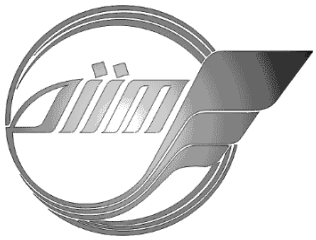
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ



УДУНТ ННІ ДІІТ

Кафедра «Комп'ютерні інформаційні технології»

Лабораторна робота №11

з дисципліни «Організація комп’ютерних мереж»

на тему: «Підключення до VPN сервера через локальну обчислювальну мережу (ЛОМ) (Windows 7)»

Виконав:
студент гр.ПЗ1911
Сафонов Д.Є.
Прийняв:
Івченко Ю.М.

Дніпро, 2022

Тема. Підключення до VPN сервера через локальну обчислювальну мережу (ЛОМ) (Windows 7).
Мета. Ознайомитися і отримати практичні навички підключення до VPN сервера через ЛОМ.

Порядок виконання роботи.

1. Ознайомитися з основними поняттями:
   - локальна обчислювальна мережа (Local Area Network, LAN);
   - набір протоколів для забезпечення захисту даних IP Security;
   - протокол тунелювання другого рівня (Layer 2 Tunneling Protocol);
   - протокол аутентифікації PAP (Password Authentication Protocol);
   - віртуальна приватна мережа (Virtual Private Network, VPN);
   - типи VPN-підключень;
   - властивості VPN-підключень.
2. Налагодити VPN підключення в Windows, для чого виконати:
   - створення нового мережевого підключення;
   - перевірку поточного стану мережевого підключення;
   - налагодження створеного VPN підключення;
   - запуск і перевірку VPN підключення.

Короткі теоретичні відомості

1. Локальна обчислювальна мережа (ЛОМ, Local Area Network, LAN) — комп'ютерна мережа, що охоплює відносно невелику територію або групу будівель (дім, офіс, фірму, університет).
2. IPsec (IP Security) — набір протоколів для забезпечення захисту даних, що передаються з використанням мережевого протоколу IP. Він дозволяє здійснювати підтвердження справжності (аутентифікацію), перевірку цілісності і/або шифрування IP-пакетів. IPsec також включає в себе протоколи для захищеного обміну ключами в мережі Інтернет. В основному, застосовується для організації VPN –з'єднання.
3. Протокол тунелювання другого рівня (Layer 2 Tunneling Protocol, L2TP) — в комп'ютерних мережах тунельний протокол, що використовується для підтримки віртуальних приватних мереж (VPN). Дозволяє створювати тунель не тільки в мережах IP, але і в таких, як ATM, X.25 і Frame Relay. Тунелювання в комп'ютерних мережах — процес, в ході якого створюється захищене логічне з'єднання між двома кінцевими точками за допомогою інкапсуляції різних протоколів, метод побудови мереж, при якому один мережевий протокол інкапсулюється в інший. Від звичайних багаторівневих мережевих моделей відрізняється тим, що протокол, який інкапсулюється, відноситься до того ж або нижчого рівня, ніж той, що використовується в якості тунелю. Суть тунелювання полягає в тому, щоб «упакувати» передану порцію даних разом з службовими полями, в новий «конверт» для забезпечення конфіденційності і цілісності всієї переданої порції, включаючи службові поля. Тунелювання може застосовуватися на мережевому і на прикладному рівнях. Комбінація тунелювання і шифрування дозволяє реалізувати закриті віртуальні приватні мережі (VPN). Тунелювання застосовується для узгодження транспортних протоколів або для створення захищеного з'єднання між вузлами мережі.
4. Протокол аутентифікації PAP (Password Authentication Protocol) — протокол простої перевірки справжності, що передбачає відправку імені користувача і пароля на сервер віддаленого доступу відкритим текстом (без шифрування).

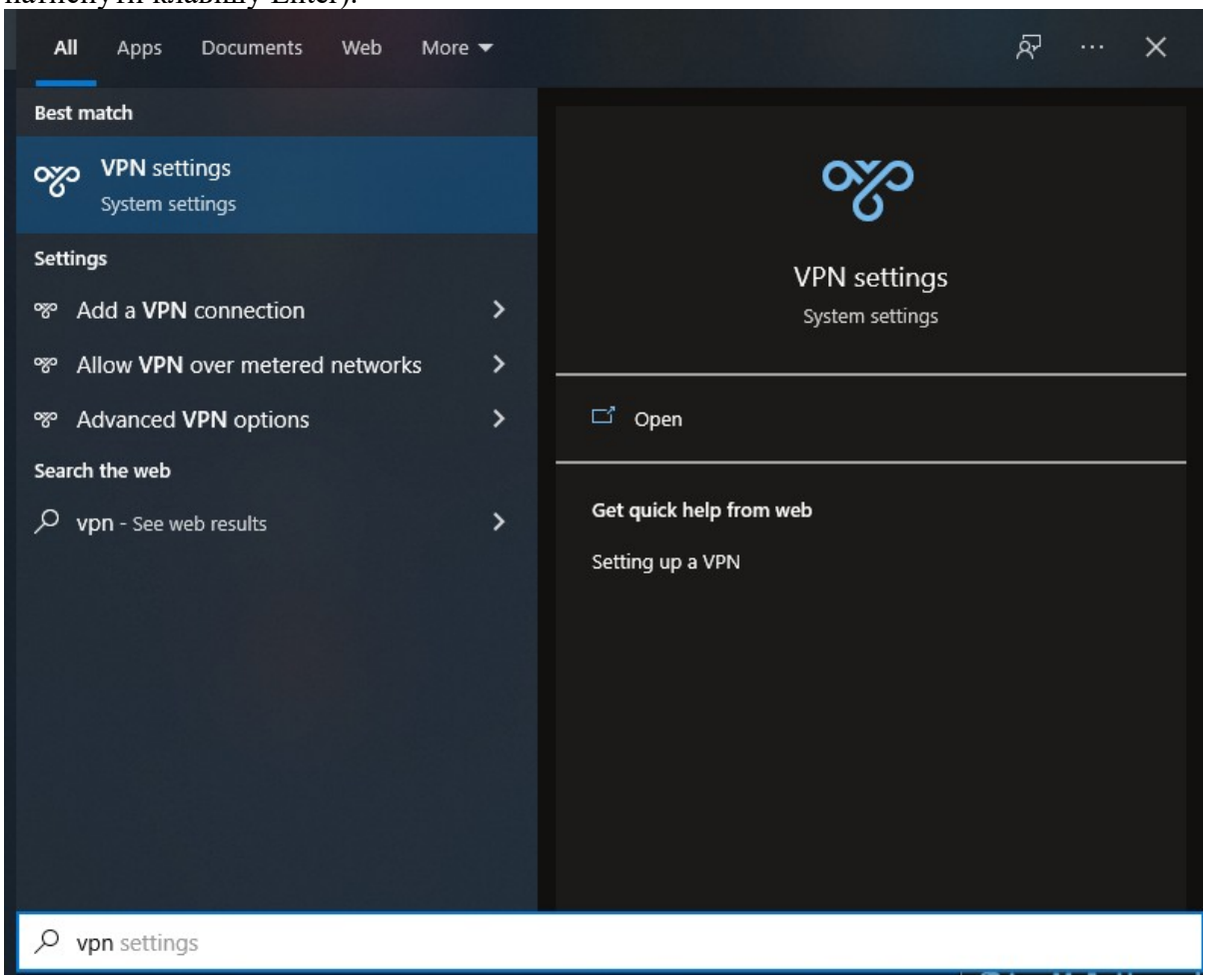
5. Віртуальна приватна мережа є підключення типу «точка-точка» в приватній або публічній мережі. При звичайній реалізації VPN клієнт ініціює через Інтернет віртуальне підключення типу «точка-точка» до сервера віддаленого доступу. Сервер віддаленого доступу відповідає на виклик, виконує перевірку справжності клієнта і передає дані між клієнтом і приватною мережею.
   Для емуляції каналу типу «точка-точка» до даних додається заголовок (виконується інкапсуляція), який містить відомості маршрутизації, які забезпечують проходження даних через загальну або публічну мережі до кінцевого пункту. Для емуляції приватного каналу і збереження конфіденційності передані дані шифруються. Пакети, що перехоплені в загальній або публічній мережі, неможливо розшифрувати без ключів шифрування.
6. IKE (Internet Key Exchange) — стандартний протокол IPsec, використовується для забезпечення безпеки взаємодії в VPN. Призначення IKE — захищене узгодження і доставка ідентифікованого матеріалу для асоціації безпеки.
7. Існує два типи VPN-підключень:
   - VPN-підключення віддаленого доступу надає користувачам можливість працювати вдома або в дорозі, отримуючи доступ до сервера приватної мережі за допомогою інфраструктури публічної мережі, наприклад, Інтернету. З точки зору користувача, VPN-підключення є підключення типу «точка-точка» між комп'ютером і сервером організації. Реальна інфраструктура мережі не має значення, тому що дані передається подібно до того, як би вони передавалися через виділений приватний канал.
   - VPN-підключення типу «мережа-мережа» («маршрутизатор-маршрутизатор») дозволяють організаціям встановлювати маршрутизовані підключення між окремими офісами (або організаціями) через публічну мережу, при цьому забезпечуючи безпеку зв'язку. Маршрутизоване VPN-підключення через Інтернет логічно подібне орендованому каналу глобальної мережі (WAN). У випадку, коли мережі з'єднані через Інтернет маршрутизатор переадресовує пакети іншому маршрутизатору через VPN-підключення. З точки зору маршрутизаторів VPN-підключення працює як канал рівня передачі даних. VPN-підключення типу «мережа-мережа» зв'язує два сегменти приватної мережі. Клієнт проходить перевірку справжності на сервері і, з метою взаємної перевірки справжності, сервер проходить перевірку справжності на клієнті.

8. VPN-підключення, що використовують протоколи PPTP, L2TP/IPsec і SSTP, мають наступні властивості:
   - інкапсуляція — VPN-технологія забезпечує інкапсуляцію приватних даних з заголовком, що містить відомості маршрутизації для передачі цих даних через транзитну мережу.
   - перевірка справжності - Існують три різних форми перевірки справжності для VPN-підключень.
     1. Перевірка справжності на рівні користувача за протоколом PPP.
        Для встановлення VPN-підключення сервер виконує перевірку справжності клієнта, який намагається встановити підключення, на рівні користувача за протоколом PPP і перевіряє, чи має клієнт необхідну авторизацію. При взаємній перевірці справжності клієнт також виконує перевірку справжності сервера, що гарантує захист від комп'ютерів, що видають себе за сервери.
     2. Перевірка справжності на рівні комп'ютера за протоколом IKE.
        Для встановлення зіставлення безпеки IPsec клієнт і сервер використовують протокол IKE для обміну сертифікатами комп'ютерів або попереднім ключем. В обох випадках клієнт і сервер виконують взаємну перевірку справжності на рівні комп'ютера. Наполегливо рекомендується обирати перевірку справжності згідно з сертифікатом комп'ютера через більшу безпеку цього методу. Перевірка справжності на рівні комп'ютера виконується тільки для підключень L2TP/IPsec.
     3. Перевірка справжності джерела даних і забезпечення цілісності даних.
        Щоб впевнитися в тому, що джерелом відправлених через VPN даних є інша сторона підключення і що вони передані в незмінному виді, дані містять контрольну суму шифрування, що ґрунтується на ключі шифрування, який відомий тільки відправнику і отримувачу. Перевірка справжності джерела даних і забезпечення цілісності даних доступні тільки для підключень L2TP/IPsec.
   - Шифрування даних
     Для забезпечення конфіденційності даних при передачі через загальні або публічні транзитні мережі вони шифруються відправником і розшифровуються отримувачем. Успішність процесів шифрування і розшифрування гарантується в тому випадку, коли відправник і отримувач використовується загальний ключ шифрування. Зміст перехоплених пакетів, відправлених через VPN-підключення в транзитній мережі, зрозумілий тільки власникам загального ключа. Довжина ключа шифрування — це важливий параметр безпеки. Тому для гарантії конфіденційності даних рекомендується використовувати найдовший можливий ключ.

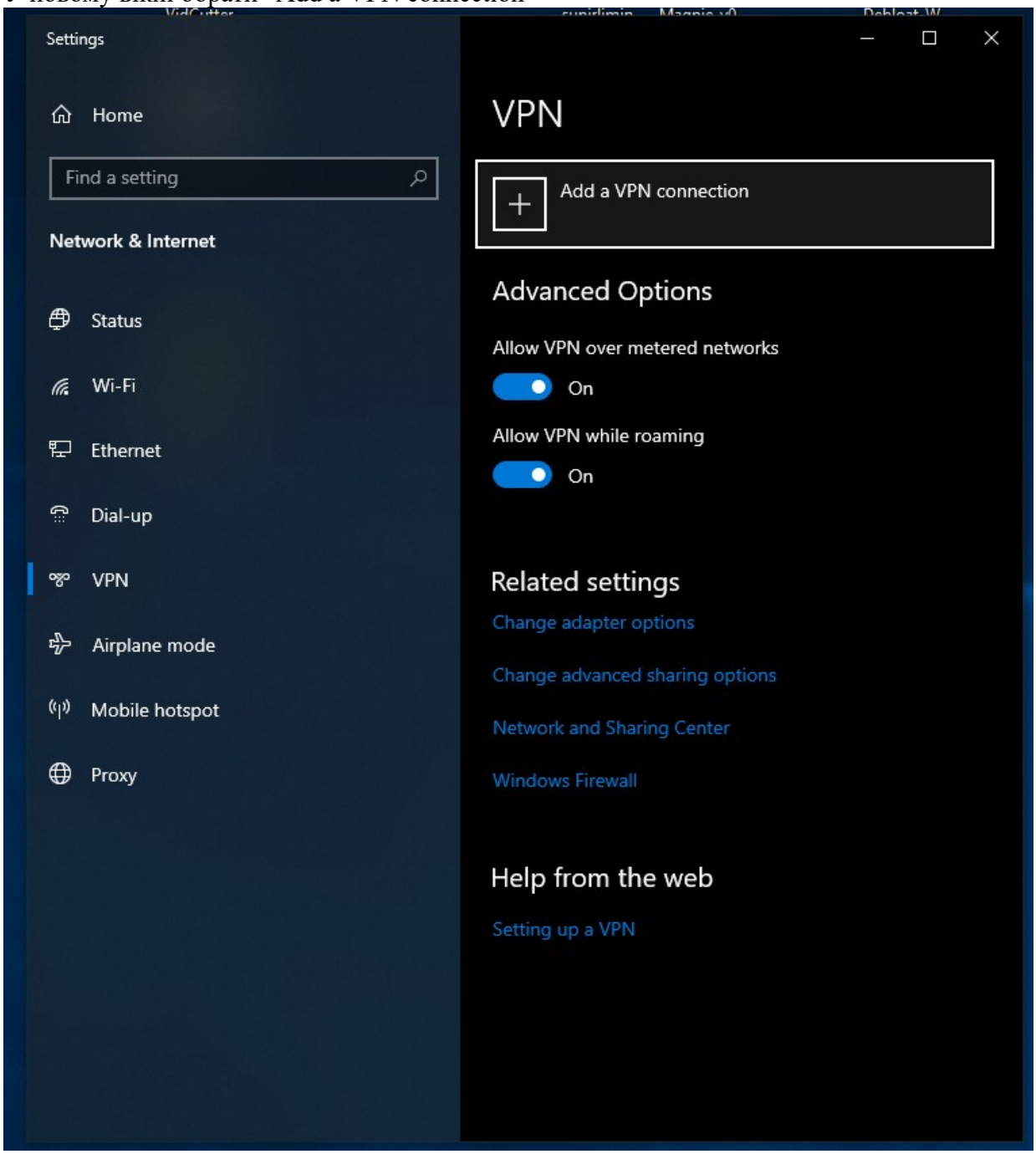
Короткий опис послідовності виконання роботи з скриншотами і аналізом отриманих результатів

Робота була виконана в Windows 10, тому продемонстровано трохи коротший путь, але в цій операційній системі присутні усі ті самі сервіси що й в Windows 7, тому можна використовувати алгоритм вказаний в методичці.

1. Натискаемо клавішу win (щоб відкрити меню пуск).
   Набираемо "vpn".
   З представлених варіантів обираємо "VPN settings" (у моему випадку достатньо натиснути клавішу Enter).

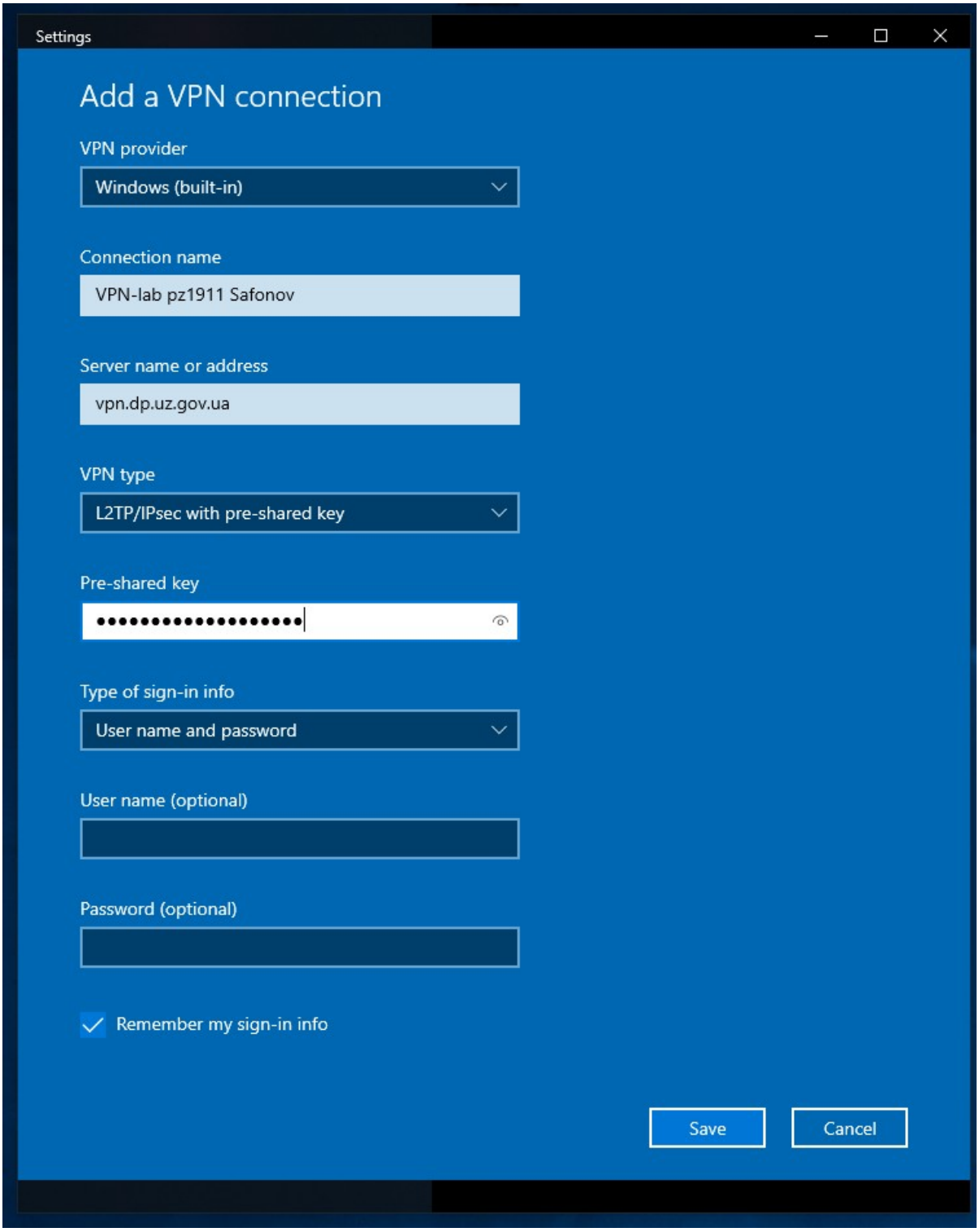


2. У новому вікні обрати "Add a VPN connection"

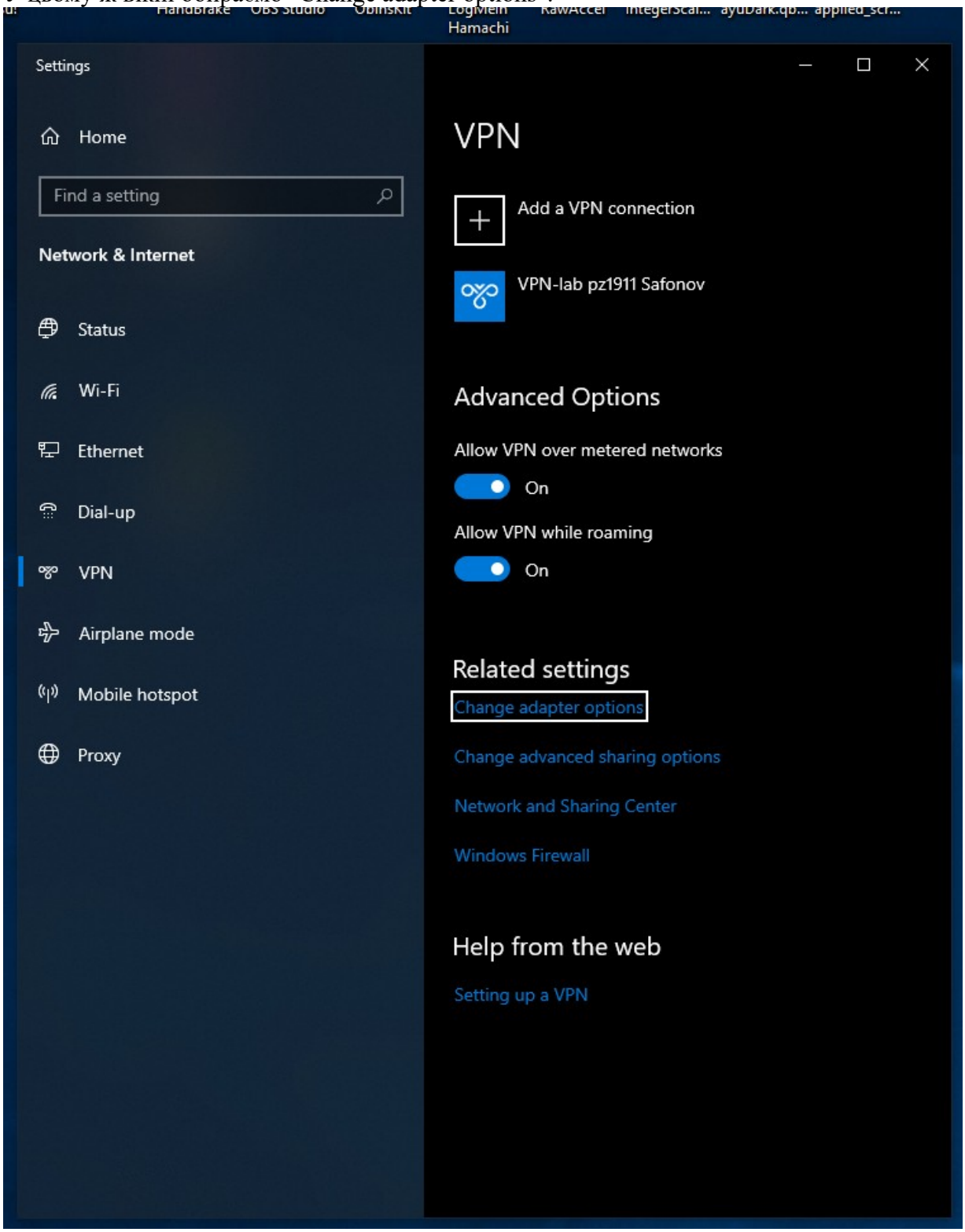


3. Заповняємо поля:
   - Ім'я підключення
   - Адреса сервера

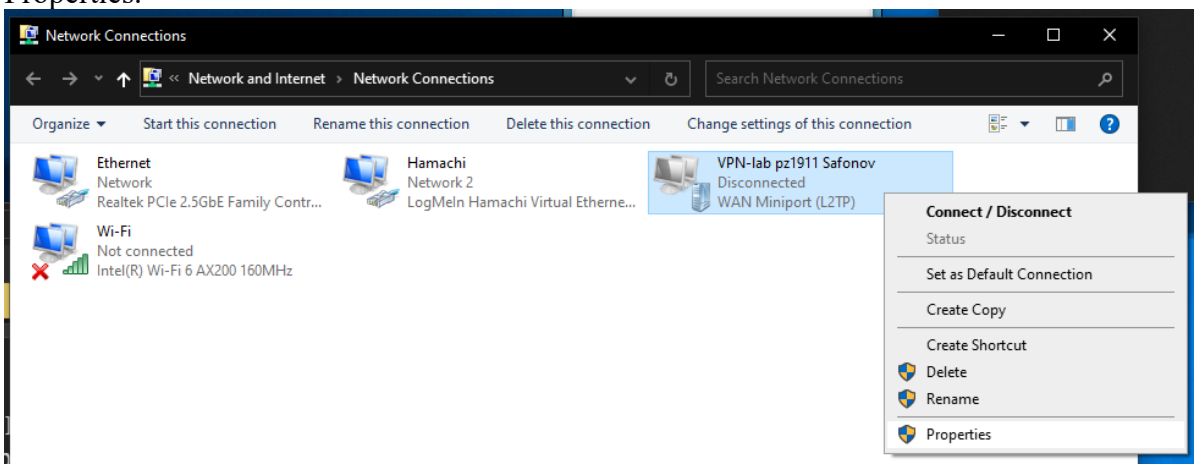
   Змінюємо тип VPN та вказуэмо ключ
   Натискаэмо Save



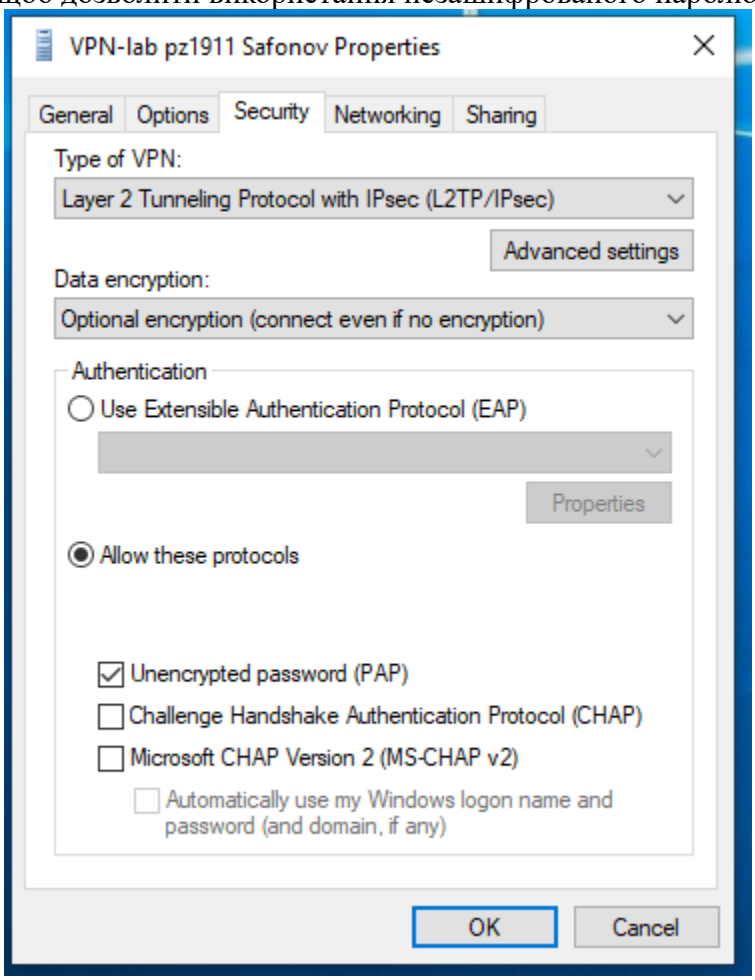
4. У цьому ж вікні обираємо "Change adapter options".



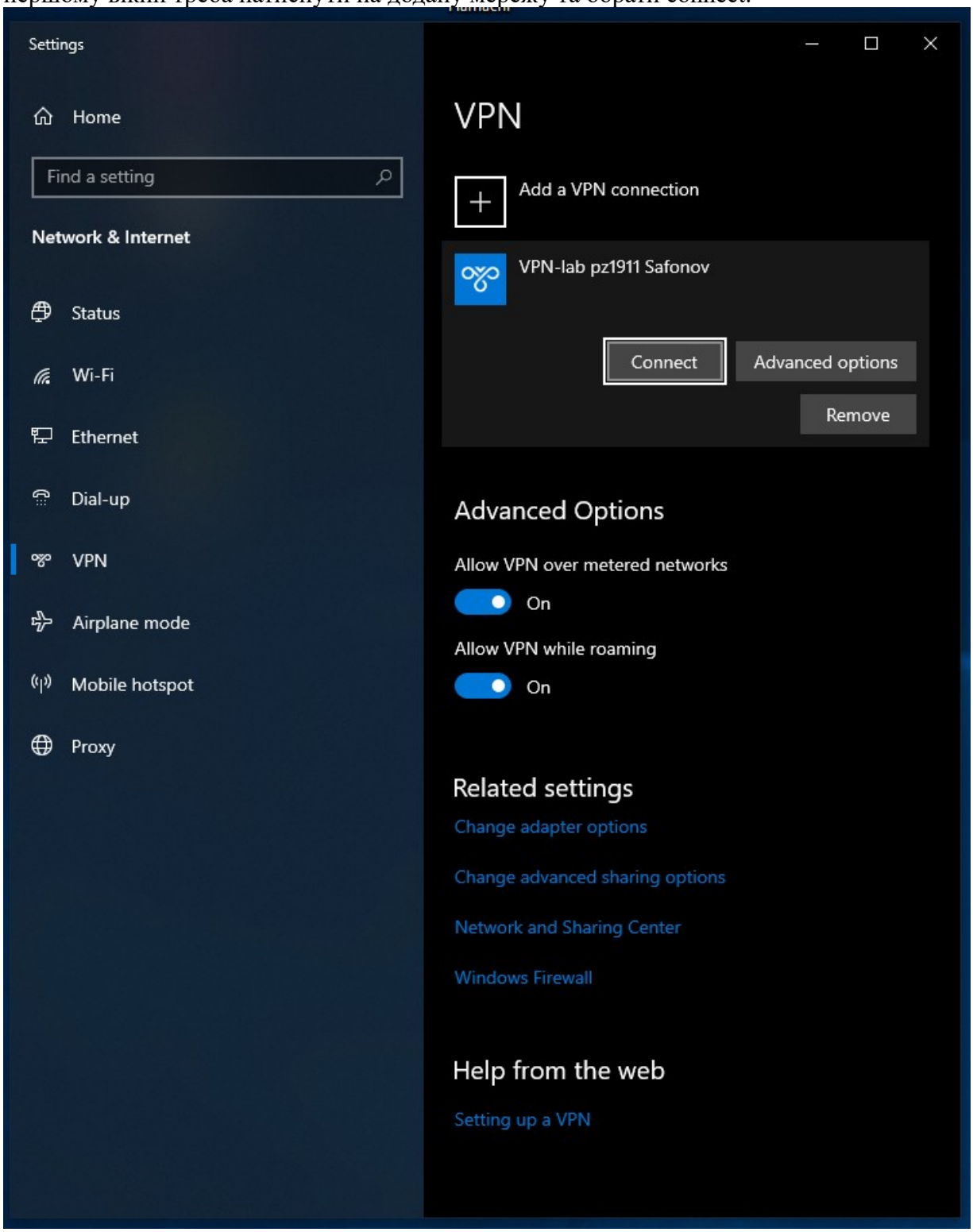
5. У новому вікні натискаємо правою кнопкою миші на створене підключення та обираємо Properties.



6. У новому вікні у вкладці Security ставимо галку на "Allow these protocols" та "Unencrypted password (PAP)", щоб дозволити використання незашифрованого паролю. Натиснути OK.



7. Після виконаних налаштувань, можно підключитися до віртуальної мережі, для цього у першому вікни треба натиснути на додану мережу та обрати connect.



8. Перевірка ipconfig /all не здійснюється тому що підключитися до вказаного VPN без ключа неможливо, тому результат не зміниться.

Висновки

В ході лабораторної роботи був розглянутий алгоритм підключення до VPN в операційній системі Windows, та було виконане підключення. Були розглянуті основні поняття при роботі з віртуальними приватними мережами, а саме:

- локальна обчислювальна мережа (Local Area Network, LAN);
- набір протоколів для забезпечення захисту даних IP Security;
- протокол тунелювання другого рівня (Layer 2 Tunneling Protocol);
- протокол аутентифікації PAP (Password Authentication Protocol);
- віртуальна приватна мережа (Virtual Private Network, VPN);
- типи VPN-підключень;
- властивості VPN-підключень.

Контрольні питання

1. **Що таке Інтернет, ідентифікатор місця розташування URL, Browser?**
   - Інтернет — всесвітнє об'єднання мереж, шлюзів, серверів і комп'ютерів, що використовує для зв'язку єдиний набір протоколів.
   - Ідентифікатор місця розташування (URL – Uniform Resource Locator) — задає сервер, до якого треба звернутися, а також метод доступу і місцезнаходження ресурсу на сервері. URL складається з декількох частин. Найпростіший набір містить: використаний протокол, двокрапка, адреса ресурсу. Адреса починається з подвійного прямого слеша (нахил вправо).

протокол	двокрапка	адреса ресурсу
https	:	//www.google.com

   - Browser — спеціальна програма з графічним інтерфейсом для перегляду World Wide Web.
2. **Послуги Інтернет: WWW, FTP, електронна пошта, Telnet.**
   - WWW (World Wide Web — всесвітня павутина) — мультимедійна служба Інтернету, містить величезну кількість гіпертекстових документів, створених на HTML (Hypertext Markup Language — мова розмітки гіпертекстових документів).
   - FTP (File Transfer Protocol) — протокол, що дозволяє легко пересилати файли і документи, реалізований на прикладному рівні моделі OSI.
   - електронна пошта - щоб послати повідомлення, Ви повинні вказати електронну адресу (e-mail address) одержувача. Ці адреси включають ідентифікатор користувача, за ним випливає знак @, потім адреса комп'ютера-одержувача.

ідентифікатор користувача	@	адреса комп'ютера-одержувача
2020kitipz	@	gmail.com

   - Telnet — один з перших протоколів Інтернету. Його можна використовувати як віддалений термінал хоста Інтернету. Під час зв'язку з хост-компьютером Інтернету Ваш комп'ютер працює так, начебто Ваші клавіатура і дисплей підключені безпосередньо до віддаленого комп'ютера. Ви можете запускати програми на комп'ютері, що знаходиться на протилежній стороні земної кулі, з тією ж легкістю, немов Ви сидите за ним.
3. **Протоколи IPsec, IKE. Протокол L2TP (тунелювання).**
   - IPsec (IP Security) — набір протоколів для забезпечення захисту даних, що передаються з використанням мережевого протоколу IP. Він дозволяє здійснювати підтвердження справжності (аутентифікацію), перевірку цілісності і/або шифрування IP-пакетів. IPsec також включає в себе протоколи для захищеного обміну ключами в мережі Інтернет. В основному, застосовується для організації VPN –з'єднання.
   - IKE (Internet Key Exchange) — стандартний протокол IPsec, використовується для забезпечення безпеки взаємодії в VPN. Призначення IKE — захищене узгодження і доставка ідентифікованого матеріалу для асоціації безпеки.
   - Протокол тунелювання другого рівня (Layer 2 Tunneling Protocol, L2TP) — в комп'ютерних мережах тунельний протокол, що використовується для підтримки віртуальних приватних мереж (VPN). Дозволяє створювати тунель не тільки в мережах IP, але і в таких, як ATM, X.25 і Frame Relay.

4. **Типи VPN-підключень.**

Існує два типи VPN-підключень:

- VPN-підключення віддаленого доступу надає користувачам можливість працювати вдома або в дорозі, отримуючи доступ до сервера приватної мережі за допомогою інфраструктури публічної мережі, наприклад, Інтернету. З точки зору користувача, VPN-підключення є підключення типу «точка-точка» між комп'ютером і сервером організації. Реальна інфраструктура мережі не має значення, тому що дані передається подібно до того, як би вони передавалися через виділений приватний канал.
- VPN-підключення типу «мережа-мережа» («маршрутизатор-маршрутизатор»). Маршрутизоване VPN-підключення через Інтернет логічно подібне орендованому каналу глобальної мережі (WAN). У випадку, коли мережі з'єднані через Інтернет маршрутизатор переадресовує пакети іншому маршрутизатору через VPN-підключення. З точки зору маршрутизаторів VPN-підключення працює як канал рівня передачі даних. VPN-підключення типу «мережа-мережа» зв'язує два сегменти приватної мережі. Клієнт проходить перевірку справжності на сервері і, з метою взаємної перевірки справжності, сервер проходить перевірку справжності на клієнті.

5. **Властивості VPN-підключень і використані протоколи.**
   VPN-підключення, що використовують протоколи PPTP, L2TP/IPsec і SSTP, мають наступні властивості:
   - інкапсуляція — VPN-технологія забезпечує інкапсуляцію приватних даних з заголовком, що містить відомості маршрутизації для передачі цих даних через транзитну мережу.
   - перевірка справжності - Існують три різних форми перевірки справжності для VPN-підключень.
     1. Перевірка справжності на рівні користувача за протоколом PPP.
        Для встановлення VPN-підключення сервер виконує перевірку справжності клієнта, який намагається встановити підключення, на рівні користувача за протоколом PPP і перевіряє, чи має клієнт необхідну авторизацію. При взаємній перевірці справжності клієнт також виконує перевірку справжності сервера, що гарантує захист від комп'ютерів, що видають себе за сервери.
     2. Перевірка справжності на рівні комп'ютера за протоколом IKE.
        Для встановлення зіставлення безпеки IPsec клієнт і сервер використовують протокол IKE для обміну сертифікатами комп'ютерів або попереднім ключем. В обох випадках клієнт і сервер виконують взаємну перевірку справжності на рівні комп'ютера. Наполегливо рекомендується обирати перевірку справжності згідно з сертифікатом комп'ютера через більшу безпеку цього методу. Перевірка справжності на рівні комп'ютера виконується тільки для підключень L2TP/IPsec.
     3. Перевірка справжності джерела даних і забезпечення цілісності даних.
        Щоб впевнитися в тому, що джерелом відправлених через VPN даних є інша сторона підключення і що вони передані в незмінному виді, дані містять контрольну суму шифрування, що ґрунтується на ключі шифрування, який відомий тільки відправнику і отримувачу. Перевірка справжності джерела даних і забезпечення цілісності даних доступні тільки для підключень L2TP/IPsec.
   - Шифрування даних
     Для забезпечення конфіденційності даних при передачі через загальні або публічні транзитні мережі вони шифруються відправником і розшифровуються отримувачем. Успішність процесів шифрування і розшифрування гарантується в тому випадку, коли відправник і отримувач використовується загальний ключ шифрування. Зміст перехоплених пакетів, відправлених через VPN-підключення в транзитній мережі, зрозумілий тільки власникам загального ключа. Довжина ключа шифрування — це важливий параметр безпеки. Тому для гарантії конфіденційності даних рекомендується використовувати найдовший можливий ключ.