

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМ.
ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ ПРИКЛАДНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА
ЕЛЕКТРОІНЖЕНЕРІЇ
КАФЕДРА КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ

Микитишин А.Г.

МЕТОДИЧНІ ВКАЗІВКИ

для виконання лабораторних робіт
з дисципліни

КОМП'ЮТЕРНІ МЕРЕЖІ

Частина 2

(лабораторні роботи №6-№9)

для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані
технології»

Тернопіль
2019

Методичні вказівки до лабораторних робіт з курсу «Комп'ютерні мережі». Частина 2 (лабораторні роботи №6-№9). Для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» / А.Г. Микитишин. – Тернопіль: ТНТУ, 2019. – 26 с.

Рецензент: д.т.н., професор Лупенко С.А.

Відповідальний за випуск: к.т.н., доцент Микитишин А.Г.

Методичні вказівки розглянуто і схвалено на засіданні кафедри комп'ютерно-інтегрованих технологій (протокол №1 від 27.08.2019 р.)

Схвалено та рекомендовано до друку Вченою Радою факультету прикладних інформаційних технологій та електроінженерії (протокол №1 від 28.08.2019 р.)

Методичні вказівки призначені для проведення лабораторних робіт дисципліни «Комп'ютерні мережі» для студентів, які навчаються за спеціальністю 151 – «Автоматизація та комп'ютерно-інтегровані технології». 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.

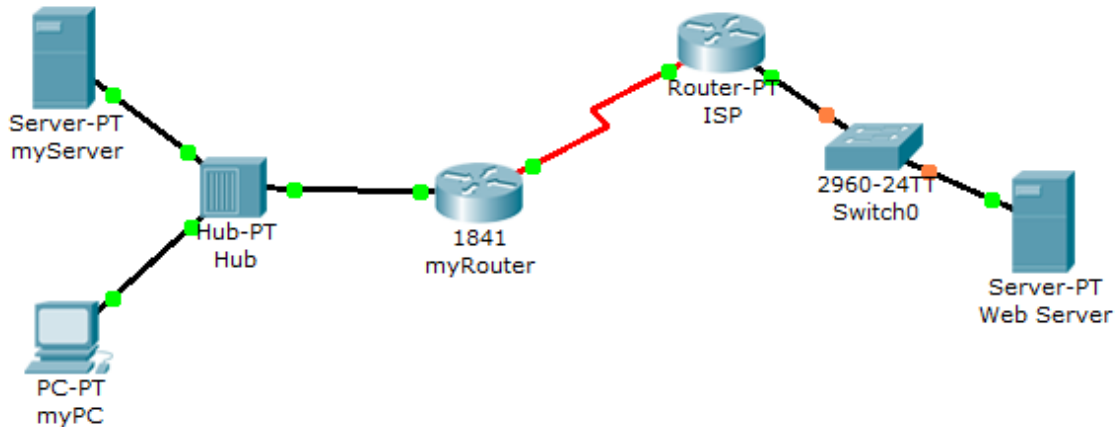
ЗМІСТ

ЛАБОРАТОРНА РОБОТА №6. Обмін даними між пристроями різних підмереж	4
ЛАБОРАТОРНА РОБОТА №7. Перегляд інформації в PDU, що проходять між клієнтом та сервером	6
ЛАБОРАТОРНА РОБОТА №8. Налаштування служби DNS	8
ЛАБОРАТОРНА РОБОТА №9. Налаштування протоколу FTP	15
РЕКОМЕНДОВАНА ЛІТЕРАТУРА	26

ЛАБОРАТОРНА РОБОТА №6

Обмін даними між пристроями різних підмереж

Мета роботи: Ознайомитись із взаємодією мережевих пристроїв із різних підмереж для обміну ресурсами.



Топологія мережі

В даній лабораторній роботі описується процес налаштування пристроїв у різних підмережах з метою їх взаємодії між собою. Важливо використовувати правильні IP-адреси пристроїв і маршрутизаторів, які з'єднують підмережі.

Крок 1: Перевірка можливості під'єднання myPC до myServer та myRouter

1. З командного рядка **myPC** відправте **ping 192.168.1.45** на **myServer** та **ping 192.168.1.33** на **myRouter**. Чи виявилися спроби відправки ехо-запитів успішними?
2. В PacketTracer, за допомогою миші (навівши вказівник на потрібний пристрій), ознайомтесь з інформацією про мережеву конфігурацію кожного пристрою (**myPC**, **myServer** та **myRouter**).
3. Запишіть IP-адресу і маску підмережі кожного пристрою в таблицю

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	IP-адреса підмережі
myPC	FastEthernet			
myServer	FastEthernet			
myRouter	FastEthernet0/0			

4. Визначте, знаходяться пристрої в одній чи різних підмережах.

Крок 2: Налаштування мережі для доступу до myServer

1. В закладці **Config (Налаштування) myPC** призначте необхідну IP-адресу для **myPC**, так щоб він знаходився в одній підмережі з інтерфейсом FastEthernet0/0 маршрутизатора **myRouter** та сервером **myServer**.

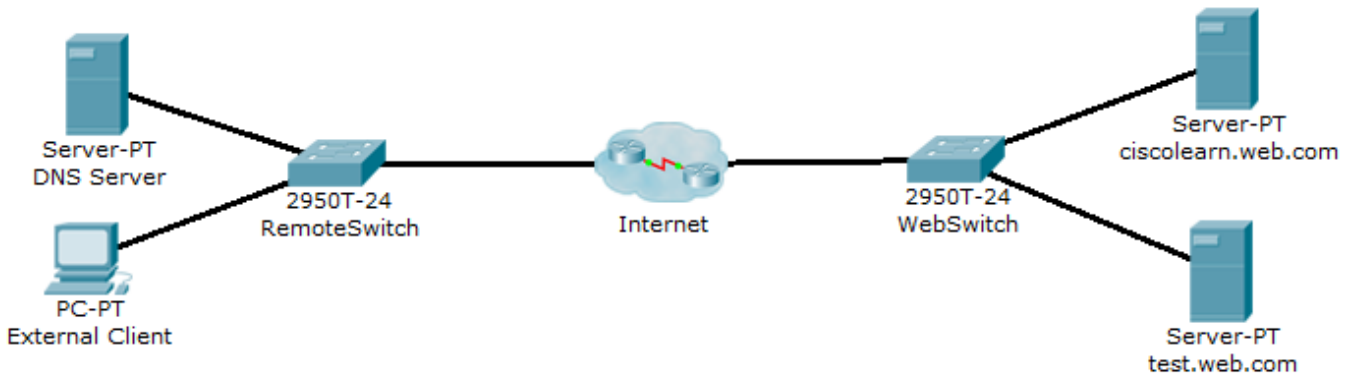
Крок 3: Перевірка під'єднання

1. Після заміни IP-адреси на **myPC** відправити **ping 192.168.1.45** на **myServer** і **ping 192.168.1.33** на **myRouter**. (Відправка echo-запиту повинна бути успішною).

ЛАБОРАТОРНА РОБОТА №7

Перегляд інформації в PDU, що проходять між клієнтом та сервером

Мета роботи: Перегляд трафіку, що надходить від клієнта до серверу при запиті до веб-служб.



Топологія мережі

Крок 1: Перегляд трафіку між клієнтом і веб-сервером

1. Увійдіть у режим моделювання, клацнувши вкладку **Simulation** у правому нижньому куті. Вона знаходиться поруч з вкладкою **Realtime** і позначена символом таймера.
2. Перевірте трафік, створивши складний PDU в режимі моделювання:
 - 2.1. Натисніть кнопку **Edit Filters** і поставте прапорці лише у полях TCP та HTTP.
 - 2.2. Натисніть кнопку **Add Complex PDU** (Додати складний PDU), клацнувши відкритий конверт, який знаходиться над позначкою режиму моделювання.
 - 2.3. Клацніть на ПК **External Client**, зробивши його його відправником пакетів.
3. Вкажіть налаштування **Complex PDU**, змінивши у вікні **Create Complex PDU** (Створення складного PDU) наступні налаштування:
 - 3.1. Розділ **PDU Settings > Select Application**: встановіть **HTTP**.
 - 3.2. Клацніть на сервері **ciscolearn.web.com** і його IP-адреса з'явиться в полі **Destination IP address** (IP адрес отримувача).
 - 3.3. У розділі **Source Port** (Порт джерела) введіть **1000**.
 - 3.4. У розділі **Simulation Settings** (Налаштування моделювання) виберіть **Periodic Interval** (Періодичний інтервал) і введіть **120** секунд.

3.5. Створіть PDU, клацнувши на кнопці **Create PDU** у вікні **Create Complex PDU**.

4. Прослідкуйте за трафіком, натиснувши кнопку **Auto Capture/Play (Автозахват/відтворення)** на панелі моделювання. Можна пришвидшити показ переміщення пакетів за допомогою повзунка відтворення. Показ переміщення трафіку буде тривати аж до повного заповнення буферу, про що буде повідомлено за допомогою спливаючого вікна **Buffer Full**. Зупинити показ переміщення пакетів **PDU** можна також клацнувши на кнопці **Auto Capture/Play**.

Крок 2: Перегляд заголовків пакетів, що переміщаються по мережі

Перевірте заголовки пакетів, якими обмінюються клієнт і сервер.

1. Відкрийте панель моделювання та двічі клацніть на будь-якому рядку у вікні **Event List (Список подій)**. У робочій області відобразиться конверт, що відповідає цьому рядку.
2. Клацніть на значок у вигляді конверта в робочій області, щоб переглянути інформацію про пакет і заголовок.
3. У вікні **OSI Model** відображається, на якому рівні OSI моделі обробляється даний пакет.

Зверніть увагу, що рівень може бути вищим або нижчим, залежно від пристрою, який обробляє даний пакет. Комутатор відображає пакет тільки до рівня 2, маршрутизатор (хмара) – до 3, а комп'ютер або сервер відображає пакет до рівня 4.

4. Прочитайте опис пакету у вікні **OSI Model**.
5. Виберіть вкладку **Inbound PDU Details** або **Outbound PDU Details** та перегляньте дані по відправленому пакеті.

Зверніть увагу на MAC-адреса в кадрі, IP-адреса в пакеті і номери портів відправника та отримувача в сегменті.

6. Клацніть інші рядки списку подій і перегляньте їх опис.

Питання для повторення.

1. Запишіть MAC-адресу, IP-адресу відправника веб-запиту.
2. Запишіть MAC-адресу, IP-адресу адресата веб-запиту.
3. Які протоколи прикладного, транспортного та мережевого рівнів використовуються у відправлених веб-запитах?
4. Яку адресу порта транспортного рівня використано відправником у веб-запиті?

ЛАБОРАТОРНА РОБОТА №8

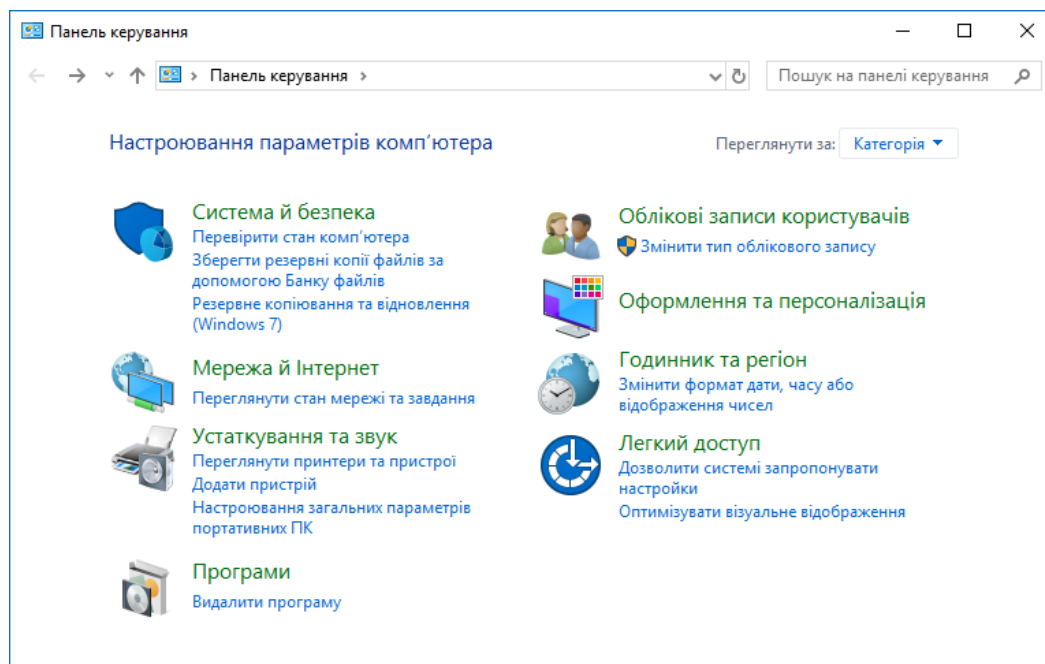
Налаштування служби DNS.

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

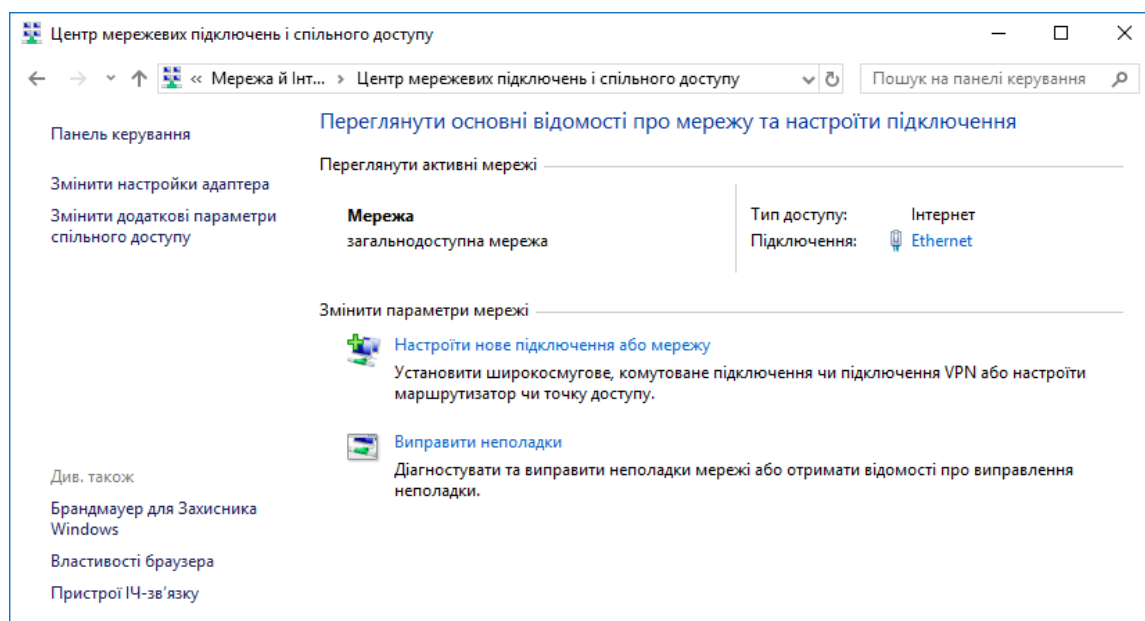
Порядок виконання роботи.

Крок 1: Включення служби DNS в операційній системі Windows 10:

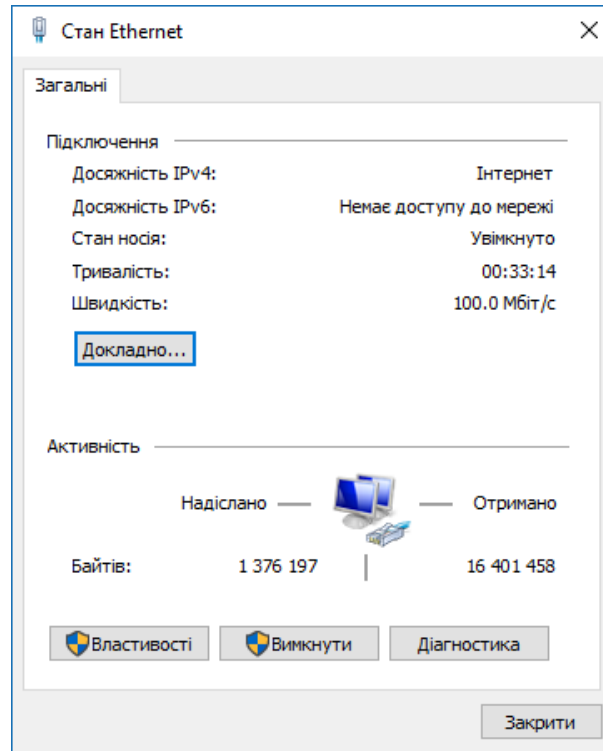
1.1. Відкрийте «Панель управління» і у ній виберіть пункт «Мережа й Інтернет».



1.2. Далі виберіть пункт «Переглянути стан мережі та завдання».

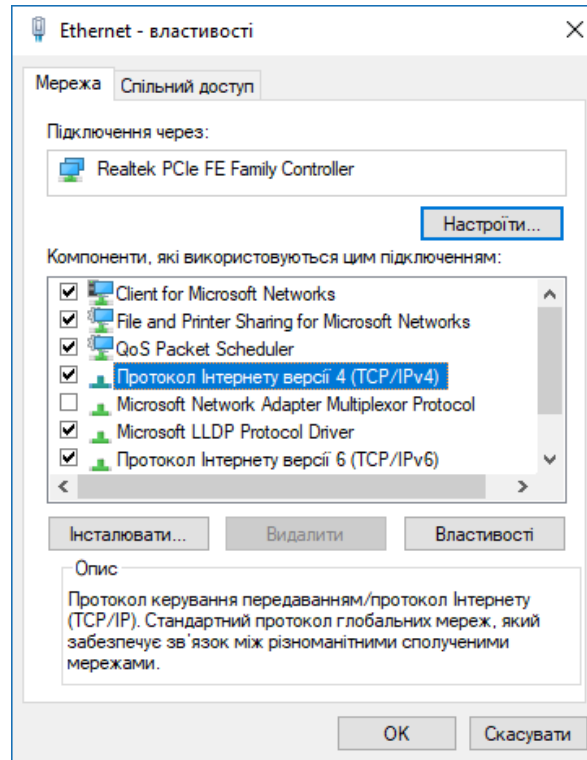


- 1.3. В розділі «Переглянути активні мережі» виберіть підключення, завдяки якому здійснюється доступ до Інтернету (те, що стоїть після «Підключення», Ethernet), і натисніть на нього.
- 1.4. Відкриється нове вікно «Стан Ethernet», в якому відображаються всі налаштування обраного підключення.

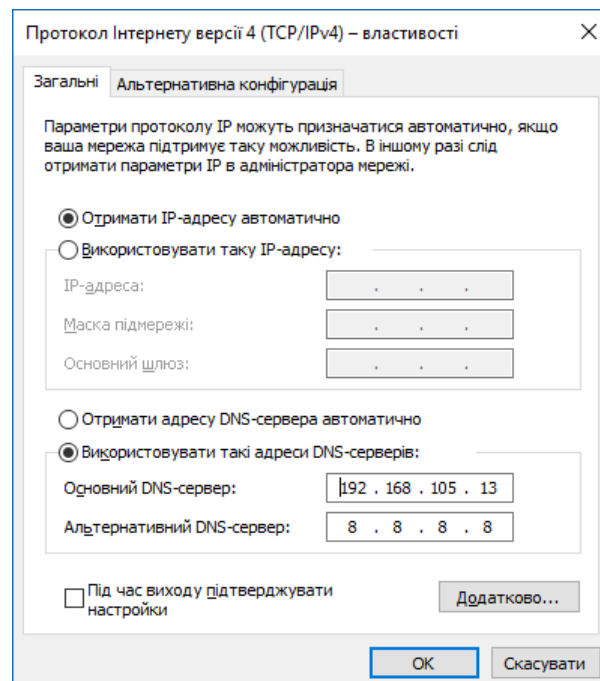


Слід натиснути кнопку «Властивості».

- 1.5. 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.



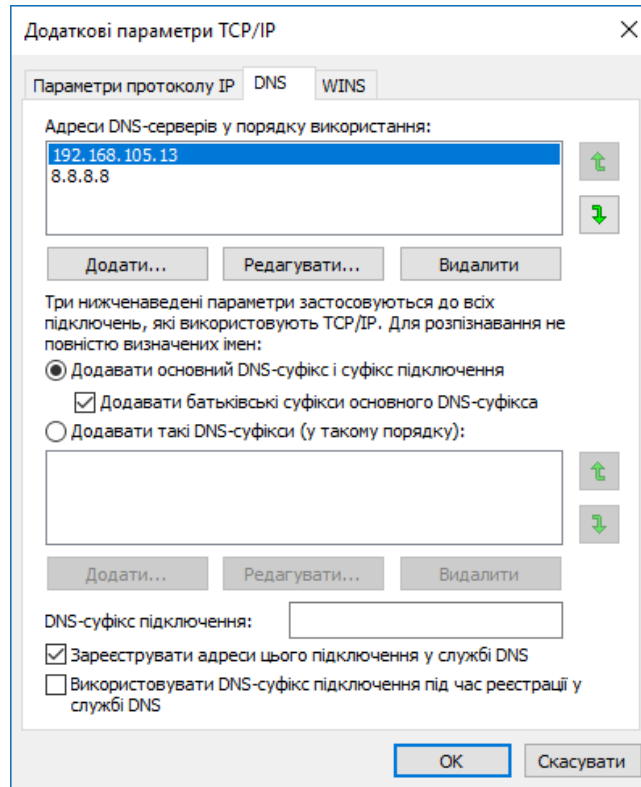
- 1.6. Активуйте пункт «Використовувати такі адреси DNS-серверів» і наберіть в текстовому полі адреса вашого сервера і додатковий, якщо перший виявиться неактивним (8.8.8.8 – публічний DNS-сервер Google).



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

Крок 2: Налаштування або зміна DNS-сервера:

- 1.1. Виконайте пункти 1-5 включення DNS.
- 1.2. Замість введення IP-адрес (які вже є) натисніть на кнопку «Додатково». У новому вікні «Додаткові параметри TCP/IP» перейдіть на вкладку DNS.



- 1.3. 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.

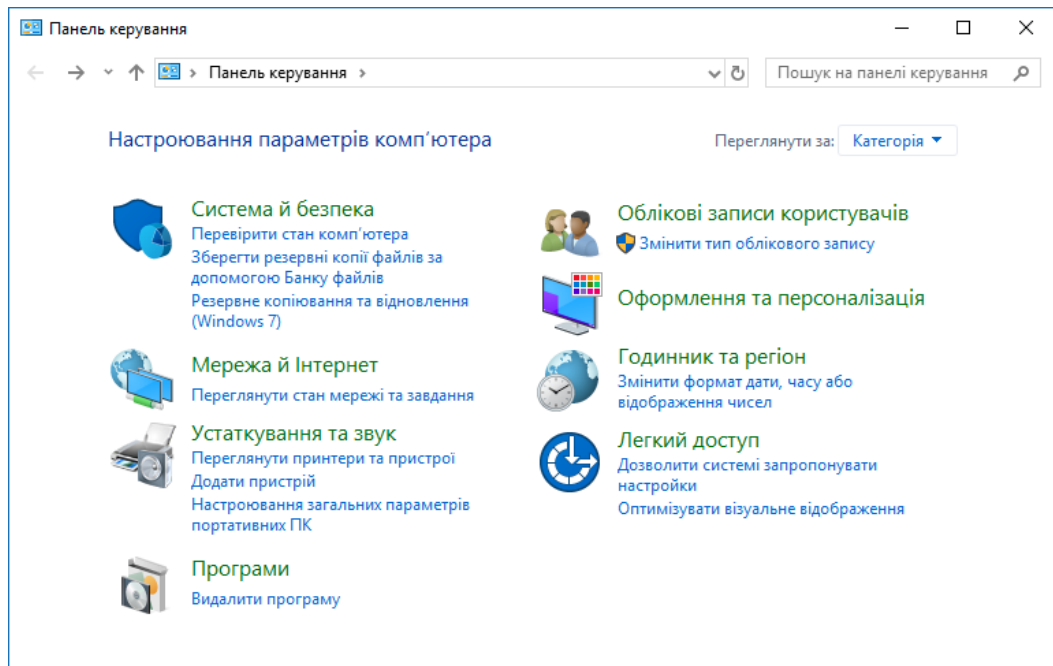
Включене налаштування «Зареєструвати адреси цього підключення в DNS» означає, що ваш комп'ютер буде зареєстрований на сервері зі своєю адресою та назвою пристрою, прописаного в налаштуваннях. Дізнатися назву вашого пристрою, можна в «Панелі управління» в пункті «Система».

Включений пункт «Використовувати DNS-суфікс підключення під час реєстрації у службі DNS» приєднає до імені вашого комп'ютера в мережі додатковий суфікс.

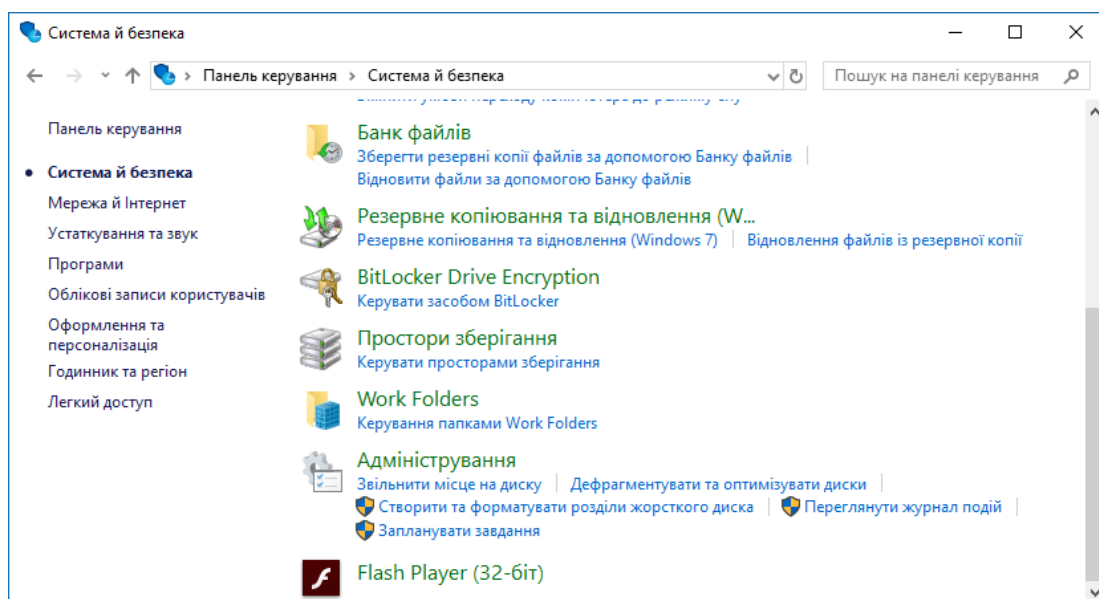
Крок 3: Усунення несправностей при роботі служби DNS

Необхідно перевірити налаштування системних служб, для цього потрібно:

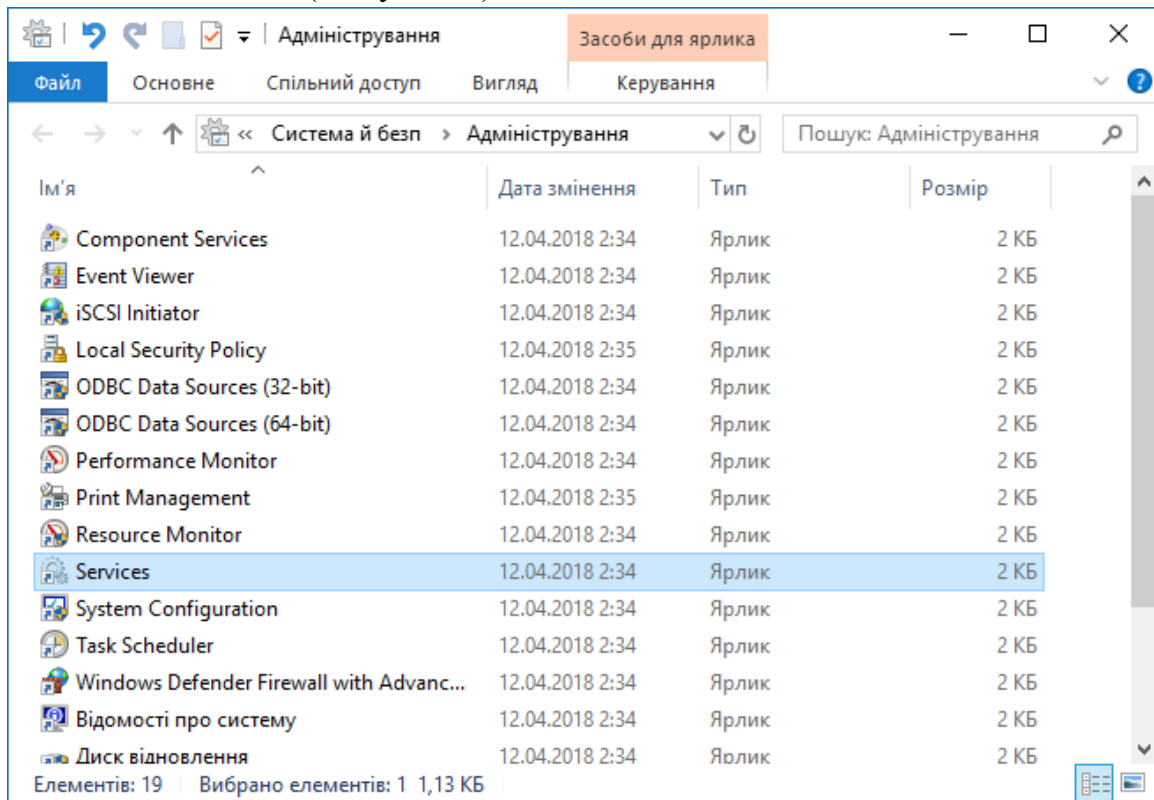
- 1.1. Відкрити «Панель управління» і у ній вибрати пункт «Система й безпека».



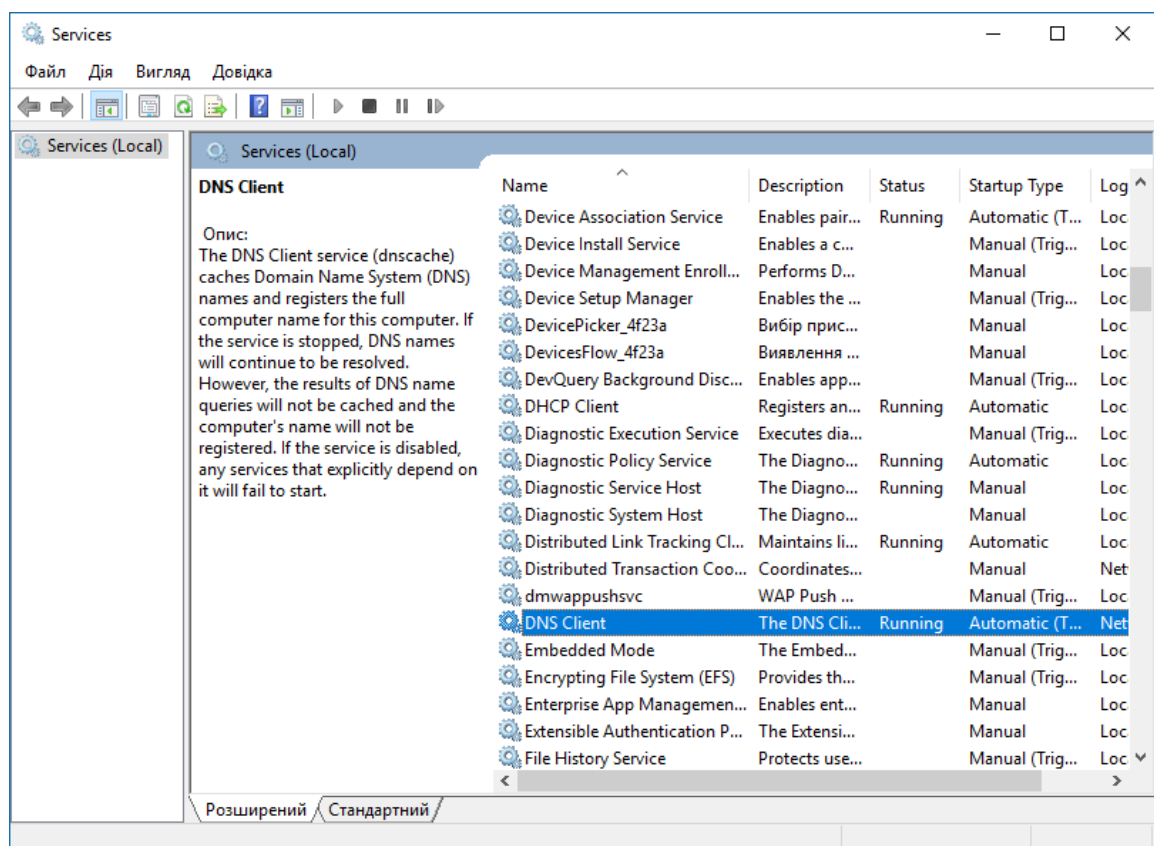
- 1.2. У наступному вікні натисніть на «Адміністрування».



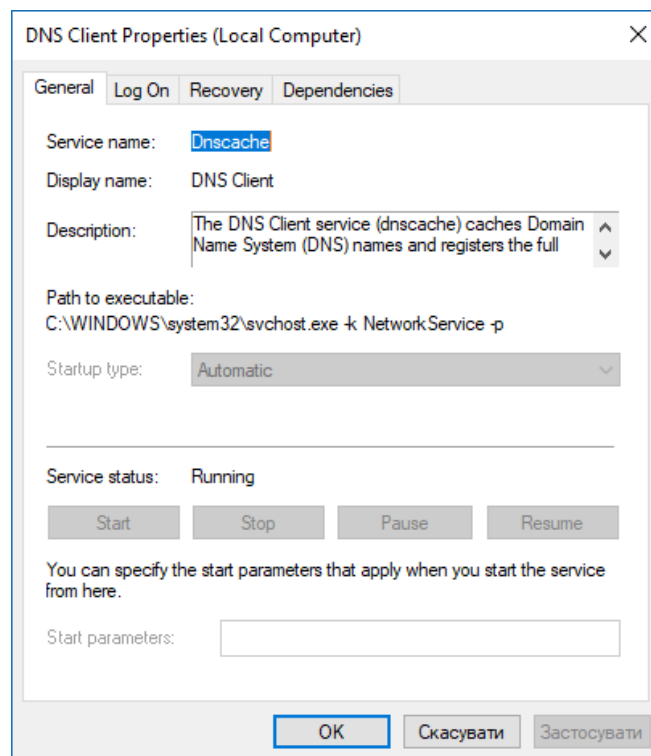
1.3. Відкриється список всіх доступних програм, виберіть пункт «Services» («Служби»).



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



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



- 1.6. Після внесених змін необхідно натиснути «Ок».

ЛАБОРАТОРНА РОБОТА №9

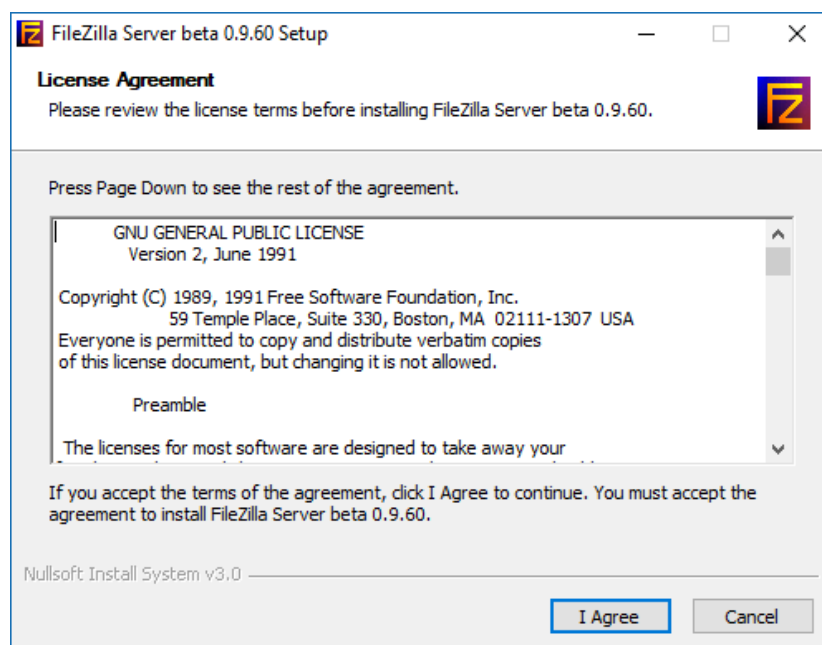
Налаштування протоколу FTP

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

Порядок виконання роботи.

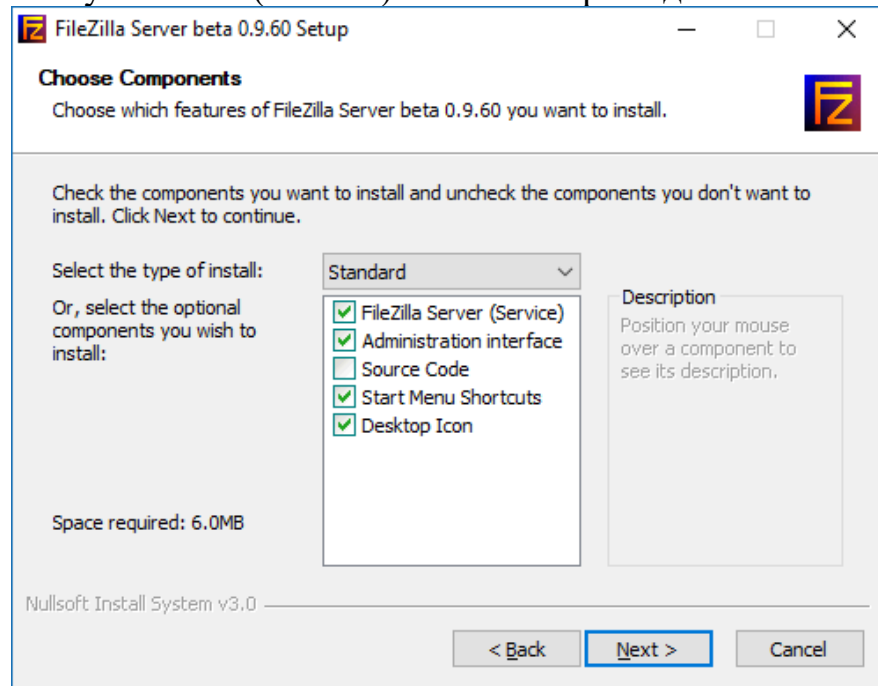
Крок 1: Встановлення FTP сервера:

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



- 1.3. 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 файлоховищем з іншого комп'ютера.
 - Інтерфейс управління (Interface only) - на відміну від попереднього пункту, ставиться тільки графічна оболонка керування сервером, але не він сам.

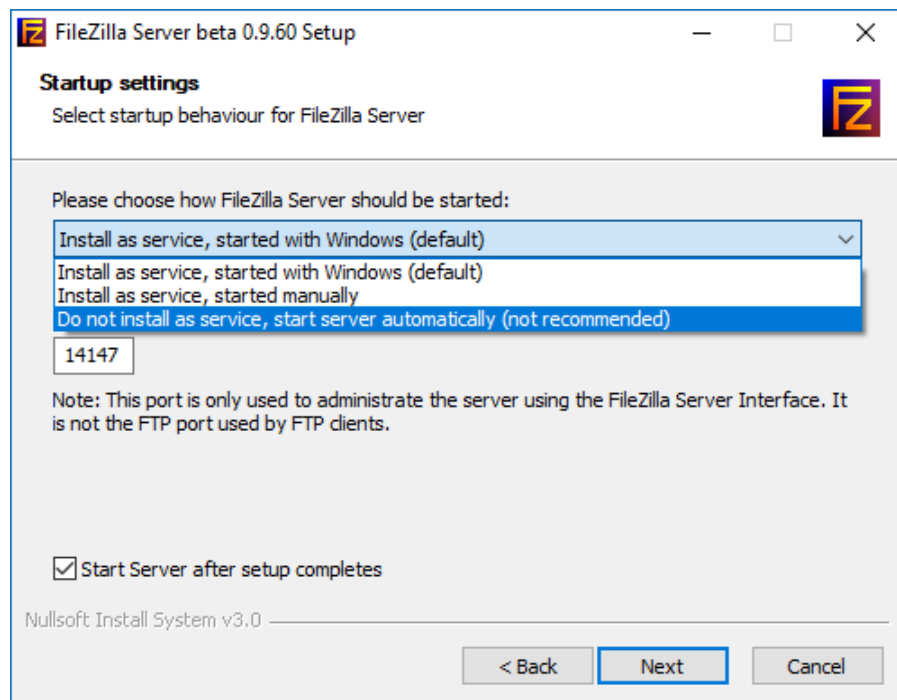
- Вибіркова установка (Custom) – можна обрати довільні компоненти.



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).

- 1.4. На наступному кроці необхідно обрати спосіб установки і запуску сервера.



Є три варіанти запуску FTP-сервера:

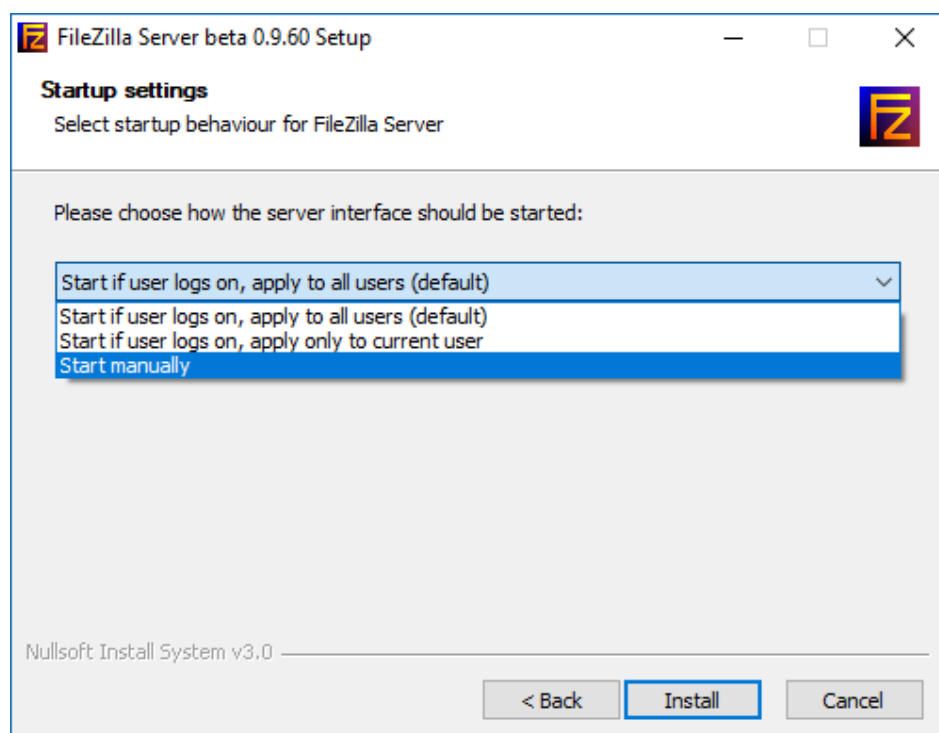
- Як службу і запускати при вході в систему (Install as service, started with Windows (default));
- Як службу і запускати вручну (Install as service, started manually);
- Проста установка, запускати вручну (Do not install as service, start server automatically).

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».

1.5. 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.

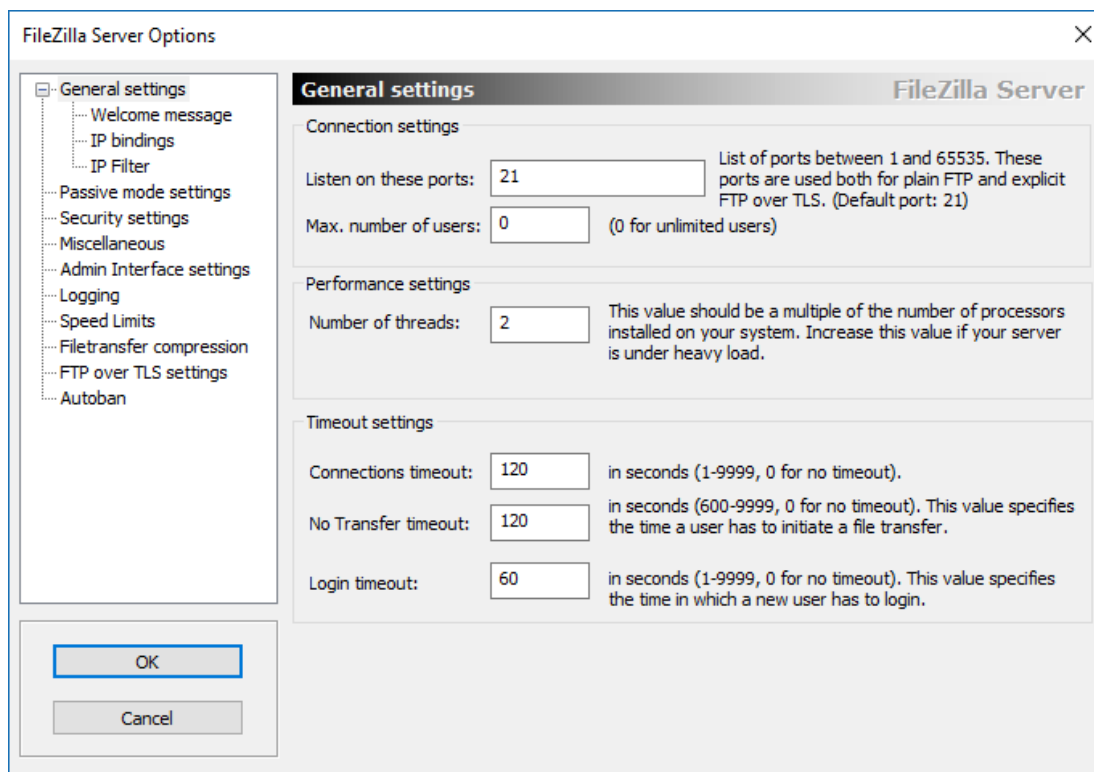
Для початку установки сервера слід натиснути кнопку «Install».

Крок 2: Налаштування FTP FileZilla Server

- 1.1. Після установки, при першому запуску інтерфейсу, з'явиться вікно, де потрібно вказати адресу і порт для підключення, а так само пароль адміністратора (при першій установці 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.

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

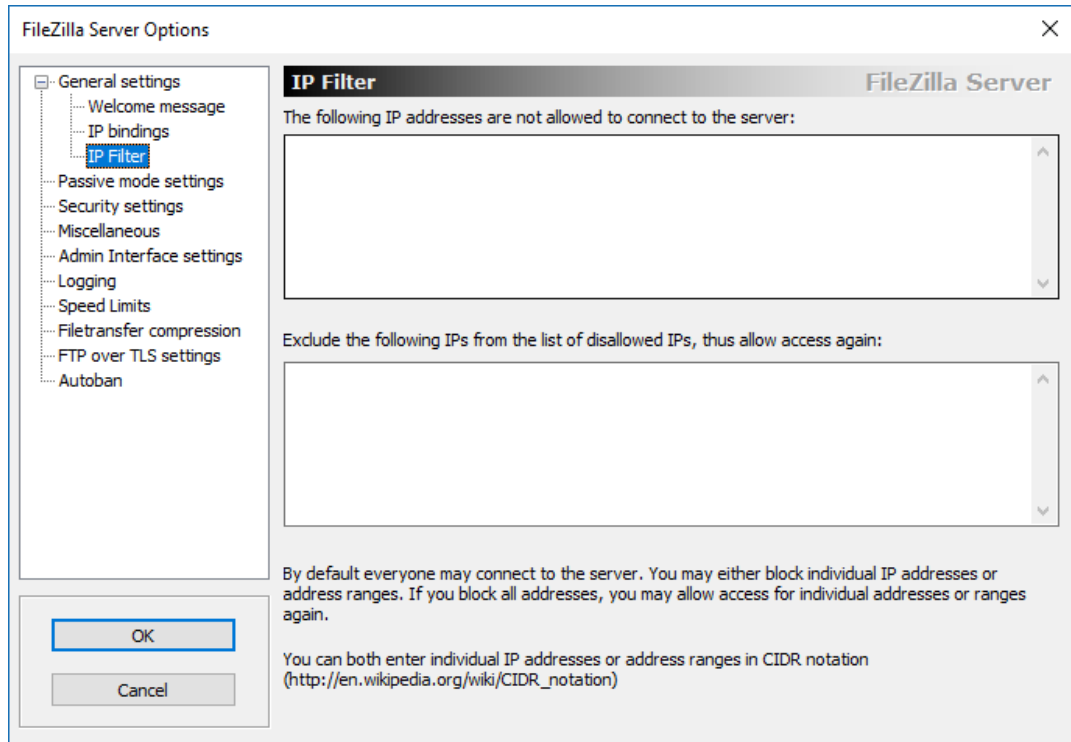


- Порт, за яким клієнти будуть підключатися до сервера (Listen on these ports), за замовчуванням 21 порт;
- Максимальна кількість клієнтів (Max. number of users), за замовчуванням встановлено значення «0», це означаючи, що кількість клієнтів не обмежена.

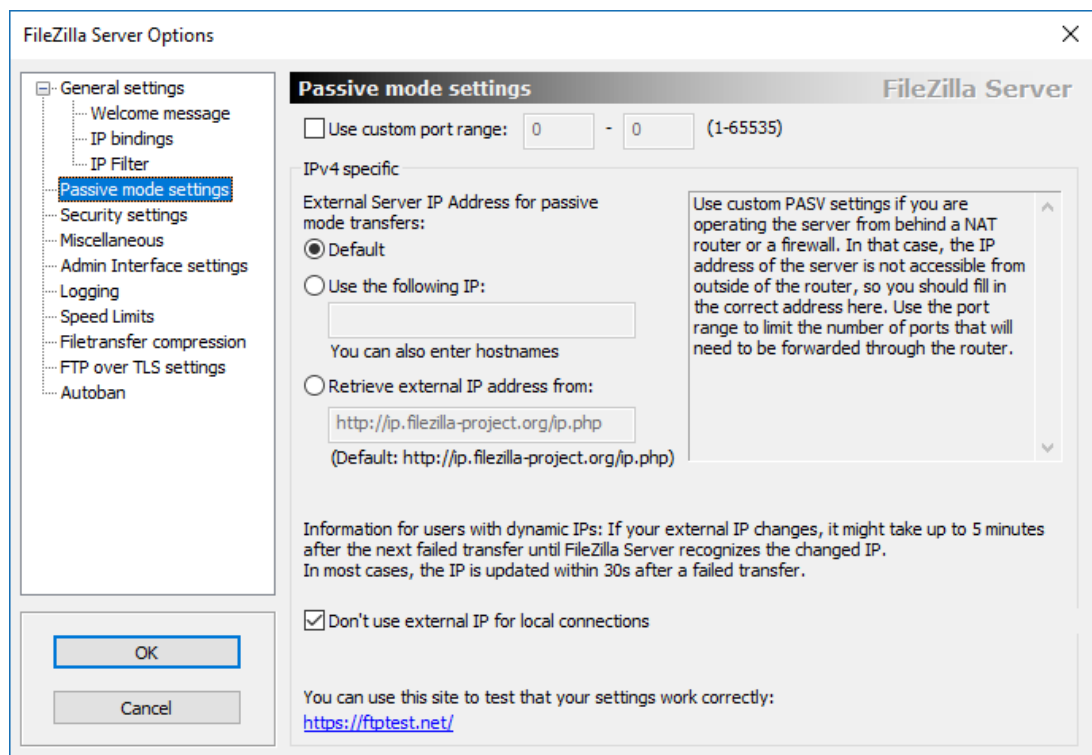
Інші параметри (Кількість потоків (Number of threads) та налаштування тайм-аутів (Timeout setting), як правило, залишають без змін.

- 1.3. У наступному підпункті (Welcome message) можна налаштувати вітальне повідомлення, яке будуть бачити користувачі при підключенні.
- 1.4. 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.
- 1.5. 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»).



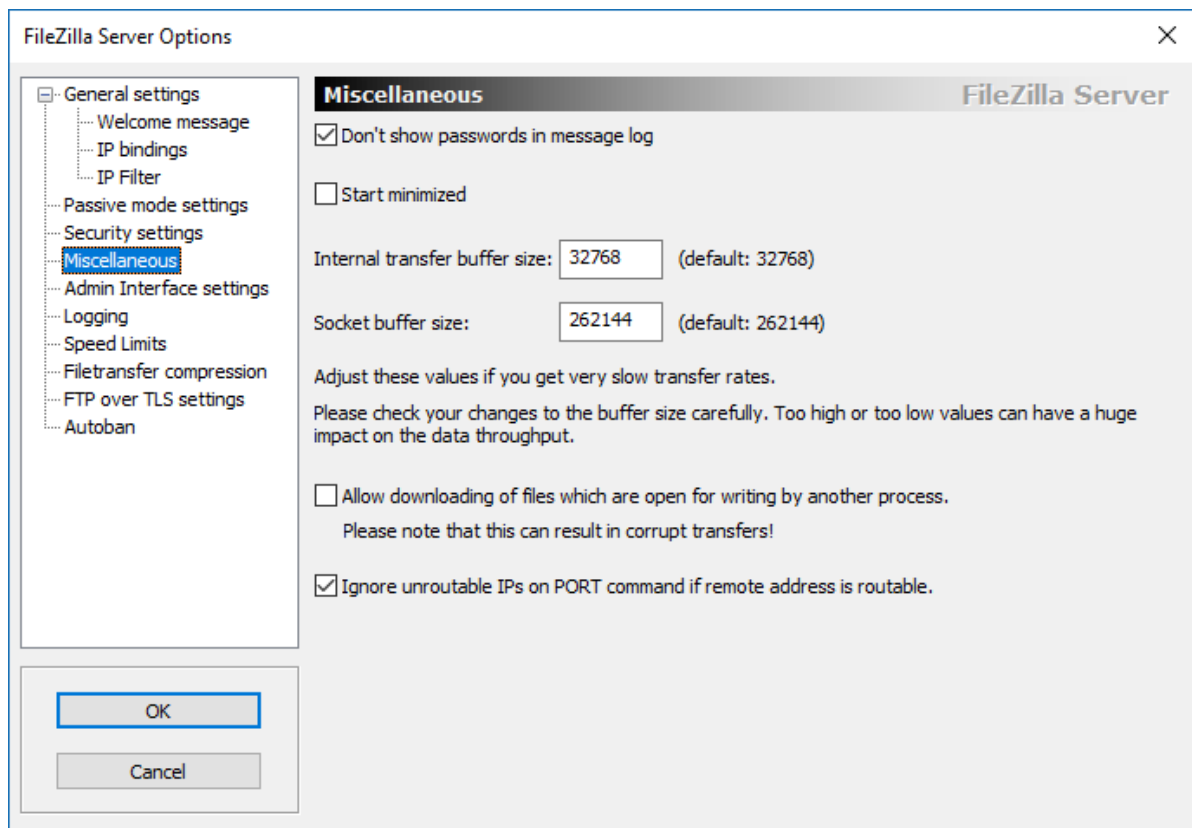
1.6. Вкладка «Passive mode settings» регламентує параметри для пасивного підключення до сервера.



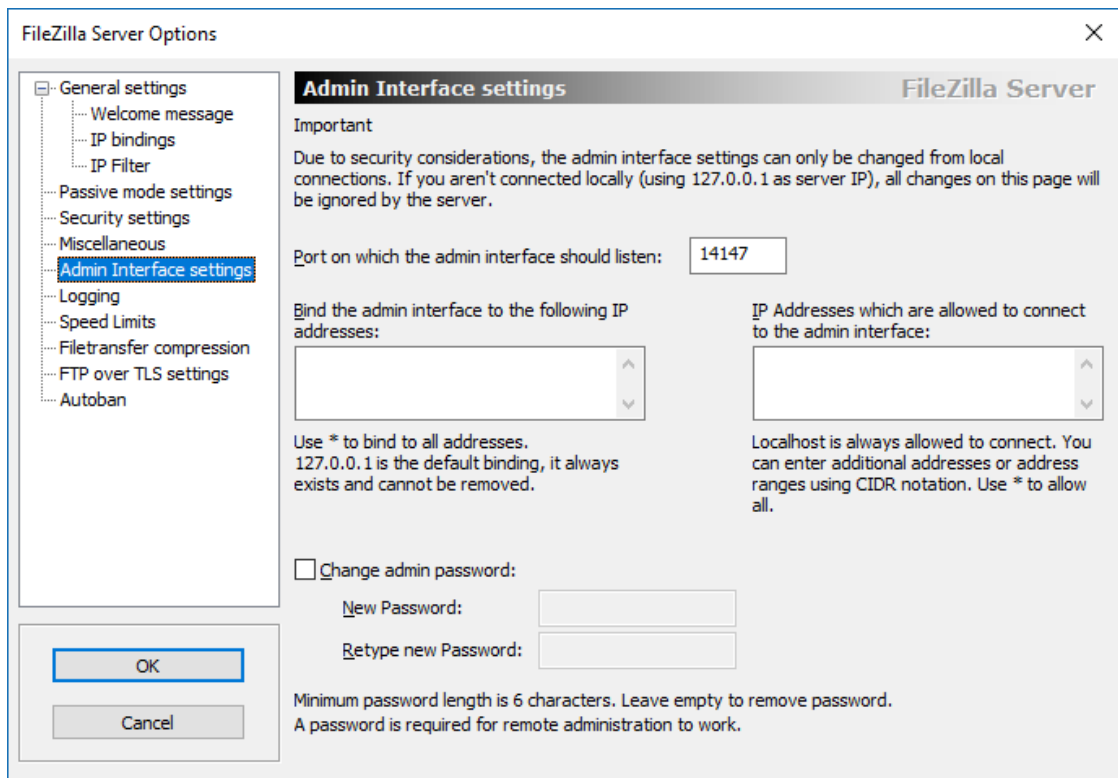
Змінювати налаштування на даній вкладці варто лише в тому випадку, якщо підключення до Інтернету здійснюється через NAT або проксі-сервер.

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 підключитися до даного FTP сервера в пасивному режимі.

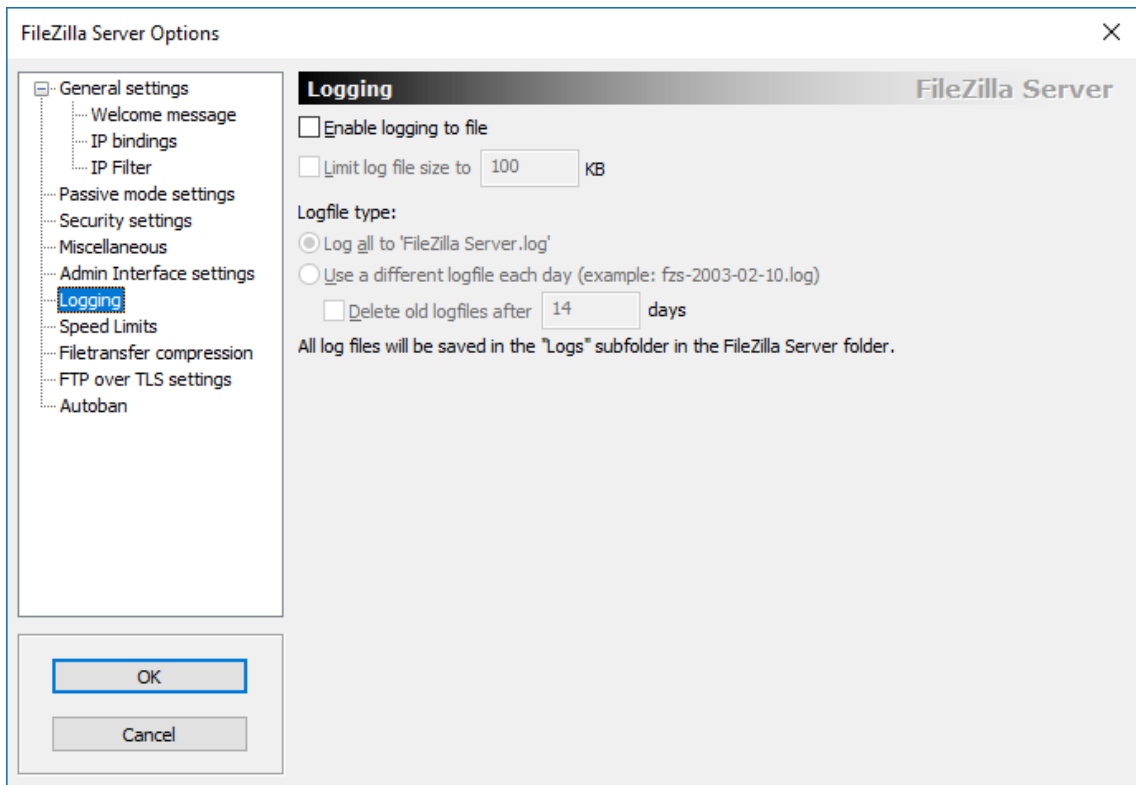
- 1.7. У пункті налаштувань «Security Settings» задаються обмеження на вхідні і вихідні з'єднання типу "сервер-сервер". Тут нічого змінювати не варто.
- 1.8. Пункт налаштувань «Miscellaneous» містить різні, як правило не суттєві, налаштування FTP-сервера настройки. Наприклад, такі як «Не показувати пароль 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.



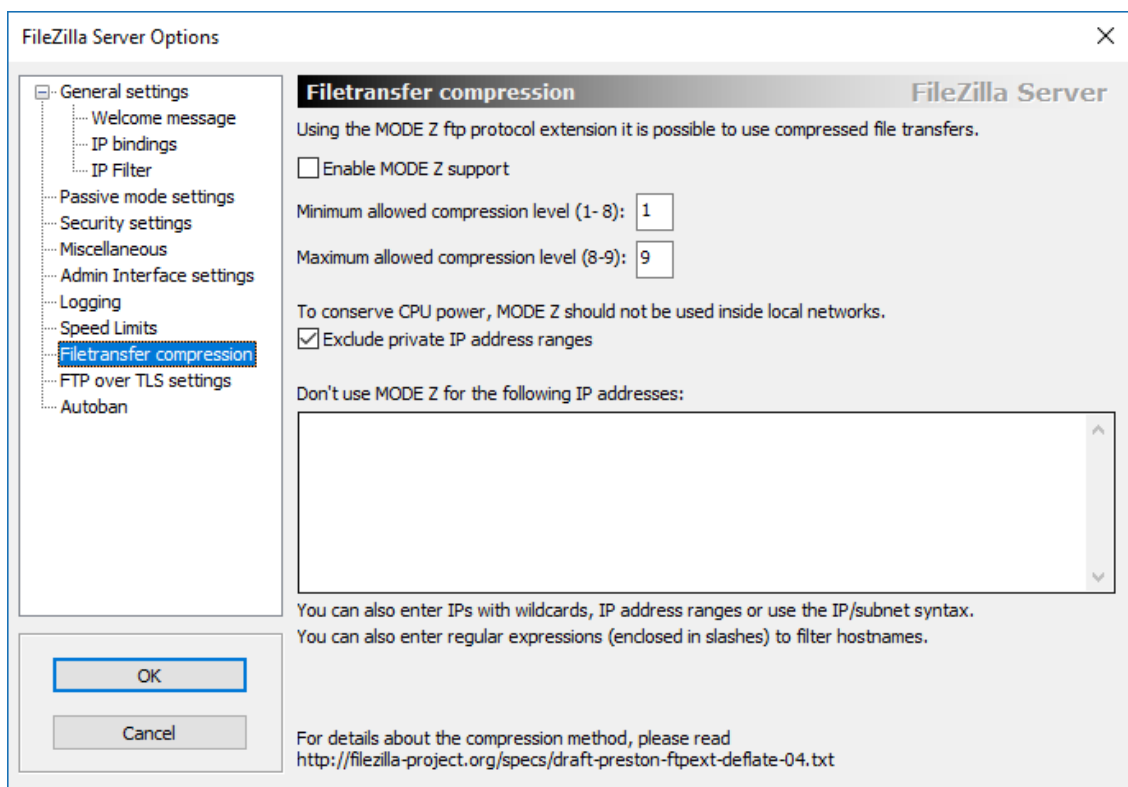
- 1.9. На вкладці «Admin Interface Settings» можна задати IP-адресу і порт, за якими буде доступний інтерфейс управління сервером (той самий, який спочатку використовували як localhost чи 127.0.0.1 і 14147). Крім того, можна вказати IP-адреси, яким дозволено підключатися до нього.



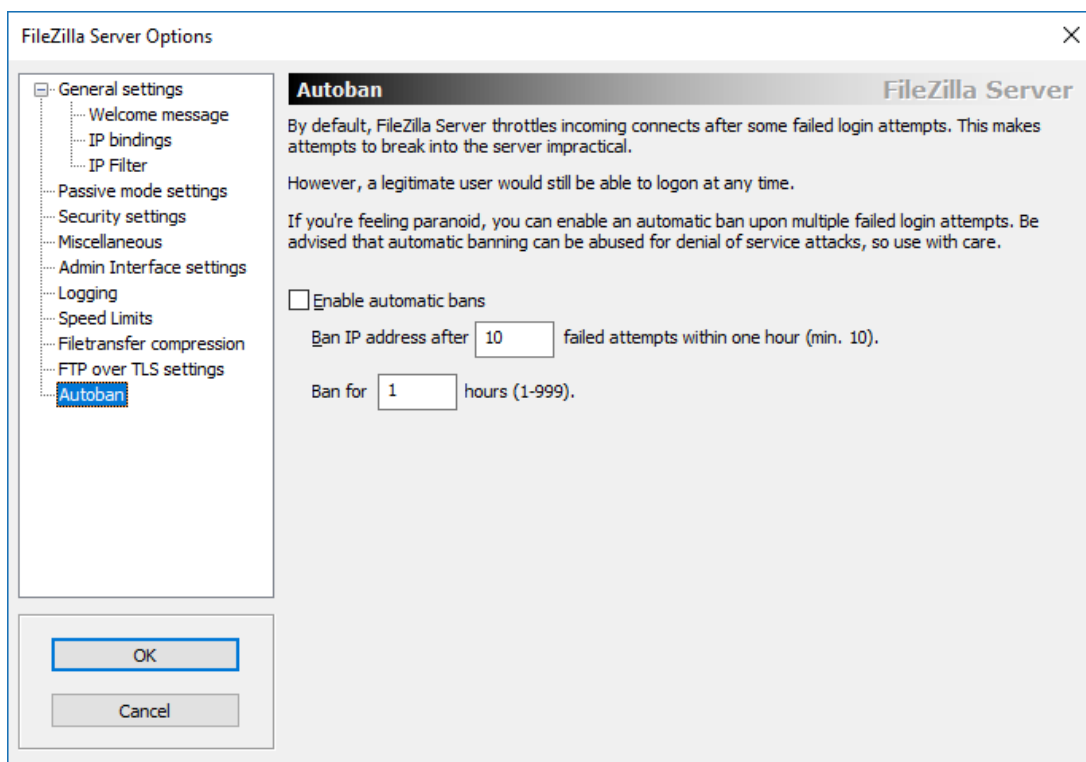
1.10. Розділ налаштувань «Logging» дозволяє включати запис лог-файлів (Enable logging to file), налаштувати їх максимальний розмір (Limit log file size to), писати все в один файл (Log all to "FileZilla Server.log") або для кожного дня створювати окремий (в цьому випадку можна обмежити їх максимальний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



- 1.11. 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.
- 1.12. 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.

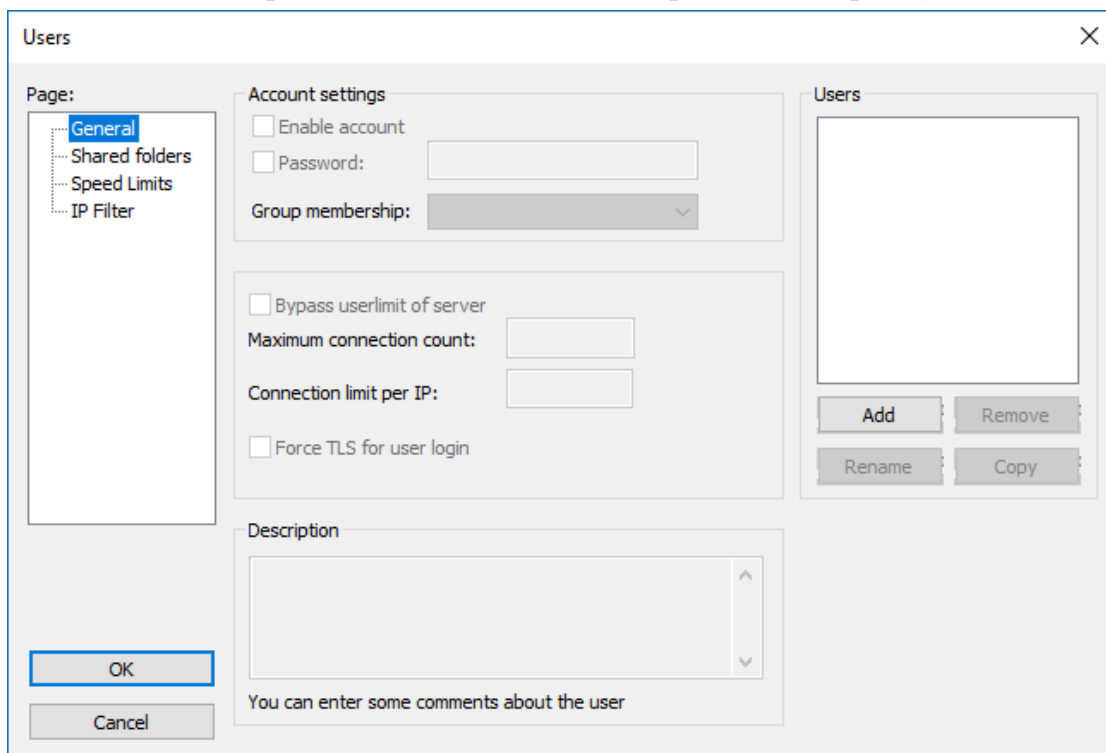


- 1.13. У розділі «FTP over TLS setting» можна налаштувати захищене з'єднання між клієнтом і сервером. Для цього потрібно включити підтримку протоколу TLS і вказати шляхи до закритого ключа, файлу сертифікату і пароль.
- 1.14. У розділі «Autobans» можна включити автоматичне блокування користувачів після 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 ".

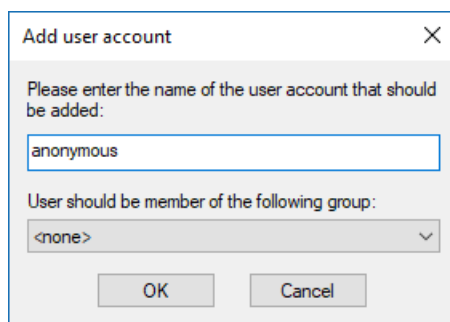


Крок 3: Початкове налаштування акаунтів користувачів (users) і доступів (share)

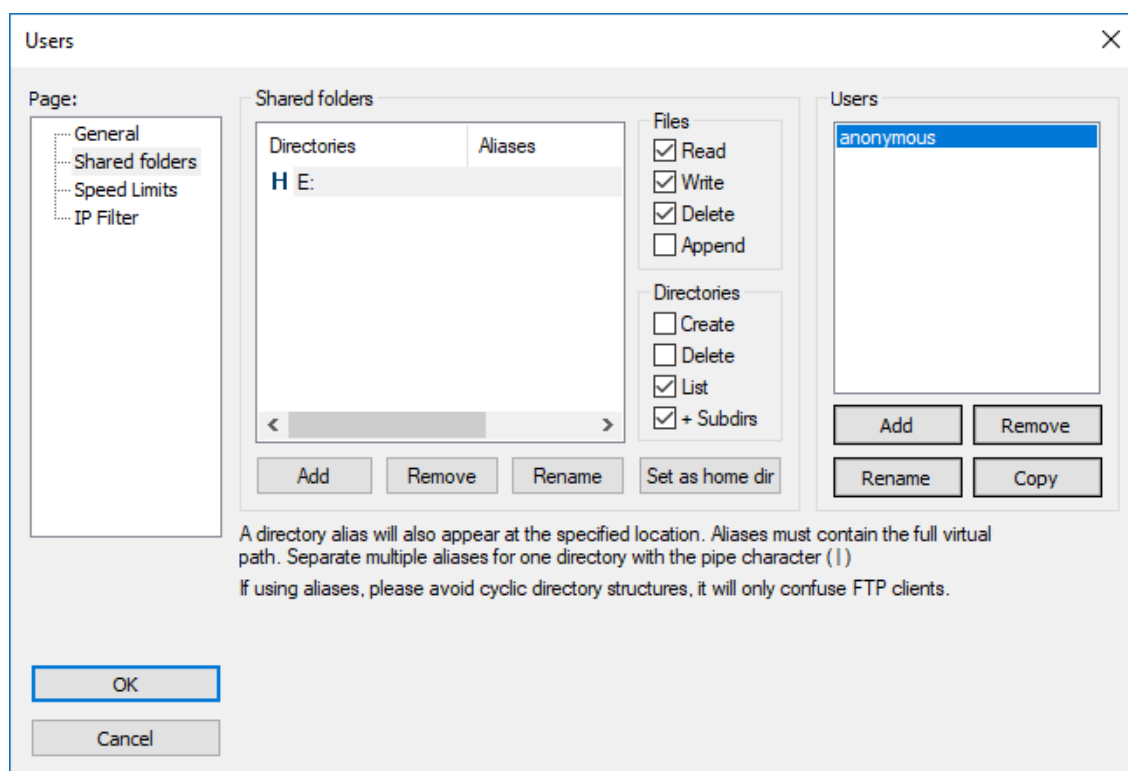
- 1.1. Для додавання нового користувача потрібно виконати команду «Edit → Users». Відкриється відповідне вікно роботи з користувачами.



- 1.2. 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».



- 1.3. Далі для даного користувача можна задати пароль і обмеження по кількості з'єднань.
- 1.4. 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.



- 1.5. 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(и) і, при необхідності, порт (якщо змінювали), які вони повинні вказати в своєму, попередньо встановленому FTP-клієнті.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] (Лист МОНУ №1/11-8052 від 28.05.12р.) - Львів, «Магнолія 2006», 2013. – 256 с.
2. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 2. [навчальний посібник] (Лист МОНУ №1/11-11650 від 16.07.12р.) - Львів, «Магнолія 2006», 2014. – 312 с.
3. Микитишин А.Г., Митник, П.Д. Стухляк. Телекомунікаційні системи та мережі – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 384 с.
4. Буров Є. Комп'ютерні мережі. 2-ге оновлене і доповн. Вид. Львів: Бак, 2003. – 584 с.
5. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі: Підручник для вищих навчальних закладів. – К.: САММІТ-КНИГА, 2010. – 640 с.
6. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. —С-Пт. : Питер, 2013. — 960 с.
7. В.Г.Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд.— СПб.: Питер, 2016. – 992 с.
8. Амато, Вито. Основы организации сетей Cisco, том 1.: Пер. с англ. - М.: Издательский дом "Вильямс", 2002.
9. Амато, Вито. Основы организации сетей Cisco, том 2.: Пер. с англ. - М.: Издательский дом "Вильямс", 2002.
- 10.Царьов Р.Ю. Структуровані кабельні системи: навч. посіб. для студентів вищих навчальних закладів. / Царьов Р.Ю., Нікітюк Л. А., Резніченко П. І. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 260 с.: іл.
- 11.Крук Б.И, Попантонопуло В.Н., Шувалов В.П. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1 – Современные технологии; под ред. проф. В.П. Шувалова. – Изд. 3-е, испр. и доп. – М.: Горячая линия-Телеком, 2003. – 647 с.
- 12.Катунин Г.П., Мамчев Г.В., Попантонопуло Б.И, Шувалов В.П. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 2 – Радиосвязь, радиовещание, телевидение; под ред. проф. В.П. Шувалова. – Изд. 3-е, испр. и доп. – М.: Горячая линия-Телеком, 2004. – 672 с.
- 13.Величко В.В., Субботин Е.А., Шувалов В.П., Ярославцев А.Ф. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 3 – Мультисервисные сети;/ под ред. проф. В.П. Шувалова. – Изд. 3-е, испр. и доп. – М.: Горячая линия-Телеком, 2005. – 592 с.
- 14.Довгий С.О., Савченко О.Я., Воробієнко П.П. та ін. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / За ред. С.О. Довгого. – К.: Український Видавничий Центр, 2002. – 520 с.