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 "СІП"

Виконав: студент VI курсу, групи КІб-602

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

_____ Микола ДАНИЛЬЦІВ
(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

Данильціву Миколі Ярославовичу
(прізвище, ім'я, по батькові)

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

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 _____ Микола ДАНИЛЬЦІВ
(підпис) (ім'я та прізвище)

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

АНОТАЦІЯ

Данильців М.Я. Розробка проєкту комп’ютерної мережі компанії «СІП»: кваліфікаційна робота на здобуття освітнього ступеня бакалавр, за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2024. 85с.

Комп’ютерна мережа побудована з використанням стандарту Gigabit Ethernet. При проектуванні мережі акцент робився на реалізації наступних показників: захищеність інформації, що передається по каналах зв’язку та надійність передачі даних; необхідний рівень продуктивності з запасом пропускної здатності; вартість проектування та експлуатації не більше від вимог замовника; масштабованість та наявність засобів моніторингу

В процесі проектування реалізовано моделювання роботи мережевої інфраструктури.

Ключові слова: комп’ютерна мережа, VLAN, Linux CentOS, NAT.

ANNOTATION

DANYLTSIV MYKOLA. Computer Network Project Development of «SIP» 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. 85p.

The computer network was built using the Gigabit Ethernet standard. When designing the network, the emphasis was placed on the following indicators: security of information transmitted through communication channels and reliability of data transmission; required level of performance with a margin of bandwidth; cost of design and operation no more than the customer's requirements; scalability and availability of monitoring tools.

In the process of designing, the modeling of the network infrastructure was implemented.

Keywords: computer network, VLAN, Linux CentOS, NAT.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

802.3ae - 10 GbE;

DNS (Domain Name System) - сервер доменних імен;

EIA (Electronic Industries Association) – асоціація електронної промисловості;

IEEE 802.3 - 10BASE-T Ethernet;

IEEE 802.3ab - 1000BASE-T Gigabit Ethernet;

IEEE 802.3u - 100BASE-TX Fast Ethernet;

IP (Internet Protocol) – Інтернет-протокол;

LAN (Local Area Network) – локальна мережа;

MAC (Media Access Control) - апаратна адреса ПК;

NAT (Network Address Translation) – мережева трансляція адес;

OSI (Open System Interface) – модель з'єднання відкритих систем;

QoS – технологія пріоретизації пакетів, що проходять через мережене обладнання;

SNMP (Simple Network Management Protocol) – протокол керування мережею;

Spanning Tree Protocol – алгоритм покриваючого дерева, використовується для прокладання резервних зв'язків між вузлами;

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

UTP (Unshielded Twisted Pair) – кабель типу неекранована скручена пара;

ОС - операційна система;

ПК - персональний комп'ютер.

ВСТУП

Комп’ютерні мережі є невід’ємною частиною будь-якого сучасного бізнесу. Складно уявити собі діяльність компанії чи організації без використання сучасних сервісів у виробничій діяльності. Технології комунікації та сервіси є складовою частиною виробничого процесу. Правильне проектування та впровадження їх у виробничу діяльність є основною для побудови бізнес процесів, дозволить заощадити кошти при модернізації, та розширені бізнесу [1].

За даними організації IEEE близько 90 відсотків всіх локальних мереж спроектовано з використанням стандартів сімейства Ethernet [2]. Використання вище описаних технологій для побудови локальної мережі підприємства чи установи дозволить отримати досить швидку в роботі мережу, зекономити кошти на придбанні мережевого обладнання, оскільки можна паралельно використовувати старе (технологія забезпечує сумісність зверху вниз), відносна простота в експлуатації.

Саме за допомогою локальних мереж можливо з найменшими зусиллями організувати роботу великої кількості комп'ютерів, вести централізоване управління, забезпечити надійну інформаційну безпеку, і антивірусний захист.

У кваліфікаційній роботі розглянуто метод організації локально-обчислювальної мережі в виробничій діяльності компанії «СІП». Впровадження необхідних мережевих ресурсів локальної мережі дозволить об’єднати окремі ПК в єдину інформаційну структуру та підвищити продуктивність роботи працівників.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

В даному підпункті роботи буде проведено аналіз вхідних вимог та розглянуто технічне завдання на проектування. Отже, детальніше:

1.1.1 Найменування та область застосування

Кваліфікаційної роботи на тему: «Розробка проєкту комп'ютерної мережі компанії «СІП». Компація «СІП» - це стиль, інженерія та проектування, тобто її діяльність пов'язаана насамперед з інженерними задачами в галузі проектування, а також аналітики, статистики та обробки даних.

Комунікаційні вимоги, що висуваються до проекту є:

1. Надати можливість спільної роботи всім ПК, що входять до різних відділів, груп та забезпечити можливість обміну трафіком між ними, звісно й всередині відділв.

2. Поділ мережі на під мережі з подальшою логічною ізоляцією трафіку, що знаходиться в межах цієї підмережі.

3. Можливість використання оргтехніки підключеної до локальної мережі групою користувачів.

4. Спільне використання підключень до мережі Інтернет.

5. Використання служб та сервісів як локланої, так і глобальної мережі Інтернет.

6. Наявність безпровідного сегменту мережі та його захищеність.

7. Підключення до ЛОМ всіх наявних пристроїв.

8. Моніторинг (метрики, файли логування).

1.1.2 Призначення розробки

Втілений на практиці проєкт, який описано в кваліфікаційній роботі спрямований на реалізацію таких можливостей:

1. Надасть можливість співробітникам корпоративного бездротового зв'язку використовувати мобільні пристрої та конектитись до ресурсів ЛОМ.

2. Можливість об'єднання наявної комп'ютерної техніки в єдину інформаційну мережу.

3. Забезпечити робочі станції можливістю спільного доступу до послуг мережі Інтернет.

4. Захист усіх хостів мережі, налаштувавши централізовані фільтри пакетів.

5. Зменшити час обробки інформації.

6. Зростання ефективності та продуктивності праці.

7. Присутність засобів зв'язку.

8. Впровадження збору даних і моніторинг.

1.1.3 Вимоги до апаратного та програмного забезпечення

З метою виконання цього завдання необхідно розробити вимоги до апаратного та програмного забезпечення.

Оскільки в мережі передбачено використання віртуальних підмереж то головний комутатор працюватиме згідно моделі OSI на третьому рівні. Обов’язкова підтримка списків доступу, статичної маршрутизації, віртуальних мережу та інші функції. Реальна швидкість портів комутатора має бути 1000 Мбіт/с. Всього має бути 24 порти і вони повинні підтримувати технологію віртуальної мережі. Комутатори для робочих груп можуть бути 8-портовими та 16-портовими, підтримувати стандарти Gigabit Ethernet і технології віртуальної мережі.

Бездротові маршрутизатори будуть вибрані відповідно до стандарту IEEE 802.11ac, мати швидкість передачі даних на цьому рівні та використовувати протокол WPA2-PSK для шифрування даних.

Сервери доступу до Інтернету та файлові сервери повинні мати високу швидкість передачі даних, якої буде достатню для виконання інших функцій.

Програмне забезпечення робочої станції повинно підтримувати програмну реалізацію стека протоколів TCP/IP. З метою здешевлення проектованої локальної мережі все ПЗ передбачається базувати на операційній системі Linux, якає є вільнопоширюваною.

1.1.4 Вимоги до документації

Завершена комп'ютерна мережа завжди повинна мати добре оформлену технічну документацію, згідно технічних стандартів. Правильно оформлена документація та її повнота сприятимуть своєчасному виконанню робіт з обслуговування локальної мережі. Отже технічна документація на ЛОМ має містити: план приміщення, логічна топологія, схема зв'язку між вузлами, внесена згідно масштабу на план приміщень (фізична топологія), інструкція з налаштування серверних сервісів.

1.1.5 Техніко-економічні показники

Зформуємо базовий перелік техніко-економічних показників:

1. Фізична топологія проектовааної мережі – Розширена зірка.
2. Стандарт побудови безпровідної частини мережі – IEEE 802.11ac.
3. К-сть точок підключення (к-сть мережевих розеток) – 45.
4. Стандарт побудови локальної мережі – IEEE 802.3ab Gigabit Ethernet.
5. Програмне забезпечення серверів використовує OpenSource на базі ОС Linux.
6. Центральний комутатор – L3, серія Cisco Catalyst.

7. Передбачувана трудомісткість інсталяції мережі - 200 люд/год.
8. Верхня межа вартості мережі – до 400 тисяч гривень

1.1.6 Стадії та етапи розробки

Загалом процес проектування локальної комп'ютерної мережі складається з певних, логічно завершених, етапів. Отже необхідно:

1. Розробити технічне завдання для проекту ЛОМ.
2. Узгодити технічні завдання з керівництвом компанії «СІП».
3. Етап планування послідовності реалізації локальної мережі.
4. Аналіз, вибір і проектувнаня логічної топології комп'ютерної мережі.
5. Проектування фізичної топології комп'ютерної мережі.
6. Аналіз і підбір необхідного активне та пасивне обладнання.
7. Укладання кабелю в кабельні канали.
8. Встановлення мережевих розеток та обжим роз’ємів.
9. Монтаж розподільної шафи та підключення комунікаційного обладнання в ній.
10. Конфігурація центрального комутатора.
11. Конфігурація комутаторів робочої групи.
12. Встановлення серверної операційної системи.
13. Налаштуйте служби сервера.
14. Процедура тестування та налагодження діючої мережі.
15. Оформлення технічної документації.
16. Здача в експлуатацію

1.1.7 Порядок контролю та прийому

Важливим етапом є контроль технічних показників локальної мережі, що спроектована. Для цього будуть використовуватись такі засоби:

1. Кабельний тестер, для тестування фізичних характеристик локальної мережі.

2. Програмні засоби тестування: утиліти операційної системи Linux, спеціалізоване програмне забезпечення.

3. Дані з системи моніторингу Prometheus, Grafana.

1.2 Опис задачі та характеристика компанії

Темою кваліфікаційної роботи є розробка проєкту комп'ютерної мережі для компанії «СІП». Абревіатура СІП, закладена в назву компанії це Статистика-Інженерія-Проектування.

Проектована мережа, як і будь яка інша ЛОМ, повинна об'єднати наявний парк комп'ютерів в єдиний інфопростір та забезпечити можливість обміну інформацією. Важливо надати всім робочим хостам спільний доступ до ресурсів ЛОМ та Інтернету. Окрім цього проєкт локальної мережі буде проектуватися з врахуванням технічної та економічної доцільності. В подальшому, в розділі 2.3 наведено таблиці активного та пасивного обладнання для мережі, а в розділі 2.4 детально описано програмне забезпечення, яке необхідне для нашого проекту.

Компанія займається збором інформації та побудовою аналітичних звітів. Структура компанії побудована в процесі розвитку компанії, є ефективною і налічує такі відділи (підрозділи):

1. Адміністрація.
2. Бухгалтерія.
3. Архів-склад.
4. Відділ обробки даних.
5. Відділ збору даних.
6. Технічний відділ.
7. Серверна.
8. Аналітично-розрахунковий відділ.
9. Відділ проектування.

10. Відділ технологів

11. Відділ впровадження.

12. Менеджери для роботи з клієнтами.

План компанії з розміщенням відповідних приміщень приведено на кресленні «План приміщення».

2. РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

Локальна мережа має багато переваг для бізнесу та іншої діяльності:

- Автоматизація виробничої діяльності.
- Спільне обладнання.
- Можливість використання локальних і глобальних мережевих сервісів.

Комп’ютерна мережа передбачає використання двох компонентів: апаратного та програмного забезпечення. Усі елементи, які дозволяють побудувати весь процес передачі/прийому даних, побудовані у вигляді семирівневої моделі OSI. Кожен такий елемент виконує певну функцію, описану моделлю.

Усі LOM працюють відповідно до одного стандарту, який використовується комп’ютерними мережами – стандарту Open Systems Interconnection (OSI). Розвиток комп'ютерних мереж є багатоетапним процесом. Його можна описати за допомогою семирівневої моделі OSI, як показано на малюнку 2.1.

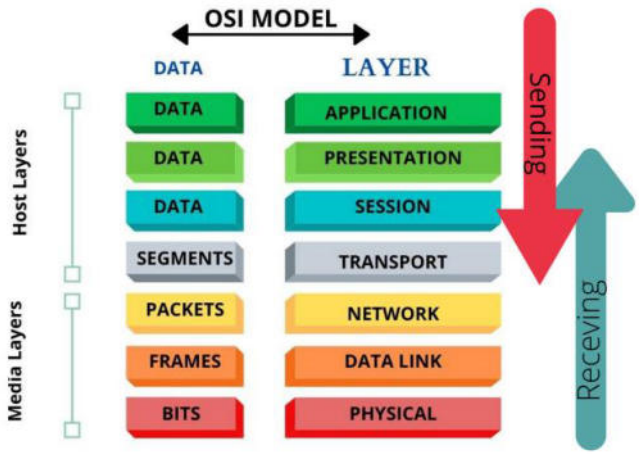

Рисунок 2.1 – Модель OSI, тобто взаємодії відкритих систем

На фізичному рівні моделі відбувається фізична передача сигналів по каналах зв’язку. Тут є важливим правильний вибір кабельної системи у відповідності до вибраного стандарту побудови [2].

На канальному рівні моделі OSI робота відбувається з MAC-адресами. На цьому рівні працюють мережеві плати, комутатори ітд. Для локальної мережі буде підібрано комутаційне програмне забезпечення відповідно до вибраного стандарту локальної мережі.

На мережевому рівні працюють маршрутизатори. Для локальної мережі буде вибрано комутатор 3-го рівня, який виконуватиме функції маршрутизації трафіку.

На транспортному рівні моделі OSI працюють протоколи TCP/UDP. Вони будуть забезпечувати транспорт для даних.

Сесійний, презентаційний та прикладний рівні відносять до програмного забезпечення, яке представлено операційною системою, серверами та службами.

Як було сказано вище, локальна мережа буде поділена на окремі логічні групи, які відображатимуть адміністративну структуру компанії. Ці часини мають назву віртуальні мережі. Це буде здійснено засобами комутатора третього рівня моделі OSI. В таблиці «Логічна адресація в ЛОМ» додатку Б містяться дані про такі віртуальні мережі.

Додатково в таблиці «Таблиця конфігурування VLAN» додатку Б знаходяться дані про типи портів комутаторів.

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з’єднань та їх прокладка

Базисом вдалого проектування будь-якої комп'ютерної мережі є правильний вибір фізичної топології. Кожна топологія має свої переваги та недоліки. Враховуючи їх відповідні переваги та недоліки, необхідно вибрати

найкращий варіант фізичної топології. Оскільки очікується, що мережа використовуватиме дротові та бездротові пристрої, буде вибрано змішану фізичну топологію.

Серед переваг:

- Вся мережа не залежить від роботи конкретної робочої станції.

- Коли один із комутаторів робочої групи виходить з ладу, лише один сегмент від'єднується від мережі. Загалом мережа продовжить працювати [6].

До недоліків можна віднести припинення роботи локальної мережі при виході з ладу центрального комутаційного обладнання. Логічна топологія така, як показано на відповідному плакаті.

2.2.2 Будова вузлів та необхідність їх застосування

Комутаційний вузол локальної мережі буде включати такі складові:

1. Центральний комутатор.
2. Патч-панель.
3. ББЖ.
4. Сервер.

На рисунку 2.2 зображено приклад організації кабельної системи ЛОМ.

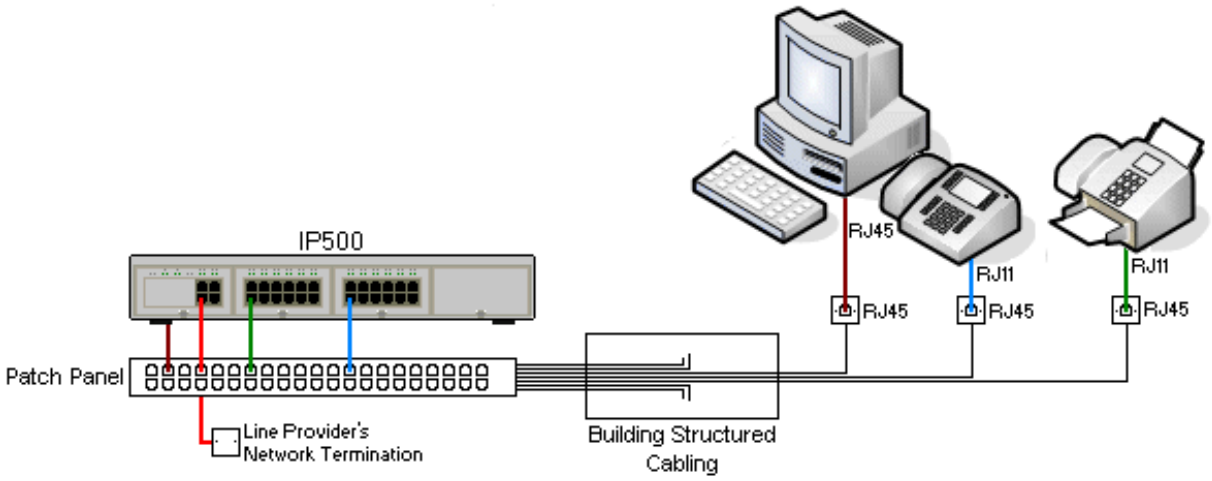

Рисунок 2.2 – Кабельна система ЛОМ

Кабельна система локальної мережі побудована з використанням неекранованої витої пари категорії 6.

2.3 Обґрунтування вибору комунікаційного обладнання

Пасивне обладнання ЛОМ:

1. Мережеві розетки.
2. Патч-панель.
3. Комутаційна шафа.

Активне мережеве обладнання:

1. Комутатори робочих груп.
2. Головний комутатор.
3. Сервери.
4. Маршрутизатори з безпровідним інтерфейсом.

Порівняльна характеристика комутаторів третього рівня моделі OSI, що можуть бути застосовані в якості центрального комутаційного вузла з можливістю поділу мережі на підмережі, маршрутизації трафіку, фільтрування трафіку на основі списків доступу приведена в таблиці «Порівняльна характеристика комутаторів 3-го рівня OSI» додатку В.

Для локальної мережі буде використано комутатор WS-C3750G (24 порти) компанії Cisco.

В таблиці «Порівняльна характеристика апаратних платформ серверів» додатку В наведено порівняння серверів, які будуть використані в якості проксі-сервера та файлового сервера. Апаратна платформа на базі HP ProLiant ML30 Gen10. Вибраний сервер HP ProLiant ML30 відображено на рисунку 2.3.

Рисунок 2.3 – Внутрішня будова серверу HP ProLiant ML30 Gen10

Для проксі-сервера вибрано аналогічну платформу з невеликими змінами. Дисковий накопичувач буде 500ГБ, на відміну від файлового сервера, для яйого буде використано 1ГБ.

В якості комутуючого пристрою відділу буде використано комутатор D-Link DGS-1216T, який має 16 портів, що підтримують швидкість передачі 1Гбіт/с. Технічні особливості D-link DGS-1216T наведено у додатку Г, сам комутатор зображено на рисунку 2.4.

Рисунок 2.4 – Зовнішній вид комутатора D-link DGS-1216T

Для невеликих робочих груп буде використано восьмипортову модель комутатора серії D-link DGS-1210.

Для побудови безпровідної частини ЛОМ планується використання безпровідного маршрутизатора TP-LINK Archer C7 AC1750. Технічні характеристики TP-LINK Archer C7 AC1750 наведено у додатку Д.

Наведено перелік обладнання, яке планується використати для побудови мережі:

1. Кабель UTP 6 (бухта 305м) - 2 шт.
2. Серверна шафа 24U - 1 шт.
3. Середня патч-панель 24 порти - 1 шт.
4. Короби, різні - 130 м.
5. Патчкорд - 65 шт.
6. Мережева розетка – 43 шт.
7. Фільтр-подовжувач (3м) – 4 шт.
8. Кабельні тримачі – 2 шт.
9. Комутатор DGS-1216T - 3 шт.
10. Комутатор Cisco WS-C3750G – 1 шт.
11. Сервера HP ProLiant ML30 - 2 шт.
12. Комутатор DGS-1210-08 - 2 шт.
13. Безпровідний маршрутизатора TP-LINK Archer C7 AC1750 – 2 шт.

2.4 Особливості монтажу мережі

Під час інсталяції кабелю вадливо уникнути розтягування кабелю, тобто сила натягу не може досягати критичних 110 Н для 4-парного кабелю 24 AWG (0,5 мм). Тут наведено лише загальну рекомендацію щодо максимальної сили натягу для 4 пар кабелів. На практиці слід дотримуватися максимальних меж натягу, визначених виробником конкретного типу кабелю [5].

Радіус вигину встановленого кабелю не повинен бути менше 4-кратного зовнішнього діаметра кабелю при монтажі горизонтальних кабелів DTP і 10-кратного зовнішнього діаметра кабелю для багатопарних магістралей UTP. Необхідно, щоб радіус вигину кабелю був невеликим, тому що при значних

вигинах пари проводів всередині кабелю будуть деформуватися і порушувати збалансовану і симетричну рівномірність середовища передачі. Це в основному призводить до серйозного погіршення параметрів, таких як NEXT. Подальше випрямлення вигину не тільки не відновить форму, але й погіршить її. Забороняється прокладати кабелі в каналах, шафах, коробах та інших монтажних пристроях, радіус закруглення або крайка яких не відповідає вимогам виробника кабелю щодо радіуса вигину [5].

Запобіжні заходи, яких слід дотримуватися під час монтажу та організації кабельних потоків, включають захист від різноманітних механічних навантажень у кабелях, викликаних силами витягування, різкими вигинами та надмірним натягом пучків кабелів.

Слід уникати негативного впливу на кабель, спричиненого наступними факторами: скручування кабелю під час протягування або інсталяції, розтягування пучка кабелю через власну вагу на підвісці кабелю, занадто тугі затискачі кабелю та різкий згин кабелю та інші фактори.

2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій в мережі

Для зменшення собівартості проекту локальної мережі буде використано операційну систему та прикладне програмне забезпечення на базі операційної системи Linux (Debian Linux 12). Ця операційна система оптимально підходить для серверів, так як для неї, написано значну кількість програмного забезпечення (серверного і додатків).

Для робочих станцій буде використано ОС Ubuntu Linux 24.04 Desktop Edition.

2.6 Обґрунтування вибору засобів захисту мережі

Захист локальної мережі передбачає використання програмного файрволу, антивірусу. В якості файрволу для ОС Linux буде використано популярний файрвол iptables. Даний файрвол дозволяє фільтрувати дані на рівні 2, 3, 4 моделі OSI. В якості антивірусу буде використано популярний продукт ClamAV.

2.7 Тестування мережі

Тестування локальної мережі – це процес перевірки функціональності, продуктивності та безпеки ЛОМ, яка об'єднує комп'ютери та інші пристрої.

Мета тестування локальної мережі полягає в тому, щоб забезпечити її стабільну та ефективну роботу. Для цього фахівці використовують різні інструменти та методи, щоб перевірити такі аспекти:

- Пропускна здатність. Вимірювання швидкості передачі даних між пристроями в мережі, щоб впевнитися, що вона відповідає вимогам користувачів.
- Затримка та джиттер. Визначення затримок у передачі даних та їх варіацій, що важливо для додатків в реальному часі.
- Втрати пакетів. Перевірка того, чи втрачаються дані при передачі через мережу, що може впливати на якість зв'язку та передачі даних.
- Безпека. Оцінка захищеності мережі від несанкціонованого доступу та потенційних загроз, таких як зломи або віруси.
- Сумісність. Перевірка, чи всі пристрої в мережі можуть взаємодіяти один з одним без проблем.

Тестування локальної мережі допомагає виявити потенційні проблеми та вузькі місця, що дозволяє адміністраторам мережі вчасно їх виправити та оптимізувати роботу мережі. Це важливо для забезпечення стабільної роботи всіх підключених до мережі пристроїв та для задоволення потреб користувачів..

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування програмного забезпечення серверів

В другому розділі кваліфікаційної роботи було проаналізовано, обгрунтовано та вибрано апаратні платформи серверів, а також серверних ОС. Далі розробимо і опишемо інструкції з налаштування сервісів і служб на серверах

3.1.1 Інструкції з налаштування проксі-сервера

Використання проксі-сервера Squid для доступу до Інтернету в компанії має декілька важливих переваг:

- Контроль доступу. Squid дозволяє адміністраторам контролювати, які сайти можуть відвідувати співробітники, і встановлювати правила доступу до Інтернету. Це може включати блокування небажаних або небезпечних веб-сайтів, обмеження доступу до певних ресурсів у робочий час тощо.
- Кешування. Squid може кешувати вміст веб-сайтів, що часто відвідуються, що зменшує навантаження на Інтернет-канал і прискорює доступ до цих ресурсів. Це також дозволяє економити пропускну здатність мережі, оскільки повторні запити до тих самих ресурсів будуть оброблятися швидше.
- Безпека. Використання проксі-сервера Squid допомагає підвищити рівень безпеки мережі, оскільки всі запити проходять через проксі, де вони можуть бути перевірені на наявність шкідливих програм і загроз. Це дозволяє запобігти доступу до шкідливих сайтів і знижує ризик зараження мережі вірусами.
- Моніторинг та аудит. Squid забезпечує можливість моніторингу та запису всіх запитів до Інтернету, що дозволяє адміністраторам відстежувати

активність користувачів у мережі. Це може бути корисно для виявлення проблем або порушень політики безпеки.

- Економія трафіку. За допомогою Squid можна встановлювати обмеження на використання Інтернет-трафіку, наприклад, забороняти завантаження великих файлів або обмежувати використання певних видів контенту, таких як відео або аудіо. Це допомагає знизити витрати на Інтернет-з'єднання.

Використання Squid як проксі-сервера дозволяє компанії ефективніше управляти доступом до Інтернету, забезпечувати безпеку мережі, оптимізувати використання ресурсів і забезпечувати дотримання політики безпеки та користування Інтернетом. На рисунку 3.1 наведено загальну схему проксі-сервера squid та його структуру.

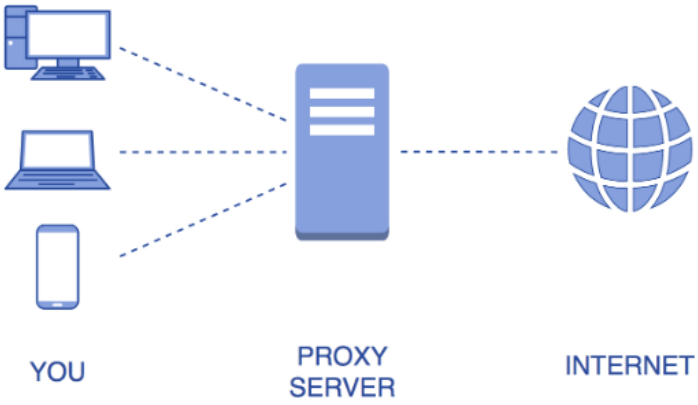

Рисунок 3.1 – Загальна схема роботи проксі-сервера

В додатку Е наведено детальні інструкції з налаштування проксі-сервера squid для задач спільного використання одного підключення до мережі Інтернет.

3.1.2 Інструкції з налаштування служби DHCP

Налаштування DHCP сервера на операційній системі Debian передбачає декілька ключових етапів, починаючи з установки необхідного програмного забезпечення і закінчуючи налаштуванням конфігураційних файлів для визначення параметрів мережі.

Спочатку необхідно оновити списки пакетів, щоб система мала актуальну інформацію про доступне програмне забезпечення. Це досягається командою sudo apt update. Після цього можна приступати до встановлення пакета isc-dhcp-server, який є популярним DHCP сервером для Linux. Це робиться за допомогою команди sudo apt install isc-dhcp-server.

Після встановлення DHCP сервера потрібно налаштувати його відповідно до потреб мережі. Основний конфігураційний файл розташований за адресою /etc/dhcp/dhcpd.conf. Відкривши цей файл для редагування, необхідно вказати параметри за замовчуванням для оренди IP-адрес, такі як default-lease-time і max-lease-time. Далі потрібно визначити мережеві параметри, такі як підмережа (subnet), діапазон IP-адрес, які будуть видаватися (range), шлюз за замовчуванням (option routers), маска підмережі (option subnet-mask), DNS-сервери (option domain-name-servers) і доменне ім'я (option domain-name). Наприклад, для мережі з IP-адресами 192.168.1.0/24, де шлюз має IP-адресу 192.168.1.1, а DNS-сервери - 8.8.8.8 і 8.8.4.4, конфігурація може виглядати так:

```
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.10 192.168.1.100;
    option routers 192.168.1.1;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
    option domain-name "example.com";
```

Аналогічним чином налаштовуємо конфігурацію для інших підмереж.

Наступним кроком є налаштування інтерфейсу, через який DHCP сервер буде роздавати IP-адреси. Це робиться у файлі /etc/default/isc-dhcp-server, де параметр INTERFACESv4 повинен містити назву відповідного мережевого інтерфейсу, наприклад, eth0.

Після внесення всіх необхідних змін у конфігураційні файли, сервер потрібно перезапустити командою sudo systemctl restart isc-dhcp-server, щоб застосувати нові налаштування. Переконатися, що сервер працює коректно, можна за допомогою команди sudo systemctl status isc-dhcp-server, яка покаже поточний стан сервісу.

Нарешті, для перевірки працездатності налаштованого DHCP сервера необхідно підключити клієнтський пристрій до мережі та переконатися, що він отримує IP-адресу автоматично. Додатково можна переглянути логи DHCP сервера командою sudo journalctl -u isc-dhcp-server, щоб переконатися у відсутності помилок або інших проблем.

Таким чином, налаштування DHCP сервера на Debian дозволяє автоматично роздавати IP-адреси пристроям у локальній мережі, забезпечуючи зручне та ефективне керування мережевими ресурсами.

3.1.3 Інструкції з налаштування файлового сервера

Налаштування Samba на операційній системі Debian дозволяє створити мережевий ресурс для спільного доступу до файлів між пристроями з різними операційними системами. Ось детальна інструкція по налаштуванню Samba на Debian.

Перше, що потрібно зробити, це встановити пакет samba, який включає всі необхідні утиліти та сервіси. Для цього слід оновити списки пакетів командою:
sudo apt update

Потім встановити пакет samba:

sudo apt install samba

Основний конфігураційний файл Samba знаходиться за адресою /etc/samba/smb.conf. sudo nano /etc/samba/smb.conf

У конфігураційному файлі Samba необхідно налаштувати загальні ресурси (мережеві диски), які будуть доступні користувачам. Наприклад, для створення загального ресурсу "docs", який розташований у директорії /srv/samba/shared, додаємо наступні рядки в кінці файлу smb.conf:

```
[docs]
  path = /srv/samba/docs
  browsable = yes
  writable = yes
  guest ok = yes
  read only = no
```

Ці налаштування визначають шлях до ресурсу, роблять його видимим у мережі, дозволяють записувати файли, дозволяють доступ без пароля (для гостьового доступу), та знімають обмеження на лише читання.

Розглянемо створення директорії для спільного доступу. Для цього необхідно створити директорію, яка буде використовуватися для загального доступу, і встановити відповідні права доступу. Для цього виконуємо наступні команди:

```
sudo mkdir -p /srv/samb/docs
sudo chown -R nobody:nogroup /srv/samba/docs
sudo chmod -R 0775 /srv/samba/docs
```

Для додавання користувачів, які матимуть доступ до ресурсів Samba, необхідно створити користувача в системі та додати його до бази користувачів Samba:

```
sudo useradd -M -s /sbin/nologin smbuser
sudo smbpasswd -a smbuser
```

Вводимо пароль для нового користувача Samba, та перезавантажуємо сервіс Samba.

Якщо на сервері увімкнений фаєрвол, необхідно дозволити доступ до портів, які використовує Samba. Виконуємо наступні команди для налаштування фаєрволу:

sudo ufw allow 'Samba'

В додатку Є наведено детальну інструкцію з налаштування файлового сервера.

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкції з налаштування головного комутатора

Налаштування створення віртуальних підмереж (VLAN) на комутаторі третього рівня Cisco включає кілька ключових етапів. Спочатку адміністратор має отримати доступ до комутатора через консоль або SSH. Після підключення до комутатора, він переходить у режим привілейованого користувача (enable mode) за допомогою команди:

Switch> enable

Адміністратор входить у режим глобальної конфігурації за допомогою команди:

Switch# configure terminal

Щоб створити VLAN, адміністратор вводить команду:

Switch(config)# vlan <VLAN_ID>

Switch(config-vlan)# name <VLAN_NAME>

Switch(config-vlan)# exit

Адміністратор повторює ці кроки для кожного VLAN, який він хоче створити. Наприклад, для створення VLAN 10 з назвою "Sales":

Switch(config)# vlan 10

```
Switch(config-vlan)# name Sales
Switch(config-vlan)# exit
```

Адміністратор призначає порти комутатора VLAN. Наприклад, щоб призначити порти Ethernet0/1 і Ethernet0/2 до VLAN 10:

```
Switch(config)# interface range Ethernet0/1-2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit
```

Розглянемо налаштування SVI (Switch Virtual Interface). Для маршрутизації між VLAN на комутаторі третього рівня, адміністратор налаштовує віртуальні інтерфейси (SVI). Для кожного VLAN створюється відповідний інтерфейс:

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.10.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Адміністратор повторює цей крок для кожного VLAN, використовуючи відповідні IP-адреси. Наприклад, для VLAN 20:

```
Switch(config)# interface vlan 20
Switch(config-if)# ip address 192.168.20.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Розглянемо налаштування маршрутизації. Адміністратор включає IP-маршрутизацію на комутаторі для забезпечення маршрутизації між VLAN:

```
Switch(config)# ip routing
```

Адміністратор перевіряє, чи правильно налаштовані VLAN і інтерфейси, за допомогою команд:

```
Switch# show vlan brief
Switch# show ip interface brief
```

Адміністратор зберігає конфігурацію, щоб налаштування збереглися після перезавантаження:

```
Switch# write memory
```

Нижче наведено приклад повної конфігурації для двох VLAN (VLAN 10 та VLAN 20):

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Sales
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name Engineering
Switch(config-vlan)# exit
Switch(config)# interface range Ethernet0/1-2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit
Switch(config)# interface range Ethernet0/3-4
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.10.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface vlan 20
Switch(config-if)# ip address 192.168.20.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Switch(config)# ip routing

Switch# show vlan brief
Switch# show ip interface brief
Switch# write memory

Таким чином, адміністратор налаштовує віртуальні підмережі на комутаторі третього рівня Cisco, забезпечуючи ефективне розділення мережевого трафіку та маршрутизацію між різними VLAN які присутні в нашій мережі.

3.2.2 Інструкції з налаштування комутаторів робочих груп

Комутатори відділів налаштуємо поступово за однаковою процедурою, поетапно.

На першому етапі потрібно задати IP-адресу комутатора, як показано на рисунку 3.2.

Рисунок 3.2 – Налаштування IP-адреси комутатора

Наступним етапом є вказання імені пристрою, як показано на рисунку 3.3.

Рисунок 3.3 – Налаштування імені пристрою

Доцільно також вказати коректну дату та час, використовуючи сервери часу Інтернет по протоколу SNTP, як показано на рисунку 3.4.

Рисунок 3.4 – Налаштування протоколу SNTP

Для інтеграції кому торів робочих груп в локальну мережі потрібно створити перелік віртуальних мереж на кожному комутаторів робочої групи, вказуючи ті робочі станції, які підключені до відповідної VLAN. Приклад наведено на рисунку 3.5.

Рисунок 3.5 – Створення VLAN

Один із портів повинен бути налаштований у режимі tagged, для передачі пакетів з відповідними мітками, про приналежність до відповідної VLAN.

3.2.3 Інструкції з налаштування безпровідних маршрутизаторів

Після підключення роутера до мережі необхідно виконати кілька важливих налаштувань, опишемо їх детально.

Спочатку потрібно підключити комп'ютер до роутера за допомогою мережевого кабелю або через Wi-Fi. Потім використовуючи веб-браузер на комп'ютері та ввести IP-адресу роутера в адресному рядку. Типові IP-адреси для доступу до веб-інтерфейсу роутера - 192.168.1.1 або 192.168.0.1.

Після входу у веб-інтерфейс потрібно перейти до розділу налаштувань інтернет-з'єднання. Тут обираємо тип з'єднання, який використовується провайдером, наприклад, PPPoE, DHCP (Automatic IP) або Static IP, і вводимо необхідні дані для підключення до інтернету, які надає провайдер (наприклад, ім'я користувача та пароль для PPPoE).

Далі потрібно перейти до розділу налаштувань безпровідної мережі, де встановити ім'я мережі (SSID) та пароль для підключення до Wi-Fi. Вибираємо також тип шифрування (зазвичай WPA2-PSK) для забезпечення безпеки мережі і зберігає зміни.

Для забезпечення безпеки потрібно змінити пароль для доступу до веб-інтерфейсу роутера на більш складний. Це дозволяє запобігти несанкціонованому доступу до налаштувань. Для додаткового захисту мережі включаємо вбудований брандмауер роутера. Якщо необхідно, налаштовуємо фільтрацію MAC-адрес для обмеження доступу до мережі тільки для дозволених пристроїв.

Після цього перевіряємо з'єднання, підключаючись до нової Wi-Fi мережі з комп'ютера або мобільного пристрою, вводячи SSID та пароль, встановлені раніше, і перевіряє доступ до Інтернет.

3.3 Інструкції з використання тестових наборів та програм

З метою тестування роботи локальної мережі та її різних параметрів будуть використовуватись кабельний тестер та утиліти ОС. Кабельний тестер виконує функцію тестування фізичних ліній зв’язку та їх відповідність заявленим технічним параметрам.

Отже, тестування логічних каналів зв’язку та роботи мережевих сервісів будуть використовуватись утиліти ОС, як:

- Ping: Ping використовується для перевірки доступності хоста в мережі та вимірювання часу відправки-прийому пакетів.

- Traceroute: Traceroute дозволяє визначити маршрут, який пакети пройшли від джерела до призначення, і визначити кількість вузлів, через які пройшов пакет.

- Netcat: Netcat (або nc) дозволяє взаємодіяти з мережевими портами, надсилаючи або приймаючи дані через TCP або UDP.

- Nmap: Nmap використовується для сканування мережі, визначення активних хостів, відкритих портів та інших характеристик мережевого обладнання.

- Wireshark: Wireshark - це мережевий аналізатор, який дозволяє перехоплювати та аналізувати пакети, що пересилаються по мережі, для виявлення проблем та відладки.

- Iperf: Iperf використовується для вимірювання пропускної здатності мережі, тобто швидкості передачі даних між системами.

- Tcpdump: Tcpdump є іншим інструментом для перехоплення та аналізу пакетів в мережі, проте він працює в командному режимі.

Ці утиліти дозволяють адміністраторам мережі відлагоджувати, тестувати та аналізувати різні аспекти мережевої роботи для забезпечення її стабільності та безпеки.

3.4 Інструкції по налаштуванню засобів захисту мережі

Питання захисту мережі і кібербезпеки в цілому є дуже актуальним, особливо в даний час. Для захисту ЛОМ від несанкціонованого доступу та фільтрації трафіку буде використано файрвол iptables. У додатку Ж приведено інструкції з налаштування файрволу iptables.

3.5 Інструкції з експлуатації та моніторингу в мережі

Для моніторингу ЛОМ використано стек Prometheus, Grafana. Нижче наведено bash-скрипт для встановлення бази даних TSDB Prometheus:

```
#!/bin/bash
# Update package index
sudo apt update
# Install necessary packages
sudo apt install -y wget tar
# Download Prometheus binary
PROM_VERSION="2.30.1"
```

```
wget
https://github.com/prometheus/prometheus/releases/download/v${PROM_VERSIO
N}/prometheus-${PROM_VERSION}.linux-amd64.tar.gz
# Extract Prometheus archive
tar -xzf prometheus-${PROM_VERSION}.linux-amd64.tar.gz
# Move Prometheus binaries to /usr/local/bin directory
sudo mv prometheus-${PROM_VERSION}.linux-amd64/{prometheus,promtool}
/usr/local/bin/
# Create Prometheus configuration directory
sudo mkdir -p /etc/prometheus
# Cleanup downloaded files
rm -rf prometheus-${PROM_VERSION}.linux-amd64.tar.gz
# Create a Prometheus configuration file (e.g., prometheus.yml)
cat <<EOF | sudo tee /etc/prometheus/prometheus.yml
global:
  scrape_interval: 15s
scrape_configs:
  - job_name: 'prometheus'
    static_configs:
      - targets: ['localhost:9090']
EOF
# Create Prometheus systemd service file
cat <<EOF | sudo tee /etc/systemd/system/prometheus.service
[Unit]
Description=Prometheus
Wants=network-online.target
After=network-online.target
[Service]
User=prometheus
```

```
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
  --config.file /etc/prometheus/prometheus.yml \
  --storage.tsdb.path /var/lib/prometheus \
  --web.console.templates=/etc/prometheus/consoles \
  --web.console.libraries=/etc/prometheus/console_libraries \
  --enable-feature=remote-write-receiver \
  --web.enable-admin-api
[Install]
WantedBy=multi-user.target
EOF
# Create Prometheus user and directories
sudo useradd -rs /bin/false prometheus
sudo mkdir -p /var/lib/prometheus /etc/prometheus/consoles
/etc/prometheus/console_libraries
sudo chown -R prometheus:prometheus /var/lib/prometheus
/etc/prometheus/consoles /etc/prometheus/console_libraries
# Reload systemd daemon and start Prometheus service
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
echo "Prometheus is now installed and running."
```

В цій базі даних будуть зберігатися метрики різних підсистем ядра мережі. Для перегляду метрик потрібно зайти на сервер використовуючи посилання http://server:9090 на вибрати меню Targets. На рисунку 3.6 показано головне вікно Prometheus.

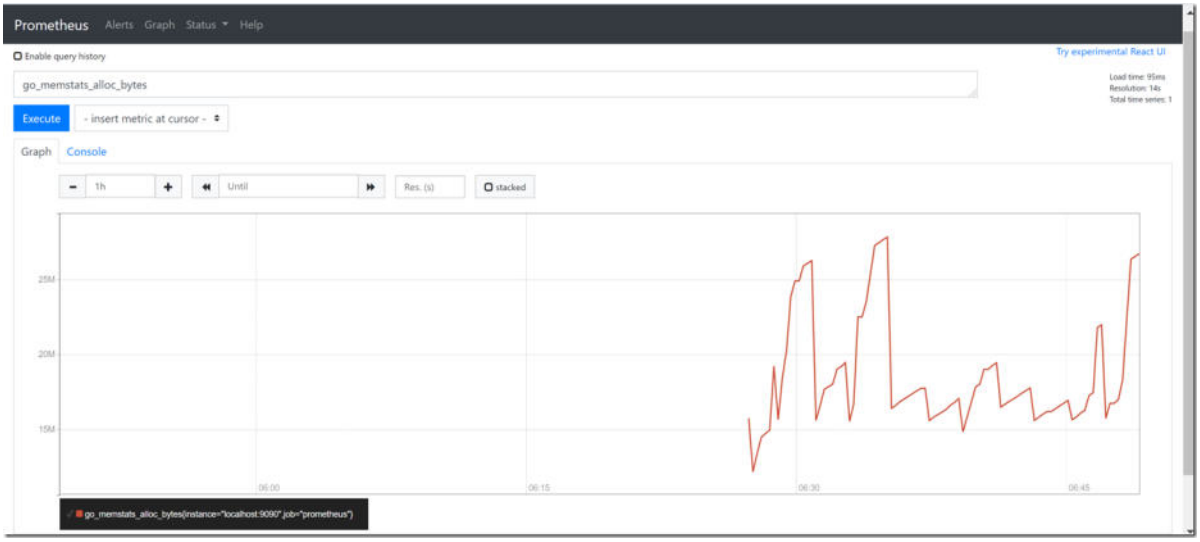

Рисунок 3.6 – Головне вікно Prometheus

Grafana призначена для візуалізації метрик з бази даних Prometheus використовуючи різні Dashboards, як показано на рисунку 3.7.

Рисунок 3.7 – Grafana Dashboards

Нижче наведено скрипт для встановлення служби Grafana:

```
#!/bin/bash
# Add Grafana repository and its GPG key
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 -
# Update apt package index and install Grafana
sudo apt-get update
sudo apt-get install -y grafana
# Start Grafana server
sudo systemctl start grafana-server
# Enable Grafana server to start on system boot
sudo systemctl enable grafana-server
# Allow Grafana server through firewall (if ufw is enabled)
sudo ufw allow 3000/tcp
# Display status and URL
echo "Grafana installed and running."
echo "You can access Grafana at http://localhost:3000"
```

3.6 Моделювання роботи локальної мережі

Моделювання роботи локальної мережі проводиться для того, щоб перевірити правильність її побудови та функціонування.

На рисунку 3.8 наведено приклад побудованої логічної топології компанії.

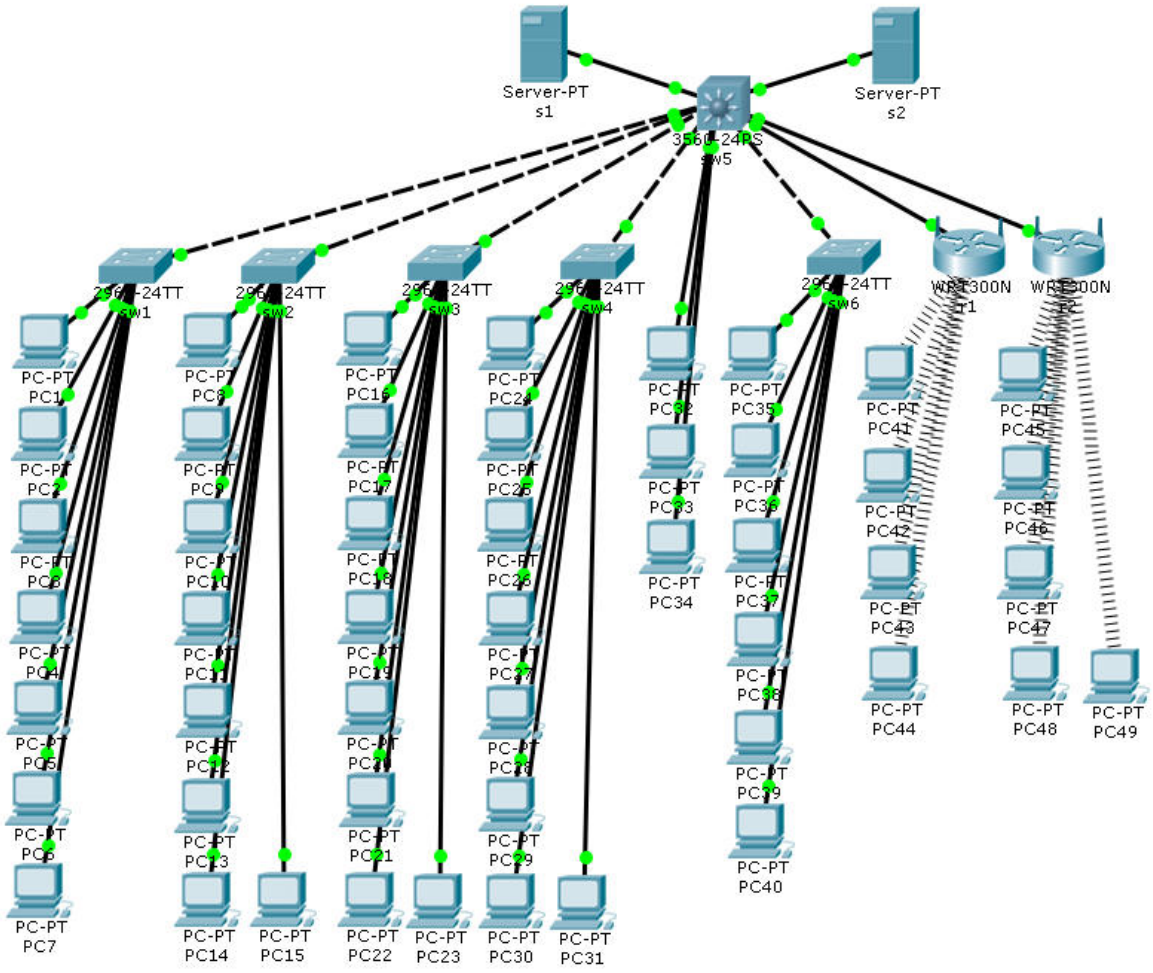

Рисунок 3.8 - Логічна топологія локальної мережі компанії

Після побудови мережі в програмі Cisco Packet Tracer потрібно сконфігурувати основні вузли, основним з яких є центральний комутатор:

Switch>enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname sw5

Sw5(config)#ip routing

Sw5(config)#

Сконфігуруємо також віртуальні мережі згідно таблиці IP-адресації. Приклад конфігурування для підмережі 192.168.100.0/24:

Sw5(config-vlan)# vlan 100 name main

Sw5(config-vlan)# exit

Sw5(config)# interface vlan 100

Sw5(config-if)#ip address 192.168.100.254 255.255.255.0

Sw5(config-if)#exit

Перевіримо зв'язок між вузлами 192.168.100.252/24 (s2) та PC30:

ping 192.168.100.253

Packet Tracer PC30 Command Line 1.0

PC30>ping 192.168.100.253

Pinging 192.168.100.252 with 32 bytes of data:

Reply from 192.168.100.253: bytes=32 time=1ms TTL=128

Reply from 192.168.100.253: bytes=32 time=0ms TTL=128

Reply from 192.168.100.253: bytes=32 time=0ms TTL=128

Reply from 192.168.100.253: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.100.253:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

Результатами моделювання є 4 відправлені пакети з вузла PC30 до вузла S2.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

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

Дана компанія займається збором і обробкою аналітичної інформації, статистикою і взаємодіє з багатьма іншими компаніями різних профілів. Також до складу компанії входить підрозділ, що надає послуги з проектування інженерних конструкцій, 3-D моделювання та реалізації інших інженерних задач.

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 техпроцесу

№ п/п	Назва стадії	Виконавець	Середній час виконання операції, год.
1	2	3	4
1	Постановка задачі на проектування, збір інформації про об'єкт	Керівник проекту	10
2	Розробка проекту	Інженер	20
3	Погодження і затвердження проекту	Керівник проекту	2

Продовження таблиці 4.1

1	2	3	4
4	Монтаж мережі	Технік	36
5	Налагодження мережі та створення технічної документації	Інженер	32
		Разом	100

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для «СІП» складає 100 годин.

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 – 120 грн./год., інженер – 90 грн./год., технік – 60 грн./год.

Отже, основна заробітна плата для:

1. Керівник проекту - $З_{осн1} = 12 \cdot 120 = 1440$ грн.

2. Інженер - $З_{осн2} = 52 \cdot 90 = 4680$ грн.

3. Технік - $З_{осн3} = 36 \cdot 60 = 2160$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 1440 + 4680 + 2160 = 8280{,}00 \text{ грн.}$$

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

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проекту - $З_{дод1} = 1440 \cdot 0{,}13 = 187{,}20$ грн.
2. Інженер - $З_{дод2} = 4680 \cdot 0{,}13 = 608{,}40$ грн.
3. Технік - $З_{дод3} = 2160 \cdot 0{,}13 = 280{,}80$ грн.

Загальна додаткова заробітна плата становить:

$$З_{дод} = 187{,}2 + 608{,}4 + 280{,}80 = 1076{,}40 \text{ грн.}$$

Звідси загальні витрати на оплату праці розраховуються за формулою 4.3:

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

$$В_{о.п} = 8280{,}00 + 1076{,}40 = 9356{,}4 \text{ грн}$$

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:

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

де ФОП – фонд оплати праці, грн.

$$B_{с.з.} = 9356{,}4 \cdot 0{,}376 = 3518{,}1 \ \ грн.$$

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	120	12	1440	127,05	-	-
2	Інженер	90	52	4680	414,00	-	-
3	Технік	60	36	2160	330,00	-	-
			Разом	8280,00	1076,40	3518,01	12874,41

Отже, загальні витрати на оплату праці становлять 12874,41 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:

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

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Матеріальні ресурси	Од. вим.	Факт. витрачено матеріалів	Ціна одиниці, грн.	Загальна сума, грн.
1	Кабель UTP 6 (бухта 305м)	шт.	2	3560	7120
2	Серверна шафа 24U	шт.	1	10210	10210
3	Патч-панель 24 порти, кат. 6	шт.	1	1500	1500
4	Короб	м.	100	50	5000
5	Патчкорд, UTP кат. 6	шт.	70	12	840
6	Мережева розетка UTP кат. 6	шт.	43	160	6880
7	Фільтр-подовжувач (3м)	шт.	3	120	360
8	Кабельні тримачі	шт.	2	200	400
9	Комутатор Cisco WS-C3750G	шт.	1	20000	20000
10	Сервер HP ProLiant ML30 Gen10 (P06781-425)	шт.	2	34000	68000
11	Комутатор D-Link DGS-1216T	шт.	3	3000	9000
12	Комутатор D-link DGS-1210-08	шт.	2	2400	4800
13	Маршрутизатора TP-LINK Archer C7 AC1750	шт.	2	2100	4200
				Всього, грн.	138310

Загальна сума матеріальних витрат на розробку мережі становить 138310,00 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 20 годин, споживана потужність - 0,5 кВт/год, вартість 1 кВт електроенергії – 4,32 грн.

Тому витрати на електроенергію будуть становити:

$$З_е = 0,5 \cdot 20 \cdot 4,32 = 43,2 \text{ грн.}$$

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:

$$Т_в = 138310,00 \cdot 0,08 = 11064,80 \text{ грн.}$$

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 20 год., балансова вартість ПК – 28000 грн., тому:

$$A = \frac{28000 \cdot 0{,}05}{150} \cdot 20 = 186{,}67 \ грн.$$

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.

$$Н_в = 12874,41 \cdot 0,3 = 3862,33 \text{ грн.}$$

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	9356,4	5,62
Відрахування на соціальні заходи	3518,01	2,11
Матеріальні витрати	138310,00	83,15
Витрати на електроенергію	43,2	0,03
Транспортні витрати	11064,80	6,65
Амортизаційні відрахування	186,67	0,11
Накладні витрати	3862,33	2,32
Собівартість	166341,41	100,00

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

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

Отже, собівартість дорівнює: $С_в$=166341,41 *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 %.

$$Ц = 166341,41 \cdot (1+0,3) \cdot (1+0,2) = 259492,60 \text{ грн.}$$

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:

$$П = Ц - С_в \quad (4.13)$$

$$П = 259492,60 - 166341,41 = 93151,19 \text{ грн.}$$

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.

$$E_p = 93151,19 \ / 166341,41 = 0,56$$

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

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

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.	166341,41 грн.
2.	Плановий прибуток, грн.	93151,19 грн.
3.	Ціна, грн.	259492,60 грн.
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,79

Отже, загальна вартість розробленої комп'ютерної мережі компанії «СІП» становить 259492,60 грн. Зважаючи на те, що показники економічної ефективності - 0,56 є досить високим, кошти, вкладені в проведення проектних робіт окупляться за 1,79 року.

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

У суспільстві із соціально орієнтованою економікою охорона праці має бути одним з найважливіших завдань соціально-економічної політики як держави, так і кожного підприємства та організації. Охорона праці – проблема складна і багатогранна.

Проте нинішній рівень науково-технічного прогресу та соціально-економічні орієнтири розвитку сучасного суспільства не спроможні створити сприятливі умови для забезпечення добробуту людини, збереження її здоров'я. Особливо гостро ця проблема постає на промислових підприємствах, зокрема машинобудівних, гірничо-видобувних, ливарних виробництвах, де зберігається переважно застаріла матеріально-технічна база виробництва при незадовільних обсягах фінансування заходів з охорони праці. Усе це призводить до високого рівня травматизму та професійної захворюваності, особливо в гірничо-видобувній галузі і, як наслідок, до збільшення видатків підприємства держави та Фонду соціального страхування на виплати й компенсації потерпілим [3].

В галузі інформаційних технологій ситуація значно краща, оскільки немає надто шкідливих факторів і умов праці, але є інші виклики, які пов'язані з професійними захворюваннями, елетробезпекою, пожежною безпекою та інше.

5.1 Дія електричного струму на організм людини, причини та наслідки уражень

Аналіз виробничого травматизму показує, що кількість травм, спричинених дією електричного струму, є незначною і становить близько 1 %. Однак із загальної кількості смертельних нещасних випадків частка електротравм становить 20-40% і посідає одне з перших місць [2].

Щороку в Україні від електричного струму гине приблизно 1500 осіб. Найбільша кількість випадків електротравматизму, в тому числі зі смертельними

наслідками, стається при експлуатації електроустановок напругою до 1000 В, що пов'язано з їх поширенням і відносною доступністю практично для кожного, хто працює на виробництві. Випадки електротравматизму під час експлуатації електроустановок напругою понад 1000 В нечасті, що зумовлено незначним поширенням таких електроустановок і обслуговуванням їх висококваліфікованим персоналом [3].

Основними причинами електротравматизму на виробництві є [3]:

- випадкове доторкання до неізольованих струмопровідних частин електроустаткування;

- використання несправних ручних електроінструментів;

- застосування нестандартних або несправних переносних світильників напругою 220 чи 127 В;

- робота без надійних захисних засобів та запобіжних пристосувань;

- доторкання до незаземлених корпусів електроустановок, що опинилися під напругою внаслідок пошкодження чи пробою ізоляції;

- недотримання правил будови, улаштування, безпечної експлуатації електроустановок та правил експлуатації електрозахисних засобів тощо.

Електроустаткування, з яким доводиться мати справу практично всім працівникам на виробництві, становить значну потенційну небезпеку ще й тому, що органи чуття людини не здатні на відстані виявляти наявність електричної напруги. У зв'язку з цим захисна реакція організму виявляється лише після того, як людина потрапила під дію електричної напруги.

Проходячи через організм людини, електричний струм справляє на нього термічну, електролітичну, механічну та біологічну дію.

Термічна дія струму спричинює опіки окремих ділянок тіла, нагрівання кровоносних судин, серця, мозку та інших органів, через які проходить струм, що призводить до виникнення в них функціональних розладів.

Електролітична дія струму характеризується розкладом (електролізом) крові та інших органічних рідин, що викликає суттєві порушення їх фізикохімічного складу.

Механічна дія струму загрожує ушкодженнями (розриви, розшарування тощо) різноманітних тканин організму внаслідок електродинамічного ефекту.

Біологічна дія струму на живу тканину спричиняє небезпечне збудження клітин та тканин організму, що супроводжується мимовільним судомним скороченням м'язів. Таке збудження може призвести до суттєвих порушень і навіть повного припинення діяльності органів дихання та кровообігу. Збудження тканин організму внаслідок дії електричного струму може бути прямим, коли струм проходить безпосередньо через ці тканини, та рефлекторним (через центральну нервову систему), коли тканини не знаходяться на шляху проходження струму.

Вплив електричного струму на організм людини класифікують за ступенем складності:

1. Електротравми – опіки, електричні знаки (специфічне ураження тканин); металізація шкіри (частина розплавленого металу); електрофтальмія (запалення зовнішніх оболонок очей під дією ультрафіолетових променів електричної дуги); механічні ушкодження (розірвання шкіри, вивихи, переломи і т. д., викликані мимовільним скороченням м’язів).

2. Електричний удар. Розрізняють 4 ступені електричного удару:

1 ступінь – судорожне скорочення м’язів без утрати свідомості;

2 ступінь – судорожне скорочення м’язів з утратою свідомості, але зі збереженням дихання і роботи серця;

3 ступінь – втрата свідомості; порушення дихання або роботи серця;

4 ступінь – клінічна смерть.

Тяжкість електротравми визначається впливом факторів:

- електричного характеру - величина напруги, сила струму, вид струму (постійний чи змінний), частота при змінному струмі;

- неелектричного характеру - тривалість дії електроструму;

- навколишнього середовища - температура, тиск, вологість повітря;

- шляху протікання струму через тіло людини [3].

Шлях протікання струму в тілі людини відіграє суттєву роль у наслідках ураження.

Шлях струму визначається місцем прикладання струмоведучих частин до тіла людини. Особливо небезпечним є ураження людей у тому випадку, коли людина торкається до струмоведучих частин верхньою половиною тіла, де на шляху протікання струму лежать життєво важливі органи – серце, легені, головний мозок.

Якщо струм проходить іншим шляхом, його дія на життєво важливі органи може бути лише рефлекторною, а не безпосередньою.

В електропатології шлях струму через тіло людини носить назву “ петля струму”, якою відбувається ураження. Номенклатуру цих петель розробив Г.Л. Френкель [3].

Найчастіше струм проходить такими шляхами:

рука – рука;

руки – ноги;

нога – нога;

голова – ноги;

голова – руки.

Менш небезпечним є шлях від однієї ноги до іншої, який отримав назву “ нижня петля ”. Він виникає під дією на людину так званої крокової напруги.

Ураження людей кроковою напругою відбувається тоді, коли людина потрапляє в місце розтікання струму по поверхні землі. Це виникає тоді, коли на землю впав обірваний провідник, що перебуває під струмом.

Кроковою напругою називається напруга між двома точками електричного поля на відстані кроку (0,8м), на яких одночасно стоїть людина в зоні розтікання струму у землі. Графічна ілюстрація крокової напруги наведена на рисунку 5.1.

Рисунок 5.1 – Спосіб виходу з зони ураження

Струм з обірваного провідника розтікається у землі радіально у всі сторони, з найбільшим потенціалом у точці торкання землі.

Зміна потенціалу на поверхні землі від точки замикання відбувається за гіперболічним законом і практично зменшується до нуля на відстані 20м.

При кроковій напрузі струм, проходить від однієї ноги до іншої, скорочує м’язи на ногах, біль стає нестерпною і людина падає. При падінні збільшується відстань між точками дотику до землі і змінюється шлях проходження струму через тіло (рука-нога). Падіння відбувається уже при іншій дії напруги, що призводить до більш тяжких наслідків.

Крокова напруга найбільш небезпечна в межах 4-5м від провідника, що лежить на землі під напругою 1000В, а при напрузі понад 1000В небезпечна зона становить 10м від точки стікання струму. Виходити з зони розтікання струму в землі потрібно короткими кроками.

5.2 Способи і засоби пожежогасіння в компанії «СІП»

В останні роки проблема пожежної безпеки офісів стала особливо актуальною. Як правило, офісні приміщення оснащуються великою кількістю комп'ютерної та оргтехніки, електроприладами, меблями, виготовленими з легкозаймистих матерів. В них одночасно працюють по кілька десятків людей.

Одним з елементів забезпечення пожежної безпеки в офісі є первинні засоби пожежогасіння. Необхідно утримувати їх в належному стані та навчити персонал користуватися ними у випадку виникнення надзвичайної ситуації [18].

До первинних засобів пожежогасіння належать: вогнегасники, кошма (покривало з негорючого теплоізоляційного полотна), ящики з піском, бочки з водою, пожежні відра, багри, ломи, сокири тощо. Найбільш зручними для використання в умовах офісу є вогнегасники. Попри обладнання будівель будь-якими типами установок пожежогасіння, пожежної сигналізації або внутрішніми пожежними кранами, офісні приміщення також мають бути забезпечені первинними засобами пожежогасіння.

Відповідальними за своєчасне та повне оснащення об'єктів засобами пожежогасіння, забезпечення їх технічного обслуговування, навчання працівників правил користування ними є власники або орендарі об'єктів.

В кожній організації наказом або розпорядженням керівника повинна бути призначена особа, відповідальна за експлуатацію вогнегасників. Це може бути особа відповідальна за дотримання вимог пожежної безпеки на об'єкті або спеціаліст відповідної категорії з іншої організації, наприклад, пункту технічного обслуговування вогнегасників.

Успішне гасіння пожежі залежить від правильного вибору типу та виду вогнегасника. Вибір типу та необхідна кількість вогнегасників здійснюється відповідно до Правил експлуатації та типових норми належності вогнегасників, затверджених наказом Міністерства внутрішніх справ України від 15 січня 2018 р. № 25 [3].

Експлуатація вогнегасників без призначення відповідального за організацію цієї роботи не допускається.

Згідно з Правилами, будинки адміністративного призначення на кожному поверсі повинні мати не менше двох переносних (порошкових чи вуглекислотних) вогнегасників з масою заряду вогнегасної речовини 5 кг і більше.

Крім того, на 20 м² площі підлоги в офісних приміщеннях з оргтехнікою, слід передбачати по одному вогнегаснику з величиною заряду вогнегасної речовини 3 кг і більше. Приміщення, у яких розміщено оргтехніку, слід оснащувати переносними газовими вогнегасниками з розрахунку один вогнегасник ВВК-1,4 чи ВВК-2, але не менше ніж один вогнегасник зазначених типів на приміщення [18].

Додатково будинки та офісні приміщення можуть оснащуватися пристроєм вогнегасним водопінним аерозольним (ВВПА), з масою заряду вогнегасної речовини 400 г і більше [18].

Для гасіння пожежі в початковій стадії в офісах, крім вогнегасників доречно мати ще кошму. Пожежні покривала повинні бути розміром не менше ніж 1 х 1 м. У місцях застосування та зберігання ЛЗР та ГР1 мінімальні розміри пожежних покривал збільшуються до величин: 2 х 1,5 м і 2 х 2 м відповідно.

Необхідна кількість первинних засобів пожежогасіння повинна визначатися відповідальним за пожежну безпеку на об’єкті окремо для кожного поверху та приміщення з урахуванням специфіки даного офісу.

Окрім цього, для гасіння пожежі передбачаються механічні засоби, які мають зберігати свою функціональність протягом розрахункового часу для гасіння пожежі (драбини, зовнішні пожежні драбини, аварійні виходи, захищені ліфти та ін.).

Система протипожежного захисту (СПЗ) - комплекс технічних засобів, що змонтований на об'єкті, призначений для виявляння, локалізування та ліквідування пожеж без втручання людини, захисту людей, матеріальних

цінностей та довкілля від впливу небезпечних чинників пожежі, провадження пожежно-рятувальних робіт.

До систем протипожежного захисту (далі - СПЗ) відносять:

- автоматичні системи пожежогасіння (далі - АСПГ);
- системи пожежної сигналізації (далі - СПС);
- системи оповіщування про пожежу та управління евакуюванням людей (далі - СО);
- системи димо- та тепловидалення та підпору повітря (далі - СДТ);
- системи централізованого пожежного спостерігання (далі - СПТС);
- системи диспетчиризації СПЗ.

Для раннього оповіщення про пожежу, а також включення автоматичної системи пожежогасіння потрібно використовувати автоматичні пожежні сповіщувачі.

Автоматичні пожежні сповіщувачі підрозділяють за:

- видом контрольованої ознаки пожежі (теплові, димові, полум'я та комбіновані);
- видом контрольованої зони (точкові, лінійні, об'ємні та комбіновані);
- видом порогу спрацювання (максимальні, диференційовані та максимально диференційовані);
- принципом дії чутливого елемента.

Чинні нормативи пожежної безпеки [18] чітко не визначають, який тип сповіщувача потрібно використовувати у тому або іншому випадку. Винятком є тільки сповіщувачі полум'я.

Димові пожежні сповіщувачі за принципом дії поділяють на іонізаційні та фотоелектричні. Радіоізотопні (йонізаційні) сповіщувачі безперервно контролюють іонізаційний струм вимірювальної камери, відкритої для доступу диму, порівнюють його зі струмом контрольної камери, яку ізольовано від впливу чинників довкілля, і формують сигнал про наявність диму у повітрі у разі перевищення межового значення співвідношення цих струмів. Іонізує повітря у

відповідних камерах джерело радіоактивного проміння. Суттєвою перевагою таких сповіщувачів є їх здатність практично однаково реагувати як на світлий, так і на темний дим.

Фотоелектричні (оптичні) сповіщувачі, зображені на рисунку 5.2 поділяють на лінійні й точкові. Конструкційно лінійні пожежні сповіщувачі базуються на принципі ослаблення через наявність диму електромагнітного випромінювання між рознесеними у просторі джерелом випромінювання і фотоприймачем.

Рисунок 5.2 - Оптичні і оптико-електронні димові пожежні сповіщувачі

Зліва на рисунку 5.2 зображено лінійні оптичні сповіщувачі диму, а праворуч оптико-електронний давач. Перевагою лінійних пожежних сповіщувачів є велику відстань їх дії (до 100 м). Вони однаково чутливо реагують як на темний, так і на сірий дим. Недоліками таких сповіщувачів є необхідність у забезпеченні прямої видимості між джерелом і приймачем випромінювання, а також можливе налипання пилу на лінзовій оптиці чи захисних елементах.

Для проектованої мережі вибрано комплект протипожежної сигналізації ТІРАС-4П.1 з вбудованим GSM комунікатором [21]. Він призначений для цілодобової централізованої пожежної охорони об'єктів і будівель, шляхом

постійного контролю чотирьох зон і передачі повідомлень, через вбудований комунікатор, за допомогою мережі GSM .

Особливості даного пристрою [24]:

- 4 шлейфи пожежної сигналізації з можливістю підключення як 2-х так і 4-х провідних сповіщувачів (максимальна кількість - 32);
- вбудований блок живлення з резервним живленням від батареї 7А * ч;
- можливість віддаленого скидання пожежі, включення/відключення сповіщувачів;
- програмування з вбудованою клавіатури або за допомогою ПК.

Прилад Тірас-4П.1 призначений для цілодобової централізованої пожежної охорони об'єктів і будівель, шляхом постійного контролю чотирьох зон і передачі повідомлень, через вбудований комунікатор, за допомогою мережі GSM. Прилад відповідає всім вимогам ДСТУ EN 54-2 та ДСТУ EN 54.

Зовнішній вигляд пристрою зображено на рисунку 5.3 [21].

Рисунок 5.3 – Блок протипожежної сигналізації ТІРАС-4П.1

Основні можливості:

– 4 шлейфи пожежної сигналізації з можливістю підключення як 2-х так і 4-х провідних сповіщувачів;

– 3 алгоритму верифікації спрацювання сповіщувачів;

– вбудований вихід для управління звуковим і світлозвуковим оповіщенням;

– 2 вбудовані релейні виходи «Пожежа» і «Несправність»;

– 2 вбудованих програмованих виходи типу "відкритий колектор";

– 2 додаткових релейних програмованих виходу (при підключення МРЛ-2.1);

– вбудований універсальний вхід;

– програмування з вбудованої клавіатури або за допомогою ПК;

– реалізація системи пожежогасіння (при підключенні ПУіЗ «Тірас-1»);

– вбудований блок живлення з резервним живленням від батареї 7А * ч;

– можливість віддаленого скидання пожежі, включення/відключення сповіщувачів;

– інтерфейс Touch Memory для зручного входу в рівень "Адміністратор", управління оповіщенням.

Використання протипожежної сигналізації ТІРАС-4П.1 дозволить оперативно сповіщати про можливі осередки пожежі та приймати швидкі і оперативні рішення.

Отже, в умовах компанії «СІП» заплановано реалізувати систему протипожежного захисту яка складається з автоматичних оповіщувачів і пульта керування, який при виникненні пожежі ввімкне пожежну сигналізацію локально і дистанційно та передасть відповідні дані по gsm-каналу відповідальній особі. Також для ручного гасіння осередків займання передбачено використання вогнегасників та подачі води через пожежний кран і рукав, що розміщені в пожежній шафі.

Схематичне розміщення елементів системи оповіщення і пожежогасіння на плані приміщень наведено на рисунку 5.4.

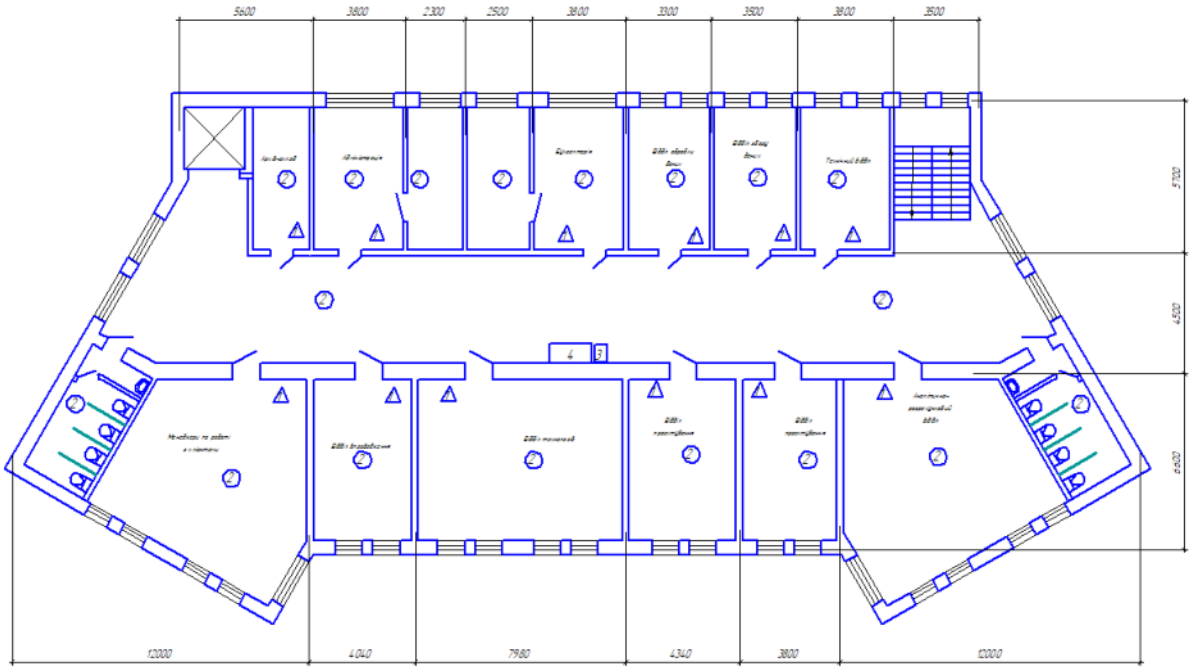

Рисунок 5.4 – Розміщення елементів системи оповіщення і пожежогасіння на плані компанії «СІП

На рисунку 5.4. прийнято такі умовні позначення:

1 – вогнегасники ВВК-5;

2 – оптичні сповіщувачі;

3 – ТІРАС-4П.1;

4 – протипожежна шафа.

ВИСНОВКИ

Для проекту локальної мережі сформовано технічне завдання, в якому сформовано основні вимоги до проекту. Розроблено фізичну та логічну топології для локальної мережі, враховуючи рух інформаційних потоків. Розроблено інструкції з моніторингу, налаштування вузлів та сервісів.

Враховуючі функціональні параметри та співвідношення функцій до вартості вибрано активне та пасивне мережеве обладнання. Для проекту локальної мережі вибрано відповідні сучасні технології та стандарти: 802.1Q, 802.3ab, 802.11ac.

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

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

Проект має практичну спрямованість і його результати будуть використані в даному центрі.

ПЕРЕЛІК ПОСИЛАНЬ

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

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

3. Жидецький В.Ц. Охорона праці користувачів комп’ютерів. Навчальний посібник. Вид. 2-ге., доп. Львів: Афіша. 20120. 176с.

4. Жуков І.А., Дрововозов В.І., Махновський Б.Г. Експлуатація комп’ютерних систем та мереж. Київ: НАУ. 2007. 361с.

5. Калита Д. М. Комп'ютерні мережі. Апаратні засоби та протоколи передачі даних: навч. посіб. для студ. вищих закл. освіти. Київ: ВПЦ "Київський університет", 2013. 326с.

6. Коваленко А. Є. Корпоративні комп'ютерні мережі та телекомунікації. Київ : НУХТ. 2014. 278 с.

7. Мельник І. Проектування та дослідження комп'ютерних мереж. Київ: Університет «Україна». 2018. 362 с.

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

9. Николайчук Я.М. Проектування спеціалізованих комп'ютерних систем: Навчальний посібник/ Я.М.Николайчук, Н.Я.Возна, І.Р.Пітух. Тернопіль: ТзОВ "Терно-граф", 2010. 392с.

10. Погорілий С.Д.. Комп'ютерні мережі. Апаратні засоби та протоколи передачі даних: Підручник/ С.Д.Погорілий, Д.М.Калита К.: ВПЦ "Київський університет, 2018. 238с.

11. Ткаченко В. Комп’ютерні мережі та телекомунікації: навч. посіб. / В. А. Ткаченко, О. В. Касілов, В. А. Рябик Харків: НТУ “ХПІ”, 2017. 224 с.

12. Черкун О.М. Сучасні технології комп’ютерної безпеки. Монографія.

Книга 7. МЕГУ, Рівне, 2012. 90с

13. Cisco Catalyst 3750G-48 Switch.: URL: http://www.cisco.com/c/en/us/ support/switches/catalyst-3750g-48-switch /model.html. (дата звернення 25.05.2024).

14. Cisco VLAN – настройка vlan на Cisco. URL: http://www.adminia.ua/cisco-vlan-nastroyka-vlan-na-kommutatore-cisco/ (дата звернення 25.05.2024).

15. DGS1216T URL: https://support.dlink.com/ProductInfo.aspx?m=DGS-1216T (дата звернення 25.05.2024).

16. TP-Link AC1750. URL: https://www.tp-link.com/uk-ua/products/details/cat-9_Archer-C7.html (дата звернення 25.05.2024).

17. Тестування кабельних ліній, мереж Ethernet та Wi-Fi. URL: https://iron-harry.ua/vyb%d1%96r-kabelnogo-testera. (дата звернення 01.06.2024).

ДОДАТКИ

Додаток А. IP-адресація хостів

Таблиця А1 – Таблиця IP-адрес

№ п/п	Ім’я вузла	IP-адреса	Маска	Шлюз	ДНС
1	2	3	4	5	6
1	WS_1	192.168.12.1-192.168.12.100	/24	192.168.12.254	8.8.8.8
2	WS_2				
3	WS_3				
4	WS_4	192.168.2.1-192.168.2.100	/24	192.168.2.254	
5	WS_5				
6	WS_6				8.8.8.8
7	WS_7				
8	WS_8	192.168.3.1-192.168.3.100	/24	192.168.3.254	8.8.8.8
9	WS_9				
10	WS_10				
11	WS_11				
12	WS_12	192.168.4.1-192.168.4.100	/24	192.168.4.254	8.8.8.8
13	WS_13				
14	WS_14				
15	WS_15				
16	WS_16	192.168.8.1-192.168.8.100	/24	192.168.8.254	8.8.8.8
17	WS_17				
18	WS_18				
19	WS_19				
20	WS_20	192.168.9.1-192.168.9.100	/24	192.168.9.254	8.8.8.8
21	WS_21				
22	WS_22				
23	WS_23				
24	WS_24	192.168.10.1-192.168.10.100	/24	192.168.10.254	8.8.8.8
25	WS_25				
26	WS_26				
27	WS_27				
28	WS_28				
29	WS_29				
30	WS_30				
31	WS_31				
32	WS_32	192.168.5.1-192.168.5.100	/24	192.168.5.254	8.8.8.8
33	WS_33				

Продовження таблиці А1

1	2	3	4	5	6
34	WS_34				
35	WS_35	192.168.7.1-192.168.7.100	/24	192.168.7.254	8.8.8.8
36	WS_36				
37	WS_37				
38	WS_38				
39	WS_39				
40	WS_40				
41	WS_41	192.168.200.1- 192.168.200.100	/24	192.168.200.254	8.8.8.8
42	WS_42				
43	WS_43				
44	WS_44				
45	WS_45	192.168.201.1- 192.168.201.100	/24	192.168.201.254	8.8.8.8
46	WS_46				
47	WS_47				
48	WS_48				
49	WS_49				
50	S_1	192.168.100.252	/24	192.168.100.254	8.8.8.8
51	S_2	192.168.100.253	/24	динамічно	8.8.8.8
		динамічно			
52	R_1	WAN – динамічно з діапазону 192.168.6.1-192.168.6.100	/24	192.168.6.254	8.8.8.8
		LAN - 192.168.200.254; Для DHCP- 192.168.200.1- 192.168.200.100			8.8.8.8
53	R_2	WAN – динамічно з діапазону 192.168.11.1-192.168.11.100	/24 /24	192.168.11.254	8.8.8.8
		LAN - 192.168.201.254; Для DHCP- 192.168.201.1- 192.168.201.100			8.8.8.8
54	SW_1	192.168.1.1	/24	-	-
55	SW_2	192.168.1.2	/24	-	-
56	SW_3	192.168.1.3	/24	-	-
57	SW_4	192.168.1.4	/24	-	-
58	SW_5	192.168.1.5	/24	-	-
59	SW_6	192.168.1.6	/24	-	-

Додаток Б. Логічна адресація в ЛОМ

Таблиця Б1- Поділ мережі на VLAN

№ п/п	Діапазон позначення вузлів	Робоча група/ К-сть вузлів	Приміщення	Назва кабінету та його номер	Номер VLAN	Адреса підмережі/ Маска
1	WS_1-WS_3	3	1	Адміністрація	12	192.168.12.0/24
2	WS_4-WS_7, SW_1	5	1	Бухгалтерія	2	192.168.2.0/24
3	WS_8-WS_11	4	1	Відділ обробки даних	3	192.168.3.0/24
4	WS_12-WS_15, SW_2	5	1	Відділ збору даних	4	192.168.4.0/24
5	WS_16-WS_19	4	1	Відділ проектування	8	192.168.8.0/24
6	WS_20-WS_23, SW_3	1	1	Відділ проектування	9	192.168.9.0/24
7	WS_24-WS_31, SW_4	9	1	Аналітично-розрахунковий відділ	10	192.168.10.0/24
8	WS_32-WS_34	3	1	Технічний відділ	5	192.168.5.0/24
9	WS_35 - WS_40, SW_6	7	1	Відділ технологів	7	192.168.7.0/24
10	WS_41 - WS_44, R_1	5	1	Відділ впровадження	6	192.168.6.0/24
11	WS_45 - WS_49, R_2	6	1	Менеджери по роботі з клієнтами	11	192.168.11.0/24
12	S_1, S_2, SW_5	3	1	Серверна	100	192.168.100.0/24

Таблиця Б2 - Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Номер порту	Тип порту	Назва мер. пристар.	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
1	WS_1-WS_3	-	-	SW_1	1-3	Access	12
2	WS_4-WS_7	-	-	SW_1	4-7	Access	2
3	WS_8-WS_11	-	-	SW_2	1-4	Access	3
4	WS_12-WS_15	-	-	SW_2	5-8	Access	4
5	WS_16-WS_19	-	-	SW_3	1-4	Access	8
6	WS_20-WS_23	-	-	SW_3	5-8	Access	9
7	WS_24-WS_31	-	-	SW_4	1-8	Access	10
8	WS_32-WS_34	-	-	SW_5	1-3	Access	5
9	WS_35 - WS_40	-	-	SW_6	1-6	Access	7
10	WS_41 - WS_44	-	-	R_1	wlan	Access	6
11	WS_45 - WS_49	-	-	R_2	wlan	Access	11
12	S_1, S_2	-	-	WS_5	4-5	Access	100
13	SW_1	8	Trunk	SW_5	6	Trunk	-
14	SW_2	9	Trunk	SW_5	7	Trunk	-
15	SW_3	9	Trunk	SW_5	8	Trunk	-
16	SW_4	9	Trunk	SW_5	9	Trunk	-
17	SW_6	8	Trunk	SW_5	10	Trunk	-
18	R_1	wan	-	SW_5	11	Access	-
19	R_2	wan	-	SW_5	12	Access	-

Додаток В. Порівняльні характеристики обладнання

Таблиця В1 - Порівняльна характеристика комутаторів 3-го рівня OSI

Модель/Параметри	Cisco WS-C3750G	Juniper EX2200-24T-4G-TAA	HP 1920-24G JG924A
1	2	3	4
Швидкість комутації, Гбіт/с	32	56	56
Пропускна здатність, млн. пакетів/с	38,7	41,7	38,6
К-сть портів 10/100/1000	24	24	24
Додаткові слоти SFP	4	4	24
Слоти 10GE	-	-	-
Підтримка протоколів 2 рівня моделі OSI	VLAN, Spaning Tree, Jumbo packet, QoS	VLAN, Spaning Tree, Jumbo packet, QoS	VLAN, Spaning Tree, Jumbo packet, QoS
Статична маршрутизація	+	+	+
Динамічна маршрутизація	RIP, OSPF, IGRP, BGP	-	-
Списки фільтрації трафіку	+	+	+
Моніторинг	SNMP, RMON, PortMirroring	SNMP, RMON, PortMirroring	SNMP, RMON, PortMirroring

Таблиця В2 - Порівняльна характеристика апаратних платформ серверів

Сервер	Dell PowerEdge T40 v04 (T40v04)	HP ProLiant ML30 Gen10 (P06781-425)	ARTLINE Business T19 (T19v12)
Тип виконання	Tower	Tower	Tower
Процесор	Intel Xeon E-2224G (3.5 - 4.7 ГГц)	Intel Xeon E-2124 (3.3 - 4.3 ГГц)	Intel Core i7-9700F (3.0 - 4.7 ГГц)
Чіпсет	Intel C246	Intel C246	Intel H370
Пам’ять оперативна	UDIMM ECC DDR4-2666 МГц (4 слоти, 64 ГБ макс.) – 32ГБ	UDIMM ECC DDR4-2666 МГц (4 слоти, 64 ГБ макс.) – 32ГБ	UDIMM ECC DDR4-2666 МГц (4 слоти, 64 ГБ макс.) – 32ГБ
Рівні RAID	0/1/5/10 - Intel Rapid Storage Technology Enterprise (RSTe)	0/1/5/10 - Intel Rapid Storage Technology Enterprise (RSTe)	0/1/5/10 - Intel Rapid Storage Technology Enterprise (RSTe)
ЖМД	HDD: 2 x 1 ТБ SSD: 2 x 250 ГБ	HDD: 2 x 1 ТБ SSD: 2 x 250 ГБ	HDD: 2 x 1 ТБ SSD: 2 x 250 ГБ
ЛОМ	Gigabit Ethernet	Gigabit Ethernet	Gigabit Ethernet

Додаток Г. Характеристики комутатора

Стандарти портів та підтримувані функції:

1. IEEE 802.3 10BASE-T Ethernet.
2. IEEE 802.3u 100BASE-TX Fast Ethernet.
3. IEEE 802.3ab 1000BASE-T Gigabit Ethernet.
4. IEEE 802.3z Gigabit Ethernet.
5. Автоузгодження ANSI/IEEE 802.3 NWay.
6. Управління потоком 802.3x.
7. Зеркалювання портів.

Кількість портів:

1. 14 портів 10/100/1000BASE-T.
2. Два комбо-порти 10/100/1000BASE-T/SFP.

Функції 2 рівні:

1. IGMP snooping: підтримка 64 багатоадресних груп (Multicast Groups).
2. 802.1D Spanning Tree.

3. Агрегація портів: до 6 груп на пристрій, до 8 портів на групу.

VLAN:

1. Стандарт 802.1Q VLAN (VLAN Tagging).
2. До 256 статичних груп VLAN.

Пропускна здатність комутатора: 32 Гбіт/с.

Додаток Д. Технічні параметри безпровідного маршрутизатора TP-LINK Archer C7 AC1750.

Апаратні характеристики:

- 4 порти LAN 10/100/1000 Мбіт/с
- 1 порт WAN 10/100/1000 Мбіт/с;
- 2 порти USB 2.0;
- 3 знімні антени (RP-SMA).

Параметри бездротового модуля:

- Стандарти бездротових мереж: IEEE 802.11ac/n/a 5 ГГц; IEEE 802.11b/g/n 2,4 ГГц;
- Діапазон частот (прийом і передача): 2,4 ГГц та 5 ГГц;
- Швидкість передачі5 ГГц: До 1300 Мбіт/с; 2,4 ГГц: До 450 Мбіт/с;
- Функції бездротового режиму: Включення/виключення бездротового мовлення, міст WDS, WMM, статистика бездротового;
- Захист бездротової мережі: 64/128-бітній WEP, WPA/WPA2, WPA-PSK/WPA2-PSK.

Особливості даного безпровідного маршрутизатора:

- Підтримка новітнього стандарту бездротового зв'язку 802.11ac.
- Загальний обсяг пропускної здатності до 1,75 Гбіт/с: до 1300 Мбіт/с на 5 ГГц і до 450 Мбіт/с на 2,4 ГГц.

Додаток Е. Інструкції з налаштування проксі-сервера Squid

SQUID може бути встановлений з вихідних текстів або у вигляді DEB-пакета. Установка DEB пакета SQUID дуже проста - для цього потрібно ввести команду:

dpkg -i squid-4.1.STABLE.deb

Вихідні коди можна одержати за адресою ftp://ftp.squid.org/. Для розпакування вихідних кодів, потрібно виконати наступні команди:

cd /usr/src/

gunzip squid-4.11.STABLE-src.tar.gz

tar -xvf squid-4.11.STABLE-src.tar.gz

cd squid

Тепер перейдемо безпосередньо до установки:

./configure -iprefix=/usr/local/squid

make all

make install

Squid буде встановлений у каталог, заданий ключем prefix - /usr/local/squid. Крім prefix можна користуватися ключами, які наведені нижче:

1. --enable-icmp - вимірювати шлях до кожного HTTP-сервера при запитах за допомогою ICMP.

2. --enable-snmp - включити SNMP-моніторинг.

3. --enable-delay-pools - керування трафіком.

4. --disable-wccp - відключити Web Cache Coordination Protocol.

5. --enable-kill-parent-hack - більш коректний shutdown.

6. --enable-splaytree - дозволяє збільшити швидкість обробки ACL.

Squid використає файл конфігурації squid.conf. Звичайно він розташовується в каталозі /etc/squid (або /usr/local/squid/etc - більш ранні версії). Відкриваємо його в будь-якому текстовому редакторі, наприклад joe /usr/local/squid/etc/squid.conf.

Вказуємо проксі провайдера:

cache_peer proxy.ml.net.ua

У нашому випадку proxy.ml.net.ua стає нашим <сусідом> (neighbour, peer) Встановимо обсяг пам'яті, доступний squid, і каталог для кешу:

cache_mem 65536

cache_dir /usr/local/squid/cache 1024 16 256

Вкажемо хости, з яких дозволений доступ до проксі:

acl allowed_hosts src 192.168.100.0/255.255.255.0

acl localhost src 127.0.0.1/255.255.255.255

Заборонимо метод CONNECT для всіх портів, крім зазначених в acl SSL_ports:

http_access deny CONNECT !SSL_ports

Заборонимо доступ усім, крім тих, кому можна:

http_access allow localhost

http_access allow allowed_hosts

http_access allow SSL_ports http_access deny all

Пропишемо користувачів, яким дозволено користуватися squid (den, admin, developer):

ident_lookup on

acl allowed_users user den admin developer

http_access allow allowed_users

http_access deny all

Нижче наведений приклад заборони доступу до будь-якого URL, що відповідає шаблону games і дозвіл доступу до нього всім іншим:

acl GaMS url_regex games

http_access deny GaMS

http_access allow all

Тепер, коли здійснено базове налаштування SQUID, його потрібно запустити:

/usr/local/squid/bin/squid -z

Параметр -z потрібний для створення (обнулення) каталогу, що містить кеш. Звичайно параметр -z потрібний тільки при першому запуску. Параметри проксі-сервера squid наведено нижче:

1. Опція –a - порт для вхідних HTTP-запитів.
2. Опція –d - налагодження (на stderr).
3. Опція -f - ім'я файлу конфігурації.
4. Опція –h – help.
5. Опція -k reconfigure - посилка сигналу HUP.
6. Опція -k shutdown - завершення роботи проксі.
7. Опція -k kill - завершення без закриття журналів.
8. Опція –u - порт для вхідних ICP запитів.
9. Опція –v – version.
10. Опція –D - не робити DNS-тест при запуску.
11. Опція –N - не ставати демоном (фоновим процесом).
12. Опція –Y - більш швидке відновлення після збоїв.

Розглянемо формат файлу squid.conf. Параметри мережі:

http_port 3128

Порт для запитів клієнтів:

icp_port 3130

Якщо сусідів (peer) нема, то потрібно встановити:

icp_port 0

htcp_port 4827

Керування кешем:

cache_swap_high число - при досягненні цього рівня заповнення кешу (у процентному співвідношенні) починається прискорений процес видалення старих об’єктів.

cache_swap_low 90 - процес видалення припиняється при досягненні цього рівня.

maximum_object_size 4096 KB - максимальний розмір кешованого об'єкта.

minimum_object_size 0 KB - файли меншого розміру не зберігаються.

Протоколювання:

cache_access_log /usr/local/squid/logs/access.log - протоколюється кожний запит до SQUID.

cache_log /usr/local/squid/logs/cache.log - журнал запусків процесів.

cache_store_log /usr/local/squid/logs/store.log - журнал запису об'єктів у кеш.

Якщо якийсь журнал не потрібний, потрібно встановити параметр none замість файлу.

Списки ACL:

ACL - визначення списку доступу. Визначається як: acl ім'я тип рядок.

Тип - це тип об'єкта, а рядок - регулярний вираз. Можна використати список acl ім'я тип <ім'я файлу> (по одному параметрі в рядку). Типи параметрів для складання списків доступу наведено нижче:

1. src ip-address/netmask - IP адреса клієнтів.
2. src addr1-addr2/netmask - діапазон адрес.
3. dst ip-address/netmask - URL хостов.
4. time [day-abbrevs] [h1:m1-h2:m2] - час, де день це одна буква з SMTWHFA.
5. port - список портів.
6. port port1-port2 - діапазон портів.
7. proto - протокол - HTTP/FTP.

Параметри доступу:

http_access allow|deny aclname - дозволяти доступ до проксі по http.

icp_access allow|deny aclname - дозволяти доступ до проксі по ICP.

Параметри адміністрування:

cache_mgr email - поштова адреса, на який буде посланий лист, якщо squid перестане функціонувати.

cache_effective_user nobody - при запуску squid від імені root змінити UID на зазначений.

visible_hostname ім’я-хоста - це ім'я буде згадуватися в повідомленнях про помилки.

hostname_aliases ім'я - список синонімів для імені хоста

Додаток Є. Інструкції з налаштування файлового сервера

Установка сервера:

```
# sudo apt-get install samba
```

Запуск сервера:

```
# /etc/init.d/smb start
```

Приклад конфігураційного файлу сервера /smb.conf, в якому ресурси розподіляються на рівні ресурсів:

```
[Global]
log file = /var/log/samba/log
guest account = ftp
smb passwd file = /etc/samba/smbpasswd
client code page = 866
character set = KOI8-R
hosts allow = 192.168.0.0/16
encrypt passwords = yes
dns proxy = no
netbios name = SAMBA file server
server string = Samba File Server
default = ftp
workgroup = MDK
max log size = 500
log level = 3
load printers = no
security = share
guest account = nobody
comment = anonymous share
hide dot files = no
map hidden = yes
```

printable = no

path = /var/ftp

public = yes

guest only = yes

[Home-admin]; Надає доступ юзеру admin (під паролем) у свій домашній каталог

comment = admin Home Dir

writable = yes

valid users = admin

path = /home/admin

Приклад конфігу /etc/samba/smb.conf, в якому ресурси розподіляються на рівні користувачів:

[Global]

log file = /var/log/samba/log

smb passwd file = /etc/samba/smbpasswd

client code page = 866

character set = KOI8-R

hosts allow = 192.168.0.0/16

encrypt passwords = yes

dns proxy = no

netbios name = SAMBA file server

server string = Samba File Server

workgroup = MDK

max log size = 500

log level = 3

security = users

[Homes]; Дає можливість всім користувачам отримувати доступ до своїх домашніх каталогів:

comment = Home directories

browseable = yes

writable = yes

Потрібно додати, що всі користувачі, які отримують доступ через Samba повинні бути:

1. Додані в систему (# userconf -text, userdrake, або adduser /passwd).

2. Додані як користувачі samba в /etc/samba/smbpasswd. Це потрібно зробити командою #smbpasswd -a admin. Замість admin може фігурувати будь-який користувач.

Перевіряємо роботу, попередньо перезапустивши SMB після редагування конфігураційного файлу:

1. mkdir /mnt/smb.

2. mount -t smbfs -o username = admin, password = ПАРОЛЬ, codepage = cp866, iocharset = koi8-r //127.0.0.1/home-admin/mnt/smb

Додаток Ж. Інструкції з налаштування файрволу iptables

Очищаємо правила:

```
iptables -F
```

(or)

```
iptables --flush
```

Вказуємо політики за замовчуванням для основних таблиць:

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
```

Задаємо список IP-адрес, які потрібно блокувати:

```
BLOCK_THIS_IP="x.x.x.x"
iptables -A INPUT -s "$BLOCK_THIS_IP" -j DROP
iptables -A INPUT -i eth0 -s "$BLOCK_THIS_IP" -j DROP
iptables -A INPUT -i eth0 -p tcp -s "$BLOCK_THIS_IP" -j DROP
```

Дозвіл вхідних з'єднань для служби SSH:

```
iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0 -p tcp -s 192.168.100.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```

Дозвіл трафіку з ЛОМ до мережі Інтернет:

iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT

Дозволити запити до DNS:

iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT

iptables -A INPUT -p udp -i eth0 --sport 53 -j ACCEPT