Міністерство освіти і науки України

Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»
(повне найменування вищого навчального закладу)

Відділення телекомунікацій та електронних систем
(назва відділення)

Циклова комісія комп'ютерної інженерії
(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра
(освітній ступінь)

на тему: Розробка проєкту комп'ютерної мережі компанії "Сітер"

Виконав: студент VI курсу, групи КІб-602

Спеціальності **123 Комп'ютерна інженерія**
(шифр і назва спеціальності)

_____ Богдан МАРТИНЮК
(ім'я та прізвище)

Керівник Андрій ЮЗЬКІВ
(ім'я та прізвище)

Рецензент _____
(ім'я та прізвище)

Тернопіль – 2024

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ТЕРНОПІЛЬСЬКИЙ ФАХОВИЙ КОЛЕДЖ
ТЕРНОПІЛЬСЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
імені ІВАНА ПУЛЮЯ»

Відділення телекомунікацій та електронних систем
Циклова комісія комп'ютерної інженерії
Освітній ступінь бакалавр
Освітньо-професійна програма: Комп'ютерна інженерія
Спеціальність: 123 Комп'ютерна інженерія
Галузь знань: 12 Інформаційні технології

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"08" травня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Мартинюку Богдану Вікторовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи **Розробка проєкту комп'ютерної мережі компанії "Сітер"**

керівник роботи Юзькві Андрій Васильович
(прізвище, ім'я, по батькові)

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університетут імені Івана Пулюя» від 07.05.2024 р №4/9-224.

2. Строк подання студентом роботи: 21 червня 2024 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проектування, стандарти побудови СКС, документація на мережеве обладнання і сервери

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Загальний розділ. Розробка технічного та робочого проєкту. Спеціальний розділ. Економічний розділ. Охорона праці, техніка безпеки та екологічні вимоги.

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

- План приміщень
- Логічна топологія
- Фізична топологія
- Таблиця IP-адрес
- Таблиця техніко-економічних показників
- Модель мережі

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Оксана РЕДЬКВА заст. директора з НВР		
Охорона праці, техніка безпеки та екологічні вимоги	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	08.05	
2	Збір і узагальнення інформації	20.05	
3	Написання першого розділу	24.05	
4	Розробка технічного та робочого проекту	28.05	
5	Написання спеціального розділу	3.06	
6	Розрахунок економічної частини	5.06	
7	Написання розділу охорони праці	7.06	
8	Виконання графічної частини	10.06	
9	Оформлення проекту	14.06	
10	Погодження нормоконтролю	17.06	
11	Попередній захист роботи	21.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 08 травня 2024 року

Студент _____ Богдан МАРТИНЮК
(підпис) (ім'я та прізвище)

Керівник роботи _____ Андрій ЮЗЬКІВ
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Мартинюк Б.В. Розробка проєкту комп'ютерної мережі компанії «Сітер»: кваліфікаційна робота на здобуття освітнього ступеня бакалавр, за спеціальністю 123 Комп'ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2024. 77с.

Кваліфікаційна робота в галузі розробки проєкту комп'ютерної мережі. Після огляду та аналізу сучасних стандартів побудови мереж вибрано логічну та фізичну топологію мережі, активне та пасивне мережеве обладнання, сервери та програмне забезпечення.

Розроблено адресацію вузлів, поділ на vlan, вибрано пасивне та активне обладнання. Огрунтовано вибір ОС, засобів тестування ти захисту мережі. Описано процедури інсталяції на налаштування мережевого обладнання та серверів. Також здійснено моделювання роботи мережі.

Ключові слова: локальна комп'ютерна мережа, віртуальна мережа, сервер, комутатор.

ANNOTATION

Martyniuk Bohdan. Computer Network Project Development of «Siter» company: qualification work for obtaining a bachelor's degree, specialty 123 Computer Engineering. Ternopil: Separate Structural Subdivision "Ternopil Professional College of Ivan Puluj National Technical University", 2024. 77p.

Qualification work in the field of computer network design. After reviewing and analyzing modern networking standards, the logical and physical network topology, active and passive network equipment, servers, and software are selected.

The addressing of nodes, division into vlan, and selection of passive and active equipment are developed. The choice of OS, network testing and security tools is justified. Installation procedures for configuring network equipment and servers are described. Network operation is also modeled.

Keywords: Local Area Network, Virtual Network, Server, Switch.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

DHCP (Dynamic Host Configuration Protocol) - протокол динамічного конфігурування стеку протоколів TCP/IP робочих станцій.

DNS (Domain Name System) - сервер доменних імен.

ОС - операційна система.

ПК - персональний комп’ютер.

EIA (Electronic Industries Association) – Асоціація електронної промисловості.

IP (Internet Protocol) – Інтернет-протокол.

ISP (Internet Service Provider) - провайдер доступу в Інтернет.

LAN (Local Area Network) - локальна мережа.

FTP (File Transfer Protocol) - протокол передачі файлів.

HTTP (Hypertext Transfer Protocol) - протокол передачі гіпертексту.

Infrastructure mode – топологія без провідної мережі, в якій всі з’єднуються з точкою доступу.

MAC (Media Access Control) - апаратна адреса ПК.

MAN (Metropolitan Area Network) - міська мережа.

NAT (Network Address Translation) – мережева трансляція адрес.

National Backbone Network - національна мережа.

TCP/IP (Transmission Control Protocol/Internet Protocol) – протокол управління передачею/Інтернет протокол.

ВСТУП

На сьогоднішній день в світі більше 200 мільйонів комп'ютерів, більша частина з яких приєднана до різного типу мереж. Це переважно локальні мережі різного розміру (локальні, регіональні). Комп'ютерні мережі є один із засобів комунікації людей.

Під локальною мережею розуміють спільне підключення певних кількості робочих станцій та мережевих пристроїв до єдиного каналу передачі даних. Завдяки локальним мережам люди одержали можливість одночасного використання мережевих ресурсів, таких як мережеві принтера, доступ до глобальної мережі і баз даних декількома користувачами, які не мають безпосереднього з’єднання з цими ресурсами.

Основною метою кваліфікаційної роботи є розробка комп’ютерної мережі для компанії «Сітер». При цьому, на основі аналізу технічного завдання необхідно розробити логічну та фізичну топологію мережі, вибрати активне та пасивне обладнання, розрахувати к-сть затрачених матеріалів та їх вартість. Також важливо розробити інструкції з інсталяції та налаштування програмного забезпечення.

Для перевірки правильності прийнятих рішень і реалізованих налаштувань необхідно виконати моделювання роботи локальної мережі в одному з програмних середовищ.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Розробка технічного завдання

Розробку технічного завдання реалізовано в декілька етапів, які описані у відповідних підпунктах.

1.1.1 Найменування та область застосування

Об’єктом розробки в кваліфікаційній роботі є проект комп'ютерної мережі для компанії «Сітер». Перед початком розробки варто детально ознайомитися з комунікаційними вимогами до проєкту самого розробника. Після аналізу цих вимог варто відзначити, що вони аналогічні до вимог інших компаній даного профілю і включають:

1. ПК, що належать до різних відділів, необхідно об’єднати в єдине мережеве середовище.

2. Спільне використання ресурсів периферії (принтерів та ін.).

3. Групове використання високошвидкісного підключення до Інтернету.

4. Ефективний і дешевий спосіб обміну інформацією, як всередині відділ так і між ними.

6. Захист робочих станцій локальної мережі від зовнішніх проникнень.

7. Обмеження трафіку шляхом поділку на підмережі.

8. Надійне і централізоване зберігання даних шляхом створення резервних копій.

9. Наявність мережевих сервісів для моніторингу та сповіщення при нештатних ситуаціях.

1.1.2 Призначення розробки

Розробка призначена для проектування з метою подальшої практичної інсталяції локальної комп’ютерної мережі для компанії-замовника. Вона зможе вирішити такі поставлені завдання:

1. Уніфікувати наявні ПК та інше комп'ютерне обладнання в єдину інформаційну мережу.

2. Надати робочим місцям загальний доступ до мережі Інтернет.

3. Впровадити сервер зберігання даних.

4. Обмежити трафік між підмережами.

5. Захистити ЛОМ від шкідливого трафіку і хакерських атак.

6. Побудова системи моніторингу та звітності.

7. Витрати на розробку мають бути низькими і не перевищувати лімітів, які закладені компанією-замовником.

Після вирішення техніко-економічних і проектних задач потрібно зробити підготовку технічної документації та розробити детальні інструкції для виконавців.

В загальному розробка має зменшити час обробки інформації та підвищити продуктивності праці в цілому.

1.1.3 Вимоги до апаратного і програмного забезпечення

Під час проектування потрібно реалізувати ряд вимог, які можна розділіти на дві великі групи – апаратного і програмного спрямування. Отже апаратні або матеріально-технічні засоби:

1. Середовище передачі даних (неекранована кручена пара, категорія 6).

2. Короби чи кабельні канали.

3. Роз'єми RJ-45.

4. Патч-панель з додатковим обладнанням, тримачами кабелю та ін..

5. Шафа розподільна комутаційна закритого типу (висота 24U).

7. Джерело безперебійного живлення (біля 2 кіловати потужності).

8. Комутатори, що підтримують технологічні стандарти Gigabit Ethernet.

9. Сервера шлюз і файл-сервер.

Другий набір вимог до програмного забезпечення буде використовуватися за потреби, в ході вирішення конкретних виробничих завдань. Мереже потребує насамперед програмного забезпечення шлюзу та файлового сервера. Пріоритет надаватиметься альтернативному програмному забезпеченню (OpenSource), як такому що має високу економічну ефективність. Щодо ПЗ на робочих місцях то воно вибиратиметься за потребами і вимогами конкретного користувача.

1.1.4 Вимоги до документації

Будь-яка локальна комп'ютерна мережа повинна мати належним чином оформлену технічну документацію. Правильно оформлена документація та її повнота сприятимуть своєчасному виконанню робіт з обслуговування локальної мережі. Технічна документація, необхідна компанії "Сіттер": план поверху (із зазначенням усіх розмірів кімнат та відділів), логічна топологія (схема зв'язків між вузлами мережі), фізична топологія, таблиця IP-адрес з налаштуванням VLAN. Після того, як мережа запрацює, необхідно створити кабельний журнал разом із описом специфікацій і параметрів робочої станції

1.1.5 Техніко-економічні показники

Проекти локальних мереж мають відповідні техніко-економічні показники для оцінки їх економічної доцільності та сфери застосування. Основними економічними показниками будуть: вартість проекту ЛВС, собівартість, вартість матеріалів та обладнання. Технічні показники локальної мережі включатимуть:

швидкість локальної мережі, фізичну та логічну топологію, протокол передачі даних, тип сервера, служби локальної мережі.

1.1.6 Стадії та етапи розробки

Для забезпечення хорошої ефективності процесу проектування локальної комп'ютерної мережі він, в більшості випадків, поділяється на наступні етапи:

1. Етап планування і узгодження етапів локальної мережі.
2. Розробка фізичної топології комп'ютерної мережі (розташування обладнання та кабельних трас на плані приміщення).
3. Проектування логічної топології ЛОМ.
4. Аналіз ринку і підбір необхідного активне та пасивне обладнання.
5. Прокладка і монтаж кабельних каналів.
6. Встановлення кабелів в кабельному каналі.
7. Монтаж мережевих розеток та роз’ємів RJ-45 (обжимка).
8. Перевірка та тестування кабелів на передачу даних.
9. Монтаж розподільної шафи та підключення комунікаційного обладнання.
10. Конфігурація комутаторів та безпровідного обладнання.
11. Налаштування операційної системи та сервісів шлюзу.
12. Інсталяція і конфігурація файлового сервера.
13. Налаштування систем моніторингу та оповіщення.
14. Підсумкове тестування та фінальне налагодження мережі.
15. Оформлення технічної та звітньої документації.
16. Здача мережі в експлуатацію.

1.2.7 Порядок контролю та прийому

Перед проектуванням комп'ютерної мережі керівник проекту та замовник складають проект технічного завдання, який визначає різні етапи проектування та розгортання локальної мережі. Після завершення та фактичного впровадження етапу проектування необхідно визначити послідовність контролю технічних параметрів локальної мережі та призначити персонал для здійснення контролю.

1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі

Компанія «Сітер» є достатньо новою але амбітною, вона займається розробкою програмного забезпечення, веб-контентом, технічною підтримкою та обслуговуванням програмного забезпечення. Компанія також надає консалтингові послуги у сфері IT та здійснює іншу супутню діяльність. Структура компанії типова для даного типу компаній і також передбачає залучення співробітників, які працюють віддалено.

Розташування різних підрозділів підприємства показано на плані 2024.КРБ.123.602.17.00.00 ПП. Зараз компанія займає шостий поверх багатоповерхової офісної будівлі. Розміщення відділів та структурних підрозділів також наведено на даному плакаті

Вимоги до проекту реалізуються у формі технічного завдання, в якому вказується проектування заданої кількості точок приєднання на визначені порти з урахуванням резервів для подальшого використання та вимог затвердженого технічного завдання.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Характеристика та обгрунтування вибору логічного типу мережі

Як правило, сучасні мережі зі стандартом Gigabit Ethernet будуються на витій парі категорії 6 (інколи 5e) і вище або на одномодовому чи багатомодовому оптоволокні. Основні комутуючи пристрої в таких мережах – комутатори, які використовуються для передачі пакетів даних у мережі.

Gigabit Ethernet зазвичай працює в повнодуплексному режимі на основі фізичної топології «зірка» або «розширена зірка» [2].

Тому при виборі технології для локальної мережі компанії «Сітер» зупинимося на варіанті Gigabit Ethernet, оскільки він є найкращим з точки зору резервів пропускної здатності, ефективності та масштабованості.

Причини вибору цієї технології включають простоту впровадження, низьку вартість обладнання та можливість майбутніх оновлень мережі для швидшої модернізації, оскільки усі технології Ethernet пропонують сумісність зверху вниз.

Локальну мережу буде розділено на окремі сегменти для кращої керованості, можливості фільтрації трафіку, що рухається між ними, і багатьох інших вимог. Сегменти мережі розділені як і фізично в межах відділ так і віртуально за допомогою технології VLAN.

Розроблений поділ на віртуальні мережі зведено у відповідні таблиці. Так У таблиці «Логічна адресація хостів локальної мережі» Додатку В наведені базові дані для конфігурації віртуальної мережі та вказана адресація мережевого рівня моделі OSI.

«Таблиця конфігурації VLAN» у Додатку Г містить дані для налаштування VLAN на мережевих пристроях.

2.2 Розробка схеми фізичного розташування кабелів та хостів

2.2.1 Типи кабелів та їх прокладка

Структурована кабельна система (СКС) - це система, яка передбачає комплексний підхід до проектування та впровадження кабельної інфраструктури для мережі певної компанії. Вона включає стандартизовані компоненти та методи, які забезпечують універсальність, гнучкість і надійність мережевої інфраструктури [1].

Причини впровадження СКС при побудові локальної мережі компанії наступні:

- Універсальність: структурована система дозволяє інтегрувати різні типи пристроїв і мережевих технологій. Це забезпечує передачу даних, голосу та відео, що в комплексі створює універсальне рішенням для комунікаційних потреб будь-якої компанії.

- Гнучкість - це здатність швидко адаптуватися до змін у комунікаційних потребах компанії. Така можливість доступна завдяки модульній структурі СКС. Наприклад, якщо вам потрібно додати нове робоче місце або перемістити існуюче, система дозволяє зробити ці зміни швидко без глобальних переробок і змін.

- Надійність – це здатність забепечувати певні функціональні параметри протягом визначеного часу. Для забезпечення надійності важливу роль відіграють стандартизація, уніфікація та використання високоякісних компонентів. Чим вища надійність тим менша ймовірність простоїв і збоїв в мережі.

- Економічна ефективність забезпечується незначними витратами на технічне обслуговування. Отже завдяки стандартизованим компонентам і методам роботи технічне обслуговування СКС є простішим і дешевшим порівняно з неструктурованими варіантами реалізаціями мереж.

- Висока швидкодія і продуктивність: стандарти СКС за замовчуванням забезпечують високу пропускну здатність і стабільність передачі даних. Ці показники є важливими для всіх співробітників компанії і загальному забезпечують потрібний рівень ефективності бізнес-процесів.

Загалом кажучи, інсталяція структурованої кабельної системи під час впровадження локальної мережі компанії «Сітер» – це інвестиція в стабільність і надійність, що в свою чергу забезпечить підтримку поточних та майбутніх потреб бізнесу і є однією з характеристик гнучкості інфраструктури.

2.2.2 Будова вузлів та необхідність їх застосування

Центральна частина структурованої кабельної системи проектованої локальної мережі буде реалізована як головний комутаційний вузол. Простіше кажучи апаратно це - комутаційна шафа, в якій буде встановлено:

1. Кабельні тримачі (cat6).
2. Патч-панель UTP (cat6).
3. Керований, центральний комутатор.
4. Сервери – дві одиниці .
5. Джерела безперебійного живлення також 2 одиниці.

Використовуючи вищенаведені пристрої, крім організації кабельної системи, можна фізично обмежити доступ до обладнання, забезпечити відповідний температурний режим, а також забезпечити швидкий і ефективний доступ при потребі перекомутування чи обслуговування.

2.3 Обґрунтування вибору комунікаційного обладнання

При стандартних підходах до побудови проекту локальної мережі використовуються активні і пасивні комунікаційні пристрої.

Як було зазначено вище, проектована мережа буде побудована на комутаторах. Ядром мережі має бути комутатор третього рівня моделі OSI, а комутаторами відділу мають бути керовані комутатори L2+. Порівняльна характеристика таких пристроїв наведена в таблиці «Порівняльна характеристика центральних комутаторів» у додатку Д.

В проекті цієї мережі було обрано комутатор Cisco WS-C3750G-24T-S [12]. Його загальний вигляд показано на рисунку 2.1. Незважаючи на те, що цей комутатор коштує дорожче, ніж аналогічні продукти, він має хороший функціонал, дуже надійний і має тривалу гарантію, тому інвестиції в нього точно окупляться протягом терміну служби.

Рисунок 2.1 – Комутатор Cisco WS-C3750G-24T-S

Цей комутатор стане ключовим вузлом у мережі, оскільки він має необхідні для проекту функціональні можливості та дуже стабільний у роботі. Він буде встановлений у головному вузлі комутації. Він повинен отримувати напругу живлення від джерела безперебійного живлення.

Таблиця «Порівняння функцій комутатора робочої групи» в Додатку Е містить порівняльний аналіз технічних характеристик 16-портового комутатора. Зваживши всі переваги і недоліки визначено, що комутатори AT-GS950/16 будуть використовуватися в робочих групах а також комутатори цієї ж серії AT-GS950/8 але на 8 портів. Техніко-експлуатаційні характеристики комутатора AT-FS750/16 наведено в відповідній таблиці в Додатку Е.

В проекті мережі потрібен шлюз доступу до Інтернету та файловий сервер. Базові вимоги до серверів є швидкодія та надійність. Швидкодія чи продуктивність - необхідна обчислювальна потужність, яку можна забезпечити використавши апаратну платформу на базі серверних процесорів Intel Xeon.

Таблиця «Порівняльна характеристика серверних апаратних платформ» Додатку З містить технічні характеристики апаратної бази сервера, який працюватиме як NAT та міжмережевий екран.

Зваживши на співвідношення ціни до функціональності виберемо сервер ARTLINE Business R25. Вибір даного сервера обумовлений достатнім рівнем його технічних та експлуатаційних характеристик [11].

Детальніше опишемо цю платформу. До її складу входить:

- материнська плата: спеціалізована серверна платформа P12R-M;
- CPU: Intel Xeon E-2336 – шестиядерний процесор з частотою до 4,2ГГц;
- 32 Гб оперативної пам’яті DDR4-3200 з корекцією помилок;
- набір необхідних інтерфейсів.

Вітчизняний виробник (агрегатор) встановив в цей сервер один із найкращих за характеристиками блок живлення Seasonic на 600 Вт, який має дуже хорошу надійність і сертифікат 80+ Bronze.

Стабілізацію електроживлення серверів, комутаторів та іншого обладання з комутаційної шафи реалізовано з використанням джерел безперебійного живлення 2U фірми APC серії Smart-UPS RT 2000 VA. Наведемо основні характеристики APC Smart-UPS RT 2000 BA:

- Топологія: онлайн (подвійне перетворення);

- Номінальна вихідна потужність: 2000VA/1400W;

- Час забезпечення вихідної напруги при повному навантаженні: - 4,5 хвилини;

- Час забезпечення вихідної напруги при навантаженні в 50% - 14,5 хвилин;

- Форма вихідної напруги: апроксимована синусоїда;

- Кількість вихідних роз'ємів для живлення пристроїв: (6/6);

- Виконання в корпусі висотою 2U;

- Частота вдіхної напруги : 46 - 65 Гц;

- Рівень вхідної напруги: 110-270В;

- Зміна форми вихідної напруги (режим батареї): ±3%;

- Можливість використання до 10 зовнішніх батерей[14].

Узагальнивши все вибране активне і пасивне обладнання для побудови локальної мережі внесемо дані в таблицю 2.1.

Таблиця 2.1 – Перелік необхідного телекомунікаційного обладнання

№ п/п	Перелік необхідного обладнання і матеріалів	Одиниці виміру	Кількість	Ціна, грн	Сума, грн.
1	2	3	4	5	6
1	Кабель вита пара UTP кат. 6 (бухта в упаковці 305 м)	шт	2	4750	9500
2	Роз'єми RJ-45	шт	120	1,6	192
3	Розетка мережева RJ-45 UTP	шт	42	200	8400
4	Кабельний тримач	шт	3	500	1500
5	Керований комутатор Cisco WS-C3750G-24T-S	шт	1	24000	24000
6	Керований комутатор Allied Telesyn AT-GS950/16	шт	3	4600	13800
7	Керований комутатор Allied Telesyn AT-GS950/8	шт	4	3570	14280
8	Файловий сервер ARTLINE Business R25	шт	1	32000	32000
9	Шлюз ARTLINE Business R25	шт	1	29800	29800
10	Комутаційна шафа 24U600x600GL	шт	1	14000	14000

Продовження таблиці 2.1

1	2	3	4	5	6
11	Патчпанель 24 порти UTP кат.6	шт	1	3400	3400
12	ББЖ APC Smart-UPS RT 2000	шт	2	18000	36000
13	Короб різного січення, загальний метраж	м	120	60	7200
14	Патчкорд категорія UTP 6	шт	80	18	1440
Сума, грн.					195512

2.4 Особливості монтажу мережі

Інсталяція і налаштування локальної мережі зі стандартом Gigabit Ethernet вимагає узгодження і дотримання технічних стандартів і системних процедур для забезпечення потрібної швидкості передачі даних і стабільності мережі. Ось кілька ключових особливостей, які слід враховувати [18]:

- Кабелі та роз'єми.

Кабельна система: для Gigabit Ethernet необхідно використовувати кабель принаймні категорії 5e (Cat5e). На даний час рекомендовано використовувати кабелі категорії 6 (Cat6) або 6a (Cat6a), які забезпечують більшу пропускну здатність і меншу втрату сигналу [16].

Роз’єми: для підключення пристроїв можна використати стандартні роз’єми RJ-45.

- Максимальна довжина сегмента.

Довжина кабелю: максимальна довжина ділянки кабелю Gigabit Ethernet становить 100 метрів. Це включає повну довжину кабелю між двома пристроями, включаючи всі патч-корди та інше.

- Мережеві компоненти.

Комутатори: для Gigabit Ethernet використовуйте комутатори, які підтримують 1Гбіт за секунду. Вони повинні бути якісними і мати реальні

показники. Також комутатори повинні обробляти великі обсяги трафіку без втрати продуктивності.

Карта мережевого інтерфейсу (NIC): усі мережеві адаптери в пристрої мають підтримувати швидкість 1 Гбіт/с.

- Монтаж і конструкція.

Організація кабелів. Рекомендується структурований підхід до прокладання кабелів із використанням кабельних каналів і органайзерів для забезпечення порядку та простоти обслуговування.

- Екранування: щоб зменшити електромагнітні перешкоди (EMI), особливо в середовищах із високим рівнем EMI, слід використовувати екрановані кабелі (STP або FTP).

- Екологічні вимоги.

Температура та вологість: мають бути забезпечені нормальні умови роботи мережевого обладнання. Слід уникати екстремальних температур і високої вологості, оскільки вони вплинуть на продуктивність і надійність обладнання.

- Джерело живлення: комутатори та інше важливе мережеве обладнання мають використовувати джерела безперебійного живлення (UPS) для захисту від перебоїв у електроживленні.

- Мережеві налаштування.

QoS (Якість обслуговування): якщо мережа підтримує QoS, її слід налаштувати так, щоб пріоритезувати критично важливі для бізнесу програми та служби.

- Віртуальна локальна мережа (VLAN): Рекомендується використовувати VLAN для розділення різних відділів або різних типів трафіку, що може підвищити безпеку та ефективність мережі.

- Тестування та сертифікація.

Тестування кабелю: після встановлення всі кабелі повинні бути перевірені спеціалізованим тестером, щоб підтвердити відповідність стандартам Cat5e, Cat6 або Cat6a.

Сертифікація: мережа має бути сертифікована, щоб продемонструвати відповідність вимогам Gigabit Ethernet.

Врахування цих особливостей забезпечить коректну інсталяцію та роботу локальних мереж стандарту Gigabit Ethernet, забезпечуючи максимальну швидкість і надійність передачі даних.

2.5 Аналіз та вибір операційних систем та ПЗ серверів і робочих станцій

Робоча станція в проекті локальної мережі використовує операційну систему Windows 10 Professional x64 і настільну операційну систему Linux Ubuntu 22.04. Обидві операційні системи підтримують стек протоколів TCP/IP і можуть працювати в локальній мережі за протоколом SMB. Використання різних операційних систем пояснюється переліком використовуваного користувачами програмного забезпечення та наявністю ліцензій OEM для операційних систем Windows.

На сервері використовується безкоштовне програмне забезпечення на основі рішень з відкритим кодом. Тому була обрана операційна система FreeBSD 13, яка підтримує можливість роботи в локальних і глобальних мережах і, крім того, має такі особливості:

1. Сумісність технології SMP.

2. Підтримка настільних та серверних процесорів, що використовують апаратні платформи x64.

3. Можливість безкоштовного завантаження оновлень безпеки операційної системи.

4. Наявність програмного забезпечення, утиліт і сервісів для організації служб локальної та глобальної мережі.

5. Можливість налаштування ядра.

6. Підтримка драйверами нового обладнання [14].

2.6 Тестування мережі

Тестування локальної комп'ютерної мережі передбачає використання різноманітних інструментів. Інструменти, що використовуються для тестування, описані в Розділі 3.2 «Інструкції з використання наборів тестів і процедур».

Крім того, програмні засоби, які будуть використовуватися для тестування апаратно-програмних компонентів мережі, що також детально описано в розділі 3.3 кваліфікаційної роботи «Інструкції з експлуатації та моніторингу в мережі».

2.7 Захист локальної комп'ютерної мережі

Сучасний стан кібербезпеки вимагає наявності систему захисту даних, що передаються або зберігаються в локальній комп'ютерній мережі. Системи захисту зазвичай поділяються на апаратні та програмні, та існує багато їх типів.

Одним із поширених варіантів захисту ЛОМ є використання брандмауера. Основним принципом його роботи є фільтрація трафіку, що надходить та/або виходить з мережі.

В операційній системі FreeBSD є досить потужна утиліта IPfw, яка призначена для управління системами трафік-фільтру. Вона надає мережевим адміністраторам можливість створювати і застосовувати різноманітні правила для керування фільтрацією, знищенням або пересиланням пакетів [14].

IPfw зазвичай використовується як окремий модуль, але існують також інструменти для його вбудовування в ядро операційної системи. IP firewall складається з таких базових компонент:

- софт-процесор для обробки правил рівня ядра;
- комплексна система обліку IP-пакетів;
- механізм розширеної статистики;
- механізм затримки і блокування пакетів;
- ipstealth (механізм підміни полів TTL для запобігання traceroute);

- інструменти управління якістю послуг (ALTQ);

- велика кількість правил взаємодії;

- механізм контролю пропускної здатності;

- система антиспуфінгу, яка може використовувати власні таблиці маршрутизації;

- внутрішні сервіси NAT, PAT і LSNAT (тільки у FreeBSD версії 7 і вище).

Отже, цей програмний файрвол добре підходить для задач фільтрування трафіку, має хороші засоби адміністрування і вільнопоширюваним. Тому він буде надалі використовуватися в нашому проекті.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування ПЗ серверів

3.1.1 Інструкції з налаштування файлового сервера

В даному підпункті опишемо налаштування файлового сервера з використанням cthdsce vsftpd під ОС Ubuntu Linux. Отже, VSFTP D (Very Secure FTP Daemon) є популярним і поширеним FTP-сервером для Unix-подібних систем. Він набув популярності бо давно відомий своєю безпекою та продуктивністю. Далі по тексту наведено покрокову інструкцію з налаштування нашого файлового сервера та служби vsftpd під керуванням ОС Ubuntu Linux.

Етап 1: Інсталяція vsftpd.

Спочатку оновлюємо список пакетів командою

```
sudo apt update
```

далі інсталюємо vsftpd командою

```
sudo apt install vsftpd
```

Етап 2: Базові настройки vsftpd

Про всяк випадок робимо резервну копію конфігурації командою

```
sudo cp /etc/vsftpd.conf  /etc/vsftpd.conf.orig
```

Переходимо до редагування конфігурації:

```
sudo nano /etc/vsftpd.conf
```

Далі наведемо приклад конфігураційного файлу:

```
# Режим запуску сервера
listen=NO
listen_ipv6=YES
# Дозвіл локальним користувачам входити
local_enable=YES
# Дозвіл запису для локальних користувачів
write_enable=YES
```

```
# Увімкнення додаткових налаштувань безпеки
chroot_local_user=YES
allow_writeable_chroot=YES
pasv_enable=YES
pasv_min_port=10000
pasv_max_port=10100
# Налаштування банерного повідомлення при підключенні
ftpd_banner=Welcome to FTP service.
# Відображення прихованих файлів
force_dot_files=YES
```

Створення директорії для FTP-користувачів:

```
sudo mkdir -p /home/ftpuser/ftp/upload
sudo chown nobody:nogroup /home/ftpuser/ftp
sudo chmod a-w /home/ftpuser/ftp
sudo chown ftpuser:ftpuser /home/ftpuser/ftp/upload
```

Етап 3: Створення нового FTP-користувача

Набираємо команду :

```
sudo adduser ftpuser
```

Етап 4: Рестарт vsftpd

Щоб зміни набули чинності робимо рестарт командою:

```
sudo systemctl restart vsftpd
```

та перевіряємо результат командою:

```
sudo systemctl status vsftpd
```

Етап 5: Налаштування самого брандмауера (UFW)

Вказуємо дозволи для портів 20, 21 і меж пасивних портів командою :

```
sudo ufw allow 20/tcp
sudo ufw allow 21/tcp
sudo ufw allow 10000:10100/tcp
sudo ufw reload
```

Етап 6: Тестування працездатності створеного FTP-сервера

Перевіримо роботу підключення до створеного FTP-сервера використовуючи будь-який FTP-клієнт (наприклад, CoreFTP). При відсутності програм-клієнтів, можна скористатися командою ftp в режимі консолі:

ftp <server-ip>

Перевірка працездатності процесу обміну даними та функціонал допоміжних компонент виконаємо за допомогою скрипта, наведено нижче:

```
#!/bin/bash
# Оновлення системи
sudo apt update
sudo apt install -y vsftpd
# Резервне копіювання конфігураційного файлу
sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig
# Створення конфігураційного файлу
cat <<EOF | sudo tee /etc/vsftpd.conf
listen=NO
listen_ipv6=YES
local_enable=YES
write_enable=YES
chroot_local_user=YES
allow_writeable_chroot=YES
pasv_enable=YES
pasv_min_port=10000
pasv_max_port=10100
ftpd_banner=Welcome to FTP service.
force_dot_files=YES
EOF
# Створення директорій для FTP
sudo mkdir -p /home/ftpuser/ftp/upload
```

```
sudo chown nobody:nogroup /home/ftpuser/ftp
sudo chmod a-w /home/ftpuser/ftp
sudo chown ftpuser:ftpuser /home/ftpuser/ftp/upload
# Створення користувача FTP
sudo adduser ftpuser
# Перезапуск служби vsftpd
sudo systemctl restart vsftpd
# Налаштування брандмауера
sudo ufw allow 20/tcp
sudo ufw allow 21/tcp
sudo ufw allow 10000:10100/tcp
sudo ufw reload
# Вивід статусу служби
sudo systemctl status vsftpd
```

Налаштування vsftpd на базі Ubuntu Linux містить послідовні етапи встановлення програмного забезпечення, налаштування сервера, створення користувача, налаштування брандмауера та тестування з'єднання. Реалізований в кваліфікаційній роботі скрипт призначений для автоматизації даного процесу.

3.1.2 Інструкції з налаштування серверу-шлюза локальної мережі - S2

У цьому розділі описано структуру і принципи побудови ланцюжків правил для фільтрації IP-трафіку. Сервер, на якому налаштована програма брандмауера, працює під керуванням операційної системи FreeBSD 13, а вхідними даними конфігурації є: локальна мережа 192.168.0.0/16;

Щоб налаштувати брандмауер, ядро потрібно перекомпілювати для реалізації ipfw [14]:

```
bsd-gate#  cd /usr/src/sys/amd64/conf/
bsd-gate#  cp GENERIC MYKERNEL
```

Спочатку відкриваємо файл MYKERNEL в текстовому редакторі і додаємо рядки:

- options Ipfirewall;

- options Ipfirewall_verbose;

- options Ipfirewall_verbose_limit=500;

- options Ipfirewall_forward;

- options Ipfirewall_default_to_accept.

Розглянемо їх докладніше:

- Ipfirewall - забезпечує базову підтримку ipfw.

- Ipfirewall_verbose - дозволяє реєструвати певні мережеві події у файлах статистики;

- Ipfirewall_verbose_limit=500 – обмежує кількість подій, які можна записати у файл статистики. В іншому випадку цією статистикою можна заповнити весь дисковий простір (особливо якщо зловмисник навмисне «заливає» цю ціль);

- Ipfirewall_forward - включає можливість пересилання пакетів. Наприклад, створіть прозорий проксі-сервер або приховайте будь-які сервери (веб-сервери, поштові) у локальній мережі, які мають бути доступні ззовні мережі;

- Ipfirewall_default_to_accept – за умовчанням брандмауер блокує весь трафік, який явно не дозволений. Той самий параметр змінює поведінку, тобто за замовчуванням дозволяє все, що явно не заборонено.

Це дуже зручно для віддаленого налаштування Під час процесу налагодження та налаштування шлюзу потрібно виконати команду ipfw –qlush. Інший варіант передбачає визначення останнього правила ipfw add Deny all from any до any, щоб брандмауер поводився так, ніби вищевказаний параметр вимкнено. Правило заборонити весь трафік від будь-якого до будь-якого стосується лише ip, вимкнення параметра Default_to_accept призведе до автоматичного блокування всього трафіку (наприклад, протоколу arp).

- Option Tcp_drop_synfin - відкидає пакети, які мають встановлені TCP-прапори SYN і FIN (у 99,99% випадків ситуація ненормальна, і пакет одночасно ініціює та розриває з'єднання). Наприклад, він іноді використовується зловмисниками для сканування хостів.

Після активації наведених вище параметрів збережіть, перезберіть і скомпілюйте ядро:

bsd-gate# cd /usr/src/

bsd-gate# make buildkernel Kernconf=mykernel

якщо все виконується без помилок, то прописуємо команди :

bsd-gate# make installkernel Kernconf=mykernel

bsd-gate# shutdown -r now

Таким чином нове ядро завантажено, далі необхідно підправити файл /etc/rc.conf, вписавші такі команди:

gateway_enable = "yes"

firewall_enable = "yes" # Set to YES to enable firewall functionality

firewall_script = "/etc/rc.ipfw" # Which script to run to set up the firewall

firewall_logging = "yes" # Set to YES to enable events logging

natd_enable = "yes" # Enable natd (if firewall_enable = YES).

natd_program = "/sbin/natd" # path to natd, if you want a different one.

natd_flags = "-f /etc/natd.conf" # Additional flags for natd.

За замловчуванням використовується firewall, який є в /etc/rc.firewall.

Далі буде описнао власний скріпт, який має власний набір правил фільтрації трафіку даних:

bsd-gate# vi /etc/rc.ipfw:

#!/bin/sh

Manual script for ipfw

echo -n "Starting firewall..."

ipfw = "/sbin/ipfw"

uports = "1025-65535"

int_if1 = "em0"

int_if2 = "em1"

ext_if = "xl0"

int_ip = "192.168.1.1"

ext_ip = "93.77.230.235"

int_net = "192.168.0.0/16"

ext_net = " 93.77.230.0/24"

Далі необхідно вирішити, які сервіси повинні бути доступні користувачам локальної мережі та самої операційної системи сервера. Таким чином дозволимо http, https, pop3, smtp які будуть доступні всім користувачам. Операційна система сервера повинна бути доступна через ftp, ssh. Для того, щоб все працювало належним чином, ім'я dns запитуваного сервера потрібно правильно транслювати.

Отже вказуємо вищевизначені параметри :

for_lan="smtp, pop3, domain, http, https"

for_rout="ftp, domain, ssh"

Services="smtp, pop3, http, https, domain, aol, ssh, ftp"

В розділі «Services» ми перерахуємо всі доступні послуги, незалежно від того, незалежно від того кому вони надаються. Брандмауер використовує файл /etc/services для перетворення імен портів у числову форму.

Далі ми опишемо стандартні правила, такі як loopback і anti-spoofing:

${ipfw} add allow all from any to any via lo0

${ipfw} add deny all from any to 127.0.0.0/8

Давайте захистимо мережу від зміни зовнішніх адрес. Зрештою, внутрішні мережі зазвичай (і в нашому випадку також) більш допустимі, ніж зовнішні мережі, тому зловмисник може спробувати змінити їхній вихідний IP, щоб обійти певні правила:

${ipfw} add deny all from 127.0.0.0/8 to any in recv $ext_if

${ipfw} add deny all from 10.0.0.0/8 to any in recv $ext_if

${ipfw} add deny all from 172.16.0.0/16 to any in recv $ext_if

${ipfw} add deny all from 192.168.0.0/24 to any in recv $ext_if

Далі наведемо правила, що фільтруватимуть трафік на зовнішньому інтерфейсі серверу:

${ipfw} add allow all from $int_net to any in recv $int_if

${ipfw} add allow all from any to $int_net out xmit $int_if

Після цього ми перенаправляємо весь необхідний трафік до демона natd, який порівнює віртуальну адресу машини в локальній мережі (трафік якої, як відомо, не направляється в Інтернет) з її реальним IP (для вхідної IP-адреси) підходити. течія, навпаки). Цей демон працюватиме на зовнішньому інтерфейсі.

Усі правила трафіку, які має обробляти демон natd, тобто трафік, який має (або може) спрямовуватися з локальної мережі на комп'ютер, мають відповідати правилам перенаправлення.

Таким чино :

${ipfw} add divert natd all from $int_net to not $int_net out xmit $ext_if

${ipfw} add divert natd all from any to $ext_ip in recv $ext_if

Дозволено вказати інший порт, на якому працює демон замість стандартного natd, але для цього той самий порт має бути вказаний у файлі конфігурації /etc/natd.conf.

Далі робота основної частини скрипта полягає в наступному - дозволити всі мінімально необхідні служби і відключити останню в кінці.

Дозволити вихідний трафік від операційної системи сервера до необхідних служб:

${ipfw} add allow tcp from $ext_ip $uports to any $Services out xmit $ext_if

Також дозволимо вхідний трафік в ЛОМ, який є їй необхідний:

${ipfw} add allow tcp from any $for_lan to $int_net $uports in recv $ext_if established

Ви повинні знати про встановлену опцію, яка обмежує це правило лише відповіддю на запитувані пакети (пакети з установленим прапорцем ACK або RST tcp).

Тоді задаємо команду для ОС сервера:

${ipfw} add allow tcp from any $for_rout to $ext_ip $uports in recv $ext_if established

Щоб DNS працював за новими правилами правимо.

${ipfw} add allow udp from $ext_ip $uports to any domain out xmit $ext_if
${ipfw} add allow udp from any domain to $ext_ip $uports in recv $ext_if
${ipfw} add allow udp from any domain to $int_net $uports in recv $ext_if

Змінимо правила для протоколу ICMP:

${ipfw} add allow icmp from any to me icmptypes 0,3,4,11,12 in
${ipfw} add allow icmp from any to $int_net icmptypes 0,3,4,11,12 in recv $ext_if
${ipfw} add allow icmp from me to any icmptypes 3,8,12 out

Додатково змінемо значення icmp кодів:

echo reply 0, destination unreachable 3, source quench 4, redirect 5, echo request 8, router adver-tisement 9, router solicitation 10, time-to-live exceeded 11, IP header bad 12, timestamp request 13, timestamp reply 14, information request 15, information reply 16, address mask request 17 and address mask reply 18.

Також правила для нашої мережі:

${ipfw} add allow tcp from $ext_ip $uports to any $uports out xmit $ext_if
${ipfw} add allow tcp from any $uports to $ext_ip $uports in recv $ext_if established

Наведені вище правила дозволяють не лише використовувати ftp, а й загалом усі служби, що працюють на портах з номерами поза 1024.

Останнім кроком є запис спроби встановлення з’єднання з операційною системою сервера у файл статистики:

${ipfw} add deny log logamount 700 tcp from any to $ext_ip in recv $ext_if setup

*logamount перебиває настройку Ipfirewall_verbose_limit.

Ну і на завершення треба заборонити передачу решти всього трафіку:

```
${ipfw} add deny all from any to any
echo "DONE"
```

Перезавантажуємо скріпт наступною командою:

```
#bsd-gate: /bin/sh /etc/rc.ipfw
```

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкція з налаштування комутатора ядра мережі

Першим етапом конфігурування комутатора 3-го рівня sw6 є задання параметрів транкових портів, до яких підключено комутатори 2-го рівня [13]:

```
sw6(config)#interface gigabitEthernet 0/1
sw6(config-if)#switchport mode trunk
sw6(config-if)#switchport trunk encapsulation dot1q
sw6(config-if)#no shutdown
sw6(config-if)#exit
sw6(config)#interface gigabitEthernet 0/2
sw6(config-if)#switchport mode trunk
sw6(config-if)#switchport trunk encapsulation dot1q
sw6(config-if)#no shutdown
sw6(config-if)#exit
sw6(config)#interface gigabitEthernet 0/3
sw6(config-if)#switchport mode trunk
sw6(config-if)#switchport trunk encapsulation dot1q
sw6(config-if)#no shutdown
sw6(config-if)#exit
sw6(config)#interface gigabitEthernet 0/4
sw6(config-if)#switchport mode trunk
sw6(config-if)#switchport trunk encapsulation dot1q
```

```
sw6(config-if)#no shutdown
sw6(config-if)#exit
sw6(config)#interface gigabitEthernet 0/5
sw6(config-if)#switchport mode trunk
sw6(config-if)#switchport trunk encapsulation dot1q
sw6(config-if)#no shutdown
sw6(config-if)#exit
sw6(config)#interface gigabitEthernet 0/6
sw6(config-if)#switchport mode trunk
sw6(config-if)#switchport trunk encapsulation dot1q
sw6(config-if)#no shutdown
sw6(config-if)#exit
sw6(config)#interface gigabitEthernet 0/7
sw6(config-if)#switchport mode trunk
sw6(config-if)#switchport trunk encapsulation dot1q
sw6(config-if)#no shutdown
sw6(config-if)#exit
```

Етап піл номером 2 - буде налаштування віртуальних мережевих інтерфейсів, які прив’язані до відповідних VLAN:

```
sw6(config)#interface vlan 101
sw6(config-vlan)#ip address 192.168.101.254 255.255.255.0
sw2(config-vlan)#no shutdown
sw6(config-vlan)#exit
sw6(config)#interface vlan 102
sw6(config-vlan)#ip address 192.168.102.254 255.255.255.0
sw6(config-vlan)#no shutdown
sw6(config-vlan)#exit
sw6(config)#interface vlan 103
sw6(config-vlan)#ip address 192.168.103.254 255.255.255.0
```

```
sw6(config-vlan)#no shutdown
sw6(config-vlan)#exit
sw6(config)#interface vlan 104
sw6(config-vlan)#ip address 192.168.104.254 255.255.255.0
sw6(config-vlan)#no shutdown
sw6(config-vlan)#exit
sw6(config)#interface vlan 105
sw6(config-vlan)#ip address 192.168.105.254 255.255.255.0
sw6(config-vlan)#no shutdown
sw6(config-vlan)#exit
sw6(config)#interface vlan 106
sw6(config-vlan)#ip address 192.168.106.254 255.255.255.0
sw6(config-vlan)#no shutdown
sw6(config-vlan)#exit
sw6(config)#interface vlan 107
sw6(config-vlan)#ip address 192.168.107.254 255.255.255.0
sw6(config-vlan)#no shutdown
sw6(config-vlan)#exit
sw6(config)#interface vlan 108
sw6(config-vlan)#ip address 192.168.108.254 255.255.255.0
sw6(config-vlan)#no shutdown
sw6(config-vlan)#exit
sw6(config)#interface vlan 109
sw6(config-vlan)#ip address 192.168.109.254 255.255.255.0
sw6(config-vlan)#no shutdown
sw6(config-vlan)#exit
sw6(config)#interface vlan 110
sw6(config-vlan)#ip address 192.168.110.254 255.255.255.0
sw6(config-vlan)#no shutdown
```

```
sw6(config-vlan)#exit
sw6(config)#interface vlan 111
sw6(config-vlan)#ip address 192.168.111.254 255.255.255.0
sw6(config-vlan)#no shutdown
sw6(config-vlan)#exit
sw6(config)#interface vlan 112
sw6(config-vlan)#ip address 192.168.112.254 255.255.255.0
sw6(config-vlan)#no shutdown
sw6(config-vlan)#exit
sw6(config)#interface vlan 113
sw6(config-vlan)#ip address 192.168.113.254 255.255.255.0
sw6(config-vlan)#no shutdown
sw6(config-vlan)#exit
```

Особливою є віртуальна мережа №113 адже в ній будуть розміщені в ній сервери.

Маршрутизації трафіку між віртуальними підмережами не буде до того часу, поки не виконати команду:

```
sw6(config)#ip routing
```

Також варто змінити IP-адресу дефолтного маршруту за замовчуванням:

```
sw6(config)#ip route 0.0.0.0 0.0.0.0 192.168.113.253
```

Увесь розроблений конфігураційний файл комутатора ядра мережі наведено в додатку Б даної роботи.

3.3 Інструкції з використання тестових наборів та програм

З метою тестування і перевірки роботи локальної мережі та її компонентів можна використовувати різні методи та інструменти, які допоможуть оцінити продуктивність, надійність та стабільність мережі. Ось докладний план тестування локальної мережі третьої сторони:

Крок 1. Перевірте фізичне підключення.

Перевірку варто почати візуального огляду. Інженери перевіряють усі кабельні з’єднання, щоб переконатися, що всі кабелі правильно під’єднано до відповідних портів комутаторів, маршрутизаторів і кінцевих пристроїв.

Переконайтеся, що всі кабелі не пошкоджені та прокладені правильно.

Перевірте світлові індикатори на мережевих платах і комутаторах. Інженери спостерігають за індикаторами на комутаторах і мережевих адаптерах, щоб визначити, чи є активні підключення.

Крок 2. Перевірте підключення до мережі.

Найпростіший і разом з тим ефективний варіант - команда ping. Він використовується для перевірки доступності інших пристроїв у мережі.

Приклад команди:

ping 192.100.100.1

Аналізуються такі параметри, як затримка та втрата пакетів.

Натупний етап - команда traceroute. Використовується для визначення маршруту для досягнення цільового пристрою.

Приклад команди:

Traceroute 4.4.4.4

Інженери аналізують маршрути та визначають можливі затримки або перешкоди.

Крок 3. Перевірте швидкість мережі.

На цьому кроці застосовано інструмент iperf. Він використовується для вимірювання пропускної здатності мережі.

Встановити iperf:

sudo apt iperf

Запустіть сервер iperf на одному з хостіві:

iperf3 -s

Запустіть клієнт iperf на хості:

iperf3 -c <IP-адреса сервера>

Далі фахівець аналізує результати роботи цих сервісів для визначення пропускної здатності між двома хостами.

Крок 4: Моніторинг основних показників мережі

Найдоступнішим варіантом є використання програмних засобів моніторингу мережі. Інженери часто використовують таке спеціалізоване ПЗ, як Nagios, Zabbix або Grafana, щоб діагностувати стан мережі в цілому та її компонентів. Важливо налаштувати куди відправляти відповідні попередження та сповіщення, коли виникають проблеми в роботі мережі чи окремих сервісів.

Крок 5. Перевірка безпеки мережі в цілому. Варто розпочати з сканування портів. Для цього можна скористатися інструментами nmap для перевірки відкритих портів і служб.

Наведемо приклад:

sudo nmap –s1 192.100.100.0/24

Після цього адміністратор системи аналізує результати, щоб виявити небажані відкриті порти.

Варто також зробити тестування вразливостей. Популярні інструменти в цій категорії ПЗ - OpenVAS або Nessus.

Крок 6: Проаналізуйте журнали.

Перевірте журнал подій. Фахівці перевіряють журнали комутаторів, маршрутизаторів і кінцевих пристроїв, щоб виявити можливі проблеми або аномалії.

Тестування локальної мережі та її компонентів включає фізичне тестування, тестування підключення, тестування швидкості мережі, моніторинг, тестування безпеки, аналіз журналів і використання спеціалізованих інструментів. Ці дії допомагають забезпечити стабільність, продуктивність і безпеку мережі.

3.4 Інструкції з експлуатації та моніторингу в мережі

Щоб налаштувати стек моніторингу, який включає Grafana, Prometheus і Alertmanager, фахівцям потрібно виконати детальний процес встановлення та налаштування цих інструментів [19].

Крок 1: Встановіть Prometheus. Оновіть список пакетів і встановіть Prometheus:

```
sudo apt update
sudo useradd --no-create-home --shell /bin/false prometheus
sudo mkdir /etc/prometheus
sudo mkdir /var/lib/prometheus
```

Команди для запуску Prometheus:

```
wget
https://github.com/prometheus/prometheus/releases/download/v2.36.2/prometheus-2.36.2.linux-amd64.tar.gz
tar xvf prometheus-2.36.2.linux-amd64.tar.gz
cd prometheus-2.36.2.linux-amd64
sudo cp prometheus /usr/local/bin/
sudo cp promtool /usr/local/bin/
sudo cp -r consoles /etc/prometheus
sudo cp -r console_libraries /etc/prometheus
sudo cp prometheus.yml /etc/prometheus
```

Далі редагуємо конфігураційний файл під власні потреби /etc/prometheus/prometheus.yml:

```
global:
 scrape_interval: 15s
scrape_configs:
 - job_name: 'prometheus'
 static_configs:
```

- targets: ['localhost:9090']

Наступний крок - творення сервісу для Prometheus:

```
sudo nano /etc/systemd/system/prometheus.service
[Unit]
Description=Prometheus
Wants=network-online.target
After=network-online.target
[Service]
User=prometheus
ExecStart=/usr/local/bin/prometheus --config.file /etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
[Install]
WantedBy=multi-user.target
```

Перезавантажуємо Prometheus командами:

```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

Крок 2: Встановлення менеджера повідомлень Alertmanager. Взірець команд:

```
wget https://github.com/prometheus/alertmanager/releases/download/v0.24.0/alertmanager-0.24.0.linux-amd64.tar.gz
tar xvf alertmanager-0.24.0.linux-amd64.tar.gz
cd alertmanager-0.24.0.linux-amd64
sudo cp alertmanager /usr/local/bin/
sudo cp amtool /usr/local/bin/
sudo mkdir /etc/alertmanager
sudo cp alertmanager.yml /etc/alertmanager/
```

Налаштування Alertmanager розпочинається з редагування конфігураційного файлу під власні потреби:

/etc/alertmanager/alertmanager.yml:

```
global:
resolve_timeout: 5m
route:
receiver: 'team-X-mails'
receivers:
- name: 'team-X-mails'
email_configs:
- to: 'team-X@example.com'
from: 'alertmanager@example.com'
smarthost: 'smtp.example.com:587'
auth_username: 'alertmanager@example.com'
auth_identity: 'alertmanager@example.com'
auth_password: 'password'
```

Далі створюємо новий сервіс для Alertmanager:

sudo nano /etc/systemd/system/alertmanager.service

Вміст файлу:

```
[Unit]
Description=Alertmanager
Wants=network-online.target
After=network-online.target
[Service]
User=alertmanager
ExecStart=/usr/local/bin/alertmanager --config.file /etc/alertmanager/alertmanager.yml
--storage.path /var/lib/alertmanager/
[Install]
WantedBy=multi-user.target
```

Запуск Alertmanager:

```
sudo systemctl daemon-reload
sudo systemctl start alertmanager
sudo systemctl enable alertmanager
```

Крок 3: Встановлення Grafana. Додавання репозиторію Grafana:

```
sudo apt-get install -y software-properties-common
sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"
wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -
sudo apt-get update
```

Встановлення Grafana:

```
sudo apt-get install grafana
```

Запуск Grafana:

```
sudo systemctl start grafana-server
sudo systemctl enable grafana-server
```

Крок 4: Інтеграція та налаштування. Інтеграція Prometheus з Grafana:

Інженер входить у веб-інтерфейс Grafana за адресою http://<server-ip>:3000. Заходить у розділ Configuration -> Data Sources та додає нове джерело даних Prometheus:

URL: http://localhost:9090

Тестує підключення і зберігає налаштування.

Налаштування Grafana для відображення метрик. Інженер створює новий дашборд і додає панелі для відображення метрик з Prometheus. Налаштовує графіки та інші візуальні елементи для моніторингу ключових параметрів системи.

Інтеграція Alertmanager з Prometheus: інженер редагує конфігураційний файл Prometheus /etc/prometheus/prometheus.yml, додавши налаштування для Alertmanager:

```
alerting:
  alertmanagers:
```

```
    - static_configs:
        - targets:
          - localhost:9093
rule_files:
  - "alert.rules"
```

Налаштування правил для Alertmanager. Інженер створює файл правил для Prometheus, наприклад /etc/prometheus/alert.rules:

```
groups:
  - name: example
    rules:
      - alert: InstanceDown
        expr: up == 0
        for: 5m
        labels:
          severity: 'critical'
        annotations:
          summary: "Instance {{ $labels.instance }} down"
          description: "{{ $labels.instance }} of job {{ $labels.job }} has been down for more than 5 minutes."
```

Перезапуск Prometheus для застосування змін:

```
sudo systemctl restart prometheus
```

Інженер налаштовує стек моніторингу, що включає Grafana, Prometheus та Alertmanager, через процес встановлення, конфігурації та інтеграції цих інструментів. Prometheus відповідає за збір метрик, Alertmanager обробляє оповіщення, а Grafana забезпечує візуалізацію даних, що дозволяє ефективно моніторити стан системи та швидко реагувати на проблеми [19].

3.5 Моделювання роботи локальної мережі

Моделювання локальної мережі проводитиметься в середовищі програми Packet Tracer 5. Packet Tracer - це симулятор мережі передачі даних, створений Cisco Systems. Метою моделювання є побудова локальної мережі за логічною топологією та перевірка правильності її побудови шляхом імітації роботи протоколу ICMP. Отже будуємо логічну топологію мережі, показану на рисунку3.1 взявши за взірець плакат «Логічна топологія»

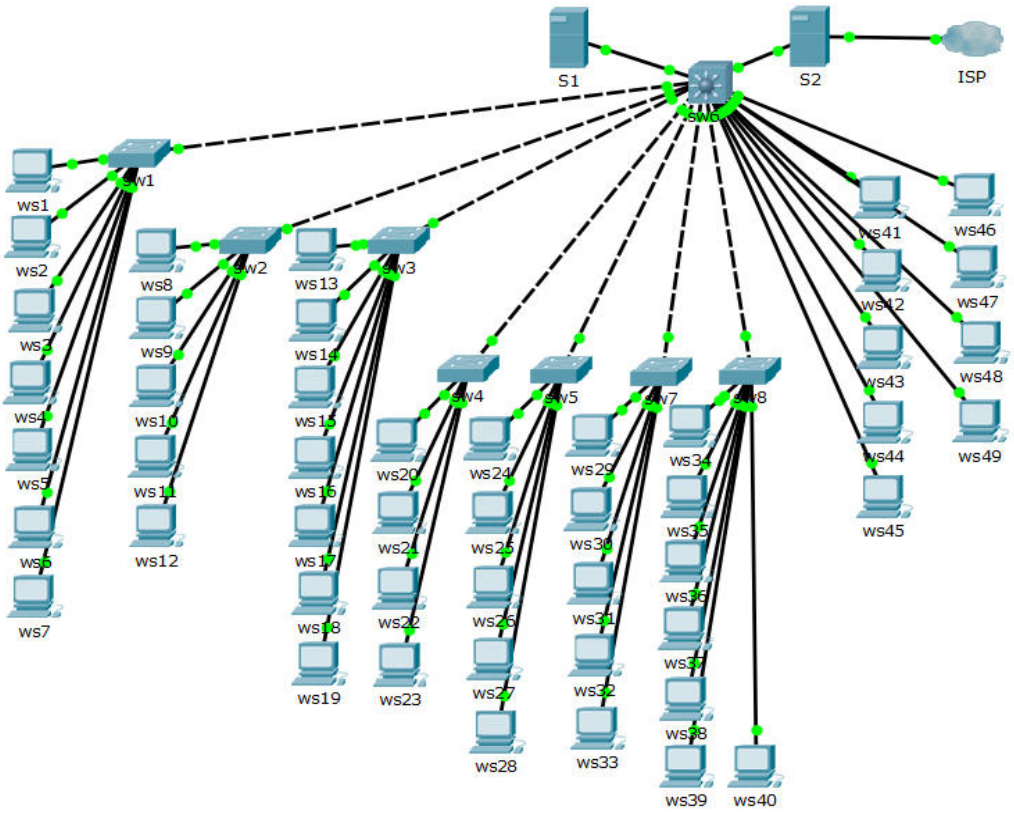

Рисунок 3.1 – Змодельована логічна топологія

Під час моделювання використовуватиметься мережеве обладнання Cisco. Для прикладу змоделюємо роботу протоколу ICMP між вузлом S_1 і PC1. Для цього потрібно налаштувати стек протоколів TCP/IP вузла S_1, за взірцем рисунку 3.2

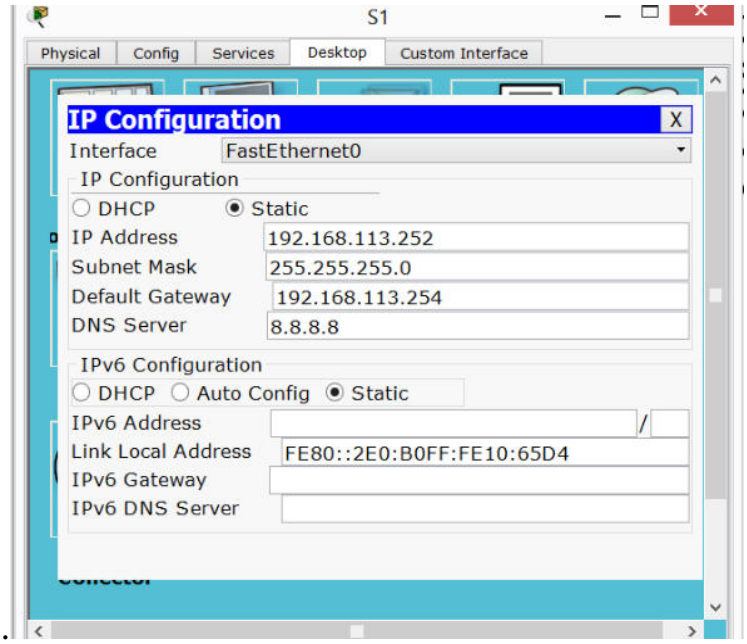

Рисунок 3.2 – Параметри протокольного стеку TCP/IP вузла S_1

Нижче, на рисунку 3.3 наведено параметри протокольного стеку TCP/IP для вузла PC1.

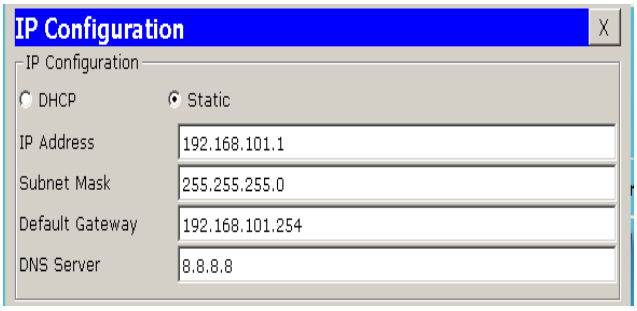

Рисунок 3.3 – Взірець конфігурування стеку TCP/IP хоста PC22

Для перевірки роботи нашого прикладу в командному рядку хоста PC1 виконаємо команду ping 192.168.113.252. Отримаємо такий результат виконання команди:

```
PC1>ping 192.168.113.252
Pinging 192.168.113.252 with 32 bytes of data:
Reply from 192.168.113.252: bytes=32 time=0ms TTL=128
Reply from 192.168.113.252: bytes=32 time=0ms TTL=128
Reply from 192.168.113.252: bytes=32 time=0ms TTL=128
Reply from 192.168.113.252: bytes=32 time=0ms TTL=128
Ping statistics for 192.168.113.252:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC1>
```

Отже, результатом моделювання є швидкий обмін пакетами і без втрат даних по налаштованому протоколу ICMP. Таким чином можна зробити висновок, що прийняті рішення і реалізовані налаштування є вірними, модель а отже і мережа в цілому будуть працювати згідно заданих параметрів.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для компанії «СІТЕР» і прийняття рішення про її подальше впровадження в роботу.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР дані витрат часу по окремих операціях технологічного процесу зводяться у таблицю 4.1.

Таблиця 4.1 - Середній час виконання НДР та стадій технологічного процесу

№ п/п	Назва стадії	Виконавець	Середній час виконання операції, год.
1	Постановка задачі та збір інформації про об'єкт	Керівник проекту	10
2	Розробка проекту	Інженер	10
3	Узгодження та затвердження проекту	Керівник проекту	1
4	Монтаж мережі	Технік	40
5	Налагодження мережі та створення технічної документації	Інженер	30
Разом			91

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для компанії «СІТЕР» складає 91 годину.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Оплата праці - грошовий вираз вартості і ціни робочої сили, який виступає у формі будь-якого заробітку, виплаченого керівником підприємства найманому працівникові за виконану роботу.

Заробітна плата працівника залежить від кінцевих результатів його роботи, регулюється податками і максимальними розмірами не обмежується.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г \,, \qquad (4.1)$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Рекомендовані тарифні ставки: керівник проекту – 80 грн./год., інженер – 70 грн./год., технік – 60 грн./год.

Отже, основна заробітна плата для:

1. Керівник проекту - $З_{осн1} = 11 \cdot 80 = 880$ грн.
2. Інженер - $З_{осн2} = 40 \cdot 70 = 2800$ грн.
3. Технік - $З_{осн3} = 40 \cdot 60 = 2400$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 880 + 2800 + 2400 = 6080{,}00 \text{ грн.}$$

Додаткова заробітна плата становить 10 – 15 % від суми основної заробітної плати та обчислюється за формулою 4.2.

$$З_{дод.} = З_{осн.} \cdot К_{допл.} \,, \qquad (4.2)$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам: 0,1 – 0,15.

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проекту - $З_{дод1}$= 880 · 0,15 = 132,00 грн.
2. Інженер - $З_{дод2}$ = 2800 · 0,15 = 420,00 грн.
3. Технік - $З_{дод3}$ = 2400 · 0,15 = 360,00 грн.

Загальна додаткова заробітна плата становить:

$$З_{дод} = 132,00+420,00+360,00 = 912,00 \text{ грн.}$$

Звідси загальні витрати на оплату праці розраховуються за формулою 4.3:

$$В_{о.п.}=З_{осн.}+З_{дод.}\,, \qquad (4.3)$$

$$В_{о.п}=6080,00+912,00 = 6992,00 \text{ грн}$$

Необхідно визначити відрахування на соціальні заходи:

1. Фонд страхування на випадок безробіття – 1,6 %;
2. Фонд по тимчасовій втраті працездатності – 1,4 %;
3. Пенсійний фонд – 33,2 %;
4. Внески на страхування від нещасного випадку на виробництві та професійного захворювання - 1,4%.

Загальна сума зазначених відрахувань становить 37,6 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.}= ФОП \cdot 0,376, \qquad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$В_{с.з.}= 6992,00 \cdot 0,376= 2628,99 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія прац.	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	80	11	880	132,00	-	-
2	Інженер	70	40	2800	420,00	-	-
3	Технік	60	40	2400	360,00	-	-
Разом				6080,00	912,00	6992,00	9620,99

Отже, загальні витрати на оплату праці становлять 9620,99 грн.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни (формула 4.5):

$$M_{Bi} = q_i \cdot p_i \qquad (4.5)$$

де q_i – кількість витраченого матеріалу i-го виду;

p_i – ціна матеріалу i-го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$З_{м.в.} = \sum M_{Bi} \qquad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Перелік матеріалів і мережевого обладнання	Од. вим.	К-сть	Ціна, грн	Сума, грн.
1	Кабель вита пара UTP кат. 6 (бухта в упаковці 305 м)	шт	2	4750	9500
2	Роз'єми RJ-45	шт	120	1,6	192
3	Розетка мережева RJ-45 UTP кат. 6	шт	42	200	8400
4	Кабельний тримач	шт	3	500	1500
5	Керований комутатор Cisco WS-C3750G-24T-S	шт	1	24000	24000
6	Керований комутатор Allied Telesyn AT-GS950/16	шт	3	4600	13800
7	Керований комутатор Allied Telesyn AT-GS950/8	шт	4	3570	14280
8	Файловий сервер ARTLINE Business R25	шт	1	32000	32000
9	Шлюз ARTLINE Business R25	шт	1	29800	29800
10	Комутаційна шафа 24U600x600GL	шт	1	14000	14000
11	Патчпанель 24 порти UTP кат.6	шт	1	3400	3400
12	ББЖ APC Smart-UPS RT 2000	шт	2	18000	36000
13	Короб різного січення, загальний метраж	м	120	60	7200
14	Патчкорд категорія UTP 6	шт	80	18	1440
Сума, грн.					195512

Загальна сума матеріальних витрат на розробку мережі становить 195512,00 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання розраховуються за формулою 4.7:

$$З_е = W \cdot T \cdot S \quad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 18 годин, споживана потужність - 0,5 кВт/год, вартість 1 кВт електроенергії для ФОП станом на червень 2024 року – 7,06 грн.

Тому витрати на електроенергію будуть становити:

$$З_е = 0,5 \cdot 18 \cdot 7,06 = 63,54 \text{ грн.}$$

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8 – 10 % від загальної суми матеріальних затрат. Транспортні витрати розраховуються за формулою 4.8.

$$Т_в = З_{м.в.} \cdot 0,08...0,1, \quad (4.8)$$

де $Т_в$ – транспортні витрати.

Отже, транспортні витрати будуть становити:

$$Т_в = 195512,00 \cdot 0,08 = 15640,96 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

Комп'ютери та оргтехніка належать до четвертої групи основних фонді. Мінімально допустимі строки їх використання 2 роки. Для визначення амортизаційних відрахувань використовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{150\%} \cdot T, \tag{4.9}$$

де A – амортизаційні відрахування за звітний період, грн.

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %;

T – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 18 год., балансова вартість ПК – 30000 грн., тому:

$$A = \frac{30000 \cdot 0{,}05}{150} \cdot 18 = 180{,}00 \ грн.$$

4.7 Обчислення накладних витрат

Накладні витрати - це витрати, не пов'язані безпосередньо з технологічним процесом виготовлення продукції, а утворюються під впливом певних умов роботи по організації, управлінню та обслуговуванню виробництва.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20 – 60 % від суми основної та додаткової заробітної плати працівників, обчислюються за формулою 4.10.

$$Н_в = В_{о.п.} \cdot 0{,}2...0{,}6, , \tag{4.10}$$

де, $Н_в$ – накладні витрати.

$$H_в = 6992,00 \cdot 0,3 = 2097,60 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Кошторис витрат являє собою зведений план усіх витрат підприємства на майбутній період виробничо-фінансової діяльності.

Результати проведених вище розрахунків зведемо у таблиці 4.4.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	6992,00	3,13
Відрахування на соціальні заходи	2628,99	1,18
Матеріальні витрати	195512,00	87,63
Витрати на електроенергію	63,54	0,03
Транспортні витрати	15640,96	7,01
Амортизаційні відрахування	180,00	0,08
Накладні витрати	2097,60	0,94
Собівартість	223115,09	100,00

Собівартість ($C_В$) НДР розрахуємо за формулою 4.11:

$$C_в = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_в + Т_в + А + Н_в \quad (4.11)$$

Отже, собівартість дорівнює: $C_в$=223115,09 *грн.*

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12:

$$Ц = С_в \cdot (1+Р_{рен}) \cdot (1+ПДВ), \quad (4.12)$$

де $С_в$ – собівартість виконання НДР;

$Р_{рен.}$ – рівень рентабельності, 30 %

ПДВ – ставка податку на додану вартість, 20 %.

$$Ц = 223115,09 \cdot (1+0,3) \cdot (1+0,2) = 348059,54 \text{ грн.}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва - категорія, яка характеризує результативність виробництва. Вона свідчить не лише про приріст обсягів виробництва, а й про те, якими витратами ресурсів досягається цей приріст, тобто свідчить про якість економічного зростання.

Прибуток розраховується за формулою:

$$П = Ц - С_в \quad (4.13)$$

$$П = 348059,54 – 223115,09 = 124944,45 \text{ грн.}$$

Економічна ефективність ($Е_р$) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою 4.14.

$$Е_р = П / С_в, \quad (4.14)$$

де $П$ – прибуток;

$С_в$ – собівартість.

$$Е_р = 124944,45 / 223115,09 = 0,56$$

Поряд із економічною ефективністю розраховують (формула 4.15) термін окупності капітальних вкладень ($Т_р$):

$$T_p = 1 / E_p \qquad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку $T_р$=1/0,56=1,79.

Всі дані розрахунків внесемо в зведену таблицю 4.5 техніко-економічних показників.

Таблиця 4.5 - Техніко-економічні показники розробки мережі

№ п/п	Показник	Значення
1.	Собівартість, грн.	223115,09 грн.
2.	Плановий прибуток, грн.	124944,45 грн.
3.	Ціна, грн.	348059,54 грн.
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,79

Загальна вартість розробленої комп'ютерної мережі для компанії «CITEP» становить 348059,54 грн. Як видно з таблиці 4.4 в кошторисі витрат 87% складають матеріальні затрати. Тому така сумарна вартість є обгрунтованою і не виходить за верхню межу встановлену замовником в 350 тис. грн.

Зважаючи на високі показники економічної ефективності - 0,56 кошти, вкладені в проведення проектних робіт окупляться за 1,79 року.

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

Охорона праці - як галузь людської діяльності - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних та лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я та працездатності людини у процесі її трудової діяльності. Основною метою охорони праці є створення безпечних умов трудової діяльності людини, забезпечення її високої та ефективної працездатності [8].

Охорона праці як соціально-технічна дисципліна вивчає теоретичні та практичні питання безпеки праці, запобігання виробничому травматизму, професійним захворюванням і отруєнням, аваріям (катастрофам), пожежам і вибухам на виробництві. Вона вивчається з метою формування у майбутніх фахівців необхідного рівня знань та умінь з правових й організаційних питань охорони та гігієни праці, виробничої санітарії, техніки безпеки, а також активної позиції щодо практичної реалізації головного принципу Конституції України - пріоритетності охорони життя та здоров'я працівників відносно результатів виробничої діяльності [6].

Предметом охорони праці як галузі знання є умови праці, а об'єктом її дослідження виступає виробнича система, яка включає людину, машину (виробниче устаткування) та середовище, в якому здійснюється виробничий процес.

5.1 Принцип дії занулення електромереж та область його застосування

Призначення захисного занулення ідентичне призначенню захисного заземлення – зменшення небезпеки враження працівників електричним струмом у випадку замикання фази на корпус електроустановки. Згідно ПУЕ, захисне

занулення корпусів електроустановок застосовується в тих же випадках, що й захисне заземлення.

Суть захисного занулення електроустановок полягає у навмисному електричному з'єднанні їх металевих нормально неструмопровідних частин, які можуть опинитись під напругою, з нульовим захисним провідником (див. рис. 5.1) [6].

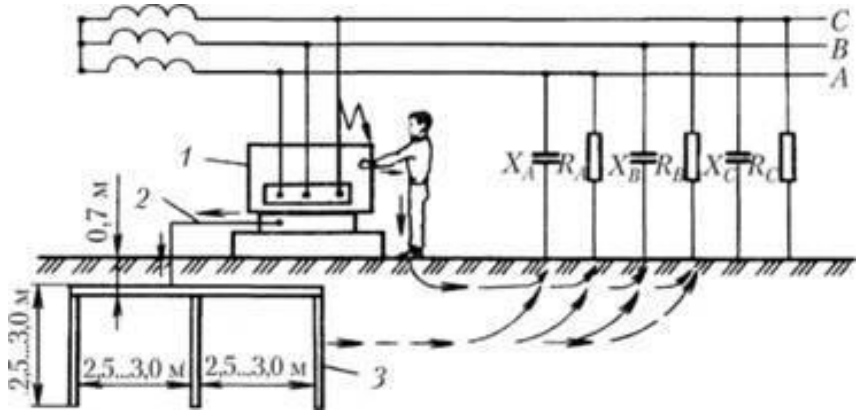

Рисунок 5.1 - Схема захисного занулення електроустановки:
1 - електроустановка; 2 - заземлюючий провідник; 3 – заземлювач.

При цьому нульовий робочий провідник з’єднаний із глухозаземленою нейтральною точкою джерела струму і призначений для живлення струмом електроспоживачів (тобто по ньому проходить робочий струм), а нульовий захисний провідник з'єднує частини електроустановки, що підлягають зануленню, з нульовим робочим провідником.

Принцип дії занулення полягає у перетворенні замикання мережі на корпус електроустановки в однофазне коротке замикання (тобто замикання між фазним та нульовим робочим провідниками) з метою раптового збільшення величини сили струму, здатної призвести до спрацювання захисного пристрою (котре полягає у перегоранні плавких запобіжників чи приведенні в дію автоматичних вимикачів) і автоматичного відімкнення пошкодженої установки від мережі живлення.

Таким чином призначення:

- нульового захисного провідника – створення для струму короткого замикання ланцюга з малим опором із метою забезпечення швидкого спрацювання захисного пристрою і автоматичного відімкнення пошкодженої установки від мережі живлення; - заземлення нейтралі джерела струму – зниження до безпечного рівня величини напруги нульового робочого провідника (і всіх під'єднаних до нього корпусів електроустановок) відносно землі при випадковому замиканні на неї фази;

- додаткового заземлення нейтралі джерела струму – зменшення небезпеки враження працівників електричним струмом у випадку обривання нульового робочого провідника.

Умова надійності захисного занулення (тобто швидкого автоматичного відімкнення пошкодженої електроустановки від мережі живлення) [8]:

$$I_{к.з.} \geq k \cdot I_{ап} \qquad (5.1)$$

де $I_{к.з}$ - струм короткого замикання;

$I_{ап}$ - струм захисного пристрою (апарата);

k - коефіцієнт кратності струму короткого замикання відносно струму захисного пристрою (k = 1,5 - для автоматичних вимикачів; k = 3,0 - для плавких запобіжників). Час відімкнення пошкодженої електроустановки від мережі живлення становить: при захисті плавкими запобіжниками 5–7 с; при захисті автоматами 1–2 с.

З метою підвищення рівня електробезпеки виробничого устаткування найчастіше застосовують його одночасне занулення та заземлення.

5.2 Розрахунок системи штучного освітлення

Розрахунок освітлення робочих місць проведемо для приміщення ІТ-відділу, оскільки саме там працює адміністратор мережі.

Розрахунок виконаємо згідно методики [6].

Розміри кімнати довжина a =3м, ширина b=2.5м, висота h=3,5м. Коефіцієнт відбиття $\rho_{стелі}$=50%, $\rho_{стін}$ = 30%. Висота робочих поверхонь (столів) h_p = 0,7 м. Для освітлення прийнято світильники типу ПО-21, які підвішуються до стелі; відстань від світильника до стелі h_c = 0,5 м. Мінімальна освітленість за нормами E_p = 250 лк.

Визначаємо висоту підвісу світильників над підлогою:

$$h_o = H - h_c \qquad (5.2)$$

$$h_o = 3{,}5 - 0{,}5 = 3 \text{ (м)}$$

Для світильників загального освітлення з лампами розжарювання потужністю до 200 Вт мінімальна висота підвісу над підлогою відповідно до СниП II-4-79 повинна бути 2,5 – 4,0 м, залежно від характеристики світильника. В нашому випадку h_o відповідає цій вимозі.

Висота підвісу світильника над робочою поверхнею (див. рис. 5.2) визначається за формулою:

$$h = h_o - h_p \qquad (5.3)$$

$$h = 3–0{,}7=2{,}3 \text{ (м)}$$

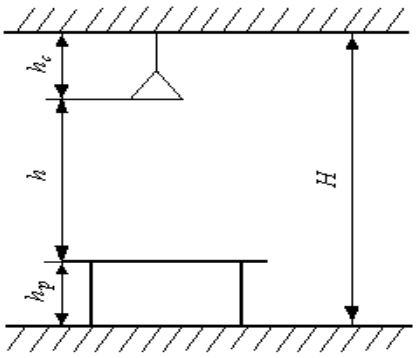

Рисунок 5.2 - Схема визначення висоти підвісу світильника

Рівномірність освітлення досягається при відповідному співвідношенні відстані між світильниками і висоти їх підвісу h.

Визначимо рекомендовану відстань між світильниками:

$$L = 0{,}7h \tag{5.4}$$

$$L = 0{,}7 \cdot 2{,}3 = 1{,}61 \text{ (м)},$$

Необхідна кількість світильників становить:

$$N = \frac{ab}{L^2} \tag{5.5}$$

$$N = \frac{3.4 \cdot 2{,}5}{1{,}61^2} = 3.32(шт.)$$

Для рівномірності освітлення приймаємо 3 світильники, розташовуємо їх у один ряд, посередині приміщення (див. рис. 5.3)

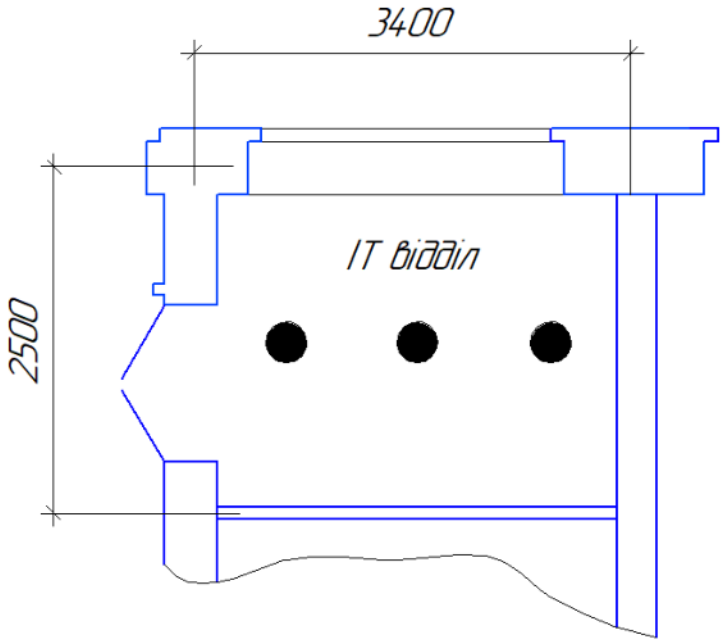

Рисунок 5.3 - Схема розташування світильників ПО-21 в ІТ-відділі

Показник приміщення *i* становить:

$$i = \frac{ab}{h(a+b)} \tag{5.6}$$

$$i = \frac{3{,}4 \cdot 2{,}5}{3 \cdot (3{,}4 + 2{,}5)} = 0{,}48$$

Знаходимо коефіцієнт використання η = 0,20 для світильника ПО–21 при i = 0,5, $\rho_{СТЕЛІ}$ = 50%, $\rho_{СТІН}$ = 30%; $К_З$=1,1; Z =1,14.

Світловий потік одного світильника, а значить і лампи, оскільки за конструктивним виконанням у світильнику встановлюється лише одна лампа, визначається за формулою:

$$\Phi_л = \frac{ESK_3Z}{N\eta} \qquad (5.7)$$

$$\Phi_л = \frac{250 \cdot 8{,}5 \cdot 1{,}1 \cdot 1.14}{3 \cdot 0{,}20} = 4441{,}25 \ лм$$

З метою економії електроенергії підбираємо світлодіодні (LED) лампи, які сумісні з даними світильниками врахувавши необхідний світловий потік.

Таким вимогам задовольняє, наприклад, лампа LED E27 Lezard 220V HP 50,0W/6400 T100, яка зображена на рисунку 5.4.

Рисунок 5.4 – Лампа LED E27 Lezard 220V HP 50

Технічні характеристик обраної лампи наведено в таблиці 5.1.

Таблиця 5.1 – Характеристики LED E27 Lezard 220V HP 50

№ п.п.	Характеристика	Значення
1	Тип	Світлодіодні лампи (LED)
2	Призначення	Промислові
3	Тип під'єднання	Однофазне
4	Потужність	50 Вт
5	Напруга	176-265 В
6	Тип цоколя	E27
7	Колірна температура	Холодний білий (6400К)
8	Світловий потік	4500Лм

Сумарна електрична потужність усіх світильників, встановлених у приміщенні становить:

$$\sum P_{СВ} = P_{СВ} N \qquad (5.8)$$

$$\sum P_{СВ} = 50 \cdot 3 = 150 Вт$$

Отже розрахунок проведено згідно існуючих вимог, вибрані джерела світла є достатньо ефективними і економними.

ВИСНОВКИ

Тема кваліфікаційної роботи – розробка проекту локальної комп'ютерної мережі компанії «Сітер».

Проект локальної мережі включає:

– План приміщення.

– Логічна топлогія.

– Фізична топологія.

– Інструкції з налаштування активного мереженого обладнання та серверів.

– Інструкції з застосування апаратних та програмних засобів діагностики неполадок локальної мережі.

Кваліфікаційна робота містить повністю завершену логічну і фізичну топології мережі, які подано в графічній частині.

Під час проектування особливу увагу звернуто на захист локальної мережі, розробку детальних інструкцій з налаштування комутаційного обладнання та серверів.

Також в процесі роботи реалізовано модель мережі і обчислено завантаження файлового серверу.

В економічній частині зроблено розрахунком повної вартості робіт по проектуванню, встановленню і запуску в експлуатацію мережі.

Останній розділ роботи описує питання охорони праці, та техніки безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Буров, Є.В. Комп’ютерні мережі: навч. посіб. Львів: Магнолія-2006. 2010. 262с.

2. Галіцин В.К., Левченко Ф.А. Багатокористувацькі обчислювальні системи та мережі. Київ: КНЕУ, 2018. 360с.

3. Горбатий І.В., Бондарєв А.В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи. Львів: Львівська політехніка. 2016. 336с.

4. Горлач В.М., Макар В.М. Побудова та адміністрування INTRANET-мереж Ч.1. Основи мережних технологій. Тексти лекцій. Львів: Львів. ун–т, 2006. 145с.

5. Горлач В.М., Макар В.М. Побудова та адміністрування INTRANET-мереж Ч.2. Адміністрування мереж Windows . Тексти лекцій. Львів: Львів. ун–т, 2008. 141с.

6. Жидецький В.Ц. Охорона праці користувачів комп’ютерів. навч. посіб.. 2-ге. вид., доп. Львів: Афіша. 2010. 176с.

7. Жуков І.А., Дрововозов В.І., Махновський Б.Г. Експлуатація комп’ютерних систем та мереж. Київ: НАУ. 2017. 361с.

8. Микитишин А.Г., Митник, П.Д. Стухляк. Телекомунікаційні системи та мережі. Тернопіль: Вид-во ТНТУ імені Івана Пулюя. 2016. 384 с.

9. Рикалюк Р.Є., Стягар О.М., Данчак П.В. Вступ до комп’ютерних мереж. Текст лекцій. Львів: Львів. ун–т, 2016. 160с.

10. Тхір І.,Калушка В., Юзьків А. Посібник користувача ПК.3-е вид. Тернопіль: Підручники і посібники. 2006. 1024с.

11. ARTLINE Business R25. URL: https://kvshop.com.ua/desktopy/artline/artline-business-r25-r25v26/ (дата звернення: 1.06.2024).

12. Cisco Catalyst 3750G-48 Switch. URL: http://www.cisco.com/c/en/us/support/switches/catalyst-3750g-48-switch/model.html. (дата звернення: 16.05.2024).

13. Cisco VLAN – настройка vlan на комутатор Cisco URL: http://www.adminia.ua/cisco-vlan-nastroyka-vlan-na-kommutatore-cisco/. (дата звернення: 23.05.2024).

14. FreeBSD Handbook. URL: https://docs.freebsd.org/en/books/handbook/ (дата звернення: 23.05.2024).

15. G950 Series Gigabit WebSmart. URL: https://www.alliedtelesis.com/products/gs950-series (дата звернення: 1.06.2024).

16. Proline 24u.URL: https://e-server.com.ua/servernye-shkafy/napolnye-shkafy/shkaf-servernyj-napolnyj-24u-600x800-detail (дата зверення: 6.06.2024).

17. Smart UPS On-line. URL: http://www.apc.com/shop/ua/ru/categories/power/ups/network-and-server/smart-ups-on-line/_/N-pgx5ae. (дата звернення: 23.05.2024).

18. Базові поняття мережевих технологій. URL: https://ami.lnu.edu.ua/wp-content/uploads/2018/01/Intranet1.pdf (дата звернення: 1.06.2024).

19. Безпека мережі. URL: https://uk.wikipedia.org/wiki/Безпека_мережі. (дата звернення: 4.06.2024).

20. Кабель категорії 6. URL: https://uk.wikipedia.org/wiki/%D0%92%D0%B8%D1%82%D0%B0_%D0%BF%D0%B0%D1%80%D0%B0/. (дата звернення: 1.06.2024).

ДОДАТКИ

Додаток А. Таблиця адресації вузлів локальної мережі

Таблиця А1 – Таблиця IP-адрес

Ім’я вузла	IP-адреса	Маска	Шлюз	DNS
1	2	3	4	5
S_1	192.168.113.252	/24	192.168.113.254	192.168.113.253
S_2	192.168.113.253	/24	93.77.230.254	93.77.230.253
	93.77.230.235	/24		
SW_1	192.168.1.1	/24	-	-
SW_2	192.168.1.2	/24	-	-
SW_3	192.168.1.3	/24	-	-
SW_4	192.168.1.4	/24	-	-
SW_5	192.168.1.5	/24	-	-
SW_6	192.168.1.6	/24	-	-
SW_7	192.168.1.7	/24	-	-
SW_8	192.168.1.8	/24	-	-
WS_1	192.168.101.1	/24	192.168.101.254	192.168.113.253
WS_2	192.168.101.2	/24	192.168.101.254	192.168.113.253
WS_3	192.168.101.3	/24	192.168.101.254	192.168.113.253
WS_4	192.168.101.4	/24	192.168.101.254	192.168.113.253
WS_5	192.168.101.5	/24	192.168.101.254	192.168.113.253
WS_6	192.168.101.6	/24	192.168.101.254	192.168.113.253
WS_7	192.168.101.7	/24	192.168.101.254	192.168.113.253
WS_8	192.168.102.1	/24	192.168.102.254	192.168.113.253
WS_9	192.168.102.2	/24	192.168.102.254	192.168.113.253
WS_10	192.168.102.3	/24	192.168.102.254	192.168.113.253

Продовження таблиці А1

1	2	3	4	5
WS_11	192.168.102.4	/24	192.168.102.254	192.168.113.253
WS_12	192.168.102.5	/24	192.168.102.254	192.168.113.253
WS_13	192.168.103.1	/24	192.168.103.254	192.168.113.253
WS_14	192.168.103.2	/24	192.168.103.254	192.168.113.253
WS_15	192.168.103.3	/24	192.168.103.254	192.168.113.253
WS_16	192.168.103.4	/24	192.168.103.254	192.168.113.253
WS_17	192.168.103.5	/24	192.168.103.254	192.168.113.253
WS_18	192.168.103.6	/24	192.168.103.254	192.168.113.253
WS_19	192.168.103.7	/24	192.168.103.254	192.168.113.253
WS_20	192.168.104.1	/24	192.168.104.254	192.168.113.253
WS_21	192.168.104.2	/24	192.168.104.254	192.168.113.253
WS_22	192.168.104.3	/24	192.168.104.254	192.168.113.253
WS_23	192.168.104.4	/24	192.168.104.254	192.168.113.253
WS_24	192.168.105.1	/24	192.168.105.254	192.168.113.253
WS_25	192.168.105.2	/24	192.168.105.254	192.168.113.253
WS_26	192.168.105.3	/24	192.168.105.254	192.168.113.253
WS_27	192.168.105.4	/24	192.168.105.254	192.168.113.253
WS_28	192.168.105.5	/24	192.168.105.254	192.168.113.253
WS_29	192.168.106.1	/24	192.168.106.254	192.168.113.253
WS_30	192.168.106.2	/24	192.168.106.254	192.168.113.253
WS_31	192.168.106.3	/24	192.168.106.254	192.168.113.253
WS_32	192.168.106.4	/24	192.168.106.254	192.168.113.253
WS_33	192.168.106.5	/24	192.168.106.254	192.168.113.253
WS_34	192.168.107.1	/24	192.168.107.254	192.168.113.253
WS_35	192.168.107.2	/24	192.168.107.254	192.168.113.253
WS_36	192.168.107.3	/24	192.168.107.254	192.168.113.253

Продовження таблиці А1

1	2	3	4	5
WS_37	192.168.107.4	/24	192.168.107.254	192.168.113.253
WS_38	192.168.107.5	/24	192.168.107.254	192.168.113.253
WS_39	192.168.107.6	/24	192.168.107.254	192.168.113.253
WS_40	192.168.107.7	/24	192.168.107.254	192.168.113.253
WS_41	192.168.108.1	/24	192.168.108.254	192.168.113.253
WS_42	192.168.108.2	/24	192.168.108.254	192.168.113.253
WS_43	192.168.109.1	/24	192.168.109.254	192.168.113.253
WS_44	192.168.109.2	/24	192.168.109.254	192.168.113.253
WS_45	192.168.110.1	/24	192.168.110.254	192.168.113.253
WS_46	192.168.110.2	/24	192.168.110.254	192.168.113.253
WS_47	192.168.111.1	/24	192.168.111.254	192.168.113.253
WS_48	192.168.111.2	/24	192.168.111.254	192.168.113.253
WS_49	192.168.112.1	/24	192.168.112.254	192.168.113.253

Додаток Б. Конфігураційний скрипт центрального комутатора

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname sw6
!
enable secret 5 $1$mERr$W0yB.XmVL7E61EqvjIL7e1
!
ip routing
!
username root secret 5 $1$mERr$W0yB.XmVL7E61EqvjIL7e1
!
spanning-tree mode pvst
!
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
```

```
!
interface GigabitEthernet0/4
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/5
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/6
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/7
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/8
switchport access vlan 108
switchport mode access
!
interface GigabitEthernet0/9
switchport access vlan 108
switchport mode access
!
interface GigabitEthernet0/10
switchport access vlan 109
switchport mode access
!
```

```
interface GigabitEthernet0/11
switchport access vlan 109
switchport mode access
!
interface GigabitEthernet0/12
switchport access vlan 110
switchport mode access
!
interface GigabitEthernet0/13
switchport access vlan 110
switchport mode access
!
interface GigabitEthernet0/14
switchport access vlan 111
switchport mode access
!
interface GigabitEthernet0/15
switchport access vlan 111
switchport mode access
!
interface GigabitEthernet0/16
switchport access vlan 112
switchport mode access
!
interface GigabitEthernet0/17
!
interface GigabitEthernet0/18
!
interface GigabitEthernet0/19
```

```
!
interface GigabitEthernet0/20
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
switchport access vlan 113
switchport mode access
!
interface GigabitEthernet0/24
switchport access vlan 113
switchport mode access
!
interface Vlan1
no ip address
shutdown
!
interface Vlan101
ip address 192.168.101.254 255.255.255.0
!
interface Vlan102
ip address 192.168.102.254 255.255.255.0
!
interface Vlan103
ip address 192.168.103.254 255.255.255.0
!
interface Vlan105
```

```
ip address 192.168.105.254 255.255.255.0
!
interface Vlan106
ip address 192.168.106.254 255.255.255.0
!
interface Vlan107
ip address 192.168.107.254 255.255.255.0
!
interface Vlan108
ip address 192.168.108.254 255.255.255.0
!
interface Vlan109
ip address 192.168.109.254 255.255.255.0
!
interface Vlan111
ip address 192.168.111.254 255.255.255.0
!
interface Vlan112
ip address 192.168.112.254 255.255.255.0
!
interface Vlan113
ip address 192.168.113.254 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
line con 0
login local
```

```
!
line aux 0
!
line vty 0
login
line vty 1 4
login local
line vty 5 15
login local
!
end
```

Додаток В. Логічна адресація вузлів локальної мережі

Таблиця В1 – Поділ на робочі групи

По-значення вузлів	Робоча група	Приміще ння*	Кабінет Назва або номер кабінету	Назва VLAN	Адреса підмережі	Маска підмере жі
1	2	3	4	5	6	7
WS_1-WS_7, SW_1	progr_vid1	Перший поверх	Відділ програмування №1	vlan101	192.168.101.0	/24
WS_8-WS_12, SW_2	testers_vid	Перший поверх	Відділ тестування	vlan102	192.168.102.0	/24
WS_13-WS_19, SW_3	buh_vid	Перший поверх	Розрахункова група, бухгалтерія	vlan103	192.168.103.0	/24
WS_20-WS_23, SW_4	dir_vid	Перший поверх	Директор, заступники	vlan104	192.168.104.0	/24
WS_24-WS_28, SW_5	seo_vid	Перший поверх	Відділ просування, SEO	vlan105	192.168.105.0	/24
WS_29-WS_33, SW_7	managers_ vid	Перший поверх	Менеджери	vlan106	192.168.106.0	/24
WS_34-WS_40, SW_8	progr_vid2	Перший поверх	Відділ програмування №2	vlan107	192.168.107.0	/24
WS_41-WS_42	it_vid	Перший поверх	IT-відділ	vlan108	192.168.108.0	/24
WS_43-WS_44	corp_vid	Перший поверх	Відділ корпоративних комунікацій	vlan109	192.168.109.0	/24
WS_45-WS_46	hr_vid	Перший поверх	Відділ підбору персоналу	vlan110	192.168.110.0	/24
WS_47-WS_48	jurid_vid	Перший поверх	Юридичний відділ	vlan111	192.168.111.0	/24
WS_49	adm_vid	Перший поверх	Адміністратор мережі	vlan112	192.168.112.0	/24
S1	servers	Перший поверх	Серверна	vlan113	192.168.113.0	/24
S2						

Таблиця В2 - Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Номер порту	Тип порту	Назва мережевого пристрою	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
1	WS_1-WS_7, SW_1	-	-	SW_1	1-7	Access	101
2	WS_8-WS_12, SW_2	-	-	SW_2	1-5	Access	102
3	WS_13-WS_19, SW_3	-	-	SW_3	1-7	Access	103
4	WS_20-WS_23, SW_4	-	-	SW_4	1-4	Access	104
5	WS_24-WS_28, SW_5	-	-	SW_5	1-5	Access	105
6	WS_29-WS_33, SW_7	-	-	SW_7	1-5	Access	106
7	WS_34-WS_40, SW_8	-	-	SW_8	1-7	Access	107
8	WS_41-WS_42	-	-	SW_6	1-3	Access	108
9	WS_43-WS_44	-	-	SW_6	4-5	Access	109
10	WS_45-WS_46	-	-	SW_6	6-7	Access	110
11	WS_47-WS_48			SW_6	8-9	Access	111
12	WS_49			SW_6	10	Access	112
13	SW_1	8	Trunk	SW_6	11	Trunk	-
14	SW_2	8	Trunk	SW_6	12	Trunk	-
15	SW_3	8	Trunk	SW_6	13	Trunk	-
16	SW_4	8	Trunk	SW_6	14	Trunk	-
17	SW_5	8	Trunk	SW_6	15	Trunk	-
18	SW_7	8	Trunk	SW_6	17	Trunk	-
19	SW_8	8	Trunk	SW_6	18	Trunk	-

Додаток Г. Порівняльні характеристики обладнання

Таблиця Г1 - Порівняльна характеристика центральних комутаторів

Виробник	Cisco	NetGear	Juniper
Модель	WS-C3750G-24T-S	M4300-28G	EX2200
К-сть портів 1000 Мбіт/с	24	24	24
К-сть додаткових портів	4 SFP	4 SFP	4 SFP
Слот розширення 10GE	-	+	+
Підтримка QoS	+	+	+
Підтримка функцій ACL	+	+	+
Статична маршрутизація	+	+	+
Моніторинг трафіку	+	+	+
Робота в стеку	+	+	+
Керування (telnet, ssh, web)	+	+	+

Таблиця Г2 - Порівняння характеристик комутаторів робочої групи

Технічні характеристики/ модель комутатора	Allied Telesyn AT-GS950/16	TP-LINK TL-SG2216	Huawei S1700-16
Швидкість комутаційної шини, Гб/с	32	32	32
Підтримка технологій FastEthernet/Gigabit Ethernet	+	+	+
К-сть портів 10/100/1000	16	16	16
Віддалене керування	Так	Так	Так
Підтримка VLAN	Так	Так	Так

Таблиця Г3 - Порівняльна характеристика 8-ми портових комутаторів

Параметр/Модель	HP 1810-8v2	Cisco SB SRW2008MP	Allied Telesyn AT-GS950/8
К-сть портів основних	8	8	8
К-сть портів SFP	-	2	2
Функції моделі OSI	2	2	2
Пропускна здатність, Гбіт/с	16	16	16
Швидкість пересилки пакетів (64байти), млн. пак./с	11,9	11,9	11,9
Функції керування	HTTP, HTTPS	HTTP, HTTPS, RMON, SNMP, Telnet, TFTP	HTTP, HTTPS, RMON, SNMP, Telnet, TFTP
Функції автовизначення портів	+	+	+
Підтримка IEEE 802.1q	+	+	+

Таблиця Г4 - Порівняльна характеристика апаратних платформ серверів

	ARTLINE Business R25	Dell PowerEdge T40
1	2	3
Процесор	Intel Xeon E3-1220	Intel Xeon E-2224G
Пам’ять	16ГБ (DDR4-2400)	16ГБ (DDR4-2400)
ЖМД	HDD: 2 x 2 ТБ SSD: 2 x 512 ГБ	HDD: 2 x 2 ТБ SSD: 2 x 512 ГБ

Продовження таблиці Г4

1	2	3
RAID-контролер	Intel Rapid Storage	Intel Rapid Storage
Висота	2U	2U
Мережевий адаптер	2 x 1000Мбіт/с (інтегрований)	2 x 1000Мбіт/с (інтегрований)
БЖ	650Вт	650Вт
Відеоадаптер	інтегрований	інтегрований

Додаток Д. Інформаційні і конфігураційні команди та утиліти

Інформація про диски:

1. mount - показує змонтовані підрозділи і прапори з монтування.

2. df - показує змонтовані підрозділи, їх розмір і вільне місце на них.

3. fdisk /dev/ad0 - показує інформацію про диск ad0 і розділах на ньому.

4. disklabel /dev/ad0s1 - показує список підрозділів в першому розділі диска ad0.

5. swapinfo - показує список підрозділів свопінгу на дисках і їх використання.

6. fstat - показує список відкритих файлів (імена файлів не виводяться).

7. pstat-f - показує список відкритих файлів (імена файлів не виводяться).

8. systat-vmstat n - кожні n секунд виводить кількість транзакцій з диском в секунду, обсяг записаних/зчитаних даних на диск в секунду, середній розмір транзакції і відсоток часу протягом якого диск був зайнятий роботою.

9. iostat - виводить інформацію, аналогічну systat-vmstat, але не виводить зайнятості диска за часом і може виводити середню статистику з моменту завантаження.

10. vmstat - виводить кількість операцій на диску в секунду.

11. Stand/sysinstall - можна подивитися і змінити розмітку диска і монтування.

12. less /etc/fstab - таблиця монтування при завантаженні.

Інформація про процесор і пам'ять:

1. systat -vmstat n - вивід показників завантаження (number of jobs in the run queue averaged over 1, 5 and 15 min), стану пам'яті (в сторінках), кількості процесів в групах, кількість викликів спеціальних функцій ядра (traps, interrupts, system calls, network software interrupts), використання процесора, трансляції імен, активність свопу, переривання, а також інформацію щодо використання диска.

2. top - аналогічна інформація в скороченому вигляді, використання пам'яті та свопу в мегабайтах, список процесів, відсортованих по використанню процесора.

3. ps afx - список запущених процесів і час процесора на кожний процес.

Інформація про мережу:

1. ifconfig - список мережевих інтерфейсів з ip-адресами, масками, mac-адресами, типами карт і їх статусами (назви мережевих плат можна подивитися у файлі конфігурації ядра).

2. systat -ifstat n - об'єм трафіку за n секунд на усіх мережевих інтерфейсах.

3. netstat - вивід активних мережевих з'єднань (сокетів).

4. systat -netstat n - аналог netstat в реальному часі.

5. netstat-ibt - список інтерфейсів, розбитих по ip-адресах з обсягом трафіку на кожному, кількістю помилок, колізій, значенням watchdog-таймера.

6. netstat -r - таблиця маршрутизації.

7. arp -a - таблиця ARP.

8. tcpdump -i rl0 host 192.168.61.20 and port 80 - сніффер пакетів на інтерфейсі rl0, фільтруючий пакети, що містять адресу 192.168.61.20 та порт 80.

9. trafshow-i rl0 - програма для сортування і виведення мережевих потоків (встановлюється додатково пакетом або з портів)