Міністерство освіти і науки України
Одеський національний технологічний університет
Кафедра комп'ютерної інженерії

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ

на тему *Проектування локальної мережі*
(назва кваліфікаційної роботи згідно наказу ОНТУ)
з бездисковими робочими станціями

Здобувача *Холодняка М.К.*
(прізвище, ініціали)
4 курсу *543а* групи

Керівники: *ст. викл. Барабаш Т.М.*
(посада, прізвище та ініціали)
доц. Сахарова С.В.
(посада, прізвище та ініціали)

Консультанти: ст. викл. Нєнов О.Л.
(посада, прізвище та ініціали)
д.е.н., проф. Басюркіна Н.Й.
(посада, прізвище та ініціали)

Кваліфікаційна робота допускається до захисту

Рішення кафедри від *10.06* 2023 р., протокол № 8

Завідувач кафедри комп. інженерії _____ Сергій АРТЕМЕНКО
(назва кафедри) (підпис) (Ім'я ПРІЗВИЩЕ)

Одеса - 2023 рік

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерної інженерії, програмування та кіберзахисту*
Кафедра *комп'ютерної інженерії*
Ступінь вищої освіти *бакалавр*
Спеціальність *123 «Комп'ютерна інженерія»*
Освітня програма *Мережеві технології та інтернет речей*

ЗАТВЕРДЖУЮ
Зав. кафедри *комп'ютерної інженерії*
Сергій АРТЕМЕНКО
« 10 » *серпень* 2022 року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА

Холодняка Михайла Кириловича

1. Тема роботи Проектування локальної мережі з бездисковими робочими станціями

Затверджена наказом університету від « *10* » *серпня* 2022 р., наказ № *440-03*

2 Термін здачі здобувачем закінченої роботи *5 червня 2023 р.*

3. Вихідні дані роботи

1. Вивчити основні аспекти проектування локальних мереж та технології бездискових робочих станцій. 2. Визначити вимоги користувачів та їх потреби стосовно бездискових робочих станцій. 3. Розробити концепцію мережі з бездисковими робочими станціями. 4. Реалізувати та налаштувати мережу з бездисковими робочими станціями

4. Перелік питань, які потрібно розробити

1. Характеристики бездискових робочих станцій.
2. Аналіз мережевих технологій та протоколів. 3. Проектування мережі

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Слайд 1. Порівняння термінаів Слайд 2. Структура підприємства
Слайд 3. Процес завантаження LTSP Слайд 4. Детальна схема роботи системи
Слайд 5. Обґрунтування вибору засобів Слайд 6. Продовження обґрунтування
Слайд 7. Налаштування елементів мережі Слайд 8. Основні завдання з адміністрування та підтримки роботи цієї мережі Слайд 9. Економічні показники
Слайд 10. Висновок

6. Консультанти по роботі, із зазначенням розділів роботи, що стосуються їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Економіка	*Басюркіна Н.Й., д.е.н., проф.*		
Охорона праці	*Нєнов О.Л., к.т.н., ст. викл.*		
Нормоконтроль	*Барабаш Т.М., ст. викл.*		

7. Дата видачі завдання *30.09.2022*

Керівник _____ *Тетяна БАРАБАШ*

_____ *Світлана САХАРОВА*

Завдання прийняв до виконання _____ *Михайло ХОЛОДНЯК*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	*Ознайомлення з літературою проектування локальних мереж і бездискових робочих станцій.*	*23.02.2023*	
2.	*Визначення мети та завдань дипломної роботи.*	*17.03.2023*	
3.	*Детальний аналіз різних технологій бездискових робочих станцій.*	*20.03.2023*	
4.	*Вивчення особливостей проектування локальних мереж.*	*06.04.2023*	
5.	*Аналіз вимог користувачів та їх потреб щодо бездискових робочих станцій.*	*12.04.2023*	
6.	*Встановлення та налаштування бездискових робочих станцій.*	*29.04.2023*	
7.	*Проведення тестування та відладки мережі.*	*10.05.2023*	
8.	*Оформлення розрахунково-пояснювальної записки дипломної роботи*	*21.05.2023*	
9.	*Підготовка графічного матеріалу*	*02.06.2023*	

Керівники роботи _____ *Тетяна БАРАБАШ*

_____ *Світлана САХАРОВА*

Несу відповідальність за ідентичність електронного та друкованого варіантів кваліфікаційної роботи, даю згоду на обробку персональних даних та не заперечую проти розміщення кваліфікаційної роботи на офіційних web-ресурсах ОНТУ.

Підтверджую, що в кваліфікаційній роботі відсутні порушення норм академічної доброчесності.

Здобувач - дипломник _____ *Михайло ХОЛОДНЯК*

АННОТАЦІЯ

Дипломна робота на тему «Проектування локальної мережі з бездисковими робочими станціями» досліджує можливості та переваги використання бездискових систем на базі *LTSP* (*Linux Terminal Server Project*). У роботі розглядаються основні принципи роботи *LTSP* та бездискових систем, їх структура та функціональні можливості.

В рамках роботи проведено аналіз існуючих рішень бездискових систем на базі *LTSP* та порівняння їх із традиційними дисковими системами. Оцінено економічні та технічні аспекти використання бездискових систем, у тому числі зручність управління та масштабування.

Також у роботі описаний процес розробки та реалізації бездискової системи на базі *LTSP*, включаючи вибір та налаштування необхідного обладнання та програм. Проведено тести системи на продуктивність та надійність.

Результати дослідження показують, що бездискові системи на базі *LTSP* можуть бути ефективним та економічно вигідним рішенням для організацій, які хочуть спростити управління та забезпечити високу продуктивність робочих станцій за низької вартості обслуговування.

ABSTRACT

The thesis on «Designing a local network with diskless workstations» explores the possibilities and advantages of using diskless systems based on LTSP (Linux Terminal Server Project). The paper examines the basic principles of LTSP and diskless systems, their structure and functionality.

As part of the work, the analysis of existing solutions of diskless systems based on LTSP and their comparison with traditional disk systems was carried out. The economic and technical aspects of using diskless systems, including ease of management and scaling, are evaluated.

The work also describes the process of development and implementation of a diskless system based on LTSP, including the selection and configuration of the necessary hardware and software. The system has been tested for performance and reliability.

The results of the study show that diskless systems based on LTSP can be an effective and cost-effective solution for organizations that want to simplify management and ensure high productivity of workstations at a low maintenance cost.

ЗМІСТ

					КРБ.КІ.1.440-03.1.5		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розробив		Михайло ХОЛОДНЯК			Проектування локальної мережі з бездисковими робочими станціями	Літ.	Арк. 6 / Акрушів 89
Перевірив		Тетяна БАРАБАШ					
Рецензент						гр. 543, ОНТУ	
Нормоконтроль		Тетяна БАРАБАШ					
Затвердив		Сергій АРТЕМЕНКО					

ВСТУП

Розпочинаючи з опису активного розвитку галузі інформаційно-комунікаційних технологій, що впроваджує різноманітні інновації, варто звернути увагу на глобальну інформаційну інфраструктуру. Ця інфраструктура, яка включає загальносвітову інформаційну мережу, системи телебачення, радіомовлення, супутникові та мобільні комунікації, відіграє ключову роль у забезпеченні масового доступу до інформації.

Цей диплом присвячений розгляду проблематики проектування та реалізації локальних мереж з бездисковими системами для підприємств. Досліджуються можливості використання бездискових систем у контексті вибору обладнання, налаштування роутера, віртуального сервера, тонкого клієнта та забезпечення безперебійного функціонування мережі. Аналізуються вимоги, методи вибору, конфігурації та підтримки бездискових систем з метою оптимізації роботи підприємств у сучасному інформаційному середовищі.

Визначення правильної мережевої архітектури є одним з ключових факторів, які слід враховувати при побудові локальної мережі з бездисковими робочими станціями. Мережеві топології бувають з різними топологіями, включаючи шину, кільце, зірку, комірку та гібридну. Вибір топології залежить від потреб організації, її розміру та фінансових можливостей.

Вибір апаратного та програмного забезпечення також має вирішальне значення при проектуванні локальної мережі з бездисковими робочими станціями. Апаратне забезпечення, що використовується в мережі, має бути здатним обробляти очікуваний трафік у мережі, а також забезпечувати достатню ємність для *NAS*. Програмне забезпечення, що використовується в мережі, має бути сумісним з апаратним забезпеченням і підтримувати потрібні мережеві служби.

Безпека також має важливе значення при проектуванні локальної мережі з бездисковими робочими станціями. Мережа має бути захищена

відповідними протоколами безпеки, щоб запобігти несанкціонованому доступу, крадіжці даних і атакам шкідливих програм. Це може включати використання брандмауерів, захищених паролем облікових записів користувачів і шифрування. Деякі постачальники, такі як *Dell Wyse*, рекламують «захист від вірусів». Прекрасним прикладом може бути, якщо користувач заходить на шкідливий веб-сайт, зараження все ще може статися, але це вплине на ОС віртуального робочого столу, а не на сам пристрій. Пристрої з тонкими клієнтами (Тонкий клієнт – це комп'ютер, який не має своїх власних ресурсів для обробки даних та виконання завдань, а натомість використовує ресурси віддаленого сервера через мережу.) ніколи не зв'язуються з шкідливим веб-сайтом, тому вони захищені від зараження.

Ряд IT-відділів переходять на цю архітектуру для централізації бізнесу з використанням технологій віртуальних десктопів.

Використання цієї технології для бізнесу та IT-інфраструктур має ряд переваг:

1. Економія витрат. При використаннні тонких клієнтів знижується наступні витрати:

- Витрати на IT-підтримку.
- Авансові витрати на покупку.
- Використання простору в дата-центрі.
- Ліцензійні витрати.
- Загальне зниження адміністративних і експлуатаційних витрат до 70%.
- Зменшує рахунок за енергію на 97%.
- Тонкі клієнти споживають в середньому 8-20 Вт в порівнянні з ПК на 150 Вт.
- Економія витрат на електроенергію може бути реінвестований спрощене управління.

2. Переваги управління мережі з тонким клієнтом є:

- Всі програмного і апаратного забезпечення, політики безпеки, зміни додатків і т. д. Можуть бути виконані в центрі обробки даних.
- IT-персонал не зобов'язаний (як і ПК) усувати окремі проблеми на робочому столі користувача.
- Скорочення часу простою, підвищення продуктивності серед кінцевих користувачів та IT-персоналу.
- Централізоване та спрощене резервне копіювання настільних комп'ютерів, ноутбуків і інших пристроїв клієнтського доступу.

3. Посилена безпека. Переваги безпеки тонкого клієнта включають в себе:

- Тонкі клієнти захищені від несанкціонованого програмного забезпечення або впровадження вірусів.
- Дані не можуть бути скопійовані на диск або збережені у будь-якому іншому місці, крім сервера.
- Централізована обробка спрощує управління і моніторинг системи
- Спростіть безпеку, захистіть інтелектуальну власність, забезпечте конфіденційність даних.

4. Збільшення продуктивності. Системи можуть бути віртуально попередньо сконфігуровані, упаковані і введені в експлуатацію за лічені хвилини.

5. Прискорення настройки і забезпечує гнучкість без спеціального персоналу.

Метою проекту є створення локальної мережі з використанням бездискових станцій для підвищення ефективності роботи підприємства.

Підсумовуючи, можна сказати, що при побудові локальної мережі з бездисковими робочими станціями слід враховувати низку факторів і процедур, зокрема архітектуру мережі, вибір апаратного та програмного забезпечення, протоколи безпеки, варіанти резервного копіювання та масштабованість.

РОЗДІЛ 1

АНАЛІТИЧНЕ ОЦІНЮВАННЯ ТЕХНОЛОГІЙ БЕЗДИСКОВИХ СИСТЕМ

1.1 Постановка задачі

Головне завдання цієї дипломної роботи полягає в тому, щоб побудувати мережу, яка буде економічно ефективна та підтримуватиме високий рівень безпеки і зможе забезпечити всім необхідним для роботи користувача, а саме:

- Операційна система: дозволяє користувачеві взаємодіяти з комп'ютером та запускати різні програми.
- Офісні програми: програми для створення документів, електронних таблиць та презентацій
- Програми для обробки фотографій: дозволяють користувачеві редагувати та покращувати фотографії.
- Інтернет: дозволяє користувачеві швидко знаходити інформацію, комунікувати з колегами та виконувати інші завдання, які потребують доступу до Інтернету.
- Електронна пошта: програма електронної пошти, яка дозволяє користувачеві отримувати та відправляти електронні листи.

1.2 Характеристика терміналів

Термінали для бездискових систем – це пристрої, які дозволяють користувачам працювати з комп'ютерними системами без необхідності використання фізичних носіїв інформації, таких як диски або флеш-накопичувачі. Натомість, дані та програмне забезпечення можуть бути передані через мережу.

Загалом термінали для бездискових систем дозволяють користувачам отримати доступ до комп'ютерних ресурсів через мережу, що підвищує гнучкість та ефективність роботи.

***1. Linux Terminal Server Project* (*LTSP*)** допомагає в мережевому завантаженні клієнтів локальної мережі з одного шаблону установки, який знаходиться в образі віртуальної машини або в *chroot* на сервері *LTSP*, або в корені сервера. Таким чином, обслуговування десятків або сотень бездискових клієнтів виконується так само просто, як обслуговування одного ПК.

LTSP був перероблений і переписаний з нуля в 2019 році компанією *alkisg* для підтримки нових технологій, таких як *systemd*, оновлені середовища робочого столу, *Wayland*, *UEFI* і т.д. Тільки нова версія активно розробляється, в той час як стара тепер називається *LTSP5* і знаходиться в мінімальної версії.

LTSP автоматично налаштовує і використовує такі інструменти:

- *iPXE*: мережевий завантажувач, який показує початкове меню завантаження клієнта і завантажує ядро /*initrd*.
- *SSH* або *SSHFS* або *LDAP*: аутентифікація користувачів на сервері;
- *dnsmasq* або *isc-dhcp-server*: сервер *DHCP*, який призначає *IP*-адреси клієнтам, або сервер *ProxyDHCP*, коли використовується інший сервер *DHCP*, наприклад, роутер.
- *NFS* або *SSHFS*: доступ до каталогу користувача /*home*, який знаходиться на сервері.
- *dnsmasq* або *tftpd-hpa*: *TFTP*-сервер, який відправляє *ipxe*/*kernel*/*initrd* клієнтам.
- *dnsmasq*: необов'язковий *DNS*-сервер для *DNS*-кешування або внесення в чорний список.
- *mksquashfs*: створює стислу копію шаблону зображення /*chroot*/*VM* для використання в якості кореня клієнта.
- *NFS* або *NBD*: відправити образ *squashfs* в мережу.
- *tmpfs* і *overlayfs*: зробити образ *squashfs* тимчасово доступним для запису для кожного клієнта, подібно живим компакт-дисків.

2. PiServer - це дистрибутив створений для образу *raspbian* і для *raspberry pi*. Ви можете спокійно видаляти або додавати необхідні програми для загального користування.

PiServer має наступні функціональні можливості:

- Встановлює *DHCP*-сервер - річ всередині маршрутизатора, яка дає всім мережевим пристроям *IP*-адресу – або в режимі проксі, або в режимі повного *IP*. Незалежно від режиму, сервер *DHCP* буде відповідати тільки на вказаний *Raspberry Pis*, що важливо для безпеки мережі.
- Автоматично виявляє *Raspberry Pis* при спробі завантаження по мережі, тому вам не потрібно визначати їх адреси *Ethernet*.
- Використовує злегка змінену збірку *Raspbian*, яка дозволяє розділяти тимчасові прогалини, не має користувача за замовчуванням «pi» і має включений *LDAP* для входу в систему.
- Створює імена користувачів і паролі для сервера. Що використовується для організації класних кімнат, повної *Pis*.

У класі *PiServer* дозволяє зберігати всі файли для уроків або проектів на центральному комп'ютері з архітектурою *x*86. Кожен користувач може мати свій профіль, і будь-які файли, які він створює, також зберігаються на сервері. Крім того, мережевий *Pis* не повинен бути підключений до Інтернету.

***3. Remote Desktop Services* (*RDS*)** - це технологія, що надає користувачам можливість працювати з віддаленими робочими столами та програмами на базі операційної системи *Windows*. *RDS* була розроблена *Microsoft* і є ефективним інструментом для централізованого управління робочими столами та додатками, а також для забезпечення віддаленого доступу до них.

За допомогою *RDS* адміністратори можуть створювати віртуальні робочі столи та надавати доступ до них віддаленим користувачам. Користувач може працювати на віддаленому робочому столі, ніби він знаходиться безпосередньо за комп'ютером. *RDS* дозволяє користувачам працювати з

віддаленими програмами, використовуючи лише інтернет-браузер, що суттєво спрощує їхню роботу.

RDS також надає можливості для забезпечення безпеки віддаленого доступу, у тому числі автентифікації користувача та шифрування даних. За допомогою *RDS* адміністратори можуть керувати доступом до віддалених робочих столів та програм, обмежувати доступ до деяких функцій, а також моніторити активність користувачів.

RDS може бути встановлена на серверах з операційною системою *Windows Server* і може використовуватися для роботи з будь-якими програмами, які працюють на *Windows*. Це може бути корисним для компаній, які працюють з різними програмними продуктами і хочуть спростити їх використання та обслуговування.

Таблиця 1.1

Порівняння терміналів

Функція/Особливість	***LTSP***	***PiServer***	***RDS***
Вартість	Безкоштовно	Безкоштовно	Платно
Платформа	*Linux*	*Raspberry Pi*	*Windows*
Масштабованість	Висока	Обмежена	Висока
Віддалений доступ	Так	Так	Так
Підтримка графіки	Так	Обмежена	Так
Рівень безпеки	Високий	Середній	Високий
Підтримка мультимедіа	Так	Обмежена	Так

З усіх трьох розглянутих термінальних платформ – *LTSP*, *PiServer* та *RDS*, *LTSP* є найкращим вибором для багатьох організацій, особливо тих, які працюють з обмеженим бюджетом. *LTSP* безкоштовна та базується на *Linux*, що дозволяє забезпечити високу масштабованість, підтримку віддаленого доступу та високий рівень безпеки.

LTSP також має досить повну підтримку графіки та мультимедіа, що дозволяє користувачам працювати з різними типами файлів. Окрім того, *LTSP* має відкритий вихідний код, що дозволяє змінювати та пристосовувати платформу для власних потреб.

Отже, обираючи *LTSP*, організація може забезпечити високу продуктивність та ефективність, а також значні економії витрат на технології.

1.3 Обгрунтування використання віртуальної машини

Оскільки ми не маємо достатньо коштів на покупку фізичних компонентів мережі, а також не маємо достатньо місця та ресурсів для збудування та управління фізичною мережею, то у такому випадку віртуалізація мережі буде відмінним варіантом. Вона дозволяє створити віртуальну мережу на одному комп'ютері, що забезпечує доступ до всіх необхідних ресурсів для створення та управління мережею. Таким чином, я можу здійснити віртуалізацію мережі на своєму комп'ютері, що дозволить отримати доступ до різноманітних функцій та можливостей, які недоступні при збудуванні фізичної мережі.

Віртуалізація мережі – це процес створення віртуальної мережі на базі фізичної інфраструктури.

VirtualBox, VMware Workstation і *Hyper-V* - це три з найпопулярніших віртуальних машин, які використовуються для віртуалізації ОС. Ось деякі короткі описи кожної з них:

- *VirtualBox* – це безкоштовна віртуальна машина, розроблена *Oracle*. Вона дозволяє виконувати різні ОС на одному комп'ютері та надає можливість настроювати віртуальні мережі, диски та інші частини.
- *VMware Workstation* – це комерційна віртуальна машина, розроблена *VMware*. Вона має широкий набір функцій та можливостей, включаючи підтримку мережевих з'єднань, сумісність з різними операційними системами та можливість керування віртуальними машинами з мобільних пристроїв.

– *Hyper-V* – це безкоштовна віртуальна машина, розроблена *Microsoft*. Вона доступна на серверних версіях операційної системи *Windows* та дозволяє використовувати віртуалізацію на різних рівнях, включаючи рівень обладнання та рівень програмного забезпечення.

Таблиця 1.2

Порівняння віртуальних машин

Характеристика	***VirtualBox***	***VMWare***	***Hyper*-V**
Вартість	Безкоштовно	Платно	Безкоштовно
Підтримувані ОС	Безліч	Безліч	*Windows*
Інтерфейс	Простий	Складний	Простий
Управління ресурсами	Обмежене	Розширене	Обмежене

З цієї таблиці можна зробити висновок, що *VirtualBox* є найкращим варіантом для виконная нашої мети. Вона має відкритий вихідний код, безкоштовна, підтримує широкий спектр операційних систем і має всю функціональність, необхідну для практичного використання віртуальних машин, включаючи створення знімків. Крім того, вона ідеально підходить для тих, хто бажає вивчати віртуалізацію з мінімальним бюджетом, а також для студентів.

Підбиваючи підсумки вибору технології для реалізації локальної мережі, можна виділити:

– Для побудови централізованої мережі терміналів було обрано технологію *LTSP*. Завдяки цій технології багато віртуальних термінальних комп'ютерів, які можуть використовуватися для роботи користувачів, можуть бути побудовані з використанням одного сервера. Це забезпечує більш ефективне використання ресурсів сервера і полегшує адміністрування всієї мережі.
– На клієнтських машинах у мережі *LTSP* працюватиме *Lubuntu* як операційна система. Ця легковагова операційна система має

мінімальні вимоги до апаратного забезпечення, що дозволяє використовувати її на старих або слабких комп'ютерах.

– У мережі *LTSP* в якості технології віртуалізації для клієнтських комп'ютерів було обрано *VirtualBox*. Ця програма забезпечує високий рівень гнучкості та масштабованості, що дозволяє використовувати її для створення мережі будь-якого масштабу.

Таким чином, вибір технологій для реалізації мережі *LTSP* на основі *VirtualBox* був ретельно обґрунтований та були враховані всі особливості проекту й мережної інфраструктури.

РОЗДІЛ 2

РОЗРОБКА СТРУКТУРНОЇ СХЕМИ ПРОЕКТОВАНОЇ ЛОКАЛЬНОЇ МЕРЕЖІ

2.1 Характеристика бездискових мереж

Ідея для бездискової мережи полягає у створенні інфраструктури, яка дозволить користувачам підключатися до сервера за допомогою терміналів або тонких клієнтів та працювати у загальному середовищі. У цьому середовищі будуть доступні спільні ресурси, такі як програми, файли та бази даних. При цьому обчислювальні потужності будуть розподілені між сервером і терміналами, що дозволить економити ресурси та зменшувати навантаження на кожен окремий комп'ютер. Однією з основних переваг мережі на *LTSP* є зручність управління спільними ресурсами. Адміністратори можуть легко керувати програмами та файлами на сервері, а користувачі можуть легко отримувати доступ до цих ресурсів. Також, у разі потреби, адміністратори можуть швидко та легко налаштувати клієнтські машини або замінити їх на нові, без необхідності встановлення та налаштування програмного забезпечення на кожному комп'ютері.

Розглянемо, як само буде працювати наша мережа. Клієнтська машина увімкнена. Після ініціалізації апаратного забезпечення мережева карта шукає *IP*-адресу через протокол *DHCP*. Сервер *LTSP* у більшості випадків діє як сервер *DHCP* для локальної мережі та надсилає клієнтській машині свою *IP*-адресу. На рисунку 2.1 показана схема процесу завантаження *LTSP*.

Після того, як мережева карта прив’язала до себе IP-адресу, вона встановлює з’єднання з сервером *LTSP* і запитує файл конфігурації *PXE*. Сервер *LTSP* надсилає цей файл назад на клієнтську машину, яка потім робить запит на образ ядра. Це основа ОС, яка надає клієнту всі апаратні драйвери, необхідні для зв’язку з сервером.

Після цього з сервером встановлюється з’єднання *NFS*. Частка *NFS* містить дуже скорочену інсталяцію Lubuntu, яка майже повністю складається

з сервера та менеджера входу на основі *SSH* для підключення до сервера. Коли клієнтська машина завершить завантаження цієї невеликої версії *Lubuntu*, користувачеві відобразиться екран входу.

Коли користувач входить в систему, тунель *SSH* відкривається до сервера, і сеанс ініціюється через цей тунель. Усі програми запускаються на сервері, і тільки графічний інтерфейс передається назад на клієнтську машину. Це дозволяє користувачеві взаємодіяти з сеансом і використовувати комп'ютер як зазвичай.

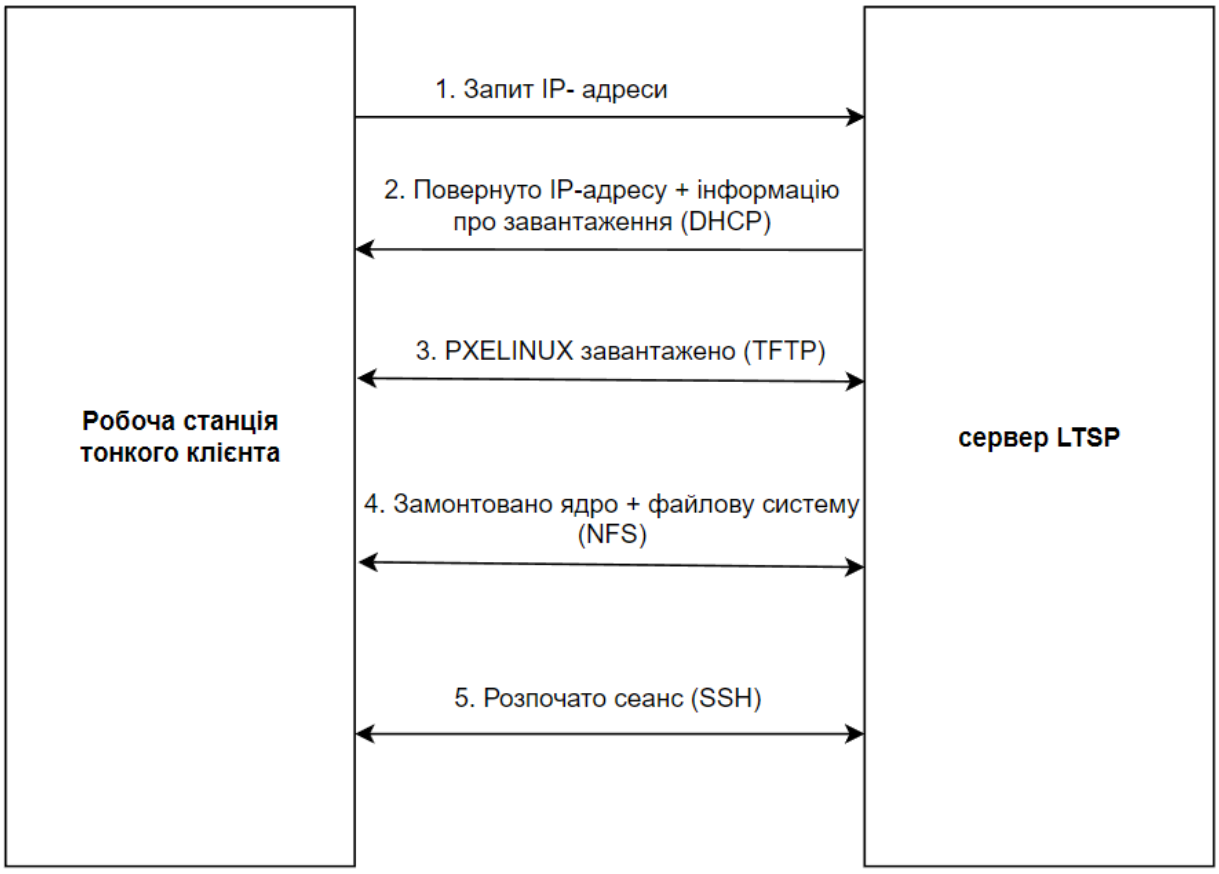

Рисунок 2.1 – Діаграма процесу завантаження *LTSP*

Коли ви використовуєте бездискову мережу за допомогою *LTSP*, усі додатки та операційна система запускаються на сервері, а не на локальному комп'ютері. Тонкий клієнт, який є робочою станцією, підключається до сервера і запускає додатки на ньому. Тонкий клієнт сам не обробляє жодних додатків, а просто передає введення користувача і виведення між клієнтом і сервером.

Коли користувач запускає застосунок на тонкому клієнті, запит на запуск застосунку надсилається на сервер *LTSP*. Сервер запускає застосунок на своєму боці і передає виведення застосунку назад на тонкий клієнт. Для цього використовується протокол відображення вікон (*X*11), який передає графічний вивід і введення користувача між тонким клієнтом і сервером.

Для передачі даних між тонким клієнтом і сервером використовується мережеве з'єднання. Тонкий клієнт надсилає запити на сервер, і сервер надсилає відповіді та дані назад на тонкий клієнт. Це означає, що вся робота з даними, включно з читанням, записом і обробкою даних, відбувається на сервері.

Таким чином, усі дані, включно з введенням користувача і виведенням, передаються через мережу між тонким клієнтом і сервером. Це означає, що для оптимальної продуктивності необхідно мати швидке мережеве з'єднання між тонким клієнтом і сервером. Крім того, сервер повинен мати досить високу продуктивність, щоб обробляти всі додатки і дані для декількох тонких клієнтів одночасно.

Бездискову систему можна використовувати в різних галузях, включаючи бізнес, охорону здоров'я та освіту. Наприклад, в освіті вона може використовуватися для створення класів з комп'ютерами, в охороні здоров'я – для створення робочих місць для медичного персоналу, а в бізнесі – для створення доступу до загальних баз даних та додатків.

Запуск додатків у сеансі користувача на сервері: при цьому додатки запускаються в контексті сеансу користувача на сервері. Кожен користувач отримує свій власний сеанс на сервері, і всі програми запускаються в цьому сеансі. Цей підхід дає змогу користувачам мати свої персональні налаштування та файли конфігурації.

Таким чином, клієнт робить запит для того, щоб відкрити яку-небудь програму або файл, зміна проходить на сервері, та показує це клієнту (рис. 2.2).

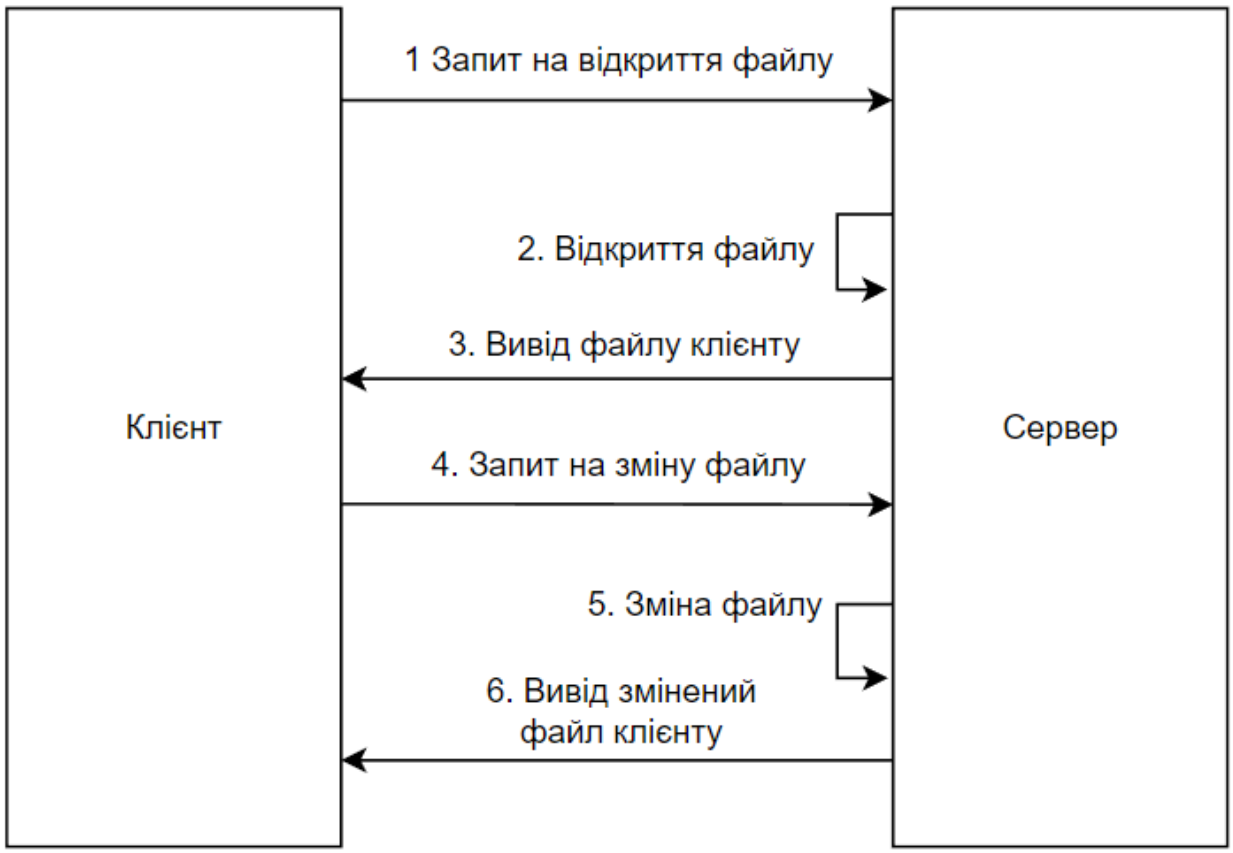

Рисунок 2.2 – Діаграма сеансу

Загалом ідея для бездискової системи полягає у створенні інфраструктури, яка дозволить користувачам працювати у загальному середовищі, використовуючи спільні ресурси. Вона може бути використана в різних областях, і дозволяє управляти ресурсами та клієнтськими машинами більш ефективно, ніж у звичайних мережах із встановленим у кожному комп'ютері програмним забезпеченням. Завдяки цьому мережа *LTSP* може значно зменшити витрати на підтримку та оновлення програмного забезпечення, а також підвищити безпеку, оскільки вся інформація зберігається на сервері та захищена від несанкціонованого доступу.

2.2 Проектування бездискових робочих станцій

Метою дипломної роботи є розробка локальної мережі на підприємстві. Дане підприємство займається питаннями продажу устаткування, складається з 3 відділів: відділ кадрів, відділ фінансів та відділ продажу. Стоїть завдання

організувати мережу на цьому підприємстві, за допомогою комутаційного обладнання, для того щоб усі відділи могли зв'язуватися з іншими.

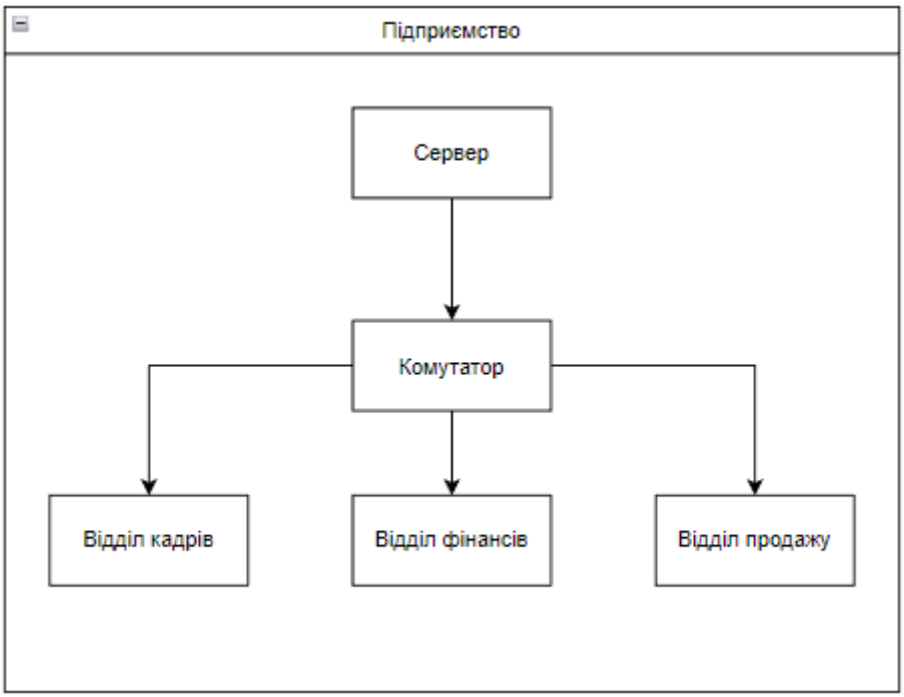

Рисунок 2.3 – Структура підприємства

Функціональна структура *LTSP* у підприємствах може включати такі компоненти:

- Сервер: центральний пристрій, на якому зберігаються всі програми та дані, що використовуються в мережі. Сервер може мати високу продуктивність та потужність для забезпечення ефективної роботи мережі та управління її ресурсами.
- Клієнтські машини: комп'ютери або термінали, які підключаються до сервера та використовують його ресурси для виконання програм та роботи з даними. Клієнтські машини не мають жорстких дисків і працюють на основі завантаження операційної системи з сервера.
- Мережеве обладнання: пристрої, які забезпечують з'єднання між сервером та клієнтськими машинами. Вони можуть включати комутатори, маршрутизатори, медіаконвертори та інші пристрої.
- Програмне забезпечення: програми, які використовуються в мережі. Вони зберігаються на сервері і можуть бути доступні для

використання на будь-якій клієнтській машині в мережі. Крім того, до функціональної структури можуть входити різні інструменти управління та моніторингу мережі.

– Адміністратори: фахівці, які відповідають за встановлення, налаштування, оновлення та підтримку мережі. Вони також можуть займатися управлінням ресурсами та забезпеченням безпеки в мережі.

Функціональна структура *LTSP* в підприємствах може мати різні конфігурації і залежати від потреб і цілей компанії. Однак, головним завданням мережі на *LTSP* є забезпечення швидкого та надійного доступу до додатків та даних, скорочення витрат на підтримку та оновлення ПЗ, а також підвищення безпеки та керованості ресурсів.

2.3 Вимоги до проектованої мережи

Для того, щоб зберегти стабільність мережі для безперервної сесії потрібно заздалегідь підготувати відділи в офісі, так як дизайнерський відділ може брати на себе велику кількість мережевих ресурсів або необхідно виділяти для дизайнерського відділу мережу на товстих клієнтах (Товстий клієнт - це комп'ютер, який має свій власний жорсткий диск та процесор, і використовується для виконання програм на локальному рівні, а не на віддаленому сервері, як у випадку з тонким клієнтом.), що підключені тільки до контролера домену.

Також для створення ефективної мережі на *LTSP* необхідно враховувати такі вимоги:

– Продуктивність сервера: сервер повинен мати достатню потужність обробки всіх запитів, які від клієнтських машин. Для більших мереж може знадобитися використання кількох серверів, що працюють у кластері, щоб забезпечити відмовостійкість мережі.

– Мережеве обладнання: для надійної роботи мережі необхідно використовувати високоякісне мережеве обладнання, що забезпечує

високу швидкість передачі даних та низьку затримку.

– Програмне забезпечення: необхідно використовувати оптимізовані операційні системи та програми для роботи в мережі.
– Клієнтські машини: повинні мати достатню продуктивність виконання завдань, використовуючи ресурси сервера. Бажано, щоб вони мали високошвидкісний доступ до мережі та підтримували роботу з технологіями віртуалізації.
– Безпека: необхідно забезпечити захист мережі від несанкціонованого доступу та вірусних атак. Для цього можна використовувати різні механізми захисту, такі як брандмауери, антивірусне програмне забезпечення, *VPN*-сервери та інші.
– Керованість: повинна існувати можливість віддаленого управління мережею. Для цього можна використовувати різні інструменти, такі як консолі, моніторинг і звітність про роботу мережі.

Відповідність вимогам, описаним вище, дозволить створити ефективну, надійну і безпечну мережу, яка відповідатиме потребам підприємства і забезпечувати ефективну роботу з додатками і даними.

1. Вимоги до мережевих сервісів.

Основні вимоги для провайдера це можливість покупки і продовження оренди для білих IP-адрес.

Так як мережа повинна бути статичною для можливості віддаленої конфігурації адміністратором.

Вибір оператора так само допоможе в майбутньому, бо може захистити від атак ззовні, які можуть відключити інтернет для сервера.

2. Вимоги до надійності мережі.

Надійність мереж має особливе значення, оскільки будь-яка втрата даних може призвести до серйозних наслідків, включаючи втрату цінних бізнес даних або особистих файлів користувачів.

− Резервне копіювання даних: це необхідність створити копію даних, які зберігаються на серверах або в хмарі, на випадок втрати або

пошкодження. Існує кілька способів резервного копіювання даних, включаючи повне, інкрементальне та диференціальне копіювання. Крім того, можна використовувати такі методи, як дзеркальне копіювання, коли дані дублюються на декількох серверах або вузлах мережі, та реплікація, коли дані копіюються на віддалені сервери.

- Контроль цілісності даних: це означає, що потрібно перевіряти, що дані, які зберігаються на серверах або в хмарі, не пошкоджені та не були змінені без дозволу користувача. Для цього можна використовувати різні методи, такі як контроль суми (*hash*-сума), який обчислює хеш-код для кожного файлу та перевіряє його щоразу, коли файл читається чи записується. Якщо хеш-код не відповідає оригінальному, значить, файл пошкоджено або змінено.
- Резервування живлення та засобів зв'язку: Для забезпечення високої надійності мереж необхідно забезпечити безперервність живлення та зв'язку. Наприклад, можна встановити додаткові джерела живлення, які будуть запасними у разі відключення основного, а також використовувати кілька засобів зв'язку (наприклад, інтернет-канали або мережні карти), щоб забезпечити надійний зв'язок між серверами та вузлами мережі.
- Моніторинг мережі та вузлів: допомагає виявляти проблеми, пов'язані з відмовами обладнання або програмного забезпечення, перш ніж вони призведуть до втрати даних. Для моніторингу можна використовувати різні інструменти, наприклад моніторинг завантаження мережі, системного журналу, сигналізації про відмови та ін.

Загалом, щоб гарантувати надійність мереж, необхідна ретельна стратегія з використанням цілого ряду методів і технологій. Дуже важливо планувати мережу так, щоб вона могла протистояти сбоям, управляти цілісністю даних, резервувати енергетичні та комунікаційні ресурси, а також стежити за тим, як працює мережа та її вузли. Всі ці методи дозволяють

захистити дані користувачів від втрати та пошкодження, забезпечуючи при цьому відмінну надійність мережі.

3. Вимоги до розширюваності.

Розширюваність бездискової мережі є важливим фактором при проектуванні та реалізації системи. У цьому розділі ми розглянемо основні вимоги щодо розширюваності:

- Масштабованість: Бездискова мережа повинна мати можливість масштабуватися залежно від зміни кількості термінальних клієнтів. Для цього необхідне відповідне обладнання та програмне забезпечення, яке забезпечить масштабованість мережі без втрати її продуктивності.
- Гнучкість: Бездискова мережа повинна бути гнучкою, щоб адаптуватися до потреб користувачів і організації. Задля цього потрібні використовувати відповідні інструменти керування, які дозволяють налаштовувати мережу під конкретні завдання та вимоги.
- Надійність: необхідне резервування компонентів мережі, а також – механізми виявлення та відновлення збоїв, відповідні інструменти моніторингу та управління.
- Сумісність: це відповідні протоколи та стандарти, які дозволяють бездисковій мережі взаємодіяти з іншими системами та додатками.
- Безпека: забезпечення відповідних механізмів аутентифікації та авторизації, шифрування даних, а також механізмів контролю доступу та моніторингу мережної активності.
- Продуктивність: обладнання та програмне забезпечення, яке забезпечить високу швидкість передачі даних та швидкий відгук системи на запити користувачів.

Всі вище перелічені вимоги є основоположними при проектуванні та реалізації бездискової мережі. Для того, щоб задовольнити всі ці вимоги, необхідно провести ретельний аналіз потреб користувачів та організації, а

також враховувати особливості існуючої інфраструктури та програмного забезпечення.

Крім того, при проектуванні бездискової мережі необхідно враховувати можливі ризики та загрози, пов'язані з безпекою даних та мережевою активністю, та розробити відповідні заходи щодо захисту та забезпечення безпеки системи.

Також необхідно приділити увагу питанням обслуговування та технічної підтримки бездискової мережі, оскільки це є важливим фактором для її надійності та ефективності.

4. Вимоги до якості обслуговування.

Сервер вимагає окремої кімнати з хорошою системою охолодження так як він буде працювати в безперервному сеансі, для підтримки віддалених робочих столів. Але це не єдина вимога, адже сам сервер потребуватиме щотижневої перевірки для його стабільної роботи і подальшого використання.

У цю перевірку входить:

– Обдув комплектуючих від пилу.
– Перевірки на підвищену температуру.
– Перевірка самого сервера на наявність сторонніх пристроїв.
– Перевірка справності безперебійного живлення.
– Зміна термопасти при підвищенні температури вище норми.

Ці мінімальні вимоги ставляться не тільки до сервера. Оскільки бездискові станції теж потребують щомісячної перевірки для збереження стабільності роботи.

2.4 Етапи створення мережі

Бездискова мережа на базі *LTSP* (*Linux Terminal Server Project*) - це тип мережі, яка дозволяє багатьом користувачам використовувати декілька терміналів на базі *Linux*, знаходячись в різних місцях, з використанням одного сервера. Основною перевагою мережі *LTSP* є те, що сервери можуть бути розташовані в центральному місці, тоді як термінали можуть бути

розповсюджені в інших місцях.

Основні етапи створення мережі на базі *LTSP*:

– Вибір сервера;

– Вибір операційної системи;

– Встановлення *LTSP*;

– Налаштування мережі;

– Налаштування віртуальної машини;

– Налаштування терміналів;

– Тестування;

Таким чином, у нас є чітко поставлені етапи створення мережі, що допомагають розуміти, яке завдання стоїть перед нами.

2.5 Основний принцип роботи *DHCP*

DHCP – це протокол динамічної настройки вузлу. Основна його робота це видавати *IP*-адреси та інші параметри для мережевих пристроїв які необхідні для *TCP*/*IP*.

Цей протокол працює за принципом «клієнт-сервер». На етапі конфігурації мережевого пристрою клієнтський комп'ютер звертається до так званого *DHCP*-сервера і запитує у нього необхідні параметри.

У початковому етапі конфігурації *DHCP* адмін може налаштувати діапазон адрес, які будуть видаватися мережевим клієнтам. Цей протокол спрощує завдання адміну, оскільки фіксація адреси в «*Address Leases*» дозволить уникнути зайвої конфігурації статичного *IP* на машинах.

Протокол *BOOTP*, розширенням якого є *DHCP*, має вирішальне значення для бездискових систем. Існує три можливі способи розподілу *IP*-адрес за допомогою *DHCP*:

– Ручний розподіл: використовуючи цей пункт, адміністратор вручну прописує всі *IP*-адреси в базу даних; в цей пункт також входить прописування *MAC*-адресів і виділення для нього IP-адресу. Так відбувається з кожною системою.

– Автоматичний розподіл (який буде використовуватися в нашому проекті): при даному способі комп'ютер отримує *IP*-адреси з мережевого «*pool'a*», виділеного адміністратором.
– Динамічний розподіл: спосіб схожий на автоматичний, але з однією умовою – всі адреси даються в тимчасову оренду для користувача.

Крім розподілу IP-адрес між клієнтами, *DHCP* може повідомляти клієнтові про додаткові параметри, які необхідні для нормальної роботи. Існує список часто використовуваних параметрів:

– Маска підмережі.
– *IP*-адреса маршутизатора.
– Ім'я домену *DNS*;.
– Адреса сервера *DNS*.

У цій схемі можна побачити основний принцип отримання *IP*-адреси:

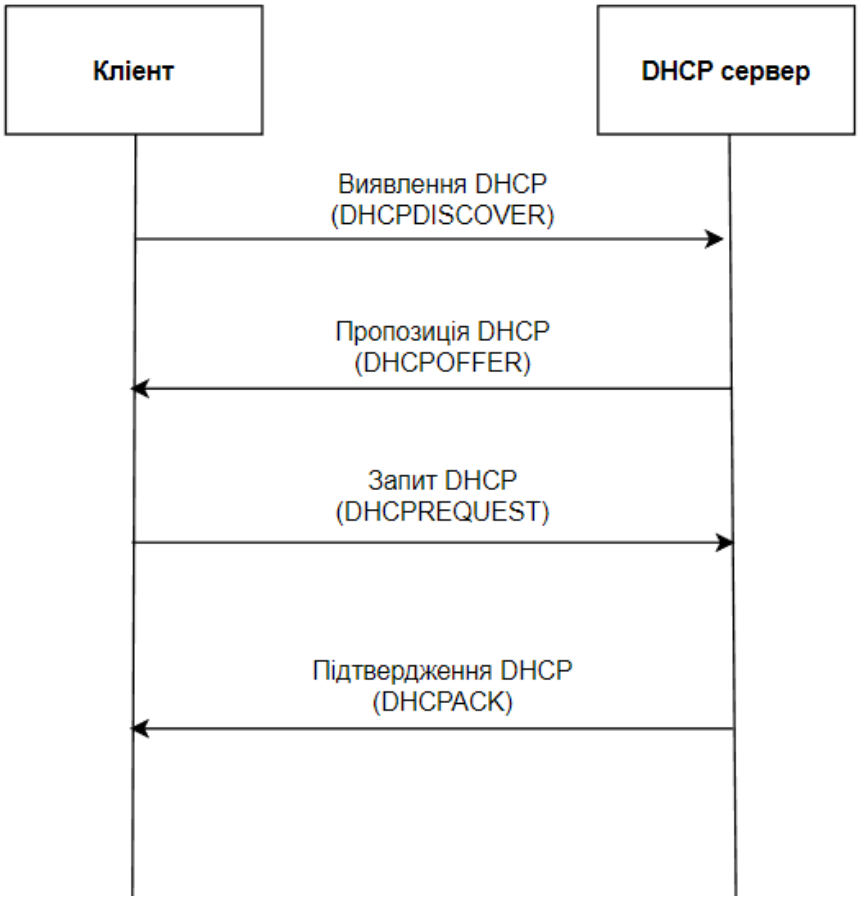

Рисунок 2.4 – Процес отримання *IP*-адреса

1. Виявлення *DHCP*. У нашому випадку тонкий клієнт на ім'я *IP*-адреси надсилає запит типу *DHCP DISCOVER*, відправляючи даний запит сам клієнт має адресу 0.0.0.0, а в якості адреси призначення використовує 255.255.255.255.

Таким чином, тонкий клієнт «пінгує» мережу на наявність *DHCP* сервером.

2. Пропозиція *DHCP*. Після виявлення *DHCP* сервера клієнт отримує відповідь *DHCPOFFER* в якому є необхідні інструкції таки як: *IP*-адреса; маска підмережі; Основний шлюз; *DNS* сервер.

3. Запит *DHCP*. *MAC*-адреса тонкого клієнта заноситься в базу домену і там фіксується прописуючи йому статичний *IP*. Цей *IP* надалі йому видаватися при вході.

4. Підтвердження *DHCP*. Це фінальний етап визначення *IP*-адреси для тонкого клієнта. Надалі від типу реєстрації адреси на домені, цей тонкий клієнт буде отримувати на сваю *MAC*-адресу – *IP*-адресу.

2.6 Характеристика протоколу *TFTP*

Простим протоколом передачі файлів є *TFTP*. Як правило, він використовується для завантаження бездискових систем (наприклад, робочих станцій або *X*-терміналів).

TFTP використовує *UDP* на відміну від протоколу передачі файлів (*FTP*), який використовує *TCP*.

Це зроблено для того, щоб зробити протокол максимально простим і компактним. Реалізації *TFTP* можуть міститися в енергонезалежній пам’яті (*ROM*) разом із необхідними *UDP*, *IP* та драйверами пристроїв. Ми використовували протокол *TFTP*. Він видавав *TFTP* запит, після того як отримав свою *IP*-адресу з використанням *RARP*.

RFC 1350 [*Sollins* 1992] є офіційною специфікацією *TFTP* другої версії. [*Stevens* 1990] надає повні вихідні коди реалізації *TFTP*-клієнта і сервера таописує деяку техніку програмування, використану в *TFTP*.

Перший запит, надісланий клієнтом серверу, полягає в тому, щоб сервер прочитав або написав файл від імені клієнта.

Початковий запит, зроблений під час запуску бездискової системи, є запитом на читання (*RRQ*). П’ять форматів повідомлень *TFTP* показано на малюнку нижче. (Формати кодів операцій 1 і 2 однакові.)

Код операції (*opcode*) — це перші два байти передачі *TFTP*. Ім’я файлу у запиті на читання (*RRQ*) і запиті на запис (*WRQ*) визначає файл сервера, який клієнт хоче прочитати або записати.

Нульовий байт означає кінець файлу. Будь-яка комбінація великих і малих літер може бути використана в режимі, який є рядком *ASCII*, який називається *netascii* або октет і закінчується байтом 0. Кожен рядок закінчується послідовністю повернення каретки з 2 символів, за якою йде розрив рядка (позначається - CR/LF), *netascii* вказує, що дані є рядками тексту *ASCII*.

Можливість конвертації між цим форматом і будь-яким іншим, що використовується на локальному хості, потрібна як для клієнта, так і для сервера.

Наступний пакет даних з номером блоку 2 є відповіддю сервера. Клієнт приймає блок номер 2. Це продовжується, доки файл не буде передано.

За винятком останнього пакета, який містить від 0 до 511 байт даних, кожен пакет даних містить 512 байт даних. Клієнт вважає, що отримав останній пакет, коли він отримує пакет даних розміром менше 512 байт.

Коли надсилається запит на запис (*WRQ*), клієнт повинен надати назву файлу та режим у *WRQ*. Сервер відповідає підтвердженням (*ACK*) і номером блоку 0, якщо клієнт може писати у файлі. Сервер відповідає *ACK* і блоком номер 1 після отримання перших 512 байт файлу від клієнта. Підтвердження протоколу зупинки та очікування (*stop-and-wait*). Він використовується виключно в простих протоколах, таких як *TFTP*.

TCP пропонує альтернативний метод підтвердження, який забезпечує швидшу пропускну здатність. *TFTP* не призначений для збільшення пропускної здатності; скоріше, він призначений для максимально легкого встановлення.

Від *TFTP* залежить, як оброблятимуться втрачені та дубльовані пакети, оскільки *TFTP* використовує нестабільний *UDP*. Відправник передає час очікування та повторює передачу в разі втрати пакета.

Можлива поява проблеми, званої «синдромом новачка» (*sorcerer's apprentice syndrome*), яка може виникнути, якщо з обох сторін буде відпрацьовано тайм-аут і здійснена повторна передача.

[*Stevens* 1990] показує, в результаті чого може виникнути подібна проблема).

Як і в більшості *UDP* додатків, контрольна сума *TFTP* повідомлення не розраховується, а це означає, що будь-яке пошкодження даних може бути визначено тільки за допомогою контрольної суми *UDP*.

Важливо зауважити, що до пакетів *TFTP* не включається інформація про логін або пароль. Оскільки *TFTP* був створений для завантаження, він не дозволяє передавати інформацію про логін і пароль. Ця функція *TFTP* широко використовувалася хакерами для отримання копій файлу паролів *Unix* і подальшого розшифрування. Щоб запобігти такому доступу, більшість *TFTP*-серверів обмежують тип файлів, які можна завантажувати по *TFTP* (зазвичай це файли з каталогу /*tftpboot* в *Unix*-системах). У цьому каталозі містяться лише завантажувальні файли, необхідні для систем без дисків.

В *Unix*-системах *TFTP*-сервер часто змінює ідентифікатор користувача (*UID*) та ідентифікатор групи (*GID*) на параметри, які не можуть бути пов'язані з реальним користувачем, для посилення захисту.

Це обмежує доступ до загальнодоступних файлів, які можна читати і змінювати.

Простий протокол *TFTP* був створений для розміщення в ПЗП (поле запиту передачі) і використовується лише під час завантаження бездискового комп'ютера.

Він використовує протокол «*stop-and-wait*» і обмежений набір форм повідомлень. Сервер *TFTP* пропонує різні типи паралелізму, щоб численні клієнти могли завантажувати одночасно.

Сервер *TFTP* відкриває новий *UDP*-порт для кожного клієнта, оскільки *UDP* не забезпечує чіткого з'єднання між клієнтом і сервером (як *TCP*).

Це дозволяє декільком клієнтам надсилати дейтаграми, які серверний модуль *UDP* демультиплексує на основі номерів портів призначення, а не самого сервера.

Без безпеки протокол *TFTP* не може бути використаний. Більшість реалізацій обмежують доступ до *TFTP* лише тими файлами, які необхідно завантажити.

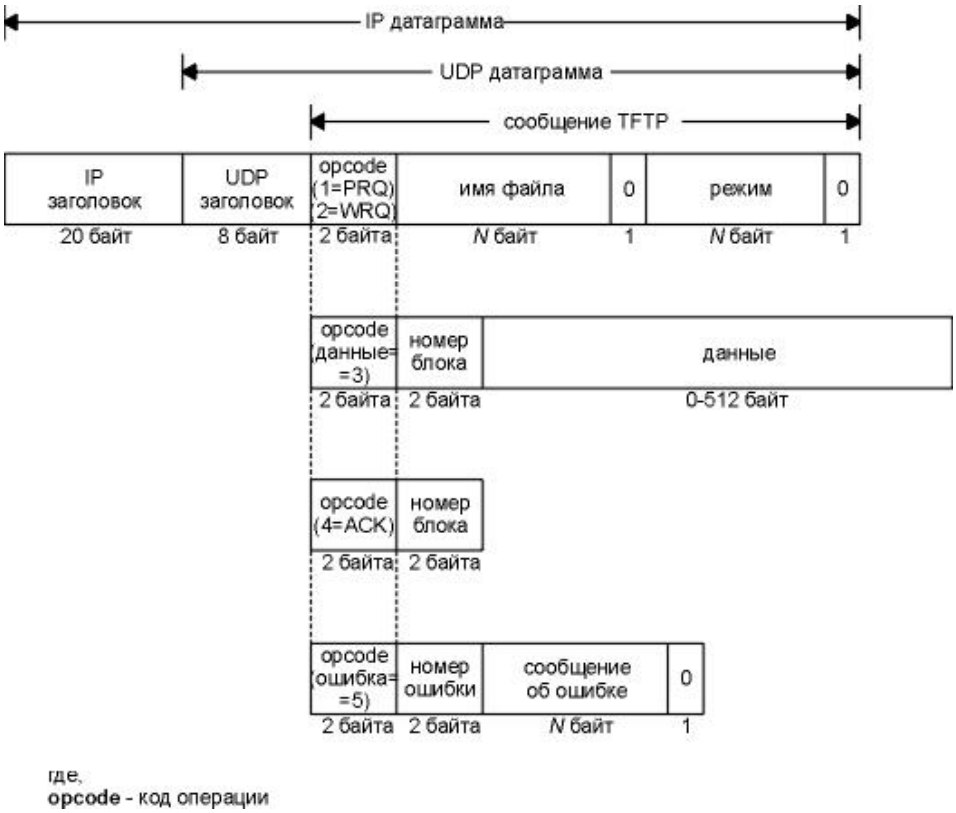

Рисунок 2.5 – Схема протоколу TFTP

2.7 Характеристика *NFS*(*Network File System*):

NFS (*Network File System*) – це протокол віддаленого файлового доступу, який дозволяє клієнтам монтувати віддалені директорії та працювати з файлами, розташованими на віддаленому сервері, так, якби вони були локальними. У контексті *LTSP NFS*-сервер використовується для зберігання та обміну файлами, необхідними для роботи клієнтів *LTSP*.

Команда *ltsp* nfs виконує такі дії:

– Встановлює необхідні пакети для *NFS*-сервера на *LTSP*-сервері, якщо вони ще не встановлені.
– Створює директорію /*opt*/*ltsp*/*images*, якщо її немає.
– Налаштовує експортовану директорію *NFS*, яка буде використовуватися для зберігання образів клієнтів *LTSP*. Зазвичай, це /*opt*/*ltsp*/*images*.
– Конфігурує файл /*etc*/*exports* для визначення правил експорту для сервера *NFS*. Зокрема він додає правило експорту для директорії /*opt*/*ltsp*/*images*, яке дозволяє клієнтам *LTSP* монтувати цю директорію.
– Перезапускає службу *NFS*-сервера, щоб зміни набули чинності.

Команда *ltsp nfs* налаштовує *NFS*-сервер для використання як сховища образів клієнтів *LTSP* та забезпечує доступ клієнтів до необхідних файлів для їхньої роботи. Це дозволяє економити ресурси комп'ютерів, оскільки операційна система та програми запускаються на сервері, а не на клієнта. Також це дозволяє легко керувати всіма клієнтами з одного місця, що спрощує процес оновлення, встановлення та налаштування операційної системи та додатків на клієнтах.

Запускаємо бездискову станцію підключену в нашу мережу. Тепер заходимо у *boot*-меню, у якому обираємо включення через *LAN*, тобто через мережу. Для цього я підключав *IPXE*, а після того як ми обираємо запуск системи по *LAN*, завантажується образ операційної системи через мережу.

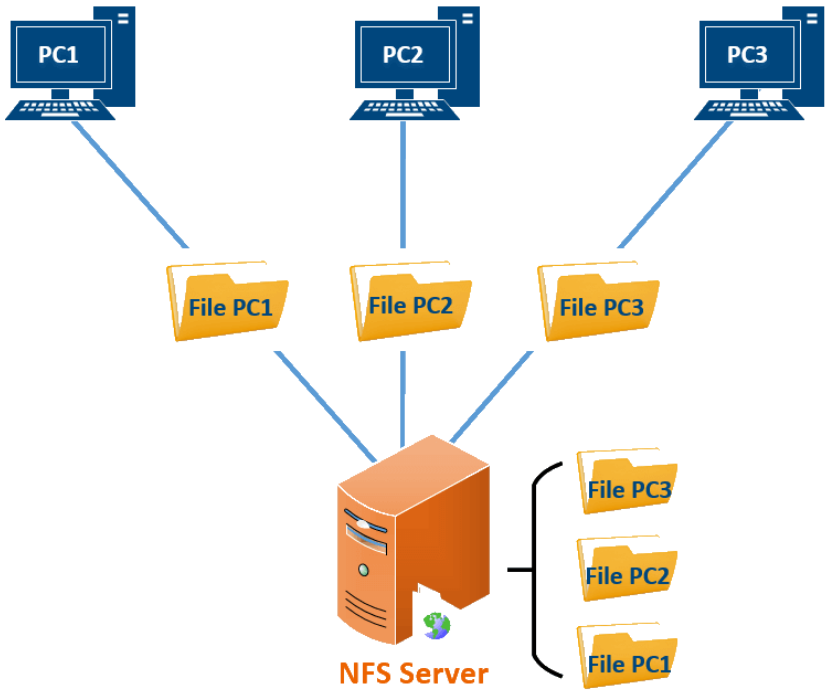

Рисунок 2.6 – Схема роботи NFS

У цьому розділі були розглянуті основні аспекти структури підприємства та мережі, що включає опис його функціональних підрозділів і взаємозв'язок між ними, вимоги до надійності та етапи створення мережі.

Також було проаналізовано структуру мережі та її вимоги до надійності. Було запропоновано заходи щодо покращення мережі, включаючи резервне копіювання, системи захисту від вірусів та атак хакерів, а також використання більш надійного обладнання.

Для створення мережі було виділено етапи, починаючи від вибору типу мережі, вибору обладнання, проведення кабельної прокладки та налаштування систем безпеки.

Ці рекомендації можуть бути використані для оптимізації роботи підприємства та підвищення якості роботи мережі.

РОЗДІЛ 3

РОЗРОБКА ФУНКЦІОНАЛЬНОЇ СХЕМИ ПРОЕКТОВАНОЇ ЛОКАЛЬНОЇ МЕРЕЖІ

3.1 Вибір обладнання для проектованої мережі

Для побудови мережі, що працює на основі *LTSP*, необхідно як мінімум один пристрій, що працює як сервер *LTSP*, і кілька терміналів, які підключатимуться до сервера.

Кількість портів на комутаторі та роутері залежить від кількості пристроїв, які підключатимуться до мережі. У нашому випадку конфігурації мережі, для підключення одного сервера *LTSP* та кількох терміналів, достатньо буде 5-8 портів на комутаторі та 2 порти на роутері.

Функції *L*2 комутатора включають забезпечення зв'язку між пристроями в одній локальній мережі і поділ трафіку на порт-базисі. Функції *L*3 комутатора включають маршрутизацію між різними мережами.

Функції *L*3 роутера включають маршрутизацію між різними мережами, а також фільтрацію трафіку і забезпечення безпеки мережі.

У нашій конфігурації мережі достатньо буде використовувати *L*2 комутатори і *L*3 роутер. Якщо мережа буде розширюватися в майбутньому, то може знадобитися додавання комутаторів *L*3 для забезпечення маршрутизації між різними мережами.

Для розрахунку вимог до обладнання на 10 користувачів, які використовують офісні додатки та браузер, можна використати такі дані:

- Середня кількість одночасних користувачів: 5
- Середня кількість запитів на сервер: 10 на хвилину
- Середній розмір запиту на сервер: 1 Мб
- Середній розмір відповіді сервера на запит: 1 Мб
- Середня кількість запитів на Інтернет: 5 на хвилину
- Середній розмір запиту на Інтернет: 2 Мб
- Середній розмір відповіді на запит з Інтернету: 2 Мб

Для оцінки вимог до обладнання можна використовувати такі формули:

Кількість одночасних користувачів: Середня кількість одночасних користувачів = Загальна кількість користувачів / 2, тобто

$$\frac{10}{2} = 5(\text{користувачів}) \quad (3.1)$$

Пропускна здатність мережі: Пропускна здатність мережі = Середня кількість запитів на сервер * (Середній розмір запиту на сервер + Середній розмір відповіді сервера на запит) + Середня кількість запитів на Інтернет * (Середній розмір запиту на Інтернет + Середній розмір відповіді на запит з Інтернету), тобто:

$$10 * \big((1\ \text{Мб} + 1\ \text{Мб}) + 5 * (2\ \text{Мб} + 2\ \text{Мб})\big) = 220\ \text{Мб/хв} \quad (3.2)$$

Розмір оперативної пам'яті на сервері: Розмір оперативної пам'яті на сервері = Кількість одночасних користувачів * 2 Гб.

$$5 * 2 = 10\ \text{Гб} \quad (3.3)$$

Продуктивність процесора: Продуктивність процесора = Кількість ядер процесора * Частота процесора * Коефіцієнт використання CPU.

$$10 * 2.2 * 0.8 = 17.6\ \text{ГГц} \quad (3.4)$$

Розмір жорсткого диска на сервері: Розмір жорсткого диска на сервері = Обсяг даних * Коефіцієнт зростання даних.

$$2 * 1 = 2\ \text{ТБ (терабайти)} \quad (3.5)$$

Кількість портів комутатора: Кількість портів комутатора = Кількість одночасних користувачів + 2.

$$10 + 2 = 12\ \text{портів} \quad (3.6)$$

Використовуючи ці формули і дані вище, можна шукати обладнання, які потрібні для нашої мережі.

3.1.1 Вибір роутера для проектованої мережі

Важливо визначитися з типом гаджета перед тим, як почати вивчати ключові якості.

Багато провайдерів, які ще не перейшли на оптику, використовують *Ethernet* або *FTTB*, що наразі є найпопулярнішим варіантом. Він має можливість передавати сигнал по кабелю і бездротовим способом.

При підключенні до оптоволоконної мережі моделі *CPON*, *CEPON* і *PON* забезпечують вищу швидкість передачі даних, ніж попередній варіант. Однак, перш ніж купувати одну з цих моделей, переконайтеся, що до вашої оселі підведено саме оптику, а не стандартну виту пару.

Універсальний роутер поєднує в собі переваги декількох попередніх варіантів. *Ethernet* + 3*G* – це найбільш практичний універсальний гаджет, що дозволяє роздавати інтернет як вдома, так і на вулиці. Звичайно, якщо є сигнал від мобільної мережі.

Для нашої бездискової мережі роутер повинен мати наступне:

- Роутер повинен підтримувати *VLAN* (*Virtual Local Area Network*), щоб поділити трафік на сегменти, пов'язані з певними клієнтами.
- Роутер повинен мати можливість налаштувати *DHCP* (*Dynamic Host Configuration Protocol*), щоб автоматично призначати *IP*-адреси та іншу мережу для клієнтів.
- Роутер повинен мати підтримку *NAT* (*Network Address Translation*), щоб переводити локальні *IP*-адреси клієнтів у глобальні *IP*-адреси, що використовуються в Інтернеті.
- Роутер повинен мати підтримку портів, які використовуються *LTSP*. Зокрема, порти 67 та 69 (*DHCP* та *TFTP* відповідно) повинні бути відкриті для вхідного трафіку.
- Роутер повинен забезпечувати надійну та безпечну передачу даних між сервером та клієнтами. Для цього можна використовувати протоколи *VPN* (*Virtual Private Network*) або *SSH* (*Secure Shell*).
- Щоб гарантувати безперебійну роботу програм на клієнтах, маршрутизатор повинен мати достатньо високу швидкість передачі даних і низьку затримку.

- Роутер повинен мати можливість забезпечувати якість обслуговування (*Quality of Service*), щоб гарантувати мінімальну затримку та втрати пакетів для програм у реальному часі, таких як *VoIP* (голосовий зв'язок через Інтернет) та відеоконференції.
- Роутер повинен мати налаштування безпеки, такі як фільтрацію *MAC*-адресу та брандмауер, щоб запобігти несанкціонованому доступу до мережі та забезпечити її безпеку.

У деяких версіях також є *USB*-порт, який слугує додатковою функцією. За потреби, до нього можна підключити зовнішній жорсткий диск або бездротовий модем.

Для розрахунку очікуваного обсягу трафіку в мережі на *LTSP*, коли клієнти використовують лише браузер для пошти та завантаження документів, можна провести наступні оцінки:

- Розмір середньої електронної пошти – 100 кБ.
- Кількість листів, які надсилають та отримують користувачі в середньому за день – 10.
- Таким чином, обсяг трафіку, пов'язаний із поштою, становитиме: 100 кБ * 10 = 1 МБ на день.
- Середній розмір завантаженого документа - 1 МБ.
- Припустимо, кожен користувач завантажує по одному документу на день.
- Таким чином, обсяг трафіку, пов'язаний зі скачуванням документів, становитиме: 1 МБ * 10 = 10 МБ на день.
- Загальний обсяг трафіку на одного користувача на день становитиме 11 МБ.
- Для розрахунку загального обсягу трафіку у мережі необхідно враховувати кількість користувачів. Якщо припустити, що у мережі на *LTSP* будуть 10 користувачів, загальний обсяг трафіку щодня становитиме: 11 МБ * 10 = 110 МБ щодня.

Таким чином, для мережі на *LTSP*, де клієнти використовують лише браузер для пошти та завантаження документів, очікуваний обсяг трафіку буде відносно невисоким.

Список моделей для покупки:

1. *Xiaomi Mi Wi-Fi mini* - мініатюрний бездротовий роутер з високою швидкістю передачі даних та простим керуванням через мобільний додаток.

2. *TP-LINK TL-WA901ND* - бездротова точка доступу з високою потужністю передачі сигналу та підтримкою режиму мосту.

3. *ASUS RT-N56U* - двохдіапазонний бездротовий роутер з швидкою швидкістю передачі даних, до 300 МБ/сек.

4. *TP-LINK TL-WR841N* - доступний бездротовий роутер з підтримкою режиму мосту та контролем пропускної здатності.

5. *ZyXEL Keenetic Start* - бездротовий роутер з підтримкою технології *SmartBeam* для збільшення покриття *Wi-Fi* сигналом та функцією контролю доступу.

6. *Huawei E*5330 - портативний бездротовий роутер з підтримкою *3G*/*4G* мереж та можливістю підключення до 10 пристроїв одночасно.

7. *TP-LINK Archer C*50 - багатодіапазонний бездротовий роутер з високою швидкістю передачі даних і підтримкою технології *Beamforming* для забезпечення стабільного та швидкого *Wi-Fi* сигналу, а також функцією гостьової мережі для забезпечення безпеки основної мережі.

Таблиця 3.1

Порівняльна таблиця

Модель	**Швидкість мережі (Мбіт/с)**	**Кількість портів**	**Ціна (грн)**	**Підтримувані технології**	**Засіб захисту**
Xiaomi Mi Wi-Fi mini	до 300	2	400	802.11*b/g/n*	*WPA*/*WPA2*

Продовження таблиці 3.1

TP-LINK TL-WA901ND	до 300	4	600	802.11*b/g/n*	*WEP/WPA/WPA2*
ASUS RT-N56U	до 300	4	900	802.11*a/b/g/n*	*WEP/WPA/WPA2*
TP-LINK TL-WR841N	до 300	4	350	802.11*b/g/n*	*WEP/WPA/WPA2*
ZyXEL Keenetic Start	до 300	4	450	802.11*b/g/n*	*WEP/WPA/WPA2*
Huawei E5330	до 150	1	250	802.11*b/g/n*	*WEP/WPA/WPA2*
TP-LINK Archer C50	до 1200	4	800	802.11*a/b/g/n/ac*	*WEP/WPA/WPA2/WPA3*

Виходячи з параметрів та вимог до мережі, яку ми обговорювали раніше, роутер *TP-LINK Archer C*50 є гарним варіантом для створення надійної та продуктивної мережі.

*TP-LINK Archer C*50 підтримує високу швидкість передачі даних бездротовою мережею, що дозволить користувачам підключатися до мережі з високою швидкістю і без перебоїв. Крім того, він має досить потужний процесор та оперативну пам'ять, щоб забезпечити продуктивність для 10 користувачів, які використовують браузер для пошти та скачування документів.

3.1.2 Вибір комутатора для проектованої мережі

Для комутатора у нашій мережі на 10 користувачів можна використовувати комутатор з 8 портами 10/100 Мбіт/с. При використанні такого комутатора можна розраховувати на достатню швидкість передачі всередині мережі для роботи офісних додатків і доступу в Інтернет.

Критерії вибору комутатора:

- Кількість портів: для мережі з 10 користувачів достатньо 8 портів, але бажано вибирати комутатор з великим запасом портів у разі збільшення кількості користувачів.

- Швидкість портів: щоб гарантувати достатню швидкість передачі даних, комутатор повинен мати порти 10/100 Мбіт/с.
- Підтримка функції *Quality of Service* (*QoS*) – це дозволяє керувати пріоритетами передачі даних у мережі та забезпечити більш високий пріоритет для програм, які потребують високої швидкості передачі даних.
- Підтримка *Virtual LAN* (*VLAN*) – дозволяє розбити мережу на окремі сегменти, покращуючи безпеку та продуктивність мережі.

Декілька варіантів комутаторів:

- *TP-Link TL-SG*108 – 8 портів 10/100/1000 Мбіт/с, *QoS, VLAN*.
- *D-Link DGS*-108 – 8 портів 10/100/1000 Мбіт/с, *QoS, VLAN*.
- *NETGEAR G*S308 – 8 портів 10/100/1000 Мбіт/с, *QoS, VLAN*.

Таблиця 3.2

Порівняльна таблиця

Комутатор	***TP-Link TL-SG108***	***D-Link DGS-108***	***NETGEAR GS308***
Кількість портів	8	8	8
Швидкість портів	10/100/1000 Мб/с	10/100/1000 Мб/с	10/100/1000 Мб/с
Підтримка *VLAN*	Так	Так	Так
Підтримка *PoE*	Ні	Ні	Ні
Ціна	1149,00 грн	1699,00 грн	1532,00 грн

Найбільш привабливий варіант це: *TP-Link TL-SG108*. Він має всі необхідні функції для невеликої мережі з 10 користувачів та має низьку ціну у порівнянні з іншими варіантами.

3.1.3 Вибір сервера для проектованої мережі

Для розрахунку потрібного сервера для мережі з приблизно 10 користувачами, необхідно врахувати такі фактори:

- Обсяг трафіку: враховуючи, що кожен користувач буде працювати з графічним інтерфейсом на віддаленому сервері, сервер повинен мати достатню швидкість передачі даних.

- Обсяг пам'яті: якщо кожен користувач працює з великими файлами або запускає потужні програми, то необхідно враховувати, що сервер повинен мати достатню кількість оперативної пам'яті.
- Кількість ядер процесора: визначає, скільки задач може обробляти сервер одночасно. Для мережі з 10 користувачами сервер повинен мати принаймні 4 ядра.
- Зберігання даних: Сервер повинен мати достатній обсяг зберігання даних для потреб мережі *LTSP*. Також, варто враховувати можливість налаштування *RAID*-масиву для забезпечення надійності зберігання.

Ось приблизні вимоги щодо характеристик сервера для мережі:

- Процесор: 17.6 ГГц або краще.
- Оперативна пам'ять: принаймні 10 ГБ або краще.
- Зберігання: принаймні 2 х 1 ТБ або краще.
- Мережеві інтерфейси: принаймні 2 х 1 Гбіт/с.

Деякі приклади серверів, які можуть бути використані для нашої мережі, включають *Dell PowerEdge T*440, *HP ProLiant DL*360 *Gen*10, *Supermicro SYS*-5019*S-L* і *Lenovo ThinkSystem ST*250.

Таблиця 3.3

Порівняльна таблиця характеристик серверів

Модель сервера	**Dell PowerEdge T440**	**HP ProLiant DL360 Gen10**	**Supermicro SYS-5019S-L**	**Lenovo ThinkSystem ST250**
Процесор	Intel Xeon Silver 4114	Intel Xeon Silver 4114	Intel Xeon E-2136	Intel Xeon E-2174G
Кількість ядер	10	10	6	4
Оперативна пам'ять	16 ГБ DDR4 ECC	16 ГБ DDR4 ECC	8 ГБ DDR4 ECC	8 ГБ DDR4 ECC
Зберігання	2 х 1 ТБ SATA HDD	2 х 1 ТБ SATA HDD	1 х 512 ГБ SSD	1 х 1 ТБ SATA HDD
Мережевий інтерфейс	4 х 1 Гбіт/с	4 х 1 Гбіт/с	2 х 1 Гбіт/с	2 х 1 Гбіт/с

Продовження таблиці 3.3

Графічний адаптер	NVIDIA NVS 310	Integrated	Integrated	Integrated
Гарантія	3 роки	3 роки	3 роки	3 роки

Ця таблиця демонструє, що сервер *Dell PowerEdge T*440 має більш потужний процесор та більше оперативної пам'яті, у порівнянніі з деякими іншими серверами. Крім того, він має більшу кількість мережевих інтерфейсів, що дозволяє краще керувати трафіком в мережі.

Наявність 2 жорстких дисків у *Dell PowerEdge T*440 також може бути корисним для налаштування *RAID*-масиву та забезпечення надійності зберігання даних.

Отже, *Dell PowerEdge T*440 буде гарним вибором для нашої мережі, бо нам потрібна висока продуктивність та надійність.

3.1.4 Вибір тонкого клієнта для проектованої мережі

Для того щоб побудувати мережу на тонких клієнтах бажано купувати готові тонкі клієнти (Тонкий клієнт - це комп'ютер, який не має своїх власних ресурсів для обробки даних та виконання завдань, а натомість використовує ресурси віддаленого сервера через мережу. Таким чином, вся обробка даних та обчислень відбувається на сервері, а тонкий клієнт лише отримує результати та виводить їх на екран).

Для бездискової мережі, побудованої на основі *LTSP*, підходять різні моделі тонких клієнтів, які можуть відрізнятися за характеристиками та вартістю.

Критерії вибору тонкого клієнта:

- Характеристики процесора та оперативної пам'яті.
- Мережевої картки (1 гігабіт в секунду).
- Підтримка підключення до монітора та інших пристроїв.
- Вартість (середня).

Деякі моделі тонких клієнтів, які можна розглянути для бездискової мережі на основі *LTSP*, включають:

- *HP t*430 *Thin Client*.
- *Dell Wyse* 3040 *Thin Client*.
- *Raspberry Pi Thin Client*.

Таблиця 3.4

Порівняння тонких клієнтів

Модель	**Характеристики процесора**	**Підтримка відеокарти**	**Підтримка мережевої картки**	**Підтримка монітора**	**Вартість**
HP t430 Thin Client	Intel Celeron N4000	До 4K	Gigabit Ethernet	DisplayPort, VGA, HDMI	Висока
Dell Wyse 3040 Thin Client	Intel Atom x5-Z8350	До 2K	Gigabit Ethernet	DisplayPort, HDMI	Середня
Raspberry Pi Thin Client	Broadcom BCM2837B0	До 1080p	Ethernet	HDMI, Composite	Низька

На підставі порівняльної таблиці можна зробити висновок, що для бездискової мережі, можна обрати *Dell Wyse* 3040 *Thin Client*. Він має достатні характеристики для підтримки більшості завдань, що виникають у бездискових середовищах, і при цьому має середню вартість. До того ж, він має підтримку підключення до різних типів моніторів, включаючи *DisplayPort* та *HDMI*, що дозволить підключати його до різних пристроїв. Таким чином, обираючи *Dell Wyse* 3040 *Thin Client*, ми отримаємо надійний та ефективний тонкий клієнт для нашої мережі, що відповідає більшості потреб користувачів.

3.1.5 Висновок до обладнання

Отже, ми маємо:

- Сервер *Dell PowerEdge T*440 має досить потужний процесор, що дозволяє йому ефективно обробляти запити від клієнтів при

використанні технології *LTSP*. Крім того, сервер має значний обсяг оперативної пам'яті, що дозволяє підтримувати високу продуктивність навіть при роботі з декількома клієнтами.

- Комутатор *TP-Link TL-SG*108 – підтримує передачу даних на швидкості 1 Гбіт/сек та має 8 портів, що дозволяє підключати до нього кілька клієнтських пристроїв. Це забезпечує швидку передачу даних.
- Роутер *TP-LINK Archer C*50 – також підтримує передачу даних на швидкості до 1 Гбіт/сек і має гарну продуктивність при роботі з кількома клієнтами.
- Тонкий клієнт *Dell Wyse* 3040 *Thin Client*, має передачу даних на 1 Гбіт/сек і має непоганий процесор, що дозволить користувачам працювати без будь-яких проблем.

З урахуванням характеристик нашого сервера, комутатора та роутера, можна очікувати досить швидке завантаження операційної системи на клієнтські пристрої при використанні технології *LTSP*. Час завантаження буде залежати від швидкості передачі даних між сервером і клієнтськими пристроями. У середньому час завантаження операційної системи на клієнтський пристрій при використанні *LTSP* буде становить від декількох секунд до 1-2 хвилин.

3.2 Налаштування роутера

Одна з ключових функцій нашої мережі буде віддалене управління. Ми повинні приділить більше уваги на роутер або маршрутизатор. Так як основна його робота – це дозволяти машинам виходити в мережу.

В налаштуваннях роутера варто приділити увагу на такі пункти:

- Налаштування *DHCP*.
- Резервування адрес.
- Налаштування статичної адреси.

Налаштування статичної адреси: насамперед, входимо в налаштування роутера. В адресному рядку браузера вводимо 192.168.0.1,

Для входу в роутер у вас запитає логін і пароль, за замовчуванням (якщо його спеціально не змінювали) логін: *admin*, пароль: *admin*. Зліва в меню натискаємо вкладку «Мережа». У списку, що розкрився обираємо «*WAN*».

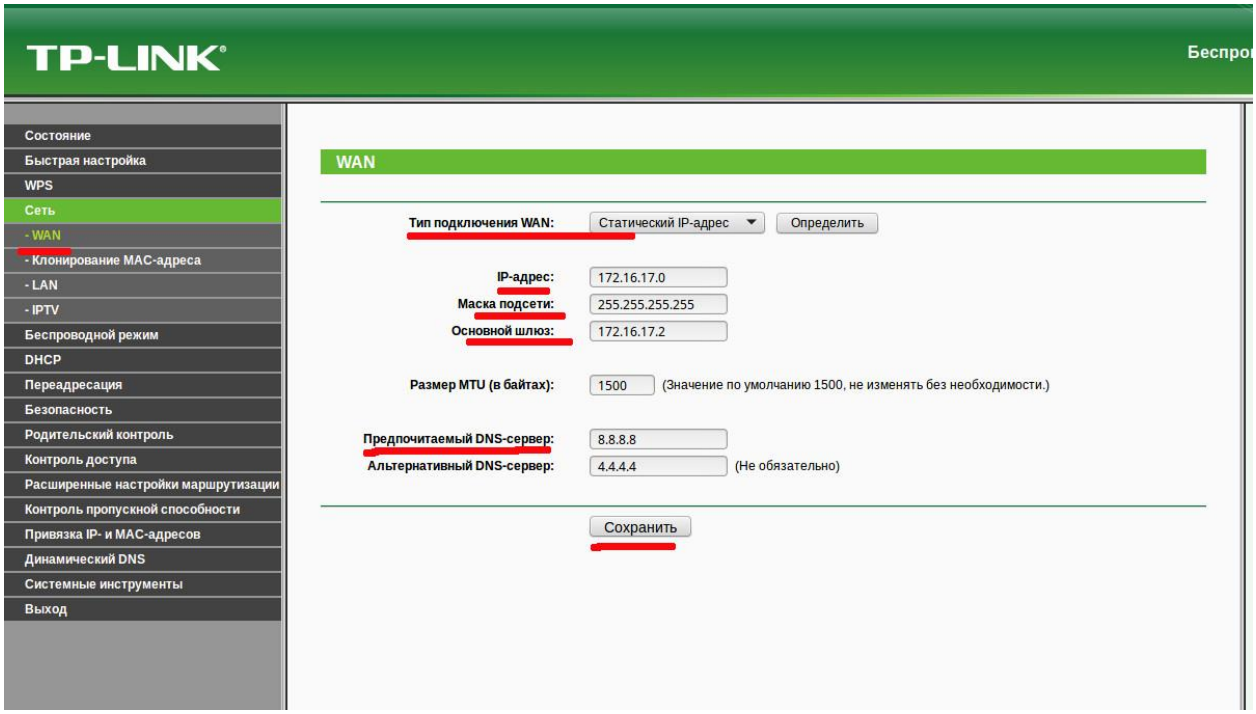

Рисунок 3.1 – Налаштування статичної адреси

Навпроти напису «Тип підключення *WAN*» у списку, що випадає, оберіть «Статична *IP*-адреса».

В інші поля вводимо дані отримані від провайдера і ті, що отримали з *IP*-калькулятора, як відображено на малюнку вище.

Щоб активувати зміни, необхідно відкрити меню зліва та вибрати «Системні інструменти». Потім обираємо «Перезавантаження» зі списку і натискаємо кнопку «Перезавантажити» у вікні.

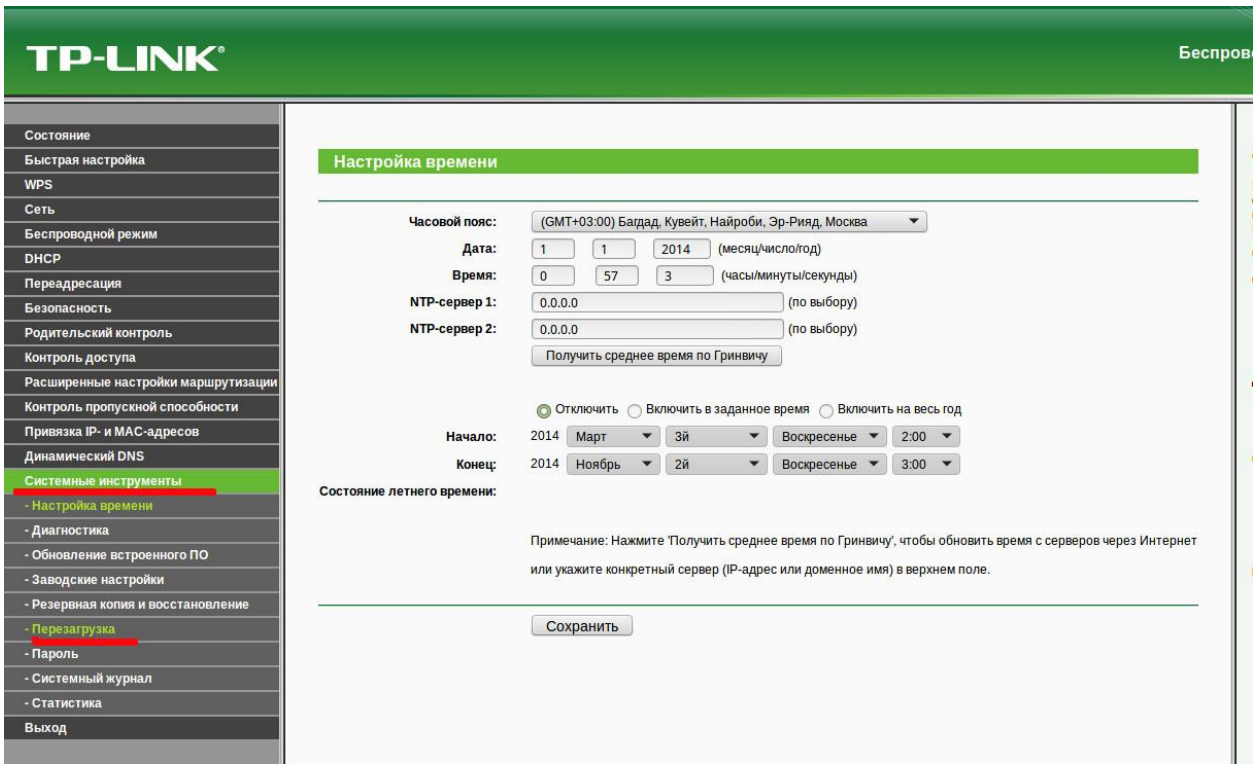

Рисунок 3.2 – Перезавантаження роутеру

Після перезавантаження, роутер буде готовий до використання і ми зможемо використовувати статичну *IP*-адресу.

Налаштування *DHCP*: у цьому пункті нам треба перевірити як працює *DHCP*. Так само варто приділити увагу на наш діапазон *IP*-адреси – надалі це нам допоможе виділити *IP-pool*.

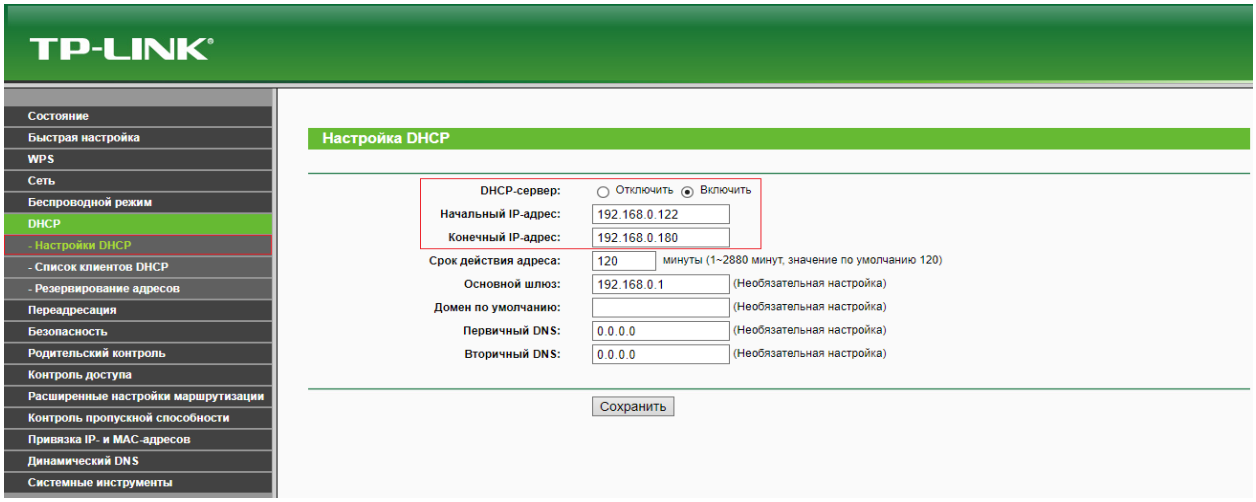

Рисунок 3.3 – Провірка pool'а DHCP

Резервування адрес: цей пункт нам знадобиться надалі, а зараз треба перевірити чи немає резервованих IP-адрес на цьому маршрутизаторі.

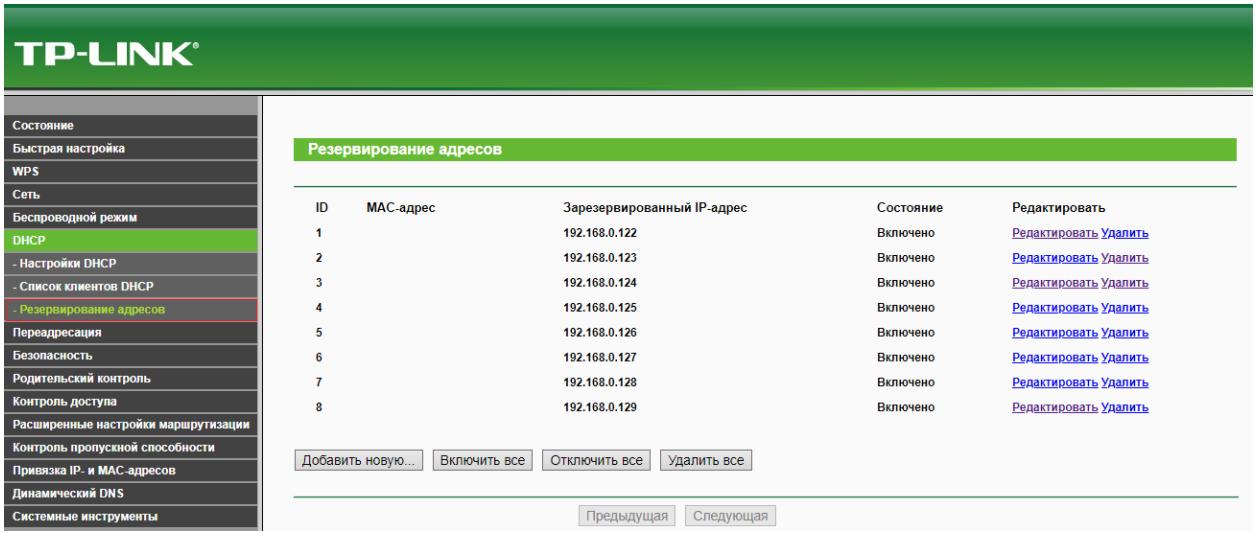

Рисунок 3.4 – Список з зарезервованими адресами

Поки що ми можемо залишити налаштування роутера, так як в подальшому ми отримаємо *MAC*-адреси від наших клієнтів і серверів, що в подальшому ми зарезервуємо.

3.3 Налаштування віртуального серверу

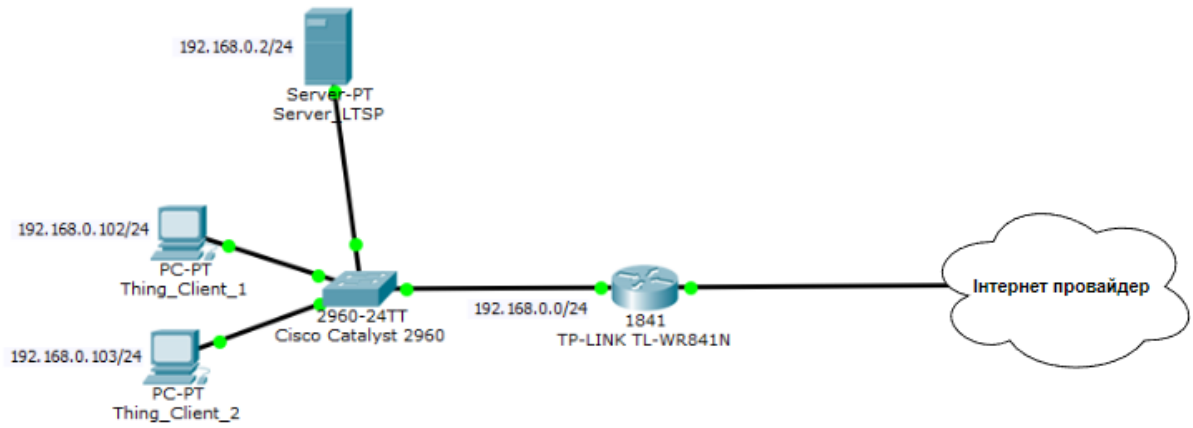

Рисунок 3.14 Схема мережі

Віртуальна сервер (*LTSP_Server*) буде служити для *LTSP* на якому буде *DHCP*, *NFS* і *PXE*. Для цього проекту машині було виділено 4 ГБ оперативної пам'яті. 4 ядра процесора і 20 ГБ жорсткого диска, а також – налаштований мережевий адаптер.

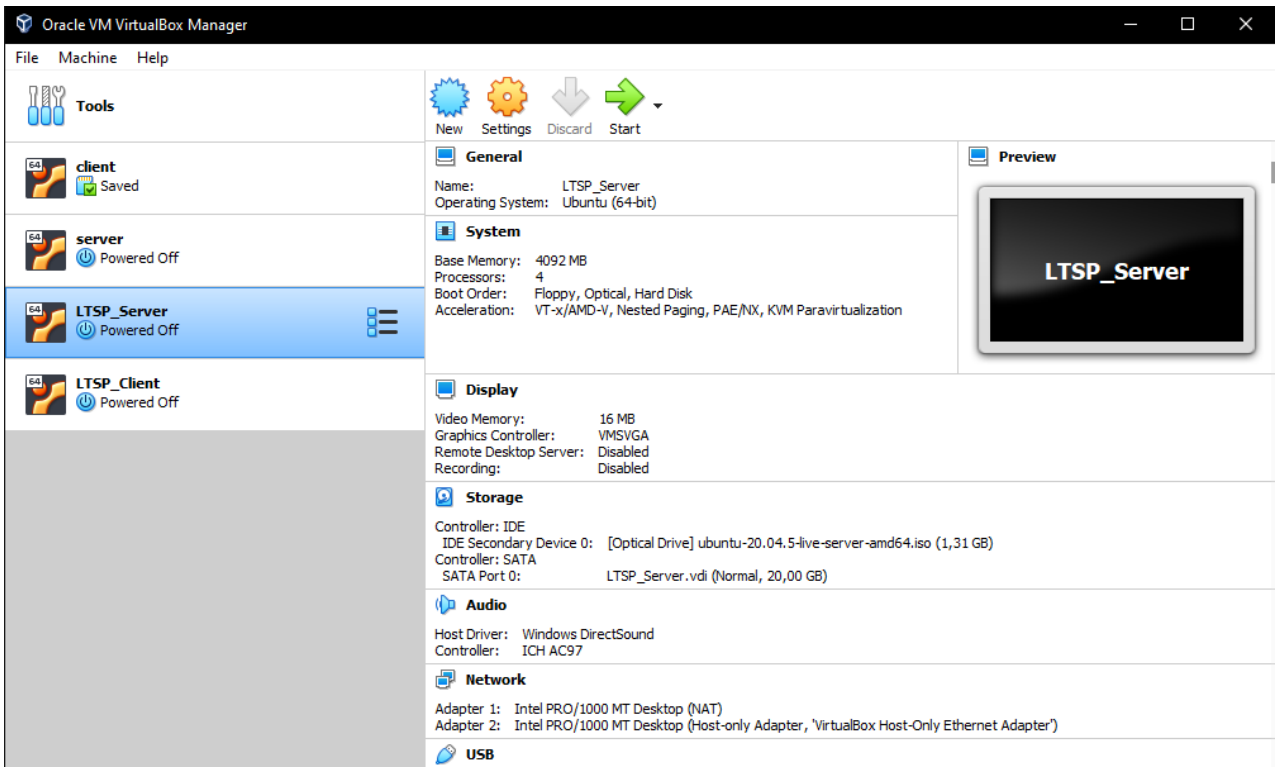

Рисунок 3.15 – Кінцевий вигляд налаштувань віртуального сервера

Після налаштування потрібно провести установку *LTSP*:

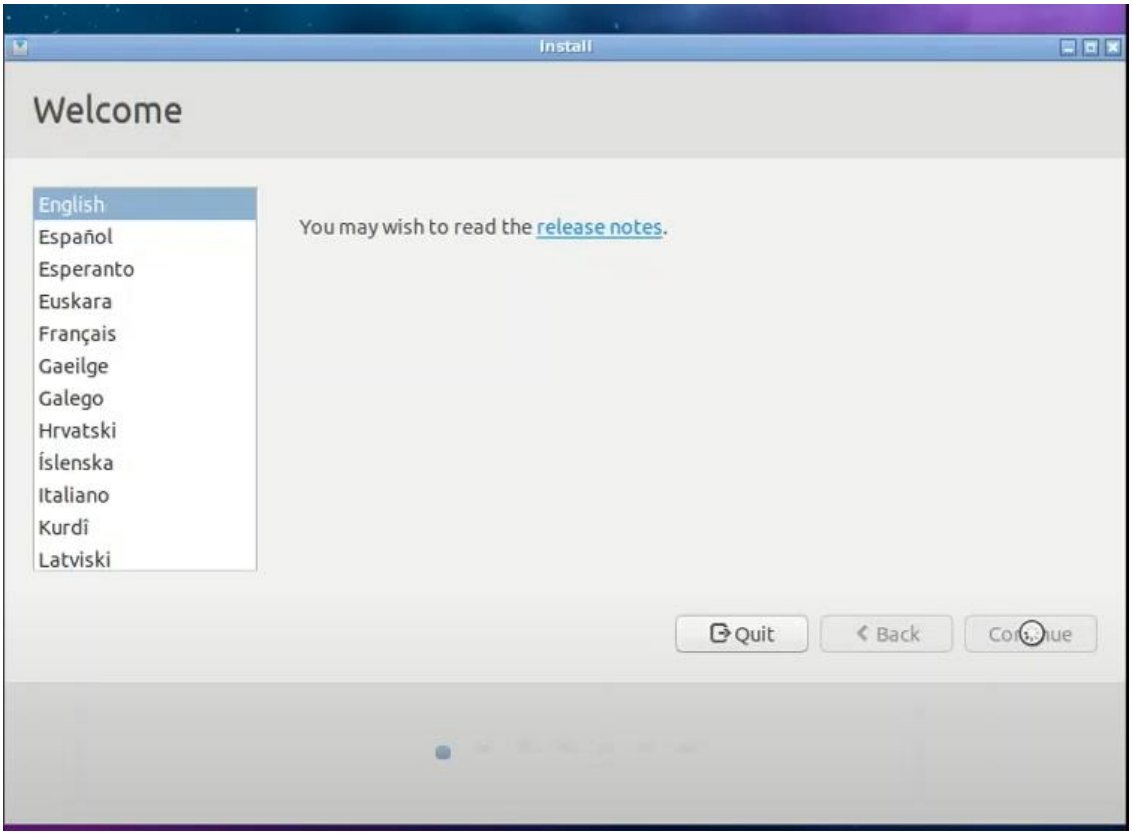

Рисунок 3.16 – Вибір мови та регіону

Перед інсталяцією *LTSP*, необхідно оновити систему до останньої версії. Для цього виконуємо команди, які оновлять пакети до останньої версії, встановлять необхідні додаткові пакети та приведуть систему в поточний стан:

```
sudo apt-get update
sudo apt-get upgrade
```

Рисунок 3.17 – Виконання команди оновлення системи

Після цього треба встановити *LTSP*, для цього виконуємо такі команди:

```
ltsp@ltsp-VirtualBox:~$ sudo su
[sudo] password for ltsp:
root@ltsp-VirtualBox:/home/ltsp# add-apt-repository ppa:ltsp
```

Рисунок 3.18 – Виконання команди переходу до прав адміністратора та встановлення *LTSP*

Ця команда є обов'язковою для дистрибутивів до 2020 року, які мають старіший *LTSP5*, і необов'язковою, але рекомендованою для нових дистрибутивів.

Встановлюємо серверні пакети *LTSP*, завдяки командам *apt install --install-recommends ltsp ltsp-binaries dnsmasq nfs-kernel-server openssh-server squashfs-tools ethtool net-tools epoptes*

```
root@ltsp-VirtualBox:/home/ltsp# apt install --install-recommends ltsp ltsp-bina
ries dnsmasq nfs-kernel-server openssh-server squashfs-tools ethtool net-tools e
poptes
```

Рисунок 3.19 – Встановлення сервісних пакетів LTSP

Команда *apt install --install-recommends ltsp ltsp-binaries dnsmasq nfs-kernel-server openssh-server squashfs-tools ethtool net-tools epoptes* використовується для встановлення пакетів, пов'язаних із системою віддаленого запуску клієнтів *Linux* (*LTSP*) та додаткових утилітів.

ltsp та *ltsp-binaries* - це пакети, які надають клієнтську та серверну частини системи *LTSP* відповідно. Вони необхідні для налаштування та використання системи віддаленого запуску клієнтів *Linux*.

dnsmasq – це пакет, який забезпечує функції *DHCP* та *DNS*-сервера для локальної мережі.

nfs-kernel-server - це пакет, який дозволяє забезпечити загальний доступ до файлів на *LTSP*-сервері через мережну файлову систему (*NFS*).

openssh-server – це пакет, який забезпечує доступ до *LTSP*-сервера за допомогою протоколу *SSH*.

squashfs-tools – це пакет, який забезпечує можливість створення стислих файлових систем, які можуть використовуватись для образів клієнтів *LTSP*.

ethtool та *net-tools* – це пакети, які містять утиліти для налаштування та діагностики мережевих інтерфейсів на сервері *LTSP*.

epoptes – це пакет, який надає утиліту для віддаленого керування клієнтами *LTSP* із центрального комп'ютера. Він дозволяє системним адміністраторам контролювати роботу навчальних комп'ютерів, використовуючи *LTSP*.

Параметр *--install-recommends* вказує менеджеру пакетів *apt* на встановлення всіх рекомендованих пакетів, пов'язаних із цими основними пакетами. Таким чином, будуть встановлені всі необхідні пакети для повноцінної роботи системи *LTSP*.

Додаємо наш сервер до групи:

```
root@ltsp-VirtualBox:/home/ltsp# gpasswd -a ltsp epoptes
```

Рисунок 3.20 – Виконання команди, яка додає користувача до группи

Команда *gpasswd -a ltsp epoptes* використовується для додавання користувача *ltsp* до групи *epoptes* (*ltsp* – це ім’я нашого серверу). Після виконання цієї команди, користувач *administrator* матиме права доступу до ресурсів та файлів, доступних для групи *epoptes*.

gpasswd - це утиліта командного рядка *Linux*, яка призначена для керування членством у групах. Параметр *-a* використовується для додавання користувача до групи. Параметр *administrator* вказує ім'я користувача, який буде додано до групи. *epoptes* - це назва групи, до якої користувач буде додано.

Далі вводимо команду *ltsp dnsmasq:*

```
root@ltsp-VirtualBox:/home/ltsp# ltsp dnsmasq
```

Рисунок 3.21 – Виконання команди встановлення пакету dnsmasq

```
root@ltsp-VirtualBox:/home/ltsp# ltsp image /
```

Рисунок 3.22 – Виконання команди створення образу

Ця команда нам потрібна для створення образу *LTSP* клієнта. За допомогою команди *ltsp image /path/to/image*, потрібно вказати шлях до директорії, в якій буде збережено образ, але так як ми використовуємо віртуальну машину, вводимо команду на рисунку (3.21). Команда створить файли, необхідні для завантаження клієнтів через мережу за допомогою сервера *LTSP*. Ці файли включають образ операційної системи, яка завантажуватиметься на клієнтах, а також файли конфігурації та управління завантаженням.

Також нам потрібно зробити на сервері обліковий запис користувача, у мене це *client1*:

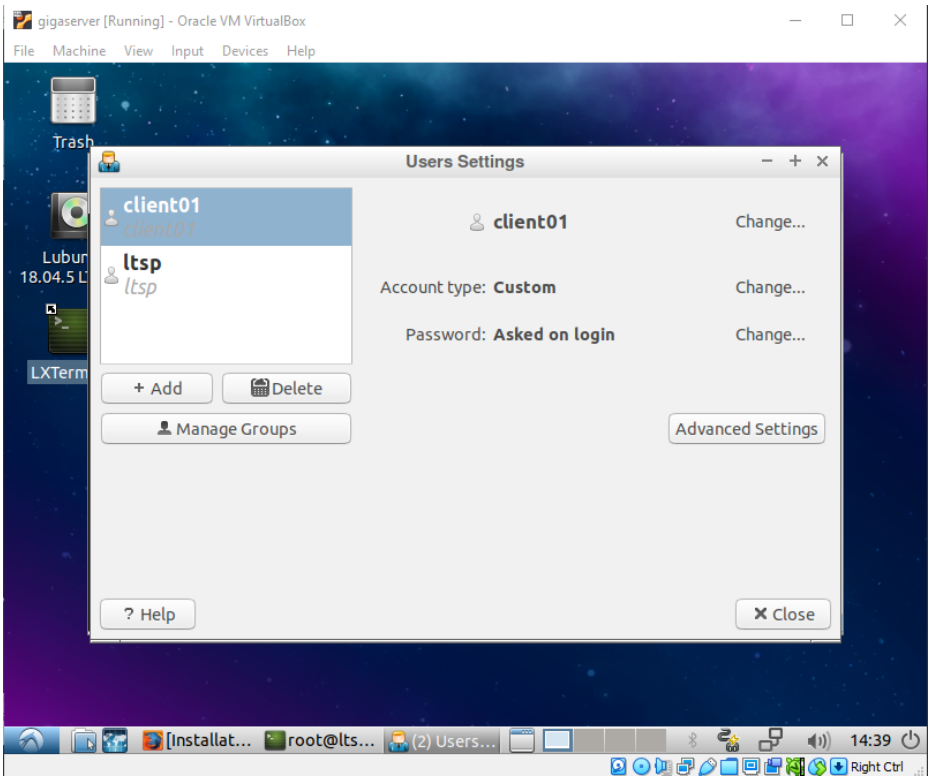

Рисунок 3.23 – Додавання облікового запису користувача

Тепер вводимо команду до командної панелі, а саме *ltsp ipxe*:

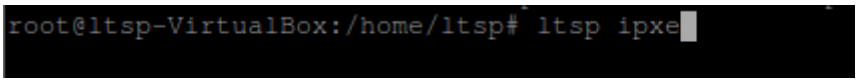

Рисунок 3.24 – Виконання команди встановлення *ipxe*

Після налаштування *ipxe*, зробим *NFS* завдяки команді *ltsp nfs*:

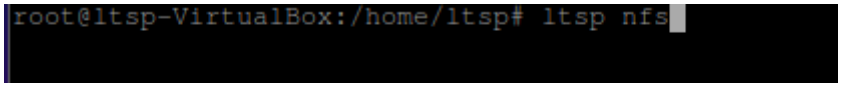

Рисунок 3.25 – Виконання команди встановлення *NFS*

Зараз наша мережа цілком собі працездатна і можна вже підключати сюди тонких клієнтів, але щоб вона працювала як треба, необхідно зробити більш детальне налаштування *DHCP*, *NFS*, *PXE*.

3.3.1 Налаштування *DHCP*

Переходимо до командної строки (*CLI*) та вводимо такі команди:

```
dhcp enable
dhcp server ip-pool pool1
network 192.168.1.0 255.255.255.0
default-gateway 192.168.1.1
dns-list 8.8.8.8
address-range 192.168.1.101 192.168.1.110
```

Рисунок 3.26 – Команди по налаштування *DHCP*

Ці команди включають *DHCP*-сервер, налаштовують *IP-pool* (*pool1)*, встановлюють адресу мережі та маску підмережі, адресу стандартного шлюзу і *DNS*-сервер. Крім того, створюється діапазон адрес від 192.168.1.101 до 192.168.1.110 за допомогою команди *address-range*.

Після цього можна призначити *IP*-адресу клієнту *DHCP*, який підключився до мережі. Клієнт отримає одну з доступних адрес в діапазоні 192.168.1.101-192.168.1.110.

3.3.2 Налаштування *NFS*

Для налаштування *NFS* (*Network File System*) на сервері, необхідно виконати такі кроки:

1. Встановити пакети, необхідні для роботи *NFS*:

```
sudo apt-get update
sudo apt-get install nfs-kernel-server
```

Рисунок 3.27 – Встановлення пакетів *NFS*

2. Створити каталог, який буде надаватися клієнтам.

```
sudo mkdir /home/nfs
sudo chown nobody:nogroup /home/nfs
sudo chmod 777 /home/nfs
```

Рисунок 3.28 – Створення каталогу

3. Налаштувати доступ клієнтів до каталогу /*home/nfs* у файлі /*etc/exports*. Дозволити доступ клієнту з *IP*-адресою 192.168.0.100:

```
sudo nano /etc/exports
```

Рисунок 3.29 Перехід до каталогу /etc/exports

Додати рядок: /*home*/*nfs* 192.168.0.100 *(rw,sync,no_subtree_check*)

4. Запустити *NFS*-сервер і застосувати зміни:

```
sudo systemctl restart nfs-kernel-server
sudo exportfs -a
```

Рисунок 3.30 – Запуск *NFS* та застосування змін

Після виконання цих команд, *NFS*-сервер буде налаштований і готовий до використання. У даному прикладі клієнти з *IP*-адресою 192.168.0.100 отримають доступ до каталогу /home/nfs з правами читання та запису.

3.5.3 Налаштування *PXE*

Налаштування *PXE* відбуватиметься за кілька кроків, а саме:

1. Встановіть пакети, необхідні для настройки *PXE*-сервера, такі як *syslinux, dnsmasq, tftpd-hpa*:

```
sudo apt-get update
sudo apt-get install syslinux dnsmasq tftpd-hpa
```

Рисунок 3.31 – Встановлення пакетів *syslinux, dnsmasq, tftpd-hpa*

2. Скопіюйте необхідні файли на сервер *PXE*. Зазвичай вони знаходяться в каталозі */usr/lib/PXELINUX*:

```
sudo mkdir /tftpboot
sudo cp /usr/lib/PXELINUX/pxelinux.0 /tftpboot/
sudo cp /usr/lib/syslinux/modules/bios/* /tftpboot/
```

Рисунок 3.32 – Команди копіювання файлів *PXE*

3. Налаштуйте файл */etc/dnsmasq.conf*, додавши наступні рядки:

```
dhcp-range=192.168.0.100,192.168.0.199,12h
dhcp-boot=pxelinux.0
enable-tftp
tftp-root=/tftpboot
```

Рисунок 3.33 – Налаштування файлу dnsmasq.conf

Тут *dhcp-range* вказує діапазон *IP*-адрес для *DHCP*, *dhcp-boot* вказує завантажувач для клієнтів, а *tftp-root* вказує кореневу директорію *TFTP*.

4. Створіть каталог *pxelinux.cfg* та налаштуйте файл *default*:

```
sudo mkdir /tftpboot/pxelinux.cfg
sudo nano /tftpboot/pxelinux.cfg/default
```

Рисунок 3.34 – Створення каталогу *pxelinux.cfg*

5. Додайте наступні рядки:

```
DEFAULT linux
TIMEOUT 100
PROMPT 0

LABEL linux
KERNEL vmlinuz
APPEND initrd=initrd.img ip=dhcp
```

Рисунок 3.35 – Налаштування файлу *default*

Тут *DEFAULT* вказує ім'я файлу ядра, *KERNEL* вказує ім'я файлу ядра, *APPEND* вказує додаткові параметри ядра.

6. Скопіюйте ядро та *initrd* на сервер *PXE*:

```
sudo cp /path/to/vmlinuz /tftpboot/
sudo cp /path/to/initrd.img /tftpboot/
```

Рисунок 3.36 – Копіювання ядра на *PXE*

7. Перезапустіть сервіси *dnsmasq* та *tftpd-hpa*:

```
sudo systemctl restart dnsmasq
sudo systemctl restart tftpd-hpa
```

Рисунок 3.37 – Перезапуск серверів

Таким чином, ми повністю налаштували сервер *LTSP*, а також впровадили в нашу мережу *DHCP*, створили образ системи, який роздаватиметься по мережі всім новим користувачам. Сервер повністю готовий до експлуатації.

3.4 Налаштування тонкого клієнта

Запускаємо бездискову станцію, підключену у нашу мережу. Тепер заходимо у *boot*-меню, у якому обираємо включення через *LAN*, тобто через мережу. Для цього я підключав *IPXE*, а після того як ми обираємо запуск системи по *LAN*, завантажується образ операційної системи через мережу.

```
VirtualBox temporary boot device selection

Detected Hard disks:

No hard disks found

Other boot devices:
 f) Floppy
 c) CD-ROM
 l) LAN

 b) Continue booting
```

Рисунок 3.25 – boot-меню тонкого клієнта

Після завантаження образу операційної системи, клієнт встановлює з'єднання з сервером. Для цього використовується протокол *NFS*, який забезпечує з'єднання з сервером та передачу даних між клієнтом та сервером.

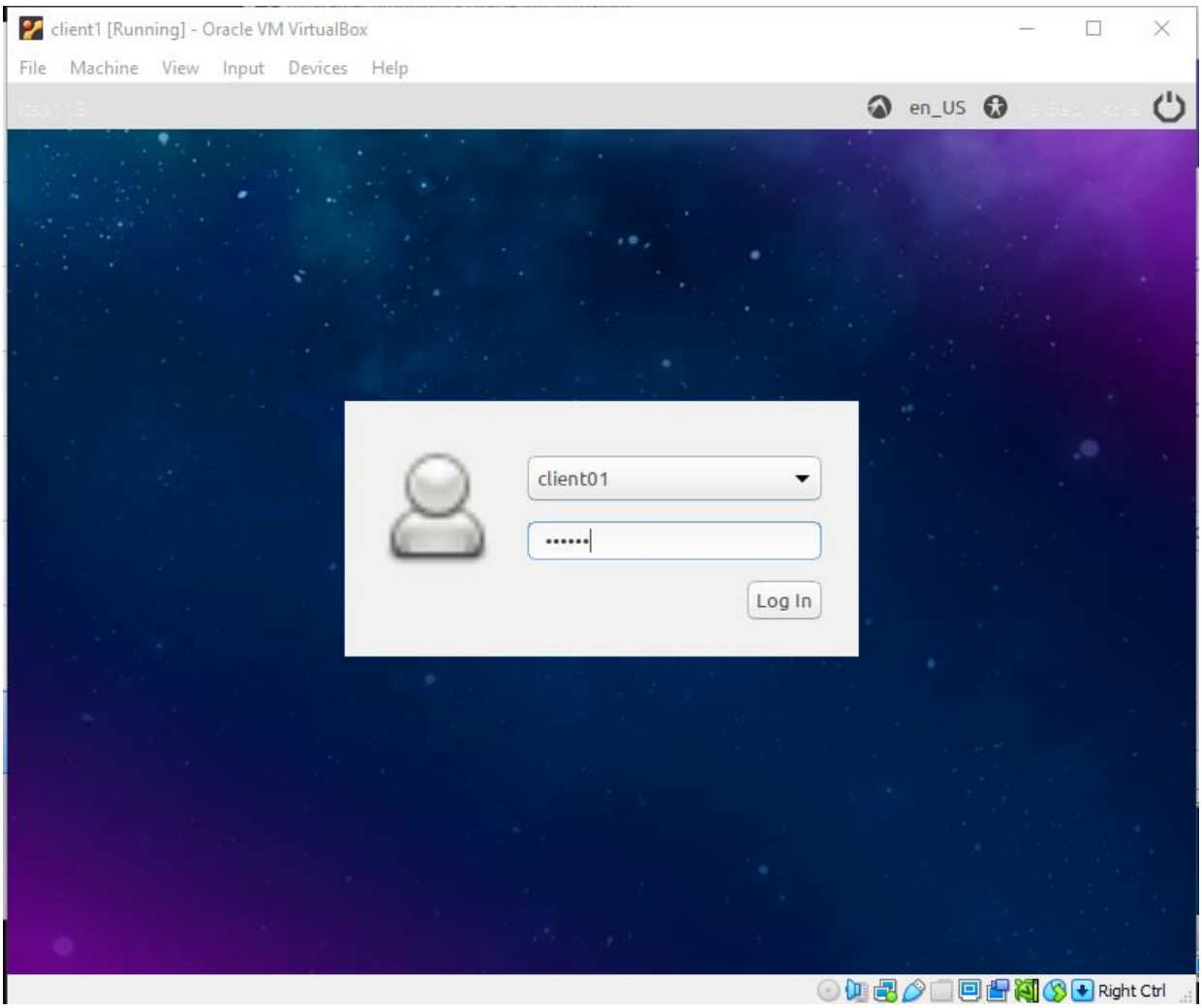

Рисунок 3.26 – Входимо до облікового запису

Коли з'єднання встановлено, клієнт отримує доступ до свого робочого столу на сервері. Робочий стіл складається з різних компонентів, таких як: меню старт, панель задач, вікна програм та інші. Усі ці компоненти зберігаються на сервері та клієнт отримує до них доступ через з'єднання з сервером.

Щоб перевірити доступ до глобальної мережі інтернет, спробуємо пропінгувати (Пінг - це утиліта командного рядка, яка використовується для перевірки доступності хоста в мережі та вимірювання часу відгуку (затримки) між відправленням запиту та отриманням відповіді.) *DNS*-сервер *Google* – 8.8.8.8 та перевіримо адресу мережі в якій ми знаходимося. Адреса 8.8.8.8, яка є IP-адресою DNS-сервера Google, часто використовується для перевірки доступності інтернету. Для цього я увійшов до терміналу, нашої операційної системи, та виконав команду – ping 8.8.8.8 та побачив, що усі пройшли та немає втрат пакетів, якби у нас були втрати пакетів, це б дало нам знати, що у нас немає доступу до мережі *Internet*.

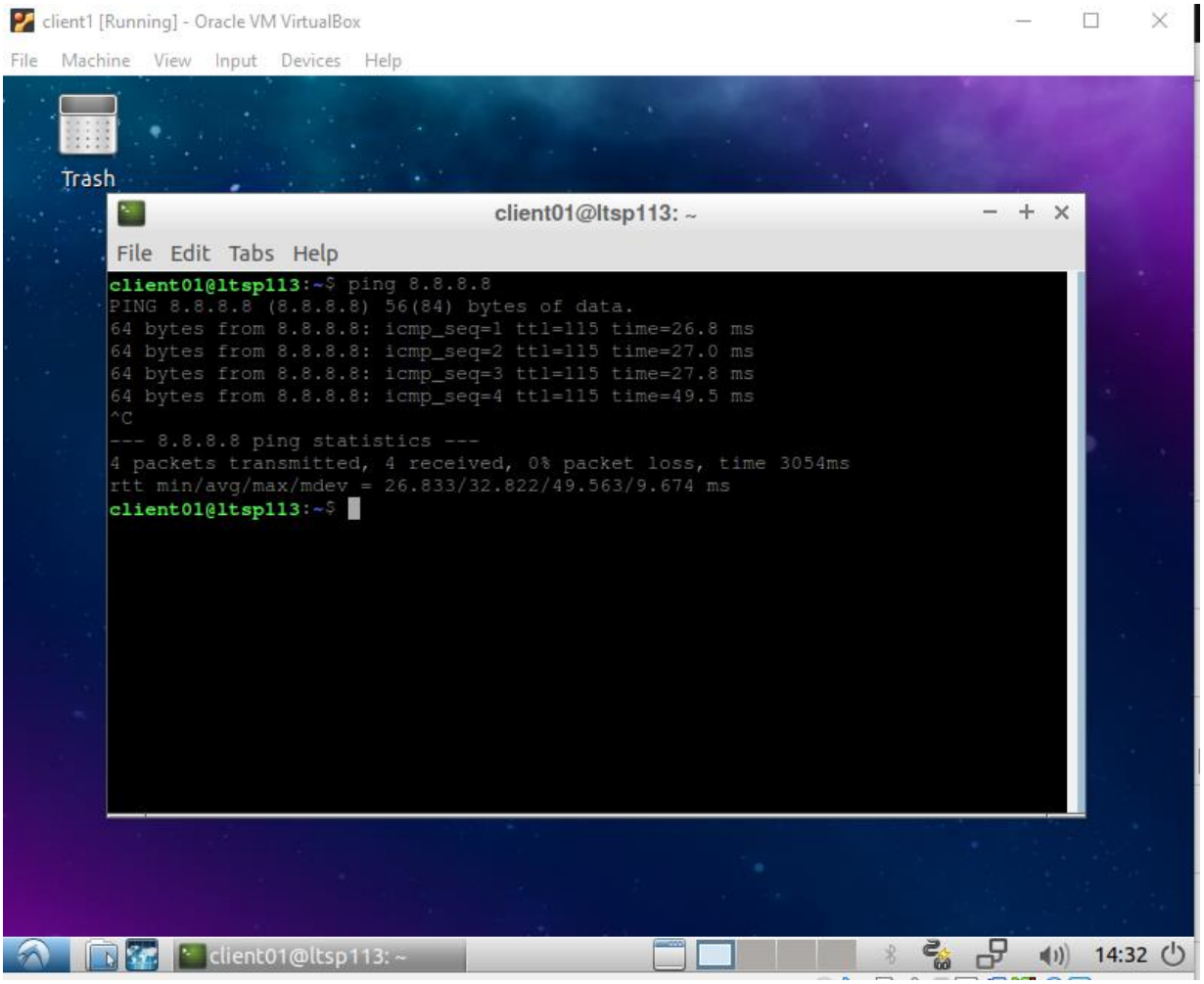

Рисунок 3.27 – Перевірка підключення до мережі інтернет

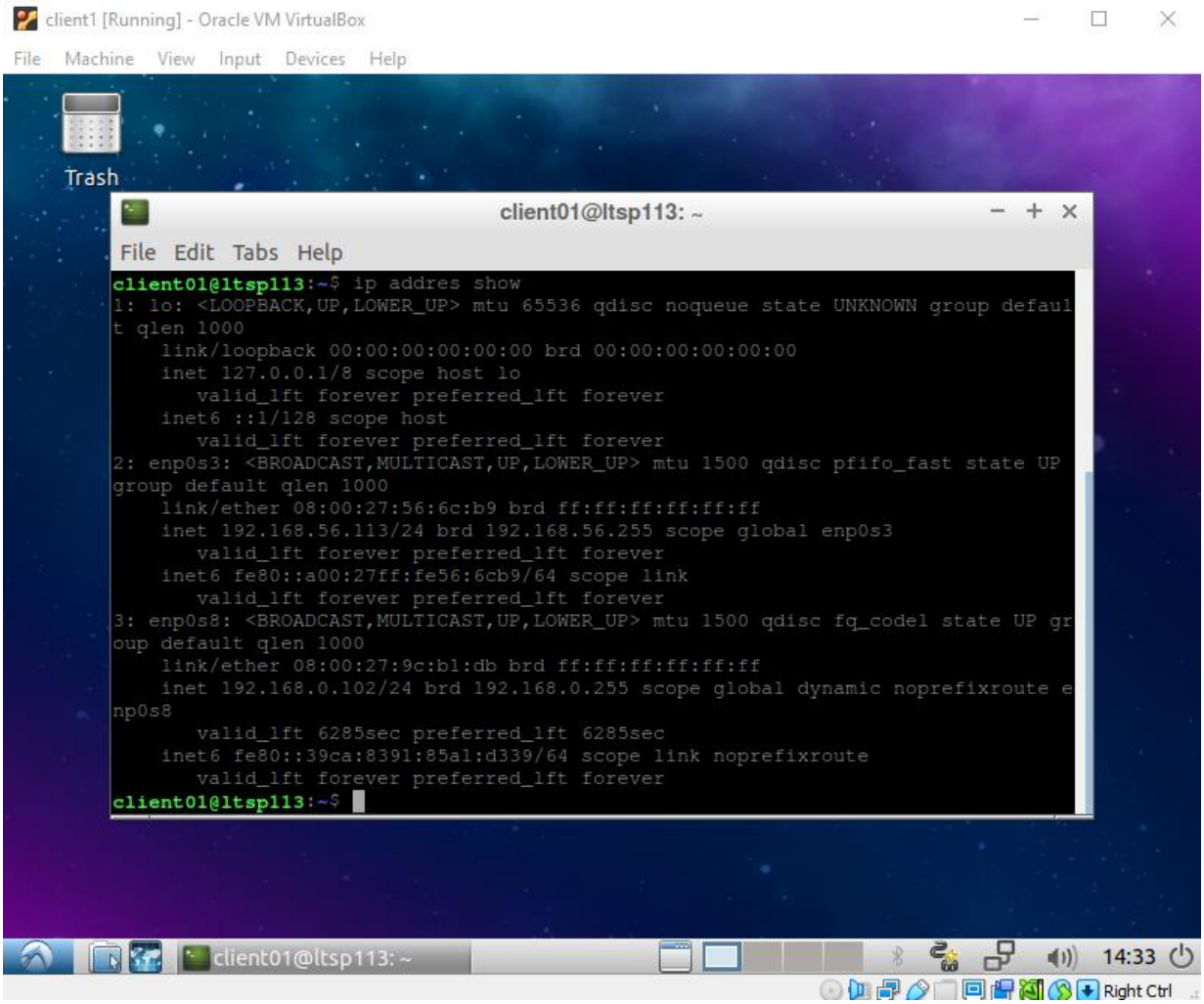

Рисунок 3.28 – Перевірка мережі

Так само треба перевірити, перебуваємо ми в нашій мережі чи ні? Для цього ми вже заздалегідь знаємо адресу нашої мережі. Вводимо в термінал нашої операційної мережі команду *ip adress show* (команда "*ip address show*" відображає інформацію про мережеві інтерфейси, включно з *IP*-адресами, масками підмереж, шлюзом за замовчуванням і станом інтерфейсів, на комп'ютері або іншому мережевому пристрої), далі дивимося на інтерфейс, до якого під'єднано нашу мережу, а саме *enp0s8*. Як бачимо на рисунку 3.28, адреса цього інтерфейсу повністю відповідає нашій мережі

Останнє, що треба зробити це перевірити робочий стіл і доступ до додатків.

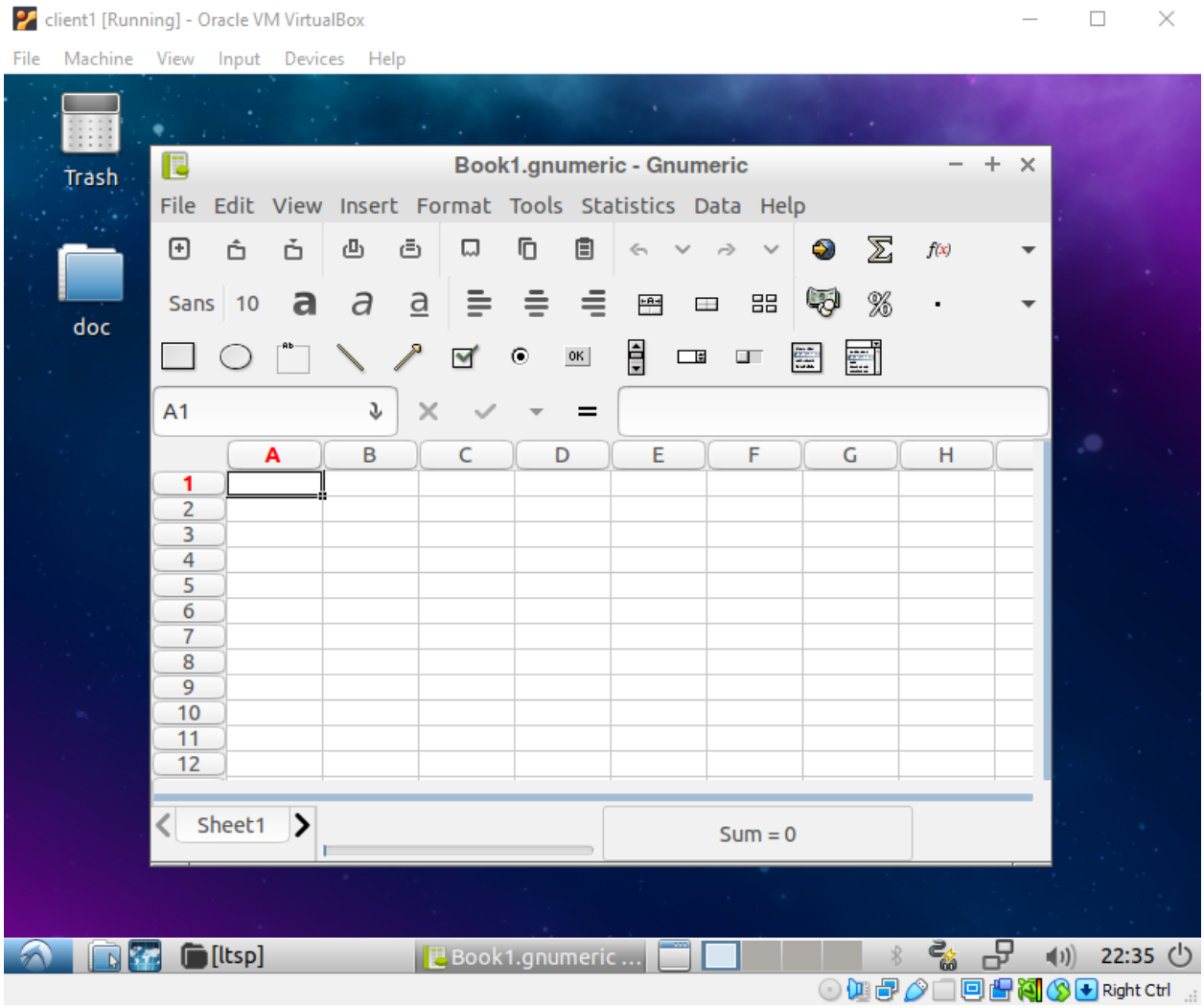

Рисунок 3.29 Перевірка програм

Та перевіримо, чи може сервер надсилати та створювати загальні папки для інших користувачів. Я створив документ у загальній папці на сервері, який називається «*rulles*» та написав у ньому текст. Для того, щоб користувач зміг увійти у папку з документом, йому потрібно увійти у директорію */home/ltsp/Public/*. (рисунки 3.30 та 3.31). Ця функція дуже важлива, для нашої мережі, оскільки вона буде використовуватися у офісі, де працівникам дуже важливо обмінюватися документами, файлами тощо.

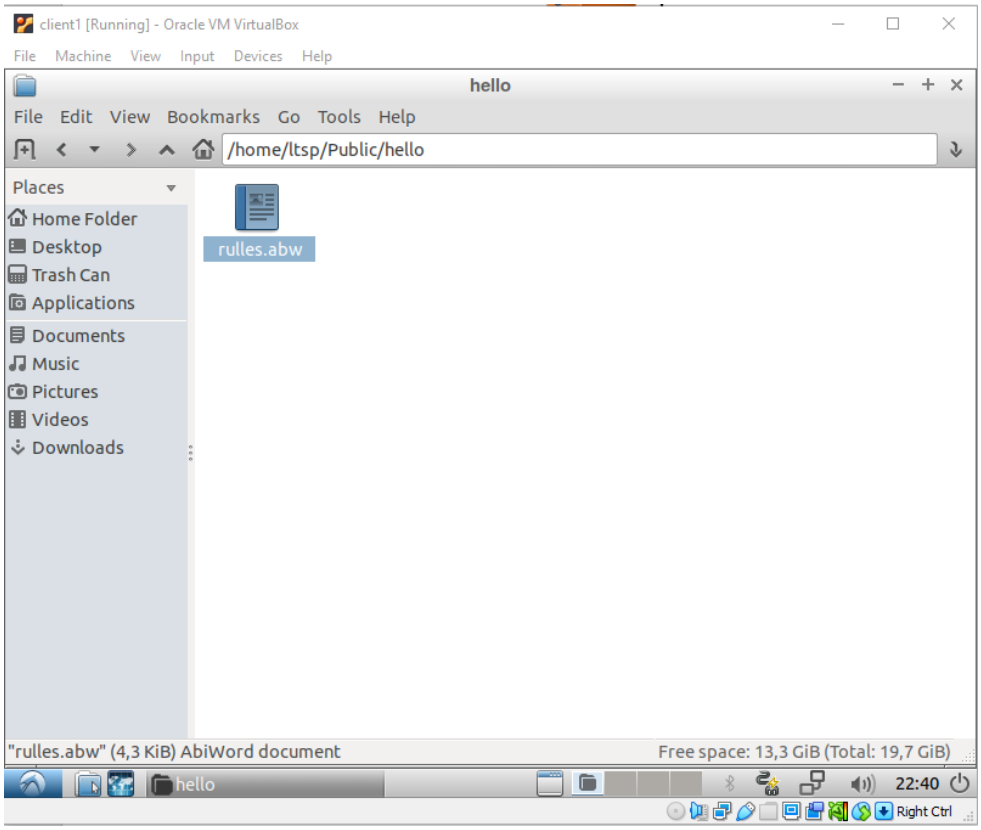

Рисунок 3.30 Перевірка доступу до документа

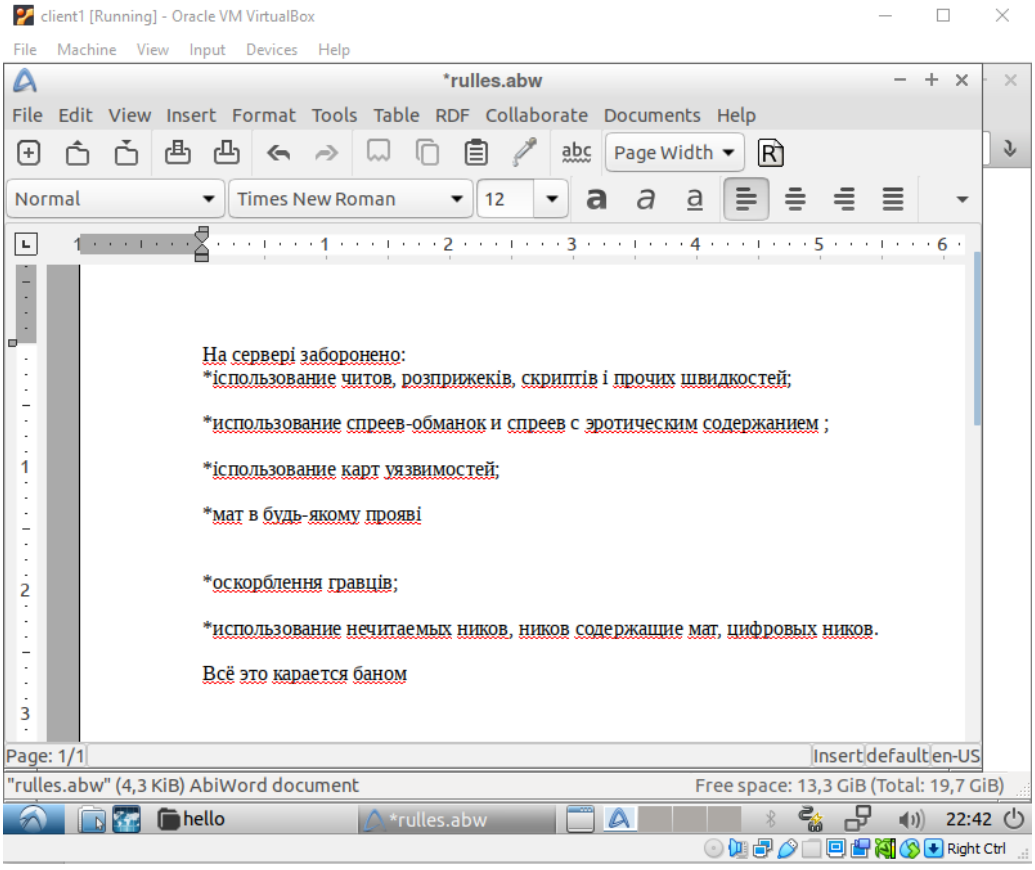

Рисунок 3.31 Відкриття файлу

Користувачі можуть отримати доступ до своїх настільних і серверних додатків, підключившись до *LTSP*-сервера з будь-якого мережевого пристрою, що підтримує протокол *NFS,* що підвищує їхню мобільність і продуктивність.

3.5 Обслуговування бездискової мережі

Обслуговування мережі – це процес підтримки та управління комп'ютерною мережею, який включає регулярні заходи з моніторингу та аналізу мережевих ресурсів, усунення проблем, оновлення програмного забезпечення та налаштування мережевих пристроїв.

Оновлення програмного забезпечення *LTSP* зазвичай виконується на сервері, на якому розміщено *LTSP*. Щоб оновити програму на *LTSP*, скористайтеся одним із поширених інструментів керування пакетами *Linux*, наприклад *apt-get, yum* або *zypper*.

Нижче наведено приклади команд для оновлення програмного забезпечення *LTSP* на *Ubuntu*, за допомогою менеджера пакетів *apt-get*:

1. Виконайте таку команду у вікні терміналу сервера LTSP: *sudo apt-get update.*

2. Оновіть пакети до останніх версій: *sudo apt-get upgrade.*

3. Якщо ви бажаєте оновити певний пакет, виконайте команду: *sudo apt-get install* <назва пакета>.

Також, щоб додати нового користувача, треба зроби такі дії:

1. Відкрийте термінал на сервері *LTSP* та виконайте команду: *sudo adduser* <ім'я_користувача>
2. Замініть <ім'я_користувача> на ім'я нового користувача, якого ви бажаєте додати.

Коли ви вводите цю команду, система запросить вас ввести пароль нового користувача. Введіть пароль та підтвердіть його.

Після цього можна додати нового користувача до групи, яка має доступ

до *LTSP*. Щоб це зробити, виконайте таку команду: *sudo usermod -a -G* <ім'я_групи> <ім'я_користувача>

Замініть <ім'я_групи> на те, до якої ви бажаєте додати користувача, та <ім'я_користувача> на те ім'я, кого ви створили.

Після цього, перезапустіть *LTSP*, щоб зміни набули чинності, а для цього виконайте таку команду: *sudo systemctl restart ltsp-server-standalone.*

Тепер новий користувач може увійти до системи за допомогою свого власного імені користувача та пароля.

3.6 Висновки

- Було проведено аналіз існуючих технологій для створення сервера *LTSP* та обрано оптимальну конфігурацію для вирішення поставлених завдань.
- Було створено сервер *LTSP* на базі операційної системи *Lubuntu* з використанням технології *VirtualBox*, що дозволило спростити встановлення та налаштування сервера.
- Проведено тестування працездатності сервера *LTSP* шляхом створення другої віртуальної машини. Результати тестування показали, що сервер *LTSP* працює правильно та забезпечує високу стабільність та продуктивність.
- Створений сервер *LTSP* може бути використаний для різних цілей, включаючи навчання та тестування нових програм та операційних систем, а також для забезпечення доступу до додатків та ресурсів у віддалених робочих станцій.

В цілому, створення сервера з використанням технології *LTSP* є ефективним способом забезпечення доступу до додатків і ресурсів віддалених робочих станцій.

РОДЗДІЛ 4

ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ПРОЄКТУ

4.1 Основні завдання організаційно-економічного та маркетингового обґрунтування проекту

Ідея для бездискової мережи полягає у створенні інфраструктури, яка дозволить користувачам підключатися до сервера за допомогою терміналів або тонких клієнтів та працювати у загальному середовищі. У цьому середовищі будуть доступні спільні ресурси, такі як програми, файли та бази даних. При цьому обчислювальні потужності будуть розподілені між сервером і терміналами, що дозволить економити ресурси та зменшувати навантаження на кожен окремий комп'ютер. Однією з основних переваг мережі на *LTSP* є зручність управління спільними ресурсами. Адміністратори можуть легко керувати програмами та файлами на сервері, а користувачі можуть легко отримувати доступ до цих ресурсів. Також, у разі потреби, адміністратори можуть швидко та легко налаштувати клієнтські машини або замінити їх на нові, без необхідності встановлення та налаштування програмного забезпечення на кожному комп'ютері.

Аналіз техніко-економічної доцільності проекту, визначення потенційних споживачів продукції, оцінка ринкового потенціалу проекту, вибір стратегії виходу на ринок, розрахунок вартості проекту та оцінка його ефективності є основними завданнями.

Розробка організаційної структури проекту, планування витрат і прибутків, оцінка ефективності використання ресурсів, розрахунок фінансових показників, виявлення можливостей фінансування проекту є частиною організаційно-економічного обґрунтування проекту.

Дослідження ринку та конкурентного середовища, визначення побажань та готовності споживачів купувати товари, формулювання маркетингової стратегії та планування маркетингових дій — все це є частиною маркетингового обґрунтування.

Усі ці обов’язки сприяють успіху проекту, шляхом максимізації його прибутковості та ефективності використання ресурсів.

Основними завданнями організаційно-економічного обґрунтування проекту “Проектування локальної мережі з бездисковими робочими станціями”є розрахунок витрат на проектування та будівництво мережі, оцінка довгострокової прибутковості та ефективності проекту, а також створення фінансового та бізнес-плану проекту.

Основними цілями маркетингового обґрунтування є визначення перспективного споживання послуг мережі доступу, створення маркетингового та рекламного плану та оцінка конкурентоспроможності мережі на ринку послуг зв'язку.

Організаційно-економічне та маркетингове обґрунтування проекту також розглядає ризики та можливості, пов’язані з його реалізацією, а також законодавчі та нормативні вимоги щодо розвитку та обслуговування мережі доступу.

У проекті з проектування локальної мережі з бездисковими робочими станціями, витрати в економічній частині можуть бути спрямовані на наступні напрямки:

1) Придбання необхідного обладнання та програмного забезпечення для функціонування мережі.
2) Навчання та підготовка персоналу для роботи з мережею, що включає в себе курси навчання, семінари та тренінги.
3) Реклама та маркетингові заходи для просування мережі серед потенційних користувачів та клієнтів.
4) Фінансування досліджень та розробок для постійного вдосконалення мережі та впровадження нових технологій.
5) Оплата витрат на електроенергію, інтернет-підключення та інші операційні витрати, пов'язані з експлуатацією мережі.

Щоб переконатися, що гроші, витрачені на проект, будуть використані максимально ефективно і що він буде успішно реалізований, ці витрати

повинні бути обґрунтовані ще на етапі планування проекту, шляхом проведення необхідних розрахунків й аналізу ринку.

Оцінка прибутковості проекту є важливою складовою його економіки. Для цього необхідно проаналізувати витрати на проект та очікувані доходи.

Витрати на проект локальної мережі з бездисковими робочими станціями можуть також включати придбання необхідних інструментів і витратних матеріалів, оплату послуг фахівців з проектування, налаштування обладнання, а також витрати на маркетинг і просування.

4.2 Обґрунтування ефективності проекту

В умовах відкритої ринкової економіки розширюється діапазон оцінки ефективності науково-технічних розробок, а отже, збільшується кількість основних видів ефективності НДДКР, які необхідно визначити з метою цієї оцінки. До них належать:

– Маркетинговий ефект: я планую просування у своїй поточній компанії, наявність диплому на тему бездискових систем може надати мені перевагу перед іншими кандидатами. Роботодавці можуть бачити мене як кандидата з додатковими знаннями та навичками, які можуть бути цінними для компанії.

– Соціальний ефект: Створення такої мережі може покращити доступ до інформації та освіти у тих місцях, де це було важко. Це може призвести до більш рівного розподілу знань та освіти у суспільстві, а також підвищить рівень освіти загалом. До розробки проекту було залучено двоє осіб, а саме: студент та викладач. Для обслуговування мережі двоє осіб буде забезпечено робочими місцями, а саме головний адміністратор та молодший адміністратор, які працюватимуть позмінно.

– Екологічний ефект: Використання бездискових систем дозволяє знизити кількість проводів та кабелів, необхідних для створення мережі. Це зменшує кількість відходів та вплив виробництва проводів на довкілля. Крім того, використання більш ефективної системи передачі даних

може знизити споживання енергії та викиди парникових газів.

– Науково-технічний ефект: Розробка мережі з бездисковими системами за допомогою *LTPS* може призвести до розвитку нових технологій та покращення існуючих. Також може відбутися суттєвий прогрес у сфері передачі даних, що може призвести до розробки нових додатків та покращення наявних.

Науково-технічну ефективність (НТЕ) результатів прикладних робіт визначають на основі показників науково-технічного рівня. Оцінка науково-технічної ефективності НДДКР відбувається на основі показника ($О_{НТЕ}$), який представляє собою ступінь досягнення максимально можливого рівня, значення якого дорівнює 1 (одиниці):

$$\mathbf{О_{НТЕ} = К^{Ф}_{НТЕ} / К^{П}_{НТЕ},} \qquad (4.1)$$

де $К^{Ф}_{НТЕ}$ – показник (коефіцієнт) фактичного рівня науково-технічної ефективності;

$К^{П}_{НТЕ}$ – показник (коефіцієнт) потенційно можливого рівня науково-технічної ефективності (дорівнює одиниці).

Значення показника $К^{Ф}_{НТЕ}$ визначають на основі шкали експертних оцінок.

Таблиця 4.1

Шкала експертних оцінок для виміру рівня науково-технічної ефективності проектів

№	Групи показників	Характеристика показників	Інтервал рейтингового числа	Коефіцієнт значущості показників
1	Науково-технічний рівень	Ступінь науково-технічного рівня бездикових систем	1-10	0.25
2	Перспективність	Можливість застосування бездикових систем в різних галузях	1-10	0.2
3	Потенційний масштаб практичного використання	Обсяг практичного застосування бездикових систем в галузі	1-10	0.3

Продовження таблиці 4.1

4	Ступінь вірогідності досягнення позитивних результатів	Ймовірність успішного впровадження бездикових систем на практиці	1-10	0.25

Примітка: об'єкт оцінки та аналог(и), які порівнюють за однаковими показниками, наведеними у співставному вигляді відхилення в значеннях кожного з показників, мають бути однаковими для варіантів, що порівнюються.

4.3 Оцінка науково-технічного рівня розробки

Визначають $К^{Ф}_{НТЕ}$ на основі експертної оцінки науково-технічного рівня розробки.

З цією метою:

− Розроблюють перелік специфічних показників, необхідних для виміру науково-технічного рівня розробки;

− формують групу аналогів, які реалізовані на світовому і вітчизняному ринках;

− здійснюють відповідні розрахунки для співставлення показників і визначення балів по Таблиці 4.1.

До числа специфічних показників відносять:

− Для нової техніки: продуктивність, споживання інженерних ресурсів на виробітку одиниці продукції, потреба в робочих, які обслуговують обладнання, експлуатаційні витрати на одиницю продукції;

− для нових матеріалів і речовин: вміст корисних речовин для виробітки готової продукції, питома вага відходів у загальному обсязі переробленої сировини, вартість одиниці нового матеріалу, додаткові витрати на екологічну компенсацію;

− для нових технологій: якість виробленої продукції, енергоємність і трудомісткість продукції, собівартість одиниці продукції.

З метою спрощення визначення $К^{Ф}_{НТЕ}$ у Таблиці 4.2 не введено

Показника витрат на одиницю продукції.

Таблиця 4.2

Порівняльні показники для виконання оцінки НТЕ

ПОКАЗНИКИ	Варіанти технології	
	розробленої	співвідносної (аналога)
Рівень новізни	Високий	Середній
Якість продукції	Висока	Середня
Споживання на 1 т продукції – тепла, Гкал – електроенергії, кВт·годину – води, $м^3$	4Гкал 1Квт $2м^3$	3Гкал 0,4Квт $4м^3$
Трудомісткість виробництва, людино-годин/ тонну	50	70

На основі співставлення даних таблиці, встановлюють бали по характеристиках чотирьох груп і на цьому розраховують значення інтегрального показника НТЕ:

$$\mathbf{НТЕ = \Sigma Б_i \times К_i^3}, \qquad (4.2)$$

де i = 1 ÷ 4,

Бі – бали (рейтингове число),

К – коефіцієнт значущості показників.

Рівень науково-технічної ефективності НДДКР розраховано на основі наведених даних прикладу (Таблиця 4.3).

Таблиця 4.3

Експертна оцінка і розрахунок величини інтегрального показника НТЕ

№	Групи показників	Рейтинг експертів			Середня за експертними оцінками	НТЕ
		1	2	3		
1	Науково-технічний рівень	8	7	9	8	2 (8 x 0,25)
2	Перспективність	9	9	8	9	3,15 (9 x 0,35)
3	Потенційний масштаб практичного використання	6	7	7	7,25	1,45 (7,25 x 0,20)

Продовження таблиці 4.3

4	Ступінь вірогідності досягнення позитивних результатів	8	8	8	8	1,6 (8, х 0,20)
В С Ь О Г О						8,2

НТЕ = 8·0,25+9·0,35+7,25·0,20+8·0,20=2+3,15+1,45+1,6 = 8,2

Отриманий результат слід порівняти з максимально можливим значенням, яке дорівнює 10 балам (10·0,25 + 10·0,35 + 10·0,20 + 10·0,20).

Отже, оцінка рівня НТЕ може бути зроблена за допомогою інтегрального коефіцієнта оцінки НТЕ ($К_{НТЕ}$):

$$К_{НТЕ} = \frac{НТЕ}{10} \cdot 100\ \% \qquad (4.3)$$

На основі даних Таблиці 4.3, можна дійти до висновку, що $К_{НТЕ}$ відповідає 82 %, тобто:

$$\frac{8,2}{10} \times 100 = 82 \qquad (4.4)$$

В тому випадку, коли значення $К_{НТЕ}$ перевищує середнє значення, яке дорівнює 5.0, має бути зроблено висновок про достатній рівень НТЕ:

- цілком достатній 5,0 – 6,0;
- достатній 6,1 – 8,0;
- достатньо високий 8,1 – 9,0;
- високий 9,1 – 10.

Таким чином, рівень НТЕ технології можна визнати достатнім. Отже, розроблену технологію пропонується впроваджувати у виробництво.

4.4 Розрахунок економічної ефективності проекту

Розрахунок економічної ефективності проекту - це процес визначення потенційного доходу та витрат проекту, а також оцінювання того, наскільки доцільно вкладати гроші у його реалізацію.

Для розрахунку економічної ефективності проекту необхідно визначити наступні показники:

1. Вартість проекту: це загальна вартість всіх витрат, пов'язаних з реалізацією проекту, включаючи затрати на розробку, впровадження та експлуатацію.
2. Прибуток від проекту: це дохід, отриманий від реалізації продукту або послуги, яку реалізовує проект.
3. Термін окупності: це період, за який витрати на реалізацію проекту повернуться від прибутку.
4. Рентабельність інвестицій (PI): це відношення чистого дисконтованого доходу до вартості інвестицій.

Припустимо, що витрати на проект складають 100000 грн, а очікуваний прибуток становить 150000 грн. Тоді ціна проекту буде розрахована за формулою:

Ціна = Витрати + Прибуток (30%-300%)

Проведемо розрахунок:

Ціна = 100 000 грн + 150 000 грн * 30% = 145 000 грн

Рентабельність проекту можна розрахувати за формулою:

R = Прибуток / Витрати * 100%

Підставляю свої значення:

R = 150 000/145 000 *100%

Рентабельність проекту дорівнює R = 104%

Строк окупності проекту можна розрахувати за формулою:

$$T = \frac{1}{R} \times 100$$

Підставляю свої значення:

$$T = \frac{1}{104\%} \times 100$$

Час, за який проект окупиться дорівнює T = 0,9 року або 11 місяці.

Отже, проект мережі доступу на базі технології *LTSP* з витратами у 100000 грн та очікуваним прибутком у 150000 грн, при реалізації за ціною 145 000 грн, матиме рентабельність 104% і буде окупатися за 11 місяців.

РОЗДІЛ 5

ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ ПРИ ВПРОВАДЖЕННІ ПРОЕКТУ

5.1 Техніка безпеки

Небезпечні фактори при монтажних роботах. При прокладці телекомунікацій в офісних приміщеннях монтажник виконує роботу як ручним-, так й електроінструментом.

Роботи, виконувані електроінструментом:

– перфорування отворів у бетонних і цегельних стінах;
– штроблення каналів у бетонних і цегельних стінах;
– обрізка кабельних каналів;
– свердлення отворів у легких перегородках (гіпсокартон, ДСП);
– загортання шурупів і гвинтів;

При цьому він користується наступним інструментом: дриль, перфоратор, кутова шліфувальна машинка, шуруповерт.

У перерахованого інструмента є обертові частини, які можуть нанести механічну травму. Крім того, при виконанні зазначених вище робіт утворюються стружка, пил, осколки оброблюваної поверхні. Вони можуть поранити шкірні покриви, очі, дихальні шляхи. Також існує небезпека електротравм - як від пробивання ізоляції в електроінструменті, так і при виникненні короткого замикання у випадку ушкодження схованої електропроводки. Не варто забувати про шуми й вібрацію, які супроводжують роботи даним інструментом. При роботі, електроінструмент і продукти його обробки можуть нагріватися, отже існує небезпека термічних травм (опіків).

Роботи, виконувані ручним інструментом:

– забивання в отвори пластикових пробок і дюбелів;
– обрізка кабелю;
– зачищення кабелю від ізоляції;
– обтиск проводів у технологічні клеми.

При виконанні даних робіт, монтажник користується наступним ручним інструментом: викрутка, молоток, пасатижі, гострозубці, бокорізи, пристосування для зачищення й обрізки кабелю. У перерахованого інструмента є гострі ріжучі крайки, об які можна порізатися.

5.2 Електробезпека

Для правильної побудови й експлуатації мережі бажано знати термінологію й розуміти основні принципи роботи мережі 220/380 Вольт. А будь-які самостійні дії можуть бути пов’язані з реальним ризиком для життя.

Всі роботи, пов’язані із прокладкою й обслуговуванням електричних мереж, повинні виконуватися тільки кваліфікованим електротехнічним персоналом з відповідною групою допуску електробезпечності!

Даний матеріал опирається на Правила пристрою електроустановок (ПУЕ), що є головним документом, який регламентує питання електричних мереж.

Електричні установки, до яких відноситься практично вся офісна оргтехніка, надає для людини можливу небезпеку, оскільки в процесі експлуатації або проведення профілактичних робіт людина може торкнутися частин, що перебувають під напругою. Проходячи через людину, електричний струм впливає на неї складним чином, викликаючи електричний, електролітичний, механічний й біологічний вплив. Кожен з перерахованих впливів струму може призвести до електричної травми, тобто ушкодженню організму, викликаному впливом електричного струму або дуги (ГОСТ 12.1.009- 776).

Умови електробезпечності залежать і від параметрів навколишнього середовища виробничих приміщень - вологість, температура тощо. Винятково важливе значення для припинення електротравматизму має правильна організація обслуговування діючих електроустановок, тобто суворе виконання ряду організаційних і технічних заходів, установлених «Правилами технічної експлуатації електроустановок споживачів» й «Правилами техніки

безпеки при експлуатації електроустановок споживачів» (ПТЕ й ПТБ).

Для попередження поразки електричним токовищем при експлуатації електроустановок використають технічні засоби захисту, до яких відносять:

– електричну ізоляцію струмоведучих частин;
– захисне заземлення;
– занулення;
– вирівнювання потенціалів;
– захисне відключення;
– електричний поділ мережі;
– мала напруга;
– подвійну ізоляцію.

Фізичний зміст ізоляції як захисної міри, полягає в обмеженні значення сили струму, що протікає через тіло людини при різних обставинах, що виникають у процесі експлуатації встаткування. В електроустановках до 1 кВ, мінімальне значення опору ізоляції повинне бути не менш 0,5 МОм. Захисне заземлення - це основна технічна міра, застосована в мережах з ізольованою нейтраллю. Під ним розуміють навмисне електричне з'єднання з «землею» або її еквівалентом металевих неструмоведучих частин, які можуть виявитися під напругою. Всі підлягаючі заземленню елементи ЕОМ приєднують до контуру-шини окремими заземлюючими провідниками.

У мережах напруги до 1 кВ захист персоналу від поразки електричним струму здійснюється зануленням. Зануленням називається навмисне електричне з'єднання з нульовим захисним провідником металевих неструмоведучих частин, які можуть виявитися під напругою (ГОСТ 12.1.009-76).

Захист відключенням являє собою швидкодіючий захист, що забезпечує автоматичне відключення електроустановки від мережі при виникненні в ній небезпеки поразки людини токовищем (ГОСТ12.4.155-85). Захисне відключення може застосовуватися як самостійний захисний засіб, так і разом

із заземленням і із зануленням.

Згідно ГОСТ 12.1.019-79, під електробезпекою розуміють систему організаційних і технічних заходів та засобів, що забезпечують захист людей від шкідливого і небезпечного впливу електричного струму, електричної дуги і статичної електрики. На відміну від інших джерел небезпеки, електричний струм не можна виявити без спеціального обладнання та приладів, тому вплив його на людину найчастіше несподіваний.

Проходячи через організм людини, електричний струм робить неможливим функціонування нервової системи та м'язів, оскільки електричні сигнали передаються по нервових волокнах, а також скорочення м'язів відбувається завдяки електричній активності. Однак при сильному впливі електричного струму на організм людини можуть виникнути небезпечні наслідки, такі як: серцева аритмія, опіки, пошкодження органів і тканин. Тому, використовуючи електрику, необхідно дотримуватися всіх необхідних запобіжних заходів безпеки. В результаті термічного впливу, здійснюється розігрів організму і виникають опіки ділянок тіла, в результаті електролітичного впливу розкладається кров і інші органічні рідини в організмі. Біологічний вплив проявляється в порушенні і роздратуванні тканин і мимовільному судорожному скороченні м'язів.

Основною причиною отримання трав від напруги є:

– контакт з оголеними проводами;

– взаємодія з комплектуючими комп'ютера;

– використання не справного обладнання;

– несправність захисних засобів, якими потерпілий торкався струмоведучих частин;

– несподіване виникнення напруги через пошкодження ізоляції там, де в нормальних умовах його бути не повинно;

– замикання фаз на землю;

– поява напруги на струмопровідних частинах обладнання в результаті помилкового включення тоді, коли на ньому виконують роботу;

Експлуатація комп'ютерної мережі передбачає використання ПК в якості пристроїв доступу до неї. Джерелом напруги живлення ПК і *Wi-Fi*-роутерів є мережа змінного струму з напругою 220 В, на яку поширюється ГОСТ 25861-83.

Згідно з вимогами для попередження уражень струмом необхідно:

– Чітко і в повному обсязі виконувати правила виконання робіт і технічної експлуатації;

– виключити можливість доступу оператора до частин обладнання, що працює під небезпечною напругою, неізольованих частин, призначених для роботи при малій напрузі і не підключеним до захисного заземлення;

– застосовувати ізоляцію, що служить для захисту від ураження електричним струмом, виконану із застосуванням міцного суцільного або багатошарового ізоляційного матеріалу, товщина якого обумовлена типом забезпечуваного захисту;

– підводити електроживлення до ПК від розетки будівлі за допомогою спеціальної вилки з занулюючим контактом;

– захистити від перевантажень по струму, розраховуючи на потужність, споживану від мережі; а також захистити від короткого замикання обладнання, вбудоване в мережу будинку;

– надійно підключити до заземлюючих затискачів металеві частини, доступні для оператора, які в результаті пошкодження ізоляції можуть опинитися під небезпечною напругою;

– перевірити, що захисний заземлювальний провідник не має вимикачів і запобіжників, а також надійно ізольований.

Мікроклімат в офісі. Згідно з ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень» встановлено такі норми допустимих параметрів мікроклімату для робіт в офісних приміщеннях (категорія робіт – легка 1а): під час холодного періоду року температура повітря повинна бути не менше +21-25°С, а температура поверхонь не менше +19-24°С; відносна вологість повітря до 75% зі швидкістю руху повітря 0,1 м/с.

В літній сезон температура приміщення повинна бути в межах +22-28°С, температура поверхонь не вище +19-24°С, відносна вологість повітря 40-60 %, а швидкість руху повітря 0.1 м/с. З цим кліматом може стабільно працювати сервер та співробітники.

ВИСНОВКИ

Під час роботи над дипломним проектом було спроектовано локальну мережу для підприємства з використанням бездискових робочих станцій.

У процесі виконання завдання на проектування, на конкретному прикладі наведені основні етапи створення локальної мережі та дії по налаштуванню обладання з метою досягнення її працездатності. При цьому, була створена найстабільніша версія мережі, з точки зору функціонування.

Так як ця мережа вимагає особливого догляду адміністратор зможе підтримувати стабільність роботи сервера для всіх користувачів і також невід'ємним плюсом є те, що ця мережа може бути обслугована з дому використовуючи віддалений доступ.

Також цей проект має дуже гарний термін окупностіі, що робить його економічно вигідним, з точки зору бюджету. На даний момент це є найстабільнішою версією.

У першій частини розділу роботи було поставлено завдання оптимізації роботи з терміналами, розглянуто характеристику терміналів і обґрунтовано використання віртуальної машини як вирішення проблем.

У другій частині було приділено увагу до основних вимог мережі для її встановлення її в будівлю. І до основних принципів роботи мережі і протоколів щоб було приблизне поняття про роботу мережі.

У третій частині буквально по слайдам був розібраний процес створення мережі, так само було приділено увагу на основні помилки які часто з'являються при створенні мережі.

Цей дипломний проект дав мені чітке уявлення, що з себе представляє мережу на бездискових станціях, її плюси і мінуси. І незважаючи на описані мінуси мережу з тонких клієнтів це відмінне рішення для вашого підприємства.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. С.М. Платунова Адміністрування мережі в windows server 2012

2. Комп'ютерні мережі. Принципи, технології, протоколи. 3-е видання / В.Г. Олифер, Н.А. Олифер. - Спб.: Пітер, 2006. - 958 с.: іл.

3. Посібник з технологій об'єднання мереж 4-е видання. Cisco Systems, пров. з англ.: Видавничий будинок «Вільямі», 2005. -1040 с.

4. Установка і налаштування Thinstation: https://imbicile.pp.ru/ustanovka-i-nastrojka-thinstation-5-5/

5. Microsoft Corporation. Комп'ютерні мережі. Навчальний курс / Пер. с англ. - М.: Видавничий відділ «Російська Редакція» ТОО «Channel Trading Ltd.». - 1997.

6. Нове життя Ethernet / Костянтин Изварский. - Експрес-Електроніка, №8,2004.

7. Практичне керівництво для адміністраторів і професійних користувачів / Мауфер Т. Пер.с англ.-М.:КУДИЦ-ОБРАЗ, 2005.

8. Мережі ЕОМ і телекомунікації / В.К. Мищенко. Курс лекцій, 2004 р. Building Wireless Community Networks. Help for Network Administrators / Rob Flickenger. - O'Reilly Publishing, 2002.

9. P. A. Porras, P.G. Neumann, EMERLAND: Event Monitoring Enabling Response to Anomalous Live Disturbance / / Proceeding of the IEEE Symposium on Research in Security and Privacy, Oakland, CA, May 1997.

10. Сети NetWare 3.12-4.1: книга ответов от Михаила Гука.

11. Блог по створенню мережі на LTSP: https://sidserra.blogspot.com/2019/09/ltsp-no-ubuntu-18.html