

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет комп'ютерних наук та технологій
(повне найменування інституту, факультету)

Кафедра комп'ютерних систем та мереж
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)

бакалавра
(ступінь вищої освіти (освітній ступінь))

на тему **РОЗРОБКА КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПРИВАТНОГО
ПІДПРИЄМСТВА "ЗАПОРІЖБУД"**

Виконав: студент 4 курсу, групи КНТ-519
спеціальності _____

123 «Комп'ютерна інженерія»
(код і найменування спеціальності)

Освітня програма (спеціалізація) _____
«Комп'ютерна інженерія»

ЛАВРЕНОВ І.О.
(ПРИЗВИЩЕ та ініціали)

Керівник _____
ГРУШКО С.С.
(ПРИЗВИЩЕ та ініціали)

Рецензент _____
ЄФИМЕНКО М.В.
(ПРИЗВИЩЕ та ініціали)

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

Факультет Комп'ютерних наук і технологій
Кафедра «Комп'ютерні системи та мережі»
Ступінь вищої освіти 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.
“17” листопада 2023 року

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

ЛАВРЕНОВА Іллі Олеговича
(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Розробка корпоративної комп'ютерної мережі приватного підприємства "ЗапоріжБуд"

керівник проєкту (роботи) к. т. н., доцент, ГРУШКО Світлана Сергіївна
(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом вищого навчального закладу від “24” березня 2023 року №71

2. Строк подання студентом проєкту (роботи) 10 травня 2023 року

3. Вихідні дані до проєкту (роботи) Комп'ютерна корпоративна приватного підприємства “ЗапоріжБуд” на 156 кінцевих вузлів, 5 віддалених філій

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1) Аналіз потреб та вимог приватного підприємства;

2) Проектування корпоративної комп'ютерної мережі;

3) Впровадження та налагодження корпоративної комп'ютерної мережі.

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

Функціональна схема мережі;

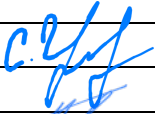
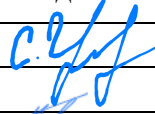
Монтажна схема мережі головного офісу (1 поверх);

Монтажна схема мережі головного офісу (2 поверх);

Монтажна схема мережі магазинів;

Монтажна схема мережі складу підприємства.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-3	ГРУШКО С. С., к.т.н., доцент		
нормоконтроль	ЩЕРБАК Н.В., ст. викл.		

7. Дата видачі завдання 01.03.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз технічного завдання. Вивчення та огляд приватного підприємства ЗапоріжБуд	01.03.2023 р.	
2	Розробка структури системи	05.04.2023 р.	
3	Розробка алгоритму роботи системи	16.04.2023 р.	
4	Реалізація проєкту	28.04.2023 р.	
5	Оформлення отриманих результатів у ПЗ	10.05.2023 р.	
6	Оформлення графічного матеріалу	19.05.2023 р.	
7	Оформлення допоміжного матеріалу	22.05.2023 р.	

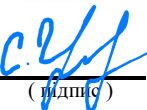
Студент (ка)


(підпис)

Ілля ЛАВРЕНОВ

(Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)


(підпис)

Світлана ГРУШКО

(Ім'я ПРИЗВИЩЕ)

РЕФЕРАТ

ПЗ: 72 с., 38 рис., 20 лістингів , 21 джерело

IP-ТЕЛЕФОНІЯ, VLAN, ВИТА ПАРА, КОМП'ЮТЕР, КОМП'ЮТЕРНА КОРПОРАТИВНА МЕРЕЖА, КОМУТАТОР, МАРШРУТИЗАТОР, НОУТБУК, ОПТИЧНИЙ КАБЕЛЬ, ПЛАНШЕТ, ПОВТОРЮВАЧ, ПРИНТЕР, СЕРВЕР, ТОЧКА ДОСТУПУ, ФАЙРВОЛ.

Об'єкт розробки – корпоративна комп'ютерна мережа приватного підприємства «ЗапоріжБуд».

Метою роботи є корпоративна комп'ютерна мережа приватного підприємства «ЗапоріжБуд», проведення аналізу сучасних мережевих технологій, моделювання та дослідження розроблюваної мережі.

Проект складається з трьох розділів.

Перший розділ присвячено опису підприємства ПП «ЗапоріжБуд». Проводиться, аналіз потреб та вимог вивчення діяльності приватного підприємства.

У другому визначили архітектуру корпоративної мережі, розробка плану її розвернення, а також розкриті питання щодо апаратної частини комп'ютерної мережі на підприємстві.

Третій розділ присвячено моделюванню та налаштуванню корпоративної мережі в емуляторі Cisco Packet Tracer.

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

В результаті виконання дипломної роботи проведено аналіз, моделювання та розробка корпоративної мережі для приватного підприємства

ЗМІСТ

Скорочення та умовні позначки	7
Вступ	8
1 Аналіз потреб та вимог приватного підприємства "запоріжбуд" до корпоративної комп'ютерної мережі	9
1.1 Вивчення діяльності підприємства, його вимог та потреб до інформаційних технологій	9
1.2 Аналіз наявних ресурсів та інфраструктури, що використовується на підприємстві	10
1.3 Корпоративна мережа. Встановлення технічних та функціональних вимог до корпоративної комп'ютерної мережі	15
2 Проектування корпоративної комп'ютерної мережі	26
2.1 Визначення архітектури мережі, включаючи фізичну топологію, протоколи зв'язку, типи мережевого обладнання	27
2.2 Розробка плану розвернення мережі та вибір оптимальних рішень з огляду на потреби підприємства "ЗапоріжБуд"	29
2.3 Встановлення мережевих засобів, налаштування мережевих пристроїв, настройка захисту мережі	33
3 Впровадження та налагодження корпоративної комп'ютерної мережі	49
3.1 Розгортання розробленої мережі на підприємстві "ЗапоріжБуд"	52
3.2 Проведення тестування та налагодження мережі для забезпечення її стабільної та безперебійної роботи	57
3.3 Впровадження заходів з моніторингу, керування та безпеки мережі	63
Висновки	67
Перелік джерел посилання	70
Додаток А	73
Додаток Б	85

Додаток В	91
Додаток Г	98
Додаток Д	100

Графічний матеріал:

Плакат 1 — Функціональна схема мережі

Плакат 2 — Монтажна схема мережі головного офісу (1 поверх)

Плакат 3 — Монтажна схема мережі головного офісу (2 поверх)

Плакат 4 — Монтажна схема мережі магазинів

Плакат 5 — Монтажна схема мережі складу підприємства

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

- IP address — Internet Protocol address, адреса інтернет-протоколу
- DHCP — Dynamic Host Configuration Protocol, протокол динамічної конфігурації хосту
- DNS — Domain Name System, система доменних імен
- HTTP — HyperText Transfer Protocol, протокол передачі гіпертексту
- NTP — Network Time Protocol, протокол мережевого часу
- EMAIL — Electronic mail, електронна пошта
- VOIP — Voice over IP, голос по IP
- LAN — Local Area Network, локальна мережа
- Wi-Fi — Wireless Fidelity, точність бездротового зв'язку
- WPA — Wi-Fi Protected Access, Wi-Fi захищений доступ
- VLAN — Virtual Local Area Network, віртуальна локальна мережа
- WLAN — Wireless Local Area Network, бездротова локальна мережа
- MAN — Metropolitan Area Network, міська обчислювальна мережа
- WAN — Wide Area Network, глобальна мережа
- VPN — Virtual Private Network, віртуальна приватна мережа
- ACL — Access Control List, список контролю доступу
- RIP — Routing Information Protocol, протокол маршрутизації інформації.

ВСТУП

Розробка корпоративної комп'ютерної мережі є актуальною для будь якого підприємства. Це зумовлено тим що між різними філіями та будівлями повинен бути безперервний обмін даними які будуть захищеними від кібератак за допомогою VPN. У цьому дипломному проекті я розглянув корпоративну мережу приватного підприємства “ЗапоріжБуд” – магазину з будівельними матеріалами та меблями.

Корпоративна комп'ютерна мережа ПП “ЗапоріжБуд” призначена для обміну інформацією між філіями, реалізації функцій інтернет-магазину, отримання співробітниками актуальних даних про замовлення, наявність на складі, повідомлень від керівництва.

Основною метою дипломного проекту є розробка корпоративної комп'ютерної мережі для ПП “ЗапоріжБуд” та налаштування пристроїв та зв'язку між ними.

Завданням дипломної роботи є моделювання корпоративної комп'ютерної мережі для ПП “ЗапоріжБуд” з використанням програмних засобів Cisco Packet Tracer.

1. АНАЛІЗ ПОТРЕБ ТА ВИМОГ ПРИВАТНОГО ПІДПРИЄМСТВА "ЗАПОРІЖБУД" ДО КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Об'єктом своєї дипломної роботи я обрав приватне підприємство "ЗапоріжБуд". Основним завданням є розробка корпоративної комп'ютерної мережі. Основними вимогами та потребами є забезпечення безпеки інформації, оптимальної швидкості і пропускної здатності мережі, забезпечення стабільного та безперервного з'єднання між усіма пристроями, легке налаштовування та керування, врахування розширюваності та додавання нових пристроїв.

1.1 Вивчення діяльності підприємства, його вимог та потреб до інформаційних технологій

Підприємство "ЗапоріжБуд", розташоване у м. Запоріжжі, має п'ять філій, а саме три магазини, центральний офіс та склад. Їхня спеціалізація – продаж будівельних матеріалів, електричних приладів, сантехніки та меблів.

Для підприємства магазину продажів будівельних матеріалів, використання інформаційних технологій є дуже важливим, оскільки це дозволяє ефективно управляти бізнесом і задовольняти потреби клієнтів.

Однією з головних вимог до інформаційних технологій є потужна комп'ютерна мережа. Вона дозволяє підприємству забезпечити швидкий доступ до інформації про товари, їх розташування, наявність та ціни. Крім того, комп'ютерна мережа дозволяє підприємству зберігати інформацію про клієнтів, що дозволяє краще розуміти їх потреби та пропонувати більш персоналізований підхід.

Також важливою вимогою є обслуговування мережі. Це потрібно для її довгої та стабільної роботи, тож налаштувати швидкий та віддалений доступ до важливих вузлів мережі, робити постійний моніторинг та діагностику для своєчасного

виявлення проблем та несправностей, часто створювати резервні копії сайту та інших важливих даних для запобігання втрати через поломку та регулярне оновлення програмного забезпечення та обладнання, це дозволяє забезпечити працездатність мережі та уникнути проблем, що виникають з часом внаслідок застарілих програм та компонентів.

Для підприємства також важливо мати можливість працювати з клієнтами в Інтернеті. Це можна зробити за допомогою власного сайту та інтернет-магазину. Такий підхід дозволяє збільшити кількість клієнтів та розширити ринок збуту. Для цього потрібні потужні сервери які будуть безперебійно працювати для цілодобового доступу до сайту.

Крім того, ще однією важливою вимогою є безпека даних. У зв'язку з великою кількістю електронної пошти, онлайн-платежів та транзакцій в Інтернеті, підприємство повинно забезпечувати захист даних своїх клієнтів та бізнес-інформації. Це може бути досягнуто за допомогою використання захищених мереж, шифрування даних та застосування інших методів кібербезпеки.

Отже, інформаційні технології є важливим елементом успішного функціонування підприємства магазину продажу будівельних матеріалів. Забезпечення швидкого доступу до інформації, обслуговування мережі, можливість роботи з клієнтами в Інтернеті та кібербезпека є важливими вимогами та потребами підприємства до інформаційних технологій комп'ютерної мережі.

1.2 Аналіз наявних ресурсів та інфраструктури, що використовується на підприємстві

Для розробки стабільно працюючої мережі ПП “ЗапоріжБуд” потрібно провести аналіз наявних ресурсів та інфраструктури що використовується на вищесказаному підприємстві.

Першочергова задача — проаналізувати комп'ютери та сервери, мережеве обладнання, ір-телефонію та забезпечення безпеки [1].

Вита пара — це пара дротів, які використовуються в кабельному зв'язку для передачі сигналу. У контексті інтернету кручена пара часто використовується для створення локальних мереж (LAN) і підключення комп'ютерів та інших пристроїв до інтернету.

Для передачі даних по цьому виду дротів використовується технологія Ethernet, яка визначає стандарти і протоколи для обміну інформації по локальній мережі. Зазвичай вона складається з восьми дротів, які об'єднуються в чотири пари.

Існує кілька типів витой пари для використання в мережевих додатках, включно з категоріями 5, 5e, 6, 6a і 7. Кожна категорія забезпечує різну швидкість передачі даних і дальність зв'язку, що дає змогу вибрати відповідний тип крученої пари залежно від вимог конкретної мережі [2].

Оптичний кабель — це тип кабелю зв'язку, який використовується для передачі даних на високих швидкостях за допомогою світлових хвиль. Він складається зі скляного або пластикового волокна, яке передає світловий сигнал від одного кінця до іншого.

Оптичний кабель забезпечує більш швидку і надійну передачу даних, ніж традиційні мідні кабелі. Він має велику пропускну здатність, що дає змогу передавати багато даних на дальні відстані без втрати якості сигналу.

Оптичний кабель використовується для передачі сигналів Інтернету, телефонії, телевізійних програм та інших видів комунікації. Він також може бути використаний у медицині та наукових дослідженнях, де потрібна передача даних на великі відстані з високою точністю [2].

Wi-Fi з'єднання — це бездротове з'єднання, яке дає змогу пристроям підключатися до Інтернету або інших мережевих пристроїв через радіохвильові сигнали. Він використовує радіочастоти для передачі даних між пристроями.

Щоб пристрій міг під'єднатися до Wi-Fi мережі, йому необхідно мати відповідний Wi-Fi адаптер, який може приймати та передавати радіохвильові

сигнали. Зазвичай це вбудований адаптер у смартфон, планшет, ноутбук, комп'ютер або окремо придбаний Wi-Fi адаптер для настільних ПК [3].

Комп'ютер — це пристрій, який виконує логічні операції та обробку даних, може використовувати пристрої введення та виведення інформації на дисплей і зазвичай містить центральний процесор (CPU) для виконання завдань.

В магазині буде використовуватись для автоматизації торгівлі. Він може бути під'єднаний до касового апарата і слугувати для оброблення платежів, управління інвентаризацією товарів, управління замовленнями тощо. В офісі буде використовуватись для роботи, а саме як облік продажів, контроль зацікавленості покупців, управління системою безпеки магазину, управління електронною поштою тощо.

Сервер — це високопродуктивний комп'ютер або програма, яка надає ресурси та послуги іншим комп'ютерам або програмам, що називаються клієнтами.

На сервері можуть бути встановлені різні програми, такі як бази даних, вебсервер, поштові сервери та інші, які забезпечують доступ клієнтів до відповідних послуг. В компанії він використовується для зберігання та обробки даних, пов'язаних із вебсайт магазину та інтернет-магазином, а також для забезпечення безпеки та доступності цих даних [4].

IP-телефонія — це технологія передачі голосового зв'язку через інтернет-протокол (IP), що дає змогу здійснювати голосові та відеодзвінки через інтернет, замість традиційної телефонної лінії. Вона використовує цифрові дані для передачі голосу, тексту та відео через мережу Інтернет.

IP-телефонія дуже корисна при використанні, оскільки вона дає змогу поліпшити комунікацію всередині магазину, полегшити роботу співробітників і підвищити якість обслуговування клієнтів [5].

В магазині та в офісі IP-телефонія буде використовуватись для:

- організування системи внутрішнього зв'язку між співробітниками магазину для поліпшення координації роботи і зниження кількості помилок;
- створення автовідповідачу для направлення дзвінків клієнтів на потрібного співробітника магазину для розв'язання їхніх питань або проблем;

- використовувати функцію "кол-центру" для більш ефективного опрацювання дзвінків від клієнтів;
- організувати конференції та наради між відділами магазину або з віддаленими співробітниками і партнерами;
- знизити витрати на телефонні дзвінки за рахунок використання інтернет-зв'язку.

Роутер — це пристрій, який використовується для перенаправлення мережевого трафіку між різними пристроями в мережі. Він отримує дані та використовує інформацію про мережеві адреси, щоб визначити, який шлях потрібно використати для доставки даних до їхнього кінцевого призначення [3].

У корпоративних мережах роутери використовуються для управління і маршрутизації трафіку між локальними мережами та інтернетом, а також для забезпечення безпеки і захисту від зовнішніх загроз. Вони також можуть використовуватися для керування трафіком усередині самої мережі та для поділу на окремі підмережі.

Wi-Fi роутер (або бездротовий маршрутизатор) — це пристрій, який використовується для створення бездротової мережі Wi-Fi в будинку, офісі або іншому місці. Він підключається до дротового інтернет-з'єднання, наприклад кабелю Ethernet, і передає сигнал Wi-Fi, щоб пристрої, підключені до цієї мережі, могли отримувати доступ до інтернету без використання дротів [3].

Wi-Fi роутери зазвичай мають кілька антен для передачі сигналу Wi-Fi, а також порти для підключення дротових пристроїв, як-от комп'ютери або принтери. Вони також можуть мати функції, наприклад захист від злому та контроль доступу, які дають змогу керувати під'єднанням до Wi-Fi мережі та забезпечувати безпеку з'єднання.

В офісах Wi-Fi роутери використовуються для забезпечення доступу до Інтернету та мережевих ресурсів без використання дротових підключень. Це дає змогу співробітникам працювати на своїх пристроях у будь-якому куточку офісу, а також підключатися до Інтернету за допомогою мобільних пристроїв. Wi-Fi

роутери також можуть бути налаштовані для створення гостьових мереж, які будуть використовуватися клієнтами та іншими відвідувачами офісу.

У магазинах Wi-Fi роутери можуть бути використані для надання безкоштовного інтернет-доступу для клієнтів. Це може поліпшити досвід покупців, дозволяючи їм використовувати свої пристрої для пошуку інформації про товари, порівняння цін тощо. Wi-Fi роутери також можуть бути використані для зв'язку різних пристроїв, як касові апарати та сканери штрих-кодів, що може підвищити ефективність роботи магазину.

Wi-Fi точка доступу — це пристрій, який дає змогу під'єднувати бездротові пристрої до мережі Інтернет через бездротове з'єднання Wi-Fi.

Він створює бездротову локальну мережу (Wireless LAN) і може підключатися до дротової мережі Інтернет. Залежно від потужності та конфігурації, Wi-Fi точка доступу може забезпечувати доступ до Інтернету на відстані від кількох метрів до кількох сотень метрів.

Основна відмінність між Wi-Fi роутером і Wi-Fi точкою доступу полягає в тому, що Wi-Fi роутер забезпечує під'єднання до Інтернету і роздає мережевий доступ, а Wi-Fi точка доступу тільки забезпечує бездротове підключення.

Комутатор — це обладнання, який використовується в комп'ютерних мережах для з'єднання безлічі пристроїв в одну мережу. Вони дають змогу передавати дані між ними в мережі, перенаправляючи інформацію тільки туди, де вона потрібні.

Комутатори працюють на канальному рівні моделі OSI, їхня головна функція полягає в передачі кадрів даних між пристроями всередині мережі. Кожен порт є окремим каналом зв'язку, і кадри, що надходять до нього, пересилаються тільки на пристрої-адресати.

Комутатори дають змогу поліпшити продуктивність і безпеку мережі, зменшити навантаження на мережу і знизити кількість помилок передавання даних. Вони широко використовуються в мережах будь-якого масштабу, починаючи від невеликих офісних і домашніх мереж і закінчуючи великими корпоративними та громадськими мережами [4].

Хаб (Hub) — це пристрій, який об'єднує кілька пристроїв в одну локальну мережу. Хаб є простим обладнанням, яке приймає сигнали від кожного під'єданого до нього пристрою і передає їх усім іншим у мережі. Це дає змогу пристроям зв'язуватися один з одним для обміну даними, створюючи таким чином мережеву топологію "зірка" (star topology) [4].

Хаби відрізняються від комутаторів (switch), які також об'єднують кілька пристроїв у мережу, але забезпечують ефективніше використання пропускної спроможності та зменшують колізії в мережі. Однак, хаби досі використовуються в деяких мережах, особливо для під'єднання пристроїв із низькою швидкістю передавання даних.

1.3 Корпоративна мережа. Встановлення технічних та функціональних вимог до корпоративної комп'ютерної мережі

Корпоративна мережа — це комп'ютерна мережа, яка об'єднує комп'ютери та інші пристрої всередині організації або компанії. Метою корпоративної мережі є забезпечення ефективного обміну інформацією між співробітниками, відділами та філіями організації [6].

Зазвичай вона надає співробітникам доступ до загальних ресурсів, таких як файли, бази даних, електронна пошта та інші додатки. Крім того, вона може забезпечувати безпеку та захист даних за допомогою різних технологій, як-от шифрування та брандмауери.

Типи корпоративних мереж:

- локальна мережа (LAN);
- міська обчислювальна мережа (MAN);
- глобальна мережа (WAN);
- віртуальна приватна мережа (VPN);
- бездротова локальна мережа (WLAN) [6].

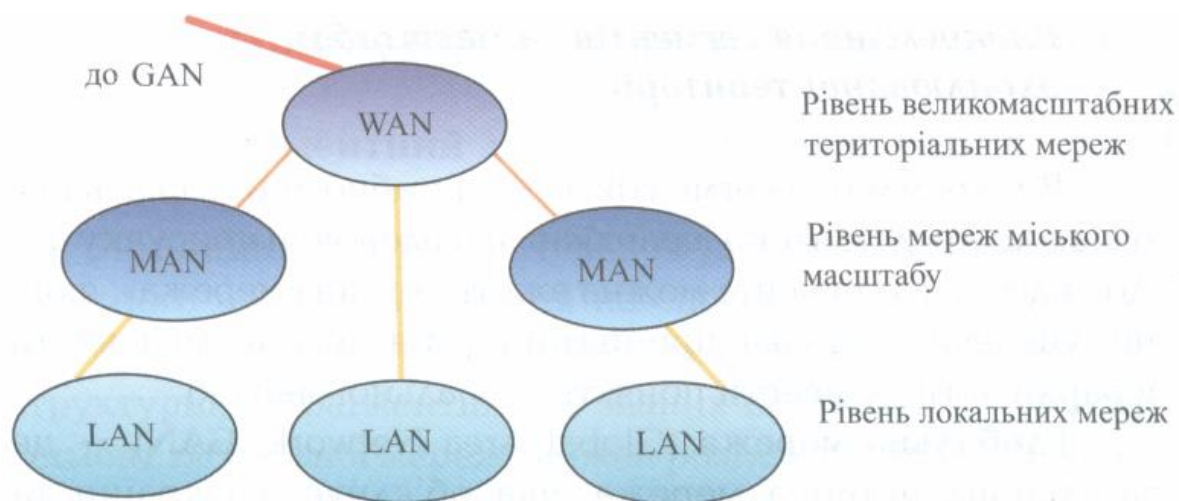


Рисунок 1.1 — Структура корпоративної мережі

Локальна мережа (LAN) — це мережа, яка об'єднує комп'ютери та пристрої в межах невеликої географічної зони, наприклад, офісної будівлі або кампусу. Цей тип мережі зазвичай використовується для спільного використання ресурсів, таких як принтери, файли та доступ до Інтернету.

До складу локальної мережі зазвичай входять комп'ютери, мережеві інтерфейсні карти, кабелі (наприклад Ethernet-кабелі або Wi-Fi), комутатори, маршрутизатори та мережева операційна система (NOS) [7].

Комп'ютери — це пристрої, що використовуються для обробки та зберігання даних, а мережеві карти — це апаратні компоненти, які дозволяють комп'ютерам підключатися до локальної мережі. Кабелі, комутатори та маршрутизатори використовуються для управління потоком даних між пристроями в локальній мережі, тоді як NOS надає такі послуги, як спільний доступ до файлів, друк та мережева безпека.

Для управління та захисту локальної мережі організації зазвичай наймають мережевого адміністратора, який відповідає за конфігурацію та обслуговування мережевої інфраструктури, включаючи маршрутизатори, комутатори, брандмауери та інші мережеві пристрої. Це допомагає забезпечити ефективну та безпечну роботу локальної мережі.

Загальна мета локальної мережі — полегшити комунікацію та обмін даними між пристроями в межах обмеженої території.

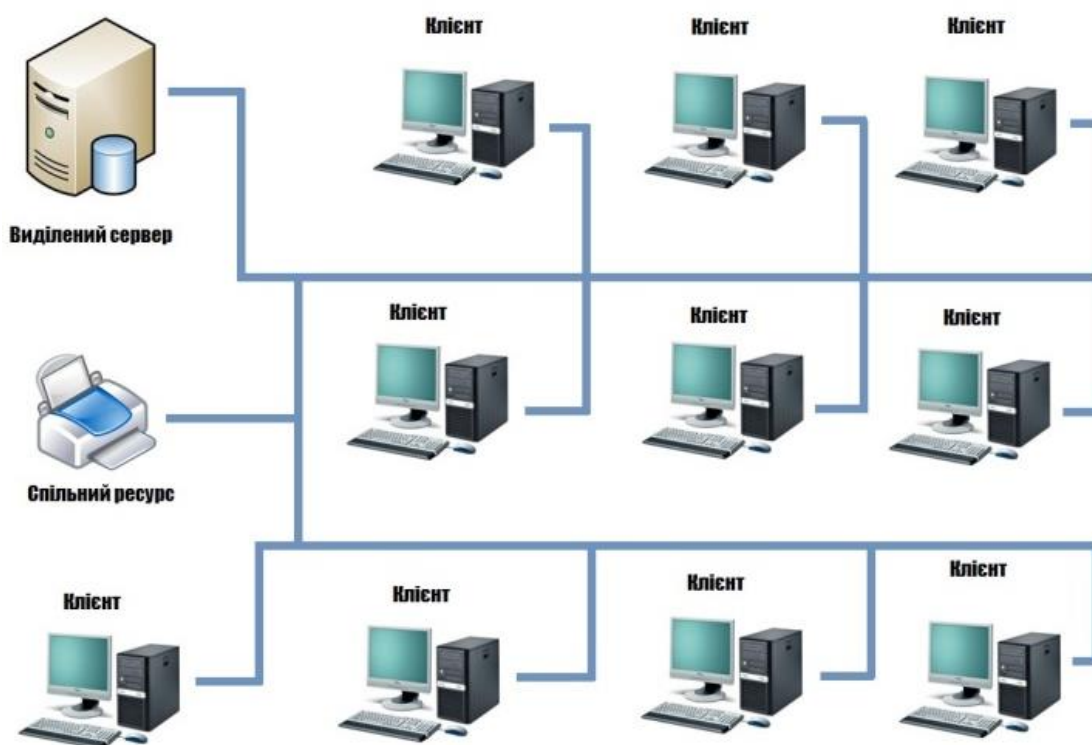


Рисунок 1.2 — Приклад локальної мережі (LAN)

Міська обчислювальна мережа (MAN) — це мережа, яка об'єднує комп'ютери та пристрої в межах мегаполісу, наприклад, міста. Цей тип мережі зазвичай використовується організаціями, які мають кілька офісів або філій, розташованих в одному місті.

MAN зазвичай складається з високошвидкісної магістральної мережі, яка з'єднує різні локальні мережі, такі як офісні будівлі, школи або лікарні, в межах мегаполісу. Магістральна мережа може використовувати різні технології, такі як оптоволокно або супутниковий зв'язок.

Крім магістральної мережі, до складу міської територіальної мережі входять різні мережеві пристрої, такі як маршрутизатори, комутатори та концентратори, які використовуються для з'єднання локальних мереж з магістральною мережею. Ці пристрої відповідають за спрямування трафіку між різними локальними мережами і гарантують, що пакети даних будуть доставлені за призначенням.

Організації та підприємства часто використовують комутатори для з'єднання своїх географічно розподілених офісів або об'єктів у межах міста чи регіону. Це

дозволяє їм спільно використовувати ресурси, такі як дані та додатки, а також більш ефективно спілкуватися [8].

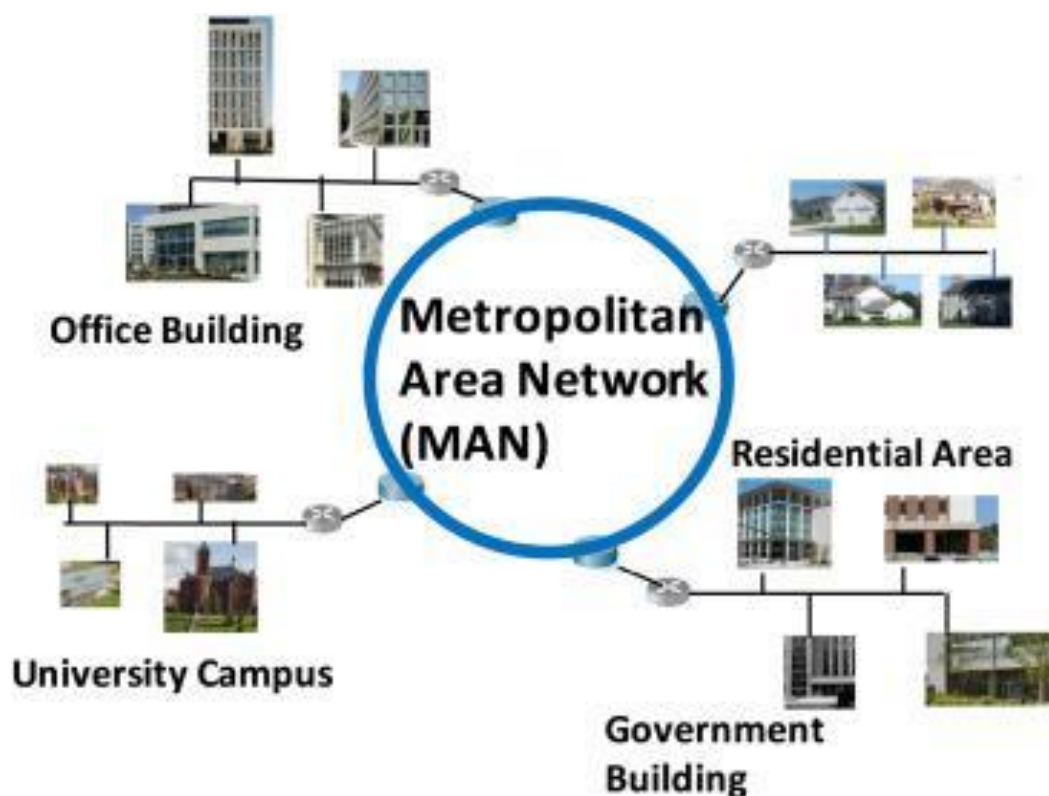


Рисунок 1.3 — Приклад міської обчислювальної мережі

Глобальна мережа (WAN) - це тип комп'ютерної мережі, яка охоплює велику географічну територію, як правило, міста або навіть країни. Глобальні мережі використовуються для з'єднання комп'ютерів, серверів та інших пристроїв на великих відстанях, що дозволяє їм спілкуватися один з одним і спільно використовувати ресурси [9].

Основна різниця між MAN і WAN полягає в їх масштабі та географічному розподілі. MAN обмежується територією міста або місцевості з відносно невеликою площею, тоді як WAN охоплює великі географічні області, такі як країни або континенти.

MAN може бути побудована за допомогою технологій, таких як оптоволоконні лінії зв'язку, бездротові мережі або кабельні мережі. Вона

забезпечує швидкий доступ до ресурсів мережі для користувачів відносно невеликої території.

WAN зазвичай використовується для підключення віддалених географічних локацій до мережі, що забезпечує широкий діапазон послуг, включаючи доступ до Інтернету, відеоконференції та обмін даними між віддаленими офісами. WAN може бути побудована за допомогою технологій, таких як супутникова мережа, оптоволоконні мережі, кабельна мережа, DSL та бездротові мережі.

Загалом, глобальні мережі є важливим засобом з'єднання віддалених місць і дозволяють користувачам отримувати доступ до ресурсів і спілкуватися один з одним на великих відстанях.

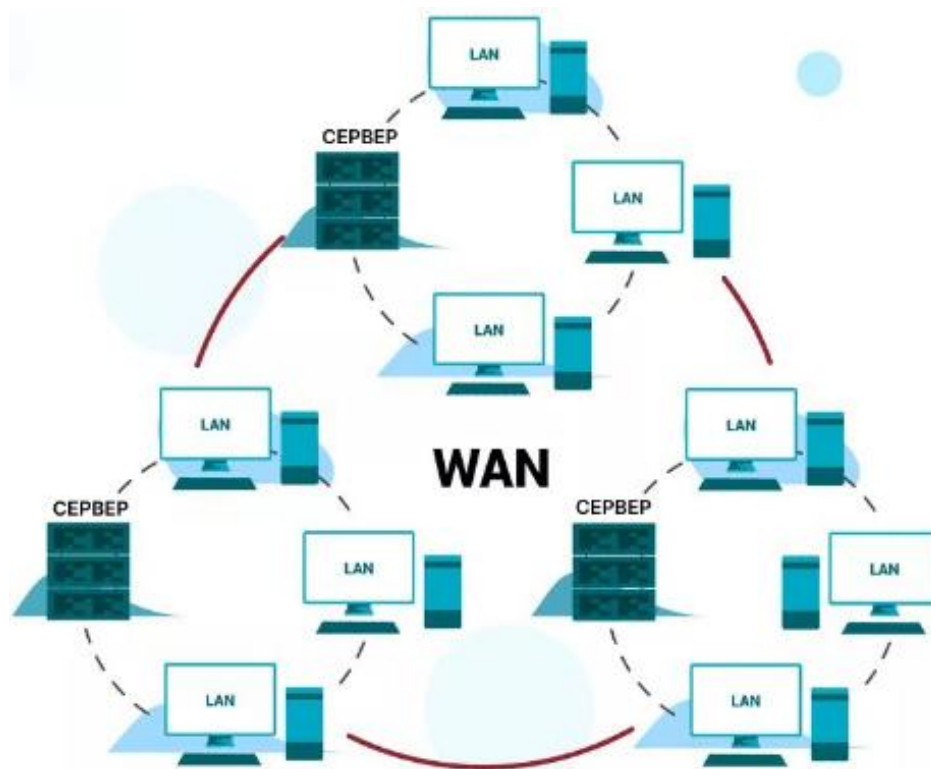


Рисунок 1.4 — Приклад глобальної мережі (WAN)

Віртуальна приватна мережа (VPN) — це мережа, яка дозволяє користувачам підключатися до приватної мережі через публічну мережу, таку як Інтернет. Цей тип з'єднання часто використовується віддаленими працівниками для доступу до ресурсів корпоративної мережі з-за меж офісу [10].

Зазвичай VPN складається з трьох основних компонентів:

VPN-клієнт: Це програмне забезпечення, яке працює на пристрої користувача, наприклад, комп'ютері, планшеті або смартфоні, і підключається до VPN-сервера. Клієнт встановлює безпечне, зашифроване з'єднання з сервером і дозволяє користувачеві отримати доступ до ресурсів у мережі VPN.

VPN-сервер: Це мережева інфраструктура, яка отримує та обробляє VPN-з'єднання від клієнтів. Сервер відповідає за створення і підтримку VPN-тунелю, який є безпечним, зашифрованим з'єднанням між клієнтом і сервером.

Протокол VPN: Це набір правил і стандартів, які регулюють передачу даних через VPN-тунель. Існує кілька протоколів VPN, включаючи OpenVPN, IPSec і PPTP. Кожен протокол має свої переваги та недоліки з точки зору безпеки, швидкості та сумісності з різними пристроями та мережами.

Загалом, VPN забезпечує безпечне і приватне з'єднання шляхом шифрування даних і маршрутизації їх через VPN-тунель. Це ускладнює перехоплення або шпигунство за діями користувача в Інтернеті і дозволяє йому отримувати доступ до ресурсів у мережі VPN так, ніби він фізично підключений до неї.

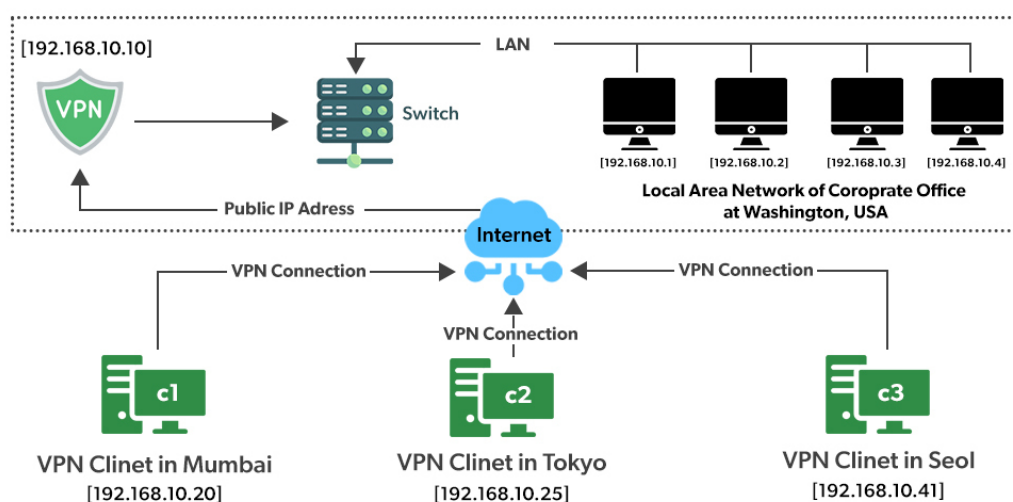


Рисунок 1.5 — Приклад віртуальної приватної мережі (VPN)

Бездротова локальна мережа (WLAN) — це локальна мережа, яка використовує бездротову мережеву технологію, наприклад, Wi-Fi, для

підключення пристроїв. Цей тип мереж часто використовується в таких місцях, як кав'ярні, аеропорти та готелі, для надання доступу до Інтернету клієнтам.

Вона зазвичай складається з бездротової точки доступу (ТД) або маршрутизатора, бездротових клієнтів, таких як ноутбуки, смартфони або планшети, і необхідної мережевої інфраструктури для підключення маршрутизатора до інтернету або інших мереж [11].

Бездротова точка доступу або маршрутизатор діє як центральний вузол мережі, дозволяючи бездротовим клієнтам підключатися до нього і спілкуватися один з одним або з пристроями в інших мережах.

Мережева інфраструктура може включати кабелі Ethernet, комутатори та модеми для забезпечення підключення до Інтернету в бездротовій локальній мережі.

WLAN може також включати додаткові компоненти, такі як мережевий брандмауер або система безпеки для захисту від несанкціонованого доступу.

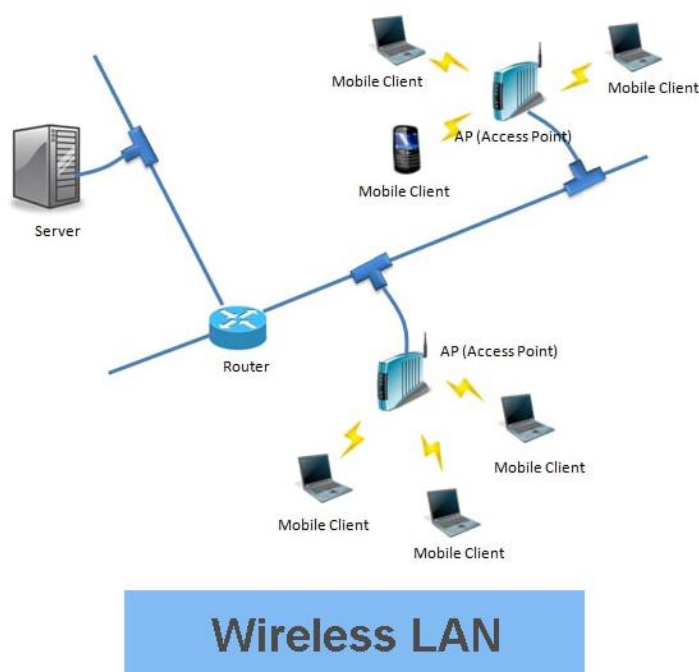


Рисунок 1.6 — Приклад бездротової локальної мережі (WLAN)

При проектуванні корпоративної комп'ютерної мережі важливо враховувати як технічні, так і функціональні вимоги. Ось деякі з ключових вимог, які слід взяти до уваги. Технічні вимоги:

Масштабованість: мережа повинна бути здатна впоратися зі зростанням кількості користувачів, пристроїв і трафіку даних без шкоди для продуктивності. Для цього потрібно використовувати пристрої та технології, які передбачатимуть удосконалення в майбутньому. Наприклад, технологія маршрутизації OSPF (Open Shortest Path First). Це протокол маршрутизації, який дає змогу налаштовувати маршрути в мережі на основі вартості та швидкості з'єднання. Він добре масштабується і може підтримувати мережі з великою кількістю вузлів.

Надійність: мережа повинна бути доступною і функціонувати в будь-який час, з мінімальним часом простою і збоями. Щоб уникнути виходу з ладу важливого обладнання, потрібно використовувати стабілізатори напруги. Вони захищають обладнання від стрибків напруги, які можуть пошкодити його електронні компоненти. Або можна використовувати ДБЖ (джерело безперебійного живлення). Його використання забезпечує резервне живлення в разі вимкнення основного електроживлення та дає змогу обладнанню працювати далі, захищає обладнання від стрибків напруги, перенапруг та інших проблем з електрикою. Так само обов'язково проводити регулярну перевірку електрообладнання. Регулярна перевірка та обслуговування допомагає виявляти й усувати проблеми з електрикою до того, як вони зашкодять обладнанню.

Безпека: мережа повинна бути захищена від несанкціонованого доступу, шкідливих програм та інших кіберзагроз. Це включає в себе впровадження брандмауерів, антивірусного програмного забезпечення та інших заходів безпеки.

Для безпеки з'єднання між філіями потрібно використовувати Virtual Private Network (VPN). VPN розшифровується як віртуальна приватна мережа. Ця технологія дозволяє створити безпечне з'єднання між комп'ютером або пристроєм та інтернетом. З'єднання захищене шляхом шифрування даних, що передаються через Інтернет, допомагає захистити вашу конфіденційність і безпеку.

VPN буває таких типів:

- VPN з віддаленим доступом — цей тип VPN дозволяє окремим користувачам безпечно підключатися до мережі компанії через Інтернет. VPN з віддаленим доступом зазвичай використовують співробітники, які працюють з дому або в дорозі;

- міжмережевий VPN — цей тип VPN створює безпечне з'єднання між двома або більше мережами, наприклад, з'єднує філію зі штаб-квартирою компанії. VPN-мережі типу "сайт-сайт" зазвичай використовуються компаніями з декількома офісами;

- SSL/TLS VPN — цей тип VPN використовує протокол SSL або TLS для створення безпечного з'єднання між пристроєм користувача та веб-програмою або веб-сайтом. SSL/TLS VPN зазвичай використовуються для віддаленого доступу до веб-додатків;

- IPsec VPN — цей тип VPN використовує протокол Internet Protocol Security (IPsec) для шифрування даних, що передаються між пристроєм користувача і VPN-сервером. IPsec VPN зазвичай використовується для з'єднань між сайтами та віддаленого доступу;

- PPTP VPN — цей тип VPN використовує протокол тунелювання "точка-точка" (PPTP) для створення безпечного з'єднання між пристроєм користувача і VPN-сервером. PPTP VPN легко налаштовуються і зазвичай використовуються для віддаленого доступу;

- L2TP VPN — цей тип VPN використовує протокол тунелювання другого рівня (L2TP) для створення безпечного з'єднання між пристроєм користувача і VPN-сервером. L2TP VPN зазвичай використовується для віддаленого доступу та з'єднань між сайтами [10].

Пропускна здатність: мережа повинна мати достатню пропускну здатність, щоб підтримувати передачу великих обсягів даних, таких як мультимедійні файли та оновлення програмного забезпечення.

Щоб підтримати велику пропускну здатність потрібно використовувати сучасні технології. Для цього по кабельному зв'язку між пристроями це можна

зробити за допомогою оптичного кабелю, який підтримує швидкість з'єднання до 2.5 Гбіт/с. Оптичний кабель являє собою тонкий, гнучкий і міцний дріт, який використовується для передачі світлових сигналів. Він складається з трьох основних елементів: серцевини, оболонки і захисного обплетення. Для повноцінної роботи потрібен пристрій, який підтримуватиме цей кабель.

Якщо потрібна висока швидкість зв'язку, але без дротів, можна використовувати Wi-Fi з'єднання на частоті 6 ГГц сьомого покоління. Wi-Fi 7 (IEEE 802.11be) є новим поколінням Wi-Fi, яке пропонує значні поліпшення порівняно з попередніми стандартами, такими як Wi-Fi 6 і Wi-Fi 6E. Основні особливості Wi-Fi 7 включають збільшення пропускної здатності до 30 Гбіт/с, меншу затримку, підтримку каналів шириною 320 МГц і 16 просторових потоків за допомогою MU-MIMO 16x16. Це дасть змогу пристроям одночасно працювати в діапазонах 5 ГГц і 6 ГГц.

Сумісність: мережа повинна бути сумісною з широким спектром пристроїв та операційних систем, як сучасних, так і майбутніх.

Для сумісності потрібно враховувати, щоб усі технології, кабелі та програмне забезпечення були сумісні з усіма пристроями, які будуть використовуватися в мережі. Для цього потрібно проаналізувати кожен пристрій і перевірити їхні характеристики [12].

Функціональні вимоги:

Простота використання: мережа повинна бути простою у використанні та навігації для всіх користувачів, незалежно від їхніх технічних навичок.

Контроль доступу: мережа повинна мати відповідні засоби контролю доступу, щоб гарантувати, що користувачі мають доступ лише до тих даних і ресурсів, які їм потрібні.

Для цього можна використовувати ACL — це список правил, який визначає, які користувачі або групи користувачів мають доступ до певних ресурсів або операцій у комп'ютерній системі або мережі.

ACL може бути налаштований на рівні операційної системи, додатків, баз даних або мережевого обладнання, такого як маршрутизатори або комутатори. Він

визначає, які користувачі мають доступ до файлів, папок, розшарених ресурсів, баз даних, портів і протоколів мережі.

Резервне копіювання та відновлення даних: мережа повинна мати надійну систему резервного копіювання та відновлення, щоб запобігти втраті даних у разі збою системи або кібератаки.

Моніторинг мережі: мережа повинна контролюватися для виявлення та усунення будь-яких проблем або вразливостей в режимі реального часу.

Управління мережею: мережа повинна мати централізовану систему управління, яка дозволяє легко конфігурувати, моніторити та обслуговувати мережеві ресурси.

Для налаштування віддаленого доступу потрібно:

- налаштування мережі: переконатися, що мережа конфігуровано правильно і доступна з інтернету. Для цього необхідно налаштувати правила маршрутизації, фаїрвол, щоб дозволити віддалений доступ і сконфігурувати NAT (Network Address Translation);

- налаштування пристрою: для дозволу віддаленого доступу до пристрою, необхідно налаштувати відповідний сервіс, наприклад, SSH, Telnet або RDP. Для цього необхідно встановити логін і пароль, сконфігурувати права доступу та визначити порт, на якому буде доступний сервіс;

- безпека: віддалений доступ має бути безпечним, щоб запобігти несанкціонованому доступу. Для цього необхідно використовувати сильні паролі, налаштувати правила брандмауера і додати VPN (Virtual Private Network), якщо це можливо;

- тестування: перед тим, як надавати віддалений доступ, необхідно протестувати його, щоб переконатися, що все працює коректно. Необхідно перевірити, що можна підключитися до пристрою віддалено, що сервіс працює без помилок і безпека не порушена;

- моніторинг: після налаштування віддаленого доступу необхідно налаштувати моніторинг, щоб контролювати доступ і виявляти можливі загрози безпеці. Важливо пам'ятати, що віддалений доступ до пристроїв має бути наданий

тільки авторизованим користувачам і має бути захищений паролем та іншими методами безпеки, щоб запобігти несанкціонованому доступу;

– мережева документація: мережа повинна мати вичерпну документацію, яка включає інформацію про топологію мережі, пристрої та конфігурації для полегшення пошуку та усунення несправностей [12].

2 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Проектування корпоративної мережі — це процес розроблення та створення інфраструктури мережі, яка забезпечує зв'язок між комп'ютерами та іншими пристроями в межах підприємства або організації. Головна мета проектування корпоративної мережі - забезпечити високу продуктивність, надійність, безпеку та масштабованість мережі, а також забезпечити доступ до ресурсів і додатків для всіх пристроїв, підключених до мережі.

Першим кроком у проектуванні корпоративної комп'ютерної мережі є оцінка потреб організації. Це передбачає аналіз розміру організації, кількості співробітників, а також типів даних і додатків, які будуть передаватися через мережу. Після того, як ці фактори визначені, мережа може бути спроектована відповідно до конкретних потреб організації.

Далі необхідно вибрати архітектуру мережі. Це включає в себе рішення про використання локальної мережі (LAN), глобальної мережі (WAN) або їх комбінації. Також необхідно вибрати топологію мережі, яка може містити зіркоподібну, кільцеву або комірчасту конфігурацію.

Після вибору архітектури та топології можна вибирати компоненти мережі. Це включає вибір відповідного обладнання, такого як маршрутизатори, комутатори та сервери, а також відповідного програмного забезпечення, такого як операційні системи, програмне забезпечення для забезпечення безпеки та програми для підвищення продуктивності.

Безпека є вирішальним фактором при побудові корпоративної мережі. Мережа повинна бути спроектована таким чином, щоб захищати від несанкціонованого доступу, крадіжки даних та інших загроз безпеці. Це може включати впровадження брандмауерів, систем виявлення вторгнень та технологій шифрування.

Нарешті, мережа повинна підтримуватися і модернізуватися в міру необхідності, щоб гарантувати, що вона продовжує відповідати потребам організації. Це включає регулярний моніторинг і тестування для виявлення і розв'язання будь-яких проблем, які можуть виникнути, а також оновлення апаратного і програмного забезпечення, щоб йти в ногу з мінливими технологіями та потребами бізнесу [13].

2.1 Визначення архітектури мережі, включаючи фізичну топологію, протоколи зв'язку, типи мережевого обладнання

Для початку роботи приватного підприємства "ЗапоріжБуд" потрібно організувати підключення та налаштування для 5 філій, а саме для 3 магазинів, складу товарів і центрального офісу розташованих у місті Запоріжжя. Важливо враховувати, що кожна з філій має свої особливості та вимоги до налаштування і підключення, які необхідно враховувати в процесі роботи.

На філіях буде використовуватися архітектура локальної мережі (LAN). Це комп'ютерна мережа, що об'єднує пристрої в межах невеликої географічної області, яка зрештою буде об'єднуватися з декількома локальними мережами в міську обчислювальну мережу (MAN).

Загалом, використання локальних і міських мереж у межах інфраструктури компанії дасть змогу забезпечити швидкий і безпечний обмін даними між співробітниками та підвищити ефективність роботи всієї організації.

У мережі буде використано загальну кількість 156 пристроїв, включно з 74 комп'ютерами, 45 IP-телефонами для зв'язку між робітниками, 6 серверами, а саме DNS-Server для переведення доменних імен в IP-адреси, 2 штуки HTTP-Server для опрацювання запитів і відправлення відповіді в інтернеті, DHCP-Server для автоматичного видавання ір-адрес різним пристроям, NTP-Server для синхронізації часу на комп'ютерах і мережевих пристроях та EMAIL-Server для надсилання та отримання електронної пошти, 6 точками доступу для підключення безпроводних користувачів, 6 роутерами для зв'язку між філіями, 6 комутаторами для під'єднання різноманітних приладів та фаєрволом для захисту мережі від зовнішніх загроз. Ці пристрої будуть підключені дротовим способом до мережі за допомогою витой пари та оптичного кабелю. Крім того, буде використано 5 репітерів, які будуть використовувати для переходу з оптичного кабелю на виту пару, для сумісності обладнання. Також у мережі буде 15 ноутбуків і 15 планшетів, які будуть підключені бездротовою мережею з використанням частоти 5 ГГц. Усі ці пристрої працюватимуть у топології мережі зірка (рисунок 2.1), де кожен пристрій буде з'єднаний із центральним роутером.

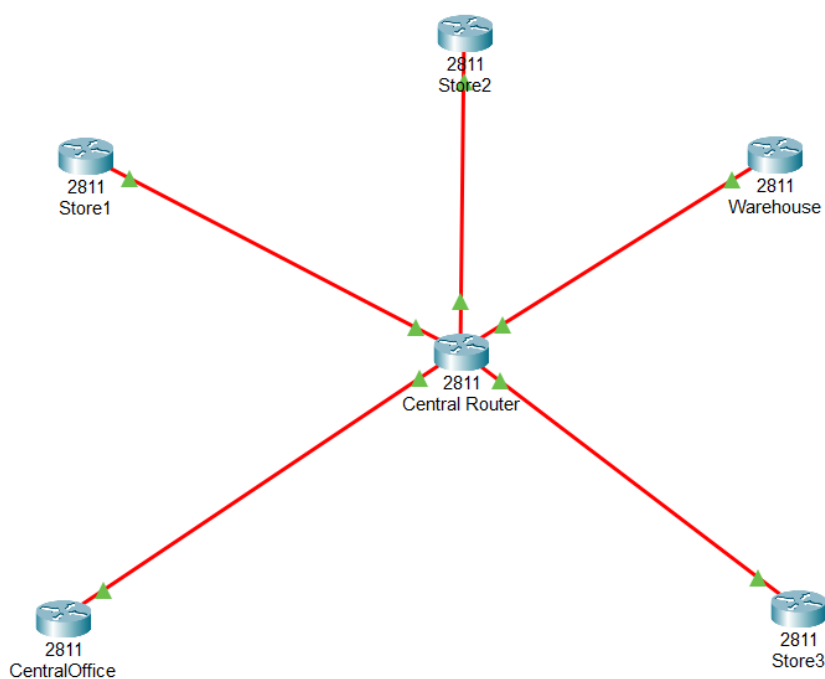


Рисунок 2.1 — Використовувана на підприємстві топологія мережі зірка

Центральний пристрій відіграє роль точки доступу і координує обмін даними між пристроями в мережі. Якщо один із пристроїв передає дані, то вони передаються через центральний пристрій і доставляються тільки адресату.

Топологія зірка є однією з найпоширеніших топологій для локальних мереж (LAN) в офісах. Вона має такі переваги:

- простота встановлення та підключення нових пристроїв до мережі;
- стійкість мережі. якщо один пристрій виходить з ладу, інші продовжать працювати;
- централізоване управління мережею.

Однак, топологія зірка має і деякі недоліки:

- якщо центральний пристрій виходить з ладу, то вся мережа стає недоступною;
- вартість встановлення мережі може бути високою через необхідність використання додаткових кабелів.

2.2 Розробка плану розвернення мережі та вибір оптимальних рішень з огляду на потреби підприємства "ЗапоріжБуд"

Розробка плану розгортання мережі та вибір оптимальних рішень для підприємства вимагає комплексного підходу, який враховує потреби бізнесу, існуючу інфраструктуру, бюджет і плани зростання в майбутньому.

Спочатку необхідно підключити та налаштувати роутер. Для цього було обрано модель Cisco 2811, оскільки вона підтримує роботу з IP-телефонією. До маршрутизатора було встановлене 3 модуля "HWIC-1GE-SFP", які дозволяють використовувати оптичний кабель зі швидкістю 1 Гігабіт для зв'язку з іншими пристроями. Декілька основних характеристики цього роутера:

- частота процесора: 260 МГц;
- об'єм оперативної пам'яті: 256 МБ (може бути розширена до 760 МБ);

- вбудована пам'ять: 64 МБ Flash-пам'яті (може бути розширена);
- 2 порти Ethernet 10/100BASE-TX (RJ-45);
- 1 порт консолі (RJ-45);
- слоти для встановлення розширювальних модулів;
- підтримка протоколів голосового зв'язку VoIP (Voice over IP), включно з H.323, SIP, MGCP, SCCP;
- можливість роботи з IP-телефонами та іншими голосовими пристроями;
- модульна архітектура дає змогу додавати додаткові модулі для розширення функціональності маршрутизатора;
- можливість встановлення модулів розширення пам'яті, модулів із додатковими інтерфейсами [14].

Наступним кроком розгортання корпоративної мережі в центральному офісі є підключення комутаторів. Оскільки офіс двоповерховий, то для оптимізації роботи було прийнято рішення встановити на кожному поверсі по окремому світчу. Була обрана модель Cisco Catalyst 3560-24PORT як оптимальне рішення, оскільки вона має можливість під'єднання оптичних кабелів і оснащена портами, здатними забезпечувати пропускну здатність в 1 гігабіт. Під'єднання оптичних кабелів забезпечує надійну та стабільну передачу даних на великі відстані без втрат якості сигналу. Порти з пропускну здатністю в 1 гігабіт дають змогу обробляти великий обсяг даних, забезпечуючи швидке й ефективне передавання інформації між пристроями в мережі. Декілька основних характеристик цього комутатора:

- кількість портів: 24 порти;
- швидкість передачі даних: 10/100/1000 Мбіт/с;
- пропускну здатність: 8.8 Gbps;
- підтримка VLAN та IPv6;
- підтримка стандартів безпеки: 802.1X, DHCP Snooping, IP Source Guard, Dynamic ARP Inspection;
- підтримка протоколів маршрутизації: статична маршрутизація, RIP, OSPF;
- управління: CLI (Command Line Interface), SNMP (Simple Network Management Protocol), Cisco Network Assistant;

- підтримка керування через веб-інтерфейс;
- підтримка управління через командний рядок [15].

Оскільки в корпоративній мережі використовується бездротове підключення, наступним кроком буде підключення точки доступу до комутатора. Вона буде використовуватися для підключення на частоті 5 ГГц.

Підключення на частоті 5 ГГц забезпечує більшу пропускну здатність. Вона забезпечує ширший канал і вищу пропускну здатність даних порівняно з 2,4 ГГц. Це дає змогу передавати більший об'єм даних і забезпечує більш стабільне та швидке під'єднання до мережі. Так само вона забезпечує кращу продуктивність у щільних середовищах. Коли в одній області знаходиться безліч бездротових мереж, наявність більшої кількості доступних каналів у 5 ГГц Wi-Fi дає змогу знизити перевантаженість мережі та забезпечити кращу продуктивність у щільних середовищах.

Оскільки в Cisco Packet Tracer точка доступу не має моделі, за основу було взято Cisco Aironet 2700 Series. Кілька основних характеристик:

- підтримка стандартів 802.11a/b/g/n/ac, що забезпечує сумісність із широким спектром пристроїв;
- порт Ethernet 1000BASE-FX (1 Гбіт/сек);
- підтримка швидкості до 1,3 Гбіт/сек у радіусі дії 5 ГГц і до 450 Мбіт/сек у радіусі дії 2,4 ГГц. Це дає змогу досягти високої пропускну здатності та забезпечити надійне бездротове з'єднання;
- має підтримку різних протоколів безпеки, включно з WPA2, автентифікацією 802.1X і VPN-підключенням. Дозволяє управлятися за допомогою програмного забезпечення Cisco Prime Infrastructure або Cisco Mobility Services Engine [16].

Наступним кроком буде підключення серверів HTTP-Server, DHCP-Server, DNS-Server, NTP-Server та EMAIL-Server до комутатора, розташованого на першому поверсі, оскільки всі сервери також знаходяться на цьому поверсі. Кожен сервер містить порт Ethernet 1000BASE-FX (1 Гбіт/сек) для високої пропускну здатності, швидкого обміну даними.

Після підключення серверів, потрібно під'єднати всі комп'ютери та принтери до комутаторів на кожному поверсі. Декілька із них буде підключено бездротовим способом до точки доступу 5 ГГц, для цього на пристроях був встановлений модуль “PT-HOST-NM-1W-AC”.

І останній пристрій, що залишилося під'єднати до комутатора це IP-телефон. Для нашої мережі ми будемо використовувати модель Cisco IP-Phone 7960. Декілька основних характеристик IP-телефона:

- Cisco IP-Phone 7960 оснащений монохромним РК-дисплеєм з роздільною здатністю 320 x 222 пікселі. Дисплей дає змогу відображати інформацію про виклики, номери та інші функції;

- телефон має 6 програмованих кнопок, які можна налаштувати для швидкого доступу до різних функцій, включно з дзвінками, гучністю та функціями повідомлень;

- IP-телефон Cisco 7960 забезпечує якісний голосовий звук з використанням технології широкосмугового аудіо (wideband audio). Телефон підтримує кодеки G.711, G.729a і G.729ab для передачі голосу;

- пристрій підтримує підключення через Ethernet за допомогою порту 10/100BASE-TX. Він також має вбудований комутатор Ethernet, який дозволяє підключати інші пристрої до мережі через IP-телефон;

- Cisco IP-Phone 7960 підтримує такі функції, як багатоканальний динамічний сегментний дисплей, виклики на утриманні, конференц-зв'язок, автоматичний набір номера, гучний зв'язок тощо [17].

Проте при розробці системи варто враховувати що в магазині та на складі використовується одна схема мережі, але різні комутатори Cisco Catalyst 2960-24Port та окремий перехідник з оптичного кабелю на виту пару для підключення до свіча. Комутатор має 2 гігабітних порта до якого підключений роутер в режимі “Trunk” та точка доступу, для високої пропускної здібності та швидкого обміну інформації. Кілька головних характеристик даного комутатора:

- кількість портів: 24;

- тип портів: Ethernet;

- швидкість передачі даних: 22 порти 100 Мбіт/с та 2 порти 1000 Мбіт/с;
- підтримка стандарту Ethernet: IEEE 802.3;
- підтримка VLAN (Virtual LAN);
- підтримка QoS (Quality of Service);
- підтримка SNMP (Simple Network Management Protocol);
- підтримка управління через командний рядок [18].

2.3 Встановлення мережевих засобів, налаштування мережевих пристроїв, настройка захисту мережі

Важливими етапами створення стабільно працюючої мережі є встановлення мережевих засобів, налаштування мережевих пристроїв, настройка захисту мережі.

Встановлення мережевих засобів — це процес під'єднання та налаштування мережевого обладнання та програмного забезпечення для створення функціональної комп'ютерної мережі.

Перший і основний пристрій який потрібно налаштувати це — роутер. Він є головним пристроєм у локальній мережі, тому що він з'єднує кілька пристроїв в одну мережу, даючи їм змогу обмінюватися даними між собою, виконує функцію переведення мережевих адрес (Network Address Translation, NAT, забезпечує безпеку локальної мережі.

Перед початком налаштувань потрібно через комп'ютер під'єднатися до роутера, увійти у консоль. Перед початком налаштувань потрібно додати роутеру за допомогою команди `hostname` назву. Команда `enable secret` використовується для встановлення пароля, який забезпечує доступ до привілейованого режиму на пристрої. Цей пароль зазвичай є більш безпечним, оскільки він зберігається в хешованому вигляді.

Команда `enable password` встановлює пароль для віддаленого доступу до роутера за протоколами, такими як Telnet або SSH.

Лістинг 2.1 — Налаштування ім'я та пароля на роутері в центральному офісі

```
hostname CentralOffice
!
enable secret C01212
enable password C0121
```

Після цього в роутері на інтерфейсах потрібно налаштувати внутрішню (локальну) та зовнішню IP-адресу (лістинг 2.2, лістинг 2.3).

Лістинг 2.2 — Налаштування зовнішньої адреси на роутері в центральному офісі

```
interface GigabitEthernet0/0/0
ip address 188.124.10.1 255.255.255.252
```

Наступним кроком буде налаштування локальної адреси. В корпоративний мережі буде використовуватись технологія VLAN, тому потрібно налаштувати інкапсуляцію за допомогою команди `encapsulation dot1Q` для того щоб передавати декілька VLAN через один порт. Так само ще використовується команда `ip helper-address` у мережах з використанням протоколу DHCP. Її метою є перенаправлення мережевого трафіку DHCP на вказану адресу.

Лістинг 2.3 — Налаштування внутрішньої (локальної) адреси на роутері в центральному офісі

```
interface GigabitEthernet1/0/0
no ip address
!
interface GigabitEthernet1/0/0.5
description Server
encapsulation dot1Q 5
ip address 172.10.1.1 255.255.255.0
!
interface GigabitEthernet1/0/0.10
description PC
encapsulation dot1Q 10
ip address 172.10.2.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet1/0/0.15
```

```

description Wi-Fi
encapsulation dot1Q 15
ip address 172.10.3.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet1/0/0.20
description Voice
encapsulation dot1Q 20
ip address 172.10.4.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet1/1/0
no ip address
!
interface GigabitEthernet1/1/0.10
description PC
encapsulation dot1Q 10
ip address 172.10.10.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet1/1/0.15
description Wi-Fi
encapsulation dot1Q 15
ip address 172.10.11.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet1/1/0.20
description Voice
encapsulation dot1Q 20
ip address 172.10.12.1 255.255.255.0
ip helper-address 172.10.1.2

```

В якості проколу маршрутизації в корпоративній мережі використовується протокол RIP.

RIP (Routing Information Protocol) — це один із протоколів динамічної маршрутизації, що використовується для обміну інформацією про маршрути між маршрутизаторами в симуляції мережі. RIP використовує алгоритм дистанційно-векторної маршрутизації і заснований на метриці hop count (кількість стрибків), щоб визначити найкращий маршрут до мережеских підмереж.

Під час використання RIP автоматично обмінюються інформацією про маршрути з сусідніми маршрутизаторами, оновлюють таблиці маршрутизації та вибирають оптимальні шляхи для доставки даних у мережі. Це дає змогу

маршрутизаторам динамічно адаптуватися до змін у мережі, наприклад, коли додаються нові маршрути або відбуваються збої у зв'язку. [19]

Лістинг 2.4 — Налаштування RIP на роутері в центральному офісі

```
version 2
network 172.10.0.0
network 188.124.0.0
```

Під час маршрутизації RIP використовується його друга версія, оскільки вона може використовувати багатоадресну розсилку, що зменшує навантаження на мережу на відміну від першої версії. Так само друга версія підтримує можливість підсумовування маршрутів (route summarization), що дає змогу зменшити розмір таблиць маршрутизації та поліпшити ефективність маршрутизації у великих мережах.

Після цих налаштувань наступним кроком буде конфігурація IP телефонії. IP телефонія, також відома як VoIP (Voice over Internet Protocol), являє собою технологію передачі голосового зв'язку мережею інтернет. Замість використання традиційних аналогових сигналів, IP телефонія перетворює аудіо сигнали в цифровий формат і передає їх через IP-мережу. Це дає змогу знизити вартість телефонних дзвінків і надає широкий спектр функцій, як-от конференц-зв'язок, переадресація викликів, голосова пошта та інші.

Перед початком її налаштування потрібно налаштувати DHCP для того щоб ір-телефони отримали ір-адресу.

Лістинг 2.5 — Налаштування DHCP для IP-телефонів на роутері в центральному офісі

```
ip dhcp pool VoiceFL1
network 172.10.4.0 255.255.255.0
default-router 172.10.4.1
option 150 ip 172.10.4.1
!
ip dhcp pool VoiceFL2
network 172.10.12.0 255.255.255.0
default-router 172.10.12.1
option 150 ip 172.10.12.1
```

Для того щоб уникнути помилок потрібно додати ір-адресу роутера у список адресів які заборонено використовувати в DHCP.

Лістинг 2.6 — Додавання адрес в список заборонених для DHCP

```
ip dhcp excluded-address 172.10.4.1
ip dhcp excluded-address 172.10.12.1
```

Після налаштування DHCP наступним кроком буде налаштування самої IP-телефонії. Першим кроком є налаштування кількості телефонів та номерів які можна додати за допомогою команд `max-ephones` та `max-dn`.

Лістинг 2.7 — Налаштування телефонного сервісу

```
telephony-service
max-ephones 16
max-dn 16
ip source-address 172.10.4.1 port 2000
auto assign 1 to 15
```

Наступним кроком є налаштування самих IP-телефонів. Для цього кожному телефону були прописані налаштування, а саме його тип, його `mac-address` та номер телефону.

Лістинг 2.8 — Налаштування IP-телефонів

```
ephone 1
device-security-mode none
mac-address 00E0.8F2E.6785
type 7960
button 1:1
!
ephone 2
device-security-mode none
mac-address 0090.2B2A.B46A
type 7960
button 1:2
!
ephone 3
device-security-mode none
mac-address 0060.4793.A31E
type 7960
```

```

button 1:3
!
ephone 4
device-security-mode none
mac-address 0001.6319.3152
type 7960
button 1:4
!
ephone 5
device-security-mode none
mac-address 0001.421B.DB8E
type 7960
button 1:5
!
ephone 6
device-security-mode none
mac-address 0007.ECA6.B29A
type 7960
button 1:6
!

```

Після налаштування IP-телефонів потрібно створити їм номери телефонів.

Лістинг 2.9 — Створення номерів телефону

```

ephone-dn 1
  number 0101
!
ephone-dn 2
  number 0102
!
ephone-dn 3
  number 0103
!
ephone-dn 4
  number 0104
!
ephone-dn 5
  number 0105
!
ephone-dn 6
  number 0106
!

```

І останнім кроком буде створення та конфігурації наборів параметрів, пов'язаних із голосовими з'єднаннями. За допомогою команди `dial-peer voice` можна налаштувати параметри з'єднання, як-от префікси набору номера (`destination-`

pattern), номери для виклику, зіставлення номерів, що викликають, і номерів, які викликаються, маршрутизацію викликів (session target ipv4:) та інші пов'язані параметри голосових послуг.

Лістинг 2.10 — Налаштування наборів параметрів голосового з'єднання

```
dial-peer voice 1 voip
destination-pattern 1...
session target ipv4:174.10.3.1
!
dial-peer voice 2 voip
destination-pattern 2...
session target ipv4:175.10.3.1
!
dial-peer voice 3 voip
destination-pattern 5...
session target ipv4:180.24.3.1
!
dial-peer voice 4 voip
destination-pattern 3...
session target ipv4:176.10.3.1
```

Наступний пристрій який потрібно налаштувати це — комутатор. Він слугує своєрідним "розгалужувачем" мережі, який дає змогу пристроям обмінюватися даними один з одним.

Коли пристрої під'єднано до комутатора, він аналізує одержувані дані та перенаправляє їх тільки на ті порти, до яких адресовано ці дані. Це дає змогу пристроям у мережі спілкуватися безпосередньо, мінаючи незв'язані з ними пристрої. Таким чином, комутатор покращує пропускну здатність і зменшує затримки в мережі.

Перед початком налаштувань комутатора потрібно додати за допомогою команди hostname назву.

Лістинг 2.11 — Налаштування ім'я комутатора в центральному офісі

```
en
conf t
hostname COFloor1
```

Наступним кроком буде налаштування VLAN. VLAN (Virtual Local Area Network) — це технологія, що дає змогу розділити одну фізичну мережу на кілька віртуальних локальних мереж. В локальній мережі центрального офісу буде декілька VLAN, а саме для сервера, комп’ютерів, Wi-Fi та голосовий зв’язок. Для створення VLAN потрібно використовувати команду `vlan` та `name`.

Після створення VLAN потрібно їх назначити на кожен підключений інтерфейс, для цього потрібно обрати інтерфейс та вписати цифру потрібного VLAN.

Лістинг 2.12 — Декілька з налаштувань інтерфейсів на комутаторі

```
interface GigabitEthernet1/0/1
switchport access vlan 5
!
interface GigabitEthernet1/0/7
switchport access vlan 10
!
interface GigabitEthernet1/0/13
switchport access vlan 10
switchport mode access
switchport voice vlan 20
!
switchport access vlan 10
!
interface GigabitEthernet1/0/22
switchport access vlan 10
!
interface GigabitEthernet1/0/23
switchport access vlan 15
!
interface GigabitEthernet1/1/1
switchport mode trunk
```

Лістинг 2.13 — Результат налаштування VLAN на комутаторі

VLAN	Name	Status	Ports
1	default	active	Gig1/0/24, Gig1/1/2, Gig1/1/3, Gig1/1/4
5	Server	active	Gig1/0/1, Gig1/0/2, Gig1/0/3, Gig1/0/4 Gig1/0/5, Gig1/0/6
10	PC	active	Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/10 Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22.
15	Wi-Fi	active	Gig1/0/23

20	Voice	active	Gig1/0/13, Gig1/0/14, Gig1/0/15, Gig1/0/16 Gig1/0/17, Gig1/0/18, Gig1/0/19
----	-------	--------	---

Наступний пристрій який потрібно налаштувати це — точка доступу. Вона використовується для створення бездротової мережі (Wi-Fi) і надання бездротового підключення пристроїв до локальної мережі та Інтернету.

Точка доступу приймає мережевий трафік від дротових пристроїв у локальній мережі та передає його радіохвилями, даючи змогу бездротовим пристроям, як-от ноутбукам, смартфонам або планшетах, підключатися до мережі та обмінюватися даними. Вона також виконує функцію маршрутизатора, який дає змогу бездротовим пристроям звертатися до ресурсів у локальній мережі та обмінюватися даними між собою. Точка доступу надає доступ до Інтернету, якщо під'єднана до мережі з доступом до Інтернету.

Для налаштування точки доступу потрібно змінити ім'я мережі (SSID), можна встановити пароль і вибрати тип шифрування для забезпечення безпеки бездротової мережі. Ці заходи допоможуть захистити мережу від несанкціонованого доступу.

Встановлення пароля дає змогу обмежити доступ до мережі лише авторизованим користувачам, які знають цей пароль. Пароль можна налаштувати на точці доступу і, надалі, вводити під час під'єднання до мережі на пристроях клієнтів.

Вибір типу шифрування визначає, як дані передаються бездротовою мережею і як вони захищені. Найпоширенішими типами шифрування є WPA2 і WPA3. Шифрування захищає дані, що передаються мережею, від несанкціонованого прослуховування та підміни.

The screenshot shows a configuration window titled 'Port 1'. It contains the following fields and options:

- Port Status:** A checkbox labeled 'On' is checked.
- SSID:** A text field containing 'WiFi Floor1'.
- 5 GHz Channel:** A dropdown menu showing '112'.
- Coverage Range (meters):** A text field containing '140,00'.
- Authentication:** A group of radio buttons with 'WPA2-PSK' selected. Other options are 'Disabled', 'WEP', and 'WPA-PSK'.
- Encryption Type:** A dropdown menu showing 'AES'.
- WEP Key:** A text field (empty).
- PSK Pass Phrase:** A text field containing 'Floor1CO'.
- User ID:** A text field (empty).
- Password:** A text field (empty).

Рисунок 2.2 — Налаштування точки доступу в центральному офісі

Наступні пристрої які потрібно налаштувати це — сервери. Перший сервер який потрібно налаштувати це DHCP-сервер.

DHCP (Dynamic Host Configuration Protocol) Server — це сервер, який автоматично призначає IP-адреси та іншу мережеву конфігурацію клієнтським пристроям у комп'ютерних мережах.

Основне завдання DHCP-сервера - надання динамічної конфігурації мережевих параметрів, таких як IP-адреса, підмережа, шлюз за замовчуванням і DNS-сервери, клієнтським пристроям, підключеним до мережі. Замість того щоб вручну налаштовувати кожен пристрій мережі мережевими параметрами, DHCP-сервер дає змогу автоматично призначати й оновлювати ці параметри в процесі під'єднання нових пристроїв або перезавантаження наявних.

Для початку потрібно налаштувати ip-адресу для сервера (рисунок 2.4), а потім увімкнути та додати налаштування до DHCP сервісу (рисунок 2.3).

DHCP

Interface: GigabitEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address: 172 10 1 0

Subnet Mask: 255 255 255 0

Maximum Number of Users: 0

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add
Save
Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
WServer	180.24.4.1	172.10.1.4	180.24.4.2	255.255.255.0	1	0.0.0.0	0.0.0.0
WWiFi	180.24.2.1	172.10.1.4	180.24.2.2	255.255.255.0	20	0.0.0.0	0.0.0.0
WPC	180.24.1.1	172.10.1.4	180.24.1.2	255.255.255.0	20	0.0.0.0	0.0.0.0
S3WiFi	176.10.2.1	172.10.1.4	176.10.2.2	255.255.255.0	20	0.0.0.0	0.0.0.0
S3PC	176.10.1.1	172.10.1.4	176.10.1.2	255.255.255.0	20	0.0.0.0	0.0.0.0
S2WiFi	175.10.2.1	172.10.1.4	175.10.2.2	255.255.255.0	20	0.0.0.0	0.0.0.0
S2PC	175.10.1.1	172.10.1.4	175.10.1.2	255.255.255.0	20	0.0.0.0	0.0.0.0
S1WiFi	174.10.2.1	172.10.1.4	174.10.2.2	255.255.255.0	20	0.0.0.0	0.0.0.0
S1PC	174.10.1.1	172.10.1.4	174.10.1.2	255.255.255.0	20	0.0.0.0	0.0.0.0
COPC (FL2)	172.10.10.1	172.10.1.4	172.10.10.2	255.255.255.0	20	0.0.0.0	0.0.0.0
COWi-Fi (FL2)	172.10.11.1	172.10.1.4	172.10.11.2	255.255.255.0	20	0.0.0.0	0.0.0.0
COWi-Fi (FL1)	172.10.3.1	172.10.1.4	172.10.3.2	255.255.255.0	20	0.0.0.0	0.0.0.0
COPC (FL1)	172.10.2.1	172.10.1.4	172.10.2.2	255.255.255.0	20	0.0.0.0	0.0.0.0

Рисунок 2.3 — Налаштування DHCP на сервері

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 172.10.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 172.10.1.1

DNS Server: 172.10.1.4

Рисунок 2.4 — Конфігурація IP-адреси на DHCP сервері

Наступний сервер який налаштувати це DNS-Server. DNS (Domain Name System) Server — це сервер, який перетворює доменні імена (наприклад, www.zpbud.com.ua) на відповідні IP-адреси комп'ютерів, на яких розміщені ресурси мережі, такі як веб-сайти, поштові сервери та інші сервіси.

Основне завдання DNS-сервера — забезпечити дозвіл доменних імен на IP-адреси, даючи змогу користувачам використовувати зручні для читання доменні імена замість запам'ятовування числових IP-адрес. Коли користувач вводить доменне ім'я у веб-браузері або іншому мережевому додатку, DNS-сервер відповідає, надаючи відповідну IP-адресу, яка потім використовується для встановлення з'єднання з потрібним сервером.

Потрібно налаштувати ip-адресу для сервера (рисунок 2.5), а потім увімкнути та створити адресу у DNS сервісі (рисунок 2.6).

IP Configuration

IP Configuration

☐ DHCP

☒ Static

IPv4 Address

172.10.1.4

Subnet Mask

255.255.255.0

Default Gateway

172.10.1.1

DNS Server

172.10.1.4

Рисунок 2.5 — Конфігурація IP-адреси на DNS сервері

DNS

DNS Service

☒ On

☐ Off

Resource Records

Name

Type

A Record

Address

Add

Save

Remove

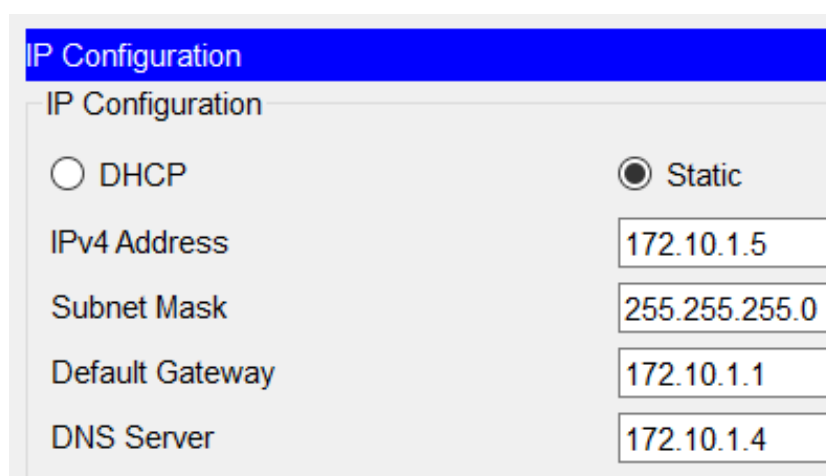
No.	Name	Type	Detail
0	www.whzpybd.com.ua	A Record	180.24.4.2
1	www.zpybd.com.ua	A Record	172.10.1.5

Рисунок 2.6 — Налаштування DNS

Далі потрібно налаштувати сервер HTTP сервер. HTTP (HyperText Transfer Protocol) Server — це програмне забезпечення, яке обробляє HTTP-запити від

клієнтів (наприклад, веб-браузерів) і надає їм HTTP-відповіді. Він використовується для доставки веб-сторінок, файлів та іншого контенту через протокол HTTP. HTTP-сервери дають змогу розміщувати веб-сайти, створювати веб-додатки та обмінюватися даними в мережі Інтернет. Вони відіграють ключову роль у веб-розробці та забезпечують взаємодію між клієнтськими та серверними компонентами веб-додатків.

Варто налаштувати IP-адресу для сервера (рисунок 2.7), а потім створити сторінку в HTTP сервісі (лістинг 2.13, лістинг 2.14).



The image shows a 'IP Configuration' window. At the top, there's a blue header bar with the text 'IP Configuration'. Below it, the title 'IP Configuration' is repeated. There are two radio buttons: 'DHCP' (unselected) and 'Static' (selected). Below these are four input fields with their corresponding values: 'IPv4 Address' is '172.10.1.5', 'Subnet Mask' is '255.255.255.0', 'Default Gateway' is '172.10.1.1', and 'DNS Server' is '172.10.1.4'.

Field	Value
IPv4 Address	172.10.1.5
Subnet Mask	255.255.255.0
Default Gateway	172.10.1.1
DNS Server	172.10.1.4

Рисунок 2.7 — Конфігурація IP-адреси на HTTP сервері

Лістинг 2.14 — Код HTTP сторінки сайту для сервера який знаходиться в центральному офісі

```
<html>
<center><font size='+2' color='Blue'>ПП "ЗапоріжВуд"</font></center>
<hr>Сайт для працівників
<p>Посилання
<br><a href='helloworld.html'>Важлива інформація</a>
<br><a href='copyrights.html'>Новини</a>
<br><a href='image.html'>Файли та інше</a>
<br><a href='cscoptlogo177x111.jpg'>Графік роботи</a>
</html>
```

Лістинг 2.15 — Код HTTP сторінки сайту для сервера який знаходиться на складі

```
<html>
```

```

<center><font size='+2' color='blue'>ПП "ЗапоріжБуд
(Склад)"</font></center>
<hr>Склад товару для магазинів
<p>Посилання:
<br><a href='helloworld.html'>Кількість товару</a>
<br><a href='copyrights.html'>Заявки</a>
<br><a href='image.html'>Працівники</a>
<br><a href='cscoptlogo177x111.jpg'>Список замовлень</a>
</html>

```

Наступний сервер, який потрібно налаштувати, це NTP-сервер. NTP (Network Time Protocol) Server — це сервер, який надає точний час і синхронізацію часу для комп'ютерів та інших пристроїв у комп'ютерних мережах.

Основне завдання NTP-сервера - забезпечити точну та узгоджену часову мітку для синхронізації всіх пристроїв у мережі. NTP-сервери отримують точний час від зовнішніх джерел часу і надають його клієнтським пристроям за запитом.

Коли комп'ютер або пристрій під'єднується до NTP-сервера, він може синхронізувати свій годинник із часом, що надається сервером. Це особливо важливо в мережах, де потрібна точна часова синхронізація.

Для його налаштування потрібно сконфігурувати IP-адресу (рисунок 2.8) та обрати правильний час який буде відображатись (рисунок 2.9).

The image shows a screenshot of a network configuration window titled "IP Configuration". The window has a blue header bar with the title. Below the header, there is a section titled "IP Configuration" with a light gray background. Inside this section, there are two radio buttons: "DHCP" (which is unselected) and "Static" (which is selected). Below the radio buttons, there are four text input fields, each with a label on the left and a value in the input box:

Field	Value
IPv4 Address	172.10.1.3
Subnet Mask	255.255.255.0
Default Gateway	172.10.1.1
DNS Server	172.10.1.4

Рисунок 2.8 — Конфігурація IP-адреси на NTP-сервері

NTP

Service ☒ On ☐ Off

Authentication

☐ Enable ☒ Disable

Key: Password:

← май 2023 →
08:35:37PM

пн	вт	ср	чт	пт	сб	вс
24	25	26	27	28	29	30
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Рисунок 2.9 — Налаштування часу в сервісі NTP

І останній сервер який потрібно налаштувати це EMAIL-сервер. EMAIL (Electronic Mail) Server — це серверне програмне забезпечення, яке обробляє, надсилає, приймає та зберігає електронні листи. Він використовується для організації електронної пошти та забезпечення обміну повідомленнями між відправниками та одержувачами.

Основне завдання поштового сервера - обробка електронних листів і доставка їх адресатам. Коли відправник надсилає лист, поштовий сервер відправника приймає його, перевіряє адресу одержувача, а потім маршрутизує і доставляє лист через Інтернет до поштового сервера одержувача. Після цього одержувач може отримати лист, коли підключається до свого поштового сервера.

Перед тим, як починати налаштування сервера, необхідно виконати два кроки. По-перше, налаштувати IP-адресу (рисунок 2.10). Потім, вказати доменне ім'я і додати користувачів (рисунок 2.11).

The screenshot shows a window titled "IP Configuration" with a blue header. Below the header, the "IP Configuration" section is expanded. It features two radio buttons: "DHCP" (unselected) and "Static" (selected). Below these are five text input fields: "IPv4 Address" with the value "172.10.1.6", "Subnet Mask" with "255.255.255.0", "Default Gateway" with "172.10.1.1", and "DNS Server" with "172.10.1.4".

Рисунок 2.10 — Конфігурація IP-адреси на Email-сервері

The screenshot shows a window titled "EMAIL". It contains two sections: "SMTP Service" and "POP3 Service", each with "ON" (selected) and "OFF" radio buttons. Below these is a "Domain Name" field containing "zpbyd.com.ua" and a "Set" button. At the bottom is a "User Setup" section with "User" and "Password" input fields, and a list box containing "Admin" and "User".

Рисунок 2.11 — Конфігурація сервісу Email на сервері

Останніми пристроями, які потрібно налаштувати, є комп'ютери та принтери. Це важливий етап процесу налаштування, де необхідно встановити відповідні параметри мережі на кожному комп'ютері та принтері. Ці параметри включають в себе IP-адреси, підмережі, шлюзи за замовчуванням і DNS-сервери які налаштовуються автоматично завдяки використанню DHCP (дротове підключення рисунок 2.12, бездротове підключення рисунок 2.13).

Для того, щоб комп'ютери та принтери могли під'єднатися бездротовим з'єднанням потрібно установити плату розширення "PT-HOST-NM-1W-AC" яка дозволяє пристрою під'єднуватися до Wi-Fi мережі на частоті 5 та 2,4 ГГц.

The screenshot shows the 'IP Configuration' window for the 'GigabitEthernet0' interface. The 'DHCP' radio button is selected, and the 'Static' radio button is unselected. The fields for IPv4 Address, Subnet Mask, Default Gateway, and DNS Server are all populated with values.

Interface	GigabitEthernet0
IP Configuration	
☒ DHCP	☐ Static
IPv4 Address	172.10.2.5
Subnet Mask	255.255.255.0
Default Gateway	172.10.2.1
DNS Server	172.10.1.4

Рисунок 2.12 — Конфігурація IP-адреси на комп'ютері з дротовим з'єднанням

The screenshot shows the 'Wireless0' configuration window. The 'Port Status' is checked and set to 'On'. The 'Bandwidth' is set to '1300 Mbps'. The 'MAC Address' is '0007.ECDD.3416'. The 'SSID' is 'WiFi Floor1'. The 'Authentication' section shows 'WPA2-PSK' selected. The 'Encryption Type' is set to 'AES'. The 'PSK Pass Phrase' is 'Floor1CO'. The 'Method' is set to 'MD5'.

Wireless0	
Port Status	☒ On
Bandwidth	1300 Mbps
MAC Address	0007.ECDD.3416
SSID	WiFi Floor1
Authentication ☐ Disabled ☐ WEP WEP Key ☐ WPA-PSK ☒ WPA2-PSK PSK Pass Phrase: Floor1CO ☐ WPA ☐ WPA2 User ID ☐ 802.1X Method: MD5 Password Encryption Type: AES	

Рисунок 2.13 — Конфігурація IP-адреси на комп'ютері з бездротовим з'єднанням

3 ВПРОВАДЖЕННЯ ТА НАЛАГОДЖЕННЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Впровадження корпоративної комп'ютерної мережі — це процес налаштування та розгортання мережевої інфраструктури в приміщеннях організації. Він включає в себе фізичне встановлення мережевого обладнання, конфігурацію мережевих пристроїв і служб, а також встановлення зв'язку між пристроями для полегшення комунікації та передачі даних.

Впровадження корпоративної комп'ютерної мережі зазвичай включає кілька ключових етапів:

Проектування та планування мережі:

На цьому етапі визначаються вимоги до мережі, такі як кількість користувачів, пристроїв і необхідна пропускна здатність, а також враховуються такі фактори, як фізичне розташування офісу і майбутня масштабованість. Топологія мережі, схема адресації та міркування щодо безпеки також визначаються на цьому етапі. Цей процес детально описаний в пункті 2

Закупівля мережевого обладнання:

На основі проекту мережі обирається та закуповується відповідне мережеве обладнання. Сюди входять маршрутизатори, комутатори, брандмауери, точки доступу, мережеві кабелі та будь-які інші необхідні компоненти. Обладнання обирається відповідно до конкретних потреб організації, беручи до уваги такі фактори, як продуктивність, надійність та сумісність.

Фізичне встановлення:

Мережеве обладнання фізично встановлюється у спеціально відведених місцях, таких як серверні кімнати або мережеві шафи. Це передбачає встановлення пристроїв, підключення їх за допомогою відповідних мережевих кабелів (Ethernet, оптоволокло тощо), а також забезпечення належного електроживлення та вентиляції обладнання.

Конфігурація мережевих пристроїв:

Мережеві пристрої, такі як маршрутизатори, комутатори та брандмауери, мають бути налаштовані, щоб забезпечити підключення до мережі та безпеку. Це включає налаштування IP-адрес, підмереж, протоколів маршрутизації, VLAN, списків контролю доступу (ACL) та інших специфічних конфігурацій для кожного пристрою. Конфігурацію можна виконати за допомогою інтерфейсу командного рядка (CLI) або графічного інтерфейсу користувача (GUI), наданого операційною системою пристрою.

Налаштування мережевих служб:

Мережеві служби, такі як DNS, DHCP, NTP та інші, повинні бути налаштовані для забезпечення необхідної функціональності для роботи в мережі. Конфігурація DNS передбачає налаштування доменних імен і зіставлення IP-адрес для ефективного вирішення імен. Налаштування DHCP автоматизує призначення IP-адрес пристроям у мережі. Налаштування NTP забезпечує точну синхронізацію часу на всіх пристроях мережі.

Реалізація мережевої безпеки:

Впровадження заходів мережевої безпеки має вирішальне значення для захисту мережі та її даних від несанкціонованого доступу та загроз. Це включає налаштування брандмауерів для контролю потоку трафіку та фільтрації вхідних і вихідних з'єднань. Для забезпечення безпечного віддаленого доступу до мережі можуть бути налаштовані VPN-мережі. Системи виявлення та запобігання вторгнень (IDPS) можуть бути розгорнуті для виявлення та пом'якшення потенційних порушень безпеки. Механізми контролю доступу, такі як автентифікація та авторизація користувачів, також впроваджуються для обмеження доступу до мережі авторизованим користувачам.

Тестування та усунення несправностей:

Після впровадження мережі проводиться ретельне тестування для забезпечення належного підключення, функціональності та продуктивності. Це включає тестування мережевого з'єднання між пристроями, перевірку доступу до мережевих ресурсів, а також перевірку функціональності мережевих служб і заходів безпеки. Будь-які проблеми або аномалії, виявлені під час тестування, виявляються і вирішуються шляхом усунення несправностей.

Документація та обслуговування:

Важливо вести точну документацію про реалізацію мережі, включаючи схеми мережі, схеми IP-адресації, конфігурації пристроїв, політики безпеки та будь-які внесені зміни. Регулярне обслуговування, оновлення та моніторинг необхідні для забезпечення безперебійної роботи мережі, вирішення будь-яких проблем з продуктивністю та адаптації до мінливих потреб організації.

Загалом, впровадження корпоративної комп'ютерної мережі передбачає системний підхід до проектування, закупівлі, встановлення, налаштування, захисту та обслуговування мережевої інфраструктури для забезпечення ефективного та безпечного зв'язку та передачі даних в організації. [20]

3.1 Розгортання розробленої мережі на підприємстві "ЗапоріжБуд"

Після процесу проектування корпоративної комп'ютерної мережі важливим етапом є розгортання розробленої мережі на підприємстві "ЗапоріжБуд". При цьому потрібно враховувати такі фактори:

- зручність у використанні;
- практичність;
- приємний зовнішній вигляд;
- результативність.

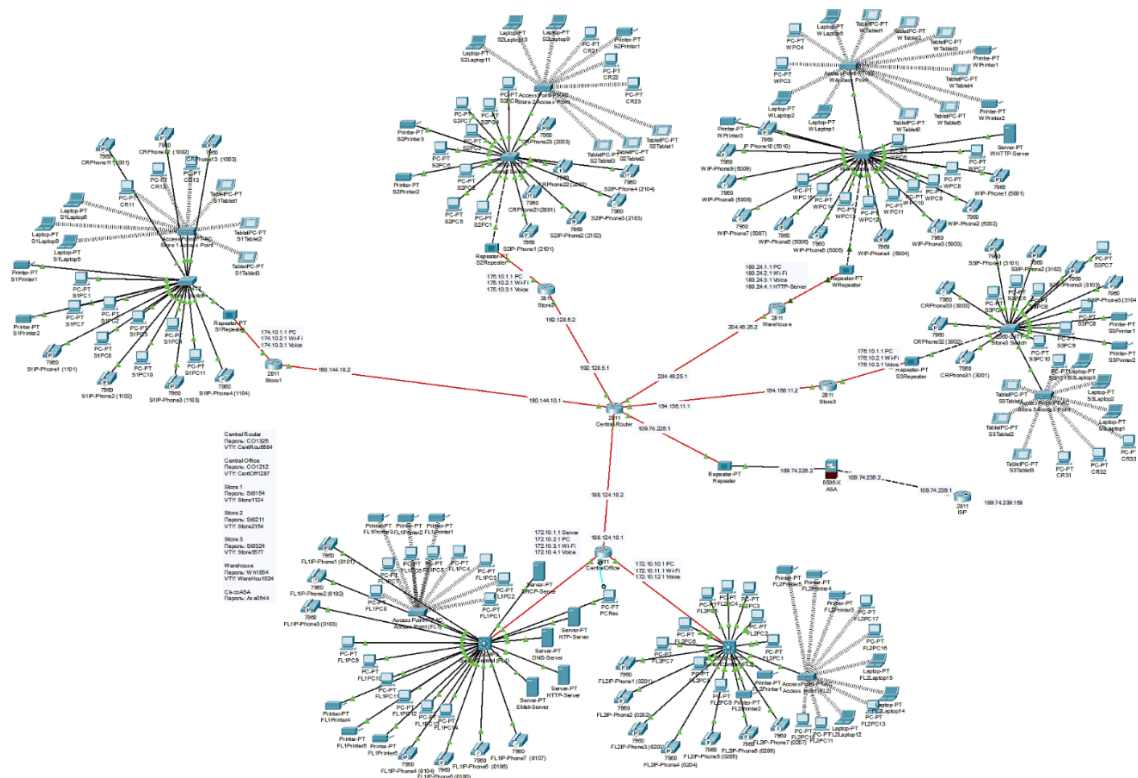


Рисунок 3.1 — Структурна схема корпоративної мережі

Першочерговою задачею є розгортання корпоративної комп'ютерної мережі у головному офісі. На рисунку 3.2 буде зображена детальна функціональна схема з'єднання у центральному офісі та на рисунку 3.3 та рисунку 3.4 зображена монтажна цієї будівлі.

В центральному офісі на першому поверсі буде розташовано 15 комп'ютерів, 6 принтерів, 7 IP-телефонів, 5 серверів, 1 точка доступу та один комутатор. На другому поверсі планується розташувати 14 комп'ютерів, 3 ноутбука, 5 принтерів, 7 IP-телефонів, 1 точка доступу та один комутатор. Всі пристрої будуть з'єднані за допомогою кабелю вита пара та бездротовим з'єднанням. Це забезпечує зручність та стабільність роботи.

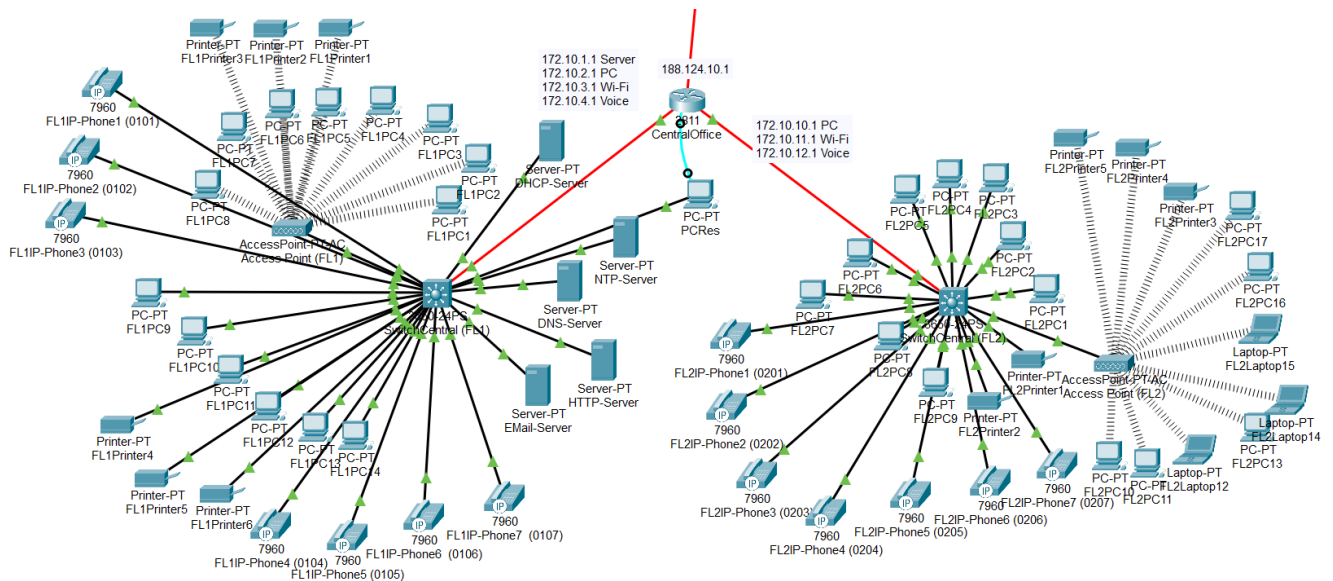


Рисунок 3.2 — Функціональна схема центрального офісу

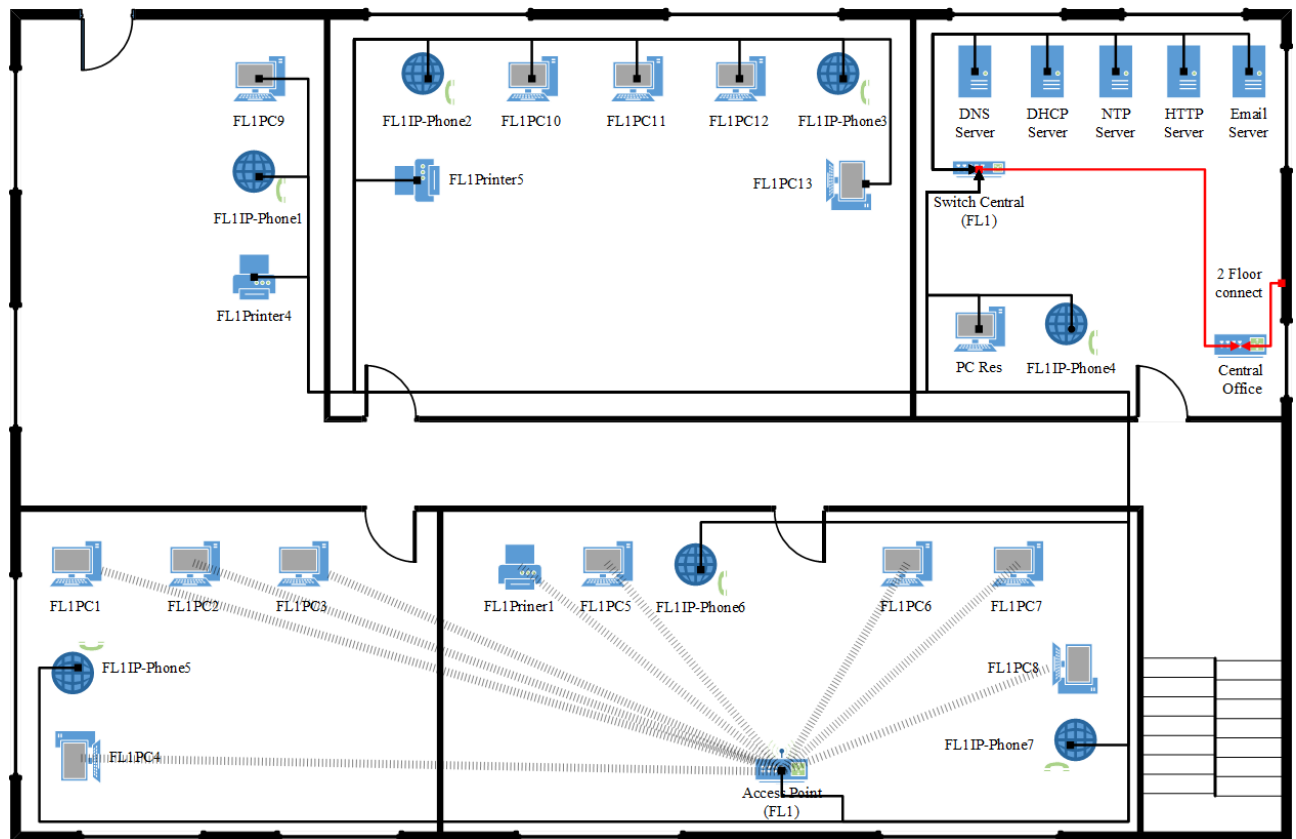


Рисунок 3.3 — Монтажна схема будівлі головного офісу (1 поверх)

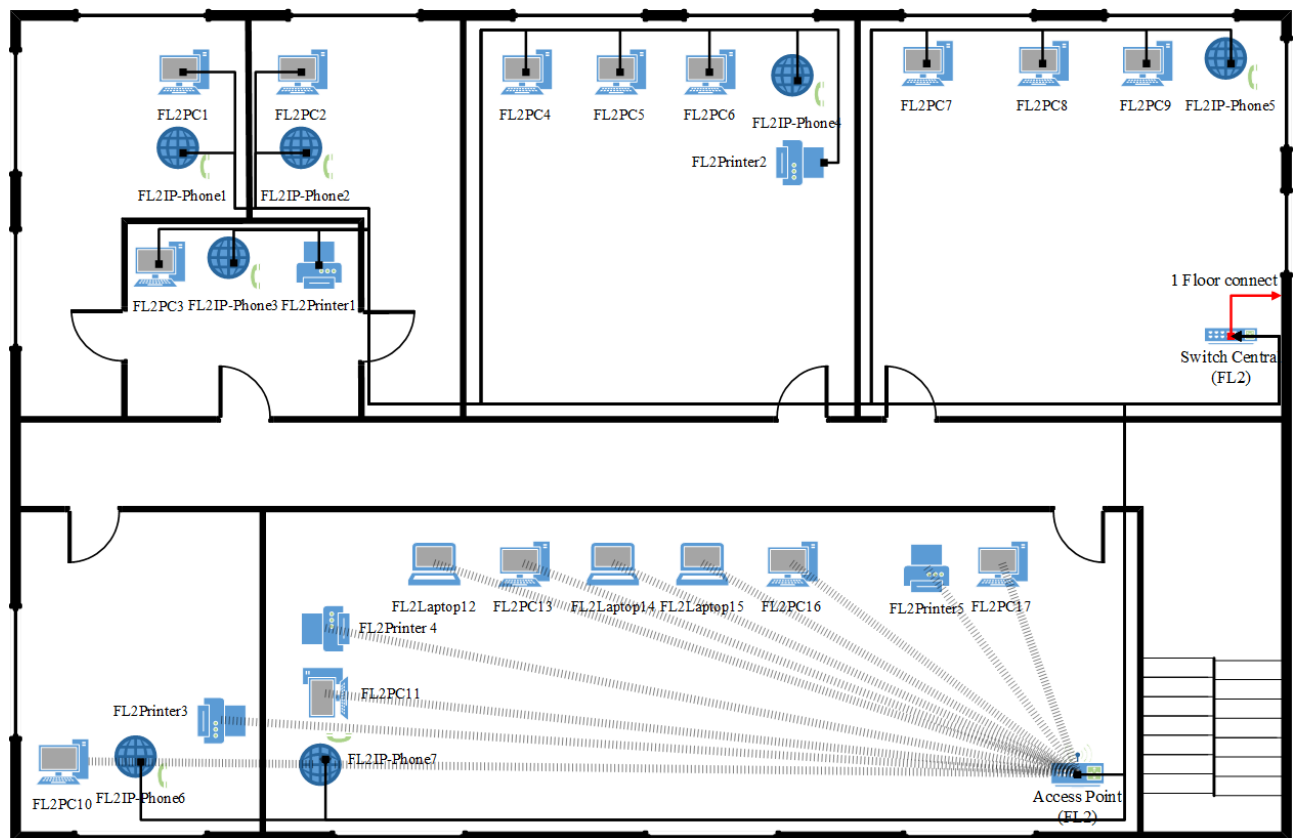


Рисунок 3.4 — Монтажна схема будівлі головного офісу (2 поверх)

Далі необхідно розгорнути мережу у магазинах. На рисунку 3.5 буде зображена детальна функціональна схема з'єднання у магазинах, на рисунку 3.6 зображена монтажна цих будівель.

В кожному магазині буде розташовано однакова кількість обладнання, а саме 8 комп'ютерів, 3 каси, 3 ноутбука, 3 планшети, 2 принтера, 7 IP-телефонів, точка доступу, комутатор та репітер. Монтажна схема магазинів знаходиться на 4 плакаті.

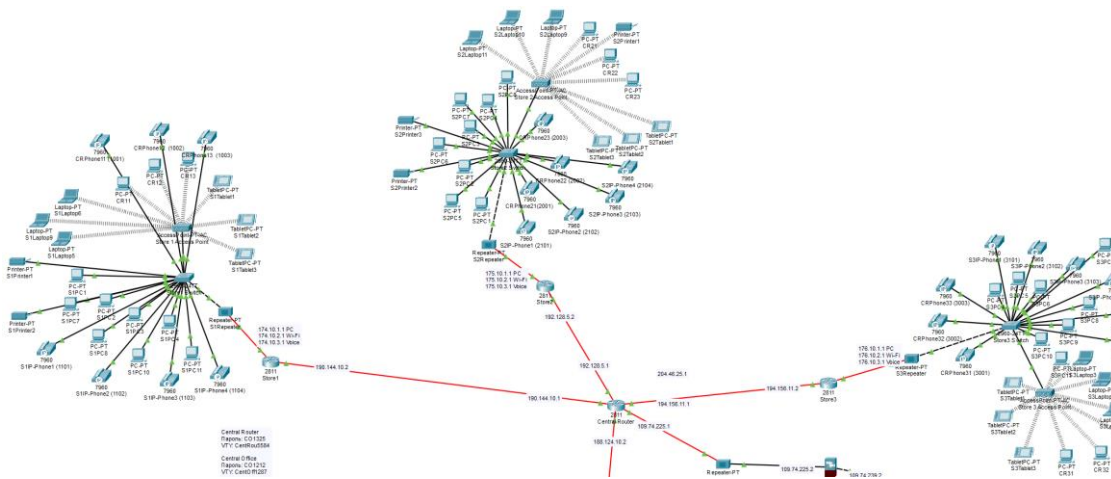


Рисунок 3.5 — Функціональна схема усіх магазинів

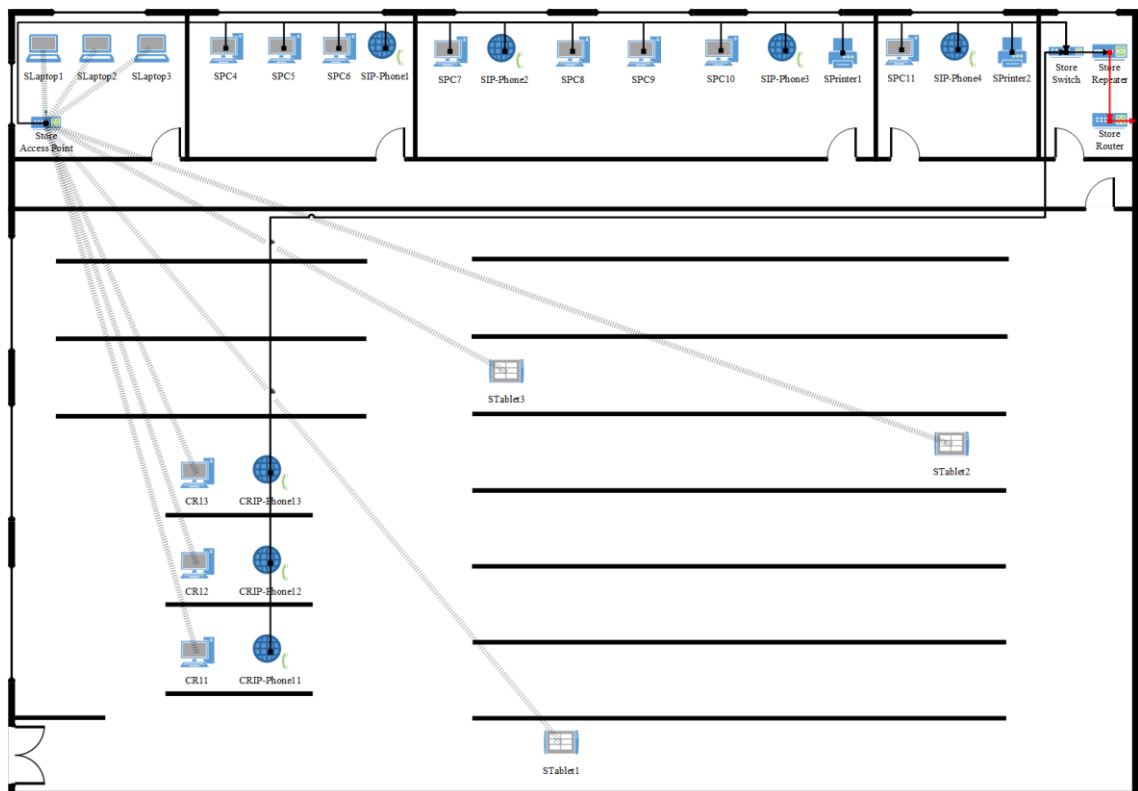


Рисунок 3.6 — Монтажна схема магазинів

І на останок залишилося розгорнути мережу на складі підприємства. На рисунку 3.7 буде зображена детальна функціональна схема з'єднання на складі, а на рисунку 3.8 зображена монтажна цієї будівлі.

На ньому буде розташовано 12 комп'ютерів, 3 ноутбуки, 6 планшетів, 3 принтери, 10 IP-телефонів, 1 сервер, 1 точка доступу, 1 комутатор та 1 повторювач. Монтажна схема складу знаходиться на 5 плакаті.

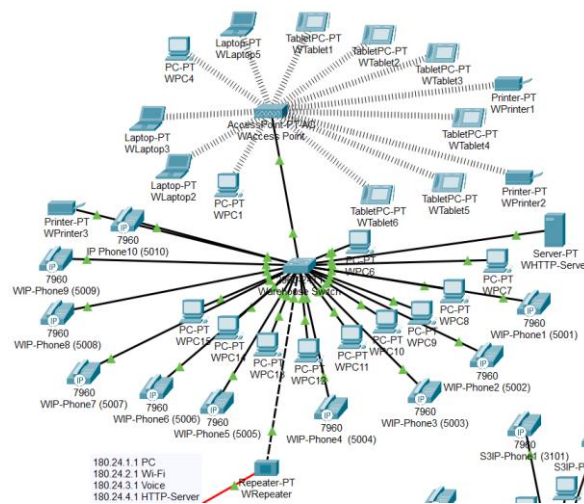


Рисунок 3.7 — Функціональна схема складу підприємства

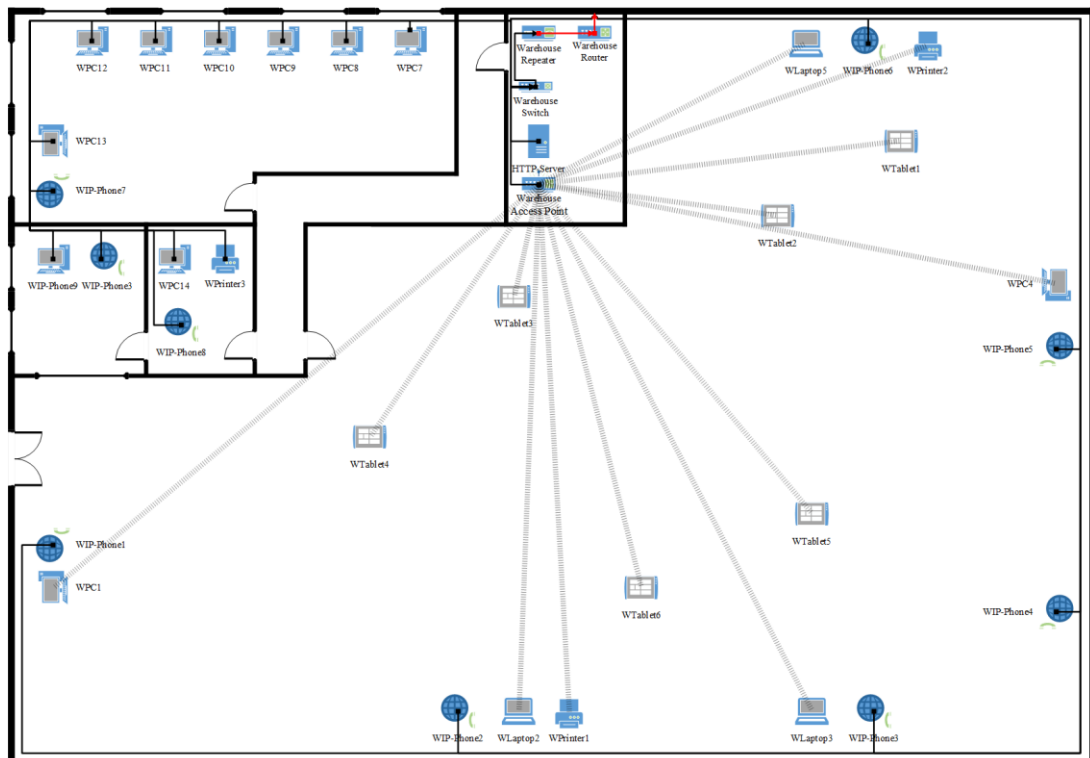


Рисунок 3.8 — Монтажна схема складу підприємства

3.2 Проведення тестування та налагодження мережі для забезпечення її стабільної та безперебійної роботи

Саме тестування і симуляція відбуватиметься в програмі Cisco Packet Tracer.

Cisco Packet Tracer — це програмне забезпечення, розроблене компанією Cisco Systems, яке являє собою симулятор мережевих пристроїв і мереж. Воно використовується для навчання і моделювання мереж, а також для виконання практичних завдань у галузі комп'ютерних мереж.

Cisco Packet Tracer надає середовище, в якому користувачі можуть створювати віртуальні мережі та експериментувати з різними мережевими конфігураціями. Він містить широкий спектр мережевого обладнання, такого як маршрутизатори, комутатори, сервери, ПК і багато іншого, яке можна налаштовувати та взаємодіяти з ними [21].

Є кілька аналогів Cisco Packet Tracer, наприклад GNS3 (Graphical Network Simulator). Ось деякі плюси GNS3 порівняно з Cisco Packet Tracer:

- реальне обладнання;
- гнучкість;
- розширюваність.

Мінуси GNS3:

- складність налаштування;
- вимоги до ресурсів;
- ліцензія та доступність образів;
- нестабільність.

Правильно розставлене обладнання ще не гарантує стабільну та безперебійну роботу, тому важливим пунктом є проведення тестування та налагодження мережі.

Перед завершенням роботи необхідно ґрунтовно перевірити всю корпоративну мережу, включно з налаштуваннями та провести тестування технологій і зв'язку, щоб переконатися в їхній належній роботі. Це важливо для забезпечення безпеки та ефективної роботи корпоративної мережі.

Під час перевірки налаштувань слід переконатися, що вони відповідають встановленим стандартам безпеки та вимогам компанії. Тестування технологій і зв'язку допоможе виявити можливі проблеми, як-от збої в мережі, неполадки в обладнанні або повільне з'єднання, які можуть вплинути на продуктивність і доступність системи. Регулярна перевірка і тестування допоможуть запобігти потенційним проблемам і забезпечити стабільну роботу корпоративної мережі.

Першим ділом потрібно перевірити зв'язок між всіма пристроями в корпоративній мережі за допомогою команди ping. Всі виміри проводилися з комп'ютера FL1PC1 який знаходиться в центральному офісі.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.10.2.8

Pinging 172.10.2.8 with 32 bytes of data:
Reply from 172.10.2.8: bytes=32 time=56ms TTL=127
Reply from 172.10.2.8: bytes=32 time=6ms TTL=127
Reply from 172.10.2.8: bytes=32 time=6ms TTL=127
Reply from 172.10.2.8: bytes=32 time=7ms TTL=127

Ping statistics for 172.10.2.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 56ms, Average = 18ms

C:\>ping 172.10.10.8

Pinging 172.10.10.8 with 32 bytes of data:
Reply from 172.10.10.8: bytes=32 time=15ms TTL=127
Reply from 172.10.10.8: bytes=32 time=4ms TTL=127
Reply from 172.10.10.8: bytes=32 time=18ms TTL=127
Reply from 172.10.10.8: bytes=32 time=16ms TTL=127

Ping statistics for 172.10.10.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 18ms, Average = 13ms

C:\>ping 174.10.1.3

Pinging 174.10.1.3 with 32 bytes of data:
Reply from 174.10.1.3: bytes=32 time=31ms TTL=125
Reply from 174.10.1.3: bytes=32 time=37ms TTL=125
Reply from 174.10.1.3: bytes=32 time=36ms TTL=125
Reply from 174.10.1.3: bytes=32 time=28ms TTL=125

Ping statistics for 174.10.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 28ms, Maximum = 37ms, Average = 33ms

C:\>ping 175.10.1.8

Pinging 175.10.1.8 with 32 bytes of data:
Reply from 175.10.1.8: bytes=32 time=6ms TTL=125
Reply from 175.10.1.8: bytes=32 time=8ms TTL=125
Reply from 175.10.1.8: bytes=32 time=30ms TTL=125
Reply from 175.10.1.8: bytes=32 time=30ms TTL=125

Ping statistics for 175.10.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 30ms, Average = 18ms
```

Рисунок 3.9 — Тестування зв'язку в корпоративній мережі

```

C:\>ping 180.24.1.18

Pinging 180.24.1.18 with 32 bytes of data:

Reply from 180.24.1.18: bytes=32 time=11ms TTL=125
Reply from 180.24.1.18: bytes=32 time=38ms TTL=125
Reply from 180.24.1.18: bytes=32 time=31ms TTL=125
Reply from 180.24.1.18: bytes=32 time=7ms TTL=125

Ping statistics for 180.24.1.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 38ms, Average = 21ms

C:\>ping 176.10.1.2

Pinging 176.10.1.2 with 32 bytes of data:

Reply from 176.10.1.2: bytes=32 time=27ms TTL=125
Reply from 176.10.1.2: bytes=32 time=17ms TTL=125
Reply from 176.10.1.2: bytes=32 time=17ms TTL=125
Reply from 176.10.1.2: bytes=32 time=8ms TTL=125

Ping statistics for 176.10.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 27ms, Average = 17ms

C:\>ping 109.74.239.158

Pinging 109.74.239.158 with 32 bytes of data:

Reply from 109.74.239.158: bytes=32 time=21ms TTL=252
Reply from 109.74.239.158: bytes=32 time=9ms TTL=252
Reply from 109.74.239.158: bytes=32 time=18ms TTL=252
Reply from 109.74.239.158: bytes=32 time=7ms TTL=252

Ping statistics for 109.74.239.158:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 21ms, Average = 13ms

```

← Склад підприємства

← Магазин №3

← Доступ до інтернету

Рисунок 3.10 — Тестування зв'язку в корпоративній мережі

Наступний етап полягає в перевірці роботи всіх серверів, і першим у списку - DHCP-сервери. Для цього потрібно перевірити наявність IP-адрес на пристроях.

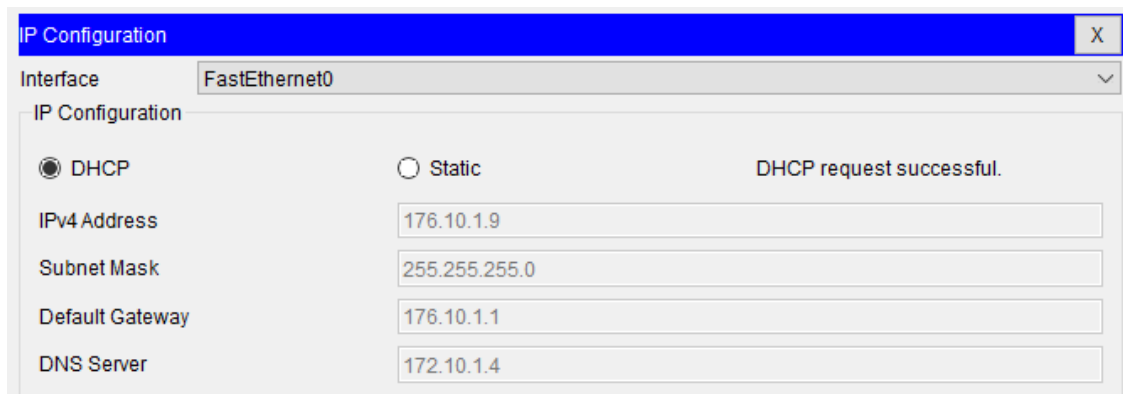


Рисунок 3.11 — Успішне отримання IP-адреси від DHCP-серверу

Наступний сервер для перевірки це DNS та HTTP сервери. Для їх перевірки потрібно відкрити сторінку www.zpbyd.com.ua або www.whzpbzd.com.ua на будь-якому пристрої.

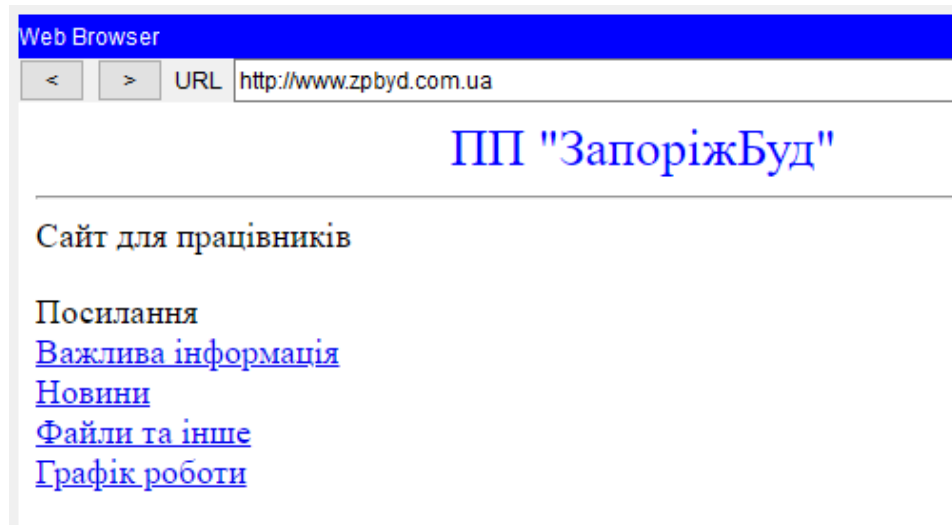


Рисунок 3.12 — Результат роботи сайту

Далі потрібно перевірити NTP-сервер. Для його перевірки необхідно відкрити будь-який пристрій або перевірити час на маршрутизаторі.

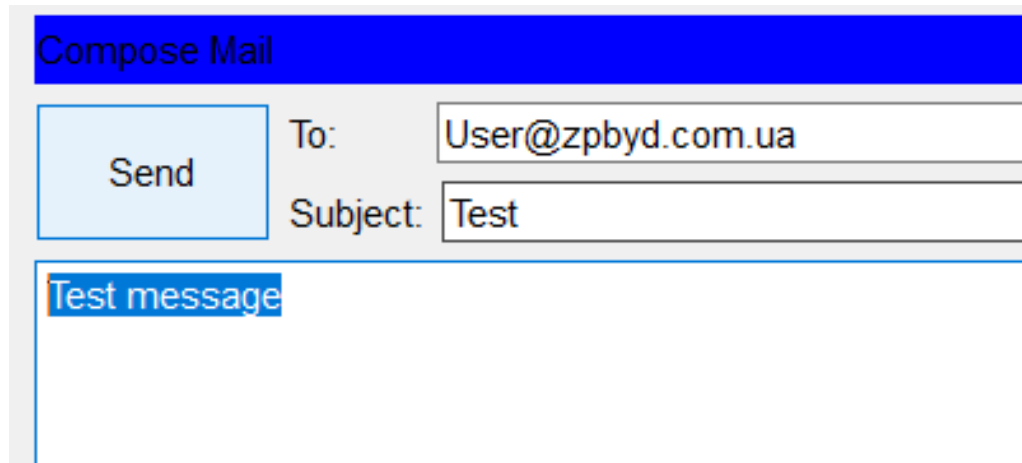


Рисунок 3.13 — Результат роботи сервера часу на ір-телефоні

Лістинг 3.1 — Перевірка часу на маршрутизаторі

```
CentRouter#show clock
2:20:49.169 UTC Mon May 8 2023
```

Остаточним етапом перевірки є перевірка Email-сервера. Для цього необхідно надіслати тестовий лист від імені користувача і переконатися в його успішному прийомі. Це дасть змогу переконатися в належній роботі Email-сервера і функціональності передавання повідомлень.



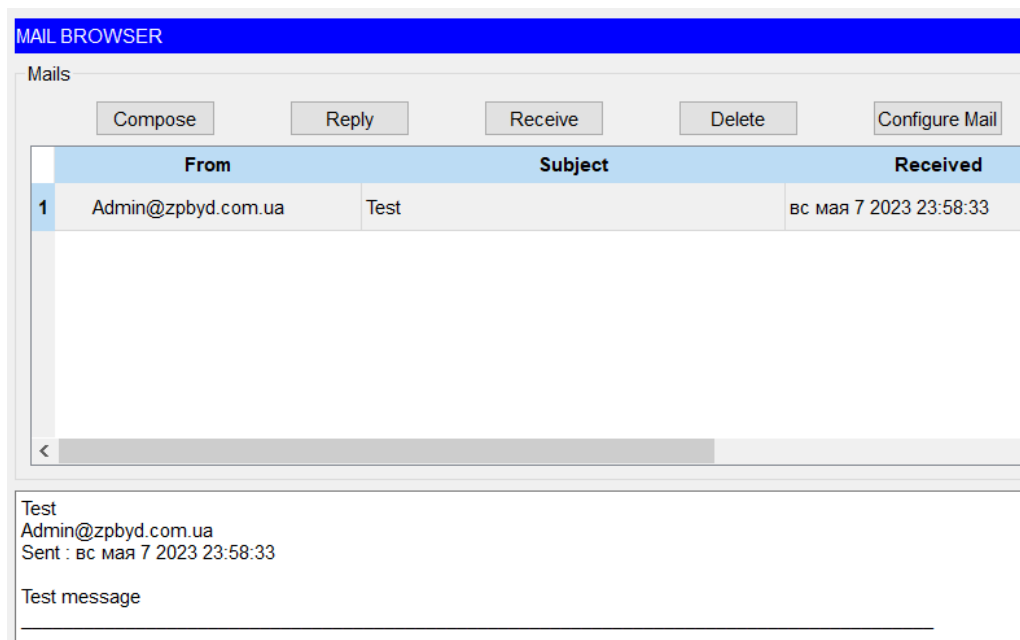
Compose Mail

Send To: User@zpbyd.com.ua

Subject: Test

Test message

Рисунок 3.14 — Відправка тестового повідомлення користувачу User



MAIL BROWSER

Mails

Compose Reply Receive Delete Configure Mail

	From	Subject	Received
1	Admin@zpbyd.com.ua	Test	вс мая 7 2023 23:58:33

<

Test
Admin@zpbyd.com.ua
Sent : вс мая 7 2023 23:58:33
Test message

Рисунок 3.15 — Успішне отримання тестового повідомлення

Далі слідує перевірка IP-телефонії, яка включає проведення тестового дзвінка. Це дасть змогу переконатися в правильній роботі системи IP-телефонії та якості зв'язку.



Рисунок 3.16 — Тестовий дзвінок на номер 5005 з номера 0101



Рисунок 3.17 — Успішний зв'язок та перевірка звуку

3.3 Впровадження заходів з моніторингу, керування та безпеки мережі

Після розгортання мережі та успішного проведення тестування потрібно подбати про впровадження заходів з моніторингу, керування та безпеки мережі.

Моніторинг мережі — це процес нагляду, збору та аналізу даних про стан і функціонування комп'ютерної мережі. Його основна мета полягає у виявленні, діагностиці та вирішенні проблем з мережею. Він відіграє значну роль у забезпеченні її ефективності та безпеки.

Для унеможливлення несанкціонованого доступу сторонніх осіб до мережевого обладнання та захисту інформації від хакерських атак потрібно зробити правильне налаштування засобів безпеки, таких як встановлення паролю, використання фаєрволу.

У разі внутрішньої корпоративної мережі, де основна загроза походить ззовні, використовується фаєрвол, який дозволяє проходження трафіку з мережі всередині (внутрішній трафік), але блокує трафік зовні (зовнішній трафік).

Першим ділом потрібно налаштувати безпеку доступу до фаєрволу для цього потрібно налаштувати пароль на доступ до привілейованого режиму.

Лістинг 3.2 — Зміна ім'я пристрою та встановлення паролю на фаєрволі

```
hostname ciscoasa
enable password Asa0544 encrypted
```

Наступним кроком потрібно налаштувати IP-адреса на внутрішньому та зовнішньому інтерфейсі.

Лістинг 3.3 — Налаштування IP-адрес та маршрутизації на фаєрволі 5506-X

```
interface GigabitEthernet1/1
  nameif inside
  security-level 100
  ip address 109.74.225.2 255.255.255.252
!
interface GigabitEthernet1/2
```

```

nameif outside
security-level 0
ip address 109.74.239.2 255.255.255.252
!
router rip
version 2
network 109.0.0.0

```

Також потрібно налаштувати фаєрвол таким чином, щоб користувачі всередині корпоративної мережі мали доступ до інтернету, але зовнішні користувачі та потенційні загрози не могли отримати доступ до внутрішньої мережі. Цього можна досягти шляхом налаштування правил фільтрації трафіку на фаєрволі, які дозволяють вихідний трафік із внутрішньої мережі, але блокують вхідний трафік із зовнішніх джерел. Таким чином, користувачі зможуть надсилати запити в інтернет і отримувати відповіді, але небажаний або потенційно небезпечний трафік буде фільтруватися фаєрволом, захищаючи внутрішню мережу від зовнішніх загроз.

Лістинг 3.4 — Налаштування правил фільтрації трафіку

```

class-map inspection_default
match default-inspection-traffic
class-map inspection
match default-inspection-traffic
class-map inspection_defaukt
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect icmp
inspect tftp
policy-map global
class inspection
inspect icmp
!
service-policy global_policy global

```

```

C:\>ping 109.74.239.158

Pinging 109.74.239.158 with 32 bytes of data:

Reply from 109.74.239.158: bytes=32 time=21ms TTL=252
Reply from 109.74.239.158: bytes=32 time=9ms TTL=252
Reply from 109.74.239.158: bytes=32 time=18ms TTL=252
Reply from 109.74.239.158: bytes=32 time=7ms TTL=252

Ping statistics for 109.74.239.158:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 21ms, Average = 13ms

```

← Доступ до інтернету

Рисунок 3.18 — Перевірка доступу до інтернету

```

Router>ping 172.10.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.10.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

```

Рисунок 3.14 — Перевірка доступу до корпоративної мережі ззовні

Також важливим аспектом який забезпечує правильну та стабільну роботу мережі є впровадження керування за рахунок віддаленого доступу.

Для забезпечення безпеки під час налаштування віддаленого режиму рекомендується встановити паролі для доступу як до привілейованого режиму (за допомогою команди "enable secret пароль"), так і для віддаленого підключення на маршрутизаторі. Це дасть змогу захистити вашу мережеву інфраструктуру від несанкціонованого доступу. Пароль для привілейованого режиму забезпечує контроль над налаштуваннями маршрутизатора, а пароль для віддаленого підключення потрібен для входу до маршрутизатора за протоколами віддаленого доступу, як-от Telnet або SSH.

Лістинг 3.5 — Налаштування безпеки на маршрутизаторі

```

enable secret St0154
!
line vty 0 4
access-class VTY in
password Store1124
login

```

```

CentralOffice#telnet 190.144.10.2
Trying 190.144.10.2 ...OpenAccess for administrators only. Enter password:

User Access Verification

Password:
Store1>sh version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 15.1(4)M4,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 15:41 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco2811 uptime is 37 minutes, 31 seconds
System returned to ROM by power-on
System image file is "flash0:c2800nm-advipservicesk9-mz.151-4.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
2 FastEthernet interface(s)
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-----
Device#    PID                      SN
-----
*0         CISCO2811/K9              FTX10171GXV-

```

Рисунок 3.19 — Результат успішного віддаленого підключення

ВИСНОВКИ

У процесі дослідження було встановлено, що розробка корпоративної комп'ютерної мережі є актуальною для приватного підприємства «ЗапоріжБуд». За допомогою цієї мережі воно зможе значно покращити ефективність своєї роботи, забезпечити безпеку даних та знизити витрати на інформаційні технології.

Завдяки розробці корпоративної мережі ПП «ЗапоріжБуд» зможе забезпечити централізоване збереження і обмін даними, підвищити безпеку від інформаційних загроз, встановити стандарти використання програмного забезпечення та зменшити ризики втрати інформації.

Додатково, розробка корпоративної комп'ютерної мережі також сприятиме покращенню комунікації між працівниками, швидкій передачі важливих даних, підвищенню ефективності роботи та зменшенню часу, що витрачається на вирішення технічних питань.

Отже, можна зробити висновок, що розробка корпоративної комп'ютерної мережі є дуже важливою для ПП «ЗапоріжБуд», оскільки вона дозволить підприємству підвищити ефективність своєї роботи.

Завдання даної дипломного проєкту полягало у розробці корпоративної комп'ютерної мережі для приватного підприємства «ЗапоріжБуд» з метою покращення управління його бізнес-процесами. Для досягнення цієї мети було сформульовано наступні завдання:

- вивчення діяльності підприємства та встановлення вимог до корпоративної комп'ютерної мережі;
- аналіз існуючої інфраструктури та ресурсів, які використовуються на підприємстві;
- встановлення технічних та функціональних вимог до корпоративної комп'ютерної мережі;
- розробка проєкту корпоративної комп'ютерної мережі на основі встановлених вимог;

- реалізація проекту та впровадження корпоративної комп'ютерної мережі на підприємстві;

- тестування та налагодження роботи корпоративної комп'ютерної мережі.

Метою дослідження була розробка та впровадження корпоративної комп'ютерної мережі, яка відповідає встановленим вимогам та дозволяє підприємству ефективно виконувати свої завдання та бізнес-процеси. Результатом роботи є покращення якості та швидкості обміну інформацією між підрозділами підприємства, зниження часу на виконання рутинних робіт, а також збільшення загальної ефективності роботи ПП «ЗапоріжБуд».

В ході дослідження було проведено детальний аналіз діяльності ПП «ЗапоріжБуд», визначені основні вимоги та потреби компанії щодо інформаційних технологій. Було встановлено, що наявна комп'ютерна мережа не відповідає потребам підприємства, оскільки її обмежені можливості не забезпечують ефективного та безперебійного функціонування бізнес-процесів. У зв'язку з цим, розробка корпоративної комп'ютерної мережі стала важливим завданням, що дозволить оптимізувати роботу працівників та покращити ефективність діяльності.

У цьому дипломному проекті був проведений аналіз всіх можливих ресурсів та інфраструктури, що використовується на підприємстві «ЗапоріжБуд». Було досліджено існуючу мережеву топологію, апаратне та програмне забезпечення, яке може бути використано на підприємстві. Виявлено, що на даний момент інфраструктура не забезпечує повної інтеграції всіх пристроїв та програмного забезпечення, що є чинником обмеження розвитку бізнесу.

Було проведено аналіз сучасних технологій та тенденцій у сфері комп'ютерних мереж, що дозволило визначити оптимальні рішення для розробки корпоративної мережі підприємства. В результаті дослідження було розроблено проект, який включає в себе необхідні засоби і технології для побудови інфраструктури, що забезпечує стабільну та надійну роботу.

Отже, дослідження всіх аспектів корпоративної мережі дозволить підприємству «ЗапоріжБуд» покращити свою інфраструктуру, забезпечити її

інтеграцію, підвищити ефективність роботи та знизити витрати на технічне обслуговування мережі.

Для вирішення поставлених завдань було обрано технології, що відповідають встановленим вимогам, враховуючи наявні ресурси підприємства. Було розроблено детальну структуру мережі та проектні рішення, які забезпечують високий рівень безпеки, ефективності та стійкості мережі.

Отже, розробка корпоративної комп'ютерної мережі ПП «ЗапоріжБуд» є важливим етапом в підвищенні ефективності роботи підприємства, забезпеченні безпеки та швидкого доступу до інформаційних ресурсів. Виконання встановлених технічних та функціональних вимог дозволить створити сучасну та надійну інфраструктуру, яка буде відповідати сучасним вимогам та готова до майбутнього розширення.

У створеній мережі є купа шляхів для вдосконалення та апгрейду. У випадку розростання магазину рекомендовано змінити тип маршрутизації на OSPF або EIGRP, тому що на відміну від інших маршрутизацій, RIP використовує просту метрику (кількість стрибків) для визначення оптимального маршруту, обмежена на кількість стрибків, високе використання пропускної здатності мережі. Для покращення швидкодії, додання нових функцій, підвищення стабільної роботи краще використовувати новітнє обладнання.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. English J. An introduction to 8 types of network devices | TechTarget. Networking. URL: <http://www.techtarget.com/searchnetworking/tip/An-introduction-to-8-types-of-network-devices> (дата звернення: 10.05.2023).

2. Behrouz A. Forouzan. "Data Communications and Networking" 5th Edition – Видавництво "McGraw Hill", 2012 р. – 1264 с.

3. What is a router? | Router definition. Cloudflare. URL: <http://www.cloudflare.com/learning/network-layer/what-is-a-router> (дата звернення: 22.05.2023).

4. Doug Lowe. Networking For Dummies 12th Edition – Видавництво "For Dummies", 2020 р. – 480 с.

5. Chai W., Contributor T. What is IP telephony? What are the businesses use cases? URL: <http://www.techtarget.com/searchunifiedcommunications/definition/IP-telephony> (дата звернення: 12.05.2023).

6. Types of computer network designs for business | jones IT. Jones IT | Managed IT Services, IT Support, IT Consulting. URL: <http://www.itjones.com/blogs/2020/12/1/types-of-computer-network-designs-for-business> (дата звернення: 12.05.2023).

7. What is a LAN? Local Area Network. Cisco. URL: <http://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html> (дата звернення: 12.05.2023).

8. What is a metropolitan area network (MAN)? Cloudflare. URL: <http://www.cloudflare.com/learning/network-layer/what-is-a-metropolitan-area-network> (дата звернення: 13.05.2023).

9. Scarpati J. What is WAN? Networking. URL: <http://www.techtarget.com/searchnetworking/definition/WAN-wide-area-network> (дата звернення: 13.05.2023).

10. William Stallings. "Network Security Essentials: Applications and Standards" 6th Edition – Видавництво "Pearson", 2016 p. – 464 с.

11. Larry Peterson and Bruce Davie. Computer Networks: A Systems Approach 6th Edition – Видавець "Morgan Kaufmann", 2021 p. – 848 с.

12. James F. Kurose and Keith W. Ross. "Computer Networking: A Top-Down Approach" 8th Edition – Видавництво "Pearson", 2020 p. – 856 с.

13. Designing A Computer Network For Your Business: A Step-By-Step Guide | Jones IT. Jones IT | Managed IT Services, IT Support, IT Consulting. URL: <https://www.itjones.com/blogs/2022/1/15/designing-a-computer-network-for-your-business-a-step-by-step-guide> (дата звернення: 19.05.2023).

14. Cisco 2800 Series Integrated Services Routers. Networking, Cloud, and Cybersecurity Solutions - Cisco. URL: https://www.cisco.com/c/dam/global/de_at/assets/unified_partners/smb/vertriebliche-positionierung/routing/downloads/isr_2800_datenblatt_e.pdf (дата звернення: 19.05.2023).

15. Cisco Catalyst 3560 Series Switches. Used Cisco Network Data Center Liquidators. URL: <https://www.andovercrg.com/datasheets/cisco-3560-catalyst-datasheet.pdf> (дата звернення: 20.05.2023).

16. Cisco Aironet 2700 Series Access Points Data Sheet. Cisco. URL: <https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-2700-series-access-point/datasheet-c78-730593.html> (дата звернення: 20.05.2023).

17. Cisco IP Phone 7960. VoIP Phone Systems, Hosting & Service | Atlanta GA: Professional Communications Management Inc. URL: https://callpcm.com/site/wp-content/uploads/cisco_7960_data_sheet.pdf (дата звернення: 20.05.2023).

18. Cisco Catalyst 2960-S Series Switches Data Sheet. Cisco. URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.html (дата звернення: 21.05.2023).

19. Brush K. What is Routing Information Protocol (RIP) and How Does It Work? Networking. URL: <https://www.techtarget.com/searchnetworking/definition/Routing-Information-Protocol> (дата звернення: 23.05.2023).

20. A Complete Guide To Business Computer Networks | Jones IT. Jones IT | Managed IT Services, IT Support, IT Consulting. URL: <https://www.itjones.com/blogs/2022/3/1/a-complete-guide-to-business-computer-networks> (дата звернення: 23.05.2023).

21. Cisco Packet Tracer - Networking Simulation Tool. Networking Academy. URL: <https://www.netacad.com/courses/packet-tracer> (дата звернення: 23.05.2023).


```
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/0
ip address 188.124.10.1 255.255.255.252
!
interface GigabitEthernet1/0/0
no ip address
!
interface GigabitEthernet1/0/0.5
description Server
encapsulation dot1Q 5
ip address 172.10.1.1 255.255.255.0
!
interface GigabitEthernet1/0/0.10
description PC
encapsulation dot1Q 10
ip address 172.10.2.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet1/0/0.15
description Wi-Fi
encapsulation dot1Q 15
ip address 172.10.3.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet1/0/0.20
description Voice
encapsulation dot1Q 20
ip address 172.10.4.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet1/1/0
no ip address
!
interface GigabitEthernet1/1/0.10
description PC
encapsulation dot1Q 10
ip address 172.10.10.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet1/1/0.15
description Wi-Fi
encapsulation dot1Q 15
```

```

ip address 172.10.11.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet1/1/0.20
description Voice
encapsulation dot1Q 20
ip address 172.10.12.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 172.10.0.0
network 188.124.0.0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CAccess for administrators only. Enter password:^C
!
!
!
!
dial-peer voice 1 voip
destination-pattern 1...
session target ipv4:174.10.3.1
!
dial-peer voice 2 voip
destination-pattern 2...
session target ipv4:175.10.3.1
!
dial-peer voice 3 voip
destination-pattern 5...
session target ipv4:180.24.3.1
!
dial-peer voice 4 voip
destination-pattern 3...
session target ipv4:176.10.3.1
!
telephony-service
max-ephones 16
max-dn 16
ip source-address 172.10.4.1 port 2000
auto assign 1 to 15
!
ephone-dn 1
number 0101

```

```
!  
ephone-dn 2  
number 0102  
!  
ephone-dn 3  
number 0103  
!  
ephone-dn 4  
number 0104  
!  
ephone-dn 5  
number 0105  
!  
ephone-dn 6  
number 0106  
!  
ephone-dn 7  
number 0107  
!  
ephone-dn 8  
number 0108  
!  
ephone-dn 9  
number 0109  
!  
ephone-dn 10  
number 0201  
!  
ephone-dn 11  
number 0202  
!  
ephone-dn 12  
number 0203  
!  
ephone-dn 13  
number 0204  
!  
ephone-dn 14  
number 0205  
!  
ephone-dn 15  
number 0206  
!  
ephone-dn 16  
number 0207  
!  
ephone 1  
device-security-mode none  
mac-address 00E0.8F2E.6785  
type 7960  
button 1:1  
!  
ephone 2
```

```
device-security-mode none
mac-address 0090.2B2A.B46A
type 7960
button 1:2
!
ephone 3
device-security-mode none
mac-address 0060.4793.A31E
type 7960
button 1:3
!
ephone 4
device-security-mode none
mac-address 0001.6319.3152
type 7960
button 1:4
!
ephone 5
device-security-mode none
mac-address 0001.421B.DB8E
type 7960
button 1:5
!
ephone 6
device-security-mode none
mac-address 0007.ECA6.B29A
type 7960
button 1:6
!
ephone 7
device-security-mode none
mac-address 0003.E430.776B
type 7960
button 1:7
!
ephone 8
device-security-mode none
mac-address 1111.1111.1111
type 7960
button 1:8
!
ephone 9
device-security-mode none
mac-address 1111.1111.1112
type 7960
button 1:9
!
ephone 10
device-security-mode none
mac-address 0030.F286.1E65
type 7960
button 1:10
!
```

```

ephone 11
device-security-mode none
mac-address 0090.210C.6533
type 7960
button 1:11
!
ephone 12
device-security-mode none
mac-address 0001.4291.1DDD
type 7960
button 1:12
!
ephone 13
device-security-mode none
mac-address 00E0.A3AB.8908
type 7960
button 1:13
!
ephone 14
device-security-mode none
mac-address 000C.CF66.C2DA
type 7960
button 1:14
!
ephone 15
device-security-mode none
type 7960
!
ephone 16
device-security-mode none
mac-address 0060.70CC.5196
type 7960
button 1:15
!
line con 0
!
line aux 0
!
line vty 0 4
password C01212
login
!
!
ntp server 172.10.1.3
!
end

```

Лістинг А.2 — Команди налаштування комутатора головного офісу (1
поверх)

```
hostname COFloor1
```

```
!  
!  
!  
!  
!  
!  
!  
no ip cef  
no ipv6 cef  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
interface GigabitEthernet1/0/1  
switchport access vlan 5  
!  
interface GigabitEthernet1/0/2  
switchport access vlan 5  
!  
interface GigabitEthernet1/0/3  
switchport access vlan 5  
!  
interface GigabitEthernet1/0/4  
switchport access vlan 5  
!  
interface GigabitEthernet1/0/5  
switchport access vlan 5  
!  
interface GigabitEthernet1/0/6  
switchport access vlan 5  
!  
interface GigabitEthernet1/0/7  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/8  
switchport access vlan 10
```

```
!  
interface GigabitEthernet1/0/9  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/10  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/11  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/12  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/13  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
!  
interface GigabitEthernet1/0/14  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
!  
interface GigabitEthernet1/0/15  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
!  
interface GigabitEthernet1/0/16  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
!  
interface GigabitEthernet1/0/17  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
!  
interface GigabitEthernet1/0/18  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
!  
interface GigabitEthernet1/0/19  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
!  
interface GigabitEthernet1/0/20  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/21  
switchport access vlan 10
```

```

!
interface GigabitEthernet1/0/22
switchport access vlan 10
!
interface GigabitEthernet1/0/23
switchport access vlan 15
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
switchport mode trunk
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
!
End

```

Лістинг А.3 — Команди налаштування комутатора головного офісу (2
поверх)

```

hostname COFloor2
!
!
!
!

```

```
!  
!  
!  
no ip cef  
no ipv6 cef  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
interface GigabitEthernet1/0/1  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/2  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/3  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/4  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/5  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/6  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/7  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/8  
switchport access vlan 10  
!  
interface GigabitEthernet1/0/9  
switchport access vlan 10  
!
```

```
interface GigabitEthernet1/0/10
switchport access vlan 10
switchport voice vlan 20
!
interface GigabitEthernet1/0/11
switchport access vlan 10
switchport voice vlan 20
!
interface GigabitEthernet1/0/12
switchport access vlan 10
switchport voice vlan 20
!
interface GigabitEthernet1/0/13
switchport access vlan 10
switchport voice vlan 20
!
interface GigabitEthernet1/0/14
switchport access vlan 10
switchport voice vlan 20
!
interface GigabitEthernet1/0/15
switchport access vlan 10
switchport voice vlan 20
!
interface GigabitEthernet1/0/16
switchport access vlan 10
switchport voice vlan 20
!
interface GigabitEthernet1/0/17
switchport access vlan 10
switchport voice vlan 20
!
interface GigabitEthernet1/0/18
switchport access vlan 10
switchport voice vlan 20
!
interface GigabitEthernet1/0/19
switchport access vlan 15
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
switchport mode trunk
!
interface GigabitEthernet1/1/2
```

```
!  
interface GigabitEthernet1/1/3  
!  
interface GigabitEthernet1/1/4  
!  
interface Vlan1  
no ip address  
shutdown  
!  
ip classless  
!  
ip flow-export version 9  
!  
!  
!  
!  
!  
!  
!  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
login  
!  
!  
!  
!  
end
```

ДОДАТОК Б

Лістинг Б.1 — Команди налаштування маршрутизатора магазинів

```

hostname Store1
!
!
!
enable secret 5 $1$mERr$iAFRpRjtxCv4d0AmFjrR3.
!
!
ip dhcp excluded-address 174.10.3.1
!
ip dhcp pool Voice
network 174.10.3.0 255.255.255.0
default-router 174.10.3.1
option 150 ip 174.10.3.1
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX10171GXV-
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1

```

```

no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/0
ip address 190.144.10.2 255.255.255.252
!
interface GigabitEthernet0/1/0
no ip address
!
interface GigabitEthernet0/1/0.10
description PC
encapsulation dot1Q 10
ip address 174.10.1.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet0/1/0.15
description Wi-Fi
encapsulation dot1Q 15
ip address 174.10.2.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet0/1/0.20
description Voice
encapsulation dot1Q 20
ip address 174.10.3.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 174.10.0.0
network 190.144.0.0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list standard VTY
permit host 188.124.10.1
!
banner motd ^CAccess for administrators only. Enter password:^
!
!
!
!
dial-peer voice 1 voip
destination-pattern 0...

```

```
session target ipv4:172.10.4.1
!
dial-peer voice 2 voip
destination-pattern 2...
session target ipv4:175.10.3.1
!
dial-peer voice 3 voip
destination-pattern 5...
session target ipv4:180.24.3.1
!
dial-peer voice 4 voip
destination-pattern 3...
session target ipv4:176.10.3.1
!
telephony-service
max-ephones 10
max-dn 10
ip source-address 174.10.3.1 port 2000
auto assign 1 to 10
!
ephone-dn 1
number 1001
!
ephone-dn 2
number 1002
!
ephone-dn 3
number 1003
!
ephone-dn 4
number 1101
!
ephone-dn 5
number 1102
!
ephone-dn 6
number 1103
!
ephone-dn 7
number 1104
!
ephone-dn 8
number 1105
!
ephone-dn 9
number 1106
!
ephone-dn 10
number 1107
!
ephone 1
device-security-mode none
mac-address 0001.C79D.8C86
```

```
type 7960
button 1:1
!
ephone 2
device-security-mode none
mac-address 00D0.5897.5EEB
type 7960
button 1:2
!
ephone 3
device-security-mode none
mac-address 0090.21BB.631B
type 7960
button 1:3
!
ephone 4
device-security-mode none
mac-address 0006.2AA6.258A
type 7960
button 1:4
!
ephone 5
device-security-mode none
mac-address 000C.856B.6AA0
type 7960
button 1:5
!
ephone 6
device-security-mode none
mac-address 00D0.979A.2E4E
type 7960
button 1:6
!
ephone 7
device-security-mode none
mac-address 000A.F301.E538
type 7960
button 1:7
!
line con 0
!
line aux 0
!
line vty 0 4
access-class VTY in
password Store1124
login
!
!
ntp server 172.10.1.3
!
end
```

Лістинг Б.2 — Команди налаштування комутатора магазинів

```
hostname S1Switch
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 10
!
interface FastEthernet0/2
switchport access vlan 10
!
interface FastEthernet0/3
switchport access vlan 10
!
interface FastEthernet0/4
switchport access vlan 10
!
interface FastEthernet0/5
switchport access vlan 10
!
interface FastEthernet0/6
switchport access vlan 10
!
interface FastEthernet0/7
switchport access vlan 10
!
interface FastEthernet0/8
switchport access vlan 10
!
interface FastEthernet0/9
switchport access vlan 10
!
interface FastEthernet0/10
switchport access vlan 10
!
interface FastEthernet0/11
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/12
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/13
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/14
switchport access vlan 10
switchport voice vlan 20
```

```
!  
interface FastEthernet0/15  
switchport access vlan 10  
switchport voice vlan 20  
!  
interface FastEthernet0/16  
switchport access vlan 10  
switchport voice vlan 20  
!  
interface FastEthernet0/17  
switchport access vlan 10  
switchport voice vlan 20  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
switchport mode trunk  
!  
interface GigabitEthernet0/2  
switchport access vlan 15  
!  
interface Vlan1  
no ip address  
shutdown  
!  
!  
!  
line con 0  
!  
line vty 0 4  
login  
line vty 5 15  
login  
!  
!  
!  
end
```

ДОДАТОК В

Лістинг В.1 — Команди налаштування маршрутизатора складу підприємства

```

hostname WRouter
!
!
!
enable secret 5 $1$mERr$Ezy9qCzZVWqT6F/JPBOnw/
!
!
ip dhcp excluded-address 180.24.3.1
!
ip dhcp pool Voice
network 180.24.3.0 255.255.255.0
default-router 180.24.3.1
option 150 ip 180.24.3.1
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX1017L7D6-
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!

```

```

interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/0
ip address 204.46.25.2 255.255.255.252
!
interface GigabitEthernet0/1/0
no ip address
!
interface GigabitEthernet0/1/0.5
description HTTP-Server
encapsulation dot1Q 5
ip address 180.24.4.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet0/1/0.10
description PC
encapsulation dot1Q 10
ip address 180.24.1.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet0/1/0.15
description Wi-Fi
encapsulation dot1Q 15
ip address 180.24.2.1 255.255.255.0
ip helper-address 172.10.1.2
!
interface GigabitEthernet0/1/0.20
description Voice
encapsulation dot1Q 20
ip address 180.24.3.1 255.255.255.0
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 180.24.0.0
network 204.46.25.0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list standard VTY
permit host 188.124.10.1
!
banner motd ^CAccess for administrators only. Enter password:^

```

```
!  
!  
!  
!  
dial-peer voice 1 voip  
destination-pattern 0...  
session target ipv4:172.10.4.1  
!  
dial-peer voice 2 voip  
destination-pattern 1...  
session target ipv4:174.10.3.1  
!  
dial-peer voice 3 voip  
destination-pattern 2...  
session target ipv4:175.10.3.1  
!  
dial-peer voice 4 voip  
destination-pattern 3...  
session target ipv4:176.10.3.1  
!  
telephony-service  
max-ephones 15  
max-dn 15  
ip source-address 180.24.3.1 port 2000  
auto assign 1 to 15  
!  
ephone-dn 1  
number 5001  
!  
ephone-dn 2  
number 5002  
!  
ephone-dn 3  
number 5003  
!  
ephone-dn 4  
number 5004  
!  
ephone-dn 5  
number 5005  
!  
ephone-dn 6  
number 5006  
!  
ephone-dn 7  
number 5007  
!  
ephone-dn 8  
number 5008  
!  
ephone-dn 9  
number 5009  
!
```

```
ephone-dn 10
number 5010
!
ephone-dn 11
number 1811
!
ephone-dn 12
number 1812
!
ephone-dn 13
number 1813
!
ephone-dn 14
number 1814
!
ephone-dn 15
number 1815
!
ephone 1
device-security-mode none
mac-address 000A.F3E6.14B1
type 7960
button 1:1
!
ephone 2
device-security-mode none
mac-address 0001.6370.E0C5
type 7960
button 1:2
!
ephone 3
device-security-mode none
mac-address 0060.5C14.AB54
type 7960
button 1:3
!
ephone 4
device-security-mode none
mac-address 00E0.F9B5.735C
type 7960
button 1:4
!
ephone 5
device-security-mode none
mac-address 0003.E4BD.D5E0
type 7960
button 1:5
!
ephone 6
device-security-mode none
mac-address 0060.47A6.A97B
type 7960
button 1:6
```

```

!
ephone 7
device-security-mode none
mac-address 0090.0CB1.8241
type 7960
button 1:7
!
ephone 8
device-security-mode none
mac-address 0090.0C34.2BBB
type 7960
button 1:8
!
ephone 9
device-security-mode none
mac-address 0060.3E53.D6DB
type 7960
button 1:9
!
ephone 10
device-security-mode none
mac-address 000A.4116.9EA0
type 7960
button 1:10
!
line con 0
!
line aux 0
!
line vty 0 4
access-class VTY in
password WareHou1024
login
!
!
ntp server 172.10.1.3
!
end

```

Лістинг В.2 — Команди налаштування комутатора складу підприємства

```

hostname WSwitch
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1

```

```
switchport access vlan 10
!
interface FastEthernet0/2
switchport access vlan 10
!
interface FastEthernet0/3
switchport access vlan 10
!
interface FastEthernet0/4
switchport access vlan 10
!
interface FastEthernet0/5
switchport access vlan 10
!
interface FastEthernet0/6
switchport access vlan 10
!
interface FastEthernet0/7
switchport access vlan 10
!
interface FastEthernet0/8
switchport access vlan 10
!
interface FastEthernet0/9
switchport access vlan 10
!
interface FastEthernet0/10
switchport access vlan 10
!
interface FastEthernet0/11
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/12
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/13
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/14
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/15
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/16
switchport access vlan 10
switchport voice vlan 20
!
```

```
interface FastEthernet0/17
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/18
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/19
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/20
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/21
switchport access vlan 10
switchport voice vlan 20
!
interface FastEthernet0/22
switchport access vlan 5
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
switchport access vlan 15
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end
```

ДОДАТОК Г

Лістинг Г.1 — Команди налаштування центрального маршрутизатора

```

hostname CentRouter
!
!
!
enable secret 5 $1$mERr$gfaQwBGkoudbaLXHM.yRG1
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX1017FC4D-
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/0
ip address 188.124.10.2 255.255.255.252
!
interface GigabitEthernet0/1/0

```

```

ip address 190.144.10.1 255.255.255.252
!
interface GigabitEthernet0/2/0
ip address 192.128.5.1 255.255.255.252
!
interface GigabitEthernet0/3/0
ip address 204.46.25.1 255.255.255.252
!
interface GigabitEthernet1/0/0
ip address 194.156.11.1 255.255.255.252
!
interface GigabitEthernet1/1/0
ip address 109.74.225.1 255.255.255.224
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 109.0.0.0
network 188.124.0.0
network 190.144.0.0
network 192.128.5.0
network 194.156.11.0
network 204.46.25.0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list standard VTY
permit host 188.124.10.1
!
banner motd ^CAccess for administrators only. Enter password:^C
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
access-class VTY in
password CentRou5584
login
!
!
ntp server 172.10.1.3
!
end

```

ДОДАТОК Д

Лістинг Д.1 — Команди налаштування файрволу 5506-х

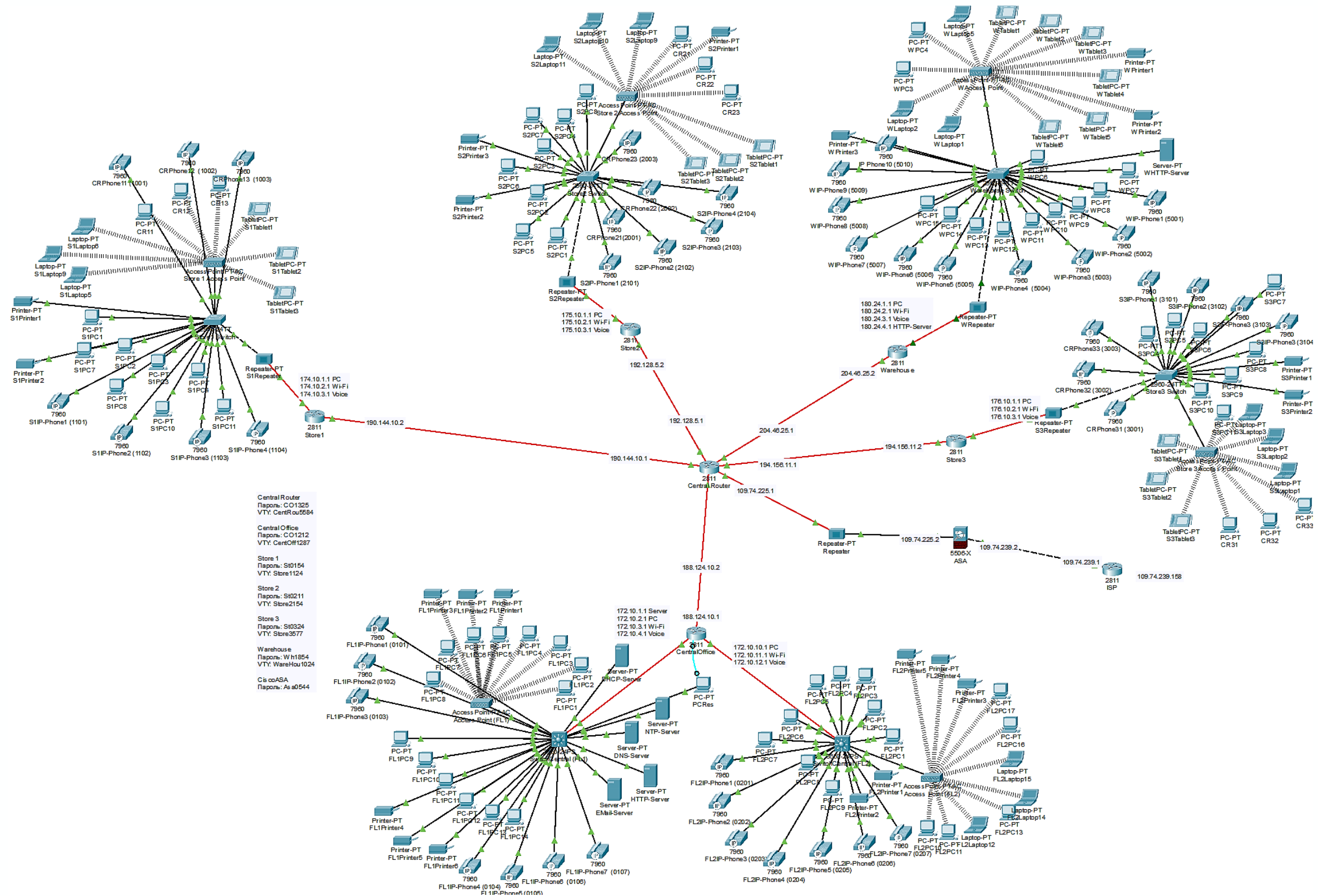
```
ASA Version 9.6(1)
!
hostname ciscoasa
enable password Zvn3e1PiXefMxhv3 encrypted
names
!
interface GigabitEthernet1/1
nameif inside
security-level 100
ip address 109.74.225.2 255.255.255.252
!
interface GigabitEthernet1/2
nameif outside
security-level 0
ip address 109.74.239.2 255.255.255.252
!
interface GigabitEthernet1/3
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/4
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/5
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/6
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/7
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/8
```

```

no nameif
no security-level
no ip address
shutdown
!
interface Management1/1
management-only
no nameif
no security-level
no ip address
shutdown
!
!
route outside 0.0.0.0 0.0.0.0 109.74.239.1 1
!
!
!
!
!
class-map inspection_default
match default-inspection-traffic
class-map inspection
match default-inspection-traffic
class-map inspection_defaukt
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect icmp
inspect tftp
policy-map global
class inspection
inspect icmp
!
service-policy global_policy global
!
telnet timeout 5
ssh timeout 5
!
!
!
!
router rip
version 2
network 109.0.0.0
!

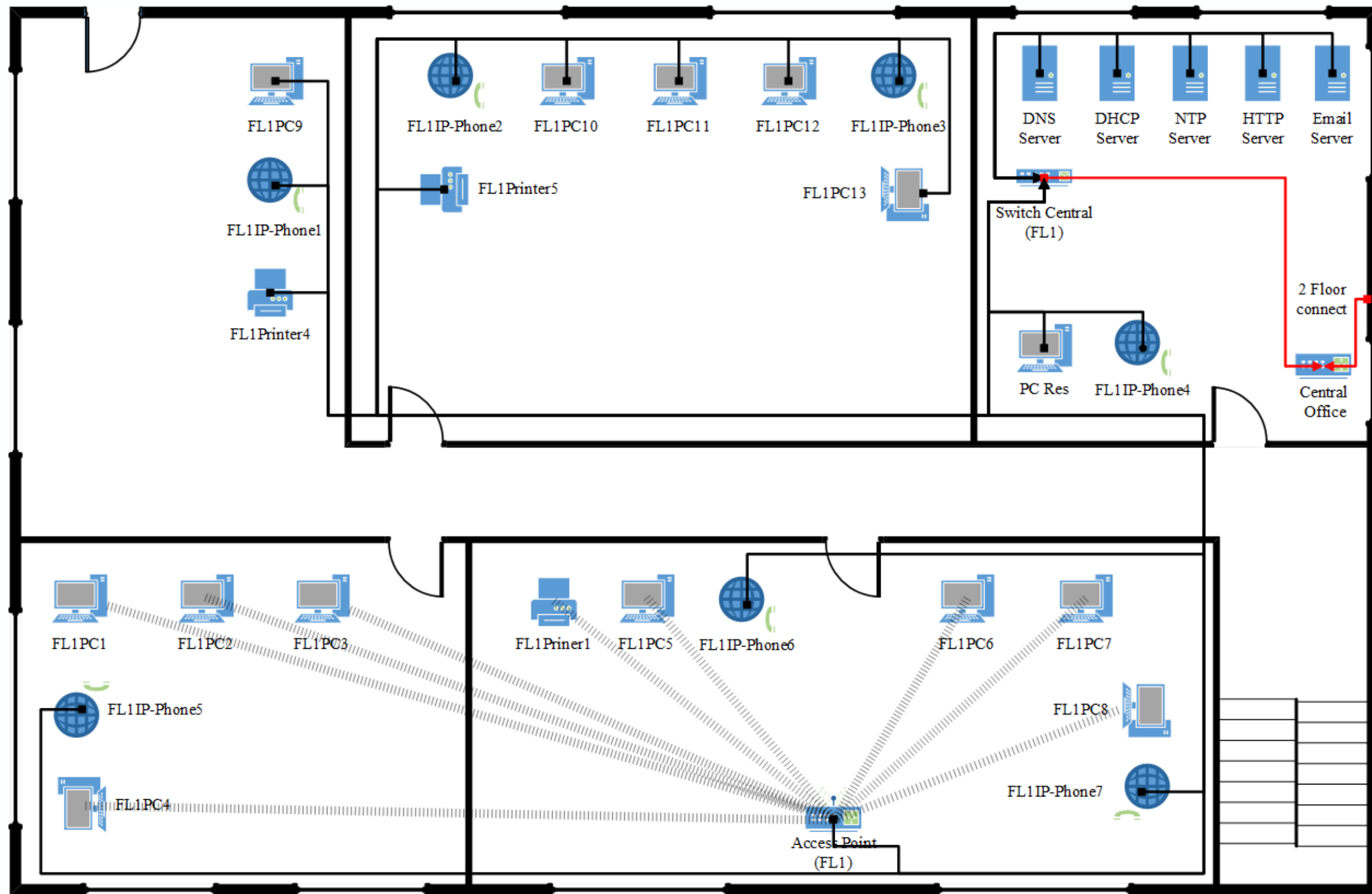
```

Функціональна схема мережі



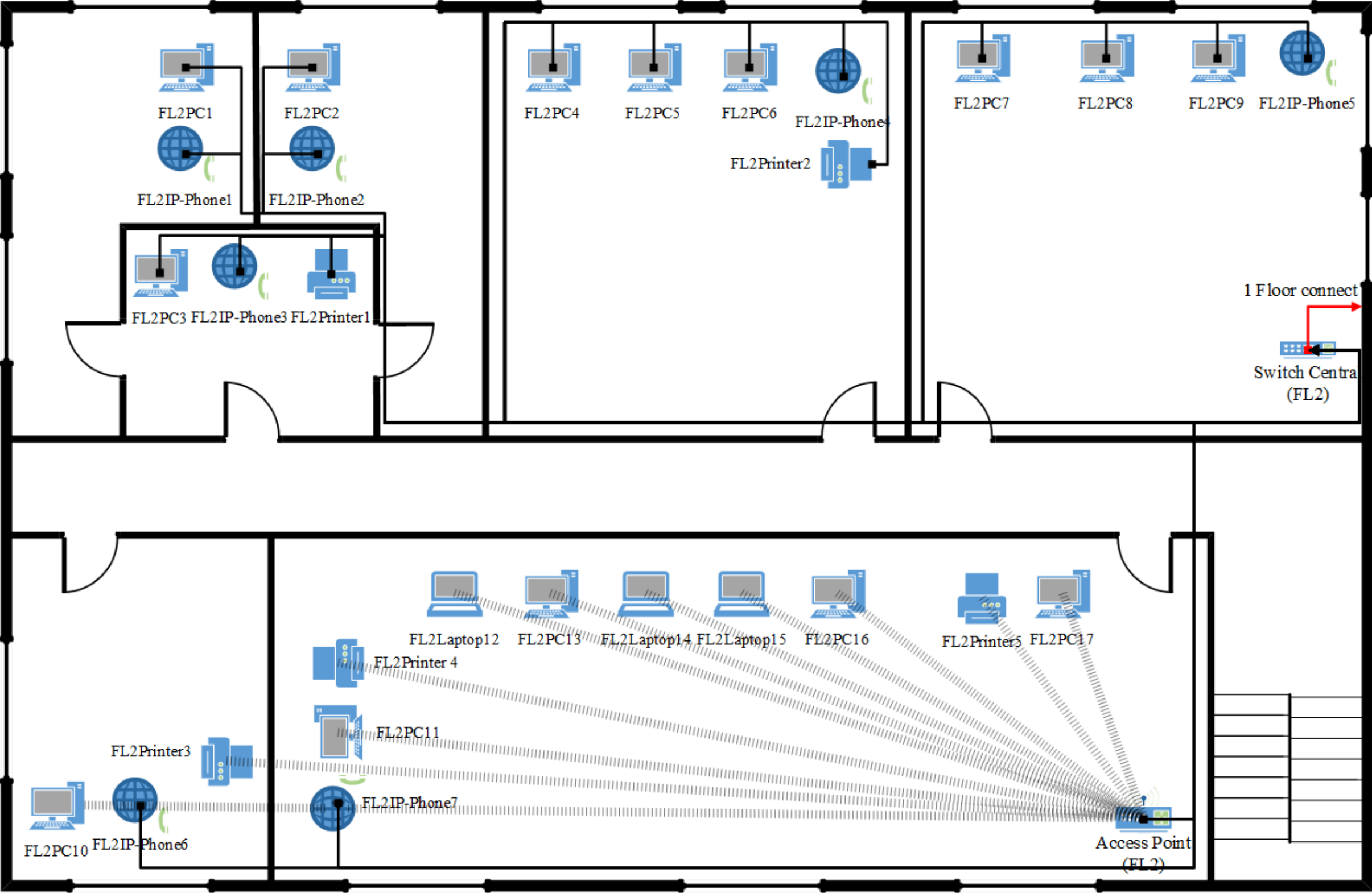
						13.02070849.51912 ПЛ1					
						Розробка корпоративної комп'ютерної мережі приватного підприємства "ЗапоріжБуд". Функціональна схема мережі	Лист.		Маса	Масшт.	
Зам.	Лист.	№ докум.	Підп.	Дата							
Розроб.		Лавренов І.О.									
Перев.		Грушко С.С.									
Т.контр.							Лист 1		Листів 1		
Н.контр.		Щербак Н.В.					НУ «Запорізька політехніка»				
Затв.		Кудерметов Р.К.					КНТ-519				

Монтажна схема головного офісу (1 поверх)



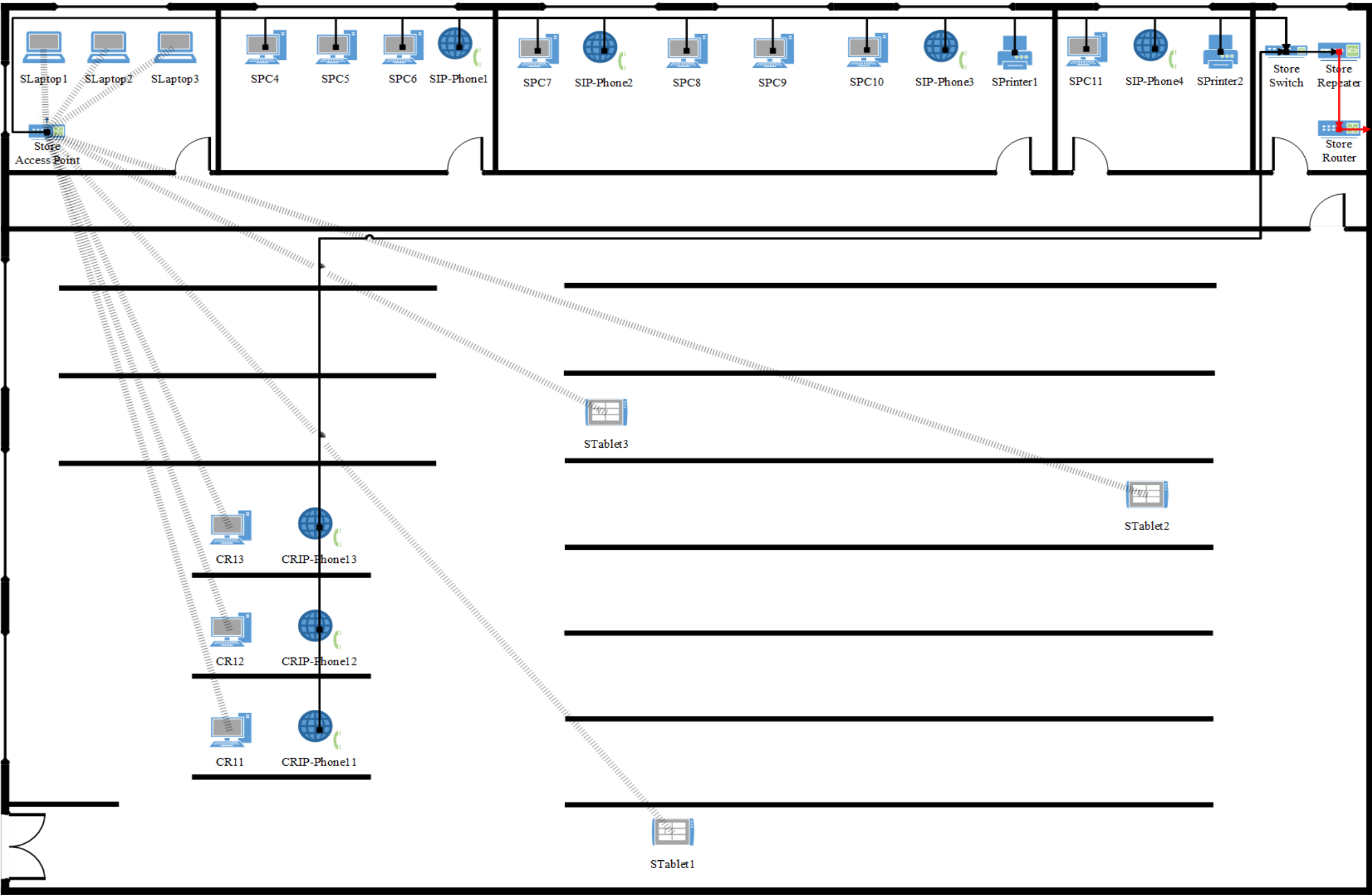
						13.02070849.51912 ПЛ2					
						Розробка корпоративної комп'ютерної мережі приватного підприємства "ЗапоріжБуд". Монтажна схема головного офісу (1 поверх)	Лист.		Маса	Масшт.	
Зам.	Лист.	№ докум.	Підп.	Дата							
Розроб.		Лавренко І.О.									
Перев.		Грушко С.С.									
Т.контр.							Лист 1		Листів 1		
							НУ «Запорізька політехніка» КНТ-519				
Н.контр.		Щербак Н.В.									
Затв.		Кудерметов Р.К.									

Монтажна схема головного офісу (2 поверх)



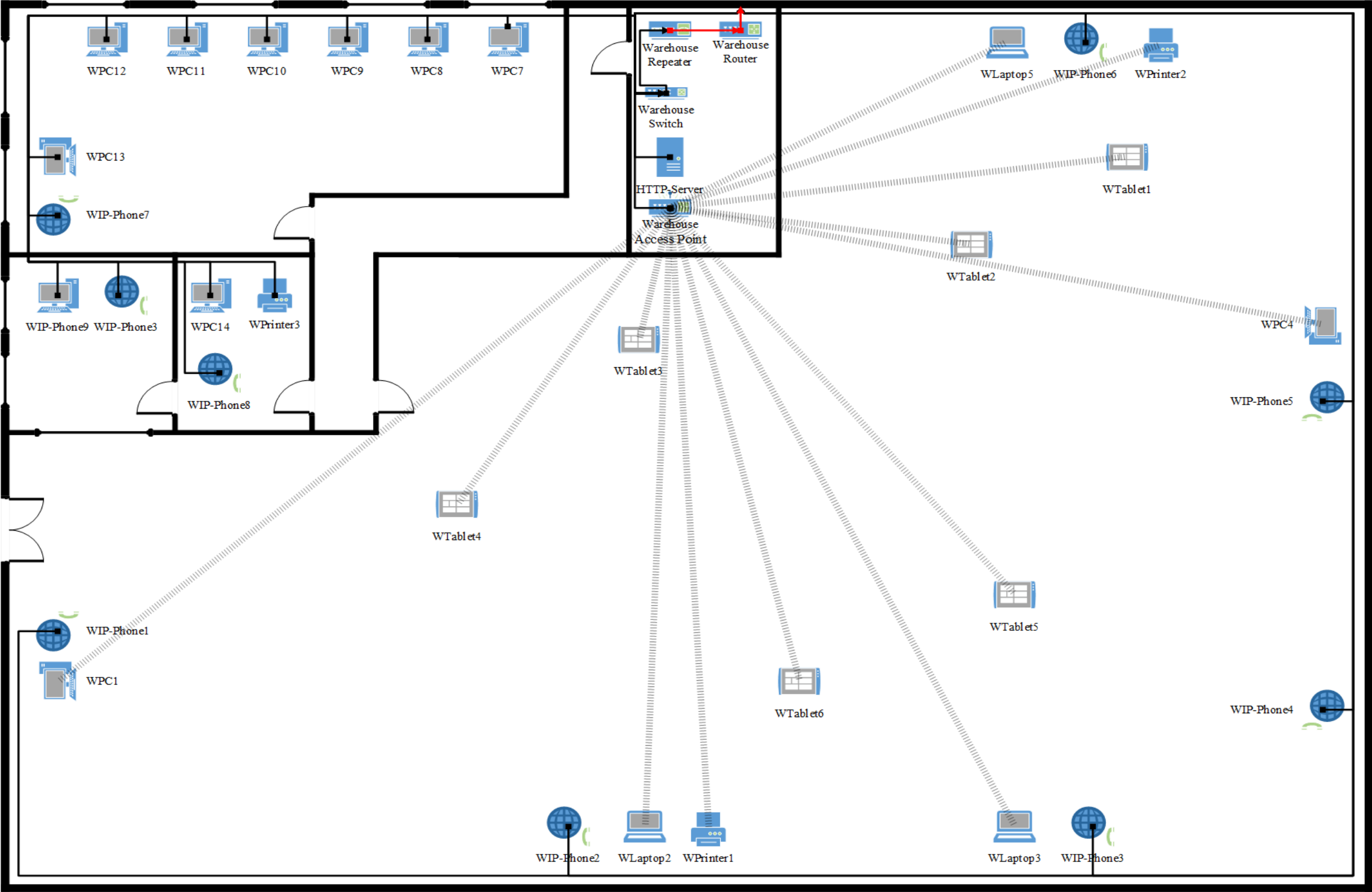
						13.02070849.51912 ПЛЗ					
						Розробка корпоративної комп'ютерної мережі приватного підприємства "ЗапоріжБуд". Монтажна схема головного офісу (2 поверх)	Лист.		Маса	Масшт.	
Зам.	Лист.	№ докум.	Підп.	Дата							
Розроб.		Лавренюк І.О.									
Перев.		Грушко С.С.									
Т.контр.							Лист 1		Листів 1		
Н.контр.		Щербак Н.В.				НУ «Запорізька політехніка» КНТ-519					
Затв.		Кудерметов Р.К.									

Монтажна схема магазинів



					13.02070849.51912 ПЛ4							
					Розробка корпоративної комп'ютерної мережі приватного підприємства "ЗапоріжБуд". Монтажна схема магазинів	Лист.			Маса		Масшт.	
Зам.	Лист.	№ докум.	Підп.	Дата								
Розроб.		Лавренів І.О.										
Перев.		Грушко С.С.										
Т.контр.						Лист 1			Листів 1			
Н.контр.		Щербак Н.В.				НУ «Запорізька політехніка» КНТ-519						
Затв.		Кудерметов Р.К.										

Монтажна схема складу підприємства



					13.02070849.51912 ПЛ5									
					Розробка корпоративної комп'ютерної мережі приватного підприємства "ЗапоріжБуд". Монтажна схема складу підприємства	Лист.			Маса			Масшт.		
Зам.	Лист.	№ докум.	Підп.	Дата										
Розроб.		Лавренов І.О.												
Перев.		Грушко С.С.												
Т.контр.														
						Лист 1			Листів 1					
Н.контр.		Щербак Н.В.				НУ «Запорізька політехніка»								
Затв.		Кудерметов Р.К.				КНТ-519								