Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

здобувача Потоцького Артема Олеговича
(ПІБ)
академічної групи 123-21-2
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему "Комп'ютерна система торгового центру з детальним опрацюванням побудови, налаштування корпоративної мережі "
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Нікулін С.Л.			
спеціальної частини	проф. Нікулін С.Л.			
розділу розробка корпоративної мережі	проф. Нікулін С.Л.			
Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2025

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

" " *червня* *2025 року*

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

здобувача Потоцького А.О. **академічної групи** 123-21-2
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

за освітньо-професійною програмою 123 «Комп'ютерна інженерія»
(офіційна назва)

на тему "Комп'ютерна система торгового центру з детальним опрацюванням побудови, налаштування корпоративної мережі"

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.05.2022 № 771-л

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2025
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2025
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2025
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2025

Завдання видано _____ проф. Нікулін С.Л.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії 16.06.2025

Прийнято до виконання _____ Потоцький А.О.

РЕФЕРАТ

Пояснювальна записка: 20 с., 4 рис., 3 табл., 1 дод., 8 джерел. Ключові слова: ТОРГОВИЙ ЦЕНТР, БЕЗПЕКА, КОРПОРАТИВНА МЕРЕЖА, СИСТЕМА, ІНФРАСТРУКТУРА, КОНТРОЛЬ.

Об’єкт розробки – комп’ютерна система управління інфраструктурою та мережевою безпекою торгового центру з детальним опрацюванням побудови та налаштування корпоративної мережі.

Мета роботи – створення комп’ютерної системи для забезпечення ефективного управління адміністративною та технічною інфраструктурою торгового центру.

У ході розробки створено багаторівневу комп’ютерну систему, яка дозволяє реалізувати гнучке управління мережею, масштабованість функцій, централізовану систему обліку та моніторингу, інтеграцію з системами контролю доступу та відеоспостереження. Система оптимізована для використання у сучасних торговельних комплексах міста Дніпро.

Основні функції розробленої системи:

контроль та адміністрування корпоративної мережі;

забезпечення безперервної роботи торгового центру;

управління доступом до службових і гостьових Wi-Fi;

облік та моніторинг споживання ресурсів;

підвищення рівня мережевої безпеки торгового центру;

резервне копіювання та аварійне відновлення даних.

Корпоративна комп’ютерна мережа, розроблена у рамках роботи, включає логічне розділення на VLAN-сегменти для адміністрації, орендарів, гостьового доступу. Усі елементи взаємодіють через централізований маршрутизатор із фаєрволом, а керовані комутатори забезпечують ізоляцію трафіку та балансування навантаження.

Модель мережі протестована у програмному середовищі Cisco Packet Tracer.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КС – комп’ютерна система;

ПК – персональний комп’ютер;

КМ – корпоративна мережа;

СКС – структурована кабельна система;

IP-адреса - унікальний ідентифікатор комп'ютера локальної мережі або мережі Інтернет;

TCP/IP - набір протоколів мережі Інтернет;

VLAN – віртуальна локальна мережа;

DHCP – протокол динамічної настройки вузла;

LAN – локальна мережа;

WAN – глобальна мережа;

ISP (від англ. Internet Service Provider)– компанія-постачальник Інтернет-послуг;

SOHO – Small office/home office

ПЗ – програмне забезпечення;

Ethernet – технологія передачі даних по мережі;

Wi-Fi –технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11;

ВСТУП

Об’єкт дослідження:

Комп’ютерна мережа торгового центру, яка об’єднює в своїй інфраструктурі технічні, адміністративні та торговельні елементи в єдину систему. Вона приймає участь в автоматизованій системи обліку у процесах торгівлі, відеоспостереження, контроль доступу, обслуговування орендарів, а також забезпечує збереження і захист даних підприємства.

Мета дослідження:

Створення та реалізація комплексної корпоративної мережі для торговельного центру, яка забезпечуватиме злагоджену роботу таких структур: адміністративних, безпеки, технічної підтримки та орендарів. Система повинна підтримувати діяльність системи внутрішнього обміну інформацією, обслуговування касових терміналів, а також включати інструменти резервного копіювання й кібербезпеки.

При розробці враховано можливість для масштабування та вдосконалення апаратної частини мережі, що дозволятиме швидше додавати користувачів, розширювати функціональність мережі й впроваджувати актуальні рішення у сфері безпеки та аналітики даних поведінки відвідувачів.

Особливості системи:

Модульна структура, дає змогу гнучко адаптувати як програмні, так і апаратні компоненти під індивідуальні потреби підприємства.
Об’єднана мережа - забезпечує надійне з’єднання між усіма структурними підрозділами, підтримку віддаленого доступу, управління правами користувачів та моніторинг IT-інфраструктури в реальному часі.

Етапи реалізації проєкту:

Впровадження проходило поетапно: від аналізу вимог торговельного об’єкта та формування технічного завдання – до проєктування мережі за допомогою Cisco Packet Tracer. Особливу увагу приділено поділу мережевого трафіку на логічні сегменти (VLAN), забезпеченню конфіденційності та цілісності

переданих даних, стабільній роботі системи при високих навантаженнях і досягненню високої відмовостійкості.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика підприємства та умов застосування комп’ютерної системи

У межах даного проєкту впровадження здійснюється на базі торгового центру – багатоповерхової будівлі з розвиненою інфраструктурою, яка включає численні приміщення для адміністративного, торговельного та сервісного призначення. Для такої структури об'єкта є необхідність створення сучасної комп’ютерної мережі, здатної забезпечити стабільно швидку та захищену передачу даних між усіма функціональними зонами, зокрема між адміністрацією, орендарями, технічним персоналом і службами безпеки.

Передбачається, що комп’ютерна інфраструктура покриватиме такі основні ділянки торгового центру:

адміністративні приміщення (включно з офісами управління, бухгалтерією та технічними підрозділами);

комерційні площі, які орендуються (магазини, заклади харчування, сервісні павільйони);

відкриті зони загального користування (гостьовий Wi-Fi, інформаційні кіоски);

серверну кімнату;

системи охорони та відеоспостереження.

Будівля поділяється на кілька рівнів, частина приміщень перебуває в оренді сторонніх компаній. Це вимагає планувати мережеву структуру з акцентом на розділення трафіку, шляхом створення незалежних сегментів, що запобігає витоку корпоративних даних.

Основні вимоги до мережевої інфраструктури в умовах експлуатації в торговому центрі належать:

висока швидкість обміну даними для стабільної роботи торгівельних систем;

надійність та відсутність простоїв завдяки резервним каналам та джерелам живлення;

можливість масштабування – швидке додавання нових пристроїв чи точок доступу;

інформаційна безпека – автентифікація користувачів, обмеження доступу, захист від кібератак;

централізоване керування і можливість дистанційного адміністрування.

З огляду на характер об’єкта, особлива увага приділяється гібридному підходу до мережевої архітектури: критичні компоненти (сервери, відеоспостереження, ПК в адміністрації) підключаються через дротове з’єднання (Ethernet), тоді як для клієнтів і мобільного персоналу використовуються бездротові технології (Wi-Fi).

Таким чином, впроваджувана комп’ютерна мережа стане фундаментом для ефективного управління торговим центром, шляхом забезпеченням стабільності бізнес-процесів, високим рівень сервісу для орендарів і зручність для відвідувачів.

1.2 Аналіз сучасних технічних рішень у сфері та визначення напрямів для реалізації завдань

У контексті цифровізації торгових центрів комп’ютерні мережі відіграють ключову роль у спрощені роботи всіх структур – від адміністративного управління до технічного обслуговування та сервісів для орендарів і відвідувачів. Ефективна інформаційна інфраструктура створює єдине середовище для обміну даними та координації дій, що є критично важливим для сучасних торгівельно-розважальних центрів.

Нижче розглянуто найбільш поширені технічні рішення для побудови корпоративних мереж у сфері громадського обслуговування з них:

1. Структуровані кабельні системи (СКС)
Основою мережевої інфраструктури сучасних ТЦ є СКС, які забезпечують стабільне дротове підключення у всіх функціональних зонах – від адміністративних до технічних. Найчастіше застосовуються кабелі категорій

5e, 6/6A що дозволяє реалізувати високошвидкісну та масштабовану мережу.

2. Централізоване керування інфраструктурою
Для належного адміністрування мережі використовуються спеціалізовані програмні комплекси – наприклад, Cisco Prime, UniFi Controller тощо. Вони дозволяють здійснювати моніторинг, конфігурацію та оптимізацію мережевих процесів, а також швидко реагувати на потенційні проблеми чи навантаження.

3. Сегментовані бездротові мережі
Wi-Fi-мережі в торгових центрах будуються з урахуванням поділу на окремі сегменти – для співробітників, клієнтів і орендарів. Системи контролю доступу, авторизація користувачів і аналіз трафіку дозволяють забезпечити безпечне та контрольоване використання бездротових ресурсів.

4. IP-системи відеоспостереження
Сучасні рішення базуються на інтеграції камер до IP-мереж, що забезпечує централізоване керування, запис та аналіз відеоданих. Такий підхід підвищує рівень безпеки об’єкта, дає змогу швидко переглядати події та зберігати архіви відеозаписів.

5. Комплексні системи захисту інформації
Для запобігання зовнішнім загрозам використовуються інструменти кібербезпеки, серед яких: брандмауери, антивірусні шлюзи, VPN-технології, VLAN-ізоляція, а також системи виявлення атак (IDS/IPS). Такі засоби сприяють збереженню конфіденційності та цілісності даних.

6. Хмарні сервіси та віртуалізація
З метою оптимізації витрат і спрощення адміністрування дедалі частіше застосовуються віртуалізовані серверні середовища та хмарні технології. Вони забезпечують гнучкість у масштабуванні, розміщенні сервісів (CRM, баз даних, відеоархівів) і зменшують потребу в фізичному обладнанні.

Напрями реалізації поставлених завдань:

Проєктування гібридної мережевої інфраструктури, яка об’єднує дротові та бездротові сегменти з можливістю подальшого розширення.

Впровадження модульної побудови мережі для полегшення інтеграції нових сервісів і систем.

Застосування концепції програмно-визначених мереж (SDN) для централізованого контролю за маршрутизацією трафіку.

Використання IoT-рішень для моніторингу інженерних систем, відеоспостереження, клімат-контролю, енергоспоживання тощо.

Автоматизація процесів резервного копіювання та реалізація комплексної стратегії кіберзахисту для безпеки критично важливих даних.

1.3 Розробка схеми організаційної структури підприємства

Управління корпоративною мережею торгового центру є невід'ємною частиною загальної системи керування об'єктом, що забезпечує безперебійну діяльність адміністративного персоналу, орендарів та клієнтів. Основою ефективного функціонування є надійне мережеве обладнання, централізоване адміністрування та злагоджена робота служб технічної підтримки.

У структурі управління комп'ютерною мережею можна виділити такі ключові компоненти:

Серверна інфраструктура, розміщена у спеціально виділеному приміщенні, забезпечує обробку та зберігання всієї важливої інформації: облікових даних користувачів, журналів доступу, контрактів орендарів, баз даних з обліку техніки, технічної документації та комерційних звітів. Сервери відповідають за роботу веб-ресурсів торгового центру, корпоративної пошти, VPN-доступу та внутрішнього документообігу.

Маршрутизатори та комутатори є основними пристроями для розподілу трафіку між підрозділами торгового центру, зонами бездротового доступу та підключення до зовнішніх мереж. Вони мають бути налаштовані на підтримку політик безпеки, сегментації мережі (наприклад, ізоляція трафіку Wi-Fi від внутрішньої адміністративної мережі), а також резервного маршрутизування на випадок аварій.

Корпоративна електронна пошта та система повідомлень виступають основним каналом комунікації між адміністрацією, технічними службами та

орендарями. Через ці системи передаються повідомлення щодо технічного обслуговування, оновлення інфраструктури, зміни в договорах або планах заходів.

Взаємодія між відділами реалізована через електронні сервіси з централізованим керуванням ролями та правами доступу. Наприклад, технічна служба має доступ до систем моніторингу обладнання, бухгалтерія – до захищених фінансових даних, а адміністрація – до загальної системи управління орендарями.

Технічна підтримка здійснює щоденний контроль за працездатністю обладнання, включаючи перевірку серверів, діагностику збоїв у мережі, підтримку користувачів, організацію кабельного менеджменту та резервне копіювання. Відділ має бути тісно інтегрований з іншими службами: групою програмістів (для розробки та оновлення системного ПЗ) та інженерним відділом (для забезпечення фізичної інфраструктури).

У разі виникнення технічних проблем працівники повідомляють відповідальних осіб через корпоративну пошту. Після фіксації звернення начальник відповідного підрозділу передає завдання на вирішення технічному персоналу. Така система дозволяє оперативно реагувати на інциденти та мінімізувати час простою.

Таким чином, методи керування корпоративною мережею торгового центру базуються на принципах централізації, ролевого доступу, автоматизації обліку і моніторингу, регулярного обслуговування інфраструктури та швидкої міжвідділової взаємодії, що забезпечує безперебійну діяльність усіх служб і комфорт користувачів мережі.

1.4 Аналіз організаційної структури підприємства

Сучасний торговий центр – це комплексна організаційна система, що об’єднує в собі різні напрями діяльності: комерційні операції, адміністративне управління, технічне забезпечення та обслуговування клієнтів. Основним завданням функціонування такого об’єкта є створення

сприятливих умов як для відвідувачів, так і для бізнес-орендарів, а також ефективна координація внутрішніх процесів, контроль інфраструктури й забезпечення інформаційної безпеки.

У складі управлінської структури торгового центру виокремлюються наступні ключові відділи:

Адміністративний підрозділ – займається загальним керівництвом об’єктом, визначає стратегію розвитку, координує роботу з орендарями, слідкує за дотриманням політик та взаємодіє із зовнішніми організаціями.

Технічна служба – відповідає за технічну справність усіх інженерних систем, включаючи енергозабезпечення, вентиляцію, водопостачання та інші комунікації. Також забезпечує впровадження новітніх технологічних рішень.

Відділ інформаційних технологій (IT) – виконує функції проектування, підтримки та захисту комп’ютерної інфраструктури. Забезпечує стабільну роботу серверів, точок бездротового доступу, робочих станцій, а також відповідає за відеонагляд і цифрові сервіси.

Служба безпеки – контролює охорону об’єкта, адмініструє системи відеоспостереження, сигналізації, доступу до приміщень та пожежну безпеку.

Фінансово-бухгалтерський відділ – виконує облік фінансових операцій, контролює надходження і витрати, веде документацію з орендарями та контрагентами.

Маркетингова команда – займається просуванням торгового центру, плануванням рекламних кампаній, організацією подій, а також підтримкою позитивного іміджу серед відвідувачів і партнерів.

Організаційна модель, як правило, побудована за лінійно-функціональним принципом, що забезпечує чіткий розподіл обов’язків, вертикаль управління та узгоджену взаємодію між підрозділами. Така структура дозволяє оперативно вирішувати поточні завдання, реагувати на критичні ситуації та підтримувати високий рівень сервісу.

Важливу роль у функціонуванні торгового центру відіграє надійна комп’ютерна мережа, яка поєднує всі служби, орендарів та інженерні

системи в єдиний інформаційний простір. Її функціональність охоплює:

Забезпечення доступу до Інтернету у службових та публічних зонах;

Обслуговування платіжних терміналів та касових апаратів;

Підключення камер відеоспостереження з IP-інтерфейсом;

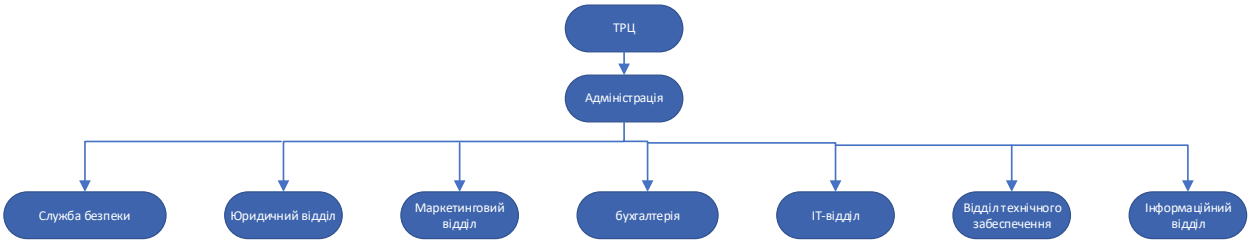
Інтеграцію з хмарними платформами та обліковими системами;

Організацію внутрішнього IP-зв'язку та сервісної підтримки;

Реалізацію механізмів резервного копіювання та кібербезпеки.

Отже, якісно спроєктована комп'ютерна мережа є критично важливим елементом функціональної стабільності торгового центру. У рамках даного проєкту основна увага приділяється її побудові з урахуванням вимог масштабованості, безпеки та надійності.

.



Організаційна структура ТРЦ

1.5 Постановка завдання

У рамках кваліфікаційної роботи передбачається створення повноцінної моделі корпоративної комп'ютерної мережі для торгового центру на основі виданої схеми (див. рисунок) та з урахуванням його географічно розподіленої інфраструктури, функціональних потреб та сучасних технічних вимог.

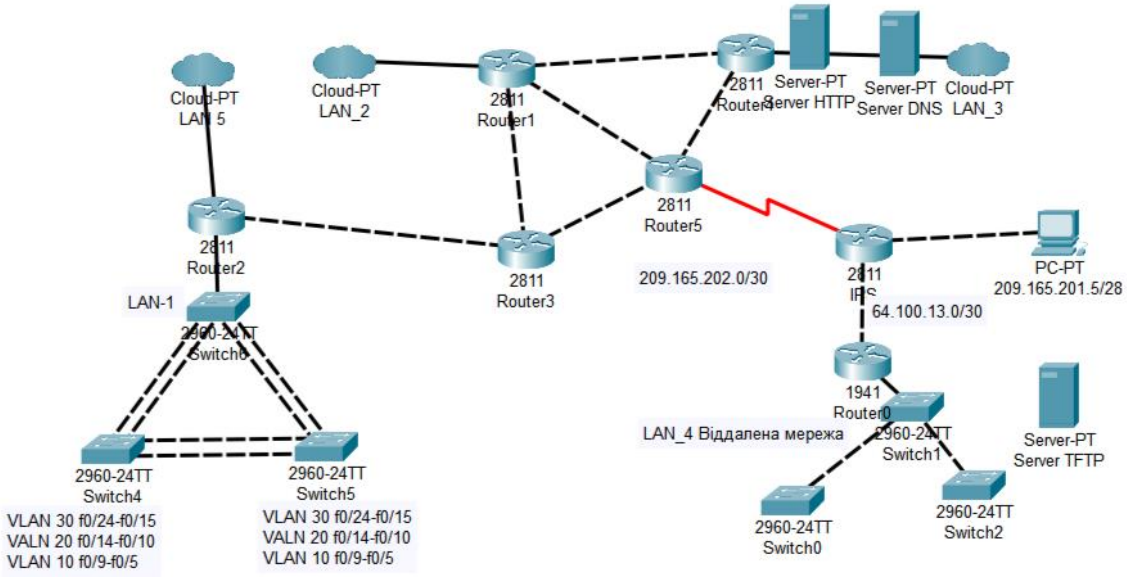


Рисунок 1.1 – Топологія за технічним завданням

Для досягнення поставленої мети необхідно вирішити такі основні завдання:

Розробити ефективну схему IP-адресації, що передбачає раціональне використання адресного простору із застосуванням методу змінної довжини маски підмережі (VLSM) та забезпечує можливість подальшого масштабування.

Спроєктувати та змоделювати мережеву інфраструктуру в програмному середовищі Cisco Packet Tracer з урахуванням використання основних мережевих компонентів – маршрутизаторів, комутаторів, серверів та кінцевих пристроїв.

Реалізувати ключові технології маршрутизації та комутації, зокрема впровадити VLAN для логічної сегментації підмереж, EtherChannel (PAgP) для підвищення пропускної здатності каналів, а також налаштувати протокол динамічної маршрутизації EIGRP для забезпечення стабільної зв’язності між усіма сегментами мережі.

Забезпечити мережеву безпеку, реалізувавши трансляцію мережевих адрес (NAT), налаштування захищеного віддаленого доступу за допомогою IPsec VPN та централізовану аутентифікацію користувачів через протокол RADIUS.

Інтегрувати IoT-рішення, зокрема впровадити систему пожежогасіння на основі Інтернету речей, що передбачає взаємодію між сенсорами, контролером та виконавчими пристроями.

Провести комплексне тестування мережі з використанням службових інструментів та команд (ping, перевірка роботи сервісів DHCP, DNS, HTTP, VPN, RADIUS), щоб переконатися у стабільності та коректності функціонування системи.Реалізація зазначених завдань має на меті створення безпечної, масштабованої та ефективної комп’ютерної мережі, яка може бути застосована як для практичного впровадження в умовах реального підприємства, так і як базовий приклад для навчальних цілей.

2 ТЕХНІЧНІ ВИМОГИ ДО СИСТЕМИ

2.1 Вимоги до системи в цілому

2.1.1 Вимоги до побудови та функціональності комп’ютерної мережі

Для стабільної роботи комп’ютерної інфраструктури в межах торгового комплексу необхідно дотримуватися ряду вимог щодо її архітектури та функціонального наповнення. Мережа повинна відповідати актуальним стандартам безпеки, бути гнучкою до розширення та забезпечувати високу доступність для всіх користувачів – як адміністрації, так і технічних підрозділів, орендарів і клієнтів.

Ключові структурні вимоги:

Організація кабельної системи:

Прокладання кабелів має здійснюватися з використанням спеціалізованих каналів, плінтусів та кріплень, що гарантує безпечне та охайне розташування комунікацій. Обов’язкове маркування кабельних ліній допомагає зменшити час обслуговування і помилок при технічних роботах. Прокладання має враховувати багаторівневу структуру будівлі (наприклад, два поверхи).

Централізоване розміщення активного обладнання:

Розміщення маршрутизаторів, комутаторів і бездротових точок доступу має здійснюватися з урахуванням оптимального покриття та навантаження. Серверна кімната повинна бути обладнана системами охолодження, аварійного електроживлення та контролю доступу.

Інформаційна безпека:

Передбачене впровадження засобів захисту, таких як протоколи автентифікації, шифрування мережевого трафіку та фільтрація доступу. Для ізоляції сегментів мережі створюються VLAN, що дозволяє обмежити доступ на основі функціонального призначення підрозділів.

Логічна організація мережі:

Всі мережеві ресурси мають бути розподілені по окремих логічних блоках, відповідно до внутрішньої структури торгового центру:

зона обслуговування клієнтів – взаємодія з відвідувачами та ведення звітності;

бухгалтерський сегмент – фінансовий облік і звітування;

юридичний блок – правова перевірка документації;

складський блок – інвентаризація техніки та взаємодія з техвідділом;

адміністративні та маркетингові підрозділи – управління внутрішніми сервісами;

технічна підтримка – контроль мережевого стану, обслуговування обладнання та вирішення технічних запитів.

Функціональні можливості мережі повинні включати:

Внутрішній обмін даними:

Забезпечення швидкої та безпечної передачі інформації між усіма структурними елементами.

Підключення до центральної бази даних:

Доступ лише для авторизованих осіб із правами на створення, редагування та перегляд інформації.

Інтеграція з корпоративною поштою та месенджерами:

Для покращення внутрішньої комунікації між працівниками.

Інтернет-доступ з обмеженням доступу:

Застосування фільтрації контенту та моніторингу трафіку відповідно до політики безпеки підприємства.

Віддалене управління:

Можливість адміністрування мережі та обладнання через захищені з'єднання (VPN або інші механізми).

Автоматизоване резервне копіювання

Створення копій важливих даних і можливість швидкого відновлення в разі непередбачуваних ситуацій.

Системи моніторингу та ведення журналів:

Постійне відстеження мережевої активності, фіксація змін у системі, збоїв та інших подій для подальшого аналізу та реагування.

2.1.2 Вимоги до кількісного складу та професійної підготовки персоналу, що забезпечує експлуатацію системи

Для безперебійного функціонування IT-інфраструктури торгового центру необхідно створити спеціалізований відділ технічної підтримки. Цей підрозділ відповідає за підтримку працездатності мережевих компонентів, серверів, комп'ютерного обладнання співробітників і всієї інформаційної системи загалом.

Фахівці служби підтримки мають володіти відповідними професійними знаннями, практичними навичками, а також здатністю оперативно реагувати на збої, здійснювати технічну діагностику, планове обслуговування обладнання й надавати допомогу кінцевим користувачам.

З огляду на те, що мережа охоплює кілька рівнів будівлі та обробляє значний обсяг цифрового трафіку, важливо не лише забезпечити достатню кількість обслуговуючого персоналу, а й грамотно організувати їх робочий час. Це дозволяє уникати перевантаження окремих працівників і зменшує ризик простоїв у роботі системи.

Таблиця 2.1 – Орієнтовна структура підрозділу технічної підтримки.

№	Посада	Кількість	Освітній рівень	Графік роботи
1	Технік-електрик	2	Середня спеціальна освіта	Денна зміна
2	Завідувач відділу	1	Вища технічна освіта	Денна зміна
3	Оператор-технолог	2	Середня спеціальна	Дві зміни

			освіта	
4	Адміністратор баз даних	1	Вища освіта	Денна зміна

Основні вимоги до персоналу:

Професійні навички:

Здатність працювати з активним мережевим обладнанням (маршрутизатори, комутатори, точки доступу, сервери тощо).

Швидкість реагування:

Уміння оперативно виявляти й усувати технічні несправності.

Розуміння мережевої безпеки:

Знання основ конфігурації захисних механізмів – міжмережевих екранів, VPN-з'єднань, фільтрації трафіку.

Володіння навичками адміністрування баз даних:

Для відповідного фахівця – досвід у роботі з системами керування базами даних, виконання резервного копіювання та відновлення даних.

Комунікація:

Здатність ефективно взаємодіяти з іншими підрозділами центру для швидкого вирішення технічних запитів.

Гнучкість графіка:

Робота у змінному режимі, що дозволяє покривати період з 9:00 до 21:00 щодня, з одним вихідним на тиждень.

Належна кількість спеціалістів разом із чіткою структурою та належним розподілом обов’язків дозволяє гарантувати ефективну технічну підтримку системи. Це мінімізує ризики простоїв та сприяє стабільній роботі всіх елементів корпоративної мережі.

2.1.3 Вимоги до стабільності та надійності мережевої інфраструктури

Надійність функціонування комп’ютерної мережі у межах торгового

центру має вирішальне значення для підтримки постійного зв’язку між відділами, захисту конфіденційної інформації та безперервної роботи внутрішніх сервісів. Інфраструктура повинна витримувати значні навантаження, бути стійкою до зовнішніх впливів і забезпечувати оперативне виявлення збоїв з подальшим їх усуненням.

Одним із чинників, що негативно впливають на мережеву безпеку, є помилки, спричинені діями персоналу. Тому важливо регулярно проводити навчання та інструктаж працівників, які мають доступ до елементів IT-системи. Співробітники повинні усвідомлювати ризики витоку важливої інформації та дотримуватись внутрішніх правил безпеки.

Основні технічні та організаційні вимоги до забезпечення високої надійності мережі включають:

Впровадження комплексного захисту мережі**,** що включає використання засобів шифрування даних, міжмережевих екранів, антивірусного програмного забезпечення, а також систем виявлення і запобігання вторгненням (IDS/IPS).

Контроль доступу до мережевих ресурсів**,** з урахуванням функціональних обов’язків і посадових рівнів користувачів, що дозволяє уникнути несанкціонованого використання інформації.

Систематичний моніторинг обладнання з використанням автоматизованих механізмів для перевірки стану мережевих вузлів та зв’язків між ними.

Наявність чітко визначених процедур реагування на технічні збої, серед яких:

оперативне усунення дрібних несправностей, таких як пошкодження кабелів або вихід з ладу комутатора, протягом одного робочого дня;

проведення розширеної діагностики та усунення критичних збоїв (наприклад, неполадки серверного обладнання чи вихід з ладу великої частини мережі) з участю фахівців у максимально стислі терміни.

Підключення резервних каналів зв’язку для стратегічно важливих

служб, зокрема бухгалтерії, юридичного відділу та технічної підтримки.

Використання інструментів для дистанційної взаємодії**,** таких як Microsoft Teams або подібні платформи, для проведення нарад і координації дій між підрозділами в онлайн-режимі.

Логування та ведення журналів подій**,** що дозволяє відстежувати активність у системі, виявляти джерела порушень і своєчасно реагувати на інциденти.

Отже, надійна мережа повинна не лише ефективно передавати інформацію, але й бути захищеною, стійкою до відмов і атак, а також здатною швидко відновлювати свою роботу після аварійних ситуацій.

2.1.4 Вимоги до безпеки мережевої інфраструктури

Захист комп’ютерної мережі торгового центру є одним із найважливіших чинників стабільного та безпечного функціонування всієї інформаційної системи. Оскільки мережева інфраструктура обслуговує різні структурні підрозділи та містить чутливі дані (включаючи клієнтську інформацію, внутрішні звіти, фінансову документацію), необхідно реалізувати надійні механізми безпеки, здатні протистояти як зовнішнім, так і внутрішнім загрозам.

Ключові заходи з організації безпеки мережі включають наступні положення:

Навчання персоналу з кібергігієни. Всі працівники, особливо керівники та технічні спеціалісти, повинні бути ознайомлені з основними сценаріями кібератак – фішинговими повідомленнями, соціальною інженерією, спробами компрометації облікових записів тощо. Регулярні інструктажі підвищують рівень обізнаності й зменшують ризик людських помилок.

Інтеграція програмно-апаратних засобів захисту, до яких належать:

мережеві екрани (Firewall) для контролю вхідного та вихідного трафіку;

антивірусні продукти з автоматичним оновленням сигнатур;

шифрування інформації при передачі, зокрема через VPN або TLS-

з'єднання;

системи виявлення та протидії вторгненням (IDS/IPS), які дозволяють виявляти аномальну активність в режимі реального часу.

Реалізація політики безпечного паролем, яка вимагає створення складних комбінацій, що складаються не менш ніж з 8 символів і включають літери обох регістрів, цифри та спеціальні знаки. Також має бути впроваджено регулярну зміну паролів для всіх користувачів.

Доступ за принципом мінімальних прав. Співробітники повинні мати доступ лише до тих ресурсів, які необхідні їм для виконання конкретних службових завдань, що дозволяє значно зменшити можливі наслідки компрометації облікових записів.

Дотримання правил техніки безпеки при роботі з IT-обладнанням. Кожне робоче місце має бути обладнане згідно з вимогами чинного трудового законодавства, зокрема нормами з охорони праці при експлуатації комп’ютерної техніки.

Відповідність чинним стандартам. Усі етапи створення, налаштування та функціонування мережевої системи повинні узгоджуватися з положеннями ДСТУ 34.603-92 «Інформаційна технологія. Види випробувань автоматизованих систем». Це дозволяє забезпечити стандартизовану перевірку безпеки на всіх рівнях.

Підсумовуючи, захист мережі має бути багатошаровим і системним, охоплюючи не лише технічні рішення, але й заходи щодо підвищення відповідальності користувачів та адаптації до новітніх загроз.

2.2 Розробка інженерних рішень для комп’ютерної системи

2.2.1 Розробка структурної схеми мережі

Структурна схема мережі розроблена з урахуванням просторової організації підприємства, функціонального розподілу підрозділів та вимог до безпеки, масштабованості та надійності комп’ютерної інфраструктури. В

основу покладено принцип географічного та логічного зонування, що дозволяє чітко розмежовувати підмережі, сервіси та точки доступу.

Головний офіс – це двоповерхова адміністративна будівля, у якій зосереджені основні керівні та підтримуючі служби підприємства.

Торговий центр (ТЦ) є основною функціональною локацією підприємства, де відбувається щоденна взаємодія з відвідувачами, орендарями та технічним персоналом. В інфраструктурі ТЦ передбачено:

Центральний пост служби безпеки з доступом до системи відеоспостереження;

Технічні приміщення з обладнанням для обслуговування комунікацій та електропостачання;

Уся інфраструктура ТЦ обслуговується підмережею LAN2, а додатковий функціонал реалізується через IoT-канали.

Перший поверх відведено під IT-відділ, службу технічної підтримки та центральну серверну кімнату. У серверній розміщене основне мережеве обладнання (маршрутизатори, комутатори), а також критично важливі сервери: баз даних, RADIUS, DNS, HTTP тощо. За обслуговування цієї зони відповідає підмережа LAN3.

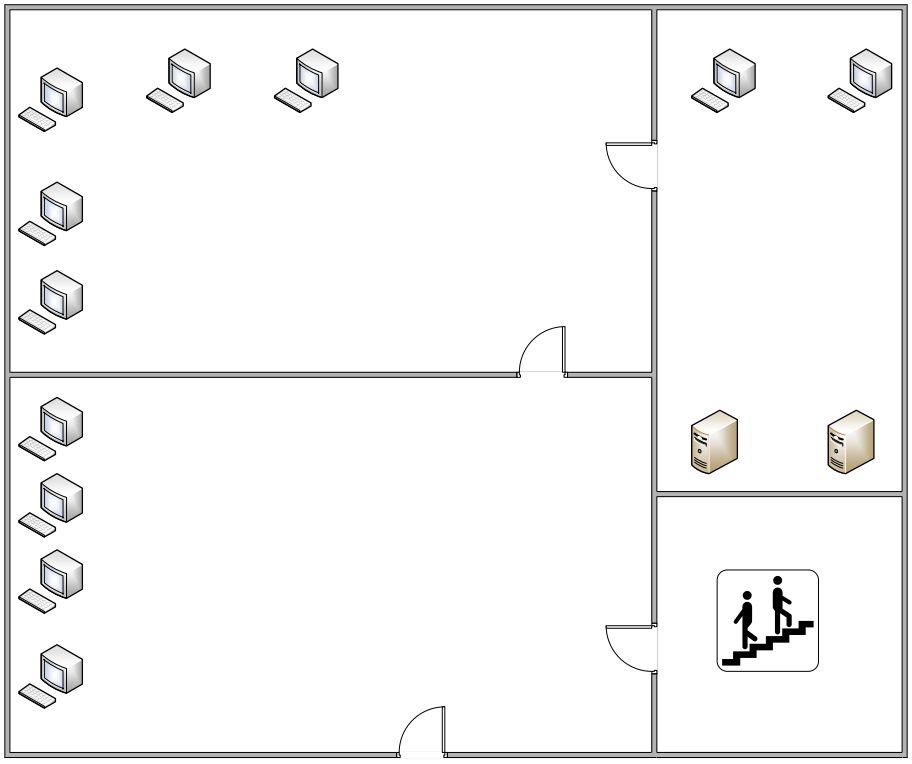


Рисунок 2.1 – Перший поверх головного офісу

Другий поверх наведений на рисунку та включає кабінети адміністрації, маркетингового відділу та фінансово-бухгалтерської служби. Для забезпечення ізольованого та безпечного функціонування цих підрозділів реалізовано дві логічні підмережі: LAN1 загальне адміністративне середовище та LAN5 фінансовий відділ.

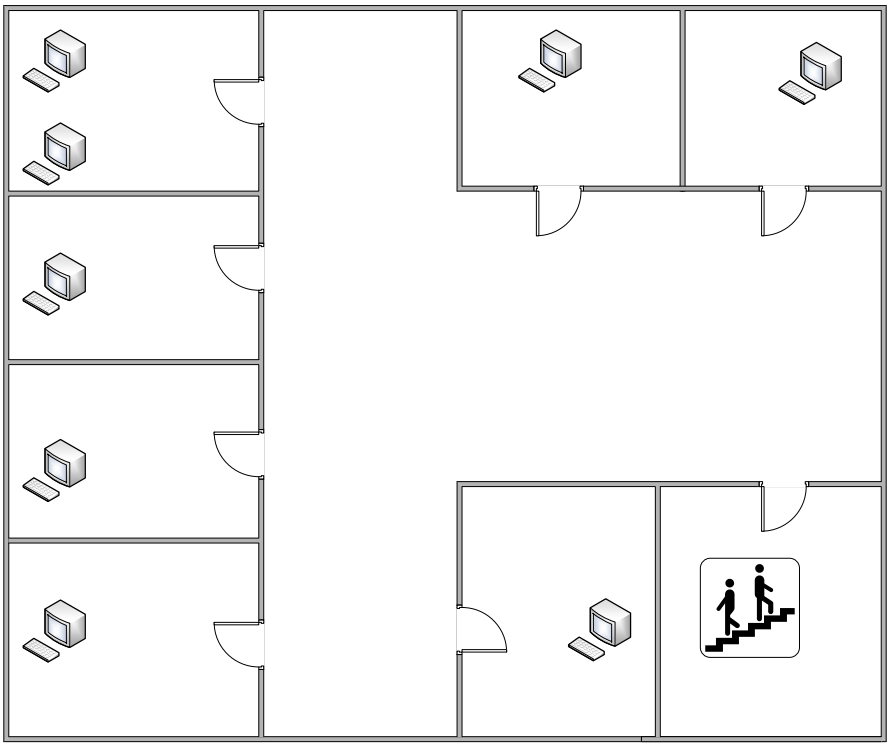


Рисунок 2.2 – Другий поверх головного офісу

Інтегрована IoT-система пожежогасіння, що взаємодіє з датчиками диму, контролерами та виконавчими пристроями. Наведена на рисунку

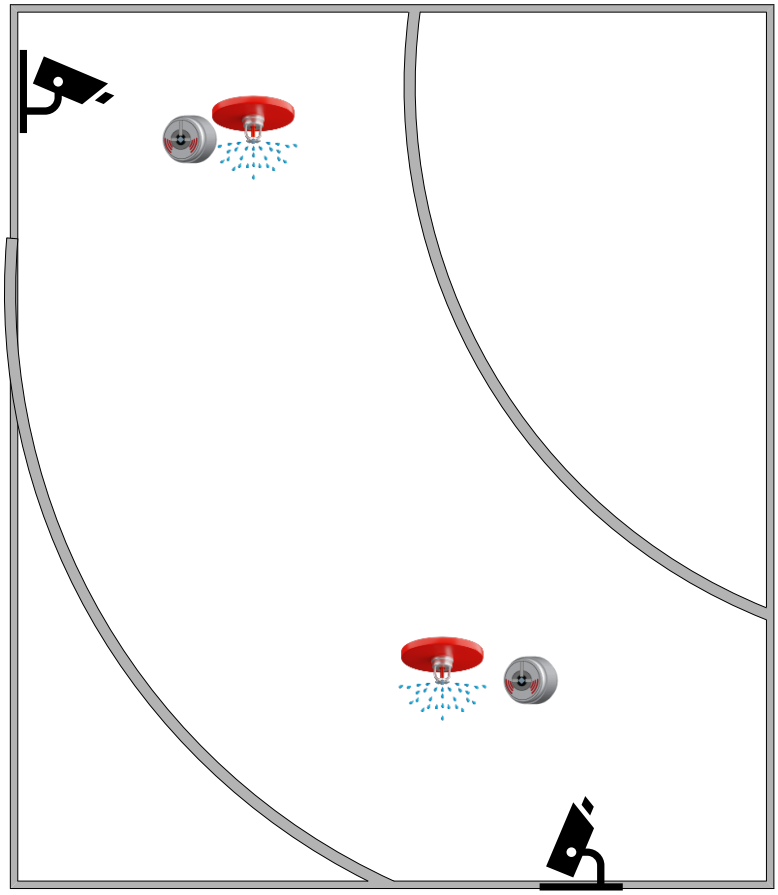


Рисунок 2.3 – Сектор ТЦ

Філіал №1 – це віддалена локація, яка може виконувати функції логістичного підрозділу, складу або додаткового офісу. Для її повноцінного включення у корпоративну мережу передбачено окрему підмережу LAN4, що забезпечує зв’язок із головним офісом через міжмаршрутизаторні канали та дозволяє філіалу працювати з внутрішніми інформаційними ресурсами підприємства.

2.2.2 Розробка специфікації апаратних засобів комп’ютерної системи

Після ретельного аналізу вимог до побудови корпоративної комп’ютерної мережі та технічного оснащення робочих місць, наступним кроком стало складання специфікації апаратного забезпечення. Вона містить перелік обладнання із зазначенням типів, технічних характеристик та кількості необхідних одиниць.

Під час підбору персональних комп’ютерів основними критеріями були компактність, стабільність роботи, зручність обслуговування, енергоефективність та готовність до швидкої інтеграції в існуючу інфраструктуру. Ураховуючи це, було вирішено зупинитися на моноблочних системах, що поєднують усі основні компоненти в одному елегантному корпусі, зменшуючи кількість кабелів та забезпечуючи зручне розміщення в офісному середовищі.

Оптимальним варіантом у рамках технічних та функціональних вимог виявився моноблок Acer Aspire C24-1600. Цей пристрій обладнаний сучасним енергоефективним процесором, швидким SSD-накопичувачем, 23,8-дюймовим Full HD IPS дисплеєм, що забезпечує високу якість зображення, а також має елегантний ультратонкий дизайн. Компактність пристрою дозволяє ефективно організувати робочий простір навіть у невеликих офісах.

До комплекту входять бездротові клавіатура та миша, що додатково спрощує організацію робочого місця та зменшує кількість дротів. Такі рішення широко використовуються в сучасних офісах, де цінується поєднання продуктивності, естетики та ергономіки. Моноблок Acer Aspire C24-1600 зображено на рисунку 2.4.

Рисунок 2.4 – Моноблок Acer Aspire C24-1600

Наступним ключовим елементом мережевої інфраструктури є серверне обладнання, яке виконує функції обробки та зберігання даних, а також забезпечує безперебійну роботу критичних служб, таких як DNS, HTTP, файлові та веб-сервери. Вибір серверної платформи ґрунтувався на таких критеріях, як надійність, масштабованість, енергоефективність, а також можливість інтеграції в існуючу мережу підприємства.

З огляду на вказані вимоги, було обрано сервер Lenovo ThinkSystem ST50 V2 — сучасне, енергоефективне та продуктивне рішення для невеликих і середніх організацій. Цей сервер побудований на базі процесорів Intel Xeon серії E-2300, підтримує до 128 ГБ оперативної пам’яті DDR4 та має можливість встановлення кількох накопичувачів, що дозволяє реалізувати надійну систему зберігання даних.

Lenovo ThinkSystem ST50 V2 відзначається тихою роботою, компактним форм-фактором (tower), а також широкими можливостями для розширення

— що робить його ідеальним для розміщення в стандартному офісному середовищі без необхідності окремого серверного приміщення. Наявність необхідних мережевих інтерфейсів і підтримка сучасних засобів адміністрування забезпечують ефективну інтеграцію цього сервера до корпоративної IT-інфраструктури.

Завдяки високому рівню стабільності та сумісності з ключовими операційними системами, Lenovo ThinkSystem ST50 V2 є оптимальним вибором для побудови надійної та гнучкої серверної платформи в рамках локальної мережі підприємства. Серверна система Lenovo ThinkSystem ST50 V2 зображено на рисунку 2.5.

Рисунок 2.5 – Серверна система Lenovo ThinkSystem ST50 V2

Комутатори є фундаментальними елементами локальної комп’ютерної мережі, оскільки забезпечують ефективну комутацію трафіку між усіма кінцевими пристроями та мережевими сегментами. При виборі комутаційного обладнання першочергову увагу приділяють кількості портів, пропускній здатності, підтримці енергозберігаючих технологій, а також

сумісності з сучасними стандартами безпеки та управління.

Серед рішень від компанії Cisco було обрано Cisco Catalyst 1000-24FP-4G-L — серію керованих комутаторів рівня доступу (Layer 2, канальний рівень моделі OSI), призначених для малих і середніх підприємств. На відміну від серій, орієнтованих на малий бізнес (наприклад, Cisco Business або аналоги від Netgear), Catalyst 1000-24FP-4G-L працює на базі повноцінної операційної системи Cisco IOS, що гарантує вищий рівень безпеки та стабільності, властивий корпоративним рішенням. У рамках проєкту використовується модель з 24 портами Gigabit Ethernet та виділеними uplink-портами, що забезпечує високу швидкість з’єднання та можливість подальшого масштабування мережі.

Cisco Catalyst 1000-24FP-4G-L вирізняється високою надійністю, простотою в налаштуванні, а також низьким енергоспоживанням. Підтримка стандартів VLAN, QoS, а також функцій безпеки (наприклад, Port Security) дає змогу формувати гнучку та захищену мережеву інфраструктуру. Комутатор також має зручний веб-інтерфейс для керування, що дозволяє IT-спеціалістам швидко здійснювати налаштування та моніторинг у реальному часі.

Завдяки поєднанню компактного форм-фактору, енергоефективності та продуктивності, Cisco Catalyst 1000-24FP-4G-L є оптимальним вибором для забезпечення стабільного функціонування офісної мережі з високим рівнем доступності та безпеки. Комутатор Cisco Catalyst 1000-24FP-4G-L зображено на рисунку 2.6.

Рисунок 2.6 – Комутатор Cisco Catalyst 1000-24FP-4G-L

У якості маршрутизатора для побудови надійної та масштабованої корпоративної мережі рекомендовано використання моделі Cisco Catalyst 8200, яка повністю відповідає сучасним вимогам до продуктивності, безпеки та інтеграції з хмарними сервісами. Цей маршрутизатор орієнтований на використання в мережах малого та середнього бізнесу, а також у філіях великих компаній.

Cisco Catalyst 8200 оснащений високопродуктивними процесорами, підтримує кілька інтерфейсів Gigabit Ethernet, а також має можливість розширення за рахунок модульної архітектури — зокрема, підтримки WAN-модулів, LTE/5G, VPN та інших опцій. Це дозволяє адаптувати пристрій до змін потреб підприємства та забезпечити високу гнучкість мережевої інфраструктури.

Завдяки підтримці SD-WAN, маршрутизатор Cisco Catalyst 8200 забезпечує інтелектуальне керування трафіком, оптимізацію пропускної здатності каналів і підвищення надійності з'єднань з віддаленими офісами або хмарними платформами. Високий рівень безпеки досягається завдяки вбудованим функціям захисту, включно з фаєрволом, шифруванням трафіку та контрольованим доступом.

Таким чином, Cisco Catalyst 8200 є сучасним і ефективним рішенням для реалізації ядра корпоративної мережі з можливістю масштабування, централізованого управління та безпечного з’єднання з географічно розподіленими об’єктами. Маршрутизатор Cisco Catalyst 8200 зображено на рисунку 2.7.

Рисунок 2.7 – Маршрутизатор Cisco Catalyst 8200

З метою підвищення надійності функціонування комп’ютерної мережі, впроваджуються джерела безперебійного живлення (ДБЖ). Вони забезпечують короткочасне живлення для критичного обладнання у разі збоїв електропостачання, запобігаючи втраті даних та пошкодженню систем.

Для захисту робочих станцій було обрано модель Powercom RPT-600A, яка відзначається оптимальним співвідношенням ціни та функціональності. Її потужності (600 ВА / 360 Вт) достатньо для підтримки роботи одного ПК з монітором. Вбудований AVR та базовий захист від стрибків напруги відповідають вимогам для цього типу обладнання.

Для захисту серверів та ключового мережевого обладнання (магістральних комутаторів та маршрутизаторів) висуваються вищі вимоги. Тому для них обрано ДБЖ класу Smart-UPS з чистою синусоїдою, наприклад, APC Smart-UPS 1500VA (SMT1500I). Ця модель забезпечує необхідний запас потужності, сумісність із серверними блоками живлення (Active PFC) та можливість віддаленого керування через мережу для коректного завершення роботи систем.

Такий диференційований підхід дозволить побудувати надійну систему резервного живлення, що враховує особливості кожного типу обладнання та

забезпечить максимальний рівень безперервності роботи IT-інфраструктури.

Джерело безперебійного живлення APC Smart-UPS 1500VA представлено на рисунку 2.8.

Рисунок 2.8 – Джерело безперебійного живлення APC Smart-UPS 1500VA

З метою посилення фізичної безпеки об’єкта та інтеграції системи охоронного спостереження в загальну IT-інфраструктуру було впроваджено централізований блок керування сигналізацією. Таке рішення дозволяє оперативно реагувати на порушення периметра, контролювати стан датчиків безпеки та забезпечувати інтеграцію з іншими системами моніторингу.

Було обрано Cisco DLC-100 Burglar Control Unit, який використовується в складі платформи AT&T Digital Life — розумної системи керування охороною та автоматизацією житлових і офісних приміщень. Пристрій виконує функцію центрального вузла, до якого підключаються сенсори руху, датчики відкриття дверей, камери спостереження, сирени та інше допоміжне обладнання.

Cisco DLC-100 забезпечує надійне двостороннє з’єднання з усіма компонентами охоронної системи та дозволяє віддалено керувати її параметрами через інтерфейс Digital Life. У разі тривоги пристрій миттєво передає сигнал на централізований пульт охорони або на мобільний додаток користувача, забезпечуючи швидке реагування.

Особливістю рішення є підтримка захищених каналів зв’язку, автономне

живлення у разі знеструмлення та можливість інтеграції з іншими системами безпеки — наприклад, пожежною сигналізацією або відеонаглядом. Впровадження Cisco DLC-100 дозволяє створити єдину безпекову платформу, яка забезпечує цілодобовий моніторинг і максимальний контроль за фізичним доступом до об’єкта. Cisco DLC-100 Представлено на рисунку 2.9.

Рисунок 2.9 – Cisco DLC-100

Таблиця 2.1 – Специфікація обладнання

Позиція	Назва	Тип пристрою	Характеристики
1	Aspire C24-1600 All-in-One Computer	Моноблок	Процесор Intel® процессор

			Pentium® Silver N6005 частота процессора 2 ГГц Оперативна пам’ять DDR4 SDRAM 8GB Об’єм пам’яті 256 ГБ
2	Lenovo ThinkSystem ST50	Сервер	Процесор Intel Xeon E-2324G Оперативна пам'ять TruDDR4 3200 8GB Відеокарта nVidia Quadro T1000
3	Cisco Catalyst 1000-24FP-4G-L	Комутатор	24 Gigabit Ethernet
4	Cisco Catalyst 8200	Маршрутизатор	12 Gigabit Ethernet
5	APC Smart-UPS 1500VA	Джерело безперебійного живлення	Вхідна частота, 50-60 Гц Номінальна потужність

			900 Вт Кількість виходів 8
6	Cisco DLC-100	Маршрутизатор	Wi-Fi (802.11b/g/n, 2.4 GHz)

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1 Розрахунок схеми адресації корпоративної мережі торгового центру

Перед проєктуванням корпоративної мережі потрібно сформувати схеми IP-адресації, згідно з технічних вимог виданого варіанту кваліфікаційної роботи. За умовами п'ятнадцятого варіанту надано адресний простір 172.25.72.0/22, який включає в себе п'ять підмереж.

Мережева інфраструктура розподілена між трьома окремими географічними локаціями:

До головного офісу віднесено мережі LAN3, що знаходиться на першому поверсі, LAN1 та LAN5, на другому поверсі;

LAN2 який знаходиться безпосередньо в самому ТЦ;

Філіал №1 який охоплює у собі єдину підмережу – LAN4.

Окрім створення локальних підмереж, слід також організувати міжмаршрутизаторні з'єднання, оскільки кожна пара маршрутизаторів має бути пов'язана окремим IP-каналом. Згідно з топологічною схемою, у мережі задіяно п'ять маршрутизаторів, які потребують цього, для яких необхідно налаштувати 6 окремих з'єднань, кожне з яких вимагає виділеної підмережі. З цією метою замовник надав адресний простір 10.0.15.0/24, який ділиться на підмережі з префіксом /30 (тобто з маскою 255.255.255.252), що дозволяє забезпечити по два активні пристрої в кожному сегменті.

З метою оптимізації використання IP-адрес у мережі застосовано метод VLSM (змінна довжина маски підмережі), який дає змогу створювати підмережі з різною ємністю відповідно до конкретних потреб. Такий підхід дозволяє зменшити кількість невикористаних адрес і забезпечує резервування вільних діапазонів для майбутнього розширення мережевої інфраструктури. У таблиці 3.1 наведено дані, що повну адресу локальних підмереж.

Таблиця 3.1 – Адресація мережі

Ім'я	Кількість вузлів	Загальна кількість вузлів	Мережева адреса	Мережнва маска	Діапазон використання
LAN4	236	254	172.25.72.0	255.255.255.0	172.25.72.1 - 172.25.72.254
LAN2	226	254	172.25.73.0	255.255.255.0	172.25.73.1 - 172.25.73.254
LAN1	197	254	172.25.74.0	255.255.255.0	172.25.74.1 - 172.25.74.254
LAN5	177	254	172.25.75.0	255.255.255.0	172.25.75.1 - 172.25.75.254
LAN3	172	254	172.25.76.0	255.255.255.0	172.25.76.1 - 172.25.76.254
Wan1	2	2	10.0.15.0	255.255.255.252	10.0.15.1 - 10.0.15.2
Wan2	2	2	10.0.15.4	255.255.255.252	10.0.15.5 - 10.0.15.6
WAN3	2	2	10.0.15.8	255.255.255.252	10.0.15.9 - 10.0.15.10
WAN4	2	2	10.0.15.12	255.255.255.252	10.0.15.13 - 10.0.15.14
WAN5	2	2	10.0.15.16	255.255.255.252	10.0.15.17 - 10.0.15.18
WAN6	2	2	10.0.15.20	255.255.255.252	10.0.15.21 - 10.0.15.22

3.2 Розробка топологічної схеми корпоративної мережі ТЦ

Комп’ютерна мережа моделюється в середовищі Cisco Packet Tracer відповідно до топології, визначеної в технічному завданні проєкту корпоративної системи (див. рисунок 1.2).

Початковим етапом побудови мережевої моделі є підбір необхідного обладнання для реалізації заданої архітектури. У Cisco Packet Tracer є великий вибір компонентів, зокрема маршрутизатори, комутатори, кабелі, кінцеві пристрої та інші елементи, що дає змогу точно відтворити структуру корпоративної мережі.

У технічній документації передбачено використання обладнання Cisco. Для організації маршрутизації було застосовувано відповідні пристрої з

бібліотеки Packet Tracer, а саме обрано модель маршрутизатора Cisco 2811, а для створення локальних мережевих сегментів – комутатори WS-C2960-24TT-L

На рисунку 3.1 зображено побудовану модель мережі, яка повністю відповідає проєктним вимогам і демонструє логічну взаємодію усіх підмереж корпоративної інфраструктури.

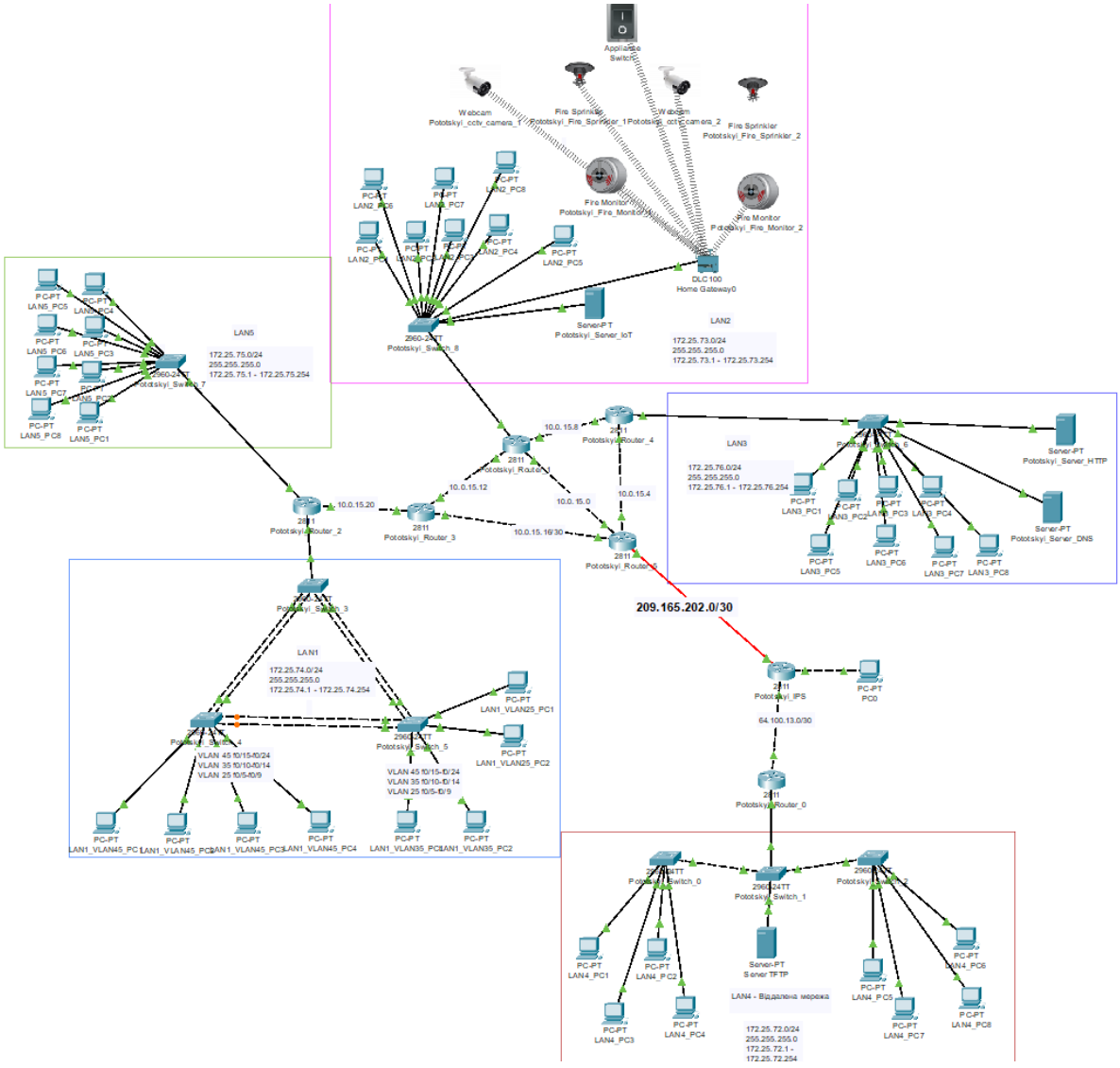


Рисунок 3.1 – Схема комп’ютерної мережі в Cisco Packet Tracer

3.3 Налаштування моделі КС ТЦ

3.3.1 Базове налаштування конфігурації пристроїв

Під час базової конфігурації мережевих пристроїв першим чином потрібно надати їм імена для зручної ідентифікації у топології, за шаблоном Прізвище_тип_пристрою_номер. Приклад: «Pototskyi_Router_3».

Щоб забезпечити стабільну та узгоджену роботу маршрутизаторів, які здійснюють з'єднання між окремими підмережами, на всіх серійних інтерфейсах типу DCE було встановлено єдину тактову частоту у 128000 біт/с. Така конфігурація є обов'язковою для визначення швидкості обміну даними у серійному каналі.

На рисунку 3.2 відображено процес встановлення тактової частоти через інтерфейс Cisco Packet Tracer.

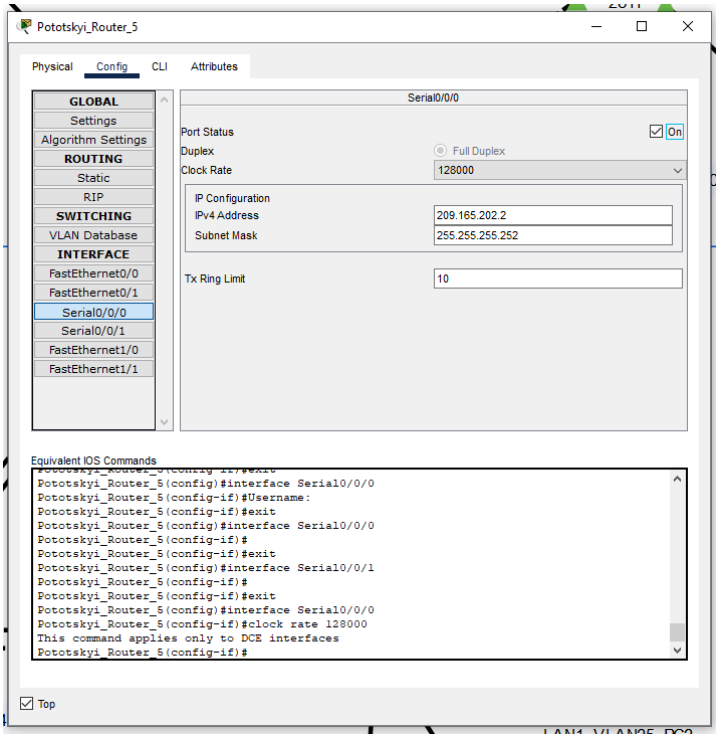


Рисунок 3.2 – Вікно інтерфейсу конфігурації маршрутизатора

Призначення IP-адрес у мережевій інфраструктурі виконується з урахуванням ролі кожного пристрою, відповідно до технічного завдання. Для маршрутизаторів резервується перша вільна IP-адреса у кожній підмережі, комутаторам надається друга, а робочі станції отримують останню доступну

адресу з виділеного діапазону.

Сервери адресуються за окремим алгоритмом: до першої можливої адреси підмережі додається значення 9 та номер варіанта 15, що забезпечує призначення двадцять п’ятої IP-адреси відповідного сегмента.

У таблиці 3.2 представлено повну IP-адресну структуру всіх мережевих пристроїв, задіяних у корпоративній мережі, із врахуванням їх функціонального призначення та топологічного розміщення в системі.

Таблиця 3.2 – Схема адресації пристроїв

Пристрій	Інтер-фейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключе-ного пристрою
Pototskyi_ Router_0	Fa0/0	64.100.13.2	/30	-	1	Pototskyi_ ISP Fa0/0
	Fa0/1	172.25.72.1	/24	-	1	Pototskyi_ Switch_1 G0/1
Pototskyi_ Router_1	Fa0/0	10.0.15.14	/30	-	1	Pototskyi_ Router_3 Fa0/1
	Fa0/1	10.0.15.9	/30	-	1	Pototskyi_ Router_4 Fa0/0
	Fa1/0	10.0.15.1	/30	-	1	Pototskyi_ Router_5 Fa0/1
	Fa1/1	172.25.73.1	/24	-	1	Pototskyi_ Switch_8 G0/1
Pototskyi_ Router_2	Fa0/1	10.0.15.22	/30	-	1	Pototskyi_ Router_3 Fa0/0
	Fa1/0.25	172.25.74.1	/26	-	25	Pototskyi_ Switch_3 G0/1
	Fa1/0.35	172.25.74.65	/26	-	35	Pototskyi_ Switch_3 G0/1
	Fa1/0.45	172.25.74.129	/26	-	45	Pototskyi_ Switch_3 G0/1
	Fa1/0.99	172.25.74.193	/26	-	99	Pototskyi_

						Switch_3 G0/1
	Fa1/1	172.25.75.1	/24	-	1	Pototskyi_ Switch_6 G0/1
Pototskyi_ Router_3	Fa0/0	10.0.15.21	/30	-	1	Pototskyi_ Router_2 Fa0/1
	Fa0/1	10.0.15.13	/30	-	1	Pototskyi_ Router_1 Fa0/0
	Fa1/0	10.0.15.18	/30	-	1	Pototskyi_ Router_5 Fa1/0
Pototskyi_ Router_4	Fa0/0	10.0.15.10	/30	-	1	Pototskyi_ Router_1 Fa0/1
	Fa0/1	10.0.15.5	/30	-	1	Pototskyi_ Router_5 Fa0/0
	Fa1/1	172.25.76.1	/24	-	1	Pototskyi_ Switch_6 G0/1
Pototskyi_ Router_5	Se0/0/0	209.165.202.2	/30	-	1	Pototskyi_ ISP Se0/0/0
	Fa0/0	10.0.15.6	/30	-	1	Pototskyi_ Router_4 Fa0/1
	Fa0/1	10.0.15.2	/30	-	1	Pototskyi_ Router_1 Fa1/0
	Fa1/0	10.0.15.17	/30	-	1	Pototskyi_ Router_3 Fa1/0
Pototskyi_ ISP	Se0/0/0	209.165.202.1	/30	-	1	Pototskyi_ Router_5 Se0/0/0
	Fa0/0	64.100.13.1	/30	-	1	Pototskyi_ Router_0 Fa0/0
	Fa1/1	209.165.201.1	/28	-	1	PC0 Fa0
Pototskyi_ Switch_0	VLAN1	172.25.72.3	/24	172.25.72.1	1	-
Pototskyi_ Switch_1	VLAN1	172.25.72.2	/24	172.25.72.1	1	-
Pototskyi_ Switch_2	VLAN1	172.25.72.4	/24	172.25.72.1	1	-
Pototskyi_	VLAN99	172.25.74.194	/26	172.25.74.193	99	-

Switch_3						
Pototskyi_ Switch_4	VLAN99	172.25.74.195	/26	172.25.74.193	99	-
Pototskyi_ Switch_5	VLAN99	172.25.74.196	/26	172.25.74.193	99	-
Pototskyi_ Switch_6	VLAN1	172.25.76.2	/24	172.25.76.1	1	-
Pototskyi_ Switch_7	VLAN1	172.25.75.2	/24	172.25.75.1	1	-
Pototskyi_ Switch_8	VLAN1	172.25.73.2	/24	172.25.73.1	1	-
Server_ DNS	Fa0	172.25.76.24	/24	172.25.76.1	1	Pototskyi_ Switch_6 Fa0/2
Server_ HTTP	Fa0	172.25.76.25	/24	172.25.76.1	1	Pototskyi_ Switch_6 Fa0/1
Server_ IoT	Fa0	172.25.73.25	/24	172.25.73.1	1	Pototskyi_ Switch_8 Fa0/9
Server_ TFTP	Fa0	172.25.72.25	/24	172.25.72.1	1	Pototskyi_ Switch_1 Fa0/3
Home_ Gateway	Internet	172.25.73.26 - 172.25.73.254	/24	172.25.73.1	1	Pototskyi_ Switch_8 Fa0/10

Першим етапом розгортання мережевої інфраструктури є налаштування ключових параметрів обладнання. До цього належать призначення унікального імені пристрою, встановлення та шифрування паролів доступу, створення привітального банера, додавання локального облікового запису користувача, а також увімкнення захищеного віддаленого підключення через SSH-протокол.

Такі стандартні дії конфігурування виконуються для кожного маршрутизатора мережі, оскільки вони формують основу безпечного адміністрування. Оскільки конфігурації мають уніфікований характер, далі наведено приклад для одного з пристроїв – Pototskyi_Router_1

Призначення імені пристрою було виконано через графічний інтерфейс, для демонстрації аналогічного способу налаштування, що продемонстровано на рисунку 3.3

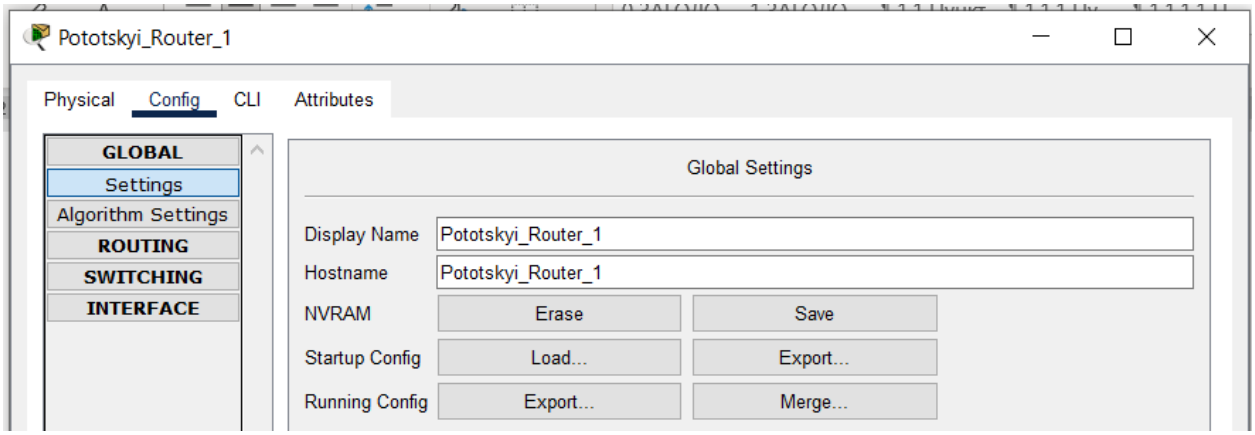


Рисунок 3.3 – Надання пристрою імені

Подальші базові налаштування були виконані у командній строці

enable

configure terminal

no ip domain-lookup

banner motd !The system is protected by a security system.!

username 123212_Pototskyi secret admincisco

ip domain-name Pototskyi_Router_1

line console 0

password cisco123

login

line vty 0 15

transport input ssh

password cisco123

login local

exit

ip ssh version 2

enable secret class

crypto key generate rsa

1024

service password-encryption

do write

Для перевірки правильності виконанань базових налаштувань

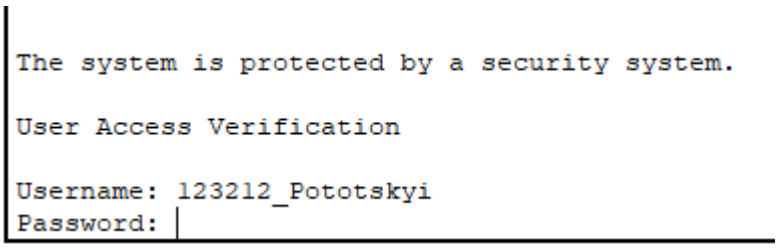


Рисунок 3.4 – Демонстрація роботи базових налаштувань

Port Aggregation Protocol (PAgP) – це фірмовий протокол компанії Cisco, призначений для автоматичного об’єднання декількох фізичних Ethernet-інтерфейсів комутатора в один логічний канал.

У межах мережі LAN_1 така агрегація була реалізована для підвищення загальної продуктивності та надійності мережевих з'єднань: фізичні порти комутаторів, які пов'язують серверну зону з сегментом робочих станцій, були об’єднані за допомогою технології EtherChannel. Вона дозволяє створити єдиний логічний інтерфейс, що працює на основі декількох фізичних лінків.

Основна перевага EtherChannel – значне збільшення пропускної здатності мережі без необхідності зміни логічної топології у разі часткової відмови. На відміну від Spanning Tree Protocol (STP), який при виявленні неполадок вимушено перебудовує мережу і активує резервні шляхи з певною затримкою, EtherChannel дозволяє продовжити роботу, просто зменшуючи загальну пропускну здатність каналу. Тобто, хоча EtherChannel не замінює STP, він значно зменшує вплив відмови окремих ліній зв'язку, усуваючи потребу в повному перерахунку топології.

Контроль поточного стану агрегованих портів здійснюється за допомогою команди show interfaces trunk.

interface range f0/1-4

switchport mode trunk

switchport nonegotiate

interface range f0/1-2

switchport nonegotiate

shutdown

channel-group 1 mode desirable

no shutdown

interface range f0/3-4

switchport nonegotiate

shutdown

channel-group 3 mode desirable

no shutdown

Результат налаштування продемонстровано на рисунку 3.5

```
Pototskyi_Switch_3#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      100
Fa0/2       on           802.1q         trunking      100
Fa0/3       on           802.1q         trunking      100
Fa0/4       on           802.1q         trunking      100
Gig0/1      on           802.1q         trunking      100

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005
Fa0/4       1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,25,35,45,99,100
Fa0/2       1,25,35,45,99,100
Fa0/3       1,25,35,45,99,100
Fa0/4       1,25,35,45,99,100
Gig0/1      1,25,35,45,99,100
```

Рисунок 3.5 – Результат роботи команди

3.4 Розрахунок налаштувань маршрутизації корпоративної мережі

Маршрутизація – це процес пересилання пакетів даних у межах мережі від одного вузла до іншого. У ході цього процесу маршрутизатори визначають найефективніший маршрут для передавання інформації, використовуючи дані про поточний стан мережі та записи в таблицях маршрутизації.

Існують два основні типи маршрутизації:

Статична маршрутизація передбачає ручне налаштування маршрутизаторів адміністратором. Всі маршрути задаються вручну і залишаються незмінними, навіть якщо конфігурація мережі змінюється. Такий підхід ефективний у стабільних мережах, де рідко відбуваються зміни.

Динамічна маршрутизація забезпечує автоматичне оновлення маршрутів. Маршрутизатори самостійно обмінюються інформацією про мережу за допомогою спеціальних протоколів, таких як OSPF, RIP, EIGRP тощо. Це дозволяє адаптуватися до змін у топології мережі без втручання адміністратора.

У розробленій мережі було реалізовано динамічну маршрутизацію за допомогою протоколу EIGRP (Enhanced Interior Gateway Routing Protocol).

Протокол EIGRP, розроблений компанією Cisco, поєднує в собі переваги як векторно-дистанційної, так і стан-орієнтованої маршрутизації. Він дозволяє досягти високої швидкості збіжності та стабільної роботи навіть у великих і складних мережах.

Основні переваги EIGRP:

Швидка адаптація до змін – маршрути оновлюються майже миттєво завдяки використанню таблиць суміжності та алгоритму DUAL (Diffusing Update Algorithm);

Підтримка VLSM та CIDR, що дозволяє ефективно використовувати адресний простір;

Мінімальне навантаження на мережу, оскільки оновлення передаються лише за зміни, а не періодично;

Можливість балансування навантаження по кількох маршрутах з різною вартістю;

Проста інтеграція в інфраструктуру Cisco, оскільки EIGRP тісно пов’язаний із обладнанням цього виробника.

Перед впровадженням EIGRP кожному пристрою було присвоєно IP-адресу та маску мережі відповідно до попередньо розробленої адресної схеми наведеної в таблиці 3.2.

Налаштування EIGRP на прикладі Pototskyi_Router_1

```
enable
configure terminal
```

route eigrp 15

network 10.0.15.0 0.0.0.3

network 10.0.15.12 0.0.0.3

network 10.0.15.8 0.0.0.3

Інші пристрої були налаштовані аналогічним чином

NAT (Network Address Translation) – це технологія, яка дозволяє змінювати IP-адреси у заголовках IP-пакетів під час їх проходження через маршрутизатор або інший пристрій. Основне призначення NAT – забезпечити взаємодію локальної мережі з глобальною мережею Інтернет, дозволяючи кільком пристроям з приватними адресами використовувати одну публічну IP-адресу.

Завдяки NAT локальні мережі можуть використовувати приватний діапазон IP-адрес, що значно зменшує потребу в унікальних публічних адресах. Крім того, NAT забезпечує базовий рівень захисту, оскільки внутрішні IP-адреси не доступні напряму з Інтернету.

Основні особливості та переваги використання NAT:

– Збереження публічних IP-адрес. NAT дозволяє десяткам або сотням пристроїв користуватися однією зовнішньою IP-адресою, що особливо важливо в умовах обмеженого ресурсу глобальних адрес;

– Безпека. Завдяки NAT внутрішні IP-адреси залишаються прихованими від зовнішнього світу, що ускладнює несанкціонований доступ до мережі ззовні;

– Гнучкість при побудові мережі. Мережеві адміністратори можуть вільно використовувати приватні діапазони IP-адрес, не турбуючись про конфлікти з глобальною адресацією;

– Маскування трафіку. NAT виступає як посередник між локальними пристроями та зовнішніми сервісами, підміняючи IP-адреси та порти, що спрощує контроль над мережевими з’єднаннями.

Налаштування NAT

ip access-list extended For_NAT

```
 deny ip 172.25.73.0 0.0.0.255 172.25.72.0 0.0.0.255
 deny ip 172.25.74.0 0.0.0.255 172.25.72.0 0.0.0.255
 deny ip 172.25.75.0 0.0.0.255 172.25.72.0 0.0.0.255
 deny ip 172.25.76.0 0.0.0.255 172.25.72.0 0.0.0.255
 permit ip 172.25.73.0 0.0.0.255 any
 permit ip 172.25.74.0 0.0.0.255 any
 permit ip 172.25.75.0 0.0.0.255 any
 permit ip 172.25.76.0 0.0.0.255 any
ip nat pool Outside 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list For_NAT pool Outside
ip nat inside source static 172.25.76.25 209.165.200.4
ip nat inside source static 172.25.76.24 209.165.200.3
int s0/0/0
ip nat outside
int f0/0
ip nat inside
int f0/1
ip nat inside
int f1/0
ip nat inside
```

DHCP (Dynamic Host Configuration Protocol) – це мережевий протокол, який автоматизує процес призначення IP-адрес та інших мережевих параметрів (маска підмережі, шлюз, DNS-сервери) пристроям у локальній мережі. Завдяки DHCP значно спрощується адміністрування мережі, адже немає потреби вручну налаштовувати параметри для кожного пристрою.

Після підключення до мережі клієнт надсилає запит DHCP-серверу, який, у свою чергу, надає вільну IP-адресу з доступного пулу та інші необхідні параметри. Це дозволяє швидко й безпомилково підключати нові пристрої до мережі.

Основні особливості та переваги використання DHCP:

– Автоматизація конфігурації. DHCP дозволяє уникнути ручного введення мережевих налаштувань, що зменшує кількість помилок та пришвидшує розгортання нових пристроїв;

– Централізоване управління. Усі IP-адреси видаються з єдиного місця – DHCP-сервера. Це полегшує контроль за адресним простором та запобігає конфліктам IP-адрес;

– Гнучкість. Можна задавати різні параметри для різних підмереж, пристроїв або груп користувачів, що дозволяє гнучко керувати мережею;

– Тимчасове надання адрес. IP-адреси надаються на обмежений час (лізинг), після чого можуть бути автоматично змінені або повторно використані, що ефективно оптимізує адресний простір.

Налаштовуємо DHCP для мережі LAN1

```
ip dhcp excluded-address 172.25.74.1 172.25.74.10
ip dhcp excluded-address 172.25.74.65 172.25.74.74
ip dhcp excluded-address 172.25.74.129 172.25.74.138

ip dhcp pool DHCP_VLAN25
network 172.25.74.0 255.255.255.192
default-router 172.25.74.1
dns-server 172.25.76.24
ip dhcp pool DHCP_VLAN35
network 172.25.74.64 255.255.255.192
default-router 172.25.74.65
dns-server 172.25.76.24
ip dhcp pool DHCP_VLAN45
network 172.25.74.128 255.255.255.192
default-router 172.25.74.129
dns-server 172.25.76.24
interface f1/0.25
encapsulation dot1Q 25
```

ip address 172.25.74.1 255.255.255.192

interface f1/0.35

encapsulation dot1Q 35

ip address 172.25.74.65 255.255.255.192

interface f1/0.45

encapsulation dot1Q 45

ip address 172.25.74.129 255.255.255.192

interface f1/0.99

encapsulation dot1Q 99

ip address 172.25.74.193 255.255.255.192

Для авторизації доступу до консолі передбачено використання протоколу RADIUS, а за його відсутності – звернення до локальної бази облікових даних. RADIUS (Remote Authentication Dial-In User Service) – це мережевий протокол, який використовується для централізованої аутентифікації, авторизації та обліку (AAA) доступу користувачів до мережевих ресурсів. Його основне призначення – забезпечення безпечного контролю доступу до мережевих пристроїв, Wi-Fi, VPN та інших служб.

Протокол RADIUS дозволяє відокремити процес перевірки прав доступу від мережевого обладнання, передаючи ці функції на окремий RADIUS-сервер. Коли користувач намагається підключитися до мережі, його облікові дані надсилаються серверу, який приймає рішення про доступ на основі збережених правил і бази користувачів.

Основні особливості та переваги використання RADIUS:

– Централізована аутентифікація. Усі запити на доступ перевіряються через один сервер, що полегшує адміністрування та забезпечує єдину політику безпеки;

– Гнучкість та масштабованість. RADIUS може працювати з великою кількістю пристроїв і користувачів, підтримуючи як локальні облікові записи, так і зовнішні бази, наприклад, LDAP або Active Directory;

– Безпека. Паролі передаються в зашифрованому вигляді, а також

підтримується детальний контроль доступу за рівнем привілеїв, IP-адресами, MAC-ідентифікаторами тощо;

– Облік і моніторинг. RADIUS фіксує всі спроби підключення, успішні та невдалі логіни, час сесій тощо. Це дозволяє проводити аудит та аналіз дій користувачів у мережі.

Налаштування протоколу RADIUS

aaa new-model

aaa authentication login default group radius local

radius server AAA

address ipv4 172.25.76.25

key radius123

exit

В якості Radius сервера будемо використовувати сервер який вже використовується для HTTP, для зменшення витрат.

Налаштування RADIUS-сервера виконується із використанням ключа автентифікації radius123. логін користувача Pototskyi_radius, а пароль – admin123. На рисунку 3.6 наведені налаштування AAA сервісу.

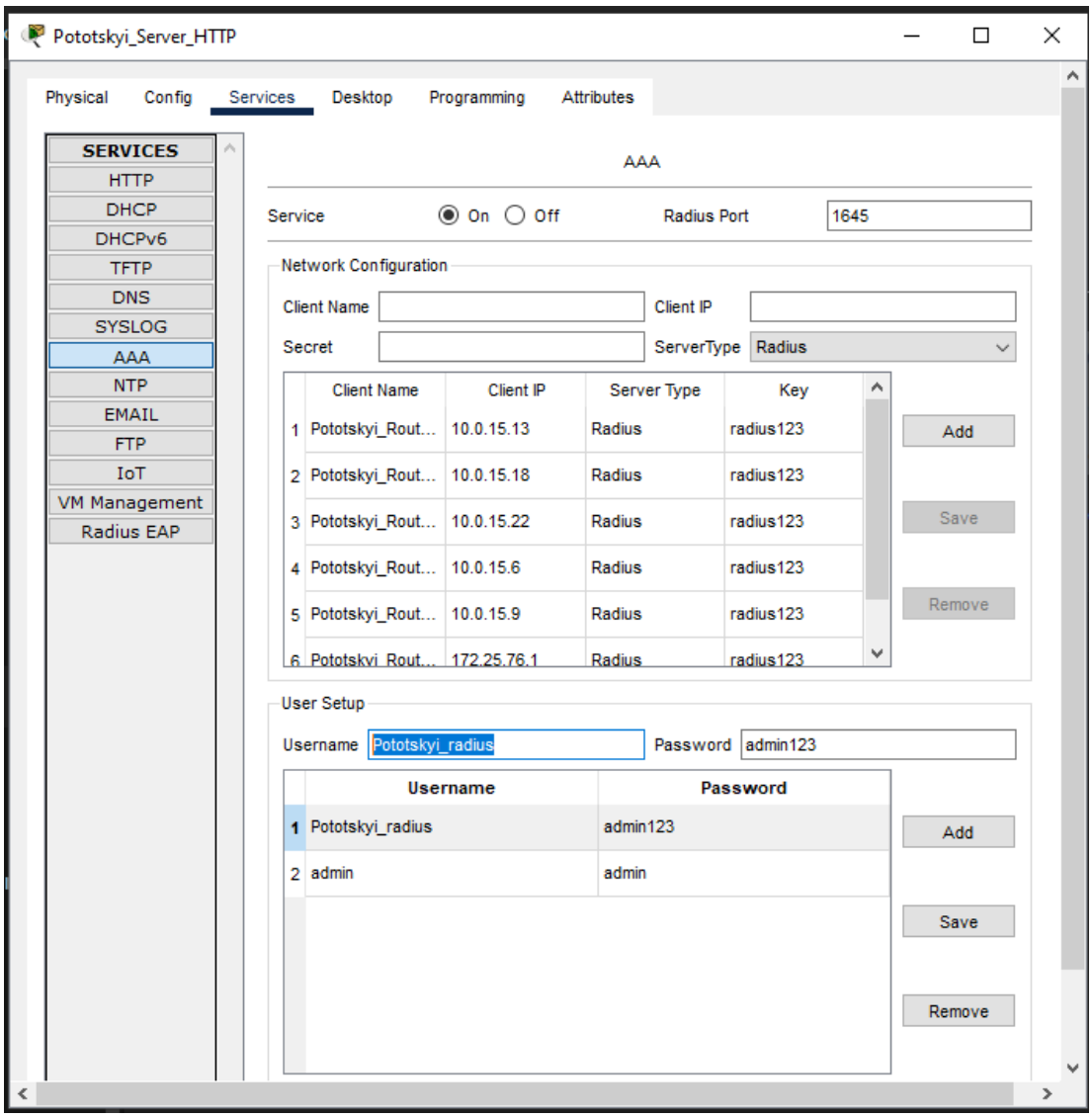


Рисунок 3.6 – Налаштування AAA сервера

Налаштування мереж VLAN

Віртуальна локальна мережа (VLAN) – це метод, що дозволяє розділяти одну фізичну мережу на кілька логічно незалежних сегментів. Кожен VLAN формує окрему групу пристроїв, які можуть взаємодіяти між собою, залишаючись ізольованими від інших віртуальних мереж. Такий підхід надає можливість структурувати мережу за принципом функціональності або організаційної належності, незалежно від фізичного розміщення обладнання.

Ключові переваги використання VLAN включають:

– Логічна сегментація мережі. VLAN дозволяє формувати незалежні групи пристроїв, які мають доступ лише до своїх ресурсів, що спрощує адміністрування та підвищує керованість мережевого середовища;

– Підвищення рівня безпеки. Ізоляція трафіку між VLAN дозволяє обмежити доступ до критичних сегментів мережі та зменшити потенційні загрози у разі зламу;

– Оптимізація мережевого трафіку. VLAN зменшує кількість широкомовних пакетів у загальному трафіку, що покращує загальну продуктивність та стабільність мережі.

Налаштування VLAN

```
interface vlan 99
ip address 172.25.74.194 255.255.255.192
no shutdown
vlan 25
name Administration
vlan 35
name Development
vlan 45
name Communications
vlan 99
name Management
vlan 100
name Native
interface range f0/5-9
switchport mode access
switchport access vlan 25
interface range f0/10-14
switchport mode access
switchport access vlan 35
interface range f0/15-24
switchport mode access
switchport access vlan 45
interface range g0/1-2, f0/1-4
```

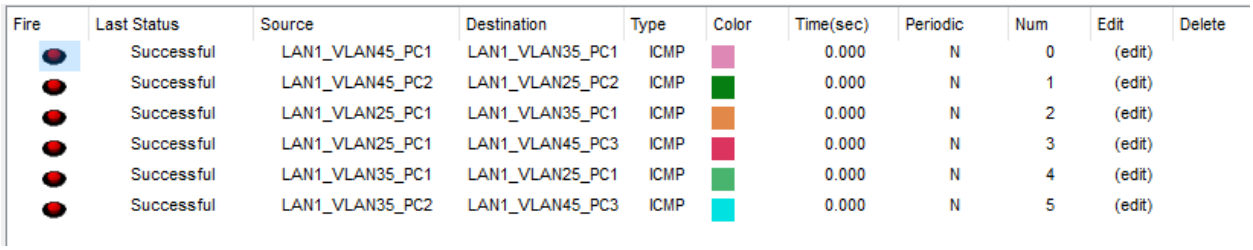
switchport mode trunk

switchport trunk allowed vlan all

switchport trunk native vlan 100

no shutdown

На рисунку зображено перевірку досяжності між VLAN



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	LAN1_VLAN45_PC1	LAN1_VLAN35_PC1	ICMP		0.000	N	0	(edit)	
	Successful	LAN1_VLAN45_PC2	LAN1_VLAN25_PC2	ICMP		0.000	N	1	(edit)	
	Successful	LAN1_VLAN25_PC1	LAN1_VLAN35_PC1	ICMP		0.000	N	2	(edit)	
	Successful	LAN1_VLAN25_PC1	LAN1_VLAN45_PC3	ICMP		0.000	N	3	(edit)	
	Successful	LAN1_VLAN35_PC1	LAN1_VLAN25_PC1	ICMP		0.000	N	4	(edit)	
	Successful	LAN1_VLAN35_PC2	LAN1_VLAN45_PC3	ICMP		0.000	N	5	(edit)	

Рисунок 3.7 – Результат перевірки VLAN

VPN (Virtual Private Network) – це технологія, яка дозволяє створити безпечне зашифроване з'єднання між користувачем і мережею через публічний Інтернет. VPN дає змогу передавати дані приватно, ніби користувач підключений до локальної мережі організації, навіть якщо він фізично знаходиться в іншому місці.

Ця технологія широко застосовується для забезпечення захищеного віддаленого доступу до корпоративних ресурсів, а також для захисту трафіку у відкритих або ненадійних мережах.

Основні особливості та переваги використання VPN:

– Конфіденційність і шифрування. Усі передані дані шифруються, що захищає їх від перехоплення, навіть у незахищених мережах (наприклад, публічному Wi-Fi);

– Віддалений доступ. Співробітники можуть безпечно працювати з корпоративною мережею з будь-якого місця світу, отримуючи доступ до внутрішніх систем і файлів;

– Захист від атак. VPN маскує реальне місцезнаходження та IP-адресу користувача, ускладнюючи спроби зовнішніх атак;

– Економія коштів. Використання VPN дозволяє об'єднувати офіси, філіали та віддалених працівників без необхідності створення окремих

фізичних з’єднань.

Налаштування VPN

```
access-list 115 permit ip 172.25.73.0 0.0.0.255 172.25.72.0 0.0.0.255
access-list 115 permit ip 172.25.74.0 0.0.0.255 172.25.72.0 0.0.0.255
access-list 115 permit ip 172.25.75.0 0.0.0.255 172.25.72.0 0.0.0.255
access-list 115 permit ip 172.25.76.0 0.0.0.255 172.25.72.0 0.0.0.255
crypto isakmp policy 10
authentication pre-share
encryption aes 256
group 5
exit
crypto isakmp key vpn address 64.100.13.2
crypto ipsec transform-set VPN-TRANSORM-SET esp-aes 256 esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
desc VPN Connect
set peer 64.100.13.2
set pfs group5
set security-association lifetime seconds 86400
set transform-set VPN-TRANSORM-SET
match address 115
exit
int f1/0
crypto map VPN-MAP
```

3.5 Перевірка роботи КС ТЦ

Проведене моделювання підтвердило, що розроблена комп’ютерна мережа працює надійно та повністю відповідає як функціональним, так і технічним вимогам, зазначеним у завданні до кваліфікаційної роботи. Успішна передача ехо-запитів між вузлами з різних підмереж свідчить про правильну конфігурацію протоколів маршрутизації, NAT, DHCP, VPN та

інших мережевих сервісів. Візуалізацію результатів тестування наведено на рисунку 3.8.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	In Progress	LAN1_VLAN45_PC3	LAN4_PC4	ICMP		0.000	N	0	(edit)	
	In Progress	LAN1_VLAN35_PC1	LAN3_PC6	ICMP		0.000	N	1	(edit)	
	In Progress	LAN1_VLAN25_PC2	LAN2_PC4	ICMP		0.000	N	2	(edit)	
	In Progress	LAN1_VLAN45_PC2	LAN5_PC1	ICMP		0.000	N	3	(edit)	
	In Progress	LAN4_PC3	LAN3_PC7	ICMP		0.000	N	4	(edit)	
	In Progress	LAN4_PC5	LAN2_PC3	ICMP		0.000	N	5	(edit)	
	In Progress	LAN4_PC6	LAN5_PC2	ICMP		0.000	N	6	(edit)	
	In Progress	LAN4_PC6	LAN5_PC2	ICMP		0.000	N	7	(edit)	
	In Progress	LAN3_PC6	LAN2_PC2	ICMP		0.000	N	8	(edit)	
	In Progress	LAN3_PC1	LAN5_PC8	ICMP		0.000	N	9	(edit)	
	In Progress	LAN2_PC5	LAN5_PC3	ICMP		0.000	N	10	(edit)	

Рисунок 3.8 – Результат перевірки КС

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

У межах корпоративної мережі була впроваджена IoT-система пожежогасіння, яка забезпечує автоматизований контроль за пожежною безпекою об’єкта та оперативне реагування на надзвичайні ситуації. Система складається з розумних датчиків диму та температури, розміщених у ключових зонах будівлі, а також з центрального контролера, який обробляє сигнали та керує відповідними пристроями гасіння.

Центральний контролер IoT-мережі Home Gateway інтегрований у підмережу LAN2.

Принцип роботи системи та взаємодія її компонентів виглядає так:

Моніторинг стану датчиків – контролер безперервно опитує датчики Fire Monitor та отримує поточні дані про рівень диму, температуру та інші показники.

Аналіз тривожних сигналів – у разі перевищення критичних порогів система миттєво активує тривогу.

Автоматичні дії – у разі підтвердженої загрози контролер запускає протипожежні засоби Fire Sprinkler.

Для реалізації даної системи було інтегровано Pototskyi_Server_IoT у корпоративну мережу. Йому було призначено IP-адресу 172.25.73.25 з мережевою маскою 255.255.255.0, що дозволяє йому взаємодіяти з іншими пристроями підмережі LAN2. Окрім цього, для забезпечення повноцінної маршрутизації та доступу до зовнішніх сервісів було вказано Default Gateway 172.25.73.1 та DNS-сервер 175.25.76.24.

Після базової конфігурації IoT-серверу, до комп’ютерної системи були додані всі необхідні пристрої,

Щоб перевірити стан підключених IoT-пристроїв та отримати доступ до функціоналу системи, необхідно з будь-якого комп’ютера мережі ввести в браузері IP-адресу IoT-сервера (172.25.73.25). Після цього відкриється веб-інтерфейс авторизації. Для входу до системи використовується обліковий

запис з логіном і паролем pototskyi. Цей рівень доступу забезпечує базову безпеку та обмежує несанкціонований доступ до критично важливої інфраструктури. На рисунку представлено процес авторизації в системі моніторингу IoT-серверу, де користувач вводить свої облікові дані для входу до панелі керування

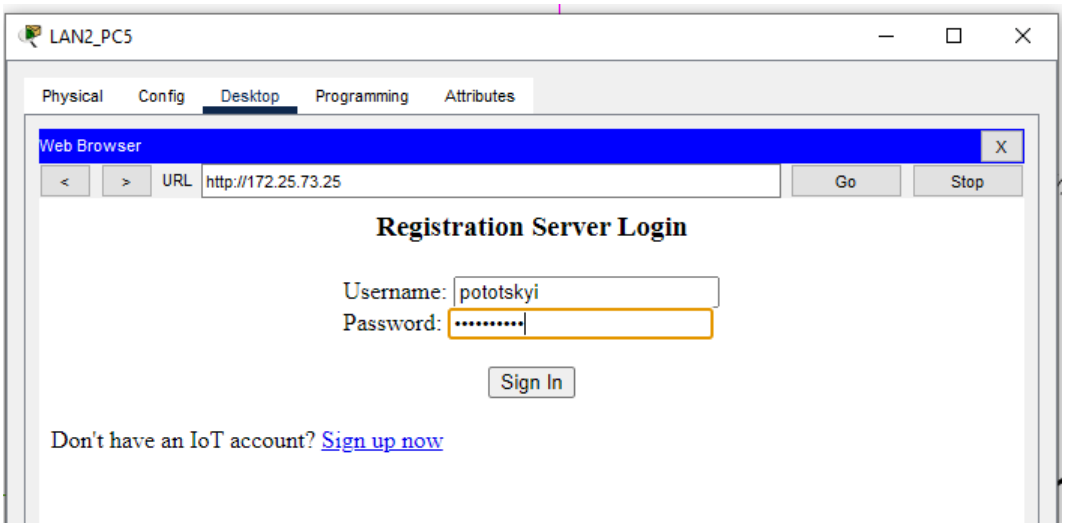


Рисунок 4.1 – Реєстрація облікового запису

Після успішної авторизації відкривається головна сторінка (див. рисунок 4.2) з інформацією про всі активні пристрої, їхній поточний стан.

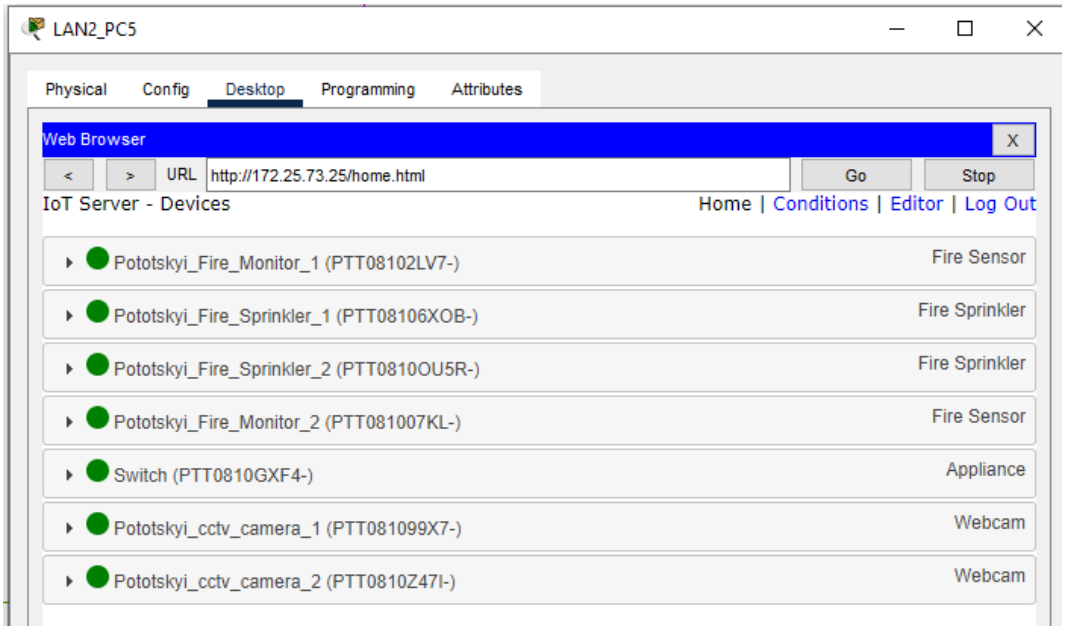


Рисунок 4.2 – Перегляд IoT-пристроїв на сервері

Переходимо до вкладки Conditions в інтерфейсі керування IoT-системою

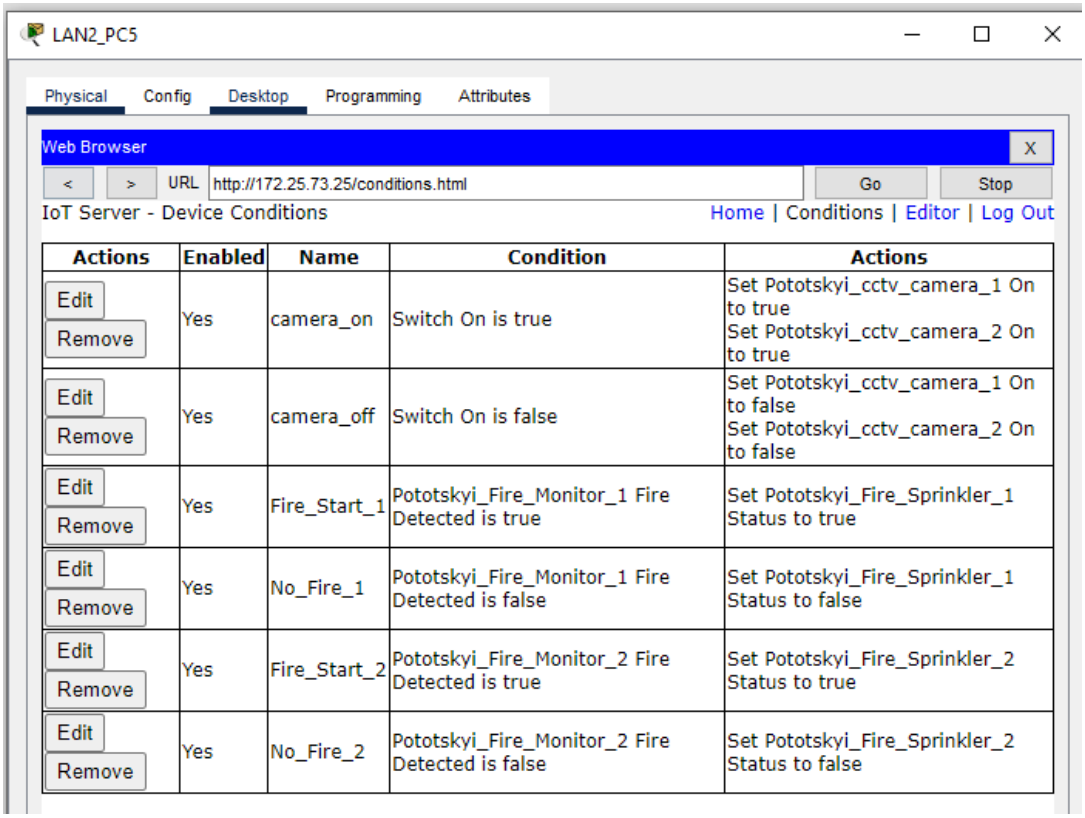
для створення списку автоматизованих подій. Саме ця вкладка відповідає за налаштування логіки взаємодії між датчиками та виконавчими пристроями у системі пожежогасіння.

Процес створення подій виконується за певним алгоритмом. Спочатку необхідно додати нову подію, натиснувши кнопку "Add", після чого потрібно задати їй унікальне ім’я, що дозволить легко ідентифікувати її серед інших. Назва має бути інформативною, наприклад, « Fire_Start_1».

Далі необхідно вибрати сенсор, який слугуватиме тригером, У нашому випадку це датчик пожежі. Після вибору сенсора переходимо до наступного етапу – вибір виконавчого пристрою, який має реагувати на спрацювання датчика. У нашій системі це автоматичний розпилювач води.

Кожна подія налаштовується індивідуально.

На рисунку наведено приклад створених подій у системі, де чітко видно взаємозв’язки між сенсорами та виконавчими пристроями, а також назви подій і тип дій, які буде виконано. Така візуалізація дозволяє легко аналізувати налаштування та вносити зміни у випадку оновлення конфігурації.



Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	camera_on	Switch On is true	Set Pototskyi_cctv_camera_1 On to true Set Pototskyi_cctv_camera_2 On to true
Edit Remove	Yes	camera_off	Switch On is false	Set Pototskyi_cctv_camera_1 On to false Set Pototskyi_cctv_camera_2 On to false
Edit Remove	Yes	Fire_Start_1	Pototskyi_Fire_Monitor_1 Fire Detected is true	Set Pototskyi_Fire_Sprinkler_1 Status to true
Edit Remove	Yes	No_Fire_1	Pototskyi_Fire_Monitor_1 Fire Detected is false	Set Pototskyi_Fire_Sprinkler_1 Status to false
Edit Remove	Yes	Fire_Start_2	Pototskyi_Fire_Monitor_2 Fire Detected is true	Set Pototskyi_Fire_Sprinkler_2 Status to true
Edit Remove	Yes	No_Fire_2	Pototskyi_Fire_Monitor_2 Fire Detected is false	Set Pototskyi_Fire_Sprinkler_2 Status to false

Рисунок 4.3 – Перелік усіх автоматизованих подій

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було створено повноцінну модель корпоративної комп’ютерної мережі для торгового центру з урахуванням географічної розподіленості, функціональних потреб та актуальних технічних вимог. Основні досягнення проєкту можна підсумувати так:

Сформовано ефективну систему IP-адресації, з використанням методу VLSM, що забезпечило раціональний розподіл адресного простору та можливість масштабування в майбутньому.

Спроєктовано та змодельовано мережеву інфраструктуру в середовищі Cisco Packet Tracer з включенням усіх необхідних компонентів: маршрутизаторів, комутаторів, серверів та кінцевих пристроїв.

Реалізовано ключові мережеві технології, зокрема VLAN для логічної сегментації, EtherChannel для збільшення пропускної здатності, а також EIGRP як динамічний протокол маршрутизації.

Забезпечено мережеву безпеку завдяки впровадженню NAT, IPsec VPN та централізованої автентифікації через RADIUS, що гарантує захищений доступ до ресурсів мережі.

Інтегровано IoT-рішення, орієнтоване на автоматизовану протипожежну систему з контролем стану датчиків та виконавчих пристроїв, що демонструє гнучкість і сучасність мережевої архітектури.

Проведено комплексне тестування усіх мережевих сервісів (DHCP, DNS, VPN, HTTP, RADIUS), що підтвердило стабільність, функціональність і готовність системи до практичного впровадження.

Таким чином, запропоноване рішення повністю задовольняє вимоги до безпечної, масштабованої та ефективної корпоративної мережі. Результати роботи можуть бути використані як основа для впровадження аналогічних систем в інших організаціях або як практичний кейс для освітніх цілей у

сфері мережевих технологій.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. .

2. https://www.acer.com/ru-ru/desktops-and-all-in-ones/aspire-all-in-ones/aspire-c24/pdp/DQ.BHRER.003#pdpSpecs.

3. https://shop.lenovo.ua/ru/servera/thinksystem-st50-v2-7d8ja02yea.html?srsltid=AfmBOoobWSsAqLoL7YWZ-S-oQpkew5qDdwiKfgH4hYjimmzYdlsfwfIj#prodSpecs.

4. https://stack-systems.com.ua/kommutator-cisco-c1000-24fp-4g-l.

5. https://stack-systems.com.ua/marshrutizator-cisco-c8200-1n-4t.

6.

ДОДАТОК А

Текст команд для налаштування комп’ютерної мережі

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.25015-01 12 01

Листів

2025

АНОТАЦІЯ

У цій програмі представлено фрагмент програмного коду, що забезпечує налаштування основних компонентів корпоративної мережі комп’ютерної системи. Основне призначення – реалізація базових конфігурацій мережевих інтерфейсів, впровадження динамічного розподілу IP-адрес за допомогою протоколу DHCP для VLAN, налаштування системи автентифікації AAA з використанням протоколу RADIUS, створення локального облікового запису користувача, конфігурування динамічної маршрутизації на основі EIGRP, забезпечення доступу до консолі та віртуальних ліній, а також налаштування VPN-з’єднання і механізму динамічного NAT.

ЗМІСТ

1. Налаштування маршрутизатора

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Pototskyi_Router_1
!
ip dhcp excluded-address 172.25.73.1 172.25.73.25
!
ip dhcp pool security
network 172.25.73.0 255.255.255.0
default-router 172.25.73.1
dns-server 172.25.76.24
!
aaa new-model
!
aaa authentication login default group radius local
!
no ip cef
no ipv6 cef
!
username 123212_Pototskyi secret 5 $1$mERr$MKp6WULHmjLdYVBw6rbD11
!
license udi pid CISCO2811/K9 sn FTX1017X8M9-
!
ip ssh version 2
no ip domain-lookup
ip domain-name Pototskyi_Router_1
```

```
!
spanning-tree mode pvst
!
interface FastEthernet0/0
ip address 10.0.15.14 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.0.15.9 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 10.0.15.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 172.25.73.1 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router eigrp 15
passive-interface FastEthernet1/1
network 10.0.15.0 0.0.0.3
```

```
network 10.0.15.8 0.0.0.3
network 10.0.15.12 0.0.0.3
network 172.25.73.0 0.0.0.255
!
router rip
!
ip classless
!
ip flow-export version 9
!
banner motd ^CThe system is protected by a security system.^C
!
radius server AAA
address ipv4 172.25.76.25 auth-port 1645
key radius123
radius server 172.25.76.25
address ipv4 172.25.76.25 auth-port 1645
key radius123
!
line con 0
password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
transport input ssh
line vty 5 15
transport input ssh
!
end
```

2 Налаштування граничного маршрутизатора

```
Current configuration : 2997 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Pototskyi_Router_5
!
aaa new-model
!
aaa authentication login default group radius local
!
no ip cef
no ipv6 cef
!
username 123212_Pototskyi secret 5 $1$mERr$MKp6WULHmjLdYVBw6rbD11
!
license udi pid CISCO2811/K9 sn FTX1017UI0S-
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key vpn address 64.100.13.2
!
crypto ipsec transform-set VPN-TRANSORM-SET esp-aes 256 esp-sha-hmac
```

```
!
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN Connect
 set peer 64.100.13.2
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set VPN-TRANSORM-SET
 match address 115
!
ip ssh version 2
no ip domain-lookup
ip domain-name Pototskyi_Router_5
!
spanning-tree mode pvst
!
interface FastEthernet0/0
 ip address 10.0.15.6 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.15.2 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 209.165.202.2 255.255.255.252
 ip nat outside
```

```
 crypto map VPN-MAP
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet1/0
 ip address 10.0.15.17 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet1/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 15
 redistribute static
 network 10.0.15.0 0.0.0.3
 network 10.0.15.4 0.0.0.3
 network 10.0.15.16 0.0.0.3
!
ip nat pool Outside 209.165.200.5 209.165.200.30 netmask 255.255.255.224
```

```
ip nat inside source list For_NAT pool Outside
ip nat inside source static 172.25.76.25 209.165.200.4
ip nat inside source static 172.25.76.24 209.165.200.3
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip flow-export version 9
!
access-list 115 permit ip 172.25.73.0 0.0.0.255 172.25.72.0 0.0.0.255
access-list 115 permit ip 172.25.74.0 0.0.0.255 172.25.72.0 0.0.0.255
access-list 115 permit ip 172.25.75.0 0.0.0.255 172.25.72.0 0.0.0.255
access-list 115 permit ip 172.25.76.0 0.0.0.255 172.25.72.0 0.0.0.255
ip access-list extended For_NAT
 deny ip 172.25.73.0 0.0.0.255 172.25.72.0 0.0.0.255
 deny ip 172.25.74.0 0.0.0.255 172.25.72.0 0.0.0.255
 deny ip 172.25.75.0 0.0.0.255 172.25.72.0 0.0.0.255
 deny ip 172.25.76.0 0.0.0.255 172.25.72.0 0.0.0.255
 permit ip 172.25.73.0 0.0.0.255 any
 permit ip 172.25.74.0 0.0.0.255 any
 permit ip 172.25.75.0 0.0.0.255 any
 permit ip 172.25.76.0 0.0.0.255 any
!
banner motd ^CThe system is protected by a security system.^C
!
radius server AAA
 address ipv4 172.25.76.25 auth-port 1645
 key radius123
radius server 172.25.76.25
 address ipv4 172.25.76.25 auth-port 1645
 key radius123
```

```
!
line con 0
 password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
 transport input ssh
line vty 5 15
 transport input ssh
!
end
```