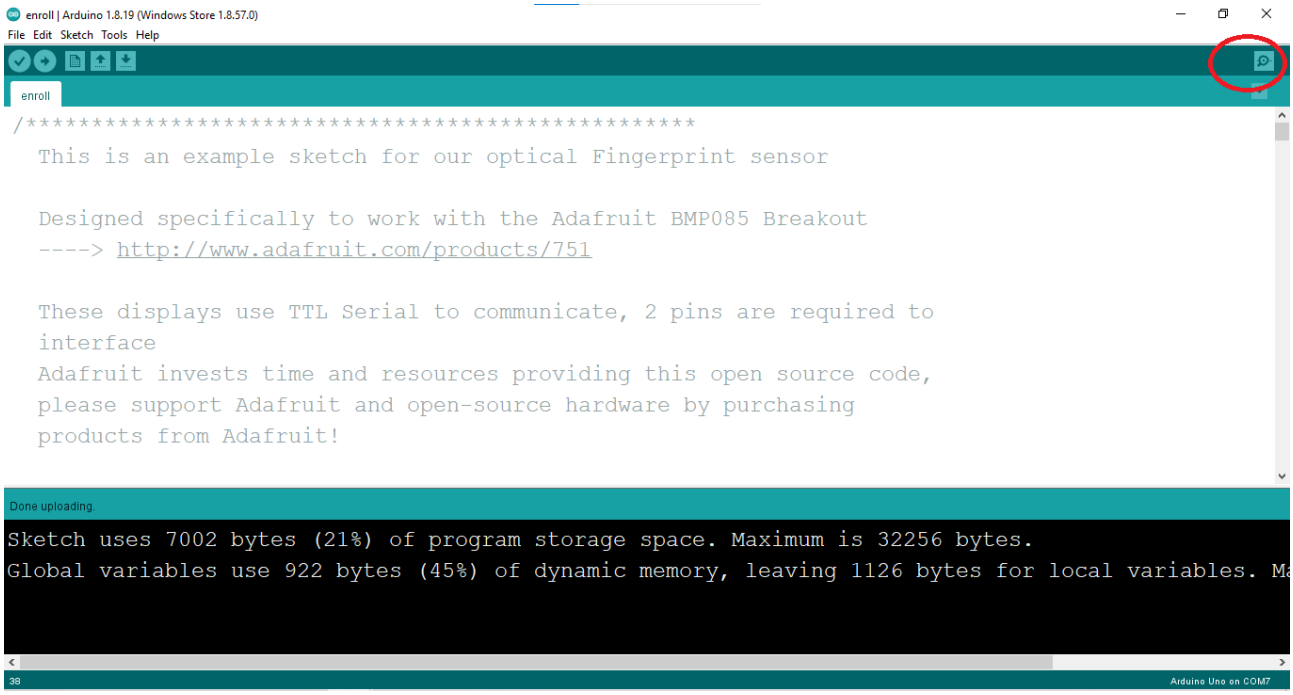


Рис. 7.11 – Монітор порту

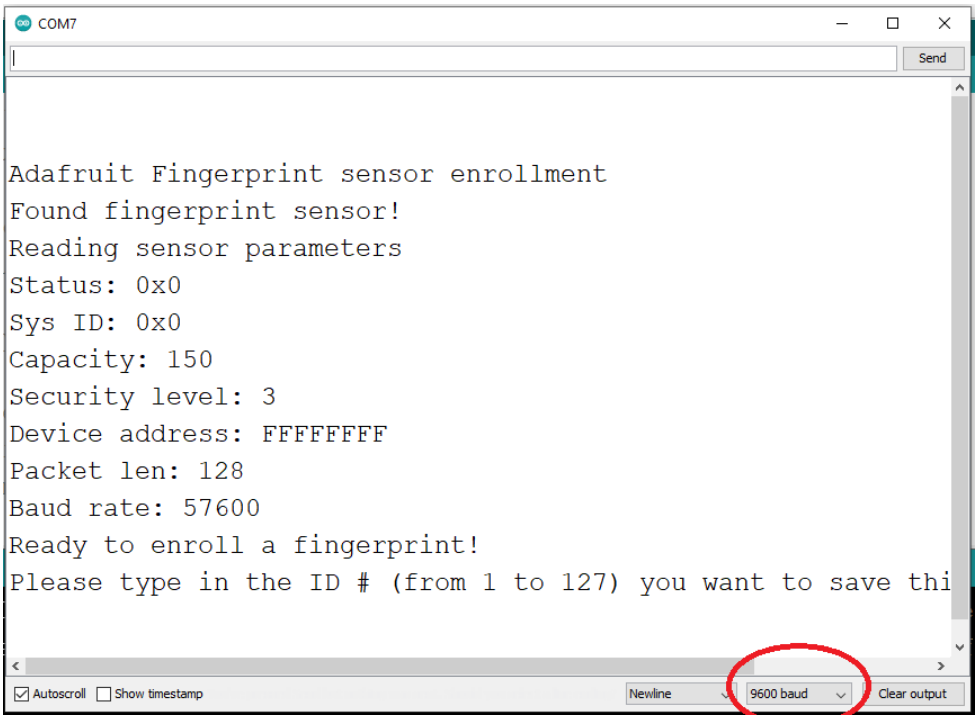


Рис. 7.12 – Вибір швидкості

11. Записати відбиток: ввести номер, просканувати перший палець, прикласти палець ще раз;
12. Записати другий відбиток: ввести номер, просканувати другий палець, прикласти палець ще раз (рис. 7.13);
13. Повторити процедуру для всіх 10 пальців (записувати відбитки можна під будь-яким номером, навіть під тим, який вже зайнятий. В такому випадку, відбиток просто перезапишеться на новий.).

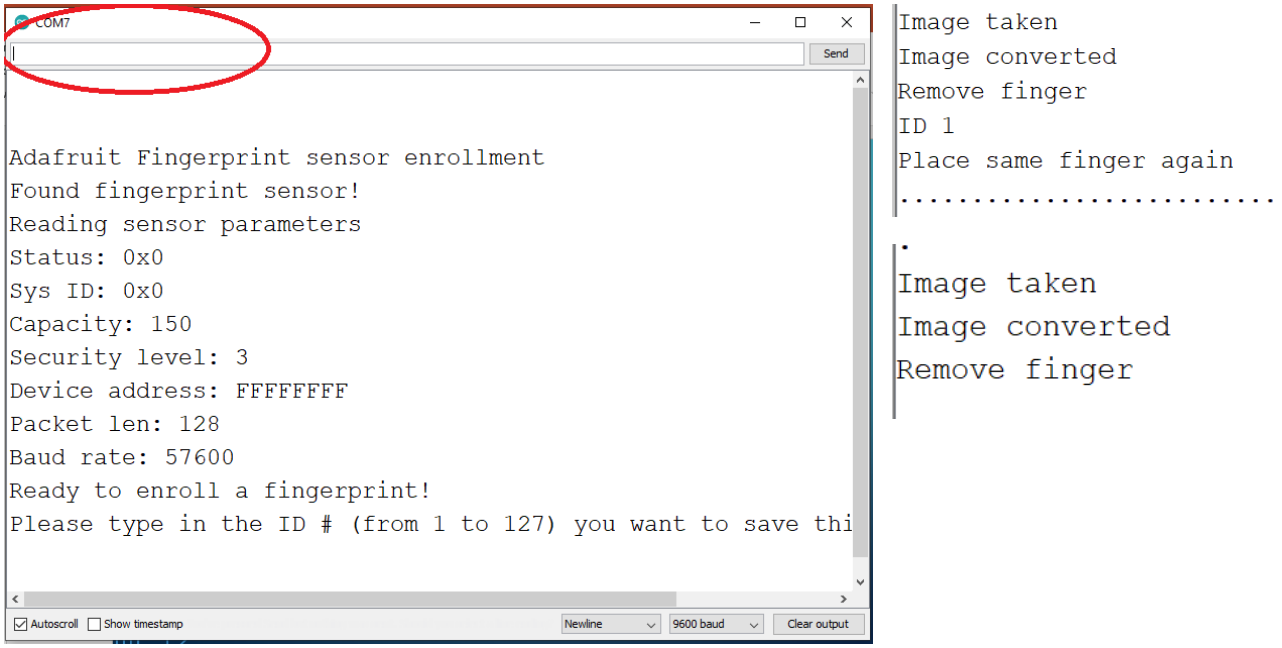


Рис. 7.13 – Процес сканування

14. Створіть програму, яка буде писати на екрані, до якої руки належить палець, який Ви приклали:
    - 14.1. Перевіримо чи є прикладений палець до сканера в базі. У старті напишемо код, який виведе в монітор порту кількість записаних відбитків і повідомлення про те, що ми очікуємо палець (рис. 7.14);
    - 14.2. Описуємо код для Setup (виконується 1 раз) (рис. 7.15);
    - 14.3. Описуємо loop (виконується циклічно безперестанку) (рис. 7.16);
    - 14.4. Описуємо функцію пошуку відбитку (рис.7. 17).

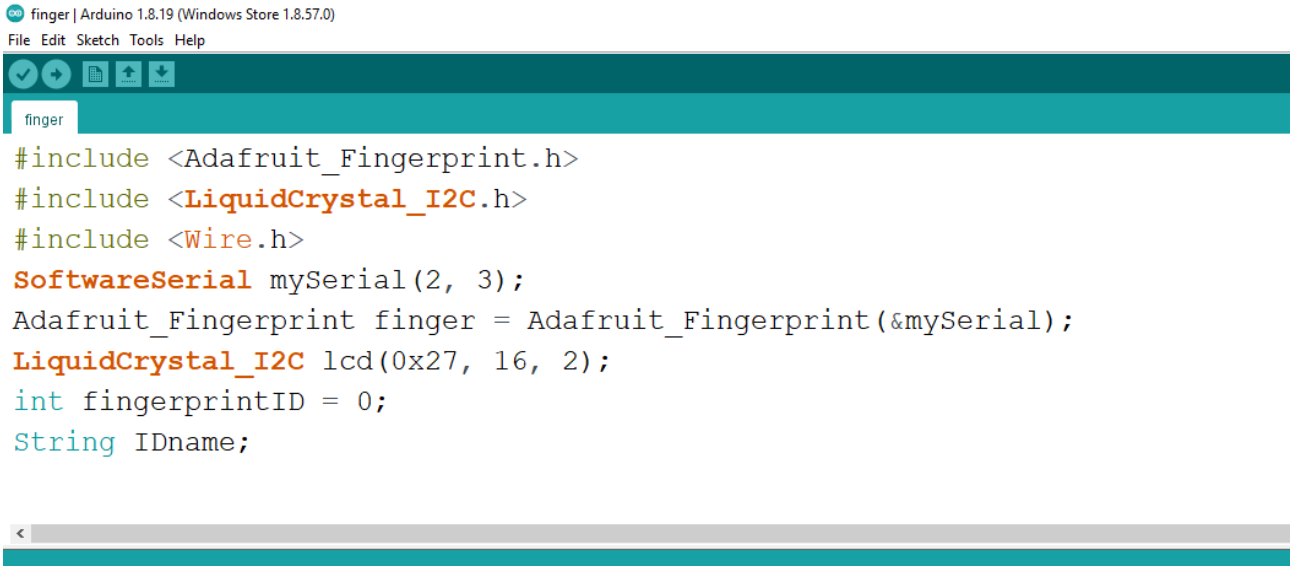


Рис. 7.14 – Опис сканера і дисплея

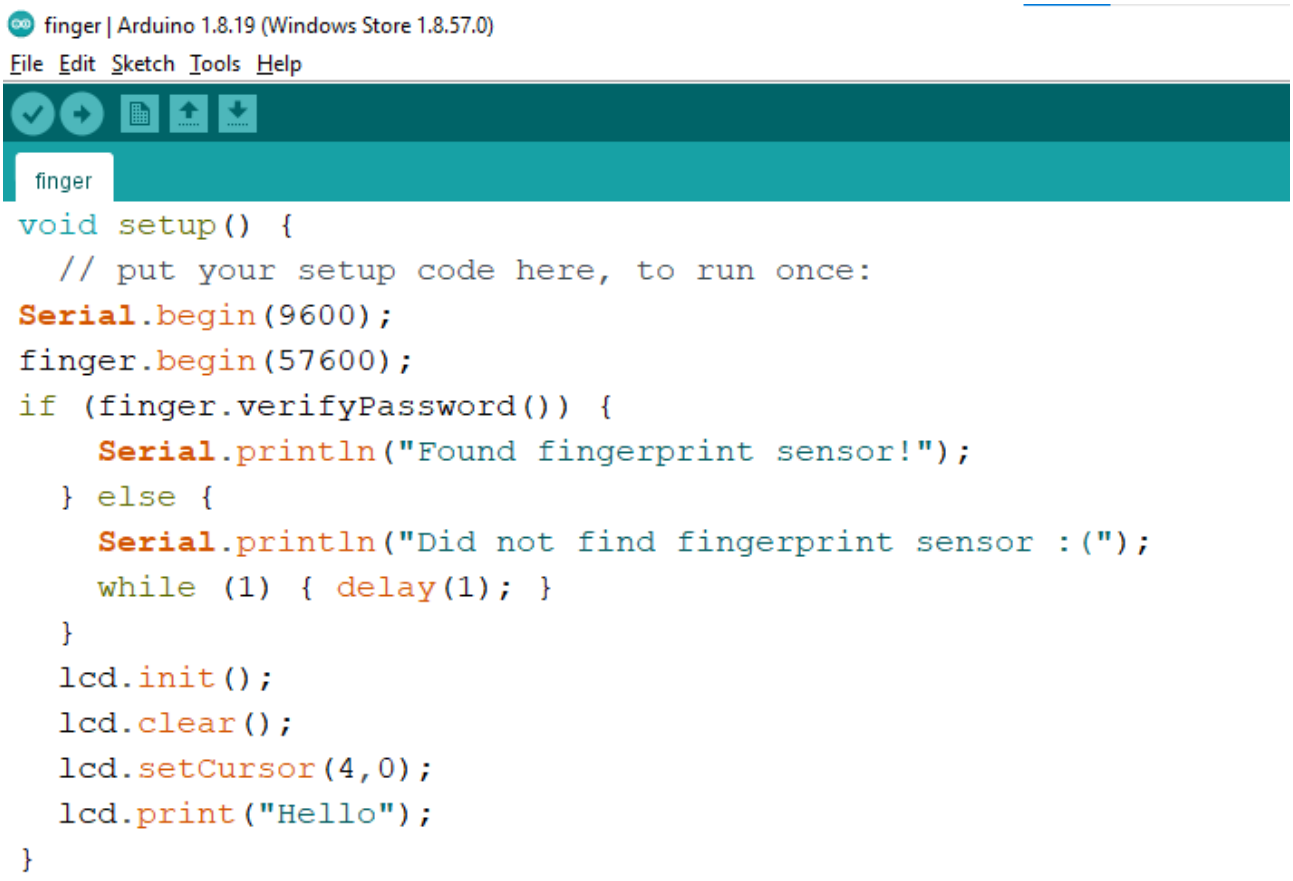


Рис. 7.15 – Код для Setup

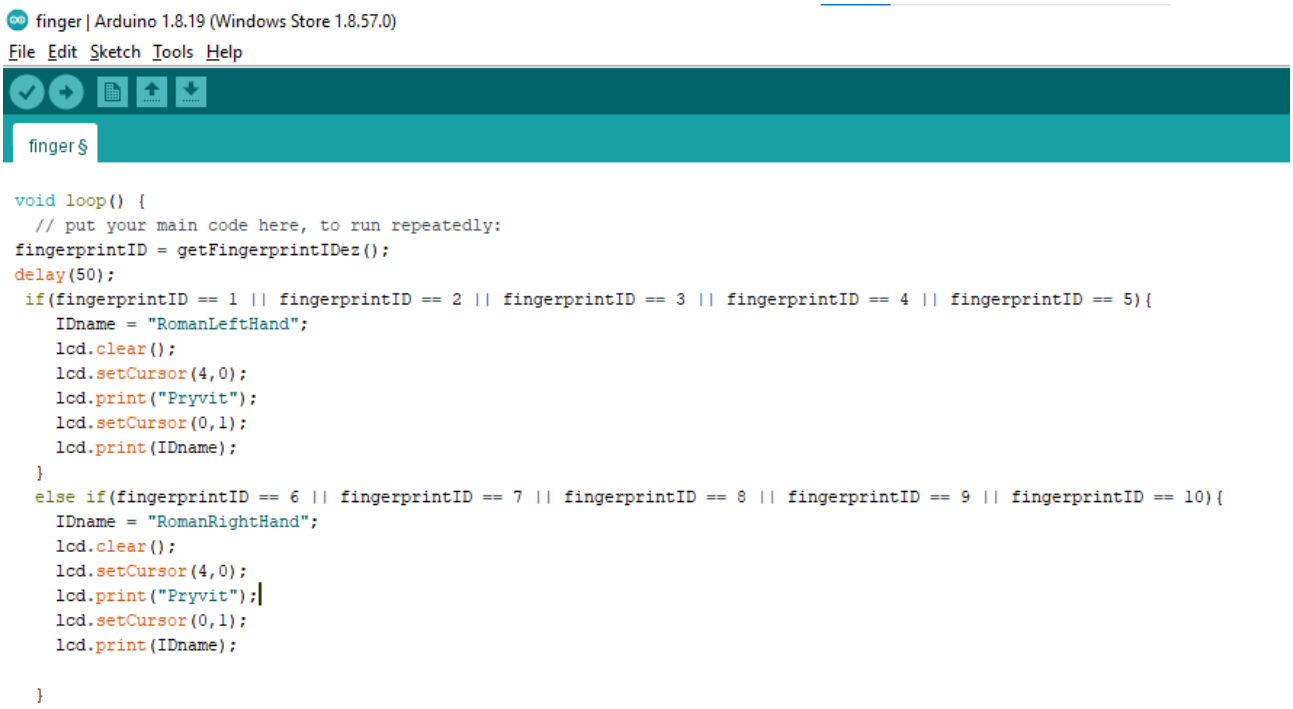


Рис. 7.16 – Код для loop

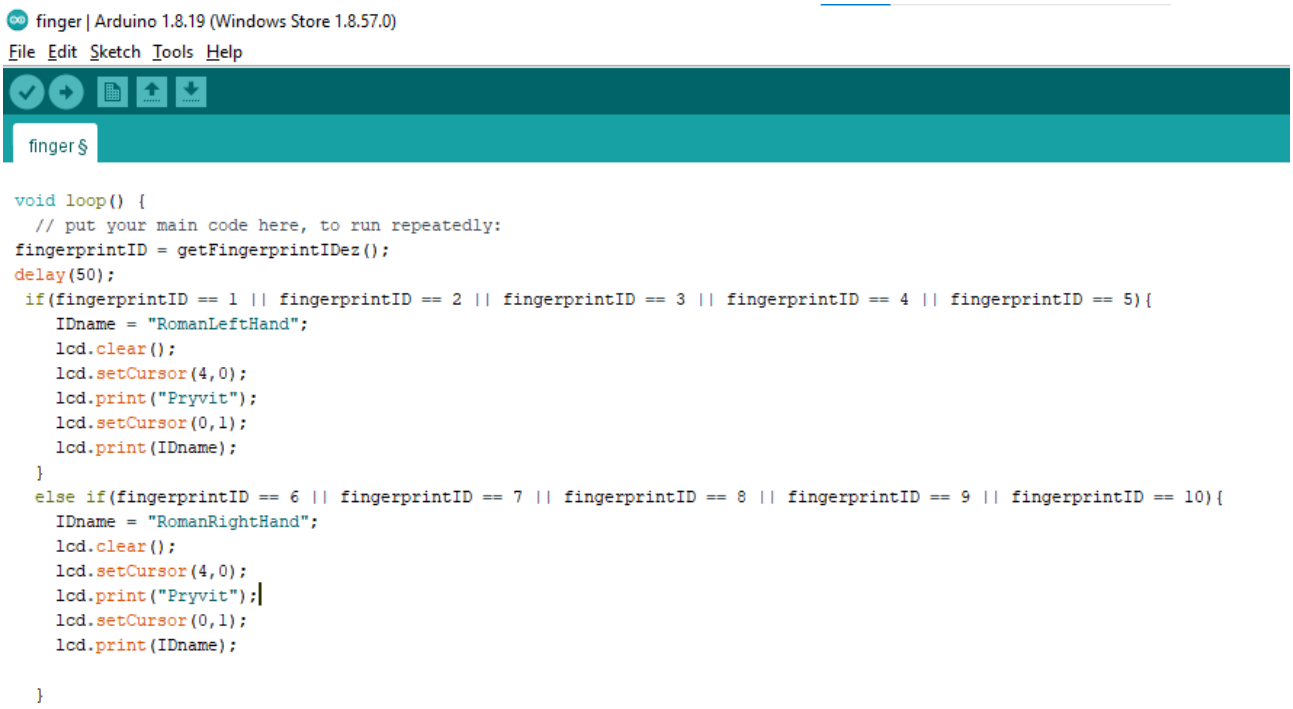


Рис. 7.17 – Функція пошуку відбитку

15. Завантажте код в Arduino.
16. Перевірте правильність роботи, скануйте в довільному порядку пальці і перевірте, чи вірно виводять повідомлення на дисплей («left hand» для пальців від 1 до 5 і «right hand» для пальців від 6 до 10).
17. Оформіть висновки по роботі.

```
#include <Keypad.h>
const byte ROWS = 4;
const byte COLS = 4;
char keys [ROWS][COLS] = {
  {'1','2','3','A'},
  {'4','5','6','B'},
  {'7','8','9','C'},
  {'*','0','#','D'},
};
byte rowPins [ROWS] = {12,9,8,7};
byte colPins [COLS] = {6,5,4,3};
Keypad keypad = Keypad (makeKeymap(keys),rowPins,colPins,ROWS,COLS);

#include <Servo.h>
Servo servo1;
int ledgreen = 18;
int ledred = 17;

#include <SPI.h>
#include <LiquidCrystal.h>
LiquidCrystal lcd (16,15,14,13,11,10);

void setup ()
{
 Serial.begin (9600);
  pinMode (ledgreen, OUTPUT);
  pinMode (ledred, OUTPUT);
  servo1.attach (2);
  lcd.begin (16,2);
}
void loop ()
{
 lcd.setCursor (0,0);
  lcd.print ("Welcome");
  char key = keypad.getKey ();
  if (key == 'C')
  {
    lcd.setCursor (0,0);
    lcd.print ("Enter password");
    lcd.setCursor (0,1);
    char pass[6];
    for (int i = 0; i < 6; i++)
    {
    label: char key = keypad.getKey ();
      if (key != NO_KEY)
      {
      pass [i] = key;
        lcd.print ("*");
        digitalWrite (ledgreen, HIGH);
        digitalWrite (ledgreen, LOW);
      }
    else goto label;
    }
    char rightpass [] = "112233";
    if (strcmp (pass, rightpass) == 49)
    {
    lcd.clear ();
      lcd.setCursor (0,0);
      lcd.print ("access is");
      lcd.setCursor (3,1);
      lcd.print ("allowed");
      servo1.write(0);
      digitalWrite (ledgreen, HIGH);
      delay (2500);
    }
    else
    {
      lcd.clear ();
      lcd.setCursor (0,0);
      lcd.print ("access denied");
      digitalWrite (ledred, HIGH);
      delay (500);
      digitalWrite (ledred, LOW);
      delay (500);
      digitalWrite (ledred, HIGH);
      delay (500);
      digitalWrite (ledred, LOW);
      delay (500);
      digitalWrite (ledred, HIGH);
      delay (500);
      digitalWrite (ledred, LOW);
      }
  delay (3000);
  servo1.write(90);
  digitalWrite (ledgreen, LOW);
   lcd.clear ();
    }
}
```

ЛІТЕРАТУРА

Основна

1. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики: Вибр. наук. праці. – К. : НІСД, 2016. – 528 с.
2. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. – Житомир: ЖНАЕУ, 2016. – 636 с.
3. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
4. Масалков А. Особенности киберпреступлений. Инструменты нападения и защита информации. – М.: ДМК Пресс, 2016. – 226 с.
5. Бабаш А.В. Актуальные вопросы защиты информации. – М.: РИОР, 2017. – 111 с.
6. Никифоров С.Н. Методы защиты информации. Защита от внешних вторжений. - СПб.: Лань, 2018. - 96 с.
7. Борисов М.А. Основы программно-аппаратной защиты информации. – М.: URSS, 2019. – 464 с.
8. Дузь-Крятченко О. П., Грицай П. М., Грищенко В. П., Клименко В. С. та ін. Основи стратегії національної безпеки та оборони держави: підруч. – К. : НУОУ ім. Івана Черняховського, 2015. – 620 с.
9. Пількевич І.А., Лобанчикова Н.М.,. Молодецька К.В. Захист інформації в автоматизованих системах управління: посібник. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
10. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. – 288 с.
11. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.

Додаткова

1. Бондарев В.В.. Введение в информационную безопасность автоматизированных систем. – М.: ГТУ им. Н.Э. Баумана, 2016. – 252 с.

2. Богуш В.М. Криптографічні застосування елементарної теорії чисел / В.М. Богуш, В.А. Мухачов. – К.: ДУІКТ, 2006. – 126 с.

3. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.

4. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / С.М. Головань, С.Б. Гордієнко, О.С. Петров, В.О. Хорошко, Л.М. Щербак; під ред. В.О. Хорошко. – Луганськ: Ноулідж, 2012. – 480 с.

Список Інтернет-ресурсів:

1. www.wired.com;
2. http://virusov-net.info;
3. www.bezpeka.com

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1 Закон України "Про інформацію" від 02.10.92 р.

2 Закон України "Про державну таємницю" від 21.12.94 р.

3 Закон України "Про науково-технічну інформацію".

4 Закон України “Про захист інформації в автоматизованих системах” від 05.07.1994.

5 Закон України “Про зв’язок”. Від 16.11.2003 р.

6 Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. № 1229.

7 Концепція технічного захисту інформації в Україні. – 1997.

8 Концепція технічного захисту інформації в галузі зв’язку України. – 1999.

9 ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

10 ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

11 ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

12 НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

13 НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.

14 НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу (Критерії базуються на аналізі Федеральних критеріїв США і критеріїв оцінки безпеки Канади).

15 НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

16 НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

17 НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

18 НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

ДЛЯ НОТАТОК