ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно- інтегрованих технологій, автоматизації, електроінженерії та радіоелектроніки
(повне найменування інституту, назва факультету)

Автоматика та телекомунікації
(повна назва кафедри)

«До захисту допущено»
Завідувач кафедри
_____ Лактіонов І.С.
_____
(підпис) (ініціали, прізвище)
"___"_____20_ р.

Випускна кваліфікаційна робота

бакалавра
(освітньо-кваліфікаційнийрівень)

на тему «Проектування і адміністрування корпоративної мережі в умовах бізнес-центру "САПФІР"»

Виконав: студент 4 курсу, групи ТКР-17
(шифр групи)

спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва напряму підготовки, спеціальності)

Коробчиць В.В. _____
(прізвище та ініціали) (підпис)

Керівник асистент каф. АТ Жуковська Д.О. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Покровськ – 2021 р.

ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно- інтегрованихтехнологій, автоматизації, електроінженерії та радіоелектроніки
(повне найменування інституту, назва факультету)

Автоматика та телекомунікації
(повна назва кафедри)

Захист відбувся_____
(дата)
з оцінкою_____
секретар ДЕК_____
(підпис)

Випускна кваліфікаційна робота

бакалавра
(освітньо-кваліфікаційний рівень)

на тему «Проектування і адміністрування корпоративної мережі в умовах бізнес-центру "САПФІР"»

Виконав студент групи ТКР-17 Коробчиць В.В.
(підпис, дата) (ініціали, прізвище)

Керівник асистент каф. АТ Жуковська Д.О.
(підпис, дата) (ініціали, прізвище)

Зав. каф. автоматики та телекомунікацій І.С.Лактіонов
(підпис, дата) (ініціали, прізвище)

Консультанти _____
(підпис, дата) (ініціали, прізвище)

_____.
(підпис, дата) (ініціали, прізвище)

_____.
(підпис, дата) (ініціали, прізвище)

Нормоконтролер Д.О.Жуковська
(підпис, дата) (ініціали, прізвище)

Покровськ – 2021 р.

ДВНЗ «Донецький національний технічний університет»

Факультет комп'ютерно- інтегрованих технологій, автоматизації електроінженерії та радіоелектроніки
Кафедра автоматика та телекомунікації
Освітній ступінь бакалавр
Спеціальність 172 Телекомунікації та радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ:
Завідувач кафедри
_____ /_____/
"____" _____20___року

З А В Д А Н Н Я
НА ВИПУСКНУ КВАЛІФІАЦІЙНУ РОБОТУ СТУДЕНТУ

Коробчиць Віктора Валерійовича
(прізвище, ім'я, по батькові)

1. Тема роботи «Проектування і адміністрування корпоративної мережі в умовах бізнес-центру "САПФІР"»

керівник роботи: Жуковська Дар'я Олександрівна, асистент каф. АТ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом від " " року № .

2. Строк подання студентом роботи _____

3. Вихідні дані до роботи: експлікація приміщень будівлі бізнес центру, характеристики абонентського складу та вихідні параметри навантаження, характеристики обладнання та технічні специфікації

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

1) Огляд найбільш близьких технічних рішень.

2) Структурна схема телекомунікаційної мережі бізнес-центру "САПФІР"»

3) Функціональна схема телекомунікаційної мережі бізнес-центру "САПФІР"».

4) Апаратний синтез мереж

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

1) Структурна схема.

2) Технічні засоби.

3) Функціональна схема.

4) Алгоритм роботи системи.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
	Затвердження теми	5.05	
	Аналіз плану будівлі, визначення кількості абонентів	8.05	
	Класифікація послуг, розрахунок трафіку	10.05	
	Розробка топології	11.05	
	Вибір технологій, розробка структурної схеми	14.05	
	Вибір протоколів, розробка функціональної схеми	18.05	
	Апаратний синтез	25.05	
	Розробка схем СКС, з'єднань, розміщення устаткування	27.05	
	IP-проектування	30.06	
	Охорона праці	3.06	
	Офромлення та перевірка роботи	6.06	
	Рецензування	12.06	

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ _____
(підпис) (прізвище та ініціали)

Лист зауважень

Посада П.І.Б.	Суть зауваження, оцінка та підпис

АНОТАЦІЯ

Коробчиць Віктор Валерійович, «Проектування і адміністрування корпоративної мережі в умовах бізнес-центру "САПФІР"»/ Випускна кваліфікаційна робота на здобуття освітнього ступеня «бакалавр» за спеціальністю 172 Телекомунікації та радіотехніка. – ДВНЗ «ДонНТУ», Покровськ - 2021.

Структура та обсяг роботи – сторінок 81, таблиць 31, рисунків 24, додатків 3 , використаних джерел 23.

Бакалаврська робота присвячена розв’язанню актуальної задачі – розробці телекомунікаційної мережі для бізнес-центру, яка надає послуги з передачі даних, телефонії та відеоспостереження

Проведений якісний аналіз об’єкту проектування та визначені характеристики послуг що будуть надаватись клієнтам. Розрахований трафік мережі. Прийняті основні проектні рішення та розроблені схеми мережі. Необхідні компоненти для побудови і реалізації мережі .

Правильність прийнятих проектних рішень підтверджена в четвертій главі шляхом імітаційного моделювання.

Ключові слова: ІНФРАСТРУКТУРА, МЕРЕЖА, СХЕМА, ПОСЛУГА, АБОНЕНТ, ОБЛАДНАННЯ, ТЕЛЕКОМУНІКАЦІЇ.

ЗМІСТ

ВСТУП

Впровадження нинішніх телекомунікаційних технологій є гарантією успіху у різних сферах виробничої діяльності. Добре продумана та добре побудована телекомунікаційна мережа - запорука успіху будь-якого бізнесу, включаючи бізнес-центр. Мультисервісні мережі сьогодні мають особливе значення. В даний час, до загальних проблемам впровадження мультисервісних мереж відносять вибір базової технології транспортного рівня мережі, яка буде відповідати швидко зростаючим вимогам, та вибір логічної структури мережі і можливість прозорого аналізу його компонентів. Завдяки мультисервісним мережам з’являються можливості для мережевих послугах на високому рівні. Наприклад, високошвидкісний доступ до мережі інтернету, якісна передача даних та пакетна передача відео і голосу. Всі ці послуги безумовно користуються попитом орендарів, і їх присутність в офісній будівлі є великим плюсом при виборі офісних приміщень для власного бізнесу.

Актуальність роботи – заключається у створенні телекомунікаційної інфраструктури у мережах бізнес-центру. За рахунок цього, зросте конкурентоспроможність, і в наслідок залучить більше клієнтів.

Мета – збільшення конкурентоспроможності у будівлі бізнес-центру, шляхом впровадження сучасних телекомунікаційних послуг.

Предмет – сучасні телекомунікаційні послуги.

Об’єкт – телекомунікаційна інфраструктура бізнес-центру "САПФІР".

Задачі:

- проаналізувати об'єкт та предмет;
- знайти типи споживачів та послуг;
- визначити типи послуг, які надаються мережею, та визначення їх характеристики;
- розробка функціональної та структурної схеми;
- обрати склад телекомунікаційного обладнання

– моделювання мережі та перевірка правильність прийнятих рішень щодо її сегментації на моделі в Packet Tracer.

Методи дослідження – методи обчислювального та аналітичного аналізу, методи порівняння, статистичні методи, моделювання.

Структура та обсяг роботи – сторінок 81, таблиць 31, рисунків 24, додатків 3 , використаних джерел 23.

1 АНАЛІЗ ОБ’ЄКТУ ПРОЕКТУВАННЯ

1.1 Загальні характеристики та задачі об’єкту проектування

Бізнес-центр "САПФІР" представляє собою окремий десятиповерховий будинок з презентабельною вхідною групою і сучасним вентильованим фасадом. Загальна площа будівлі становить 4500 кв.м., де на кожен поверх припадає 500 кв.м. корисної площі, на якій можна на найвигідніших умовах орендувати офіс від власника в Києві. Технічне оснащення бізнес-центру «САПФІР»:

1. центральна система вентиляції і кондиціонування;
2. два ліфти OTIS;
3. центральне опалення і водопостачання.

Офісна будівля класу В + знаходиться під цілодобовою охороною і має в своєму розпорядженні відкриту паркову, яка розташована перед центральним входом в будівлю. Бізнес-центр «САПФІР», вигідно виділяється своїм розташуванням в центральній частині Києва у зоні ділової активності, де створені всі умови для активного розвитку бізнесу будь-якого напрямку. Всього в декількох хвилинах ходьби від офісного центру знаходиться станція метро «Арсенальна» та зупинки громадського транспорту, а сама вул. Московська, що примітна не тільки своєю розвиненою інфраструктурою, а й можливістю зручного виїзду на центральні магістралі Печерського району.

Характеристики

- загальна площа будівлі 4500 кв.м;
- 9 поверхів типового планування 500 кв.м;
- 2 ліфти виробництва OTIS;
- офісні блоки від 100 кв.м;
- паркінг перед будівлею;
- орендна ставка від 600 грн / кв.м / міс з ПДВ [1].

На рис. – 1.1 - 1.10, зображено план поверхів будівлі.

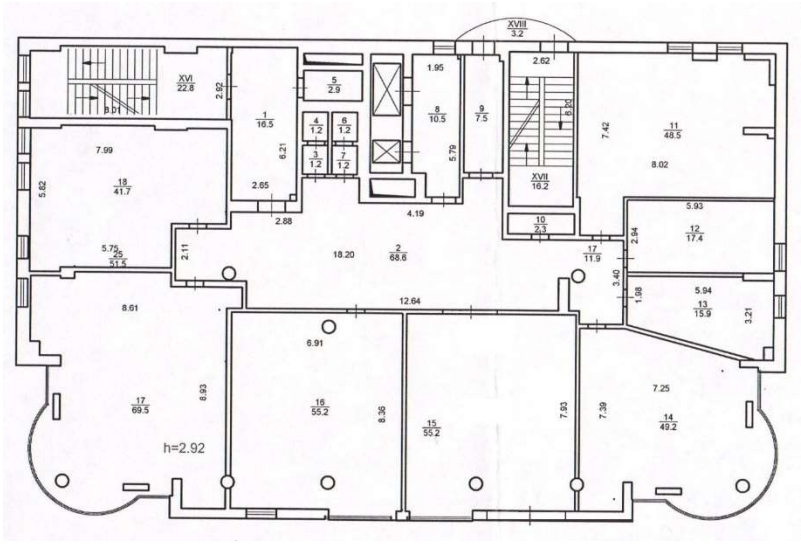


Рисунок 1.1 – План першого поверху будівлі

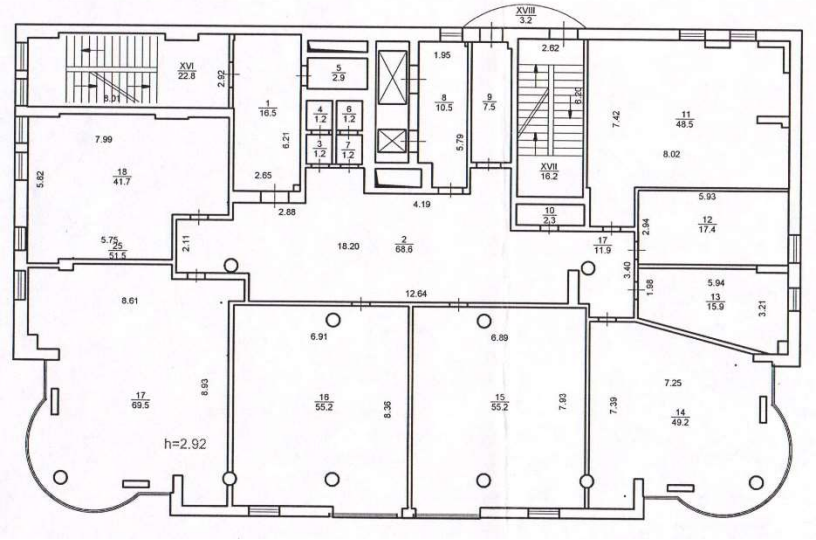


Рисунок 1.2 – План другого поверху будівлі

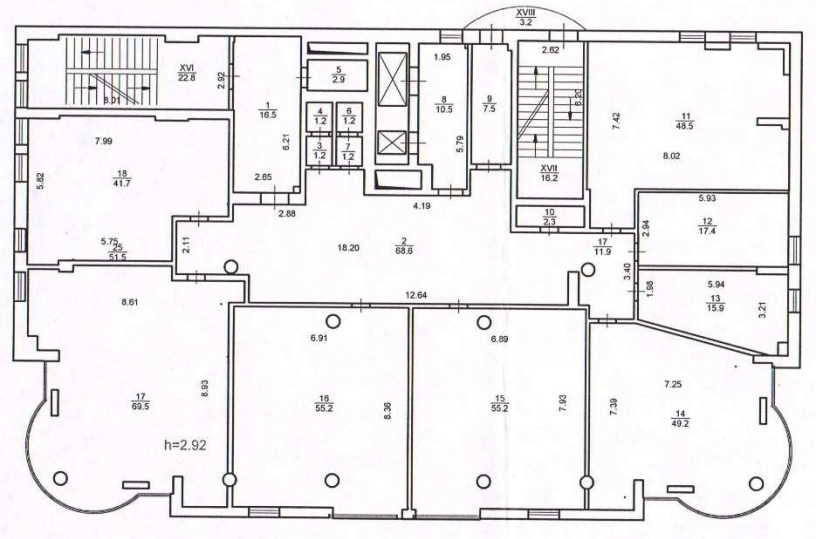


Рисунок 1.3 – План третього поверху будівлі

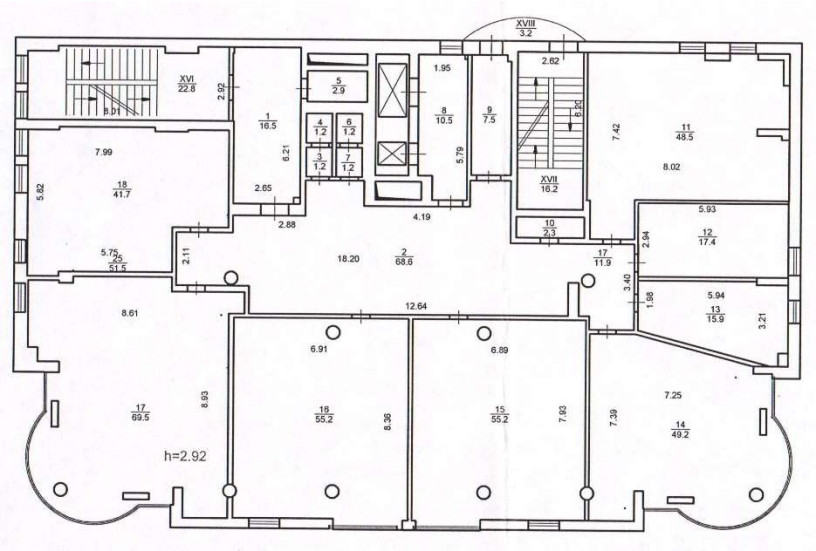


Рисунок 1.4 – План четвертого поверху будівлі

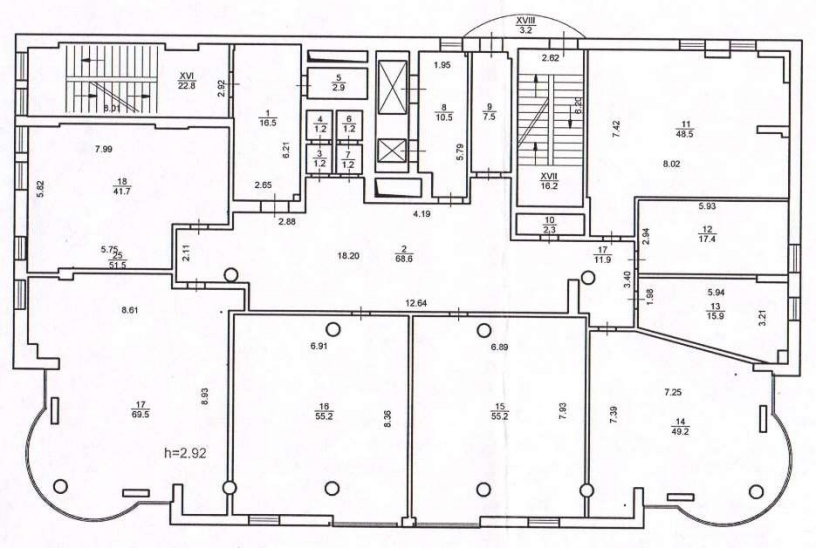


Рисунок 1.5 – План п’ятого поверху будівлі

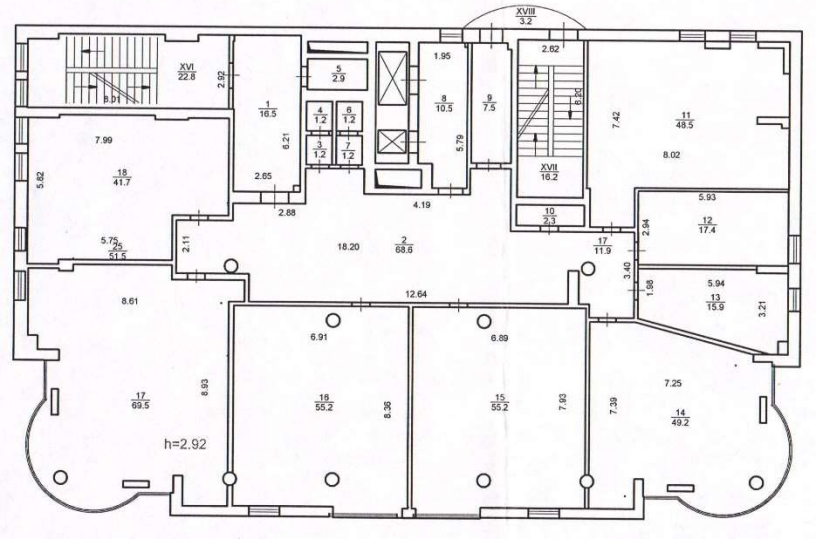


Рисунок 1.6 – План шостого поверху будівлі

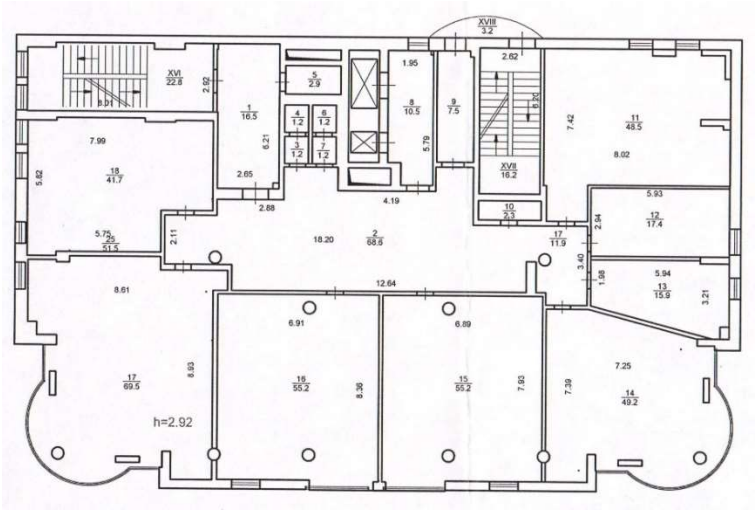


Рисунок 1.7 – План сьомого поверху будівлі

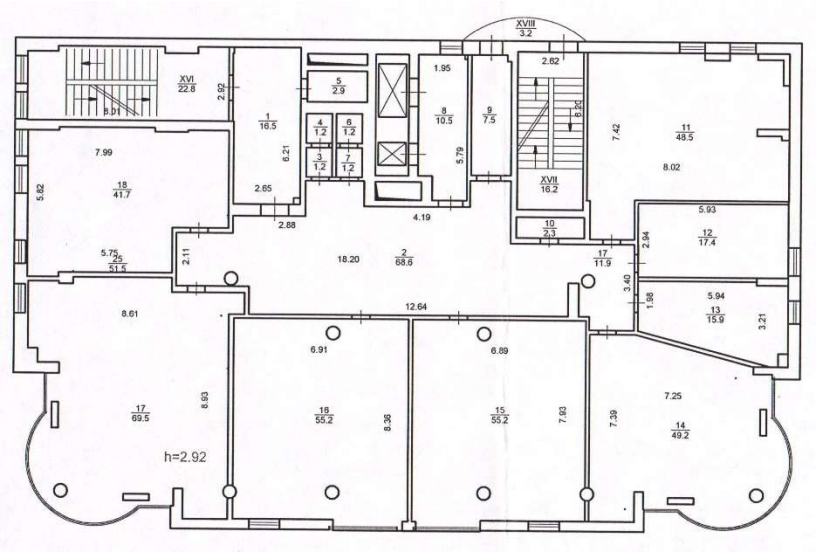


Рисунок 1.8 – План восьмого поверху будівлі

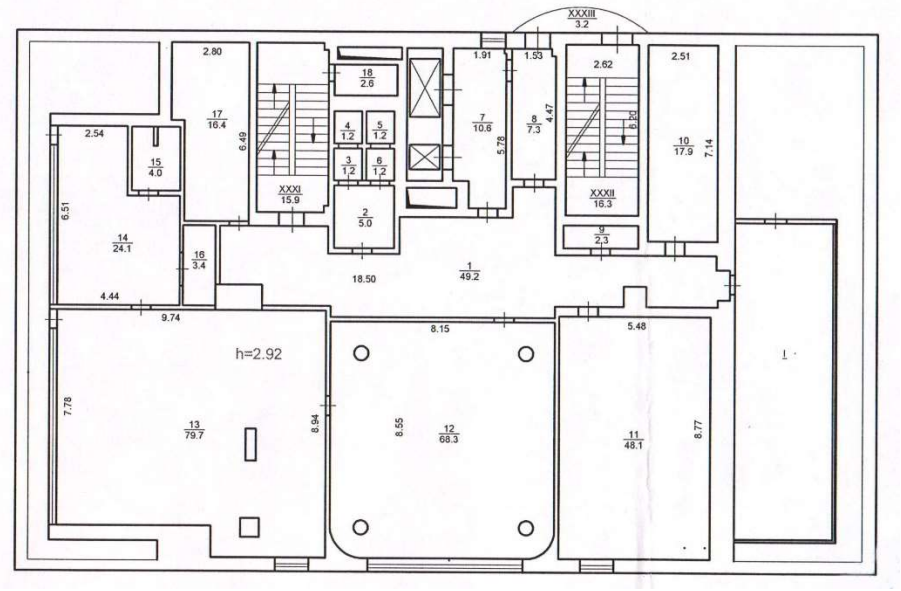


Рисунок 1.9 – План дев’ятого поверху будівлі

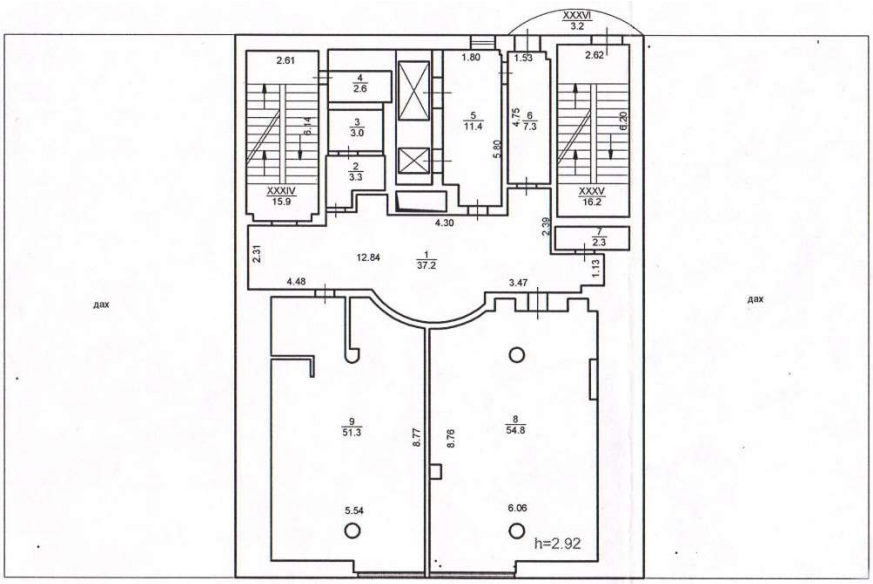


Рисунок 1.10 – План десятого поверху будівлі

У таблиці 1.1 наведені характеристики кожного поверху з точки зору кількості офісів та кількості робочих місць.

Таблиця 1.1 – Характеристика поверхів бізнес-центру "САПФІР"

Поверх	Призначення поверху	Кількість приміщень	Кількість робочих місць
1	інженерно-технічних служб	7	21
2	офісні приміщення	9	30
3	офісні приміщення	9	30
4	офісні приміщення	9	30
5	офісні приміщення	9	30
6	офісні приміщення	9	30
7	офісні приміщення	9	30
8	адміністрація	9	20
9	адміністрація	2	5
Всього		72	236

На першому поверсі є приміщення для інженерно-технічних служб, включаючи насосну станцію, центральну систему вентиляції та кондиціонування, охоронну систему з відеоспостереженням, центральне опалення та інші об'єкти, а також рецепцію та охоронну зону будівлі. Другий, третый, четвертий, п'ятий, шостий і сьомий поверхи мають офісні приміщення, і здаються в оренду. Восьмий і дев'ятий поверхи - це поверхи адміністрації бізнес-центу. У дипломному проекті буде проведено проектування комплексу

телекомунікаційної мережі, для забезпечення локальної та телефонної мережі, мережі безпроводного доступу, та систему відеоспостереження. Всі робочі місця будуть обладнані необхідною кількістю термінальних розеток для отримання доступу до локальної та телефонної мережі. У таблиці 1.2 представлено розподіл термінальних абонентських пристроїв згідно з кількістю поверхів бізнес-центру.

Таблиця 1.2 – Термінальні пристрої, та їх розподіл

Поверх	Кількість ПК	Кількість ТА	Кількість безпроводових клієнтів (робітники бізнес-центру)	Кількість відеокамер спостереження
1	21	21	50	7
2	30	30	20	5
3	30	30	20	5
4	30	30	20	5
5	30	30	20	5
6	30	30	20	5
7	30	30	20	5
8	20	20	20	5
9	5	5	5	3
Всього	236	236	195	45

Згідно з таблиці загальна кількість телекомунікаційних пристроїв становить:

- Персональний комп’ютер - 236 шт.;
- Телефонний апарат - 236 шт.;
- Безпровідні підключення - 195 шт.;
- Відеокамери спостереження - 45 шт.

1.2 Опис послуг та створення інформаційної моделі

Кожна розвинута телекомунікаційна мережа повинна надавати пакет послуг:

– Телефонія
– Відеокамери спостереження
– Інтернет доступ
– Передача даних

Усі сучасні телекомунікаційні послуги так чи інакше розподіляються між абонентами та пристроями абонентів. Щоб надати можливість відповідним абонентам підпорядкування послуг пропонується розділити всіх наявних абонентів та структуру в цілому на 4 категорії. У таблиці 1.3 показано розподіл існуючих абонентів за групами та послуги, що їм надаються.

Таблиця 1.3 – Групи та послуги користувачів

Група	Послуги	Тип користувачів
1	Телефонні апарати, мережа інтернету, файловий сервер	офісні співробітники
2	WiFi	гостьові абоненти
3	Телефонні апарати, отримання даних з серверу спостереження	співробітники служби охорони
4	Передача даних на сервер спостереження	відеокамери

На рисунку 1.11 наведена схема взаємодії інформації між різними відділами та групами учасників. Цей показник дає відповідь на питання, які послуги належать до певної групи абонентів, і визначає розширений склад загальних послуг, таких як телефонія та Інтернет.

Рисунок 1.11 – Схема взаємодії інформації

Послуги телефонного зв’язку - це місцеві дзвінки між місцевими учасниками та дзвінки на телекомунікаційну мережу загального користування. Обміну файлами, доступ до Інтернету для орендарів та без пароля до Інтернету для клієнтів та відвідувачів будівель – це мережа предачі даних.

Послуги відеоспостереження мають підтримувати та забезпечувати електронні архіви і трансляцію в Інтернеті в режимі реального часу та на моніторах у охорони.

Зазначені послуги надаються на основі зведеної IP-мережі. Враховуючи цей фактор, необхідно забезпечити розширену функціональність кожної з послуг. Ці характеристики складаються з:

- Пз - пропускна здатність
- Чв - частота викликів
- Т - тривалість спілкування
- П - пачечність

Для визначення параметру Х, потрібно розрахувати навантаження в Мбіт / с, згідно формулі (1.1):

$$X = \frac{Пз * Чв * Т}{П * 3600}, Мбіт/с \quad (1.1)$$

Таблиця 1.4 показує значення параметрів послуг та розраховані параметри навантаження на кожну послугу, виключенням є послуга «телефонія».

Таблиця 1.4 – Параметри навантаження

	Пр, Мбіт/с	П	Чв	Т, с	Х, Мбіт/с	Х, Ерл
Загальний інтернет	2,048	2	150	5	0,213	0,208
Wi-Fi доступ	0,512	10	50	15	0,0107	0,208
FTP server	100	20	10	30	0,417	0,083
Камери відеоспостереження (зовнішнє, внутрішнє)	0,384	1	1	3600	0,384	1
Підключення до серверу відеоспостереження	0,384	1	1	3600	0,384	1

1.3 Розрахунок навантаження на мережу передачі даних

Навантаження слід розрахувати у два етапи, визначити навантаження на локальну мережу та супутні послуги та розрахувати пропускну здатність зовнішніх каналів [2].

Для виконання розрахунків першого кроку відповідно до інформаційної моделі ми визначаємо кількість користувачів кожної послуги (табл. 1.5).

Значення в таблицях 1.3 та 1.5 необхідно перемножити та визначаємо навантаження на кожен поверх і для кожного відділу. Результат узагальнений у таблиці 1.6.

Таблиця 1.5 - Розподіл користувачів за підрозділами на кожному поверсі

Послуга	Поверх										Всього
	1	2	3	4	5	6	7	8	9	10	
Локальна телефонія	21	30	30	30	30	30	30	20	5	2	228
Доступ до ТМЗК	21	30	30	30	30	30	30	20	5	2	228
Інтернет	19	29	29	29	29	29	29	19	4	2	218
Інтернет Wi-Fi	60	40	40	40	40	40	40	30	20	8	358
FTP сервер	19	29	29	29	29	29	29	19	4	2	218
Камери відеоспостереження	7	5	5	5	5	5	5	5	2	3	47
Доступ до сервера відеоспостереження	2	1	1	1	1	1	1	1	1	2	12

Таблиця 1.6 – Навантаження в мережі

Послуга	Навантаження на поверх, Мбіт/с										Всього, Мбіт/с
	1	2	3	4	5	6	7	8	9	10	
Інтернет орендаторів	4,047	6,177	6,177	6,177	6,177	6,177	6,177	4,047	0,852	0,426	46,434
Інтернет Wi-Fi	0,642	0,428	0,428	0,428	0,428	0,428	0,428	0,321	0,214	0,0856	3,8306
Файловий сервер	7,923	12,093	12,093	12,093	12,093	12,093	12,093	7,923	1,668	0,834	90,906
Камери спостереження	2,688	1,92	1,92	1,92	1,92	1,92	1,92	1,92	0,768	1,152	18,048
Доступ до сервера спостереження	0,768	0,384	0,384	0,384	0,384	0,384	0,384	0,384	0,384	0,768	4,608
Всього, Мбіт/с	16,068	21,002	21,002	21,002	21,002	21,002	21,002	14,595	3,886	3,2656	163,8266

1.4 «Телефонія» - розрахунок навантаження

Вихідними даними для розрахунків є кількість кінцевих споживачів послуг, інтенсивність, тип кодека та типи протоколів, що використовуються для надання послуг IP-телефонії. Нижче перелічені значення, необхідні для подальших розрахунків:

- у місцевій телефонній групі кількість користувачів n = 228;
- для телефонної групи з правом доступу до телефонної мережі загального користування кількість користувачів n = 228;
- в розряднику перенапруги для групи телефонних послуг загальне значення навантаження в = 0,25;

- в розряднику для перенапруги для місцевої телефонної служби середнє значення навантаження y = 0,1Erl;
- в розряднику перенапруги для телефонної служби з правом доступу до загальної телефонної мережі середнє значення навантаження y = 0,1Erl;
- вибір кодека - G.711;
- час вибірки - 10 мс;
- протокол - Ethernet;
- мережевого протокол – IP протокол;
- транспортний протокол - UDP;
- мультимедійний протокол - RTP.

Відповідно до цього треба розрахувати загальне навантаження на IP-мережу, а також кількість зовнішніх каналів, необхідних для телефонної комутованої мережі загального користування.

Загальне навантаження розраховується з урахуванням загальної кількості учасників 228. Для цього ми використовуємо формулу (1.2):

$$Y = \frac{y_{аб} \cdot N}{1 + y_{аб}}, \tag{1.2}$$

Для групи з 228 учасників, загальне навантаження учасників становить 0,25. Визначимо все загальне навантаження на мережу:

$$Y = \frac{y_{аб} \cdot N}{1 + y_{аб}} = \frac{0{,}25 * 228}{1 + 0{,}25} = 45{,}6 \text{ Ерл}$$

Визначаємо обсяг даних за формулою 1.3:

$$b = \frac{t_s \cdot R}{8}, \tag{1.3}$$

Значення даних у семплі буде такие (це корисна інформація):

$$b = \frac{t_s \cdot R}{8} = \frac{0{,}01 * 64000}{8} = 80 \text{ байт}$$

Значення загальної пропускної здатності у каналі зв'язку залежить від значення показника службової інформації, що додається до даних і становить (1.4):

$$B_{аб} = \frac{H_2 + H_3 + H_4 + H_5 + b}{b} \cdot R, \qquad (1.4)$$

Обсяг службової інформації залежить від заголовків.

H2 - розмір заголовка Ethernet Link Technology, який становить 18 байт.

H3 - 20-байтний розмір заголовка IP-мережі.

H4 - розмір 8-байтового транспортного заголовка UDP.

H5 - црозмір заголовка RTP для потокового передавання, який становить 12 байт. А отже вся пропускна здатність у каналі зв'язку для однієї розмови становитиме:

$$B_{аб} = \frac{H_2 + H_3 + H_4 + H_5 + b}{b} \cdot R = \frac{18+20+8+12+80}{80} 64 = 110{,}4, \text{Кбіт/с.}$$

Кількості еквівалентних комплектів підключення знаходиться згідно з формулою (1.5) :

$$B = B_{аб} * V, \qquad (1.5)$$

тож, пропускна здатність становитиме:

$$B = B_{аб} * V = 110{,}4 * 66 = 7{,}12 \text{ Мбіт/с}$$

Виходячи з розрахунку, додаткове навантаження на IP-мережу становить 7,12 Мбіт / с і зазвичай 165,28 Мбіт / с.

Зі значенням групи з 228 учасників, загальне навантаження учасників становить 0,1. Розраховуємо навантаження, створене для телефонної мережі загального користування (за 1.2):

$$Y = \frac{y_{аб} \cdot N}{1+y_{аб}} = \frac{0,1*228}{1+0,1} = 20,73 \text{ Ерл}$$

А отже, *Y=20,73* Ерл та *P=0,001*, значення кількості каналів складає 36 ліній.

Висновки до розділу 1

У першій частині дипломного проекту проводиться аналіз об'єкта проектування. Загальна кількість точок доступу до ресурсів телекомунікаційної мережі становить 861 порт. Запланована мережа надаватиме Інтернет-послуги, обмін файлами, телефонний зв’язок та відеоспостереження. Виходячи із загальної кількості користувачів та мережевого трафіку, розраховувався трафік для всієї мережі та для окремих послуг. Загальне навантаження мережі 163,83 Мбіт / с, пропускна здатність Інтернету 50,2646 Мбіт / с, кількість ліній для підключення телефонної мережі до ТМЗК – 36.

2 ПРОЕКТУВАННЯ АРХІТЕКТУРИ МЕРЕЖІ

2.1 Вибір технології ї та топології мережі

Запланована мережа відповідає за надання інформації між терміналами та гарантує оптимальні параметри надійності, швидкості передачі та безпеки. Побудова фізичного рівня може бути на основі різних топологій, типів каналів зв'язку та різних технологій. Технології Ethernet і WiFi можна фізично використовувати для створення мережі у цілому. Різниця між технологіями полягає у базовій швидкості, типі фізичного носія інформації, затримці та способі доступу до носія інформації. У таблиці 2.1 ми порівнюємо вибрані технології [3].

Таблиця 2.1 – Порівняння технологій

	WiFi	Ethernet
Спосіб доступу до середовища	CSMA/CA	CSMA/CD
Значення затримки (мс)	0,03	0,006
Швидкості (Мбіт/с)	56, 72, 144, 300	10, 100, 1000, 10000
Тип середовища	радіоканали 2,4, 5 ГГц	мідний кабель вита пара, оптичні одно-та багатомодовий кабель
Специфіка IEEE	802.11	802.3

На основі цього порівняння можна використовувати обидві технології в офісній будівлі. Для більш безпечного рівня зв’язку та підвищеної безпеки каналів передачі даних використовується технологія Ethernet для надання послуг орендарям та працівникам будівель. Технологія WiFi використовується у зв'язку з доступом до Інтернету без пароля для відвідувачів офісної будівлі.

Ethernet технологія передає використання різних фізичних носіїв і має широкий спектр специфікацій. Огляд сімейства Ethernet можна знайти у таблиці 2.2.

Таблиця 2.2 – Сімейство Ethernet

Стандарт	Середовище	Максимальна довжина сегменту, м	Швидкість (Мбіт/с)
10 Base	оптичний кабель/ мідний	0,1/2	10
100 Base	оптичний кабель/ мідний	0,1/50	100
1000 Base	оптичний кабель/ мідний	0,1/100	1000
10 Gbase	оптичний кабель/ мідний	0,015/40	10000

На основі короткого аналізу технологій Ethernet оптимальним буде 100 Base-T для використання. Ця технологія повністю реагує на пропускну здатність і довжину сегмента кабелю для підключення кінцевих користувачів. Лінії зв'язку - це вита пара мідних кабелів категорії 5е, які дозволяють забезпечити надійний і безперешкодний зв’язок на відстані 100 м і дозволяють в майбутньому перейти на технологію 1000 Base-TX. 1000 Base-TX використовується для побудови магістральної мережі між комутаторами.

Одна з технологій сімейства WiFi використовується для організації гостьового доступу без пароля. У таблиці 2.3 узагальнено основні характеристики.

Таблиця 2.3 – Характеристики WiFi

IEEE	Частотний діапазон (ГГц)	Максимальна пропускна здатність (Мбіт/с)	Назва
802.11 n	2,4	150	wireless N 150 Mbps
	2,4	270	wireless N speed
	2,4	300	wireless N 300 Mbps
	2,4/5	300	wireless dual band N
	2,4/5	450	wireless N 450 Mbps
802.11 g	2,4	54	wireless g
	2,4	108	super g
802.11 b	2,4	11	wireless b
802.11 a	5	54	wireless a

На сьогодні найбільш часто використовують абонентське обладнання, що працює в діапазоні частот 2,4 ГГц і відповідає стандартам 802,11 b / g / n, ми не будемо відступати від загальновизнаної тенденції у розробці та використанні 802,11 b / г / н.

Топологія проектованої мережі складатиметься з частки рівнів, а це виходить з визначення ієрархії ї IP-мереж [3]. Рис. 2.1 дмонструє топологічну схему мережі.

Рисунок 2.1 – Топологічна схема мережі

2.2 Розробка схеми структури мережі

Проектована структурна схема повністю відповідає топологічному рішенню та обраним мережевим технологіям. Планова мережа складається з 2х рівнів і складається з ядра мережі та рівнів доступу. Базовий рівень представлений центральним телекомунікаційним вузлом, який створений у топології зірка з використанням технологій 100 Base-T, 1000 Base-TX і складається з наступних компонентів:

- Центральний маршрутизатор - підключення зовнішнього каналу та загальне управління мережею;
- Центральний комутатор - підключення комутаторів рівня доступу та серверного обладнання;
- Серверне обладнання - організація мережевих служб;
- IP-АТС - організація взаємодії між абонентами телефонної мережі та АТС, підключення зовнішніх каналів.

Рівень доступу використовується для підключення пристроїв кінцевих користувачів до мережі. Топологія зірки організована з використанням технологій 100 Base-T та 802.11 b / g / n та складається з наступних пристроїв:

- Перемикач доступу - підключення дротових користувачів;
- Точка доступу Point WiFi - підключайте користувачів через бездротову мережу.

Пристрої телефонної мережі абонента, камери спостереження та бездротові точки доступу підключаються до мережі за допомогою технології 100 Base-T через віддалене джерело живлення через Ethernet - PoE.

Топологія фізичних зв’язків на всіх рівнях мережі є зіркою.

2.3 Розробка функціональної схеми мережі

Функціональна схема мережі показана на рис. Б.1, додатка Б. Функціональна схема - це симбіоз топологічних та структурних діаграм. Данна схема повністю відображає функціональний склад мереж:

- кількість приладів;
- тип обладнання;
- кількість функціональних портів мережевих пристроїв;
- необхідні протоколи.

Давайте опишемо призначення кожного мережевого пристрою, протоколи та технології, необхідні для реалізації мережі:

- Комутатори Swit Access працюють за протоколом Ethernet і оснащені 1000 портами Base-TX для підключення до центрального комутатора та 100 портами Base-T з підтримкою PoE для підключення терміналу.
- Файловий сервер використовується для організації функцій обміну між ПК та станціями користувачів та для зберігання заархівованих даних та інших даних.
- Маршрутизатор, яки оснащений 2-ма портами 1000 Base-TX, які працюють за протоколом Ethernet. Пристрій виконує функції маршрутизації, підключення до Інтернету.
- Бездротові точки доступу використовуються для підключення бездротових пристроїв (ноутбуків, планшетів, смартфонів). Вони оснащені 100 портами Base-T з підтримкою PoE та інтерфейсом 802.11 b / g / n.
- IP-АТС дозволяє абонентам локальної мережі взаємодіяти з телефонною мережею загального користування та між собою.
- Сервер системи нагляду «Server» дозволяє керувати архівами відеоспостереження, обробляти зображення та передавати їх на монітори безпеки та в IP-мережу на прохання користувачів.
- Центральний комутатор використовується для зв'язку мережі розподілу IP із серверними пристроями та центральним маршрутизатором. Комутатор оснащений 1000 портами Base-TX і працює за протоколом Ethernet.

Розглянемо основні принципи роботи мережі.

Локальна мережа регулюється протоколом TCP / IP, який використовується для управління процесом передачі даних в мережах IP та підмережах. Усі активні мережеві з'єднання мають IP-адреси, які використовують протокол IRv4, протокол адресації в IP-мережах та використовують 4-байтову нотацію. Використання IPv6 у локальних мережах недоцільне. Розподіл адресного простору в мережі здійснюється відповідно до правил протоколу DHCP - протокол дозволяє терміналам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі TCP / IP. Для реалізації функціональних можливостей мережі та моніторингу роботи мережевих протоколів використовуються:

- ICMP - використовує базову підтримку IP, насправді є невід'ємною частиною IC, і повинен бути реалізований кожним модулем IP. Повідомлення ICMP надсилаються в декількох ситуаціях: наприклад, коли дейтаграма не може досягти місця призначення, коли шлюз не має ємність буферизації для пересилання дейтаграми, а також коли шлюз може направити хоста на пересилання трафіку за коротшим маршрутом [10].
- ARP - gротокол дозволу адрес - це протокол рівня 2, який використовується для зіставлення MAC-адрес з IP-адресами. Усі хости в мережі розташовані за своєю IP-адресою, але мережуі карти не мають IP-адрес, вони мають MAC-адреси. ARP - це протокол, який використовується для прив’язки IP-адреси до MAC-адреси. Коли хост хоче надіслати пакет іншому хосту, скажімо, IP-адреса 10.5.5.1, у своїй локальній мережі (LAN), він спочатку відправляє (транслює) пакет ARP. Пакет ARP містить просте запитання: Яка MAC-адреса відповідає IP-адресі 10.5.5.1? Хост, налаштований на використання IP-адреси, відповідає пакетом ARP, що містить його MAC-адресу [11].
- UDP - User Datagram Protocol (UDP) - це полегшений протокол передачі даних, який працює над IP. UDP забезпечує механізм виявлення пошкоджених даних у пакетах, але не намагається

вирішити інші проблеми, що виникають із пакетами, такі як втрачені або непрацюючі пакети. Ось чому UDP іноді називають протоколом ненадійних даних. UDP простий, але швидкий, принаймні в порівнянні з іншими протоколами, які працюють через IP. Він часто використовується для чутливих до часу програм (таких як потокове передавання відео в режимі реального часу), де швидкість важливіша за точність [12].

Організація місцевих робочих станцій базується на використанні протоколів:

- XML - є популярним вибором при розробці комунікаційних протоколів, оскільки аналізатори XML є всюдисущими. Фраза «XML через TCP» є хорошим резюме [13].
- FTP - протокол передачі файлів - це протокол зв'язку, який використовується для передачі файлів з комп'ютера на комп'ютер, при цьому один із них виконує роль сервера, забезпечуючи з'єднання з Інтернетом. Мережний протокол між клієнтом та сервером, FTP дозволяє користувачам завантажувати веб-сторінки, файли та програми, доступні на інших послугах. Коли користувач хоче завантажити інформацію на власний комп'ютер, він використовує FTP. FTP не використовує шифрування. Для автентифікації він покладається на імена користувачів та паролі відкритого тексту, що робить передачу даних, що надсилається через FTP, уразливим для звичайних методів підслуховування, видавання себе за інших та інших атак [14].
- HTTP - протокол передачі гіпертексту є основою Всесвітньої павутини і використовується для завантаження веб-сторінок за допомогою гіпертекстових посилань. Протокол прикладного рівня, призначений для передачі інформації між мережевими пристроями і працює поверх інших рівнів стеку мережних протоколів. Типовий потік через HTTP включає клієнтську машину, яка робить запит на сервер, який потім надсилає відповідне повідомлення [15].

Найважливішим мережевим пристроєм є маршрутизатор. До маршрутизатора підключені локальна мережа та зовнішній Інтернет-канал.

Зовнішній канал до Інтернету має пропускну здатність 50 2646 Мбіт / с. Прямий доступ до Інтернету здійснюється через зовнішній канал. Для підключення до Інтернету використовуються наступні функції та протоколи маршрутизатора [2]:

- TCP / IP - це протокол управління мережею.
- NAT - Служба перекладу мережевих адрес - доступ до Інтернету для клієнтських пристроїв (ПК)
- TCP / IP - це протокол управління мережею.
- FireWall - захист від зовнішніх перешкод, реалізований за допомогою списків доступу та служби NAT;

Ресурси локальної мережі розподіляються за допомогою логічної структуризації з використанням протоколу 802.1q VLAN.

Розподіливши кінцеві пристрої в підмережах, подивимось, як працюють окремі служби.

IP-телефонна мережа складається з АТС та IP-телефону. Гібридна IP-АТС оснащена портом інтерфейсу 100 Base-T та двома портами E1 для підключення до мережі ТМЗК. IP-телефони оснащені роз'ємом 100 Base-T, який підтримує віддалене живлення через мережі PoE Ethernet. Всі пристрої належать одному Vlan і мають загальний простір IP-адрес, що надається сервером DHCP. IP-телефонна мережа налаштована відповідно до рекомендацій, регламентованих протоколом SIP.

Мережа використовує систему зберігання відео, яка складається з відеосерверу, який обробляє та зберігає відеозображення та організовує доступ до перегляду відео в Інтернеті або у відеотеках та відеокамерах, які є джерелами зображень. відео відправляється на сервер. Пристрої інтегровані в єдиний Vlan і мають загальний простір IP-адрес, який розподіляється в автоматизованому маршрутизаторі через службу DHCP. На основі розрахунків трафіку мережа використовує протокол стиснення зображень H.264. На додаток до цього протоколу, відеокамери та відеосервери використовують такі: RTP,

UDP, IPv4, HTTP. Протокол UDP використовують для обміну контрольними та інформаційними повідомленнями, протокол RTP безпосередньо відповідає за передачу відео через мережу IP. Прямий доступ до камер спостереження забезпечується через протокол HTTP.

Висновки до розділу 2

У другому розділі дипломного проекту було визначено найважливіші протоколи та технології для реалізації мережі. На початку розділу було обрано топологію мережі, розширено ієрархічну зірку, і мережа використовує первинний рівень, рівень розподілу та рівень доступу. Технології та протоколи побудови мережі відповідають сьоми рівням та моделям OSI. Основним протоколом налаштування мережі є Ethernet. Також у мережі для повнофункціональних протоколів. На основі проектних рішень були розроблені та описані структурні та функціональні схеми.

3 ПРОЕКТУВАННЯ АПАРАТНОЇ АРХІТЕКТУРИ МЕРЕЖІ

3.1 Визначення груп пристроїв та постачальників

Проектована мережа використовує активні та пасивні пристрої. Активні пристрої представлені такими пристроями:

- маршрутизатор;
- перемикач;
- IP-телефон точка бездротової точки доступу;
- відеоспостереження;
- IP відеореєстратор;
- IP-АТС;
- точка бездротової точки доступу.

Пасивні пристрої представлені такими компонентами:

Мідний витий парний кабель;

- польове поле;
- сполучний шнур;
- розетка телекомунікаційна;
- монтажний шафа.

Перелічимо основні вимоги до активних виробників пристроїв:

- висока надійність обладнання;
- розумне співвідношення ціна / якість;
- потреба в сертифікованому обслуговуючому персоналі;
- розвинена мережа торгових офісів та сервісних центрів.

Маючи великий обмінний фонд та швидкий час реагування на гарантійні справи та післягарантійне обслуговування.

На українській території велика кількість марок виробників активного обладнання. У таблиці 3.1 ми перелічимо основних виробників та їх відповідність вимогам [4].

Таблиця 3.1 – Перелік виробників активного устаткування

	Watson	Cisco	Zyxel	Planet	D-link
Якість /ціна	незадовільна	надвисока	незадовільна	середня	середня
Авторизовані точки продажу	15	35	5	10	75
Необхідний перелік устаткування	так	так	частково	частково	так
Сертифікований персонал	ні	первинне налаштування та подальше обслуговування	ні	ні	первинне налаштування
Надійність	середня	надвисока	середня	висока	висока
Сервісне обслуговування	5	10	5	10	30

Враховуючи необхідну кількість активного обладнання та, як наслідок, кінцеву вартість, ми вибираємо D-Link як постачальника активного обладнання для нашої мережі.

Щодо пасивних мережевих компонентів та виробників застосовуються завищені вимоги, що пов'язано з тривалим терміном служби мережевих компонентів (табл.3.2).

Таблиця 3.2 – Вимоги до пасивних мережевих компонентів

Вимога	Наявність
Мережна сертифікація	+
Гарантований термін служби	Гарантія не менше 20 років
Стандарти	Відповідність стандартам та вимогам SCS
Термін служби	Понад 30 років

Основними виробниками пасивних компонентів є: R&M, Molex ,Ok-Net, QTECH. Таблиця 3.3 порівнює торгові марки з цими вимогами.

Таблиця 3.3 - Порівняння виробників пасивних пристроїв

	QTECH	Ok-Net	Molex	R&M
Строк служби по гарантії	25	15	20	25
Термін експлуатації	40	30	30	50
Сертифікація	так	так	так	так
Відповідність СКС	так	так	так	так
Умовна вартість за порт (грн)	220	150	210	275

Виходячи з таблиці вище, з точки зору вартості та експлуатаційних параметрів ви можете використовувати продукти QTECH,R&M. За ціною продукція QTECH знаходиться в більш дешевому стані, вона використовується для побудови мережі.

3.2 Підбір активних компонентів

3.2.1 Вибір апаратного забезпечення ядра

Центральний маршрутизатор є основним пристроєм мережі. Він відповідає за багато функцій, він повинен організувати захист локальної мережі від зовнішніх перешкод і запропонувати місцевим користувачам можливість підключення до Інтернету. У Таблиці 3.4 представлені вимоги до обладнання. Відповідно до правил і розрахунків, маршрутизатор має наступні вимоги:

Таблиця 3.4 –Вимоги до обладнання

кількість портів	Fast Ethernet 1000 Base-TX - 2
пропускна здатність	не менше 200 Мбіт / с
підтримка протоколів	TCP / IP, 802.1q, IPv4, ARP, DHCP, NAT, VLAN

можливість монтажу	19-дюймова телекомунікаційна стійка

Кілька маршрутизаторів обраної марки D-Link відповідають потребам. Порівняльна характеристика додавання до таблиці 3.5.

На підставі порівняння найкраще використовувати DFL-1660, який зображено на рис. 3.1 [16].

Рисунок 3.1 – Маршрутизатор DFL-1660

Таблиця 3.5 – Порівняння маршрутизаторів

	DFL-1660	DFL-260E	DFL-2500
Споживання енергії	27,2 Вт	18,6 Вт	39 Вт
Тип та кількість портів	6xGE, 2xUSB, 1xRS232	1xWANxGE, 1xDMZxGE, 5xLAnxGE, 1xConsolexRJ-45	8 GE
Споживання енергії	Споживання енергії	Споживання енергії	Споживання енергії
Продуктивність	Продуктивність міжмережного екрану 1200 Мбіт/с Кількість паралельних сесій 600 000 Політики 4000	Продуктивність міжмережного екрану 150 Мбіт/с Кількість паралельних сесій 25 000 Політики 500	Продуктивність міжмережного екрану 600 Мбіт/с Кількість паралельних сесій 1 000 000 Політики 4000

Мережні функції	DHCP сервер/клієнт DHCP Relay Маршрутизація на основі політик IEEE 802.1q VLAN: 1024 VLAN на основі портів IP Multicast: IGMP v3	DHCP сервер/клієнт DHCP Relay Маршрутизація на основі політик IEEE 802.1q VLAN: 8 VLAN на основі портів IP Multicast: IGMP v3	DHCP клієнт/север DHCP relay Маршрутизація на основі політик IEEE 802.1Q VLAN IP Multicast: IGMP v1-v3, IGMP Snooping
Міжмережний екран	Прозорий режим NAT, PAT Протокол динамічної маршрутизації OSPF H.323 NAT Traversal Політики за розкладом Application Layer Gateway (ALG) Технологія Zone-Defense Активна мережна безпека	Прозорий режим NAT, PAT H.323 NAT Traversal Політики за розкладом Application Layer Gateway (ALG) Технологія Zone-Defense Активна мережна безпека	PPPoE Прозорий режим NAT, PAT Протокол динамічної маршрутизації OSPF H.323 NAT Traversal Політики за розкладом Application Layer Gateway (ALG) Технологія Zone-Defense

Міжмережні екрани NetDefend UTM оснащені системою виявлення і запобігання, антивірусом і фільтрацією Web-вмісту для перевірки і захисту вмісту на 7 рівні. Використовуваний в даних пристроях апаратний прискорювач збільшує продуктивність IPS і AV, керуючої бази пошуку в Web, що містить мільйони URL для фільтрації Web-вмісту (WCF). Сервіси поновлення IPS, антивіруса і бази даних URL захищають офісну мережу від вторгнень, черв'яків, шкідливих кодів і задовольняють потребам бізнесу з управління доступом співробітників до Інтернет [5].

3.2.2 Вибір центрального комутатора

Центральний перемикач використовується для підключення периферійних пристроїв сервера та перемикачів рівня доступу до поверху будівель. У Таблиці 3.6 представлені вимоги до обладнання. До центрального комутатора застосовуються такі вимоги:

Таблиця 3.6 –Вимоги до обладнання

директива	COS

кількість портів	1x100BaseTX, 9x1000 BaseT
підтримка	VLAN
підтримка режиму використання	безпечний режим

У таблиці 3.7 порівнюються можливі продукти D-Link, які можуть виконувати роль центрального комутатора.

Таблиця 3.7 - Порівняння вимикачів

	DGS-1500-20	DGS-3612G	DGS-1210-20
Підтримка VLAN, 802.1q	так	так	так
Комутаційна спроможність	40	24	40
CoS	так	так	ні
Енергоспоживання (Вт)	15,7	22,4	14,06
Конфігурація	16 10/100/1000BASE-T, 4 SFP	8 SFP, 4 комбо-порта 10/100/1000 BASE-T/ SFP, 1 RS-232	16 10/100/1000BASE-T, 2 SFP
OSI	2	3	2

Залежно від функціонального складу, властивостей та середнього споживання ми вибираємо перемикач DGS-1500-20, який зображено на рис. 3.2.

Рисунок 3.2 – перемикач DGS-1500-20

3.2.3 Вибір комутатора для поверхневого доступу

Перемикач наземного доступу використовується для підключення ПК, IP-телефонів, IP-камер та бездротових точок доступу. У Таблиці 3.8 представлені

вимоги до обладнання. До вимог доступу в транспортному засобі застосовувались такі вимоги:

Таблиця 3.8 –Вимоги до обладнання

кількість портів	48x100BaseTX, 1x1000 BaseT
директива	COS
підтримка	VLAN
технологія	PoE
підтримка режиму використання	безпечний режим

У таблиці 3.9 порівнюються можливі, які можуть виконувати роль перемикача доступу.

Таблиця 3.9 - Порівняльні властивості вимикачів

	DWS-3024	DES-3200-52P	DGS-3620-52P
Максимальний рівень потужності на порт, Вт	14	14	14
Енергоспоживання, Вт	27	25	24,2
Підтримка Vlan	повна	повна	повна
Вартість, грн	24577	9570	32205
Конфігурація портів	24 10/100/1000BASE-T PoE, 4 SFP	48x10/100 Base,PoE,2xRJ-45 10/100/1000 Base, 2xSFP	48 10/100/1000BASE-T PoE, 4 SFP

Оптимальною конфігурацією для кількості портів і вартості є використання комутаторів DES-3200-52P, який зображено на рис. 3.3 [17].

Рисунок 3.3 – Комутатор DGS-1500-20

3.2.4 Вибір точки доступу

При виборі точок доступу слід враховувати наступні технічні вимоги до розподілу. У Таблиці 3.10 представлені вимоги до обладнання.

Таблиця 3.10 –Вимоги до обладнання

кількість портів	100Base-TX та PoE
інтерфейс	RJ-45
бездротовийй стандарт	802.11b / g / n
частотний діапазон	2,4 ГГц
ппропускна здатність	не менше 18 Мбіт / с
технологія	PPoE, WEP,WPA

Ці продукти були проаналізовані, та під час аналізу продуктів увагу звернено на D-Link. Властивості зведені у таблицю 3.11.

Таблиця 3.11 - Характеристики точки доступу

	DWL-2600AP	DWL-3600AP	DWL-6600AP
Потужність (дБм)	7	21	11
Використання у закритих приміщеннях	низька	середня	висока
Енергоспоживання (Вт)	12	12,5	12
Безпровідний інтерфейс	802.11b/g/n 2,4 ГГц 2x2 MIMO	802.11b/g/n 2,4 ГГц 2x2 MIMO	802.11b/g/n 2,4 ГГц 2x2 MIMO
Вартість (грн)	685	1334	2368
Дротовий інтерфейс	10/100 Fast Ethernet	10/100/1000 Gigabit Ethernet	10/100/1000 Gigabit Ethernet
PoE	так	так	так

На основі порівняльних властивостей була обрана модель DWL-3600AP, яка зображена на рис. 3.4. Вибір цієї точки доступу заснований на рівні потужності, що дозволяє використовувати її в приміщенні з змішаними будівельними матеріалами [18].

Рисунок 3.4 – Точка доступу DWL-3600AP

3.2.5 Вибір компонентів системи відеоспостереження

Для системи відеоспостереження необхідно використовувати два основних компоненти - мережеві IP-камери та мережевий відео реєстратор.

У Таблиці 3.11 представлені вимоги до обладнання.

IP-відеокамери мають такі вимоги:

Таблиця 3.11 –Вимоги до обладнання

кодек	H.264
протоколи	DHCP, IPv4, Ethernet
потужність камер	не повинна перевищує 14 Вт
технологія	PoE

У таблиці 3.12 порівняно кілька камер із сімейства D-Link.

Таблиця 3.12 – Порівняння IP-камер

	DCS-3112	DCS-6112	DCS-6513	DCS-6314
Механічне керування	ні	ні	так	так
Потужність (дБм)	3,6	4,4	10,5	10
Формат	HD	Full HD	Full HD	Full HD
Вбудована пам'ять (Мб)	ні	128, слот для карт пам'яті	ні, слот для карт пам'яті	ні, слот для карт пам'яті
Вид виконання	вулична	купольна	купольна	купольна
Кодек	H.264, MPEG-4, MJPEG	H.264, MPEG-4, MJPEG	H.264, MPEG-4, MJPEG	H.264, MPEG-4, MJPEG
Інтерфейс	10/100 BASE-TX Fast Ethernet PoE	10/100 BASE-TX Fast Ethernet PoE	10/100 BASE-TX Fast Ethernet PoE	10/100 BASE-TX Fast Ethernet PoE
Нічна зйомка	так	ні	так	так

Виходячи із загального порівняння вартості та ключових характеристик, камера DCS-6314 була б оптимальною для використання, яка зображена на рис. 3.5.

Рекордери D-Link можуть бути реалізовані відповідно до двох концепцій: з використанням власної апаратної платформи або з використанням програмного забезпечення на базі апаратної платформи користувача. На ринку представлено лише дві моделі апаратних мережевих відео реєстраторів. Порівняння показано у таблиці 3.8 [19].

Рисунок 3.5 – Камера DCS-6314

Таблиця 3.13 – Порівняння відео реєстраторів

	DNR-326	DNR-322L
Формат для зберігання архівів	H.264, MPEG-4, M-JPEG	H.264, MPEG-4, M-JPEG
Інтерфейс	100/1000 Base-T/RJ-45	100 Base-T/RJ-45
Потужність (Вт)	48	25,2
Дистанційний перегляд	Так	так
Операційна система	Linux	Linux
Об'єм дискового масиву (Тб)	10	2
Кількість камер	обмежена пропускною здатністю	9
Вид	професійний	начальний

На основі порівняння пристрій DNR-326, який зображено на рис. 3.6. Він відповідає вимогам щодо властивостей (тобто наявності гігабітного інтерфейсу) [20].

Рисунок 3.6 – Пристрій DNR-326

3.2.6 Вибір компонентів системи IP-телефонії

Телефонна система базується на протоколі IP-телефонії SIP. Введення телефонної мережі вимагає використання АТС та IP-телефонів. У Таблиці 3.14 представлені вимоги до обладнання.

До IP-АТС застосовуються наступні вимоги:

Таблиця 3.14 –Вимоги до обладнання

зовнішні лінії	39
внутрішні лінії	260
IP-телефонія	SIP
підтримка	ISDN-PRI / BRI

Основними елементами телефонної мережі є прямі IP-АТС та телефони.

Звичайно, рішення приймається стосовно відкритих джерел. У Таблиці 3.15 представлені вимоги до обладнання. Серед товарів, які розповсюджуються безкоштовно, найпопулярнішими є:

Таблиця 3.15 –Вимоги до обладнання

програмна платформа	SipXecs
кроссплатформенная програма	Yate
телефонная платформа	FreeSWITCH
компьютерное приложение	Asterisk

Кожна з представлених систем має свої особливі характеристики. Найчастіше вживаний продукт - зірка.

Asterisk - це повноцінна програмна АТС. Вона може працювати на таких операційних системах, як Linux, BSD, Windows і OS X і надає Вам всі можливості, які є у звичайній міні АТС і навіть більше. Функціонування Asterisk засноване на протоколах, які забезпечують передачу голосу через мережі заснованих на IP протоколі (VOIP) і, завдяки цьому, дана АТС може працювати практично з будь-яким обладнанням для IP-телефонії, які використовують стандартні протоколи для VOIP, при цьому використовуючи відносно недороге апаратне забезпечення. Asterisk надає функції голосової пошти (Voicemail), конференцій, інтерактивного голосового меню (IVR), центру обробки викликів і їх обробки (Call Queuing). Він також має підтримку таких сервісів, як переклад викликів іншому абоненту, сервіс визначення і передачі абонента, якому разом із дзвінком (callerID), протоколи ADSI, SIP, H.323 (як в режимі терміналу, так і в режимі гейтування), MGCP (тільки для call

manager) і SCCP / Skinny (в повному обсязі). У розділі Можливості Ви можете знайти більш повний список функцій, які може виконувати Asterisk.

Asterisk не потребує додаткового апаратного забезпечення для реалізації передачі голосу через IP мережі (VOIP). Можна використовувати єдиного (або декількох) провайдерів VOIP для вхідних та / або викликів (вхідні та вихідні дзвінки можуть оброблятися різними провайдерами Інтернет і / або звичайної телефонії) [21].

Тип телефону, який можна використовувати з обраною гібридною IP-АТС, може бути будь-яким, але він повинен відповідати таким специфікаціям. У Таблиці 3.16 представлені вимоги до обладнання.

Таблиця 3.16 –Вимоги до обладнання

інтерфейс	10/100 Base-T
технологія	PoE
протокол	SIP
споживання енергії	14 Вт

У таблицях 3.17 приведені порівняльні властивості IP-телефонів D-Link.

Таблиця 3.17 – Порівняння IP-телефонів

	DPH-150S/F2	DPH-400SE/E/F3	DPH-150SE/F3
PoE	ні	так	G.711a/u (64 Кбіт/с) G.729A/B (8 Кбіт/с) G.723.1 (високий/низький) G.726-32 G.722
Аудіо кодек	G.711a/u (64 Кбіт/с) G.729A/B (8 Кбіт/с) G.723.1 (високий/низький) G.726-32 G.722	G.711a/u (64 Кбіт/с) G.729A/B (8 Кбіт/с) G.723.1 G.722 G.726-32	1 порт WAN 10/100BASE-TX PoE для LAN, 1 порт LAN 10/100BASE-TX для ПК
IP-телефонії	SIP	SIP	DPH-150SE/F3
Споживана потужність (Вт)	1,8	2,8	так
Тип портів	1 порт WAN 10/100BASE-TX для LAN, 1 порт LAN 10/100BASE-TX для ПК	1 порт WAN 10/100BASE-TX PoE для LAN, 1 порт LAN 10/100BASE-TX для ПК	SIP

На основі порівняння модуль розширення DPH-400SE / E / F3 відповідає вимогам щодо своїх властивостей, який зображено на рис. 3.7 [22].

Рисунок 3.7 – Модуль розширення DPH-400SE / E / F3

3.3 Повний набір мережевих вузлів

Комплектація кожного поверху наведена в таблиці 3.18.

Таблиця 3.18 - Специфікація активного обладнання

Розташування	Вузол	Тип пристрою	Поверхи, що обслуговуються
1-ий поверх	Центр	DFL-1660	1
		DGS-1500-20	
		DES-3200-52P	
		DWL-3600AP	
		DCS-6314	
		DNR-326	
		TrixBox	
		DPH-400SE/E/F3	
		Сервер	
2-й поверх	2-й поверх	DES-3200-52P	2
		DCS-6314	
		DPH-400SE/E/F3	
		DWL-3600AP	

3-й поверх	3-й поверх	DES-3200-52P	3
		DCS-6314	
		DPH-400SE/E/F3	
		DWL-3600AP	
4-й поверх	4-й поверх	DES-3200-52P	4
		DCS-6314	
		DPH-400SE/E/F3	
		DWL-3600AP	
5-й поверх	5-й поверх	DES-3200-52P	5
		DCS-6314	
		DPH-400SE/E/F3	
		DWL-3600AP	
6-й поверх	6-й поверх	DES-3200-52P	6
		DCS-6314	
		DPH-400SE/E/F3	
		DWL-3600AP	
7-й поверх	7-й поверх	DES-3200-52P	7
		DCS-6314	
		DPH-400SE/E/F3	
		DWL-3600AP	
8-й поверх	8-й поверх	DES-3200-52P	8
		DCS-6314	
		DPH-400SE/E/F3	
		DWL-3600AP	
9-й та 10-й поверхи	9-й поверх	DES-3200-52P	9,10
		DCS-6314	
		DPH-400SE/E/F3	
		DWL-3600AP	

3.4 Ієрархічна кабельна система

Ієрархічна кабельна система будівельної групи - СКС. Він може бути представлений у декількох серіях структурних підсистем:

- комп’ютерна база та комп’ютерний дистрибутор;
- основна лінія будинку та розподільник будинку;
- горизонтальний підлоговий кабель та розподільник підлоги.

В рамках проектного проекту СКС існують такі структурні підсистеми:

- основні та вітчизняні дистрибутори (вертикальні)
- горизонтальний підлоговий кабель і розподільник підлоги (горизонтальні).

Для створення СКС потрібні такі технічні описи:

- диспетчерська (технічна кімната, де створюються пристрої групового зв'язку, пристрої загальнодоступної мережі: АТС, сервер, комутаційні центри)
- кросовер (технічний пакет, що містить комутатор СКС, який обмежує обмежену групу користувачів).

В офісній будівлі є десять поверхів з кабінетами для співробітників, IP-камерами, точками доступу, офісами, технічними приміщеннями. Для кожного поверху необхідно виділити приміщення для перетину та приміщення для центральної диспетчерської. Для цих технічних приміщень необхідно визначити їх місце розташування і переконатись, що в цих приміщеннях існують умови роботи приладів. Також необхідно розрахувати кількість кабелів і розробити СКС для кожного поверху (горизонтальний СКС) і для будівлі в цілому (вертикальний СКС).

Для того, щоб підключити мережеві пристрої до робочих станцій встановлюються зовнішні розетки.

Кабель горизонтальної підсистеми СКС прокладається під стелею перекриттів, кабель вертикальної підсистеми в спеціальних кабельних трубопроводах між поверхами. Кабелі горизонтальної підсистеми СКС повинні прокладатися в спеціальних кабельних лотках на стелі. Мінімальна відстань між дротовими інформаційними мережами та мережею електропостачання повинна бути не менше 200 мм.

QTECH використовується як постачальник пасивних компонентів.

У таблиці 3.19 наведені характеристики обраного пасивного обладнання.

Таблиця 3.19 – Пасивне устаткування

Пасивне устаткування	Тип
QTECH-QS 18	Шафа 19 дюймова 18U
QTECH-TP-UTP-45	Розетка RJ-45, cat 5e
QTECH-ПП-24-UTP-45	Патч панель RJ-45 UTP, 24 порта
QTECH-TP-2xUTP-45	Розетка 2xRJ-45, cat 5e
QTECH-ВП-4x2	Кабель мідний CAT5e
QTECH-QS 28	Шафа 19 дюймова28 U
QTECH-PC-UTP-0,5	Птач-корд UTP RJ-45
QTECH-QS 32	Шафа 19 дюймова 32 U

Висновки до розділу 3

Третя частина дипломного проекту стосується апаратної реалізації телекомунікаційної мережі. Визначено основні групи пристроїв, на яких буде реалізована мережа - комутатори, маршрутизатори, міні-автоматичні телефонні станції, компоненти системи відеоспостереження, бездротові точки доступу, кабелі, патч-панелі, патч-шнури, роз'єми та телекомунікаційні шафи. В рамках детального аналізу телекомунікаційного ринку України та порівняльного аналізу представлених брендів D-Link було обрано постачальником активних пристроїв та QTECH для пасивних пристроїв. Пасивна складова планової мережі будується відповідно до вимог СКС, тобто. Н. Фізичне середовище є уніфікованим і легко трансформується для передачі голосу та даних.

4. РОЗРОБКА IP-МЕРЕЖІ, ПРОВЕДЕННЯ МОДЕЛЮВАННЯ МЕРЕЖІ ЗА ДОПОМОГОЮ ПАКЕТУ PACKET TRACER

4.1 Постановка задачі

Проектована телекомунікаційна мережа, що включає дві підмережі, які мають можливість підключатися до мережі Інтернет. Основне мета – налаштувати цю телекомунікаційну мережу.

Задачі, що необхідно вирішити:

1. Налаштувати VPN між двома мережами.

2. Налаштувати DHCP.

3. Налаштувати VLAN, один VLAN повинен бути загальний між двома мережами.

4. Налаштувати STP протокол.

Результат – розробка IP-мережі, проведення моделювання мережі за допомогою пакету Packet Tracer.

Результати розробки можуть бути використані при створенні реальної мережі.

4.2 Проектування топологічної схеми

На цьому етапі виконується побудування структурної схеми мережі. Для цього треба виділити відділи відповідно завдання, позначити їхні типи та кількість комп’ютерів у них. Мережа будується за стандартною трирівневою топологією. Кожний відділ може бути підключений до одного комутатора рівня доступу; кілька відділів підключаються до одного комутатора рівня розподілу. Тому для побудування структурної схеми мережі треба обрати одне з приміщень, у якому буде розташовано комутатор рівня розподілу; доречно,

щоби це приміщення співпадало з приміщенням, у якому є будь-який відділ і відповідний комутатор рівня розподілу.

Приміщення, у яких розташовано відділи зі своїми комутаторами рівня доступу, з'єднуються з приміщенням, у якому розташовано комутатор рівня розподілу лініями зв'язку. Проектування фізичних ліній, вибір технологій канального рівня не є предметом даної роботи. Тому лінії зв'язку прокладають дещо абстрактно, не прив'язуючи їх до конкретних типів середовища передачі даних. Але все-таки варто провести деяку оптимізацію топології, виходячи з мінімальної загальної довжини ліній проектованої мережі. При цьому основну оптимізацію треба проводити стосовно ліній, які з'єднують між собою комутатор рівня доступу і комутатори рівня розподілу. А далі обрати аналогічно приміщення, у яких будуть розташовані маршрутизатори рівня ядра. Для проектування топології основний критерій – найменша довжина ліній зв'язку, а структурне підпорядкування відділів не має ніякого значення.

Топологію записано у вигляді таблиці, яка показує, який комутатор до якого підключено – таблиця 4.1 Кожен з маршрутизаторів ядер має 2-3 комутатори розподілу. Логічна топологія буде – «ієрархічна зірка» з надлишковими зв'язками. Деякі комутатори розподілу мають декілька резервних ліній сполучення з комутаторами доступу, таким чином створюються надлишкові зв'язки.

Кожний пристрій підключається до комутаторів доступу, доступ до мережі Інтернет здійснюється за допомогою одного маршрутизатора.

Перелік усіх пристроїв, що використовувались у побудові мережі :

1. 23 комп'ютерів.

2. 11 серверів.

3. 15 комутаторів Cisco.

4. 3 маршрутизатори Cisco.

Усього: 52 пристрої.

Таблиця 4.1 – Сполучення маршрутизаторів між собою

Комутатор доступу	Комутатор розподілу	Маршрутизатор ядра
Switch1.1.1	Switch1.1	Network 1

Switch1.1.2		
Switch1.2.1	Switch1.2	
Switch1.2.2		
Switch1.2.3		
Switch10	Switch17	Network 2
Switch12	Switch11	
Switch13		
Switch14		
Switch15		
Switch16		
PC-Інтернет	-	Network 3

4.3 Розподіл адресного простору

На цьому етапі треба визначити адреси для всіх мереж відділів і ліній сполучень. Є кілька підходів для того, щоб розподілити адреси між відділами і філіями. Перший підхід – порядок роздачі за структурним принципом, а саме: всі відділи, які мають однакове призначення, отримують адреси один за одним. Логіка розподілу така: впорядкувати список відділів за алфавітом, однакові відділи – за кількістю обладнання. Далі видавати адреси мереж, починаючи з першої у обраному загальному просторі (обрано адресний простір 10.0.0.). При цьому розмір мережі (мережна маска) обирається з деяким запасом, приблизно півтора, й округляється вгору до найближчого ступеню двійки. Так, якщо у мережі кількість обладнання 28, то для неї можна обрати мережу десь на 28*1.5=42 вузли, округляємо до 64, і визначаємо маску 255.255.255.192 (26 біт). Цей розподіл зручно робити за таблицею IP-лото. Наприклад, можна запропонувати таке визначення адрес – таблиця 4.2.

Таблиця 4.2 – Розподіл адресного простору за структурним принципом

Мережа	Адреса мережі	Маска
Switch1.1.1	10.0.0.0	255.255.255.192

Switch1.1.2	10.0.0.32	255.255.255.224
Switch1.2.1	10.0.1.0	255.255.255.0
Switch1.2.2	10.0.2.0	255.255.255.0
Switch1.2.3	10.0.1.0	255.255.255.128
Switch10	10.0.2.0	255.255.255.128
Switch12	10.0.2.128	255.255.255.128
Switch13	10.0.2.0	255.255.255.192
Switch14	10.0.2.32	255.255.255.224
Switch15	10.0.2.64	255.255.255.224
Switch16	10.0.3.0	255.255.255.128
PC-Інтернет	10.0.3.128	255.255.255.128

Тепер спробуємо інший спосіб розподілу адрес – за географічним принципом. Будемо видавати сусідні адреси відділам з одного географічного розташування. (таблиця 4.3).

Таблиця 4.3 - Розподіл адрес за географічним принципом

Мережа	Адреса мережі	Маска
Switch1.1.1	10.0.21.128	255.255.255.192
Switch1.1.2	10.0.25.224	255.255.255.224
Switch1.2.1	10.0.9.0	255.255.255.0
Switch1.2.2	10.0.0.0	255.255.255.0
Switch1.2.3	10.0.24.128	255.255.255.128
Switch10	10.0.17.0	255.255.255.128
Switch12	10.0.17.128	255.255.255.128
Switch13	10.0.34.128	255.255.255.192
Switch14	10.0.30.160	255.255.255.224
Switch15	10.0.18.128	255.255.255.224
Switch16	10.0.20.0	255.255.255.128
PC-Інтернет	10.0.33.0	255.255.255.252

Є також і лінії сполучень між маршрутизаторами, які теж є окремими мережами і для них треба визначати адресний простір і адресну маску. Така мережа називається «точка-точка», адресний простір для неї має тільки 2.

На рис.4.1 можна побачити схему проектованої IP-мережі. Слід зауважити, що це лише фрагмент від усієї схеми, але цього фрагменту достатньо для того, що показати основні налаштування та можливості програмного продукту Cisco Packet Tracer.

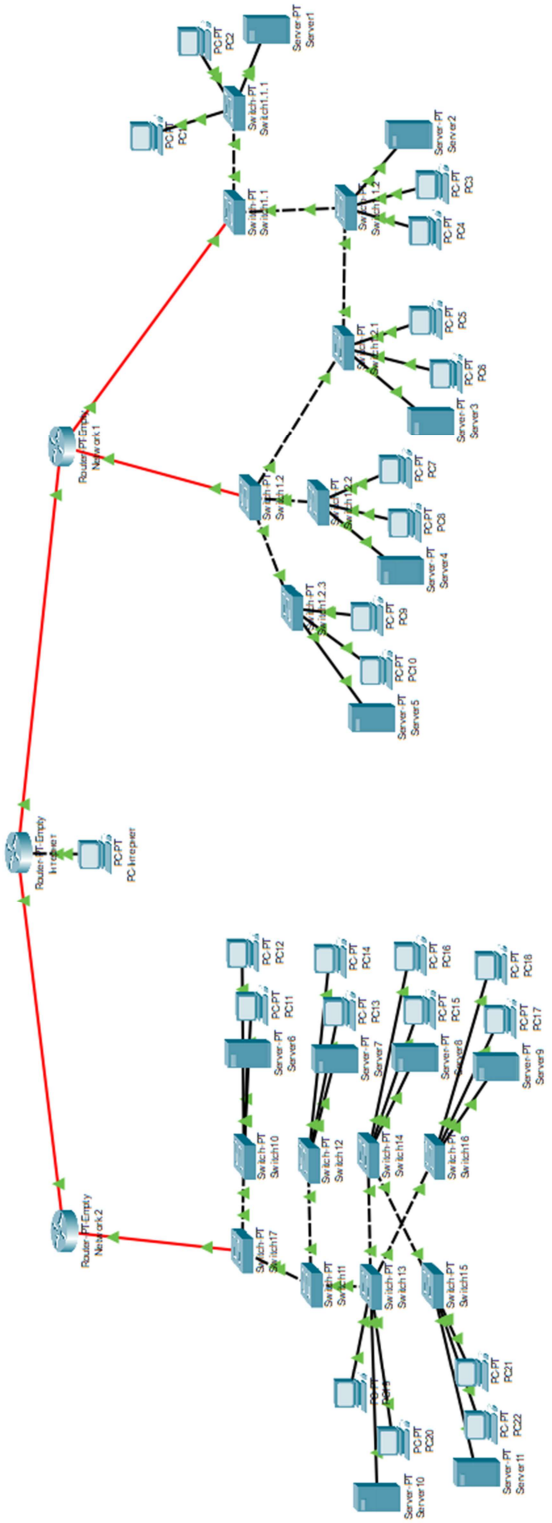


Рисунок 4.1 – Схема мережі

4.4 Конфігурація VLAN

4.4.1 Конфігурація VLAN в режимі Config-vlan

Конфігурація VLAN в режимі Config-vlan:

Процес конфігурації:

1) Виконати команду "configure terminal", щоб перейти в режим конфігурації.

2) Створити VLAN командою "vlan <number>".

2) Виконати команду "interface [type] mod / port>", щоб перейти в режим конфігурації інтерфейсу.

3) Виконати команду "switchport mode access", щоб сконфігурувати режим порту.

4) Виконати команду "switchport access <vlan-id>", щоб вказати до якого VLAN'у буде відноситься інтерфейс.

5) Щоб перевірити конфігурацію VLAN, виконати команду "show vlan".

Приклад налаштування на комутаторі Switch1.1.1:

```
Switch1.1.1 (config)#vlan 101
Switch1.1.1 (config-vlan)#name Accounting
Switch1.1.1 (config-vlan)#exit
Switch1.1.1 (config)#int fa1/0
Switch1.1.1 (config-if)#switchport mode access
Switch1.1.1 (config-if)#switchport access vlan 101
Switch1.1.1 (config-if)#end
```

4.4.2 Конфігурація VLAN в режимі VLAN database

Процес конфігурації:

1) Виконати команду "vlan database", щоб перейти в режим редагування VLAN database.

2) Виконати команду "vlan vlan-id> name vlan-name" щоб додати VLAN і призначити йому номер і ім'я.

3) Щоб застосувати зміни, виконати команду "apply", після чого виконати команду "exit", щоб вийти з режиму конфігурації VLAN.

4) Виконати команду "interface [type] mod / port>", щоб перейти в режим конфігурації інтерфейсу.

5) Виконати команду "switchport mode access", щоб сконфігурувати режим порту.

6) Виконати команду "switchport access <vlan-id>" щоб вказати до якого VLAN'у буде відноситься інтерфейс.

7) Для перевірки конфігурації VLAN, виконати команду "show vlan".

Приклад налаштування на комутаторі Switch1.1.1:

```
Switch1.1.1 #vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

 Switch1.1.1 (vlan)#vlan 104 name user
VLAN 104 added:
    Name: user
Switch1.1.1 (vlan)#apply
APPLY completed.
Switch1.1.1 (vlan)#exit
APPLY completed.
Exiting....
```

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1.1.1 (config)#int fa1/0
Switch1.1.1 (config-if)#switchport mode access
Switch1.1.1 (config-if)#switchport access vlan 2
Switch1.1.1 (config-if)#end
```

Base Initial configuration:

Рис. 4.2 демонструє приклад налаштування VLAN 101 та приєднання інтерфейсу.

Аналогічно налаштовуються й інші комутатори доступу.

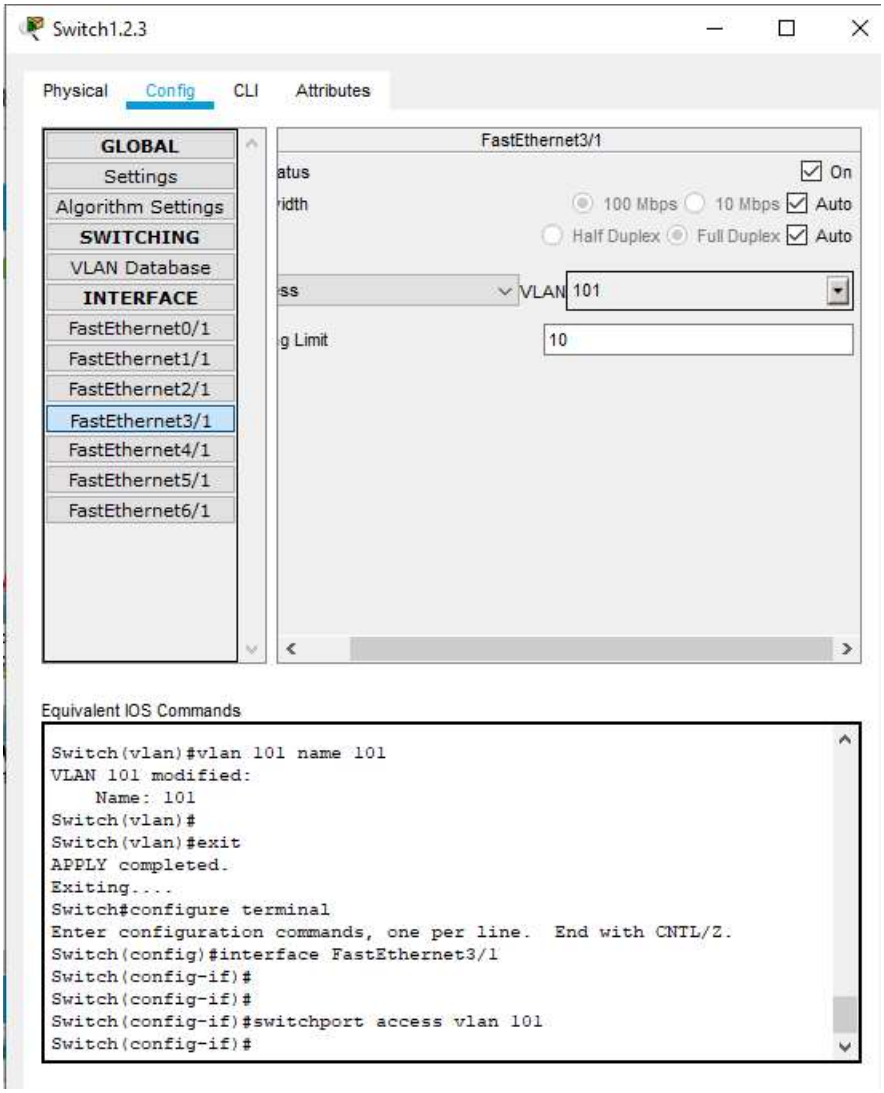


Рисунок 4.2 – Приклад налаштування VLAN

4.5 Налаштування DHCP

Протокол DHCP - дозволяє проводити автоматичну настройку мережі на комп'ютерах і інших пристроях. DHCP може бути налаштований на маршрутизаторах Cisco або на базі будь-якого сервера. Однак, маршрутизатор може працювати і як DHCP клієнт - отримуючи адресу на один зі своїх інтерфейсів. Про це можна прочитати детальніше тут. Налаштування DHCP сервера на маршрутизаторі це зручно в тому плані, що якщо вже є працюючий маршрутизатор, то простіше додати до нього максимальну кількість функціоналу (інтернет, NAT, DHCP і т.п.) щоб кожен пристрій мав своє

призначення. DCHP дозволяє автоматично налаштовувати на клієнті наступні основні параметри:

- IP адресу;
- основний шлюз;
- маску під мережі;
- DNS сервера;
- ім'я домену.

Це найбільш часте використання DHCP, але можна передаватись і величезна кількість інших параметрів. Наприклад, можна передавати додаткові маршрути, щоб в різні мережі комп'ютер підключвся через різні шлюзи. Або, за допомогою DHCP можна організовувати завантаження пристроїв по мережі. У цьому випадку клієнт отримує крім основних параметрів, адресу TFTP сервера і ім'я файлу на ньому (мається на увазі ім'я файлу - завантажувача ОС, яку необхідно завантажити по мережі).

Коли клієнт, наприклад, звичайний комп'ютер, запускається, ОС бачить, що для якоїсь мережної карти треба «Отримати параметри по DHCP». Такий комп'ютер не має поки IP адреси і відбувається наступна процедура отримання:

- Комп'ютер відправляє широкомовний запит. При цьому на другому рівні в фреймі стоїть мак адреса відправника - адреса комп'ютера, мак адреса одержувача - ffff.ffff.ffff, а на третьому рівні - в пакеті адреса відправника відсутня, адреса одержувача 255.255.255.255. Таке DHCP повідомлення називається «DHCP discover».
- Далі всі пристрої в мережі отримують це широкомовне повідомлення. DHCP сервера (а їх теоретично може бути кілька) і відповідають клієнту. Сервер резервує в своєму пулі адрес якусь адресу (якщо не було резервації до цього для даної mac-адреси клієнта) і виділяє цей ip клієнту на якийсь час (lease time). Беруться інші налащтування та все разом висилається. При цьому в якості адрес одержувача використовується вже новий виділений клієнтський ip і клієнтський mac. Це називається «DHCP offer».

– Клієнт вибирає вподобаний йому сервер (зазвичай він всього один) або вибирається той хто відповів першим. І відправляє зі свого mac і нового ip на mac і ip вже конкретного сервера «DHCP request» - згоду з отриманими параметрами.
– Сервер резервує за клієнтом виділену адресу на якийсь час (lease time). До цього моменту адреса була виділена, але не зарезервована. Тепер же вона остаточно закріплена за клієнтом. Сервер вносить так само рядок в свою ARP-таблицю і висилає клієнту, повідомлення, що він успішно зареєстрований - «DCHP Acknowledge».
– Клієнт починає працювати [6].

Налаштування DHCP:

```
Switch>en //·Привілейований·режим·EXEC¶
Switch#conf·t //·Режим·глобальної·конфигурації¶
Switch(config)#ip·dhcp·pool·101 //·створюємо·новий·пул·з·ім'ям·101¶
Switch(dhcp-config)#network·10.0.21.128·255.255.255.192//·Вказуємо·мережу,·адреси·
якої·будуть·присвоюватися·пристроям¶
Switch(dhcp-config)#default-router·10.0.21.129//·Вказуємо·IP-адресу·шлюзу¶
Switch(dhcp-config)#dns-server·8.8.8.8·//·Вказуємо·IP-адресу·dns·сервера¶
Switch(dhcp-config)#domain-name·test.ua·//·Вказуємо·адресу·домену¶
Switch(dhcp-config)#ex·//·Виходимо·з·режиму·конфігурації·dhcp·пулу/¶
```

Аналогічно налаштовуються й інші комутатори доступу.

На рис 4.3 приведено приклад налаштування серверу 1.

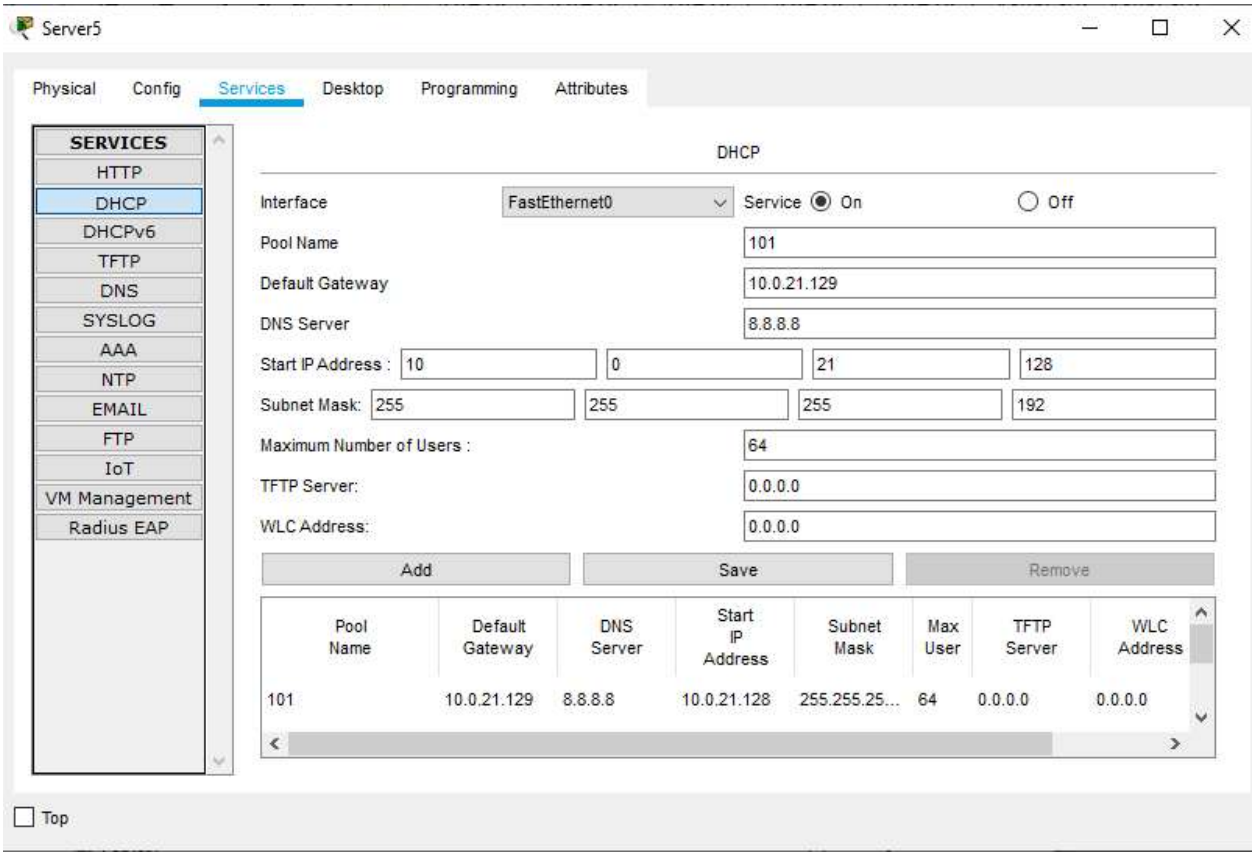


Рисунок 4.3 – Приклад налаштування DHCP

4.6 Налаштування STP протоколу

4.6.1 Відомості про STP протокол

STP (Spanning Tree Protocol) - мережевий протокол (або сімейство мережевих протоколів) призначений для автоматичного видалення циклів (петель комутації) з топології мережі на канальному рівні в Ethernet-мережах. Початковий протокол STP описаний в стандарті 802.1D. Пізніше з'явилося кілька нових протоколів (RSTP, MSTP, PVST, PVST +), що відрізняються деякими особливостями в алгоритмі роботи, в швидкості, відношенні до VLAN і ряді інших питань, але в цілому вирішуючих ту ж задачу схожими способами. Всі їх прийнято узагальнено називати STP-протоколами.

Протокол STP свого часу був розроблений мамою Інтернету Радіей Перлман (Radia Perlman), а пізніше, на початку 90-х перетворився на стандарт IEEE 802.1D.

В даний час протокол STP (або аналогічний) підтримується багатьма Ethernet-комутаторами, як реальними, так і віртуальними, за винятком найпримітивніших.

4.6.2 Алгоритм дії STP

Після включення комутаторів в мережу, за замовчуванням кожен комутатор вважає себе кореневим (root).

Кожен комутатор починає посилати по всіх портах конфігураційні Hello BPDU пакети раз в 2 секунди, максимальний проміжок 20 секунд.

Якщо міст отримує BPDU з ідентифікатором моста (Bridge ID) меншим, ніж свій власний, він припиняє генерувати свої BPDU і починає ретранслювати BPDU з цим ідентифікатором. Таким чином в кінці кінців в цій мережі Ethernet залишається тільки один міст, який продовжує генерувати і передавати власні BPDU. Він і стає кореневим мостом (root bridge).

Решта мости, що ретранслюють BPDU кореневого моста, додаючи в них власний ідентифікатор і збільшуючи лічильник вартості шляху (path cost).

Для кожного сегмента мережі, до якого приєднані два і більше портів мостів, відбувається визначення designated port - порту, через який BPDU, що приходять від кореневого моста, потрапляють в цей сегмент.

Після цього всі порти в сегментах, до яких приєднані 2 і більше портів моста, блокуються за винятком root port і designated port.

Кореневий міст продовжує посилати свої Hello BPDU раз в 2 секунди.

BPDU кадр.

Bridge Protocol Data Unit

Protocol Identifier розмір 2 байти

Protocol Version Identifier розмір 1 байт

BPDU Type розмір 1 байт

Flags розмір 1 байт

Root Identifier розмір 8 байт

Root Path Cost розмір 4 байт

Bridge Identifier розмір 8 байт

Port Identifier розмір 2 байт

Message Age розмір 2 байт

Max Age розмір 2 байт

Hello Time розмір 2 байт

Forward Delay розмір 2 байт

На рис. 4.4 зображно як виглядає BPDU кадр STP.

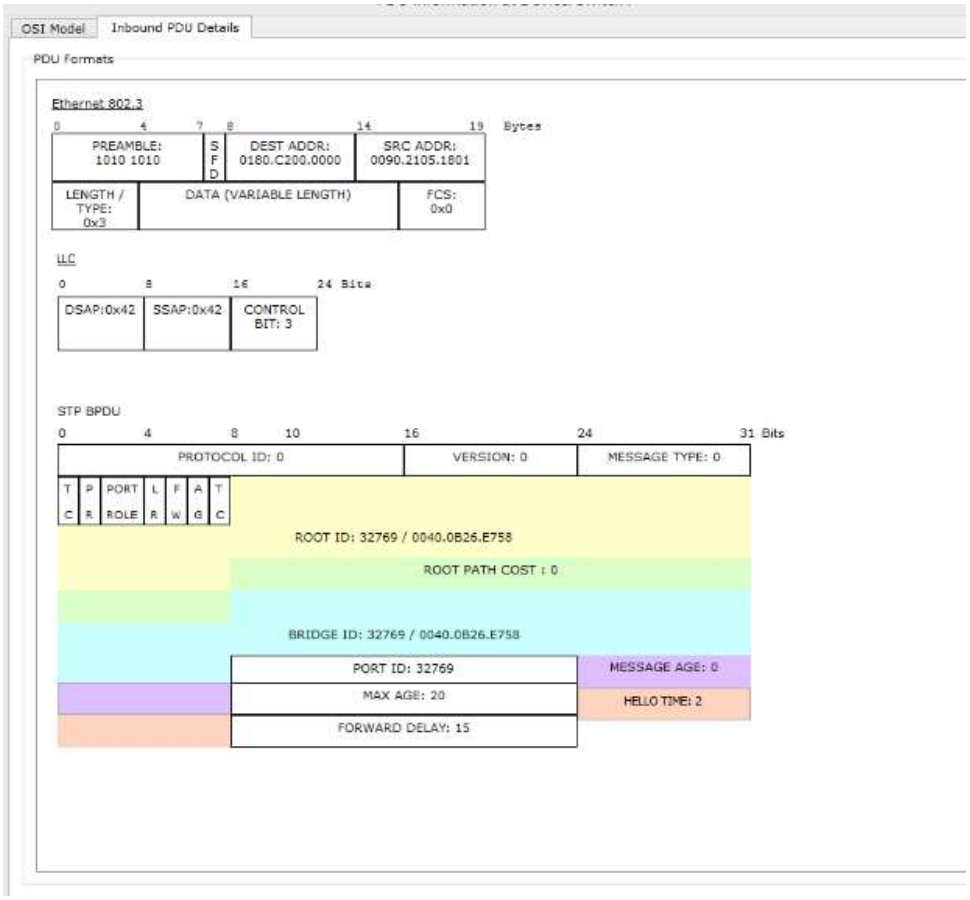


Рисунок 4.4 – Кадр BPDU

Стан портів:

1. Блокування (blocking)

2. Прослуховування (listening)

3. Навчання (learning)

4. Передача (forwarding)

4.6.3 Налаштування STP

Приклад роботи і налаштування STP. Два комутатора з'єднаних двома лінками (рис.4.5), видно то STP вже працює і один порт у другого комутатора погашений щоб не було петлі.

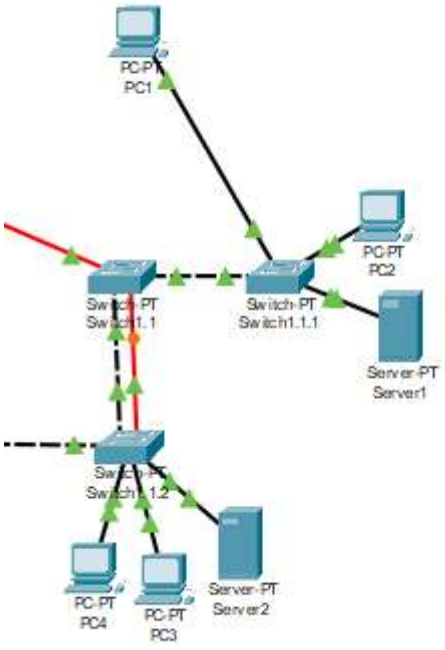
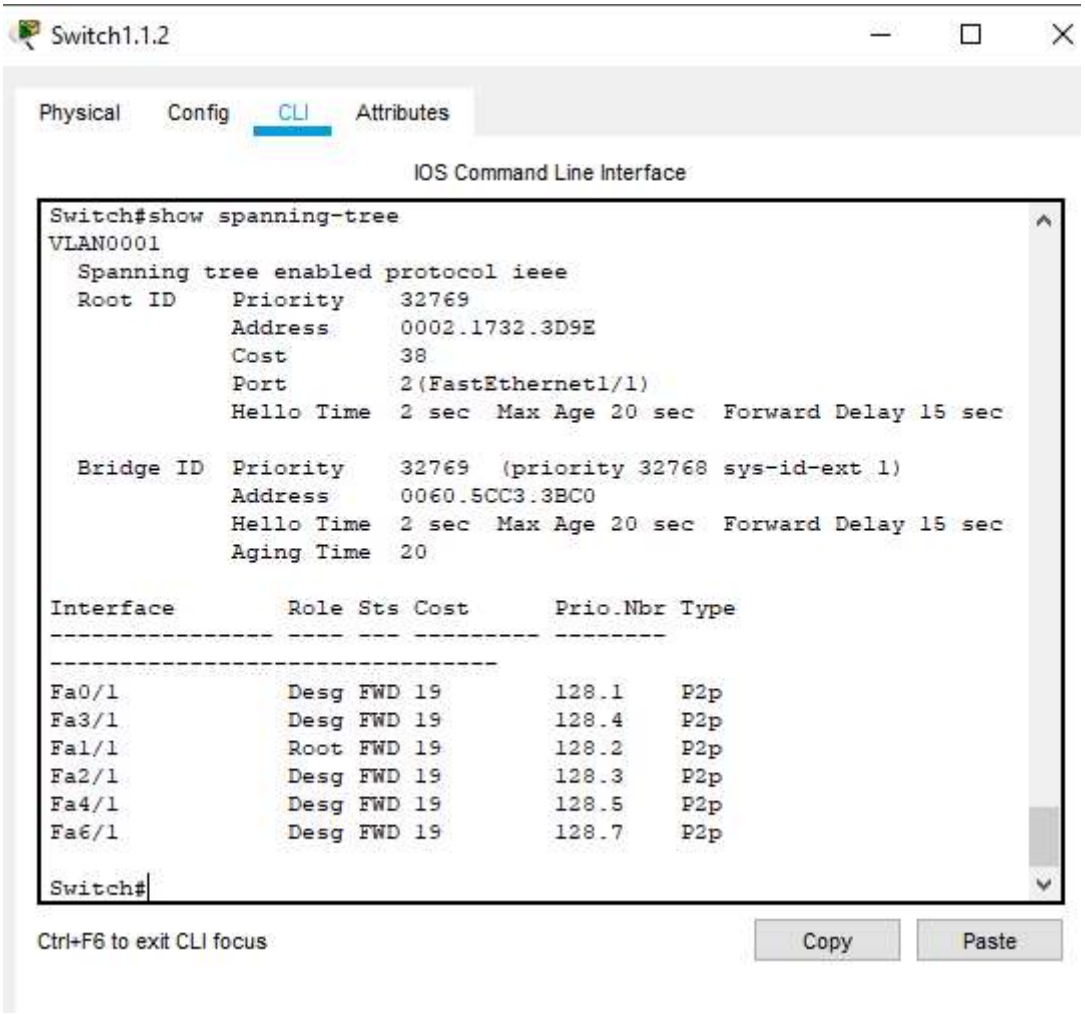
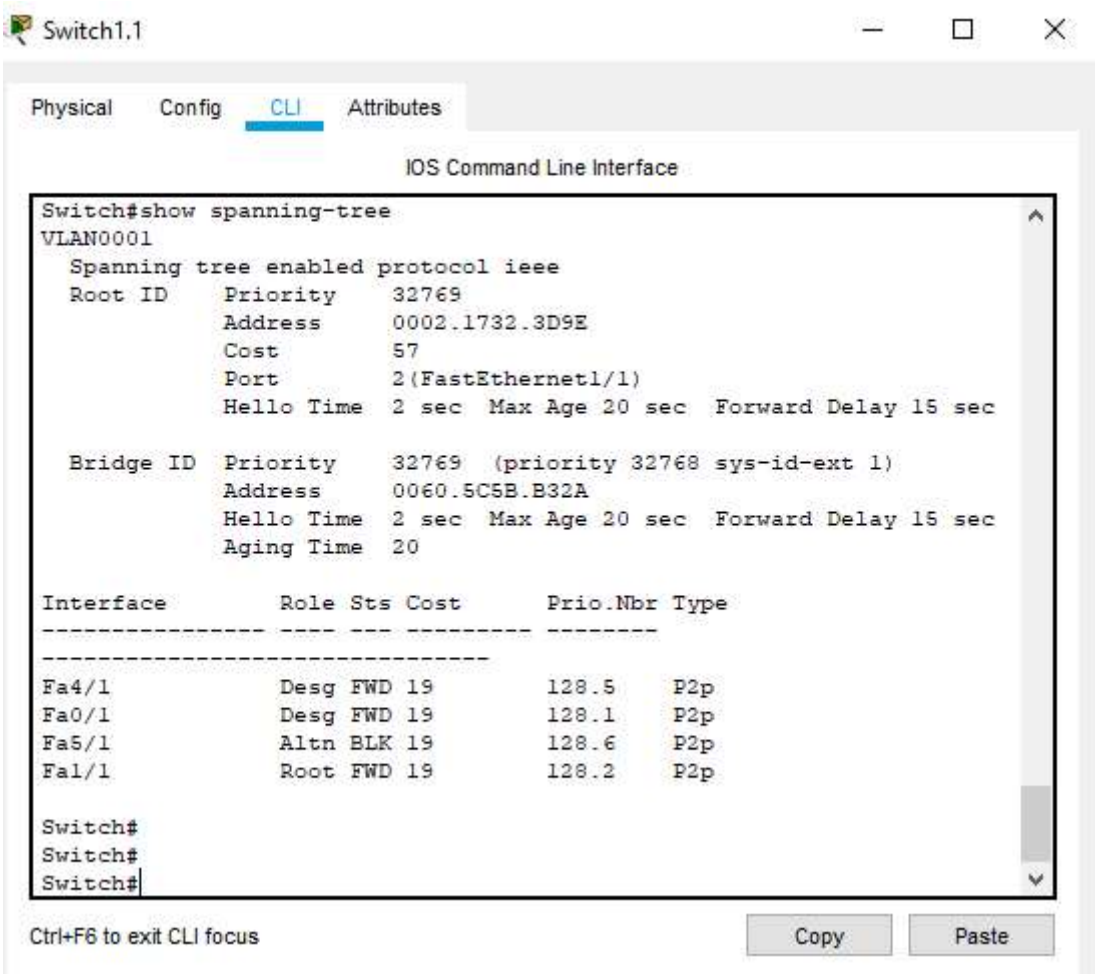


Рисунок 4.5 – Фрагмент мережі з петлею



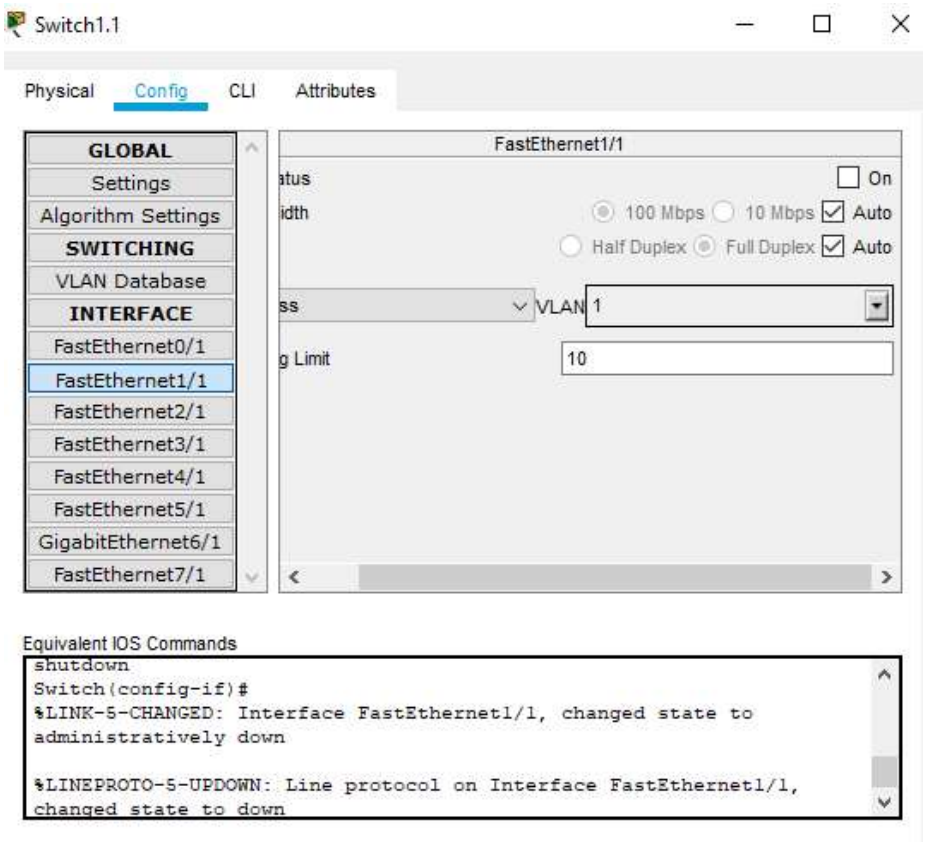
Бачимо, що це рутовий комутатор і всі порти в стані «передача».

Дивимося, теж на другому комутаторі.

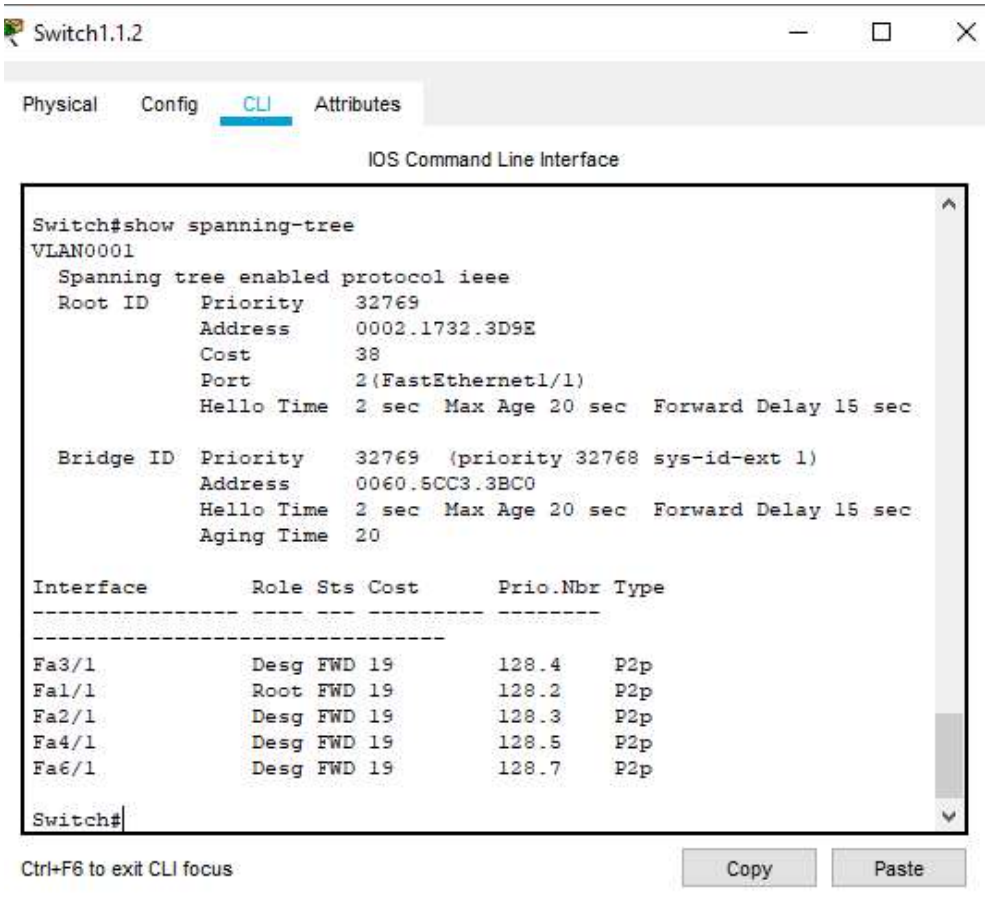


Бачимо, що це не рутовий комутатор. Інтерфейс Fa1/1 є рутовий портом. Fa5/1 чекає в запасі.

Тепер припустимо, що інтерфейс Fa1/1 впав, що буде. Для прикладу вимкнемо його. Заходимо на 1 комутатор.

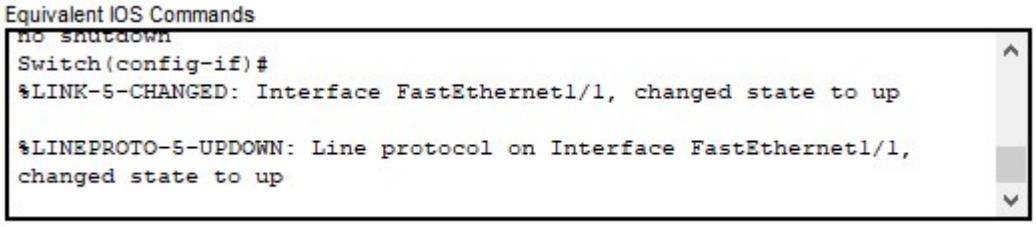


Зайдемо в цей момент на другий комутатор і подивимося стан портів.



Бачимо, що порт Fa1/1 в стані навчання. Тепер в режимі передачі, пройшло близько 20 секунд і лінк піднявся.

Відновимо на першому комутаторі Fa1/1.



Все миттєво відновилося.

Висновки до розділу 4

В даному розділі було розроблено проект телекомунікаційної мережі, використовуючи те обладнання, що було у наявності. Виконані необхідні налаштування вузлів мережі, підключення елементів, створено перевірку роботоздатність рішення. Загалом, мережа була змодельована у програмному забезпеченні Cisco Packet Tracer version 7.3.0.

ВИСНОВКИ

У першій частині дипломного проекту був проведений аналіз об'єкта проектування. Загальна кількість точок доступу до ресурсів телекомунікаційної мережі становить 861 порт. Запланована мережа надаватиме Інтернет-послуги, обмін файлами, телефонний зв’язок та відеоспостереження. Виходячи із загальної кількості користувачів та мережевого трафіку, розраховувався трафік для всієї мережі та для окремих послуг. Загальне навантаження мережі 163,83 Мбіт / с, пропускна здатність Інтернету 50,2646 Мбіт / с, кількість ліній для підключення телефонної мережі до ТМЗК – 36.

У другому розділі дипломного проекту було визначено найважливіші протоколи та технології для реалізації мережі. На початку розділу було обрано топологію мережі, розширено ієрархічну зірку, і мережа використовує первинний рівень, рівень розподілу та рівень доступу. Технології та протоколи побудови мережі відповідають сьоми рівням та моделям OSI. Основним протоколом налаштування мережі є Ethernet. Також у мережі для повнофункціональних протоколів. На основі проектних рішень були розроблені та описані структурні та функціональні схеми.

Третя частина дипломного проекту стосується апаратної реалізації телекомунікаційної мережі. Визначено основні групи пристроїв, на яких буде реалізована мережа - комутатори, маршрутизатори, міні-автоматичні телефонні станції, компоненти системи відеоспостереження, бездротові точки доступу, кабелі, патч-панелі, патч-шнури, роз'єми та телекомунікаційні шафи. В рамках детального аналізу телекомунікаційного ринку України та порівняльного аналізу представлених брендів D-Link було обрано постачальником активних пристроїв та QTECH для пасивних пристроїв. Пасивна складова планової мережі будується відповідно до вимог СКС, тобто. Н. Фізичне середовище є уніфікованим і легко трансформується для передачі голосу та даних.

В заключному розділі було розроблено проект телекомунікаційної мережі, використовуючи те обладнання, що було у наявності. Виконані

необхідні налаштування вузлів мережі, підключення елементів, створено перевірку роботоздатність рішення. Загалом, мережа була змодельована у програмному забезпеченні Cisco Packet Tracer version 7.3.0.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Технические характеристики офисной постройки [Електронний ресурс]. – Режим доступу: http://www.sapphire.kiev.ua/ – Дата доступу: травень 2021. – Назва з титул. екрана.

2. Методичні вказівки до курсового проекту за курсом «Проектування засобів та систем телекомунікаційних мереж» для студентів заочної форми навчання по спеціальності «Телекомунікаційні системи а мережі» / Укл.: доц. Дегтяренко І.В., ас. Ступак Г.В., ас. Прядко Л.О. – Донецьк: ДонНТУ, 2007. – 58 с.

3. Компьютерные сети. Принципы, технологии, протоколы / В.Г Олифер, Н.А Олифер – СПб: Питер, 2000 – 672с.

4. А.Ретана, Д.Слайс, Р.Уайт. Проектирование корпортивных IP-сетей. "Вильямс", 2002. – 368 с.

5. D-Link [Електронний ресурс]. – Режим доступу: https://www.dlink.ee/md/products/6/1380.html – Дата доступу: травень 2021. – Назва з титул. екрана.

6. DHCP сервер на маршрутизаторе cisco [Електронний ресурс]. – Режим доступу: http://ciscotips.ru/dhcp-server – Дата доступу: травень 2021. – Назва з титул. екрана/.

7. Ethernet [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/tech/lan-switching/ethernet/index.html – Дата доступу: травень 2021. – Назва з титул. екрана/.

8. What is WiFi Technology (Wireless Fidelity) 802.11 [Електронний ресурс]. – Режим доступу: https://freewimaxinfo.com/wifi-technology.html – Дата доступу: травень 2021. – Назва з титул. екрана/.

9. Олифер В. Олифер Н., Компьютерные сети. – Санкт-Петербург: Питер, 2003.

10. INTERNET CONTROL MESSAGE PROTOCOL [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc792 – Дата доступу: травень 2021. – Назва з титул. екрана/.

11. Networking on z/OS [Електронний ресурс]. – Режим доступу: https://www.ibm.com/docs/en/zos-basic-skills?topic=layer-address-resolution-protocol-arp – Дата доступу: травень 2021. – Назва з титул. екрана/.

12. User Datagram Protocol (UDP) [Електронний ресурс]. – Режим доступу: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:transporting-packets/a/user-datagram-protocol-udp – Дата доступу: травень 2021. – Назва з титул. екрана/.

13. XML over TCP/IP [Електронний ресурс]. – Режим доступу: https://blog.stephencleary.com/2009/07/xml-over-tcpip.html – Дата доступу: травень 2021. – Назва з титул. екрана/.

14. File Transfer Protocol (FTP) [Електронний ресурс]. – Режим доступу: https://www.hypr.com/file-transfer-protocol-ftp/ – Дата доступу: травень 2021. – Назва з титул. екрана/.

15. What is HTTP? [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/ – Дата доступу: травень 2021. – Назва з титул. екрана/.

16. МЕЖСЕТЕВОЙ ЭКРАН D-LINK DFL-1660 NETDEFEND [Електронний ресурс]. – Режим доступу: https://lanport.ua/ua/shop/product/136 – Дата доступу: травень 2021. – Назва з титул. екрана/.

17. D-Link DGS-1500-20 [Електронний ресурс]. – Режим доступу: https://mcgrp.ru/manual/d-link/dgs-1500-20 – Дата доступу: травень 2021. – Назва з титул. екрана.

18. D-Link [Електронний ресурс]. – Режим доступу: https://www.dlink.ru/ru/products/1366/1597.html – Дата доступу: травень 2021. – Назва з титул. екрана.

19. D-Link [Електронний ресурс]. – Режим доступу: https://dlink.ru/ru/products/1433/1837.html – Дата доступу: травень 2021. – Назва з титул. екрана.

20. D-Link [Електронний ресурс]. – Режим доступу: https://dlink.ru/ru/products/1433/1605.html – Дата доступу: травень 2021. – Назва з титул. екрана.

21. Asterisk [Електронний ресурс]. – Режим доступу: http://asterisk.ru/knowledgebase/Asterisk – Дата доступу: травень 2021. – Назва з титул. екрана.

22. D-Link [Електронний ресурс]. – Режим доступу: https://dlink.ru/ru/products/8/1332.html – Дата доступу: травень 2021. – Назва з титул. екрана.

23. Спеціалізовані системи імітаційного моделювання обчислювальних мереж. Застосування програми Packet Tracer для моделювання комп'ютерної мережі Критерії вибору програми моделювання емуляції комп'ютерних мереж [Електронний ресурс]. – Режим доступу: https://shyza.ru/uk/specializirovannye-sistemy-imitacionnogo-modelirovaniya-vychislitelnyh.html – Дата доступу: травень 2021. – Назва з титул. екрана.

ДОДАТОК А

Охорона праці та пожежна безпека під час монтажних робіт

Розроблений на підставі Законів України «Про охорону праці», «Про пожежну безпеку» та «Про охорону навколишнього середовища, державних будівельних норм України ДБН А.3.2-2-2009 «Охорона праці і промислова безпека в будівництві», комплекс заходів забезпечує в даному проекті безпеку будівельно-монтажних робіт і подальшу експлуатацію обладнання комплексної системи.

До початку виробництва будівельних або монтажних робіт робочі майданчики повинні бути забезпечені питною водою, аптечками, засобами для надання першої медичної допомоги, телефонним зв'язком.

На робочих площах повинні бути організовані пожежні пости з протипожежними засобами.

Робочі майданчики повинні бути оснащені сучасною контрольно-вимірювальною апаратурою.

До робіт з монтажу обладнання та кабельних ліній зв'язку допускаються особи, які досягли 18-річного віку, пройшли медичний огляд, навчені безпечним методам роботи і мають посвідчення про перевірку знань з охорони праці та електробезпеки.

Зазначені особи повинні пройти вступний інструктаж на робочому місці. У бригаді монтажників обов'язково повинне бути присутнім особа, що спостерігає за безпекою виконання робіт. Такою особою бажано призначати старшого по бригаді.

До робіт не допускаються працівники, що знаходяться в стані алкогольного або наркотичного сп'яніння.

Виробництво робіт по монтажу обладнання і кабельних ліній зв'язку виробляти в суворій відповідності з нормативними документами:

- НПАОП 0.00-1.15-07 Правила охорони праці під час Виконання робіт на висоті;

- НПАОП 40.1-1.01-97 (ДНАОП 1.1.10-1.01-97) Правила безпечної ЕКСПЛУАТАЦІЇ електроустановок;
- НПАОП 0.00-1.04-07 Правила Вибори та застосування засобів індивідуального захисту органів дихання;
- НПАОП 40.1-1.32-01 (ДНАОП 0.00-1.32-01) Правила будови електроустановок. Електрообладнання спеціальних установок;
- НПАОП 40.1-1.21-98 (ДНАОП 0.00-1.21-98) Правила безпечної експлуатації електроустановок споживачів;
- ДБН В.1.1-7 Пожежна безпека об`єктів будівництва;
- ГОСТ 12.1.030-81 Електробезпека. Захисне заземлення. Занулення.

Основні рішення з промислової безпеки;

- «ССБП. Охорона праці и промислова безпека в будівництві. Основні положення «з урахуванням місцевих умов. Крім того, при розробці розділу використані нормативні документи:
- ГОСТ 12.1.002-84 «Електричні поля промислової частоти допустимі рівні напруженості і вимоги до проведення контролю на робочих місцях»;
- ГОСТ 12.1.005-88 «Загальні санітарно-гігієнічні вимоги до повітря робочої зони»;
- ДСТУ Б А.3.2-13: 2011 Системи стандартів безпеки праці. Будівництво. Електробезпечність. Загальні вимоги (ГОСТ 12.1.013-78, MOD);
- ГОСТ 12.1.030-81 ССБТ. «Електробезпека. Захисне заземлення. Занулення»;
- ГОСТ 12.2.003-91 ССБТ. «Обладнання протидимне. Загальні вимоги безпеки»;
- ГОСТ 12.2.007.0-75 * ССБТ. «Вироби електротехнічні. Загальні вимоги безпеки»;
- ДСТУ IEC 60745-1: 2010 Інструмент ручний електромеханічний.

Безпека. Частина 1. Загальні вимоги;

- ГОСТ 12.3.032-84 * ССБТ «Роботи електромонтажні. Загальні вимоги безпеки»;
- ГОСТ 12.4.051-87 (СТ РЕВ 5803- 86) ССБТ. «Засоби індивідуального захисту органів слуху»;
- ГОСТ 464-79 «Заземлення для стаціонарних установок проводового зв'язку, радіорелейних станцій, радіотрансляційних вузлів проводового мовлення і антен систем колективного прийому телебачення. Норми опору»;
- ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку»;
- НПАОП 0.00-1.71-13 «Правила охорони праці під час роботи з інструментом та пристроями»;
- НПАОП 40.1-1.21-98 (ДНАОП 0.00-1.21-98) «Правила безпечної експлуатації електроустановок споживачів»;
- НПАОП 64.2-1.07-96 (ДНАОП 5.2.30-1.07-96) «Правила безпеки при роботах на кабельних лініях зв'язку і проводового мовлення»;
- НПАОП 63.12-1.03-96. (ДНАОП 7.1.00-1.03-96) «Правила охорони праці при експлуатації баз, складів і сховищ, виконанні вантажо-розвантажувальних робіт на об'єктах оптової торгівлі».

Існуючі системи опалення та вентиляція повинні відповідати:

ДБН В.2.5-67 «Опалення, вентиляція та кондиціонування» Опалення, вентиляція і кондиціювання ГОСТ 12.1.005-88 «Загальні санітарно-гігієнічні вимоги до повітря робочої зони».

Блискавкозахист будівлі повинна відповідати ДСТУ Б В.2.5-38: 2008 «Інженерне обладнання будинків і споруд. Улаштування будівель і споруд »(IE C 62305: 2006, NEQ).

Влаштування заземлення повинно відповідати ГОСТ 12.1.030-81 «ССБТ. Електробезпечність. Захисне заземлення. Занулення».

Розділ з охорони праці.

Повинні бути передбачені необхідні заходи і засоби для забезпечення безпеки і нормальних санітарних умов праці, як при проведенні монтажних

робіт, так і при експлуатації комплексної системи безпеки відповідно до нормативних документів:

- Закон України «Про охорону праці»;
- ДСТУ 7238: 2011 Системи стандартів безпеки праці. «Засоби колективного захисту працюючих. Загальні вимоги та класифікація»;
- ДСТУ 7239: 2011 Системи стандартів безпеки праці. «Засоби індивідуального захисту. Загальні вимоги та класифікація»;
- НПАОП 40.1-1.21-98 (ДНАОП 0.00-1.21-98) «Правила безпечної експлуатації електроустановок споживачів»;
- НПАОП 63.12-1.03-96. (ДНАОП 7.1.00-1.03-96) «Правила охорони праці при експлуатації баз, складів і сховищ, виконанні вантажо-розвантажувальних робіт на об’єктах оптової торгівлі».
- НПАОП 64.2-1.07-96 (ДНАОП 5.2.30-1.07-96) «Правила безпеки при роботах на кабельних лініях зв’язку і проводового мовлення»;
- НПАОП 64.2-1.08-96 (ДНАОП 5.2.30-1.08-96) «Правила безпеки при роботах на телефонних і телеграфних станціях»;
- НПАОП 0.00-1.71-13 «Правила охорони праці під час роботи з інструментом та пристроями»;
- НПАОП 40.1-1.07-01 (ДНАОП 1.1.10-1.07-01) «Правила експлуатації електрозахисних засобів»;
- ДсанПіН 3.3.2.007-98 «Державні санітарні правила и норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин».

Безпечне обслуговування проектованого обладнання забезпечується системою заходів, передбачених «Правилами улаштування електроустановок» ПУЕ-2009, ПТЕЕС «Правила технічної експлуатації електроустановок споживачів України».

Протипожежні заходи.

Обслуговуючий персонал зобов’язаний дотримуватися встановленого протипожежного режиму на об’єкті, виконувати встановлені правила і інші нормативні акти з питань пожежної безпеки.

Кожен працівник у разі виявлення пожежі або запаху диму, гару, надмірного підвищення температури зобов’язаний негайно повідомити про це в пожежну охорону (при цьому назвати адресу об’єкта, місце виникнення пожежі, наявність людей, а також повідомити своє прізвище) і вжити заходів щодо його ліквідації та рятування людей і майна.

Основні вимоги щодо пожежної безпеки було встановлено відповідно до НАПБ А.01.001-2014 «Правила пожежної безпеки в Україні», НАПБ В.01.053-2016 / 520« Правила пожежної безпеки в галузі зв’язку» і ДБН В.1.1-7 «Захист від пожежі. Пожежна безпека об’єктів будівництва».

Протипожежні системи, установки, устаткування будівель, споруд і приміщень (протидимний захист, пожежна автоматика, протипожежне водопостачання, протипожежні двері, клапани, інші захисні пристрої у протипожежних стінах і перекриттях і т.п.) повинні постійно утримуватися в справному стані.

Евакуація здійснюється по шляхах евакуації через евакуаційні виходи. Евакуаційні шляхи в межах приміщення повинні забезпечувати безпечну евакуацію людей через евакуаційні виходи з даного приміщення. Кількість і загальна ширина евакуаційних виходів з приміщень визначаються в залежності від максимально можливого числа евакуйованих через них людей і гранично допустимого відстані від найбільш віддаленого місця можливого перебування людей (робочого місця) до найближчого евакуаційного виходу.

Протидимний захист будівель повинна виконуватися відповідно з ДБН В.2.5-67. Система оповіщення про пожежу повинна виконуватися відповідно з ДБН В.1.1-7, ДБН 2.5-56-2014 і І 220-008-91.

Для прокладки кабелів зв’язку в приміщеннях слід застосовувати кабелі з негорючим покриттям, рекомендовані фірмами виробниками мережного обладнання.

У приміщеннях, де розташовується телекомунікаційне обладнання, дозволяється зберігати для виробничих потреб не більше 0,15 л бензину, 0,25 л ацетону і 1 л спирту в розрахунку на 100 куб. м об’єму приміщення.

Приміщення, де розташовано телекомунікаційне обладнання, повинні бути обладнані первинними засобами пожежогасіння та протипожежним інвентарем відповідно до встановлених норм згідно НАПБ В.01.053-2016 / 520 «Правила пожежної безпеки в галузі зв’язку». На стіні у вихідний двері приміщення повинен встановлюватися порошковий або вуглекислотний вогнегасник так, щоб відкривається двері не ускладнювала його використання.

ДОДАТОК Б

Структурна схема

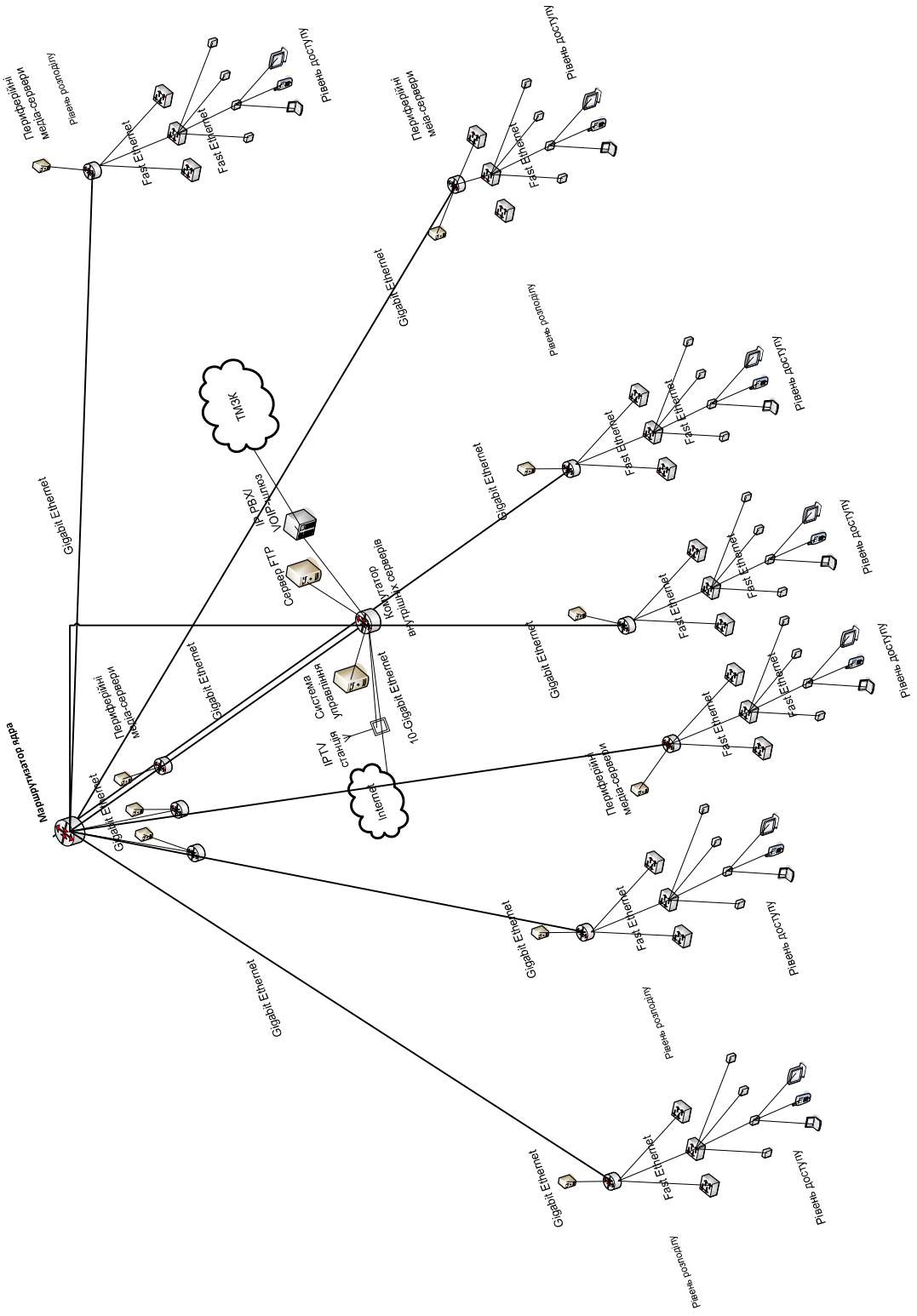


Рисунок Б.1 – Структурна схема мережі

ДОДАТОК В

Функціональна схема

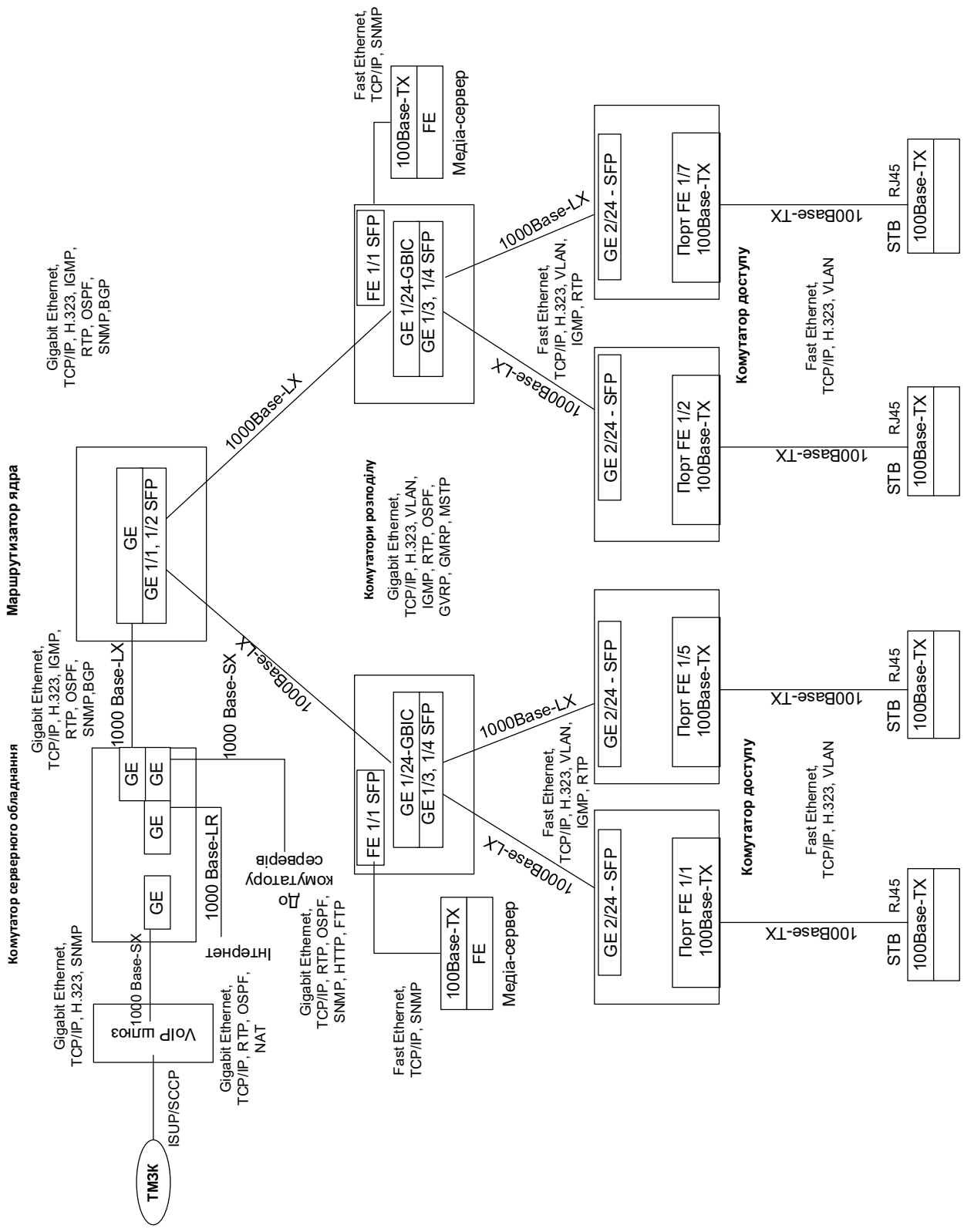


Рисунок В.1 – Функціональна схема мережі