Форма № Н-9.02

Міністерство освіти і науки України

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

Відділення інформаційних технологій, менеджменту, туризму і підготовки іноземних громадян
(назва відділення)

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра
(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі компанії «ТК Галич»**

Виконав: студент IV курсу, групи КІ-418

Спеціальності **123 «Комп'ютерна інженерія»**
(шифр і назва напряму підготовки, спеціальності)

Зоряна ЯРОШ
(ім'я та прізвище)

Керівник Василь ПИЖ
(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 **інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян**
Циклова комісія **комп'ютерної інженерії**
Освітньо-професійний ступінь **фаховий молодший бакалавр**
Освітньо-професійна програма: **Обслуговування комп'ютерних систем і мереж**
Спеціальність: **123 Комп'ютерна інженерія**
Галузь знань: **12 Інформаційні технології**

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"03" квітня 2024 року

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

_____Ярош Зоряні Віталіївні____
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Розробка проєкту комп'ютерної мережі компанії «ТК Галич»

керівник роботи __Пиж Василь Степанович
(прізвище, ім'я, по батькові)

Затверджені наказом ВСП «Тернопільський фаховий коледж ТНТУ імені Івана Пулюя» від 02.04.2024 р №4/9-157.

2. Строк подання студентом роботи: 17 червня 2024 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проєктування, стандарти ANSI/EIA/TIA 568 - "Commercial Building Telecommunications Wiring Standart" і ANSI/EIA/TIA 569 - "Commercial Building Standart for Telecommunications Pathwais and Spaces

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)
- плани приміщень;
- фізична топологія мережі;
- логічна топологія;
- таблиця IP-адрес;
- таблиця техніко-економічних показників.

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Богдана МАРТИНЮК викладач		
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	04.04	
2	Збір і узагальнення інформації	13.05	
3	Написання першого розділу	20.05	
4	Розробка технічного та робочого проекту	27.05	
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	12.06	
10	Погодження нормоконтролю	14.06	
11	Попередній захист роботи	17.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 04 квітня 2024 року

Студент _____ Зоряна ЯРОШ
(підпис) (ім'я та прізвище)

Керівник роботи _____ Василь ПИЖ
(підпис) (ім'я та прізвище)

ЗМІСТ

АНОТАЦІЯ

Метою даної кваліфікаційної роботи є розробка проекту комп’ютерної мережі компанії «ТК Галич».

Пояснювальна записка складається з п’яти розділів.

В першому розділі поставлено завдання на проектування. Описано призначення та область застосування даної мережі, вимоги до програмного, апаратного забезпечення, стадії та етапи розробки мережі, вимоги до документації.

В другому розділі приведено загальний опис задачі та специфічні особливості. Описано схеми фізичного розташування кабелів та вузлів, їх прокладка. Обґрунтовано вибір операційних систем, програмного забезпечення та обладнання для мережі.

Третій розділ містить інформацію про налаштування активного мережевого обладнання.

В четвертому розділі розраховано собівартість розроблюваної мережі та економічну ефективність проекту.

П’ятий розділ проводить опис техніки безпеки. При написанні даного розділу роботи було використано матеріали мережі Інтернет.

Робота містить пояснювальну записку на 84 аркушах формату А4 та графічну частину на 5 аркушах формату А1.

ВСТУП

На сьогоднішній день у світі зростає кількість ПК, які об'єднані в різноманітні інформаційно-обчислювальні мережі від малих локальних мереж в офісах до глобальних мереж типу Internet.

Всесвітня тенденція до об'єднання комп'ютерів у мережі обумовлена поруч важливих причин, таких як прискорення передачі інформаційних повідомлень, можливість швидкого обміну інформацією між користувачами, одержання і передача повідомлень (факсів, E - Mail листів і іншого) не відходячи від робочого місця, можливість миттєвого одержання будь-якої інформації з будь-якої точки земної кулі, а так само обмін інформацією між комп'ютерами різних фірм виробників працюючих під різним програмним забезпеченням.

Такі величезні потенційні можливості які несуть у собі обчислювальна мережа і той новий потенційний підйом який при цьому відчуває інформаційний комплекс, а так само значне прискорення виробничого процесу не дають нам (юриста, юрисконсульта, суддям і т.п.) право не приймати це до розробки і не застосовувати їх на практиці.

Тому необхідно розробити принципове вирішення питання по організації ІТТ (інформаційно-обчислювальної мережі) на базі вже існуючого комп'ютерного парку та програмного комплексу відповідає сучасним науково-технічним вимогам з урахуванням зростаючих потреб і можливістю подальшого поступового розвитку у зв'язку з появою нових технічних і програмних рішень.

При фізичному з'єднанні двох або більше комп'ютерів утворюється комп'ютерна мережа.

У загальному випадку, для створення комп'ютерних мереж необхідно спеціальне апаратне забезпечення (мережеве обладнання) і спеціальне програмне забезпечення (мережні програмні засоби).

Всі комп'ютерні мережі без винятку мають одне призначення ~ забезпечення спільного доступу до загальних ресурсів.

Слово ресурс - дуже зручне. У залежності від призначення мережі в нього можна вкладати той чи інший зміст. Ресурси бувають трьох типів: апаратні, програмні та інформаційні. Наприклад, пристрій друку (принтер) - це апаратний ресурс. Ємності жорстких дисків - теж апаратний ресурс. Коли всі учасники невеликий комп'ютерної мережі користуються одним загальним принтером, це означає, що вони поділяють спільний апаратний ресурс. Те ж можна сказати і про мережі, що має один комп'ютер зі збільшеною ємністю жорсткого диска (файловий сервер), на якому всі учасники мережі зберігають свої архіви і результати роботи.

Крім апаратних ресурсів комп'ютерні мережі дозволяють спільно використовувати програмні ресурси. Так, наприклад, для виконання дуже складних і тривалих розрахунків можна підключитися до віддаленої великий ЕОМ і відправити обчислювальне завдання на неї, а після закінчення розрахунків точно так само отримати результат назад. .

Дані, що зберігаються на віддалених комп'ютерах, утворюють інформаційний ресурс. Роль цього ресурсу сьогодні видно найбільш яскраво на прикладі Інтернету, який сприймається, перш за все, як гігантська інформаційно-довідкова система.

Такі приклади з розподілом ресурсів на апаратні, програмні та інформаційні досить умовні. Насправді, при роботі в комп'ютерній мережі будь-якого типу одночасно відбувається спільне використання всіх типів ресурсів.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Завдання даної кваліфікаційної роботи є створення проекту комп’ютерної мережі для компанії «ТК Галич».

Мережа повинна забезпечити потреби різних відділів підприємства: обмін інформацією, взаємодію та доступ до спільних файлів, документів, доступ до мережевого принтера.

Створення локальної мережі проводиться з ціллю об’єднання всіх комп’ютерів та інших мережевих пристроїв, для розділення та спільного використання мережевих ресурсів, пришвидшити пошук та відправку інформації, розподіл доступу до неї різним категоріям користувачів.

1.1.2 Призначення розробки

Призначення даної розробки є питання про організацію локальної мережі на базі нового комп'ютерного парку і програмного комплексу, що відповідає сучасним технічним вимогам, з урахуванням зростаючих потреб і можливістю подальшого поступового розвитку мережі в зв'язку з появою нових технічних і програмних рішень (в разі необхідності розширення мережі має бути залишено кілька вільних портів в комутатора).

Сучасний розвиток потребує автоматизації будь-яких видів діяльності та роботи, ведення бухгалтерських робіт та проведення навчальних занять, передачу інформації по локальним каналам.

1.1.3 Вимоги до апаратного та програмного забезпечення

В якості фізичного середовища передачі даних в даній локальній мережі необхідно використовувати середовище передачі котре є загальнодоступним, просте в встановлення, котре не потребує складного обладнання для встановлення, а також на основі нього можна зробити мережу котра є найпоширенішою на наш час.

В якості комутуючого обладнання слід обрати комутатор третього рівня. Всі порти повинні підтримувати швидкість 100/1000 Mb/s.

Апаратне та програмне забезпечення, як елемент комп'ютерної мережі повинні відповідати таким вимогам розроблюваної мережі:

- висока продуктивність;
- достатня надійність і безпека;
- можливість розширюваності і масштабованості;
- мати можливість швидкої заміни (ремонту).

1.1.4 Вимоги до документації

При завершенні роботи по створенню комп'ютерної мережі передається повний комплект документів, що містить в собі основні відомості по структурі пропонованої для реалізації комп'ютерної мережі, що допоможе в подальшому обслуговуванню, модернізації чи усуненні несправностей у мережі. Даний документ, в деталях, розкриває всі аспекти реалізації системи. Комплект цих документів повинен включати:

- загальний опис структури кабельної системи і її функціональних можливостей;
- інформацію про терміни і етапи процесу монтажу, а також специфікацію устаткування, що поставляється, перелік виконуваних робіт;

– логічну та фізичну топологію мережі;
– інструкції з налаштування необхідних установок для робочих станцій і серверів;
– інформацію про користувачів та їх права у мережі.

1.1.5 Техніко-економічні показники

Розроблена мережа повинна бути:

– сучасною, недорогою, масштабованою
– швидкість передачі інформації — 1000 Мбіт\с,
– мати доступ до мережі Інтернет
– мережа повинна мати безпровідний сегмент.

1.1.6 Стадії та етапи розробки

Весь обсяг робіт по розробці проекту комп'ютерної мережі поділяється на три стадії: підготовчу стадію, стадії проектування та впровадження.

Перша стадія – підготовча передбачає:

– ознайомлення із приміщенням, в якому буде прокладатися мережа;
– ознайомлення з основними вимогами до параметрів мережі;
– розрахунок необхідної кількості розхідних матеріалів;

На стадії проектування виконується:

– розробка логічної топології мережі;
– розробка фізичної топології мережі;
– вибір необхідного активного та пасивного комунікаційного обладнання на основі порівняння продукції різних фірм-виробників.

Завершальною є стадія впровадження.

– тестування, маркування, виявлення несправностей в кабельних сегментах;

– встановлення активного комутаційного устаткування, джерел безперебійного живлення;

– встановлення програмного забезпечення на робочих станціях та серверах;

– тестування та налагодження роботи комп’ютерної мережі;

– підготовка необхідної документації;

– здача комп’ютерної мережі.

1.1.7 Порядок контролю та прийому

Після завершення розробки проекту комп’ютерної мережі створюється спеціальна комісія для перевірки дієздатності та ефективності даної мережі. Дана комісія повинна складатись із представників двох сторін: керівництва товариства (чи уповноважених осіб) і представників розробника (керівника проекту, техніка, інженера).

Створена комісія має перевірити надійність та швидкодію мережі, стійкість до несанкціонованого доступу, доцільність використання ресурсів, виділених на створення даного проекту, надійність збереження інформації у випадку аварійної ситуації.

Також потрібно впевнитись, що всі роботи виконані згідно діючих стандартів.

Після завершення перевірки виконаних робіт, сторонами підписується акт прийому-здачі, який засвідчує, що розробка комп’ютерної мережі виконана в повному обсязі і згідно технічного завдання.

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

Завданням кваліфікаційної робити є розробка проекту комп'ютерної мережі компанії «ТК Галич».

Офісна будівля, для якої розробляється проект мережі складається з одного поверху і має таку структуру:

– каса

– керівник

– серверна

– робочий зал.

2. РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Розробка та обґрунтування логічної та фізичної схем мережі [9,10]

Першим етапом в проектуванні мережі буде розробка топології для цієї мережі. Вибір топології є дуже важливим етапом адже вона впливає на склад необхідного мережного обладнання та його характеристики, можливості розширення мережі, засоби керування мережею.

Під топологією комп'ютерної мережі розуміється фізичне розташування комп'ютерів в мережі один щодо іншого та спосіб їх з’єднання лініями зв'язку. Важливо відзначити, що поняття топології ставиться, насамперед, до локальних мереж, у яких структуру зв’язків можна легко простежити. У глобальних мережах структура зв’язків схована від користувачів і не надто важлива, тому що кожний сеанс зв'язку може виконуватися по своєму власному шляху.Топологія комп'ютерної мережі відображає структуру зв’язків між її основними функціональними елементами. В залежності від компонентів, що розглядаються, розрізняють фізичну і логічну структури локальних мереж. Фізична структура визначає топологію фізичних з'єднань між комп'ютерами. Логічна структура визначає логічну організацію взаємодії комп'ютерів між собою. Доповнюючи одна одну, фізична та логічна структури дають найповніше уявлення про комп'ютерну мережу.

Виділяють кілька базових топологій побудови комп’ютерних мереж.

1) Топологія типу зірка (Star)

Усі вузли в топології типу зірка з’єднанні з центральним пристроєм, відомого як пристрій-концентратор, використовуючи з'єднання точка-точка. Пристрій-концентратор може бути одним із наступних:

– 1-го рівня - пристрої такі як концентратор або повторювач;

– 2-го рівня пристрої такі як свіч або міст;

– 3-го рівня пристрої такі як маршрутизатор або мережевий шлюз.

Як і в шинній топології концентратор поводить себе як єдина точка котра може вийти з ладу. Якщо концентратор ламається, то з'єднання між усіма вузлами втрачається. Кожна комунікація між вузлами проходить тільки через концентратор. Топологія типу зірка не настільки дорога, для підключення ще одного вузла, необхідний лише один кабель, а конфігурування такої топології є простим. Топологія зображена на рисунку 2.1.

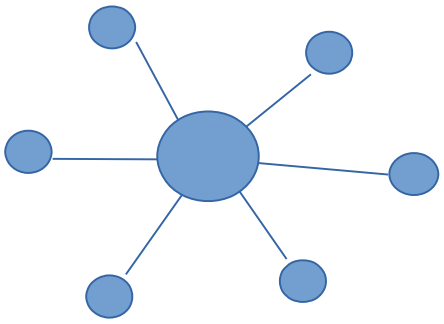


Рисунок 2.1 – Топологія типу зірка (Star)

2)Топологія типу кільце (Ring)

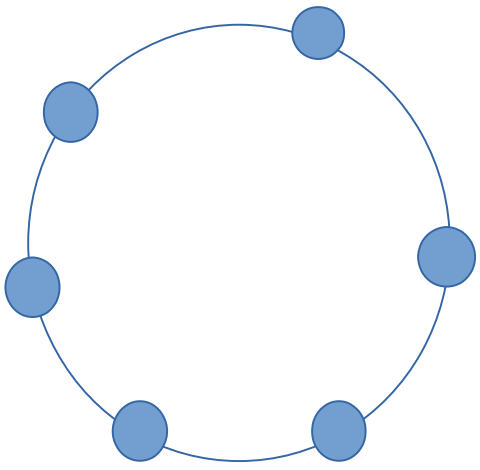


Рисунок 2.2 – Топологія типу кільце (Ring)

В кільцевій топології кожна станція-вузол з’єднана з двома іншими станціями створюючи круглу мережеву структуру. Коли один вузол намагається з’єднатись або відправити повідомлення вузлу, який не є суміжним до нього, дані проходять крізь усі проміжні вузли. Щоб підключити ще один вузол до існуючої структури адміністратору буде необхідний лише один додатковий кабель.

Поломка будь-якого з вузлів виведе з ладу усе кільце. Таким чином, кожне з'єднання в кільці є точкою де може вийти з ладу уся топологія. Є методи, в яких використовується ще одне запасне кільце. Дана топологія зображена на рисунку 2.2.

3) Топологія типу сітка (Mesh)

В цьому типі топології вузол з'єднаний до одного або кількох вузлів. Ця топологія включає в себе підключення типу точка-точка з кожним іншим вузлом або також може мати вузли, які мають з'єднання типу точка-точка лише до декількох вузлів. Вузли в сітковій топології також працюють як запасні для інших вузлів, що не мають прямих з'єднань точка-точка. Сіткова топологія ділиться на 2 типи:

– Повна сітка – усі вузли мають з’єднання точка-точка до кожного іншого вузла в мережі. Таким чином для кожного нового вузла необхідно n(n-1)/2 з'єднань. Це забезпечує найбільш надійну мережеву структуру із усіх мережевих топологій.

– Часткова сітка – не усі вузли мають з’єднання точка-точка до кожного іншого вузла в мережі. Вузли з’єднані один з одним довільним чином. Ця топологія існує тоді, коли необхідно забезпечити надійність лише для деяких вузлів із усіх.

Сіткова топологія представлена на рисунку 2.3.

4)Топологія типу дерево (розширена зірка)

Також відома як ієрархічна топологія, це найпопулярніша форма топології, що використовується на даний момент. Ця топологія імітує розширену зірку і успадковує властивості шинної топології.

Ця топологія ділить мережу на кілька рівнів (шарів) мережі. В основному в LAN-мережах, мережа є розділена в 3 типи мережевих пристроїв.

Найнижчий рівень - рівень доступу, куди підключаються комп'ютери.

Середній рівень, відомий розподільний рівень, що працює як посередник між вищим рівнем і нижчим рівнем.

Найвищий рівень відомий як стержневий рівень, і є центральною точкою в мережі, наприклад верх в дереві від якого відходять усі гілки.

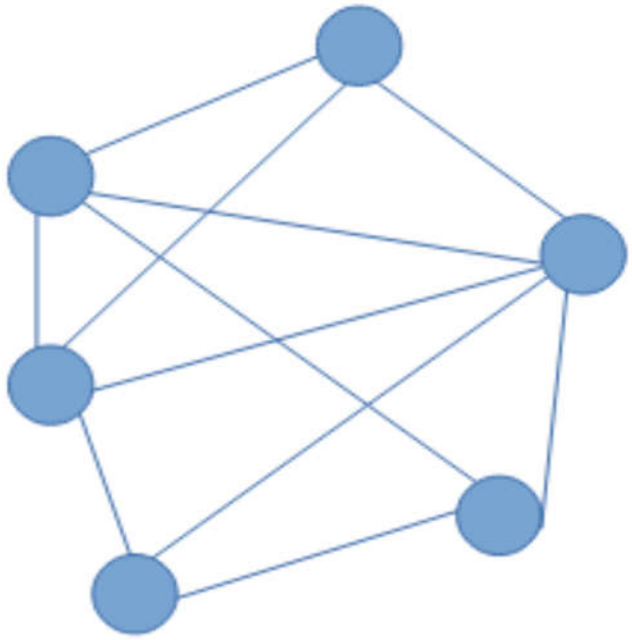


Рисунок 2.3 – Топологія типу сітка (Mesh)

Усі сусідні вузли між собою мають з’єднання типу точка-точка. Схоже до шинної технології якщо стержневий рівень виходить з ладу, виходить з ладу вся мережа.

Хоча це не єдина точка де все може зламатися. Кожне з'єднання є точкою зламу усіх вузлів, що знаходяться нижче (див. рис. 2.4).

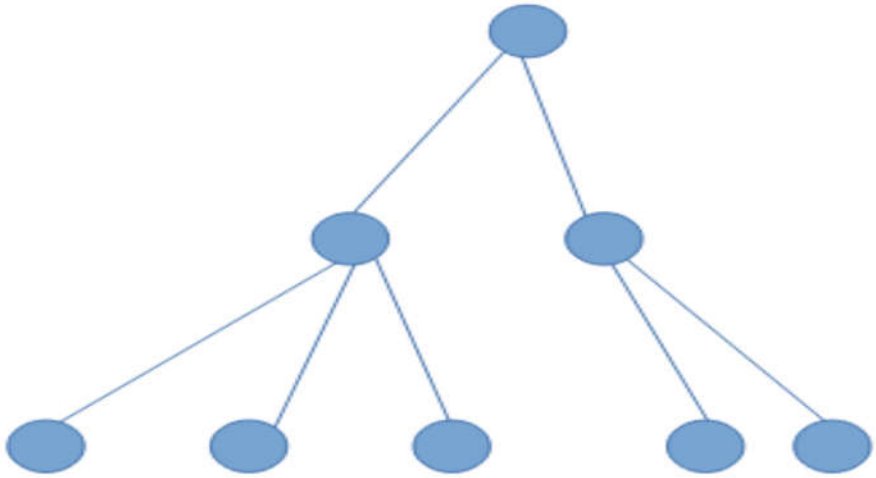


Рисунок 2.4 – Топологія типу дерево (розширена зірка)

5) Гібридна (змішана) топологія (Hybrid)

Мережева структура дизайн якої включає в себе більше ніж одну топологію.

Гібридна топологія успадковує переваги і недоліки усіх вище перерахованих топологій. Комбінування топологій може включати в себе атрибути зіркової, кільцевої, шинної топологій.

Інтернет є найкращим прикладом величезної гібридної топології.

Для побудови мережі було обрано логічну топологію типу «гібридна», оскільки саме вона забезпечить необхідну мережеву інфраструктуру.

Вибір кабельної підсистеми диктується типом мережі й обраною топологією.

Необхідні для стандарту фізичні характеристики кабелю закладаються при його виготовленні, про що і свідчать нанесені на кабель маркування.

Серед всіх можливих середовищ передачі даних мережа Ethernet 1000Base T передбачає використання кабелю кручена пара категорії 5, 5e, 6 та 7.

Кабельна система локальної мережі побудована на основі неекранованої витої пари категорії 5e (див.рис.2.5).

Даний тип кабелю, як і будь-який інший має свої характеристики, правила монтажу та експлуатації. Недотримання цих вимог призведе до передчасного зносу кабельної системи. Використовуваний кабель є дешевий та простий для прокладання. Як концентратори можна використати багато різних пристроїв.

Мережа на скрученій парі проста в обслуговуванні, експлуатації та діагностуванні пошкоджень.

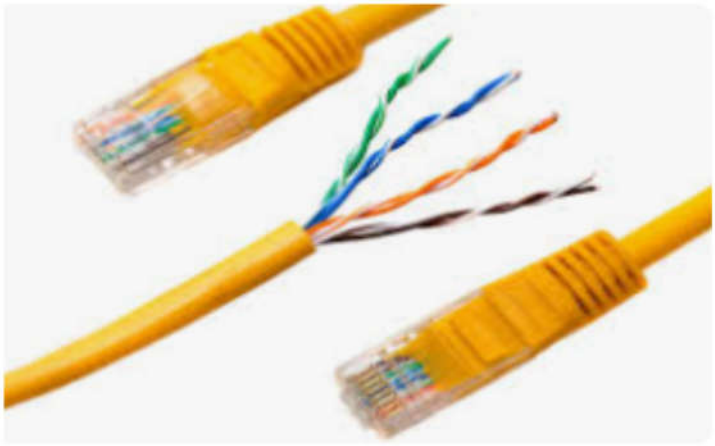


Рисунок 2.5 —Вигляд неекранованої витої пари категорії 5e

Кабелі горизонтальної системи повинні використовуватися разом з комутаційним устаткуванням і патч-кордами (або перемичками) тієї ж або більш високої категорії робочих характеристик.

Проектована мережа буде поділена на сегменти, IP адреси яких, назви приміщень та робочих груп, VLANи зведено в таблиці 2.1 та таблиці 2.2.

Таблиця 2.1 – Логічна адресація в мережі

Позначення вузлів	Робоча група/ Кількість вузлів		Назва кабінету	Номер VLAN	Адреса підмережі/ Маска
1	2	3	4	5	6
WS_1--WS_11	WORK	11	Офіс1	11	192.168.11.0/24
WS_13--WS_16		4			
WS_7--WS_12		6			
WS_12		1	керівник		
WS_17		1	каса		
S_1	serverna	1	серверна		192.168.0.0/24
SW_4		1			192.168.0.0/24
AP_1	WORK	1	Офіс1		192.168.0.0/24

Таблиця 2.2 - Таблиця конфігурування VLAN

№ п/п	Познач. вузла	Номер порту	Тип порту	Назва мереж. пр-ю	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
2	SW_2	1	Access	SW_1	16	Access	11
4		2	Access	SW_2	16	Access	11
5		4	Access	WS_17	ethernet	Access	11
6		6	Access	AP_1	wan	Access	11
7		8	Access	S_1	ethernet	Access	11

2.2 Обґрунтування вибору обладнання для мережі

У комп'ютерній мережі для організації необхідно використати:

– два 12-16 портових комутаторів для робочих груп,

– один центральний керований комутатор,

– 1-у точки доступу.

Виберемо комутатори робочих груп.

Вибір цих комутаторів зосереджено серед трьох моделей, порівняльна характеристика яких наведена в таблиці 2.3.

Таблиця 2.3 – Порівняльна характеристика комутаторів

модель	NETGEAR GS116GE	TP-LINK TL-SG116E	Cudy GS1010PE
1	2	3	4
Вартість, грн	4 200	2 700	3 460
Керування	Некерований	Керований	Некерований
Порти	Gigabit Ethernet RJ-45	Gigabit Ethernet RJ-45	Gigabit Ethernet RJ-45
Кількість портів	16 x Gigabit Ethernet	16 x Gigabit Ethernet	10 x Gigabit Ethernet
Smart-управління	Немає	Є	Немає
Підтримка PoE	Немає	Немає	Є
Форм-фактор	Настільний	Настільний	Настільний
Гарантія, міс	12	24	12

Виходячи з таблиці 2.3, враховуючи співвідношення ціни до технічних характеристик пристрою для мережі вибрано комутатор TP-LINK TL-SG116E , зовнішній вигляд якого зображено на рисунку 2.6 [11]

Рисунок 2.6 – Зовнішній вигляд комутатора TP-LINK TL- SG116E

Також у комп'ютерній мережі передбачено використання керованого комутатора.

Також у комп'ютерній мережі передбачено використання головного комутатора. Проведемо вибір комутатора. В таблиці 2.4 приведені три моделі, котрі є зараз на ринку.

Таблиця 2.4 – Порівняльна характеристика керованих комутаторів

	Planet (GS-4210-24P2S)	Mikrotik Layer 3 CRS125 24G-1S-IN	ZyXEL (GS1900-24HP)
1	2	3	4
ціна	9 400 грн	7 530 грн	11 141 грн
Порти	Gigabit Ethernet, SFP, Консольний порт RJ-45	Gigabit Ethernet, SFP, Комбо-порти	Gigabit Ethernet, SFP, Комбо-порти
Вн пр здат-ність, Гбіт / сек	24 x Ethernet 10/100/1000 Мбіт/сек	24 x Ethernet 10/100/1000 Мбіт/сек	10/100/1000 Мбіт/сек

В якості головного комутатора використаємо рішення MikroTik CRS125 24G-1S-IN (див.рис. 2.7) Cloud Router Switch - це нова серія Smart Switch.

Він поєднує в собі найкращі функції повнофункціонального маршрутизатора та свіча Layer 3, який підтримує RouterOS.

Всі спеціальні параметри комутатора доступні в спеціальному меню "Перемикач", але, якщо потрібно, порти можуть бути вилучені з конфігурації комутатора та використовуватися для цілей маршрутизації.

Ідеальний SOHO шлюзовий маршрутизатор, комутатор, все в одному вікні: Ethernet, Fiber або 4G (з додатковим USB-модемом) шлюз з'єднання з Інтернетом Маршрутизатор RouterOS / брандмауер / VPN з пасивним охолодженням до двадцяти п'яти гігабітних портів (1xSFP та 24xRJ45)

Характеристика комутатора:

– Код продукту CRS125-24G-1S-IN

– Архітектура MIPSBE

– Процесор AR9344

– Кількість центральних процесорів 1

– Номінальна частота процесора 600 МГц

– Розміри 285x145x45мм

– Ліцензійний рівень 5

– Операційна система RouterOS

– Розмір ОЗП 128 Мб

– Розмір пам'яті 128 Мб

– Память типу NAND

– Тестована температура навколишнього середовища від -35С до + 65С

Рисунок 2.7 – Зовнішній вигляд комутатора MikroTik CRS125 24G-1S-IN

У мережі використовується безпровідна точка доступу.

На сучасному ринку представлено дуже багато моделей пристроїв різних виробників, але ми зупинили наш вибір на трьох моделях, порівняльна характеристика яких наведена в таблиці 2.5

Таблиця 2.5 – Порівняльна характеристика точок доступу

	TP-LINK TP-Link EAP115	TP-LINK EAP225	MikroTik RBCAPGI-5ACD2ND
Режим роботи	Бездротовий клієнт, Міст, Точка доступу	Точка доступу	Бездротовий клієнт, Точка доступу
Версія протокола Wi-Fi	802.11n, 802.11g, 802.11b	802.11n, 802.11g, 802.11b	802.11b, 802.11g 802.11n,
Швидкість	300 Мбит/с	867 Мбіт/с	300 Мбит/с
Частота работи Wi-Fi	2.4 ГГц	2.4 ГГц 5 ГГц	2.4 ГГц
Гарантія	24 місяця	12 місяців	12 місяців
Ціна, грн	1200 грн	3500 грн	3100 грн

Виходячи з таблиці 2.5, враховуючи співвідношення ціни до технічних характеристик пристрою для мережі вибрано безпровідну точку доступу MikroTik cAP (RBcAP2nD), зовнішній вигляд якої зображено на рисунку 2.8[12]

Рисунок 2.8 – Зовнішній вигляд безпровідної точки доступу MikroTik RBCAPGI-5ACD2ND

Дводіапазонна бездротова потужна точка доступу з робочою частотою 2.4/5 ГГц. Встановлюється на стіну чи стелю всередині приміщень. У розпорядженні користувача — два Gigabit Ethernet порти (один із виходом PoE).

На частоті 2.4 ГГц точка доступу підтримує стандарти Wi-Fi 802.11 b/g/n, а частоті 5 ГГц — 802.11 a/n/ac. Сукупна швидкість Wi-Fi сягає 1.167 Гбіт/с. Пристрій забезпечує все спрямованість сигналу на 360 градусів.

Точка доступу обладнана чотириядерним процесором IPQ-4018 з тактовою частотою 716 МГц та 128 МВ оперативної пам'яті. Посилення антени на частоті 2.4 ГГц становить 2 dBi, але в частоті 5 ГГц — 2.5 dBi за максимальної потужності радіомодуля обох частотах 26 dBm.

Попри те, що пристрій підтримує режим ретранслятора, два порти Ethernet дозволяють розширити мережу за допомогою кабелю, навіть якщо потрібне живлення по витій парі, оскільки cAP ac підтримує стандарт PoE

802.3af/at з напругою 17-57 V (PoE in) на першому порту та Passive PoE (PoE out) на другому порту.

Точка доступу працює під керуванням операційної системи MikroTik RouterOS 4, яка дозволяє розгортати бездротові мережі будь-якої конфігурації. Пристрій також підтримує апаратне прискорення IPsec, а також систему керування та контролю точками доступу MikroTik CAPsMAN, причому для роботи контролера не потрібні додаткові комп'ютер та сервер.

Пристрій постачається в комплекті з двома корпусами (круглим та квадратним), тому можна вибрати дизайн, який вам більше подобається. Це багатофункціональний пристрій з витонченим корпусом, який може стати ще непомітнішим при натисканні кнопки, що відключає звуки і світлодіоди. Її можна переналаштувати на запуск будь-якого скрипту RouterOS.

У комп’ютерній мережі передбачено використання серверного комп’ютера, призначення якого бути шлюзом в інтернет. Для цього компютера не потрібно потужного «заліза», то ж скористаємося послугами відомого інтернет магазину та оберемо свій сервер.

Я виберу для цього серверний пк ARTLINE Business T15v20 (показаний на рисунку 2.9)

Характеристики Сервер ARTLINE Business T15v20

Процесор Чотириядерний Intel Core i3-12100 (3.3 - 4.3 ГГц)

Материнська плата PRIME H670-PLUS D4

Тактова частота процесора 3.3 ГГц

Обсяг встановленої оперативної пам'яті 16 ГБ

Характеристики оперативної пам'яті 16 ГБ DDR4-3200 A-brand

Контролери SAS/SATA вбудовано в чипсет

Рівні RAID 0/1/5/10

Кількість ядер одного процесора 4

Блок живлення TUF 450 Вт 80+ Bronze

Кількість дискових накопичувачів в комплекті 2

Максимальна швидкість мережевої карти 2.5 Гбіт/с

Встановлене ПЗ Без ОС

Гарантія 38 місяців

Сокет LGA1700

Рисунок 2.9 – Зовнішній вигляд ARTLINE Business T15v20

Отже, ми обрали таке обладнання:

Комутатор робочих станцій TP-LINK TL- SG116E — 2700 грн

Керований комутатор MikroTik CRS125 24G-1S-IN – 7530 грн

Точка доступу MikroTik RBCAPGI-5ACD2ND — 3100 грн

Серверний ПК ARTLINE Business T15v20 — 29800 грн

2.3 Особливості монтажу мережі [13]

Найбільш серйозною проблемою при створенні СКС для роботи високошвидкісних додатків (категорія 3 і вище) є якість монтажу. За даними BICSI (Building Industry Consuling Service International) - міжнародної асоціації професіоналів телекомунікаційної промисловості, 80% всіх структурованих кабельних систем США, побудованих на компонентах категорії 5, не можуть бути кваліфіковані як системи категорії 5 внаслідок порушення правил монтажу.

Існують спеціальні вимоги і рекомендації по монтажу СКС, виконання яких гарантує збереження початкових робочих характеристик окремих компонентів, зібраних в лінії, канали і системи. Стандарти ISO / IEC 11801 та ANSI / TIA / EIA-568A встановлюють в якості вимог кілька основних правил монтажу, що передбачають методи і акуратність виконання з'єднання компонентів і організації кабельних потоків, які в значній мірі підвищують продуктивність системи і полегшують адміністрування встановлених кабельних систем.

Зменшенню спотворення переданого сигналу сприяють спеціальні методи підготовки кабелю і його параметрів завершення відповідно до інструкцій виробника, а також хороша організація кабельних потоків, розташування й монтажу телекомунікаційного устаткування, що обслуговує кабельну систему.

Ці правила особливо стосуються високопродуктивних кабелів, як мідних, так і волоконно-оптичних. Мідні кабелі особливо чутливі до зовнішніх аномалій. Наприклад, розвиток пари мідних провідників на величину, що перевищує максимально допустиму стандартами, негативно впливає на характеристики перехресних перешкод пари або пар. Порушення вимог до мінімального радіусу вигину кабелю також впливає на його робочі характеристики.

Зі збільшенням частоти передачі зростає ризик того, що неправильно змонтований кабель вплине на продуктивність системи. Якщо смуга частот менше 16 МГц, а швидкість передачі нижче 10 Мбіт / с (наприклад, 10BASE-T Ethernet), можна і не помітити, що технологія монтажу була порушена. Однак цей же кабель, який працює при ширині смуги мережі понад 50 МГц і швидкості передачі 100 Мбіт / с або вище, може функціонувати неправильно.

Загальний закон, який установлюють стандартами, говорить: змонтована кабельна система UTP класифікується відповідно до найгіршими робочими характеристиками компонента лінії.

Нижче перераховані ті основні правила, яких необхідно дотримуватися при монтажі СКС для забезпечення їх функціонування на рівні вимог стандартів. Правила розділені по групах найтиповіших монтажних об'єктів.

Неекранований кабель

Щоб уникнути розтягування кабелю під час монтажу сила натягу не повинна перевищувати 110 Н для 4-парних кабелів калібру 24 AWG (0,5 мм). При монтажі кабельних систем в складних умовах (усередині або між будівлями), при протяжності безперервного кондуїту більше 30 м або сумі кутів поворотів при протягуванні, що перевищує 180 градусів, рекомендується застосовувати динамометр, що дозволяє контролювати натяг кабелю з метою залишитися в межах специфікацій виробника.

Вище наведені лише загальні рекомендації по максимальній силі натягу 4-парного кабелю. На практиці слід дотримуватися обмеження по максимальному натягу, певні виробником конкретного виду кабелю.

Радіуси вигину встановлених кабелів не повинні бути менше наступних значень: 4 зовнішніх діаметра кабелю для горизонтальних кабелів DTP і 10 зовнішніх діаметрів кабелю для багатопарних магістральних кабелів UTP. Необхідність підтримки невеликих радіусів вигину кабелю обумовлена тим, що при різких вигинах пари всередині кабелю деформуються і порушується

однорідність збалансованої симетричною середовища передачі. Подальше випрямлення вигину може не тільки не відновити, але і погіршити форму пари.

Забороняється розміщувати кабелі в ті канали, кабінети, корпуси та інші монтажні пристрої, у яких радіуси заокруглень або країв не відповідають вимогам виробників кабелів до радіусу їх вигину.

До запобіжних заходів, дотримуваним при монтажі та організації кабельних потоків, відноситься запобігання різних механічних напружень в кабелі, що викликаються натягом, різкими вигинами і надмірним стяганням пучків кабелю.

Слід уникати негативних впливів на кабель, що викликаються: його перекручуванням під час протягування або монтажу, розтягуванням кабельних пучків під дією власної ваги на кабельних підвісках, туго затягнутими кабельними хомутами, різкими вигинами кабелю.

Групуючи і пов'язуючи вільні кабелі необхідно стежити, щоб вони не були перетягнуті, і використовувати спеціальні м'які кабельні хомути.

Забороняється кріпити кабелі металевими скобами, їх слід встановлювати в трасах і просторах, що забезпечують захист від погодних умов та інших небезпечних факторів навколишнього середовища.

У кабельному елементі величина розкручування пар на комутаційному обладнанні повинна бути якомога менше. Видаляти оболонку кабелю слід лише на стільки, скільки потрібно для зручності параметрів завершення.

Для ліній з компонентами категорії 4 рекомендується, щоб розкручення пари не перевищувало 25 мм, а для ліній з компонентами категорії 5 -13 мм.

Дотримання наведених рекомендацій має мінімізувати вплив параметрів завершення на робочі характеристики. Збереження цілісності пар якомога ближче до місця забезпечує мінімальний вплив сигналів один на одного. Розкручені під час монтажу кабельні пари не слід скручувати знову.

Правильне скручування контролюється виробником кабелю, неправильне може негативно вплинути на робочі характеристики.

У полях параметрів завершення, які потребують частого доступу (наприклад, кросах, використовуваних для змін в мережі) можна користуватися патч-кордами і патч-панелями з приєднаними коннекторами, які в комбінації відповідають вимогам до даної категорії. Застосування пасивне для переміщень і змін може зменшити відхилення робочих характеристик, що виникають в результаті недбалих або неправильних методів монтажу кабельних компонентів в польових умовах.

Компанія-монтажник повинна дотримуватися вимог до радіусів вигину і зусиллям на розтягнення для кабелів UTP і волоконно-оптичних кабелів під час підготовки і в ході монтажу.

Кабельні траси повинні монтуватися або вибиратися таким чином, щоб мінімальний радіус вигину кабелю відповідав вимогам його виготовлювача, як під час, так і після його прокладки. Кабелі повинні підтримуватися за допомогою пристосувань, спроектованих спеціально для цих цілей і встановлених незалежно від інших структурних компонентів.

При каблировании в місцях з підвісними або фальш-стелями кошти кріплення кабелю повинні бути структурно незалежними від елементів підвісної стелі, його арматури або засобів кріплення. Елементи кріплення кабелю повинні бути розташовані з інтервалами 1,2 - 1,5 м.

Засоби підтримки кабелю - хомути, кільця і гачки - повинні розташовуватися один від одного на відстані не більше 1,5 м.

Кабельні траси, приміщення і мідні кабелі, що проходять паралельно з флуоресцентними лампами, повинні монтуватися з мінімальним зазором в 127 мм від флуоресцентних ламп.

У разі, якщо до внутрістіновим просторів є вільний доступ, компанія-монтажник повинна прокладати кабельні сегменти всередині стін. Якщо ж до-

ступ до стін утруднений, слід знайти інший метод прокладки, наприклад, з використанням металевого кондуїту або поверхневих систем розподілу.

У телекомунікаційному шафі, в місцях використання кабельних лотків і стійок, групи горизонтального кабелю укладаються за допомогою кольорових кабельних хомутів.

Апаратні стійки і шафи повинні мати достатні проходи спереду, ззаду і збоку для доступу до кабелів. Вільно стоять апаратні стійки і кабінети повинні мати проходи для доступу, вимірювані від вертикальних опор / рами кабінету: односторонні проходи - спереду і ззаду по 1 м (окремі стійки або ряди). Повинні бути виконані мінімальні вимоги до проходів відповідних нормативів та інструкцій, більш жорсткі, ніж зазначені вище.

Такі проходи забезпечують доступ до обладнання для його обслуговування, а також простір для організації кабельних потоків. Ряди стійок, розташовані послідовно, повинні мати по одному проходу з кожного боку, а розташовані паралельно один одному, можуть мати спільні проходи.

Особливу увагу слід приділяти заповнення кабельних каналів і дотримання інструкцій виробників каналів. Занадто велика кількість кабелів в каналі може привести до зайвого тиску на розташовані нижче кабелі. Кабелі, прокладені в каналах кабінетах і т. П., Що мають спеціально спроектовані обмежувачі радіуса вигину, схильні до "пролежнів" через неправильне проектування радіусів вигину і завантаження трас. "Пролежні" з часом можуть призвести до утворення перегинів, що виникають під тиском, що лежать нагорі кабелів.

Система заземлення

Стандарт СКС вимагає дотримання правил безпеки, пов'язаних із заземленням екранів кабелів і інших металевих компонентів кабельних систем. З'єднання повинні виконуватися відповідно до вимог електричних нормативів.

Екрани всіх кабелів повинні бути заземлені в телекомунікаційій шафі. Шлях до "землі" повинен бути постійним і безперервним.

2.4 Тестування мережі

Відсутність помилок на канальному рівні ще не гарантує, що інформація у вашій мережі не спотворюється.

Вплив помилок канального рівня на роботу мережі сильно перебільшено. Наслідком помилок нижнього рівня є повторна передача кадрів. Завдяки високій швидкості мережі Ethernet (особливо Fast Ethernet) і високої продуктивності сучасних комп'ютерів, помилки нижнього рівня не істотно впливають на час реакції прикладного ПЗ.

Випадки, коли ліквідація лише помилок нижніх (канального та фізичного) рівнів мережі дозволяла суттєво покращити час реакції прикладного програмного забезпечення. Здебільшого проблеми пов'язані з серйозними дефектами кабельної системи мережі.

Значно більший вплив на роботу прикладного ПЗ в мережі мають такі помилки, як безслідне зникнення або спотворення інформації в мережевих платах, маршрутизаторах або комутаторах за повної відсутності інформації про помилки нижніх рівнів. Ми вживаємо слово " інформація " , оскільки у момент спотворення дані ще оформлені як кадр.

Причина таких дефектів у наступному. Інформація спотворюється (або зникає) "в нетрях" активного обладнання - мережної плати, маршрутизатора або комутатора. При цьому приймально-передавальний блок цього обладнання обчислює правильну контрольну послідовність (CRC) вже спотвореної раніше інформації, і коректно оформлений кадр передається по мережі. Жодних помилок у цьому випадку, природно, не фіксується. SNMP-агенти, вбудовані у активне обладнання, тут нічим допомогти не можуть.

Іноді, крім спотворення, спостерігається зникнення інформації. Найчастіше воно відбувається на дешевих мережних платах або комутаторах Ethernet-FDDI. Механізм зникнення інформації у разі зрозумілий. У ряді комутаторів Ethernet-FDDI зворотний зв'язок швидкого порту з повільним (або навпаки) відсутній, в результаті інший порт не отримує інформації про перевантаження вхідних/вихідних буферів швидкого (повільного) порту. В цьому випадку при інтенсивному трафіку інформація на одному з портів може зникнути.

Досвідчений адміністратор мережі може заперечити, що крім захисту інформації на канальному рівні в протоколах IPX та TCP/IP можливий захист інформації за допомогою контрольної суми.

Повною мірою на захист за допомогою контрольної суми можна покладатися, тільки якщо прикладне програмне забезпечення як транспортний протокол задіює TCP або UDP. Тільки за їх використання контрольною сумою захищається весь пакет. Якщо як "транспорт" застосовується IPX/SPX або безпосередньо IP, то контрольною сумою захищається лише заголовок пакета.

Навіть за наявності захисту з допомогою контрольної суми описане спотворення чи зникнення інформації викликає значне збільшення часу реакції прикладного ПЗ.

Якщо ж захист не встановлено, то поведінка прикладного програмного забезпечення може бути непередбачуваною.

Крім заміни (відключення) підозрілого обладнання, виявити такі дефекти можна двома способами.

Перший спосіб полягає у захопленні, декодуванні та аналізі кадрів від підозрілої станції, маршрутизатора або комутатора. Ознакою описаного дефекту є повторна передача пакета IP або IPX, якій не передує помилка нижнього рівня мережі. Деякі аналізатори протоколів та експертні системи полегшують завдання, виконуючи аналіз траси або самостійно обчислюючи контрольну суму пакетів.

Другим способом є метод стресового тестування мережі.

Висновки. Основне завдання діагностики канального рівня мережі – виявити наявність підвищеного числа колізій та помилок у мережі та знайти взаємозв'язок між числом помилок, ступенем завантаженості каналу зв'язку, топологією мережі та місцем підключення вимірювального приладу. Усі виміри слід проводити на тлі генерації аналізатором протоколів власного трафіку.

Якщо встановлено, що підвищена кількість помилок та колізій не є наслідком перевантаженості каналу зв'язку, то мережне обладнання, під час якого спостерігається підвищена кількість помилок, слід замінити.

Якщо не вдається виявити взаємозв'язку між роботою конкретного обладнання та появою помилок, то проведіть комплексне тестування кабельної системи, перевірте рівень шуму в кабелі, топологію ліній заземлення комп'ютерів, якість напруги живлення.

Які параметри слід відстежувати під час діагностики мережі? Методика попереджувальної діагностики мережі

Методика попереджувальної діагностики ось у чому. Адміністратор мережі повинен безперервно або протягом тривалого часу спостерігати за роботою мережі. Такі спостереження бажано проводити з моменту встановлення. На підставі цих спостережень адміністратор повинен визначити, по-перше, як значення параметрів, що спостерігаються, впливають на роботу користувачів мережі і, по-друге, як вони змінюються протягом тривалого проміжку часу: робочого дня, тижня, місяця, кварталу, року і т. д. .

Спостережуваними параметрами зазвичай є:

– параметри роботи каналу зв'язку мережі - утилізація каналу зв'язку, кількість прийнятих та переданих кожною станцією мережі кадрів, кількість помилок у мережі, кількість широкомовних та багатоадресних кадрів тощо;

– параметри роботи сервера - утилізація процесора сервера, кількість відкладених запитів до диска, загальна кількість кеш-буферів, кількість "брудних" кеш-буферів і т.п.

Знаючи залежність між часом реакції прикладного ПЗ і значеннями параметрів, що спостерігаються, адміністратор мережі повинен визначити максимальні значення параметрів, допустимі для цієї мережі. Ці значення вводяться як порогів (thresholds) в діагностичний засіб. Якщо в процесі експлуатації мережі значення параметрів, що спостерігаються, перевищать порогові, то діагностичний засіб проінформує про цю подію адміністратора мережі. Така ситуація свідчить про наявність у мережі проблеми.

Спостерігаючи досить довго за роботою каналу зв'язку та сервера, можна встановити тенденцію зміни значень різних параметрів роботи мережі (утилізації ресурсів, числа помилок тощо). На підставі таких спостережень адміністратор може зробити висновки щодо необхідності заміни активного обладнання або зміни архітектури мережі.

У разі появи в мережі проблеми адміністратор в момент її прояву повинен записати в спеціальний буфер або файл дамп канальної траси і на підставі аналізу її вмісту зробити висновки про можливі причини проблеми.

2.5 Захист комп’ютерної мережі [14]

Безпека мережі — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу. Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів. Мережева безпека включає в себе дозвіл на доступ

до даних в мережі, який надається адміністратором мережі. Користувачі вибирають або їм призначаються ID і пароль або інші перевірки автентичності інформації, що дозволяє їм здійснити доступ до інформації і програм у рамках своїх повноважень. Мережева безпека охоплює різні комп'ютерні мережі, як державні, так і приватні, які використовуються в повсякденних робочих місцях для здійснення угод і зв'язків між підприємствами, державними установами та приватними особами. Мережі можуть бути приватними, такими як всередині компанії або відкритими, для публічного доступу. Мережева безпека бере участь в організаціях, підприємствах та інших типів закладів. Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю.

Мережева безпека починається з аутентифікації, що зазвичай включає в себе ім'я користувача і пароль. Коли для цього потрібно тільки одна деталь аутентифікації (ім'я користувача), то це називають однофакторною аутентифікацією. При двофакторній аутентифікації, користувач ще повинен використати маркер безпеки або 'ключ', кредитну картку або мобільний телефон, при трьохфакторній аутентифікації, користувач повинен застосувати відбитки пальців або пройти сканування сітківки ока.

Після перевірки дійсності, брандмауер забезпечує доступ до послуг користувачам мережі. Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень (IPS).

Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб зберегти конфіденційніст.

Система безпеки мережі не ґрунтується на одному методі, а використовує комплекс засобів захисту. Навіть якщо частина обладнання виходить з ладу, решта продовжує захищати дані Вашої компанії від можливих атак.

Встановлення рівнів безпеки мережі надає Вам можливість доступу до цінної ділової інформації з будь-якого місця, де є доступ до мережі Інтернет, а також захищає її від загроз.

Система безпеки мережі:

Захищає від внутрішніх та зовнішніх мережних атак. Небезпека, що загрожує підприємству, може мати як внутрішнє, так і зовнішнє походження. Ефективна система безпеки стежить за активністю в мережі, сигналізує про аномалії та реагує відповідним чином.

Забезпечує конфіденційність обміну інформацією з будь-якого місця та в будь-який час. Працівники можуть увійти до мережі, працюючи вдома або в дорозі, та бути впевненими у захисті передачі інформації.

Контролює доступ до інформації, ідентифікуючи користувачів та їхні системи. Ви маєте можливість встановлювати власні правила доступу до даних. Доступ може надаватися залежно від ідентифікаційної інформації користувача, робочих функцій, а також за іншими важливими критеріями.

Забезпечує надійність системи. Технології безпеки дозволяють системі запобігти як вже відомим атакам, так і новим небезпечним вторгненням. Працівники, замовники та ділові партнери можуть бути впевненими у надійному захисті їхньої інформації.

Засоби захисту комп’ютерних мереж:

Брандмауери. Централізовані брандмауери та брандмауери окремих комп’ютерів можуть запобігати проникненню зловмисного мережного трафіку до мережі, яка підтримує діяльність компанії.

Антивірусні засоби. Більш захищена мережа може виявляти загрози, що створюють віруси, хробаки та інше зловмисне програмне забезпечення, і боротися з ним попереджувальними методами, перш ніж вони зможуть заподіяти шкоду.

Знаряддя, які відстежують стан мережі, грають важливу роль під час визначення мережних загроз.

Захищений віддалений доступ і обмін даними. Безпечний доступ для всіх типів клієнтів із використанням різноманітних механізмів доступу грає важливу роль для забезпечення доступу користувачів до потрібних даних, незалежно від їх місце знаходження та використовуваних пристроїв.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкція по установці Ubuntu 20.04 сервер

Для установки Ubuntu 20.04 LTS Сервера качаємо образ на сторінці офіційного сайту, записуємо скачаний образ дистрибутива на USB і завантажується з нього.

– У першому вікні, вибираємо мову установки.

– На наступному етапі буде запропоновано використовувати дійсний інсталятор, або оновити його. Оновлення відбувається у фоновому режимі і займає не більше 10 секунд, поновіть його:

Виберіть розкладку клавіатури.

Вибираємо мову розкладки:

Налаштуйте мережу. За замовчуванням, отримання IP адреси налаштоване по DHCP. У нашому прикладі ми будемо використовувати статичний IP адрес. Використовуючи інтуїтивно зрозумілу навігацію, заповніть необхідні поля

Якщо доступ в інтернет у вас здійснюється через proxy-сервер, вкажіть його:Вказівка проксі-сервера

Далі, установник запропонуємо вам найближче дзеркало (Mirror), виходячи з вашого регіонального розташування. Залиште запропоноване за замовчуванням, або вкажіть свій.

На цьому етапі буде запропоновано розмітити дисковий простір. Вибравши «Use an entire disk» установник сам розмітить диски в автоматичному режимі. Залежно від завдань, ви можете виконати розбивку розділів на власний розсуд, вибравши «Custom storage layout»:

Наступний приклад для наочності, виносити розділ boot окремо немає необхідності, ви можете все віддати під корінь «/», що буде рівнозначно «Use

an entire disk». Ви можете зробити окремим розділом boot або swap, вибрати формат файлової системи. Так само є можливість створення LVM розділів. Меню інтуїтивно зрозуміле:

Вкажіть ім'я сервера і призначені для користувача дані для доступу до сервера. Ви можете вибрати будь-якого користувача крім «root» і «admin», які зарезервовані системою. Так само придумайте складний пароль, він повинен бути не менше 10 символів, включати в себе малі і великі символи латинського алфавіту, а так само цифри і спецсимволи.

Установка призначених для користувача даних

Відзначте установку OpenSSH Server, для можливості віддаленого підключення до нього, і натисніть «Done»:

Перед вами з'явиться довгий список того що можна встановити «з коробки». Дуже цікавий етап, тут доступна і інтеграція з Kubernetes 1.18, etcd, інтеграція з Google Cloud, Postgresql10, Prometheus і багато чого іншого. Вибирати компоненти для установки потрібно усвідомлено, за умови, що вам це дійсно необхідно для задач.По закінченню установки, внизу інтерактивної консолі з'явиться «Reboot». Вийміть носій з монтажником і виконайте перезавантаження сервера.

Первісне перезавантаження займе більш тривалий час, ніж це буде в подальшому. Будуть ініційовані служби snapd, виконається ініціалізація пристроїв cloud-init та інше. Все залежить від того, яким чином встановлюється Ubuntu, на гіпервізора, або baremetall. По закінченню ви побачите вікно аутентифікації в систему. Так само, сервер буде доступний по ssh.

Налаштування сервера

При підключенні, встановіть мінімальний набір утиліт, які знадобляться для роботи:

root @ GAL: ~ # apt-get update

root @ GAL: ~ # apt-get install atop wget ntp vim net-tools -y

Підключення до сервера по ssh

Перше, на що варто звернути увагу, це те, що в Ubuntu користувач root відключений від аутентифікації. Це виконано з точки зору безпеки. Підключення до сервера відбувається по імені користувача, який вказаний при установці:

admt @ freehost: ~ $ ssh user@178.20.152.78

user@178.20.152.78's password:

Щоб потрапити в режим суперкористувача, введіть наступну команду, яка проситиме пароль користувача user і перемкне в суперкористувача:

user @ GAL: ~ # sudo su

[Sudo] password for user: **********

root @ GAL: / home / user #

Якщо з якихось причин ви хочете дозволити доступ користувача root при підключенні по ssh, то змініть для нього пароль:

root @ GAL: ~ # passwd root

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

root @ GAL: ~ #

Потім в конфігураційному файлі / etc / ssh / sshd_config розкоментуйте рядок PermitRootLogin вказавши значення yes:

PermitRootLogin yes

Однак, з метою безпеки сервера, доступ за логіном root краще не надавати.

Налаштування мережевих інтерфейсів

Починаючи з Ubuntu 18.04 налаштування мережевих інтерфейсів відбувається не в звичному каталозі / etc / network / interfaces як це реалізовано в Debian-подібних дистрибутивах, а в каталозі / etc / netplan /. Після установки ОС, в ньому буде згенеровано конфігураційний файл 00-installer-config.yaml

Якщо конфігураційний файл з якоїсь причини порожній, згенеруйте го:

root @ GAL: ~ # netplan generate

Для прикладу, виконаємо з ним деякі операції. Перейменуємо його у більш зручний вид:

root @ GAL: ~ # mv /etc/netplan/00-installer-config.yaml /etc/netplan/01-netcfg.yaml

Застосувати налаштування:

root @ GAL: ~ # netplan apply

Конфігураційний файл має наступний вигляд:

файл конфігурацій

Він має формат Html і чутливий регістру. При конфігурації файлів даного формату табуляція неприпустима. Тільки парна послідовність пробілів і структура успадкування директив, інакше, ви отримаєте синтаксичну помилку.

У нашому прикладі, мережевий інтерфейс має назву eth0, але при інсталяції Ubuntu він мав назву enp0s8. Перейменувати в конфіг мережевий інтерфейс недостатньо. Так само слід правити завантажувач grub:

root @ GAL: ~ # mcedit / etc / default / grub

знайдіть і відредагуйте значення:

GRUB_CMDLINE_LINUX = "net.ifnames = 0 biosdevname = 0"

root @ GAL: ~ # grub-mkconfig -o /boot/grub/grub.cfg

root @ GAL: ~ # reboot

Видалення непотрібних компонентів

root @ GAL: ~ # echo 'datasource_list: [None]' | sudo -s tee /etc/cloud/ cloud.cfg.d/90_dpkg.cfg

root @ GAL: ~ # apt-get purge cloud-init -y

root @ GAL: ~ # rm -rf / etc / cloud /

root @ GAL: ~ # rm -rf / var / lib / cloud /

Пакетний менеджер snap

Давайте так само, командою lsblk відобразимо наші носії пам'яті:

Відображення дискових пристроїв

Починаючи з версії 16.04, Ubuntu все наполегливіше намагається просунути менеджер управління пакетами snap. Наведемо коротке пояснення з офіційного сайту розробників:

«Snap пакети Ubuntu містять саму програму, а також всі її залежності. Це має кілька переваг перед звичайними deb або rpm пакетами, обробними залежності. А головне, з них - розробник може бути впевнений що немає ніяких регрессий через зміни версій бібліотек в системі »

Snap це зручна річ, і ми рекомендуємо з ним ознайомитися, документація Ubuntu досить інформативна як на російськомовних, так і на англомовних ресурсах.

Відобразимо список встановлених пакетів, які встановилися при інсталяції:

root @ GAL: ~ # snap list

Якщо нам щось не потрібно, видалимо:

root @ GAL: ~ # snap remove lxd

root @ GAL: ~ # snap remove core18

Додати пакет можна наступним чином:

root @ GAL: ~ # snap install docker

Оновити всі пакети:root @ GAL: ~ # snap refresh

Оновити певний пакет:

root @ GAL: ~ # snap refresh docker

Подивитися список доступних пакетів:

root @ GAL: ~ # snap changes

Замість snap можете використовувати пакетний менеджер apt. Якщо у вас snapd не встановлено, встановити його можна в такий спосіб:

root @ GAL: ~ # apt install snapd

Підключення swap розділу і настройка кешування

Для початку переконайтеся, що він не підключений:

root @ GAL: ~ # swapon —show

Якщо список порожній, створіть файл підкачки, наприклад 2Gb. Змініть права, і активуйте його. Порядок команд наступний:

root @ GAL: ~ # fallocate -l 2G / swapfile

root @ GAL: ~ # sudo chmod 600 / swapfile

root @ GAL: ~ # mkswap / swapfile

root @ GAL: ~ # swapon / swapfile

Перевірка результату:

root @ GAL: ~ # swapon -show

root @ GAL: ~ # free -h

Налаштуємо swappiness. Параметр vm.swappiness за замовчуванням має значення 60, і контролює відсоток вільної пам'яті. Він контролює значення, після якого почнеться активний скидання даних в swap. Значення «60» означає наступне: 100-60 = 40%. Іншими словами, при завантаженні ОЗУ більш ніж

40%, дані почнуть кешedfnbcz в swap. Не існує оптимального значення, він обумовлений тільки конфігурацією вашого сервера. Якщо ОЗУ досить, це значення можна зменшити наступними командами:

root @ GAL: ~ # sysctl vm.swappiness = 10

В кінці файлу /etc/sysctl.conf додайте наступний рядок:

vm.swappiness = 10

Налаштуйте кешування. Змініть параметр vfs_cache_pressure, що відповідає за швидкість видалення індексів з кеша. За замовчуванням це значення дорівнює 100. Так як звернення до індексів задоволене часте, це значення ви можете зменшити:

root @ GAL: ~ # sysctl vm.vfs_cache_pressure = 50

В кінці файлу /etc/sysctl.conf додайте наступний рядок:

vm.vfs_cache_pressure = 50

Опціонально, не буде зайвим видалити підтримку IPv6. Навіть якщо ви цей протокол не використовуєте, деяке програмне забезпечення все одно його прослуховує і іноді трапляються збої в його роботі:

root @ GAL: ~ # sh -c 'echo 1> / proc / sys / net / ipv6 / conf / all / disable_ipv6'

В кінці файлу /etc/sysctl.conf додайте наступний рядок, в залежності від інтерфейсів:

Відключення на всіх інтерфейсах

net.ipv6.conf.all.disable_ipv6 = 1

Відключення на певному інтерфейсі

net.ipv6.conf.eth0.disable_ipv6 = 1

Примітка: При написанні даного пункту використовувалися інструкції з мережі Інтернет.

3.2 Інструкція з налаштування проксі-сервера Squid [15]

Механізми управління доступом в Squid дозволяють гнучко реалізовувати політику доступу до інтернет-ресурсів, грунтуючись на тимчасових інтервалах, інформації про кешування, доступу до певних сайтів і т.д. Управління доступом в Squid грунтується на двох різних компонентах: ACL-елементах і списках доступу (access list). Список доступу фактично дозволяє або забороняє доступ до сервісу.

Деякі найважливіші типи ACL-елементів перераховані нижче

src: Джерело, тобто IP-адреса клієнта;

dst: Приймач, тобто IP-адреса серверу;

srcdomain: Джерело, тобто доменне ім'я клієнта;

dstdomain: Приймач, тобто доменне ім'я серверу;

time: Час дня і день тижня;

url_regex: Регулярний вираз для перевірки відповідності URL;

urlpath_regex: Регулярний вираз для перевірки відповідності URL-шляху разом з назвою протоколу і ім'ям хоста;

proxy auth: Перевірка автентичності користувача за допомогою зовнішнього процесу;

maxconn: Максимальна кількість з'єднань на одну клієнтську IP-адресу.

Щоб застосувати, треба визначити набір ACL і застосувати до них правила. Формат ACL-виразів:

aci acl_element_name type_of_acl_element values_to_acl

Зауваження:

acl_element_name може бути любим ім'ям, призначеним користувачем ACL елементу.

Два ACL не можуть мати одинакових імені;

Будь-який ACL складається із списку значень. При перевірці на відповідність декільком значенням використовується АБО-логика. Іншими словами, ACL елемент відповідає, коли знайдена відповідність хоча б для одного із значень.

Не всі ACL елементи можуть використовуватися із списками доступу всіх типів.

Різні ACL елементи, розташовані на різних рядках, групуються squid'ом в єдиний список;

Доступні декілька різних типів списків доступу. Ті які ми збираємося використовувати приведені нижче:

http access: Дозволяє HTTP-клієнтам здійснювати доступ на HTTP-порт. Це основний список управління доступом.

no_cache: Визначає кешування відповідей на запити.

Зауваження:

Правила перевіряються в тому порядку, в якому вони записані; перевірка уривається, як тільки знайдена відповідність одному з правил;

Список доступу може складатися з декількох правил;

Якщо не була знайдена відповідність жодному з правил, то виконується дія за умовчанням, протилежне останньому правилу в списку. Дію за умовчанням краще указувати явно;

Над всіма елементами в списку доступу виконується операція І (AND), а декілька виразів http_acess об'єднуються операцією АБО (OR);

http_access Action statement 1 AND statement2 AND statement OR http_access Action statement3;

Правила завжди читаються від низу до верху.

Управління доступом до Інтернет

Різноманітні механізми і правила управління доступом пропонують дуже хороший і гнучкий шлях контролю клієнтського доступу до Інтернет. Приклади настройок, що часто використовуються, приведені нижче; у жодному випадку не можна обмежуватися тільки цими настройками.

1. Дозволити доступ до Інтернет вибраним машинам

aci allowed_clients src 192.168.0.10 192.168.0.20 192.168.0.30

http_access allow allowed_clients

http_access deny !allowed clients

Тут дозволений доступ до Інтернет машинам з IP-адресами 192.168.0.10, 192.168.0.20 і 192.168.0.30, а всім іншим (в списку їх немає) - заборонений.

Обмежити доступ певним часом:

aci allowed_clients src 192.168.0.1/255.255.255.0

aci regular_days time MTWHF 10:00-16:00

http_access allow allowed_clients regular_days

http_access deny allowed_clients

Тут доступ надається всім машинам мережі 192.168.0.1 протягом часу з понеділка по п'ятницю з 10:00 ранку до 4:00 дня.

Доступ в різний час для різних клієнтів

aci host1 src 192.168.0.10

aci host2 src 192.168.0.20

aci host3 src 192.168.0.30

acl morning time 10:00-13:00

acl lunch time 13:30-14:30

acl evening time 15:00-18:00

http_access allow host1 morning

http_access allow host1 evening

http_access allow host2 lunch

http_access allow host3 evening

http_access deny all

Вищенаведені правила дозволяють доступ комп'ютеру hostl ранком (з 10:00 до 13:00) і увечері (з 15:00 до 18:00), а комп'ютерам host2 і host3 після обіду (з 13:30 до 14:30) і увечері відповідно (з 15:00 до 18:00).

Всі елементи запису доступу об'єднуються операцією I (AND) і виконуються таким чином:

http_access Action statement1 AND statement2 AND statement OR.

Множинні оголошення http_access об’єднуються операцією АБО (OR), а елементи доступу в них об'єднуються операцією I. У зв'язку з цим рядок http_access allow host1 morning evening ніколи не спрацює, оскільки виразів morning AND evening ніколи не буде істинним (ранок і вечір ніколи не перетинаються), і, отже, ніяких дій не буде.

Блокування сайтів

Squid може запобігти доступу до певних сайтів або сайтів, адреса яких містить певне слово. Це може бути реалізовано таким чином:

aci allowed_clients src 192.168.0.1/255.255.255.0

aci banned_sites url_regex abc.com *()(*.com

http_access deny banned_sites

http_access allow allowed_clients

Аналогічним чином можна заборонити доступ до сайтів, адреса яких містить визначене слів, наприклад dummy і fake

aci allowed_clients src 192.168.0.1/255.255.255.0

aci banned_sites url_regex dummy fake

http_access deny banned_sites

http_access allow allowed_machines

acl allowed_clients src 192.168.0.1/255.255.255.0

acl banned_sites url_regex "/etc/banned.list"

http_access deny banned_sites

http_access allow allowed_clients

Оптимізація

Squid може обмежувати максимальну кількість з'єднань за допомогою елемента maxconn.

Для використовування цієї можливості, повинна бути включена підтримка client db.

acl mynetwork 192.168.0.1/255.255.255.0

acl numconn maxconn 5

http_access deny mynetwork numconn

Зауваження: ACL maxconn використовує порівняння "менше-чим". ACL спрацьовує, якщо кількість з'єднань більше заданого значення. Тому maxconn і не указується в списку http_access.

Кешування

Відповіді на запити кешуються і це добре для статичних сторінок. Немає ніякої потреби кешувати cgi-сторінки або сервлети.

Цьому можна запобігти використовуванням ACL-елемента no_cache.

acl cache_preventl url_regex cgi-bin /?

acl cache_prevent2 url_regex Servlet

no_cache_deny cache_preventl

no_cache_deny cache_prevent2

Створення власних повідомлень про помилки

Можна створити свої власні повідомлення про помилки доступу за допомогою опції deny_info. Всі повідомлення про помилки Squid за умовчанням зберігаються в каталозі /etc/squid/errors.

Каталог з файлами повідомлень про помилки може бути змінений за допомогою error_directory.

Можна навіть змінити самі повідомлення.

acl allowed_clients src 192.168.0.1/255.255.255.0

acl banned_sites url_regex abc.com *()(*.com

http_access deny banned_sites

deny_info ERRBANNEDSITE banned_sites

http_access allow allowed_clients

У вищенаведеному прикладі спеціальне повідомлення відображається як тільки користувач намагається дістати доступ до сайту, що містить в назві заборонене слово. Файл з ім'ям ERRBANNEDSITE повинен знаходиться у вищенаведеному каталозі помилок. Повідомлення про помилку повинне бути в HTML-форматі. Всі розглянуті приклади, демонструють лише невелику частину реальних можливостей ACL. Пояснення призначення ACL-елементів і елементів доступу, необхідне для більш серйозного їх використовування можна знайти в FAQ на домашній сторінці Squid.

3.3 Налаштування головного комутатора

Підключитися через Winbox до роутера. Для цього підключаємо кабель в один з портів маршрутизатора (крім першого). Запускаємо Winbox. Далі необхідно вибрати вкладку Neighbors;

Клікнути Connect.

Налаштування локальної мережі MikroTik.

Налаштування портів в режим світча. Виконаємо об'єднання портів MikroTik ether2 - ether5 в світч:

Вибираємо подвійним клацанням миші інтерфейс ether3;

У списку Master Port вибираємо ether2 (головний порт світча);

Натискаємо кнопку ОК.

Цю операцію повторюємо для інтерфейсів ether4, ether5.

У підсумку навпроти портів ether3-ether5 повинна стояти буква S (Slave - ведений).

Призначення IP адреси локальної мережі

Налаштуємо IP адрес локальної мережі MikroTik:

Відкриваємо меню IP;

Вибираємо Addresses;

Натискаємо кнопку Add (червоний хрестик);

У полі Address вводимо адресу і маску локальної мережі, 192.168.11.1/24;

У списку Interface вибираємо bridge-local. Натискаємо кнопку ОК.

Налаштування DHCP сервера. Щоб комп'ютери чи точки доступу, під-ключені до роутера, отримували мережеві настройки автоматично, налаштує-мо DHCP сервер MikroTik:

Відкриваємо меню IP;

Вибираємо DHCP Server;

Натискаємо кнопку DHCP Setup;

У списку DHCP Server Interface вибираємо bridge-local

Натискаємо кнопку Next;

У цьому вікні вибирається мережу для DHCP. Ми залишаємо без змін і натискаємо кнопку Next;

У наступному вікні вказується адреса шлюзу. Натискаємо кнопку Next;

У цьому вікні прописується діапазон IP адрес, які роздаватиме DHCP сервер. Натискаємо кнопку Next;

Далі вводяться адреси DNS серверів. Натискаємо кнопку Next;

Тут задається час резервування IP адрес. Натискаємо кнопку Next;

Налаштування DHCP сервера успішно завершена. Тиснемо кнопку OK. Тепер мережевий кабель комп'ютера відключаємо від роутера і ще раз підключаємо до нього.

Налаштування Firewall і NAT

Щоб комп'ютери отримували доступ до інтернету, необхідно налаштувати Firewall і NAT на роутері MikroTik.

Відкрийте меню New Terminal для введення команд.

Налаштування NAT виконується наступними командами:

ip firewall nat add chain = srcnat out-interface = інтерфейс провайдера action = masquerade

Де інтерфейс провайдера - це інтерфейс, на який приходить інтернет від провайдера, наприклад ether1.

Protect router - команди для захисту роутера:

ip firewall filter add action = accept chain = input disabled = no protocol = icmp

ip firewall filter add action = accept chain = input connection-state = established disabled = no in-interface = інтерфейс провайдера

ip firewall filter add action = accept chain = input connection-state = related disabled = no in-interface = інтерфейс провайдера

ip firewall filter add action = drop chain = input disabled = no in-interface = інтерфейс провайдера

Protect LAN - захист внутрішньої мережі:

ip firewall filter add action = jump chain = forward disabled = no in-interface = інтерфейс провайдера jump-target = customer

ip firewall filter add action = accept chain = customer connection-state = established disabled = no

ip firewall filter add action = accept chain = customer connection-state = related disabled = no

ip firewall filter add action = drop chain = customer disabled = no

Призначаємо типи інтерфейсів для захисту внутрішньої мережі (external - зовнішній, internal - внутрішній LAN):

ip upnp interfaces add disabled = no interface = ether1 type = external

ip upnp interfaces add disabled = no interface = ether2 type = internal

ip upnp interfaces add disabled = no interface = ether3 type = internal

ip upnp interfaces add disabled = no interface = ether4 type = internal

ip upnp interfaces add disabled = no interface = ether5 type = internal

ip upnp interfaces add disabled = no interface = bridge-local type = internal

Ізоляція трафіку на MikroTik за допомогою VLAN

На перший порт роутера MikroTik приходить інтернет провайдера,

На другий порт підключено головний комутатор мережі,

Третій порт - резервний,

Четвертий та п’ятий порти використовуються для підключення точок доступу.

Зайдіть в налаштування MikroTik і відкрийте меню Interface. Тут з'являється п'ять мережевих портів ether1-ether5.

Перейдіть на вкладку VLAN і додайте необхідні VLAN інтерфейсів (див. табл. 2.1) :

vlan_11 з VLAN ID: 11 на порту ether2

vlan_0 з VLAN ID: 0 на порту ether2

Щоб трафік з VLAN інтерфейсів з номерами 0, 11 видавався до відповідних LAN порти, потрібно створити бридж інтерфейси і об'єднати в них відповідні VLAN і мережеві порти.

Спочатку створимо бридж інтерфейси:

Відкрийте меню Bridge і натисніть червоний плюсик;

В полі Name вкажіть назву бридж інтерфейсу, наприклад bridge_0. Натисніть кнопку OK; Додайте по аналогії інтерфейси bridge_11

Додавання портів в бриджі виконується наступним чином:

Перейдіть на вкладку Ports і натисніть червоний плюсик;

У списку Bridge виберіть ім'я бридж інтерфейсу bridge_0;

У списку Interface виберіть відповідний мережевий порт ether2; Натисніть OK;

Натисніть ще раз червоний плюсик для додавання VLAN інтерфейсу в bridge_0;

У списку Bridge виберіть ім'я бридж інтерфейсу bridge_0;

У списку Interface виберіть відповідний VLAN інтерфейс vlan_0;

Натисніть OK. Додайте по аналогії порти в бриджі bridge_11

Останнє що потрібно зробити, це налаштувати пересилання dns. Робиться це в меню IP (1) → DNS (2) В поле Servers вводимо надані провайдером IP address DNS серверів.

3.4 Налаштування точуи доступу

Налаштування WiFi на MikroTik

Для настройки WiFi на MikroTik необхідно зайти в меню Wireless;

Вибрати вкладку interface;

Вибрати бездротовий інтерфейс wlan1, клацнувши по ньому два рази лівою кнопкою миші. Відкриються основні настройки WI-FI; тут необхідно вибрати вкладку Wireless;

Включити розширений режим натиснувши кнопку Advance Mode;

Налаштувати ім'я мережі WiFI в поле SSID;

Вибрати в полі Frequency Mode — regulatory-domain;

В поле Country необхідно вибрати Ukraine.

В поле Adaptive Noise Immunity необхідно вибрати режим ap and client mode;

Натискаємо кнопку OK для застосування всіх змінених налаштувань.

Далі переходимо до налаштування security profiles (пароля) на Wi-Fi, для цього необхідно:

У Wireless Tables вибрати Security Profiles;

Зайти в налаштування профілю, клікнувши два рази лівою кнопкою миші;

У вкладці general, вибрати в полі mode-dynamic keys;

Authentication Types виставити значення WPA PSK і WPA2 PSK;

Виставити алгоритм шифрування aes com;

Ввести пароль на мережу WiFI в поле WPA Pre-Shared Key і WPA2 Pre-Shared Key. Застосувати всі налаштування кнопкою OK.

Налаштування мережевих інтерфейсів в MikroTik .

Перейдемо до налаштування мережевих параметрів провайдера на роутері мікротік.

Встановимо IP адресу на інтерфейс WAN, який відповідає значенню - ваш IP. Для цього необхідно зайти в меню IP → address → plus Введемо IP address в поле Address і виберем інтерфейс ether1 в полі Interface.

Далі необхідно налаштувати основний шлюз (gate). Робиться це в меню IP → Routes → plus.

У вікні необхідно ввести значення IP address вашого шлюзу в поле Gateway

3.5 Інструкція з використання тестових наборів та тестових програм

Для діагностики мережі використовуються команди PING і TRACERT.

Якщо є підозра, що відсутній зв'язок з деяким вузлом мережі, то команда PING (Packet Internet Groper)– перша, до якої необхідно звернутись. З допомогою цієї команди, можна перевірити правильність встановлення TCP/ IP-з'єднання на локальному (віддаленому) комп'ютері.

Основна функція цієї утиліти – перевірка наявності фізичного зв'язку між двома системами в мережі. Для обміну пакетами з віддаленою системою, використовується протокол ICMP. Віддалена система відсилає пакети назад, і таким чином, коло замикається. Команда PING видає інформацію про те, скільки часу виконувалась ця операція, а також повідомляє про помилки, якщо пакети не повернулись.

Синтаксис команди в операційних системах сімейства Windows має наступний вигляд:

ping [ключі] адреса (ім'я) вузла

Ключі:

– t – продовжує відправку запитів , доки робота не буде перервана командою Ctrl-C;

– a – дозволяє використовувати імена вузлів замість IP-адрес;

– n число – вказує кількість exo запитів для відправки ;

– l довжина – вказує довжину exo – запитів;

– f – забороняє фрагментування пакету, визначає, чи пристрій змінював розмір пакету;

– i час – встановлює час життя пакету (Time to Live -TTL) відправляємих пакетів;

– v тип – встановлює тип обслуговування (TOS)

– r число – відображає шляхи для заданого числа переприйомів;

– s число – відмічає час для вказаного числа переприйомів;

– j список вузлів – маршрутизація пакетів через вказані вузли. Послідовні вузли можуть бути розділені шлюзами;

– k список вузлів - маршрутизація пакетів через вказані вузли. Послідовні вузли не можуть бути розділені шлюзами.

– w час – встановлює час очікування відповіді в мілісекундах.

Команда TRACERT також використовує протокол ICMP для визначення всіх пристроїв, через які проходить пакет на шляху до вузла призначення.

За допомогою цієї команди, можна отримати досить обширну інформацію про те, як функціонує мережа.

Має наступний синтаксис :

tracert [ключі] ім’я вузла

Ключі :

– d – використовувати імена вузлів замість IP адрес;

– h максимальне число переприйомів – максимально допустиме число переприйомів для досягнення мети;

– j список вузлів - маршрутизація пакетів через вказані вузли. Послідовні вузли можуть бути розділені шлюзами. Вільний вибір шляху серед систем у вказаному списку;

– w час – встановлення часу очікування в мілісекундах.

Існує також команда IPCONFIG, яка використовується для отримання інформації про настройку TCP/IP сервера або робочої станції Windows NT.

Команда IPCONFIG виводить інформацію про всі мережеві карти, встановлені в системі і зв’язках PPP. В базову інформацію входять:

– IP-адреса;

– маска підмережі;

– шлюз по замовчуванню;

– сервери DNS;

– домен NT.

Якщо застосувати в даній команді ключ /all, то буде виведений список апаратних MAC-адрес пристроїв і інформацію по DHCP.

Примітка: При написанні даного пункту використовувалися інструкції з мережі Інтернет.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проекту локальної комп'ютерної мережі компанії «ТК Галич» і прийняття рішення про її подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

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

Таблиця 4.1 - Середній час виконання НДР та стадії (операції) технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час вико-нання операції, год.
1	Підготовка. Розробка проекту мережі	Інженер	16
2	Монтаж пасивного обладнання	Лаборант	24
3	Налаштування активного комутаційного обладнання	Технік	10
4	Встановлення та на лаштування програмного забезпечення	Технік	15
5	Тестування мережі	Технік	4
Р а з о м		–	69

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

Основна заробітна плата розраховується за формулою:

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

де $Тс$ – тарифна ставка, грн.;

$Кг$ – кількість відпрацьованих годин.

$З_{осн.}$=110*16+80*25+70*29=5790,00 грн.

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

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

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам.

$З_{дод.}$= 5790,00 *0,15=868,50 грн.

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

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

$В_{о.п.}$ = 5790,00 +868,50=6658,50 грн.

Крім того, слід визначити відрахування на заробітну плату:

єдиний соціальний внесок – 22 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{з.п.}=ФОП \cdot 0,22, \quad (4.4)$$

де *ФОП* – фонд оплати праці, грн.

$В_{з.с.}$ =6658,50*0,22=1464,87 грн.

Проведені розрахунки зведемо у наступну таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Дод. заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на опл. пр., грн. 6=3+4+5
		Тарифна ставка, грн.	К-сть від-працьов. год.	Факт. нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1	Інженер	110	16	1760,00	264,00	-	-
2	Технік	80	25	2000,00	300,00	-	-
3	Лаборант	70	29	20230,00	304,50	-	-
	Разом	-	-	5790,00	868,50	1464,87	8123,37

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

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

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

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

$$З_{м.в.} = 38480{,}00 \text{ грн}$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	2	3	4	5	6
1	Комутатор робочих станцій TP-LINK TL- SG116E	шт	1	2700	2700
2	Керований комутатор MikroTik CRS125 24G-1S-IN	шт	1	7530	7530
3	Точка доступу MikroTik RBCAPGI-5ACD2ND	шт	1	3100	3100
5	Комутаційна шафа	шт	1	12000	12000
6	Кабель мережевий	шт	4	2800	11200

Продовження таблиці 4.3

1	2	3	4	5	6
7	Короб 20х40х2000	шт	50	39	1950
	Разом				38480,00

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S, \qquad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Для розробки проекту даної локальної комп'ютерної мережі використовується один ПК, потужність якого W = 0,5 кВт і який працює 27 годин.

$$З_е = 0{,}50*27*7{,}00 = 94{,}5 \text{ грн.}$$

4.5 Визначення транспортних затрат

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

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

де $Т_В$ – транспортні витрати.

$Т_В = 38480{,}00*0{,}08 = 3078{,}4$ грн

4.6 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному вигляді необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Мінімально допустимі строки їх корисного використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{100\%}, \qquad (4.9)$$

де A – амортизаційні відрахування за звітний період, грн.;

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

$Н_А$ – норма амортизації, %.

Для проектування даної комп'ютерної мережі використовується один комп'ютер (вартість якого становить 19870 грн.), який працює 27 годин.

Тоді:

$$A = 19870*0,04*27/150=143,06 \text{ грн.}$$

4.7 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створення необхідних умов праці.

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

$$Н_в = В_{о.п.} \cdot 0{,}2 \ldots 0{,}6, \quad (4.10)$$

де $Н_В$ – накладні витрати.

$Н_В$=6658,50*0,5=3329,25 грн.

4.8 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 4.4.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до заг. суми
Витрати на оплату праці	8123,37	14,61
Відрахування на соціальні заходи	1464,87	2,63
Матеріальні витрати	38480,00	69,21
Витрати на електроенергію	94,5	0,17
Транспортні витрати	3078,4	5,54
Амортизаційні відрахування	143,06	0,54
Накладні витрати	3329,25	7,30
Собівартість	54869,07	100,00

Собівартість (СВ) НДР розрахуємо за формулою:

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

$С_в$=54869,07 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_B \cdot (1 + P_{рен}) \cdot K + B_{н.і.}}{K} \cdot (1 + ПДВ), \qquad (4.12)$$

де $P_{рен.}$ – рівень рентабельності;

K – кількість замовлень, од.;

$B_{і.н.}$ – вартість носія інформації, грн.;

$ПДВ$ – ставка податку на додану вартість, (20 %).

$Ц$=54869,07*(1+0,26)*(1+0,2)= 82962,03 грн.

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Для визначення ефективності продукту розраховують чисту теперішню вартість (ЧТВ) і термін окупності ($T_{ОК}$).

$$ЧТВ = -K_B + \sum_{i=1}^{t} \frac{Г_П}{(1+i)^t}, \qquad (4.13)$$

де K_B – затрати на проект;

$Г_п$ – грошовий потік за t–ий рік;

t – відповідний рік проекту;

i - величина дисконтної ставки (10…15%).

$ЧТВ$ = –54869,07+46357,96/(1+0,15)+ 46357,96/(1+0,15)^2=20495,47 (грн.)

Якщо ЧТВ ≥ 0, то проект може бути рекомендований до впровадження.

Термін окупності визначається за формулою:

$$T_{ок} = T_{пв} + \frac{H_в}{Г_{пр}}, \qquad (4.14)$$

де $T_{ПВ}$ – період до повного відшкодування витрат, років;

$H_В$ – невідшкодовані витрати на початок року, грн.;

$Г_{ПР}$ – грошовий потік на початок року, грн.

$T_{ОК}$=1+14557,8/46357,96=1,3

Таблиця 4.5 - Економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	54869,07
2.	Плановий прибуток, грн.	14265,96
3.	Ціна, грн.	82962,03
4.	Чиста теперішня вартість, грн	20495,47
5.	Термін окупності, рік	1,3

В результаті аналізу економічних показників, розрахованих та зведених у таблицю 4.5, можна прийти до висновку, що при терміні окупності – 1,3 року проводити роботи по впровадженню даної мережі є доцільним та економічно вигідним.

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Пожежна профілактика в компанії «ТК Галич»

Зазначимо, що основні причини виникнення пожеж на виробничих об’єктах пов'язані з людським фактором. Це куріння в місцях, не призначених для цього, спалювання сміття і відходів, помилки під час експлуатації промислового устаткування, газових мереж та електричних пристроїв, навмисні підпали. Крім людського фактора, до пожеж призводять самозаймання обладнання, матеріалів і речовин, блискавки та інші фактори ризику.

Значний відсоток пожеж стається через незадовільний стан електричного устаткування та приладів, порушення правил їх монтажу та експлуатації.

Короткі замикання виникають унаслідок неправильного монтажу або експлуатації електроустановок, старіння або пошкодження ізоляції. Струм короткого замикання залежить від потужності джерела струму, відстані від джерела струму до місця замикання та виду замикання. Потужні струми замикання зумовлюють іскріння та нагрівання струмопровідних частин до високої температури, що може бути причиною займання ізоляції провідників та горючих будівельних конструкцій.

Струмові перевантаження виникають у разі ввімкнення до мережі додаткових споживачів струму або зниження напруги в мережі. Тривале перевантаження призводить до нагрівання провідників, що може спричинити займання ізоляції.

Потенційну небезпеку виникнення пожежі або вибуху в умовах виробництва становлять і хімічні речовини, які під час контакту з повітрям чи водою, взаємодії між собою виділяють велику кількість теплової енергії.

Дотримання заходів щодо забезпечення пожежної безпеки є актуальним завданням для будь-якого об'єкта житлової, торгової чи промислової нерухомості, адже допомагає зберегти не тільки майно, а й людські життя.

Пожежна профілактика – це комплекс заходів, які спрямовані на запобігання пожежі, запобігання розповсюдженню вогню, передбачення можливих шляхів евакуації людей і матеріальних цінностей та створення умов для швидкої ліквідації пожеж.

Технічні заходи – планування належної кількості виходів, коридорів потрібної ширини, систем протидимового захисту, виконання будівельних конструкцій з вогнетривких матеріалів, дотримання протипожежної відстані, наявність засобів пожежогасіння, пожежних драбин, водоймищ, під'їздів до будівель, пожежної сигналізації.

Організаційні заходи – це організація навчання правил пожежної безпеки; розробка інструкцій щодо роботи з пожежонебезпечими матеріалами та дій персоналу під час пожежі.

Система запобігання пожежам має два напрями: запобігання формуванню горючого середовища і виникнення в цьому середовищі джерела займання.

Запобігання утворенню горючого середовища:

– застосування негорючих і важкогорючих матеріалів;

– обмеження кількості горючих речовин і безпечні способи їх розташування;

– ізоляція горючого середовища;

– установка пожежонебезпечного устаткування в ізольованих приміщеннях чи на відкритих площадках;

– застосування пристроїв захисту виробничого обладнання з горючими речовинами від ушкоджень і аварій, установок автоматичного відключення.

Запобігання утворенню джерел займання:

– застосування пристроїв, під час експлуатації яких не утворюються джерела займання;

– застосування у конструкціях швидкісних засобів захисного вимкнення можливих джерел займання;

– використання блискавкозахисту;

– підтримка температури нагрівання поверхні механізмів, що можуть увійти в контакт із горючим середовищем, на рівні 80% від температури самозаймання;

– унеможливлення появи іскри в горючому середовищі;

– застосування під час роботи з легкозаймистими рідинами і горючими газами інструментів, що не іскрять;

– унеможливлення теплового або хімічного самозаймання речовин.

Система протипожежного захисту – це комплекс заходів та засобів, які спрямовані на виявлення, локалізацію пожежі, створення умов для ліквідації пожежі, захист людей і матеріальних цінностей.

Пожежна автоматика – це комплекс технічних засобів, призначений для автоматичного протипожежного захисту об'єкта.

Для вчасного виявлення пожеж застосовують пожежну сигналізацію. Складовими частинами систем автоматичної сигналізації є датчики, що монтуються на території об'єктів і служать для подачі сигналу про пожежу; приймальні апарати, що забезпечують прийом сигналів від датчиків; лінії комунікацій; джерела електропостачання. У чому користь пожежної сигналізації? У разі пожежі всі працівники дізнаються про неї та будуть готові до дій щодо усунення вогню або до евакуації. Якщо немає пожежної сигналізації, жертв та збитків буде значно більше.

Установки для запобігання пожежі призначенні для введення в небезпечну зону вогнегасних засобів або зміни режиму роботи устаткування і запобігання виникненню вибухів та загорянь.

Установки для гасіння пожеж призначенні для повної ліквідації осередків горіння вогнегасним засобом або створення умов, за яких горіння припиняється. Їх поділяють на теплові (реагують на підвищення температури), димові, світлові (появу полум'я), ультразвукові (зміну частоти коливання), фотоелектричні (перетин інфрачервоних променів).

Дренчерна система призначена для утворення водяних завіс у приміщенні для запобігання розповсюдженню вогню.

Спринклер – це пристрій, що автоматично відкриває вихід води у разі підвищення температури в приміщенні. Вода, яка витікає з отвору спринклера, вдаряється в спеціальну розетку і розприскується.

Установки локалізації пожеж призначені для стримування розвитку осередку горіння дією вогнегасних засобів на вогонь до прибуття підрозділу пожежної охорони.

Протипожежний захист досягається:

– застосуванням засобів пожежогасіння і відповідних видів пожежної техніки;

– застосуванням автоматичних установок пожежної сигналізації і пожежогасіння;

– застосуванням будівельних матеріалів з нормованими показниками пожежної небезпеки;

– просочення конструкцій об'єктів антипіренами і нанесенням на їхні поверхні вогнезахисних фарб;

– організацією за допомогою технічних засобів своєчасного оповіщення й евакуації людей;

– застосуванням засобів колективного й індивідуального захисту людей від небезпечних факторів пожежі;

– застосуванням засобів протидимного захисту.

До всіх будівель на території об’єкта повинен бути вільний доступ для пожежних машин. Це забезпечить швидке гасіння загоряння.

Горючі та легкозаймисті речовини не повинні зберігатися поруч з нагрівальними елементами або відкритим вогнем.

Територію підприємства слід регулярно очищати від виробничих відходів, які створюють ризик загоряння.

На території об’єкта повинні бути системи автоматичного гасіння пожеж для максимально швидкого гасіння загоряння.

Приміщення, де проводять роботи з горючими речовинами, повинні бути зроблені з протипожежних матеріалів та оброблені відповідними вогнезахи-

сними речовинами.

Не менш важливі евакуаційні виходи для кожного об’єкта! Адже під час пожежі основний вихід може бути перекритий димом або вогнем.

План евакуації допоможе зорієнтуватися в екстреній ситуації та евакуювати персонал з мінімальними втратами. Наявність планів обов'язкова на всіх об’єктах.

Дотримання всіх правил організації протипожежної профілактики допоможе звести до мінімуму втрати людей і матеріальні збитки в разі виникнення загоряння.

5.2 Штат служби охорони праці в компанії «ТК Галич»

Одним із заходів, спрямованих на гарантування безпеки праці, є створення на підприємстві служби охорони праці.

Одним з основних суб’єктів, що здійснюють управління охороною праці на підприємстві, є служба охорони праці. У якій формі вона створюється та функціонує, залежить від кількості працівників, що працюють на підприємстві.

Створення служби охорони праці на підприємствах будь-якої форми власності передбачено ст. 15 Закону України «Про охорону праці» і є обов’язком роботодавця, якщо кількість найманих працівників складає 50 і більше осіб. На підприємствах виробничої сфери при кількості працюючих до 50 осіб (невиробничої сфери — до 100 чоловік) функції служби охорони праці можуть виконувати особи з відповідною професійною підготовкою за сумісництвом.

На підприємстві з кількістю працівників менше 50 створення цілої служби не є обов’язковим і доцільним. Її функції можуть виконувати за сумісництвом особи, які мають відповідну підготовку та освіту: фахівці або інженери з охорони праці.

В організаціях з кількістю працівників менше 20 для виконання функ-

цій служби охорони праці можуть залучатися фахівці на договірній основі. При цьому вони повинні мати стаж роботи не менше 3 років і пройти навчання з охорони праці.

Очевидно, що ставлення власника (керівника) до створення служби охорони праці віддзеркалює його ставлення до створення безпечних, здорових умов праці, а власне — до збереження життя та здоров'я підпорядкованих працівників.

Служба охорони праці підпорядковується безпосередньо керівникові підприємства. За своїм посадовим положенням та умовами оплати праці керівник та спеціалісти служби прирівнюються до керівників і спеціалістів основних виробничо-технічних служб підприємства. Діє така служба на підставі Типового положення, затвердженого наказом Держнаглядпраці від 15.11.2004 р. № 255. На основі Типового положення з урахуванням специфіки виробництва, видів діяльності, кількості працівників, умов праці та інших факторів, роботодавець розробляє Положення про службу охорони праці відповідного підприємства, яке затверджується наказом по підприємству. Цей документ визначає структуру служби охорони праці, чисельність, завдання, функції та права її працівників відповідно до чинних нормативно-правових актів.

Яке ж основне призначення служби охорони праці?

Згідно із Законом України «Про охорону праці» служба охорони праці створюється роботодавцем для організації виконання правових, організаційно-технічних, санітарно-гігієнічних, соціально-економічних і лікувально-профілактичних заходів, спрямованих на запобігання нещасним випадкам, професійним захворюванням і аваріям у процесі праці.

Роботу служби охорони праці спрямовано на створення здорових і безпечних умов праці, на збереження життя та здоров'я працівників у процесі виконання ними трудових обов'язків.

Перш за все слід розуміти, що служба охорони праці на підприємстві повинна забезпечити виконання вимог чинного законодавства України з пи-

тань охорони праці, а також забезпечити нормативно-правовими актами з охорони праці, що діють у межах підприємства, посібниками, навчальними матеріалами з цих питань; організовувати роботу кабінету з охорони праці, наради, семінари та інші заходи з цих питань.

Однією з найважливіших функцій, які покладені на службу охорони праці, є участь у розслідуванні нещасних випадків, професійних захворювань і аварій на виробництві. Також фахівці з охорони праці беруть участь у складанні санітарно-гігієнічної характеристики робочих місць працівників, які проходять обстеження щодо профзахворювань; у проведенні внутрішнього аудиту охорони праці та атестації робочих місць на відповідність нормативно-правовим актам з охорони праці; у складанні списків професій і посад, згідно з якими працівники повинні проходити обов'язкові попередні та періодичні медичні огляди; в організації навчання з питань охорони праці та роботи комісії з перевірки знань з цих питань.

Служба охорони праці на підприємстві покликана також контролювати дотримання роботодавцем вимог законодавства з охорони праці, тому має право видавати керівникам структурних підрозділів підприємства обов'язкові для виконання приписи щодо усунення наявних недоліків і отримувати від них необхідні відомості, документацію і пояснення з питань охорони праці.

Припис спеціаліста з охорони праці може скасувати лише роботодавець. Такий припис складається у двох примірниках, один з яких видається керівнику робіт, об'єкта, цеху, другий залишається і реєструється в службі охорони праці і зберігається протягом 5 років. Якщо керівник структурного підрозділу підприємства відмовляється від підпису в отриманні припису, спеціаліст охорони праці направляє відповідне подання на ім'я особи, якій адміністративно підпорядкований цей структурний підрозділ, або роботодавцю.

Отже, для організації роботи служби охорони праці необхідно:

1. Видати комплексний наказ про створення служби охорони праці на підприємстві, яким закріпити, зокрема, такі основні моменти:

1. створити службу охорони праці на підприємстві;

2. затвердити Положення про службу охорони праці (про яке згадувалось вище);

3. призначити керівника та працівників служби охорони праці;

4. затвердити Положення про проведення навчань з питань охорони праці, Положення про систему охорони праці, інші нормативні акти з питань охорони праці, враховуючи специфіку підприємства;

5. закріпити відповідальних працівників служби охорони праці за проведення інструктажів та перевірки знань з питань охорони праці.

2. Забезпечити проведення навчання та перевірку знань з питань охорони праці (цього вимагає п. 1.6 Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці та Перелік робіт з підвищеною небезпекою: (наказ Держнаглядпраці від 26.01.2005 р. № 15) «Навчання та перевірка знань з питань охорони праці працівників служби охорони праці проводяться в установленому законодавством порядку під час прийняття на роботу та періодично один раз на три роки»).

3. Опрацювати та затвердити у керівника підприємства посадову інструкцію керівника та працівника служби охорони праці.

4. Забезпечити ведення нормативної, технічної та іншої документації з питань охорони праці на підприємстві, її належне зберігання та контроль.

5. Створити кабінет охорони праці. Згідно з Рекомендаціями Держгірпромнагляду від 07.02.2008 р. кабінет має відповідати вимогам будівельних норм і правил. Його площа визначається із розрахунку працюючих: до 1000 осіб — 24 м2, більше 1000 — додається 6 м2. Виходячи із завдань, покладених на кабінет охорони праці, він має бути відповідно оснащений з урахуванням специфіки діяльності підприємства (сьогодні нормативно не закріплено обов'язок суб'єктів господарювання створювати кабінет охорони праці. Вирішення цього питання покладається на розсуд роботодавця. Типове положення про кабінет охорони праці визнано таким, що втратило чинність, згідно з наказом Держгірпромнагляду від 02.10.2007 р. за № 235. Проте у деяких чин-

них документах згадується про кабінет охорони праці, зокрема в Типовому положенні про порядок проведення навчання і перевірки знань з питань охорони праці.

Відомо, що працівники служби охорони праці несуть персональну відповідальність:

– за невідповідність прийнятих ними рішень вимогам чинного законодавства з охорони праці;

– за невиконання своїх функціональних обов’язків;

– за недостовірність та несвоєчасність підготовки статистичних звітів з охорони праці;

– за низьку якість проведеного ними розслідування нещасних випадків на виробництві.

5.3 Штучна вентиляція виробничих приміщень компанії «ТК Галич»

Штучна (механічна) вентиляція, на відміну від природної, дає можливість очищувати повітря перед його викидом в атмосферу, вловлювати шкідливі речовини безпосередньо біля місць 'іх утворення, обробляти припливне повітря (очищувати, підігрівати, зволожувати), більш цілеспрямовано подавати повітря в робочу зону. Окрім того, механічна вентиляція дає можливість організувати повітрозабір в найбільш чистій зоні території підприємства і навіть за її межами.

Загальнообмінна штучна вентиляція

Загальнообмінна вентиляція забезпечує створення необхідного мікроклімату та чистоти повітряного середовища у всьому об'ємі робочої зони приміщення. Вона застосовується для видалення надлишкового тепла при відсутності токсичних виділень, а також у випадках, коли характер технологічного процесу та особливості виробничого устаткування виключають можливість використання місцевої витяжної вентиляції.

Розрізняють чотири основні схеми організації повітрообміну при загальнообмінній вентиляції: зверху вниз, зверху вверх, знизу вверх, знизу вниз (див.рис.5.1).

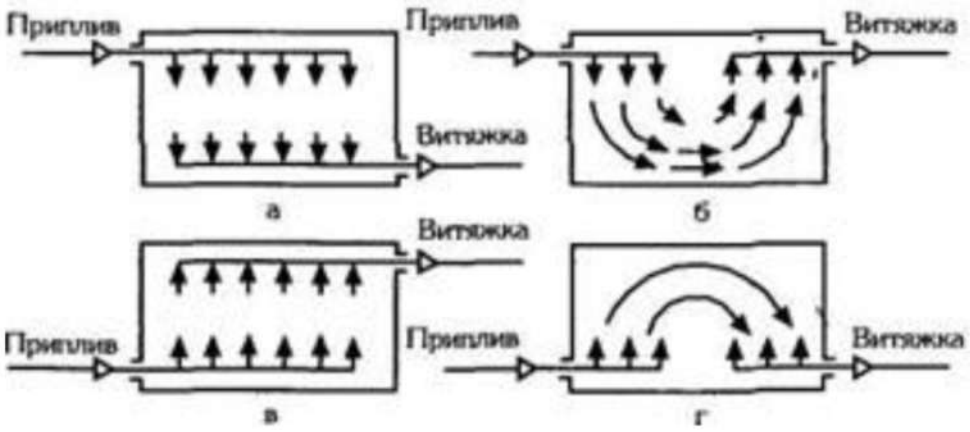


Рисунок 5.1 - Схема організації повітрообміну при загальнообмінній вентиляції

Схеми зверху вниз та зверху вверх доцільно застосовувати у випадку, коли припливне повітря в холодний період року має температуру нижчу температури приміщення. Припливне повітря перш ніж досягти робочої зони нагрівається за рахунок повітря приміщення. Інші дві схеми рекомендується використовувати тоді, коли припливне повітря в холодний період року підігрівається і його температура вища температури внутрішнього повітря.

Якщо у виробничих приміщеннях виділяються гази та пари з густиною, що перевищує густину повітря (наприклад, пари кислот, бензину, гасу), то Загальнообмінна вентиляція повинна забезпечити видалення 60% повітря з нижньої зони приміщення та 40% — з верхньої.

Якщо густина газів менша за густину повітря, то видалення забрудненоп повітря здійснюється у верхній зоні.

Припливна вентиляція. Схема припливної механічної вентиляції (див.рис. 5.2) включає: повітрозабірний пристрій 1; фільтр для очищенні повітря

2; повітронагрівач (калорифер) 3; вентилятор 5; мереж, повітроводів 4 та припливні патрубки з насадками 6. Якщо нема необхідності підігрівати припливне повітря, то його пропускають безпосередньо у виробничі приміщення через обвідний канал 7.

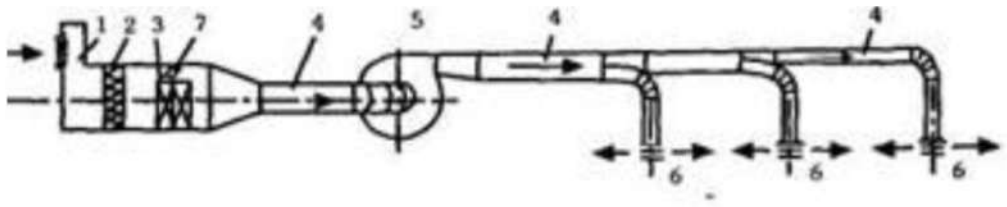


Рисунок 5.2 - Схема припливної вентиляції

Повітрозабірні пристрої необхідно розташовувати в місцях, де повітря не забруднене пилом та газами. Вони повинні знаходитись і нижче 2 м від рівня землі, а від викидних каналів витяжної вентиляції по вертикалі — нижче 6 м і по горизонталі — не ближче 25 м.

Припливне повітря подається в приміщення, як правило, розсіяне потоком для чого використовуються спеціальні насадки.

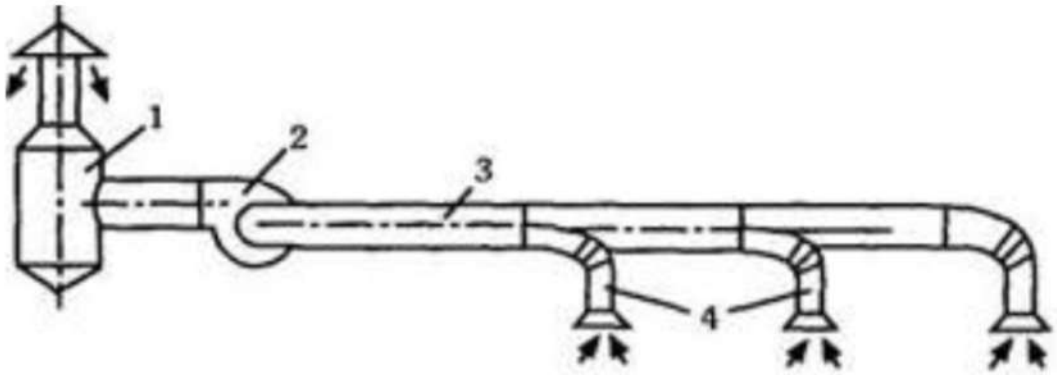


Рисунок 5.3 - Схема витяжної вентиляції

Витяжна та припливно-витяжна вентиляція. Витяжна вентиляція (див.рис. 5.3) складається із очисного пристрою 1, вентилятора 2, центрального 3 та відсмоктуючих повітроводів 4.

Повітря після очищення необхідно викидати на висоті не менше ніж 1 м над гребенем даху. Забороняється робити викидні отвори безпосередньо у вікнах.

В умовах промислового виробництва найбільш розповсюджена припливно-витяжна система вентиляції із загальним припливом в робочу зону та місцевою витяжкою шкідливих речовин безпосередньо з місць їх утворення.

У виробничих приміщеннях, де виділяється значна кількість шкідливих газів, парів, пилу витяжка повинна бути на 10% більшою ніж приплив, щоб шкідливі речовини не витіснялись у суміжні приміщення з меншою шкідливістю.

В системі припливно-витяжної вентиляції можливе використання не лише зовнішнього повітря, але й повітря самих приміщень після його очищення. Таке повторне використання повітря приміщень називається рециркуляцією і здійснюється в холодний період року для економії тепла, витраченого на підігрівання припливного повітря. Однак можливість рециркуляції обумовлюється цілою низкою санітарно-гігієнічних та протипожежних вимог.

Місцева вентиляція

Місцева вентиляція може бути припливною і витяжною.

Місцева припливна вентиляція, при якій здійснюється концентроване подання припливного повітря заданих параметрів (температури, вологості, швидкості руху), виконується у вигляді повітряних душів, повітряних та повітряно-теплових завіс.

Повітряні душі використовуються для запобігання перегріванню робітників в гарячих цехах, а також для утворення так званих повітряних оазисів (ділянок виробничої зони, які різко відрізняються своїми фізико-хімічними характеристиками від решти приміщення).

Повітряні та повітряно-теплові завіси призначені для запобігання надходження в приміщення значних мас холодного зовнішнього повітря при необхідності частого відкривання дверей чи воріт. Повітряна завіса створюється струменем повітря, що подається із вузької довгої щілини, під деяким кутом назустріч потоку холодного повітря. Канал зі щілиною розміщують збоку чи зверху воріт (дверей).

Місцева витяжна вентиляція здійснюється за допомогою місцевих витяжних зонтів, всмоктуючих панелей, витяжних шаф, бортових відсмоктувачів (див.рис. 5.4).

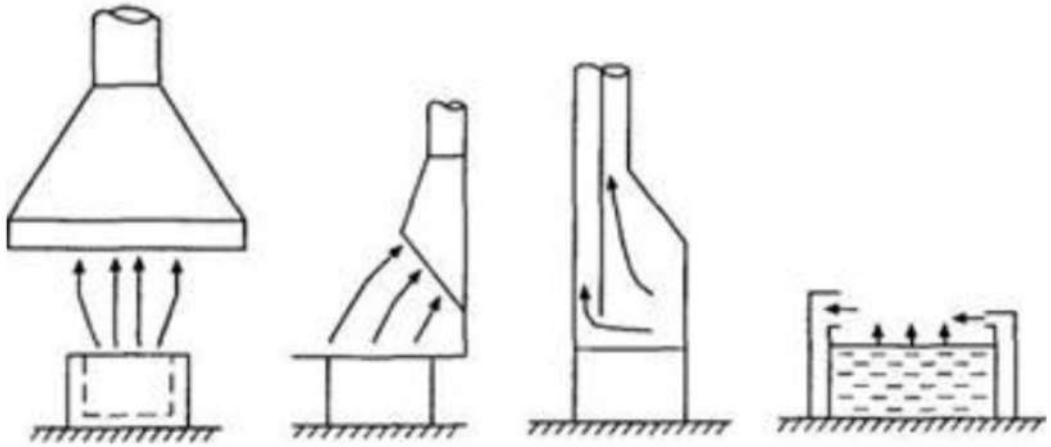


Рисунок 5.4 - Приклади місцевої витяжної вентиляції: а — витяжний зонт, б — всмоктувальна панель, в — витяжна шафа з комбінованою витяжкою, г — бортовий відсмоктувач з передувом

Конструкція місцевої витяжки повинна забезпечити максимальне вловлювання шкідливих виділень при мінімальній кількості вилученого повітря. Крім того, вона не повинна бути громіздкою та заважати обслуговуючому персоналу працювати і наглядати за технологічним процесом.

Основними чинниками при виборі типу місцевої витяжки є характеристики шкідливих виділень (температура, густина парів, токсичність), положення робітника при виконанні роботи, особливості технологічного процесу та

устаткування.

У випадках, коли джерело виробничих шкідливостей можна помістити всередині простору, обмеженого стінками, місцеву витяжну вентиляцію влаштовують у вигляді витяжних шаф, кожухів, вітринних відсмоктувачів. Якщо за умовами технології або обслуговування джерело шкідливостей не можна ізолювати, тоді встановлюють витяжний зонт або всмоктувальну панель. При цьому потік повітря, що видаляється, не повинен проходити через зону дихання робітника.

Окремим випадком місцевої витяжної вентиляції є бортові відсмоктувачі, якими обладнують ванни (гальванічні, травильні) чи інші ємкості з токсичними рідинами, оскільки необхідність використати при їх завантаженні підіймально-транспортного обладнання унеможливлює використання витяжних зонтів та всмоктувальних панелей. При ширині ванни 1 м і більше необхідно встановлювати бортовий відсмоктувач з передувом, у якого з одного боку ванни повітря відсмоктується, а з іншого — нагнітається. При цьому рухоме повітря ніби екранує поверхню випаровування токсичних рідких продуктів.

Примітка: При написанні даного пункту використовувалися інструкції з мережі Інтернет.

ВИСНОВКИ

В ході проектування спроектовано комп’ютерну мережу компанії «ТК Галич». Зроблено аналітичний огляд літератури та існуючих рішень, та на його основі спроектовано логічну та фізичну топологію мережі. Вибрано пасивне та активне комутаційне обладнання, сервер, точку доступу та програмне забезпечення.

Кваліфікаційна робота містить повністю завершену логічну і фізичну топології мережі, таблицю IP-адресації та техніко-економічних показників які подано в графічній частині.

В економічному розділі розраховано собівартість мережі, її економічну ефективність, термін окупності та інші показники.

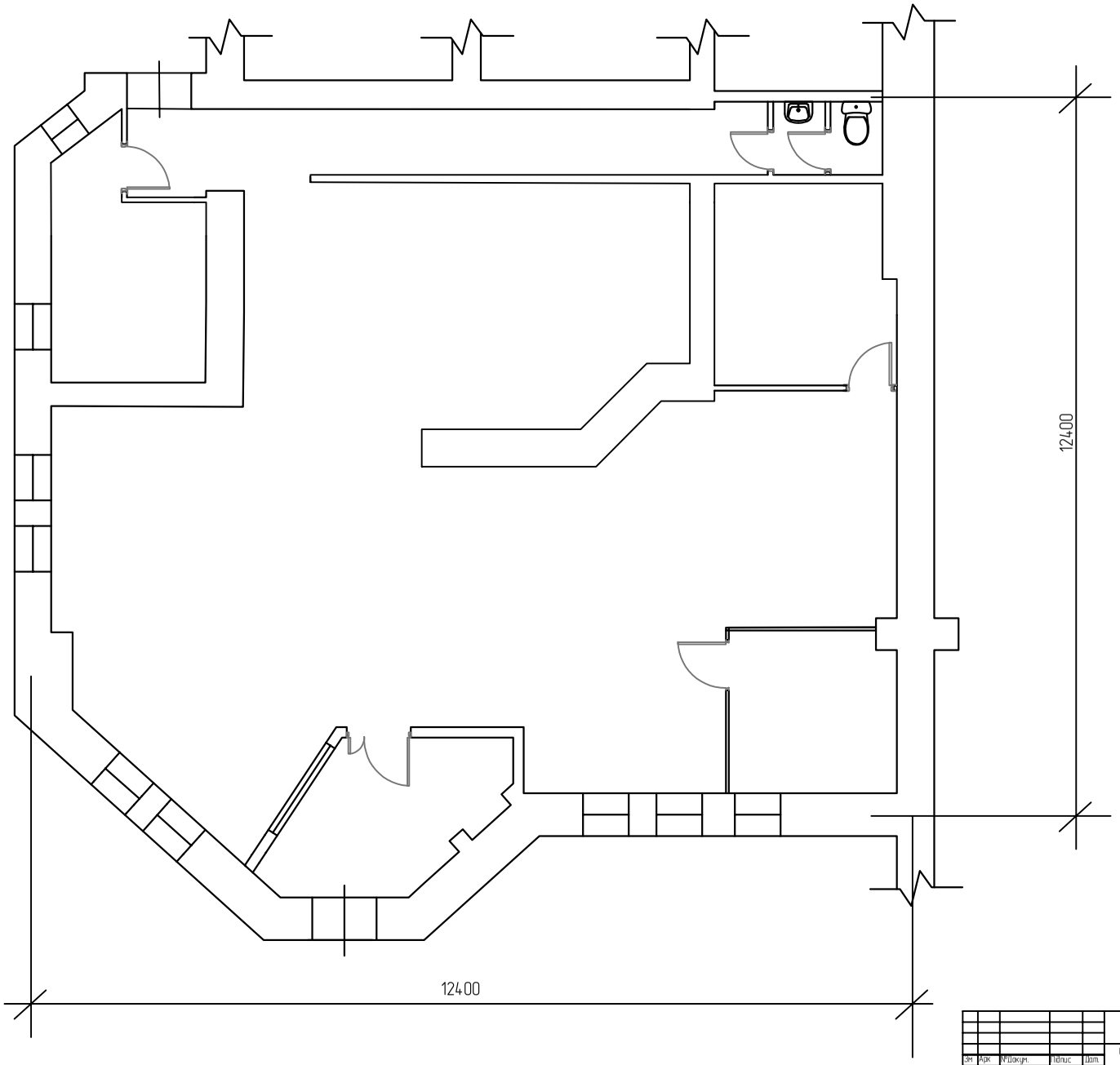
Останній розділ кваліфікаційної роботи описує питання охорони праці, та техніки безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

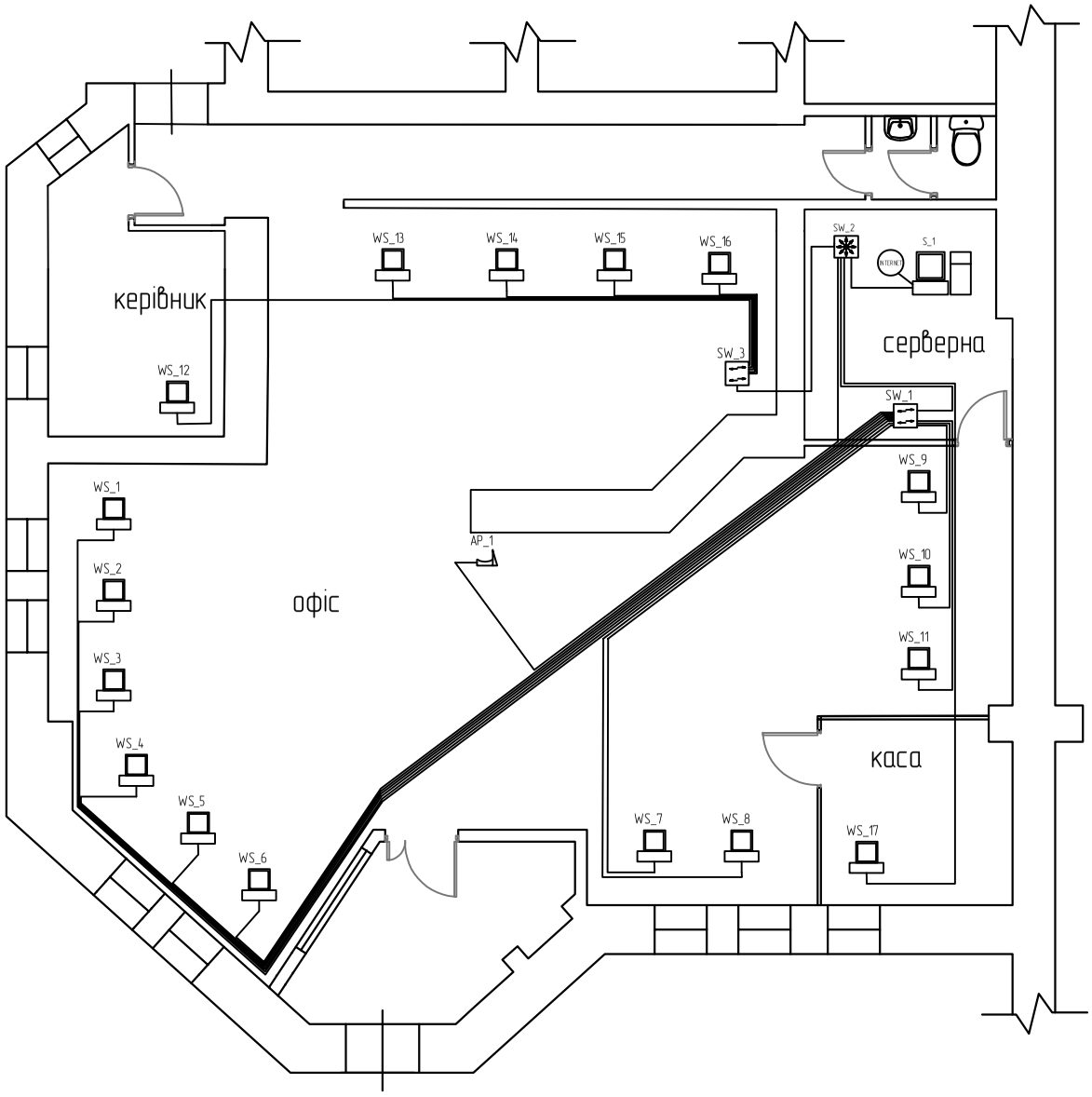
1. Антонов В.М. Сучасні комп'ютерні мережі. Підручник — К.: "МК-Прес", 2005. — 480 с.
2. Буров Є. Комп'ютерні мережі, 2-е видання. - БаК, 2004. – 584 с.: іл.
3. Додонов О. Г., Ланде Д. В., Путятін В. Г. Інформаційні потоки в глобальних комп’ютерних мережах. — К.: Наук, думка, 2009. — 295 с
4. Іртегов Д.В. Введення в мережні технології, К., 2014.
5. Шорошев В. В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп’ютерних систем. Монографія. - К.: ДУПСТ, 2011. - с.257.
6. Business Products URL: http://www.trendnet.com/products/business/ category/ switches – (дата звернення: 11.05.2024)
7. Комутатори URL: http://hotline.ua/computer/kommutatory/ – (дата звернення: 21.04.2024)
8. Москальова В.М. Охорона праці – URL: http://studentbooks.com.ua/content/view/1327/76/ – (дата звернення: 19.04.2024).
9. Топологія мереж URL: https://uk.wikipedia.org/wiki/%D0%A2%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6 (дата звернення: 1.05.2024)
10. Топології та технології мереж URL: https://studfile.net/preview/9649745/ (дата звернення: 11.05.2024)
11. Дипломна робота Карнаух В URL: https://elartu.tntu.edu.ua/bitstream/lib/42050/1 /dyplom Karnaukh V 2023-.pdf (дата звернення: 19.04.2024)
12. Маршрутизатор rbcapqj 5acd2nd URL: https://ktc.ua/goods/marshrutizator mikrotik rbcapqj 5acd2nd.html (дата звернення: 19.05.2024)

13. Монтаж мереж СКС URL: https:ZZstud.wiki/radio/3c0a65635b3bc68a4d53b88421216d37 O.html (дата звернення: 19.05.2024)
14. Безпека мережі URL: https://uk.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96 (дата звернення: 29.05.2024)
15. Налаштування проксі-сервера squit URL: https://kursoviks.com.ua/bd kompyuternyye/article post/3762-Iaboratorna-robota-no12-listi-dostupu (дата звернення: 02.06.2024)

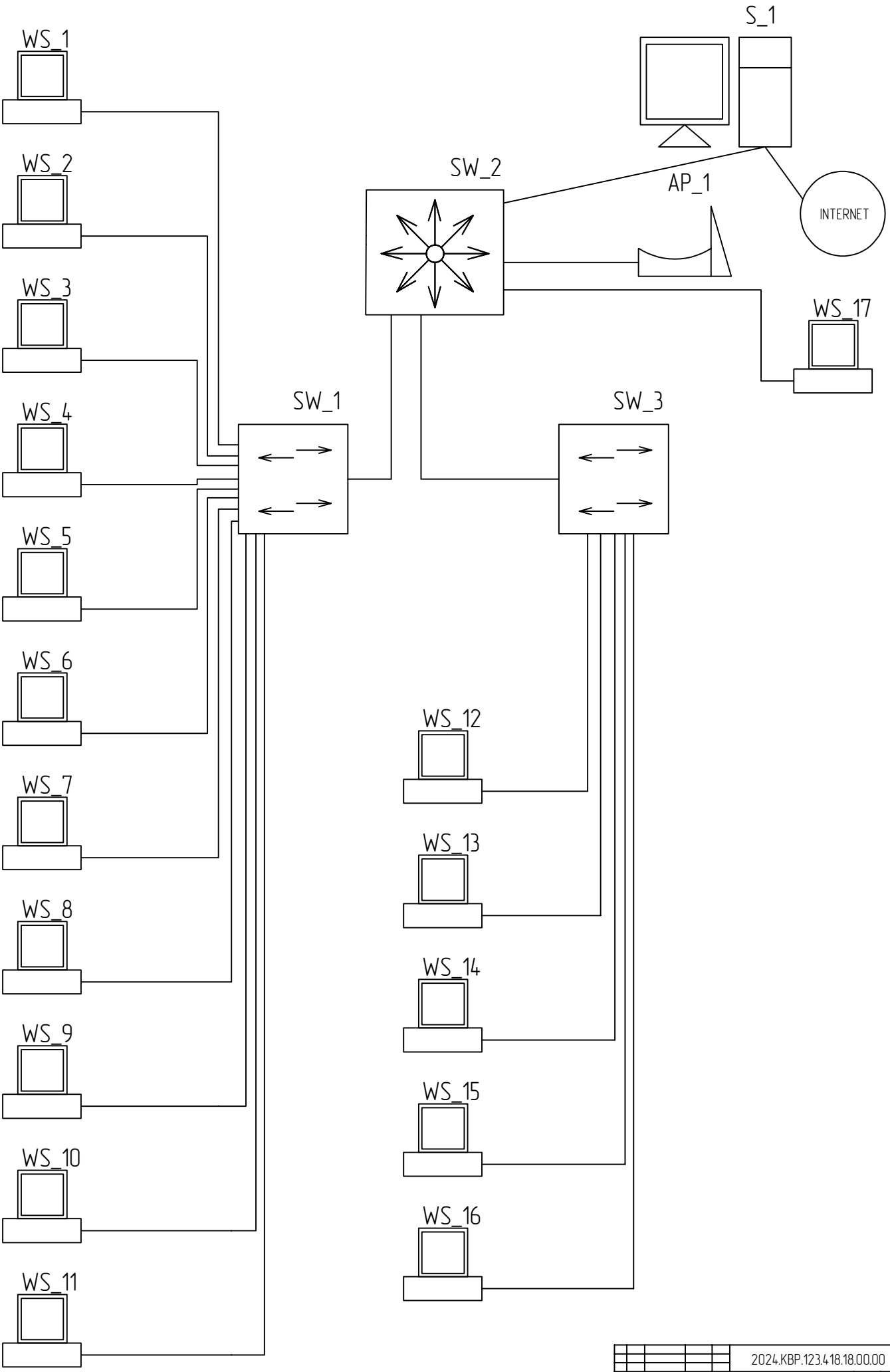
2024.КВР.123.418.18.00.00 ТБ



						2024.КВР.123.418.18.00.00 ПП	
Зм.	Арк.	№докум.	Підпис.	Дат.	Розробка проекту комп'ютерної мережі компанії "ТК Галич"	Літ.	Маса. Масшт.
Розроб.		Яраш З В					
Керів.		Луж В С			План приміщень		-
Т.контр.		Юзьків А В				Аркуш 1	Аркушів 1
Затв.						ВСП ТФК ТНТУ КІ-418, м.Тернопіль	



						2024.КВР.123.418.18.00.00 ФТ	
Зм.	Арк.	№докум.	Підпис.	Дат.	Розробка проекту комп'ютерної мережі компанії "ТК Галич"	Літ.	Маса.	Масшт.
Розроб.		Ярош З В						
Керів.		Луж В С			Фізична топологія		-	
Т.контр.		Язьків А В				Аркуш 1	Аркушів 1	
Затв.						ВСП ТФК ТНТУ КІ-418, м.Тернопіль		



					2024.КВР.123.418.18.00.00 /ІТ	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії "ТК Галич"	Літ. / Маса / Масшт.
Розроб.		Ярош З. В.				
Керів.		Пиж В. С.			План приміщень	Аркуш 1 / Аркушів 1
Н.контр.		Юзьків А. В.				ВСП ТФК ТНТУ КІ-418, м.Тернопіль
Реценз.						
затв.						

ТАБЛИЦЯ ТЕХНІКО-ЕКОНОМІЧНИХ ПОКАЗНИКІВ

№ п\п	параметр	одиниці вимірювання	значення	№ п\п	параметр	одиниці вимірювання	значення
1	технологія мережі	–	ethernet 100\1000	8	марка сервера	–	ARTLINE Business T15v20
2	топологія мережі	–	гібридна	9	операційна система робочих станцій	–	windows
3	середовище передачі	–	Вита пара кат. 5Е	10	операційна система сервера терміналів	–	Ubuntu 20.04
4	кількість вузлів мережі	шт	37	11	тип доступу до Internet	–	реальна IP, вита пара
5	марка головного комутатора	–	MikroTik CRS125 24G-1S-IN	12	термін окупності	рік	1,3
6	марка комутатора робочих груп	–	TP-LINK TL- SG116E	13	Чиста теперішня вартість, грн	–	20495,47
7	марка точки доступу	–	MikroTik RBCAPGI-5ACD2ND	14	ціна	грн	82962,03

						2024.КВР.123.418.18.00.00 ТБ	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії "ТК Галич"	Літ.	Маса	Масшт.
Розроб.		Яраш З В						
Керів		Лук В С			План приміщень		-	
Н.контр.		Юськів А В				Аркуш 1	Аркушів 1	
Затв.						ВСП ТФК ТНТУ КІ-418, м.Тернопіль		

ТАБЛИЦЯ IP-АДРЕСАЦІЇ В МЕРЕЖІ				
№ П.П	НАЗВА	IP-АДРЕСА	МАСКА	РОБОЧА ГРУПА/vlan
1	WS_1	192.168.11.11	255.255.255.0	WORK/11
2	WS_2	192.168.11.12	255.255.255.0	WORK/11
3	WS_3	192.168.11.13	255.255.255.0	WORK/11
4	WS_4	192.168.11.14	255.255.255.0	WORK/11
5	WS_5	192.168.11.15	255.255.255.0	WORK/11
6	WS_6	192.168.11.16	255.255.255.0	WORK/11
7	WS_7	192.168.11.17	255.255.255.0	WORK/11
8	WS_8	192.168.11.18	255.255.255.0	WORK/11
9	WS_9	192.168.11.19	255.255.255.0	WORK/11
10	WS_10	192.168.11.20	255.255.255.0	WORK/11
11	WS_11	192.168.11.21	255.255.255.0	WORK/11
12	WS_12	192.168.11.22	255.255.255.0	WORK/11
13	WS_13	192.168.11.23	255.255.255.0	WORK/11
14	WS_14	192.168.11.24	255.255.255.0	WORK/11
15	WS_15	192.168.11.25	255.255.255.0	WORK/11
16	WS_16	192.168.11.26	255.255.255.0	WORK/11
17	WS_17	192.168.11.27	255.255.255.0	WORK/11
34	SW_2	192.168.11.100	255.255.255.0	WORK/11
35	AP_1	192.168.11.110	255.255.255.0	WORK/11
33	S_1	192.168.11.120	255.255.255.0	WORK/11