Міністерство освіти і науки України

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

Відділення телекомунікацій та електронних систем
(назва відділення)

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
до кваліфікаційної роботи

бакалавра
(освітній ступінь)

на тему: Розробка проєкту комп'ютерної мережі для приватного підприємства «UNGAS Smart»

Виконав: студент VI курсу, групи КІб-602

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

Богдан ГЕВКО
(ім'я та прізвище)

Керівник Андрій ЛЯПАНДРА
(ім'я та прізвище)

Рецензент
(ім'я та прізвище)

Тернопіль – 2025

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ТЕРНОПІЛЬСЬКИЙ ФАХОВИЙ КОЛЕДЖ
ТЕРНОПІЛЬСЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
імені ІВАНА ПУЛЮЯ»

Відділення телекомунікацій та електронних систем
Циклова комісія комп'ютерної інженерії
Освітній ступінь бакалавр
Освітньо-професійна програма: Комп'ютерна інженерія
Спеціальність: 123 Комп'ютерна інженерія
Галузь знань: 12 Інформаційні технології

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"___" _____ 2025 року

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

Гевку Богдану Васильовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Розробка проєкту комп'ютерної мережі для приватного підприємства «UNGAS Smart»

керівник роботи Ляпандра Андрій Степанович
(прізвище, ім'я, по батькові)

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університетут імені Івана Пулюя» від 05 травня. 2025 р №4/9-217

2. Строк подання студентом роботи: 20 червня 2025 року.

3. Вихідні дані до роботи: плани приміщень, вимоги та рекомендації від замовника, стандарти побудови СКС, документація на мережеве обладнання і сервери

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Загальний розділ. Розробка технічного та робочого проєкту. Спеціальний розділ. Економічний розділ. Безпека життєдіяльності, основи охорони праці.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
   - План приміщень
   - Логічна топологія
   - Фізична топологія
   - Таблиця IP-адрес
   - Таблиця техніко-економічних показників
   - Модель мережі

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Оксана РЕДЬКВА заст. директора з НВР		
Охорона праці, техніка безпеки та екологічні вимоги	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	08.05	
2	Збір і узагальнення інформації	20.05	
3	Написання першого розділу	23.05	
4	Розробка технічного та робочого проекту	28.05	
5	Написання спеціального розділу	3.06	
6	Розрахунок економічної частини	5.06	
7	Написання розділу охорони праці	6.06	
8	Виконання графічної частини	10.06	
9	Оформлення проекту	13.06	
10	Погодження нормоконтролю	17.06	
11	Попередній захист роботи	20.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 8 травня 2025 року

Студент _____ Богдан ГЕВКО
(підпис) (ім'я та прізвище)

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

АНОТАЦІЯ

У кваліфікаційній роботі розглядається процес створення комп’ютерної мережі для приватного підприємства «UNGAS Smart». Головною метою є розробка ефективної мережевої інфраструктури для підприємства. Для реалізації поставленої задачі у роботі викладено п’ять основних розділів, у яких детально описані всі етапи виконаних робіт.

У першому розділі визначено завдання проектування, наведені вимоги до мережі, її структури та тестування, а також описана організаційна структура підприємства.

Другий розділ присвячений вибору технології, топології та мережевого обладнання, необхідних для створення мережі.

У третьому розділі детально розглядається обладнання, що підлягає налаштуванню, та основні аспекти його конфігурації.

Четвертий розділ містить розрахунки, проведені для спроектованої мережі.

П’ятий розділ присвячено питанням безпеки життєдіяльності та охорони праці, що мають враховуватися під час розробки та експлуатації мережі.

Обсяг пояснювальної записки становить 89 аркуші формату А4.

Графічна частина виконана на 5 плакатах формату А3.

ANNOTATION

The qualification work examines the process of creating a computer network for the private enterprise «UNGAS Smart». The main goal is to develop an effective network infrastructure for the enterprise. To implement the task, the work contains five main sections, which describe in detail all the stages of the work performed.

The first section defines the design tasks, outlines the requirements for the network, its structure and testing, and describes the organizational structure of the enterprise.

The second section is devoted to the selection of technology, topology, and network equipment required to create a network.

The third section examines in detail the equipment to be configured and the main aspects of its configuration.

The fourth section contains calculations performed for the designed network.

The fifth section is devoted to issues of life safety and occupational health and safety that must be taken into account during the development and operation of the network.

The volume of the explanatory note is 89 sheets of A4 format.

The graphic part is made on 5 posters of A3 format.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

CLI – Command Line Interface;

ISO – International Standarts Organization;

LAN – Local Area Network;

RAID – Redundant Array of Independent Disks;

STP – Shielded Twisted Pair;

TCP/IP – Transmission Control Protocol/ Internet Protocol;

UTP – Unshielded twisted pair;

VLAN – Virtual Local Area Network;

ДБЖ – джерело безперебійного живлення;

ОС – операційна система;

ПК – персональний комп’ютер;

ПП – приватне підприємство;

СКС – структурована кабельна система.

ВСТУП

За допомогою локальної мережі можна ефективно організувати роботу великої кількості комп’ютерів, забезпечити централізоване адміністрування, високий рівень захисту даних та антивірусну безпеку. Використання персональних комп’ютерів у складі мережевої інфраструктури є обов’язковим елементом функціонування будь-якого підприємства чи установи. Таке об’єднання техніки сприяє спільній діяльності співробітників, що має важливе значення в умовах сучасних вимог до організації праці.

Мережі, що використовуються у підприємствах та організаціях, забезпечують можливість спільної роботи працівників, які у своїй діяльності користуються як локальними ресурсами, так і послугами Інтернету. Застосування різних видів мережевих рішень, у тому числі провідних і бездротових, сприяє підвищенню ефективності обробки даних та раціональному використанню мережевих ресурсів усіма підключеними комп’ютерами та пристроями. Це створює умови для зручного обміну інформацією, спільної роботи над завданнями, взаємного доступу до даних і сервісів, а також для підключення до централізованих систем технічної підтримки. Усі ці можливості позитивно впливають на організацію робочого процесу та сприяють підвищенню продуктивності праці.

Отже робота над побудовою та налаштуванням комп’ютерної мережі є актуальною, оскільки вона забезпечує ефективну взаємодію працівників, безперервний обмін даними, централізоване управління ресурсами та високий рівень захисту інформації. Надійна мережа сприяє стабільності бізнес-процесів і підвищенню продуктивності діяльності будь-якої організації.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Темою кваліфікаційної роботи є розробка проєкту комп’ютерної мережі для приватного підприємства «UNGAS Smart».

Проект стосується побудови структурованої локальної комп’ютерної мережі в офісному приміщенні підприємства, що спеціалізується на розробці, впровадженні та технічному супроводі програмного забезпечення. Розробка в цілому або окремі її частини можуть бути використані керівництвом організації.

1.1.2 Призначення розробки

Проектована локальна комп’ютерна мережа має на меті інтеграцію робочих комп’ютерів підприємства в єдину інформаційну систему, що забезпечує колективне користування периферійним обладнанням, зокрема принтерами, централізований доступ до файлів, сервісів та вихід у глобальну мережу Інтернет. Усі користувачі локальної мережі повинні мати можливість взаємодії з основним сервером, який виконує функції управління правами доступу, адміністрування спільних ресурсів і контролю трафіку в середині мережі.

Побудова мережевої інфраструктури здійснюється з урахуванням внутрішнього планування офісних приміщень. Окрему увагу приділено питанням інформаційної безпеки.

Загалом мережа має забезпечити високу швидкодію, надійність, гнучкість масштабування та захищеність усіх компонентів корпоративної IT-інфраструктури.

1.1.3 Вимоги до апаратного та програмного забезпечення

Комп'ютерну мережу можна умовно поділити на апаратну і програмну складові. До апаратної складової належать: кабелі, роз'єми, мережеві плати, комутатори, сервери та інше обладнання, програмна складова включає операційні системи серверів та комутаційного обладнання. [1]

Комутаційне обладнання, яке використовується у складі локальної комп’ютерної мережі, повинно забезпечувати [1]:

– стабільне підключення всіх клієнтських пристроїв у мережі;

– безперебійну роботу впродовж щонайменше п’яти років за умови належного технічного обслуговування;

– швидкість обміну даними між користувачами мережі на рівні 1 Гбіт/с;

– зовнішній канал із пропускною спроможністю не менше 40 Мбіт/с для виходу до Інтернету;

– можливість візуального контролю працездатності обладнання (світлодіодна індикація стану);

– інструменти для моніторингу трафіку та керування потоками даних;

– захищеність переданих у мережі даних;

– централізоване зберігання робочої та службової інформації;

– можливість подальшого розширення мережі без повної її перебудови.

Програмні засоби, встановлені на серверах і комп’ютерах локальної мережі, мають надавати такі функції: [1]

– доступ усіх користувачів до спільного файлового сховища;

– чітке розмежування рівнів доступу для різних категорій працівників;

– контроль стану каналів зв’язку та спостереження за їх стабільністю.

Серед основних вимог до побудови такої мережі можна виділити: високу надійність, стабільну роботу, можливість подальшого розширення.

1.1.4 Вимоги до документації

Для забезпечення стабільної роботи локальної мережі, а також для оперативної діагностики та усунення можливих технічних несправностей, необхідно сформувати відповідний комплект технічної документації, який включає [1]:

1. Схематичне зображення топології мережі — графічні діаграми із зазначенням ключових вузлів мережі, способів їх взаємодії та маршрутів передавання даних.

2. Деталізовані відомості про серверне обладнання, включаючи найменування, функціональне призначення, IP-адресацію, конфігурацію накопичувачів, встановлені операційні системи та інші важливі параметри.

3. Призначення портів активного мережевого обладнання — опис конфігурації підключення до глобальної мережі, використаних VLAN, відповідність портів конкретним пристроям або службам.

4. Налаштування ключових мережевих сервісів, що забезпечують повноцінну роботу інфраструктури.

5. Інформація щодо політик доступу та користувацьких профілів — перелік категорій користувачів, встановлені для них права доступу, обмеження, а також методи автентифікації та авторизації.

6. Опис критичних програмних компонентів, які використовуються у діяльності підприємства.

1.1.5 Техніко-економічні показники

Техніко-економічні характеристики, наведені в кваліфікаційній роботі, узагальнюють ключові параметри, що визначають ефективність і доцільність впровадження локальної комп’ютерної мережі на підприємстві.

Розглянемо основні параметри:

– швидкість передачі даних по безпровідній мережі – 100 Мбіт/с.

– швидкість передачі даних в локальній мережі – 1 Гбіт/с;

– можливість для встановлення додаткових робочих місць ;

– доступ до глобальної мережі Інтернет;

– повна вартість мережі – 603465,55 грн.

1.1.6 Стадії та етапи розробки

Впровадження проекту локальної мережі повинно здійснюватися поетапно, з дотриманням логічної послідовності дій. Основні етапи реалізації включають [1]:

1. Оцінювання потреб підприємства у комунікаціях з урахуванням наявної IT-інфраструктури та рівня реалізованих рішень.

2. Проектування логічної структури мережі .

3. Техніко-економічне обґрунтування та вибір мережевого обладнання, яке задовольняє вимоги щодо продуктивності, вартості та масштабованості.

4. Урахування особливостей планування приміщень.

5. Створення схеми фізичного розміщення обладнання і прокладання кабельних трас, враховуючи зручність монтажу та обслуговування.

6. Дослідження технічних нюансів встановлення окремих мережевих елементів із визначенням специфіки монтажу.

7. Конфігурування апаратної частини і встановлення необхідного програмного забезпечення для забезпечення повноцінної функціональності мережі.

8. Проведення тестування побудованої системи з метою перевірки працездатності та усунення можливих помилок.

1.1.7 Порядок контролю та прийому

Перед тим як мережу буде введено в експлуатацію, проводиться її остаточне випробування. Особливу увагу на цьому етапі приділяють перевірці всіх змонтованих кабельних трас. Під час тестування здійснюється комплексний контроль стану кабельної інфраструктури: перевіряється цілісність усіх прокладених ліній, уточнюється правильність маркування, а також усуваються можливі технічні похибки або недоліки, що виникли на етапі монтажу. Крім того, проводиться паспортизація всієї кабельної системи згідно з встановленими вимогами.

Після завершення перевірки кабельних сегментів здійснюється додатковий контроль якості електроживлення обладнання. Зокрема, перевіряється правильність подачі напруги на активні комутатори, сервери та клієнтські машини, а також оцінюється коректність налаштування конфігурацій мережевих пристроїв, операційних систем та серверного середовища. Якщо всі випробування пройдено успішно, і помилок або критичних відхилень не зафіксовано, учасники, відповідальні за проведення контрольних процедур, складають відповідний акт завершення робіт, що підтверджує готовність системи до повноцінної експлуатації.

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

Приватне підприємство «UNGAS Smart» здійснює діяльність у сфері створення, розвитку та підтримки програмного забезпечення для підприємств, установ та організацій різних напрямів. Основною метою проекту є інтеграція робочих місць усіх підрозділів компанії в єдину інформаційно-технологічну мережу для ефективної внутрішньої взаємодії.

Передбачається впровадження локальної мережевої інфраструктури, яка забезпечуватиме безперервний зв’язок між комп’ютерами, що розташовані в різних офісах та кабінетах. Крім того, планується організація стабільного доступу до ресурсів глобальної мережі Інтернет, що дозволить працівникам використовувати онлайн-сервіси та інструменти, необхідні для щоденної роботи.

Для зручнішого адміністрування та підвищення ефективності управління мережевими ресурсами було розроблено структуру, що передбачає поділ локальної мережі на кілька сегментів, які відповідають структурі підприємства «UNGAS Smart».

В структуру підприємства входять:

– відділ продажів;

– відділ закупівлі і перевірки обладнання;

– юристи;

– відділ кадрів

– головний бухгалтер;

– бухгалтерія;

– директор;

– офіс-менеджер;

– приймальня;

– технічний директор;

– керівник проєктів;

– відділ тестування;

– відділ сертифікації;

– відділ розробки ПЗ;

– відділ управління проєктами;

– два санвузли.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1. Опис та обґрунтування вибору логічного типу мережі

До початку побудови комп’ютерної мережі важливо визначити її логічну топологію, яка є одним із ключових елементів у проектуванні мережевої інфраструктури. Під логічною топологією розуміють схему організації обміну даними між мережевими пристроями, незалежно від їх фактичного фізичного розташування чи способу підключення. Іншими словами, це спосіб у який інформація передається між вузлами, що впливає на ефективність функціонування мережі. Вибір відповідної структури значною мірою залежить від масштабів мережі, її функціонального призначення, вимог до швидкодії та можливості масштабування [2].

На рисунку нижче (див. рис. 2.1) наведено найбільш типові варіанти організації логічної топології комп’ютерних мереж.

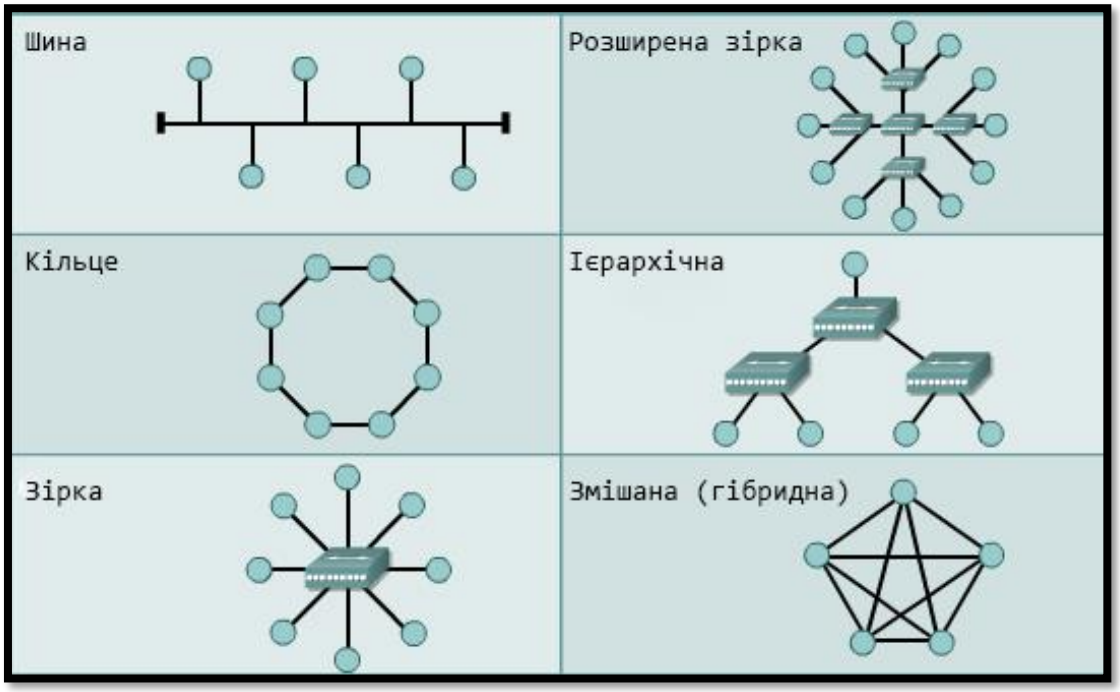


Рисунок 2.1 – Основні мережеві топології

Після вивчення організаційної структури ПП «UNGAS Smart» та врахування вимог до функціонування майбутньої комп’ютерної мережі, було прийнято рішення реалізувати дротовий сегмент мережі на основі топології «розширена зірка» з додатковим підключенням безпровідних сегментів мережі.

У випадку з архітектурою «розширеної зірки» (див. рис. 2.2), центральним елементом виступає головний комутатор, до якого підключаються інші мережеві вузли, а також допоміжні комутатори, які розширюють структуру мережі. Всі з’єднання утворюють мережеву конфігурацію, що нагадує зірку, проте з можливістю масштабування у кількох напрямках. Такий підхід добре підходить для приміщень зі складеним плануванням або тих, де мережа вже частково реалізована — наприклад, в офісах, навчальних класах, лікувально-діагностичних кабінетах або невеликих установах.

Ця модель забезпечує простоту керування, централізований контроль і дозволяє ефективно реалізувати короткі фізичні з’єднання між елементами мережі, що позитивно впливає на стабільність та швидкість передачі даних.

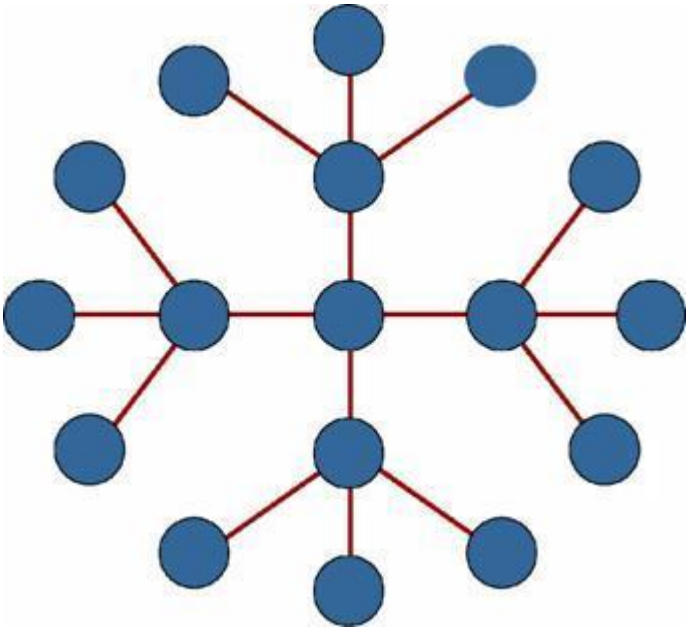


Рисунок 2.2 – Логічна топологія типу «розширена зірка»

Переваги розширеної зіркоподібної топології [2]:

– масштабованість, мережу легко розширити шляхом підключення нових вузлів або комутаторів без порушення роботи існуючої структури;

– контроль мережевого трафіку зосереджено через головний комутатор, що спрощує адміністрування;

– простота пошуку несправностей оскільки у разі відмови одного вузла або лінії, інші частини мережі продовжують працювати без перебоїв;

– можна адаптувати до різних планувань будівель і організаційних структур.

Недоліки розширеної зіркоподібної топології [2]:

– залежність від центрального вузла оскільки вихід з ладу головного комутатора призводить до відключення значної частини або всієї мережі;

– складніша прокладка кабелів оскільки у порівнянні з іншими топологіями потребує більше кабельної інфраструктури;

– вища вартість впровадження через використання кількох комутаторів, розгалужень і додаткового обладнання;

– потенційні затримки в мережі при великому навантаженні на центральний вузол можливе зниження продуктивності.

У процесі проектування сучасної комп’ютерної мережі важливим завданням є розмежування трафіку між різними логічними групами користувачів для підвищення безпеки, зменшення навантаження та оптимізації доступу до ресурсів. Одним із найбільш ефективних способів є впровадження віртуальних локальних мереж тобто VLAN [2].

VLAN це технологія, що дозволяє логічно розділити одну фізичну мережу на кілька ізольованих сегментів.

Структура поділу мережі на логічні сегменти наведена в таблиці 2.1. Мережна адресація, що використовується для налаштування мережевих пристроїв і вузлів, відображена в таблиці 2.2.

Таблиця 2.1 – Локальна адресація в мережі

Позначення вузлів	Кількість вузлів	Назва кабінету та його номер	Номер VLAN	Адрес підмержі/ Маска
WS_1 – WS_2	2	Відділ продажів	15	192.168.15.0/24
WS_3 – WS_4	2	Відділ закупівлі і перевірки обладнання	15	192.168.15.0/24
WS_5 – WS_ 6, PR_1	3	Юристи	20	192.168.20.0/24
WS_7 – WS_ 8	2	Відділ кадрів	25	192.168.25.0/24
WS_9, PR_2, SW_1, AP_1	4	Головний бухгалтер	30	192.168.30.0/24
WS_10 – WS_11, PR_3	3	Бухгалтерія	30	192.168.30.0/24
WS_12	1	Директор	35	192.168.35.0/24
WS_13, PR_4, AP_2	3	Офіс-менеджер	35	192.168.35.0/24
WS_14	1	Приймальня	40	192.168.40.0/24
WS_15	1	Технічний директор	45	192.168.45.0/24
WS_16	1	Керівник проєктів	50	192.168.50.0/24
WS_17 – WS_19, SW_ 2	4	Відділ тестування	55	192.168.55.0/24
WS_20 – WS_22	3	Відділ сертифікації	60	192.168.60.0/24
WS_23 – WS_28, AP_3, SW_3, S_1, S_2	10	Відділ розробки ПЗ	10	192.168.10.0/24
WS_29 – WS_30	2	Відділ управління проєктами	65	192.168.65.0/24

Таблиця 2.2 – Конфігурування груп VLAN

№ п/п	Позначення вузла	Назва мережевого пристрою	Номер порта	Тип порта	Номер VLAN
1	2	3	4	5	6
1	WS_1 – WS_2	SW_1	1-2	Access	15
2	WS_3 – WS_4	SW_1	3-4	Access	15
3	WS_5 – WS_6	SW_1	5-6	Access	20
4	PR_1	SW_1	7	Access	20
5	WS_7 – WS_8	SW_1	8-9	Access	25
6	WS_9	SW_1	10	Access	30
7	PR_2	SW_1	11	Access	30
8	AP_1	SW_1	12	Access	30
9	WS_10 – WS_11	SW_1	13-14	Access	30
10	PR_3	SW_1	15	Access	30
11	WS_12	SW_1	16	Access	35
12	PR_4	SW_1	17	Access	35
13	WS_13	SW_1	18	Access	35
14	AP_2	SW_1	19	Access	35
15	SW_1	SW_3	1	Trunk	30
16	WS_14	SW_2	1	Access	40
17	WS_15	SW_2	2	Access	45
18	WS_16	SW_2	3	Access	50
19	WS_17 – WS_19	SW_2	4-6	Access	55
20	WS_20 – WS_22	SW_2	7-9	Access	60
21	SW_2	SW_3	2	Trunk	55
22	WS_23 – WS_28	SW_3	3-8	Access	10
23	AP_3	SW_3	9	Access	10

Продовження таблиці 2.2.

1	2	3	4	5	6
24	S_1	SW_3	10	Access	10
25	S_2	SW_3	11	Access	10
26	WS_29 – WS_30	SW_3	12-13	Access	65

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з’єднань та їх прокладка

Мережеві кабелі є невід’ємною частиною апаратної інфраструктури комп’ютерних мереж. Вони слугують засобом фізичного з’єднання між мережевими пристроями — такими як комп’ютери, комутатори, маршрутизатори та інше обладнання — забезпечуючи передачу даних у межах мережі.

Кабельне з'єднання виконує роль каналу, яким інформація передається від одного пристрою до іншого. Вибір типу мережевого кабелю залежить від низки факторів: зокрема, обраної топології мережі, масштабу мережевого середовища та специфіки експлуатації. Тому тип кабелю, який використовується в конкретній інфраструктурі, має істотне значення для надійності, швидкодії та загальної ефективності роботи мережі, незалежно від галузі її застосування [3].

Кабелі типу «вита пара» є одним з найпоширеніших засобів передавання даних у комп’ютерних мережах, зокрема при прокладанні мереж на значні відстані. Особливість конструкції полягає в тому, що провідники скручені між собою це дозволяє значно зменшити вплив електромагнітних завад, які можуть виникати під час передавання сигналу.

Найбільш поширеними варіантами кабелів типу «вита пара» є STP та UTP (див рис.2.3). У цих скороченнях літера S вказує на наявність екранування, U — на його відсутність, а TP у обох випадках позначає скручування провідників у пари.

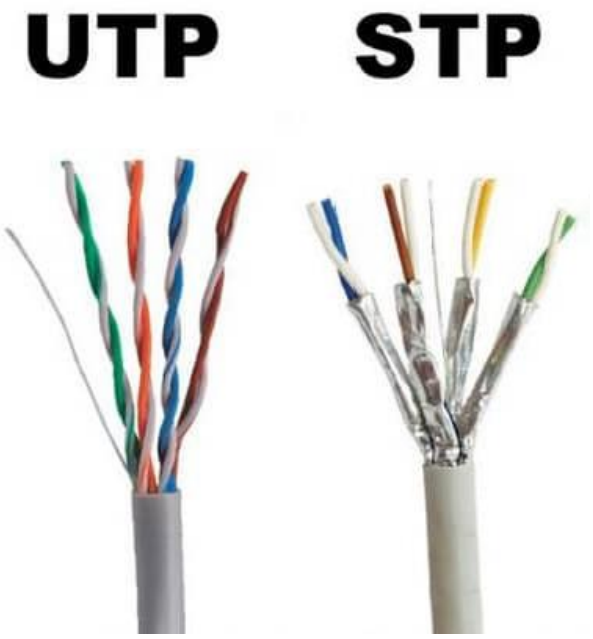


Рисунок 2.3 – Найбільш поширені кабелі типу «вита пара»

З урахуванням технічних вимог до побудови мережі було прийнято рішення використовувати неекранізовану виту пару (UTP).

Переваги неекранізованої витої пари [3]:

– низька вартість оскільки є найдешевшим варіантом серед мережевих кабелів;

– простота монтажу тому що він гнучкий, легкий у прокладці, не вимагає спеціального заземлення;

– популярність оскільки широко представлений на ринку, легко знайти кабелі потрібної категорії;

– сумісність зі стандартним обладнанням.

Недоліки неекранованої витої пари [3]:

– чутливість до електромагнітних перешкод та радіочастотних перешкод;

– обмежена відстань передачі сигналу;

– нижча пропускна здатність на великих відстанях.

2.2.2 Будова вузлів та необхідність їх застосування

Уся комп'ютерна техніка, що підлягає об'єднанню в єдину мережеву інфраструктуру, розташована в межах одного офісного приміщення. Ключовим принципом, який враховується при побудові мережі, є логічне розмежування трафіку шляхом поділу мережі на окремі сегменти за допомогою віртуальних локальних мереж (VLAN). Відомості про реалізацію цього підходу наведено у таблицях вище.

У результаті проектування було визначено, що мережа буде організована на основі трьох основних комутаційних вузлів. Один із них передбачається встановити у кабінеті головного бухгалтера, інший у відділі тестування, а третій вузол буде розміщено у відділі розробки програмного забезпечення.

Слід окремо підкреслити, що у відділі розробки програмного забезпечення передбачено встановлення двох серверних пристроїв. Один із них (S_1) виконуватиме функцію файлового сервера, який забезпечуватиме централізоване зберігання та доступ до внутрішніх даних компанії. Інший сервер (S_2) виконуватиме роль маршрутизуючого вузла, тобто буде використовуватися як мережевий шлюз, що забезпечуватиме вихід усіх робочих станцій підприємства до глобальної мережі Інтернет.

Підключення до Інтернету здійснюється через локальне з'єднання з провайдером, яке забезпечує доступ до зовнішнього трафіку для всієї організації.

2.3 Обґрунтування вибору обладнання для мережі (пасивного та активного)

Для впровадження локальної мережі на базі ПП «UNGAS Smart» необхідне використання активного і пасивного обладнання.

Для пасивного обладнання було використано:

– патч-панель на 24 порти (див. рис. 2.4);

– патч-корди категорії 6 UTP довжиною 0,5 м (див. рис. 2.5);

– патч-корди категорії 6 UTP довжиною 2 м (див. рис. 2.6);

– однопортова комп’ютерна розетка RJ-45, категорія 6 (див. рис. 2.7);

– двопортова комп’ютерна розетка RJ-45, категорія 6 (див. рис. 2.8);

– зовнішній настінний бокс для монтажу мережевого обладнання (див. рис. 2.9);

– підлогова серверна шафа (див рис. 2.10).

Рисунок 2.4 - Патч-панель на 24 порта

Рисунок 2.5 - Патч-корди категорії 6 UTP довжиною 0,5 м

Рисунок 2.6 - Патч-корди категорії 6 UTP довжиною 2 м

Рисунок 2.7 - Однопортова комп’ютерна розетка RJ-45, категорія 6

Рисунок 2.8 - Двопортова комп’ютерна розетка RJ-45, категорія 6

Рисунок 2.9 - Зовнішній настінний бокс для монтажу мережевого обладнання

Рисунок 2.10 - підлогова серверна шафа

Для активного обладнання було використано:

Обраний комутатор Cisco C1300-24P-4G (див. рис. 2.11) є оптимальним рішенням серед проаналізованих моделей завдяки поєднанню продуктивності, функціональності та енергоефективності. Комутатор підтримує розширені функції керування, безпеки та пріоритезації трафіку, що є важливим у середовищах з підвищеними вимогами до стабільності та надійності.

Попри те, що вартість цього комутатора може бути дещо вищою у порівнянні з альтернативними рішеннями, його функціональна насиченість, довготривала надійність та підтримка корпоративних протоколів безпеки повністю виправдовують вибір на користь даної моделі. Технічні характеристики та порівняння Cisco C1300-24P-4G з іншими аналогами наведено в таблиці А1 додатку А.

Рисунок 2.11 – Зовнішній вигляд Cisco C1300-24P-4G

Обрана модель Dell PowerEdge T40 v04 (див. рис. 2.12) була визначена як оптимальний варіант серед проаналізованих серверних рішень завдяки поєднанню високої продуктивності, стабільності та підтримки критично важливих функцій для офісного середовища. Сервер оснащений потужним процесором Intel Xeon, підтримує масштабовану оперативну пам’ять та має достатній обсяг внутрішніх накопичувачів для виконання широкого спектра завдань. Додатковою перевагою є вбудована підтримка RAID-масивів, що підвищує надійність зберігання даних. Характеристики обраної моделі та її порівняння з іншими аналогами подано в таблиці Б1 додатку Б.

Рисунок 2.12 – Зовнішній вигляд Dell PowerEdge T40 v04

Обраний комутатор Ubiquiti USW-24-POE Gen 2 (див. рис. 2.13) вирізняється серед інших розглянутих моделей завдяки розширеним функціональним можливостям і підтримці технології PoE на 16 з 24 портів. Це дозволяє живити мережеві пристрої без використання окремих джерел живлення, що значно спрощує інфраструктуру.

Попри помірну вартість, USW-24-POE Gen 2 забезпечує функціональність, яка на практиці перевищує деякі дорожчі аналоги, що робить цей комутатор доцільним вибором за критерієм ефективності витрат. Технічні характеристики та альтернативні варіанти комутаторів другого рівня, що розглядалися для порівняння, наведено в таблиці В1 додатку В.

Рисунок 2.13 – Зовнішній вигляд Ubiquiti USW-24-POE Gen 2

Обрана модель маршрутизатора TP-Link Archer AX80 (див. рис. 2.14) демонструє високий рівень продуктивності та функціональності, що робить її конкурентоспроможною серед представлених варіантів. Пристрій підтримує стандарти Wi-Fi 6 що забезпечує стабільне з’єднання та високу швидкість бездротової передачі даних у навантажених мережах.

З огляду на оптимальне поєднання вартості, технічних характеристик та зручності адміністрування, ця модель є вдалою альтернативою багатьом дорожчим маршрутизаторам, Порівняльні характеристики TP-Link Archer AX80 та його аналогів подано в таблиці Г1 додатку Г.

Рисунок 2.14 – Зовнішній вигляд Keenetic Giant

Обраний принтер HP LaserJet M211dw (див. рис. 2.15) обрано оптимальним варіантом серед розглянутих моделей завдяки балансу між

вартістю, швидкодією та функціональністю. Цей пристрій забезпечує високу якість монохромного друку, підтримує сучасні інтерфейси підключення, включно з Wi-Fi, USB та LAN, що дозволяє інтегрувати його в локальну мережу підприємства.

Серед важливих переваг також варто відзначити швидкість друку до 29 сторінок на хвилину, наявність лотка для 150 аркушів, компактний корпус і підтримку мобільного друку, що є корисним у динамічному офісному середовищі. Завдяки помірній вартості модель вигідно відрізняється на тлі аналогів, пропонуючи необхідний функціонал без надлишкових опцій.

Таким чином, HP LaserJet M211dw забезпечує стабільну роботу в мережевій інфраструктурі, високу продуктивність і мінімальні витрати на обслуговування, що робить його практичним вибором для використання в офісі. Порівняльні характеристики даного принтера та альтернативних моделей наведено в таблиці Д1 додатку Д.

Рисунок 2.15 – Зовнішній вигляд HP LaserJet M211dw

Обрана модель APC Smart-UPS 750VA 230V (див. рис. 2.16) є надійним джерелом безперебійного живлення серед розглянутих варіантів, що забезпечує до 500 Вт активної потужності. Цей показник дозволяє ефективно підтримувати роботу окремих серверів, мережевого обладнання або офісної техніки під час збоїв електропостачання, забезпечуючи короткочасну автономну роботу для безпечного завершення процесів і збереження даних.

Порівняльні характеристики даної моделі та її аналогів подано в таблиці Е1 додатку Е.

Рисунок 2.16 – Зовнішній вигляд APC Smart-UPS 750VA 230V

В підсумку для розробки комп'ютерної мережі потрібно використати пасивне та активне мережеве обладнання, яке наведене в таблиці 2.3.

Таблиця 2.3 – Використане активне та пасивне мережеве обладнання

№ п/п	Назва елемента	Позначення	Модель	Ціна, грн.	Од. виміру	Кількість
1	2	3	4	5	6	7
1	Серверна платформа	S_1, S_2	Dell PowerEdge T40 v04	30 000	шт.	2
2	Комутатор	SW_3	Cisco C1300- 24P-4G	36 400	шт.	1
3	Комутатор	SW_1, SW_2	Ubiquiti USW-24-Poe Gen2	14 550	шт.	2

Продовження таблиці 2.3.

1	2	3	4	5	6	7
4	Роутер	AP_1, AP_2, AP_3	TP-Link Archer AX80	7 200	шт.	3
5	ДБЖ	-	APC Smart-UPS 750VA 230V	31 500	шт.	2
6	Жорсткий диск 3.5, 2 ТВ	-	Toshiba	2 640	шт.	4
7	Патч панель 1U 24 порта	-	-	2 050	шт.	3
8	Вита пара U/UTP-cat.6, 305 м	-	-	5 340	шт.	4
9	Патч-корд Cat 6 UTP 0.5m	-	UTP	75	шт.	40
10	Патч-корд Cat 6 U/UTP 2m	-	UTP	120	шт.	35
11	Комп'ютерна розетка Rj-45 1xSTP, cat 6.	-	-	80	шт.	5
12	Комп'ютерна розетка Rj-45 2xSTP, cat 6.	-	-	120	шт.	20
13	Зовнішня шафа для мережевого обладнання	-	-	5700	шт.	1

Продовження таблиці 2.3.

1	2	3	4	5	6	7
17	Принтери	PR_1, PR_2, PR_3, PR_4	HP LaserJet M211dw	8 000	шт.	4
18	Кабельний організатор	-	-	200	шт.	3
19	Шафа серверна підлогова	-	-	16 300	шт.	1
20	Короб	-	40x25	53	м.	100
21	Короб	-	25x25	24	м.	150

2.4 Особливості монтажу мережі

Щоб забезпечити надійну роботу структурованої кабельної системи, важливо дотримуватися усіх технічних вимог під час виконання прокладання, обтискання та монтажу мережевих компонентів. Кожен з цих етапів має свої особливості, які необхідно враховувати. Для досягнення стабільної та якісної передачі даних слід звернути увагу на низку критичних технічних моментів, що впливають на ефективність функціонування всієї мережі.

1. Для прокладання кабельної інфраструктури доцільно використовувати якісні короби, які забезпечують як механічний захист, так і зручність обслуговування. Хоча з естетичної точки зору внутрішній (прихований) монтаж вважається привабливішим, у практичному сенсі зовнішнє розміщення кабелю типу «вита пара» у спеціалізованих коробах є значно ефективнішим. Такий підхід дозволяє мінімізувати ризик фізичних пошкоджень, а також спрощує доступ при обслуговуванні або заміні сегментів кабелю без необхідності демонтажу стінових покриттів [3].

2. Врахування зовнішнього вплив оскільки особливої уваги потребує прокладання неекранованих типів кабелів, які мають знижений рівень захисту від електромагнітних перешкод. Їх небажано розміщувати поряд із силовими лініями, обігрівальними приладами або іншими джерелами випромінювання, оскільки це може спричинити порушення якості передавання сигналу.

3. Контроль радіуса вигину кабелю оскільки вита пара (особливо екранована) є чутливою до надмірних вигинів. Під час прокладання потрібно враховувати мінімальний радіус вигину. Для неекранованих кабелів рекомендований радіус становить щонайменше 8 діаметрів, а для екранованих не менше 10 діаметрів кабелю, щоб уникнути пошкодження внутрішньої структури провідників.

4. Правильне виконання обтискання тому що монтаж конекторів має здійснюватися відповідно до чинних стандартів, з урахуванням типу обладнання, що підключається. Якщо йдеться про підключення комп'ютера до комутатора — використовується прямий обтиск. У випадку з'єднання двох однакових пристроїв між собою доцільним є перехресне обтискання.

Окрім базових технічних вимог, визначених документацією, при виконанні монтажу структурованої кабельної системи доцільно також враховувати розширені рекомендації, що надаються виробниками мережевого обладнання та компонентів. Ці поради є результатом практичного досвіду, тестувань і відповідають міжнародним стандартам якості, зокрема ISO/IEC 11801 та TIA/EIA-568, які регламентують проектування, інсталяцію й тестування структурованих систем. Такі рекомендації включають, зокрема, вибір правильного способу прокладання, використання сертифікованих монтажних матеріалів і дотримання допустимих параметрів вигину кабелю, розташування відносно джерел перешкод, а також способів кріплення ліній. Комплексне виконання цих порад сприяє збільшенню строку служби системи, зниженню частоти відмов і спрощенню подальшого обслуговування мережі [3].

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

Операційна система є фундаментальним програмним забезпеченням, що забезпечує взаємодію користувача з апаратним забезпеченням комп'ютера, а також керує ресурсами системи. В корпоративних мережах ОС виконує ключову роль у забезпеченні стабільної, безпечної та ефективної роботи всієї інфраструктури.

Основні функції операційної системи [4]:

1. Управління процесором і планування завдань: ОС виконує розподіл процесорного часу між одночасно працюючими процесами та потоками, забезпечуючи ефективне багатозадачне середовище. Використовуються алгоритми пріоритетного планування, кругового планування та інші.

2. Управління пам'яттю: ОС керує оперативною пам'яттю, виділяючи її процесам із застосуванням механізмів віртуальної пам'яті, сторінкової організації та сегментації. Це дозволяє ізолювати процеси і запобігати конфліктам доступу до пам'яті.

3. Файлова система: корпоративні ОС підтримують різні типи файлових систем (NTFS, ReFS у Windows; ext4, XFS, Btrfs у Linux), які забезпечують надійне зберігання даних, контроль доступу на рівні файлів та директорій, а також журналювання для захисту від пошкоджень.

4. Мережеві протоколи та служби: ОС підтримує стандартні протоколи TCP/IP, DHCP, DNS, LDAP, SMB, FTP, HTTP/S, що забезпечує інтеграцію з іншими системами та доступ до мережевих ресурсів.

5. Віртуалізація**:** корпоративні ОС підтримують гіпервізори (Hyper-V у Windows Server, KVM у Linux), що дозволяє створювати віртуальні машини для ефективного використання апаратних ресурсів і ізоляції служб.

6. Відновлення та резервне копіювання: ОС мають вбудовані інструменти для створення резервних копій системи та даних, а також механізми відновлення після збоїв (Windows Backup, Linux rsync, Bacula).

Беручи до уваги технічні характеристики комп'ютерного обладнання в різних офісах, специфіку діяльності співробітників компанії, рівень їхніх користувацьких навичок та необхідність диференціації доступу до мережевих ресурсів, можна зробити такі висновки:

1. У всіх відділах на персональних комп'ютерах буде інстальовано операційну систему Windows 10 Pro.

2. У серверному приміщенні на двох машинах буде встановлено Debian 11. Перший із цих серверів виконуватиме функції мережевого файлового сховища (файл-сервера). Другий сервер призначений для розгортання служби DNS, яка забезпечить організацію шлюзу для підключення всіх робочих станцій до Інтернету.

2.6 Тестування та налагодження мережі

Процес тестування та налагодження комп'ютерної мережі є невід'ємною складовою частиною її проектування і впровадження. Він дозволяє переконатися у тому, що всі компоненти мережі працюють коректно, відповідають технічним вимогам, а користувачі отримують стабільний і безпечний доступ до ресурсів. Ефективне тестування допомагає виявити помилки на ранніх стадіях, що значно знижує ризик виникнення збоїв у роботі мережі в подальшому.

На початковому етапі тестування необхідно провести ретельний візуальний огляд усіх елементів фізичної інфраструктури. Це включає перевірку кабелів, конекторів, розеток та обладнання на наявність механічних пошкоджень або дефектів монтажу. Важливо впевнитися, що кольорова схема

кабелів відповідає стандартам, а всі з’єднання виконані згідно з вимогами. Надійність фізичних з’єднань є базовою умовою для подальшої безперебійної роботи мережі.

Далі здійснюється перевірка цілісності кабельної системи за допомогою спеціальних тестерів (див. рис. 2.17), що дають змогу виявити обриви, короткі замикання, перехресні з’єднання та інші дефекти, які можуть негативно вплинути на якість передачі сигналу. Також вимірюється рівень загасання, який безпосередньо впливає на дальність та якість комунікації. Ці вимірювання допомагають переконатися, що фізична мережа відповідає технічним стандартам і здатна забезпечити необхідну пропускну здатність [3].

Рисунок 2.17 – Тестер кабельний LP-468N

Після успішного проходження фізичних тестів проводиться перевірка мережевих налаштувань. Це передбачає аналіз коректності призначення IP-адрес, масок підмереж, шлюзів за замовчуванням і серверів DNS на всіх клієнтських пристроях та серверах. Для цього застосовуються різноманітні утиліти, які дозволяють перевірити досяжність вузлів, відстежити маршрути проходження пакетів, а також отримати інформацію про налаштування мережевих інтерфейсів. Результати цих перевірок свідчать про те, що конфігурація мережі є правильною і забезпечує зв’язок між усіма її компонентами.

Особливу увагу під час тестування приділяють визначенню реальної пропускної здатності мережі. Для цього застосовуються спеціальні програми, які дозволяють виміряти швидкість передачі даних між двома вузлами, оцінити стабільність з’єднання та затримки у передачі пакетів. Результати таких тестів порівнюються із заявленими технічними характеристиками використовуваного обладнання, що дає змогу виявити проблеми, пов’язані з недостатньою пропускною здатністю чи перевантаженням окремих сегментів мережі [4].

Не менш важливою складовою є перевірка безпеки мережі. Сучасні корпоративні мережі піддаються численним загрозам, серед яких — несанкціонований доступ, атаки типу «відмова в обслуговуванні», віруси та інші шкідливі програми. Для оцінки захищеності системи проводять сканування відкритих портів, аналізують роботу служб і виявляють потенційно вразливі ділянки. Важливо також перевірити правильність налаштування політик контролю доступу, наявність шифрування каналів зв’язку та коректність налаштувань фаєрволів і систем виявлення вторгнень. Для цього застосовуються спеціалізовані утиліти, які дозволяють автоматизувати процес виявлення вразливостей і оперативно реагувати на потенційні загрози [4].

Після завершення тестування починається безпосередній процес налагодження мережі. Виявлені несправності фізичного рівня усуваються шляхом заміни пошкоджених кабелів або ремонту розеток, а також перевірки працездатності активного обладнання — комутаторів, маршрутизаторів та інших пристроїв. Важливо забезпечити коректне функціонування апаратних компонентів, адже навіть незначні фізичні дефекти можуть спричиняти втрату пакетів або падіння швидкості з’єднання.

Також у процесі налагодження здійснюється корекція конфігурації програмного забезпечення. Виправляються помилки у налаштуваннях IP-адресації, DHCP, DNS, а також здійснюється оптимізація маршрутизації, що може включати налаштування віртуальних локальних мереж (VLAN) для

розмежування трафіку між різними відділами чи групами користувачів. Важливо правильно налаштувати політики безпеки, включаючи правила файрволів, обмеження доступу до ресурсів і впровадження механізмів пріоритетизації трафіку що особливо актуально для забезпечення стабільної роботи критичних служб.

Таким чином, тестування та налагодження мережі це комплексна і безперервна діяльність, що вимагає системного підходу і застосування сучасних інструментів. Вона охоплює як технічні аспекти фізичної і логічної організації мережі, так і питання безпеки та продуктивності, що є критично важливими для успішної роботи будь-якої організації. Лише систематичне і ретельне виконання цих процедур може гарантувати стабільність, швидкість і безпеку корпоративної мережі, що відповідає сучасним вимогам інформаційної безпеки і бізнес-процесів.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкція з налаштування програмного забезпечення серверів

У рамках проектованої комп'ютерної мережі передбачається встановлення двох серверів. Перший з них – S_1 виконуватиме функції файл серверу підприємства. Другий сервер — S_2 буде використовуватись як шлюз до глобальної мережі Інтернет, а також забезпечуватиме функції маршрутизатора та мережевого екрана, що дозволить підвищити рівень захисту від несанкціонованих підключень. Виходячи з висновків, наведених у підрозділі 2.5, в якості операційної системи для обох серверів обрано Debian 11.

Далі у роботі буде детально описано послідовність налаштувань кожного з цих серверів відповідно до їх призначення. Спочатку встановимо операційну систему: необхідно завантажити відповідний ISO-образ дистрибутива та записати його на USB-накопичувач або інший завантажувальний носій. Після цього у налаштуваннях BIOS або UEFI слід встановити обраний носій як основне джерело завантаження, щоб під час запуску комп'ютера система почала інсталяцію саме з цього пристрою. Щоб змінити порядок завантаження, під час ввімкнення комп'ютера, на етапі появи стартового екрана (до запуску операційної системи), натисніть клавішу Delete або F2 — залежно від моделі материнської плати. Після відкриття меню BIOS чи UEFI необхідно вказати USB-накопичувач із записаним образом Debian як пріоритетний пристрій для завантаження.

Інструкція із встановлення Debian [6]:

Після запуску вам буде запропоновано обрати тип встановлення — з графічним середовищем або у текстовому режимі. Далі ми розглянемо процес інсталяції Debian з використанням графічного інтерфейсу. Виберіть мову встановлення та натисніть «Continue». На наступному етапі потрібно вказати

своє географічне розташування, що дозволить системі автоматично визначити часовий пояс. Також слід обрати потрібну клавіатурну розкладку. Після завершення кожного пункту слід натиснути «Continue». Після цих дій відбудеться дозавантаження необхідних образів із флешки.

Далі потрібно задати назву для вашого комп'ютера, вона буде використовуватись для його ідентифікації в мережевому середовищі. Ви можете ввести будь-яке ім'я, наприклад «debian». Якщо у вас є домен, введіть його на наступному кроці. У разі відсутності доменного імені це поле можна залишити порожнім. Після цього натисніть «Continue». На наступному кроці введіть root-пароль, повторіть його у полі нижче.

Далі система запропонує створити обліковий запис адміністратора. Спершу потрібно ввести ім'я користувача для системи, а потім задати ім'я для облікового запису, з якого здійснюватиметься вхід.

Далі знову відбудеться завантаження необхідних компонентів, а потім розмітка диска для установки дистрибутива де можна вибрати один із кількох варіантів. Вибираємо варіант автоматичного створення розділів по всьому диску. Далі потрібно визначити носій, на якому буде виконуватись розмітка. Вказуємо варіант, при якому всі дані зберігатимуться в одному розділі. Для підтвердження розмітки натискаємо відповідну кнопку, після чого зміни будуть записані на диск. Коли цей етап завершиться, установка основних компонентів системи «Debian» продовжиться автоматично. Наприкінці з'явиться запит щодо сканування ще одного носія — цю дію слід пропустити.

Далі потрібно вибрати дзеркало пакетів, вкажіть «deb.debian.org». У разі, наміру користуватися HTTP-проксі, на наступному етапі необхідно ввести відповідні дані. Якщо ж проксі не використовується, це поле можна залишити порожнім.

На наступному етапі відбудеться налаштування системи керування пакетами. Після цього з'явиться запит щодо участі у зборі статистичних даних

про найбільш уживані пакети. За небажання брати участь оберіть відповідну опцію. Далі процес інсталяції продовжиться і почнеться вибір і встановлення необхідного програмного забезпечення.

На цьому етапі потрібно обрати компоненти програмного забезпечення, які будуть інстальовані разом із системою. Відмітьте потрібні пункти та натисніть «Continue». Після завершення установки з’явиться запит на дозвіл інсталяції завантажувача «GRUB» погодьтеся та вкажіть диск, на який його буде встановлено. Через певний час система повідомить про успішне завершення встановлення. Натисніть «Continue» комп’ютер автоматично перезавантажиться. Після перезавантаження для входу до системи введіть свій логін і пароль, потім натисніть «Enter».

Інструкція із налаштування Debian [6]:

Оскільки інсталяція здійснювалась із зовнішнього носія, варто перевірити, чи доступні оновлення, і за потреби встановити їх. Щоб це зробити, виконайте наступні кроки. Через пошуковий рядок відкрийте програму «Термінал» і виконайте команду «su». Після цього введіть пароль який встановлювався раніше і виконайте по черзі команди:

apt-get update

apt-get upgrade

Виконайте перезавантаження через команду «reboot»

Рекомендується встановити утиліту «sudo», яка дозволяє надавати адміністративні привілеї окремим користувачам і спрощує доступ із правами уникнувши необхідності постійного введення пароля «root».

apt-get install sudo

Надаємо права користувачу

Adduser UserName sudo (UserName ім'я користувача, якому видаються права)

Shutdown -r now

Інструкція із налаштування репозиторія [6]:

Внесіть необхідні репозиторії до системної конфігурації, використовуючи команди:

security updates

deb http://security.debian.org/debian-security bellseye/updates main contrib non-free

deb-src http://security.debian.org/debian-security bellseye/updates main contrib non-free

binary and source packages

deb http://deb.debian.org/debian/ bellseye main contrib non-free

deb-src http://deb.debian.org/debian/ bellseye main contrib non-free

apt update

Інструкція із встановлення та запуску FTP-сервера – vsftpd [7] :

Здійснюємо підключення до сервера з облікового запису користувача з правами адміністратора, після чого вводимо наступні команди:

apt-get install vsftpd

sudo systemctl enable --now vsftpd

systemctl status vsftpd

На сервер S_2 який використовується для доступу до інтернету потрібно встановити проксі-сервер Squid.

Інструкція із встановлення проксі сервера [8]:

Щоб змінити конфігурацію локальної мережі або внести отримані від провайдера установки для підключення сервера до мережі Інтернет, необхідно відредагувати лише один файл конфігурації:

nano /etc/network/interfaces

auto eth0

iface eth0 inet dhcp

auto eth1

iface eth1 inet static

address 192.168.0.1

netmask 255.255.255.0

service networking restart

Після чого потрібно перевірити правильність конфігурування інтерфейсів:

Ifconfig

Отримані дані повинні мати приблизно наступний вигляд:

eth0 Link encap:Ethernet HWaddr 00:16:3c:fc:93:a6

inet addr:185.22.174.75 Bcast:185.22.174.255 Mask:255.255.255.0

inet6 addr: 2a00:1838:36:1c3::7385/64 Scope:Global

inet6 addr: fe80::216:3cff:fefc:93a6/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:7576291 errors:0 dropped:0 overruns:0 frame:0

TX packets:65851 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:628650171 (628.6 MB) TX bytes:10778431 (10.7 MB)

eth1

Link encap:Ethernet HWaddr 0a:19:bc:0d:00:9d

inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0

inet6 addr: fe80::819:bcff:fe0d:9d/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:12581 errors:0 dropped:0 overruns:0 frame:0

TX packets:8484 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:100

RX bytes:1884987 (1.8 MB) TX bytes:1123251 (1.1 MB)

Інструкція з встановлення і налаштування DHCP сервера [8]:

Встановлюємо DHCP-сервер за допомогою такої команди:

sudo apt-get install isc-dhcp-server

Далі відбувається мінімальне налаштування за допомогою команд:

```
# minimal sample /etc/dhcp/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.150 192.168.1.200;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "mydomain.example";
}
```

Інструкція з налаштування NAT:

Функції NAT реалізуються через мережевий фільтр iptables, який також виконує роль міжмережевого екрана. Щоб правила iptables автоматично застосовувалися під час завантаження системи, спочатку створимо порожній конфігураційний файл і потім відкриємо для редагування:

```
sudo touch /etc/nat
nano /etc/nat
```

Отримані дані повинні мати приблизно наступний вигляд:

```
#!/bin/sh
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -A FORWARD -i tap0 -o eth0 -j ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.0.1/24 -j
MASQUERADE
iptables -A FORWARD -i eth0 -m state --state ESTABLISHED,RELATED
-j ACCEPT
```

iptables -A FORWARD -i eth0 -o tap0 -j REJECT

chmod +x /etc/nat

Після цього слід забезпечити автоматичне виконання створеного файлу під час запуску сервера. Для цього відкриваємо файл «interfaces» і рядок:

nano /etc/network/interfaces

post-up /etc/nat

reboot

Інструкція з встановлення та налаштування Squid [9]:

Для початку встановлення потрібно використати команду:

apt-get install squid3

Після успішної інсталяції служба буде автоматично запущена. Щоб забезпечити зручність у подальшій роботі, рекомендується створити копію конфігураційного файлу в тій самій директорії під іншою назвою, це дозволить зберегти оригінальні налаштування для швидкого відновлення у разі потреби:

cp /etc/squid3/squid.conf /etc/squid3/backup-squid.conf

acl SSL_ports port 443

acl Safe_ports port 80 # http

acl Safe_ports port 21 # ftp

acl Safe_ports port 443 # https

acl Safe_ports port 70 # gopher

acl Safe_ports port 210 # wais

acl Safe_ports port 1025-65535 # unregistered ports

acl Safe_ports port 280 # http-mgmt

acl Safe_ports port 488 # gss-http

acl Safe_ports port 591 # filemaker

acl Safe_ports port 777 # multiling http

acl CONNECT method CONNECT

```
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localhost
http_access deny all
http_port 3128
coredump_dir /var/spool/squid3
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern (Release|Packages(.gz)*)$ 0 20% 2880
refresh_pattern . 0 20% 4320
```

За замовчуванням доступ до Squid дозволено лише з сервера Для надання доступу клієнтам із локальної мережі необхідно створити нове правило з параметром src, і дозволити доступ:

```
acl localnet src 192.168.0.0/24
http_access allow localnet
```

Зазначимо порт служби Squid і налаштуємо її на функціонування в прозорому режимі.

```
http_port 192.168.0.1:3128 intercept
```

Базове налаштування конфігураційного файлу Squid завершено, тож можна переходити до розгляду політик інформаційної безпеки. Параметр «src» використовується для керування доступом клієнтів із фіксованими IP-адресами:

```
acl UserGroup src 192.168.0.2-192.168.0.9
acl SingleUser src 192.168.0.10
http_access allow UserGrour
```

http_access allow SingleUser

http_access deny all

Параметр «dst» дає змогу задати список IP-адрес, до яких клієнт намагається встановити з'єднання. Щоб обмежити або дозволити доступ за доменним ім’ям, використовується параметр «dstdomain» він дозволяє вказати доменне ім’я, до якого надсилається запит. Якщо необхідно фільтрувати за доменом, з якого надходить запит, застосовується параметр «srcdomain». Для використання шаблонів або часткових збігів у правилах доступу можна скористатися параметрами «srcdom_regex» і «dstdom_regex», які дозволяють працювати з регулярними виразами.

Отже, попри велику кількість доступних параметрів у «Squid», для початкового налаштування достатньо лише базового набору. Використання проксі-сервера «Squid» дає змогу оперативно впровадити контроль доступу для окремих користувачів або цілих груп, а також здійснювати моніторинг активності та збирати статистичні дані щодо використання інтернет-каналу.

3.2 Інструкція з налаштування активного комутаційного обладнання

Розглянемо порядок налаштування комутаторів. У проектуванні використовується три комутатори: SW_1, SW_2 SW_3. Їх налаштування здійснюватиметься через консоль і програму, також потрібно налаштувати роутери і мережеві принтери.

Спочатку налаштуємо комутатор третього рівня – SW_3 [10]:

1. Підключаємо комутатор до ПК за допомогою консольного кабелю.

2. Відкриваємо «Device Manager» та визначаємо COM-порт який використовується для підключення (див. рис. 3.1).

3. Відкриваємо програму «PuTTY Configuration» у вікні налаштувань (див. рис. 3.2) змінюємо тип з’єднання на «Serial» та вказуємо номер COM-

порту який визначений у «Device Manager» і у полі «Speed» задаєм значення швидкості. Після цього слід натиснути кнопку «Open», щоб ініціювати з'єднання по послідовному інтерфейсу та перейти до керування пристроєм за допомогою командного рядка.

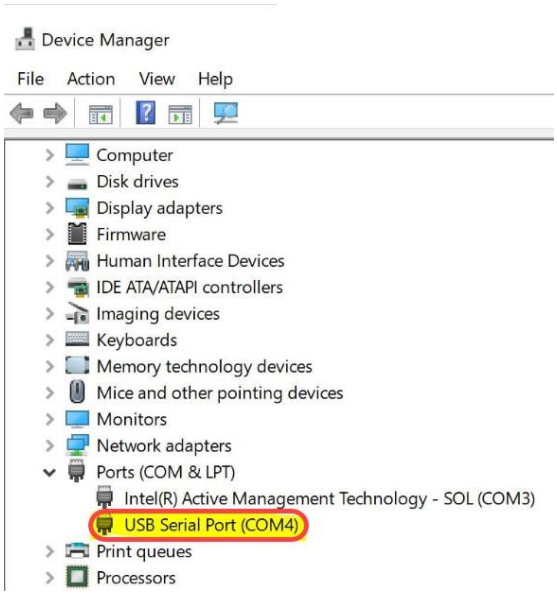


Рисунок 3.1 – Підключення комутатор через COM-порт

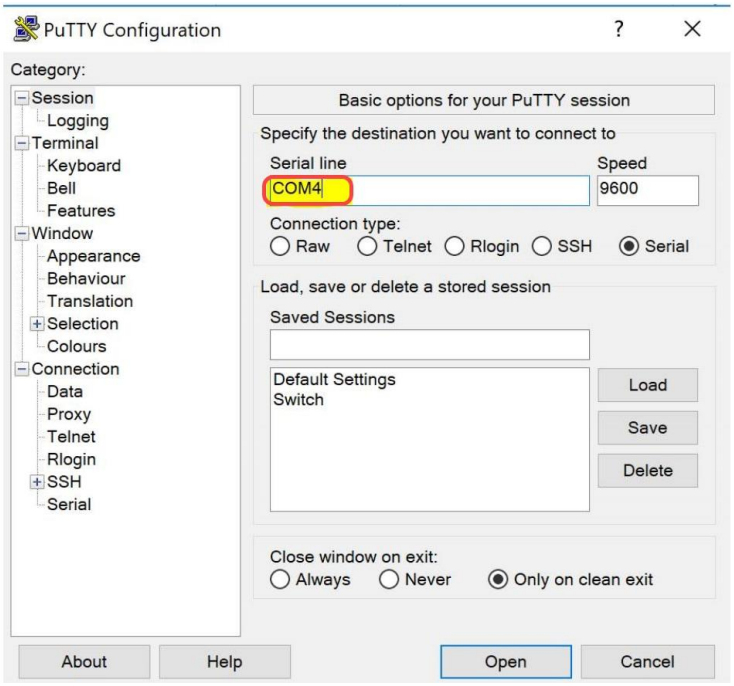


Рисунок 3.2 – Налаштування комутатора у «PuTTY Configuration»

Налаштування комутатора третього рівня наведено у додатку Ж.

Налаштування двох комутаторів другого рівня (SW_1 та SW_2) здійснюється у UniFi Network Application (див. рис. 3.3) [11].

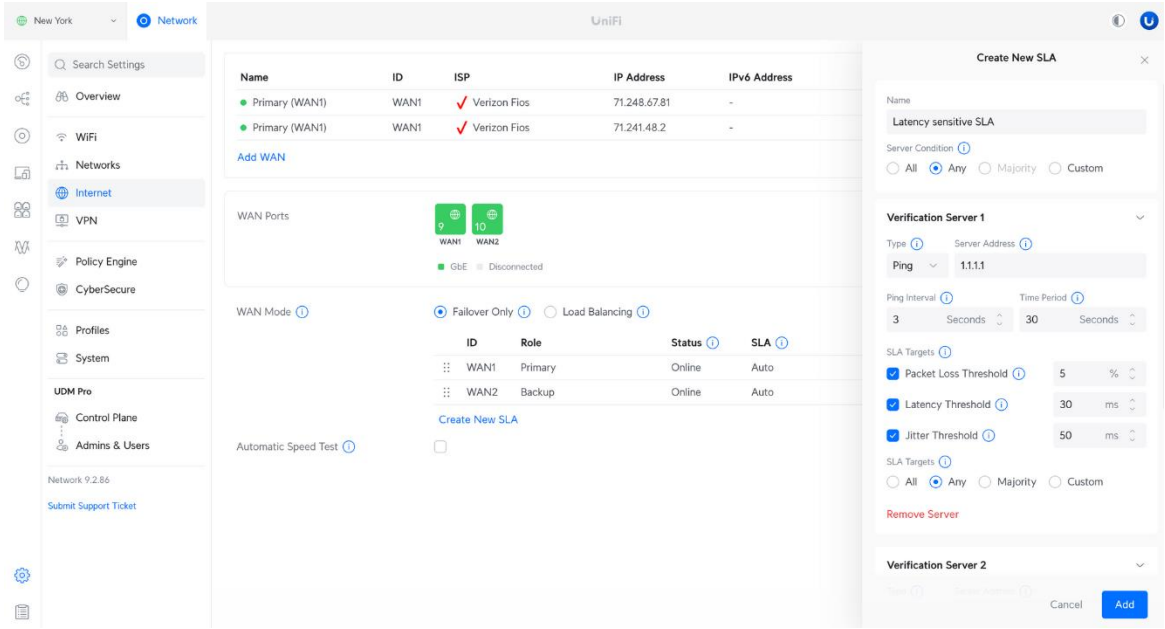


Рисунок 3.3 – Інтерфейс програми UniFi Network Application

Потрібно перейти у вкладку «Devices» у обидва комутатори визначатимуться як «Pending Adoption», обрати кожен із них і натиснути «Adopt». Далі потрібно призначити ip-адреси відповідно до таблиці і для кожного комутатора потрібно перейти у вкладку «Devices» вибрати SW_1 потім SW_2, перейти у «Settings/Network/Management Network» і вибрати «Static IP»:

IP-Address: 192.168.30.52 (SW_1) і 192.168.55.54 (SW_2)

Subnet Mask: 255.255.255.0

Gateway: 192.168.10.20

DNS: 192.168.20 (також можна обрати 8.8.8.8)

зберегти налаштування і зачекати поки комутатор перезавантажиться. Далі необхідне створення VLAN відповідне до топології та таблиці ip-адрес, для

цього потрібно перейти у «Settings/Network» і додати «New Network» для кожної групи VLAN згідно тої ж таблиці ip-адрес, зберегти результат.

Далі потрібно призначити VLAN порти, потрібно перейти у «Devices/SW_1(SW_2)/Ports» вибрати «Port Profile», якщо порт для кінцевого пристрою потрібно обрати «Access» і вибрати відповідний VLAN, якщо порт для між мережевих пристроїв потрібно обрати «Trunk», зберегти і повторити для всіх портів відповідно до топології і таблиці ip-адрес. Для точок доступу потрібно увімкнути PoE, відкриваємо «Ports» вибираємо порт куди підключена точка доступу – відкривається меню налаштувань, знаходимо розділ «PoE» і вибираємо «Auto» і зберігаємо результат.

Тепер потрібно налаштувати роутер «TP-Link Archer AX80», для цього потрібно підключити кабель від провайдера до синього порту (WAN) на маршрутизаторі. Після цього з'єднайте роутер із комп'ютером через мережевий кабель, підключивши один його кінець до будь-якого з LAN-портів пристрою, а інший до мережевого порту комп'ютера.

Інструкція із налаштування роутера [12]:

Необхідно відкрити браузер на комп'ютері і в адресному рядку набрати «http://192.168.0.1» або «http://192.168.1.1». В сторінці авторизації набрати в полях імені користувача та пароля слово «admin» (див. рис. 3.4).

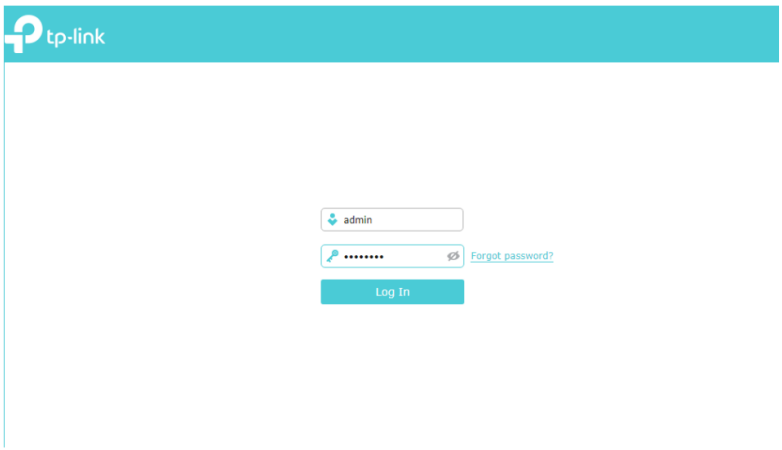


Рисунок 3.4 – Сторінка авторизації

Переходимо на вкладку «Advanced» (див. рис. 3.5).

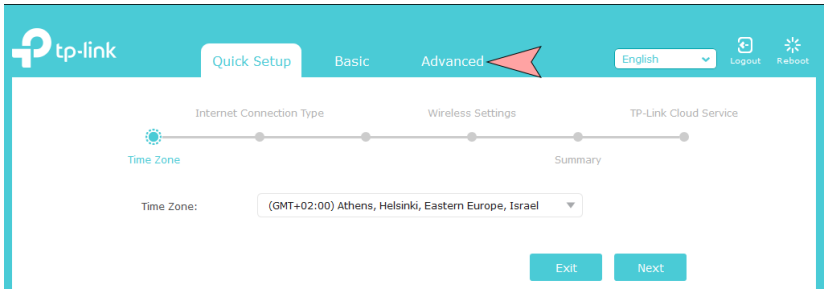


Рисунок 3.5 – Перехід на вкладку Advanced

Налаштовуємо інтернет з'єднання у розділі «Network — Internet» вибираємо «Internet Connection Type — PPPoE», у полях «User Name» і «Password» вказуємо відповідно логін і пароль (див рис 3.6), далі розкриваємо розділ «Advanced».

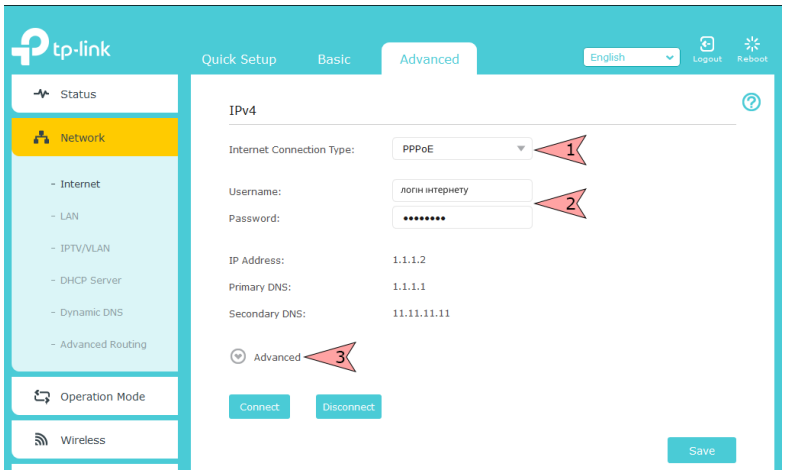


Рисунок 3.6 - Вікно налаштування PPPoE-з'єднання

У пункті «Secondary Connection» обираємо «Dynamic IP», у пункті «IP Address» обираємо «Get dynamically from ISP», у пункті «DNS Address» обираємо «Get dynamically from ISP», у пункті «Connection Mode» обираємо «Auto», зберігаємо налаштування кнопкою «Save» (див рис.3.7).

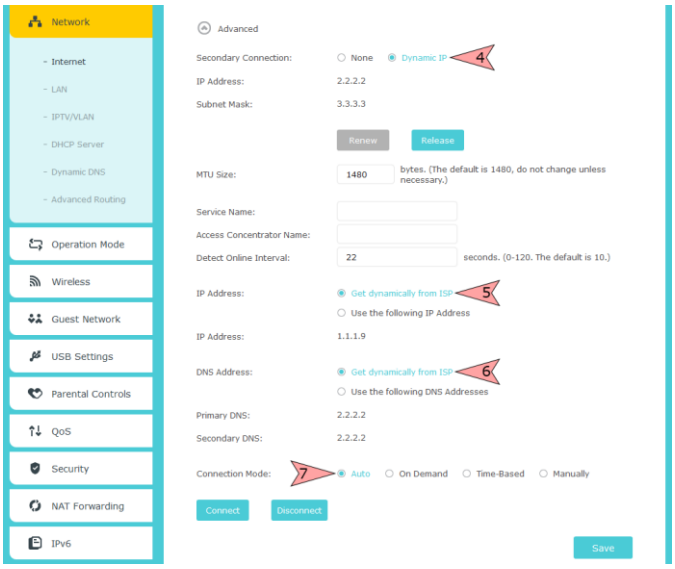


Рисунок 3.7 – Налаштування Інтернет - з'єднання

Для налаштування бездротової мережі Wi-Fi (див. рис. 3.8) потрібно перейти у розділ «Wireless — Wireless Settings», обираємо режим мережі «2.4GHz», у полі «Network Name SSID» встановлюємо бажане ім'я Wi-Fi мережі. У полі «Security» режим «WPA/WPA2 – Personal» обираємо пункти «WPA2-PSK і AES», далі у полі «Password» вводимо бажаний пароль мережі який повинен бути не менше вісьми символів та зберігаємо налаштування.

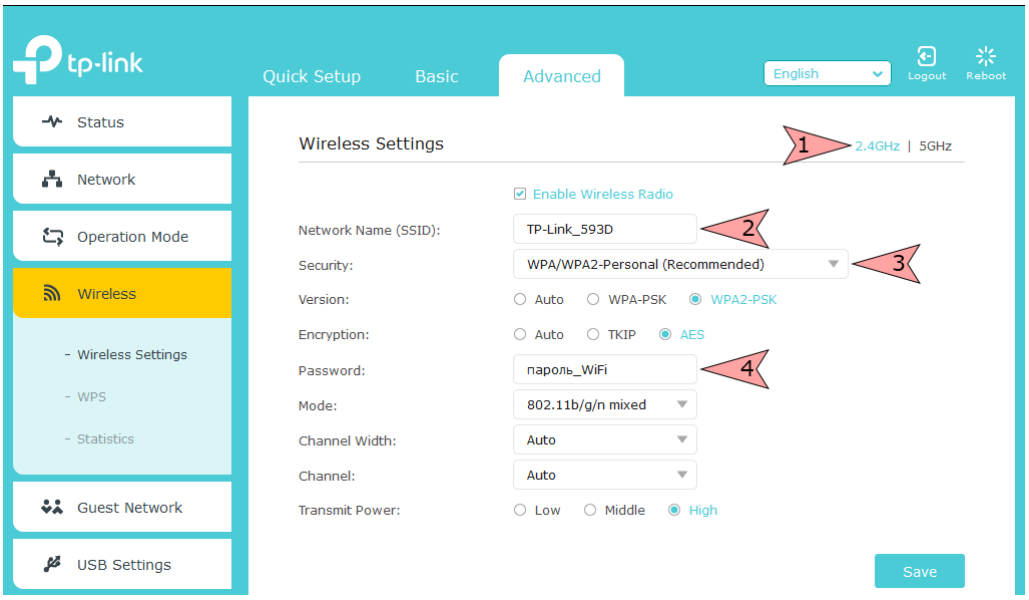


Рисунок 3.8 - Налаштування бездротової мережі Wi-Fi

Далі виберемо режим мережі «5GHz» (див. рис. 3.9). У полі «Network Name SSID» вводимо бажане ім'я Wi-Fi мережі, у полі «Security» встановлюємо режим «WPA/WPA2 – Personal» і обираємо «WPA2-PSK и AES», повторюємо процедуру з паролем та зберігаємо налаштування.

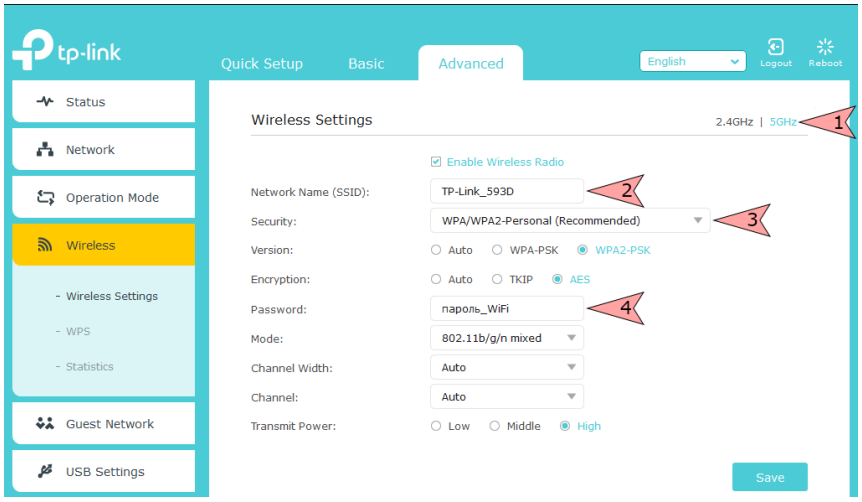


Рисунок 3.9 – Налаштування режиму 5GHz

Для того щоб змінити прив'язку до пристрою потрібно підключити кабель в WAN-порт роутера. Перейти в розділ «Status» і в розділі «Internet» необхідно повідомити оператору підтримки значення з поля «MAC Address» (див.рис. 3.10) або можна самостійно змінити MAC-адресу в особистому кабінеті.

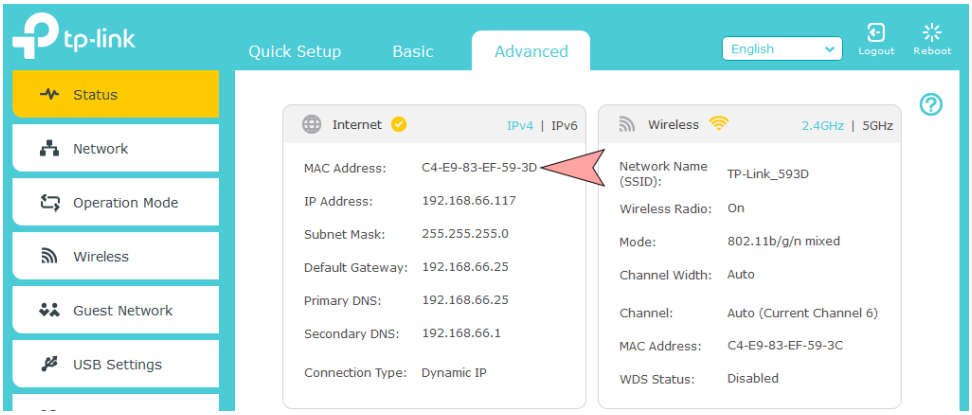


Рисунок 3.10 – MAC Address пристрою

Інструкція з налаштування мережевих принтерів [13]:

Щоб комп’ютери в локальній мережі мали змогу використовувати принтер, підключений до одного з пристроїв, слід налаштувати не лише сам принтер для мережевого доступу, а також коректно сконфігурувати комп’ютер, до якого він приєднаний. Для цього потрібно здійснити наступні кроки:

1. Зайти в панель управління Windows та вибрати «Панель управління/Мережа та Інтернет/Центр управління мережами і загальним доступом», після чого відкрити посилання «Змінити додаткові параметри спільного доступу», доступне в лівому меню.

2. У відкритому вікні буде доступно три вкладки, навпроти яких потрібно вибрати такі пункти: включити мережеве виявлення, активувати загальний доступ до файлів та принтерів, відключити парольний захист.

3. Зберегти налаштування та перейти в розділ «Панель управління/Обладнання і звук/Пристрої та принтери», в якому необхідно вибрати свій принтер серед доступних, клацнути на ньому правою кнопкою мишки та вибрати вкладку «Властивості принтера». Далі необхідно перейти до розділу «Доступ» й поставити галочку навпроти пункту «Загальний доступ до цього принтера».

4. Зайти у вкладку «Безпека», вибрати в групах та користувачах «Всі» та поставити галочку навпроти пункту «Друк».

Результатом налаштування є повноцінна інтеграція принтера в інформаційну інфраструктуру з можливістю його використання з будь-якого комп’ютера, підключеного до локальної мережі.

3.3 Інструкція з використання тестових наборів та тестових програм

Усі робочі станції передбачені в мережі функціонуватимуть під керуванням операційної системи Windows 10. Далі буде розглянуто декілька

вбудованих інструментів цієї ОС, які дозволяють виконувати базову перевірку стану мережевого підключення.

Найпопулярніші мережеві утиліти це є «Ping», «Tracert», «IPConfig». Вони надають можливість здійснювати управління та моніторинг мережевих підключень без потреби у встановленні сторонніх програм.

Розглянемо найпопулярнішу з них команду «PING», це утиліта командного рядка, за допомогою якого можна перевірити, чи в мережі той чи інший сервер. Перевірити пінг до сервера на комп'ютері можна за допомогою командного рядка. У разі успішної перевірки буде відображено ім'я сервера, його IP-адресу, час відгуку у мілісекундах, а також кількість надісланих і отриманих пакетів [14].

Якщо вдається виконати пінг за IP-адресою, але не вдається зробити те саме за доменним іменем того ж сервера, ймовірною причиною є проблема з розпізнаванням доменного імені в IP-адресу. У такому випадку слід перевірити правильність налаштувань DNS-серверів [14].

У разі невдалої спроби виконати пінг до сервера можуть з'явитися повідомлення типу «unknown host» або «request timeout». Ці відповіді допомагають визначити, з якого боку виникла проблема — на вашому пристрої чи на стороні сервера. Повідомлення «unknown host» свідчить про те, що комп'ютеру не вдалося надіслати запит до сервера. Це, як правило, вказує на проблему з боку користувача — наприклад, відсутнє підключення до мережі або вказано некоректну чи неіснуючу адресу. Повідомлення «request timeout» означає, що комп'ютер надіслав пінг-запит, однак відповідь від сервера не надійшла у відведений для цього час. Це може свідчити про неполадки на боці сервера або про проблеми в мережевому маршруті між клієнтом і сервером — наприклад, сервер тимчасово недоступний, вийшов з ладу або доступ до нього блокується провайдером. Щоб переконатися, чи сервер дійсно працює, спробуйте встановити з'єднання через SSH. Якщо підключення вдається —

сервер функціонує коректно. Крім простої перевірки з'єднання із сервером, є кілька варіацій команди, розглянемо найпопулярніші з них [14].

Постійний пінг — за замовчуванням команда пінг у Windows відправляє чотири пакети, а в Linux та MacOS діє безперервно. Щоб запустити безперервний ping сайт у Windows, використовуйте опцію -t:

ping -t 123.45.67.89

Пінг із зазначенням розміру пакету — зазвичай розмір переданих пакетів становить 32 або 64 байти, проте цей параметр можна змінити вручну. Наприклад, щоб надіслати пакети обсягом 1025 байт під час виконання команди ping:

ping -l 1024 123.45.67.89

3.4 Інструкція по налаштуванню засобів захисту мережі

З метою безперервної та безпечної роботи внутрішньої мережі слід впровадити надійні заходи кіберзахисту. Як приклад, розглянемо основні кроки щодо захисту мережі під час конфігурації маршрутизатора «TP-Link Archer AX80» [15]:

Захист мережі від кібератак.

Брандмауер SPI здатен захищати мережу від несанкціонованих атак і здійснювати контроль трафіку, що проходить через маршрутизатор, з урахуванням протоколів передачі даних. Ця опція активована за замовчуванням, тому доцільно залишити її без змін. Механізм захисту від DoS-атак допомагає запобігти спробам перевантаження мережі надмірною кількістю запитів до сервера, тим самим зберігаючи стабільність роботи мережі. Щоб увімкнути брандмауер і налаштувати захист від DoS, виконайте такі дії:

1. Відвідайте http://tplinkmodem.net та увійдіть, використовуючи пароль, який ви встановили для маршрутизатора.

2. Перейдіть до розділу Advanced/Security/Firewall & DoS Protection (див. рис. 3.11).

3. Увімкніть IPv4 SPI Firewall та DoS Protection.

4. Встановіть рівень захисту для фільтрації атак ICMP-FLOOD, UDP-Flood, TCP-FLOOD, збережіть налаштування натиснувши Save.

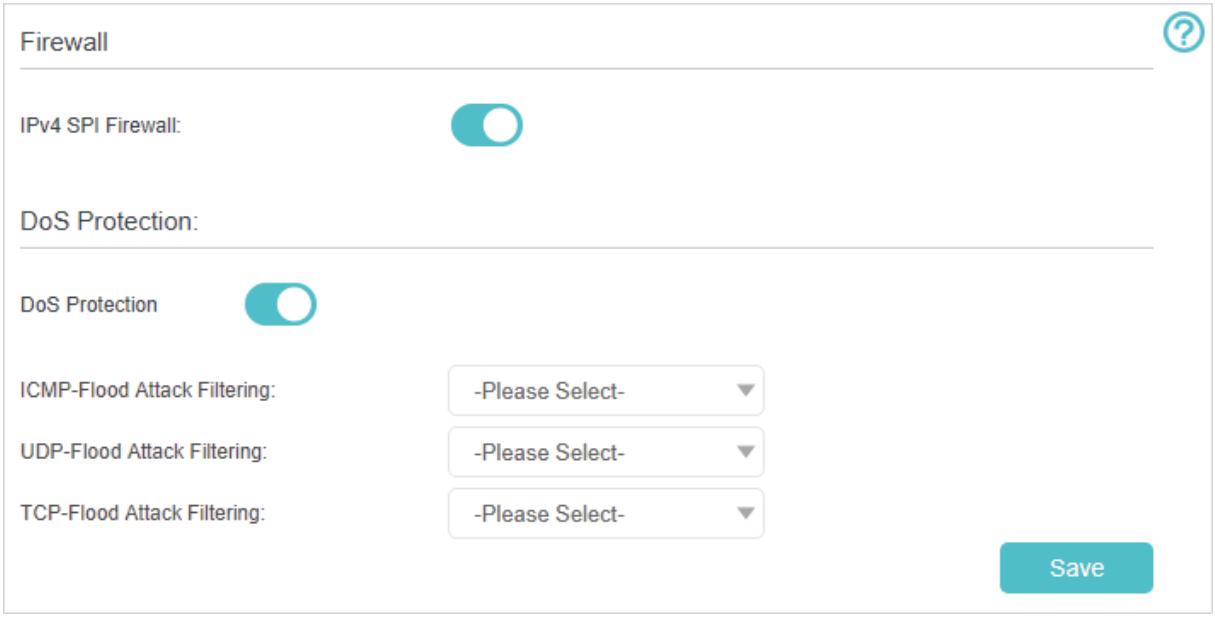


Рисунок 3.11 – Інтерфейс налаштування Брандмауер і захисту від DoS-атак

За допомогою фільтрації послуг можливо заборонити певним користувачам доступ до вказаної служби, навіть повністю заблокувати доступ до Інтернету:

1. Відвідайте http://tplinkmodem.net та увійдіть, використовуючи пароль, який ви встановили для маршрутизатора.

2. Перейдіть до розділу Advanced/Wireless/Service/Filtering і увімкніть Service Filtering та натисніть Add (див рис. 3.12).

3. Виберіть тип послуги зі спадного списку, і наступні чотири поля будуть заповнені автоматично.

4. Вкажіть IP-адресу, до якої застосовуватиметься це правило фільтрації та натисніть кнопку Save.

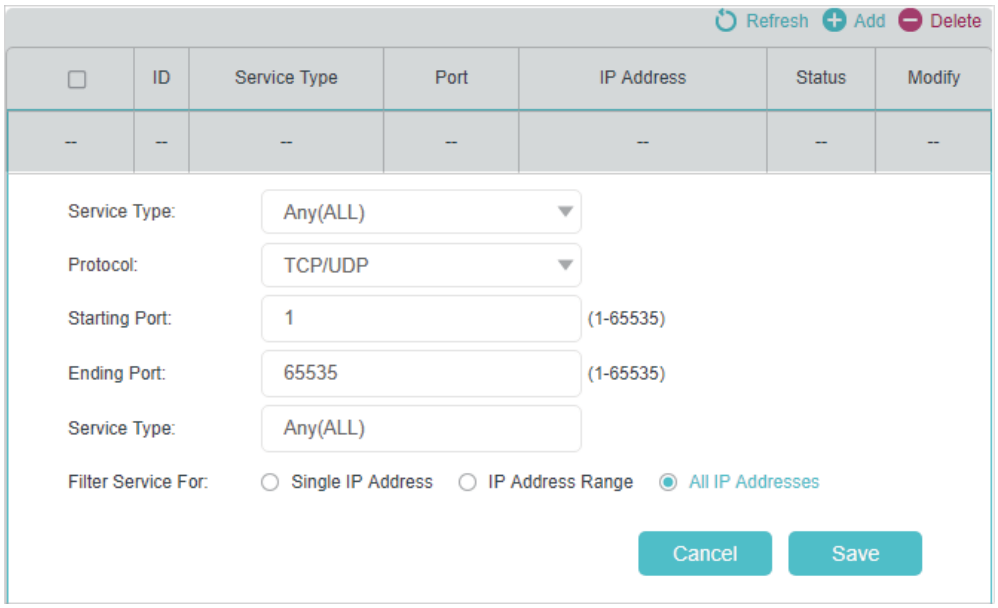


Рисунок 3.12 – Інтерфейс налаштування фільтрації

Контроль доступу використовується для блокування або дозволу певним клієнтським пристроям доступу до вашої мережі на основі списку заблокованих пристроїв або списку дозволених пристроїв:

1. Відвідайте http://tplinkmodem.net та увійдіть, використовуючи пароль, який ви встановили для маршрутизатора.

2. Перейдіть до розділу Advanced > Security > Access Control and enable Access Control (див рис. 3.13).

3. Виберіть режим доступу, щоб заблокувати або дозволити пристрої зі списку.

4. Щоб заблокувати певний пристрій виберіть Blacklist і натисніть Save, виберіть пристрій який потрібно заблокувати у таблиці онлайн-пристроїв та натисніть Block, вибрані пристрої будуть автоматично додані заблоковані.

5. Щоб дозволити доступ певним пристроям виберіть Whitelist і натисніть Save і далі Add. Виберіть назву пристрою та його MAC-адресу і натисніть Save.

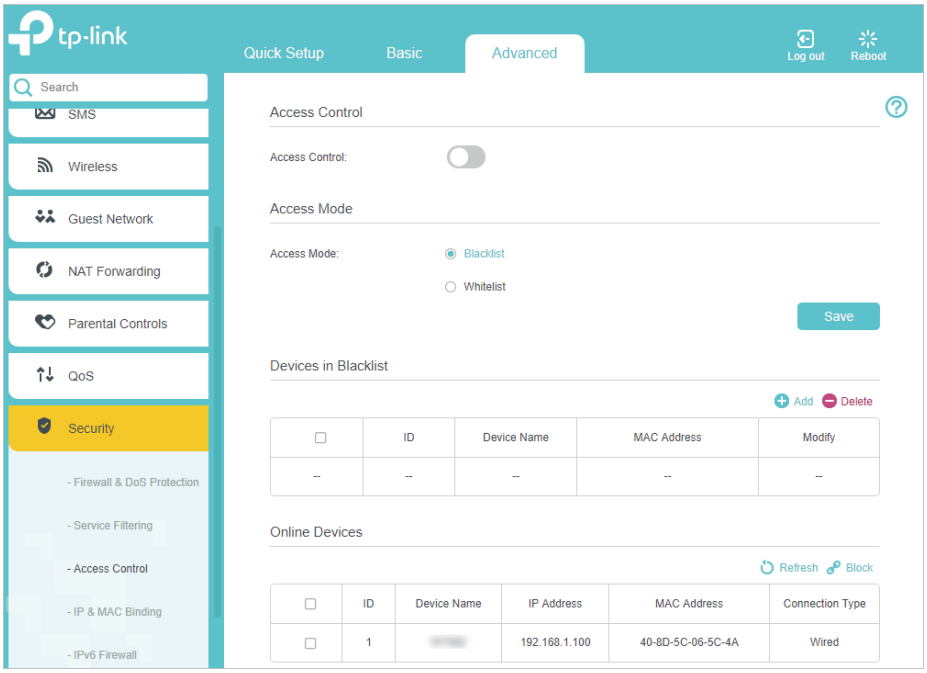


Рисунок 3.13 – Інтерфейс налаштування контролю доступу

3.5 Інструкція з експлуатації та моніторингу в мережі

Для комфортної експлуатації мережі було розроблено документи: план приміщення, фізична топологія, логічна топологія, таблиця IP-адрес.

Для моніторингу мережі використана програма: Zabbix, це потужна система моніторингу з відкритим вихідним кодом. Вона дозволяє комплексно стежити за станом мережі. Zabbix користується великою популярністю серед компаній різного масштабу завдяки своїй гнучкості, масштабованості та безкоштовній ліцензії.

Zabbix забезпечує всебічний моніторинг комп'ютерної мережі завдяки використанню різних протоколів та методів збору даних. Для отримання інформації про стан мережевого обладнання, такого як маршрутизатори, комутатори чи сервери, Zabbix застосовує протоколи SNMP, ICMP для перевірки доступності вузлів, IPMI для відстеження апаратного стану серверів [16].

Однією з важливих функцій є обробка SNMP-трапів, спеціальних сповіщень, які мережеве обладнання надсилає автоматично у разі збоїв або змін у роботі. Це дає змогу оперативно реагувати на несправності. Вся зібрана інформація зручно відображається у веб-інтерфейсі Zabbix: адміністратор може налаштувати інтерактивні дашборди, переглядати карти мережі з позначенням стану пристроїв у реальному часі, а також аналізувати графіки трафіку та навантаження на обладнання [16].

Уразі виявлення відхилень або аварійних ситуацій система автоматично надсилає сповіщення через електронну пошту, SMS чи месенджери, що дозволяє швидко вжити заходів для усунення проблеми.

Крім того, Zabbix формує звіти, що допомагають оцінювати історію роботи мережі, планувати технічне обслуговування та модернізацію інфраструктури. Завдяки цьому Zabbix є ефективним інструментом для підтримки стабільної та безпечної роботи комп'ютерної мережі [16].

3.6 Моделювання мережі в Cisco Packet Tracer

Моделювання розробленої комп'ютерної мережі здійснюватиметься у програмі Cisco Packet Tracer.

Cisco Packet Tracer (див. рис. 3.14) є одним з найпоширеніших програмних засобів для моделювання комп'ютерних мереж, розробленим компанією Cisco Systems. Це багатофункціональний симулятор, призначений переважно для навчання та підготовки спеціалістів у галузі комп'ютерних мереж, а також для відпрацювання практичних навичок роботи з мережевим обладнанням без необхідності використання фізичних пристроїв.

Основна мета це надати користувачам можливість створювати віртуальні мережі різної складності, виконувати налаштування маршрутизаторів, комутаторів та інших мережевих пристроїв, аналізувати роботу протоколів

передачі даних і відслідковувати рух мережевого трафіку у зручній графічній формі.

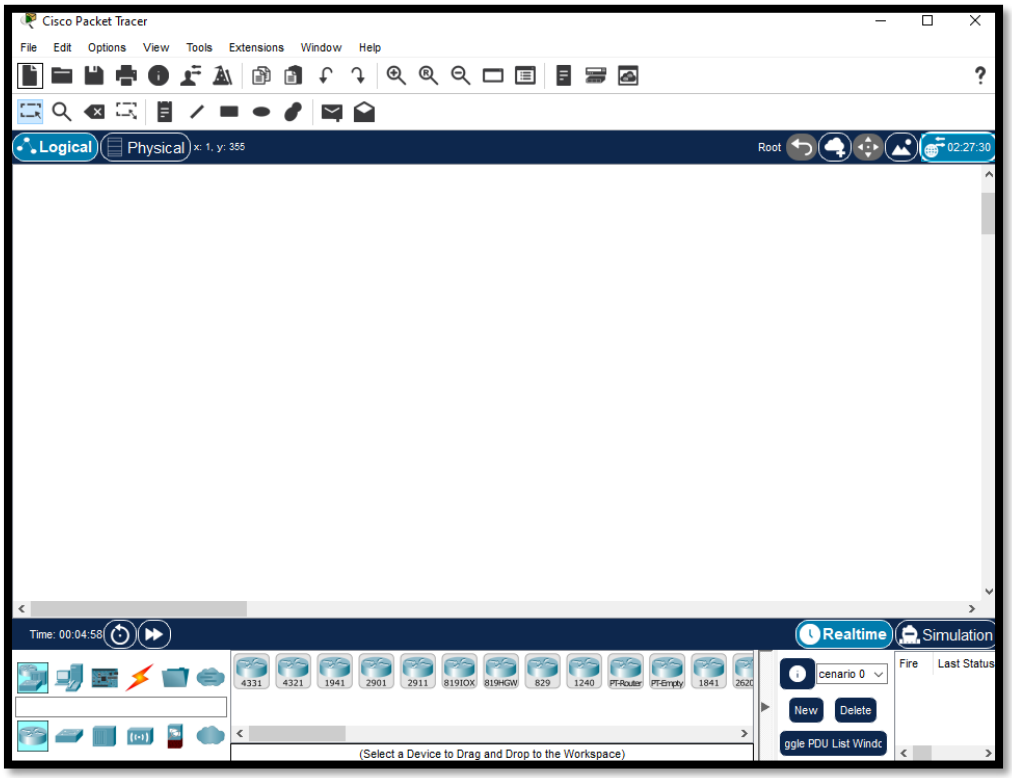


Рисунок 3. 14 – Інтерфейс програми Cisco Packet Tracer

У верхній частині інтерфейсу програми розміщено головне меню та панель інструментів, які забезпечують доступ до основних функцій програми, наприклад: меню управління файлами, кнопки швидкого доступу, інструменти малювання і коментування, засоби навігації та інші додаткові опції [17].

У нижній частині інтерфейсу програми розміщено елементи, які допомагають працювати з моделлю мережі та керувати процесом симуляції, наприклад: панель режимів роботи, панель відображення пакетів, інструменти управління симуляцією та інші додаткові опції. Крім того у нижній частині програми розміщується перелік доступних моделей пристроїв. Під час вибору певного пристрою користувач має змогу переглянути його фізичне зображення

(див. рис. 3.15), що дозволяє додатково підключати або замінювати різні модулі всередині обладнання [17].

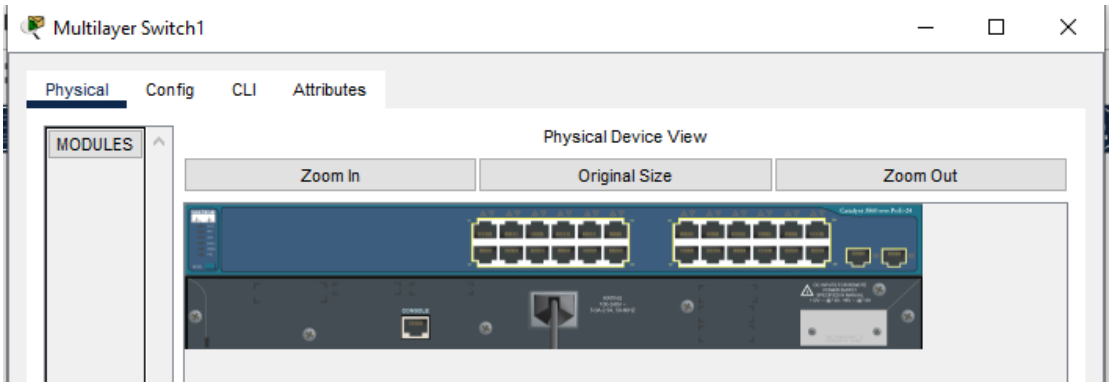


Рисунок 3.15 – Фізичне зображення комутатора

В результаті проектування моделі мережі виходить наступний проект мережі (див. рис. 3.16).

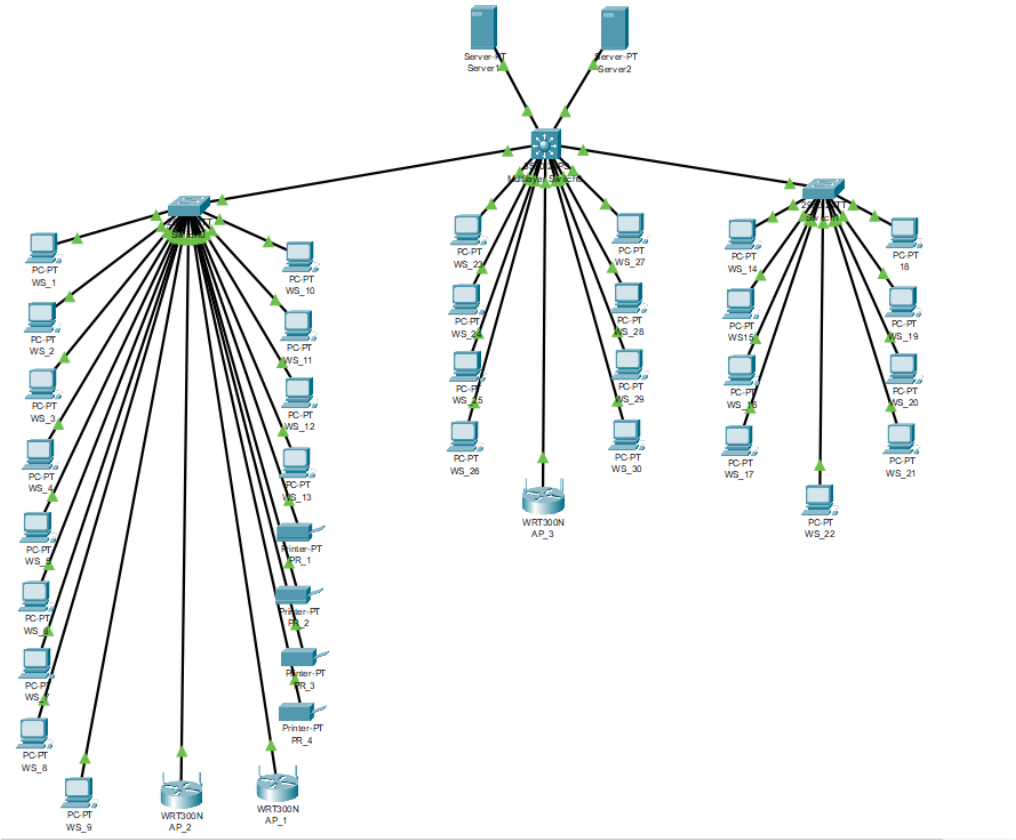


Рисунок 3.16 – Змодельована локальна мережа

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини дипломного проекту є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проекту комп'ютерної мережі для приватного підприємства «UNGAS Smart» і прийняття рішення про її подальше впровадження в роботу.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

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

Таблиця 4.1 – Середній час виконання НДР та стадії технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Постановка задачі та збір інформації про об’єкт	Керівник проєкту	10
2.	Розробка проєкту	Інженер	20
3.	Монтаж мережі	Технік	35
4.	Тестування та остаточне налаштування	Інженер	15
5.	Налагодження мережі та створення технічної документації	Інженер	15
6	Здача проекту	Керівник проєкту	5
Разом			100

Загальний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для приватного підприємства «UNGAS Smart» становить 100 годин.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Оплата праці - грошовий вираз вартості і ціни робочої сили, який виступає у формі будь-якого заробітку, виплаченого власником підприємства працівникові за виконану роботу.

Заробітна плата працівника залежить від кінцевих результатів роботи підприємства, регулюється податками і максимальними розмірами не обмежується.

Основна заробітна плата розраховується за формулою 4.1:

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

де Тс – тарифна ставка, грн.; Кг – кількість відпрацьованих годин.

Основна заробітна плата становить:

1. Керівник проекту: $З_{осн1} = 280 \cdot 15 = 4\ 200$ грн.;
2. Інженер: $З_{осн2} = 160 \cdot 50 = 8\ 000$ грн.;
3. Технік: $З_{осн3} = 125 \cdot 35 = 4\ 375$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 4200 + 8000 + 4375 = 16575 \text{ грн.}$$

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

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проекту: $З_{дод1} = 4200 \cdot 0,14 = 588$ грн.;

2. Інженер: $З_{дод2} = 8000 \cdot 0,14 = 1120$ грн.;

3. Технік: $З_{дод3} = 4375 \cdot 0,14 = 615,5$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод} = 588 + 1120 + 615,5 = 2323,50 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п..}$) визначаються за формулою 4.3:

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

$$В_{о.п} = 16575 + 2323,50 = 18898,50 \text{ грн.}$$

Відрахування на соціальні заходи становлять 22%. Отже, сума відрахувань на соціальні заходи буде обчислюватися за формулою 4.4:

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

де ФОП – фонд оплати праці, грн.

$$В_{с.з.} = 18898,50 \cdot 0,376 = 7105,84 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

4200 + 8000 + 4375

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	280	15	4200	588	-	-
2	Інженер	160	50	8000	1120	-	-
3	Технік	125	35	4375	615,50	-	-
Разом				16575	2323,50	7105,84	26004,34

Загальні витрати на оплату праці становлять 26004,34 грн.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються за формулою 4.5 як добуток кількості витрачених матеріалів та їх ціни:

$$M_{Bi} = q_i \cdot p_i, \tag{4.5}$$

де q_i – кількість витраченого матеріалу і-го виду; p_i – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$З_{м.в.} = \sum M_{Bi}, \tag{4.6}$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Назва елемента	Од. виміру	Факт. Витрачено матеріалів	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	2	3	4	5	6
1	Серверна платформа Dell PowerEdge T40 v04	шт.	2	30 000	60 000
2	Комутатор Cisco C1300-24P-4G	шт.	1	36 400	36 400
3	Комутатор Ubiquiti USW 24-Poe Gen2	шт.	2	14 550	29 100
4	Маршрутизатор TP-Link Archer AX80	шт.	3	7 200	21 600

Продовження таблиці 4.3

1	2	3	4	5	6
5	ДБЖ APC Smart-UPS 750VA	шт.	2	31 500	63 000
6	Жорсткий диск Toshiba 3.5, 2 ТВ	шт.	4	2 640	10 560
7	Патч панель 1U 24 порта	шт.	3	2 050	6 150
8	Вита пара -cat.6, 305 м	шт.	4	5 340	21 360
9	Патч-корд UTP Cat 6 UTP 0.5m	шт.	40	75	3 000
10	Патч-корд UTP Cat 6 U/UTP 2m	шт.	35	120	4 200
11	Комп'ютерна розетка Rj-45 1xSTP, cat 6.	шт.	5	80	400
12	Комп'ютерна розетка Rj-45 2xSTP, cat 6.	шт.	20	120	2 400
13	Зовнішня шафа для мережевого обладнання	шт.	1	5 700	5 700
14	Принтери HP LaserJet M211dw	шт.	4	8000	32 000
15	Кабельний організатор	шт.	3	200	600
16	Шафа серверна підлогова	шт.	1	16 300	16 300
17	Короб 40x25	м	100	55	5 500
18	Короб 25x25	м	150	24	3 600

Загальна сума матеріальних витрат становить 321870 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою 4.7:

$$З_е = W \cdot T \cdot S \text{ ,} \quad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 50 години, споживана потужність - 0,6 кВт/год., вартість 1 кВт електроенергії – 7 грн. Тому витрати на електроенергію будуть становити:

$$З_е = 0,6 \cdot 50 \cdot 7 = 210 \text{ грн.}$$

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8-10 % від загальної суми матеріальних затрат. Транспортні витрати розраховуються за формулою 4.8.

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

де $Т_В$ – транспортні витрати.

Отже, транспортні витрати будуть становити:

$$Т_В = 321870 \cdot 0,09 = 28968,30 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

Комп’ютери та оргтехніка належать до четвертої групи основних фондів. Мінімально допустимі строки їх використання 2 роки. Для визначення амортизаційних відрахувань застосовуємо формулу 4.9:

$$A = \frac{Б_В \cdot Н_А}{100\%} \cdot \text{Т}, \tag{4.9}$$

де А – амортизаційні відрахування за звітний період, грн.

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

$Н_А$ – норма амортизації, %;

Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 50 год., балансова вартість ПК – 25200 грн., тому:

$$\text{А}= \frac{25200*0,04}{150} * 50 = 336 \text{ грн}$$

4.7 Обчислення накладних витрат

Накладні витрати - це витрати, не пов'язані безпосередньо з технологічним процесом виготовлення продукції, а утворюються під впливом певних умов роботи по організації, управлінню та обслуговуванню виробництва.

В залежності від організаційно-правової форми діяльності господарюючого суб’єкта, накладні витрати можуть становити 20 – 60 % від суми основної та додаткової заробітної плати працівників, обчислюються за формулою 4.10.

$$H_в = B_{о.п.} \cdot 0{,}2...0{,}6\,, \qquad (4.10)$$

де $Н_В$ – накладні витрати.

$$Н_В = 18898{,}50 \cdot 0{,}5 = 9449{,}25 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Кошторис витрат являє собою зведений план усіх витрат підприємства на майбутній період виробничо-фінансової діяльності.

Результати проведених вище розрахунків зведемо у таблиці 4.4, де зазначено наступні види витрат: витрати на оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування, накладні витрати.

Таблиця 4.4 – Кошторис витрат НДР

Зміст витрат	**Сума, грн.**	**В % до загальної суми**
Витрати на оплату праці	18898,50	4,89 %
Відрахування на соціальні заходи	7105,84	1,84 %
Матеріальні витрати	321870	83,20 %
Витрати на електроенергію	210	0,05 %
Транспортні витрати	28968,30	7,49 %
Амортизаційні відрахування	336	0,09 %
Накладні витрати	9449,25	2,44 %
Собівартість	386836,89	100

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

$$C_В = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_е + Т_в + А + Н_в\,, \qquad (4.11)$$

Собівартість дорівнює $С_В$ = 386 836,89 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12:

$$Ц = Св \cdot (1+Р_{рен}) \cdot (1+ПДВ), \quad (4.12)$$

де $Р_{рен.}$ – рівень рентабельності; ПДВ – ставка податку на додану вартість.

$$Ц = 386836,89 \cdot (1+0,3) \cdot (1+0,2) = 603465,55 \text{ грн.}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

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

Прибуток розраховується за формулою 4.13

$$П = Ц - С_в \quad (4.13)$$

$$П = 603465,55 - 386836,89 = 216628,66$$

Економічна ефективність ($Е_р$) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою 4.14,

де П – прибуток;

$С_в$ – собівартість.

$$Е_р = П / С_в \quad (4.14)$$

$$Е_р = 216628,66 / 386836,89$$

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

$$T_р = 1 / E_р \quad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку:

$$T_р = 1 / 0,56 = 1,8$$

Всі дані внесемо в зведену таблицю 4.5 техніко-економічних показників.

Таблиця 4.5 - Техніко-економічні показники проекту комп'ютерної мережі до приватного підприємства «UNGAS Smart».

№ п/п	Показник	Значення
1	Собівартість, грн.	386836,89
2	Плановий прибуток, грн.	216628,66
3	Ціна, грн.	603465,55
4	Термін окупності, рік	1,8

Загальна вартість розробленої мережі для приватного підприємства «UNGAS Smart» становить 603465,55 грн. Термін окупності – 1,8 року, проводити роботи по впровадженню даної мережі є доцільним та економічно вигідним.

5 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

5.1 Вжиті режимно-організаційні заходи, які забезпечують пожежну безпеку ПП «UNGAS Smart»

Для забезпечення пожежної безпеки на підприємстві ПП «UNGAS Smart» впроваджено комплекс організаційних та режимних заходів, спрямованих на запобігання виникненню пожеж та зменшення їх наслідків у разі виникнення. Вказані заходи відповідають вимогам Кодексу цивільного захисту України, Правил пожежної безпеки в Україні, а також внутрішнім нормативним документам підприємства. До основних заходів належать [18]:

– призначення відповідальних осіб, наказом по підприємству визначено особу, відповідальну за забезпечення пожежної безпеки. Також у структурних підрозділах призначені відповідальні особи за дотримання пожежного режиму на місцях;

– проведення протипожежних інструктажів, організовано проведення вступного, первинного, повторного, позапланового та цільового інструктажів з питань пожежної безпеки для всіх працівників. Ведеться належна документація, включаючи журнали реєстрації інструктажів;

– забезпечення первинними засобами пожежогасіння, робочі приміщення обладнані відповідною кількістю вогнегасників, які підлягають періодичній перевірці технічного стану та перезарядці згідно з встановленими нормативами;

– у всіх приміщеннях розміщено схеми евакуації, інструкції з дій у разі пожежі, а також інформаційні таблички з номерами телефонів екстрених служб. Встановлено оповіщувачі про небезпеку пожежі;

– контроль стану електрообладнання, проводиться регулярне обстеження електромережі та електроприладів, заборонено використання

несправного обладнання та саморобних подовжувачів. Передбачено своєчасне відключення приладів після завершення роботи;

– організація евакуаційних шляхів та виходів, евакуаційні маршрути та виходи постійно утримуються у вільному стані, оснащені відповідними покажчиками та позначеннями згідно з вимогами нормативних документів.

– дотримання протипожежного режиму, на території підприємства заборонено куріння у приміщеннях;

– періодично проводиться перевірка справності електромережі та обладнання, що використовується в офісних та технічних приміщеннях.

Таким чином, дотримання перелічених організаційно-регламентних заходів дозволяє підтримувати належний рівень пожежної безпеки на підприємстві та забезпечує безпечні умови праці для персоналу.

На рисунку 5.1 наведено план евакуації та поставлені на ньому знаки пожежної безпеки

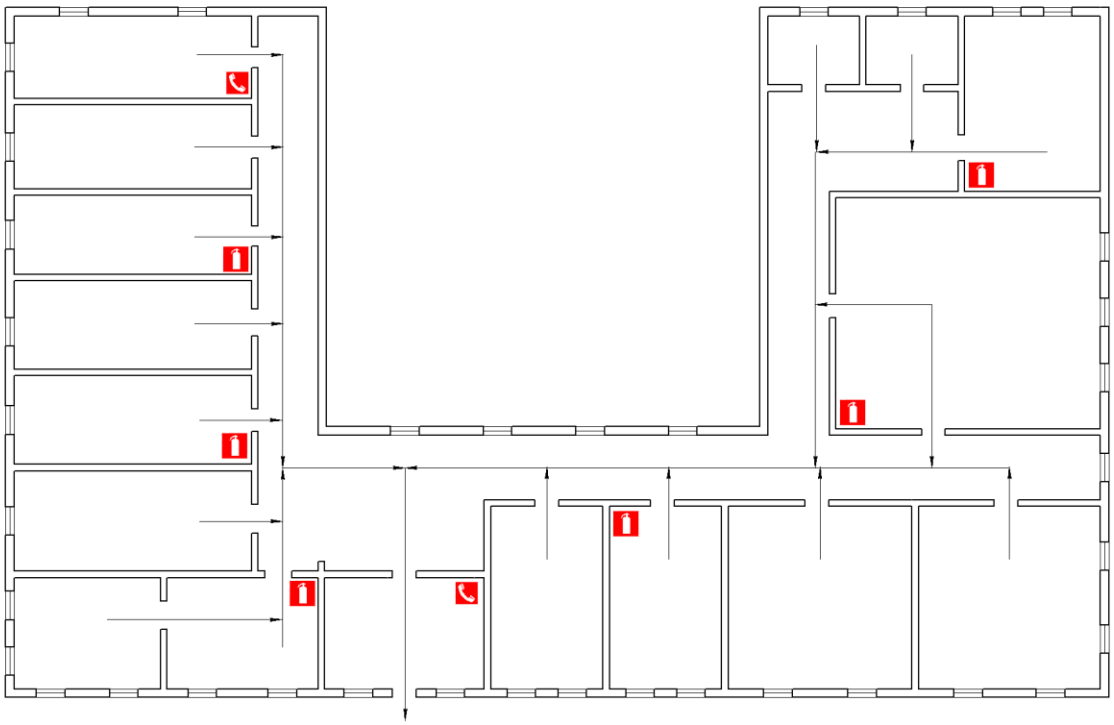


Рисунок 5.1 – План евакуації та знаки пожежної безпеки

5.2 Заходи щодо забезпечення санітарно-технічних вимог в ПП «UNGAS Smart»

Забезпечення санітарно-технічних умов праці є одним з ключових напрямів охорони праці та важливим фактором збереження здоров'я персоналу. На ПП «UNGAS Smart» реалізується система заходів, спрямованих на створення безпечного та відповідного до гігієнічних нормативів виробничого середовища. Усі дії з організації санітарно-технічного забезпечення відповідають вимогам чинного законодавства України, а саме [19]:

- закону України «Про охорону праці»;
- державних санітарних норм і правил, зокрема ДСанПіН 3.3.2.007-98 (санітарні норми мікроклімату виробничих приміщень);
- ДБН В.2.2-10:2021 — Будівлі і споруди. Адміністративні та офісні приміщення.

В офісних та технічних приміщеннях підприємства підтримується стабільний мікроклімат, що відповідає нормативним параметрам температури, вологості й швидкості руху повітря.

У робочих зонах температура повітря в холодну перу року підтримується в межах +20…+22 °С, а в теплий +22…+25 °С. Для цього в будівлі функціонують системи централізованого опалення, кондиціонування та припливно-витяжної вентиляції. Кожне приміщення обладнане системами природного й штучного провітрювання, що дозволяє уникнути скупчення шкідливих речовин та зберігати оптимальний рівень вуглекислого газу в повітрі. Згідно з графіком, щоквартально проводиться очищення вентиляційних каналів та фільтрів кондиціонерів. На підприємстві організовано раціональне комбіноване освітлення — природне та штучне. Вікна у приміщеннях забезпечують достатній рівень природного освітлення у світлу пору доби. [19]

Для штучного освітлення використано енергозберігаючі LED-світильники, які забезпечують нормативну освітленість не менше 300 лк у робочих зонах. У місцях з обмеженим природним світлом передбачено аварійне освітлення на випадок вимкнення електроенергії. Всі системи освітлення регулярно перевіряються на предмет справності та ефективності.

Будівля ПП «UNGAS Smart» підключена до централізованих систем холодного та гарячого водопостачання, каналізації та опалення. Працівники мають вільний доступ до сучасно обладнаних санвузлів, які відповідають вимогам ДБН В.2.5-64:2012 щодо кількості і розташування. У кожному санітарному вузлі забезпечено наявність [19]:

- питної води (через підключені фільтри або бутильовану воду);
- умивальників із рідким милом та сушарками для рук;
- туалетного паперу та санітарних засобів для прибирання.

Прибирання офісних приміщень здійснюється щоденно відповідно до затвердженого графіка. Щотижнево проводиться вологе прибирання із застосуванням сертифікованих дезінфікуючих засобів. Раз на місяць організовується генеральне прибирання всіх службових зон, включно з вентиляційними решітками, стінами та стелями. З метою контролю дотримання гігієнічних вимог на підприємстві впроваджено журнал санітарного стану приміщень, у якому відповідальні особи відмічають результати перевірок та необхідні коригувальні дії.

Таким чином, заходи щодо дотримання санітарно-технічних вимог є системними та відповідають чинним нормативам. Їх реалізація забезпечує комфортні, безпечні та здорові умови праці, що сприяє підвищенню ефективності роботи персоналу та зниженню ризиків професійних захворювань.

ВИСНОВКИ

У ході роботи над кваліфікаційною роботою спроектовано комп’ютерну мережу приватного підприємства «UNGAS Smart».

У першому розділі кваліфікаційної роботи сформульовано технічне завдання до проекту, а також проаналізовано рівень комп’ютеризації підприємства та його потреби в комунікаційних засобах.

У другому розділі вибрано і вказано характеристики мережевого кабелю, активного та пасивного комутаційного обладнання. Вибрано операційні системи серверів та робочих станції.

У результаті виконання другого розділу була розроблена схема логічних зв’язків між мережевими об’єктами та представлено варіант її фізичної реалізації. Обидві топології логічна й фізична відображені на окремих графічних плакатах, що входять до графічної частини кваліфікаційної роботи.

У третьому розділі кваліфікаційної роботи подано вказівки з налаштування серверів, активного комутаційного обладнання мережі.

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

У останньому розділі розглянуто питання безпеки життєдіяльності та охорони праці.

В підсумку робота містить комплексну документацію по проектуванню та впровадженню в експлуатацію локальної мережі.

ПЕРЕЛІК ПОСИЛАЛЬ

1. Тетяна Коробейникова, Сергій Захарченко. Комп’ютерні мережі, 2022.

2. Євсеєв С. П., Дженюк Н.В. Комп’ютерні мережі Книга 1 Технології комп’ютерних мереж, 2024.

3. А. О. Азарова, Н. В. Лисак. Комп’ютерні мережі та телекомунікації, 2014.

4. О.С. Роговий, С.В., С.В. Мазур. Комп’ютерні мережі та програмне забезпечення, 2019.

5. Методичні вказівки до виконання дипломної роботи бакалавра за напрямом підготовки 6.050102 «Комп'ютерна інженерія» напрямок «Комп’ютерні мережі» [Електронний ресурс] – Режим доступу: https://eguru1.tk.te.ua/pluginfile.php/76350/mod_resource/content/1/Metod_vkaziv_DP.pdf – дата звернення: 12.05.2025.

6. Настанова з інсталації Debian [Електронний ресурс] – Режим доступу: https://d-i.debian.org/manual/uk.amd64/install.uk.pdf – дата звернення: 30.05.2025.

7. Встановлення сервера FTP vsftpd [Електронний ресурс] – Режим доступу: https://vps.ua/wiki/ukr/install-vsftpd/ - дата звернення: 30.05.2025.

8. How to install and configure isc-dhcp-server [Електронний ресурс] – Режим доступу: https://documentation.ubuntu.com/server/how-to/networking/install-isc-dhcp-server/ - дата звернення: 30.05.2025.

9. Встановлення та налаштування проксі-сервера Squid [Електронний ресурс] – Режим доступу: https://veesp.com/ukr/blog/how-to-setup-squid-on-ubuntu/ - дата звернення: 03.06.2025.

10. Access the CLI via PuTTY using a Console Connection [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-

300-series-managed-switches/smb4984-access-the-cli-via-putty-using-a-console-connection-on-300-a.html – дата звернення: 03.06.2025.

11. UniFi Switch US-24 Quick Start Guide [Електронний ресурс] – Режим доступу: https://dl.ubnt.com/guides/UniFi_Switch/UniFi_PoE_Switch_US24_QSG.pdf – дата звернення 05.06.2025.

12. Налаштування роутера TP-Link [Електронний ресурс] – Режим доступу: https://www.briz.ua/help/goluboi-interfeis_link – дата звернення: 10.06.2025

13. Як підключити та налаштувати роботу принтера через мережу [Електронний ресурс] – Режим доступу: https://lanet.help/blog/yak-pidklyuchyty-ta-nalashtuvaty-robotu-pryntera-cherez-merezhu/ - дата звернення: 10.06.2025.

14. Як перевірити пінг через командний рядок [Електронний ресурс] – Режим доступу: https://hostiq.ua/wiki/ukr/ping/ - дата звернення: 10.06.2025.

15. Archer User Guide [Електронний ресурс] – Режим доступу: https://www.tp-link.com/us/user-guides/Archer-MR200_V4/chapter-6-network-security#ug-sub-title-1 – дата звернення: 13.06.2025.

16. Zabbix: Що це і як ним користуватися [Електронний ресурс] – Режим доступу: https://alexhost.com/uk/faq/zabbix-what-it-is-and-how-to-use-it/ - дата доступу: 13.06.2025.

17. Знайомство Cisco Packet Tracer [Електронний ресурс] – Режим доступу: https://nickshevtsov.blogspot.com/2017/10/cisco-packet-tracer.html – дата доступу: 15.0.6.2025.

18. Пожежна безпека на робочому місці: обов'язки роботодавця [Електронний ресурс] – Режим доступу: https://t1p.de/8add8 – дата доступу 17.06.2025.

19. Вимоги виробничої санітарії до робочого місця [Електронний ресурс] – режим доступу: https://oppb.com.ua/articles/gigiyena-pratsi-v-podrobytsyah-vymogy-vyrobnychoyi-sanitariyi-do-robochogo-mistsya – дата доступу:17.06.2020

ДОДАТКИ

Додаток А. Порівняльна характеристика керованих комутаторів третього рівня.

Таблиця А1. порівняльна характеристика керованих комутаторів третього рівня:

	Обрана модель	Аналог 1	Аналог 2
Назва	Cisco C1300-24P-4G	HPE Aruba Instant	TP-Link TL-SG3452X
Фото			
Форм-фактор	1U	1U	1u
Розміри, мм	445×299×44 мм	442×304×44	440×220×44
Кількість портів	24	24	48
Пропускна здатність, Гбіт/с	124	176	176
Автовизначення швидкості	10/100/1000 Mbps	10/100/1000 Mbps	10/100/1000 Mbps
Таблиця MAC-адрес	16 000	16 000	16 000
Підтримка VLAN	Layer 2/3, 4 k+ 802.1Q VLAN, L3	L3: VLAN, STP, RIP, OSPF, ACL	L3: 802.1Q VLAN
Енерго-споживання, Вт	230	445	32.7
Вартість, грн	36 400	24 485	27999

Додаток Б. Порівняльна характеристика серверів.

Таблиця Б1. Порівняльна характеристика серверів:

	Обрана модель	Аналог 1	Аналог 2
Назва	Dell PowerEdge T40 v04	PRIMERGY TX1310 M3	ARTLINE Business T22 v02
Фото			
Процесор	1× Intel Xeon E-2224G	1× Intel Xeon E3-1200 v6	AMD Ryzen 3 Pro 4350G
Об’єм ОЗП Гб	32	32	32
Тип ОЗП	4× 2666 MT/s DDR4 UDIMM	4 × DDR4 ECC	4 × DDR4 UDIMM
Дискова підсистема	До 3× 3,5″ cabled SATA HDD/SSD, Intel RSTe RAID 0/1/5/10	До 3× 3,5″ cabled SATA HDD/SSD, Intel RSTe RAID 0/1/5/10	4 × 3.5″ SATA HDD, AMD RAIDXpert2 RAID 0/1/10
БЖ, Вт	300	250	400
Мережева карта	1× RJ-45 GigE (Intel i219), 10/100/1000	1× RJ-45 GigE (Intel i219), 10/100/1000	1× RJ-45 GigE (Intel i219), 10/100/1000
Кріплення сервера	Tower	Tower	Tower
Вартість, грн	30 000	23 540	32 900

Додаток В. Порівняльна характеристика комутаторів другого рівня

Таблиця В1. Порівняльна характеристика комутаторів другого рівня:

	Обрана модель	Аналог 1	Аналог 2
Назва	Ubiquiti USW-24-POE Gen 2	H3C SMB-S1224F	TP-Link TL-SG3428X
Фото			
Макс. пропускна спроможність, Гбіт/с	52	48	128
Управління	L2	L2	L2
Кількість портів	24	24	24
VLAN	IEEE 802.1Q	IEEE 802.1Q	IEEE 802.1Q
Швидкість пересилання пакетів, мп/с	39	35.7	95.2
Розмір таблиці MAC, К	8	8	16
Потужність споживання, Вт	25	20	23
Живлення від PoE-in	Присутнє	Відсутнє	Відсутнє
Ethernet порти (Uplink)	2× SFP 1 GbE	2× SFP 1 GbE	4× 10 GbE SFP+
Живлення	AC 100–240 V	AC 100–240 V	AC 100–240 V
Вартість, грн	14 550	12 670	10 799

Додаток Г. Порівняльна характеристика роутерів.

Тавбиця Г1. Порівняльна характеристика роутерів:

	Обрана модель	Аналог 1	Аналог 2
Назва	TP-Link Archer AX80	Keenetic Giant	Xiaomi Redmi AX5400
Фото			
Швидкість LAN портів, Гбіт/с.	1×2.5 GbE WAN/LAN, 3×1 GbE LAN	1×GbE WAN/SFP combo, 8×GbE LAN	1×1 GbE WAN, 3×1 GbE LAN
Частота роботи двохдіапазонного Wi-Fi, ГГц.	5 + 2.4	5 + 2.4	5 + 2.4
Швидкість Wi-Fi, Мбіт/с.	6000	1200	5300
Стандарт зв'язку Wi-Fi	802.11ax (Wi-Fi 6), MU-MIMO 4×4, OFDMA)	802.11ac Wave 2, MU-MIMO)	802.11ax (Wi-Fi 6), MU-MIMO, HE160
Інтерфейси, Мбіт/с.	1 x 2.5 Гбіт/с WAN/LAN 1 x 1 Гбіт/с WAN/LAN 3 x 1 Гбіт/с LAN порти	8 x RJ-45 Gigabit Ethernet (1 Гбіт/с) LAN 1 x Combo RJ-45/SFP Gigabit Ethernet (1 Гбіт/с)	1 x 2.5 Gigabit WAN/LAN 3 x Gigabit LAN
Кількість антен	9	4	4
Кількість WAN	2	1	2
Підтримка протоколів	OpenVPN, PPTP, L2TP; HomeShield; WPA3	KeeneticOS: VLAN, захист, Mesh, OpenVPN, USB-модеми	WPA-PSK/WPA2-PSK/WPA3-SAE; Mesh, NPU
Вартість, грн.	7 200	6 370	6 100

Додаток Д. Порівняльна характеристика принтерів.

Таблиця Д1. Порівняльна характеристика принтерів:

	Обрана модель	Аналог 1	Аналог 2
Назва	HP LaserJet M211dw	Kyocera Ecosys P2235dw	Pantum P3300DN
Фото			
Тип	монохромний, лазерний	монохромний, лазерний	монохромний, лазерний
Підключення	Gigabit Ethernet, USB-B, Wi-Fi	Ethernet, USB-B, Wi-Fi	Ethernet, USB-B
Кількість картриджів	1	1	1
Формат	A4	A4	A4
Роздільна здатність друку, dpi	600x600	1200x1200	1200x1200
Ч/б друк, стр/хв.	29	35	33
Друк першої сторінки, сек	7	6	8
Лоток подачі, арк.	150	250	250
Лоток видачі, арк.	100	250	100
Передача даних	Ethernet 1 Gb/s; Wi-Fi Direct, AirPrint, Mopria	Ethernet 1 Gb/s; PCL5/6, KPDL3, USB; Wi-Fi	Ethernet 10/100 Mb/s; PCL5e/6, PS3, PDF
Вартість, грн.	8 000	11 120	7 355

Додаток Е. Порівняльна характеристика ДБЖ.

Таблиця Е1. Порівняльна характеристика ДБЖ:

	Обрана модель	Аналог 1	Аналог 2
Назва	ДБЖ APC Smart-UPS 750VA 230V	PowerWalker VFI 10000	Eaton Ellipse ECO 800VA
Фото			
Форм-фактор	Tower	Tower, Rackmount	Tower
Активна потужність, Вт	600	9 000	600
Повна потужність, ВА	750	10 000	800
Форма вихідного сигналу	Синусоїдна	Синусоїдна	Синусоїдна
Робота при макс. навантаженні, хв	5	3	5
Захист	AVR, smartslot, LCD	AVR, EPO, REPO, OBM	IEC 61643-1, Ecocontrol
Розміри, мм	363 × 138 × 161 мм	688 × 190 × 442 мм	263 × 81 × 235 мм
Вартість, грн	31 500	126 720	8 000

Додаток Ж. Налаштування комутатора третього рівня.

Налаштування комутатора третього рівня Cisco C1300-24P-4G:

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW_3
```

Створення VLAN

```
SW_3(config)# vlan 10
SW_3(config-vlan)# name Software_Dev
SW_3(config-vlan)# exit

SW_3(config)# vlan 65
SW_3(config-vlan)# name Project_Management
SW_3(config-vlan)# exit
```

Конфігурація Trunk-портів

```
SW_3(config)# interface range gigabitEthernet 0/0/1 - 2
SW_3(config-if-range)# switchport trunk encapsulation dot1q
SW_3(config-if-range)# switchport mode trunk
SW_3(config-if-range)# no shutdown
SW_3(config-if-range)# exit
```

Призначення портів до VLAN 10

```
SW_3(config)# interface gigabitEthernet 0/0/3
SW_3(config-if)# switchport mode access
SW_3(config-if)# switchport access vlan 10
SW_3(config-if)# exit

SW_3(config)# interface gigabitEthernet 0/0/4
SW_3(config-if)# switchport mode access
SW_3(config-if)# switchport access vlan 10
```

```
SW_3(config-if)# exit

SW_3(config)# interface gigabitEthernet 0/0/5
SW_3(config-if)# switchport mode access
SW_3(config-if)# switchport access vlan 10
SW_3(config-if)# exit

SW_3(config)# interface gigabitEthernet 0/0/6
SW_3(config-if)# switchport mode access
SW_3(config-if)# switchport access vlan 10
SW_3(config-if)# exit

SW_3(config)# interface gigabitEthernet 0/0/7
SW_3(config-if)# switchport mode access
SW_3(config-if)# switchport access vlan 10
SW_3(config-if)# exit

SW_3(config)# interface gigabitEthernet 0/0/8
SW_3(config-if)# switchport mode access
SW_3(config-if)# switchport access vlan 10
SW_3(config-if)# exit
```

Призначення портів до VLAN 65

```
SW_3(config)# interface gigabitEthernet 0/0/9
SW_3(config-if)# switchport mode access
SW_3(config-if)# switchport access vlan 65
SW_3(config-if)# exit

SW_3(config)# interface gigabitEthernet 0/0/10
```

```
SW_3(config-if)# switchport mode access
SW_3(config-if)# switchport access vlan 65
SW_3(config-if)# exit
```

IP-адреси для SVI

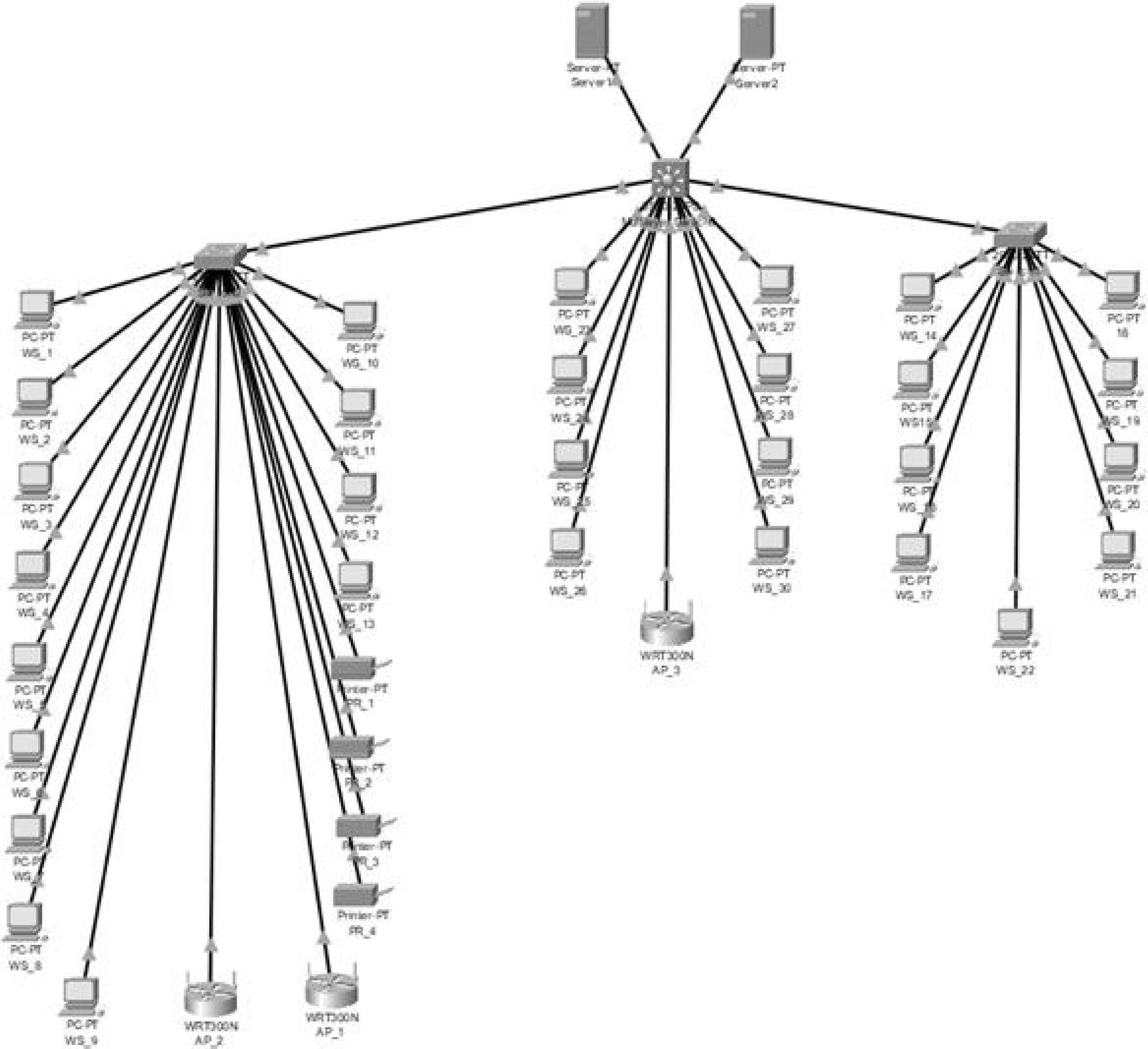
```
SW_3(config)# interface vlan 10
SW_3(config-if)# ip address 192.168.10.254 255.255.255.0
SW_3(config-if)# exit

SW_3(config)# interface vlan 65
SW_3(config-if)# ip address 192.168.65.254 255.255.255.0
SW_3(config-if)# exit
```

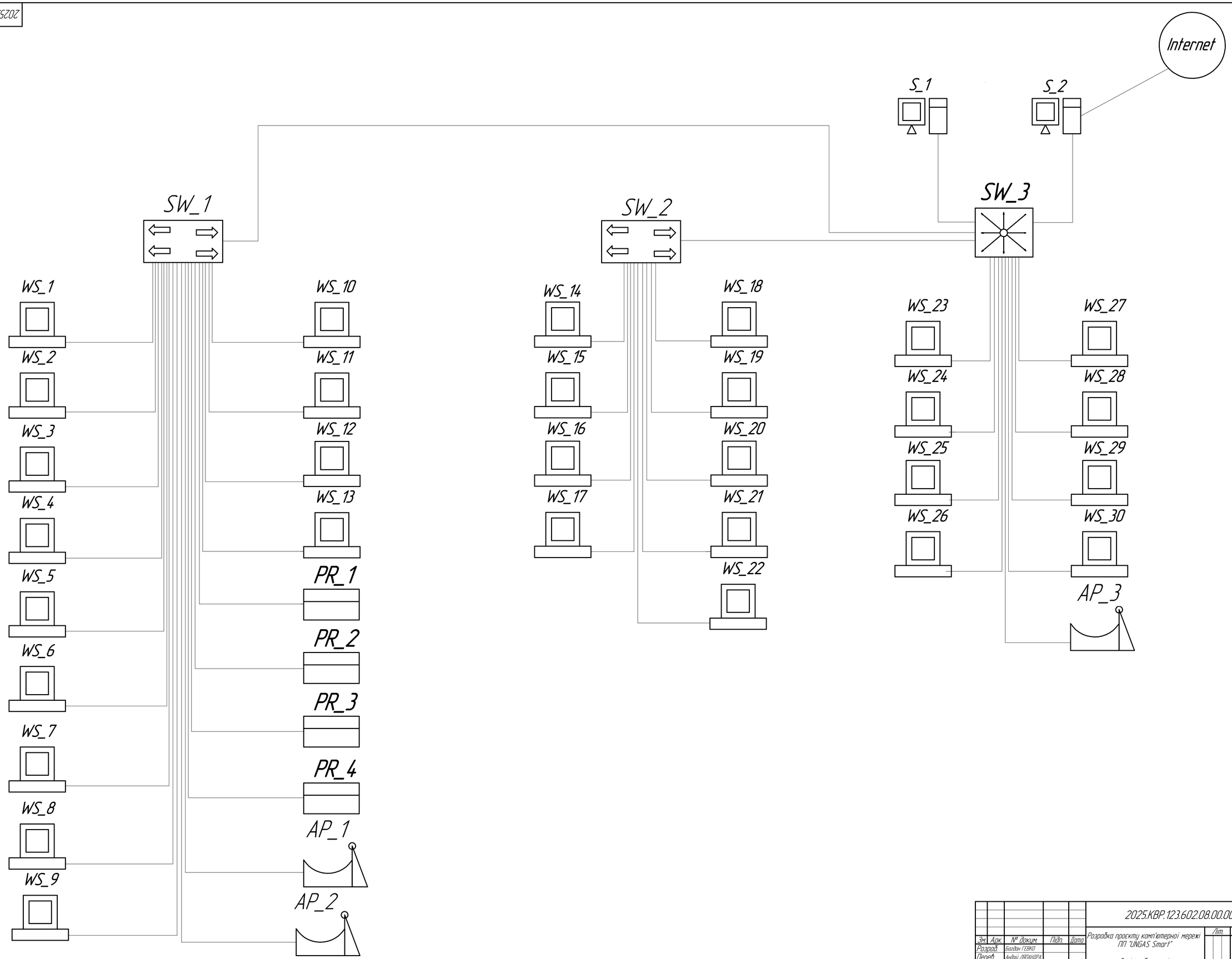
Шлюз за замовчуванням

```
SW_3(config)# ip default-gateway 192.168.10.20
```

Вимкнення маршрутизації між інтерфейсами

```
SW_3(config)# ip routing
SW_3(config)# exit
```


Server-PT
Server1
Server-PT
Server2
PC-PT
WS_1
PC-PT
WS_2
PC-PT
WS_3
PC-PT
WS_4
PC-PT
WS_5
PC-PT
WS_6
PC-PT
WS_8
PC-PT
WS_9
WRT300N
AP_2
WRT300N
AP_1
PC-PT
WS_10
PC-PT
WS_11
PC-PT
WS_12
PC-PT
WS_13
Printer-PT
PR_1
Printer-PT
PR_2
Printer-PT
PR_3
Printer-PT
PR_4
PC-PT
WS_24
PC-PT
WS_25
PC-PT
WS_26
PC-PT
WS_27
PC-PT
WS_28
PC-PT
WS_29
PC-PT
WS_30
WRT300N
AP_3
PC-PT
WS_14
PC-PT
WS_15
PC-PT
WS_16
PC-PT
WS_17
PC-PT
WS_22
PC-PT
18
PC-PT
WS_19
PC-PT
WS_20
PC-PT
WS_21



Перш. застос.

Справ. №

Підп. і дата

Інв. № дубл.

Взам. інв. №

Підп. і дата

Інв. № оригіл.

Зм.	Арк.	№ докум.	Підп.	Дата
Розроб.		Богдан ГЕВКО		
Перев.		Андрій ЛЯПАНДРА		
Т.контр.				
Рецензія.				
Н.контр.		Віктор ПРИЙМАК		
Затв.				

2025.КВР.123.602.08.00.00 /ЛТ

Розробка проекту комп'ютерної мережі ПП "UNGAS Smart"

Логічна Топологія

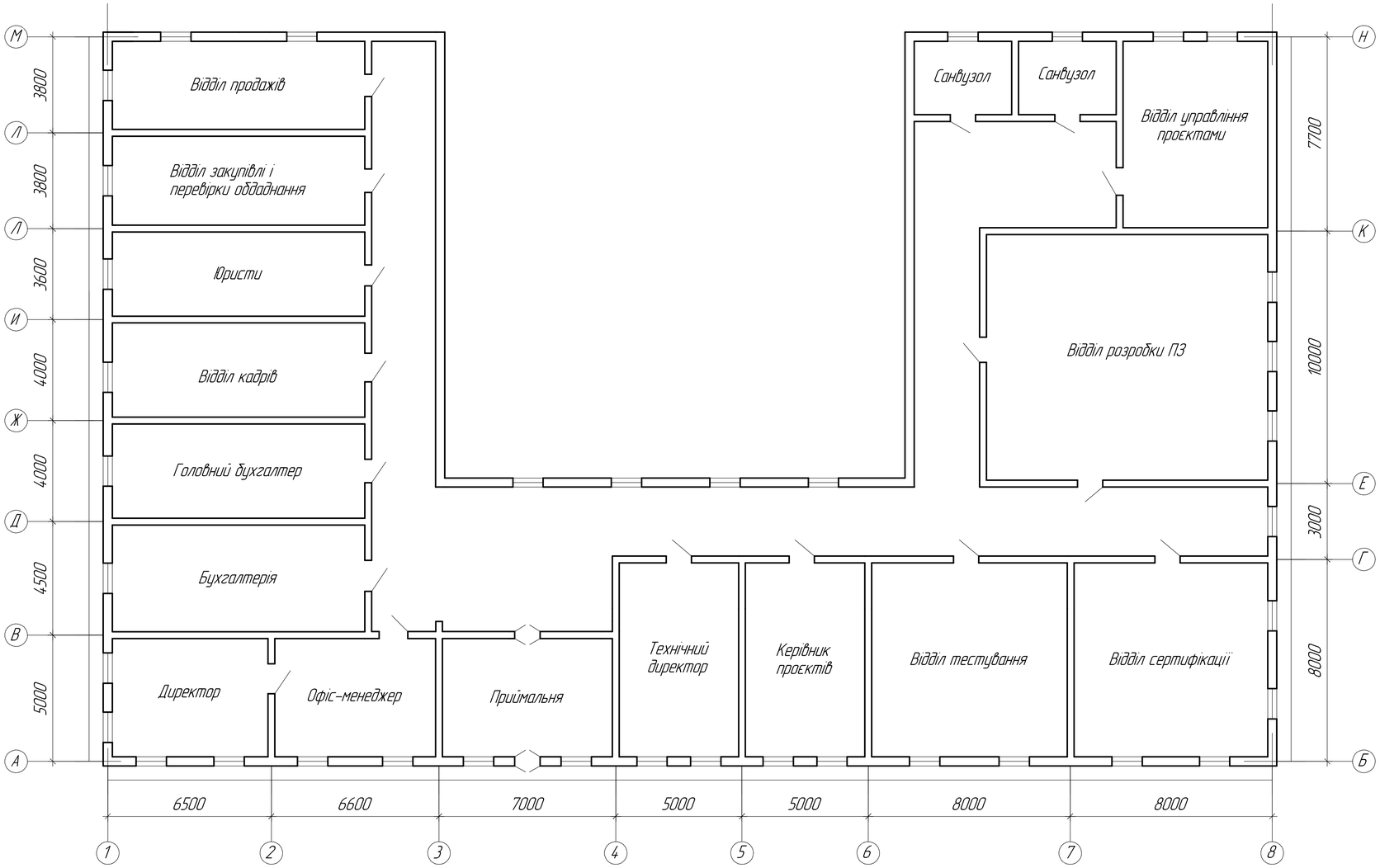
Літ.	Маса	Масштаб
Аркуш	Аркушів 1	

ВСП "ТФК ТНТУ", гр. КІ-602

м. Тернопіль

Копіював

Формат А1



						2025.КВР.123.602.08.00.00 ПП	
Зм.	Арк.	№ докум.	Підп.	Дата	Розробка проекту комп'ютерної мережі ПП "UNGAS Smart"	Літ.	Маса / Масштаб
Розроб.		Богдан ГЕВКО					1:100
Перев.		Андрій ЛЯПАНДРА			План приміщення	Аркуш	Аркушів 1
Т.контр.						ВСП "ТФК ТНТУ", гр. КІ-602	
Реценз.						м. Тернопіль	
Н.контр.		Віктор ПРИЙМАК					
Затв.							

Копіював Формат А1

Перш. застос. | Сповід. № | Підп. і дата | Інв. № дубл. | Взам. інв. № | Підп. і дата | Інв. № орига.

Таблиця техніко-економічних показників

№ п/п	Показник	Одиниця вимірювання	Значення
1	Топологія мережі	–	Гібридна
2	Середовище передачі даних	–	кабель UTP cat.6
3	Кількість комутаторів	шт.	3
4	Керований комутатор, L3	–	Cisco C1300-24P-4G
5	Керований комутатор, L2	–	Ubiquiti USW-24-Poe Gen2
6	Кількість точок доступу	шт.	3
7	Модель точки доступу	–	TP-Link Archer AX80
8	Кількість мережевих принтерів	шт.	4
9	Модель мережевого принтера	–	HP LaserJet M211dw
10	ДБЖ	–	APC Smart-Ups 750VA
11	Операційні системи серверів	–	Debian 11
12	Операційні системи робочих станцій	–	Windows 10 Pro
13	Кількість робочих станцій	шт.	30
14	Собівартість	грн.	386836,89
15	Плановий прибуток	грн.	216628,66
16	Ціна	грн.	603465,55
17	Термін окупності	рік	1,8

Перш. застос.

Справ. №

Інв. № дубл. | Підп. і дата

Взам. інв. № | Підп. і дата

Інв. № подл.

Зм.	Арк.	№ докум.	Підп.	Дата
Розроб.		Богдан ГЕВКО		
Перев.		Андрій ЛЯПАНДРА		
Т.контр.				
Реценз.				
Н.контр.		Віктор ПРИЙМАК		
Затв.				

2025.КВР.123.602.08.00.00 ТБ

Розробка проекту комп'ютерної мережі ПП "UNGAS Smart"

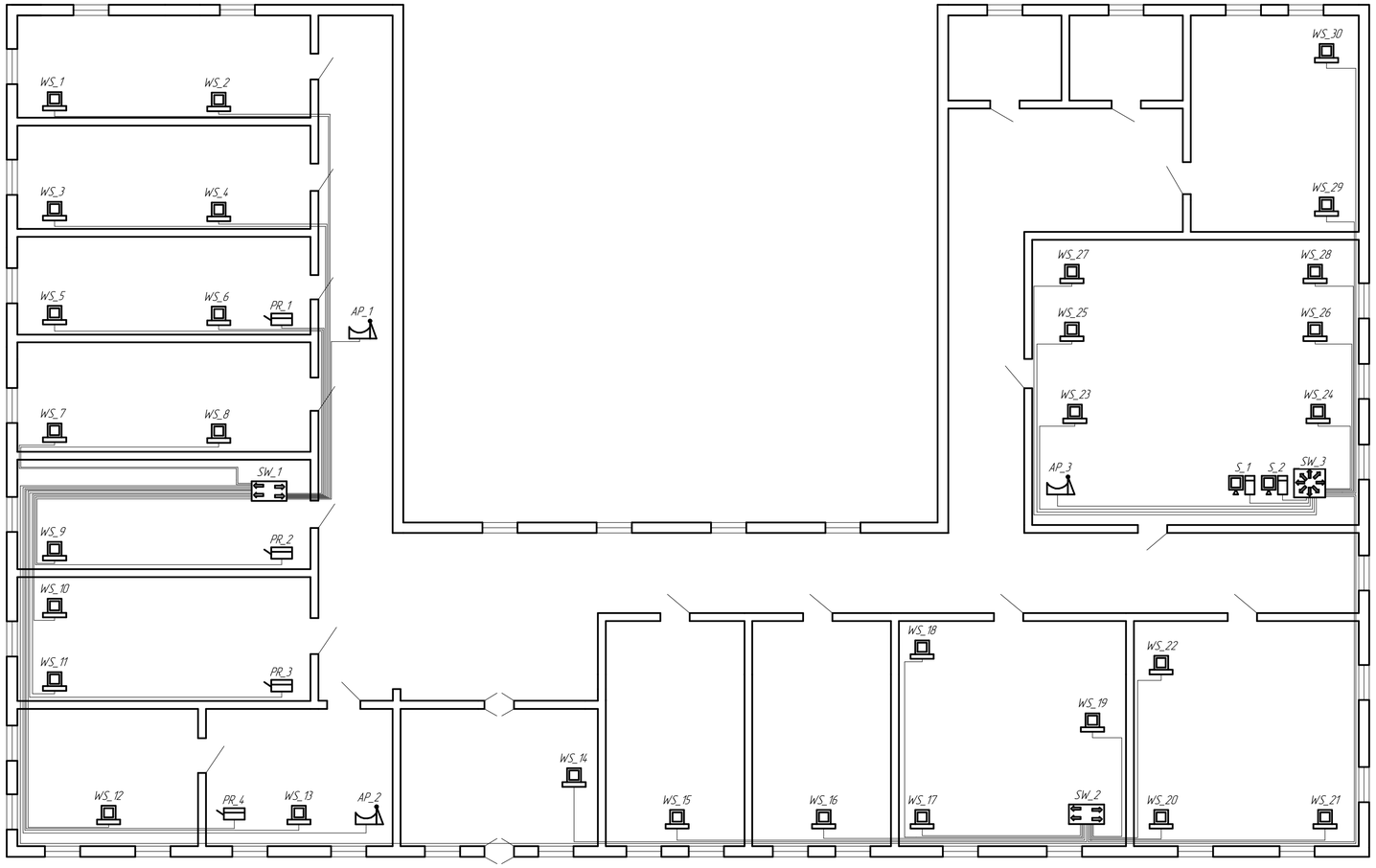
Таблиця техніко-економічних показників

Літ.	Маса	Масштаб
Аркуш	Аркушів 1	

ВСП "ТФК ТНТУ", гр. КІ-602
м. Тернопіль

Копіював

Формат А1



Зм.	Арк.	№ докум.	Підп.	Дата	2025.КВР.123.602.08.00.00 ФТ		
Розроб.		Богдан ГЕЙКО			Розробка проекту комп'ютерної мережі ІПП "UNGAS Smart"	Літ.	Маса	Масштаб
Перев.		Андрій ЛЯТАНДРА						1:100
Т.контр.					Фізична Топологія	Аркуш	Аркушів 1	
Реценз.						ВСП "ТФК ТНТУ", гр. КІ-602		
Н.контр.		Віктор ПРИЙМАК				м. Тернопіль		
Затв.								

Копіював

Формат А1

Перш. застос.

Справ. №

Підп. і дата

Інв. № дубл.

Взам. інв. №

Підп. і дата

Інв. № ориг.

Таблиця IP-адрес

п/п	Назва вузла	Місце розташування	IP-адреса	Маска підмережі	Шлюз	Група VLAN
1	S_2	Відділ розробки ПЗ	X.X.X.X	Призначає провайдер	–	-
			192.168.10.20	/24	–	10
2	SW_3	Відділ розробки ПЗ	192.168.10.50	/24	–	10
3	S_1	Відділ розробки ПЗ	192.168.10.22	/24	192.168.10.20	10
4	WS_1	Відділ продажів	192.168.15.100	/24	192.168.10.20	15
5	WS_2	Відділ продажів	192.168.15.102	/24	192.168.10.20	15
6	WS_3	Відділ закупівлі і перевірки обладнання	192.168.15.104	/24	1192.168.10.20	15
7	WS_4	Відділ закупівлі і перевірки обладнання	192.168.15.106	/24	192.168.10.20	15
8	WS_5	Юристи	192.168.20.108	/24	192.168.10.20	20
9	WS_6	Юристи	192.168.20.110	/24	192.168.10.20	20
10	WS_7	Відділ кадрів	192.168.25.112	/24	192.168.10.20	25
11	WS_8	Відділ кадрів	192.168.25.114	/24	192.168.10.20	25
12	WS_9	Головний бухгалтер	192.168.30.116	/24	192.168.10.20	30
13	WS_10	Бухгалтерія	192.168.30.118	/24	192.168.10.20	30
14	WS_11	Бухгалтерія	192.168.30.120	/24	192.168.10.20	30
15	WS_12	Директор	192.168.35.122	/24	192.168.10.20	35
16	WS_13	Офіс-менеджер	192.168.35.124	/24	192.168.10.20	35
17	WS_14	Приймальня	192.168.40.126	/24	192.168.10.20	40
18	WS_15	Технічний директор	192.168.45.128	/24	192.168.10.20	45
19	WS_16	Керівник проектів	192.168.50.130	/24	192.168.10.20	50
20	WS_17	Відділ тестування	192.168.55.132	/24	192.168.10.20	55
21	WS_18	Відділ тестування	192.168.55.134	/24	192.168.10.20	55
23	WS_19	Відділ тестування	192.168.55.136	/24	192.168.10.20	55
24	WS_20	Відділ сертифікації	192.168.60.138	/24	192.168.10.20	60
25	WS_21	Відділ сертифікації	192.168.60.140	/24	1192.168.10.20	60
26	WS_22	Відділ сертифікації	192.168.60.142	/24	192.168.10.20	60
27	WS_23	Відділ розробки ПЗ	192.168.10.144	/24	192.168.10.20	10
28	WS_24	Відділ розробки ПЗ	192.168.10.146	/24	192.168.10.20	10
29	WS_25	Відділ розробки ПЗ	192.168.10.148	/24	192.168.10.20	10
30	WS_26	Відділ розробки ПЗ	192.168.10.150	/24	192.168.10.20	10
31	WS_27	Відділ розробки ПЗ	192.168.10.152	/24	192.168.10.20	10
32	WS_28	Відділ розробки ПЗ	192.168.10.154	/24	192.168.10.20	10
33	WS_29	Відділ управління проектами	192.168.65.156	/24	192.168.10.20	65
34	WS_30	Відділ управління проектами	192.168.65.158	/24	192.168.10.20	65
35	PR_1	Юристи	192.168.20.200	/24	192.168.10.20	20
36	PR_2	Головний бухгалтер	192.168.30.202	/24	192.168.10.20	30
37	PR_3	Бухгалтерія	192.168.30.204	/24	192.168.10.20	30
38	PR_4	Офіс-менеджер	192.168.35.206	/24	192.168.10.20	35
39	AP_1	Головний бухгалтер	192.168.30.210	/24	192.168.10.20	30
40	AP_2	Офіс-менеджер	192.168.35.212	/24	192.168.10.20	35
41	AP_3	ВідділрозробкиПЗ	192.168.10.214	/24	192.168.10.20	10
42	SW_1	Головний бухгалтер	192.168.30.52	/24	192.168.10.20	30
43	SW_2	Відділ тестування	192.168.55.54	/24	192.168.10.20	55

Перш. застос.

Справ. №

Підп. і дата

Інв. № дубл.

Взам. інв. №

Підп. і дата

Інв. № оригі.

Зм.	Арк.	№ докум.	Підп.	Дата
Розроб.		Богдан ГЕВКО		
Перев.		Андрій ЛЯПАНДРА		
Т.контр.				
Реценз.				
Н.контр.		Віктор ПРИЙМАК		
Затв.				

2025.КРБ.123.602.08.00.00 ТА

Розробка проекту комп'ютерної мережі ПП "UNGAS Smart"

Таблиця IP-адрес

Літ.	Маса	Масштаб
Аркуш	Аркушів 1	

ВСП "ТФК ТНТУ", гр. КІ-602 м. Тернопіль

Копіював

Формат А1