Навчально-методична література

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ
УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
КАФЕДРА КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ

МЕТОДИЧНІ ВКАЗІВКИ

для виконання лабораторних робіт
з дисципліни

КОМП'ЮТЕРНІ МЕРЕЖІ

(Модуль 2)

для студентів спеціальності
123 «Комп'ютерна інженерія»

Тернопіль
2023

Методичні вказівки для виконання лабораторних робіт з курсу «Комп’ютерні мережі». Модуль 2. Для студентів спеціальності 123 «Комп’ютерна інженерія» /укл. А. Г. Микитишин, О. С. Голотенко. // ТНТУ. – 2023. – 49 с.

Укладачі: Андрій МИКИТИШИН, канд. техн. наук, доц.
Олександр ГОЛОТЕНКО, канд. техн. наук, доц.

Рецензент: Сергій МАРЦЕНКО, канд. техн. наук, доц.

Відповідальний за випуск: Олександр ГОЛОТЕНКО, канд. техн. наук., доц.

Схвалено та рекомендовано до друку:

Протокол кафедри КТ №1 від 22.08.2023 р.

Протокол НМК факультету прикладних інформаційних технологій та електроінженерії №1 від 30.08.2023 р.

Методичні вказівки призначені для проведення лабораторних робіт з дисципліни «Комп'ютерні мережі» для студентів, які навчаються за спеціальністю 123 «Комп’ютерна інженерія». Викладені матеріали приведені з урахуванням модульної системи навчання, рекомендацій до самостійної роботи і індивідуальних завдань, тем лабораторних занять, тестів, екзаменаційних питань, типової форми та вимог для комплексної перевірки знань з дисципліни.

ЗМІСТ

Лабораторна робота №8.1
Розподіл мережі IPv4 на підмережі

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
CustomerRouter	G0/0			N/A
	G0/1			
	S0/1/0	209.165.201.2	255.255.255.252	
LAN-A Switch	VLAN1			
LAN-B Switch	VLAN1			
PC-A	NIC			
PC-B	NIC			
ISPRouter	G0/0	209.165.200.225	255.255.255.224	N/A
	S0/1/0	209.165.201.1	255.255.255.252	
ISPSwitch	VLAN1	209.165.200.226	255.255.255.224	209.165.200.225
ISP Workstation	NIC	209.165.200.235	255.255.255.224	209.165.200.225
ISP Server	NIC	209.165.200.240	255.255.255.224	209.165.200.225

Цілі та задачі
Частина 1: Розроблення схеми розподілу мережі на підмережі
Частина 2: Налаштування пристроїв
Частина 3: Перевірка та усунення неполадок у мережі

Довідкова інформація / Сценарій

У цьому завданні, ви повинні розподілити мережу Customer на декілька підмереж. При створенні схеми підмережі необхідно врахувати кількість вузлів комп'ютерів у кожній підмережі та інші аспекти, наприклад, майбутнє розширення вузлів у мережі.

Після створення схеми підмережі та заповнення таблиці відсутніми IP-адресами вузлів й інтерфейсів, налаштуйте вузли ПК, комутатори та інтерфейси маршрутизатора.

Після налаштувань мережних пристроїв і вузлів ПК, використайте команду **ping** для перевірки мережних з’єднань.

Інструкції

Частина 1: Розроблення схеми розподілу мережі на підмережі
Крок 1: Створити схему розподілу підмереж, яка відповідає необхідній кількості підмереж і адрес вузлів.

У цьому сценарії ви є мережним фахівцем, який здійснює налаштування нової мережі. Вам потрібно створити декілька підмереж з адресного простору мережі 192.168.0.0/24, для забезпечення таких вимог:

a. Перша підмережа LAN-A потребує не менше 50 IP-адрес вузлів.
b. Друга підмережа LAN-B потребує не менше 40 IP-адрес вузлів.
c. Вам також потрібно не менше двох додаткових підмереж для розширення мережі в майбутньому.

Примітка: Маска підмережі змінної довжини, не використовуватиметься. Всі маски підмережі для пристроїв повинні бути однакової довжини.

d. Відповіді на наступні запитання допоможуть створити схему підмережі, яка забезпечить поставлені вимоги до мережі:

Скільки необхідно адрес вузлів у найбільшій підмережі?

Яка мінімальна необхідна кількість підмереж?

Мережа, яку необхідно розподілити на підмережі, має адресу - 192.168.0.0/24. Якою буде маска підмережі /24 в двійковому форматі?

e. Маска підмережі складається з двох частин: мережної та вузлової. У двійковому форматі вони подаються у масці підмережі одиницями і нулями.

Що визначають одиниці в масці мережі?

Що визначають нулі в масці мережі?

f. Для розподілу мережі, біти з вузлової частини заданої маски мережі замінюються бітами підмережі.
Кількість бітів у підмережі визначатимуть кількість підмереж.

Яка кількість підмереж і вузлів створюється в кожному прикладі з огляду на всі можливі маски підмережі, які подано в двійковому форматі?

Порада: Пам'ятайте, що кількість вузлових бітів (піднесених до другого ступеня) визначатиме кількість вузлів у підмережі (відняти 2), а кількість бітів підмережі (піднесених до другого ступеня) визначатиме кількість підмереж. Біти підмережі (виділені жирним шрифтом) - це біти, які були запозичені поза межами заданої маски мережі /24. /24 - це запис префікса, що відповідає масці в десятковому форматі розділеному крапками 255.255.255.0.

1) (/25) 11111111.11111111.11111111.**1**0000000

Маска підмережі в десятковому форматі розділеному крапками, еквівалентна:

Яка кількість підмереж? Яка кількість вузлів?

2) (/26) 11111111.11111111.11111111.**11**000000

Маска підмережі в десятковому форматі розділеному крапками, еквівалентна:

Яка кількість підмереж? Яка кількість вузлів?

3) (/26) 11111111.11111111.11111111.**111**00000

Маска підмережі в десятковому форматі розділеному крапками, еквівалентна:

Яка кількість підмереж? Яка кількість вузлів?

4) (/28) 11111111.11111111.11111111.**1111**0000

Маска підмережі в десятковому форматі розділеному крапками, еквівалентна:

Яка кількість підмереж? Яка кількість вузлів?

5) (/29) 11111111.11111111.11111111.**11111**000

Маска підмережі в десятковому форматі розділеному крапками, еквівалентна:

Яка кількість підмереж? Яка кількість вузлів?

6) (/30) 11111111.11111111.11111111.**11111**00

Маска підмережі в десятковому форматі розділеному крапками, еквівалентна:

Яка кількість підмереж? Яка кількість вузлів?

Враховуючи ваші відповіді вище, які маски підмережі відповідають мінімальній необхідній кількості адрес вузлів?

Враховуючи ваші відповіді вище, які маски підмережі відповідають мінімальній необхідній кількості підмереж?

Враховуючи ваші відповіді вище, які маски підмережі відповідають як мінімальній необхідній кількості вузлів, так і мінімальній необхідній кількості підмереж?

Після визначення вами маски підмережі, яка відповідає усім висунутим до мережі вимогам, визначте кожну з підмереж. Впорядкуйте підмережі від першої до останньої в таблиці. Пам'ятайте, що першою є підмережа 192.168.0.0 з новою визначеною маскою підмережі.

Адреса підмережі	Префікс	Маска підмережі

Крок 2: Внести відсутні IP-адреси до таблиці адресації

Призначте IP-адреси, виходячи з наступних критеріїв: наприклад, використовуйте мережні параметри ISP.

a. Призначити першу підмережу LAN-A.

1) Використати першу адресу вузла для маршрутизатора CustomerRouter, під’єднаного до комутатора LAN-A.
2) Використати другу адресу вузла для комутатора LAN-A. Переконайтеся, що для комутатора призначено адресу шлюзу за замовчуванням.
3) Використати останню адресу вузла для PC-A. Переконайтеся, що для PC призначено адресу шлюзу за замовчуванням.

b. Призначити другу підмережу LAN-B.

1) Використати першу адресу вузла для маршрутизатора CustomerRouter, під'єднаного до комутатора LAN-B.
2) Використати другу адресу вузла для комутатора LAN-B. Переконайтеся, що для комутатора призначено адресу шлюзу за замовчуванням.
3) Використати останню адресу вузла для PC-B. Переконайтеся, що для PC призначено адресу шлюзу за замовчуванням.

Частина 2: Налаштування пристроїв

Встановіть базові налаштування на PC, комутаторах та маршрутизаторах. Зверніться до адресної таблиці для визначення імен пристроїв та іншої адресної інформації.

Крок 1: Налаштувати маршрутизатор CustomerRouter.

a. Встановити **Class123** як секретний пароль входу на CustomerRouter.
b. Встановити **Cisco123** як пароль для входу на консоль.
c. Налаштувати **CustomerRouter** як ім'я вузла для маршрутизатора.
d. Налаштувати інтерфейси G0/0 і G0/1 з IP-адресами та масками підмережі й увімкнути інтерфейси.
e. Зберегти поточну конфігурацію у файлі конфігурації запуску.

Крок 2: Налаштувати два комутатори локальної мережі LAN.

Налаштуйте IP-адреси на інтерфейсі VLAN 1 на двох комутаторах LAN. На кожному комутаторі налаштуйте шлюз за замовчуванням.

Крок 3: Налаштувати інтерфейси PC.

Налаштуйте IP-адресу, маску підмережі та параметри шлюзу за замовчуванням на **PC-A** та **PC-B**.

Частина 3: Перевірка та усунення неполадок у мережі

У Частині 3, ви будете використовувати команду **ping** для перевірки мережних з'єднань.

a. Перевірте, чи може PC-A встановити зв'язок із своїм шлюзом за замовчуванням. Який результат отримано?
b. Перевірте, чи може PC-B встановити зв'язок із своїм шлюзом за замовчуванням. Який результат отримано?

c. Перевірте, чи може PC-A взаємодіяти із PC-B. Який результат отримано?

Якщо ви відповіли негативно на будь-яке із заданих вище запитань, то поверніться на початок і перевірте введені IP-адреси та маски підмережі, а також переконайтеся в тому, що шлюзи за замовчуванням налаштовані правильно на PC-A і PC-B.

Лабораторна робота №8.2

Реалізація схеми адресації підмережі IPv6

Таблиця адресації

Пристрій	Інтерфейс	Адреса IPv6	Локальна адреса каналу (LLA)
R1	G0/0	2001:db8:acad:00c8::1/64	fe80::1
	G0/1		fe80::1
	S0/0/0		fe80::1
R2	G0/0		fe80::2
	G0/1		fe80::2
	S0/0/0		fe80::2
PC1	NIC	Auto Config	
PC2	NIC	Auto Config	
PC3	NIC	Auto Config	
PC4	NIC	Auto Config	

Цілі та задачі

Крок 1: Визначити підмережі IPv6 та схему адресації.

Крок 2: Налаштувати адресацію IPv6 на маршрутизаторах та ПК.

Крок 3: Перевірити IPv6-з'єднання.

Довідкова інформація / Сценарій

Адміністратори мережі повинні знати, як реалізувати IPv6 у своїх мережах. Вас попросили створити мережу для використання торговим персоналом для демонстрації клієнтам. Мережа буде використовувати ряд послідовних підмереж IPv6 для чотирьох локальних мереж. Вашим завданням є призначення підмереж локальним мережам і налаштування на маршрутизаторах та комп'ютерах параметрів адресації IPv6. Обов'язково налаштуйте всі необхідні компоненти для маршрутизації IPv6 на маршрутизаторах.

Інструкції

Крок 1: Визначити підмережі IPv6 та схему адресації.

Як вихідну задано підмережу IPv6 **2001:db8:acad:00c8::/64**. Для кожної необхідної мережі вам знадобиться ще чотири підмережі. Збільшуйте адреси підмережі послідовно на одиницю, щоб досягти чотирьох необхідних підмереж. Заповніть наступну таблицю.

Таблиця підмереж

Підмережа	Адреса
R1 G0/0/ LAN	2001:db8:acad:00c8::0/64
R1 G0/1 LAN	
R2 G0/0 LAN	
R2 G0/1 LAN	
R1 to R2 link network	

Крок 2: Налаштувати адресацію IPv6 на маршрутизаторах та ПК.

Заповнити наведену вище таблицю адресації, щоб використовувати її як довідник для налаштування пристроїв.

- Призначити першу IP-адресу в підмережі інтерфейсам маршрутизатора локальної мережі (LAN).
- Призначити локальну адресу каналу зазначену в таблиці адресації.
- Для з'єднання між маршрутизаторами призначити першу адресу в підмережі R1.
- Для з'єднання між маршрутизаторами призначити другу адресу в підмережі R2.
- Встановити на всіх чотирьох вузлах автоматичне налаштування IPv6-адрес.

Крок 3: Перевірити IP-з’єднання.

Якщо адресацію було налаштовано правильно, ПК повинні мати можливість обмінюватися ехо-запитами по відношенню один до одного.

Лабораторна робота №9.1

Використання команди ipconfig

Цілі та задачі

Пошук неправильного налаштування комп'ютера за допомогою команди **ipconfig**.

Вихідні дані

Один з чотирьох комп'ютерів в офісі невеликої компанії не підключається до мережі Інтернет. На всіх комп'ютерах налаштована статична IP-адресація. Знайдіть неправильно налаштований пристрій за допомогою команди **ipconfig /all**.

Крок 1: Перевірка конфігурацій

1. Відкрийте командний рядок **Desktop (Робочий стіл)** > **Command Prompt (Командний рядок)** кожного комп'ютера і введіть команду: **ipconfig /all**.
2. Перевірте IP-адреси, маски підмережі та шлюзи по замовчуванню кожного комп'ютера. Запишіть ці налаштування IP для кожного комп'ютера, щоб виявити неправильно налаштований ПК.

Крок 2: Виправлення помилкових налаштувань

1. Виберіть неправильно налаштований комп'ютер і відкрийте вкладку **Config**.
2. Клацніть вкладку **Desktop > IP Configuration** та усуньте помилки.
3. Натисніть кнопку **Check Results** у нижній частині вікна для перевірки роботи.

Лабораторна робота №9.2

Використання команди ping

Цілі та задачі

Пошук неправильного налаштування комп'ютера за допомогою команди **ping**.

Вихідні дані:

Власник невеликої компанії дізнався, що користувач PC2 не може відкрити веб-сторінку. На всіх комп'ютерах налаштована статична IP-адресація. Знайдіть несправність за допомогою команди **ping**.

Крок 1: Перевірка підключення

1. Відкрийте вкладку **Desktop > Web Browser** на кожному ПК і введіть URL **ciscolearn.more.com**.
2. Визначіть який комп'ютер не може підключитися до веб-серверу. Всім пристроям потрібен час для завершення процесу завантаження. Дочекайтесь відповіді сервера (це може зайняти до хвилини часу).

Крок 2: Відправлення echo-запиту на веб-сервер з PC2

1. Відкрийте командний рядок **PC2 (Desktop > Command Prompt)**.
2. Введіть команду: **ping ciscolearn.more.com**.
3. Чи отримано відповідь на echo-запит? Яку IP-адресу повернено у відповідь (якщо повернено)?

Крок 3: Відправлення echo-запиту на веб-сервер з PC1

1. Відкрийте командний рядок **PC1 (Desktop > Command Prompt)**.
2. Введіть команду: **ping ciscolearn.more.com**.
3. Чи отримано відповідь на echo-запит? Яку IP-адресу повернено у відповідь (якщо повернено)?

Крок 4: Перевірка доступності веб-сервера за допомогою echo-запиту по IP-адресі з PC2

1. Відкрийте командний рядок **PC1 (Desktop > Command Prompt)**.
2. Спробуйте підключитися до веб-сервера по його IP-адресі за допомогою команди **ping 192.15.2.10**.
3. Чи отримано відповідь на echo-запит? Якщо так, значить, PC2 може підключатися до веб-сервера з використанням IP-адреси, а не імені домену. Можливо, проблема в налаштування сервера DNS PC2.

Крок 5: Порівняння налаштування DNS-сервера PC2 з налаштуваннями інших ПК у локальній мережі

1. Відкрийте **командний рядок** PC1.
2. Перевірте налаштування DNS-сервера PC1 за допомогою команди **ipconfig /all**.

3. Відкрийте **командний рядок** PC2.
4. Перевірте налаштування DNS-сервера PC2 за допомогою команди **ipconfig /all**. Переконайтесь в ідентичності налаштувань.

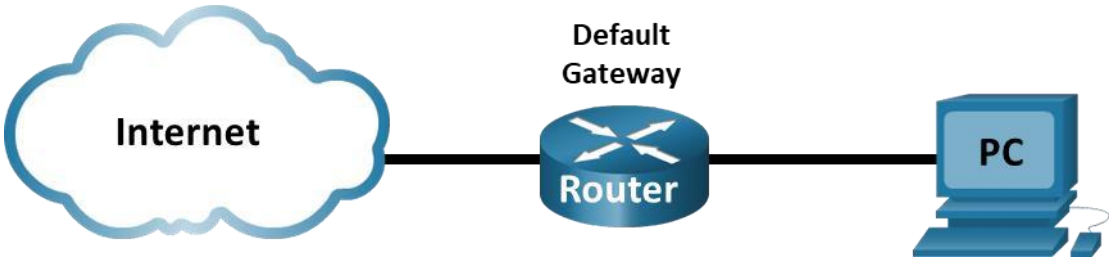
Крок 6: Зміна налаштування PC2

1. Відкрийте вкладку **Config** PC2 і внесіть всі необхідні зміни до конфігурації.
2. Відкрийте веб-браузер із вкладки **Desktop > Web Browser**, підключіться до **ciscolearn.more.com** і перевірте, чи допомогли зміни вирішити проблему.
3. Натисніть кнопку **«Check Results»** у нижній частині вікна для перевірки роботи.

Лабораторна робота №9.3

Тестування мережної затримки за допомогою команд Ping і Traceroute

Топологія



Цілі та задачі

Частина 1: Застосування команди Ping для дослідження затримки у мережі

Частина 2: Використання команди Traceroute для дослідження затримки в мережі

Довідкова інформація / Сценарій

Щоб отримати реалістичну статистику затримки в мережі, це завдання потрібно виконувати в реальній мережі. Не забудьте проконсультуватися з вашим інструктором щодо локальних обмежень безпеки при використанні команди **ping** в мережі.

Мета цієї лабораторної роботи полягає у вимірюванні та оцінці мережної затримки з плином часу і в різні періоди доби, щоб отримати репрезентативну вибірку типової мережної активності. Цього можна досягти шляхом аналізу затримки повернення з віддаленого комп'ютера відповіді на запит **ping**. Час затримки повернення, виміряний в мілісекундах, буде підсумовано шляхом обчислення середньої затримки (середнє значення) і діапазону (максимальне і мінімальне значення) часу затримки.

Необхідні ресурси

- 1 ПК з доступом в Інтернет

Інструкції

Частина 1: Застосування команди Ping для дослідження затримки в мережі

У частині 1 ви дослідите мережну затримку декількох веб-сайтів у різних частинах земної кулі. Цей процес можна використовувати в корпоративній виробничій мережі для визначення базового рівня продуктивності.

Крок 1: Перевірте з'єднання.

Пропінгуйте такі веб-сайти Регіонального Інтернет-реєстру (RIR, Regional Internet Registry) для перевірки з'єднання:

C:\Users\User1> **ping www.lacnic.net**

C:\Users\User1> **ping www.afrinic.net**

C:\Users\User1> **ping www.apnic.net**

Примітка. Оскільки www.ripe.net і www.arin.net не відповідають на запити ICMP, їх не можна використовувати для цієї лабораторної роботи.

Примітка. Якщо веб-сайти мають доступ до IPv6-адрес, за бажанням можна використовувати параметр -4 для визначення IPv4-адрес. Команда має вигляд **ping -4 www.arin.net**.

Крок 2: Зберіть мережні дані.

Ви зберете достатній обсяг даних для обчислення статистики по результатах виконання команди **ping**, відправивши 25 ехо-запитів на кожну адресу, вказану в кроці 1. Цей крок може потребувати адміністративних привілеїв, залежно від вашої операційної системи. Запишіть результати для кожного веб-сайту в текстові файли.

a. У командному рядку введіть **ping**, щоб переглянути доступні параметри.

   C:\Users\User1 > **ping**

b. Використовуючи команду **ping** з опцією count, ви можете відправити 25 ехо-запитів до місця призначення, як показано нижче. Крім того, програма створить текстовий файл з назвою **arin.txt** у поточному каталозі. Цей текстовий файл буде містити результати ехо-запитів.

   C:\Users\User1 > **ping —n 25 www.lacnic.net > lacnic.txt**

Примітка: Термінал залишається порожнім, доки команда не завершиться, оскільки вихідний файл у цьому прикладі був перенаправлений до текстового файлу **lacnic.txt**. Символ **>** використовується для перенаправлення вихідних даних з екрану до файлу та перезапису файлу, якщо

він вже існує. Якщо потрібно додати більше результатів до файлу, замініть > на >> у команді**.** c. Повторіть команду **ping** для інших веб-сайтів.

C:\Users\User1 > **ping —n 25 www.afrinic.net > afrinic.txt**
C:\Users\User1 > **ping—n 25 www.apnic.net > apnic.txt**

Крок 3: Перевірте збір даних.

Щоб переконатися, що файли створено, скористайтеся командою dir, щоб переглянути список файлів у каталозі. Також символом підстановки * можна скористатися для відфільтровування лише текстових файлів.

C:\Users\User1 > **dir *.txt**

Volume in drive C is OS

Volume Serial Number is 0A97-D265

Directory of C:\Users\User1

02/07/2013 12:59 PM 1,642 afrinic.txt
02/07/2013 01:00 PM 1,615 apnic.txt
02/07/2013 12:58 PM 1,589 lacnic.txt

Щоб переглянути результати у створеному файлі, скористайтеся командою **more** в командному рядку.

C:\Users\User1 > **more lacnic.txt**

Примітка. Натисніть клавішу ПРОБІЛ, щоб відобразити решту файлу, або натисніть клавішу **q**, щоб вийти.

Запишіть результати в наведену нижче таблицю.

	Мінімум	**Максимум**	**Середнє значення**
www.afrinic.net			
www.apnic.net			
www.lacnic.net			

Порівняйте результати затримки. Як на затримку впливає географічне положення?

Частина 2: Використання команди Traceroute для дослідження затримки в мережі

Відстежені маршрути можуть проходити через безліч переходів і декількох різних Інтернет-провайдерів залежно від величини провайдерів і місця

розташування вузлів джерела та призначення. Команду **traceroute** також можна використовувати для спостереження за затримкою мережі. У частині 2 команда **tracert** використовується для трасування шляху до того ж місця призначення, що й в частині 1. Команда **tracert** - це версія команди traceroute в ОС Windows.

Команда **tracert** використовує пакети ICMP TTL Exceed і exo-відповіді ICMP для трасування шляху.

Крок 1: Скористайтесь командою tracert і запишіть вихідні дані в текстові файли.

Скопіюйте такі команди для створення файлів traceroute:

C:\Users\User1 > **tracert www.lacnic.net > traceroute_lacnic.txt**

C:\Users\User1 > **tracert www.afrinic.net > traceroute_afrinic.txt**

C:\Users\User1 > **tracert www.apnic.net > traceroute_apnic.txt**

Примітка. Якщо веб-сайти мають доступ до IPv6-адрес, за бажанням можна використовувати параметр -4 для перетворення IPv4-адрес. Команда має вигляд **tracert -4** www.**lacnic**.net **> traceroute_lacnic.txt**.

Крок 2: Використовуйте команду More для вивчення трасованих шляхів.

a. Скористайтеся командою **more**, щоб отримати доступ до вмісту цих файлів:

   C:\Users\User1 **more traceroute_arin.txt**

   У цьому прикладі для отримання відповіді від шлюзу за замовчуванням (192.168.0.1) знадобилося менше 1 мс. Для 6 переходів туди і назад до адреси 4.28.58.177 було витрачено в середньому 37 мс. Для проходження шляху в обидва кінці до www.lacnic .net в середньому потрібно було 225 мс.
   Між рядками 8 і 9 є більші затримки мережі, на що вказує збільшення часу в обидва кінці в середньому з 78 мс до 298 мс

b. Виконайте такий же аналіз інших результатів трасування.

   Який можна зробити висновок щодо взаємозв'язку між часом

   і географічним положенням?

Частина 3: Розширена команда Traceroute

Хоча команда **traceroute** має різні реалізації в залежності від платформи, всі версії дозволяють користувачеві коригувати її поведінку. У Windows це можна зробити за допомогою параметрів і перемикачів в командному рядку **tracert**.

a. Зворотне визначення імені (перетворення IP-адреси на доменне ім'я) може додати затримку до результатів **tracert** і призвести до неточних результатів. Щоб команда **tracert** не намагалася виконати зворотне

перетворення IP-адрес переходів, додайте параметр **–d** до командного рядка **tracert** :

C:\Users\User1 > **tracert —d www.lacnic.net > traceroute_d_lacnic.txt**

C:\Users\User1 > **tracert —d www.afrinic.net > traceroute_d_afrinic.txt**

C:\Users\User1 > **tracert —d www.apnic.net > traceroute_d_apnic.txt**

b. Скористайтеся командою **more**, щоб отримати доступ до вмісту цих файлів:

C:\Users\User1 **more traceroute_d_lacnic.txt**

Чим відрізняється результат виконання команди **tracert** при використанні параметра **-d** ?

Примітка. Команда Windows **tracert** надасть список доступних параметрів та їх опис, якщо буде запущена без будь-яких параметрів.

Примітка. Реалізація **traceroute** у Cisco IOS також дозволяє здійснювати точне налаштування, але вона не залежить від параметрів командного рядка. Розширена команда Cisco IOS traceroute представляє собою ряд простих запитів, які дозволяють адміністратору надавати значення для потрібних параметрів.

Питання для самоперевірки

1. Результати **tracert** і **ping** можуть надати важливі відомості про затримку мережі. Що вам потрібно зробити, якщо ви хочете отримати точну базову картину щодо мережної затримки для вашої мережі?

2. Як можна використовувати базову інформацію?

Лабораторна робота №10
Обмін даними TCP і UDP

Цілі та задачі

Частина 1. Створення мережного трафіку в режимі моделювання

Частина 2. Вивчення функціональності протоколів TCP і UDP

Довідкова інформація

Це завдання з моделювання покликане сформувати основу для детального розуміння процесів TCP і UDP. Режим моделювання Packet Tracer надає можливість переглядати стан різних протокольних одиниць даних (PDU) під час їх транспортування мережею.

Цей режим дозволяє відстежувати кожен протокол і відповідні йому PDU. Наведені нижче кроки познайомлять вас з усіма етапами процесу звернення до мережних служб, які використовуються різними застосунками, доступними на клієнтському ПК. Ви зможете дослідити функціонування протоколів TCP і UDP, мультиплексування та ролі номерів портів при визначенні локального застосунку, який запитує або надсилає дані.

Інструкції

Частина 1: Створення мережного трафіку в режимі моделювання та перегляд мультиплексування

Крок 1: Створення трафіку для заповнення таблиці протоколу визначення адрес (ARP).

Для зменшення обсягу мережного трафіку, що переглядатиметься при моделюванні, виконайте такі дії.

a. Натисніть на **MultiServer**, оберіть вкладку робочого стола **Desktop** і перейдіть до режиму командного рядка **Command Prompt**.

b. Введіть команду **ping -n 1 192.168.1.255**. Це звернення за широкомовною адресою клієнтської локальної мережі. Згідно з налаштуваннями команда надсилатиме лише один запит ping, замість звичних чотирьох. За кілька секунд кожен пристрій у мережі відповість на це звернення від MultiServer.

c. Закрийте вікно **MultiServer**.

Крок 2: Створення веб-трафіку (HTTP).

a. Перейдіть до режиму моделювання (**Simulation mode**).

b. Клацніть на **HTTP Client** і на робочому столі відкрийте **Web Browser**.

c. У полі URL введіть **192.168.1.254** і натисніть **Go**. У вікні топології з'являться конверти (PDU).

d. Згорніть, але не закривайте вікно налаштування **HTTP Client**.

Крок 3: Створення FTP-трафіку.

a. Натисніть на **FTP Client** і на робочому столі відкрийте **Command Prompt**.

b. Введіть команду **ftp 192.168.1.254**. У вікні моделювання з'являться відповідні PDU.

c. Згорніть, але не закривайте вікно налаштування **FTP Client**.

Крок 4: Створення DNS-трафіку.

a. Клацніть на DNS Client і відкрийте **Command Prompt**.

b. Введіть команду **nslookup multiserver.pt.ptu**. У вікні моделювання з'являться PDU.

c. Згорніть, але не закривайте вікно налаштування **DNS Client**.

Крок 5: Створення трафіку електронної пошти.

a. Клацніть на **E-Mail Client** і відкрийте на робочому столі інструмент **E Mail**.

b. Натисніть **Compose** і введіть таку інформацію:

1) **To:** user@multiserver.pt.ptu

2) **Subject:** вкажіть тему на власний розсуд

3) **E-Mail Body:** введіть свій текст Email-повідомлення**.**

c. Натисніть **Send**.

d. Згорніть, але не закривайте вікно налаштування **E-Mail Client**.

Крок 6: Підтвердження створення трафіку і його готовності до моделювання.

На панелі моделювання повинні з'явитися PDU для кожного з клієнтських комп'ютерів.

Крок 7: Вивчення мультиплексування при передаванні трафіку мережею.

Зараз скористайтесь **кнопкою Caps/Forward** на панелі моделювання для дослідження протоколів, залучених до мережної взаємодії.
Примітка: **Кнопка** Caps/Forward ' >| ' — це маленька стрілка, що вказує праворуч, з вертикальною рискою поруч.

a. Один раз натисніть кнопку **Caps/Forward** . Усі PDU прямують до комутатора.

b. Натисніть шість разів на кнопку **Capture/Forward** і перегляньте, як PDUs від різних вузлів ширяться мережею. Зверніть увагу, що у заданий момент

часу лише одна протокольна одиниця даних може перетинати канал у кожному напрямку.

Як це називається?

На панелі моделювання у списку подій відображаються різноманітні PDUs. Що позначають різні кольори конвертів?

Частина 2: Вивчення функціональності протоколів TCP і UDP

Крок 1: Дослідіть HTTP-трафік у процесі взаємодії клієнтів із сервером.

a. Натисніть кнопку **Reset Simulation**.

b. Відфільтруйте трафік, таким чином, щоб відображалися лише протокольні одиниці даних для **HTTP** і **TCP**. Для фільтрування трафіку:

   1) Натисніть кнопку **Edit Filters** і перемкніть кнопку **Show All/None**.

   2) Виберіть **HTTP** і **TCP**. Для закриття вікна Edit Filters клацніть на червоній позначці «x» у верхньому правому куті вікна. Серед видимих подій (Visible Events) тепер повинні спостерігатися лише PDUs **HTTP** і **TCP** .

c. Відкрийте браузер на HTTP Client і в полі URL введіть **192.168.1.254**. Натисніть кнопку **Go** для з'єднання із сервером за протоколом HTTP. Згорніть вікно HTTP-клієнта.

d. Натисніть кнопку **Caps/Forward**, допоки не з'явиться PDU для HTTP. Зверніть увагу, що колір конверта у вікні топології відповідає кольоровому позначенню PDU для HTTP на панелі моделювання.

Чому для появи протокольних одиниць даних HTTP знадобився деяких час?

e. Клацніть на конверті PDU для перегляду його детальної інформації. Перейдіть на вкладку **Outbound PDU Details** (інформація про вихідний PDU) і прокрутіть вниз до передостаннього розділу.

Як позначений цей розділ?

Чи можна вважати це з'єднання надійним?

Запишіть значення **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** і **NUM ACK**.

f. Зверніть увагу на значення у полі прапорців (Flags), розташованому поруч із полем Window. Значення праворуч від «b» відповідають TCP-прапорцям, встановленим на цьому етапі з'єднання. Кожній із шести позицій відповідає свій прапорець. Наявність «1» на будь-якій позиції свідчить про те, що прапорець встановлений. Одночасно можуть бути встановлені декілька прапорців. Позиції прапорців наведені нижче.

Положення прапорця	**6**	**5**	**4**	**3**	**2**	**1**
Значення	URG	ACK	PSH	RST	SYN	FIN

Які TCP-прапорці встановлені у цьому PDU?

g. Закрийте PDU і натискайте **Caps/Forward** допоки конверт із галочкою не повернеться до **HTTP Client**.

h. Клацніть на конверті PDU і оберіть відомості про вхідний PDU - **Inbound PDU Details**.

Чим номери портів і порядкові номери відрізняються від значень, розглянутих раніше?

i. Клацніть на HTTP PDU, який **HTTP Client** підготував для надсилання до **MultiServer**. Це початок HTTP-з'єднання. Клацніть на конверті другого PDU і оберіть **Outbound PDU Details**.

Які відомості тепер містяться у розділі TCP? Чим номери портів і порядкові номери відрізняються від отриманих для двох попередніх PDU?

j. Перемкніть процес моделювання (Reset simulation).

Крок 2: Дослідіть FTP-трафік у процесі взаємодії клієнтів із сервером.

a. Перейдіть до режиму командного рядка на робочому столі FTP-клієнта. Розпочніть FTP-з'єднання, увівши **ftp 192.168.1.254**.

b. На панелі моделювання налаштуйте фільтри - **Edit Filters**, для відображення лише **FTP** і **TCP**.

c. Натисніть **Capture/Forward**. Відкрийте другий конверт PDU.

   Перейдіть на вкладку інформації про вихідний PDU - **Outbound PDU Details** і прокрутіть униз до розділу TCP.

   Чи можна вважати це з'єднання надійним?

d. Запишіть значення **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** і **ACK NUM**.

   Яке значення поля прапорця?

e. Закрийте PDU і натисніть **Capture/Forward** допоки PDU не повернеться до **FTP Client** із галочкою.

f. Клацніть на конверті PDU і оберіть відомості про вихідні PDU **Inbound PDU Details**.

   Чим номери портів і порядкові номери відрізняються від значень, розглянутих раніше?

g. Перейдіть на вкладку **Outbound PDU Details**.

   Чим номери портів і порядкові номери відрізняються від попередніх результатів?

h. Закрийте PDU і натисніть **Capture/Forward** допоки другий PDU не повернеться до **FTP Client**. Цей PDU позначений іншим кольором.

i. Відкрийте PDU і оберіть **Inbound PDU Details**. Прокрутіть вниз повз розділ TCP.

   Що міститься у повідомленні від сервера?

j. Натисніть кнопку Reset Simulation.

Крок 3: Перевірте трафік DNS у процесі взаємодії клієнтів із сервером.

a. Для генерування DNS-трафіку повторіть кроки з Частини 1.

b. На панелі моделювання змініть налаштування фільтрів - **Edit Filters** для перегляду лише **DNS** і **UDP**.

c. Для відкриття клацніть на конверті PDU.

d. Перегляньте інформацію щодо моделі OSI для вихідного PDU.

Який протокол використовується на Рівні 4?

Чи можна вважати це з'єднання надійним?

e. Відкрийте вкладку Outpound PDU Details і знайдіть розділ UDP форматів PDU. Запишіть значення **SRC** і **DEST PORT**.

Чому немає порядкового номеру і підтвердження?

f. Закрийте **PDU** і натисніть **Capture/Forward** допоки воно із позначкою не повернеться до **DNS Client**.

g. Клацніть на конверті PDU і оберіть відомості про вихідні PDU - **Inbound PDU Details**.

Чим номери портів і порядкові номери відрізняються від розглянутих раніше?

Як називається останній розділ **PDU**? Яка IP-адреса відповідає імені **multiserver.pt.ptu**?

h. Натисніть кнопку Reset Simulation.

Крок 4: Перевірте трафік електронної пошти у процесі взаємодії клієнтів із сервером.

a. Повторіть кроки, описані в Частині 1, щоб надіслати повідомлення електронної пошти до **user@multiserver.pt.ptu**.

b. На панелі моделювання змініть налаштування **Edit Filters** аби стежити лише за протоколами **POP3, SMTP** і **TCP**.

c. Відкрийте PDU, клацнувши на першому конверті.

d. Перейдіть на вкладку **Outbound PDU Details** і прокрутіть до останнього розділу.

Який протокол транспортного рівня використовує трафік електронної пошти?

Чи можна вважати це з'єднання надійним?

e. Запишіть значення **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** і **ACK NUM**. Яке значення поля прапорця?

f. Закрийте **PDU** і натискайте **Capture/Forward,** допоки PDU не повернеться до **E-Mail Client** із позначкою.

g. Натисніть на конверт TCP PDU і оберіть **Inbound PDU Details**.

Чим номери портів і порядкові номери відрізняються від розглянутих раніше?

h. Перейдіть на вкладку **Outbound PDU Details**.

Чим номери портів і порядковий номер відрізняються від попередніх двох результатів?

i. Тут можна побачити другий **PDU** іншого кольору, який **E-Mail Client** підготував для надсилання до **MultiServer**. Це початок обміну email-повідомленнями. Клацніть на конверті другого PDU і оберіть **Outbound PDU Details**.

Чим номери портів і порядкові номери відрізняються від отриманих для двох попередніх **PDU**?

Який email-протокол пов'язаний із TCP-портом 25? Який протокол пов'язаний із TCP-портом 110?

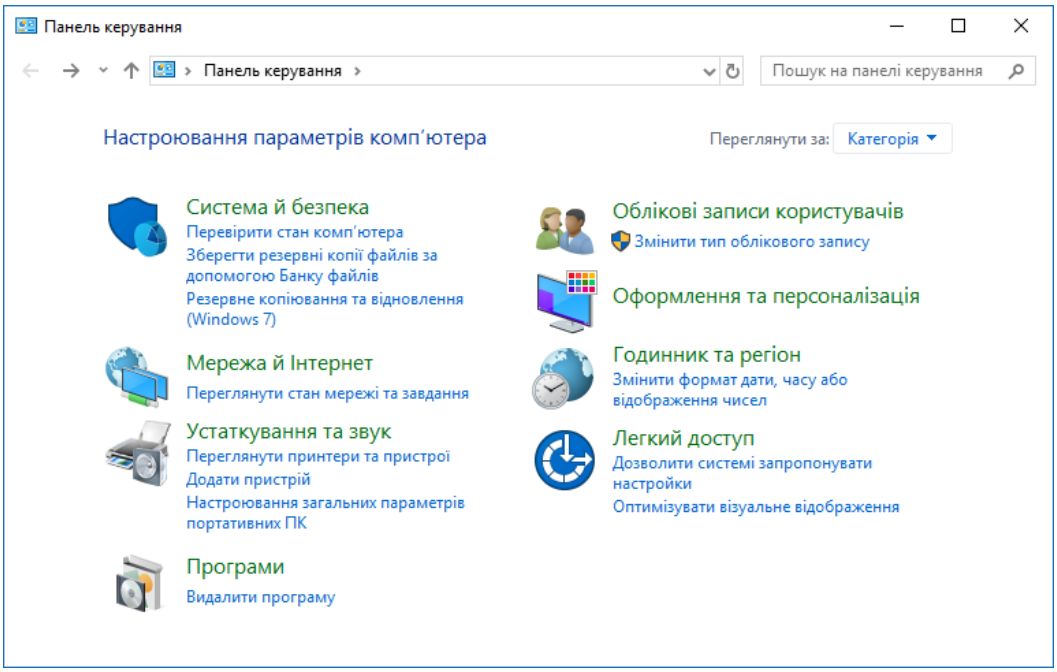
Лабораторна робота №11.1
Налаштування служби DNS

Мета роботи: Навчитись налаштовувати службу DNS в операційній системі Windows 10.

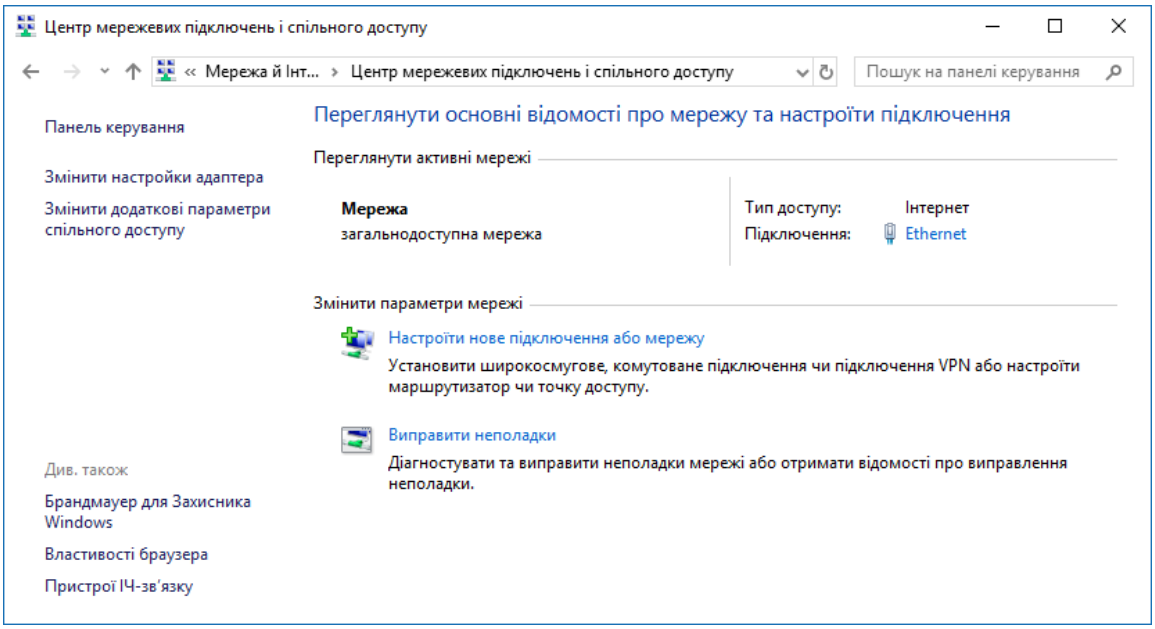
Порядок виконання роботи.

1. **Включення служби DNS в операційній системі Windows 10:**

a. Відкрити «Панель управління» і у ній вибрати пункт «Мережа й Інтернет».

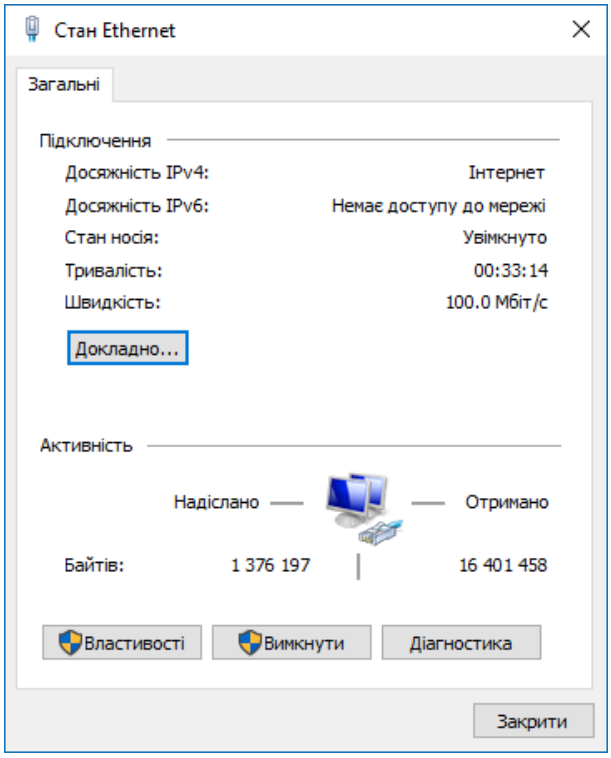


b. Далі потрібно вибрати пункт «Переглянути стан мережі та завдання».



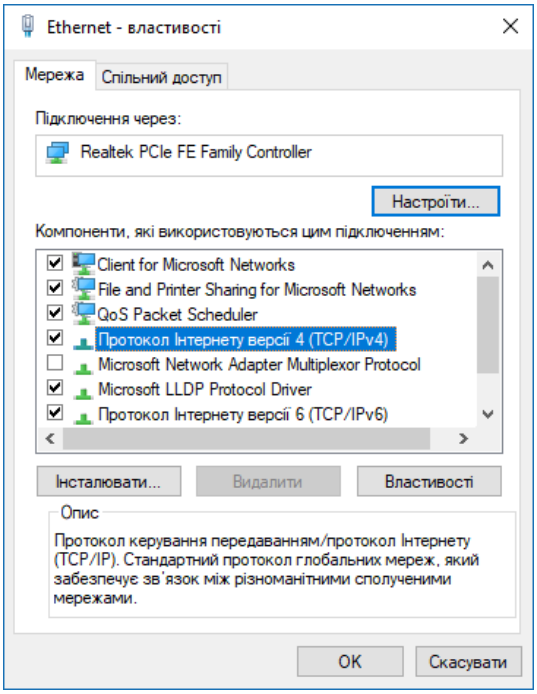
c. В розділі «Переглянути активні мережі» потрібно вибрати підключення, завдяки якому здійснюється доступ до Інтернету (те, що стоїть після «Підключення», Ethernet), і натиснути на нього.

d. Відкриється нове вікно «Стан Ethernet», в якому відображаються всі налаштування обраного підключення.

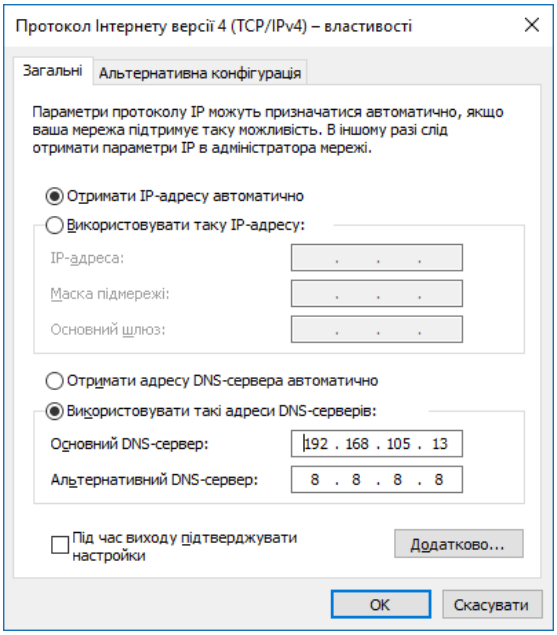


Слід натиснути кнопку «Властивості».

e. Серед компонентів, які використовуються підключенням, потрібно обрати «Протокол Інтернету версії 4 (TCP/IPv4)» або «Протокол Інтернету версії 6 (TCP/IPv6)» і клацнути по кнопці «Властивості» для відповідного протоколу.



f. Активуйте пункт «Використовувати такі адреси DNS-серверів» і наберіть в текстовому полі адреса вашого сервера і додатковий, якщо перший виявиться неактивним (8.8.8.8 – публічний DNS-сервер Google).

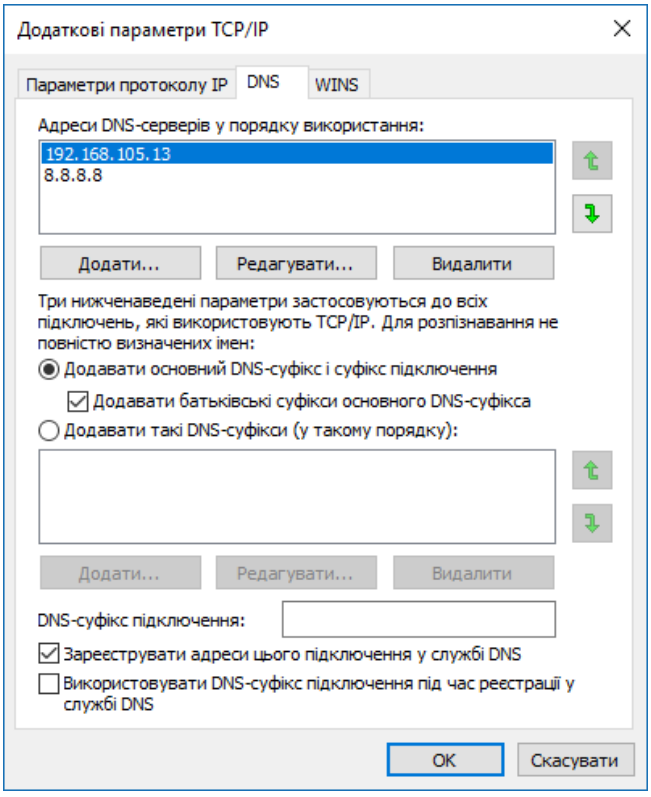


g. Після цього натисніть «Ок», щоб ваші зміни збереглися.

2. Налаштування або зміна DNS-сервера:

a. Виконайте пункти 1-5 включення DNS.

b. Замість введення IP-адрес (які вже є) натисніть на кнопку «Додатково». У новому вікні «Додаткові параметри TCP/IP» перейдіть на вкладку DNS.



c. На вкладці DNS змініть налаштування сервера та натисніть кнопку «Ок», щоб зберегти їх.

На одному з етапів ви вводили адресу основного сервера і альтернативного. Це потрібно тому, що доменні імена зі всього світу не можуть зберігатися в одному місці. Коли комп'ютер шукає серед DNS-серверів запитуване ім'я, він обходить кілька серверів за порядком, який ви можете самостійно задати у полі «Адреси DNS-серверів у порядку використання». Тут може бути введено декілька додаткових адрес DNS-серверів.

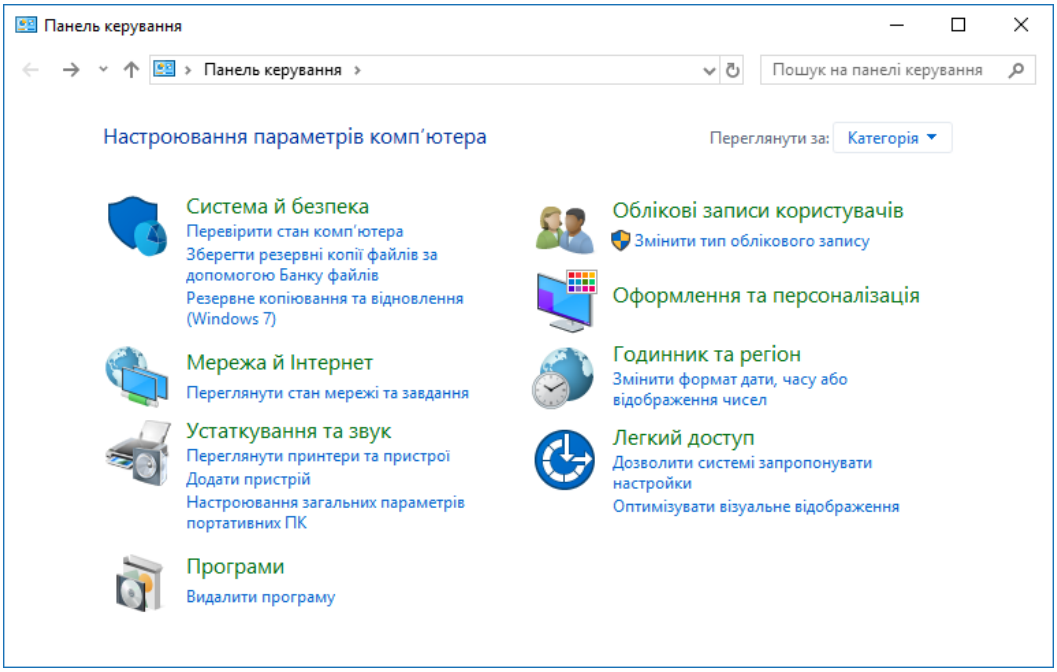
DNS-суфікси потрібні для формування внутрішніх мереж, піддоменних імен (наприклад, subdomain.domain.com). Якщо сервер вам необхідний тільки для підключення до Інтернету, можна пропустити цю настройку та залишити її за замовчуванням. Якщо ви користуєтеся, наприклад, внутрішньої корпоративною мережею, введіть суфікси її піддоменів у відповідне поле.

Включене налаштування «Зареєструвати адреси цього підключення в DNS» означає, що ваш комп'ютер буде зареєстрований на сервері зі своєю адресою та назвою пристрою, прописаного в налаштуваннях. Дізнатися назву вашого пристрою, можна в «Панелі управління» в пункті «Система». Включений пункт «Використовувати DNS-суфікс підключення під час реєстрації у службі DNS» приєднає до імені вашого комп'ютера в мережі додатковий суфікс.

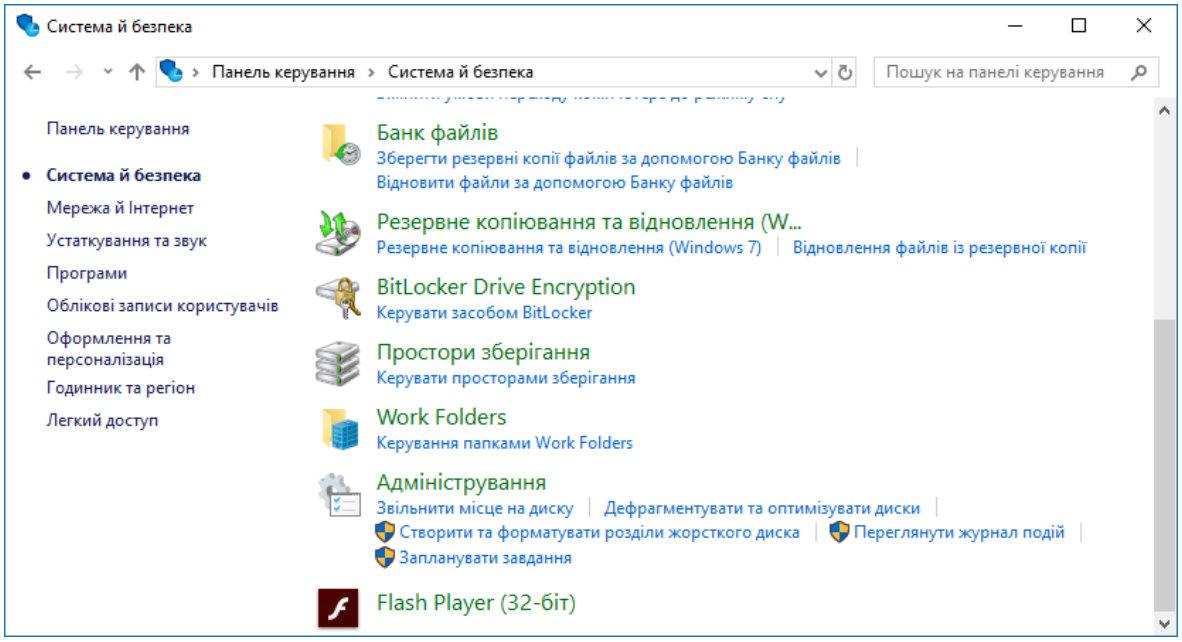
3. Усунення несправностей при роботі служби DNS

Необхідно перевірити налаштування системних служб, для цього потрібно:

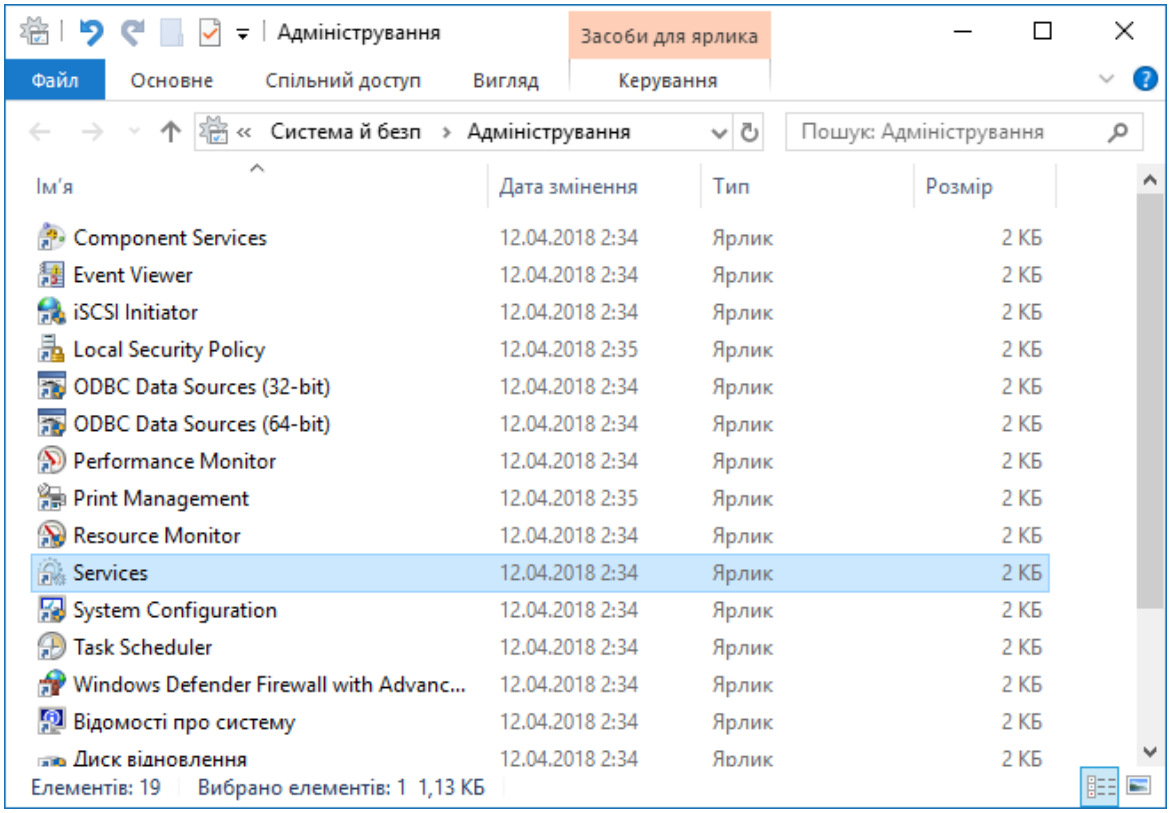
a. Відкрити «Панель управління» і у ній вибрати пункт «Система й безпека».



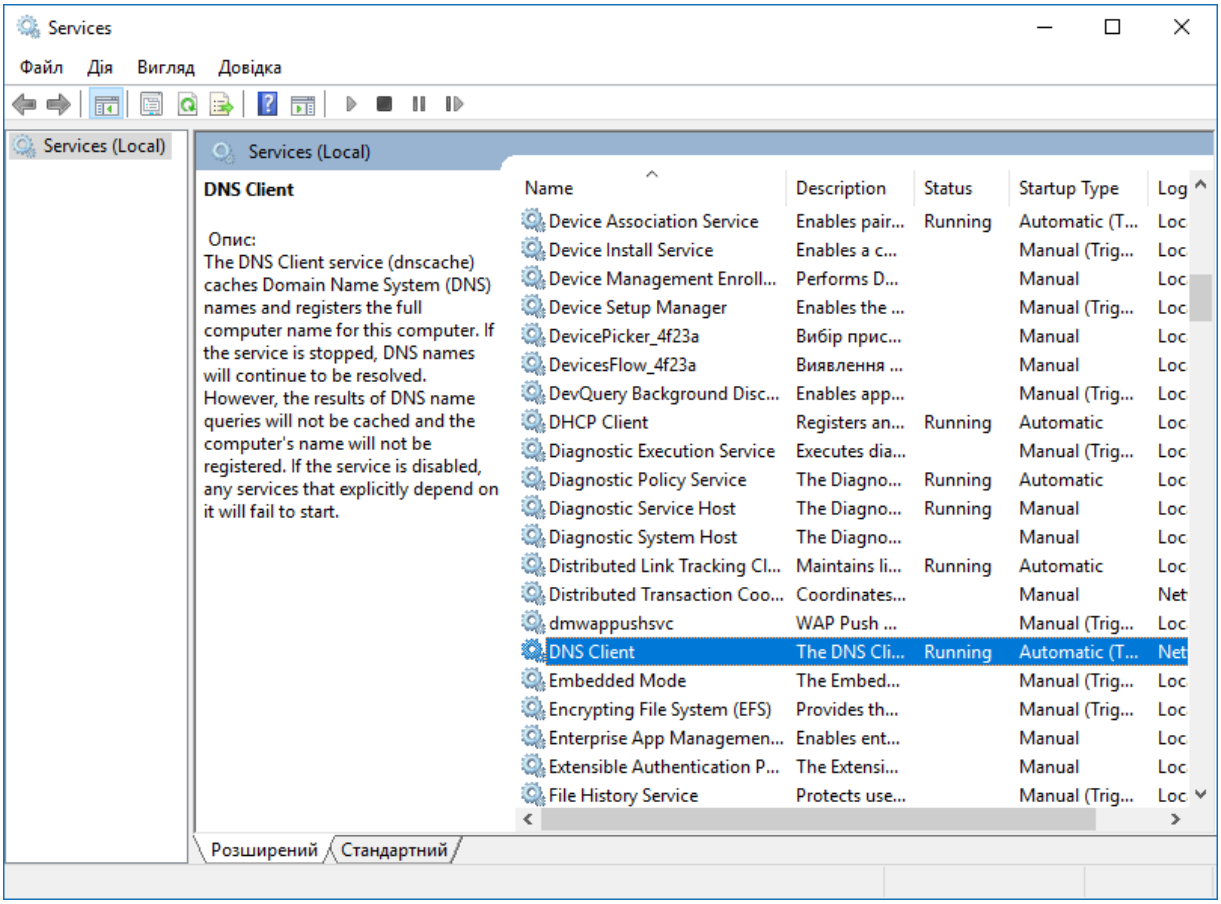
b. У наступному вікні натисніть на «Адміністрування».



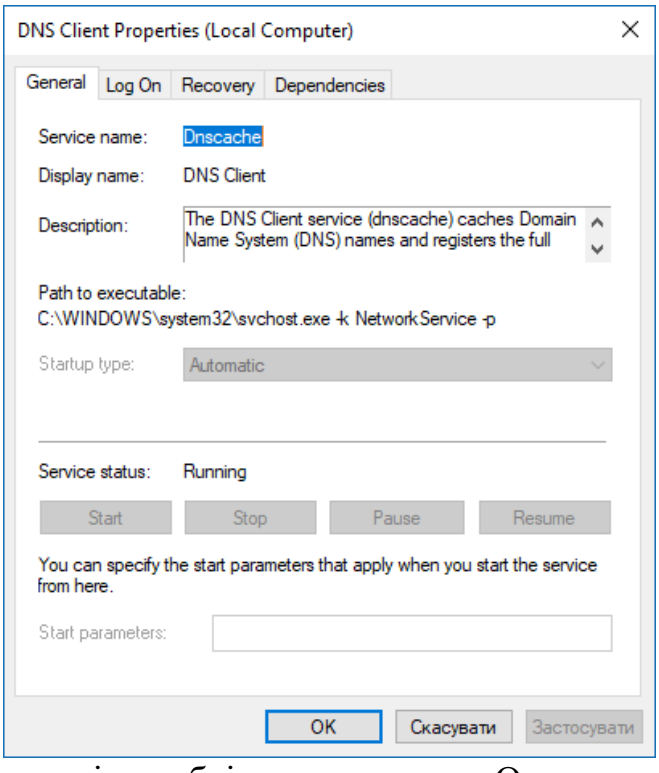
c. Відкриється список всіх доступних програм, виберіть пункт «Services» («Служби»).



d. Знайдіть пункт «DNS-клієнт» і двічі клацніть по ньому мишкою.



е. Зверніть увагу на поле «Startup Type» («Тип запуску») — цей пункт повинен мати параметр «Автоматично».



Після внесених змін необхідно натиснути «Ок».

4. Оформити звіт по виконаній роботі.

Лабораторна робота №11.2
Відстеження DNS-перетворень

Цілі та задачі

Частина 1. Спостереження за перетвореннями протоколу DNS URL-адрес на IP-адреси

Частина 2. Дослідження DNS-пошуку адреси веб-сайту за допомогою команди nslookup

Частина 3. Дослідження DNS-пошуку поштових серверів за допомогою команди nslookup

Довідкова інформація / Сценарій

Система доменних імен (Domain Name System, DNS) викликається під час уведення в адресному рядку веб-браузера Уніфікованого покажчика ресурсів (Uniform Resource Locator, URL), наприклад **http://www.cisco.com**. Перша частина URL описує протокол, який використовується. Традиційно до них належать протокол передавання гіпертексту (HTTP), протокол передавання гіпертексту через рівень захищених сокетів (Secure Socket Layer, SSL) - (HTTPS) і протокол передавання файлів (FTP).

DNS використовує другу частину URL-адреси, у даному прикладі - www.cisco.com. DNS перетворює доменне ім'я (www.cisco.com) на IP-адресу, щоб вихідний вузол зміг досягти кінцевого сервера. У цій лабораторній роботі ви матимете можливість спостерігати за протоколом DNS у дії і скористаєтесь командою **nslookup** (пошук сервера імен) для отримання додаткової інформації про DNS.

Необхідні ресурси

1 PC (Windows із доступом до Інтернету і режиму командного рядка)

Частина 1: Спостереження за перетвореннями протоколу DNS URL-адрес на IP-адреси

a. Відкрийте вікно командного рядка Windows.
b. У командному рядку проінгуйте URL-адресу Інтернет-корпорації з призначення імен і номерів (ICANN) за адресою **www.icann.org**. ICANN координує DNS, IP-адреси, системи керування доменними іменами верхнього рівня та функції керування кореневими серверами. Комп'ютеру потрібно перетворити cisco.com на IP-адресу, щоб знати, куди надсилати пакети Інтернет-протоколу керуючих повідомлень (Internet Control Message Protocol, ICMP).

Перший рядок виводу відображає виконане за допомогою DNS перетворення **www.icann.org** на IPадресу. Результат роботи DNS повинен бути доступний для перегляду, навіть якщо у вашому заклад використовується міжмережний екран, який запобігає пінгуванню, або якщо сервер призначення забороняє звертатися за допомогою команди ping до свого веб-сервера.
Примітка: Якщо ім'я домену перетворюється на адресу IPv6, використовуйте команду **ping -4 www.icann.org** для переходу на адресу IPv4, якщо потрібно.

Запишіть IP-адреси для www.icann.org.

c. Замість URL-адреси використайте для звернення у веб-браузері адреси IPv4 з кроку b. Введіть **https://192.0.32.7** у веб-браузері. Якщо вдалося отримати IPv6-адресу, її також можна застосувати: **https://[2620:0:2d0:200::7]**.

d. Зверніть увагу, що домашня веб-сторінка ICANN відображається без використання DNS. Людям здебільшого легше запам'ятовувати слова, аніж цифри. Якщо ви скажете комусь перейти на **www.icann.org**, вони, ймовірно, пам'ятатимуть саме цю адресу, а не 192.0.32.7, яка, мабуть, важча для сприйняття. Комп'ютери оперують числами. DNS - це процес переклад слів у числа. Окрім цього, має місце ще одне перетворення інформації. Люди сприймають десяткові числа. Комп'ютери обробляють дані у двійковому форматі. Десяткова IP-адреса 192.0.32.7 у двійковому форматі має вигляд 11000000.00000000.00100000.00000111. Що станеться, якщо скопіювати ці двійкові значення і використати їх у браузері?

e. У режимі командного рядка пропінгуйте **www.cisco.com**. **Примітка**: Якщо для доменного імені визначено адресу IPv6, скористайтесь командою **ping -4 www.cisco.com** для перетворення на IPv4, якщо потрібно.

C:\> **ping www.cisco.com**
C:\> ping -4 www.cisco.com

При використанні команди ping www.cisco.com чи отримали ви таку ж IP-адресу, що й у прикладі? Поясніть.

У адресному рядку браузера введіть IP-адресу, яку ви отримали при пінгуванні www.cisco.com. Чи відображається веб-сайт? Поясніть.

Частина 2: Дослідження DNS-пошуку адреси веб-сайту за допомогою команди nslookup

a. У командному рядку введіть команду **nslookup**. Ваш результат може відрізнятися від наведеного у прикладі.

C:\> nslookup

Який DNS-сервер використовується за замовчуванням?

b. Зверніть увагу на зміну позначки командного рядка на більше (>). Це ознака команди **nslookup**. З появою цієї позначки можна вводити команди, пов'язані з DNS.

У полі курсора введіть **?** для перегляду списку всіх команд, доступних для використання у режимі **nslookup** .

c. Введіть **www.cisco.com**.

> www.cisco.com
Default Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
Name: e2867.dsca.akamaiedge.net
Addresses: 2600:1404:a:395::b33
2600:1404:a:38e:b33
172.230.155.162 Aliases:
www.cisco.com
www.cisco.com.akadns.net
wwwds.cisco.com.edgikey.net
wwwds.cisco.com.edgakey.net.globalredir.akadns.net

Яка адреса IPv4 відповідає уведеному доменному імені?

Примітка: IP-адреса, що відповідає вашому розташуванню, найімовірніше, буде відрізнятися, оскільки Cisco використовує дзеркальні сервери у різних локаціях по всьому світу.

Чи збігається вона з IP-адресою, виявленою за допомогою команди **ping**?

Окрім IP-адреси 172.230.155.162, відображаються такі числа: 2600:1404:a:395::b33 і 2600:1404:a:38e::b33. Що вони позначають?

d. У режимі nslookup введіть IP-адресу веб-сервера Cisco, яку ви щойно виявили. За допомогою **nslookup** можна отримати доменне ім'я, якщо URL-адреса вам невідома.

> 172.230.155.162

Default Server: one.one.one.one
Address: 1.1.1.1

Name: a172-230-155-162.deploy.static.akamaitechnologies.com
Address: 172.230.155.162

Інструмент **nslookup** можна використовувати для перетворення доменних імен на IP-адреси. Також він дозволяє виконувати зворотні перетворення IP-адрес на доменні імена.
Використовуючи інструмент **nslookup**, запишіть IP-адреси, пов'язані з **www.google.com**.

Частина 3: Дослідження DNS-пошуку поштових серверів за допомогою команди nslookup

a. У режимі nslookup введіть **set type=mx**, щоб використати **nslookup** для визначення поштових серверів.

> **set type=mx**

b. У режимі nslookup введіть **cisco.com**.

> cisco.com
Server: one.one.one.one
Address: 1.1.1.1
Non-authoritative answer:
cisco.com MX preference = 20, mail exchanger = rcdn-mx-01.cisco.com cisco.com MX preference = 30, mail exchanger = aer-mx-01.cisco.com cisco.com MX preference = 10, mail exchanger = alln-mx-01.cisco.com

Резервування (налаштування більше одного поштового сервера) є одним з основоположних принципів побудови мережі. За його впровадження, у разі відмови одного з поштових серверів, комп'ютер намагається звернутися із запитом до іншого поштового сервера. Адміністратори електронної пошти використовують параметр **MX preference** аби визначити, до якого поштового сервера слід звертатися у першу чергу. Насамперед звертаються до поштового сервера з найнижчим показником **MX preference**. Беручи до уваги отримані вище дані, до якого поштового сервера спершу йтиме звернення при надсиланні листа до cisco.com?

c. У режимі **nslookup** введіть **exit**, щоб повернутися до звичайного режиму командного рядка ПК. d. Введіть **ipconfig /all**.

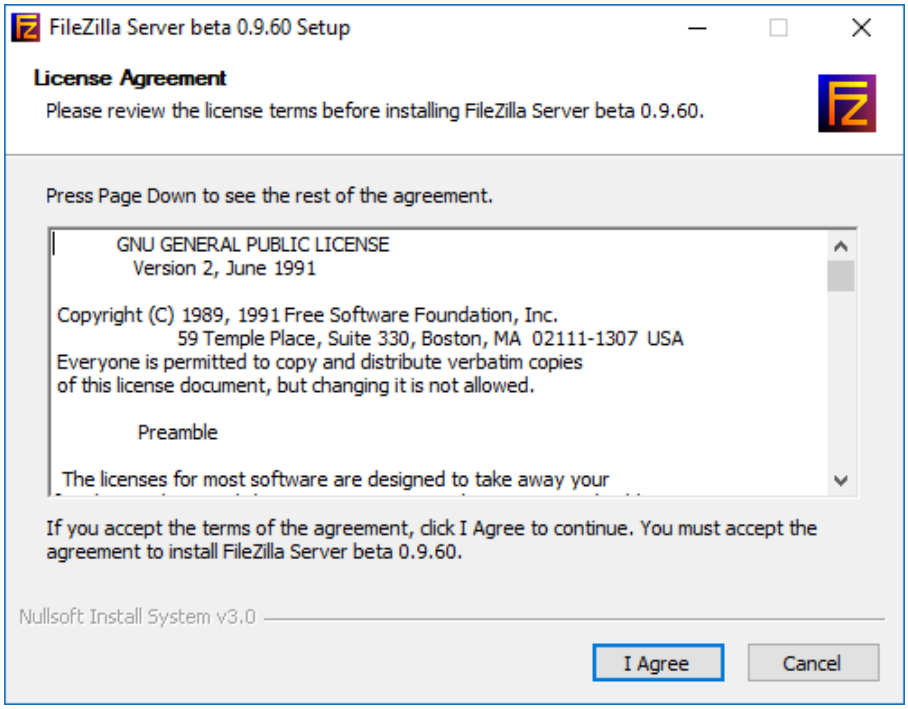
Запишіть IP-адреси усіх DNS-серверів, які використовує ваш навчальний заклад.

Лабораторна робота №12
Налаштування протоколу FTP

Мета роботи: Навчитись встановлювати та налаштовувати FTP сервер на базі FileZilla Server.

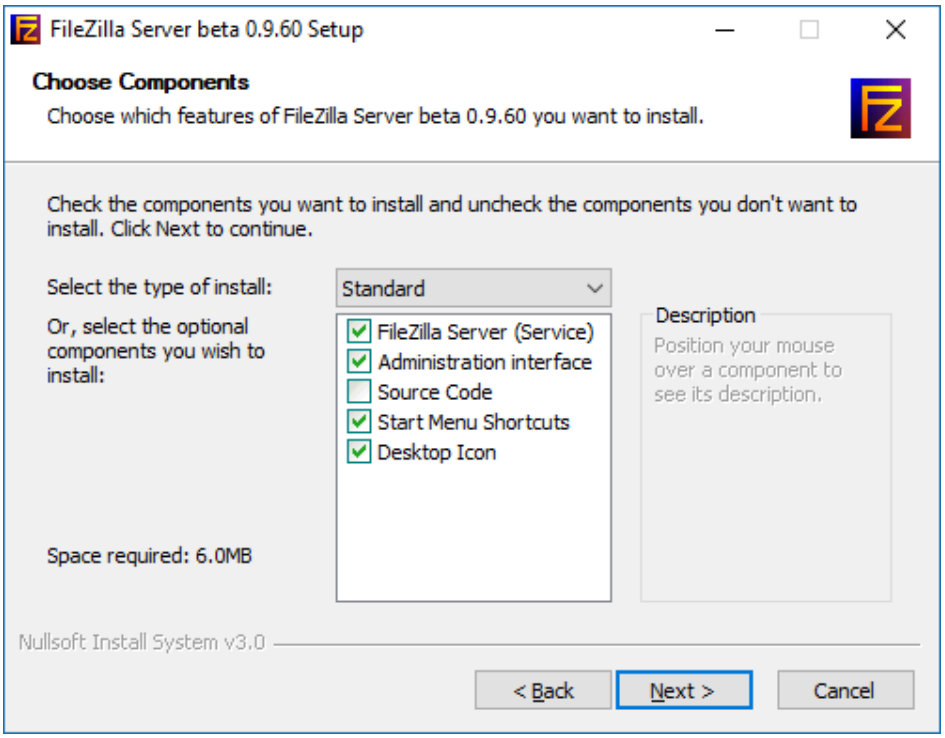
Порядок виконання роботи.

1. **Встановлення FTP сервера:**
   a. Для установки необхідно завантажити один з дистрибутивів, які допоможуть розвернути FTP-сервер. В лабораторній роботі будемо використовувати безкоштовний дистрибутив FileZilla Server.
   b. Після скачування дистрибутива, необхідно запустити його установку і дотримуйтесь рекомендацій нижче. В першому вікні потрібно погодитися з ліцензійною угодою, натисніть «I Agree».



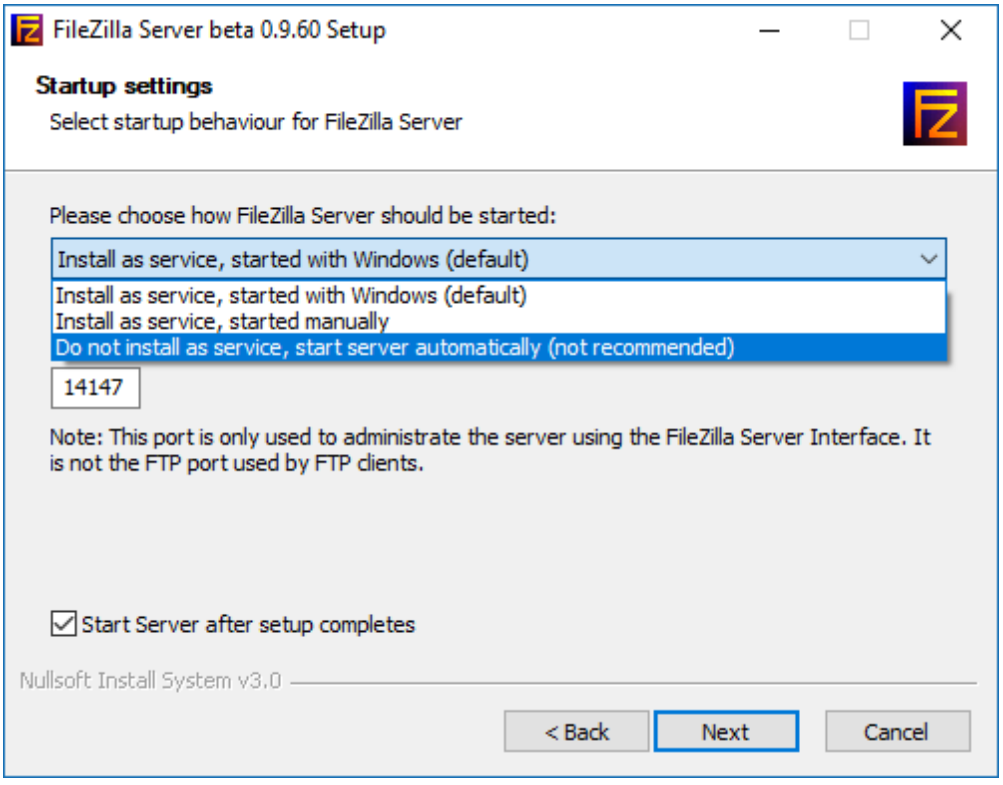
   c. Далі потрібно вибрати тип установки. Усього їх п'ять:
      - Стандартний (Standart) – варіант для установки з нуля для повного функціонування сервера.
      - Повний (Full) – практично теж саме, додатково в папку установки буде скопійований вихідний код програми.
      - Тільки FTP сервіс (Service only) – встановлюється лише FTP сервіс, без доступу до нього через інтерфейс. Корисно, якщо необхідно керувати своїм файлосховищем з іншого комп'ютера.
      - Інтерфейс управління (Interface only) - на відміну від попереднього пункту, ставиться тільки графічна оболонка керування сервером, але не він сам.

- Вибіркова установка (Custom) – можна обрати довільні компоненти.



Оберіть стандартний варіант (Standart) та натисніть «Next».
На наступному вікні необхідно вибрати папку установки, наприклад, «C:\Program Files (x86)\FileZilla Server». Після вибору переходьте до наступного вікна (Next).

d. На наступному кроці необхідно обрати спосіб установки і запуску сервера. Є три варіанти запуску FTP-сервера:



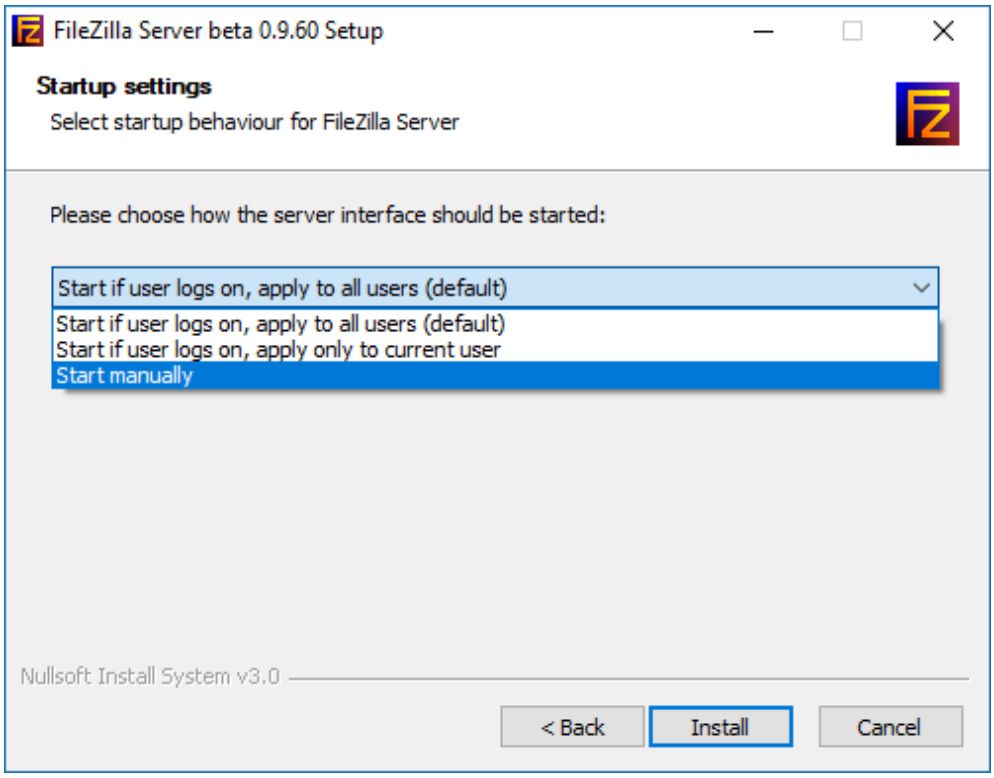
- Як службу і запускати при вході в систему (Install as service, started with Windows (default);
- Як службу і запускати вручну (Install as service, started manually);
- Проста установка, запускати вручну (Do not install as service, start server automatically.

Рекомендується обрати перший або другий варіант. Різниця лише в тому, що в другому випадку для роботи сервера, Вам необхідно буде переходити в «Панель управління - Адміністрування - Управління службами», знаходити там службу в списку і запускати її самостійно, натиснувши на кнопочку запуск.

Крім того, на цьому етапі слід вказати порт, по якому буде підключатися інтерфейс керування сервером. Для підвищення безпеки, рекомендується змінити його зі стандартного (14147) на будь-який інший. За замовчуванням встановлена опція «Запустити сервер після установки» (Start Server after setup completes).

Далі переходьте до останнього вікна, використовуючи кнопку «Next».

е. На наступному кроці необхідно обрати варіанти запуску інтерфейсу.



Інтерфейс являє собою адміністративну програму, яка дозволяє стежити за станом сервера, запускати/зупиняти і налаштовувати його.

Є три варіанти запуску інтерфейсу:

- При вході в систему, для всіх користувачів (Start if user logs on, apply to all users (default);
- При вході в систему, для поточного користувача (Start if user logs on, apply only to current user);
- Вручну (Start manually).

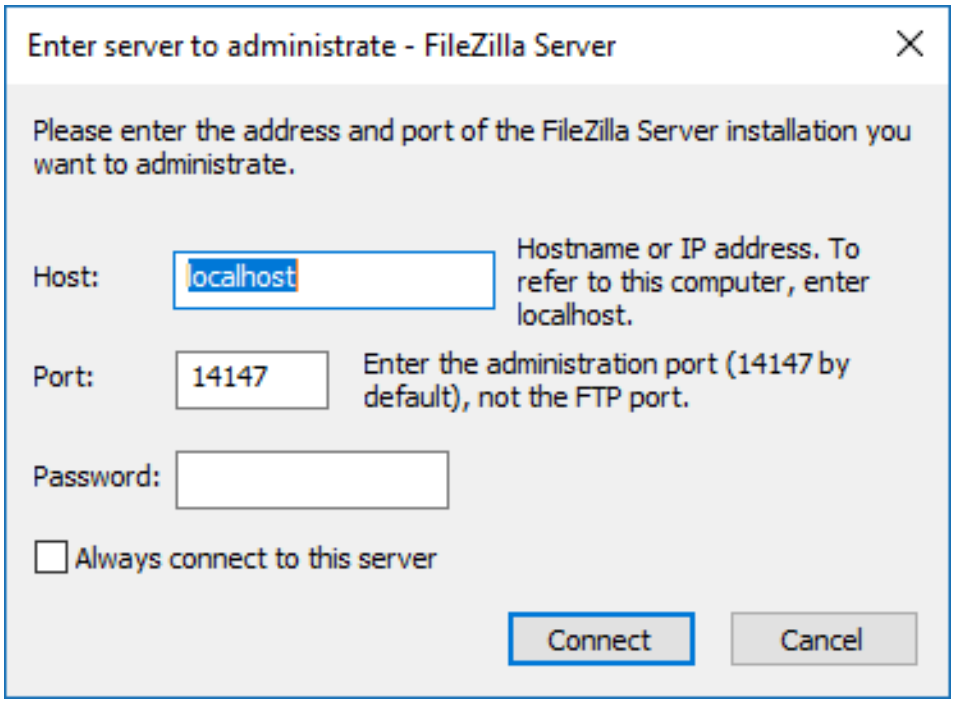
Перший варіант, в основному, використовується коли за комп'ютером, куди встановлюється FTP-сервер, працює один користувач. Другий підходить для тих, хто працює на комп'ютері не один (на комп'ютері кілька акаунтів, які використовуються різними людьми) і хоче, щоб ніхто інший не керував його FTP сервером. І третій варіант задає параметр запуску тільки вручну, сервер не буде стартувати разом із системою, а тільки в ручну.

Прапорець «Start Interface after setup completes» в даному вікні задає запуск інтерфейсу відразу в кінці установки.

Для початку установки сервера слід натиснути кнопку «Install».

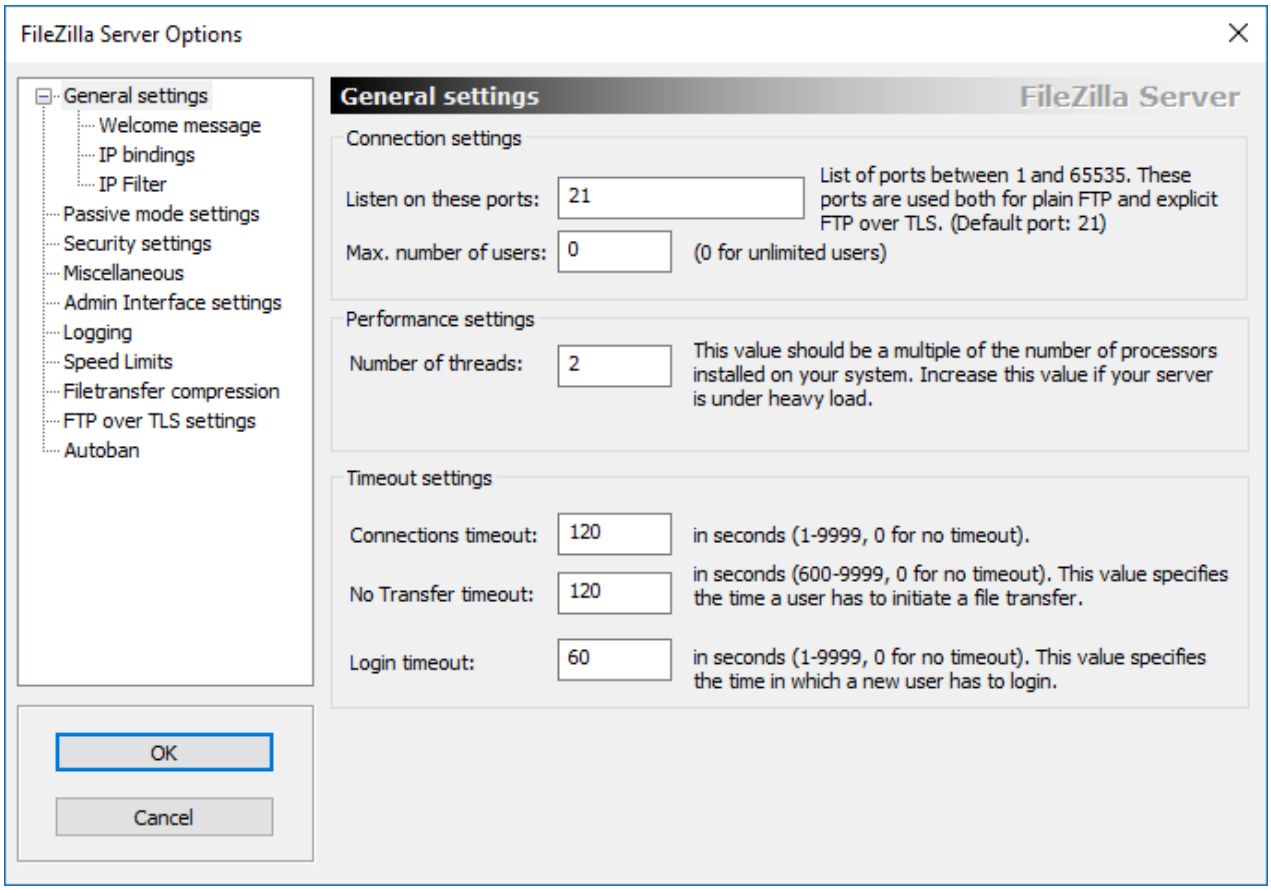
2. Налаштування FTP FileZilla Server

a. Після установки, при першому запуску інтерфейсу, з'явиться вікно, де потрібно вказати адресу і порт для підключення, а так само пароль адміністратора (при першій установки його немає). Можна відзначити опцію «Весь час зв'язуватись з цим сервером» (Always connect to this server). Натискаємо "Ok".



Як видно, це підключення до сервера є локальним, на що вказує ім’я хоста localhost (або IP адреса 127.0.0.1) і порт 14147.

b. Тепер перейдемо до налаштувань. Це робиться шляхом переходу за адресою «Edit -> Settings». відкриється вікно налаштувань. На першій вкладці (General Settings) можна задати наступні параметри:

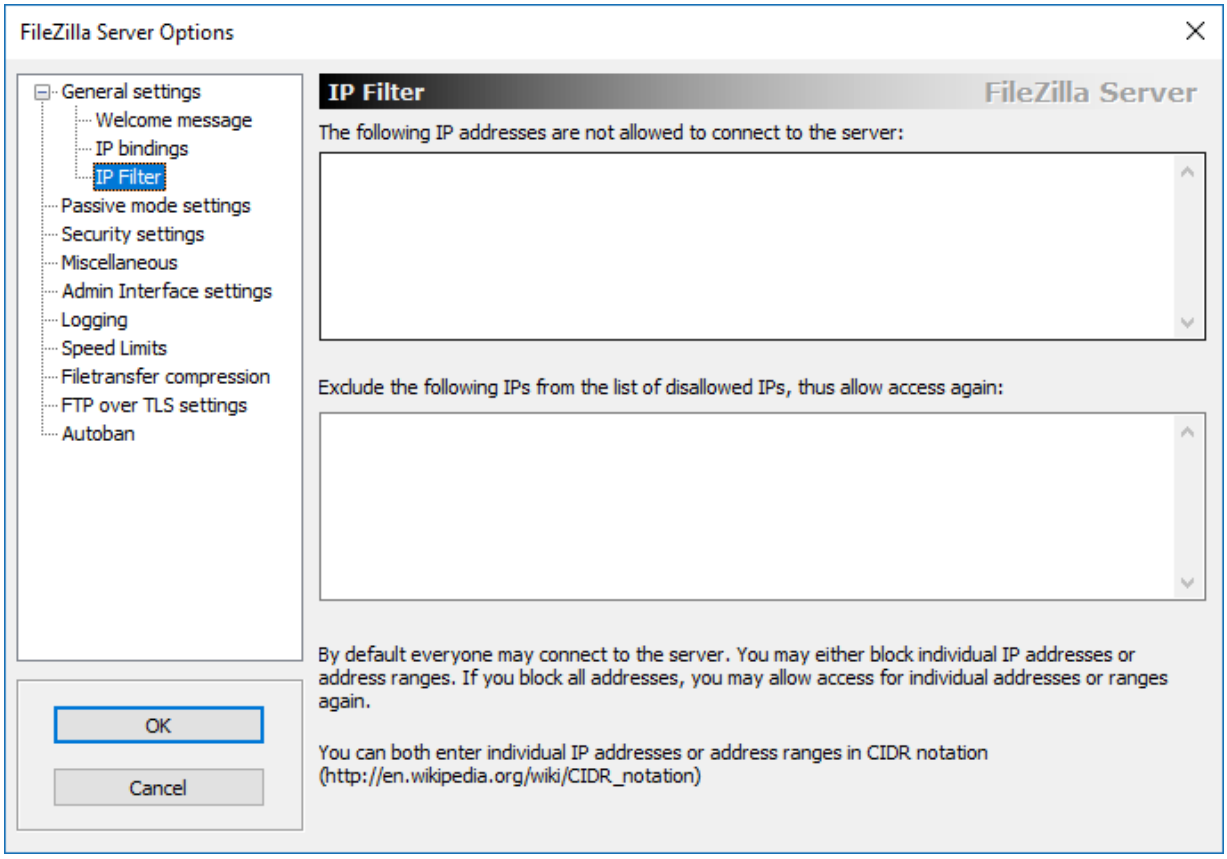


- Порт, за яким клієнти будуть підключатися до сервера (Listen on these ports), за замовчуванням 21 порт;
- Максимальна кількість клієнтів (Max. number of users), за замовчуванням встановлено значення «0», це означаючи, що кількість клієнтів не обмежена.

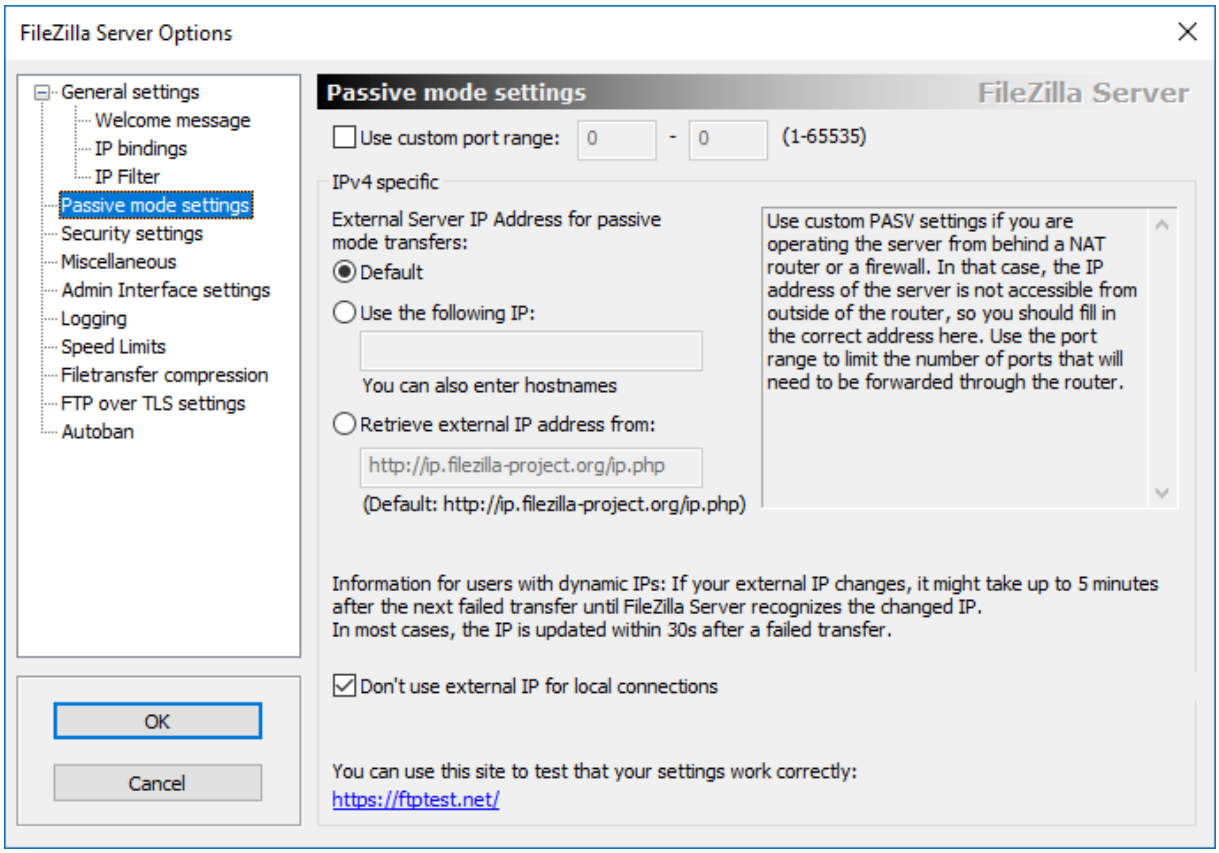
Інші параметри (Кількість потоків (Number of threads) та налаштування тайм-аутів (Timeout setting), як правило, залишають без змін.

c. У наступному підпункті (Welcome message) можна налаштувати вітальне повідомлення, яке будуть бачити користувачі при підключенні.
d. У підпункті «IP bindings» налаштовуються IP-адреси, за якими буде доступний FTP сервер. Якщо необхідно, щоб сервер був доступний тільки з локальної мережі, то замість зірочки, слід вказати локальну IP-адресу, наприклад, 192.168.1.5. В іншому випадку, не варто нічого змінювати.
e. У підпункті «IP Filter» можна задати IP адреси (або їх діапазон), яким буде заборонено підключатися до даного FTP сервера, а також задати виключення із заданого діапазону. Наприклад, якщо потрібно комусь заборонити потрапляти на даний FTP сервер, то необхідно вказати його IP-адресу в першому полі («The following IP addresses are not allowed to connect to the server»). Якщо ж необхідно надати доступ лише певним користувачам і заборонити всім іншим, то слід поставити зірочку (*) в

першому полі і вказати список дозволених IP-адрес в другому («Exclude the following IPs from the list of disallowed IPs, thus allow access again»).

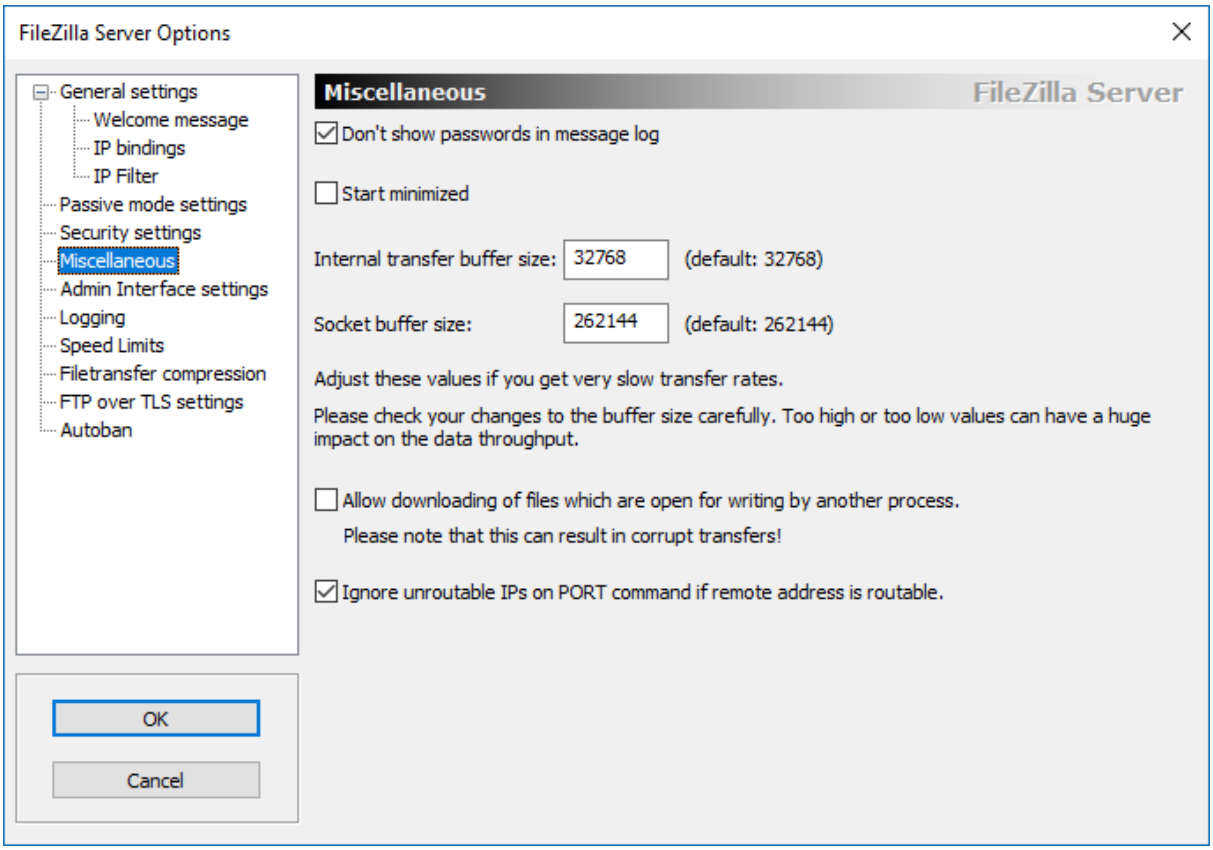


f. Вкладка «Passive mode settings» регламентує параметри для пасивного підключення до сервера.

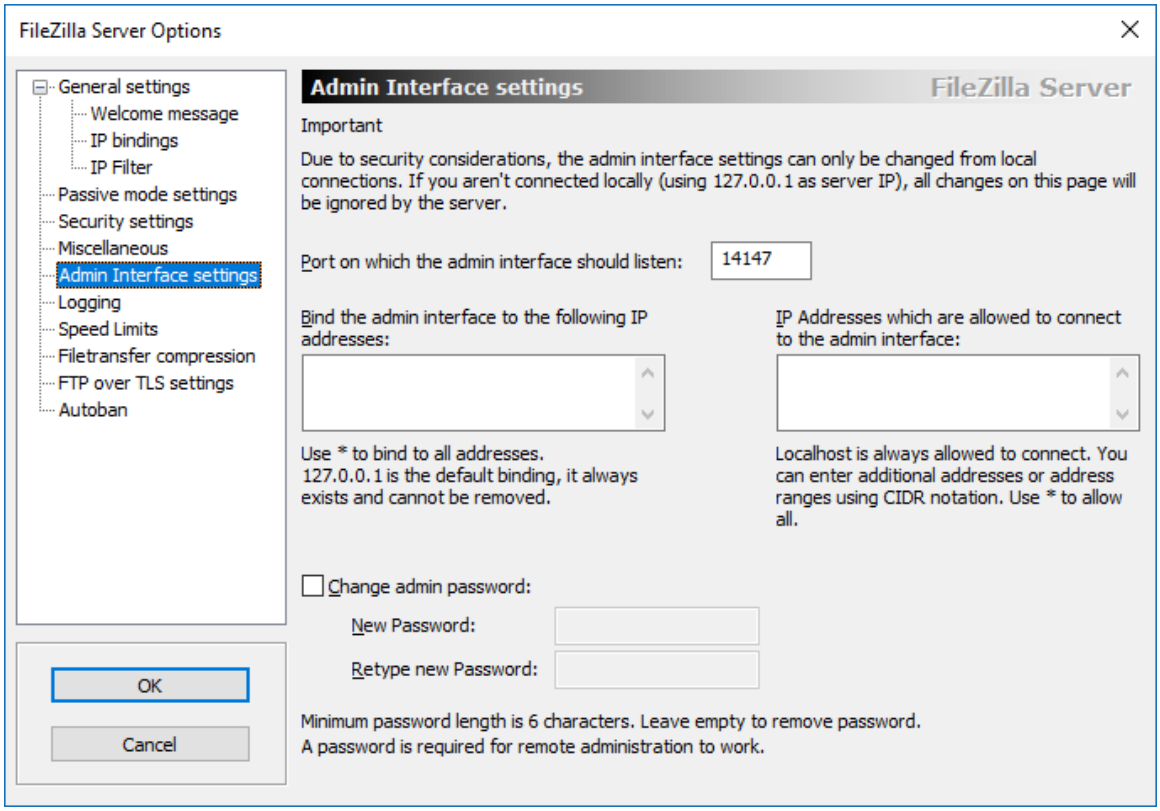


Змінювати налаштування на даній вкладці варто лише в тому випадку, якщо підключення до Інтернету здійснюється через NAT або проксі-сервер.
У цьому випадку необхідно вказати в полі «Use the following IP» свою зовнішню IP-адресу, а також в полі «Use custom port range» задати діапазон портів, через які клієнт зможе підключатися до даного FTP сервера в пасивному режимі.

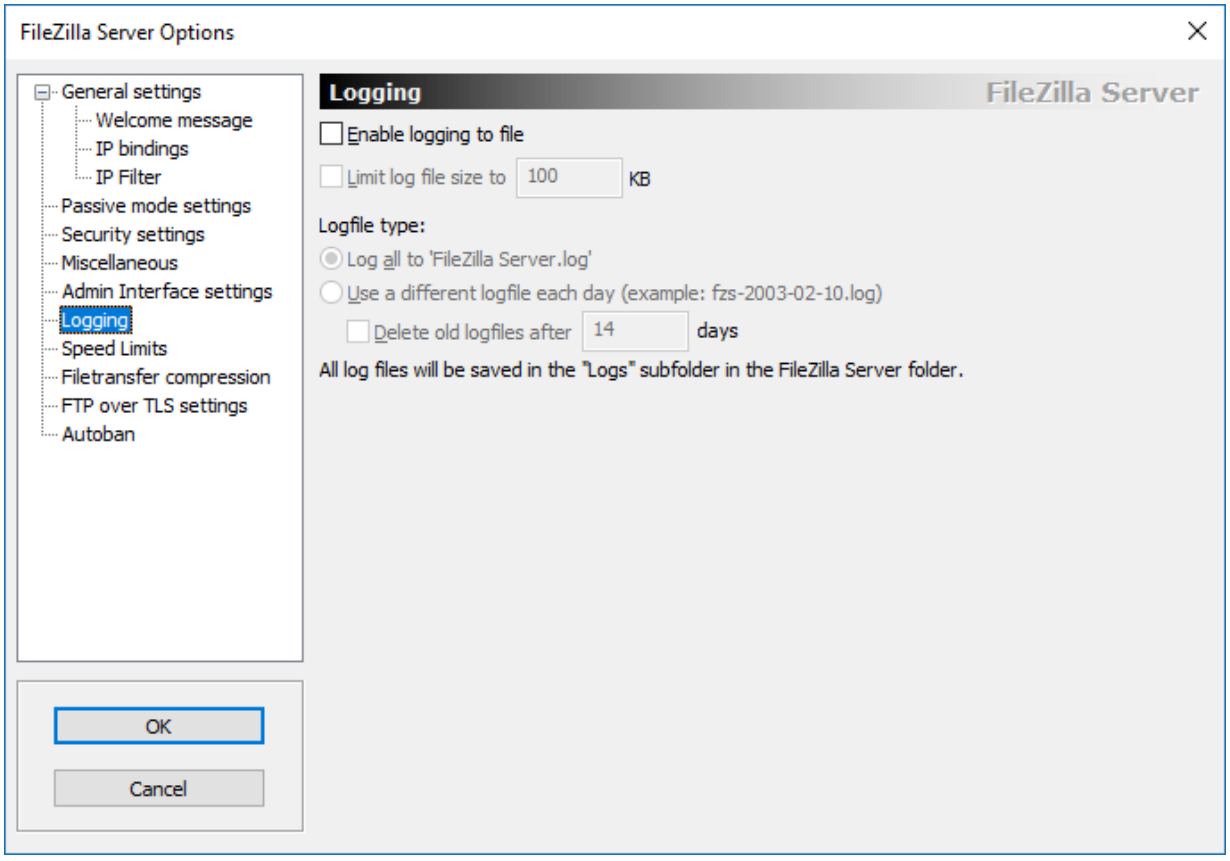
g. У пункті налаштувань «Security Settings» задаються обмеження на вхідні і вихідні з'єднання типу "сервер-сервер". Тут нічого змінювати не варто.
h. Пункт налаштувань «Miscellaneous» містить різні, як правило не суттєві, налаштування FTP-сервера настройки. Наприклад, такі як «Не показувати пароль в лог-файлах» (Don't show passwords in message log), «Запускати інтерфейс згорнутим» (Start minimized), а так само розміри буферів передачі. Змінювати тут, в загальному, нічого не потрібно.



i. На вкладці «Admin Interface Settings» можна задати IP-адресу і порт, за якими буде доступний інтерфейс управління сервером (той самий, який спочатку використовували як localhost чи 127.0.0.1 і 14147). Крім того, можна вказати IP-адреси, яким дозволено підключатися до нього.

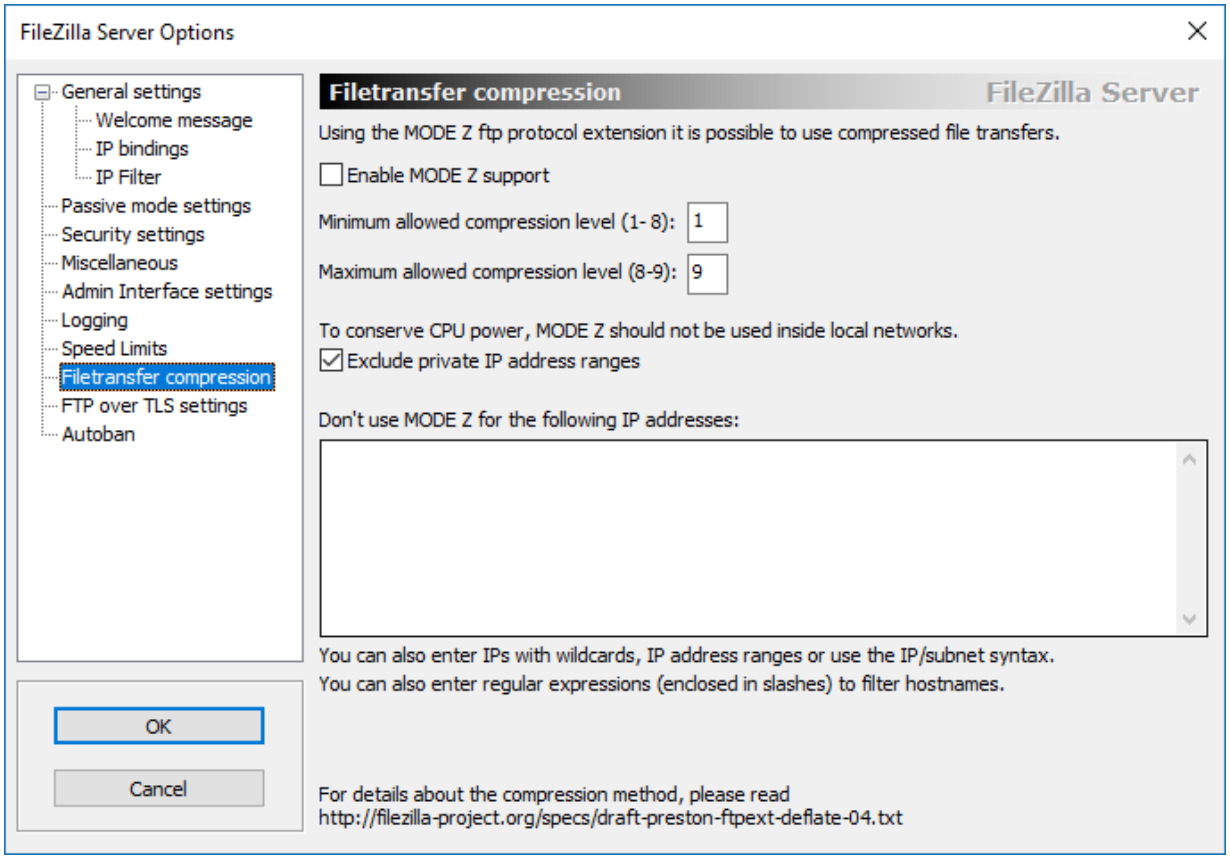


j. Розділ налаштувань «Logging» дозволяє включати запис лог-файлів (Enable logging to file), налаштувати їх максимальний розмір (Limit log file size to), писати все в один файл (Log all to "FileZilla Server.log") або для кожного дня створювати окремий (в цьому випадку можна обмежити їх максимальний термін зберігання).



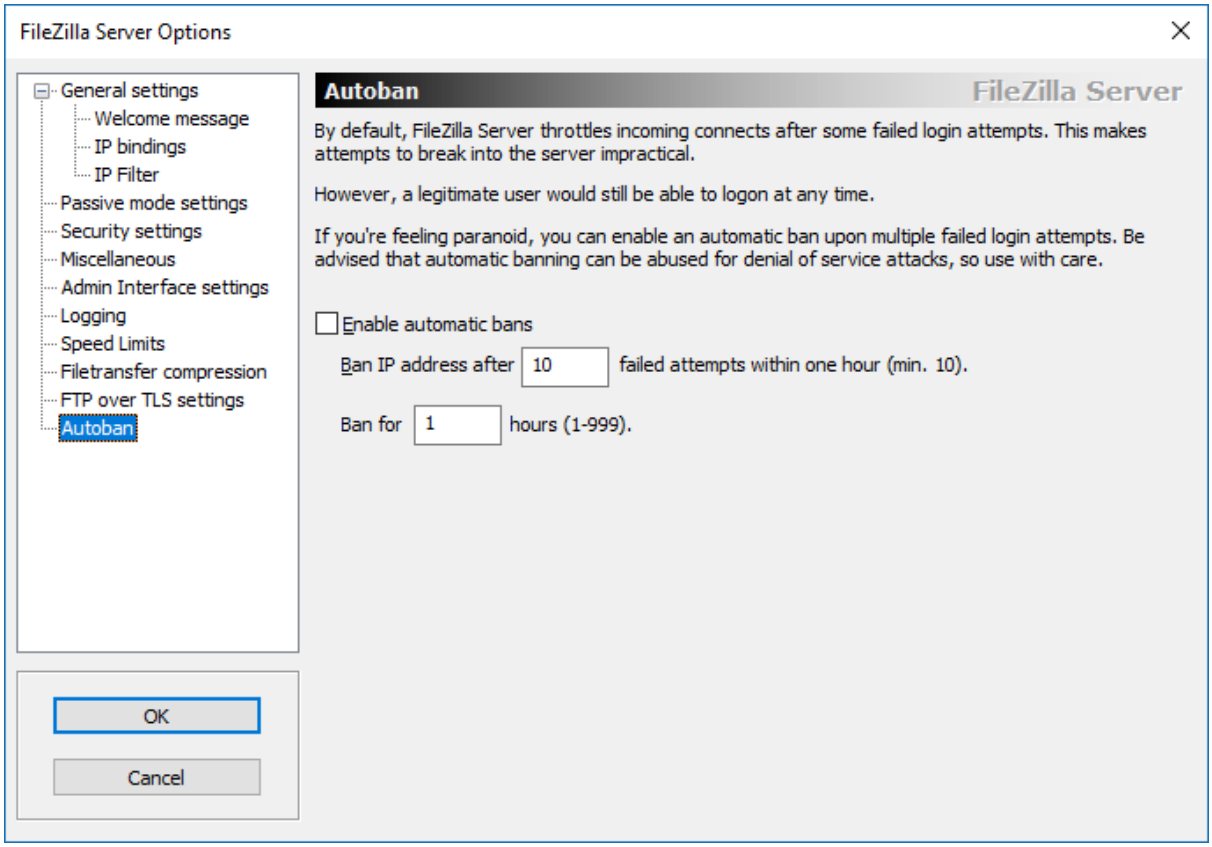
k. Розділ налаштувань «Speed Limits» дозволяє обмежити швидкість вхідних і вихідних з'єднань. Є два шляхи обмеження: задати постійне обмеження на весь час або створити правила на конкретний день і/або годину. Обмеження задаються в кілобайтах.

l. Розділ «Filetransfer compression» дозволяє включити режим стиснення файлів при передачі. При цьому можна налаштувати мінімальний і максимальний рівні стиснення, а також вказати IP-адреси, для яких не буде використовуватися компресія.

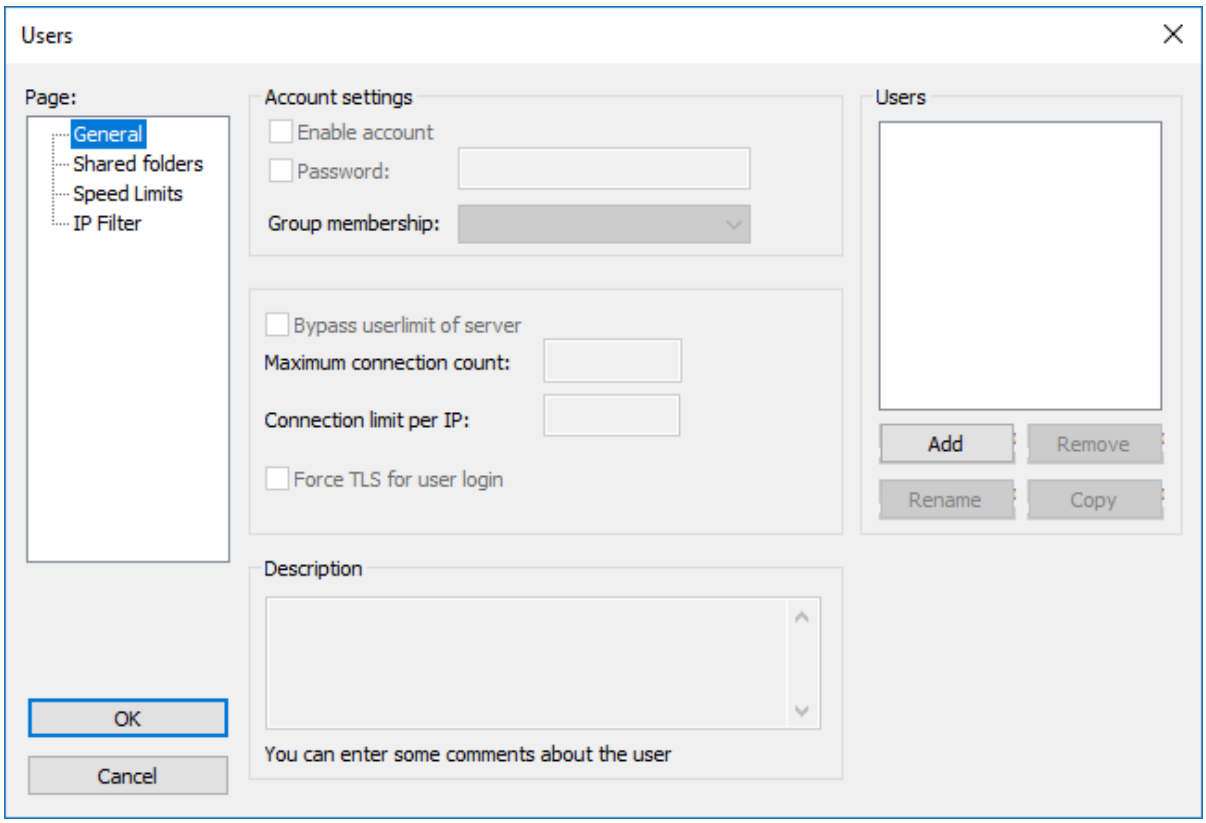


m. У розділі «FTP over TLS setting» можна налаштувати захищене з'єднання між клієнтом і сервером. Для цього потрібно включити підтримку протоколу TLS і вказати шляхи до закритого ключа, файлу сертифікату і пароль.

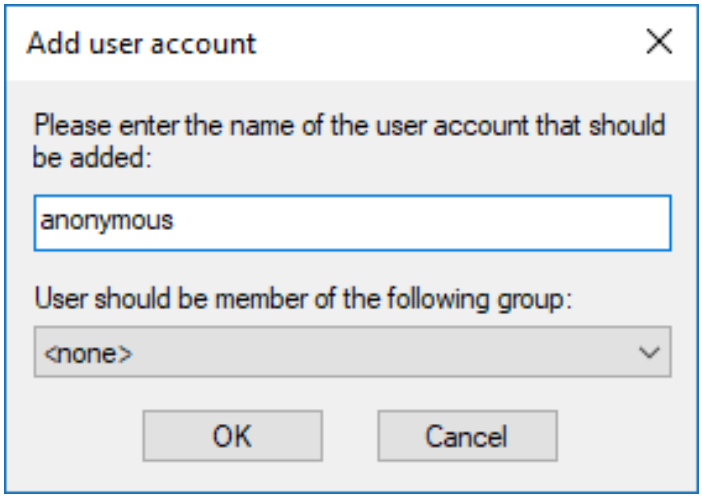
n. У розділі «Autobans» можна включити автоматичне блокування користувачів після n-их спроб невдалих підключень і термін блокування. Для цього потрібно встановити прапорець «Enable automatic bans», вказати в графі "Ban IP adress after" кількість спроб після яких буде здійснюватися блокування, а також час блокування в полі "Ban for ".



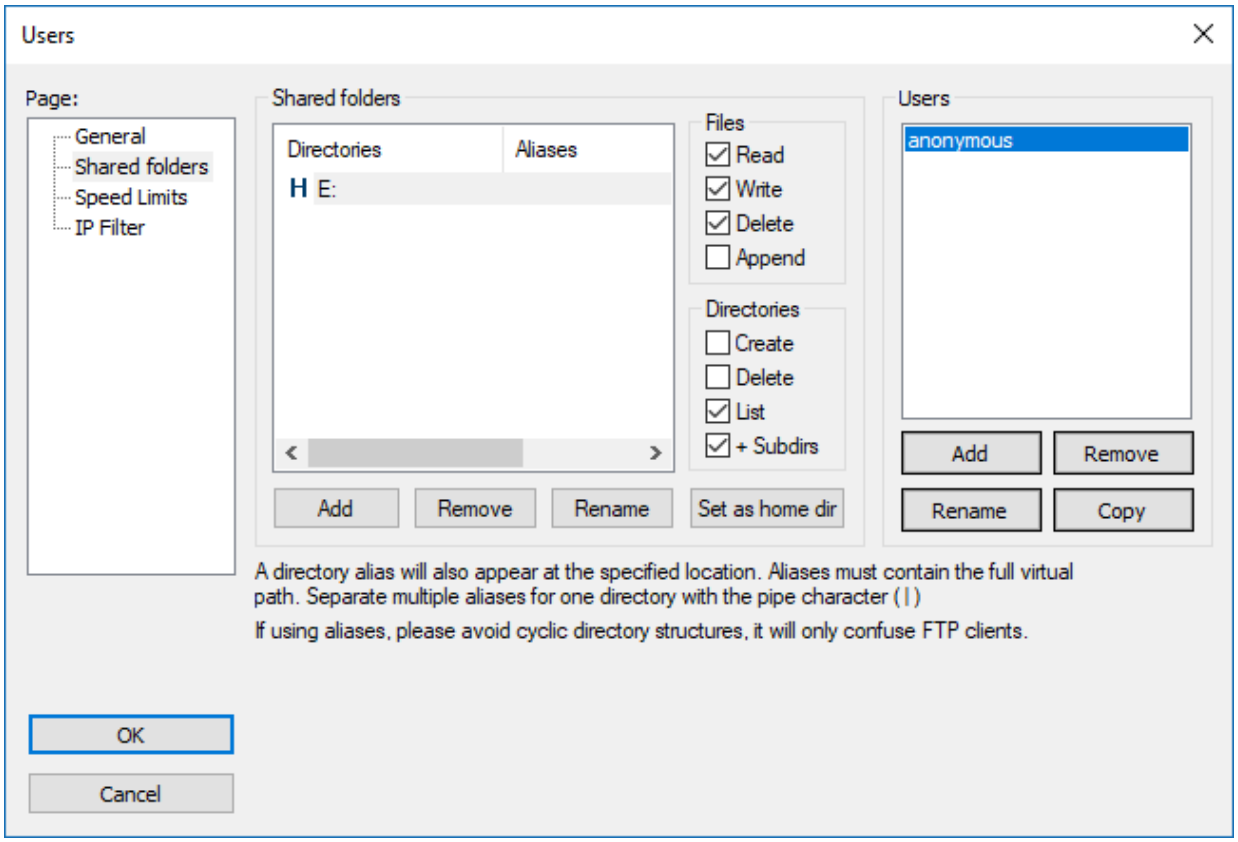
3. **Початкове налаштування акаунтів користувачів (users) і доступів (share)**
   a. Для додавання нового користувача потрібно виконати команду «Edit -> Users». Відкриється відповідне вікно роботи з користувачами.



b. Для додавання нового користувача необхідно натиснути «Add». Далі потрібно буде задати його ім'я, наприклад, anonymous, і приналежність до групи (можна не вказувати). Натиснути «Ok».



c. Далі для даного користувача можна задати пароль і обмеження по кількості з'єднань.
d. Далі у розділі «Share Folders» потрібно задати папки, до яких користувач матиме доступ. Для цього слід натиснути «Add» і вибрати потрібну папку на диску. Зліва можна задати права доступу до неї: тільки читання – «Read», запис – «Write», видалення – «Delete» і можливість зміни існуючих файлів в директорії – «Append». Нижче можна дозволити створення, видалення, отримання списку файлів і поширення дозволів на підкаталоги.



е. Після задання необхідних параметрів натисніть «Ок». На цьому налаштування сервера FTP завершено.

Для того, щоб інші користувачі могли використовувати даний FTP сервер, необхідно надати їм його IP-адресу, а також задані логін(и), пароль(і) і, при необхідності, порт (якщо змінювали), які вони повинні вказати в своєму, попередньо встановленому FTP-клієнті.

4. Показати результати викладачу.
5. Оформити звіт по виконаній роботі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Микитишин А.Г. Комп'ютерні мережі. Книга 1.: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: «Магнолія 2006». 2013. – 256 с.
2. Микитишин А.Г. Комп'ютерні мережі. Книга 2.: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: «Магнолія 2006». 2013. – 328 с.
3. Микитишин А.Г. Телекомунікаційні системи та мережі / Микитишин А.Г., Митник М.М., Стухляк. П.Д. – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 384 с.
4. Микитишин А.Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с.
5. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1 / Буров Є.В., Митник М.М.; За заг. ред. Пасічника В.В. – Львів: «Магнолія 2006». 2019. – 334 с.
6. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі: Підручник для вищих навчальних закладів. – К.: САММІТ-КНИГА, 2010. – 640 с.
7. ISO/IEC 11801 Information technology – Generic cabling for customer premises – Edition 2. 2.
8. EN 50173– Information Technology – Generic cabling systems.
9. TIA/EIA–568–C Commercial Building Telecommunications Cabling Standard.
10. ISO/IEC TR 14763–2. Information technology – Implementation and operation of customer premises cabling – Part 2: Planning and installation.
11. ISO/IEC 14763–1 Information technology – Implementation and operation of customer premises cabling – Part 1: Administration.
12. Barry J Elliott Designing a structured cabling system to ISO 11801 2nd edition 2002, Published by Wood head Publishing Limited, Abington Hall, Abington Cambridge, England.