

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Комп'ютерних наук і технологій

(повне найменування інституту, факультету)

Комп'ютерні системи та мережі

(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

бакалавра

(ступінь вищої освіти)

на тему Розробка мультитехнологічної оптоволоконної
мережі для аеропорту

Виконав: студент(ка) 4 курсу, групи
КНТз-517

Спеціальності 123 Комп'ютерна інженерія
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Комп'ютерні системи та мережі

Якименко М.В.

(прізвище та ініціали)

Керівник Зеленьова І.Я.

(прізвище та ініціали)

Рецензент

(прізвище та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування вищого навчального закладу)

Інститут, факультет інформатики та радіоелектроніки, комп'ютерних наук і технологій

Кафедра «Комп'ютерні системи та мережі»

Ступінь вищої освіти (освітній ступінь) бакалаврський

Спеціальність 123 Комп'ютерна інженерія
(код і найменування)

Освітня програма (спеціалізація) Комп'ютерна інженерія
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Завідувач кафедри Кудерметов Р.К.

« » 2021 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

Якименка Микити Вадимовича

(прізвище, ім'я, по батькові)

1. Тема проєкту (роботи) Розробка мультитехнологічної оптоволоконної локальної мережі.

керівник проєкту (роботи) Зеленьова Ірина Яківна, к. т. н., доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від «17» 03 2021 р. № 81

2. Строк подання студентом проєкту (роботи) 07 травня 2021

3. Вихідні дані до проєкту (роботи) основи організації локальних мереж, топологія, мережеві протоколи, технічні характеристики мережевого обладнання.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1) Аналіз та вибір методів побудови локальної мережі;

2) Вибір технічних засобів;

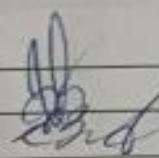
3) Аналіз та підключення системи моніторингу;

4) Захист інформації.

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

Структурна схема реалізації локальної мережі по приміщенню підприємства, план 1-го поверху, план 2-го поверху

6. Консультанти розділів проєкту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	Зеленьова І.Я., к. т. н., доцент		
Нормоконтроль	Зелік О.В., асистент		

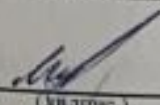
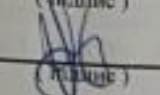
7. Дата видачі завдання 01.03.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз умов підприємства, топології побудови локальної мережі	01.03.2021 р.	
2	Аналіз моделей локальних мереж, видів кабелю	09.03.2021 р.	
3	Визначення з архітектурою локальної мережі	15.03.2021 р.	
4	Визначення мережевих протоколів, робота з ними	25.03.2021 р.	
5	Порівняння мережевого обладнання, систем безперебійного живлення та вибір відповідно до вимог підприємства.	01.04.2021 р.	
6	Сервіси моніторингу мережі, визначення параметрів	07.04.2021 р.	
7	Опрацювання захисту мережі на рівні обладнання та захист кабелю (вибір матеріалів)	13.04.2021 р.	
6	Оформлення отриманих результатів у ПЗ	21.04.2021 р.	
7	Оформлення графічного матеріалу	27.04.2021 р.	
8	Оформлення допоміжного матеріалу	04.05.2021 р.	

Студент

Керівник проєкту (роботи)


 (ПІДПИС)

 (ПІДПИС)

М.В. Яким

(ІНІЦІАЛИ ТА ПОСАДА)

І.Я. Зелень

(ІНІЦІАЛИ ТА ПОСАДА)

РЕФЕРАТ

ПЗ: 62 с., 34 рис., 2 табл., 11 джерел.

КОМП'ЮТЕРНА МЕРЕЖА, КОМУТАТОР, МАРШРУТИЗАТОР, РОБОЧА СТАНЦІЯ, СЕРВЕР, СТРУКТУРОВАНА КАБЕЛЬНА СИСТЕМА

Об'єкт розробки – оптоволоконна локальна мережа будівлі.

Метою роботи є розробка мультитехнологічної оптоволоконної локальної мережі будівлі КП «Міжнародний Аеропорт», проведення аналізу сучасних мережевих технологій, моделювання та дослідження розроблюваної мережі.

Проект складається з чотирьох розділів.

Перший розділ присвячено опису підприємства КП «Міжнародний Аеропорт». Проводиться детальний огляд об'єкта, опис використаних мережевих технологій та їх аналіз.

У другому розділі розкриті питання щодо використовуваного мережевого обладнання, типу кабелю, проміжного мережевого обладнання на підприємстві.

Третій розділ присвячено моделюванню локальної мережі в емуляторі Packet Tracer.

В кінці розділу надано рекомендації щодо покращення роботи локальної мережі та її модернізації відповідно до сучасних умов виробництва.

В четвертому розділі визначаються заходи безпеки з використанням мережевих протоколів та вибір допоміжних матеріалів для правильного монтажу СКС та подальшої її експлуатації з дотриманням вимог.

В результаті виконання дипломної роботи проведено аналіз, моделювання та дослідження розроблюваної локальної мережі.

ЗМІСТ

Вступ.....	6
1 Аналіз та вибір методів побудови локальної мережі.....	9
1.1 Аналіз умов підприємства.....	9
1.2 Топологія мережі.....	11
1.3 Стандарти Ethernet.....	15
1.4 Архітектура мережі.....	18
1.5 Кабельні системи.....	19
1.6 Мережеві протоколи.....	25
1.7 Постановка завдання розробки.....	29
2 Вибір технічних засобів.....	30
2.1 Вибір мережевого обладнання.....	30
2.2 Допоміжне мережеве обладнання для підключення декількох робочих місць за допомогою одного волокна.....	33
2.3 Вибір кабелю для реалізації локальної мережі.....	35
2.4 Вибір системи безперебійного живлення.....	39
3 Аналіз та вибір системи моніторингу.....	43
4 Забезпечення відмовостійкості мережі та захисту інформації.....	48
4.1 Захист інформації в телекомунікаційних мережах.....	48
4.2 Захист оптичного кабелю від зовнішніх пошкоджень.....	53
4.3 Забезпечення відмовостійкості мережі.....	54
Висновки.....	57
Перелік джерел посилання.....	58
Графічний матеріал:	
Плакат 1 – Структурна схема мережі підприємства	
Плакат 2 – Схема мережі 1-го поверху	
Плакат 3 – Схема мережі 2-го поверху	
Плакат 4 – Спрощена функціональна схема мережі	

ВСТУП

Стрімкий розвиток телекомунікаційних мереж у сучасному світі беззупинно веде суспільство до ускладнення взаємозв'язку між різними ланками виробництва, збільшення інформаційних потоків в усіх сферах суспільної діяльності. На сьогоднішній день майже кожен процес у житті сучасної людини не може повноцінно відбуватися без інформаційного обміну інформації та своєчасної її передачі, використовуючи різні засоби та системи зв'язку.

Зростання ринку мультисервісних послуг, впровадження нових телекомунікаційних і інформаційних технологій, їх конвергенції - це основні напрямки розвитку мереж телекомунікацій сьогодні. Широкосмугове підключення до Інтернету стало однією з найбільш успішних послуг всього кілька десятиріч тому, але за такий відносно малий проміжок часу кількість користувачів зросла до 200 млн., більшість із них поки обмежуються доступом до Інтернету з комп'ютера або ноутбука.

Сучасний розвиток комп'ютерних мереж характеризується їхньою конвергенцією. Всі, хто працює у сфері телекомунікаційних мереж намагаються зробити максимальний внесок для того, щоб побудувати універсальні мережі, які будуть однаково ефективно та швидко надавати послуги різноманітних типів. Одним з найнеобхідніших кроків їх розвитку є цифрування, що являє собою модернізацію мереж зв'язку загального користування на основі концепції NGN (Next Generation Network) - мереж зв'язку наступного покоління. У перспективі розвитку та розробки мереж нового покоління припускається створення мультисервісної, дійсно високотехнологічної мережі з винесенням функціональності послуг в граничні вузли мережі, створення досконалого керування послугами у вигляді окремої мережевої підсистеми, а також розширення номенклатури інтерфейсів для підключення устаткування, що надається операторами зв'язку. Мультисервісні мережі можуть бути створені як новий клас мереж, які матимуть змогу взаємодіяти з існуючими мережами.

Сутність мережі нового покоління полягає у переході від багатоплатформності, яка є дуже складною та витратною в побудові, обслуговуванні системи, до простої та ефективної мережі, розробленої спеціально для того, щоб надавати всі види послуг. З погляду технології, на нас чекає перехід від традиційної мережі до мережі нового покоління. Якщо сьогодні більш розвиненими та використовуваними є окремо існуючі мережі з комутацією каналів і мережі з комутацією пакетів, то на заміну їм придуть мультисервісні мережі, що здібні функціонувати як в першому, так і в другому режимі комутації. Одержані у результаті цього переходу мережі будуть пристосовані до роботи з усіма видами послуг. Цими мережами буде набагато легше керувати, і, водночас, якість послуг більшою мірою буде контролюватись самими клієнтами.

На сьогоднішній день розвиток інфокомунікаційних послуг здійснюється, в основному, в рамках комп'ютерної мережі Інтернет, доступ до послуг якої виконується через традиційні мережі зв'язку. Проте у ряді випадків послуги Інтернет, зважаючи на обмежені можливості її транспортної інфраструктури, не відповідають сучасним вимогам, що ставлять до послуг різних операторів зв'язку. У зв'язку з цим розвиток інфокомунікаційних послуг вимагає рішення задач ефективного управління інформаційними ресурсами з одночасним розширенням функціональності мереж зв'язку. У свою чергу, це стимулює процес інтеграції Інтернет і мереж зв'язку.

Для розробки та моделювання мультисервісних мереж можна застосовувати різні програмні середовища. На жаль, не всі програмні середовища можуть забезпечити максимальну швидкодію та зручність для моделювання, більшість з них не можуть здійснити пошук та вказати на конкретні помилки у створеній моделі.

Cisco Packet Tracer - це багатфункціональна програма моделювання мереж, яка надає можливість експериментувати з поведінкою створеної моделі за допомогою будь-яких змін. Будучи невід'ємною частиною комплексної середовища мережевої академії, Packet Tracer надає функції моделювання,

візуалізації, авторської розробки, атестації та співробітництва, а також полегшує викладання і вивчення складних технологічних принципів.

1 АНАЛІЗ ТА ВИБІР МЕТОДІВ ПОБУДОВИ ЛОКАЛЬНОЇ МЕРЕЖІ

1.1 Аналіз умов підприємства

Діяльністю КП «Міжнародний аеропорт» є прийом, відправлення, базування повітряних суден та обслуговування повітряних перевезень, що має для цих цілей аеродром, аеровокзал (зазвичай в великих аеропортах можна зустріти два і більше), один або кілька вантажних терміналів і інші наземні споруди та необхідне для функціонування підприємства обладнання.

На території розташована нова будівля терміналу, для якої і потрібно розробити локальну мережу. Будівля складається з двох поверхів.

На першому поверсі 7 приміщень: 3 приміщення з 2-ма робочими місцями в кожному; 4 приміщення з 1-м робочим місцем в кожному. Також у залі 8 робочих місць для реєстрації пасажирів і 1 місце на вході в аеропорт для зустрічі та інформування пасажирів.

На другому поверсі 14 приміщень: 1 приміщення – серверна; 9 приміщень з 2-ма робочими місцями в кожному; 1 приміщення – відділ продажу квитків, 4 робочих місця; 1 приміщення на 4 робочих місця; 1 кабінет на 1 робоче місце; 1 кабінет для розміщення обладнання для відеоспостереження – 2 робочих місця. Також у залі розміщено 5 точок митного контролю та буде розташовано 2 Wi-Fi точки у залі очікування.

За вимогами замовника, для 8 точок у залі на першому поверсі потрібно встановити окремий комутатор з 8-ма мідними та 2-ма оптичними портами з підтримкою швидкості до 1Гбіт/с; на другому поверсі розробити так само та додати дві точки мобільного доступу.

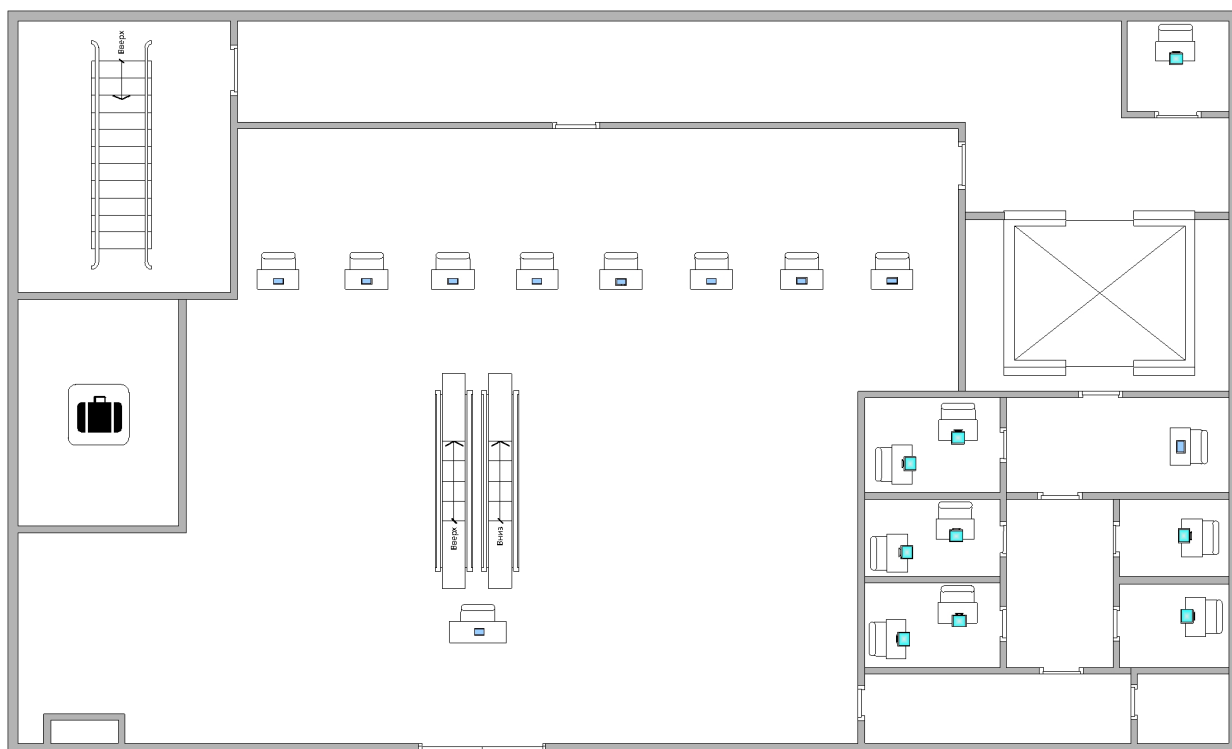


Рисунок 1.1 – Схема 1-го поверху

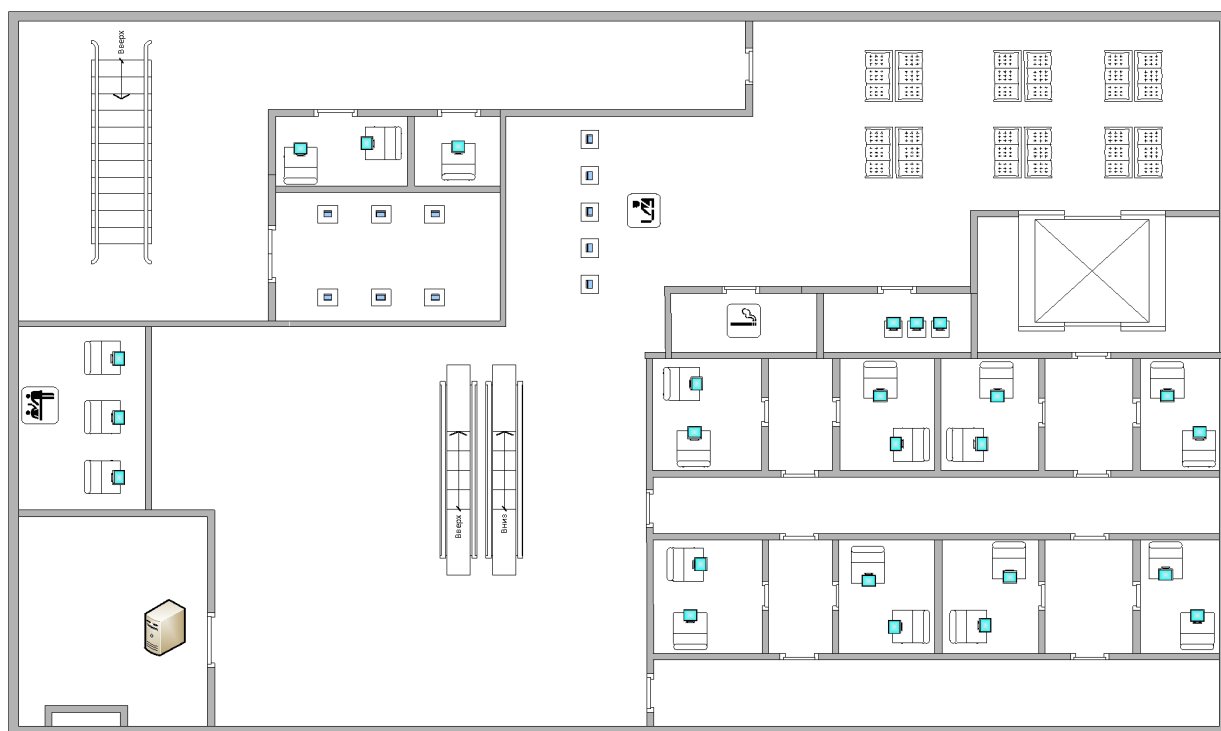


Рисунок 1.2 – Схема 2-го поверху

1.2 Топологія мережі

Топологія визначає спосіб з'єднання пристроїв мережі (комп'ютерів і комунікаційного обладнання) або їх груп фізичними лініями зв'язків.[1]

Поняття топології відноситься, перш за все, до локальних мереж, в яких є можливість прослідкувати структуру зв'язків. Порівняно з глобальними мережами, реалізація цього є неможливою через те, що структура зв'язків прихована від користувачів і може змінюватись з часом.

Під топологією локальної мережі розуміється конфігурація графа, вершинами якого є її вузли (комп'ютери та інше комунікаційне обладнання), а ребрами – фізичні лінії зв'язку. [1]

Якщо об'єднати одразу декількох вузлів (2-3) мережі проблем з лініями зв'язку не виникне. А ось коли таких вузлів в мережі буде від п'яти і більше, то кількість ліній буде від 10, що сильно ускладнить роботу мережі та призведе до сильного навантаження. Тому розрізняють два види топологій:

- повнозв'язні топології передбачають наявність окремої лінії зв'язку для будь-якої пари вузлів;
- неповнозв'язні топології одержуються з повнозв'язної топології шляхом видалення окремих ліній зв'язку.

Якщо в мережі налічується N вузлів, то для утворення повнозв'язної топології необхідно $N(N-1)/2$ ліній зв'язку. Тобто, така конфігурація виявляється громіздкою при збільшенні кількості вузлів і тому не набула поширення.

Для зменшення кількості використовуваних ліній зв'язку треба надати окремим вузлам мережі можливість пересилати повідомлення «транзитом». Такими вузлами можуть виступати як універсальні комп'ютери, так і спеціалізовані пристрої (мости, комутатори та ін.). В цьому випадку повідомлення від одного вузла до іншого можуть передаватись через «ланцюжок» транзитних вузлів, при цьому зменшується кількість безпосередніх, прямих з'єднань. Така конфігурація називається неповнозв'язною, бо не кожен комп'ютер з'єднується з

усіма. У порівнянні з попередніми конфігураціями, неповнозв'язні набули широкого поширення і стали основними в технологіях локальних мереж.

При об'єднанні більше ніж двох комп'ютерів, зі зростанням кількості вузлів мережі стрімко зростає кількість варіантів її з'єднань. Це відбувається за рахунок неповнозв'язних конфігурацій.

Існують три базові топології локальних мереж:

- шина (Bus) – всі комп'ютери підключаються до однієї спільної лінії зв'язку;
- зірка (Star) – до одного центрального комп'ютера приєднується решта периферійних комп'ютерів, причому кожний з них використовує окрему лінію зв'язку;
- кільце (Ring) – комп'ютери послідовно об'єднуються в «кільце»: кожен з них отримує дані лише від попереднього і передає дані лише наступному. [1]

Також базові топології можна з'єднувати між собою, змінювати відповідно до своїх вимог та створювати більш складні, змішані топології.

В топології «шина» всі вузли мають рівноправний доступ до лінії зв'язку, яка використовується ними по черзі, як показано нижче – на рисунку 1.3.

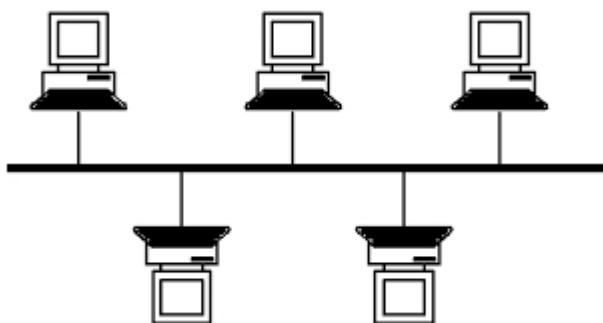


Рисунок 1.3 – Топологія «Шина»

Топологію, в якій один з вузлів виступає у ролі центрального та до якого підключають інші вузли, називають «зіркою». Найчастіше для головного вузла використовують комутатори. Обмін інформацією між периферійними вузлами

здійснюється виключно через центральний вузол, тому він виявляється найбільш завантаженим, як показано на рисунку 1.4.

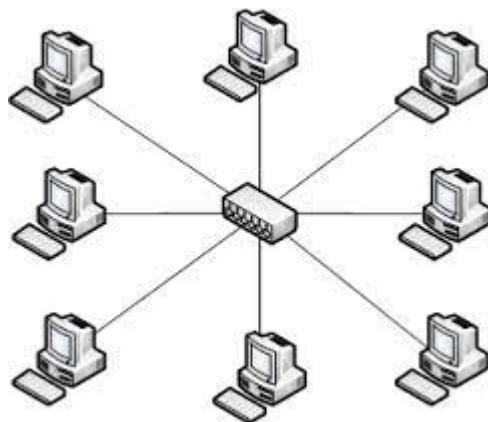


Рисунок 1.4 – Топологія «Зірка»

В топології «кільце», що показана на рисунку 1.5, кожний вузол сполучається лініями зв'язку лише з сусідніми: від одного одержує інформацію, а іншому передає.

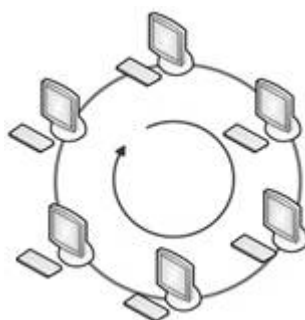


Рисунок 1.5 – Топологія «Кільце»

Базові топології є основою для створення інших, більш складних конфігурацій. Так у результаті комбінації кількох мереж з топологією «зірка» утворюється топологія «дерево» (tree), показана на рисунку 1.6. При цьому в ієрархічному порядку об'єднуються лише центральні вузли.[1]

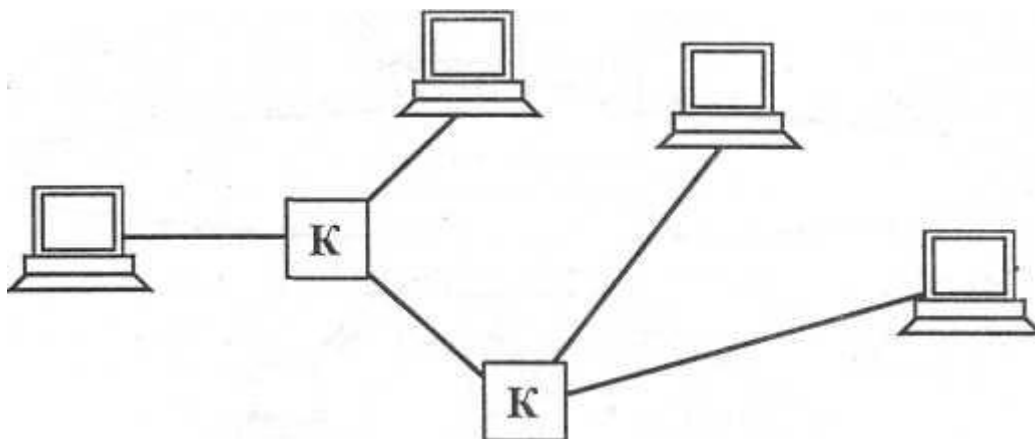


Рисунок 1.6 – Топологія «Дерево»

Досить поширеною є зірково-шинна (Star-Bus) топологія, показана на рисунку 1.7, в якій підмережі з топологією «Шина» підключаються до спільного центрального вузла.

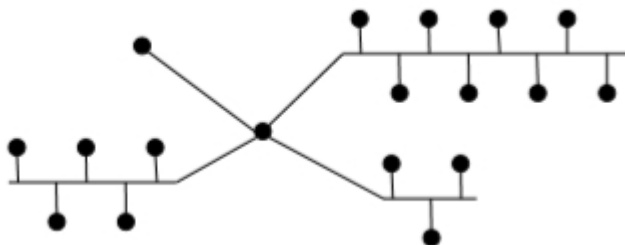


Рисунок 1.7 – Топологія «Зірка-шина»

Центральні вузли «Зірки» можуть об'єднуватись між собою, утворюючи, так названу, магістральну або опорну шину. Таким чином вдається комбінувати переваги шинної і зіркової топологій, а також легко нарощувати мережу.[1]

У разі об'єднання центральних вузлів зірок у кільце утворюється зірково-кільцева (Star-Ring) топологія, яку показано на рисунку 1.8.

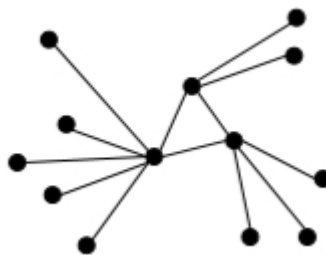


Рисунок 1.8 – Топологія «Зірка-кільце»

Вона дозволяє комбінувати переваги відповідно зіркової і кільцевої топологій, наприклад, для збільшення розмірів мережі.

1.3 Стандарти Ethernet

Можна сказати, що архітектура Ethernet об'єднує в собі цілий набір стандартів, що багато спільних рис, але є і деякі відмінності. Спочатку створенням та розвитком архітектури була фірма Херох, починаючи роботу над нею ще в середині 70-х рр. і тоді була представлена системою передачі зі швидкістю до 2,93 Мбіт/с. Коли ще дві компанії прийняли участь в розвитку та допрацюванні архітектури Ethernet, та саме завдяки цьому вона стала основою прийнятого в 1985 р. стандарту IEEE 802.3, який визначив для неї наступні параметри:

- топологія – «шина»;
- метод доступу – CSMA/CD; швидкість передачі – до 10 Мбіт/с;
- середовищем передачі виступає коаксіальний кабель;
- максимально допустима довжина сегменту мережі – до 500 м;
- максимальна довжина мережі – до 2,5 км;
- максимальна кількість комп'ютерів в сегменті – 100;
- максимальна кількість комп'ютерів в мережі – 1024.

У початковій версії Ethernet було передбачено застосування коаксіального кабелю двох видів – «товстого» і «тонкого» (стандарти 10Base-5 та 10 Base-2, відповідно), однак на початку 90-х рр. також з'явилися специфікації для побудови мереж Ethernet з використанням виті пари (10Base-T) та оптоволокна (10Base-FL). Пізніше, у 1995 р, було опубліковано стандарт архітектури Fast Ethernet (IEEE 802.3u), що забезпечує передачу на швидкостях до 100 Мбіт/с, у 1998 р. – стандарт Gigabit Ethernet (IEEE 802.3z та 802.3ab), а в 2002 – стандарт 10 Gigabit Ethernet (IEEE 802.3ae).[1]

(IEEE 802.3z та 802.3ab), а в 2002 – стандарт 10 Gigabit Ethernet (IEEE 802.3ae).[1]

Слід зазначити що у сучасних версій Ethernet вже не передбачається використання топології шина. Також залишилося дуже мало мереж, в яких для роботи використовується коаксіальний кабель. Однією з таких систем є Супутникова Станція Зв'язку на базі Тоoway.

Таблиця 1.1 – Характеристики різних стандартів Ethernet

Реалізація	Швидкість передачі даних, Мбіт/с	Топологія	Середовище передачі	Максимальна довжина кабелю, м
<i>Ethernet</i>				
10Base-5	10	«шина»	товстий коаксіальний кабель	500
10Base-2	10	«шина»	тонкий коаксіальний кабель	185; реально – до 300
10Base-T	10	«зірка»	вита пара	100
10Base-FL	10	«зірка»	оптоволокно	500 (станція концентратор); 2000 (між концентраторами)
<i>Fast Ethernet</i>				
100Base-TX	100	«зірка»	вита пара категорії 5 (використовується дві пари)	100
100Base-T4	100	«зірка»	вита пара категорії 3, 4 або 5 (використовується чотири пари)	100

Продовження таблиці 1.1 – Характеристики різних стандартів Ethernet

Реалізація	Швидкість передачі даних, Мбіт/с	Топологія	Середовище передачі	Максимальна довжина кабелю, м
100Base-FX	100	«зірка»	багатомодове або одномодове оптоволокно	2000 (багатомодовий); 15000 (одномодовий); реально - до 40 км
<i>Gigabit Ethernet</i>				
1000Base-T	1000	«зірка»	кручена пара категорії 5 або вище	100
1000Base-CX	1000	«зірка»	спеціальний кабель типу STP	25
1000Base-SX	1000	«зірка»	оптоволокно	220-550 (багатомодовий), в залежності від типу
1000Base-LX	1000	«зірка»	оптоволокно	550 (багатомодовий); 5000 (одномодовий); реально – до 80 км
<i>10 Gigabit Ethernet</i>				
10GBase-x (x – набір стандартів)	10000	«зірка»	оптоволокно	300-40000 (залежно від типу кабелю і довжини хвилі лазера)

Основний недолік мереж Ethernet пов'язаний з використанням в них методу доступу до середовища CSMA/CD (множинний доступ з контролем несучої і виявленням зіткнень). Він проявляється коли збільшується кількість робочих станцій, тоді збільшується і кількість зіткнень, тим самим знижуючи пропускну здатність мережі та значно підвищує час передачі кадрів. Тому навантаження, що рекомендується для мереж Ethernet є рівень в 30-40% від загальної смуги пропускання. Але сьогодні цей недолік в мережі дуже легко усунути, бо на заміну концентраторів приходять комутатори та мости, до функціоналу яких входить «ізолювання» передачі даних між двома комп'ютерами в мережі від інших.[1]

Переваг у архітектури Ethernet дуже багато. По-перше, дана технологія достатньо проста в реалізації. Відповідно, Ethernet-пристрої є на порядок дешевшими ніж аналогічні пристрої інших мережевих архітектур. В Ethernet представлена можливість використання майже будь-якого типу кабелю, а

застосування оптоволокна дозволяє об'єднувати ділянки мереж, які розміщені далеко одна від одної. Сумісність різних варіантів Ethernet дуже висока, що дозволяє не лише нарощувати потужності мережі з використанням існуючої кабельної інфраструктури, а й легко розширювати мережу, підключаючи до неї нові, більш швидкісні сегменти. Тому на сьогоднішній день архітектура Ethernet є провідною в сфері локальних мережах.[1]

1.4 Архітектура мережі

Архітектура (від лат. architectura) – мистецтво проектування і будівництва. Архітектура системи відбиває склад і взаємозв'язок компонентів системи, тобто визначає технологію її функціонування.

Архітектура комп'ютерної мережі – це макет побудови мережі, де зображено основні елементи мережі, яка структура (топологія) мережі використовується, функції кожного її елементу, фізичну і логічну організацію взаємодії елементів мережі.[1] За її допомогою можна детально розглянути мережу та ознайомитися з усіма її аспектами.

За формою представлення комп'ютерних мереж розрізняють фізичну та логічну архітектури. Фізична архітектура – форма представлення комп'ютерної мережі у вигляді взаємодіючих апаратних засобів.

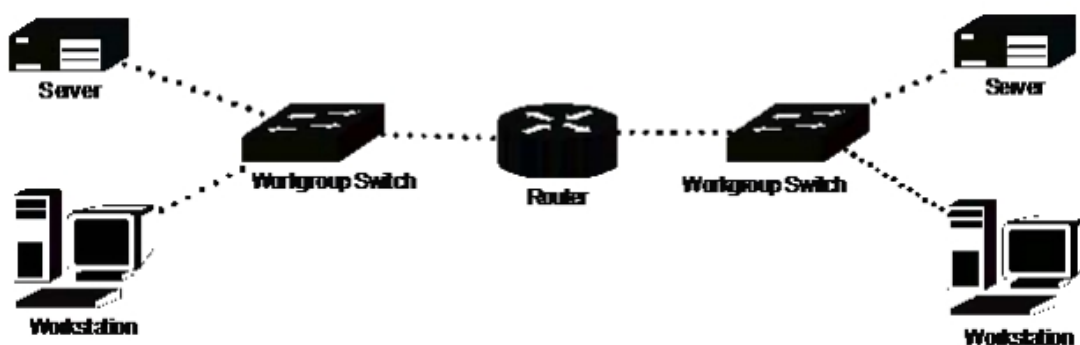


Рисунок 1.9 – Фізична архітектура мережі

Логічна архітектура – форма представлення комп'ютерної мережі у вигляді взаємопов'язаних елементів (функцій). Приклад логічної архітектури комп'ютерної мережі зображено на рисунку 1.10. Логічна архітектура відбиває цілісну технологію комп'ютерної мережі і може бути деталізованою через рівні фізичної архітектури.

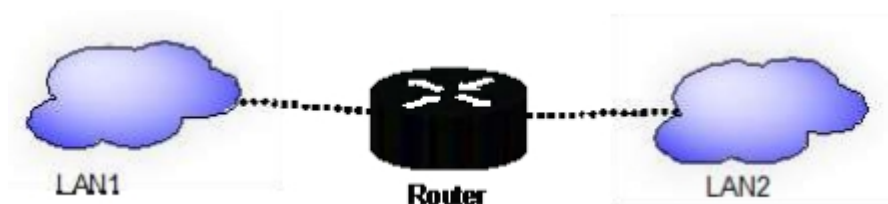


Рисунок 1.10 – Логічна архітектура мережі

1.5 Кабельні системи

Для цілей побудови та розвитку телекомунікацій у світі, саме кабельні системи стали використовуватися найпершими в історії.

Основними типами кабелів, які використовуються при побудові комп'ютерних мереж, є:

Вита пара

Сьогоднішні кабельні системи ґрунтуються на використанні так названої витої пари.

Вита пара (Twisted Pair) – кабель, що складається з двох скручених проводів у спільній ізоляції, як показано на рисунку 1.11.

Рівномірне розподілення зовнішніх шумів є сутністю та перевагою витої пари перед іншими мідними кабелями.



Рисунок 1.11 – Зовнішній вигляд витії пари

Якщо взяти два паралельних провідника не витії пари у яких різниця напруги складає 2В. Якщо вони опиняться під впливом зовнішнього шуму і один з провідників може потрапити в зону електромагнітного поля, що додатково утворює напругу 9В, а інший в зону поля з напругою 5В. Тоді різниця складатиме не 2В, а 6В, як показано на рисунку 1.12.[1]

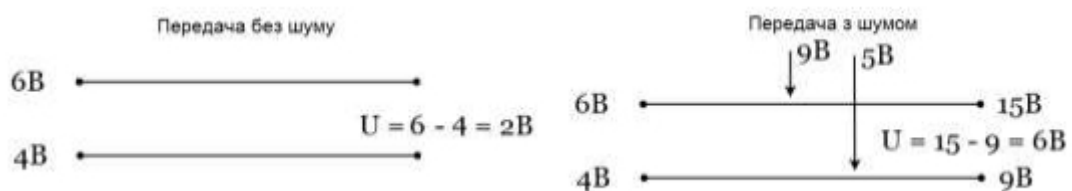


Рисунок 1.12 – Шуми у не витій парі

Для того, щоб зовнішнє джерело шуму рівномірно утворювало в провідниках напругу і не змінювало її різницю треба скрутити провідники, як у витій парі, як зображено на рисунку 1.13.

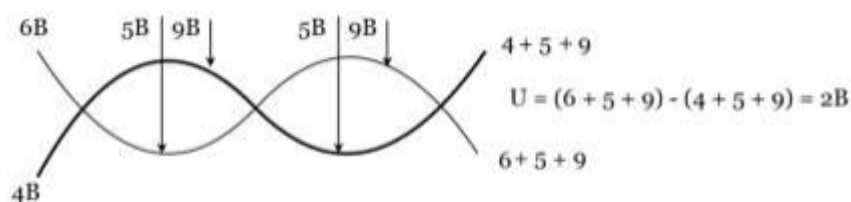


Рисунок 1.13 – Шуми у витій парі

Таблиця 1.2 – Категорії кабелів для телефонного зв'язку та доступу у мережу Інтернет

Категорія	Призначення і характеристики	Швидкість передачі
1	Звичайний телефонний кабель, в якому пари проводів не виті.	20 Кбіт/с
2	Кабель з витих пар для передачі даних у полосі частот до 1 МГц. Зараз використовується рідко.	100 Мбіт/с
3	Широко використовується для передачі даних і голосу в полосі частот до 16 МГц. Містить 9 витків на метр. Зараз найбільш поширений	10 Мбіт/с
4	Використовується для передачі даних в полосі частот до 20 МГц. Призначався для роботи в мережах по стандарту IEEE 802.5 (Token Ring Lan). Зараз використовується рідко.	16 Мбіт/с
5	Розрахований на передачу даних в полосі частот до 100 МГц. Містить не менше 27 витків на метр. На сьогодні найбільш досконалий кабель, що рекомендується для використання в сучасних високошвидкісних мережах (типу Fast Ethernet).	100 Мбіт/с
5e	Найбільш поширений в комп'ютерних мережах. Переваги – в меншій собівартості та товщині.	100 Мбіт/с (2 пари) 1000 Мбіт/с (4 пари)
6	Неекранований кабель (UTP) складається з 4 пар провідників, здатний передавати дані на відстань до 55 м.	10 Гбіт/с
6A	Складається з 4 пар провідників. Передає дані на відстань до 100 метрів. Кабель має або спільний екран (F / UTP), або екрани навколо кожної пари (U / FTP).	10 Гбіт/с
7	Кабель цієї категорії має загальний екран і екрани навколо кожної пари (F / FTP, або S / FTP).	10 Гбіт/с

Продовження таблиці 1.2 – Категорії кабелів для телефонного зв'язку та доступу у мережу Інтернет

Категорія	Призначення і характеристики	Швидкість передачі
7A	Кабель цієї категорії має загальний екран і екрани навколо кожної пари (F / FTP, або S / FTP). Полоса частот – до 1000 МГц.	10 Гбіт/с
8/8.1	Повністю сумісний з кабелем кат. 6A. Швидкість передачі даних до 40 Гбіт/с при використанні стандартних конекторів 8P8C. Кабель цієї категорії має або загальний екран, або екрани навколо кожної пари (F / UTP або U / FTP). Полоса частот – 1600....2000 МГц	40 Гбіт/с
8.2	Сумісний з кабелем кат. 7A. Швидкість передачі даних до 40 Гбіт/с при використанні стандартних конекторів 8P8C або GG45 / ARJ45 і TERA. Кабель має загальний екран і екрани навколо кожної пари (F / FTP або S / FTP). Полоса частот – 1600....2000 МГц	40 Гбіт/с

Волоконно-оптичні кабелі

Оптоволоконний кабель складається з одного або кількох оптичних волокон, що розміщуються у спільній захисній оболонці, всередині якої також знаходиться гідрофобний гель, що забезпечує цілісність оптичних волокон під час транспортування та експлуатації. Кожне волокно складається з центрального провідника, який має високий показник заломлення світла, і скляної оболонки, яка має низький показник заломлення світла. Основними видами оптичних волокон є:

- одномодовий кабель;
- багатомодовий кабель.

В одномодових кабелях застосовуються серцевини дуже малого діаметру, який є одного порядку, з довжиною хвилі – близько 8...9 мкм. Найбільш розповсюдженими та використовуваними є одномодові кабелі 9/125 мкм, де 9 мкм – діаметр серцевини – світловоду, а 125 мкм – діаметр скляної оболонки. В такому кабелі існує лише одна мода. Виробництво світловодів такого малого діаметру – це складний технологічний процес, і тому вартість таких кабелів дуже висока. Але

порівняно з багатомодовими кабелями, шоловною перевагою одномодових – це передача даних на великі відстані з високими швидкостями (десятки Гбіт/с).

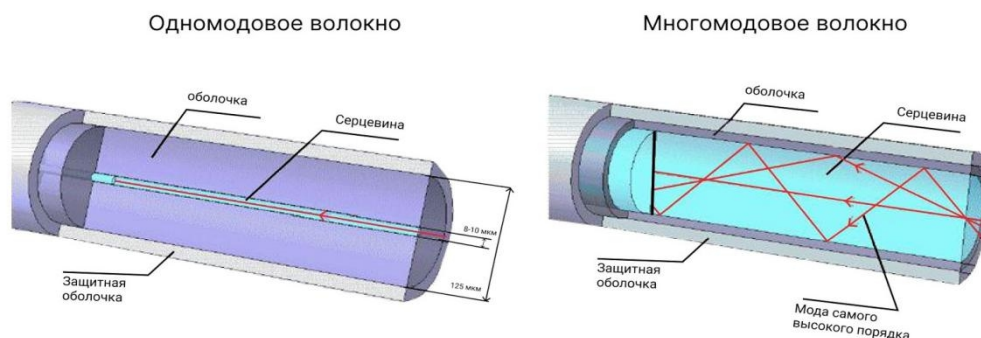


Рисунок 1.14 – Одномодовий та багатомодовий кабелі

Порівняно з одномодовими кабелями, у багатомодових використовують ширші серцевини, щоб зробити їх дешевшими. Технологія виготовлення є менш складною та не потребує таких великих затрат. Розповсюдженими є багатомодові кабелі діаметром 50/125 мкм, але в них може поширюватися кілька мод, що призводить до дисперсії імпульсу передачі, інтерференції променів, і в цілому веде до погіршення характеристик кабелю. Частіше за все багатомодові кабелі використовують при передачі даних на невеликі відстані (до 2000 м) з невисокими швидкостями (до 1 Гбіт/с).

В якості джерела світла використовуються напівпровідникові лазери, або світлодіоди з довжинами хвиль 850, 1300 або 1550 нм, що відповідають «вікнам прозорості» оптоволокон. В цілому, перевагами оптоволоконного кабелю є: висока перешкодозахищеність, невисоке затухання сигналів та висока швидкість їх розповсюдження.

Основними недоліками оптоволоконного кабелю є чутливість до іонізуючих випромінювань, що зменшують прозорість, чутливість до температурних

перепадів, що призводять до утворення тріщин, а також складність монтажу (мала гнучкість кабелю, оптична точність установки). Через складність монтажу оптоволоконний кабель продається у вигляді нарізаних шматків з встановленими роз'ємами.

Коаксіальний кабель

Коаксіальний кабель представляє собою електричний кабель, що складається з центрального мідного провідника і металевої оплітки (екрану), розділених шаром діелектрика і поміщених у зовнішню ізолюючу оболонку.

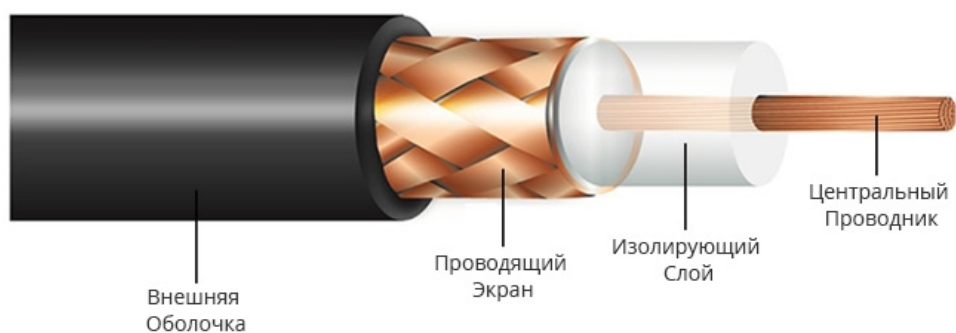


Рисунок 1.15 – Коаксіальний кабель, його структура

Металева оплітка відіграє подвійну роль – служить для передачі даних та захищає центральний провід від зовнішніх шумів.

Для побудови комп'ютерних мереж використовують товстий коаксіальний кабель (діаметр центрального провідника – 2,17 мм, зовнішнім діаметр – близько 1 см) і тонкий коаксіальний кабель (діаметр центрального провідника 0,89 мм, зовнішній діаметр – близько 0,5 см). Хвильовий опір обох кабелів однаковий і складає близько 50 Ом. [1]

Раніше коаксіальні кабелі використовувались досить широко, але на даний час вони використовуються лише для Супутникових Станцій Зв'язку (Тоoway) через широке використання витої пари і оптоволокна.

1.6 Мережеві протоколи

Протокол – це набір правил і технічних процедур, що регулюють здійснення зв'язку між комп'ютерами в мережі.

Стек протоколів – це комбінація протоколів, працюючих на одному комп'ютері. Навіщо потрібні протоколи? Безпосередньо процес передачі даних по мережі розбивається на кілька кроків. При цьому черговість виконання даних кроків чітко визначена. Завданням протоколів є визначення таких кроків і контроль за їх виконанням. Наприклад, якщо два протоколи будуть по-різному розбивати дані на пакети і додавати до них службову інформацію, тоді комп'ютер, який використовує один з цих протоколів, не зможе успішно зв'язатися з комп'ютером, на якому працює інший протокол. [2]

Основними протоколами є:

HTTP

Hyper Text Transfer protocol є основним для функціонування всіх інтернет-ресурсів. Робота протоколу HTTP пов'язана з наданням можливостей запиту ресурсів, що потрібно для віддалених систем.[5]

HTTP прийнято називати клієнт-серверним протоколом, бо саме відправка необхідних даних відбувається лише з однієї конкретної сторони. Головні особливості HTTP пов'язані з:

- простотою — легке сприйняття алгоритмів людьми;
- розширюваністю — щоб змінити щось у семантиці, буде достатньо усього-на-всього узгодження між серверами та клієнтами;
- сесійністю — відсутність послідовного зв'язку між запитами, кожна сесія має свій певний контекст;
- транспортним рівнем — завдяки управлінню на транспортному рівні протокол знаходиться за межами HTTP.

За допомогою HTTP можна керувати кешем, аутентифікацією, проксі, а також сесіями. Але в останній час є дуже актуальним перехід на HTTPS, який підвищує довіру до інтернет-ресурсу.

IP

Internet Protocol – це протокол маршрутизації на мережевому рівні TCP/IP. Об'єднання різних комп'ютерних мереж в одну глобальну мережу стало можливим саме завдяки цьому протоколу.[5] основне завдання протоколу IP – це доставка пакетів між чисельним та різноманітним мережевим обладнанням. Характерними властивостями протоколу є:

- відсутність надійності — він не є гарантом того, що доставка пакетів пройде без помилок, її можуть забезпечити лише на більш високих рівнях протоколів. IP не виключає дублювання, пошкодження, порушення порядку та навіть відсутність надсилання даних;
- унікальність — завдяки цьому протоколу кожен комп'ютер має свою унікальну IP-адресу, завдяки якій пристрої можуть знаходити і ідентифікувати один одного в інтернеті;
- фрагментованість — протокол проходить через різноманітні канали доставки, і в разі перевищення можливостей певних вузлів передбачено дроблення пакетів.

Даний алгоритм реалізований за допомогою таких видів, як IPv4 і IPv6. У моделі TCP/IP він відноситься до мережевого рівня.[5]

SSH

Протокол Secure Shell має місце на рівні додатків і призначений для дистанційного керування системою за допомогою надання захищеного каналу. Даний протокол є широко використовуваним в роботі багатьох технологій. Підключення по SSH мають такі особливості:

- шифрування — характерна властивість SSH — авторизація з використанням ключа доступу, що являє собою кодування всього трафіку, включно й паролі, за допомогою безлічі алгоритмів;

- безпеку — дана властивість витікає з попередньої, бо саме за допомогою шифрування підвищується надійність віддаленої роботи;
- можливість стиснення — ця властивість має місце при передачі інформації.

Копіювання файлів використовуючи SSH призводить для підвищення рівня захисту в процесі передачі інформації. Secure Shell прийнято називати протоколом прикладного рівня, а його безпосереднім призначенням — забезпечення віддаленого доступу.[5]

FTP

File Transfer Protocol — один з найстаріших прикладних варіантів. Завданням цього протоколу є доступ до віддалених хостів і передача програмного забезпечення.[5] Для того, щоб повністю розуміти, як працює FTP та його можливості, перш за все потрібно розібратися з його особливостями. Властивості протоколу:

- результативність — протокол є гарантом успішного надсилання або видачу помилки, завдяки застосуванню квотної системи;
- варіативність шифрування — в різних випадках буде можливість анонімного підключення або передача паролів і логінів відкритим текстом;
- вбудовану аутентифікацію — користувачі одразу будуть аутентифіковані в системі за замовчуванням;
- застосування декількох портів — FTP-протокол використовує, як мінімум подвійне підключення.

Бінарний режим передачі дозволяє зменшити витрати трафіку і часу, який необхідний для відправки великих файлів. Тобто слугує для економії трафіку та часу при відправці файлів.[5]

POP3

Post Office Protocol Version 3 — стандартний варіант на прикладному рівні, який використовується клієнтами email-сервісів. Головне завдання POP3 — забезпечення отримання пошти з віддаленого сервера за допомогою TCP-з'єднання.[5]

Крім цього стандарту, щоб отримати електронну пошту, також використовується ІМАР. Зараз у сучасних клієнтів, в основному, реалізовані обидва варіанти. Особливості POP3:

- постійний доступ до листів, які збережені на комп'ютері, навіть якщо відсутній зв'язок з мережею;
- відкриття вкладень одночасно з повідомленням;
- постійне звільнення пам'яті ящика — листи перезавантажуються на жорсткий диск комп'ютера.

Проте, не зважаючи на переваги, є й недолік — це ризик зараження користувацьких комп'ютерів вірусами. Також може з'явитися необхідність достатньо частого бекапу. Щоб правильно організувати резервне копіювання даних, необхідно заручитися підтримкою надійного хостинг-провайдера.[5]

MAC

Media Access Control – протокол, що розміщений на низькому рівні. Його завдання – ідентифікація пристроїв локальних мереж. Властивості MAC:

- унікальність — для кожного пристрою MAC-адреса унікальна, яка з самого спочатку задана виробником;
- захист від помилок — додатковий захист на цьому рівні можна забезпечити за допомогою створення і перевірки алгоритмів;
- контроль — MAC контролює доступ до фізичного середовища передачі.

Механізми управління доступом до каналу на MAC-рівні реалізовані як метод множинного доступу. Таким чином, відразу кілька станцій можуть застосовувати одне й те ж фізичне середовище.[5]

1.7 Постановка завдання розробки

Для інформаційного забезпечення та швидкого доступу до інформації необхідно спроектувати і розробити комп'ютерну мережу, яка повинна виконувати наступні функції:

- створення єдиного інформаційного простору, який буде мати можливість охопити всіх користувачів та кожному з них надати доступ до інформації, яка створена за допомогою різного програмного забезпечення та у різний час;
- підвищення достовірності інформації, а так само створення архівів даних, які можна використовувати надалі, але на даний момент необхідності в них немає;
- забезпечення ефективної системи накопичення, зберігання і пошуку необхідної інформації стосовно поточної роботи і для доступу і роботи з інформацією, яка знаходиться в архіві, за допомогою глобальних баз даних.

Розробка проекту локальної мережі повинна передбачати наступні етапи:

- Аналіз подібних існуючих систем;
- Побудова інформаційних потоків системи;
- Розробка структурної та функціональної схеми мережі;
- Вибір апаратних та програмних засобів;
- Організація захисту даних в мережі.

2 ВИБІР ТЕХНІЧНИХ ЗАСОБІВ

2.1 Вибір мережевого обладнання

За проханням клієнта в якості мережевого обладнання будуть розглянуті комутатори фірми D-Link, тому що в них дуже якісна продукція, відносно невисокої вартості, зручна та зрозуміла в експлуатації.

Розглянувши лінійку комутаторів D-Link DGS в наявності є один, який підходить нашим параметрам, це D-Link DGS-1210XS/ME.



Рисунок 2.1 – Комутатор D-Link DGS-1210XS/ME

Комутатор, який є хорошим інструментом для проведення корпоративних мереж, розроблений компанією D-Link. Оснащений 24 гігабітними портами Base-X SFP і 4 портами 10Gigabit Base-X SFP +. Всі порти підтримують автоматичне визначення типу використовуваного в них кабелю, а також різновиди стандарту 802.3 / u / ab / az / x / ae. Має додатковий консольний порт як засіб управління (роз'єм - RJ-45). [10]

Завдяки можливостям комутаційної матриці, даний комутатор здатний забезпечити швидкість передачі даних до 128 Гбіт в секунду об'ємом до 94.24 mpps. Має так само вбудовану таблицю MAC-адрес на 16 тисяч записів, ОЗУ на 256 МБ DDR3 і Flash-пам'ять на 32 Мб. Підтримує функції другого і третього

рівнів, багатоадресну розсилку другого рівня, функціонал для проведення віртуальних локальних мереж VLANs, функціонал якості обслуговування пропускної смуги QoS, засоби захисту та управління і кілька інших стандартів і технологій. Керувати цим пристроєм і мережею Ви зможете за допомогою WEB-інтерфейсу, Telnet, TFTP-клієнта (всі три технології з підтримкою протоколів IPv4 / IPv6) і, як уже згадувалося раніше, за допомогою безлічі інших функцій.[10]

Інтерфейси:

- 24 порти 100 / 1000Base-X SFP;
- 4 порту 10GBase-X SFP +;
- Авто визначення MDI / MDIX для всіх портів на основі виті пари;
- Індикатори: Power, Console (на пристрої), Link / Active / Speed (на порті), Fan Error;
- Мережеві кабелі: UTP категорії 5, 5e (макс. 100 м), консольний порт, RJ-45;
- Комутаційна матриця: 128 Гбіт / с;
- Швидкість перенаправлення 64-байтних пакетів: 95,24 Mpps;
- Таблиця MAC-адрес: 16K записів;
- Об'єм оперативної пам'яті: 256 Мб DDR3;
- Буфер пакетів: 1,5 Мб;
- Flash-пам'ять: 32 Мб.

Стандарти та функції портів:

- IEEE 802.3 10Base-T Ethernet (мідна кручена пара);
- IEEE 802.3u 100Base-TX Fast Ethernet (мідна кручена пара);
- IEEE 802.3ab 1000Base-T Gigabit Ethernet (мідна кручена пара);
- IEEE 802.3az;
- Автоузгодження;
- Управління потоком IEEE 802.3x;
- IEEE802.3ae 10 Gigabit Ethernet.

Основне програмне забезпечення:

- Функціонал другого рівня;
- Багатоадресна розсилка другого рівня;

- VLAN;
- Функціонал третього рівня;
- Якість обслуговування / QoS;
- Списки управління доступом (ACL);
- AAA;
- функціонал безпеки;
- OAM;
- функції управління;
- MIB;
- IETF;
- IPv6.
- Напруга на вході: 100-240 В змінного струму, 50-60 Гц;
- MTBF (годинник): 243 237;
- Рівень шуму: 48,9 дБ;
- Тепловиділення: 115,17 BTU / ч;
- Макс. споживана потужність: 33,4 Вт / 16,7 Вт (в режимі очікування);
- Система вентиляції: 2 вентиляторів Smart;
- Захист від статичної електрики: всі Ethernet-порти підтримують стандарт IEC61000-4-5 вбудованої захисту від статичної електрики 6 кВ;
- Температура: робоча від -5 до 50 ° C, зберігання від -20 до 70 ° C.
- Вологість: від 0% до 95% без конденсату для експлуатації та зберігання;
- Розміри: 440 мм x 210 мм x 44 мм;
- Для установки в стандартну 19-дюймову стійку.

Мережа буде реалізована “Деревом”, тому нам знадобиться 2 таких комутатори.

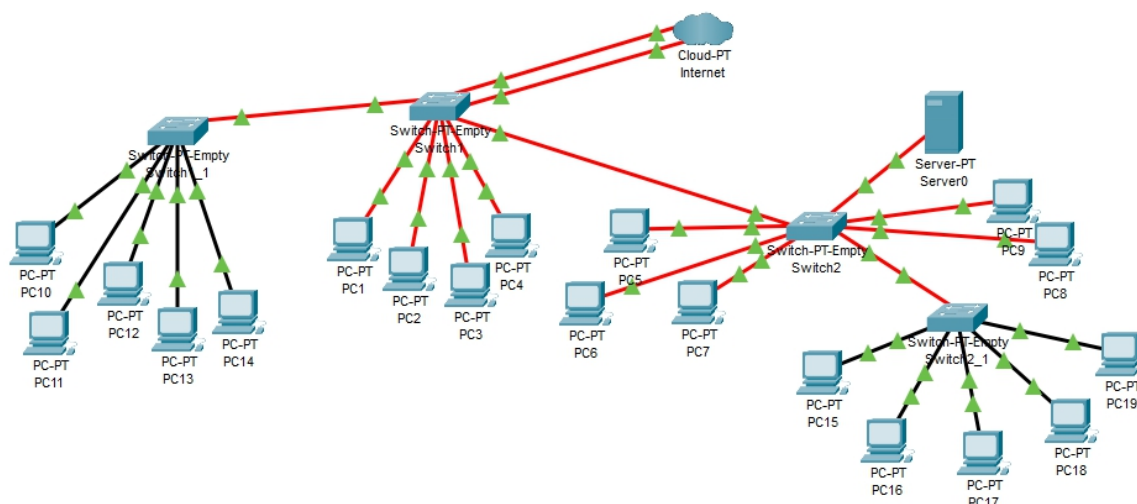


Рисунок 2.2 – Спрощена функціональна схема мережі у Cisco Packet Tracer

Схема є спрощеною, бо у програмі Cisco Packet Tracer можна моделювати лише обладнання Cisco, але це не завадило зробити хоча б тестовий варіант мережі. На рисунку зображено цілком робочу схему мережі мережі.

2.2 Допоміжне мережеве обладнання для підключення декількох робочих місць за допомогою одного волокна

В якості проміжного мережевого обладнання будуть використовуватися 2 комутатори D-Link DGS-1210-10P/ME.

Комутатор DGS-1210-10P / ME є ідеальним рішенням для застосування в мережах Metro Ethernet. Даний комутатор оснащений 8 портами 10/100 / 1000Base-T з підтримкою PoE для підключення по витій парі, а також 2 SFP-портами, що застосовуються для організації підключення до високошвидкісної магістралі. Захист від статичної електрики 6 кВ забезпечує стійкість до перепадів напруги, а повний набір функцій безпеки і аутентифікації захищає мережу від внутрішніх і зовнішніх загроз.[11]

8 портів даного комутатора підтримують стандарт IEEE 802.3at PoE. Кожен порт PoE подає харчування потужністю до 30 Вт при загальному бюджеті комутатора 78 Вт, що дозволяє користувачам підключати до DGS-1210-10P / ME пристрої, сумісні зі стандартом 802.3at. Це дозволяє розміщувати обладнання в важкодоступних місцях незалежно від розташування електричних розеток і мінімізувати прокладку кабелю.[8]

Комутатор DGS-1210-10P / ME підтримує протоколи Spanning Tree (STP): 802.1D-2004 edition, 802.1w і 802.1s. Протоколи STP дозволяють організувати резервний маршрут передачі даних, який використовується в разі виникнення несправностей в мережі. DGS-1210-10P / ME також підтримує агрегування каналів 802.3ad, яке забезпечує об'єднання в групи декількох портів і, як наслідок, збільшення смуги пропускання і підвищення відмовостійкості з'єднань. Даний комутатор підтримує стандарт 802.1p для управління якістю обслуговування (QoS), що дозволяє класифікувати трафік в режимі реального часу на 8 черг з використанням механізмів їх обробки Strict і Weighted Round Robin (WRR). Класифікація пакетів здійснюється на основі TOS, DSCP, MAC-адреси, IPv4 / IPv6-адреси, VLAN ID, номера порту TCP / UDP, типу протоколу або вмісту пакетів, що визначається користувачем, і надає можливість гнучкого налаштування для певних мультимедійних додатків, таких як VoIP або IPTV. [11]

DGS-1210-10P / ME підтримує управління доступом 802.1X на основі порту вузла, можливість створення гостьового VLAN, а також аутентифікацію RADIUS / TACACS + для управління доступом до мережі. Функція IP-MAC-Port Binding дозволяє контролювати доступ комп'ютерів до мережі на основі їх IP- і MAC-адрес, а також порту підключення, розширюючи, таким чином, можливості контролю над доступом. Вбудована функція D-Link Safeguard Engine [™] забезпечує ідентифікацію і пріоритизацію пакетів, призначених для обробки процесором комутатора, з метою запобігання шкідливих атак, здатних перешкодити нормальному функціонуванню комутатора. Крім того, функція списків управління доступом (ACL) підвищує безпеку і продуктивність мережі.

[11] Зовнішній вигляд комутатора D-Link DGS-1210-10P/ME представлений на рисунку 2.3



Рисунок. 2.3 – Комутатор D-Link DGS-1210-10P/ME

2.3 Вибір кабелю для реалізації локальної мережі

Завод «Одескабель» був заснований в 1949 році. За всі роки постійного розвитку, підприємство стало одним з найбільших та відомих виробників кабелів зв'язку в Україні і одним з провідних заводів з виробництва кабелів у країнах Східної Європи.

Будучи спеціалістом по виробництву телекомунікаційних кабелів, Одеський кабельний завод засвоює і випускає широкий асортимент мідних і волоконно-оптичних кабелів зв'язку, радіочастотних, а також цифрових або LAN-кабелів на які є попит в останні десятиліття та номенклатура яких є найширшою в країнах ЄС.

Основними споживачами продукції «Одескабель» є компанії, що працюють в сфері телекомунікацій, енергетики, будівництва, машинобудування, гірничодобувної галузі і ряді інших галузей. В Україні споживачами продукції «Одескабель» є найбільші оператори зв'язку - «Укртелеком», «Київстар»,

«Lifecell», «Інтертелеком», група компаній «Вега», атомні електростанції, залізниця, «Укренерго», «Укртранснафта», «Нафтогаз», «Криворіжсталь» та інші.

Волоконно-оптичні кабелі виробництва «Одескабель» поділяються на такі види, виходячи з області застосування та найчастіше використовуваних у телекомунікаціях:

- для прокладки всередині будівель;
- неброньований для кабельної каналізації;
- броньований для кабельної каналізації;
- для укладання в ґрунт;
- підвісний самонесучий;
- з тросом.

Кабелі для прокладки всередині будівель поділяють на розподільні, з яких формується мережа в цілому, і абонентські, які використовуються безпосередньо для прокладки по приміщенню до кінцевого споживача.

Конструкція оптоволоконних кабелів для прокладки в будівлях включає в себе оптичне волокно, захисне покриття і центральний силовий елемент, наприклад, пучок арамідних ниток.[1] До оптичного кабелю, що прокладається в приміщеннях, є особливі вимоги з протипожежної безпеки, такі як нерозповсюдження горіння і низьке димовиділення, тому в якості оболонки для них використовується не поліетилен, а поліуретан. Інші вимоги - це низька маса кабелю, гнучкість і невеликий розмір. З цієї причини багато моделей мають полегшену конструкцію, іноді з додатковим захистом від вологи. Так як протяжність оптики всередині будівель зазвичай невелика, то і загасання сигналу незначне і не впливає на передачу даних. Кількість оптичних волокон в таких кабелях не перевищує дванадцяти. На рисунку 2.4 зображена структура кабелю для прокладки всередині будівель – це кабель ОКТ-Д (1,0) П-2Е1 (2-волоконний).



Рисунок 2.4 – Оптичний кабель ОКТ-Д (1,0) П-2Е1 для прокладки всередині будівлі

Оптичний кабель ОКТ-Д (1,0) П-2Е1 можна використовувати, як самонесучий.

Броньовані оптоволоконні кабелі використовуються при наявності великих зовнішніх навантажень, особливо, на розтягнення. Бронювання може бути різним, стрічковим або дротяним, останній підрозділяється на одно- і двоповівне. Кабелі з стрічковим бронюванням використовуються в менш агресивних умовах, наприклад, при прокладці в кабельної каналізації, трубах, тунелях, на мостах.[1] Стрічкове бронювання являє собою сталеву гладку або гофровану трубку товщиною в 0,15-0,25 мм. Гофрування, за умови, що це єдиний захисний шар кабелю, є кращим, тому що оберігає оптоволокну від гризунів і в цілому підвищує гнучкість кабелю. При більш суворих умовах експлуатації, наприклад, при закладці в ґрунт або на дно річок використовуються кабелі з дротяною бронею.[1]

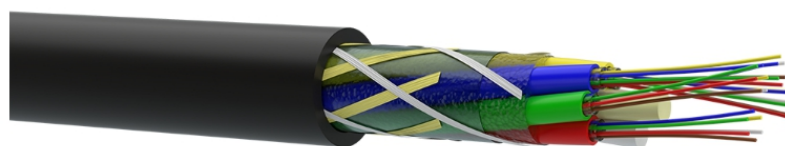


Рисунок 2.5 – Неброньований оптичний кабель для кабельної каналізації



Рисунок 2.6 – Броньований кабель для кабельної каналізації та закладання у ґрунт

Також кабель на рисунку 2.6 можна використовувати для закладання у ґрунт, тому що він має спеціальні характеристики для цього. Прокладка оптичного кабелю здійснюється в траншею або за допомогою кабелеукладачів. В умовах вологого ґрунту використовується модель кабелю, оптоволоконна частина якого укладена в герметичну металеву трубку, а бронеповіви дроту просочені спеціальним водовідштовхувальним компаундом.

Оптичні кабелю з тросом - це різновид самоутримних кабелів, які також використовуються для повітряної прокладки. Посилення оптичного кабелю тросом (профільованим сердечником) вважається досить ефективним методом. Сам трос є сталевим дротом, укладеним в окрему оболонку, яка в свою чергу з'єднується з оболонкою кабелю. Вільний простір між ними заповнюється гідрофобним гелем.



Рисунок 2.7 – Оптичний кабель з тросом

Отже, розглянувши всі види оптичного кабелю та ознайомившись з середовищем їх використання, ми зупинимося на кабелі для внутрішнього

прокладання марки Одескабель ОКТ-Д (1,0) П-2Е1, бо його набагато простіше монтувати у кабельні системи та короба, в нього невисока ціна та він не потребує особливих навичок при роботі.

2.4 Вибір системи безперебійного живлення

Система безперебійного живлення – це один з найважливіших елементів мережі. Вона необхідна для безперервної роботи мережевого обладнання та для запобігання виходу його із строю під час стрибків напруги або раптового відключення світла.

Спочатку ми розглянемо два джерела безперебійного живлення для першого поверху та на основі їх характеристик та вимог виберемо той, який підійде найбільше, а після цього оберемо одне з них для коректної та безперебійної роботи комутатора та серверу.

Першим ми розглянемо Powercom VGS-2000. ДБЖ з подвійним перетворенням серії Vanguard VGS призначений для захисту комп'ютерів, робочих станцій, серверів, груп комп'ютерів, мережевих комутаторів та іншого обчислювального і телекомунікаційного обладнання, що вимагає високої якості електропостачання. Можливість роздільного управління сегментами навантаження дозволяє здійснювати поетапне відключення обладнання при пропажі вхідної напруги, використовуючи енергію акумуляторних батарей найбільш ефективно.

ДБЖ в серії Vanguard передбачено енергозберігаючий режим. При його активації в залежності від якості енергопостачання ДБЖ автоматично перемикається між режимом подвійного перетворення і обхідним режимом. Якщо якість напруги електромережі незадовільна, ДБЖ постійно знаходиться в режимі подвійного перетворення. При хорошій якості напруги електромережі ДБЖ автоматично перемикається в обхідний режим, зменшуючи таким чином втрати

на перетворення. У той же час ДБЖ реєструє будь-які дефекти напруги в електромережі та миттєво повертається в режим подвійного перетворення. Використання режиму високої ефективності зменшує втрати енергії при перетворенні і збільшує термін служби акумуляторних батарей.

Сегментація навантаження – роздільне управління вихідними розетками ДБЖ (сегментами). Дозволяє розділяти навантаження таким чином, щоб найбільш відповідальна обладнання якомога довше залишалося забезпеченим гарантованим електроживленням. Разом з тим, сегментація навантаження дозволяє дотримуватися безпечної для ваших даних послідовності виключення мережевих пристроїв і серверів.



Рисунок 2.8 – Powercom VGS-2000

Наступним буде ДБЖ Powercom MAC-2000 ІЕС. Джерело безперебійного живлення Powercom MAC-2000, 2000. ВА, 2000. Вт (MAC-2K) має високий коефіцієнт ефективності, що дорівнює 0,97. Подвійне перетворення енергії забезпечує стабільну напругу у вигляді чистої синусоїди. Незалежно від частоти вхідного напруги, пристрій забезпечує стабільну частоту 50/60 Гц (визначається користувачем).

ДБЖ MAC виконані у вигляді вежі, призначені для захисту комп'ютерів, робочих станцій, серверів, груп комп'ютерів, мережевих комутаторів та іншого

обчислювального і телекомунікаційного обладнання, що вимагає високої якості електропостачання.

На жаль, в Інтернеті не вдалося знайти більше інформації про цей пристрій, бо він нещодавно вийшов.



Рисунок 2.9 – Powercom MAC-2000 IEC

Врешті решт, хоч завжди кажуть, якщо пристрій новіший, то він кращий, але зі свого досвіду можу сказати, що Powercom VGS-2000 досить непоганий в роботі і в складних та непередбачуваних умовах ніколи не підводив. Тому саме він і буде обраний для першого поверху. Для першого поверху знадобиться 2 одиниці.

Що ж стосується другого поверху, будуть представлені візуально два однакових ДБЖ, але по навантаженню один з них буде краще.

Почнемо з KSTAR UBR 2000VA. Джерело безперебійного живлення Kstar UBR серії - це універсальний засіб для забезпечення безперебійного живлення, а також вирішення проблем з напругою для серверних кімнат, обчислювальних

машин і сховищ даних, приватних домоволодінь, медичних клінік, виробничо-офісних об'єктів.

ДБЖ забезпечує повний контроль над параметрами струму і зміною параметрів експлуатації фізично і програмно. Прекрасно взаємодіючи зі стрибками, провалами і постійними розривами мережі, джерело безперебійного живлення Kstar забезпечує стабільну чисту синусоїду змінного струму на виході і розумний розподіл потенціалів потужності.

Режим «by Pass» дозволяє безперебійно синхронізовувати вхідні мережу з виходом ДБЖ, міняючи функціональні блоки ІБП, що в подальшому дозволить перевести навантаження на механічний «by Pass» для безпечного обслуговування або ремонту джерела безперебійного живлення.

Також дане ДБЖ має надійний захист від зміни форми кривої напруги і мікросекундних імпульсів, можливість роботи в мережах з нестабільною частотой і плавною стабілізацією напруги з високою точністю. Наявна можливість підключення акумуляторної батареї більшої ємності практично для всіх моделей ДБЖ. Моделі UBR серії надають розширений функціонал підключення, віддаленого управління і контролю за допомогою встановленого SNMP-модулю, масштабування потужності. За описом на сайті виробника вони однакові.



Рисунок 2.10 – KSTAR UBR 2000VA



Рис. 2.11 – KSTAR UBR 3000VA

Єдина відмінність між ними полягає в тому, що у першого вихідна повна потужність 2000ВА, а у другого 3000ВА. Тобто якщо брати ДБЖ з більшою потужністю, то сервер та мережеве обладнання буде працювати довше. Ще однією особливістю даного ДБЖ від тих, що будуть на першому поверсі в тому, що у цього зовнішнє підключення акумуляторної батареї. В даному випадку буде використовуватися акумуляторна батарея з номінальною напругою 12В та ємністю 150А*г, що забезпечить тривалий час роботи обладнання.

3 АНАЛІЗ ТА ВИБІР СИСТЕМИ МОНІТОРИНГУ

Моніторинг локальної мережі забезпечує видимість та контроль працездатності локальної комп'ютерної мережі, включаючи усі пристрої, які входять до складу мережі. Забезпечення контролю продуктивності мережі та відправка попереджень про різні проблеми та збої у ній надають інструменти для моніторингу локальних мереж. До таких проблем можна віднести переключення принтеру у автономний режим або проблеми із роботою маршрутизатора або комутатора.[3]

Розглянемо декілька провідних сервісів моніторингу мережі, такі як:

- OpManager. Комплексна система управління мережею, яку можна встановити на Windows та Linux. Інструмент використовує SNMP для контролю роботи мережевих пристроїв;
- Pandora NMS. Мережевий сервіс моніторингу, керований SNMP, який містить модулі управління IP-адресами та управління конфігурацією;
- Zabbix. Безкоштовний мережевий сервіс моніторингу з відкритим кодом, який також використовує SNMP для відстеження стану мережевих пристроїв.

Кожен сервіс моніторингу мають свої власні монітори локальної мережі та можуть відрізнятися складністю, починаючи інструментами контролю пакетів, закінчуючи повними системами адміністрування мереж. Завдяки моніторингу у користувачів є можливість використовувати основні функції такі, як можливість відслідковувати використання певного об'єкту мережі, забезпечуючи тим, зоб обладнання не перевантажувалося, контроль помилок та можливість повного контролю та забезпечення усього обладнання певної мережі. Монітори локальної мережі надають інформацію у режимі реального часу, щоб одразу була можливість усунути проблеми, перш ніж вони вплинуть на продуктивність. однак, ця функція доступна далеко не в кожному сервісі, тому до вибору системи моніторингу треба підходити з розумом, та враховувати кожен, навіть найменшу деталь.

За допомогою OpManager від компанії ManageEngine можна забезпечити належний моніторинг мережі малого підприємства. Він оснований на використанні протоколу SNMP. Зараз цей протокол вбудовують майже в усе нове обладнання для сумісності з мережею будь-якого типу та отримувати зворотній зв'язок про мережеву діяльність пристроїв мережі в режимі реального часу. Ще одна поширена технологія, яка лежить в основі системи OpManager – це методика моніторингу трафіку NetFlow. [3]

Дане програмне забезпечення може бути встановлено на будь-яку систему Linux або Windows. Він включає можливість взаємодії з базами даних на основі

SQL та MySQL, Active Directory та Eventlog. Інформаційна панель включає в себе можливість контролю пристрою через додаток на планшеті або смартфоні для доступу до інформації про стан мережі. [3]

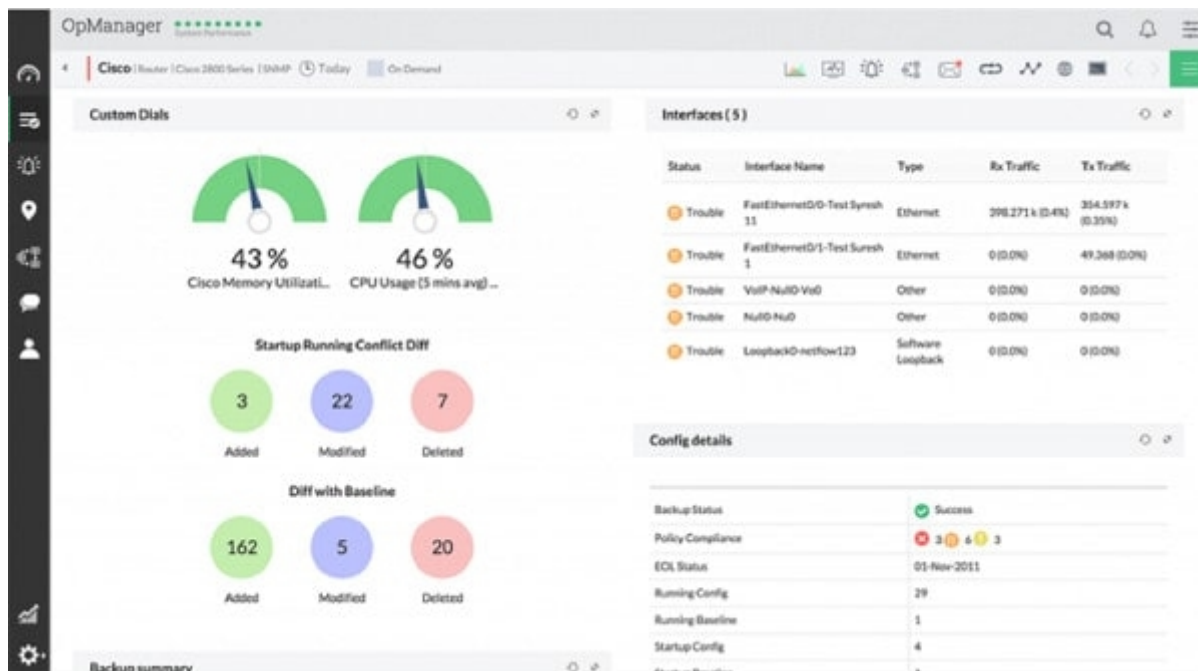


Рисунок 3.1 – Зовнішній вигляд сервісу OpManager

Установка Pandora NMS починається з розгортки мережі, яка дозволяє системі відображати вашу топологію. Мережева карта – це лише одна із графіків, що містяться на панелі інструментів, що допомагає відслідковувати систему з першого погляду.

Функції моніторингу NMS Pandora також засновані на процедурах SNMP тому що це один з найпоширеніших та зручних способів моніторингу з широким функціоналом. Робота системи основана на тому, що центральний вузол адміністратора мережі буде постійно опитувати систему для відстеження стану пристроїв. Стандартні сповіщення SNMP повідомляють про критичні умови, оскільки вони виникають, не чекаючи запиту статусу від менеджера мережі. Двигун Pandora здатний спілкуватися з пристроями, що використовують SNMPv1, v2c та v3.[3]

Пакет Pandora не охоплює моніторинг мережі в реальному часі саме так, як було описано вище. Ширша система, що називається Pandora FMS, включає управління адресами, а також вбудований IPAM. Менеджер IP-адрес може працювати як з IPv4, так і з IPv6 адресами.

Третім елементом Pandora FMS та дуже корисним на мій погляд, є система управління конфігурацією, що дозволяє відслідковувати стан виправлень програмного забезпечення компанії та виявляти неправомірне програмне забезпечення в системі.



Рисунок 3.2 – Зовнішній вигляд сервісу Pandora FMS

Zabbix – система з відкритим кодом. Перевага програмного забезпечення з відкритим кодом полягає в тому, що кожен може створювати додатки. Основна програма доступна безкоштовно, тому дуже багато доповнень.[3]

Незважаючи на те, що вона безкоштовна, приладова панель має дуже професійний вигляд. Передбачена можливість вимкнути елементи приладної панелі, щоб отримати найважливішу інформацію, помітну на найвизначніших ділянках екрана. Особливості інформаційної панелі включають списки даних про

події, графіки та кольорове кодування, щоб зробити важливу інформацію негайно впізнаваною.

Модуль моніторингу мережі в реальному часі Zabbix покладається на SNMP, як і в попередніх сервісах. Є дуже корисна можливість скористатися агентами пристроїв, які вже встановлені в обладнання виробниками. Система Zabbix може відслідковувати хмарні сервіси, продуктивність додатків, апаратні засоби, такі як стійки, ДБЖ та сервери. Система також може реалізовувати віддалений моніторинг.[3]

У Zabbix немає одразу написаного модуля звітності, але користуючись такою функцією, як відкритий код можна створити свої власні спеціальні звіти, які будуть зручніші для користувача і це є дуже великий плюс. Також можна спростити собі життя та пошукати вже готові формати звітів, які написані іншими користувачами на форумах спільнот веб-сайту Zabbix та цілком підходять по функціоналу за відповідними потребами.

Слабкою стороною багатьох протоколів мереж є те, що вони працюють на нижчих рівнях у стеку протоколів, що ускладнює шифрування. Zabbix включає шар шифрування, який блокує прослуховувачі та снупери та забезпечує моніторинг даних для безпечного проходження по мережі. Система шифрування робить доступними процедури аутентифікації, щоб ви могли створити різні рівні дозволу для доступу до даних, доступних на інформаційній панелі мережевого монітора.[3]

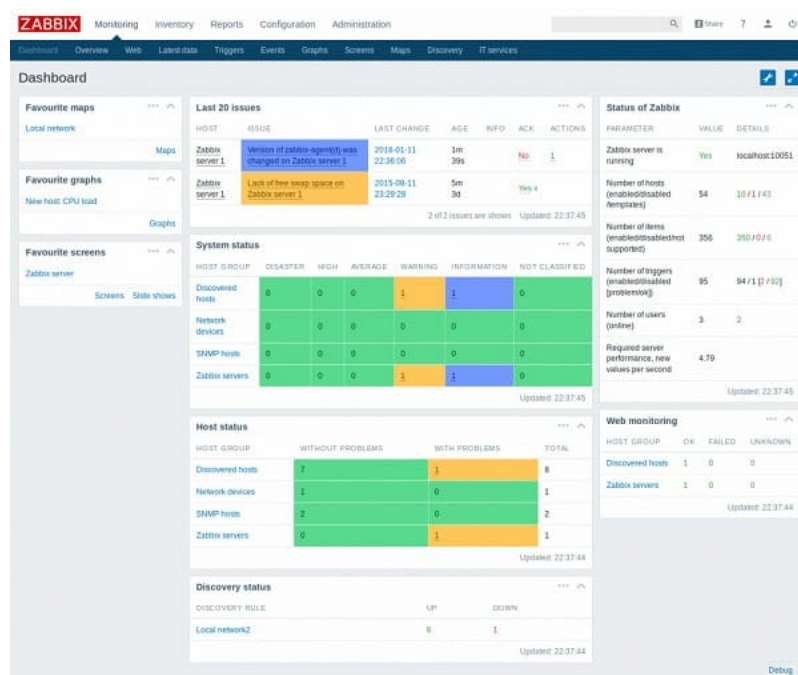


Рисунок 3.3 – Зовнішній вигляд сервісу Zabbix

Отже, провівши аналіз та ознайомившись з функціями, можливостями та складністю використання перелічених сервісів можна сказати, що найкращим є Zabbix за рахунок відкритого коду, який можна модернізувати та зробити зручніше для себе. Також він дуже простий у використанні, немає нічого зайвого та водночас він виглядає, як професійний та досконалий сервіс моніторингу.

4 ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ МЕРЕЖІ ТА ЗАХИСТУ ІНФОРМАЦІЇ

4.1 Захист інформації в телекомунікаційних мережах

На сьогоднішній день майже в усіх сферах повсякденної діяльності має місце дуже швидке зростання використання інформаційних технологій. Саме з цієї причини, проблема захисту інформації, користувачів, каналів передачі даних та інформаційних ресурсів від зловмисників є однією з найбільш актуальних.

Розміщення цінної інформації в комп'ютерах змушує зловмисників шукати все більш вишукані способи її викрадення та подальшого використання у власних цілях, а служби безпеки, відповідно, підсилювати контроль над нею з метою захисту. [8] Можливість викрадення важливої або конфіденційної інформації навіть без відома користувача є причиною складності створення системи захисту інформації, бо це робиться за допомогою прихованого шпигунського програмного забезпечення. Цінність деяких даних полягає у володінні ними, а не в їх знищенні або зміні.

Існують такі програмно-апаратні методи захисту локальних мереж:

- міжмережеві екрани;
- антивірусні програми;
- віртуальні захищені канали;
- криптографічний захист;
- біометричні технології аутентифікації.

Міжмережеві екрани можуть виконувати свої завдання на різних рівнях протоколів моделі OSI. На мережевому рівні виконується фільтрація вхідних і вихідних пакетів по IP—адресам (наприклад, не пропускаються пакети з мережі Internet, які направлені на ті сервери, доступ до яких зовні заборонено). [3] На транспортному рівні фільтрація відбувається ще й за номерами портів TCP і прапорців, що містяться в пакетах (наприклад, запити на встановлення з'єднання). На прикладному рівні виконується аналіз прикладних протоколів (FTP, HTTP, SMTP) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь—яких типів файлів: рекламної інформації або виконуваних програмних модулів). [5]

Дуже багато компанії створюють віртуальні приватні мережі(VPN), використовуючи загальнодоступну мережу Інтернет. Як показує практика, є ряд недоліків зв'язку через Інтернет, а саме те, що вона схильна до потенційних порушень захисту та конфіденційності. У той самий час VPN може гарантувати, що трафік, який направляється через Інтернет так само захищений, як і передача

всередині локальної мережі. Віртуальні мережі забезпечують колосальну економію витрат у порівнянні з вмістом власної мережі глобального масштабу.[8]

Антивірус – програмний засіб, призначений для боротьби з вірусами. Виходячи з визначення, основними завданнями антивірусу є:

- перешкодження проникненню вірусів у комп'ютерну систему;
- виявлення наявності вірусів у комп'ютерній системі;
- Безпечне знищення вірусів з комп'ютерної системи без нанесення ушкоджень іншим об'єктам системи;
- мінімізація збитку від дій вірусів;
- технології виявлення вірусів.

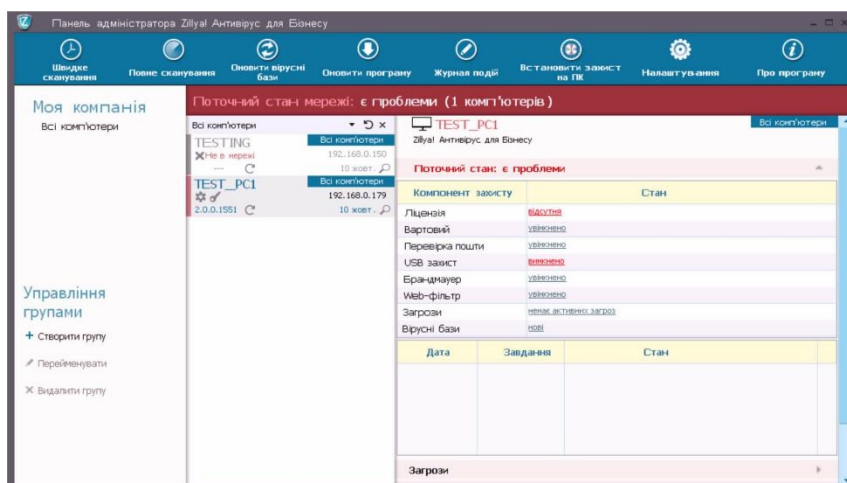


Рисунок 4.1 – Тестове налаштування антивірусу на комп'ютері

Криптографічний захист (шифрування) інформації – це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Порівняно з тайнописом, що приховує саме передачу повідомлення, зашифровані повідомлення передаються відкрито, але елементом, який приховується є лише їхній зміст. [8]

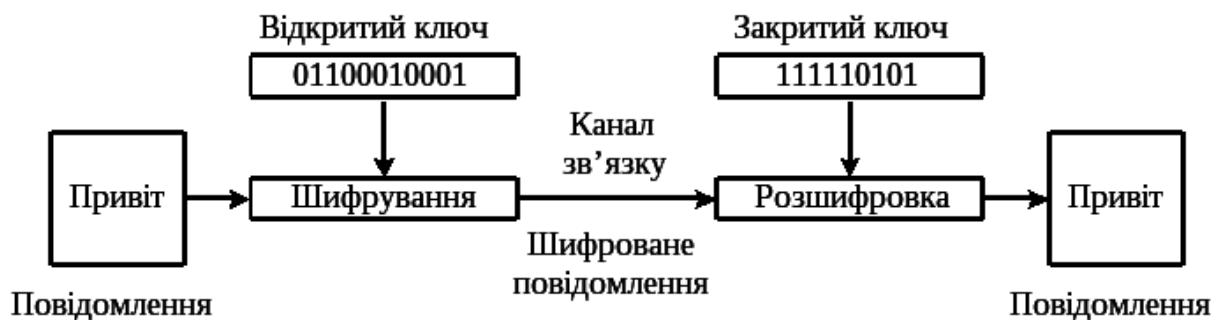


Рисунок 4.2 – Схема роботи криптографічного шифрування у мережі

Системи біометричного захисту використовують унікальні для кожної людини вимірювані фізіологічні характеристики для перевірки особи людини. Цей процес називається електронною аутентифікацією. Задачею цього процесу є визначення того, чи є людина саме тією особою, якою себе називає. Це відрізняє аутентифікацію від ідентифікації та авторизації. Мета ідентифікації – перевірити, чи відома ця людина системі, чи є самозванцем, наприклад перевіркою пароля, а авторизація полягає в наданні користувачеві доступу до певних ресурсів залежно від його особи. [8]

Також використовуються домени компанії в які мають доступ лише перевірені та зареєстровані співробітники компанії. Також встановлюються обмеження на використання USB-роз'ємів, для уникнення витіку секретної інформації. [8]

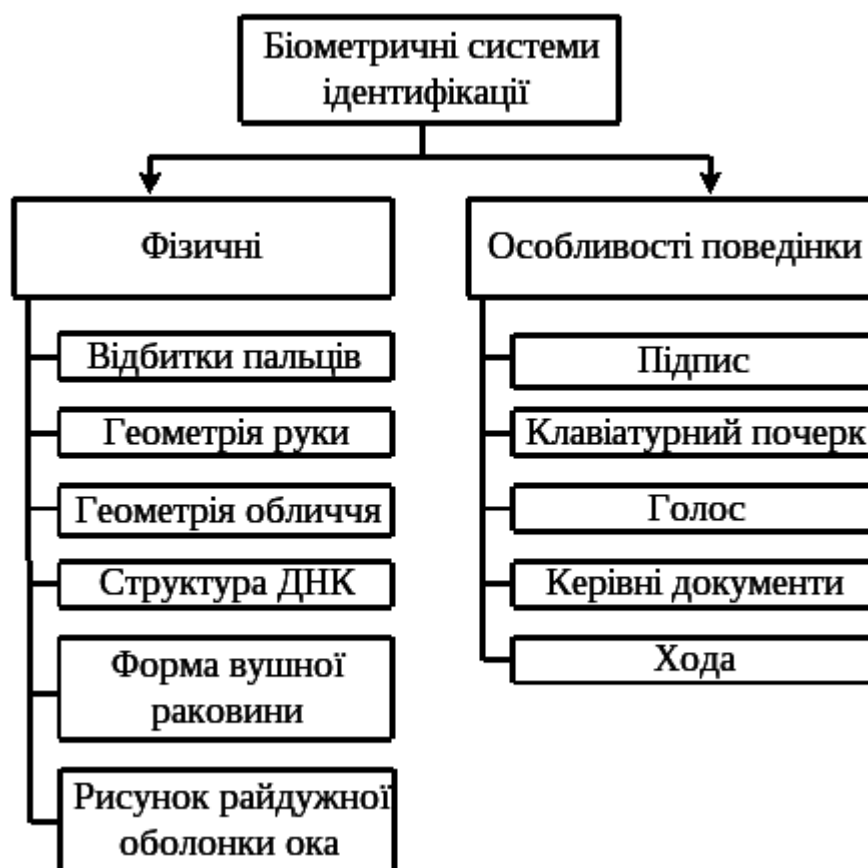


Рисунок 4.3 – Способи біометричної ідентифікації

Важливою особливістю авторизації є обмежені можливості користувачів, щоб уникнути установки неліцензійного програмного забезпечення. Завдяки цьому ніхто не зможе встановити програму на робочий комп'ютер або видалити вже наявну, а також мінімізується можливість проникнення вірусу в систему і \ зменшується ймовірність появи помилок через дії користувачів.

В налаштуваннях фільтрації пакетів в Firewall закриті майже всі порти і відкриті найнеобхідніші. Це робиться для того, щоб захистити комп'ютер від шкідливих програм і від злому системи. Також це зводить до мінімуму можливість використання персональної інформації і порушення роботи операційної системи або програм.

4.2 Захист оптичного кабелю від зовнішніх пошкоджень

При прокладанні оптичний станційний кабель повинен бути захищений від механічних пошкоджень, для чого він повинен прокладатися в пластмасовій трубі, коробі або з використанням кабельростів. Для захисту кабелю, що прокладений в отворах або трубах між приміщеннями, а також в отворах між поверхами, вільний простір обов'язково повинен бути заповнений негорючими матеріалами, які легко видаляються, наприклад мінеральною ватою. Для прокладання кабелів і проводів повинні встановлюватися такі конструкції: відкриті або закриті металеві повітряні жолоби (кабельрости, лотки), решітки, підпільні або підлогові канали (короба), трубопроводи, консолі.[4] Прокладання всіх видів та типів кабелів і проводів, як правило, передбачається у кабельних жолобах для відкритого прокладання. Жолоби, здебільшого, виконуються у вигляді горизонтальних і вертикальних сходових конструкцій (кабельростів), які забезпечують зручний доступ під час монтажу кабелів, проводів і шин, а також візуальний контроль за їх станом. Кабельні жолоби передбачаються з урахуванням виготовлення в майстернях за кресленнями типових матеріалів.[7]



Рисунок 4.4 – Монтаж кабелю всередині будівлі за всіма необхідними вимогами

Для монтажу кабелю будемо використовувати окремі кабельрости та гофру, щоб забезпечити найменшу вірогідність пошкодження кабелю.

4.3 Забезпечення відмовостійкості мережі

Однією з найважливіших задач є забезпечення відмовостійкості мережі, бо якщо один з вузлів перестане функціонувати, вийде з ладу або взагалі пошкодять лінію зв'язку провайдера, а такому підприємству, як аеропорт ні в якому разі не можна призупиняти свою роботу навіть на віть на хвилину. В іншому випадку будуть відкладені рейси, призупиниться робота основних служб і т.д.

Причинами виходи із ладу основних вузлів локальної мережі може бути велика навантаженість через велику кількість запитів та великий об'єм інформації. З цієї причини на практиці дуже часто в запас встановлюють допоміжне обладнання, наприклад, на яке можна переключитися у разі такої ситуації. На обладнанні, яке ми розглядали раніше є спеціально виділені порти до яких можна провести резерв та підключити. Коли працездатний основний канал, резервний буде у режимі очікування, а коли буде перебіг система сама переключиться на резерв. Це можна реалізувати за допомогою підключення та налаштування протокола LACP – це відкритий протокол агрегування каналів. Його призначення заключається в об'єднанні двох фізичних каналів в один логічний та використовується для підвищення пропускної здатності та відмовостійкості мережі. [2] Для роботи протоколів необхідно, щоб була однакова швидкість і ємність каналів. Функціями протоколу є відправка ініціюючим пристроєм пакетів LACPDU через інтерфейси на яких він підключений. Завдяки цим пакетам обладнання призначає приналежність портів до того чи іншого логічного каналу. У разі відключення одного з логічних каналів обладнання продовжує працювати на другого, але перед цим встановлює, який саме канал працює, завдяки цим пакетам.

Налаштування LACP на комутаторі S1

```
//Створення групи агрегування (тип каналу lacp і задаємо
алгоритм агрегування)
create link_aggregation group_id 1 type lacp
create link_aggregation group_id 1 type lacp
config link_aggregation algorithm mac_destination
config link_aggregation group_id 1 master_port 21 ports 21-24
state enable //Включення портів 21-24 в групу та налаштування 21
порту в якості майстер-порту.
config lacp_port 21-24 mode active//Налаштування активного
режиму роботи для портів 21-24.
```

Налаштування коммутатора S2

```
create link_aggregation group_id 1 type lacp
config link_aggregation algorithm mac_source
config link_aggregation group_id 1 master_port 21 ports 21-24
state enable
config lacp_port 21-24 mode passive
```

Також, окрім резервного мережевого обладнання всередині будівлі, особлива увага приділяється резервному каналу від іншого оператора зв'язку. Це робиться для того, щоб не стати жертвою раптового відключення каналу у зв'язку з пошкодженням оптичного кабелю оператору. Але проблема все одно залишається, бо в основному оптичні кабелі проходять у кабельній каналізації і завжди знайдуться люди, які захочуть вчинити злочин, шукаючи мідний кабель. Результатом таких походів є відсутність каналу обох операторів. Саме тому найбільш важливі сервіси повинні мати 3g/LTE – модеми, що забезпечать підтримку мережі. Вийнятками будуть лише митниця та прикордонна служба, тому що вони використовують супутниковий канал зв'язку на базі Tooway у якості резерву.

Що стосовно серверної – треба зробити мікроклімат. Завдяки цьому, постійно буде контролюватися температура всередині та буде забезпечена

довготривала робота обладнання та комфортні умови для експлуатації. Для цього будуть використовуватися датчики температури, регулярне провітрювання та прибирання приміщення, та обов'язкове встановлення датчиків диму та резервуар для пожежогасіння у разі виникнення пожежі.

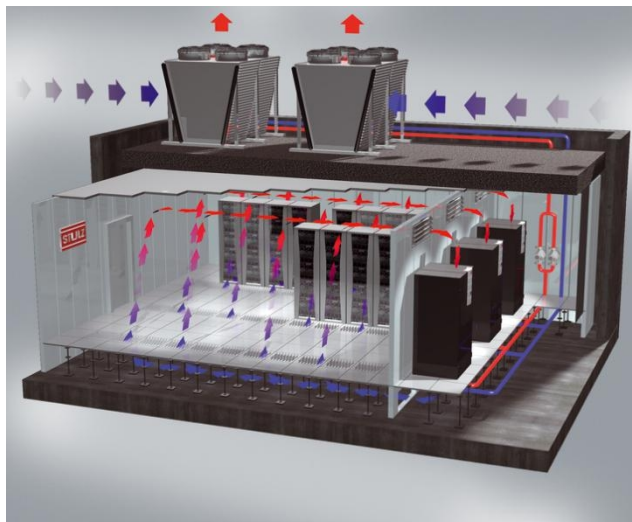


Рисунок 4.5 – Система провітрювання та кондиціювання серверного приміщення

ВИСНОВКИ

В результаті розробки мережі для КП «Міжнародний Аеропорт» ми розглянули можливі топології мережі, порівняли їх, та вибрали ту, яка підходить замовнику, та впровадили її. Ознайомилися з типами кабелів, з середовищем їх використання, порівняли з іншими кабелями, та на фоні цього стало зрозуміло, що оптичні кабелі на сьогоднішній день – це краще рішення, бо в нього дуже багато переваг порівняно з іншими, наприклад: низька затримки, вища швидкість обміну та передачі. Зроблено огляд обладнання, яке буде встановлене під час монтажу мережі, підібрана система безперебійного живлення та акумуляторна батарея для безперебійної роботи мережевого обладнання та серверу у разі непередбачуваних ситуацій.

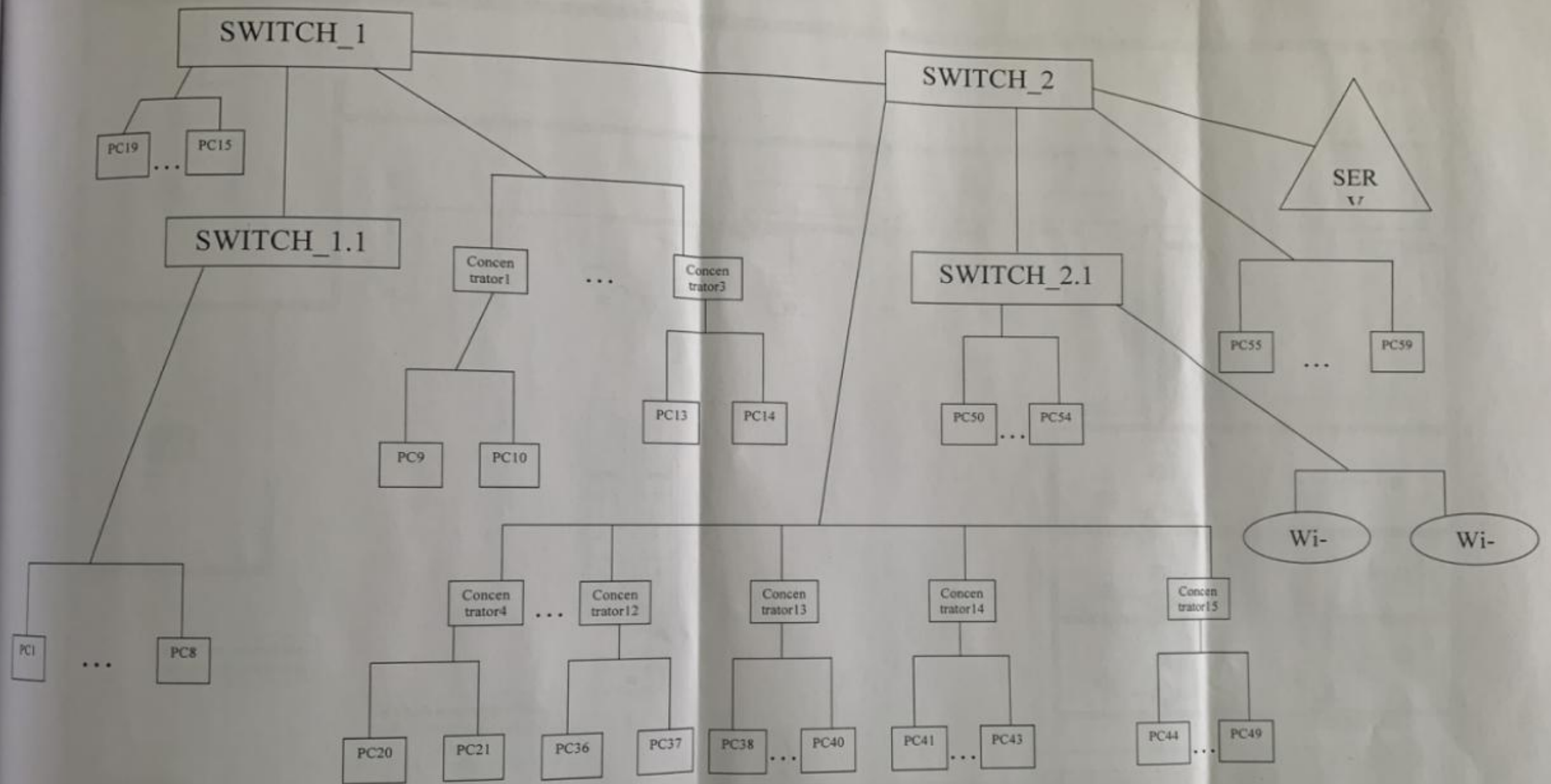
Розглянуті плани поверхів аеропорту та зроблені розрахунки кількості робочих станцій та обладнання, що необхідно для розробки. На основі цього розроблена локальна мережа та схеми прокладки кабелю по будівлі.

Для захисту від фізичних пошкоджень кабелю використовуються кабель рости та гофри. Заборонений вхід до серверної стороннім людям. Розглянуті способи захисту мережі від витіку інформації, несанкціонованого входу та хакерських атак.

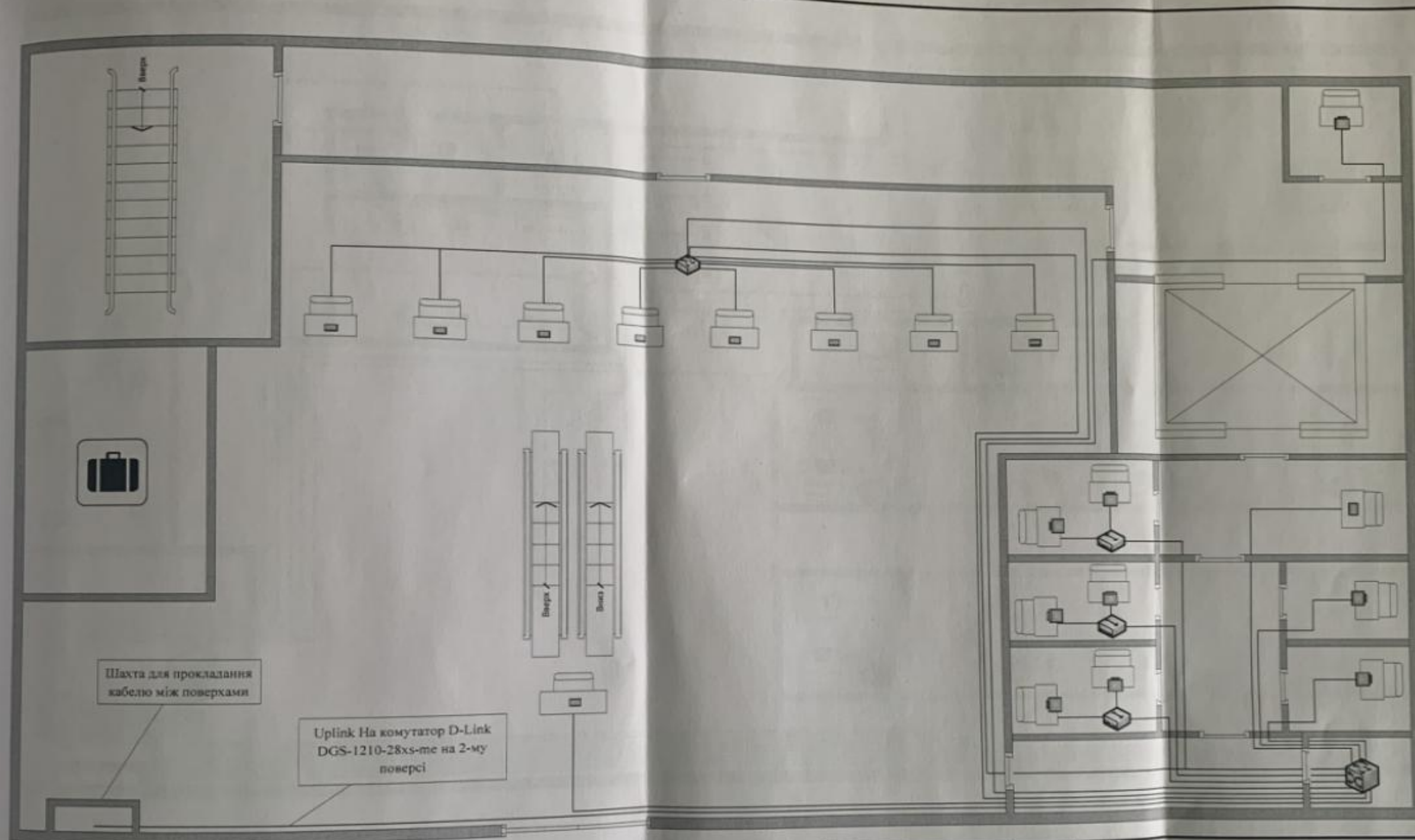
Також представлені варіанти забезпечення відмовостійкості мережі на базі протоколу агрегування для можливості об'єднання в один логічний канал та можливість переключення між ними у разі відмови одного з них. Запропонована ідея щодо створення мікроклімату у приміщенні серверної для контролю сприятливої температури роботи обладнання та запобігання виходу його з ладу у разі перегріву або переохолодження.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

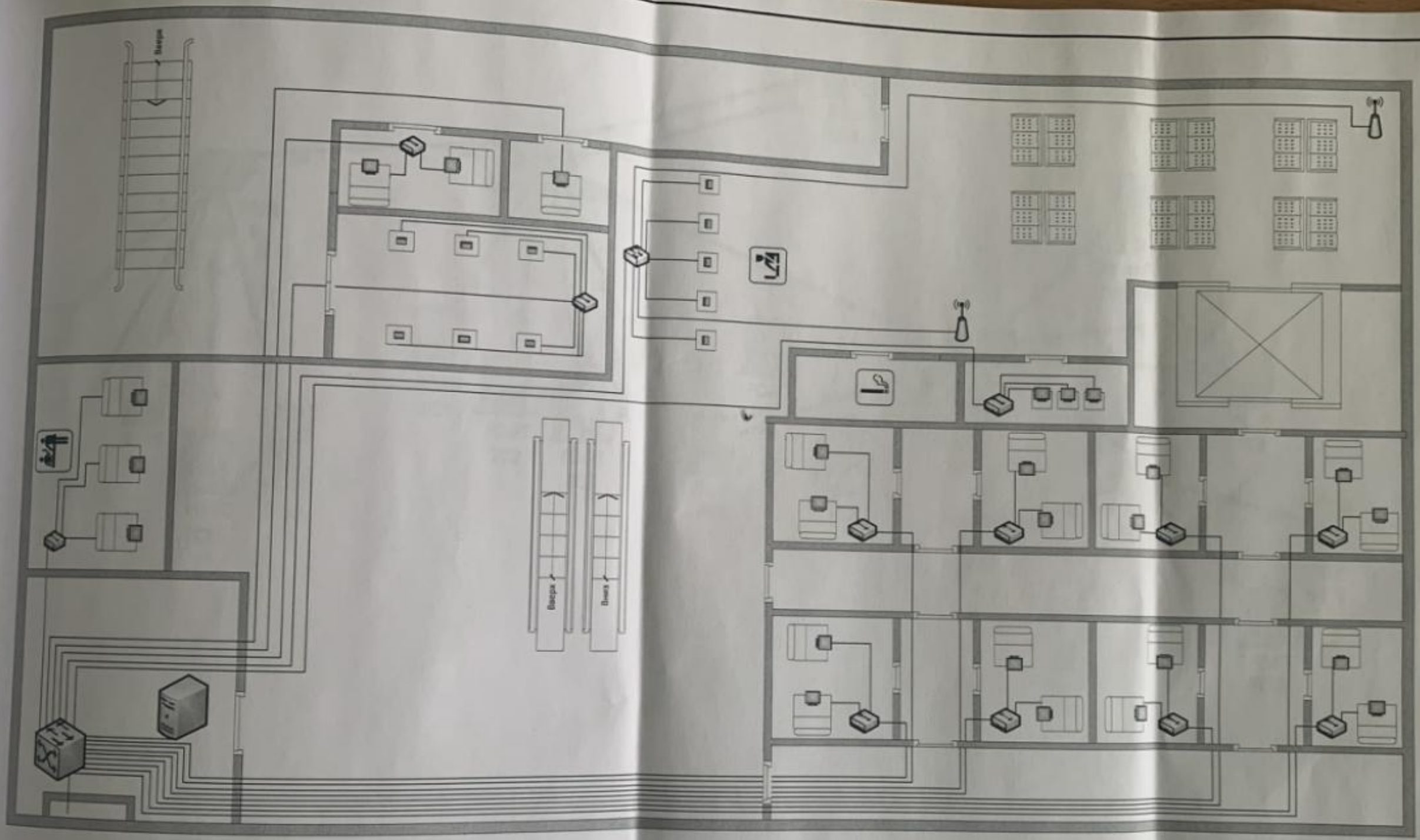
1. Організація комп'ютерних мереж [Електронний ресурс] : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстові дані (1 файл: 45,7 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.
2. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: Учебник / В. Олифер, Н. Олифер. - СПб.: Питер, 2016. - 318 с.
3. Системи моніторингу URL: <https://networkguru.ru/monitoring-seti-setevogo-oborudovaniia-serverov/>
4. Семенов, А. Б. Структурированные кабельные системы. Стандарты, компоненты, проектирование, монтаж и техническая эксплуатация / А.Б. Семенов, С.К. Стрижаков, И.Р. Сунчелей. - М.: КомпьютерПресс, 2018. - 482 с.
5. Смирнова, Е.В. Технологии современных сетей Ethernet. Методы коммутации и управления потоками данных / Е.В. Смирнова. - М.: БХВ-Петербург, 2017. - 480 с.
6. Малишев Р.А. Локальні обчислювальні мережі: Навчальний посібник / РГАТА. - Рибінськ, 2005. - 83 с.
7. Олифер В.Г., Олифер Н.А. Мережеві операційні системи / В.Г. Олифер, Н.А. Олифер. - СПб.: Пітер, 2002. - 544 с.: Іл.
8. Камаліян А.К., Кульов С.А., Назаренко К.М. та ін Комп'ютерні мережі та засоби захисту інформації: Навчальний посібник / Камаліян А.К., Кульов С.А., Назаренко К.М. та ін - Воронеж: ВДАУ, 2003.-119с.
9. Стандарты Ethernet. URL: <https://habr.com/ru/post/208202/>
10. Комутатор D-Link DGS-1210XS/ME URL: <https://comtrade.ua/d-link-28-port-gigabit-fiber-metro-ethernet-switch-dgs-1210-28xs-me/>
11. Комутатор D-Link DGS-1210-10p-ME URL: <https://www.dlink.ru/ru/products/1/2049.html>



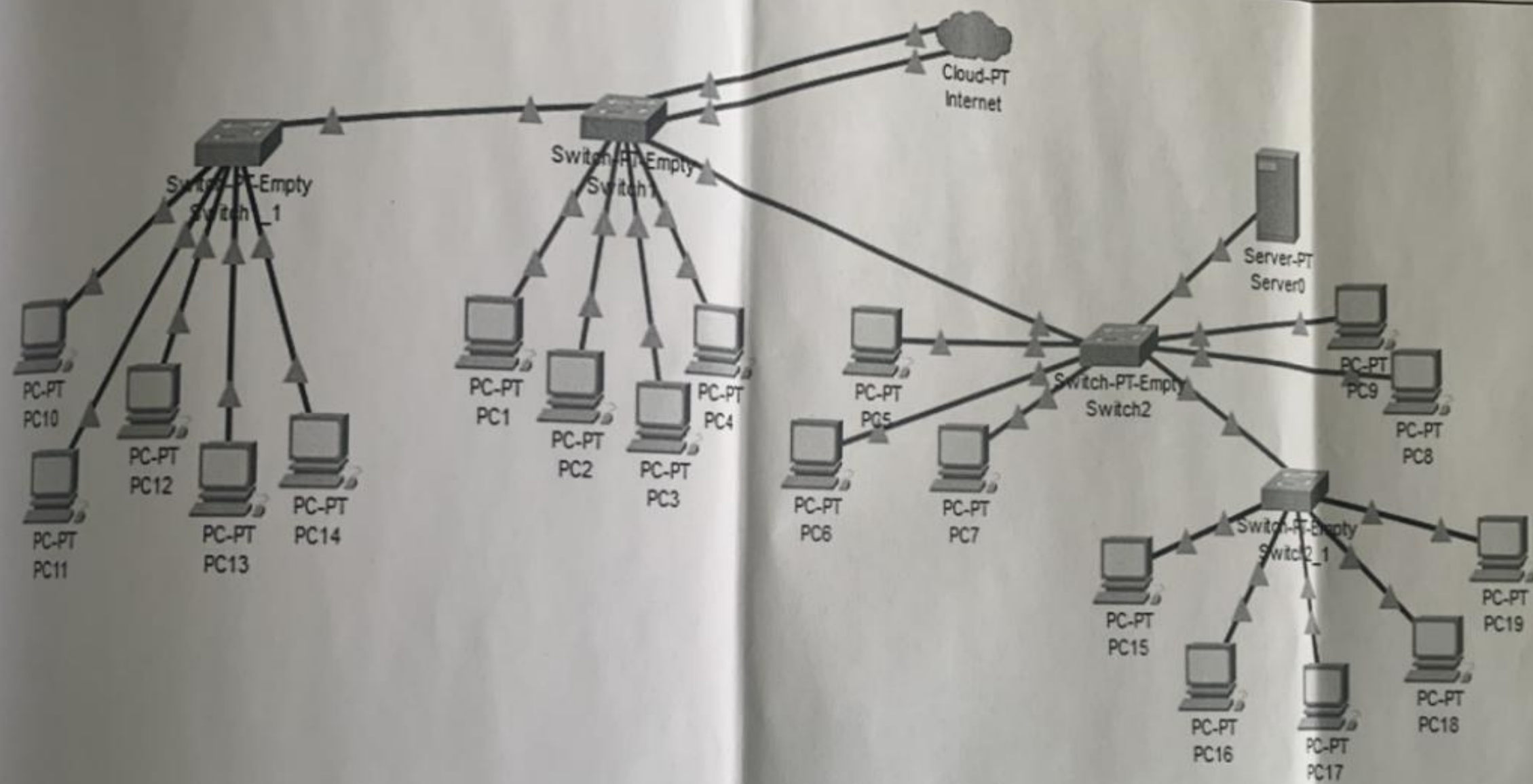
					13.02070849.00069 ПЛ1			
Изм.	Лист	№ докум.	Подпись	Дата	Розробка мультитехнологічної оптоволоконної мережі для аеропорту. Структурна схема мережі підприємства	Лист	Маса	Масштаб
Розроб.		Якименко М.В.						
Провер.		Зеленьова І.Я.						
Т. Контр.								
Реценз.								
Н. Контр.		Данил				Лист	Листов	1
Утверд.						НУЗП, КНТЗ-517		



					13.02070849.00069 ПЛ1		
					Розробка мультитехнологічної оптиволоконної мережі для аеропорту.		
					Схема мережі 1-го поверху		
Изм.	Лист	№ докум.	Подпись	Дата	Лит.	Масш	Масштаб
Разраб.		Якименко М.В.					
Провер.		Зеленьова Г.Я.					
Т. Контр.							
Реценз.							
Н. Контр.		Белла					
Утверд.							
					Лист	Листов	1
					НУЗП, КНТ-517		



						13.02070849.00069 ПЛІ					
						Розробка мультитехнологічної оптичолоконної мережі для аеропорту.			Лит.	Масса	Масштаб
Изм.	Лист	№ докум.	Подпись	Дата							
Разраб.		Якименко М.В.									
Провер.		Зеленьова І.Я.									
Т. Контр.									Лист	Листов	1
Реценз.									НУЗП, КНТЗ-517		
Н. Контр.											
Утверд.											



					13.02070849.00069 ПЛП1		
Изм.	Лист	№ докум.	Подпись	Дата	Розробка мультитехнологічної оптиковолоконної мережі для аеропорту. Спрощена функціональна схема мережі	Лист	Масштаб
Разраб.		Якименко М.В.	<i>[Signature]</i>				
Проект.		Зеленьова І.Я.	<i>[Signature]</i>				
Т. Контр.							
Реценз.							
Н. Контр.		<i>[Signature]</i>	<i>[Signature]</i>				
Утверд.						Листов	1
						НУЗП, КНТ-517	