Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра
(бакалавра, спеціаліста, магістра)

студента Омельяненка Андрія Олексійовича
(ПІБ)

академічної групи 123-18ск-1
(шифр)

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

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

на тему « Комп'ютерна система ТОВ «М - Систем» з детальним опрацюванням побудови, налаштування та підсистеми захисту віддаленого доступу до корпоративної мережі »
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Шедловський І.А.			
розділів:				
апаратний розділ	Доц. Ткаченко В.В.			
проектування мережі та захист інформації	ас. Панферова Я.В.			
програмне забезпечення	ас. Бешта Л.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2021

ЗАТВЕРДЖУЮ
Завідувач кафедри
Інформаційних
технологій та
комп'ютерної інженерії

проф._____В.В. Гнатушенко
"__" _____ 2021 р.

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту Омельяненко А.О академічної групи 123-18ск-1
(прізвище та ініціали) (шифр)
спеціальності 123 «Комп'ютерна інженерія»

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

на тему « Комп'ютерна система ТОВ «М - Систем» з детальним опрацюванням побудови, налаштування та підсистеми захисту віддаленого доступу до корпоративної мережі »
затверджена наказом ректора НТУ "Дніпровська політехніка" від 07.06.2021 р. №317-с

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	Застосувати звіт з виробничої практики, інших науково-технічних джерел та розробити технічні вимоги до комп'ютерної системи цеху збирання ТОВ "Усі мотоблоки"	20.03.21р.
Технічні вимоги до комп'ютерної системи	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної системи цеху збирання ТОВ "Усі мотоблоки"	24.04.21р.
Спеціальна частина	Розв'язати завдання з розробки комп'ютерної системи цеху збирання ТОВ "Усі мотоблоки"	15.05.21р
Графічна частина	Графічні результати розробки системи подати у вигляді рисунків електричних схем та інших креслень на 10 арк. формату А4	10.06.21р.

Завдання видано _____ доц. Шедловський І.А.
(підпис керівника) (прізвище та ініціали)
Дата видачі 03.02.2021 р.

Дата подання до екзаменаційної комісії 12.06.2021 р.
Прийнято до виконання _____ Омельяненко А.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 65с., 35 рис., 4 табл., 4 додатка, 14 джерел.

Об’єкт проектування: комп’ютерна система товариства з обмеженою відповідальністю «М - Систем».

Мета – розробити комп’ютерну систему товариства, яка займається продажами сільгосптехніки для об’єднання інформаційних ресурсів та полегшення роботи працівників з базами даних та обліку товарів.

Спроектована система дає можливість збільшити робочі місця та мережеві пристрої за необхідністю.

Розроблена система виконана з можливостю гнучкої зміни числа пристроїв для збільшення робочих місць за необхідністю.

Розробка комп’ютерної мережі виконана відповідно до завдання на кваліфікаційну роботу ступеня бакалавра.

Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco PacketTracer, де перевірена її робота.

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці та додатках.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IT – Information Technology (Інформаційні технології).

DNS– Domain Name System.

HTTP – HyperText Transfer Protocol

IP – Internet Protocol

LAN – Local Area Network

КС – Комп'ютерна система

ТОВ – Товариство з обмеженою відповідальністю

Bt Бітовий інтервал

ВСТУП

У сучасному світі ІТ має дуже важливу роль у економічних, комунікативних, промислових та інших галузях. Залежність інфраструктури, онлайн-сервісів, онлайн-банкінгу від Інтернету зростає у геометричній прогресії.

Інформаційні технології, ІТ — це система методів, процесів та способів використання обчислювальної техніки і систем зв'язку для створення, збору, передачі, пошуку, оброблення та поширення інформації з метою ефективної організації діяльності людей [1].

ІТ технології тісно пов’язані з технологією Інтернет. Для того, щоб розуміти всю залежність цих технологій, потрібно поглибитись у історію розробки та спроби реалізації технології у її прототипах.

Інтернет (від англ. Internet), міжнародна комп'ютерна мережа, — всесвітня система сполучених комп'ютерних мереж, що базуються на комплекті Інтернет-протоколів.

У наш час Інтернет став доступним не лише через комп'ютерні мережі, але й через супутники зв'язку, радіосигнали, кабельне телебачення, телефонні лінії, мережі стільникового зв'язку, спеціальні оптико-волоконні лінії і електропроводи. Всесвітня мережа стала невід'ємною частиною життя у розвинутих країнах, та країнах, що розвиваються [2].

До пристроїв, які зазвичай використовуються для бездротових мереж, належать портативні комп’ютери, настільні комп’ютери, ручні комп’ютери, персональні цифрові помічники (КПК), стільникові телефони, комп’ютери на основі ручок та пейджери. Бездротові мережі працюють подібно до дротових мереж, проте бездротові мережі повинні перетворювати інформаційні сигнали у форму, придатну для передачі через повітряне середовище. Бездротові мережі служать багатьом цілям. В деяких випадках їх використовують як заміну кабелю, тоді як в інших випадках вони надають доступ до корпоративних даних із віддалених місць.

Бездротову інфраструктуру можна побудувати за дуже невеликі витрати порівняно з традиційними дротовими альтернативами. Але побудова бездротових мереж лише частково стосується економії грошей. Надаючи людям у вашій місцевій громаді дешевший та простіший доступ до інформації, вони безпосередньо виграють від того, що може запропонувати Інтернет. Економія часу та зусиль завдяки доступу до глобальної мережі інформації перетворюється на багатство в місцевому масштабі, оскільки більша робота може бути виконана за менший час та з меншими зусиллями.

Бездротові мережі дозволяють віддаленим пристроям підключатися без труднощів, незалежно від них, що знаходяться на відстані декількох футів або декількох кілометрів. І не потрібно проривати стіни, щоб пропустити кабелі або встановити роз'єми. Це зробило використання цієї технології дуже популярним, швидко поширюючись.

Існує багато різних технологій, які відрізняються частотою передачі, швидкістю та діапазоном їх передачі.

У дипломному проекті буде детально описана комп'ютерна мережа ТОВ «М - Систем», з подальшою її модернізацією та розширенням сучасними як програмними, так і апаратними засобами.

Необхідність модернізації комп'ютерної мережі обумовлена дуже швидким розвитком технологій, відповідно, втратою продуктивності в порівнянні з сучасними темпами і тенденціями збільшення швидкості передачі даних по локальних та глобальної мережі і деякими апаратно-програмними оновленнями в міру їх попиту.

Розширення мережі трактується оновленням штату робітників компанії та додавання нових спектрів послуг в переліку виконуваних робіт.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика системи, що проектується

Компанія «М - Систем» займається онлайн та офлайн консультаціями з супроводження бізнесу роздрібної та оптової торгівлі. Засновниками підприємства являються юридичні фірми та фізичні особи. Вони э дилером онлайн площадки Prom.ua. Реалізація послуг охоплює Україну та деяких закордонних замовників [3].

Prom.ua — український маркетплейс, проект IT-компанії EVO. На його платформі підприємці самостійно створюють інтернет-магазини або розміщують свої товари в загальному каталозі. Для покупців на Промі зібрано більше 100 мільйонів товарів [4].

Однією зі сфер діяльності компанії є налаштування контекстної реклами на конкретний товар, групу товарів. Контéкстна рекла́ма (англ. Content-targeted advertising) — принцип розміщення реклами, коли реклама орієнтується на зміст інтернет-сторінки вручну або автоматично, може бути у вигляді банера чи текстового оголошення. Наприклад, на сайті, присвяченому мотоциклам, контекстна реклама пов'язуватиметься з мотоциклами та мотоциклістами. Принцип контекстної реклами характерний також для друкованих ЗМІ, де відповідно до змісту матеріалів чи тематики видання публікується та чи інша інформація.

1.2 Організаційна структура компанії ТОВ «М - Систем»

Компанія складається з керівництва та підпорядкованих їй команд, це відображено на Рис. 1.1.

До керівництва входять:

- генеральний директор;
- заступник директору;
- головний бухгалтер;
- керівники відділів.

Генеральний директор виступає найвищим керівником. Здійснює адміністративно-розпорядчі функції та приймає рішення по всіх питаннях діяльності компанії. Він організовує усю роботу компанії і несе повну відповідальність за її інтернет діяльність.

Відділ залучення трафіку відповідає за постачання послуг налаштування контекстної реклами, SEO просування, правки контенту на сайтах клієнтів. Від нього, в основному залежить виконання виробничих завдань і поліпшення техніко-економічних показників компанії. Він тісно пов'язаний зі всіми іншими відділами, так як технічні завдання виконують саме ці спеціалісти.

Залученням клієнтів в основному займається відділ перших продаж. Спеціалісти, що пройшли кваліфікаційне навчання у галузі продаж, мають базу "теплих" клієнтів, що потенційно можуть бути зацікавлені у галузі просування його товару у інтернет майданчику Prom.ua, або ж які можуть мати "зовнішні" сайти, які потребують SEO оптимізації та консультації у розвитку його бізнесу. У разі, якщо клієнт замовляє послуги у компанії, за ним закріплюється професійний бізнес-консультант (аккаунт-менеджер).

Тим клієнтам, які потребують бізнес-консультації, прогнозування на ціни ринку, релевантність пошукових запитів, оптимізації їх товарних позицій, прикріплені персональні бізнес-консультанти (аккаунт-менеджери).

Саме ці спеціалісти виконують зв'язуючу функцію у компанії, так як вони складають технічні завдання для відділу залучення трафіку.

Для клієнтів, що мають бажання швидко інтегруватися у ринок, існує відділ повторних продажів. У цьому відділі компанія займається продажом вже готових рішень та сайтів, що попередньо налаштовані під галузь, якою бажає торгувати їх клієнт.

Рисунок 1.1 – Ієрархія організації посад ТОВ «М - Систем»

1.3 Організація комп'ютерного та мережевого обладнання

Мережа нових офісів ТОВ «М - Систем», (Рис. 1.2) розташована за адресами:

- набережна Перемоги, 36а;
- Олександра Поля, 22;
- проспект Дмитра Яворницького, 34б;
- Михайла Грушевського, 12.

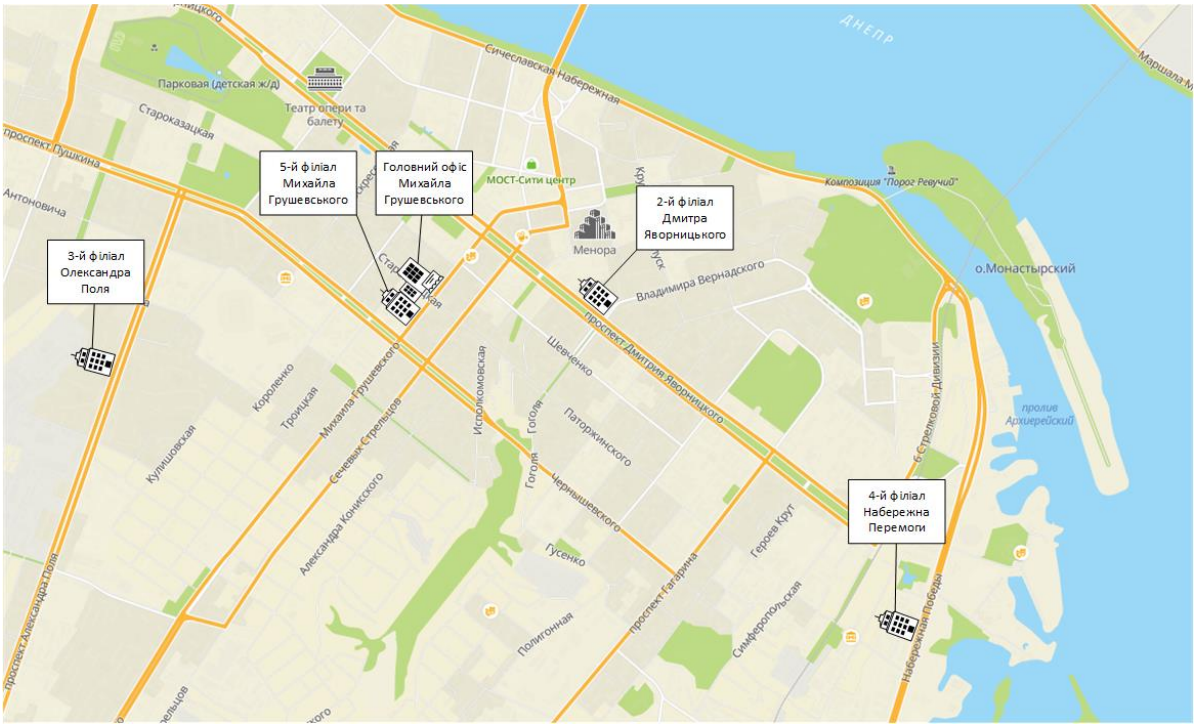


Рисунок 1.2 Територіальне розміщення філіалів ТОВ «М - Систем»

У нових офісах на даний момент відсутнє необхідне нам обладнання для побудови як локальної, так і повноцінної корпоративної мережі, тому ми будемо брати приклад з вже існуючої структури мережі, яка знаходиться у головному офісі компанії, розташованим за адресом: вул. Михайла Грушевського 8, відмічено

на мапі (Рис. 1.3)

На даний момент у головному офісі компанії знаходиться наступне обладнання:

– 21 комп'ютер, на яких встановлена операційна система Windows 10;

– CRM система MegaPlan, що працює у хмарному режимі;

– маршрутизатор, на який заходить основне інтернет з'єднання;

– 5 Wi-fi адаптерів для ПК, що знаходяться у складних місцях для прокладання дротового Інтернет зв'язку.

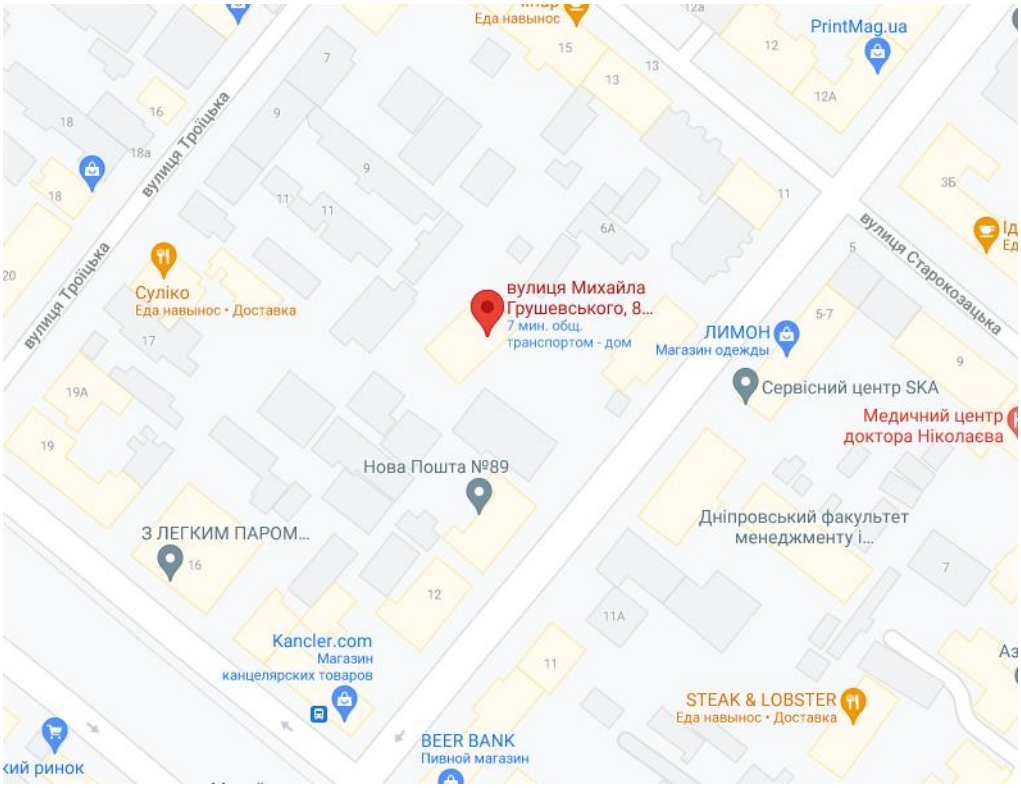


Рисунок 1.3 Територіальне розміщення головного офісу ТОВ «М - Систем»

Розподіл інтернету у мережі головного офісу відбувається за рахунок популярного у даній сфері рішення «Розетка-порт» (Рис. 1.4.)

Рисунок 1.4 Розетка-порт

Завдяки цим пристроям здійснюється доступ до глобальної мережі на робочих комп'ютерах. Також вони з'єднують маршрутизатори TP-Link TL-WR845N з доступом до інтернету, та комутатор STN-2410 на 24 порти.

Для комп'ютерів, що мають бездротовий доступ до маршрутизаторів, компанія придбала USB Wi-fi адаптери Tenda W311 Mi.

У плані топології, мережа головного офісу представляє собою об'єднання «Зіркою» (Рис. 1.5.), але з однією особливістю. Комутатори, до яких під'єднані робочі станції, мають по 24 порти для їх з'єднання. У мережі головного офісу будуть знаходиться 122 робочі станції, які будуть з'єднані декількома комутаторами на 24 порти.

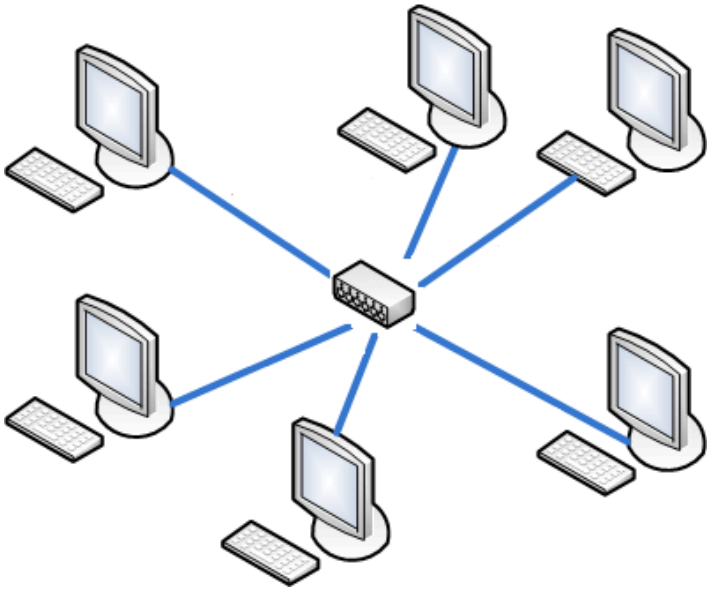


Рисунок 1.5 Топологія «Зірка»

1.4 Завдання і мета роботи

Для аутсорсингової компанії з реалізацією інтернет-послуг, підтримка надійного та швидкісного інформаційного обміну є важливим фактором. При цьому необхідно не тільки забезпечувати передачу різнорідної інформації, але і управляти територіально розподіленими офісами. Тому метою роботи є створення сучасної інформаційної мережі передачі даних, яка об'єднує адміністрацію ТОВ «М - Систем» з його структурними підрозділами, забезпечивши надходження всієї необхідної інформації в центр для оперативного та ефективного управління. Особливість проектування мережі передачі даних для територіально розподілених офісів залежить від переданої інформації і вимог до їх ефективності.

Метою випускної кваліфікаційної роботи є проектування інформаційної мережі компанії шляхом об'єднання територіально розподілених офісів. Для досягнення поставленої мети потрібно вирішити наступні завдання:

- вивчення структури офісів;
- має бути визначений розмір мережі. Під розміром мережі в даному випадку розуміється як кількість об'єднуваних в мережу комп'ютерів, так і відстань між ними;
- потрібно чітко уявляти собі, яка кількість активних і пасивних пристроїв буде в мережі, оскільки це сильно впливає на продуктивність і складність обслуговування мережі, а також на вартість необхідних програмних засобів. Тому помилки в даному випадку можуть мати досить серйозні наслідки.

1.5 Аналіз та розміщення робочих місць в офісі ТОВ «М - Систем»

Перед тим, як проектувати мережу, потрібно підрахувати кількість необхідних робочих місць і їх розміщення. У головному офісі компанії знаходиться 122 робочих місця на декількох поверхах. Всі поверхи ідентичні і розміщення робочих місць не змінюється, тому наведено в приклад один з поверхів, що зображено на рисунку 1.6

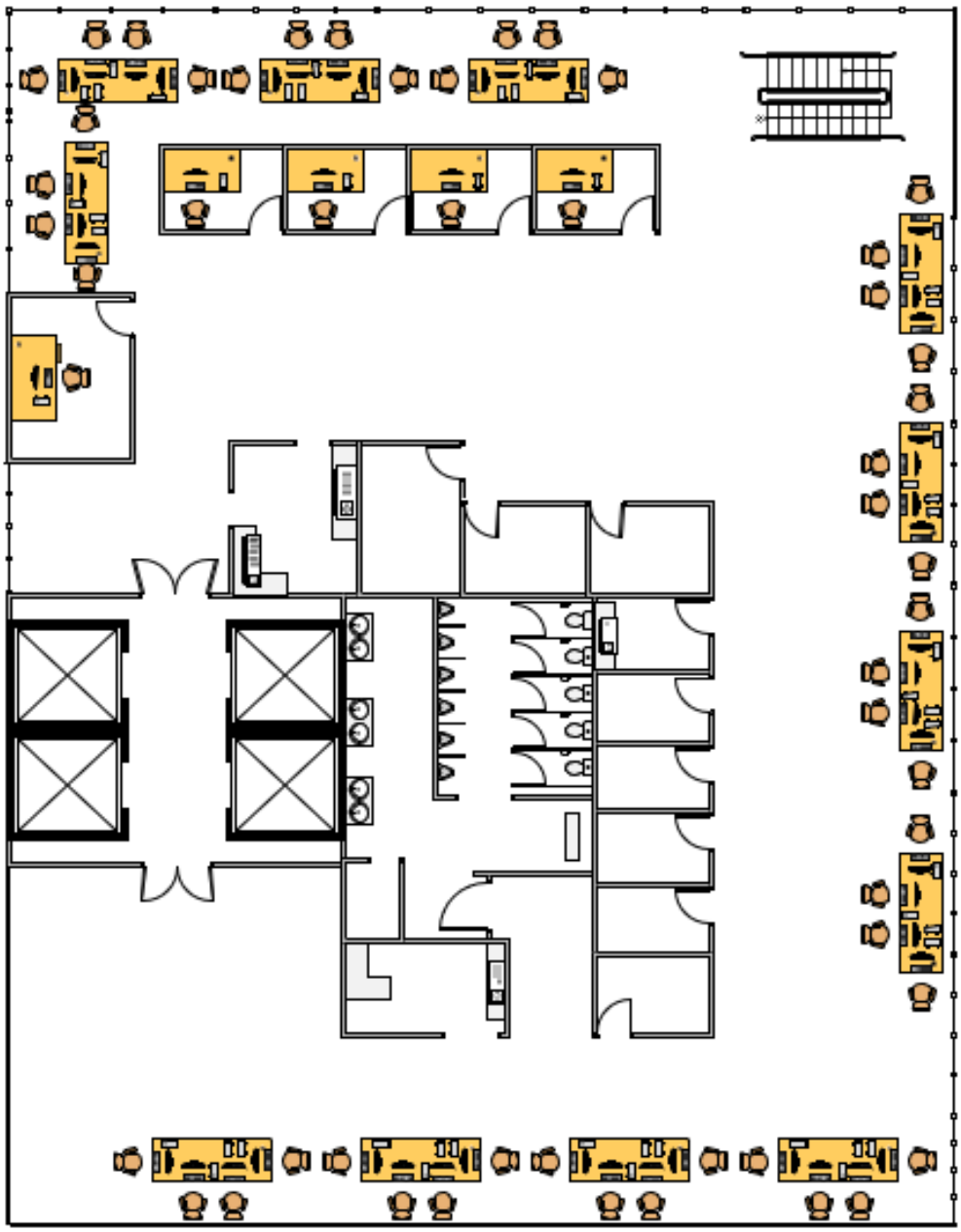


Рисунок 1.6 План розміщення робочих станцій головного офісу ТОВ «М - Систем»

2 ТЕХНІЧНІ ВИМОГИ ДО КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Вимоги до системи в цілому

Для того, щоб без перешкод розширювати та модернізувати вже існуючу мережу та об'єднання її з новими, висунуті наступні вимоги:

- наявність Інтернет на кожному ПК;
- Wi-Fi доступ для працівників офісів;
- має бути придбано нове комп'ютерне та мережеве обладнання;
- доступ для працівників компанії до хмарної CRM-системи на кожному ПК;
- обладнання повинно бути вибране, засновуючись на технічних характеристиках, задовольняючих вимогам швидкісної передачі даних;
- безпечність обладнання у разі ураження електричним струмом також повинно задовольняти вимогам;
- кількість робочих комп'ютерів у головному офісі – 112;
- робочий комп'ютер як місце для роботи, повинен являтися повноцінним для використання та роботи на ньому;
- розташування робочих місць та обладнання повинно задовольняти стандартам розміщення;
- фінансові витрати на створення локальних мереж та їх об'єднання повинні бути мінімізовані;
- інформаційна кабельна підсистема повинна будуватися відповідно до стандарту ISO / IEC 11801 Class D, Категорія 5e.

  – Всі провідні системи локальних мереж повинні бути захищені від зовнішніх факторів, включаючи: прокладення кабелів за гіпсокартоновими стінами, у спеціальних кабель-каналах, кріплення кабелів стяжками по всій довжині.

2.1.1 Вимоги до структури і функціонування системи

У корпоративній мережі, що розробляється, треба передбачати всі варіанти її застосування у даній компанії, для цього необхідно:

- Забезпечити вільний обмін інформацією між кожним користувачем мережі;
- Забезпечити працівникам компанії вільний доступ у Інтернет;
- Забезпечити надійність каналів обміну інформації, як в межах локальних мереж, так і поза ними;
- Забезпечити вільний для працівників компанії доступ до периферії;
- Підготувати основу для створення інформаційного простору;
- Обов'язкове забезпечення системами безпеки на етапі розгортання та інших етапів передачі даних.

2.1.2 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему і режиму його роботи

Для головного офісу та декількох філіалів ТОВ «М - Систем» по м. Дніпро потрібно буде як штатний системний адміністратор, так і підрядний, який буде відповідати за інші три офіси компанії, та які будуть працювати згідно з затвердженим загальним графікам цієї компанії.

Обов'язки системного адміністратора у ТОВ «М - Систем»:

- встановлення програмного забезпечення на робочі станції користувачів;
- забезпечення оновлення програмного забезпечення до оптимальних для роботи версій;
- підтримка робочого стану апаратного та програмного забезпечення на комп'ютерах користувачів;

- призначення та ведення реєстру ідентифікаторів для користувачів мережі ТОВ «М - Систем», надання паролів доступу до необхідних для роботи ресурсів;
- навчати та підказувати користувачам щодо роботи з специфічним програмним забезпеченням, відповідати на запитання щодо експлуатації периферії;
- складання технічних інструкцій щодо експлуатації під час роботи того чи іншого програмного забезпечення або ресурсів мережі;
- контроль ресурсів та доступу у мережу;
- організація доступу до локальних або глобальної мережі;
- встановлення специфічних обмежень доступу до інформації, що може бути, або являє собою комерційну таємницю.
- забезпечення своєчасних бекапів операційних систем, інформації, відновлення даних;
- своєчасно звертатися до технічного персоналу у випадках виявлення перебою або поломки периферійного, апаратного або мережевого обладнання;
- приймання участі під час роботи з відновлення працездатності систем при виникненні неполадок або виходу з ладу периферійного, апаратного або мережевого обладнання;
- виявлення помилок користувачів мережі і відповідно, мережевого обладнання, проведення відновлення працездатності систем;
- проведення моніторингу мереж, розробка пропозицій для поліпшення роботи мережі а також її модернізації,

Системний адміністратор повинен забезпечувати:

- захист від підозрілих спроб авторизації у мережі, несанкціонованого перегляду файлів і даних користувачами, які не є персоналом з допуском до цієї інформації;
- супроводження поштових та хмарних ресурсів;

- безпека меж мережевого доступу, взаємодії, передачі файлів, інформації;
- забезпечення захисту від вірусного програмного забезпечення.

Також він забезпечує:

- контролює процес прокладки та монтажу кабельних систем мережі, її апаратної частини, фахівцями із підрядних організацій;
- повідомляє безпосередньому керівнику о випадках зловживання мережевими ресурсами і вжиті заходи, щоб вони не повторювалися;
- ведення журналу користувачів і системи;
- ведення технічної документації;
- ведення таблиці комутацій, схеми маршрутизації;
- ведення журналу відомості про інвентаризацію технічних цінностей відділу інформаційних технологій.

Системний адміністратор повинен мати навички у наступних програмних та мережево-апаратних засобах:

- ОС MSWindows 7/8/10;
- ОС WindowsServer 2012/2016/2019;
- Linux (*CentOS*);
- серверне устаткування HP, Cisco, Dell;
- TCP/IP, VPN;
- віртуалізація VirtualBox, VMware або Hyper-V;
- резервне копіювання;
- технології дротового і бездротового доступу до Інтернет;
- ActiveDirectory, DNS, DHCP;
- офісний пакет MS Office, Libre Office (для Linux систем);
- англійська мова, рівня Technical (Технічний рівень знань) для можливості читати та писати на ній.

2.1.3 Вимоги до надійності і захисту інформації від несанкціонованого доступу

Локальна мережа офісів повинна забезпечувати:

- незмінність та збереження інформації, що оброблюється, при спробах зовнішніх або несанкціонованих впливів на неї;
- доступ користувачів мережі до інформації, що в ній міститься, повинен бути безперешкодний;
- захист від не передбачених дій користувачів на інформацію, що міститься у мережі, від знищення, модифікації та блокування;

В мережі, як в програмному так і в апаратному плані, повинне бути забезпечення:

- цілісності та доступності даних, їх підтримка;
- попередження та можливі заходи щодо несприятливих послідків порушення доступу до даних;
- регулярне проведення заходів, щодо запобігання неправомірних дій над інформацією;
- запобігання впливу на апаратно-технічні засоби загального користування, що може призвести до порушення їх функціонування;
- можливість відновлення інформації у короткий термін, заміненої або стертої внаслідок несанкціонованого доступу або неправомірних дій;
- проведення профілактичних або практичних заходів щодо контролю захищеності інформації;
- можливість ведення журналу мережевого трафіку;

Заходи про забезпечення захисту інформації приведені нижче:

- виявлення загроз до безпеки інформації, складання на їх основі моделювання загроз;
- розробку на базі моделі небезпек системи оборони інформації, що гарантує нейтралізацію можливих небезпек з використанням методів і методик оборони інформації;

- випробування готовності засобів оборони інформації до застосування зі складанням рішень в здатності їх експлуатації;
- встановлення і вступ в використання засобів оборони інформації відповідно до експлуатаційної та технічної документації;
- підготовка людей, що користуються засобами оборони інформації, що використовуються в інформаційній мережі загального користування, послідовністю та правилам роботи з цими засобами;
- обрахування використовуваних засобів оборони інформації, технічної та експлуатаційної документації;
- нагляд за дотриманням вимог експлуатації засобів оборони інформації, передбачених технічною та експлуатаційною документацією;
- проведення розгляду і складання рішень по прецедентах невиконання умов застосування засобів оборони інформації, які мають всі шанси привести до порушення захищеності інформації або ж інших порушень, що знижують ступінь безпеки системи, розробку і вживання заходів щодо запобігання можливим небезпечних наслідків аналогічних порушень.

2.2 Вимоги до функцій, які виконує КС

2.2.1 Імена робочих груп

Робоча група – це сукупність робочих станцій у локальній мережі, які мають спільний доступ до файлообміну та периферії.

У мережі компанії ТОВ «М - Систем» існує кілька робочих груп, які розділяються на:

- Робочу групу, яка належить керівництву, під назвою «LeadGroup». До неї належить ПК директору, його замісника, бухгалтера та керівників відділу Залучення трафіку, аккаунтінгу та перших продажів;

- Та групу, до якої належать усі інші робітники компанії під назвою «WorkGroup», такі як:
    - Менеджери перших продажів;
    - Аккаунт-менеджери;
    - Спеціалісти відділу залучення трафіку.

2.2.2 Ідентифікатори користувачів локальної мережі

Кожен ПК захищений паролем доступу до персонального акаунту, та який забезпечує доступ до інформації та ресурсам мережі. Одним комп'ютером може користуватись лише один працівник компанії. Ідентифікатором робітника являється логін та пароль до входу в робочу систему.

Якщо розглядати тему ідентифікації користувачів з боку мережі, то кожний ПК має свою MAC-адресу, що визначається мережевою картою. Саме за цією адресою дається доступ до мережі та існуючих на ній ресурсах.

У противному випадку, якщо MAC-адреса пристрою буде змінена, або у мережу додають будь-який інший пристрій, доступ до обчислюваної мережі таких несанкціонованих випадків, буде припинено або одразу заборонено [5].

2.2.3 Паролі користувачів

У кожного користувача локальної мережі, або ж працівника компанії на його робочому комп'ютері встановлений власний пароль та обліковий запис. Таким чином даний метод захисту інформації дозволяє контролювати кожного користувача мережі, та запобігає несанкціонованому витоку інформації. Розподілення ресурсів локальної мережі дозволяє не тримати конфіденційну інформацію на видному місці та ховає її від небажаного втручання. Розділення ресурсів приймається як на рівні програмного забезпечення персональних комп'ютерів, так і на рівні мережі [5].

2.2.4 Підключення ПЕОМ користувачів до мережі

Локальна мережа повинна бути влаштована так, щоб користувачі або ж робітники компанії, не мали можливості додати зайвий пристрій або комп'ютер до локальних мереж офісів [5].

Налаштування комутаторів у плані безпеки та адресації персональних комп'ютерів в мережах VLAN має бути таким, що:

- одному вузлу і тільки йому, доступний доступ до порту;
- в ситуації, коли системи безпеки порушені, порт автоматично вимикається;
- в поточну конфігурацію статичним шляхом додається MAC адреса пристрою.

2.3 Вимоги до видів забезпечення КС

2.3.1 Вимоги до інформаційного забезпечення

Інформаційне забезпечення системи належить бути необхідним для виконання всіх функцій мережі, гарантувати інформаційну сумісність підсистем із суміжними.

В базі даних системи повинна бути присутня сукупність інформаційних масивів та зберігаємих на хмарному сховищі. Це пов'язано із великими обсягами інформації та з метою нарощування швидкодії роботи, і також з довгими термінами зберігання [5].

В системі повинні бути враховані заходи по контролю і оновлення даних в інформаційних масивах і відновлення масивів при збоях технічних приладів.

В системі зобов'язаний бути врахований швидкий доступ до важливої інформації.

Форми вихідних документів як екранних, так і друкованих на фізичних носіях інформації, зобов'язані виділятися наочністю з метою облегшення перцепції інформації робітників компанії.

ВИСНОВОК

Технічні вимоги, що буди розглянуті і розроблені вище, достатні для побудови локальної обчислювальної мережі головного офісу та інших філіалів ТОВ «М - Систем» і є підставою для побудови і розробки схеми електричної структурної, вибору бази елементів, розробки електричної функціональної схеми і схеми електричної монтажної.

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ КОМПАНІЇ

3.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

Будь-яка компанія робить та формулює вимоги до локальної мережі самостійно. У першу чергу визначається кількість людей, що будуть користуватися саме цією мережею. Відштовхуючись від цього, ми можемо далі проектувати етапи створення локальної обчислювальної мережі.

Кількість вузлів, а саме персональних комп'ютерів, залежить від максимального числа робітників, яка є у планах компанії, стосовно їх наймання. Другим фактором являється ієрархія фірми. Для компаній, що має виражену вертикальну ієрархію, характерно те, що інформацію, доступну керівництву, слід закривати від робітників, виконуючих технічні завдання або роль менеджера. Найкращим рішенням для такої компанії є проектування мережі на основі серверу.

Головний офіс ТОВ «М - Систем» має 112 вузлів, як робочих станцій, так і периферійних пристроїв. 106 вузлів для робочого персоналу у одній мережі, та 6 вузлів для керівництва та бухгалтерії. Поряд з головним офісом знаходиться будівля філіалу №5 з 32-ма вузлами під робочий персонал, тому з'єднання між мережами буде фізичним. У інших трьох офісах знаходиться 168, 241, 172 вузлів відповідно. Всі робочі та периферійні вузли необхідно об'єднати в локальну обчислювальну мережу.

Схема з'єднань обчислювальної мережі ТОВ «М - Систем» зображена на рисунку 3.1. Так як мережа компанії досить велика, та обчислюється дуже великою кількістю вузлів, на рисунку зображено по 3 вузли для кожної підмережі, що існує у компанії.

Одним з найважніших етапів проектування комп'ютерних мереж є створення схеми, що вказана вище. Стосовно від типу локальної

обчислювальної мережі, залежить необхідна довжина кабелю, що буде її з'єднувати. Для невеликих офісів це питання не має такого значення в порівнянні з офісами компаній, що охоплюють два-три поверхи, або будівель. У нашому випадку має сенс встановлення репітерів через те, що як і головний, так і побічні філіали офісів ТОВ «М - Систем» мають декілька поверхів для розташування всіх вузлів мережі.

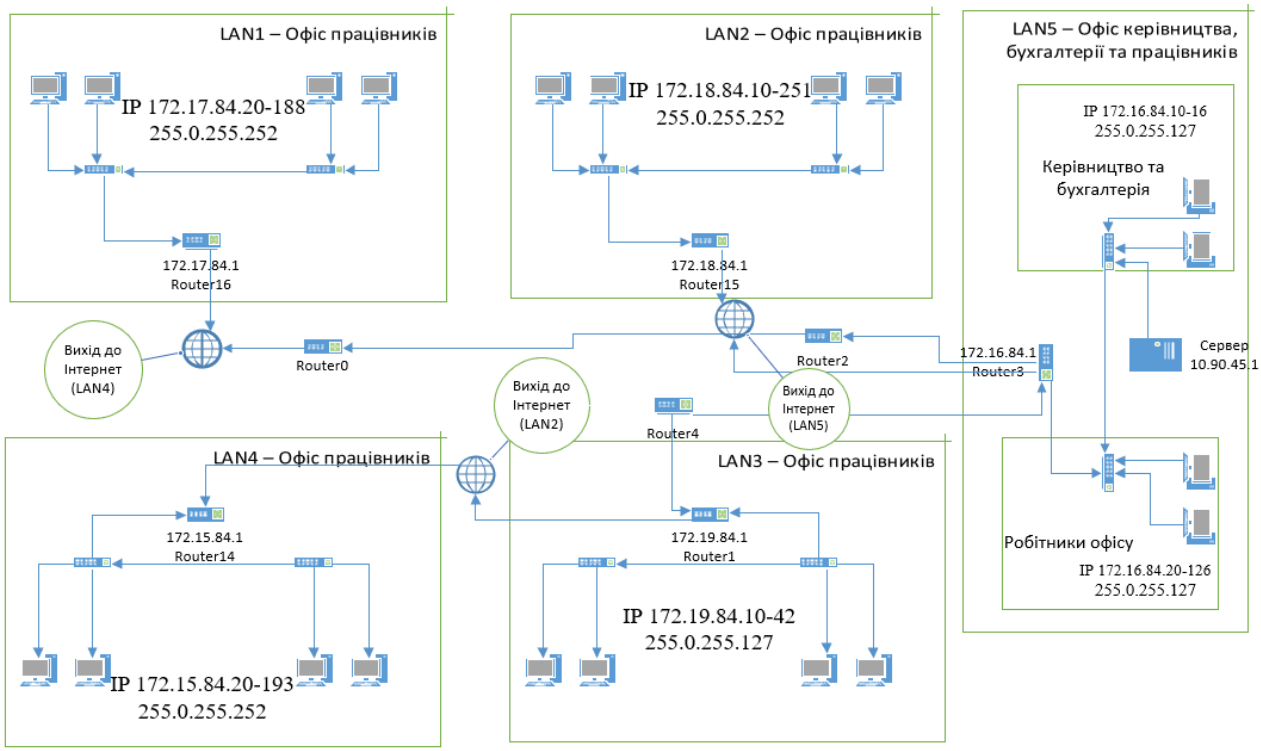


Рис. 3.1 Схема мережі ТОВ «М - Систем»

3.2 Розробка специфікації апаратних засобів КС

3.2.1 Вибір обладнання

Список обладнання, що необхідне для нових робочих місць, наведене в таблиці 1.

Таблиця 3.1 – Обладнання.

Тип обладнання	Підрозділи	Назва пристрою	Кількість	Характеристика
Монітор	Керівництво	Dell SE2416H 24"	2	Тип матриці: IPS Час реакції матриці: 12 мс Яскравість дисплея: 250 кд/м2 Контрастність дисплея: 3000:1 Інтерфейси: DVI, HDMI
	Бухгалтерія	Asus VZ229HE 21.5"	4	Тип матриці: IPS Час реакції матриці: 5 мс Яскравість дисплея: 250 кд/м² Контрастність дисплея: ASCR: 80000000:1 Інтерфейси: VGA, HDMI
	Працівники офісу	Thomson M24FC1240 1 (SRT 001611) 23.8"	118	Тип матриці: IPS Час реакції матриці: 6.5 мс Яскравість дисплея: 250 кд/м2 Контрастність дисплея: 1000:1 Інтерфейси: HDMI, VGA
Персональний комп’ютер	Керівництво	Artline Business Plus B25 v18	2	Intel Pentium Gold G5400 (3.7 ГГц)/ RAM 8 ГБ / SSD 120 ГБ / DVD-Super-Multi / кард-ридер / LAN
	Бухгалтерія	SCORPIO X1 Digitalfury	2	AMD Quad-Core A8-7680 (3.5 - 3.8 ГГц)/ RAM 8 ГБ / HDD 500 ГБ / AMD Radeon Graphics/ DVD+/-RW / LAN / кардрідер /
	Працівники офісу	ARTLINE Business B14 v03	118	Intel Celeron J1900 (2.0 ГГц)/ RAM 8 ГБ / SSD 240 ГБ / DVD-Super-Multi

Тип обладнання	Підрозділи	Назва пристрою	Кількість	Характеристика
Клавіатура	Керівництво	Logitech K120 USB RUS OEM (920-002522)	1	Тип: мембранні, інтерфейс: USB
	Бухгалтерія		2	
	Працівники офісу		118	
Миша	Керівництво	Logitech B100 USB Black (910-003357)	1	Тип датчика: оптичний Інтерфейс: USB Кількість кнопок: 3
	Бухгалтерія		2	
	Працівники офісу		118	
Навушники	Керівництво	Esperanza EH115 Black (EH115)	1	Тип навушників: накладні Діапазон частот: 20 кГц Матеріал корпусу: Пластик
	Бухгалтерія		2	
	Працівники офісу		118	

У якості роутерів, що будуть об’єднувати мережу, виступатимуть MIKROTIK hAP ac (рис. 3.2.), до яких будуть підключені 24-портові комутатори MIKROTIK CRS326-24G-2S+IN з підтримкою 10/100/1000 Мбіт / с. (рис 3.3)

Рисунок 3.2 Wi-Fi роутер MIKROTIK hAP ac

MIKROTIK hAP ac має характеристики, що приведені нижче:

– стандарт: IEEE 802.11a/b/g/n/ac;

– швидкість передачі даних 2,4 ГГц – 300 Мбіт / с, 5 ГГц – 867 Мбіт / с;
– роз’єми: 2 x Gigabit RJ-45 LAN, 1 x Gigabit RJ-45 WAN/LAN;
– діапазон частот: 2,4 ГГц, 5 ГГц;
– безпека: WPA, WPA-PSK, WPA2, WPA2-PSK;
– використання WiFi Mesh системи дозволить усунути області зі слабким сигналом. Пристрої працюють з технологією Wi-Fi Mesh для створення єдиної мережі з одним мережевим ім'ям. MIKROTIK hAP ac забезпечує швидке і стабільне з'єднання зі швидкістю до 1200 Мбіт / с і працює з будь-яким стандартним модемом або маршрутизатором [6].

Рисунок 3.3 Комутатор MIKROTIK CRS326-24G-2S+IN

Завдяки надійності і забезпечення високої якості передачі, 26- портовий перемикач PoE DH-PFS4226-24ET-360 10/100 / 1000Mb / s типу «робочий стіл» є ідеальним рішенням для розширення офісної мережі.

Основні характеристики комутатора MIKROTIK CRS326-24G-2S+IN:

- кількість портів: 26;
- кількість портів PoE: 24;
- кількість портів SFP: 2;
- потужність: 30Вт на канал;
- наявність індикації: є;
- стандарт PoE: IEEE802.3af, IEEE802.3at, Hi-PoE;
- Швидкість передачі пакетів: 6.55 Mpps [7].

3.2.2 Вибір типу кабельного з'єднання

Звита пара. (Рис. 3.4)

Існують наступні види звитої пари:

- UTP (*Unshielded twisted pair*) - захист і екранування відсутні, це найдешевший вид кручений пари і призначений для використання всередині приміщень (звичайно, такий кабель можна використовувати і зовні, але в силу своєї незахищеності довго він не прослужить);
- FTP (*Foiled twisted pair*) -є один загальний екран (для всіх пар) з фольги. Тип більш захищений, ніж UTP;
- STP (*Shielded twisted pair*) - екранована звита пара, присутній один екран для кожної пари;
- S / FTP (*Shielded Foiled twisted pair*) - майже те ж, що і FTP, але присутній додатковий зовнішній екран з мідного обплетення;
- S / STP (*Screened shielded twisted pair*) - схожий на STP, але присутній додатковий загальний зовнішній екран;
- U / STP (*Unshielded Screened twisted pair* - незахищений кабель з екрануванням кручений пари) - кабель не має загального екрану, але кожна пара має фольгований захист;
- SF / UTP або SFTP (*Screened Foiled Unshielded twisted pair* - звитапара із захистом) - має два зовнішніх екрану. Один з мідної сітки, а другий з екрану-фольги. Між ними дренажний дрот [8] [9].

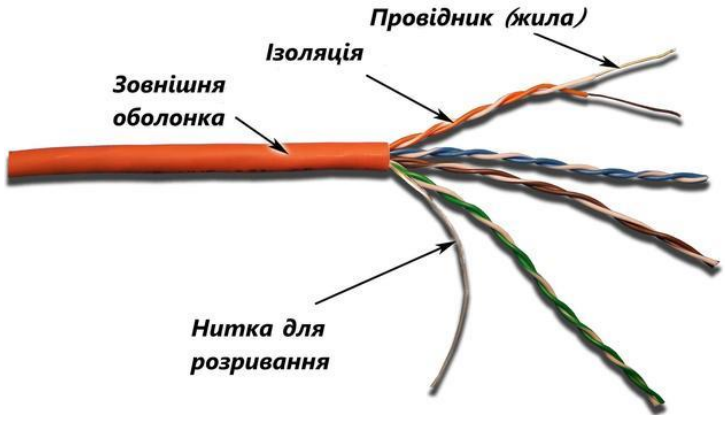


Рисунок 3.4 «Звита пара»

Типи звитої пари наведені в міру зростання і вартості. Для зовнішнього використання рекомендується STP. Хоча якщо дозволяють кошти, то можна купити і S / STP.

За способом прокладки зовнішньої кручений пари:

- без несучої сталевого дроту;
- з несучим сталевим дротом

За кількістю жил в кабелі:

- з 2-ма парами провідників;
- з 4-ма парами провідників.

За способом виконання:

- з екрануванням (*FTP*) - для захисту кручений пари від зовнішнього електромагнітного поля;
- без екранування (*UTP*).

За матеріалом виготовлення:

- мідь;
- біметал.

Категорії звитої пари

Існують різні категорії звитої пари. Чим вище категорія, тим кабель більш якісний і дорогий. Вита пара 1-4 категорії вже не застосовується для побудови мереж. Для побудови сучасних Ethernet-мереж використовують кручену пару з 5 - 7 категорії. П'ята категорія це 4-парний кабель (4 пари жил) і служить для побудови мереж 100Base-TX. У цих мережах задіяні всього 2 пари (4 дроти), при цьому досягається швидкість передачі даних до 100 Мбіт / с. При покупці кабелю варто звернути увагу на написи на зовнішній оболонці-краще купити CAT5E, ніж просто CAT5, модернізована версія може використовуватися для побудови мереж Gigabit Ethernet. Для передачі даних зі швидкістю 1000 Мбіт / с використовуються всі 4 пари.

У цьому дипломному проекті для з'єднання вузлів мережі, най оптимальнішим варіантом буде використано кабель «звита пара» типу CAT5

Необхідна довжина кабелю, що буде задіяна у міжмережжі та для з’єднання робочих станцій, периферійних пристроїв, складатиме:

Робочі станції на поверсі, всі розрахунки відстані між мережами ідентичні:

7м*12пк+5м*8пк+8м*5пк+10м*12пк+12м*2пк+13м*1пк+14м*5пк+15м*3пк+18м*4пк= 508 метрів кабелю типу «звита пара» знадобиться для зв’язана всіх вузлів у мережі.

Міжмережеве з’єднання:

2м+6м+10м = 18 метрів кабелю типу «звита пара» знадобиться для зв’язання всіх комутаторів з роутерами.

508м+18м = 526 метрів кабелю у спільному.

3.3 Розробка архітектури мережі компанії

Для того, щоб зробити висновки та зрозуміти, яка оптимальна архітектура підходить до мережі більш за все, було проаналізовано всі існуючі типи топологій, але найбільш популярною виявилася наступна:

Топологія «зірка» (*Star*)

Між комп'ютерами немає прямих з'єднань. Замість цього вони всі об'єднані один з одним через концентратор (або хаб), кожен - за допомогою свого кабелю. (рис. 3.5)

Концентратор (англ. *Hub*) – розвітляючий пристрій, що служить центральною ланкою в локальних мережах, що мають топологію "зірка". Концентратор має кілька портів для підключення окремих комп'ютерів і для з'єднання з іншими хабами.

Пакети даних передаються від кожного вузла концентратора, який в свою чергу пересилає пакети адресату. Концентратор зазвичай забезпечує з'єднання від 5 до 48 входів, що визначає число комп'ютерів, які можна до нього підключити. Залежно від числа з'єднуваних комп'ютерів може знадобитися кілька концентраторів.

Переваги:

– найбільш швидкодіюча з усіх топологій, оскільки передача даних між робочими станціями відбувається через центральний вузол по окремих лініях, використовуваним тільки цими робочими станціями;
– порушення з'єднання між будь-яким комп'ютером і концентратором не впливає на інші вузли мережі, так як кожен з них має власне з'єднання з концентратором;
– функціонування мережі не залежить від стану окремої робочої станції, тому PC в будь-який час, без переривання роботи всієї мережі, можуть бути відключені або підключені до неї [10].

Недоліки:

– високі витрати на прокладку кабелів (витрачається більше кабелю, чим при шинної топології), особливо коли концентратор географічно розташований не в центрі. Концентратор також є додатковою статтю витрат;
– у разі виходу з ладу концентратора порушується робота всієї мережі [11] [12].

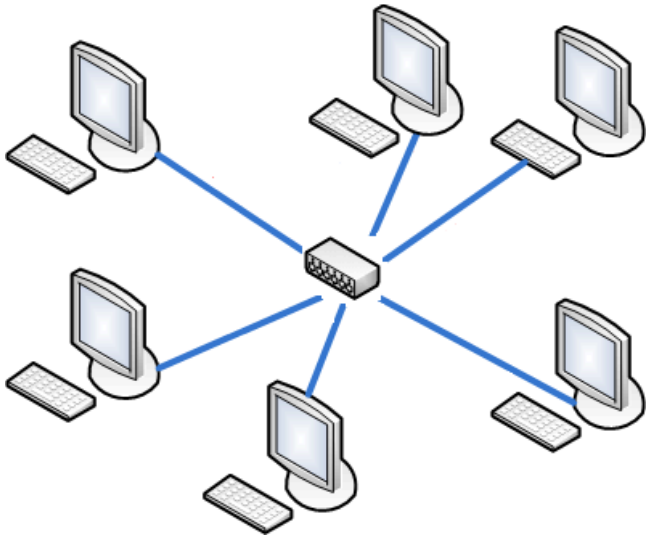


Рисунок 3.5 Топологія «Зірка»

У даному проекті буде використовуватися топологія типу «Зірка», так як проаналізувавши всі переваги та недоліки, дана топологія відрізняється своєю надійністю у разі виходу з ладу однієї з кінцевих станцій, та з економічної

точки зору потребує менше фінансових затрат. Більш за все відрізняється її поширення у офісних мережах, як топологія, що добре себе зарекомендувала.

Топологія типу «зірка» також найкраще підходить для відносно невеликих офісних мереж, як раз такої, що і розроблена у даному проекті.

На рисунку 3.6 зображена схема розміщення робочих станцій у офісній будівлі, та схема з'єднання цих станцій з комутаторами. Червоними лініями позначені патч-корди, що з'єднують кінцеві вузли з 24-портовими комутаторами.

У свою чергу, зелена лінія вказує на розташування кабелю, що з'єднує як комутатори у одну мережу, так і роутер, який являється виходом до наступного рівня мережі (між мережевий рівень у компанії).

Всі патч-корди вмонтовані у спеціальні магістралі за фальш-стелею. Завдяки цьому рішенню, доступ до кабелів можна отримати, підставив драбину та відштовхнувши секцію фальш-стелі. Електричні магістралі розташовані так, щоб не перешкоджати роботі звитої пари, у перетинах з ними проходять перпендикулярно.

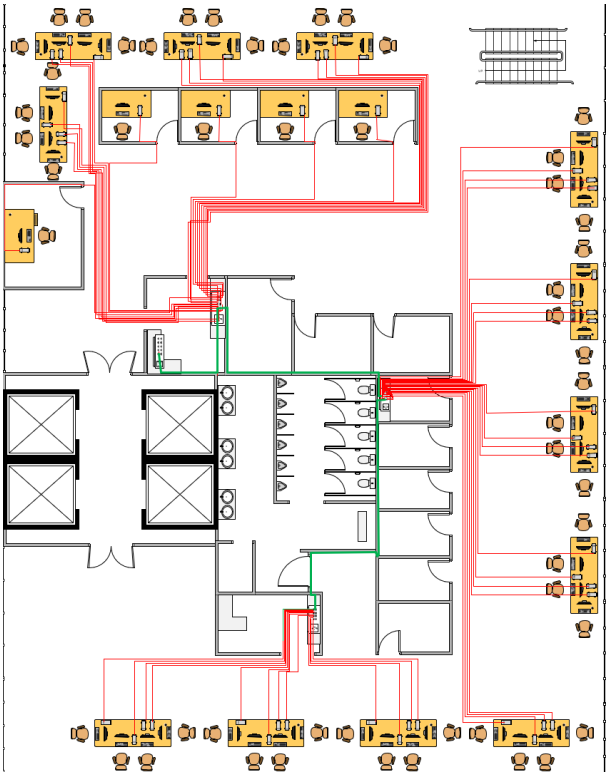


Рисунок 3.6 – Схема розташування обладнання у мережі

Досить важливою характеристикою під час обміну пакетами або інформації в локальній обчислювальній мережі є методи доступу. Вони створюють правила щодо порядку доступу кінцевих вузлів до ресурсів мережі.

Основний недолік мереж Ethernet обумовлений методом доступу до середовища передачі: При наявності в мережі великої кількості одночасно з'єднаних станцій зростає кількість колізій, а пропускна здатність мережі падає. В екстремальних випадках швидкість передачі в мережі може впасти до нуля. Але навіть в мережі, де середнє навантаження не перевищує максимально допустиму рекомендовану (30-40% від загальної смуги пропускання), швидкість передачі становить 70-80% від номінальної. В деякій мірі цей недолік може бути усунутий застосуванням комутаторів (*switch*) замість концентраторів (Hub). При цьому трафік між портами, приймає мережеві адаптери та ізолюється від інших портів і адаптерів.

Вельми істотною перевагою різних варіантів Ethernet є зворотна сумісність, яка дозволяє використовувати їх спільно в одній мережі, в ряді випадків навіть не змінюючи існуючу кабельну систему.

Мережа, побудована із застосуванням кабелю на основі витої пари - найпоширеніший тип мережі. Сталося це завдяки її легкої розширюваності і достатньому запасу продуктивності. Використовуючи кабель п'ятої категорії, можна добитися швидкості передачі даних в 100 Мбіт / с, чого цілком вистачає для виконання більшості завдань. Мало того, якщо дотримуватися стандартів обтиску кабелю, то можна в подальшому використовувати цей ж кабель для модернізації мережі до рівня Gigabit Ethernet.

Також, досить важливим аспектом у мережі є спільний доступ до мережевих ресурсів (модеми, принтери, факс та ін.).

Ресурси, перераховані вище, можуть застосовуватися як в мережах з сервером, так і в одноранговых. В разі з одноранговою мережею, можна взяти у увагу декілька недоліків:

- Для того, щоб працювати з ресурсами, їх необхідно встановлювати на робочу станцію або додавати до неї периферійні пристрої.

- У разі відключення станції, всі ресурси і служби стають недоступними для спільного застосування.

У разі ж мережі з виділеним сервером, така станція існує завжди, якщо не брати до уваги не тривалі зупинки для обслуговування. Даним способом забезпечується постійний доступ до мережевої периферії для клієнтів мережі.

Таким чином, одразу відпадає питання про підключення, наприклад, принтерів або сканерів до локальної обчислювальної мережі.

Але, так як у цієї мережі не буде виділеного серверу під принтери та інші периферійні пристрої, підключати їх будемо до звичайних робочих станцій. Для забезпечення безперебійності їх роботи, достатньо не вимикати ці станції.

3.4 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі компанії

Для більш простого розуміння та для прискорення розрахунків, зазвичай дані щодо затримок поширення сигналів в повторювачів, беруть з довідкових даних IEEE. Таблиця 2 та 3 має дані, що потребуються для розрахунків PDV (Path Delay Value – подвійний оборот сигналу) для фізичних стандартів Ethernet. bt позначено як бітовий інтервал. Для того щоб не було необхідності в подвійних складаннях затримки, що спричиняє кабель, у таблицях одразу заносяться подвійні величини затримок (bt*2).

У таблицях також задіються такі визначення, як правий, лівий та проміжні сегменти. Лівим сегментом являється початок дороги сигналу від виходу передавача. Після цього сигнал здійснює дорогу через проміжний сегмент і доходить у приймач. Має увагу те, що правий сегмент приводиться завжди найбільш видаленим вузлом найбільш видаленого сегменту.

Таблиця 3.2 Затримка кабеля для розрахунків PDV

Тип кабеля	bt*2 на 1 м.	Максимальна довжина сегмента, м
UTP Cat 3	1,14	
UTP Cat 4	1,14	
UTP Cat 5	1,112	18
STP	1,112	
Оптоволоконний кабель	1,0	

Таблиця 3.3 Затримка адаптерів для розрахунку значення PDV.

Тип комутатору	Подвійна затримка bt.
комутатор TX/FX	100
комутатор T4	135

Розрахування затримок полягає в їх обчисленні, що заносяться кожним сегментом кабелю та затримок на проміжних вузлах, що встановлені на дорозі проходу сигналу, після цього їх підсумовування. У таблиці 2 наведена затримка сигналу на одному метрі кабелю та яка умножається на довжину поточного сегмента. Значення PDV не повинне бути вище 575 [13].

Найбільшим по довжині є сегмент від однієї з робочих станцій до іншої станції на різних поверхах офісу. Схема сегменту вказана на рисунку 3.7.

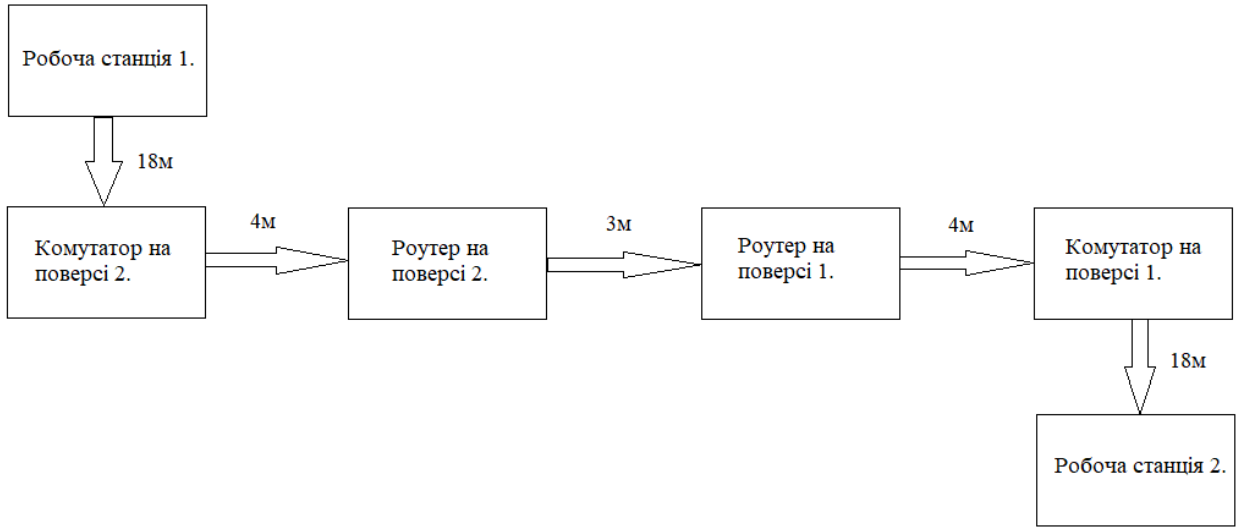


Рисунок 3.7 Найдовший сегмент проектованої мережі

Розраховуємо значення PDV:

PDV= 1,112*18+135+1,112*4+100+100+135+18*1,112=514,48

Сумарне значення PDV є 510,48, що є гранично допустимим значенням, так як 514,48<575.

Розрахунок значення PVV

Для того щоб конфігурація мережі була виправдано коректна, необхідно визначити значення зменшення міжкадрового інтервалу репітерами, тобто значення PVV.

Значення PVV не повинно перевищувати 49 бітових інтервалів. Вихідні дані для розрахунку PVV були взяті з затверджених стандартів, рекомендованими IEEE, і наведені в таблиці 4 [14].

Таблиця 3.4 - Скорочення міжкадрового інтервалу повторювачами.

Тип сегмента	Передавальний сегмент	Проміжний сегмент
100 Base TX	10,5	8
100 Base T4	10,5	8
1000 Base T	10,5	8

Відповідно до цих даних розрахуємо значення PVV:

Лівий сегмент: має скорочення 10,5 бітових інтервалів;

Проміжний сегмент 1: 8 бітових інтервалів;

Проміжний сегмент 2: 8 бітових інтервалів;

Проміжний сегмент 3; 8 бітових інтервалів;

Правий сегмент: 10,5 бітових інтервалів.

PVV=10,5+8+8+8+10,5=45.

Значення PVV у найбільшому сегменті проектованої мережі дорівнює 45, що менше 49 допустимих бітових інтервалів. Мережа відповідає визначеному стандарту Ethernet.

4 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ КОМПАНІЇ

4.1 Розрахунок схеми адресації корпоративної мережі

Для того, щоб кожен мережевий пристрій і персональний комп'ютер працювали, кожному з цих вузлів необхідно надати унікальну IP адресу

Проектована мережа має 5 підмереж.

1) Мережа 172.16.84.0/24;
2) Мережа 172.17.84.0/24;
3) Мережа 172.18.84.0/24;
4) Мережа 172.19.84.0/24;
5) Мережа 172.20.84.0/24;

IP адреси керівництва та бухгалтерії розташовані у одній підмережі головного офісу разом з робочими станціями інших працівників офісу, та мають наступні унікальні адреси:

- Генеральний директор: 172.16.84.10;

Замісник директору: 172.16.84.11;

- Бухгалтерія має 4 робочих станції, яким визначений наступний діапазон адрес: 172.16.84.12-16;
- До іншої частини підмережі відносяться працівники офісу, які мають наступний діапазон: 172.16.84.20-126/255.255.255.127

До інших 4-х підмереж відносяться тільки працівники офісів, відповідно діапазон IP адрес для LAN1,LAN2,LAN3,LAN4:

- LAN1: 172.17.84.20-188/255.255.255.252;
- LAN2: 172.18.84.10-251/255.255.255.252;
- LAN3: 172.19.84.10-42/255.255.255.127;
- LAN4: 172.15.84.20-193/255.255.255.252.

Таблиця 4.1 – Схема адресації.

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Діапазон можливих адрес вузлів у підмережі
LAN1	168	172.17.84.0	255.255.255.252	172.17.84.1-188
LAN2	241	172.18.84.0	255.255.255.252	172.18.84.1-251
LAN3	32	172.19.84.0	255.255.255.127	172.19.84.1-42
LAN4	173	172.15.84.0	255.255.255.252	172.15.84.1-193
LAN5	112	172.16.84.0	255.255.255.127	172.16.84.1-126

4.2 Розробка топологічної схеми корпоративної мережі

Моделювання мережі компанії буде здійснюватися в середовищі Cisco Packet Tracer.

Cisco Packet Tracer – це емулятор для моделювання віртуальних мереж. Має не всі доступні для моделювання мереж функції, але якщо подивитися з іншого боку, до цього часу підтримує моделювання та створення GRE-тунелів, динамічну маршрутизацію - BGP. У той же час він досить простий в освоєнні. Має можливість налаштування серверів FTP, TFTP, DHCP, DNS, HTTP, NTP, RADIUS, SMTP, POP3, і багатьох типів кінцевих вузлів (принтери, факси, персональні комп'ютери).

Спочатку необхідно побудувати мережу компанії. У приклад буде поставлена підмережа, де буде значитися бухгалтерія і керівництво. Так-же в даній підмережі присутні робочі станції співробітників компанії.

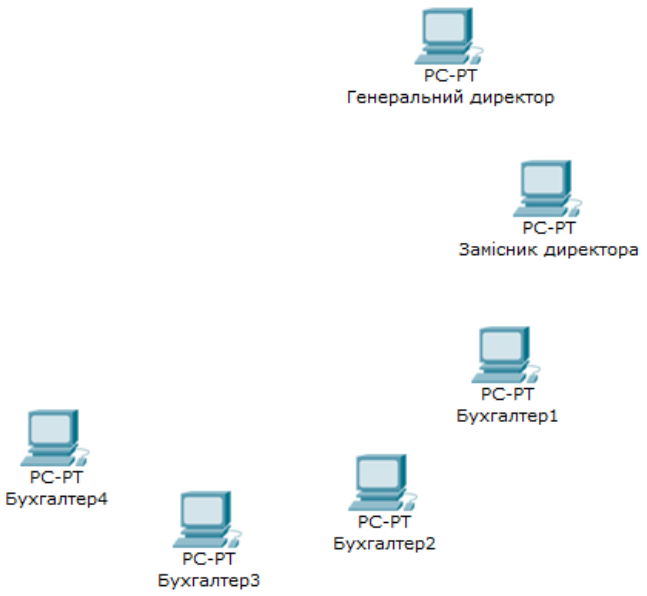


Рисунок 4.1. – Розташування робочих станцій керівництва і бухгалтерії

Після розміщення необхідних вузлів мережі, необхідно встановити маршрутизатор, який буде відповідати за транзит пакетів всередині підмережі, між її вузлами

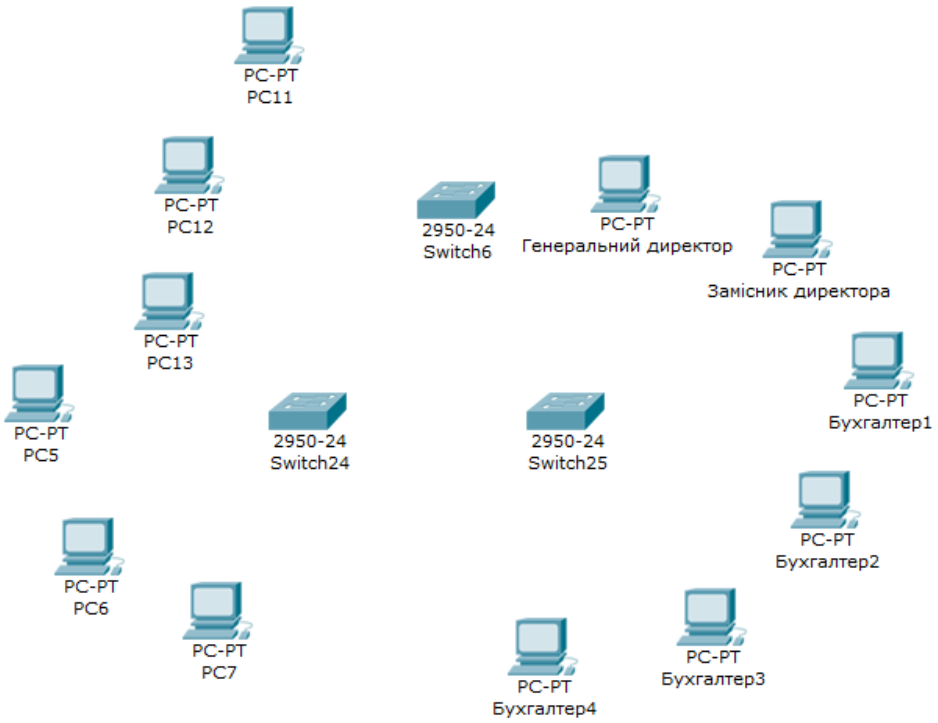


Рисунок 4.2. – Встановлення необхідної кількості маршрутизаторів та інших вузлів підмережі

Таким самим чином були розміщені і інші підмережі, які з'єдналися необхідним для них типом з'єднання. Для кожної підмережі існує свій вихід в Інтернет.

Для мережі головного офісу з бухгалтерією і керівництвом - Router 2.

Для LAN2 - Router 14.

LAN3 - Router1, інтернет до якого маршрутизован з Router 2 з підмережі головного офісу.

LAN4 – Router 16, LAN1 - Router 15.

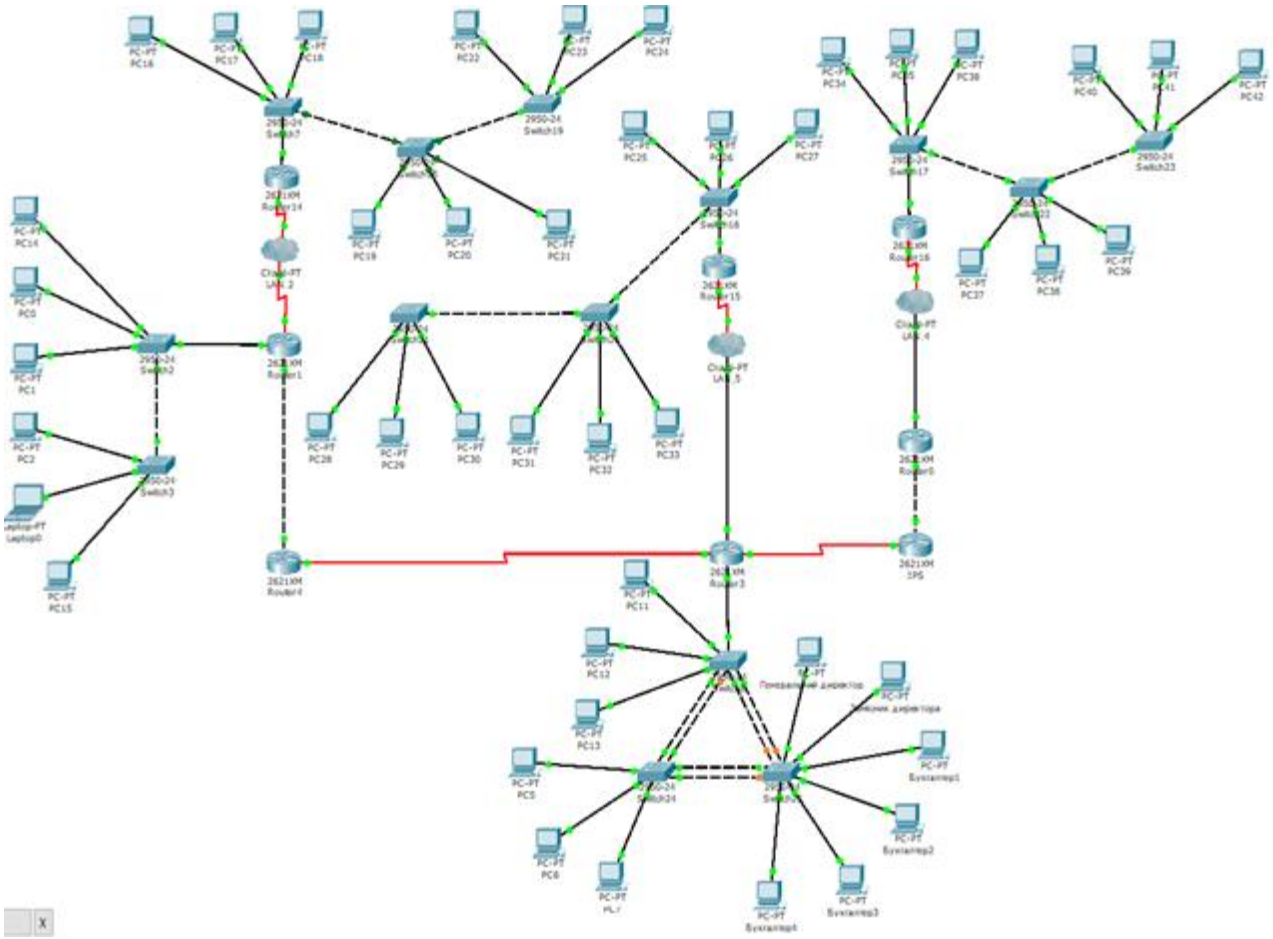


Рисунок 4.3 ¬ Детальна схема проекту мережі ТОВ «М - Систем»

4.3 Розробка топологічної схеми корпоративної мережі

4.3.1 Базове налаштування конфігурації пристроїв

Як і пояснювалося вище, до кожної робочої станції і навіть проміжного вузла, підв'язується свою унікальну IP адресу.

Щоб привласнити його, необхідно зайти у вікно "Desktop", налаштувань пристрою, як зображено на рисунку 4.4.

Рисунок 4.4 – Вкладка «Desktop»

Та перейти до пункту «*IP Configuration*» (Рис. 4.5)

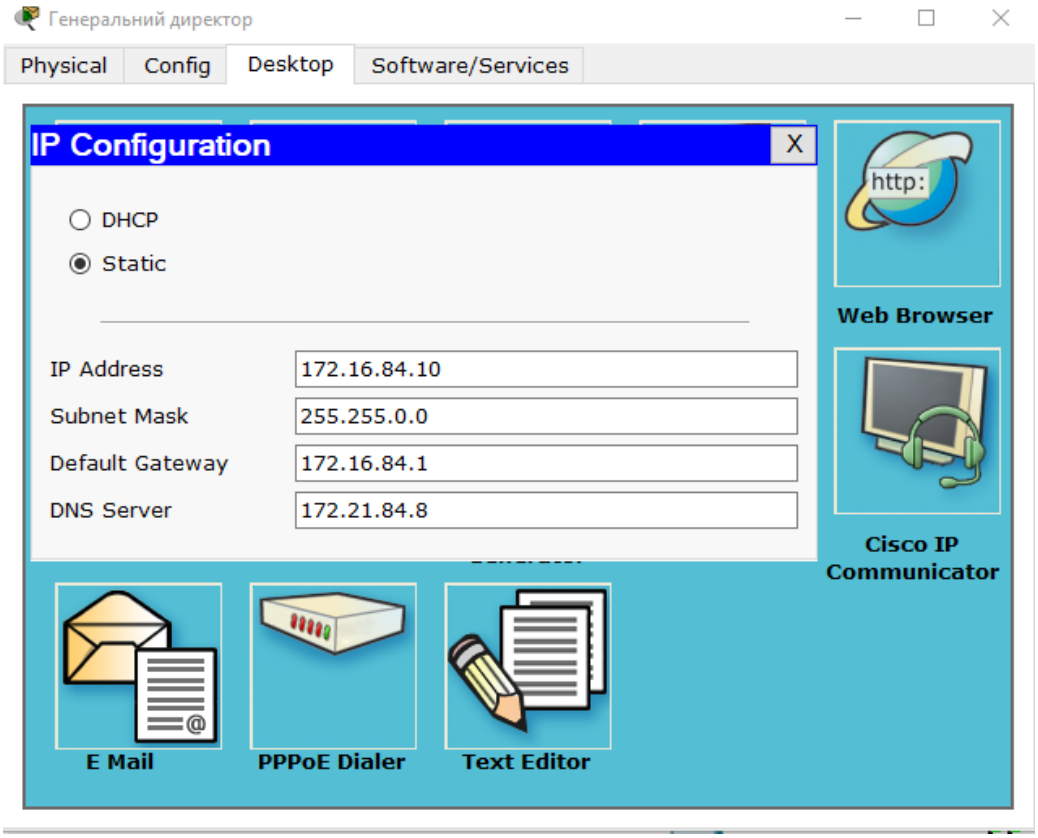


Рисунок 4.5 – «IP Configuration»

У даному вікні нам необхідно вказати IP адресу.

У «*Default Gateway*» ми вписуємо IP адресу роутера, який знаходиться на виході з цієї підмережі. У випадку з мережею, де працюють керівники та бухгалтерія, ця адреса - 172.16.84.1

Такі ж самі дії ми повторюємо для всіх вузлів мережі, вказуючи їй IP адресу, що буде відповідати поточній підмережі.

4.3.2 Налаштування маршрутизаторів корпоративної мережі

В емуляторі Packet Tracer налаштовувати обладнання можна двома способами:

- Графічне представлення (*GUI*);
- Консольне управління (*CLI*).

У ряді деяких недоліків графічного представлення (*GUI*), для більш гнучкого налаштування роутерів, тієї ж маршрутизації між підмережами, використовується консоль (*CLI*).

У командному поданні існує кілька режимів управління, і в залежності від кожного, існує свій набір команд. На малюнку 4.6 зображений набір команд для звичайного, або стандартного режиму.

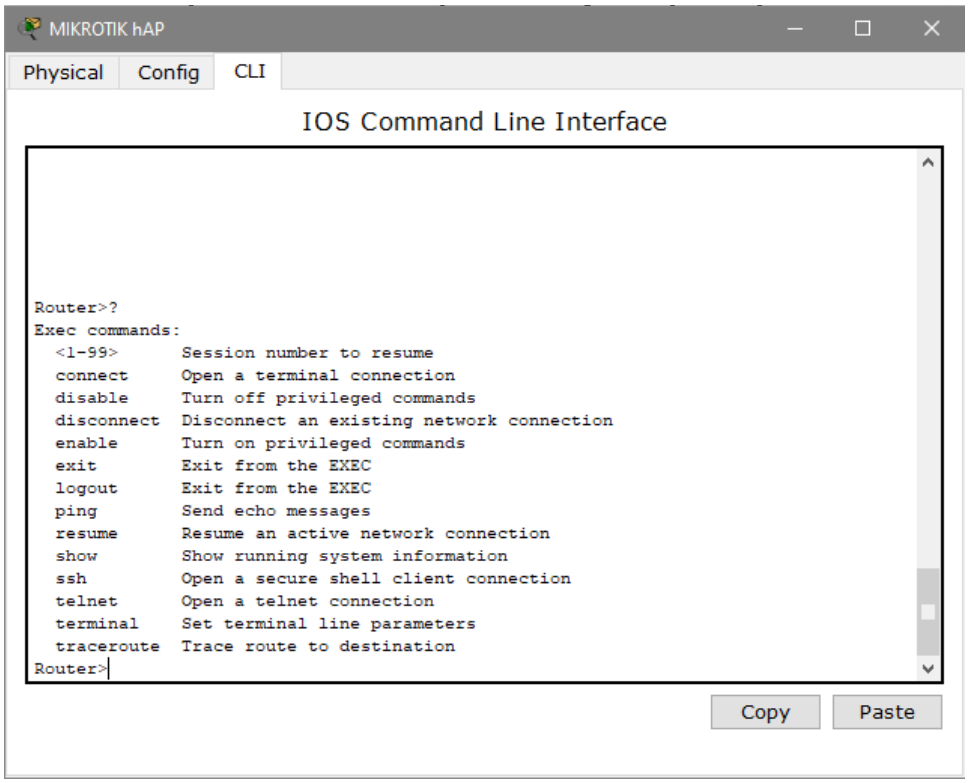


Рисунок 4.6 – Набір команд для стандартного режиму у роутері

Для того, щоб потрапити у режим з привілеями, необхідно, знаходившись у стандартному режимі, ввести команду «enable». (Рис. 4.7.)

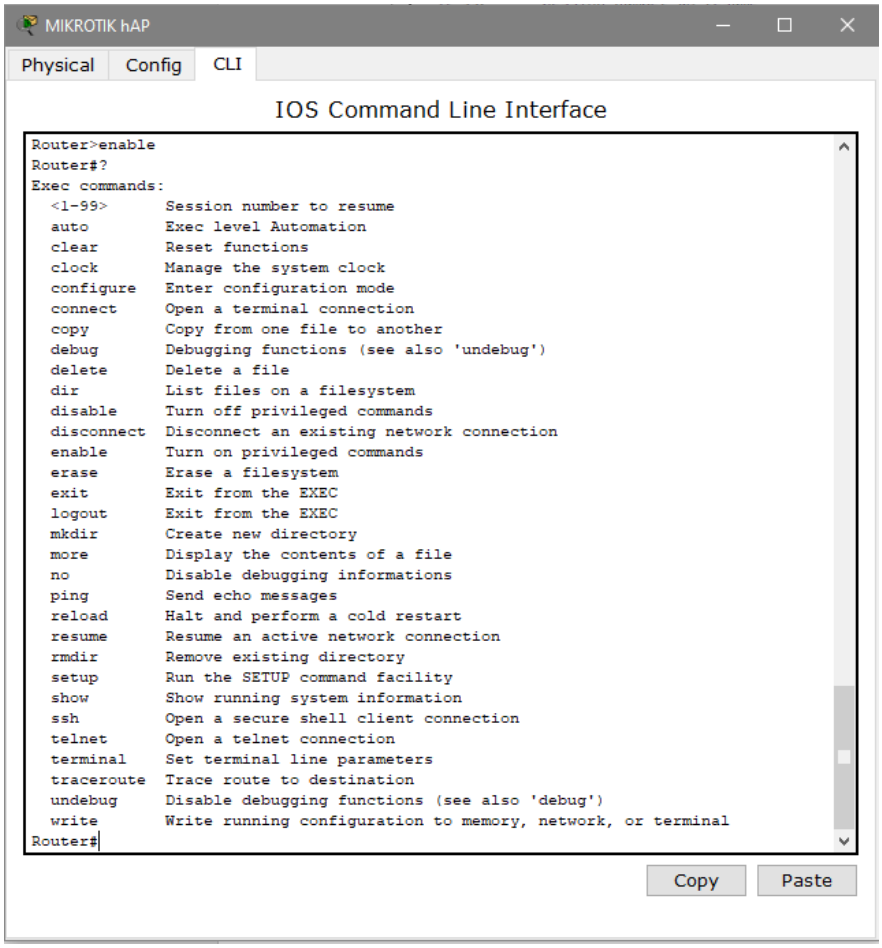


Рисунок 4.7 – Всі команди привілейованого режиму

Щоб роутер повноцінно працював в мережі, необхідно призначити йому IP адресу для порту, який виходить в під мережу (fa 0/1) і потім призначити IP адресу для порту, який повинен бути спрямований у бік виходу в Інтернет (fa 0/0). Налаштування IP адреси для портів роутерів, вказане на рисунку 4.8.

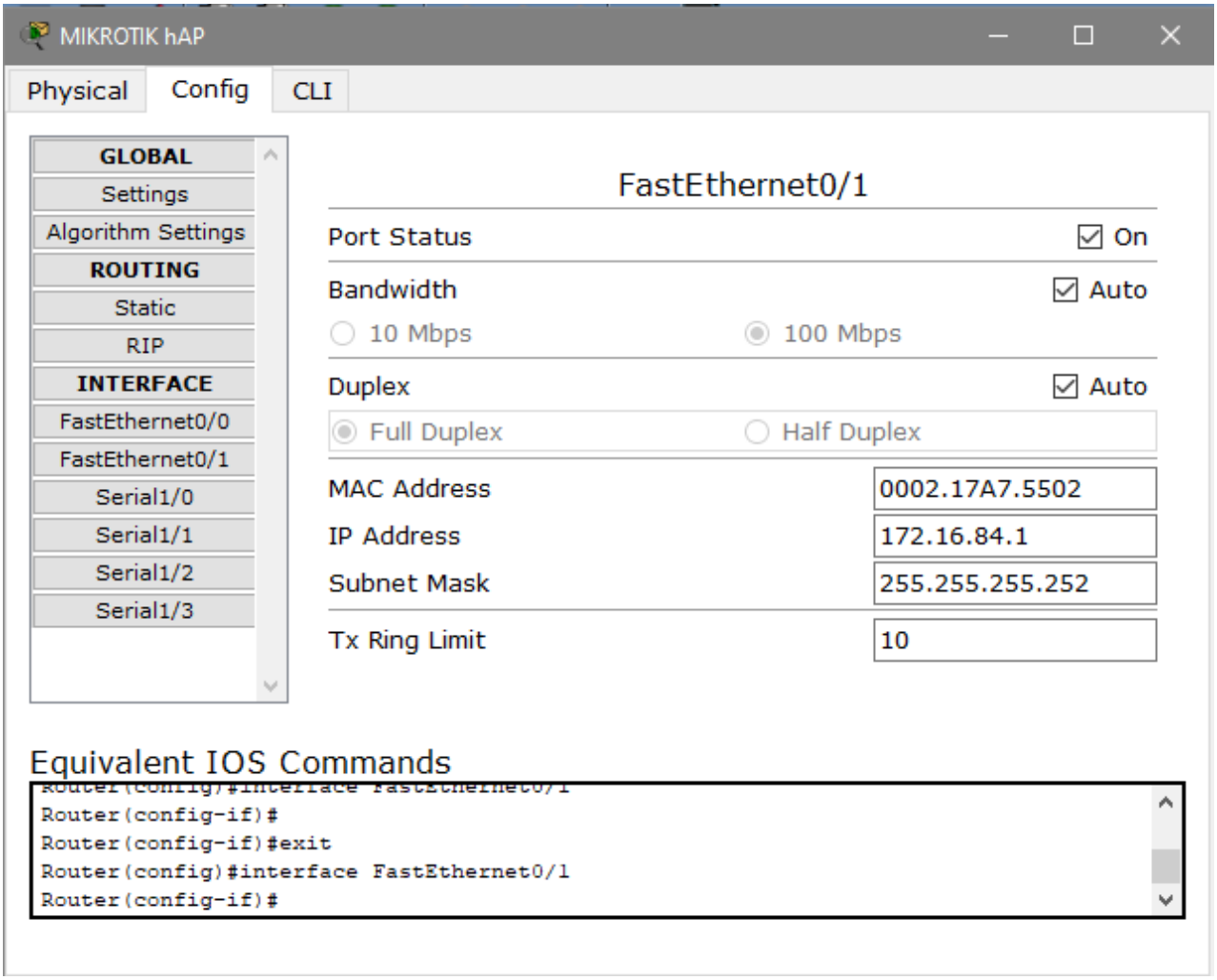


Рисунок 4.8 – Налаштування IP адреси для порту Fast Ethernet

Для порту, який виходить в підмережа, ми призначимо IP адреса 172.16.84.1

Для другого порту, що дивиться в бік виходу в Інтернет, ми призначимо IP 108.177.16.10

Для інших підмереж IP адреса для порту, що виходить в мережу Інтернет, залишається тим же самим. Єдина відмінність буде для портів, які виходять в підмережі. Їм ми присвоюємо відповідні підмережам IP адреси.

4.3.3 Налаштування роботи Інтернет

Щоб налаштувати роботу Інтернет у всіх підмережах компанії, на схемі необхідно встановити і підключити сервер, для подальшого його налаштування. Сервер, в свою чергу, слугуватиме в якості WEB постачальника і хмарного сховища, до якого необхідно провести маршрут від робочих станцій. Завершена топологічна схема вказана на рисунку 4.9.

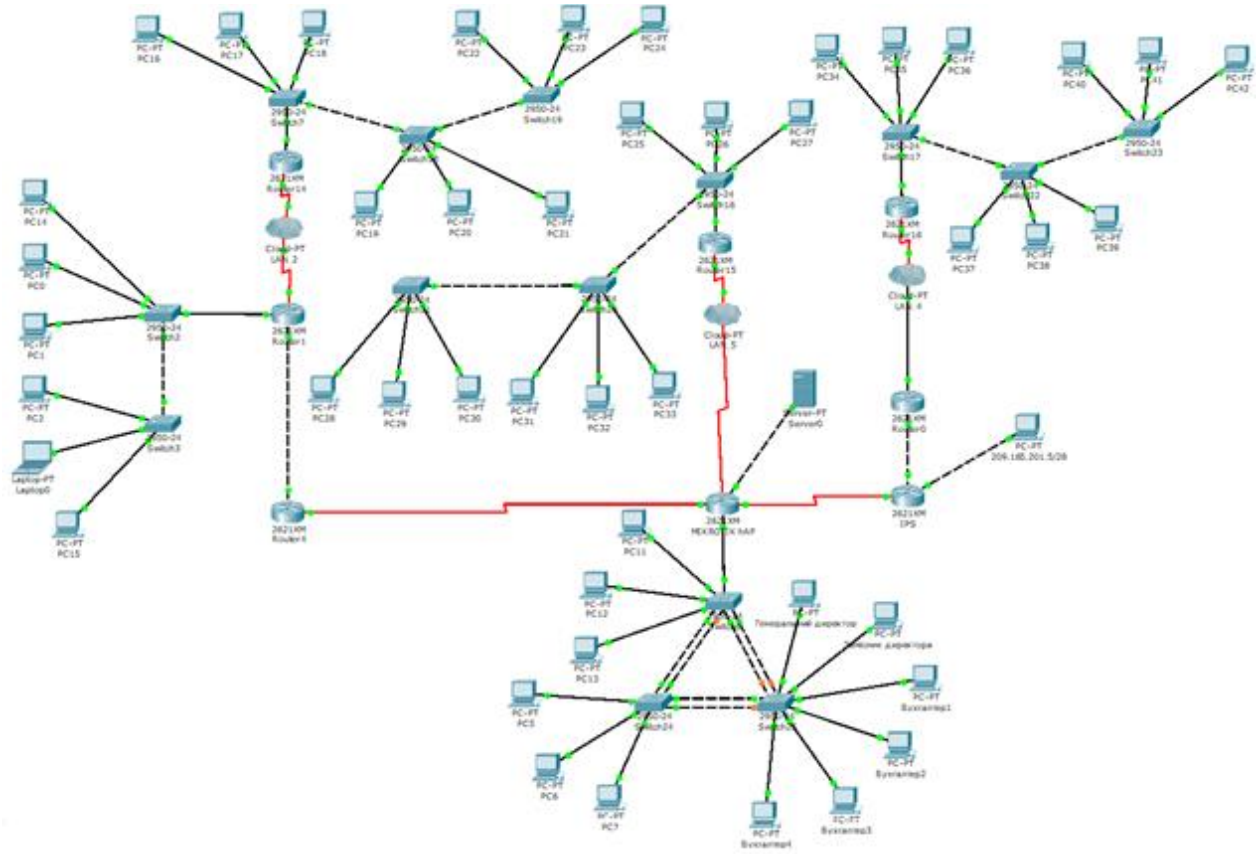


Рисунок 4.9 – Топологічна схема мережі що з’єднана з сервером

Щоб налаштувати сервер, необхідно увійти на вкладку "*Config*" і задати зовнішній IP адреса (рис.4.10), який в разі реальної фізичної мережі, задається самим провайдером.

У разі нашого налаштування, задаємо йому IP 10.90.45.1

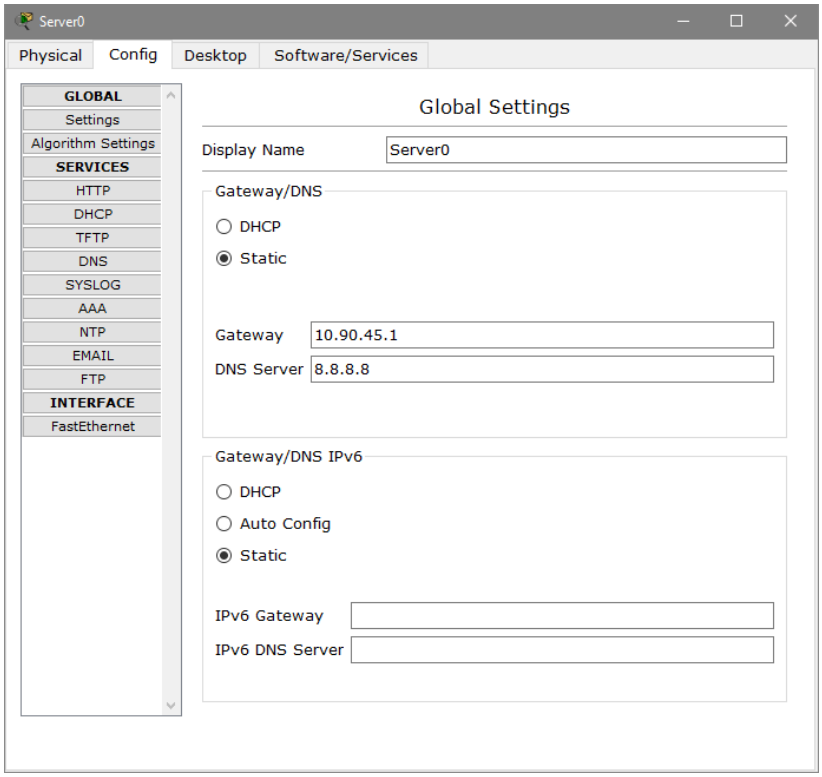


Рисунок 4.10 – Призначення IP для сервера

Також необхідним кроком є створення web-ресурсу на сервері. Для його створення, існує вкладка "*Config*", в якій необхідно перейти на сторінку "*DNS*". В даному пункті ми вказуємо назву сайту (доменне ім'я), за яким надалі можна буде шукати його, не вписуючи адресу сервера. (Рис. 4.11)

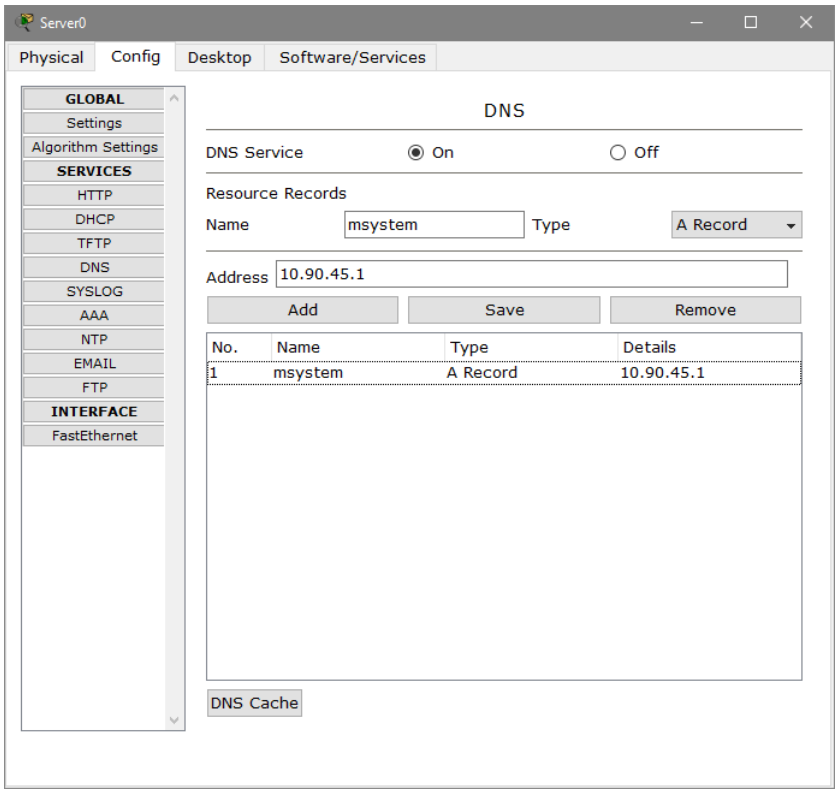


Рисунок 4.11 – Додавання web-ресурсу

4.3.4 Перевірка роботи комп’ютерної системи

Щоб перевірити працездатність комп'ютерної мережі, зайдемо в емулятор командного рядка на потрібних нам робочих станціях.

Запуск командного рядка здійснюється заходом у вкладку "*Desktop*", далі переходом в значок "*Command Prompt*". (Рис. 4.12)

Рисунок 4.12 – Вкладка «Desktop» на робочій станції

Далі прописуємо в командному рядку команду "*ping*", після чого вказати IP адресу, до якої буде перевірятися пересилання пакетів.

Після перевірки зв'язку між усіма робочими станціями, був отриманий результат. Нижче, на рисунках 4.13 - 4.16 показані результати перевірки пересилань пакетів між різними підмережами. Обрані були тільки найнеобхідніші робочі станції, так як в мережі присутня велика кількість кінцевих вузлів.

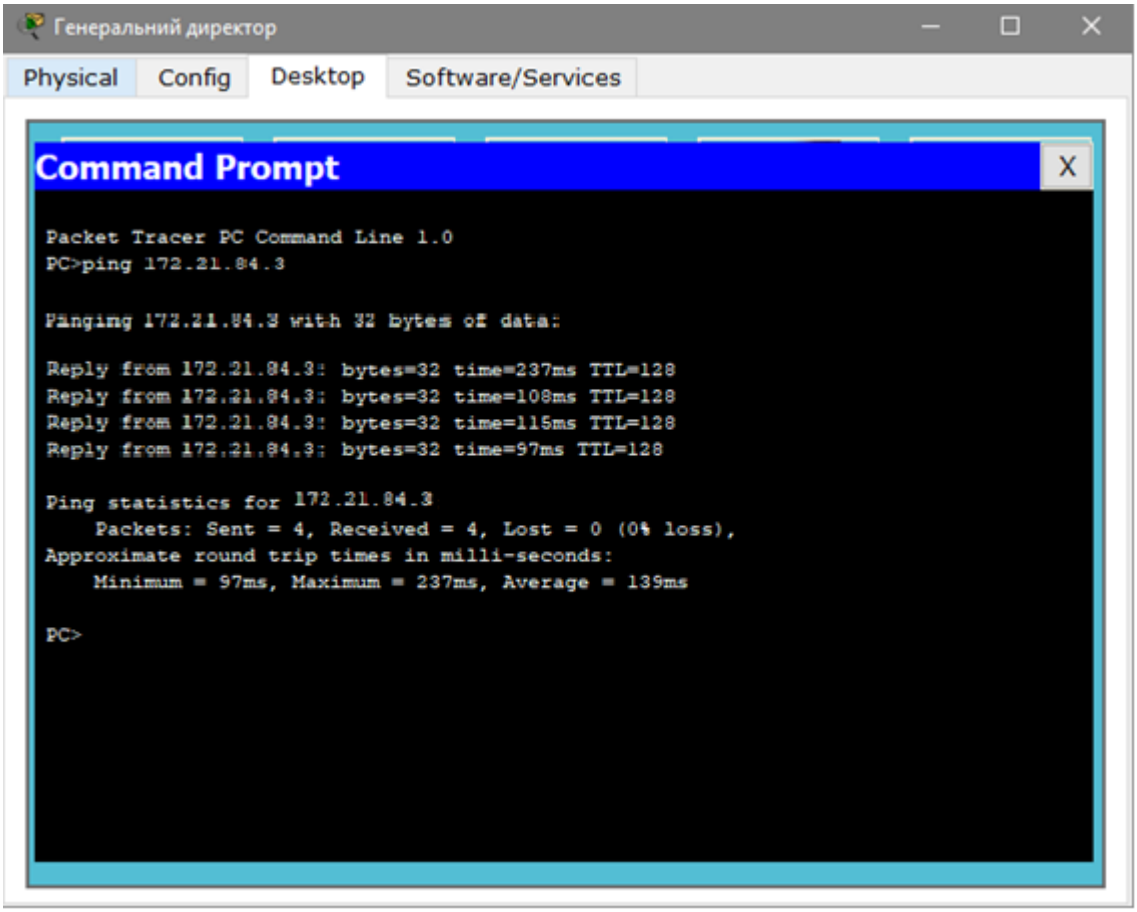


Рисунок 4.13 – Перевірка робочої станції генерального директора на доступність для передачі пакетів між підмережами

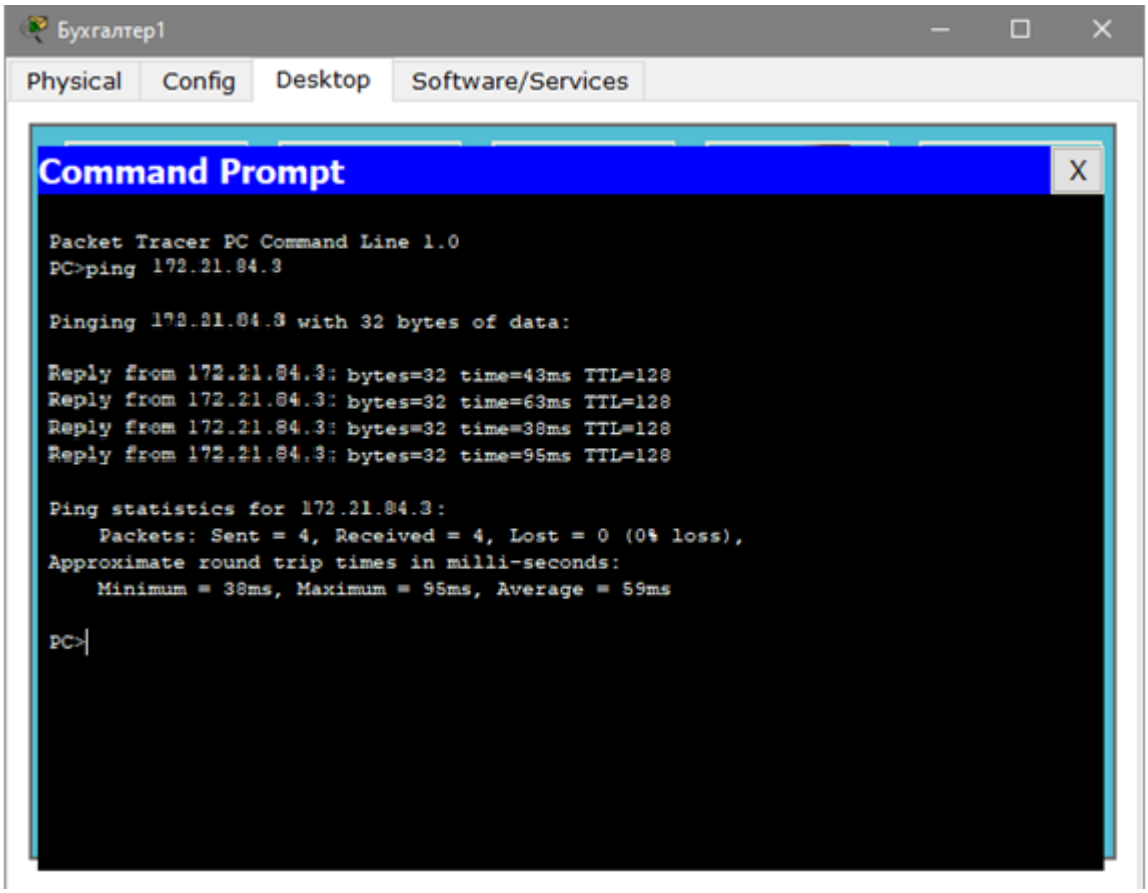


Рисунок 4.14 – Перевірка робочої станції бухгалтера

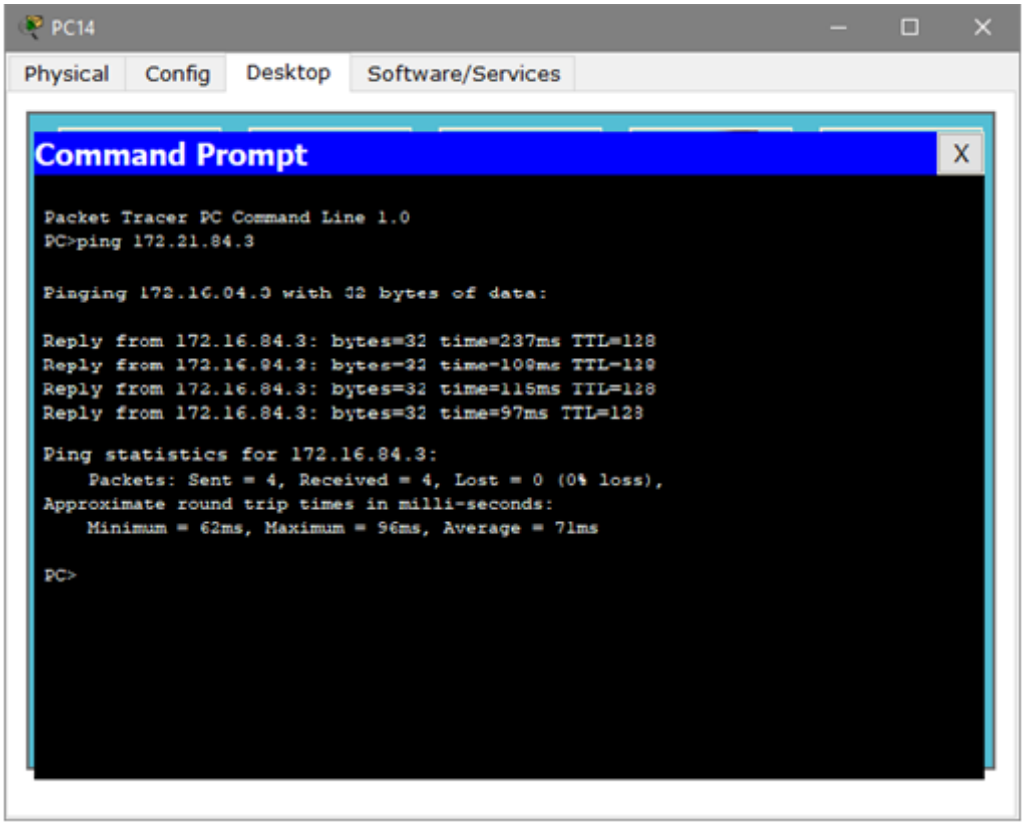


Рисунок 4.15 – Перевірка віддаленої робочої станції працівника офісу

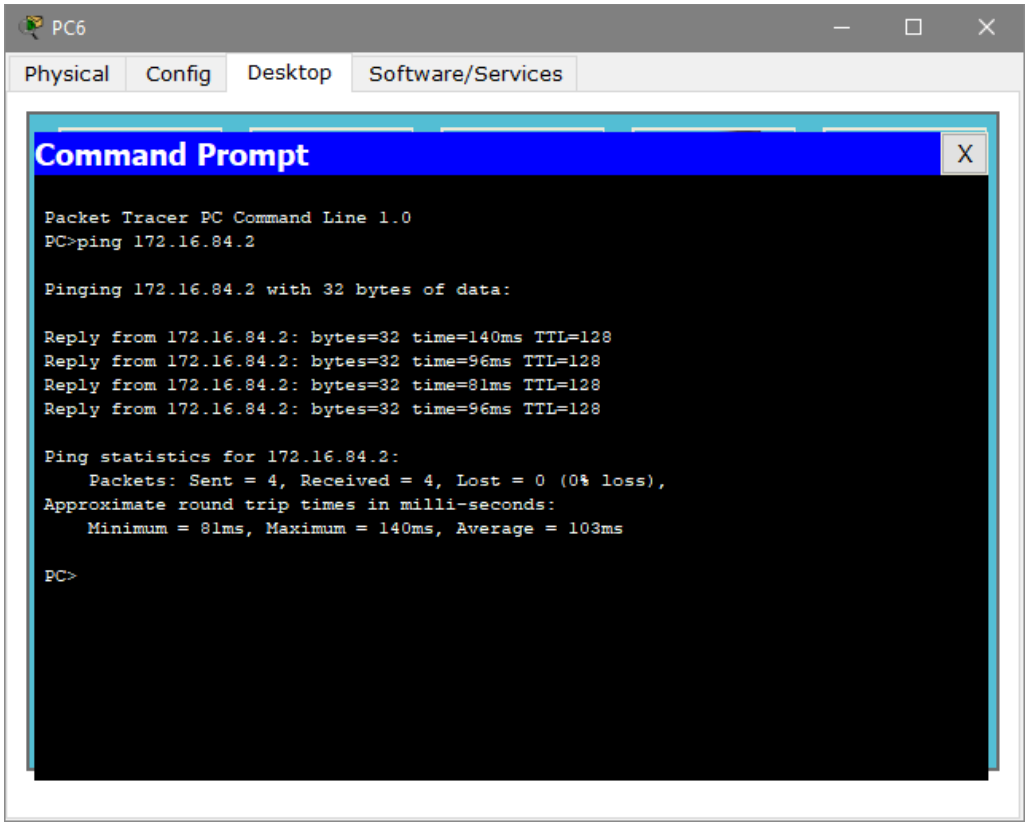


Рисунок 4.16 – Перевірка робочої станції працівника офісу

Для ТОВ «М – систем» була розроблена повністю робоча і справна мережу. Всі робочі станції мають доступ до мережевих ресурсів, а так само мають можливість з'єднатися з іншим співробітником компанії.

5 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

5.1 Розробка методів для захисту інформації в комп'ютерній системі

Коли стоїть питання про рішення завдання безпеки і захисту інформації в корпоративної мережі, в першу чергу потрібно скласти модель загроз за важливістю, щоб оцінити наскільки значима та чи інша загроза для локальної мережі.

Несанкціоноване проникнення в локальну обчислювальну мережу буває наступних видів:

1. Прямий доступ, коли зловмисник має фізичний доступ до даних;
2. Не прямий, відповідно, без фізичної взаємодії з носіями даних.

Часто застосовувані способи для несанкціонованого проникнення до інформації в локальній мережі:

- крадіжка фізичних носіїв даних;
- організація програмних пасток для користувачів;
- запис відео або фотографування екрану;
- перехоплення електромагнітних хвиль моніторів;
- копіювання, яке буде вважатися забороненим;
- брут форс (*Broot force*) - спосіб перебору даних для отримання доступу до локальної мережі;
- використання слабких місць у безпеці програмних комплексів або операційних систем;
- впровадження вірусів в локальну мережу.

Кожен вищевказаний шахрайський спосіб проникнення в локальну мережу можна припиняти. Як говорить статистика, приблизно до вісімдесяти відсотків несанкціонованих проникнень пов'язані саме з діями внутрішніх користувачів локальної мережі, до яких зловмисники в результаті отримували доступ.

У разі отримання зловмисниками доступу до локальної мережі, це може обернутися серйозними наслідками.

- спотворення даних;
- знищення даних третіми особами, на носіях даних або після випадкового зараження робочої операційної системи за допомогою вірусних програмних комплексів;
- передбачити, як сильно атака зловмисників вплине на акції компанії, неможливо. Однак у більшості випадків такі проникнення тягнуть за собою істотне зниження капіталізації і зниження курсу їх акцій.

Різні способи захисту інформації потрібно враховувати ще на етапі складання архітектури мережі.

Існує чотири способи захисних методів:

- програмні;
- апаратно-програмні;
- апаратні або технічні;
- організаційні.

Всі вищевказані методи створені для припинення несанкціонованого доступу до локальної мережі компанії.

Бар'єри даних методів вказані далі:

- перепони фізичного характеру, які служать бар'єром для контакту апаратно частини локальної мережі з третіми особами;
- управління доступом і система контролю, яка прописує рівні прав користувачів виходячи з його посадових обов'язків;
- шифрування системних розділів і локальних дисків на фізичних носіях;
- впровадження дисциплінарних і навіть кримінальних покарань за порушення регламенту щодо зберігання інформації.

Так само існують і організаційні методи захисту інформації, і до них відносять:

- доступ до робочих приміщень по системі пропусків;
- розподіл прав користувачів локальної мережі з різними масивами інформації;
- наявність спеціальних робочих станцій без доступу в Інтернет, під задачу обробки інформації;
- облік фізичних носіїв і присвоєння їм унікальних ідентифікаторів для запобігання підміни;
- виділення особливого місця для розміщення офлайн-робочої станції для обробки інформації, щоб запобігти візуальний контакт з монітором;
- забезпечення для захисту виведення інформації з принтерів, контроль інформації що виводиться на друк;
- затирання даних на фізичних носіях при їх відправленні на сервісне обслуговування в разі виведення з ладу;
- установка датчиків відкритого корпусу на кожну з робочих станцій, так звана система сигналізації.

Регламентація дій користувачів локальної мережі проводиться наступним чином:

- впровадження комерційної таємниці для певного переліку інформації в компанії;
- складання трудових договорів таким чином, щоб кожен співробітник підписував їх в тому числі і про нерозголошення комерційних таємниць компанії;
- проведення регулярних тренінгів для співробітників компанії, що стосуються захисту інформації.

Контроль захисту інформації лежить на обов'язках Служби безпеки та персоналу.

Існують також технічні пристосування для захисту інформації і їх вартість виправдано висока. Вони користуються популярністю серед багатьох організацій і компаній. Такі пристосування створені для ультимативного

захисту тієї системи або програмного забезпечення, для якого вони призначені. Діляться вони на дві групи:

1) Апаратні, які інтегруються в робочу систему по призначеним для них інтерфейсів. Існують, наприклад, пристрої на базі інтерфейсу PCI-Express або USB. Можуть так само вбудовуватися в SATA роз'єм.

2) Фізичні, які можуть бути як і фізичними пристроями, так і архітектурою приміщень, що захищають локальну мережу і складаються в ній вузли від несанкціонованого доступу.

Існують не тільки зовнішні загрози, але і внутрішні, такі як людський фактор. Захисне програмне забезпечення може захищати і від такого.

Залежно від необхідного завдання, методи програмного захисту даних так само поділяються на такі типи:

- антивірусні програмні комплекси;
- програми-шифратори даних, що шифрують дані як на фізичних носіях, так і при передачі їх на інший носій;
- міжмережеві екрани, які не дозволяють зайвому трафіку проникати на ключові робочі станції в локальній мережі;
- впровадження електронного підпису документів, які вказують на їх справжність;
- програмне забезпечення, що ведуть журнал спроб отримання несанкціонованого доступу до локальної мережі;
- програмне забезпечення, що контролює копіювання даних на знімні носії, запобігаючи незаконне копіювання цінної інформації;
- програмні утиліти, що контролюють роздрук секретної інформації на принтерах, вказуючи на користувача, з робочої станції якого була запущена дана дія;
- аудит даних в локальній мережі.

Також можна виділити методи щодо захисту переданої та збереженої інформації в локальній мережі, яка відноситься до апаратно-програмних засобів:

- засоби, що апаратним способом здійснюють контроль доступу;
- організація RAID масивів, які спеціалізовані на безпеку зберігання даних;
- зберігання даних не тільки на жорстких дисках, а й на стрічкових накопичувачах. Термін зберігання інформації на такого типу накопичувачах набагато довший, ніж на магнітних доріжках.

Апаратно-програмну частину слід вибирати ретельно і з можливістю подальшої модернізації. У порівнянні з програмними комплексами по забезпеченню безпеки, їх модернізація і заміна є куди більш складним завданням, як фізично так і фінансово.

5.2 Налаштування мереж VLAN

Простіше кажучи, VLAN - це набір робочих станцій у локальній мережі, які можуть взаємодіяти між собою так, ніби вони перебувають в одній ізольованій локальній мережі. Що означає сказати, що вони "спілкуються між собою так, ніби вони перебувають в єдиній ізольованій локальній мережі"?

Серед іншого, це означає, що:

- широкомовні пакети, надіслані однією з робочих станцій, будуть надходити до всіх інших у VLAN;
- трансляції, надіслані однією з робочих станцій у VLAN, не потраплять на будь-які робочі станції, які відсутні у VLAN;
- трансляції, надіслані робочими станціями, які не перебувають у VLAN, ніколи не потраплять на робочі станції, які перебувають у VLAN;
- всі робочі станції можуть спілкуватися між собою, не потребуючи проходження через шлюз. Наприклад, IP-з'єднання встановлюються ARPing для цільового IP і надсилання пакетів безпосередньо на робочу станцію призначення - не буде потреби для відправки пакетів на шлюз IP для переадресації;

– робочі станції можуть обмінюватися даними між собою, не використовуючи протоколи. Основною причиною поділу мережі на VLAN є зменшення перевантажень у великій локальній мережі.

Щоб зрозуміти цю проблему, нам потрібно коротко поглянути на те, як розвивалися локальні мережі за ці роки.

Спочатку локальні мережі були дуже плоскими - всі робочі станції були підключені до одного шматка коаксіального кабелю або до наборів ланцюжкових концентраторів. У плоскій локальній мережі кожен пакет, який будь-який пристрій вкладає в провід, надсилається на кожен інший пристрій у локальній мережі. У міру зростання кількості робочих станцій у типовій локальній мережі вони почали безнадійно перевантажуватися; було просто занадто багато зіткнень, оскільки більшу частину часу, коли робоча станція намагалася надіслати пакет, виявилося, що провід вже зайнятий пакетом, надісланим якимсь іншим пристроєм.

У цьому розділі описано три рішення для цієї перевантаженості, які були розроблені:

– Використання маршрутизаторів для сегментації локальних мереж;
– Використання перемикачів для сегментування локальних мереж;
– Використання VLAN для сегментації локальних мереж.

Раннім рішенням цієї проблеми було сегментування мережі за допомогою маршрутизаторів. Це розбило б мережу на кілька менших локальних мереж. У кожній локальній мережі було б менше робочих станцій, а отже, менше заторів.

Звичайно, маршрутизовані дані, що надсилаються між локальними мережами, повинні були бути маршрутизовані, тому адреси рівня 3 повинні бути організовані так, щоб кожна локальна мережа мала ідентифікований набір адрес які можна перенаправити, наприклад, в підмережу IP або зону AppleTalk. Протоколи, що не підлягають маршрутизації, повинні були б бути об'єднані між собою, що не зовсім зменшує затори, оскільки мости спрямовують усі трансляції. Але, принаймні для одноадресних пакетів, міст пересилає пакети,

лише якщо він знає, що адреса призначення не знаходиться у вихідній локальній мережі.

Налаштування мережі VLAN з одним комутатором вимагає трохи зусиль: досить налаштувати кожен порт так, щоб вказати йому номер VLAN, до якої він належить. При наявності декількох комутаторів слід враховувати додаткові концепції перенаправлення трафіку між ними. Коли мережі VLAN використовуються в мережах з декількома сполученими між собою комутаторами, на каналах зв'язку між ними застосовується магістральний з'єднання VLAN (*VLAN trunking*). Магістральне з'єднання VLAN на увазі використання комутаторами процесу призначення тегів VLAN (*VLAN tagging*), коли передавальний комутатор додає до кадру інший заголовок перед його передачею по магістральному каналу. Цей додатковий заголовок включає поле ідентифікатора VLAN (*VLAN ID*), що дозволяє передавальному комутатора асоціювати фрейм з конкретною мережею VLAN, а отримує комутатора дізнатися, до якої саме VLAN належить даний фрейм.

Мережі VLAN при наявності декількох комутаторів, але без магістрального з'єднання

Для підтримки кожної мережі VLAN потрібен окремий фізичний канал зв'язку між комутаторами. Якби знадобилося 10 або 20 мереж VLAN, то між комутаторами довелося б прокласти 10 або 20 каналів зв'язку і використовувати для них 10 або 20 портів на кожному комутаторі.

Магістральний з'єднання VLAN створює між комутаторами один канал зв'язку, здатний підтримувати стільки мереж VLAN, скільки необхідно. Комутатори розглядають магістральний канал як частина всіх VLAN. Проте трафік в магістральному каналі VLAN залишається роздільним, і фрейми VLAN 10 аж ніяк не потраплять на пристрої VLAN 20 (і навпаки), оскільки, перетинаючи магістральний канал, кожен фрейм ідентифікований номером VLAN.

Магістральний з'єднання дозволяє комутаторів передавати фрейми декількох мереж VLAN по одному фізичному каналу за рахунок додавання невеликого заголовка до кадру Ethernet.

Впроваджуючи технологію VLAN, створена локальна мережа буде поділена на п'ять підмереж. Підмережа з керівництвом і бухгалтерією, поряд з офісними працівниками та інші чотири підмережі включають в себе виконавчі відділи з офісними працівниками.

Схема поділення загальної мережі на підмережі зображена на рисунку 5.1

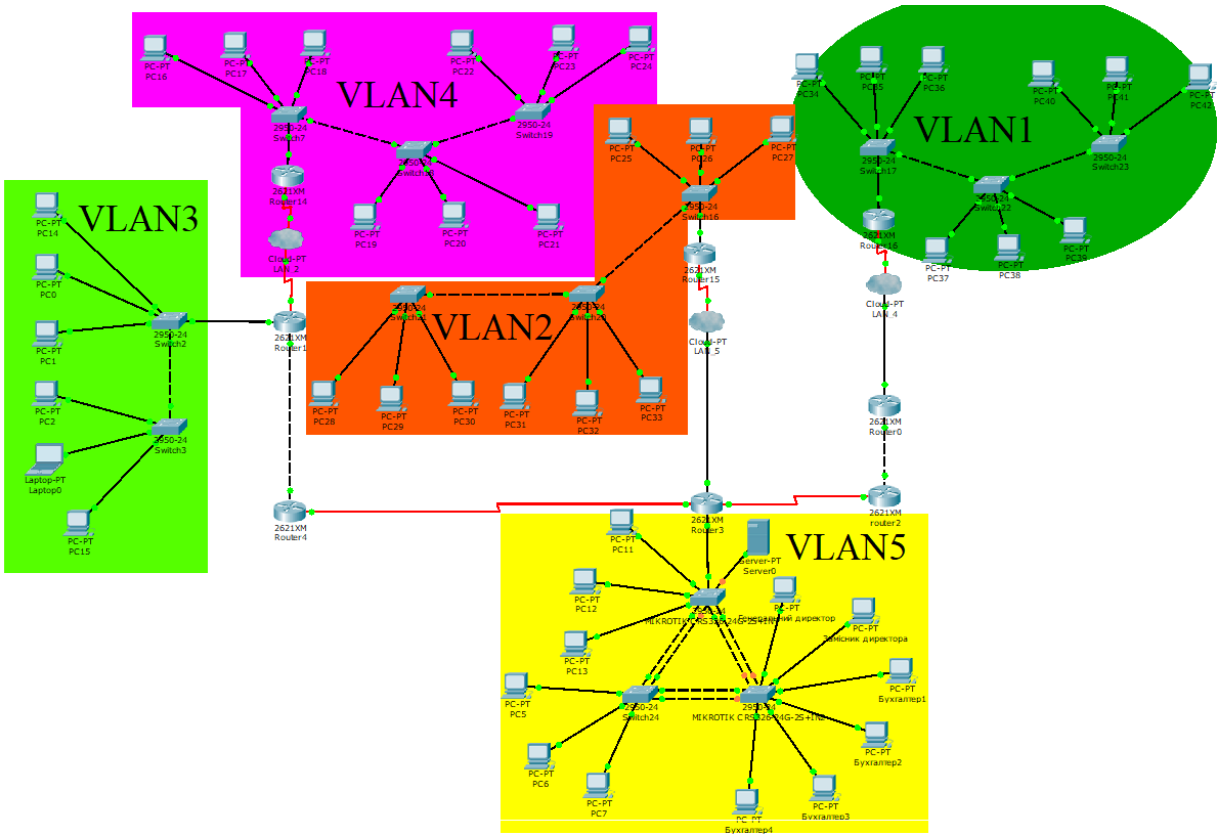


Рисунок 5.1 Розділення локальної мережі на підмережі

Щоб створити вищевказані VLAN, на прикладі Cisco Packet Tracer, потрібно зайти в налаштування кожного комутатора, що існує в кожній підмережі, пройти в його консоль, і ввести спеціальні для цього команди. Ними створити і призначити відповідний VLAN. Команди для даної операції вказані на малюнку 5.2

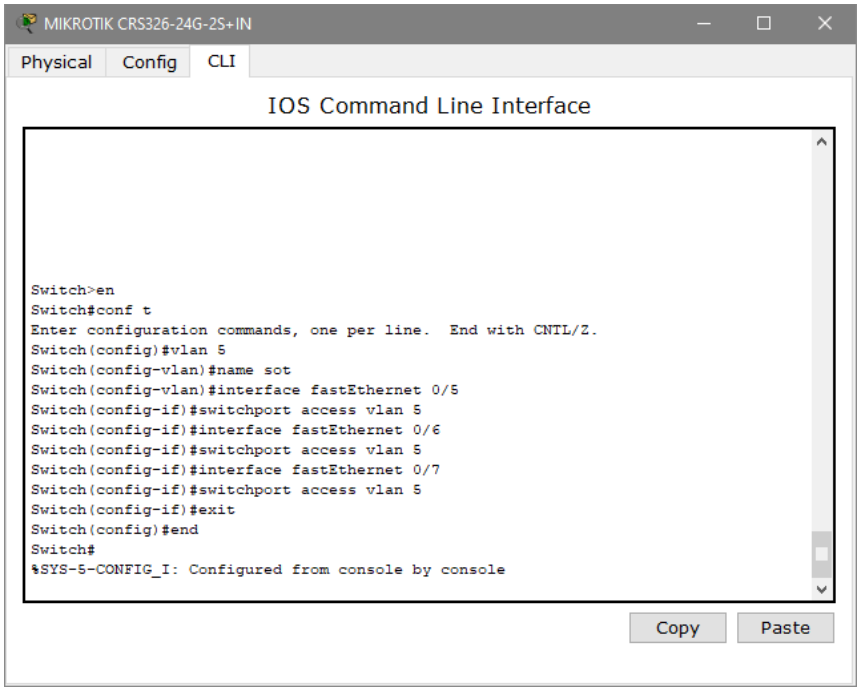


Рисунок 5.2 Налаштування VLAN на комутаторі

Перевірка коректно створеної VLAN можна перевірити командою «*show vlan*» (рис. 5.3)

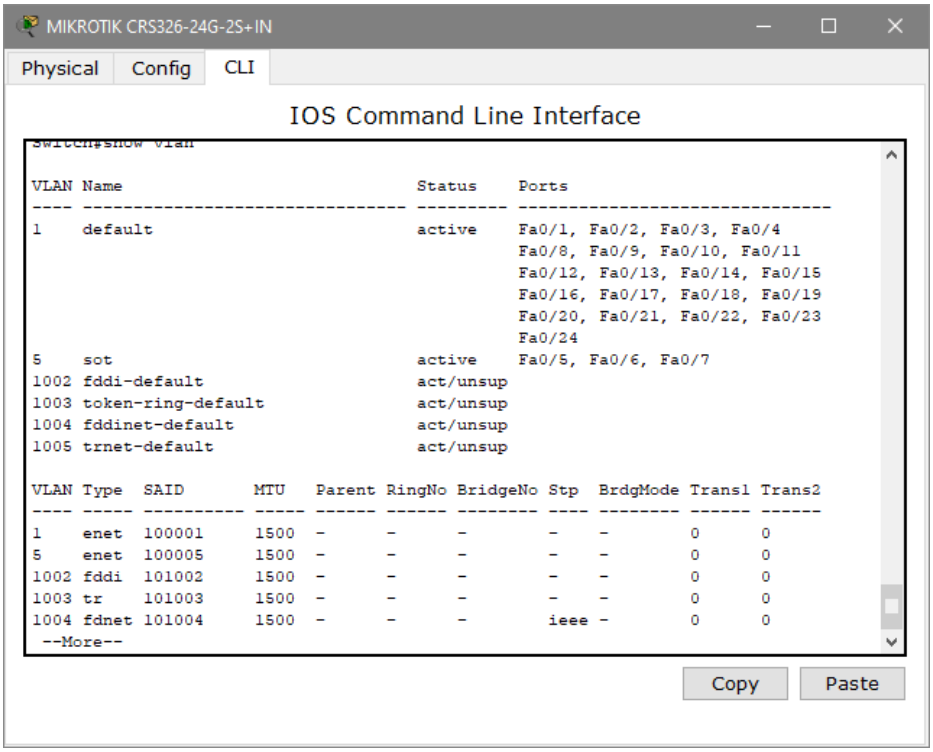


Рисунок 5.3 VLAN створена для працівників офісу

Також у цій же підмережі, але вже до іншого комутатора, була створена інша група працівників для керівництва та бухгалтерії, які також є у підмережі VLAN5 (Рисунок 5.4, 5.5)

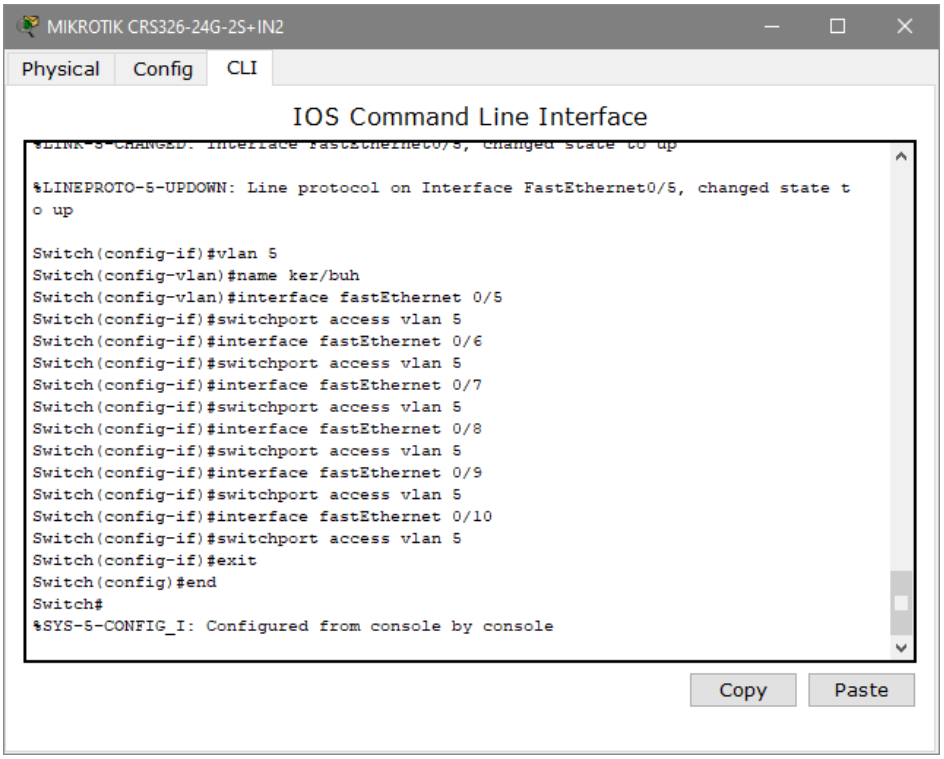


Рисунок 5.4 налаштування VLAN для керівництва та бухгалтерії

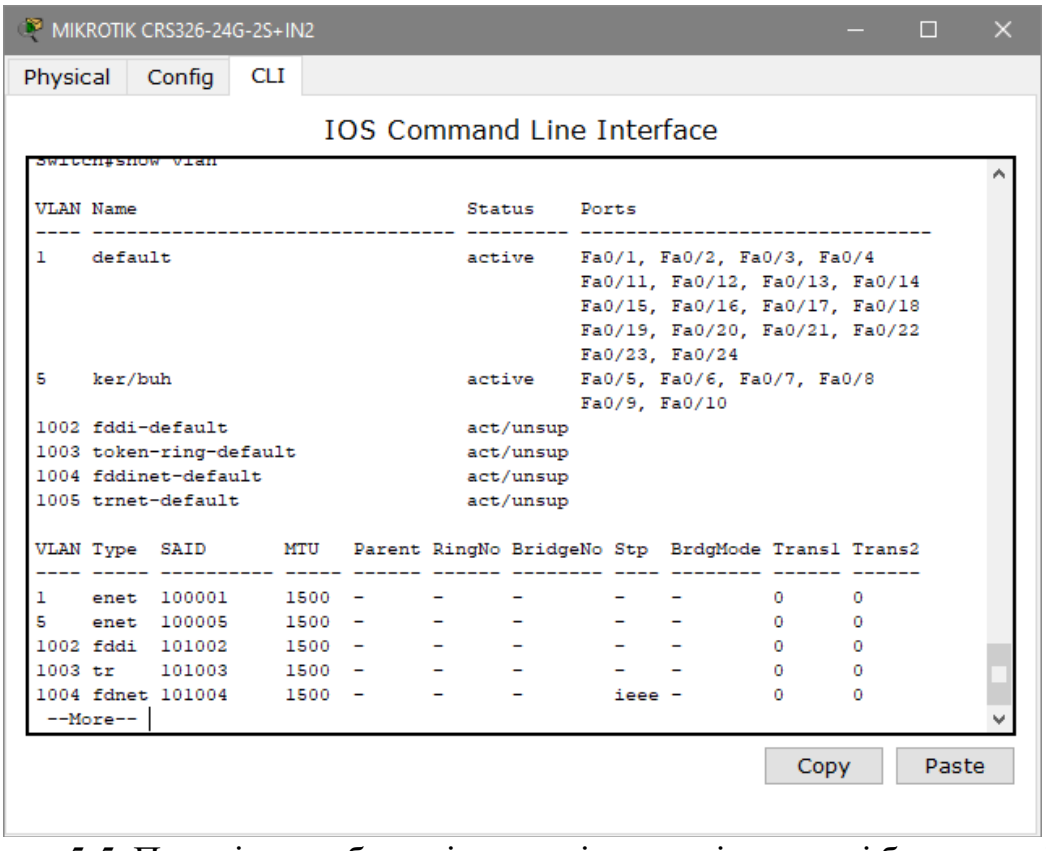


Рисунок 5.5 Перевірка роботи підмережі для керівництва і бухгалтерії

Вищевказані дії були виконані для кожного комутатора в локальній мережі компанії. Всі підмережі були розділені і мають свої назви.

5.3 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

Для того, щоб налаштувати параметри, що відповідають за безпеку світчей і адресації робочих станцій всередині підмереж VLAN необхідно щоб:

- тільки один вузол підмережі мав доступ до потрібного порту;
- при несанкціонованої спробі проникнення в мережу, порт вимикався.

Рисунки 5.6 та 5.7 показує команди, що необхідно ввести на кожному комутаторі в кожній підмережі для забезпечення безпеки.

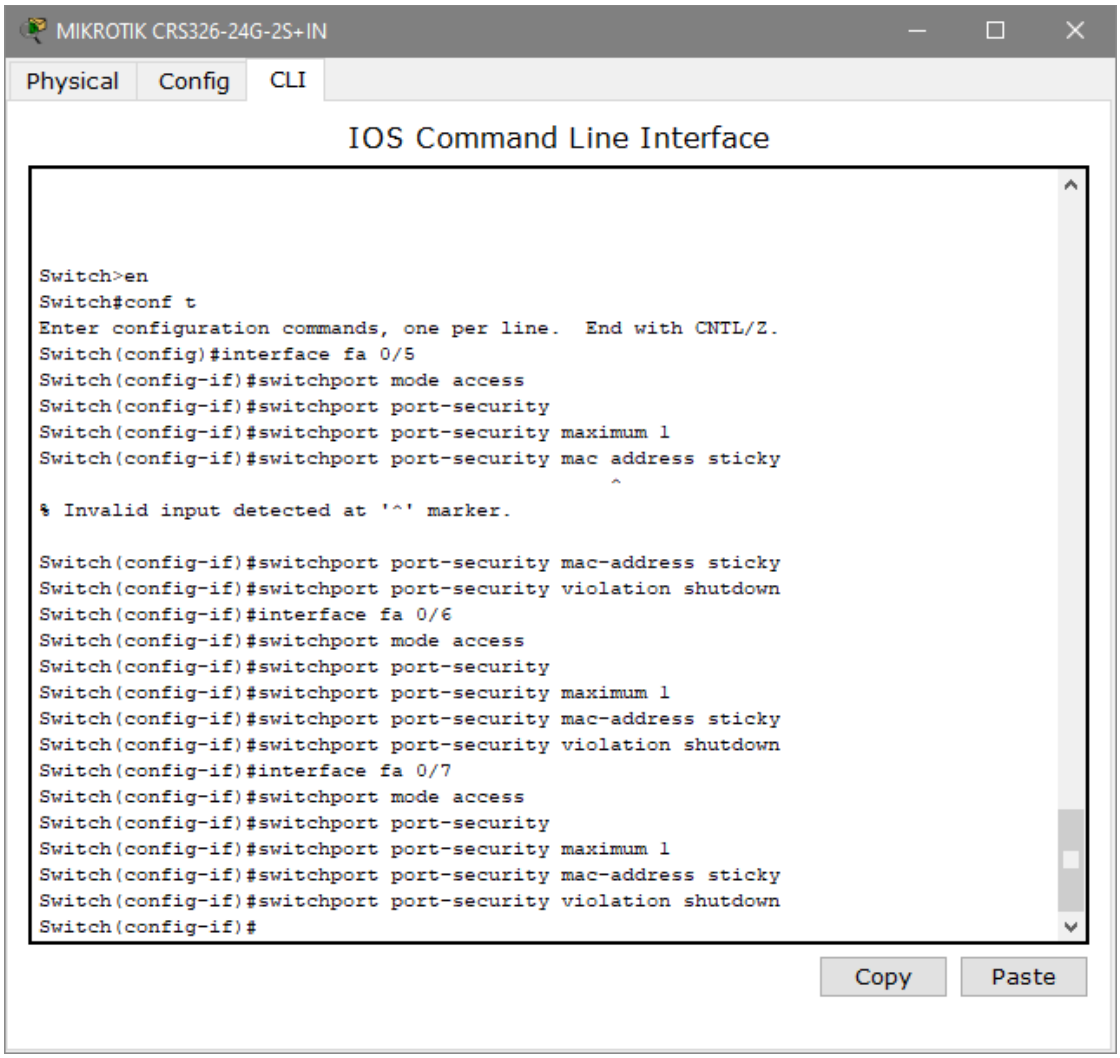


Рисунок 5.6 Команди для комутатору для забезпечення безпеки порту

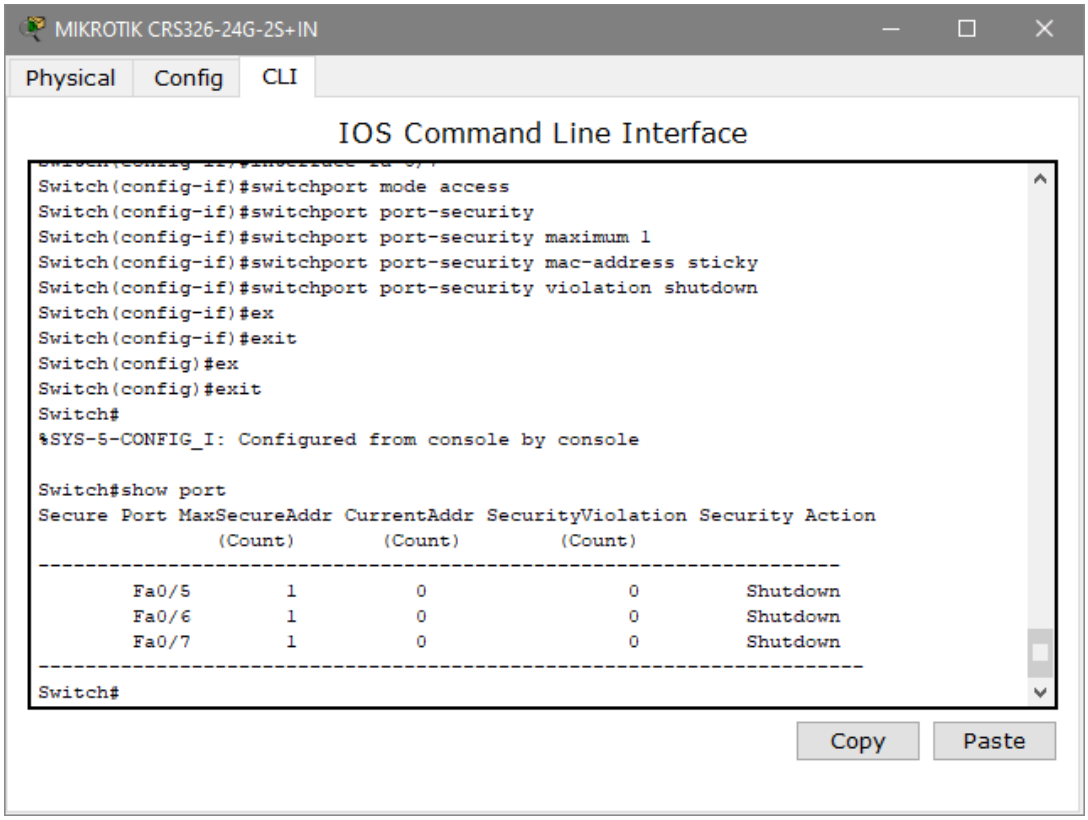


Рисунок 5.7 Перевірка працездатності системи безпеки

ВИСНОВКИ

Темою і метою дипломного проекту було створення локальної мережі ТОВ «М - Систем» для п'яти різних офісів, їх об'єднання в єдину мережу з виходом в Інтернет.

У цьому проекті була створена і модернізована корпоративна локальна мережа на основі сучасних вимог по швидкості передачі даних, безпеки та технічними можливостями.

У процесі створення мережі були вирішені такі питання:

- проаналізовані мережеві архітектури і обрана найбільш підходяща для офісів компанії;
- проведений аналіз сучасних топологій, на основі якого обрано найоптимальнішу;
- тип кабельного з'єднання обраний виходячи з фінансової рентабельності і популярності на ринку;
- виходячи з зручності керування мережею, був обраний відповідний тип управління;
- на основі всіх вищевказаних конфігурацій мережі, підібрано оптимальне апаратне забезпечення, підраховано необхідну кількість маршрутизаторів і комутаторів;
- налаштоване управління мережевими ресурсами і співробітниками компанії на робочих станціях;
- проведений аналіз сучасних тенденцій з безпеки мережі, на основі яких в мережу були впроваджені найнеобхідніші з них.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

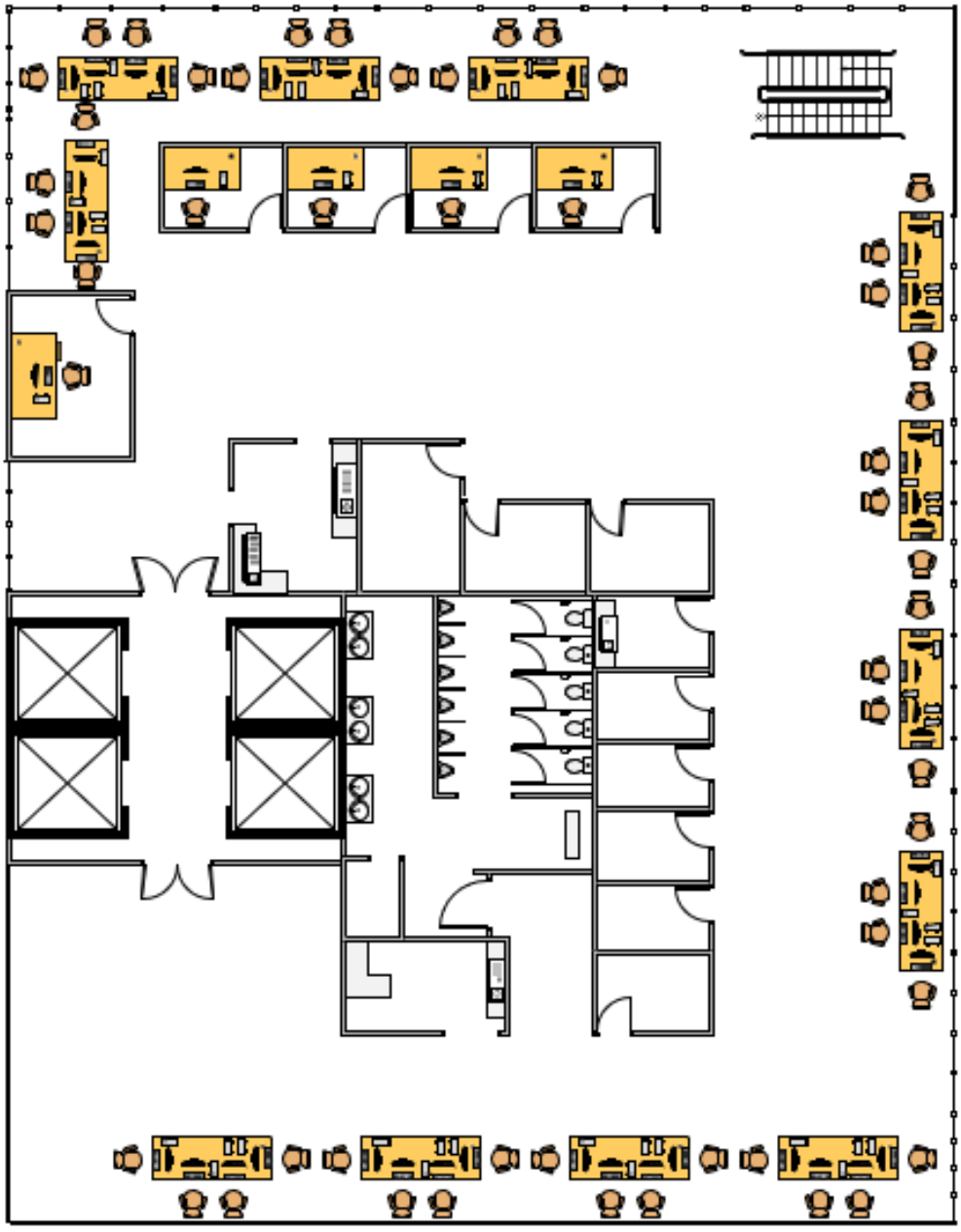
1. Термін Інформаційних технологій https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97
2. Інтернет - https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82
3. Офіційна сторінка ТОВ «М - Систем» https://msystem.com.ua/about/
4. Що таке Prom.ua - https://uk.wikipedia.org/wiki/Prom.ua
5. Цвіркун Л.І. Комп'ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с.
6. Роутер MIKROTIK hAP ac https://can.ua/mikrotik-hap-ac-rb962uigs-5hact2hnt/p62226/
7. Комутатор MIKROTIK CRS326-24G-2S https://can.ua/mikrotik-crs326-24g-2splusin/p233396/#tab=characteristics
8. Роз'яснення UTP/STP https://bumotors.ru/uk/telefonnyi-kabel-yavlyaetsya-variantom-vitoi-pary-vitaya-para-raznovidnosti.html
9. Роз'яснення UTP/STP (2) https://bumotors.ru/uk/klassifikaciya-vitoi-pary-vidy-kabelya-vitaya-para-kratko.html
10. Пояснення про топологію «Зірка» https://studopedia.su/13_92580_topologii-obchislyuvalnoi-merezhi.html
11. Топологія «Зірка» (1) http://um.co.ua/8/8-8/8-84314.html
12. Топологія «Зірка» (2) https://mydocx.ru/3-57134.html
13. Розрахунок PDV https://infopedia.su/2x40d6.html#:~:text=%D0%97%D0%B0%D0%B3%D0%B0%D

0%BB%D1%8C%D0%BD%D0%B5%20%D0%B7%D0%BD%D0%B0%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20PDV%20%D0%BD%D0%B5%20%D0%BF%D0%BE%D0%B2%D0%B8%D0%BD%D0%BD%D0%B5,%D1%83%20%D0%B4%D1%80%D1%83%D0%B3%D1%96%D0%B9%20%2D%20%D1%81%D0%B5%D0%B3%D0%BC%D0%B5%D0%BD%D1%82%20%D1%96%D0%BD%D1%88%D0%BE%D0%B3%D0%BE%20%D1%82%D0%B8%D0%BF%D1%83.

14. Розрахунок PVV https://infopedia.su/2x40d6.html

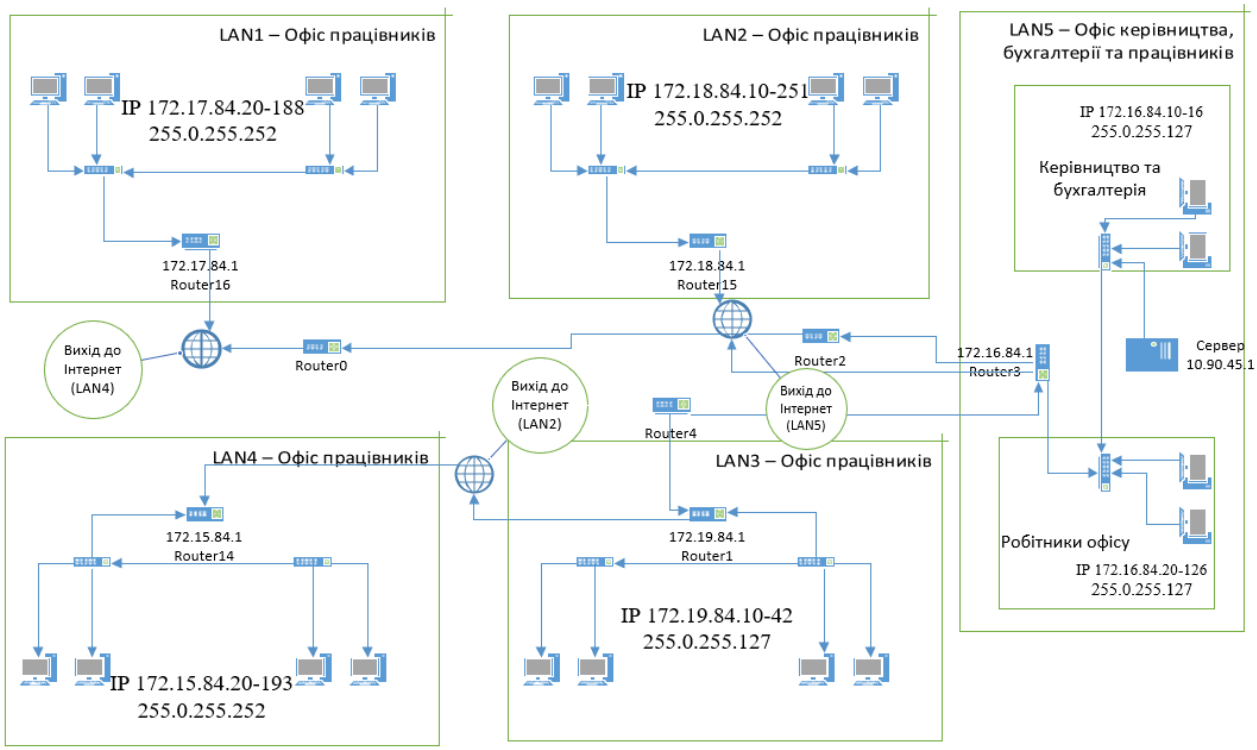
ДОДАТОК А

План розміщення робочих станцій у головному офісі



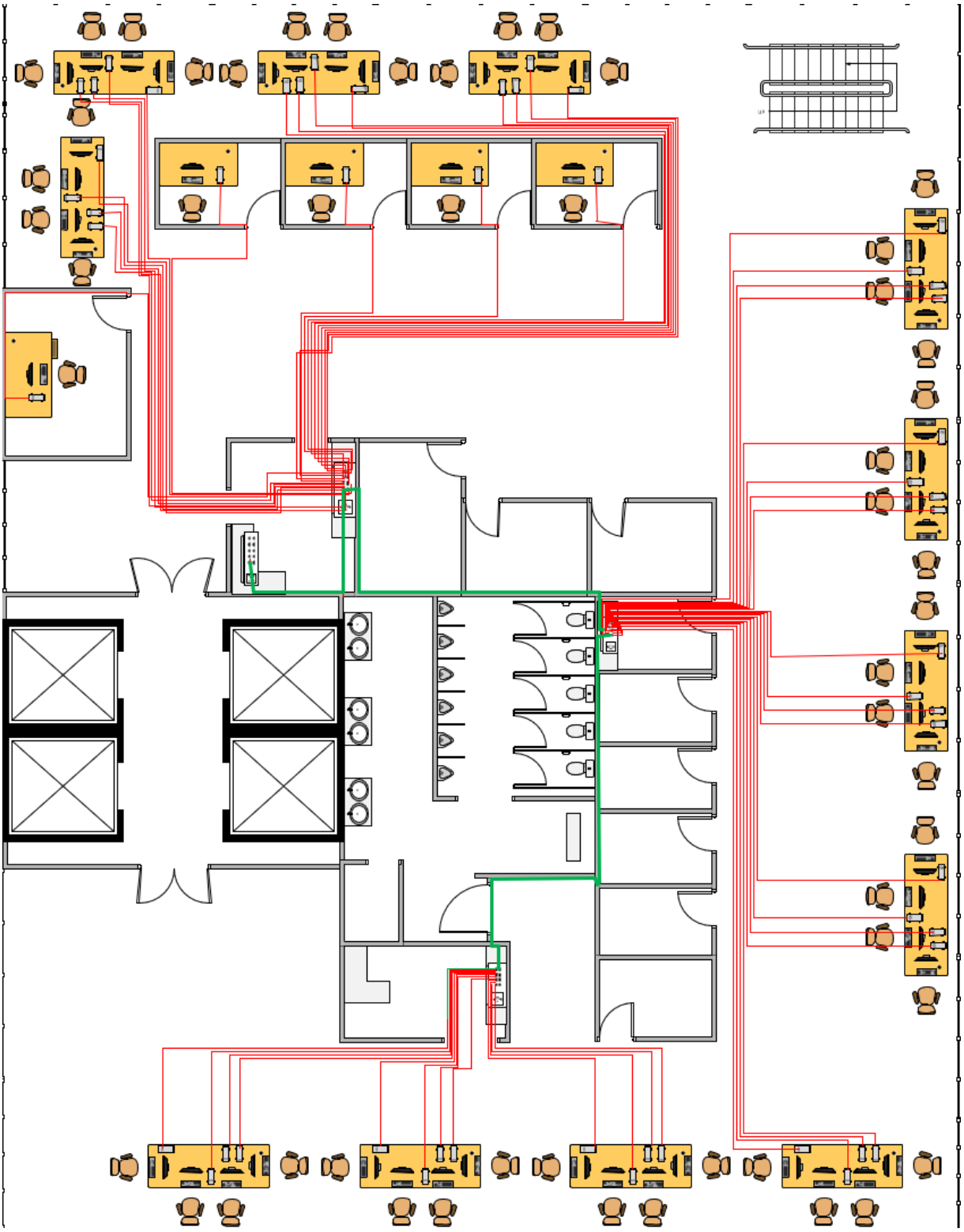
ДОДАТОК Б

Схема з’єднань локальної обчислювальної мережі



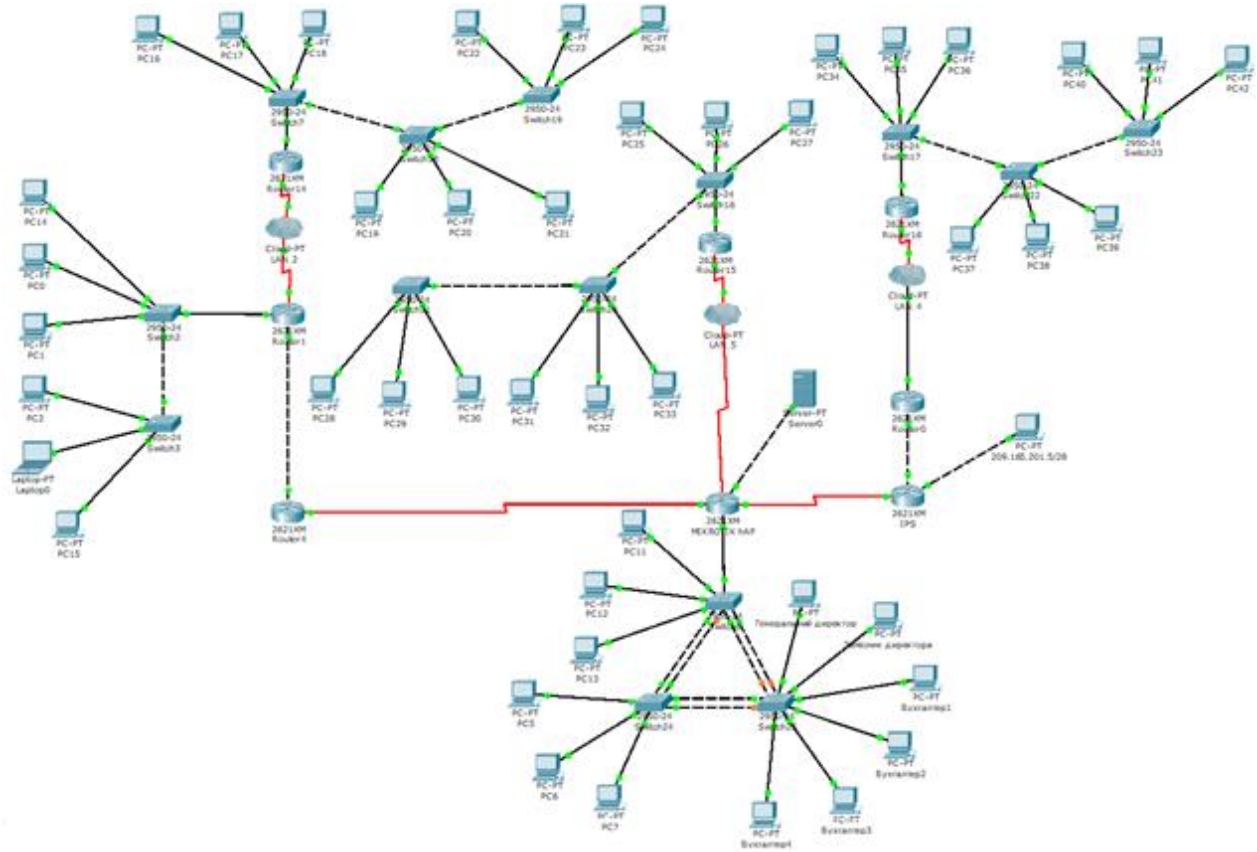
ДОДАТОК В

Схема розташування мережевого обладнання у головному офісі



ДОДАТОК Г

Загальна схема топології корпоративної мережі



ДОДАТОК Д

ТЕКСТ ПРОГРАМИ НАЛАШТУВАННЯ МЕРЕЖІ
КОМП'ЮТЕРНОЇ СИСТЕМИ

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.21007-01 12 01

Листів 13

2021

АНОТАЦІЯ

Програма призначена для програмування комутаторів та маршрутизаторів комп'ютерної системи ТОВ «М - Систем» відповідно до завдання до кваліфікаційної роботи.

Середовище розробки та налагодження скриптів – пакет моделювання мереж Packet Tracer в середовищі операційної системи Windows 10.

ЗМІСТ

// _1. Програмування комутатора Omelyanenko_Switch_1

version 12.2

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption *// _Шифрування* password

// _

hostname Omelyanenko_Switch_1 *// _Призначення ім'я пристрою*

// _

enable password 7 0822404F1A0A *// _Пароль привілейованого режиму*

// _

ip domain-name Omelyanenko_Switch_1 *// _Призначення домену*

// _

username 123171_Omelyanenko privilege 1 password Krivich123171

// _Призначення користувача та пароля

// _

spanning-tree mode pvst

spanning-tree extend system-id

/// _Програмування інтерфейсів

interface FastEthernet0/1

switchport access vlan 28

// _

interface FastEthernet0/2

switchport access vlan 28

// _Програмування безпеки на портах, до яких підключені сервери

interface FastEthernet0/3

switchport access vlan 38

switchport mode access

switchport port-security

```
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
// _
interface FastEthernet0/4
switchport access vlan 38
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0090.2BE6.564D
// _
interface FastEthernet0/5
switchport access vlan 38
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 00D0.D38C.1AA9
// _
interface FastEthernet0/6
switchport access vlan 48
// _
interface FastEthernet0/7
switchport access vlan 48
// _
```

```
interface FastEthernet0/8
switchport access vlan 48
// _
interface FastEthernet0/9
switchport access vlan 48
// _
interface FastEthernet0/10
switchport access vlan 48
// _
interface FastEthernet0/11
switchport access vlan 48
// _
interface FastEthernet0/12
switchport access vlan 48
// _
interface FastEthernet0/13
switchport access vlan 48
// _
interface FastEthernet0/14
switchport access vlan 48
// _
interface FastEthernet0/15
switchport access vlan 48
// _
interface FastEthernet0/16
switchport access vlan 48
// _
interface FastEthernet0/17
```

```
switchport access vlan 48
// _
interface FastEthernet0/18
switchport access vlan 48
// _
interface FastEthernet0/19
// _
interface FastEthernet0/20
// _
interface FastEthernet0/21
// _
interface FastEthernet0/22
// _
interface FastEthernet0/23
// _
interface FastEthernet0/24
// _Програмування транкових портів
interface GigabitEthernet0/1
switchport trunk native vlan 100
switchport trunk allowed vlan 1,28,38,48,99-100
switchport mode trunk
// _
interface GigabitEthernet0/2
switchport trunk native vlan 100
switchport trunk allowed vlan 1,28,38,48,99-100
switchport mode trunk
// _
interface Vlan1
```

```
no ip address
shutdown
// _Програмування інтерфейсу керування
interface Vlan99
mac-address 0030.a313.1801
ip address 192.168.144.99 255.255.255.248
// _
// _Програмування банеру MOTD
banner motd ^CThis is a secure system. Authorized Access Only!^C
// _Програмування ліній консолі, vty і ssh
line con 0
password 123171
login local
// _
line vty 0 4
password 123171
login local
transport input ssh
line vty 5 15
password 123171
login local
transport input ssh
// _
end
```

// 2. Програмування маршрутизатора Omelyanenko_Router_5

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption *// _Включення шифрування паролів*
// _

hostname Omelyanenko_Router_5 *// _Призначення ім'я пристрою*

enable password Omelyanenko123171 *// _Вказано пароль до привілейованого режиму*
// _

ip dhcp excluded-address 192.168.146.1 *// _Видалення адрес з пулу DHCP*

ip dhcp excluded-address 192.168.146.2

ip dhcp excluded-address 192.168.146.3

// _

ip dhcp pool LAN5 *// _Призначення та Програмування пулу для локальної мережі*

network 192.168.146.0 255.255.255.128

default-router 192.168.146.1

dns-server 192.168.144.123

// _

aaa new-model *// _Програмування аутентифікації через AAA-сервер*

// _

aaa authentication login default group radius local

// _

no ip cef

no ipv6 cef

// _

username 123171_Omelyanenko password Omel123171

// _Призначення користувача та пароля

```
// _ Програмування VPN
license udi pid CISCO2911/K9 sn FTX15241V68-
license boot module c2900 technology-package securityk9
// _
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
// _
crypto isakmp key cisco address 64.100.13.1
// _
crypto ipsec transform-set TS esp-3des esp-md5-hmac
// _
crypto map CMAP 10 ipsec-isakmp
set peer 64.100.13.1
set transform-set TS
match address FOR-VPN
// _
ip domain-name Omelyanenko_Router_5 // _Призначення і'мя домену
// _
spanning-tree mode pvst
// _
interface GigabitEthernet0/0 // _Програмування інтерфейсів
ip address 192.168.146.1 255.255.255.128
ip nat inside
duplex auto
speed auto
// _
```

```
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
// _
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
// _
interface Serial0/2/0
ip address 10.0.18.18 255.255.255.252
ip nat inside
clock rate 128000
// _
interface Serial0/2/1
ip address 10.0.18.30 255.255.255.252
ip nat inside
// _
interface Serial0/3/0
ip address 10.0.18.34 255.255.255.252
ip nat inside
// _
interface Serial0/3/1
ip address 209.165.200.1 255.255.255.224
ip access-group ACL_LAN4 out
// _
```

```
ip nat outside
ip summary-address eigrp 16 192.168.144.0 255.255.248.0 5
crypto map CMAP
// _
interface Vlan1
no ip address
shutdown
// _Програмування динамічної маршрутизації
router eigrp 16
eigrp router-id 5.5.5.5
redistribute static
passive-interface GigabitEthernet0/0
network 192.168.146.0 0.0.0.127
network 10.0.18.28 0.0.0.3
network 10.0.18.16 0.0.0.3
network 10.0.18.32 0.0.0.3
network 209.165.202.0 0.0.0.3
// _Програмування NAT
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list 18 pool Internet
ip nat inside source list Internet interface Serial0/3/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.2
// _
ip flow-export version 9
// _Програмування списків доступу
ip access-list extended FOR-VPN
permit ip 192.168.144.0 0.0.7.255 192.168.145.0 0.0.0.127
ip access-list extended Internet
```

deny ip 192.168.144.0 0.0.7.255 192.168.145.0 0.0.0.127

permit ip 192.168.144.0 0.0.7.255 any

ip access-list standard ACL_LAN4

deny 192.168.145.128 0.0.0.127

// _

// _Програмування банеру MOTD

banner motd ^CThis is a secure system. Authorized Access Only!^C

// _Програмування Radius сервера

radius-server host 192.168.144.91 auth-port 1645 key radius123

radius-server host 192.168.144.122 auth-port 1645 key radius123

// _Програмування ліній консолі, vty і ssh

line con 0

password 123171

// _

line aux 0

// _

line vty 0 4

password 123171

transport input ssh

line vty 5 15

password 123171

transport input ssh

// _

End