Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування закладу вищої освіти)

Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту, назва факультету (відділення))

Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

магістр
(ступінь вищої освіти)

на тему **Удосконалення та дослідження характеристик телекомунікаційної мережі підприємства**

Виконав: студент 6 курсу, групи 601ТТ
спеціальності 172 «Телекомунікації та
(шифр і назва напряму підготовки, спеціальності)
радіотехніка

Мірошниченко Т.Ю.
(прізвище та ініціали)
Керівник Сільвестров А.М.
(прізвище та ініціали)
Рецензент Дрючко О.Г.
(прізвище та ініціали)

Полтава – 2023 рік

Національний університет «Полтавська політехніка імені Юрія Кондратюка»

Інститут Навчально-науковий інститут інформаційних технологій і робототехніки

Кафедра Автоматики, електроніки та телекомунікацій

Ступінь вищої освіти Магістр
Спеціальність 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ

Завідувач кафедри автоматики,
електроніки та телекомунікацій

_____ О.В. Шефер
“ 04 ” 09 2023 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Мірошниченку Тарасу Юрійовичу

1. Тема проекту (роботи) **«Удосконалення та дослідження характеристик телекомунікаційної мережі підприємства»**
Керівник проекту (роботи) **Сільвестров Антон Миколайович, д.т.н., професор,**

затверджена наказом вищого навчального закладу від “ 04 ” 09 2023 року № 986
2. Строк подання студентом проекту (роботи) 13.12.2023 р.
3. Вихідні дані до проекту (роботи) Технологія Ethernet; Cisco Pocket Tracer, технічна документація Cisco.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Огляд сучасних мережевих технологій. Огляд топологій телекомунвкаційних мереж. Дослідження середовищ поширення сигналів. Огляд комутаційних засобів мережі. Розробка логічної та фізичної моделв мережі. Вибір мережевого обладнання. Розробка схеми резервного живлення.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів):
1) Модель OSI.
2) Топологія комп’ютерних мереж.
3) Середовища передачі даних.
4) Комутаційні засоби мережі.
5) Фізична модель мережі.
6) Логічна модель мережі.
7) Вибір мережевого обладнання.
8) Забезпечення безперебійного живлення.

9) Висновки.

6. Дата видачі завдання 04.09.2023 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів магістерської роботи	Термін виконання етапів роботи			Примітка (плакати)
1	Аналіз розвитку сучасних мережевих технологій	13.09.23		15%	Сл. 3
2	Аналіз топологій комп'ютерних мереж	27.09.23	I	30%	Сл. 4
3	Аналіз серидовищ передачі даних	10.10.23		40%	Пл. 5
4	Аналіз актуального комутаційного оладнання мережі	17.10.23		50 %	Сл. 6
5	Розробка фізичної моделі мережі	24.10.23	II	60%	Сл. 7
6	Розробка логічної моделі мережі у середовищі моделювання Cisco Pocket Tracer	08.11.23		70%	Сл. 8
7	Вибір мережевого обладнання та забезпечення безперебійного живлення	20.11.23	III	100%	Сл. 12

Магістрант _____ Мірошниченко Т.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Сільвестров А
(підпис) (прізвище та ініціали)

ЗМІСТ

ВСТУП

Комп’ютерні технології стрімко розвиваються, кожен новий рік промисловість пропонує нові пристрої та технології, які в подальшому знаходять застосування як у побутовому житті, так і на виробництві. Вийнятком не стали і комп’ютерні мережі, які також пройшли довгий еволюційний шлях.

Комп’ютерні мережі будуються за сегментним підходом. Сегменти поділяють за масштабно — територіальною ознакою. Такий підхід передбачає поділ сегментів за ієрархією.

Глобальна мережа (Global Area Network, GAN) - це загальнопланетарна мережа, яка об’єднує всі країни та континенти, забезпечує досту користувачів мережі в будь-якій точці земної кулі.

Великомасштабна територіальна мережа (Wide Area Network, WAN) – сегмент, призначений для об’єднання мереж міського масштабу або сільських районів, розташованих на території великого регіону, держави, континенту, а також на різних континентах.

Мережа мегаполісу (Metropolitan Area Network, MAN) – сегмент, що охоплює територію міста, сільського району, області або регіону.

Локальна мережа (Local Area Network, LAN) – сегмент, у якому основна частина трафіку замикається всередині невеликої території, установи, промислового підприємства і т. п. Сегментами типу LAN також є мережі, утворені поєднанням декількох локальних мереж, розташованих на невеликій відстані один від одного (мережі кампусів).

Метою дослідження є модернізація корпоративної мережі підприємства .

Об’єктом дослідження є приватне підприємство.

Предмет дослідження — телекомунікаційна мережа підприємства. Задачі квалафікаційної роботи: Модернізація локальної мережі підприємства у зв’язку з розширенням виробничих спроможностей. Розроблена і побудована локальна мережа повинна складатися з робочих станцій та преиферійних пристроїв,

маршрутизаторів, також повинні бути точки доступу Wi – Fi, сервер для резервного копіювання даних.

Окремою вимогою буде наявність джерела безперебійного живлення для комп’ютерів та маршрутизаторів, а також резервного генратора для роботи мережі в умовах, коли є проблеми з живленням.

Для перевірки працездатності локальної мережі під час проектування буде використовуватися Cisco Pocket Tracer – симулятор мережі передачі, розроблений компанією Cisco Systems. Вона дозволяє будувати працездатні комп’ютерні мережі, налаштовувати маршрутизатори та комутатори.

1 ОСНОВНІ ЕЛЕМЕНТИ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ

1.1 Мережні топології

Топологія «шина» передбачає, що всі пристрої мережі підключені до одного кабеля (Рисунок 1.1), на кінцях якого повіинні бути заглушки (термінатори). На базі такої тоаології будуються 10-ти Мегабітні мережі Ethernet (10Base – 2, 10Base – 5). Використовується, як правило, коаксіальний кабель. Така мережа проста у налаштуванні та монтажі, дешева, якщо виходуть з ладу одна робоча станція, мережа продовжує працювати. Але якщо виникає якась несправність в якомк — небуть місці, то виходить з ладу вся мережа. Досить складно шукати несправності. Низька продуктивність у порівнянні з іншими топологіями.

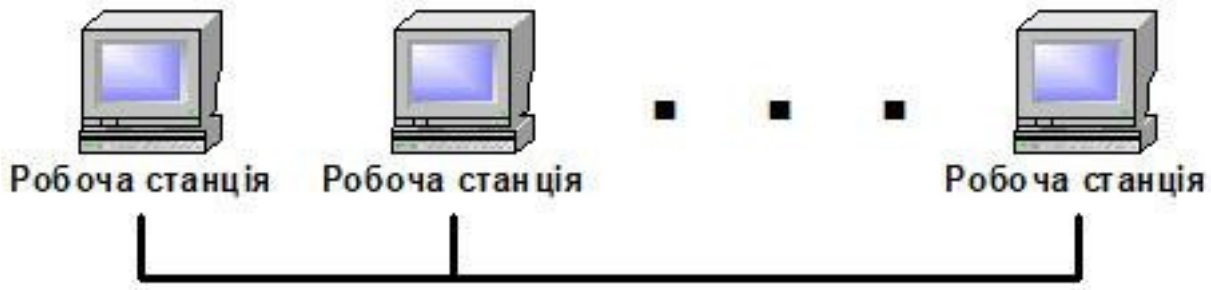


Рисунок 1.1 — Топологія «шина»

Топологія «кільце» передбачає, що усі робочі станції зв’язані фізичним кільцем. Як серидовище передачі даних використовуються, переважно, вита пара та оптоволокно. Повідомлення циркулюють по колу. Якщо комп’ютер розпізнає адресовані йому дані, він копіює їх у внутрішній буфер. Час передачі повідомлень зростає пропорційно збільшенню кількості робочих станцій у мережі. Для мереж Ethernet така топологія не використовується.

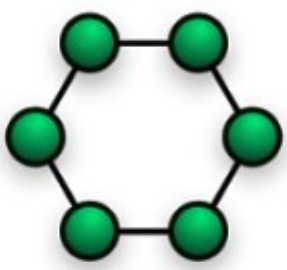


Рисунок 1.2 — Топологія «кільце»

В основі локальної мережі, яка побудована за топологією «зірка» (Рисунок 1.3). Її принцип полягає у тому, що кожен комп’ютер або інший пристрій підключається кабелем не до іншого комп’ютера, а до спеціального мережевого обладнання, в ролі якого можути виступати концентратор (hub), комктатор (switch), маршрутизатор (router). Перевагою такої топології є те, що при розриві з’єднання між одним з підключених пристроїів і, наприклад, комутаторои, то вся інша мережа продовжує працювати.

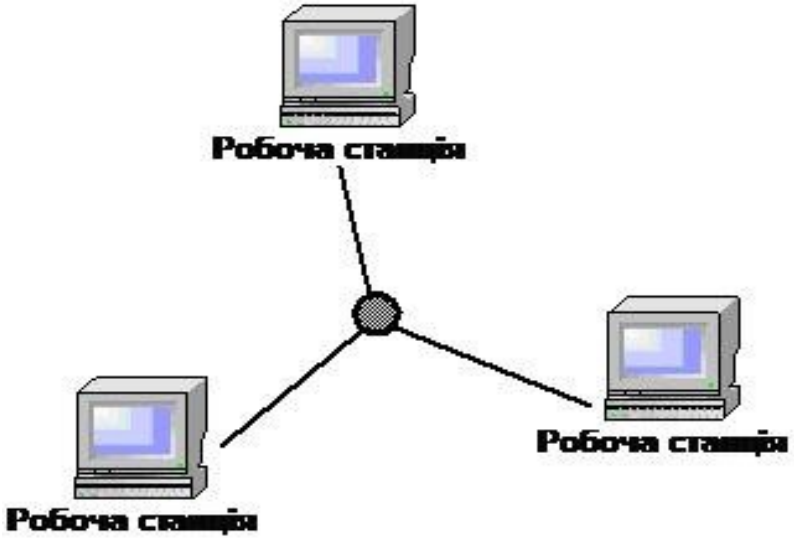


Рисунок 1.3 - Топологія "зірка"

Правда, якщо цим пристроєм був єдиний сервер, то відновити роботу мережі буде досить важко. При виході з ладу концентратора (або іншого "центра") мережа перестане працювати. Така топологія має перевагу при пошуку ушкоджень елементів мережі: кабеля, мережних адаптерів, з'єднань та ін.. Така топологія також зруна при додаванні нових пристроїв до мережі. Як серидовище передачі даних використовується вита пара та оптоволоконні кабелі. В теперішній час 100 і 1000 Мбітні мережі Ethernet будуються переважно за топологією "зірка".

1.2 Кабельні системи

Невід’ємною частиною будь — якої телекомунікаційної мережі є лінії зв’язку. Лінія зв'язку складається в загальному випадку з фізичного середовища, по якому передаються електричні інформаційні сигнали, апаратури передачі даних і проміжної апаратури. инонімом терміна лінія зв'язк (line) є термін канал зв'язку (channel)[2].

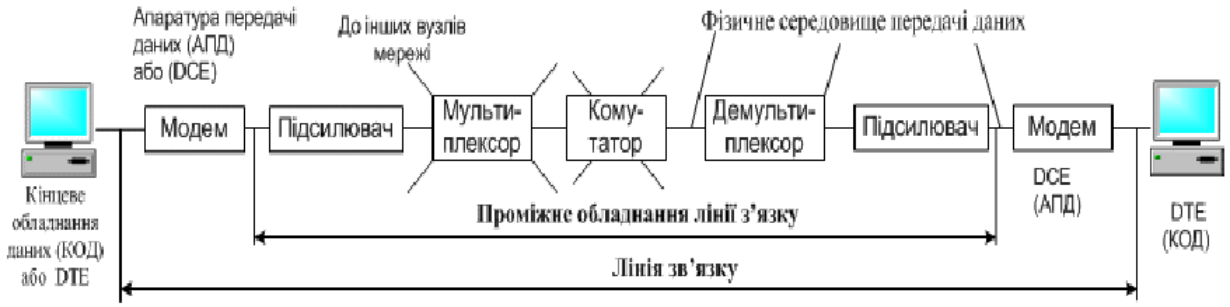


Рисунок 1.4 — Схема лінії зв’язку

Схама каналу зв’язку зображенан на рисунку 1.4. Серидовище передачі даних може представляти собою як кабель (Рисунок 1.5) — набір провідників і ізоляційних оболонок, так і земну атмосферу чи косміний простір, через які поширюються електромагнітні хвилі (Рисунок 1.6).

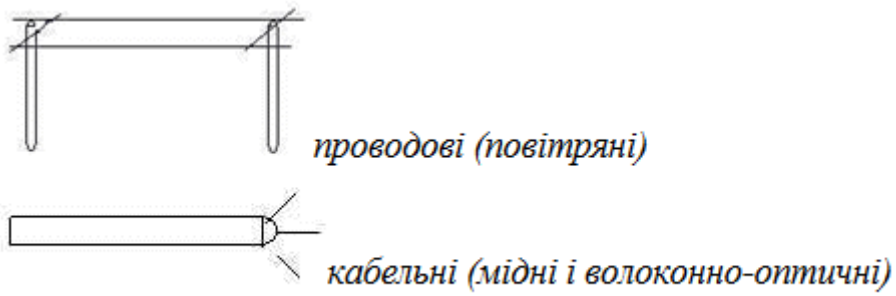
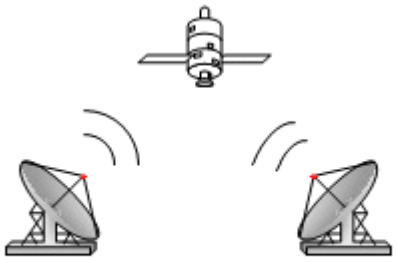


Рисунок 1.5 — Проводові та кабельні канали зв’язку



радіоканали наземного і супутникового зв'язку

Рисунок 1.6 — Канал супутникового зв’язку

Проводові лінії зв’язку представляють собою провід без ізоляції, який прокладений по стовпам і висить у повітрі. Такі лінії зв’язку, як правило, використовуються для передачі телефонних чи телеграфних сигналів, а за потреби ними можна передавати і комп’ютерні данні. Швидкість передачі даних і завадозахищеність у таких лініях далеко не найкраща, тому сьогодні вони швидко витісняються кабельними каналами зв’язку.

Кабельні лінії являють собою досить складну конструкцію. Кабель складається з провідників, укладених у кілька шарів ізоляції: електричної, електромагнітної, механічної, а також, можливо, кліматичної. Кабель може бути оснащений роз'ємами, що дозволяють швидко виконувати приєднання до нього різного устаткування[2].

У комп’ютерних мережах використовуються три основні типи кабелів:

1. Кабелі на основі витої пари мідних провідників.

2. Коаксіальні кабелі з мідною жилою.

3. Волоконно — оптичні кабелі.

Тип кабелю «вита пара» або «скручена пара» є найпоширенішим. Він містить дві або більше пари провідників. В кожній парі провідники скручені один з одним по всій довжині кабелю. Це дозволяє підвищити завадостійкість кабелю і зменшити вплив сигналу в кожній парі на всі інші. Максимальна відстань передавання при його використанні 1.5-2.0 км, а максимальна

швидкість- 1.2 Гбіт/с. Тривалість поширення сигналу 8-12 нс/м. Загасання сигналу 12-28 Дб на 100 м на частоті 10 МГц.

Найпоширенішим серидовищем для передачі даних на короткі відстані (до 100 метрів) є неекранована вита пара UTP (Unhielded Twisted Pair). Кручена пара UTP – це вісім мідних дротів, скручені попарно в спільній ізоляції. Вона є найпоширенішою та найдешевшою крученою парою, проте в разі її експлуатації виникають проблеми з електромагнітною сумісністю[2].

Є також екрановані варіанти витої пари:

1. FTP (Foiled Twisted Pair) – фольгована вита пара.

2. STP (Shielded Twisted Pair) – екранована вита пара.

У порівнянні з UTP, екрановані варіанти витої пари мають ширший частотний діапазон передавання, менше електромагнітне випромінювання, але їх ціна значно дорожча, а також вони складніші у монтажі. Більш детально це показано у таблиці 1.1.

Таблиця 1.1 — Порівняльні характеристики скручених пар

Показник	UTP	FTP	S/FTP	S/STP
Ціна в $ за 1 км	200-300	280-420	460-690	700-1050
Максимальна частота, МГц	100	150	300	300
Товщина, мм	5.1	6.2	6.5	7.3
Встановлення	Легке	Легке	Легке	Важке
Заземлення	Легке	Важке	Легке	Легке

Коаксіальний кабель (coaxial) має несиметричну конструкцію і складається з внутрішньої мідної жили й оплетки, відділеної від жили шаром ізоляції. Існує кілька типів коаксіального кабелю, що відрізняються характеристиками й областями застосування — для локальних мереж, для глобальних мереж, для кабельного телебачення і т.п.[2].

Будова коаксіального кабелю зображена на рисунку 1.7.

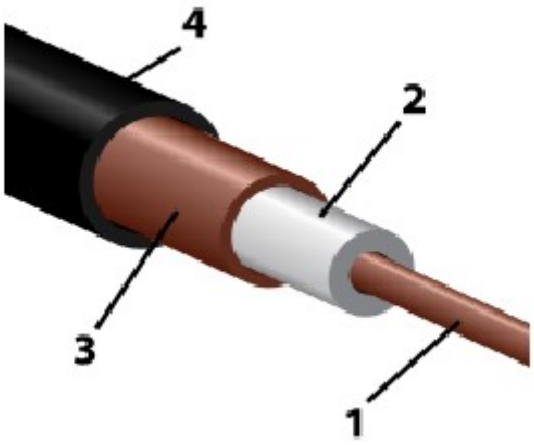


Рисунок 1.7 — Будова коаксіального кабеля

1 — Центральна жила.

2 — Внутрішня ізоляція.

3 — Металева оплітка.

4 — Зовнішня оболонка.

Донедавана широко застосовувався і був досить популярний через те, що має кращу завадозахищеність, ніж вита пара. Тако такий тип кабелю має більш широку смугу пропускання (більше 1 ГГц), До нього важче механічно підключитися для несанкціонованого прослуховування мережі, він дає також помітно менше електромагнітних випромінювань зовні[2]. Але монтаж і обслуговування такого кабелю більш складніші, ніж витої пари, вартість вища в 1,5 — 2 рази. Складніша і установка роз'ємів на кінцях кабелю. Через ці фактори зараз його застосовують рідше.

Волоконно-оптичний кабель (optical fiber) складається з тонких (5-60 мікрон) волокон, по яких поширюються світлові сигнали. Це найбільш якісний тип кабелю — він забезпечує передачу даних з дуже високою швидкістю (до 10 Гбіт/з і вище) і до того ж краще інших типів передавальної середовища забезпечує захист даних від зовнішніх перешкод. Будова волоконно — оптичного кабеля зображена на рисунку 1.8.

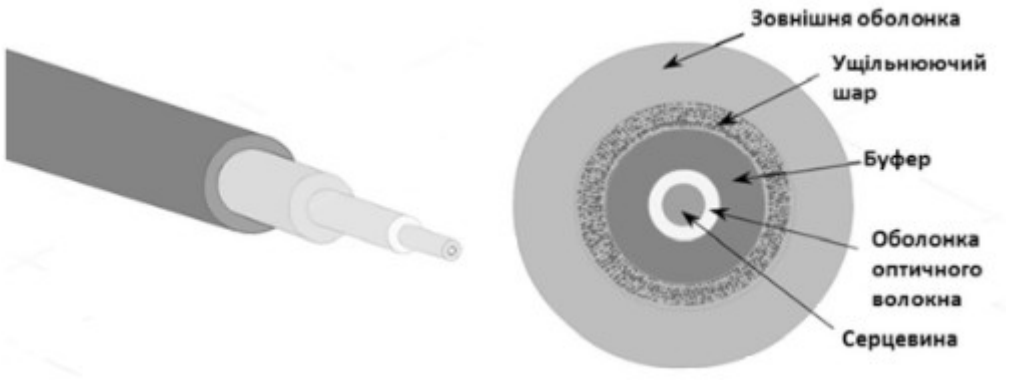


Рисунок 1.8 — Будова волоконно-оптичного кабеля

У центрі кабеля знаходиться серцевина — серидовище, по якому сигнали передаються у вигляді модульованих світлових імпульсів. Навколо серидовища розмщена оболонка з великим коефіцієнтом переломлення, завдяки чому промінь світла відбивається в серцевину ВОК. Це запобігає розсіюван ню світла при проходженні його по кабелю. Все це захищає зовнішня оболонка. Може бути виконана у вигляді броньованого плетіння зі сталі, чи пластику.

Оптоволоконні кабелі бувають 2-ох типів: одномодові та багатомодові.

Товщина жили в одномодовому кабелі відповідає довжині хвилі світлового сигналу (~10мкм), ослаблення сигналу незначне. Світло генерують напівпровідникові лазери. Максимальна швидкість передавання доходить до 200 Гбіт/с, а відстань передачі до 110 км.

У багатомодовому кабелі декілька жил, є можливість одночасно посилати кілька потоків даних. Відстань передачі до 2-3 км.

Оптоволоконний кабель має багато переваг: велика відстань передачі (сигнал у волокні майже не згасає), висока швидкість передачі даних, висока завадозахищеність (немає залежності від електромагнітних перешкод), захищеність від несанкціонованого підключення. Основними недоліками є висока вартість кабелю і обладнання для його підключення, а сам кабель є дуже чутливим і має погану гнучкість. Через ці фактори оптоволоконні кабелі використовують при створенні магістральних ліній зв’язку, де важлмва саме дальність зв’язкую.

Радіоканали наземного і супутникового зв'язку утворяться за допомогою передавача і приймача радіохвиль. Існує велика кількість різних типів радіоканалів, що відрізняються як використовуваним частотним діапазоном, 75 так і дальністю каналу. Діапазони коротких, середніх і довгих хвиль (КХ, СХ і ДХ), називані також діапазонами амплітудної модуляції (Amplitude Modulation, АМ) по типі використовуваного в них методу модуляції сигналу, забезпечують далекий зв'язок, але при невисокій швидкості передачі даних. Більш швидкісними є канали, що працюють на діапазонах ультракоротких хвиль (УКВ), для яких характерна частотна модуляція (Frequency Modulation, FM), а також діапазонах надвисоких частот (НВЧ чи microwaves)[2].

Кожен пристрій мережі оснащений антеною яка є одночасно і приймачем і передавачем електромагнітних хвиль, які поширюються у атмосфері або вакуумі зі швідкістю $3 * 10^8$ м/с.

Електромагнітний спектр має багато діапазонів. Є ділянки частотного діапазони, які виділили для використання пристроями, що не вимагають ліцензії наглядових органів. Це периферійні пристрої ПК, бездротові LAN, бездротові телефони. Такі пристрої працюють на частотних діапазонах 900 МГц, 2,4 ГГц, і 5 ГГц.

Для побудови бездротових локальних комп’ютерних мереж використовують технологію Wi – Fi. Це загальновживана назва для стандарту IEEE 802.11 передавання цифрових потоків даних по радіоканалах[2]. Стандарт IEEE 802.11n використовує смугу частот 2,4 ГГц. Також набирає популярність стандарт IEEE 802.11ax (Wi – Fi 6), який використовує смугу частот 5 ГГц.

1.3 Комунікаційні засоби мережі

Модель OSI/ISO є концепцією застосування відкритих стандартів, спрямованою на забезпечення сумісності між різними системами, що дозволяє мінімізувати кількість угод, які не мають безпосереднього відношення до організації самого з’єднання між системами. Перша версія стандартів моделі

OSI/ISO була випущена як стандарт X.200. Робота зі стандартизації моделі OSI/ISO, спільну участь у якій беруть ISO і ITU-T, триває до сьогодні[1].
Ця модель передбачає 7 рівнів, як показано у таблиці 1.1.

Таблиця 1.1 — Рівні моделі OSI

№ рівня	Українська назва	Англійська назва	Позначення рівня
7	Прикладний	Application	A
6	Представлення	Presentation	P
5	Сеансовий	Session	S
4	Транспортний	Transport	T
3	Мережевий	Network	N
2	Канальний	DataLink	DL
1	Фізичний	Physical Link	PL

На фізичному рівні описується як розміщуються біти інформації у серидовищі передачі даних. Це може бути вита пара, коаксіальний кабель, оптоволоконний кабель або радіоканал. На цьому рівні основними характеристиками є смуга пропускання, завадозахищеність, хвильовий опір та інше.Також реалізуються фізичні інтерфейси пристроїв з передавальним середовищем та пристроями, між якими виконується передавання бітів.

Канальний рівень відповідає за якість передачі інформації між двома вузлами мережі, які зв’язані фізичним каналом з урахуванням особливостей серидовища передачі даних. Якщо з’єднання встановлюється між двома кінцевими системами, не пов’язаними безпосередньо, то воно буде включати декілька незалежно функціонуючих фізичних каналів передачі даних. При цьому фізичні середовища передачі можуть відрізнятися (мідь, оптичне волокно, ефір). Несумісними можуть виявитися й вимоги до формату подання даних у кожному каналі, що називається лінійним кодуванням[1]. У такому випадку канальний рівень виконує функцію адаптайії даних до типу фізичного каналу зв’язку. Блок даних на канальному рівні називається кадром або фреймом. Іншою важливою функцією канального рівня є керування доступом

до каналу зв’язку, синхронізація кадрів, керування потоком даних, адресація, встановлення з’єднання та роз’єднання. Протоколи канадбного рівня:

1. HDLC – процедура управління ланкою даних верхнього рівня для послідовни з’єднань.

2. IEEE 802.2 – забезпечує управління логічним каналом, а також правління доступом до середовища передачі (MAC).

3. Ethernet (IEEE 802.3) – локальна мережа на основі протоколу CSMA/CD.

4. Token Ring (IEEE 802.5) – мережева архітектура з топологією «кільце»розроблена фірмою IBM і працююча зі швидкістю 4 Мбіт/с.

Мережевий рівень — це комплексний рівеь, який виконує найважливішу функцію телекомунікаційної мережі — забезпечує зв’язок між кінцевими пристроями мережі. Це забезпечується шляхом надання наскрізного каналу, який комутований з окремими ділянками відповідно до оптимально обраного маршруту, логічного віртуального каналу або безпосередньої маршрутизації блоку даних у процесі його доставки. Основною функцією мережевого рівня є маршрутизація. Вона полягає в прийнятті рішення, через які конкретно проміжні пункти повинен пройти маршрут передавання даних, які направляються з однієї кінцевої системи в іншу, та як має виконуватися комутація (яка відповідає конкретному маршруту) між входами та виходами мережевих пристроїв, розташованих у проміжних пунктах мережі[2]. Основними протоколами мережевого рівня є IPv4, IPv6, ICMP, IGMP, IPX.

Транспортний рівень заезпечує керуванням і безпомилкову передачу даних мід двома користувачами мережі. Чим вища складність протоколів транспортного рівня зворотно пропорційна надійності сервісів нижчерозташованих рівнів (мережевого, канального й фізичного). Це вимагає розбиття великих блоків данних на менші фрагменти, які називаються сегментами, оскільки мережевий рівень визначає максимальний розмір пакета, який називається максимальною одиницею передачі (MTU), і який залежить від максимального розміру пакета, що накладається всім каналом передачі даних.

Обсяг даних у сегментімає бути достатньо малим, щоб вмістити заголовок мережевого рівня та заголовок транспортного рівня. Транспортний рівень також контролює надійність заданого зв’язку між вихідним і кінцевим хостом за допомогою контрольного потоку, контролю помилок і підтвердження послідовності та існування. Транспортний рівень також забезпечить підтвердження успішної передачі даних і надсилає наступні дані, якщо не виявить помилок. Основні протоколи транспортного рівня: TCP, UDP, SCTP.

Сеансовий рівень створює, налаштовує, контролює та завершує з’єднання між двома чи більше хостами. Сеансовий рівень забезпечує виконання функцій керування сеансом зв'язку (сесією), орієнтованим на наскрізну передачу повідомлень, таких, наприклад, як встановлення й завершення сесії; керування черговістю й режимом передачі даних (симплекс, напівдуплекс, дуплекс); синхронізація; керування активністю сесії; складання звітів про надзвичайні ситуації. Разом із транспортним рівнем сеансів рівень формує протоколи, орієнтовані на встановлення з'єднання й протоколи, які забезпечують для вищих рівнів надійний сервіс без встановлення з'єднання[2]. Протоколи сеансового рівня: RPC, PAP, L2TP, gRPC.

Рівень представлення встановлює формат даних і перетворення даних у формат, визначений прикладним рівнем, а також зворотне перетворення. Забезпечує подання даних в узгоджених форматах і синтаксис і, трансляцію й інтерпретацію програм з різних мов, шифрування й стиснення даних. Протоколи рівня представлення: AFP, ICA, LPP, NCP, NDR, XDR, X.25 PAD.

Прикладний рівень — це рівень, який є найближчим до користувача і це означає, що користувач взаємодіє із додатком, в якому реалізована клієнт - серверна архітектура. Прикладом таких додатків є веб — браузер, сервіси електронної пошти, файл — сервер. Цей рівень надає сервіси безпосередньо для прикладних програмам користувачів, ідентифікує і встановлює наявність прикладних процесів, а також встановлює і погоджує процедури усунення помилок і управління цілісністю інформації [1].

Повторювачі (Repeaters) – виконують функцію відтворення сигналів і цим

дозволяють подовжити максимальну довжину кабельного сегменту. Сегменти Ethernet, з'єднані повторювачами, створюють єдине розділене середовище передачі або домен колізій, тобто в усіх сегментах вести передачу може тільки один пристрій. Мета такої ретрансляції сигналів складається виключно в збільшенні довжини мережі[2].

Концентратор (hub) – це багатопортовий повторювач. Через це він об'єднує всі пристрої в мережу.

Концентратори іноді втручаються в обмін, допомагаючи усувати деякі явні помилки обміну. У будь-якому випадку вони працюють на першому рівні моделі OSI, так як мають справу тільки з фізичними сигналами, з бітами пакету і не аналізують вміст пакету, розглядаючи пакет як єдине ціле. На першому ж рівні працюють і трансівери, і репітери.

На даний момент вважається застарілим, майже не використовується. Його замінили комутатори і маршрутизатори.

Рисунок 1.9 — Зовнішній вигляд концентратора

Мости (Bridges) також з'єднують сегменти мережі, але на відміну від повторювачів, мають певну логіку. Він, як і повторювач, відтворює сигнал, який надходить до нього. Але він також має можливість перевірити фізичну адресу, яка надходить у пакеті, на які діляться дані під час передачі. Мости передають лише ті пакети мережі, які потрібні в конкретному сегменті мережі. Для мостів є багато алгоритмів фільтрації пакетів. Мости ділять мережу на сегменти (підмережі). Таблиця моста спочатку порожня, але як тільки міст отримує і

передає вперед пакет, він створює в своїй таблиці вхід з вихідною адресою і інтерфейсом прибуття. З тих пір міст знає, від кого надходить кожен пакет, до якого пункту призначення, від якого інтерфейсу. Міст також робить запис інформації про пункт призначення, використовуючи інформацію, що міститься в пакеті. Міст зберігає таблицю відповідності між MAC-адресами пристроїв і номерами своїх портів, к яким підключені сегменти з даними пристроями[2].

Комутатор (Switch) використовує топологію типу "зірка", є пристроєм 2-го рівня і функціонально являє собою багатопортовий міст, до кожного порту якого може бути підключений окремий хост, концентратор, сервер або маршрутизатор[2].

Він здійснює сегментацію мережі (поділ мережі на підмережі). Також забезпечує механізм міжсегментного обміну інформації з високою швидкістю.

При підключенні до комктатора кінцевого пристрою мережі (робоча станція чи інше обладнання) встановлюється двобіний (дуплексний) режим зв’язку.

Комутатор має внутрішню таблицю MAC – адрес, де кожному порту присвоюється MAC – адреса підключеного до нього пристрою. Таку таблицю може створити адміністратор мережі , або вона може створюватись автоматично комутатором. За допомогою таблиці адрес і адрес одержувача, комутатор організує віртуальне з'єднання порту відправника з портом одержувача і передає пакет через це з'єднання.

Таблиця 1.2 — Таблиця MAC-адрес комутатора

MAC – адреса	Номер порта
A	1
B	2
C	3
D	4

На Рисунку 1.10 вузол A посилає пакет вузлу D. Коли комутатор знаходить адресу отримувача в своїй віртуальній таблиці, він передає пакет у

порт 4.

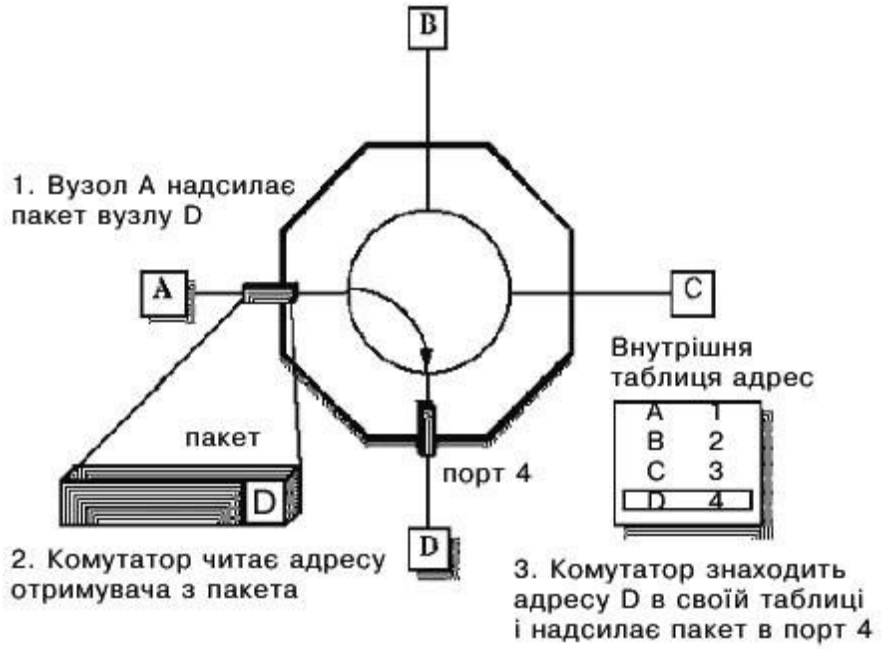


Рисунок 1.10 - Віртуальне з'єднання

Віртуальне з’єднання залишається на час передачі одного пакета, для кожного нового пакета віртуальне з'єднання організується знову на основі адреси, що міститься в даному пакеті.

Пакет надходить лише на той порт, до якого підключений адресат, інші користувачі (у нашому випадку — B і C) не отримують цей пакет. За допомогою такої технології комутатори забезпечують засоби безпеки, які недоступні для концентраторів та повторювачів.

Передача даних між будь — якими парами портів відбуваються незалежно, це означає, що для кожного віртуального з’єднання виділяється вся смуга пропускання каналу. Комутатор 10 Мбіт/с на Рисунку 1.11 забезпечує одночасну передачу пакета з A в D і з порту B порт C зі смугою 10 Мбіт/с для кожного з'єднання.

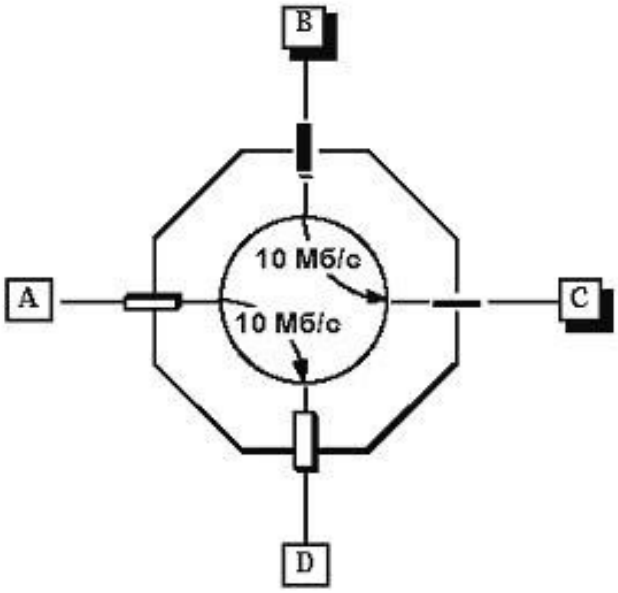


Рисунок 1.11 — Одночасне з’єднання

Для кожного з’єднання виділяється смуга пропускання 10 Мбіт/с, отже сумарна пропускна здатність комтатора, який приведено вище, складає 20 Мбіт/с. У випадку, коли дані передаються між більшим числом пар портів, смуга пропускання відповідно розширюється. Для прикладу, 48 портовий, 100 мегабітний комутатор Ethernet може забезпечувати сумарну пропускну здатність 2400 Мбіт/с.

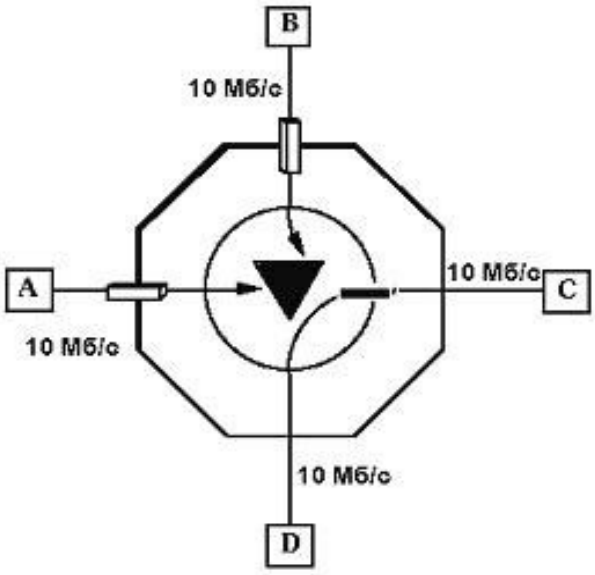


Рисунок 1.12 — Варіант блокування

Висока пропускна здатність комутатора забезпечується лише за умови,

коли організовано одночасне з'єднання між усіма парами портів. Але реальний трафік, як привило, представляє собою ситуацію «один до багатьох» (наприклад, багато користувачів мережі звертаються до одного сервера). У такому режимі роботи пропускна здатність комутатора, що наведено у прикладі, не буде перевищувати 10 Мбіт/с. За такого режиму роботи комутатор не матиме суттєвої переваги, порівняно з звичайним концентратором або повторювачем.

На рисунку 1.12 три вузли A, B і D передають дані вузлу C. Комутатор зберігає пакети від вузлів A і B у своїй пам'яті доти, доки не завершиться передача пакета з вузла D. Після завершення передачі пакета комутатор починає передавати пакети від вузлів A та B, які збереглися в пам'яті комутатора.

У даному випадку перепускна здатність комутатора визначається смугою каналу C (у даному випадку 10 Мбіт/с).

Одним з найважливіших параметрів є продуктивність комутатора. В якості параметрів продуктивності використовують такі показники:

1. Швідкість передвчі даних між портами.

2. Загальна пропускна здатність.

3. Затримка.

Швидкість передачі даних між портами. При смузі пропускання 10 Мбіт/с Ethernet може передавати 14880 пакетів мінімального розміру (64 байта) в секунду (PPS). Ця характеристика залежить від властивостей серидовища передаяі даних. У такому випадку можна сказати, що комутатор цілком використовує можливості серидовища, надаючи користувачам максимальну смугу пропускання.

Загальна пропускна здатність. Вимірюється в Мбіт/с або PPS і вказує, з якою максимальною швидкістю можуит передаватися пакети через коумутатор адресатам. Для прикладу, якщо усі порти комутатора мають максимальну швидкість 10 Мбіт/с, сумарна пропускна здатність дорівнює максимальній швидкості порту помноженої на число віртуальних з'єднань, що можуть існувати одночасно (число портів, поділене на 2). У комутатора, який здатний забезпечувати максимальну швидкість передачі, не має внутрішнього

блокування.

Затримка. Затримкою низивають часовий інтервал між між отриманням пакета від відправника і передачею його адресату. Затримку вимірюють щодо першого біта пакета. Через те, що адреса отримувача розміщена на початку пакета, комутатор Ethernet починає передачу до того, як пакет буде цілком прийнятий від відправника. Ця технологія має назву «комутація на льоту (cut-through)» і забезпечує мінімальну затримку. Це має велике значення, оскільки затримка напряму впливає на швидкодію комутатора. Але такий метод не передбачає перевірку пакетів на помилки, тому коли комутатор використовує такий метод, він передає усі пакети, включаючи ті, які мають помилки. Також комутацію на льоту неможливо використовувати при передачі пакетів з порту, який має низьку швідкість, у порт, який має більшу швидкість (наприклад з потру 10 Мбіт/с у порт 100 Мбіт/с). Якщо не застосувати буферизацію пакетів, виникатимуть помилки.

Мала затримка підвищує продуктивність мереж, у яких дані передаються у виді послідовності окремих пакетів, кожний з який містить адресу одержувача. У мережах, де дані передаються у формі послідовності пакетів з організацією віртуального каналу, мала затримка менше впливає на продуктивність.

Маршрутизатори (Routers) — це пристрій, який з’єднує між собою мережі з різними мережними адресами. Він працює на трьох рівнях моделі OSI. На фізичному рівні він відновлює отриманий сигнал. На канальному рівні аршрутизатор перевіряє фізичні адреси (джерело і пункт призначення), що містяться в пакеті. На мережевому рівні маршрутизатор еревіряє адреси мережевого рівня (адреси в рівні IP).

Функції, які може виконувати маршрутизатор:

1. З’єднувати локальні мережі.

2. З’єднувати разом мережі загального призначення.

3. Підключати локальні мережі до мереж загального призначення.

Є три головні відмінності між маршрутизатором з ретранслятором або мостом:

1. Маршрутизатор має фізичний і логічний (IP) адреса для кожного з його інтерфейсів

2. Маршрутизатор діє тільки на тих пакетах, в яких адреса одержувача відповідає адресі інтерфейсу, куди пакет прибуває. Це вірно для односпрямованої, групової або широкомовної адреси 132

3. Маршрутизатор змінює фізичну адресу пакета (і джерело, і пункт призначення), коли він передає пакет вперед[2].

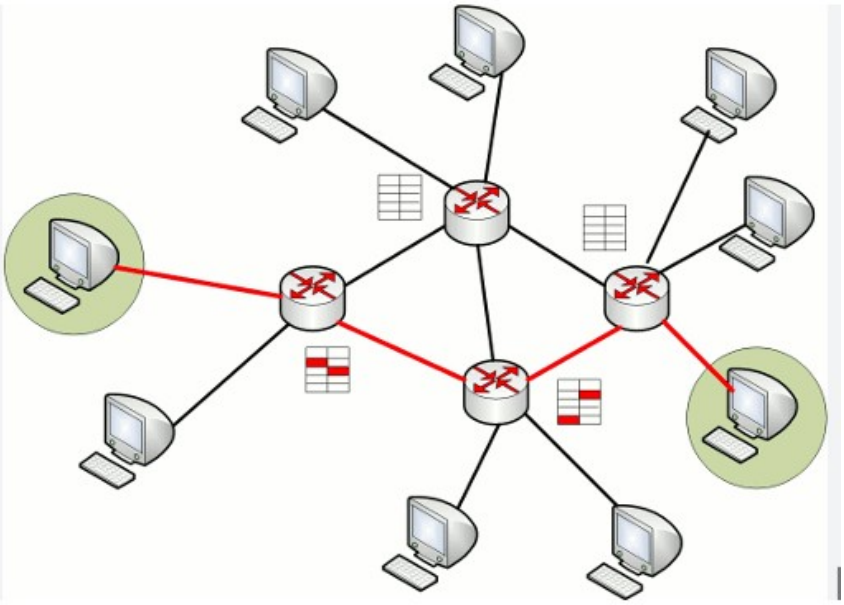


Рисунок 1.13 — Схема мережі з використанням маршрутизаторів

На відміну від моста/комутатора, який не володіє інформацією про те, як зв'язані сегменти мережі за межами його портів, маршрутизатор аналізує всі існуючі зв'язки підмереж, тому він може вибрати оптимальний за деяким критерієм маршрут при наявності декількох альтернативних маршрутів. Рішення про вибір того чи іншого маршруту приймається кожним маршрутизатором, через який проходить пакет.

Робота маршрутизаторів залежить від мережних протоколів і визначається зв'язаною з протоколом інформацією, переданої в пакеті.

Мережевий шлюз (Рисунок 1.14) – пристрій для об’єднання мереж, які використовують різні стеки протоколів або окремі протоколи. Шлюз може працювати на всіх рівнях моделі ISO/OSI. Шлюзи використовуються для зв’язку

систем, які використовують різні структури і формати даних, кодування, мають різну архітектуру[2].

В залежності від призначення, шлюз може використовувати всі рівні моделі OSI, а може обмежитися декількома або одним.

Рисунок 1.14 — Зовнішній вигляд мережевого шлюзу

Мережевий адартер (мережевий контролер, інтерфейс) — це інтерфейс, основною функцією якого є з’єднання комп’ютера(або іншого пристрою) з мережею і утворення каналу зв’зку. Він працює на першому та другому рівні моделі OSI.

Мережевий адаптер може бути виконаний у вигляді окремої плати розширення, яка монтується у слот PCI або PCI – e або бути інтегрованим у системну плату комп’ютера або іншого пристрою мережі. Сучасні системні плати комп’ютерів мають інтегрований мережевий інтерфейс, який підтримує швидкість передачі даних до 1 Гбіт/с. Мережевий адаптер взаємодіє як із системною шиною комп’ютера (пізнання своєї магістральної адреси, пересилання даних в комп'ютер і з комп'ютера, вироблення сигналу переривання процесора і т.д.), так і забезпечує функції спілкування з мережею.

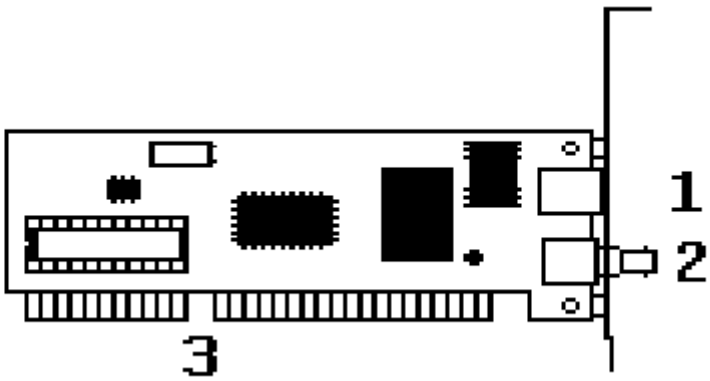


Рисунок 1.15 — Схема мережевої карти

1 — роз’єм RJ – 45 (для витої пари);

2 — роз’єм коаксіального кабелю;

3 — роз’єм слоту PCI.

2 ПРОЕКТУВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

2.1 Вихідні дані на проектування

Вихідні дані для проектування комп’ютерної мережі наведені у таблиці 2.1.

Мережа повинна складатися із трьох підмереж (VLAN):

1. Відділ технічної підтримки.
2. IT – відділ.
3. Конструкторський відділ.

Таблиця 2.1 — Вихідні дані для проектування.

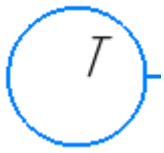
Технології	Кількість поверхів	Площа кімнат [м^2]	Кімнат на поверсі	Комп'ютерів у кімнаті	Організація коридору *
100Base – TX,	3	30	4	10	1 * 3.5 м

2.2 Фізична модель мережі

Фізична модель мережі показує як розташовуються станції (комп'ютери) в межах поверхів. Також слід передбачити розміщення та з'єднання мережного обладнання. Для цього створено умовні плани поверхів зі з'єднаннями в межах поверху, та загальний план будівлі зі з'єднаннями між поверхами. На планах також слід дотримуватись відповідності масштабу для певних елементів.

Умовні позначення елементів мережі на схемі показано у таблиці 2.2.

Таблиця 2.2 — Умовні позначення на планах.

	робоча станція, що відповідає одному робочому місцю в мережі
	комутатор

	набір всіх ліній, що йдуть від терміналів до концентратора, тобто вони не з'єднуються в одну, а просто використовують суміжний простір кімнати для свого прокладання

На рисунку 2.1 зображено умовний план поверху будівлі, в якій прокладається комп’ютерна мережа.

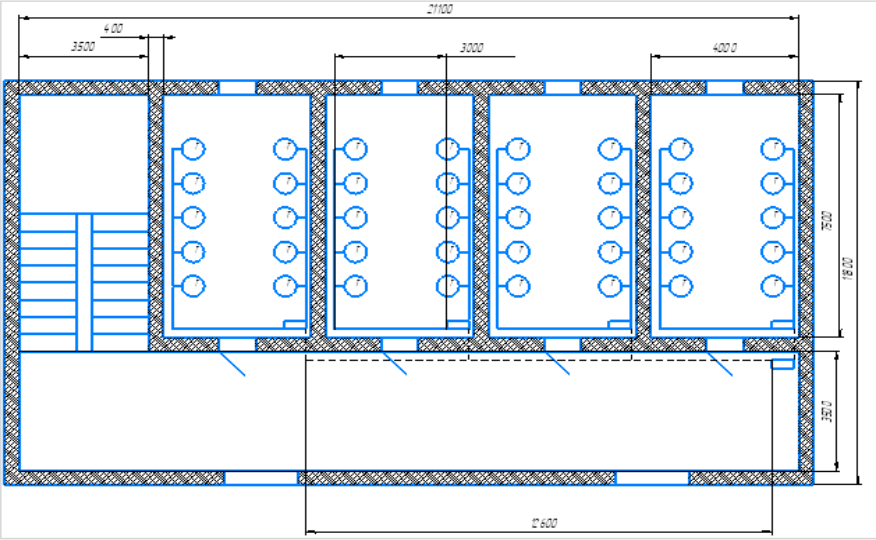


Рисунок 2.1 — Фізична модель поверху

На рисунку 2.2 показані розрізи відповідних поверхів. Представлені кімнати з розташуванням в них станцій. Відповідно до умовних графічних позначень, що описані вище, на рисунках представлені всі зв'язки мережі, всі пристрої, що забезпечують функціонування мережі та зв'язки, що йдуть до інших поверхів.

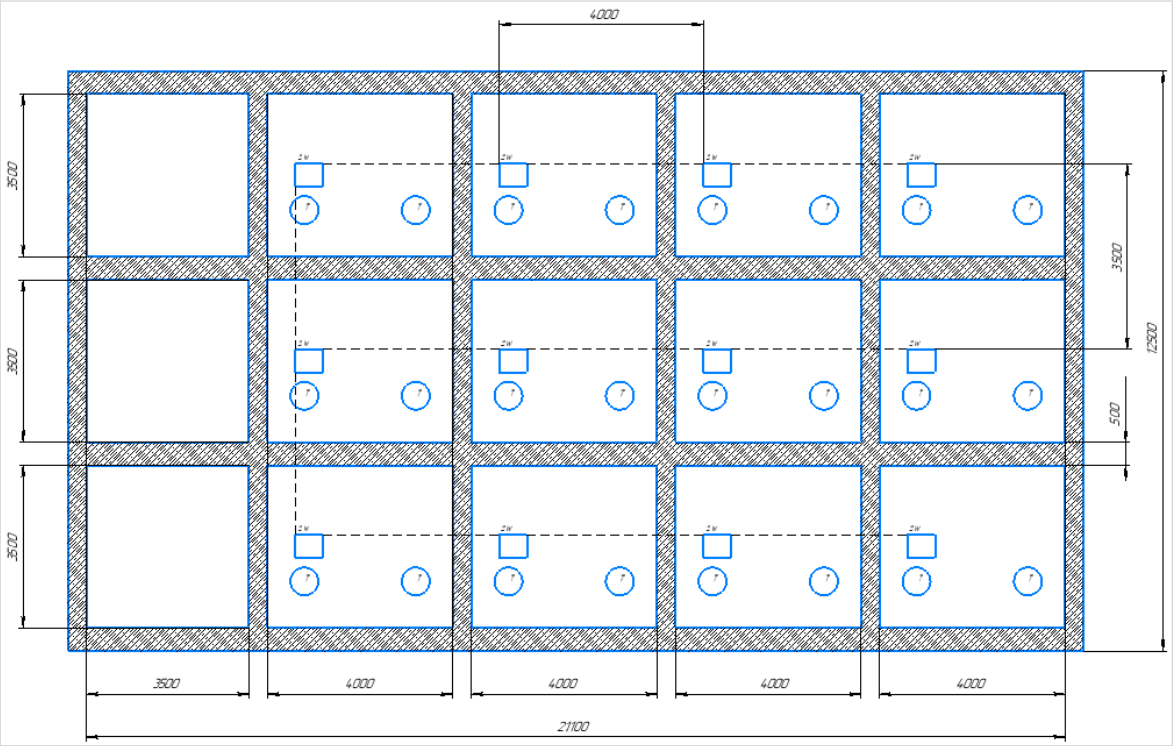


Рисунок 2.2 — Фізична модель у розрізі

Пропорційно вимірам представлені робочі місця (кружечки), концентратори та комутатори. Це обумовлене тим, що нам необхідно лише "точне" значення довжини з'єднань між вузлами і правдиві розміри робочого місця та кімнат, а комутатори та концентратори повинні демонструвати всі під'єднані до них лінії.

Окремо слід виділити перший поверх (рисунок 2.3), оскільки там буде знаходитись головний маршрутизатор та файл — сервер (FTP – server).

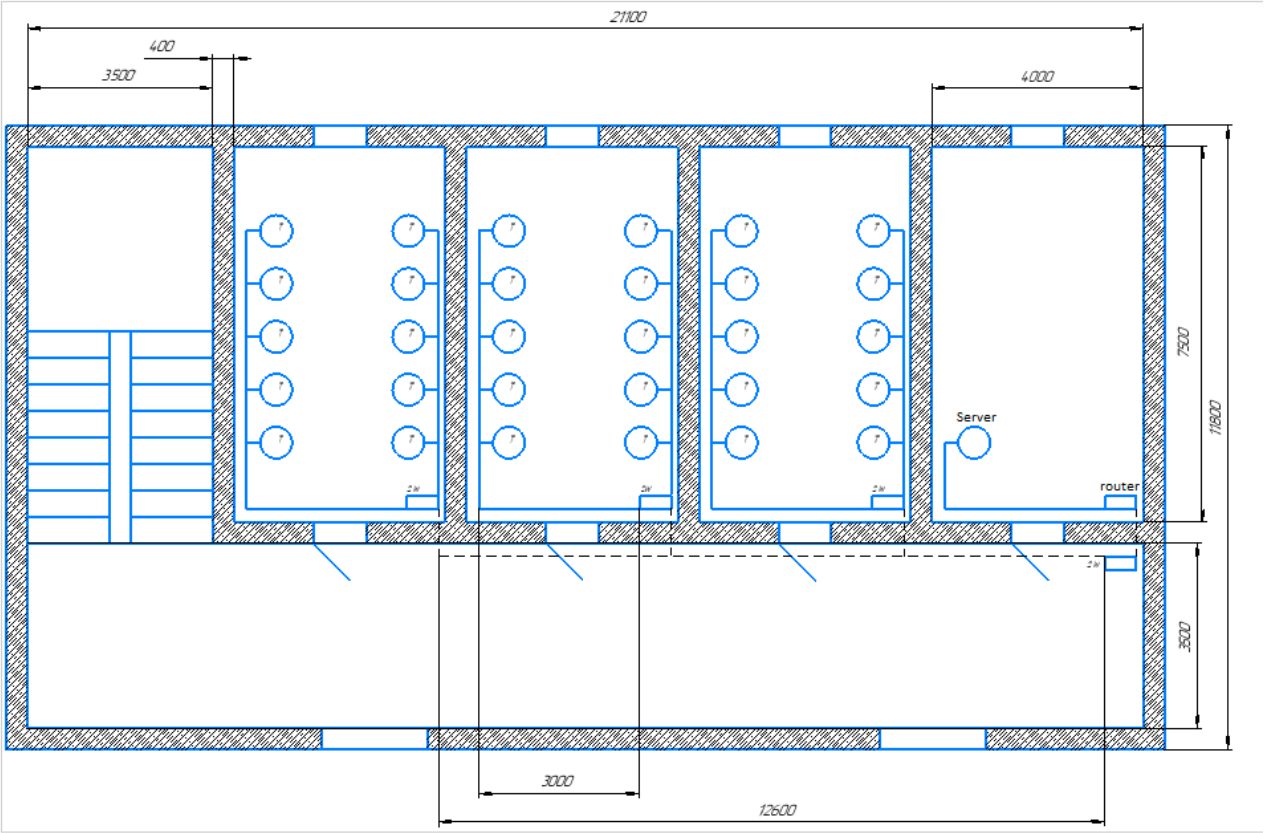


Рисунок 2.3 — Фізична модель першого першого поверху

2.3 Логічна модель мережі

Логічна модель комп’ютерної (рисунок 2.4) мережі відображає шлях проходження інформації по мережі. Тому на ній, як правило, вказуються підмережі (VLAN, маски, адреси), мережеві пристрої, такі як маршрутизатори та комутатори, а також протоколи маршрутизації.

В рамках моделі взаємодії відкритих систем (OSI) інформація на логічній моделі мережі відповідає інформації 3-го рівня моделі OSI. Третій рівень OSI (мережевий рівень) — це рівень абстракції, який відображає те, як відбувається пересилання пакетів через проміжні маршрутизатори. На другому рівні представлені канали передачі даних між сусідніми вузлами, а на першому рівні — тільки їх фізичне розташування.

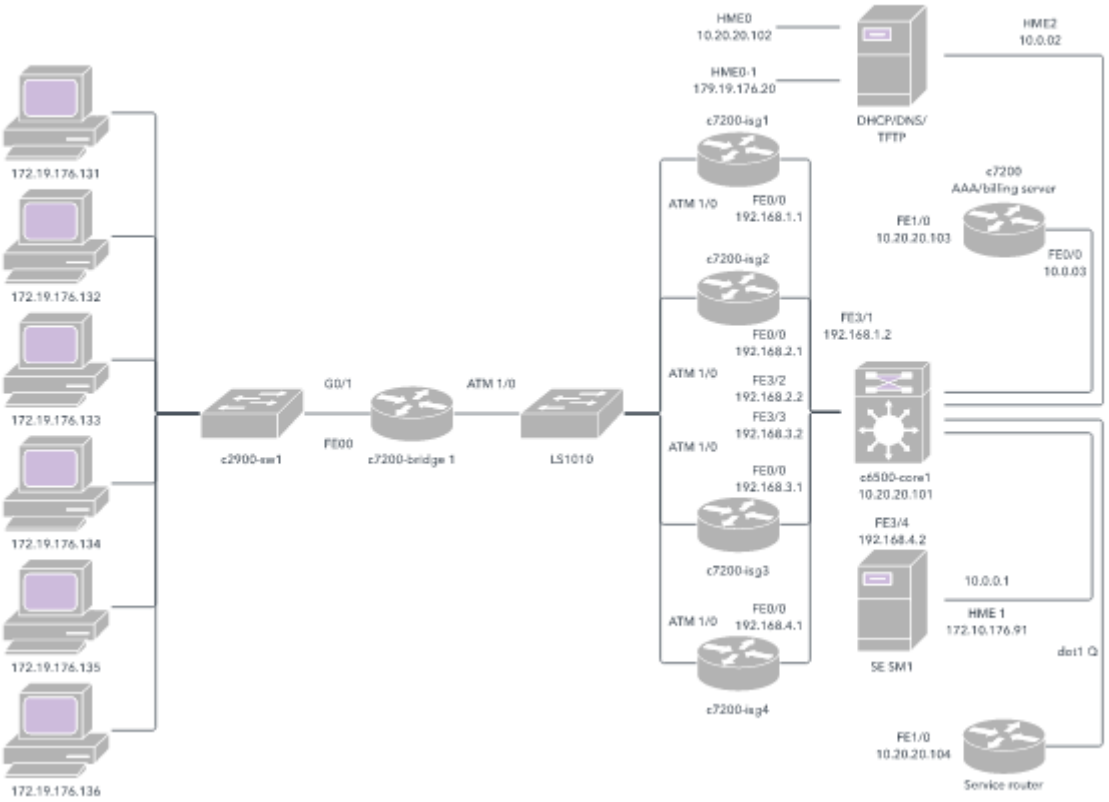


Рисунок 2.4 — Приклад логічної моделі мережі.

Логічна модель мережі буде створюватися за допомогою симулятора передачі даних Cisco Pocket Tracer.

Cisco Pocket Tracer — це симулятор передачі даних, розроблений фірмою Cisco Systems. Він дозволяє створювати працездатні моделі мереж, налаштовувати (командами Cisco IOS) маршрутизатори та комутатори, взаємодіяти між декількома користувачами (через «хмару»).

Pocket Tracer дозволяє проектувати складні та великі мережі, що, найчастіше, неможливо з фізичним обладнанням через великі грошові затрати.

Cisco IOS (Internetwork Operating System) — програмне забезпечення, яке використовується маршрутизаторами та мережевими комутаторами Cisco. Cisco IOS представляє собою багатозадачну операційну систему, яка виконує функції мережевої організації, маршрутизації, комутації та передачі даних.

В Cisco IOS є інтерфейс командного рядка. Інтерфейс пропонує набір багатослівних команд згідно вибраному режиму і рівню привілейованості користувача. Режим глобального конфігурування (Global configuration mode)

надає можливість для зміни налаштувань системи та мережевих інтерфейсів. Всім командам надається певний рівень привілеїв від 0 до 15, і до них можуть звертатися тільки користувачі з відповідним рівнем привілеїв. Через командний інтерфейс можна визначити доступні команди для кожного рівня.

2.4 Побудова логічної моделі мережі

Як зазначалося у попередньому розділі, моделювання роботи телекомунікаційної мережі буде проводитися у середовищі симуляції передачі даних Cisco Pocket Tracer.

Розпочнемо побудову моделі з встановлення головного маршрутизатора мережі (рисунок 2.5). Він буде керувати пересиланням пакетів між різними сегментами мережі, а також надавати IP – адреси пристроям локальної мережі за допомогою технології DHCP, а також виконувати функції DNS — сервера.

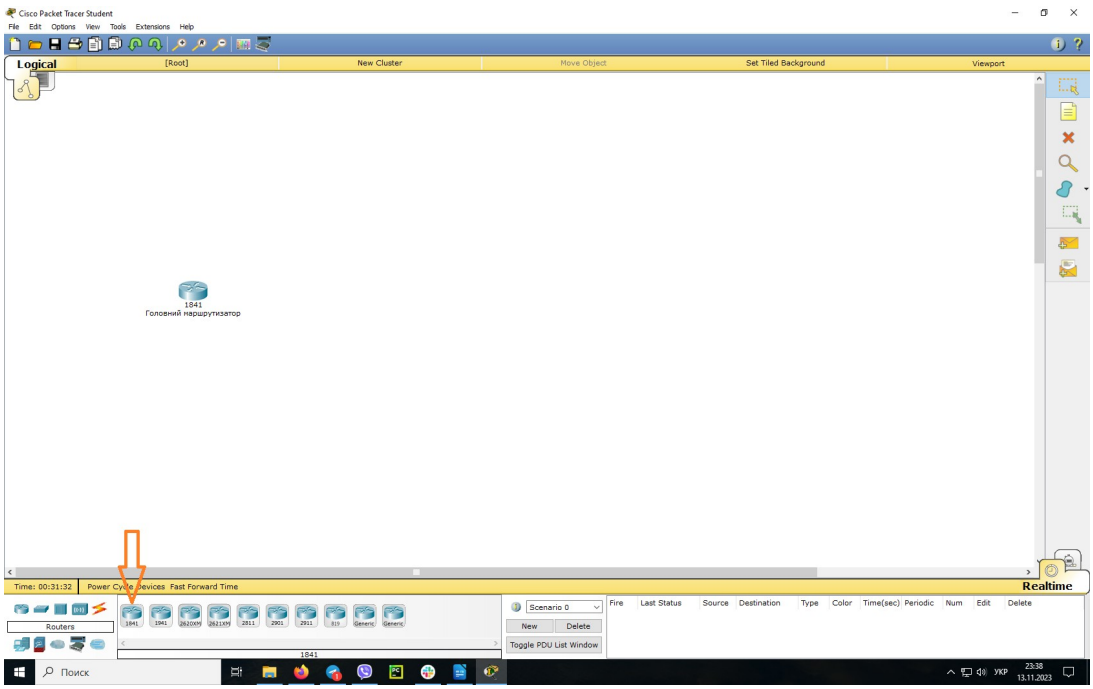


Рисунок 2.5 — Встановлення головного маршрутизатора

Так, як мережа займає три поверхи, додаємо три комутатори, по одному для кожного з поверхів. Вони будуть послідовно з’єднані з маршрутизатором

(рисунок 2.6). Назва маршрутизатора відповідатиме назві підмережі, за яку він буде відповідати.

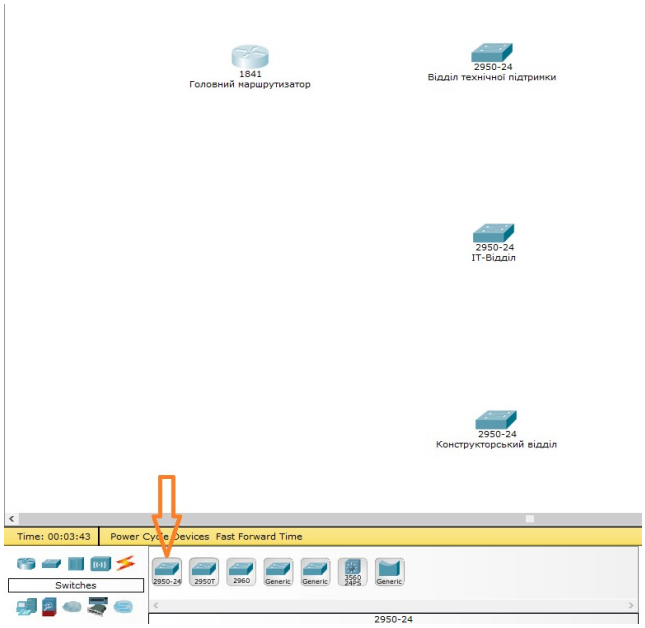


Рисунок 2.6 — Встановлення комутаторів для відділів

Виконуємо послідовне з’єднання комутаторів між собою та головним маршрутизатором (рисунок 2.7). Для цього використаємо перехресний кабель (крос — кабель) — це тип кабелю Ethernet, який виконує перехресне з’єднання сигналів прийому та передачі. Найчастіше він використовується для з’єднання однотипних пристроїв один з одним, наприклад двох хабів або двох мережевих комутаторів. Для з’єднання пристроїв різного типу, наприклад комутатора та маршрутизатора або комп’ютера та комутатора використовують прямий кабель.

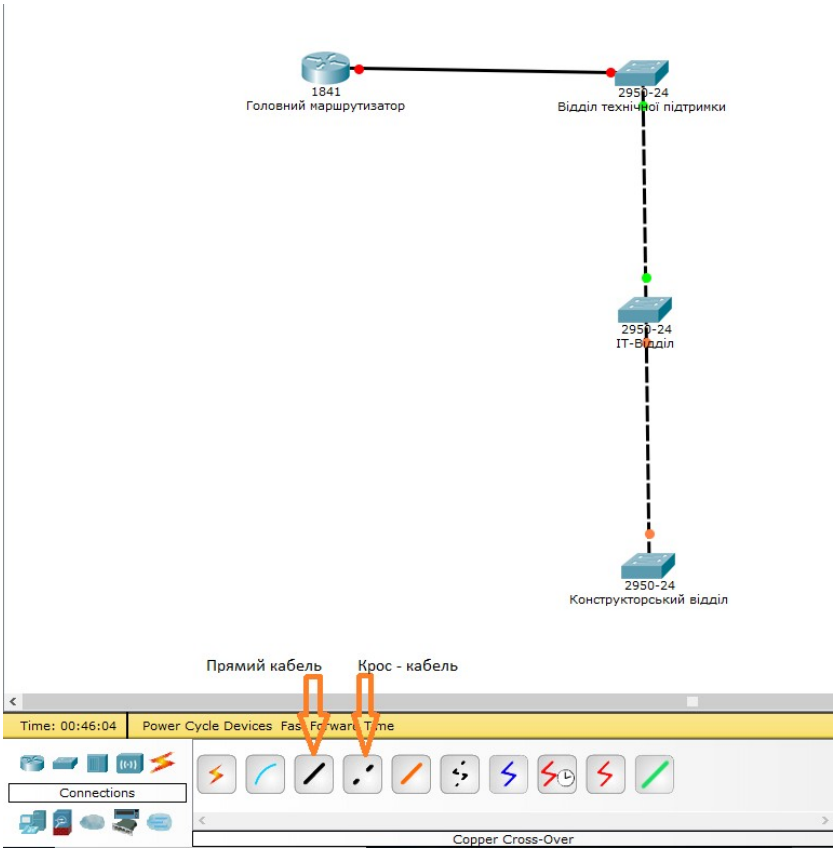


Рисунок 2.7 — З’єднання комутаторів і маршрутизаторам

Оообов’язковою умовою є наявність у мережі файл — сервера для зберігання даних, куди працівники підприємства зможуть завантажувати резервні копії важливих даних. Файл — сервер працюватиме за протоколом FTP.

FTP (File Transfer Protocol) – один з найстаріших протоколів Internet. Обмін даними в FTP проходить по TCP — каналу і побудований за технологією «клієнт — сервер» (рисунок 2.8).

В FTP підключення ініціюється інтерпретатором протоколу користувача. Керування обміном даними виконується по каналу керування в стандарті протоколу Telnet. Команди FTP генеруються інтерпретатором протоколу користувача і передаються на сервер. Відповіді сервера надсилаються користувачу також по каналу керування.

Команди FTP визначають параметри каналу передачі даних і сам процес передачі. Вони також визначають і характер роботи з віддаленою і локальною

файловими системами.

Сесія керування ініціалізує канал передачі даних. При організації каналу передачі даних послідовність дій відрізняється від тої, що відбувається під час організації каналу керування. В цьому випадку сервер ініціює обмін даними у відповідності з параметрами, які були узгоджені під час сесії керування.

Канал передачі даних встановлюється для того самого хоста, що і канал керування, через який відбувається налаштування каналу даних. Канал даних може використовуватися як для прийому, так і для передачі інформації.

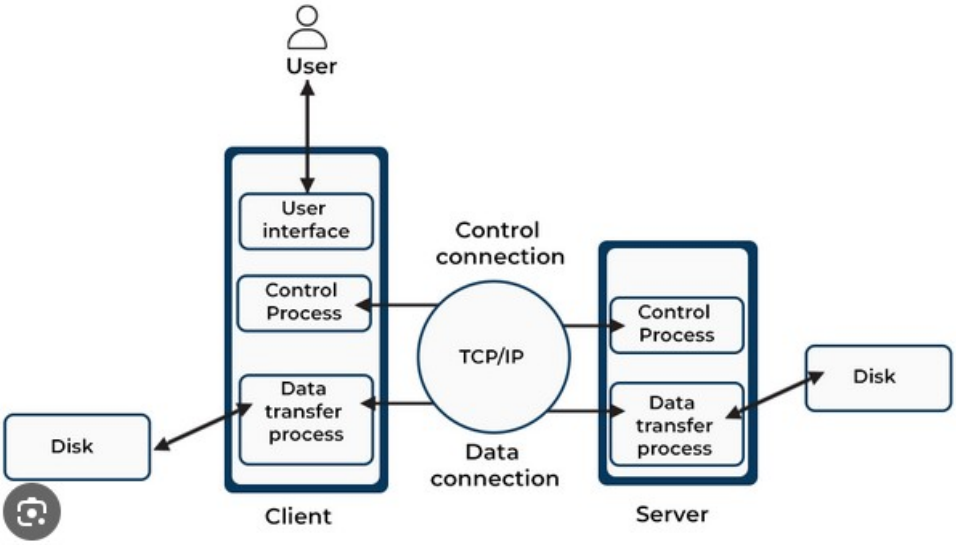


Рисунок 2.8 — Модель протоколу FTP

Можлива ситуація, коли дані можуть передаватися на третій пристрій мережі. У цьому випадку користувач організує як канал керування двома серверами, так і прямий канал даних між ними. Команди керування йдуть через машину користувача, а дані — напряму між серверами.

Канал керування повинен бути відкритий при передачі даних між пристроями. У випадку його закриття передача даних завершується.

Вибираємо сервер у розділі «End devices» і підключаємо його до маршрутизатора (рисунок 2.9).

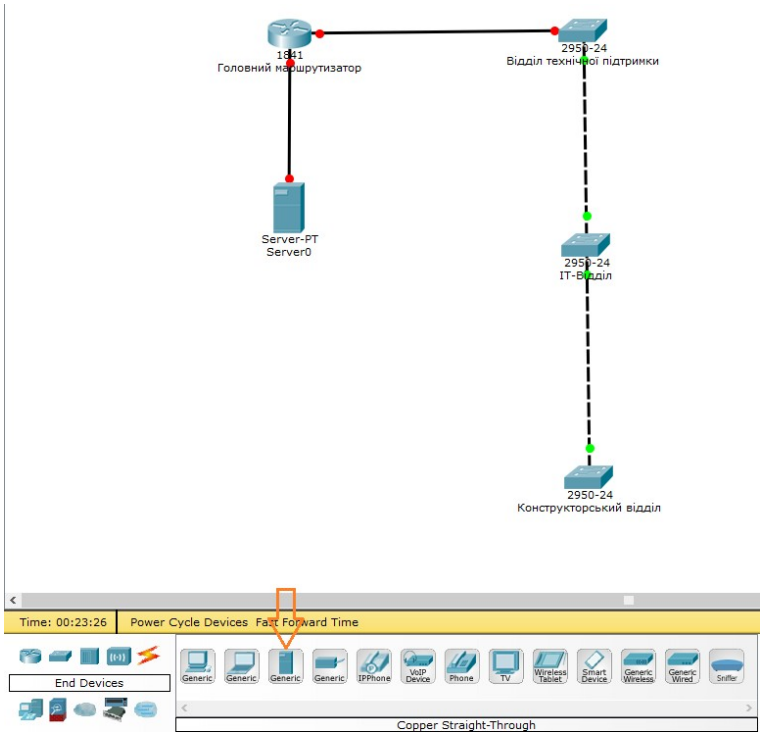


Рисунок 2.9 — Підключення сервера до мережі

Для того, щоб сервер працював у режимі FTP, у розділі «Services» треба вибрати пункт «FTP» і встановити його у режим «On». Всі інші режими треба переключити у положення «Off». У розділі «User Setup» додаємо користувачів і надаємо їм відповідні права (рисунок 2.10). Список користувачів наведено у таблиці 2.3.

Таблиця 2.3 — Список користувачів для FTP — сервера.

Ім’я користувача	Пароль	Режими роботи
User	user	Write (запис), read (читання), list (вивід вмісту каталогів)
Admin	admin	Write (запис), read (читання), delete (видалення), rename (перейменування), list (вивід вмісту каталогів)

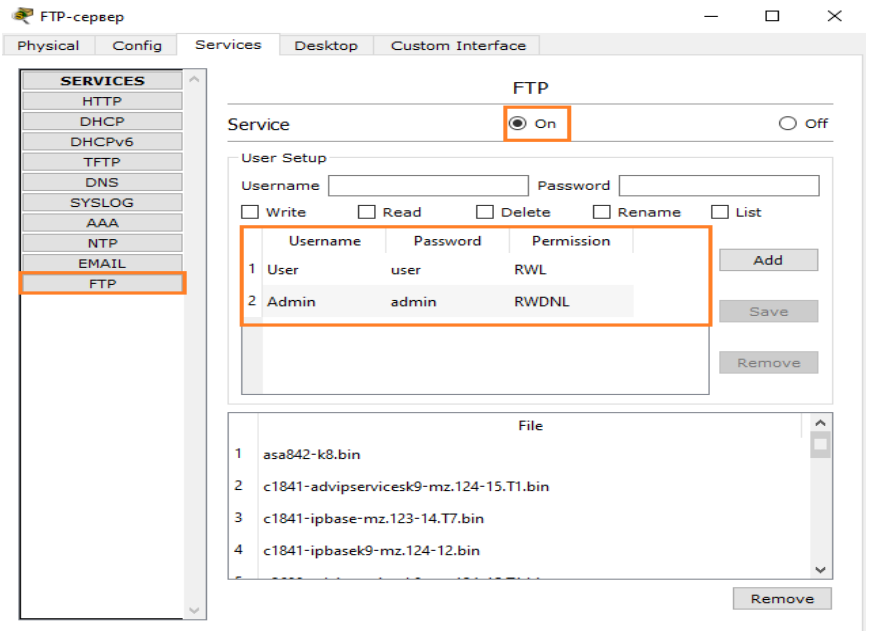


Рисунок 2.10 — Налаштування FTP – сервера

Наступним кроком буде призначення серверу статичної IP – адреси. IP – адреса представляє собою 4 — байтову послідовність, кожен байт цієї послідовності записується у вигляді десяткового числа. Адреса складається з двох частин: адреси мережі і номер хоста. Під поняттям «хост» розуміють комп'ютер, але це може бути і принтер з мережевою картою, термінал або будь — який пристрій, який має власний мережевий інтерфейс.

Існує декілька класів IP – адрес, які відрізняються один від одного кількістю біт, відведених для адреси мережі і адреси хоста в мережі. У таблиці 2.4 показана класифікація IP – адрес.

Таблиця 2.4 — Класи IP – адерс

Клас IP – адреси	Найменша адреса	Найбільша адреса	Кількість хостів для класу
Class A	1.0.0.0	126.255.255.255	Приблизно 16 мільйонів хостів
Class B	128.0.0.0	191.255.255.255	16320 мереж з 65024 хостами у

			кожній
Class C	192.0.0.0	223.255.255.255	Близько 2 мільйонів мереж з 254 хостами у кожній
Class D, E	224.0.0.0	254.0.0.0	Є дослідними

Спочатку треба призначити IP – адресу порту маршрутизатора, до якого підключений FTP — сервер. Для цього на головному маршрутизаторі треба зайти у розділ «CLI» і увійти в привілейований режим за допомогою команди «enable». Далі входимо у режим глобального конфігурування за допомогою команди «config terminal». Обираємо інтерфейс, який з'єднує маршрутизатор та сервер (в даному випадку це інтерфейс Ethernet 0/0/0) командою «interface Ethernet0/0/0». Наступними командами виконуємо налаштування інтерфейсу:

1. no shutdown – зробити інтерфейс активним;

2. ip address 128.96.10.1 255.255.0.0 – призначаємо інтерфейсу IP – адресу 128.96.10.1 та маску підмережі 255.255.0.0

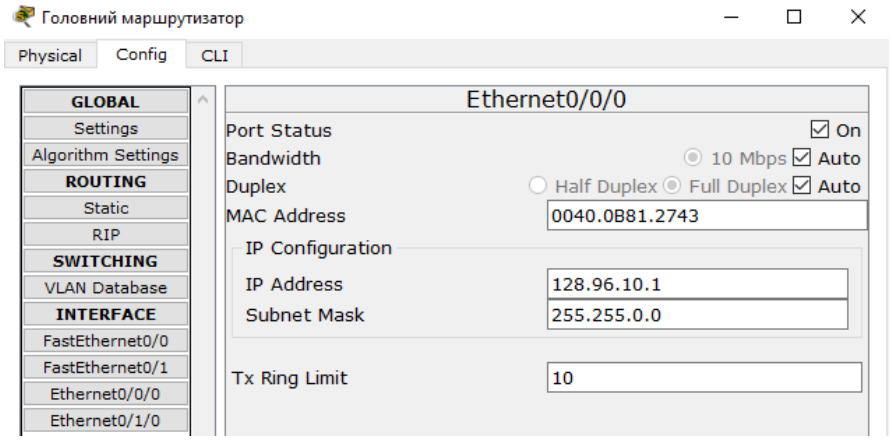


Рисунок 2.11 — Налаштування інтерфейсу Ethernet 0/0/0

Тепер призначаємо IP – адресу самому FTP – серверу. Щоб це зробити,

потрібно в налаштуваннях сервера перейти у розділ «Desktop». У ньому буде пункт «IP Configuration», в ньому прописуємо IP – адресу нашого серверу та маску підмережі. У параметрі «Default Gateway» вказуємо адресу інтерфейсу роутера, до якого під'єднаний сервер (рисунок 2.12).

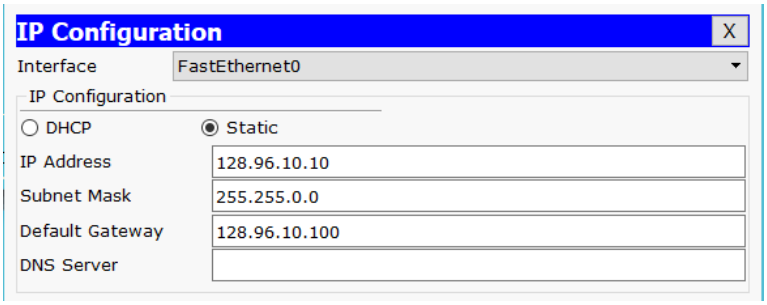


Рисунок 2.12 — Призначення адреси серверу

Наступним кроком буде розширення логічної моделі відповідно до вимог завдання магістерської роботи. Середовище розробки Cisco Pocket Tracer дозволяє для зручності виділити кольорами різні частини однієї мережі. Як зазначалося раніше, мережа, яка проектується в рамках магістерської роботи, складається із трьох підмереж:

1. Підмережа конструкторського відділу: 30 робочих станцій, 3 комутатори.

2. Підмережі IT – відділу: 40 робочих станцій, 4 комутатори.

3. Підмережа відділу технічної підтримки: 40 робочих станцій, 4 комутатори.

Окремо слід виділити серверну, де знаходиться маршрутизатор та FTP – сервер.

Розпочнемо розширення моделі з побудови підмережі конструкторського відділу. Для цього потрібно розмістити три комутатори (один комутатор на одну кімнату) , які знаходяться у розділі «Switches». До кожного комутатора підключаємо 10 робочих станцій, які можна знайти у розділі «End Devices» → «Laptop – PT» або «PC – PT». З'єднуємо комутатори з основним комутатором поверху за допомогою кросового кабелю. Підключаємо робочі комп'ютери з комутаторами прямим кабелем. Відмічаємо відповідними кольорами підмережу серверної та конструкторського для того, щоб зробити модель більш детальною

(рисунок 2.13).

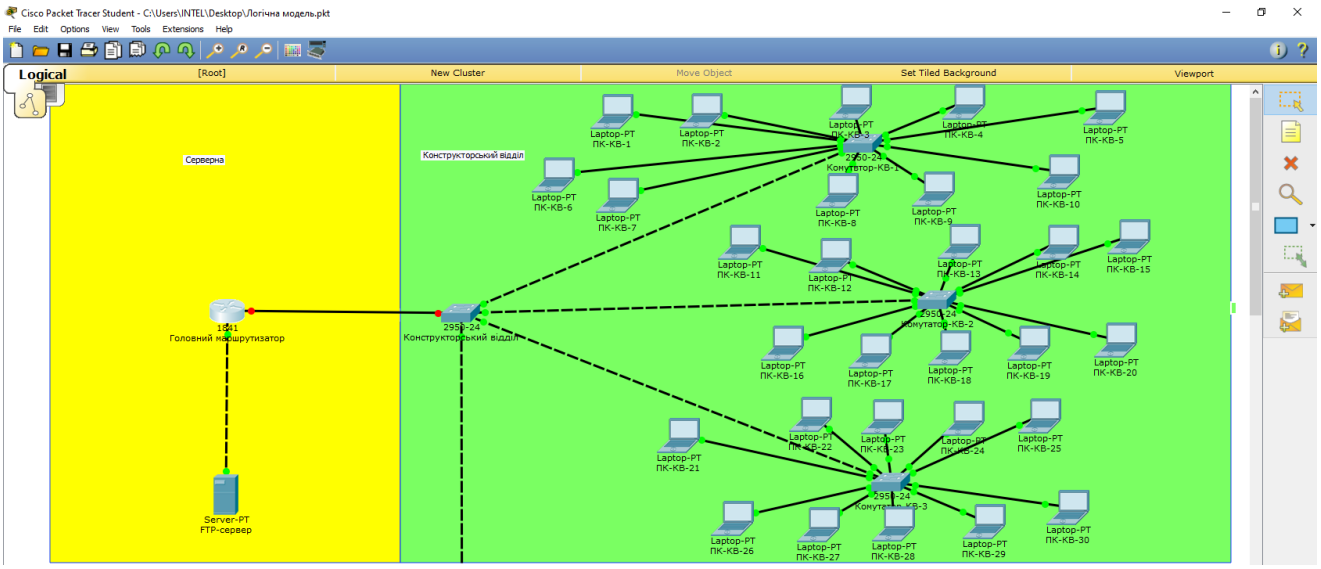


Рисунок 2.13 — Підмережа конструкторського відділу та серверна

За допомогою такого ж алгоритму додаємо до моделі IT — відділ (рисунок 2.14) та відділ технічної підтримки (рисунок 2.15). Вони відрізняються від конструкторського відділу лише тим, що мають більшу кількість комутаторів і робочих станцій.

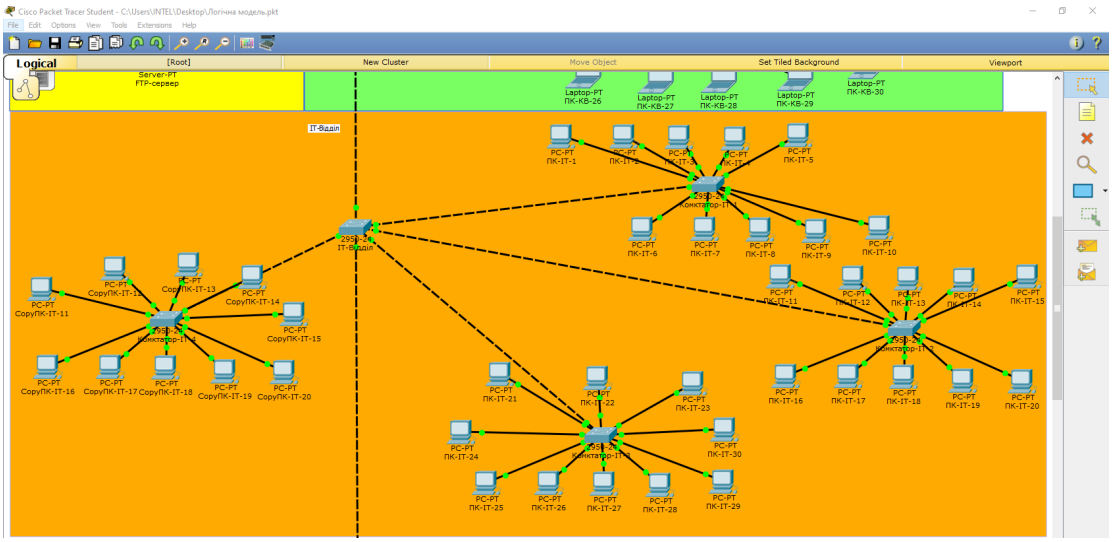


Рисунок 2.14 — Підмережа IT — відділу

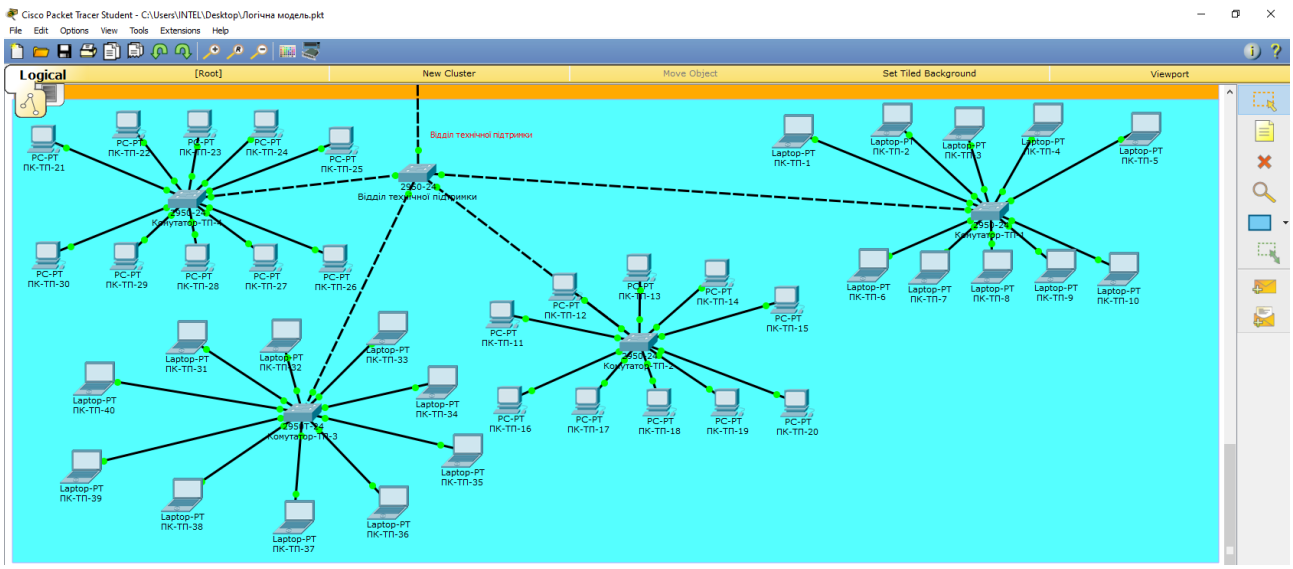


Рисунок 2.15 — Підмережа відділу технічної підтримки

2.4 Розподіл мережі на підмережі та налаштування динамічної IP – адресації

Як зазначалося вище, основною функцією логічної моделі мережі є демонстрація, як передається інформація в межах мережі. Оскільки мережа, яка розробляється, повинна охоплювати декілька відділів підприємства, в рамках забезпечення інформаційної безпеки, слід розділити відділи так, щоб вони не мали доступу один до одного. Це можна реалізувати за допомогою технології віртуальних локальних мереж (VLAN).

Віртуальна локальна мережа — це група вузлів мережі, трафік якої на канальному рівні повністю ізольований від інших вузлів мережі. Це означає, що передача кадрів між різними віртуальними мережами на основі адреси канального рівня незалежно від типу адреси — унікального, групового чи широкомовний. Однак всередині віртуальної мережі кадри передаються за технологією комутації, а точніше на той порт, який пов’язаний з адресою призначення кадру. В той же час віртуальні мережі можуть пересікатися, якщо один або декілька хостів входять до складу більше ніж однієї віртуальної мережі.

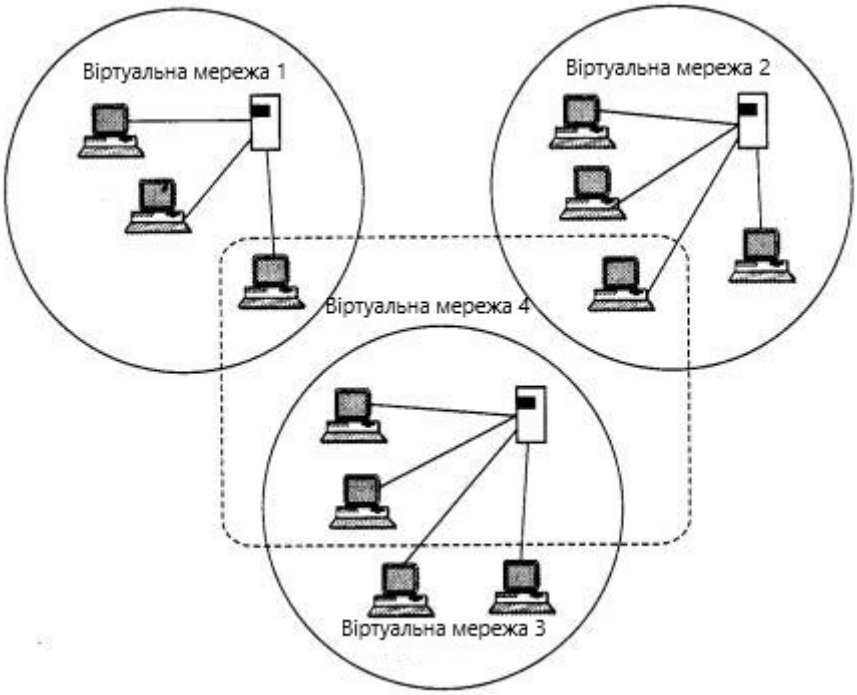


Рисунок 2.16 — Схема взаємодії віртуальних мереж

На рисунку 2.16 сервер електронної пошти входить до складу третьої і четвертої віртуальної мережі. Це означає, що його кадри передаються комутаторами всім комп'ютерам, які входять в ці підмережі. Але якщо якийсь комп'ютер входить до складу лише віртуальної мережі 3, то його кадри до мережі 4 доходити не будуть, але він може взаємодіяти з комп'ютерами віртуальної мережі 4 через спільний поштовий сервер. Така схема не повністю захищає віртуальні мережі.

Технології віртуальних мереж призначені для полегшення процесу створення ізольованих мереж, які потім повинні зв'язуватися за допомогою маршрутизаторів, які реалізують протоколи мережевого рівня, наприклад IP. Такий спосіб побудови створює набагато більш складні перешкоди на шляху помилкового трафіку із одної мережі в іншу. На сьогоднішній день вважається, що будь-яка велика комп'ютерна мережа повинна включати в себе маршрутизатори, інакше потоки помилкових кадрів будуть періодично перевантажувати всю мережу через прозорі для них комутатори, роблячи мережу непрацездатною.

Технологія VLAN створює гнучку і масштабовану основу для побудови великих мереж, об’єднаних маршрутизаторами, оскільки комутатори дозволяють створювати повністю ізольовані сегменти програмним шляхом, не використовуючи фізичну комутацію.

До того, як з’явилася технологія віртуальних локальних мереж, для побудови окремої мережі або фізично ізольовані сегменти коаксіального кабелю, або не пов’язані між собою сегменти, побудовані з використанням повторювачів і мостів. Потім ці сегменти зв’язувалися маршрутизаторами в єдину мережу (рисунок 2.17).

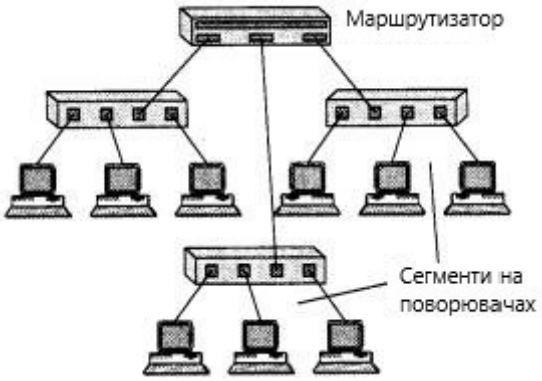


Рисунок 2.17 — Структура підмереж, побудованих на основі повторювачів

Зміна складу сегментів (перехід користувача в іншу мережу) за використанням такої технології вимагає фізичної перекомутації портів на передніх панелях повторювачів, що зменшує надійність та зручність великих мереж: через велику кількість фізичної роботи збільшується вірогідність виникнення помилки.

Для того, щоб уникнути проблеми фізичної перекомутації вузлів, стали використовувати багатосегментні концентратори. Стало можливо програмувати склад сегмента, який відділяється, без фізичної перекомутації.

Але така організація накладає значні обмеження на структуру мережі — кількість сегментів такого повторювача невелика у порівнянні з тим, як це можна зробити за допомогою комутатора. Також за використанням такого

підходу усю роботу по передачі даних виконують маршрутизатори, що не дозволяє максимально використати продуктивність комутаторів. Через це мережі, які побудовані з використанням повторювачів з конфігурованою комутацією, як і раніше використовують розділення середовища передачі даних між великою кількістю вузлів і мають меншу продуктивність у порівнянні з мережами, побудованими на базі комутаторів.

При використанні технології VLAN у комутаторах одночасно вирішуються такі задачі:

1. Підвищення продуктивності в кожній віртуальній мережі, так як кадри в такій мережі передаються лише вузлу призначення.

2. Розмежування мереж між собою для керування правами доступу і створення захисних бар'єрів для запобігання широкомовних штормів.

Для зв'язування віртуальних мереж між собою необхідно використати мережевий рівень (третій рівень моделі OSI). Це можна зробити за допомогою комутатора або за допомогою комутатора 3-го рівня (L3 Switch). Це комутатор, який має програмне забезпечення для роботи на третьому рівні моделі OSI.

Хоч технології віртуальних локальних мереж і були реалізовані багатьма виробниками комутаторів, але довгий час стандартизація у цій галузі не проводилася. Але це змінилося у 1998 році після прийняття стандарту IEEE 802.1Q, який визначає базові правила і принципи побудови віртуальних локальних мереж, які не залежать від протоколу канального рівня, який підтримує комутатор.

Спосіб організації VLAN основі стандарту IEEE 802.1q передбачає розміщення всередині кадру Ethernet додаткового службового поля розміром 4 байти, що дозволяє передавати таку інформацію (рисунок 1.5):

1) Tag Protocol Identifier (TPID) − ідентифікатор протоколу розміром 16 біт − 0x8100, який відповідає стандарту 802.1q, що вказує на використання у кадрі другого рівня цього стандарту;

2) Tag Control Information (TCI) – поле керування розміром 16 біт, що містить в собі такі поля:

− Priority – пріоритет кадру розміром 3 біти відповідно до стандарту IEEE 802.1p;

− Canonical Format Indicator (CFI) – індикатор канонічного формату розміром 1 біт, який вказує на формат MAC-адреси (0 – канонічний, 1 – неканонічний), що забезпечує сумісність між мережами Ethernet та Token Ring

− VLAN Identifier (VID або VLAN ID) – ідентифікатор VLAN розміром 12 біт (діапазон можливих значень ідентифікатора в десятковому форматі становить від 0 до 4095, що надає можливість утворення 4095 віртуальних мереж). Відмітимо, що мінімальний та максимальний розміри поля даних кадру Ethernet зменшується на величину службових полів стандарту 802.1q, тобто на 4 байти, а контрольна сума FCS обчислюється знову з урахуванням цих полів.

Порти комутаторів, які використовуються для організації VLAN на основі стандарту 802.1q, мають тип Trunk (tagged, маркований порт). Ці порти можуть передавати кадри Ethernet, які містять службове поле відповідно до стандарту IEEE 802.1q, від декількох VLAN, що дозволяє здійснювати з'єднання комутаторів мережі тільки одним трактом передачі (рисунок 1.6), на відміну від VLAN на основі портів.

Для роботи комутатора з несумісним обладнанням, за стандартом IEEE 802.1q, передбачаються порти типу Access (untagged, немарковані порти). З рисунка 1.6 видно, що порти комутаторів, до яких приєднані персональні комп'ютери (тут вважається, що мережеві адаптери комп'ютерів не мають підтримки стандарту IEEE 802.1q), мають тип Access. Відмітимо, що порти типу Access можуть бути використані для організації VLAN на основі портів[3].

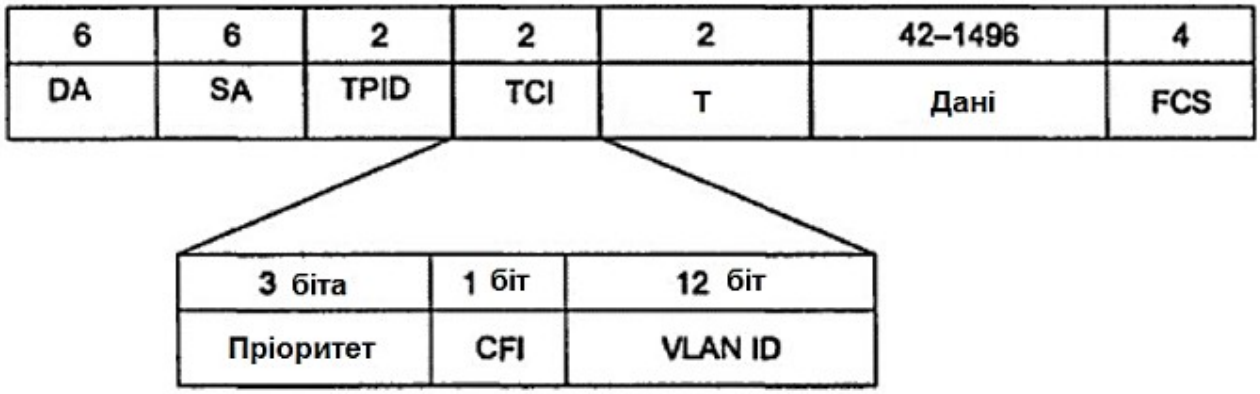


Рисунок 2.18 — Структура кадру Ethernet відповідно до стандарту IEEE 802.1q

Через те, що для технології VLAN довгий час буда відсутня стандартизація, кожен великий виробник комутаторів розробляв свою технологію віртуальних мереж, яка найчастіше не була сумісною з технологією іншого виробника. Навіть поява стандарту не виключала ситуації, коли віртуальні мережі, побудовані з використанням одного виробника не розпізнавалися обладнанням іншого виробника.

При побудові віртуальних мереж з використанням одного комутатора використовують метод, який передбачає, що кожен порт приписується до тої чи іншої мережі (рисунок 2.19).

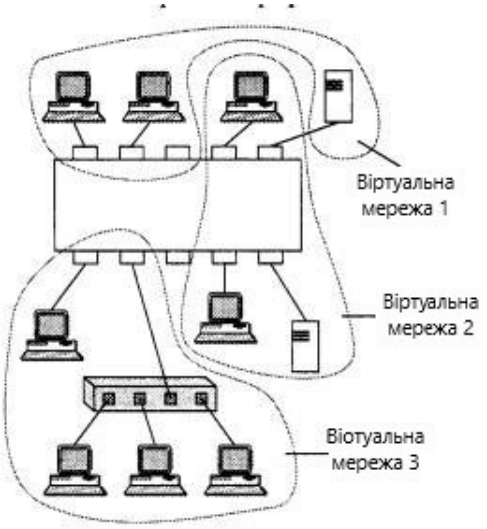


Рисунок 2.19 — Структура віртуальних мереж, побудованих на одному комутаторі

Кадр, який прийшов від порту, наприклад, віртуальної мережі 1, не буде переданий порту, який належить іншій мережі. Існує можливість присвоїти порт декільком віртуальним мережам, але, як правило, так не роблять через те, що зникає ефект повної ізоляції мереж.

Найбільш раціональний спосіб побудови VLAN — групування портів для одного комутатора. Віртуальних мереж, побудованих на базі одного комутатора не може бути більше, ніж портів на самому комутаторі. Якщо до порту підключений сегмент, організований за допомогою повторювача, то немає сенсу включати вузли такого сегменту в різні мережі, все одно трафік цих вузлів буде спільним.

Такий спосіб побудови віртуальних мереж не потребує від адміністратора мережі багато фізичної роботи — достатньо кожен порт прописати до відповідної мережі. Це робиться за допомогою спеціального програмного забезпечення комутатора. Адміністратор за допомогою спеціальних команд створює та іменує віртуальні мережі.

Віртуальні мережі створені для того, щоб розділити комп'ютерну мережу на сегменти за допомогою комутаторів (Virtual Local Area Networks – **VLAN**). Вони представляють собою групу робочих станцій мережі, об'єднаних за певною функцією чи призначенням (рисунок 2.20).

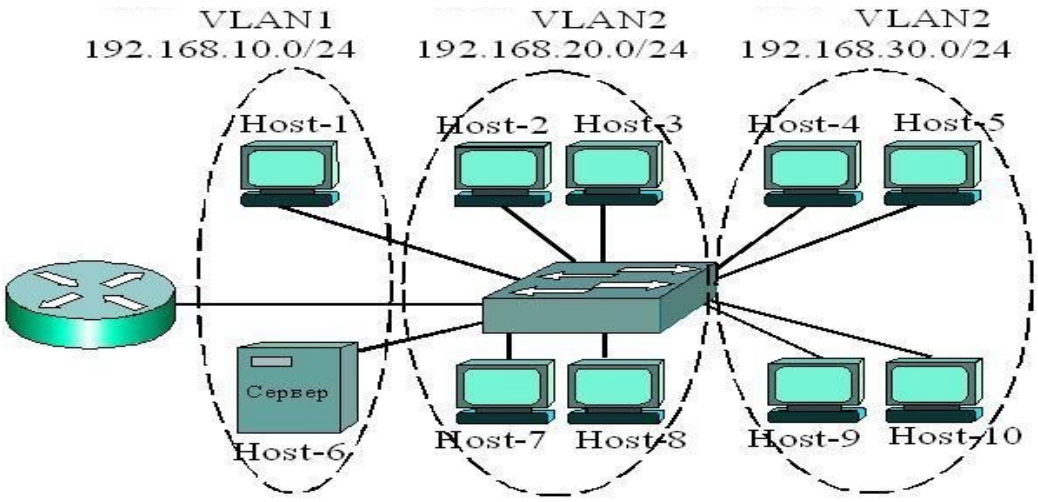


Рисунок 2.20 — Будова віртуальних локальних мереж VLAN

Зазвичай робочі станції об’єднуються у VLAN за функціональними особливостями роботи, незалежно від фізичного розташування користувачів. Обмін інформацією відбувається лише між пристроями, які розташовані в одній віртуальній мережі. Обмін даними між різними VLAN відбувається тільки через маршрутизатори. Робоча станція Host – 1 у віртуальній мережі VLAN 1 обмежена обміном даними лише з сервером, який знаходиться в цій самій підмережі. Віртуальні мережі сегментують комп’ютерну мережу на широкомовні домени так, щоб пакети передавалися тільки між тими портами, що входять в одну й ту саму віртуальну мережу.

Для коректної роботи віртуальних мереж необхідно на комутаторі визначити і налаштувати всі віртуальні локальні мережі визначити, які порти будуть належати до відповідних VLAN. Якщо кадр повинен пройти через комутатор і MAC — адреса призначення відома, то комутатор надсилає кадр на відповідний порт. Якщо MAC — адреса невідома, то відбувається широкомовна передача у всі порти широкомовного домену, а якщо детальніше — всередині VLAN, окрім вихідного порту, звідки був отриманий кадр. Але це зменшує захищеність мережі.

Керування віртуальними локальними мережами відбувається через першу мережу VLAN 1 і реалізується через керування портами комутатора. Мережа VLAN 1 є мережею за замовчуванням (default VLAN). Але на практиці адміністратори міняють номер мережі за замовчуванням, оскільки хакери будуть намагатися атакувати в першу чергу цю мережу.

При налаштуванні кожній віртуальній мережі треба призначити IP – адресу та маску підмережі для того, щоб віртуальні мережі могли взаємодіяти між собою. Наприклад VLAN 1 (рисунок 2.20) може мати адресу 192.168.10.0/24, VLAN 2 – 192.268.20.0/24, VLAN 3 – 192.168.30.0/24. Кожній робочій станції мережі потрібно присвоїти IP – адресу із діапазону відповідної віртуальної мережі. Для прикладу host-1 – адреса 192.168.10.1, host-2 – адреса 192.168.20.1, host-3 – адреса 192.168.20.2, host-7 – адреса 192.168.20.3, host-10 –

адреса 192.168.30.4.

Ідентифікатори віртуальних мереж можуть призначатися із нормального діапазону 1 — 1005, де ідентифікатори 1002 — 1005 зарезервовані для VLAN, які будуються на базі Token Ring та FDDI. Також існує розширений діапазон ідентифікаторів 1006 — 4094, але для оптимізації керування рекомендовано, щоб підмереж було не більше 255 і вони не розширювалися поза другим рівнем моделі OSI (рівень, на якому працює комутатор).

Таким чином VLAN представляє собою широкомовний домен, який був створений за допомогою одного і більше комутатора. На рисунку 2.21 представлено три VLAN, які були побудовані за допомогою одного маршрутизатора та трьох комутаторів. Трафіком між віртуальними мережами керує маршрутизатор.

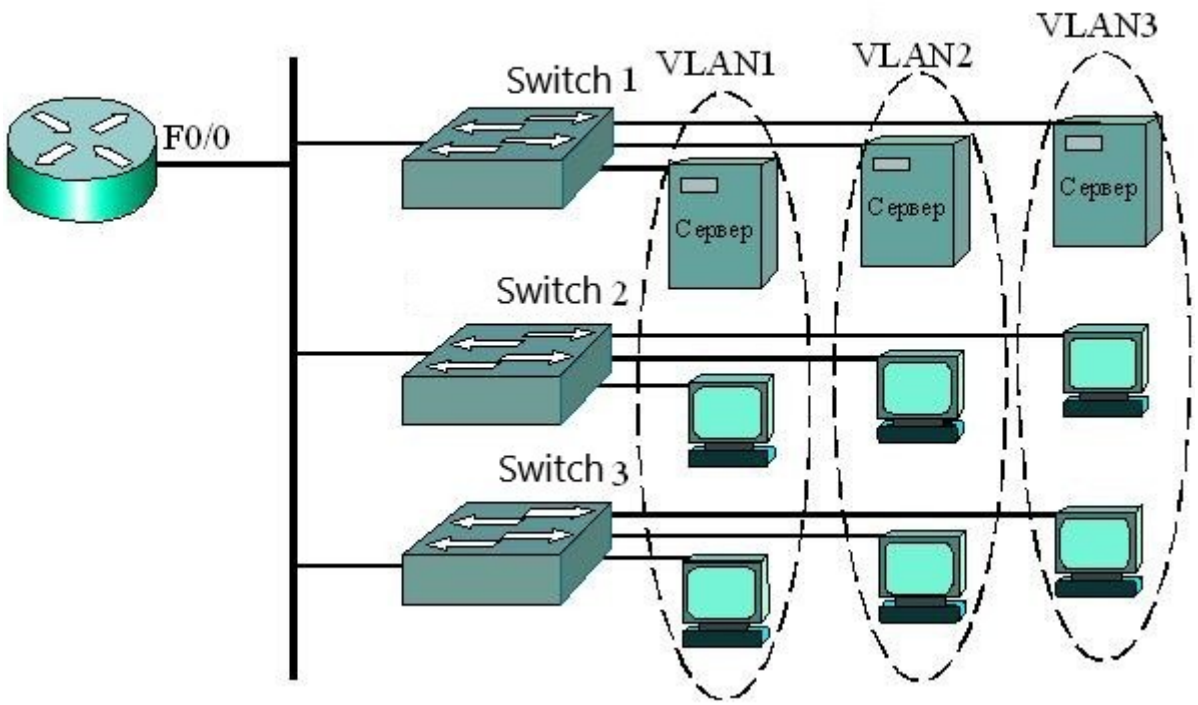


Рисунок 2.21 — Схема трьох віртуальних мереж VLAN

Якщо комп’ютер з VLAN 1 відправить кадр комп’ютеру, який знаходиться в тій самій підмережі, адресою призначення кадра буде MAC — адреса мережевої карти комп’ютера, якому призначено повідомлення. Якщо

робоча станція з VLAN 1 відправить кадр робочій станції з VLAN 2, кадри будуть відправлені на MAC — адресу інтерфейсу F0/0 маршрутизатора. Маршрутизація виконується через IP – адресу інтерфейсу F0/0 маршрутизатора.

Щоб виконувати свої функції у віртуальних мережах, комутатор поаинен мати таблиці комутації для кожного VLAN. Для коректної передачі кадрів, проводиться пошук адреси в таблиці тільки для даної VLAN. Якщо адреса джерела раніше не була відома, то при отриманні кадру комутатор додає цю адресу до таблиці.

Для нормальної роботи мережі потрібно кожному мережевому інтерфейсу, на який надходять IP — пакети, призначити IP — адресу. Це можна виконувати вручну, але при цьому системний адміністратор повинен пам’ятати, які IP — адреси з наявної кількості вже зайняті, а які вільні. Для великих мереж така процедура не є надійною, оскільки через великий об’єм ручної роботи більший шанс виникнення помилки. Цю проблему виправляє протокол DHCP.

DHCP (Dynamic Host Configuration Protocol) — мережевий протокол, який дозволяє пристроям мережі автоматично отримувати IP — адресу та інші параметри, необхідні для роботи в мережі TCP / IP[4].

DHCP підтримує автоматичний динамічний розподіл адрес. Він працює за клієнт — серверною архітектурою. Під час запуску комп’ютер, який виступає у ролі DHCP — клієнта, відправляє у мережу широкомовний запит на отримання IP — адреси. У відповідь DHCP — сервер посилає повідомлення, в якому міститься IP — адреса та інші конфігураційні параметри. Передбачається, що DHCP — клієнт і DHCP — сервер знаходяться в одній IP — мережі.

На таблиці 2.5 показана структура протоколу DHCP.

Таблиця 2.5 — структура протоколу DHCP.

Поле	Опис	Довжина(в байтах)
op	Тип повідомлення. Наприклад може приймати значення: BOOTREQUEST (1,	1

	запит від клієнта до сервера) і BOOTREPLY (2, відповідь від сервера до клієнта).	
htype	Тип апаратної адреси. Допустимі значення цього поля визначені в RFC1700 «Assigned Numbers». Наприклад, для MAC-адреси Ethernet 10 Мбіт/с це поле приймає значення 1.	1
hlen	Довжина апаратної адреси в байтах. Для MAC-адреси Ethernet — 6.	1
hops	Кількість проміжних маршрутизаторів (так званих агентів ретрансляції DHCP), через які пройшло повідомлення. Клієнт встановлює це поле в 0.	1
xid	Унікальний ідентифікатор транзакції, що генерується клієнтом на початку процесу отримання адреси.	4
secs	Час в секундах з моменту початку процесу отримання адреси. Може не використовуватися (в цьому випадку воно встановлюється в 0).	2
flags	Поле для прапорів — спеціальних параметрів протоколу DHCP.	2
ciaddr	IP-адреса клієнта. Заповнюється тільки в тому випадку, якщо клієнт вже має власну IP-адресу і здатний	4

	відповідати на запити ARP (це можливо, якщо клієнт виконує процедуру поновлення адреси після закінчення терміну оренди).	
yiaddr	Нова IP-адреса клієнта, запропонована сервером.	4
siaddr	IP-адреса сервера. Повертається в реченні DHCP (див. нижче).	4
giaddr	IP-адреса агента ретрансляції, якщо такий брав участь в процесі доставки повідомлення DHCP до сервера.	4
chaddr	Апаратна адреса (зазвичай MAC-адреса) клієнта.	16
sname	Необов'язкове ім'я сервера у вигляді нуль-термінованого рядка.	64
file	Необов'язкове ім'я файлу на сервері, що використовується бездисковими робочими станціями при віддаленому завантаженні. Як і sname, представлено у вигляді нуль-термінованого рядка.	128
options	Поле опцій DHCP. Тут вказуються різні додаткові параметри конфігурації. На початку цього поля вказуються чотири особливих байта зі значеннями 99, 130, 83, 99 («чарівні числа»).	змінна

Він працює автоматично, без участі системного адміністратора, видаючи клієнту випадкову IP — адресу із множини доступних. Множину доступних адрес визначає адміністратор при налаштуванні DHCP — сервера. Адреса видається на постійній основі, строк оренди не обмежений. Ідентифікатор клієнта повинен відповідати його IP — адресі. Це відбувається під час першого призначення DHCP — сервером IP — адреси клієнту. При наступних запитах клієнт отримує ту саму адресу.

При динамічному розподілі IP — адреса видається клієнту на певний час, який має назву час оренди (lease duration), це дає можливість повторно використати одну і ту саму IP — адресу але для іншого комп'ютера. Це підсилює основну перевагу DHCP і дозволяє будувати мережі, де робочих станцій більше, ніж доступних IP — адрес, які є у розпорядженні адміністратора.

Технологія DHCP забезпечує просту та надійну конфігурацію мереж TCP/IP, забезпечує відсутність дублювання адрес за рахунок централізованого розподілу. Якщо DHCP — клієнт видаляється із мережі, адреса стає вільною. Він також може призначати такі налаштування як маска підмережі, IP — адресу маршрутизатора за замовчуванням, адресу сервера доменних імен (DNS).

Для розподілу мережі на VLAN у Cisco Pocket Tracer для початку потрібно визначити назву та номер відповідних підмережі. Це буде представлено у таблиці 2.6.

Таблиця 2.6 — віртуальні мережі.

Назва відділу	Назва VLAN	Номер VLAN
Конструкторський відділ	IT-Department	10
Відділ технічної підтримки	Tech-support	20
Конструкторський відділ	Construction-department	30

Після того потрібно у кожному комутаторі мережі додати назви і номери цих віртуальних мереж (рисунок 2.22).

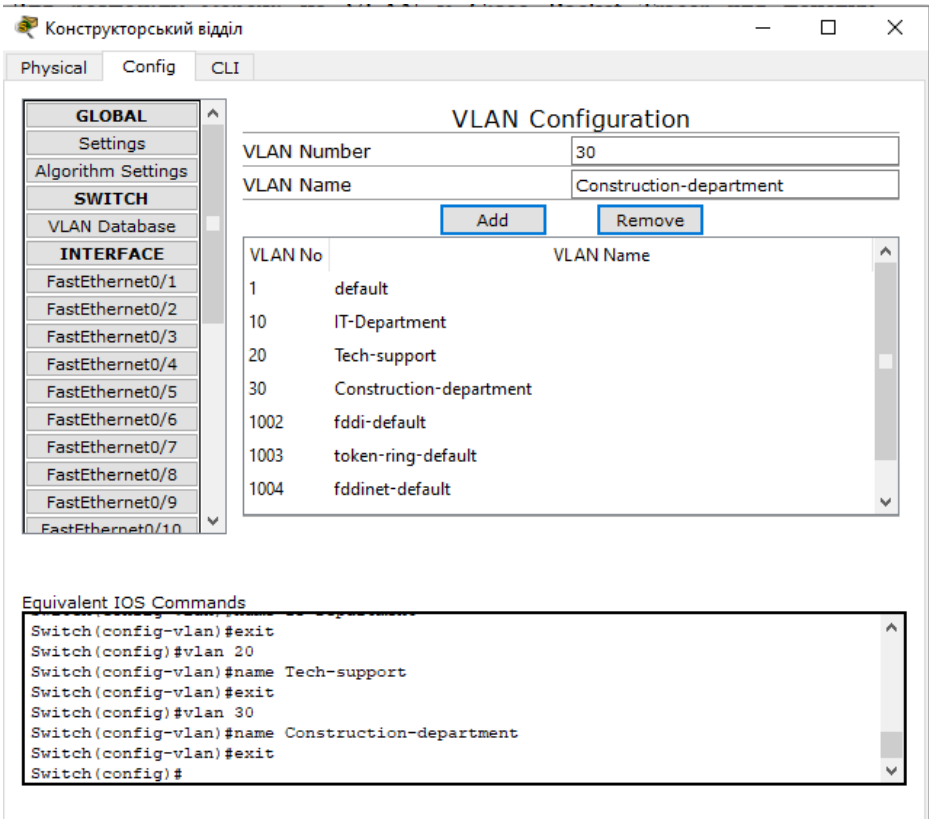


Рисунок 2.22 — Віртуальні мережі у параметрах комутатора

Для подальшого налаштування спочатку потрібно активувати порт, який з’єднує маршрутизатор та комутатор. Це можна зробити, якщо у налаштуваннях маршрутизатора вибрати відповідний інтерфейс (у даному випадку це інтерфейс FastEthernet 0/0) і активувати пункт «Port Status» (рисунок 2.23).

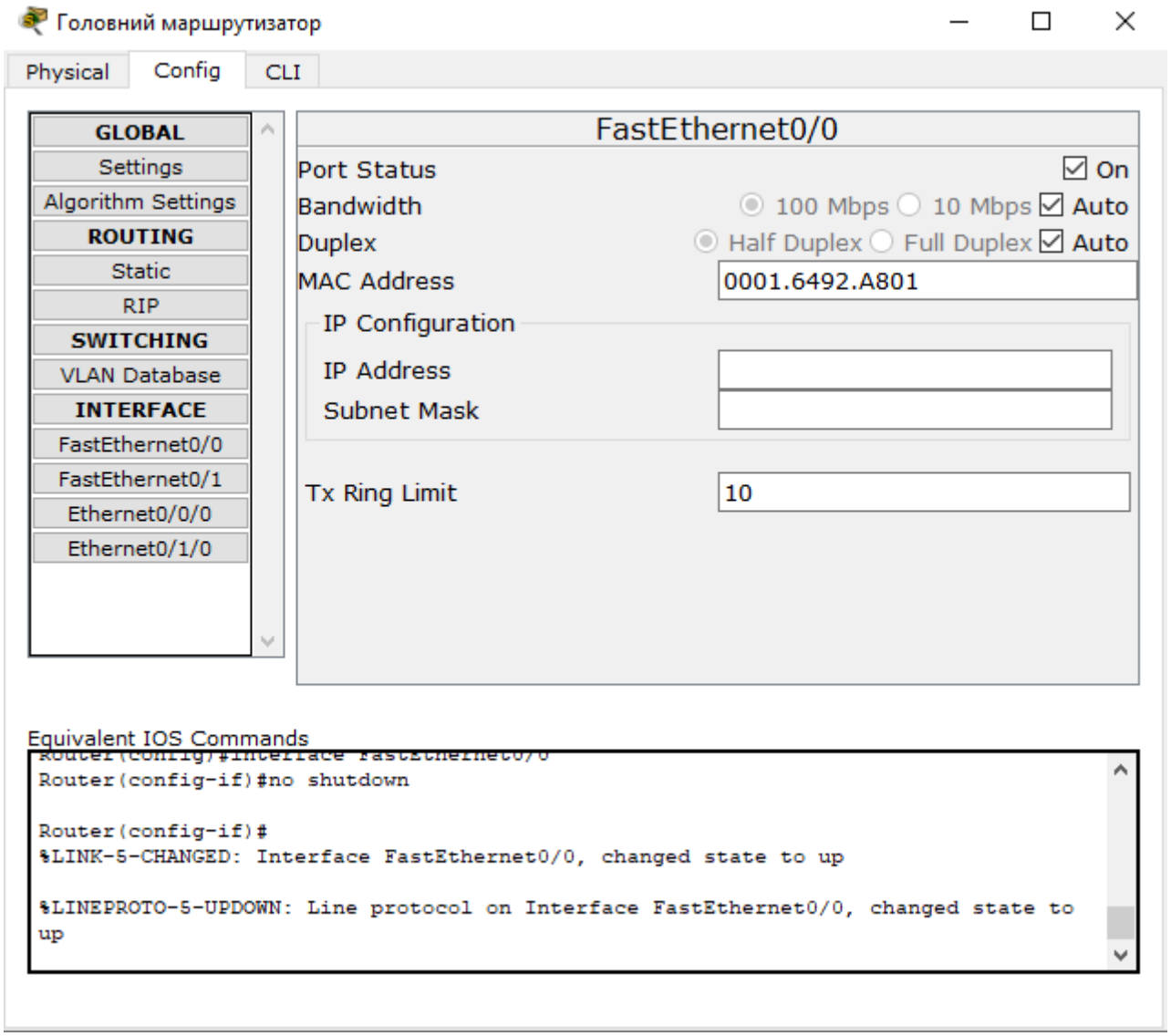


Рисунок 2.23 — Активація інтерфейсу FastEthernet 0/0

Для подальшого налаштування віртуальних мереж варто перейти до командного рядка (CLI) операційної системи маршрутизатора. Для цього потрібно виконати наступні команди:

1. enable — вхід у розширений режим;

2. configure terminal — режим глобального конфігурування;

3. interface FastEthernet0/0.10 — ініціалізація на інтерфейсі FastEthernet0/0 субінтерфейсу FastEthernet0/0.10, який буде відповідати за віртуальну мережу з порядковим номером 10 (IT — відділ).

Отже, потрібний субінтерфейс створений. Тепер потрібно помістити у нього VLAN IT — відділу, ця процедура називається інкапсуляцією. Вона

використовується тоді, коли потрібно передавати декілька підмереж через один порт. У Cisco Pocket Tracer за це відповідає команда encapsulation dot1q. Для інкапсуляції 10 — го VLAN треба виконати команду encapsulation dot1q 10.

Тепер можна призначити субінтерфейсу IP — адресу та маску підмережі, як і фізичному інтерфейсу. Це відбувається за допомогою команди ip address 192.168.10.1 255.255.255.0.

Таким самим способом додаємо субінтерфейси підмереж конструкторського відділу та відділу технічної підтримки (рисунок 2.24).

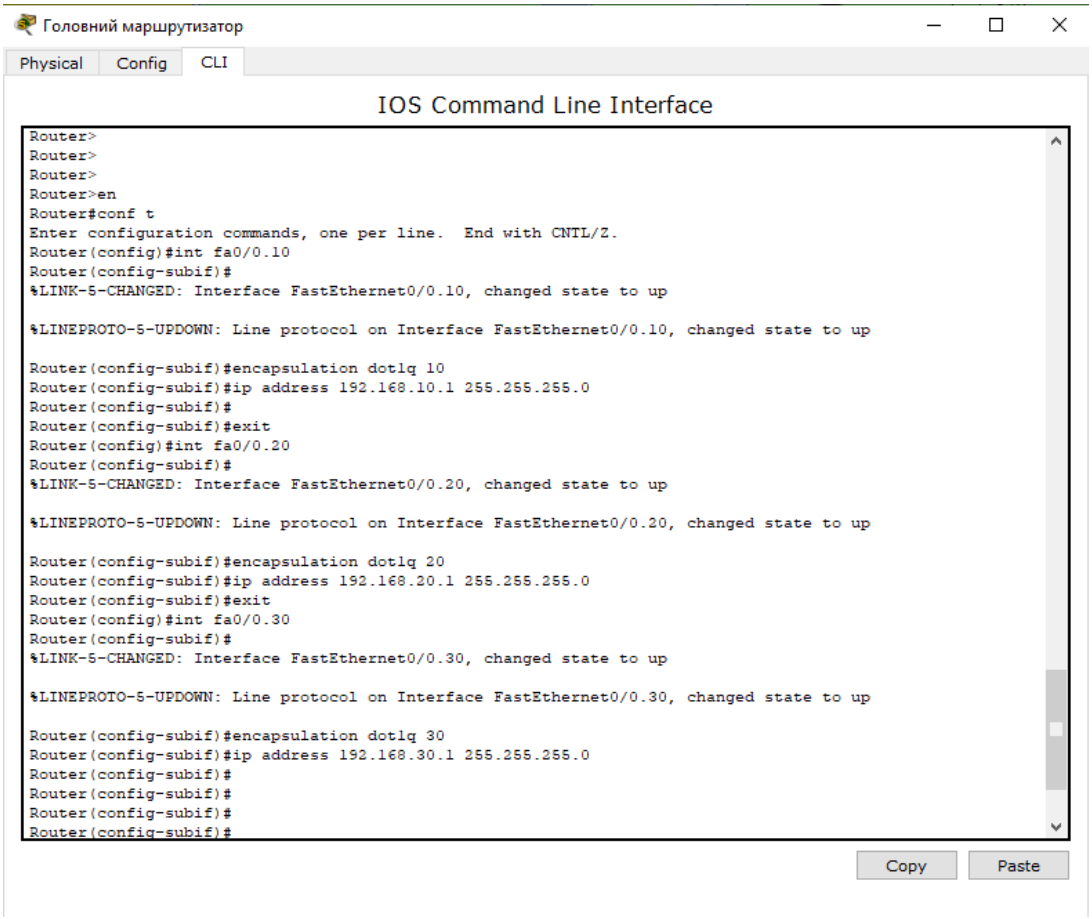


Рисунок 2.24 — Налаштування субінтерфейсів для підмереж

Після налаштування субінтерфейсів, перебуваючи у режимі глобального конфігурування, також треба налаштувати DHCP — сервер для автоматичного призначення IP — адреси відповідно до віртуальної мережі. Для цього потрібно використати наступні команди:

1. ip dhcp pool itd — визначає DHCP — пул, назва якого вказується в якості останнього параметра;

2. network 192.168.10.0 – задаємо мережу, яка буде призначатися;

3. default – router 192.168.10.1 — задаємо шлюз, в якості якого буде виступати маршрутизатор;

4. dns – server 8.8.8.8 — призначаємо сервер доменних імен.

5. ip dhcp excluded – address 192.168.10.0, ip dhcp excluded – address 192.168.10.1 — визначаємо IP — адреси, які не можуть бути призначені.

Аналогічним чином налаштовуємо динамічне призначення IP — адрес для інших підмереж, тільки третім октетом адреси вказуємо номер відповідної підмережі (рисунок 2.25).

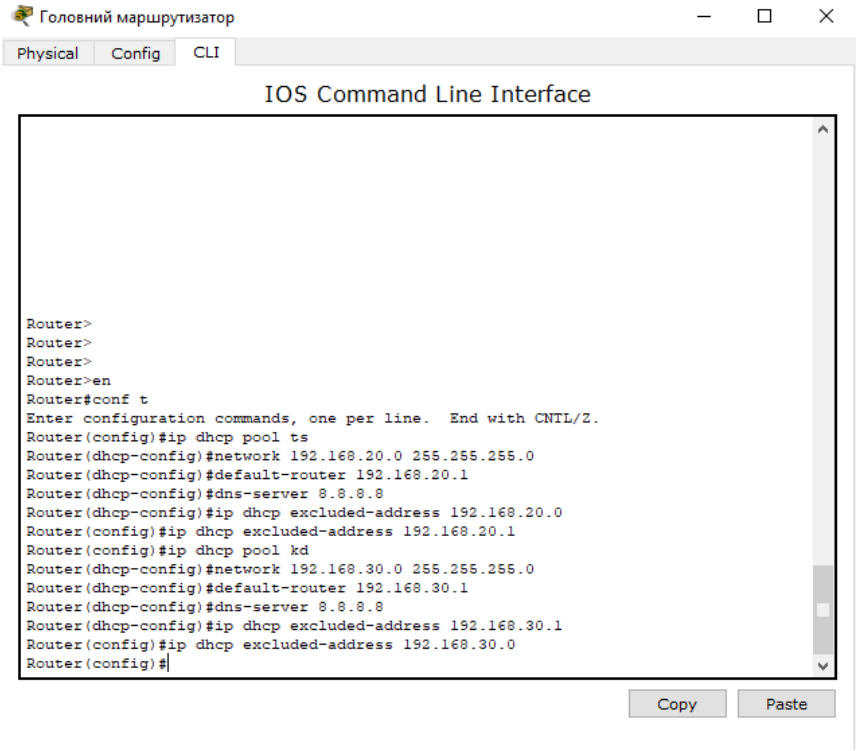


Рисунок 2.25 — Налаштування DHCP для віртуальних мереж 20 та 30

Тепер треба задати портам комутаторів відповідні віртуальні мережі, в яких будуть працювати пристрої, які підключені до цих портів (рисунок 2.26). Порти, які з’єднують між собою два комутатори або комутатор та маршрутизатор слід визначити як trunk – порт. За допомогою trunk – портів відбувається передача трафіка декількох VLAN по одному каналу зв’язку (рисунок 2.27).

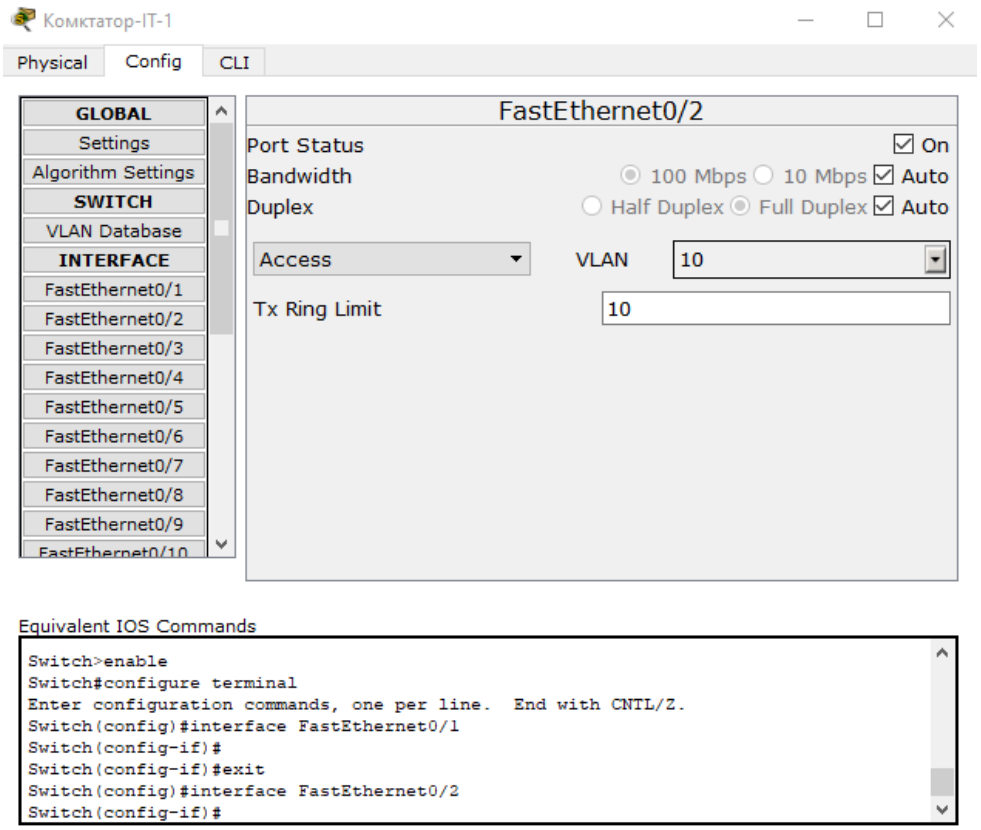


Рисунок 2.26 — Налаштування порту для роботи у VLAN 10

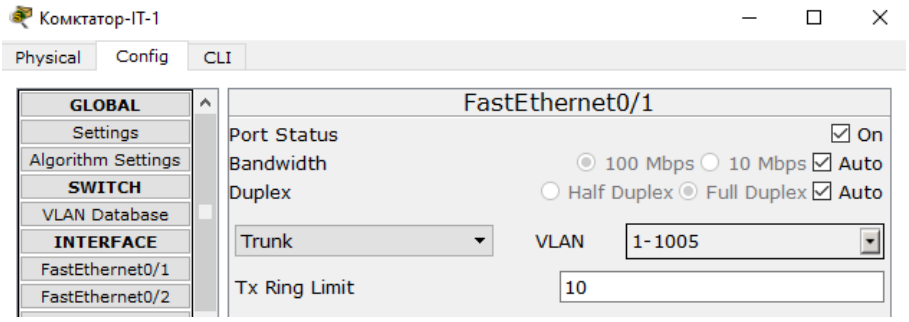


Рисунок 2.27 — Налаштування trunk – порту

Отже, для перевірки правильності роботи служби DHCP потрібно зайти в параметри пристрою та у розділі «Desktop» вибрати пункт «IP Configuration» і переключити його у положення DHCP (рисунок 2.28).

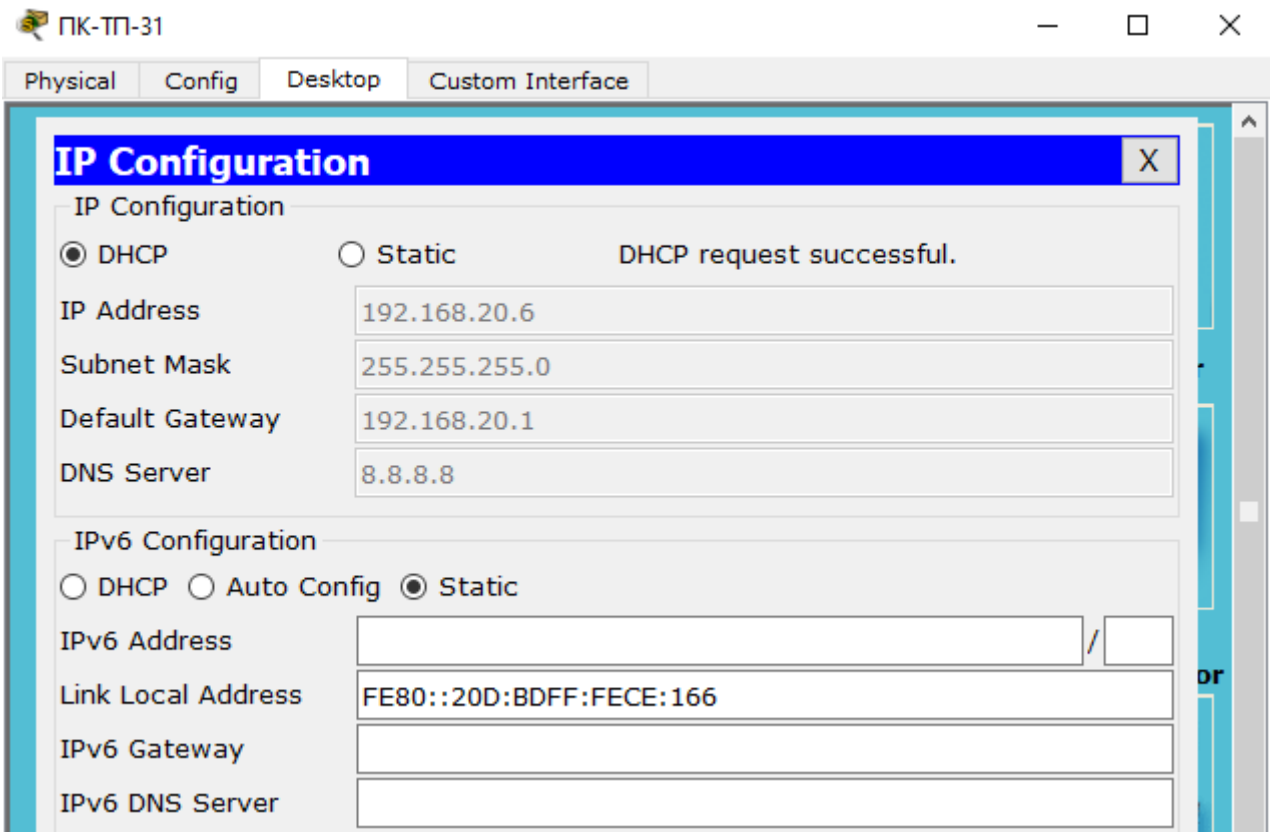


Рисунок 2.28 — Налаштування динамічного отримання IP — адреси

Адреса буде залежати від віртуальної мережі, якій призначений порт.

Для реалізації можливості підключення за допомогою технології Wi – Fi у Cisco Pocket Tracer потрібно для кожної віртуальної мережі додати точку доступу Wi – Fi (Access Point). Кожну точку доступу слід підключити до комутатора і призначити їй відповідний VLAN, у якому вона буде працювати. У налаштуваннях необхідно вказати SSID (назва Wi – Fi мережі), а також у розділі «Authentification» встановити пароль для запобіганню сторонніх підключень (рисунок 2.29).

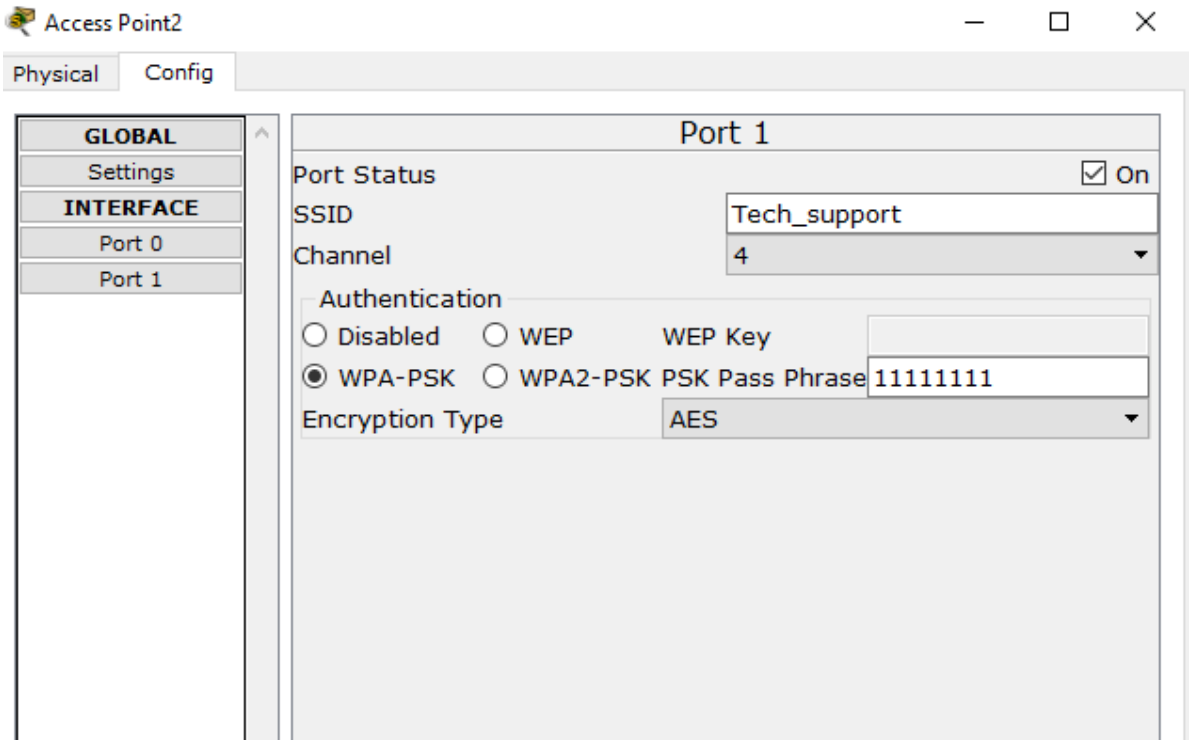


Рисунок 2.29 — Налаштування точки доступу

Робоча станція, для підключення до бездротової мережі, повинна мати спеціальну плату розширення (Wi – Fi адаптер). Після його встановлення потрібно перейти до параметрів пристрою і вибрати розділ «PC Wireless». У розділі «Connect» з'явиться список доступних Wi – Fi мереж (рисунок 2.30). Із цього списку вибираємо потрібну мережу і підключаємося до неї.

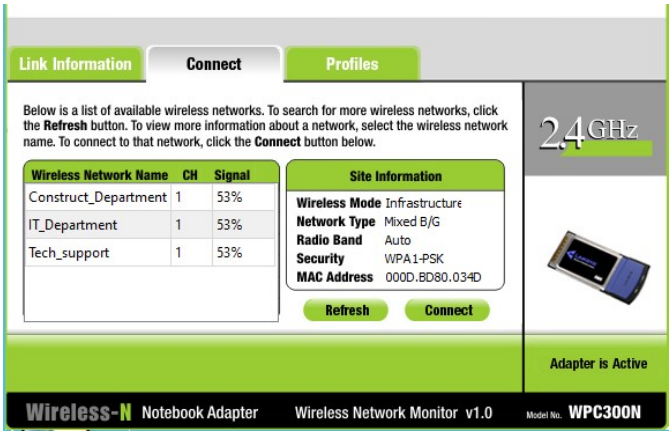


Рисунок 2.30 — Список доступних бездротових мереж

Для реалізації основного призначення технології віртуальних мереж, а саме розмежування доступу між різними відділами, потрібно використати access control list (список доступу).

Access control list (ACL) працює на пристроях третього рівня моделі OSI, можуть бути налаштовані на окремому сервері або на маршрутизаторі, і керують як вхідним, так і вихідним трафіком.

Для того, щоб створити списки доступу у Cisco Pocket Tracer, потрібно перейти у параметри маршрутизатора, а саме у командний рядок Cisco IOS. Потім створені списки доступу присвоюються відповідним інтерфейсам або субінтерфейсам.

Для ініціалізації списку доступу потрібно перейти у розширений режим операційної системи Cisco командою «enable». Далі треба увійти у режим глобальної конфігурації, ввівши команду «config terminal». Списки доступу можуть бути стандартними (standart) або розширеними (extended). Команда «ip access-list standart construct-department» створить стандартний список доступу, який матиме назву construct-department, через те, що він призначений для підмережі конструкторського відділу. Після того, як список доступу був створений, потрібно налаштувати його. За керування доступом відповідають команди «deny» - заборонити та «permit» - дозволити. За умовами завдання, конструкторський відділ не повинен мати доступу до IT — відділу та відділу технічної підтримки. Зробити це можна командою «deny 192.168.20.0 0.0.0.255» та «deny 192.168.10.0 0.0.0.255»: вказавши адресу мережі, до якої доступ заборонено та зворотню маску підмережі. Команда «permit any» дозволить доступ до всіх інших мереж. Але створити список доступу не достатньо, потрібно присвоїти його відповідній підмережі. Це виконується шляхом зв’язування ACL з відповідним інтерфейсом або підінтерфейсом. Для цього необхідно перейти на субінтерфейс віртуальної мережі командою «interface FastEthernet0/0.30» Команда «ip access-group construct-department out» присвоїть підінтерфейсу FastEthernet0/0.30 ACL construct-department, який буде фільтрувати вихідний трафік. Тому користувач робочої станції, яка знаходиться у конструкторському відділі, не зможе звернутися до комп’ютерів інших підрозділів (рисунок 2.31).

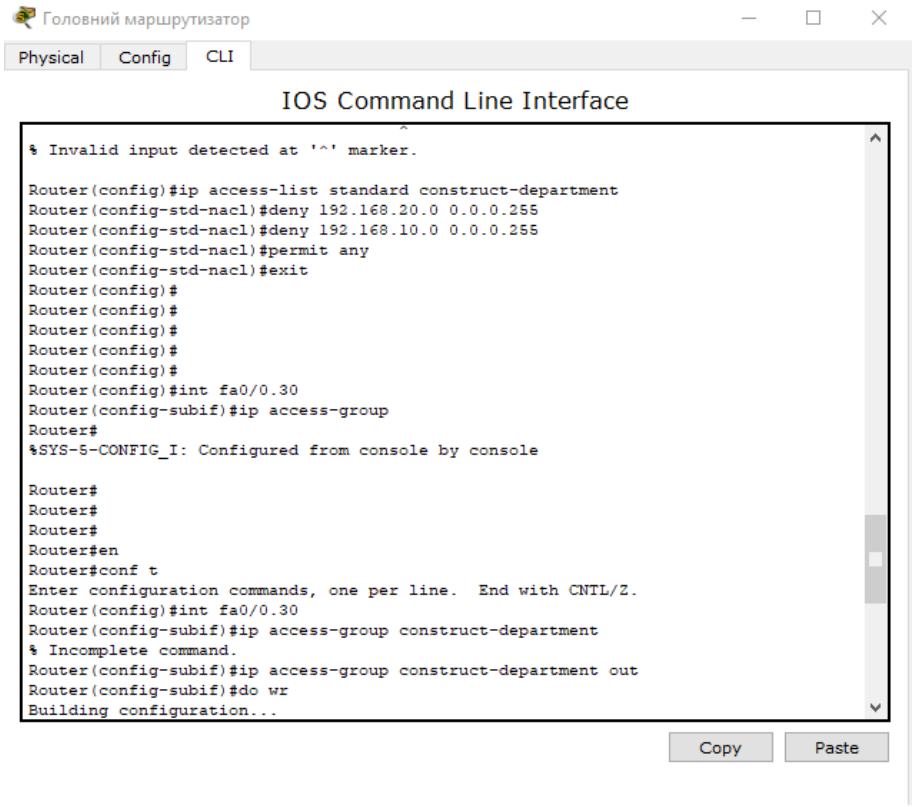


Рисунок 2.31 — Налаштування ACL для конструкторського відділу

За таким самим принципом створюємо списки доступу для IT — відділу та відділу технічної підтримки і зв’язуємо їх з відповідними субінтерфейсами. Для IT — відділу буде заблоковано вихідний трафік, який призначається конструкторському відділу та відділу техпідтримки, а для відділу техпідтримки — трафік, кий надходить IT та конструкторським відділам (рисунок 2.32 та рисунок 2.33).

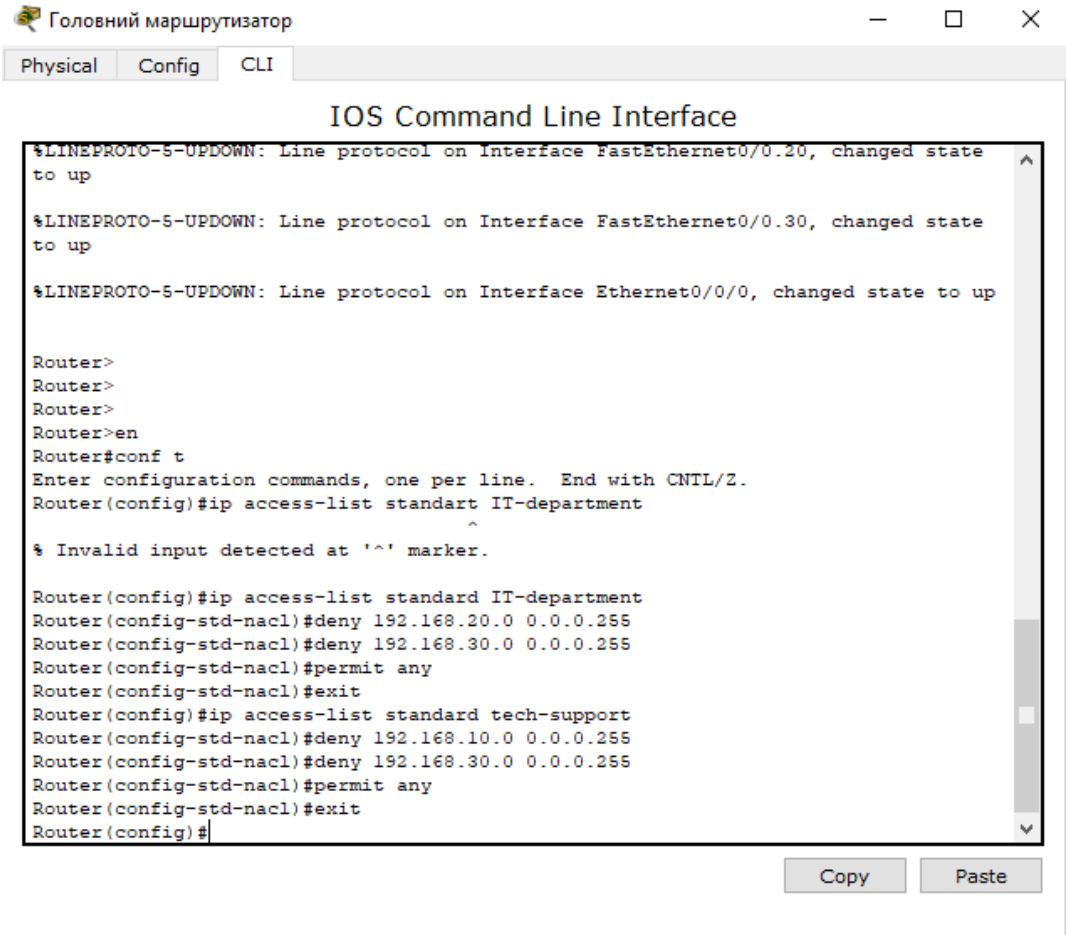


Рисунок 2.32 — налаштування списків доступу для IT — відділу і техпідтримки

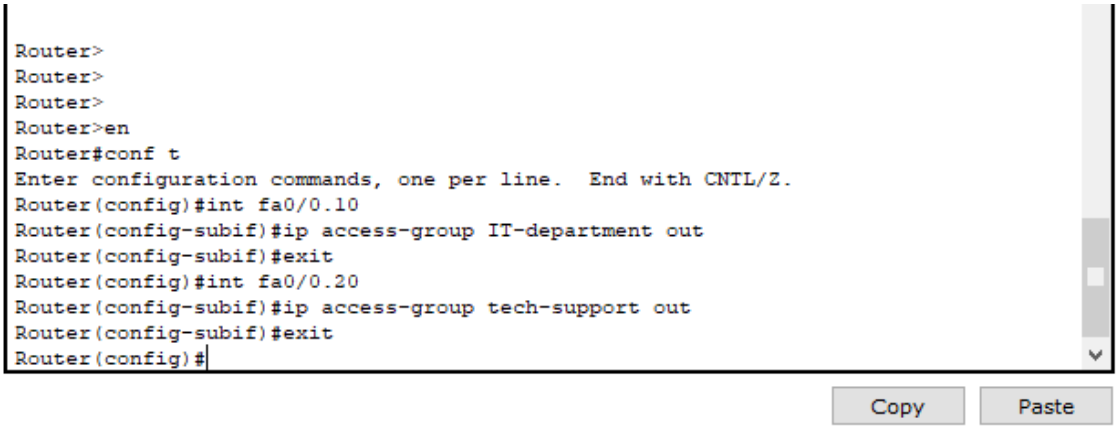


Рисунок 2.33 — присвоювання субінтерфейсам відповідних access control list

Перевірка логічної мережі на працездатність та коректність роботи.

1. Перевірка, чи можуть робочі станції мережі звертатися до FTP — сервера. Для цього у командному рядку комп’ютера потрібно ввести команду

«ftp 128.96.10.10». При правильних налаштуваннях у командному рядку повинно з’явиться поле для вводу ім’я користувача та пароль (рисунок 2.34).

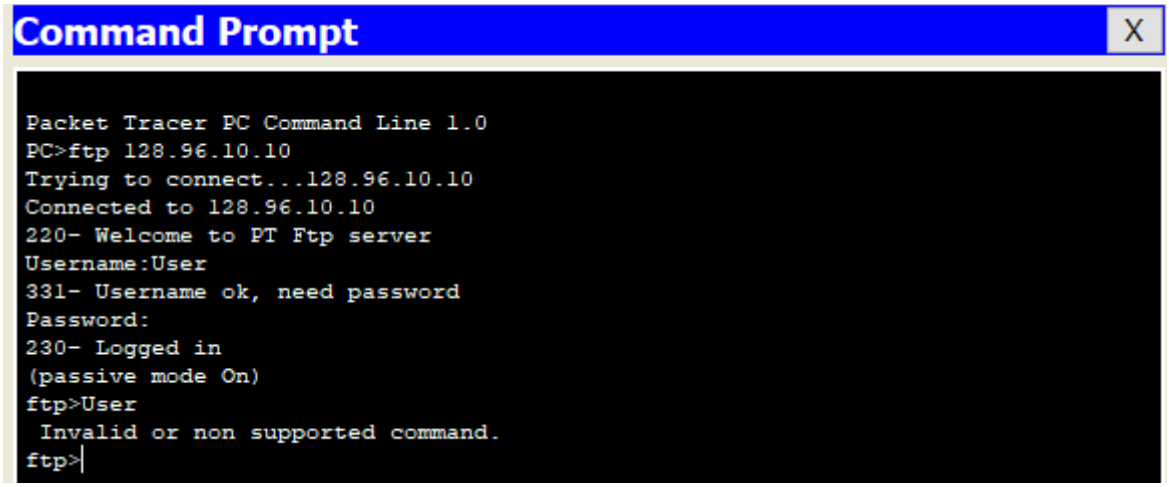


Рисунок 2.34 — Звернення до FTP - сервера

2. Перевірка роботи списків доступу для віртуальних мереж. Це можна зробити, використавши команду «ping» у парі з відповідною IP — адресою. Результатом роботи буде показник, скільки з тестових пакетів дійшли до комп’ютера, якому вони надсилалися. У приведеному на рисунку 2.35 прикладі комп’ютер з IP — адресою 192.168.30.4 надсилає тестові пакети лептопу, який має адресу 192.168.20.9. Вони знаходяться у різних підмережах і, за умовами завдання, не мають доступу один до одного.

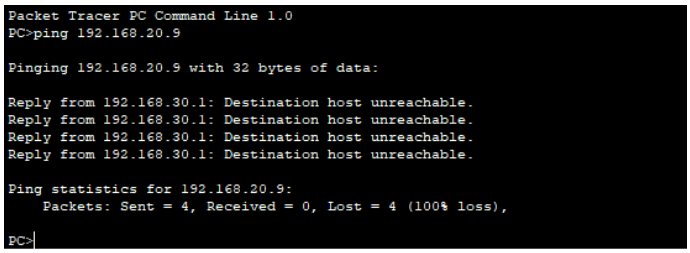


Рисунок 2.35 — перевірка доступу до робочої станції іншої підмережі

Як бачимо, не один із тестових пакетів не досяг адреси призначення, оскільки втрати сягають 100%. Якщо ж «пропінгувати» комп’ютер з тієї ж віртуальної мережі, то всі пакети досягнуть адреси призначення (рисунок 2.36).

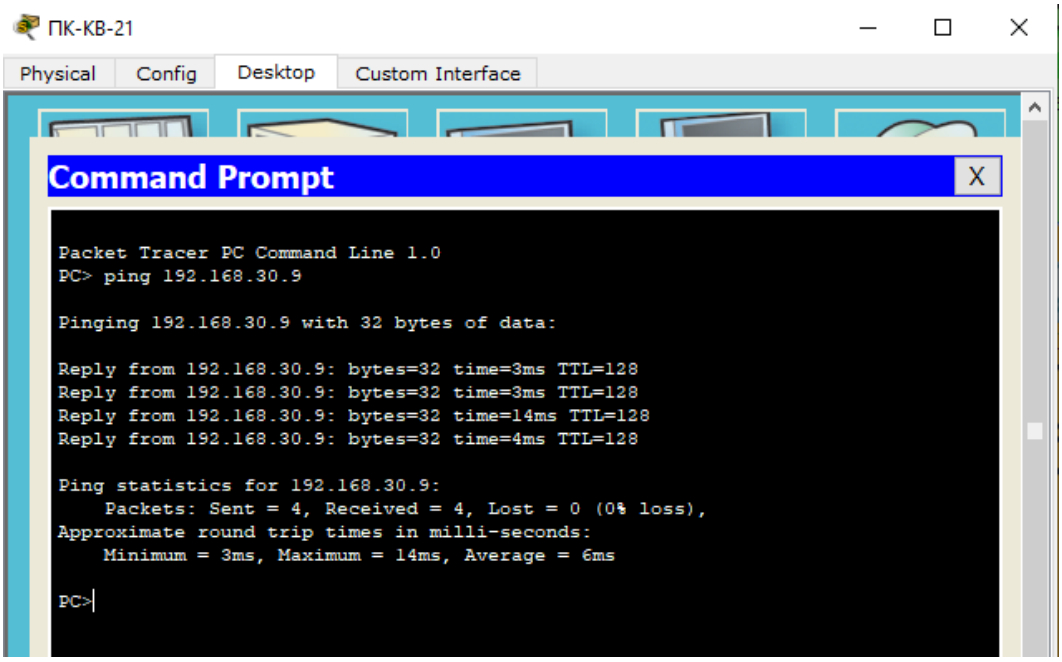


Рисунок 2.36 — перевірка доступу до комп’ютера однієї мережі

Отже, можна зробити висновок, що логічна модель телекомунікаційної мережі працює коректно і показує, як інформація циркулює у раках усієї мережі та у межах окремих віртуальних мереж.

3 ВИБІР ОБЛАДНАННЯ ДЛЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

3.1 Маршрутизатор

Роль головного маршрутизатора мережі буде виконувати MikroTik Router

BOARD RB750GR3 hEX (рисунок 3.1). Це пятипортовий GigabitEthernet маршрутизатор. Він має 16 Мб флеш — пам’яті, USB — порт, слот для карти пам’яті MicroSD І підтримку апаратного шифрування. Більш детальні характеристики наведені у таблиці 3.1.

Таблиця 3.1 — Характеристики маршрутизатора

Швидкість портів	1 Гбіт/с
Процесор	MT7621A
Частота процесора	880 МГц
Кількість ядер / потоків	2 / 4
Оперативна пам’ять	256 Мб
Флеш — пам’ять	16 Мб
Інтерфейси	5 * LAN 10/10/1000, 1 * USB type A
Підтримка протоколів	PPTP, L2TP, Ipsec, PPPoE, DHCP, NAT

Рисунок 3.1 - MikroTik Router BOARD RB750GR3 hEX

3.2 Комутатори

Під час побудови телекомунікаційної мережі буде застосовуватися дві моделі комутаторів: Cisco SB SF110D – 08 – EU (рисунок 3.2) та TP – LINK TL – SF1016D (рисунок 3.3). Перший буде розміщуватися у коридорах, до нього будуть підключатися комутатори, які знаходяться в кабінетах. Їх параметри показані у таблиці 3.2.

Таблиця 3.2 — Характеристики комутаторів

Модель	Cisco SB SF110D-08-EU	TP -LINK TL-SF1016D
Кількість портів Ethernet	8 * RJ45 10/100 Мбіт/с	16 * RJ45 10/100 Мбіт/с
Тип	некерований	некерований

Рисунок 3.2 — Комутатор Cisco SB SF110D-08-EU

Рисунок 3.3 — Комутатор TP -LINK TL-SF1016D

3.3 Робочі станції

Вибір комп’ютерів, які будуть працювати в мережі, має велике значення через те, що від їх параметрів залежить якість і швидкість роботи, яку вони будуть виконувати. Тому було прийняте рішення обрати для цієї ролі моноблоки. Це комп’ютер або міні — комп’ютер, у якого всі пристрої вводу — виводу знаходяться в одному корпусі разом з монітором. Такі пристрої мають ряд переваг, найголовнішими із яких є компактність (не потрібно додаткове місце для системного блоку) та енергоефективність (в таких системах встановлюються комплектуючі, які мають малий обсяг споживання

електроенергії для кращого охолодження в компактному корпусі).

Найоптимальнішим вибором буде моноблок HP 200 G4 (рисунок 3.4). Його характеристики показані у таблиці 3.3.

Таблиця 3.3 — Характеристики HP 200 G4

Модель	HP 200 G4
Дисплей	21.5” IPS 1920 * 1080
Процесор	Intel Core i3 – 1215U (3.3 – 4.4 ГГц)
Оперативна пам’ять	4 Гб
Графічний адаптер	Intel UHD Graphics
Операційна система	Windows 11 Home

Рисунок 3.4 — Моноблок HP 200 G4

3.4 Файл — сервер

Файл — сервер є одним з найголовніших мережевих пристроїв, через те, що на ньому буде зберігатися багато важливої інформації з різних відділів підприємства. Його наявність дає наступні переваги:

1. Дає можливість розподілити області зберігання за будь — яким типом та налаштувати допуск до інформації для визначених користувачів.

2. Покращує інформаційну безпеку.

3. Дозволяє розподілити об’єм дискового простору.

Для швидкої та надійної роботи потребує потужного процесора, значного обсягу оперативної пам’яті та накопичувачів, які мають високу швидкість запису та читання для швидкого доступу до інформації.

У якості файлового серверу було обрано сервер ARTLINE Business

R17v14 (рисунок 3.5). Він має параметри, які задовольняють наведені вище вимоги.

Таблиця 3.4 — Параметри сервера ARTLINE Business R17v14

Модель	ARTLINE Business R17v14
Процесор	Intel Core i5 – 10400F
Кількість ядер / потоків	6 / 12
Тактова частота	2.9-4.3 ГГц
Чіпсет	Intel H470
Оперативна пам’ять	16 ГБ DDR4-2666
HDD	2 * 1TB
SSD	250 GB
Графічний адаптер	Nvidia GeForce GT 710 1 GB
Блок живлення	400 Ват
Операційна система	Linux Fedora – Server 39

Такі характеристики дозволять серверу швидко відповідати на запити клієнтів мережі, а операційна система Linux забезпечить надійність та швидкодію. Вона також є безкоштовною, оскільки це програмне забезпечення з відкритим вихідним кодом

Рисунок 3.5 — Сервер ARTLINE Business R17v14

4 РЕЗЕРВНЕ ЖИВЛЕННЯ МЕРЕЖІ

Забезпечення резервного живлення мережі має надважливе значення, бо саме це дозволяє продовжити нормальну роботу підприємства в умовах відключення електроенергії або блекауту. Тож різке знеструмлення негативно впливає на пристрої мережі, особливо на сервер та робочі станції через те, що інформація у них зберігається на накопичувачах на жорстких магнітних дисках. Якщо різко вимкнути живлення, такий накопичувач може не зберегти дані, які записувалися на нього записувалися або інформація може записатися не коректно, що унеможливить її зчитування згодом. А враховуючи особливості конструкції жорстких дисків, такі особливості експлуатації призведуть до швидкого виходу з ладу накопичувача з усією наявною інформацією на ньому.

4.1 Забезпечення резервного живлення маршрутизатора та комутаторів

Для того, щоб реалізувати аварійне живлення для маршрутизатора, існують спеціальні пристрої, які мають назву Mini UPS. Такі пристрої мають компактний розмір та прості у експлуатації.

У нашому випадку найоптимальнішим вибором буде Mini DC UPS KA –

DC1018P. Він призначений для забезпечення живлення дрібних електроприладів при екстреному відключенні електроенергії. Його можливості вказані у таблиці 4.1.

Таблиця 4.1 — параметри Mini DC UPS KA – DC1018P

Вихідна потужність	18 Ват
Діапазон вхідної напруги	85 — 265 Вольт змінного струму
Вихідні напруги	5, 9, 12 Вольт
Ємність акумулятора	8800 Міліампер / годин
Час роботи роутера від акумулятора	8 — 10 Годин

Рисунок 4.1 — Mini DC UPS KA – DC1018P

4.2 Забезпечення резервного живлення робочих станцій

Розглянуті вище блоки безперебійного живлення можуть забезпечити роботу комутатора, маршрутизатора чи іншого пристрою, який споживає досить небагато енергії. Але їх потужності явно не вистачить для живлення комп’ютера або іншої подібної очислювальної техніки. Тому тут варто шукати більш енергоємкісне рішення. Таким рішенням буде ДБЖ LogicPower LPM – 525VA – P (LP3170). В таблиці 4.2 приведені його можливості.

Таблиця 4.2 — ДБЖ LogicPower LPM – 525VA – P (LP3170)

Кількість розеток	2
Вихідна потужність	525 ВА / 367 Вт
Діапазон вхідної напруги	145 — 290 V
Акумуляторна батарея	вбудована
Тип батареї	Свинцево — кислотний, 12 V, 4.5 А / годин
Тип архітектури	Лінійно — інтерактивні
Час роботи за повного навантаження	10 — 15 хвилин

Рисунок 4.2 - ДБЖ LogicPower LPM – 525VA – P

4.3 Забезпечення резервного живлення сервера

На сервері зберігаються великі обсяги інформації підприємства, втрату яких не можна допустити, з цього виходить, що вимоги до пристрою, який забезпечуватиме аварійне живлення, мають бути більш суворими. Ці вимоги задовільнить ДЖБ Must EO20 – R600W (DS275619). Всі його можливості ілюструє таблиця 4.3.

Таблиця 4.3 — параметри ДЖБ Must EO20 – R600W

Кількість розеток	2
Вихідна потужність	750 ВА / 600 Вт
Вхідна частота	50 Гц
Вихідна напруга	220 V
Вихідна частота	50 Гц
Акумуляторна батарея	зовнішня
Напруга акумулятора	12 V
Кількість фаз	1
Час перемикання на батарею	≤ 4 мс

Рисунок 4.3 — параметри ДЖБ Must EO20 – R600W

4.4 Застосування генератора для довгострокової роботи

Наявність блоків безперебійного живлення вирішують проблему знеструмлення лише частково, оскільки заряд акумулятора з часом закінчується, такі рішення вирішують проблему лише частково, поки не буде задіяно резервний генератор струму.

Електричний генератор — це пристрої, у яких механічна енергія перетворюється в електричну. Широке застосування отримали генератори змінного струму через легкість його отримання і перетворення, а також через простоту конструкції генераторів і двигунів[4]. На рисунку 4.4 показана модель генератора змінного струму.

Генератором струму для мережі, яка розробляється, буде виступати дизельний генератор Daewoo DDAE 10500DSE – 3G, потужністю 6 кВт. Він оснащений автоматичним регулятором напруги (AVR), вольтметром, даитчиком рівня палива, лічильником мотогодин. Час його автономної роботи становить 12 годин, а рівень споживання палива — 1.65 літри на годину роботи. Після відновлення електропостачання система AVR автоматично відключить живлення від генератора.

Рисунок 4.5 — генератор Daewoo DDAE 10500DSE – 3G

ВИСНОВОК

У процесі виконання магістерської роботи було проаналізовано актуальні тенденції розвитку телекомунікаційних мереж. Було детально розглянуто

топології комп’ютерних мереж, середовища розповсюдження сигналів, принципи роботи комутаційних мережевих пристроїв та їх функціональні можливості. Також розглядалася еталонна модель взаємодії відкритих систем (модель OSI) та її рівні, на основі яких проектуються телекомунікаційні мережі.

Розроблено фізичну модель комп’ютерної мережі, яка детально показує, як мережеве обладнання та робочі станції розташовуються у межах приміщення.

Також була побудована логічна модель мережі за допомогою середовища моделювання та симуляції Cisco Pocket Tracer, яка детально демонструє, як інформація передається по мережі, налаштування комутаторів та маршрутизатора, та на які віртуальні мережі поділена телекомунікаційна мережа і як ці підмережі взаємодіють між собою.

Було вибране відповідне обладнання, а саме комутатори, маршрутизатор, сервер, робочі станції, які відповідають сучасним вимогам.

Для підвищення надійності і сталості роботи було розроблено систему резервного живлення при аварійному відключенні електроенергії. Вона включає в себе блоки безперебійного живлення, які мають акумулятори, та дизельний генератор.

За результатами проведених досліджень було спроектовано телекомунікаційну мережу, яка розташована на трьох поверхах та розділена на три відділи:

1. Конструкторський відділ.
2. IT — відділ.
3. Відділ технічної підтримки.

Користувачі можуть взаємодіяти в рамках одного відділу, а різні відділи не мають доступу один до одного.

Наявність блоків безперебійного живлення запобігає різкому відключенню пристроїв при знеструмленні, а наявність генератора дасть продовжити роботу далі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Борисова Л.В. Основи побудови телекомунікаційних систем та мереж: конспект лекцій / Л.В. Борисова. — Харків: Національний університет цивільного захисту України, 2017 — 205с.

2. Жураковський Б.Ю. Комп’ютерні мережі: навчальний посібник / Б.Ю. Жураковький, І.О. Зенів. — Київ: КПІ імені Ігоря Сікорського, 2020 — 328с.

3. Приходько С. І. Віртуальні локальні мережі VLAN: конспект лекцій / С.І. Приходько, О.С. Жученко, М.А. Штомпель, С.В. Сколота. - Харків: Українська державна академія залізничного транспорту, 2018 — 42с.

4. Співак В.М. Загальна електротехніка і основи електроніки: навчальний посібник / В.М. Співак, А.М. Гуржий, А.Т. Нельга, О.С. Ітякін. - Київ: НМЦ МОУН, 2020 — 267с.

5. Мірошниченко Т.Ю. Дослідження протоколу «Ethernet» та його можливостей при побудові комп'ютерних мереж: збірник наукових праць / Т.Ю. Мірошниченко, А.М. Сільвестров. - Полтава: Національний університет «Полтавська політехніка імені Юрія Кондратюка», 2023 — 140с.

6. Воробієнко П.П. Телекомунікаційні та інформаційні мережі: підручник / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. - Київ: САММІТ — Книга, 2019 — 708с.

7. Л.Ю. Спінул Основи цифорової електроніки : курс лекцій / Л.Ю. Спінул, В.А. Святенко. - Київ: КПІ імені Ігоря Сікорського, 2022 — 118с.

8. Мережева модель OSI. — Режим доступу: https://uk.wikipedia.org/wiki.

9. Мережевий комутатор. — Режим доступу: https://uk.wikipedia.org/wiki.

10. Карпов Ю.О. Теоретичні основи електротехніки: конспект лекцій. / Ю.О. Карпов, С.Ш. Кацив, В.В. Кухарчук, Ю.Г. Ведміцький. - Вінниця: ВНТУ, 2017 — 26с.

11. Організація комп'ютерних мереж. — Режим доступу: https://kremenetskyy.blogspot.com/2017/10/blog-post.html.

12. Сервер ARTLINE Business R17v14. — Режим доступу: https://artline.ua/product/server-artline-business-r17v14.

13. Джерело безперебійного живлення (ДБЖ) LPM-525VA-P (367Вт). — Режим доступу: https://logicpower.ua/ua/ibp-lineyno-interaktivnye/istochnik-bespereboynogo-pitaniya-ibp-lpm-525va-p-367vt.

14. Технічні характеристики ПК HP 200 G4 22. — Режим доступу: https://support.hp.com/ua-uk/document/ish_4694132-4196652-16.

15. Cisco Packet Tracer / Courses. — Режим доступу: https://www.netacad.com/courses/packet-tracer.

16. Кузьменко М.І. Теорія графів: навчальний посібник. / М.І. Кузьменко. - Київ: КПІ імені Ігоря Сікорського, 2020 — 71с.

17. Зайцев В.Г. Операційні системи: навчальний посібник. / В.Г. Зайцев, І.П. Дробязко. - Київ: КПІ імені Ігоря Сікорського, 2019 — 240с.

18. Fedora Linux Srever. — Режим доступу: https://fedoraproject.org/server/.

19. Intel® Core™ i5-10400F Processor. – Режим доступу: https://ark.intel.com/content/www/us/en/ark/products/199278/intel-core-i5-10400f-processor-12m-cache-up-to-4-30-ghz.html.

20. Tanenbaum A.S. Computer Networks: Fifth ediдtion. / A.S. Tanenbaum, Wetherall D.J. - University of Washington Seattle, WA, 2018 – 962c.

ДОДАТКИ

1 BASIC ELEMENTS OF NETWORK TECHNOLOGIES

1.1 Network topologies

The "bus" topology assumes that all network devices are connected to one cable (Figure 1.1), at the ends of which there should be plugs (terminators). Based on this technology, 10 Megabit Ethernet networks (10Base – 2, 10Base – 5) are being built. As a rule, coaxial cable is used. Such a network is easy to configure and install, cheap, if one workstation fails, the network continues to work. But if there is a malfunction in any part - there is no place, then the entire network fails. It is quite difficult to find faults. Low performance compared to other topologies.

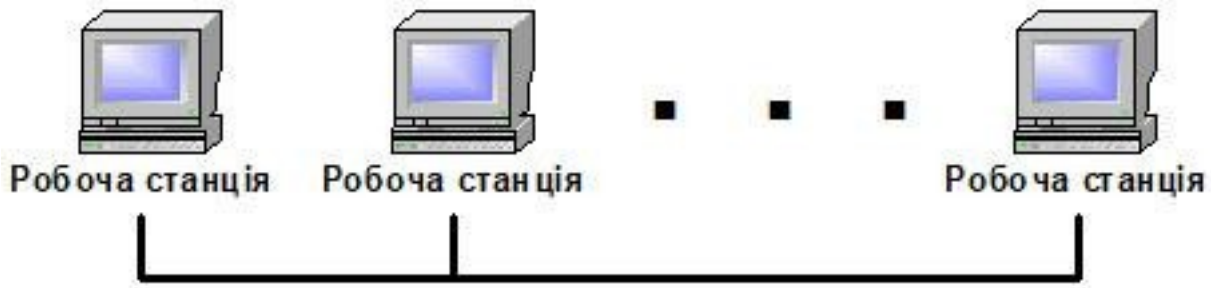


Figure 1.1 — Bus topology

A "ring" topology assumes that all workstations are connected by a physical ring. Twisted pair and optical fiber are mainly used as a data transmission medium. Messages circulate in a circle. If the computer recognizes the data addressed to it, it copies it to the internal buffer. Message transfer time increases in proportion to the increase in the number of workstations in the network. This topology is not used for Ethernet networks.

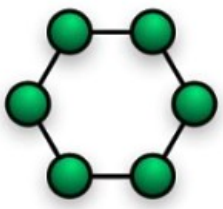


Figure 1.2 — Ring topology

At the heart of the local network, which is built according to the "star" topology (Figure 1.3). Its principle is that each computer or other device is connected by a cable not to another computer, but to special network equipment, which can act as a hub, switch, or router. The advantage of such a topology is that if the connection between one of the connected devices and, for example, switches, is broken, the rest of the network continues to work.

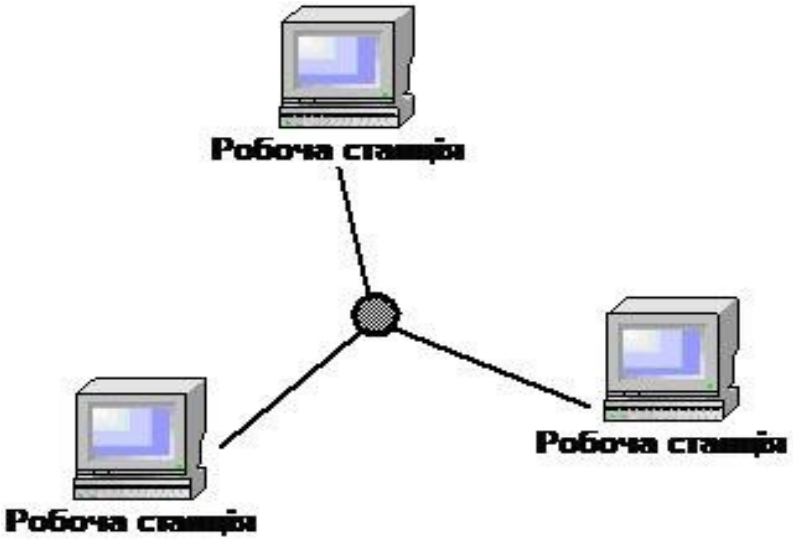


Figure 1.3 - Star topology

True, if this device was the only server, then it will be quite difficult to restore the network. If the hub (or other "center") fails, the network will stop working. This topology has an advantage when searching for damage to network elements: cable, network adapters, connections, etc.. This topology is also useful when adding new devices to the network. Twisted pair and fiber optic cables are used as a data transmission medium. Currently, 100 and 1000 Mbit Ethernet networks are built mainly according to the "star" topology.

1.2 Cable systems

Communication lines are an integral part of any telecommunications network. A communication line generally consists of a physical medium through which electrical information signals are transmitted, data transmission equipment, and

intermediate equipment. a synonym of the term communication line (line) is the term communication channel (channel)[2].

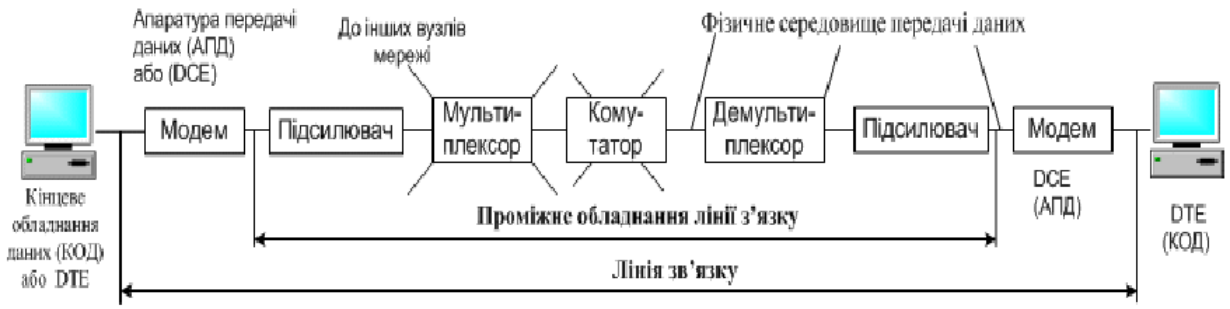


Figure 1.4 — Diagram of a communication line

The diagram of the communication channel is shown in Figure 1.4. The data transmission medium can be either a cable (Figure 1.5) — a set of conductors and insulating sheaths — or the earth's atmosphere or outer space, through which electromagnetic waves propagate (Figure 1.6).

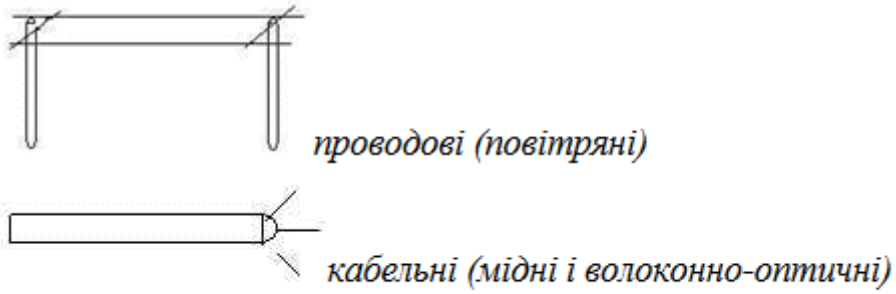


Figure 1.5 — Wire and cable communication channels

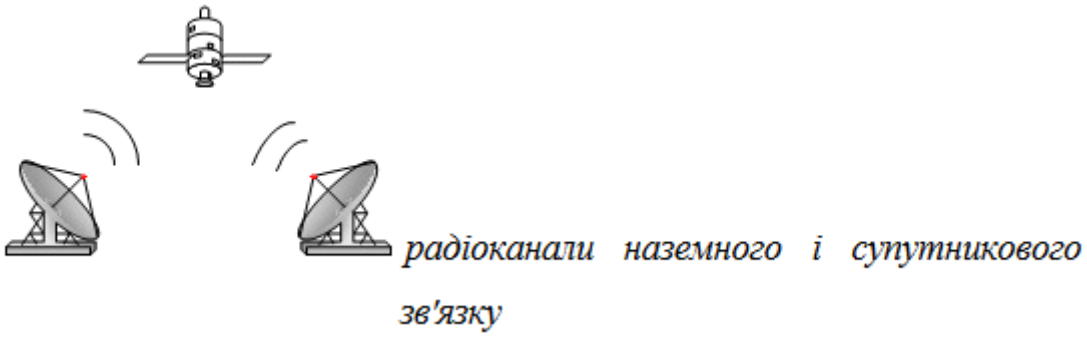


Figure 1.6 — Satellite communication channel

Wired communication lines are wires without insulation, which are laid on poles and hang in the air. Such communication lines, as a rule, are used to transmit

telephone or telegraph signals, and if necessary, they can also transmit computer data. Data transfer speed and immunity in such lines are far from the best, so today they are quickly replaced by cable communication channels.

Cable lines are a rather complex structure. The cable consists of conductors wrapped in several layers of insulation: electrical, electromagnetic, mechanical, and possibly climatic. The cable can be equipped with connectors that allow you to quickly connect various equipment to it[2].

There are three main types of cables used in computer networks:

1. Cables based on a twisted pair of copper conductors.
2. Coaxial cables with a copper core.
3. Fiber optic cables.

The twisted pair or twisted pair cable type is the most common. It contains two or more pairs of conductors. In each pair, the conductors are twisted together along the entire length of the cable. This allows you to increase the interference resistance of the cable and reduce the influence of the signal in each pair on all others. The maximum transmission distance when using it is 1.5-2.0 km, and the maximum speed is 1.2 Gbit/s. The duration of signal propagation is 8-12 ns/m. Attenuation of the signal is 12-28 dB at 100 m at a frequency of 10 MHz.

The most common medium for data transmission over short distances (up to 100 meters) is unshielded twisted pair UTP (Unshielded Twisted Pair). UTP twisted pair is eight copper wires twisted in pairs in common insulation. It is the most common and cheapest twisted pair, however, in the case of its operation, there are problems with electromagnetic compatibility [2].

There are also shielded versions of twisted pair:

1. FTP (Foiled Twisted Pair) – foil twisted pair.
2. STP (Shielded Twisted Pair) – shielded twisted pair.

Compared to UTP, shielded versions of twisted pair have a wider transmission frequency range, less electromagnetic radiation, but their price is much more expensive, and they are also more difficult to install. This is shown in more detail in Table 1.1.

Table 1.1 — Comparative characteristics of twisted pairs

Name	UTP	FTP	S/FTP	S/STP
Price in $ for 1 km	200-300	280-420	460-690	700-1050
Maximum frequency, MHz	100	150	300	300
Thickness, mm	5.1	6.2	6.5	7.3
Installation	Easy	Easy	Easy	Hard
Grounding	Easy	Hard	Easy	Easy

Coaxial cable (coaxial) has an asymmetric design and consists of an internal copper core and a braid separated from the core by a layer of insulation. There are several types of coaxial cable, differing in characteristics and areas of application — for local networks, for global networks, for cable television, etc. [2].

The structure of a coaxial cable is shown in Figure 1.7.

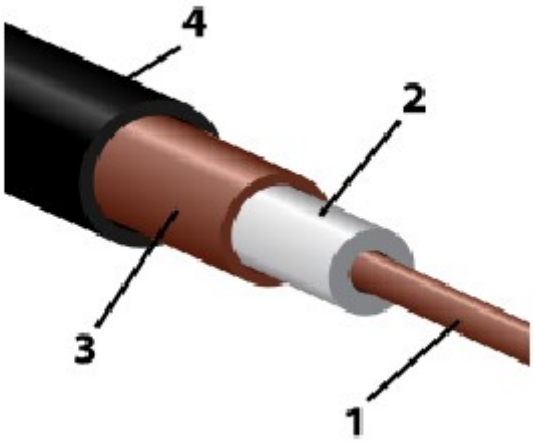


Figure 1.7 — Structure of a coaxial cable

1 — Central vein.

2 — Internal insulation.

3 — Metal braid.

4 — Outer shell.

Until recently, it was widely used and quite popular due to the fact that it has better immunity than twisted pair. Since this type of cable has a wider bandwidth (more than 1 GHz), it is more difficult to mechanically connect to it for unauthorized eavesdropping, and it also emits significantly less electromagnetic radiation outside [2]. But the installation and maintenance of such a cable is more difficult than that of a twisted pair, the cost is 1.5 to 2 times higher. Installation of connectors at the ends of the cable is also more complicated. Due to these factors, it is now used less often.

An optical fiber consists of thin (5-60 microns) fibers through which light signals propagate. This is the highest quality type of cable — it provides data transmission at a very high speed (up to 10 Gbit/s and higher) and, moreover, better than other types of transmission medium, it provides data protection from external interference. The structure of a fiber-optic cable is shown in Figure 1.8.

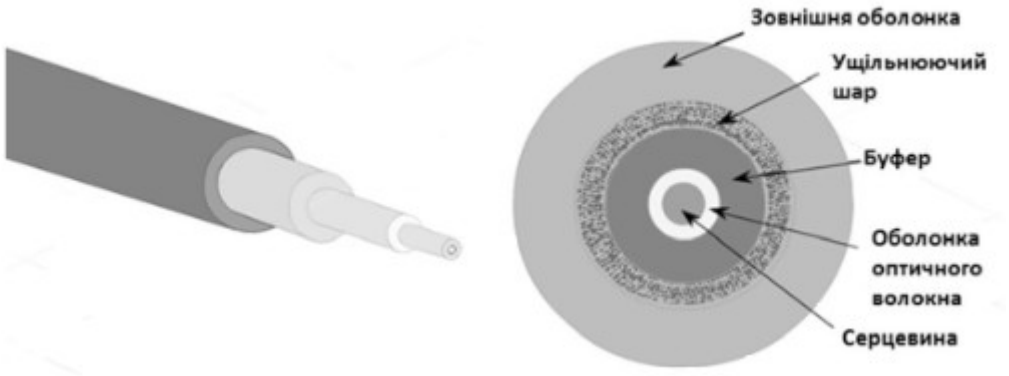


Figure 1.8 — Structure of a fiber optic cable

In the center of the cable there is a core — a core, through which signals are transmitted in the form of modulated light pulses. A shell with a high refractive index is arranged around the core, thanks to which the light beam is reflected into the core of the VOK. This prevents scattering of light when passing through the cable. All this is protected by the outer shell. It can be made in the form of armored weaving of steel or plastic.

Fiber optic cables are of 2 types: single-mode and multi-mode.

The thickness of the core in the single-mode cable corresponds to the wavelength of the light signal (~10μm), the attenuation of the signal is insignificant. Light is generated by semiconductor lasers. The maximum transmission speed reaches 200 Gbps, and the transmission distance is up to 110 km.

In a multimode cable, there are several cores, it is possible to send several data streams at the same time. Transmission distance up to 2-3 km.

Fiber optic cable has many advantages: long transmission distance (the signal in the fiber almost does not fade), high data transfer speed, high interference immunity (no dependence on electromagnetic interference), protection against unauthorized connection. The main disadvantages are the high cost of the cable and the equipment for connecting it, and the cable itself is very sensitive and has poor flexibility. Due to these factors, fiber optic cables are used in the creation of main communication lines, where the communication range is important.

Terrestrial and satellite radio channels will be formed using a radio wave transmitter and receiver. There are a large number of different types of radio channels, differing both in the frequency range used, 75 and the range of the channel. The short, medium and long wave bands (KX, CX and XX), also called the amplitude modulation bands (Amplitude Modulation, AM) according to the type of signal modulation method used in them, provide long-distance communication, but at a low data transfer rate. The channels operating on the ultra-short wave (UHF) bands, which are characterized by frequency modulation (Frequency Modulation, FM), as well as the ultra-high frequency bands (MHF or microwaves) [2] are faster.

Each network device is equipped with an antenna that is both a receiver and a transmitter of electromagnetic waves that propagate in the atmosphere or vacuum at a speed of 3 * 108 m/s.

The electromagnetic spectrum has many ranges. There are areas of frequency bands that have been allocated for use by devices that do not require a license from the supervisory authorities. These are PC peripherals, wireless LANs, wireless phones. Such devices operate on frequency bands of 900 MHz, 2.4 GHz, and 5 GHz.

Wi-Fi technology is used to build wireless local computer networks. This is a commonly used name for the IEEE 802.11 standard for transmitting digital data streams over radio channels[2]. The IEEE 802.11n standard uses the 2.4 GHz frequency band. The IEEE 802.11ax (Wi-Fi 6) standard, which uses the 5 GHz frequency band, is also gaining popularity.

1.3 Communication tools of the network

The OSI/ISO model is a concept of the application of open standards aimed at ensuring interoperability between different systems, which allows to minimize the number of agreements that are not directly related to the organization of the connection between systems. The first version of the OSI/ISO model standards was released as the X.200 standard. The work on the standardization of the OSI/ISO model, in which ISO and ITU-T jointly participate, continues to this day [1].

This model involves 7 levels as shown in Table 1.1.

Table 1.1 — Levels of the OSI model

№ layer	Name	Short name
7	Application	A
6	Presentation	P
5	Session	S
4	Transport	T
3	Network	N
2	DataLink	DL
1	Physical Link	PL

At the physical level, it describes how bits of information are placed in the data transmission medium. It can be twisted pair, coaxial cable, fiber optic cable or radio channel. At this level, the main characteristics are bandwidth, immunity, wave resistance, etc. Physical interfaces of devices with the transmission medium and devices between which bits are transmitted are also implemented.

The channel layer is responsible for the quality of information transmission between two network nodes that are connected by a physical channel, taking into account the characteristics of the data transmission environment. If a connection is established between two end systems that are not directly connected, it will involve several independently functioning physical data links. At the same time, the physical medium of transmission may differ (copper, optical fiber, ether). The requirements for the data presentation format in each channel, which is called linear coding[1], may also be incompatible. In this case, the channel layer performs the function of data adaptation to the type of physical communication channel. A block of data at the channel level is called a frame. Another important function of the link layer is channel access control, frame synchronization, data flow control, addressing, connection establishment and disconnection. Datalink level protocols:

1. HDLC is a high-level data link control procedure for serial connections.

2. IEEE 802.2 – provides logical channel management, as well as media access control (MAC).

3. Ethernet (IEEE 802.3) is a local network based on the CSMA/CD protocol.

4. Token Ring (IEEE 802.5) is a network architecture with a "ring" topology developed by IBM and operating at a speed of 4 Mbit/s.

The network layer is a complex layer that performs the most important function of a telecommunications network — it provides communication between network end devices. This is ensured by providing an end-to-end channel that is switched with individual sections according to the optimally chosen route, a logical virtual channel or direct routing of the data block during its delivery. The main function of the network layer is routing. It consists in deciding through which specific intermediate points the route of data transmission sent from one end system to another should pass, and how the switching (corresponding to a specific route) should be performed between the inputs and outputs of network devices located at the intermediate points of the network[2]. The main protocols of the network layer are IPv4, IPv6, ICMP, IGMP, IPX.

The transport layer provides control and error-free data transmission between two network users. The higher the complexity of the protocols of the transport layer is inversely proportional to the reliability of the services of the lower layers (network, channel and physical). This requires breaking large blocks of data into smaller pieces, called segments, because the network layer defines a maximum packet size, called the Maximum Transmission Unit (MTU), which depends on the maximum packet size imposed by the entire data link. The amount of data in the segment must be small enough to accommodate the network layer header and the transport layer header. The transport layer also controls the reliability of a given connection between the source and destination host through control flow, error control, and consistency and existence validation. The transport layer will also provide confirmation of successful data transfer and send further data if no errors are detected. The main protocols of the transport layer: TCP, UDP, SCTP.

The session layer establishes, configures, monitors, and terminates connections between two or more hosts. The session layer provides communication session (session) management functions focused on end-to-end message transfer, such as, for example, session establishment and termination; management of queue and mode of data transmission (simplex, half-duplex, duplex); synchronization; session activity management; drawing up reports on emergency situations. Together with the session transport layer, the layer forms connection-oriented protocols and protocols that provide reliable connectionless service to higher layers[2]. Session level protocols: RPC, PAP, L2TP, gRPC.

The presentation layer sets the format of the data and the conversion of the data to the format defined by the application layer, as well as the reverse conversion. Provides data presentation in consistent formats and syntax, translation and interpretation of programs from different languages, data encryption and compression. Representation layer protocols: AFP, ICA, LPP, NCP, NDR, XDR, X.25 PAD.

The application layer is the layer that is closest to the user and it means that the user interacts with the application in which the client-server architecture is

implemented. An example of such applications is a web browser, e-mail services, a file server. This level provides services directly to the user's application programs, identifies and establishes the presence of application processes, and also establishes and agrees procedures for error elimination and information integrity management [1].

Repeaters - perform the function of reproducing signals and thus allow you to extend the maximum length of the cable segment. Ethernet segments connected by repeaters create a single separated transmission environment or collision domain, meaning that only one device can transmit in all segments. The purpose of such relaying of signals consists exclusively in increasing the length of the network[2].

A hub is a multiport repeater. Because of this, it connects all devices to the network.

Hubs sometimes intervene in the exchange, helping to resolve some obvious exchange errors. In any case, they work at the first level of the OSI model, since they deal only with physical signals, with the bits of the packet and do not analyze the content of the packet, considering the packet as a whole. Transceivers and repeaters work on the first level.

At the moment it is considered obsolete, almost not used. It was replaced by switches and routers.

Figure 1.9 — Appearance of the hub

Bridges also connect network segments, but unlike repeaters, they have a certain logic. It, like a repeater, reproduces the signal that comes to it. But it also has

the ability to check the physical address that comes in the packet that the data is divided into during transmission. Bridges forward only those network packets that are needed on a particular network segment. There are many packet filtering algorithms for bridges. Bridges divide the network into segments (subnets). The bridge table is initially empty, but as soon as the bridge receives and forwards the packet, it creates an entry in its table with the source address and destination interface. Since then, the bridge knows from whom each packet comes, to which destination, from which interface. The bridge also makes a record of the destination information using the information contained in the packet. The bridge stores a correspondence table between the MAC addresses of devices and the numbers of its ports to which the segments with these devices are connected[2].

The switch uses a "star" topology and is a 2nd device level and functionally represents a multi-port bridge, to each port of which a separate host, hub, server or router can be connected[2].

It performs network segmentation (dividing the network into subnets). It also provides a mechanism for high-speed inter-segment exchange of information.

When connecting to the terminal device of the network (workstation or other equipment), a two-way (duplex) communication mode is established.

The switch has an internal MAC address table, where each port is assigned the MAC address of the device connected to it. Such a table can be created by the network administrator, or it can be created automatically by the switch. With the help of the table of addresses and addresses of the recipient, the switch organizes a virtual connection of the sender's port with the recipient's port and transmits the packet through this connection.

Table 1.2 — Switch MAC address table

MAC – address	Number of the port
A	1
B	2
C	3
D	4

In Figure 1.10, node A sends a packet to node D. When the switch finds the recipient address in its virtual table, it forwards the packet to port 4.

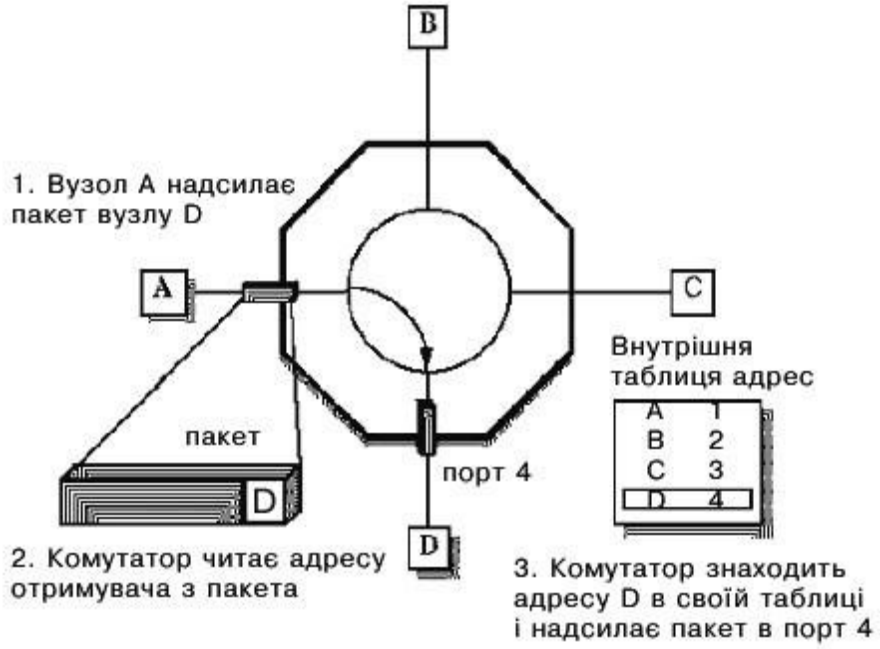


Figure 1.10 - Virtual connection

The virtual connection remains for the duration of the transmission of one packet, for each new packet the virtual connection is established again based on the address contained in the given packet.

The packet arrives only on the port to which the addressee is connected, other users (in our case — B and C) do not receive this packet. With this technology, switches provide security features that are not available to hubs and repeaters.

Data transfer between any pair of ports occurs independently, which means that the entire bandwidth of the channel is allocated to each virtual connection. The 10 Mbit/s switch in Figure 1.11 allows simultaneous transmission of a packet from A to D and from port B to port C with a bandwidth of 10 Mbit/s for each connection.

Each connection is allocated a bandwidth of 10 Mbit/s, so the total bandwidth of the switch shown above is 20 Mbit/s. In the case when data is transferred between a larger number of port pairs, the bandwidth is expanded accordingly. For example, a 48-port, 100 megabit Ethernet switch can provide a total bandwidth of 2400 Mbps.

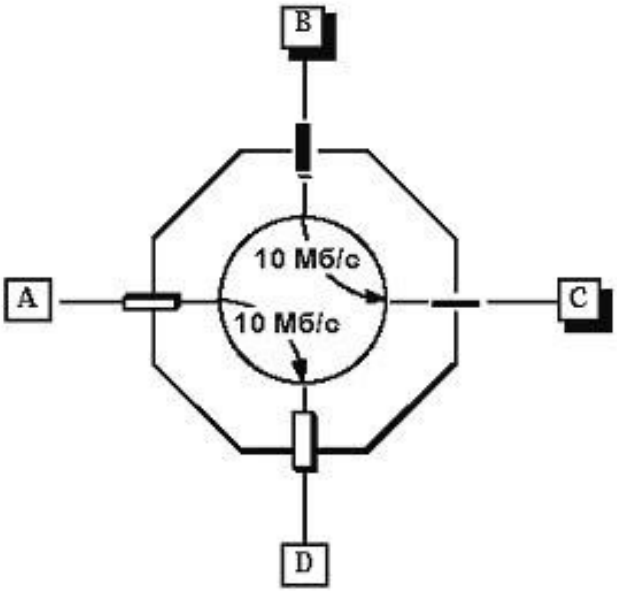


Figure 1.11 — Simultaneous connection

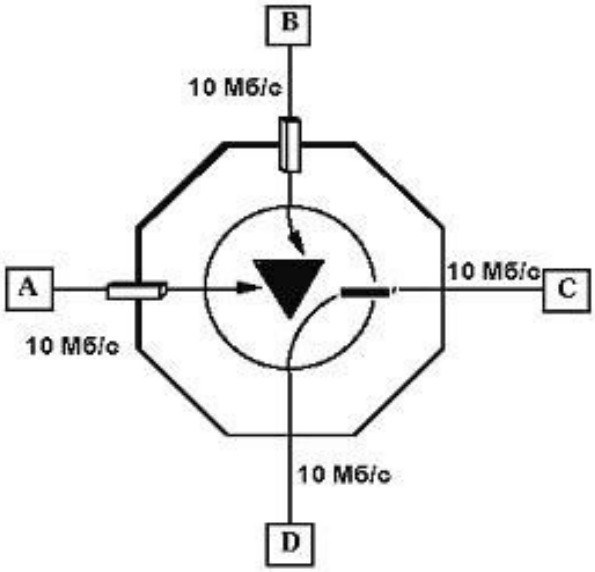


Figure 1.12 — Block option

The high throughput of the switch is ensured only if a simultaneous connection is organized between all pairs of ports. But real traffic is usually a one-to-many situation (for example, many network users are accessing the same server). In this mode of operation, the bandwidth of the switch given in the example will not exceed 10 Mbit/s. In this mode of operation, the switch will not have a significant advantage compared to a conventional hub or repeater.

In Figure 1.12, three nodes A, B, and D transmit data to node C. The switch stores packets from nodes A and B in its memory until the packet transmission from node D is completed. After the packet transmission is completed, the switch starts transmitting packets from nodes A and B, which are stored in the memory of the switch.

In this case, the bandwidth of the switch is determined by the bandwidth of the C channel (in this case, 10 Mbit/s).

One of the most important parameters is the performance of the switch. The following indicators are used as performance parameters:

1. Speed of data transfer between ports.

2. Total bandwidth.

3. Delay.

Data transfer speed between ports. At a bandwidth of 10 Mbps, Ethernet can transmit 14,880 packets of minimum size (64 bytes) per second (PPS). This characteristic depends on the properties of the data transmission medium. In this case, it can be said that the switch fully utilizes the capabilities of the network, providing users with the maximum bandwidth.

Total bandwidth. It is measured in Mbit/s or PPS and indicates the maximum speed at which packets can be transmitted through the switch to the addressees. For example, if all switch ports have a maximum speed of 10 Mbps, the total bandwidth is equal to the maximum port speed multiplied by the number of virtual connections that can exist at the same time (the number of ports divided by 2). The switch, which is capable of providing the maximum transmission speed, has no internal blocking.

Delay. The delay reduces the time interval between receiving the package from the sender and transferring it to the addressee. The delay is measured with respect to the first bit of the packet. Because the recipient address is placed at the beginning of the packet, the Ethernet switch starts transmitting before the packet is fully received from the sender. This technology is called "switching on the fly (cut-through)" and ensures minimal delay. This is important because the delay directly affects the speed of the switch. But this method does not check packets for errors, so when a switch

uses this method, it forwards all packets, including those that have errors. Also, on-the-fly switching cannot be used when transferring packets from a port that has a low speed to a port that has a higher speed (for example, from a 10 Mbit/s port to a 100 Mbit/s port). Failure to apply packet buffering will result in errors.

Low latency improves the performance of networks in which data is transmitted as a sequence of individual packets, each of which contains the address of the recipient. In networks where data is transmitted in the form of a sequence of packets with a virtual channel organization, low latency has less impact on performance.

Routers are devices that interconnect networks with different network addresses. It operates at three layers of the OSI model. At the physical level, it restores the received signal. At the channel level, the router checks the physical addresses (source and destination) contained in the packet. At the network level, the router checks network-level addresses (IP-level addresses).

Functions that the router can perform:

1. Connect local networks.

2. To connect together general purpose networks.

3. Connect local networks to general purpose networks.

There are three main differences between a router with a repeater or a bridge:

1. A router has a physical and logical (IP) address for each of its interfaces.

2. The router acts only on those packets in which the address of the recipient corresponds to the address of the interface where the packet arrives. This is true for a unicast, multicast, or broadcast address.

3. The router changes the physical address of the packet (both source and destination) when it forwards the packet[2].

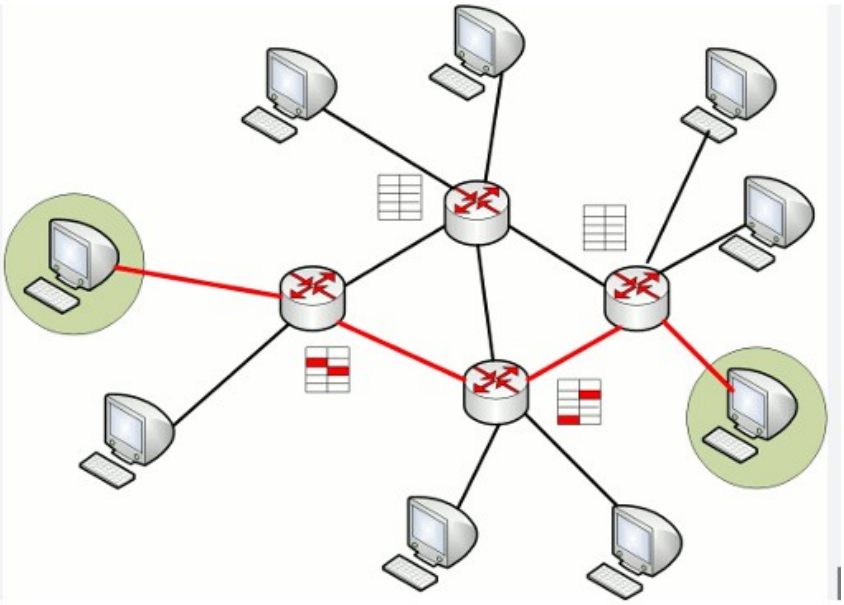


Figure 1.13 — Network diagram using routers

Unlike a bridge/switch, which does not have information about how the network segments outside its ports are connected, a router analyzes all existing subnet connections, so it can choose the route that is optimal for some criterion in the presence of several alternative routes. The decision to choose one or another route is made by each router through which the packet passes.

The operation of routers depends on network protocols and is determined by the protocol-related information transmitted in the packet.

A network gateway (Figure 1.14) is a device for connecting networks that use different protocol stacks or separate protocols. The gateway can work at all levels of the ISO/OSI model. Gateways are used to connect systems that use different data structures and formats, coding, and have different architecture[2].

Depending on the purpose, the gateway can use all levels of the OSI model, or it can be limited to several or one.

A network adapter (network controller, interface) is an interface whose main function is to connect a computer (or other device) to the network and create a communication channel. It operates on the first and second layers of the OSI model.

Figure 1.14 — Appearance of the network gateway

The network adapter can be made as a separate expansion card that is mounted in a PCI or PCI-e slot or be integrated into the system board of a computer or other network device. Modern computer motherboards have an integrated network interface that supports data transfer rates of up to 1 Gbps. The network adapter interacts both with the system bus of the computer (knowing its trunk address, sending data to and from the computer, generating a processor interrupt signal, etc.), and provides functions of communication with the network.

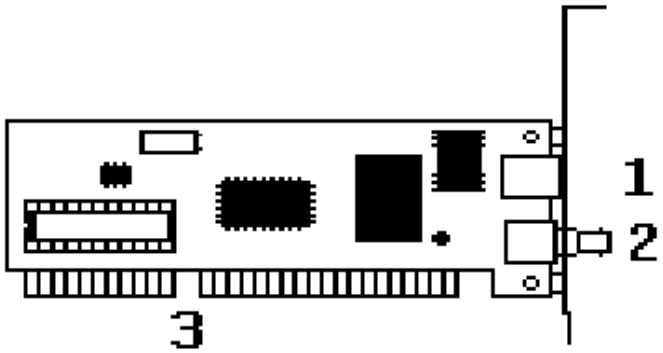


Figure 1.15 — Diagram of a network card

1 — RJ-45 connector (for twisted pair);

2 — coaxial cable connector;

3 — PCI slot connector.

УДК 621.9

А.М. Сільвестров, д.т.н., професор

Т.Ю. Мірошниченко, студент

Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ДОСЛІДЖЕННЯ ПРОТОКОЛУ «ETHERNET» ТА ЙОГО МОЖЛИВОСТЕЙ ПРИ ПОБУДОВІ КОМП'ЮТЕРНИХ МЕРЕЖ

Комп'ютерна мережа – невід'ємна частина сучасної інформаційної інфраструктури. Це комунікаційна система, яка дозволяє користувачам комп'ютерів (в даному випадку - мережних робочих станцій) обмінюватися інформацією, спільно використовувати прикладні програми, передавати файли між комп'ютерами, розділяти доступ і спільно використовувати ресурси комп'ютерів, а також таких пристроїв, підключених до мережі, як принтери, плотери, диски, модеми, ін.

Постійне зростання можливостей і продуктивності комп'ютерів обумовило зростання вимог до ефективності функціонування мереж.

Ethernet – найпопулярніший протокол кабельний комп'ютерних мереж, працює на фізичному та канальному рівні мережевої моделі OSI. Станом на 2016 рік близько 85 % усіх комп'ютерів у світі були підключені до комп'ютерних мереж по протоколу Ethernet. Цей протокол відноситься до сімейства протоколів стандарту IEEE 802.3, характеристиками якого є:

– топологія - шина;

– середовище передачі - коаксіальний кабель;

– швидкість передачі — 10 Мбіт/с;

– максимальна довжина мережі - 5 км;

– максимальна кількість абонентів - до 1024;

– довжина сегмента мережі - до 500 м;

– кількість абонентів на одному сегменті - до 100.

Ethernet було спроєктовано згідно з технологією CSMA/CD (множинний доступ з контролем несучої та виявленням колізій). Хоча з широким застосуванням мережевих комутаторів та способу передачі «повний дуплекс» проблема виникнення колізій в мережах Ethernet майже не зустрічається.

Як середовище передачі даних – використовуєть вита пара. Існує також стандарт для застосування в мережі оптоволоконного кабелю. Для обліку цього у стандарті IEEE 802.3 були зроблені відповідні зміни.

В 1995 році був ввдений додатковий стандарт для Ethernet, що працює на швидкості 100 Мбіт/с (так званий Fast Ethernet, стандарт IEEE 802.3u), що використовує як середовище передачі кручену пару або оптоволоконний кабель. В 1997 році з'явилася й версія на швидкості 1000 Мбіт/с (Gigabit Ethernet, стандарт IEEE 802.3z).

Існують основні топології Ethernet: шина (послідовне з‘єднання комп‘ютерів за допомогою Т-подібних роз‘ємів (Т-конекторів)), зірка та розширена зірка (з‘єднання комп‘ютерів за допомогою комутуючого обладнання).

Модифікації Ethernet:

1. 10 Мбіт/с Ethernet підтримує стандарти: 10BASE5 (товстий коаксіальний кабель); 10BASE2 (тонкий коаксіальний кабель); 10BASE-T (кручена пара); 10BASE-FL (оптоволоконний кабель).

2. Fast Ethernet (100 Мбіт/с) підтримує стандарти: 100BASE-T4 (зчетверена кручена пара); 100BASE-TX (здвоєна кручена пари); 100BASE-FX (оптоволоконний кабель).

3. Gigabit Ethernet (1 Гбіт/с).

4. 10 Gigabit Ethernet (10 Гбіт/с).

5. 40/100 Gigabit Ethernet (40/100 Гбіт/с).

Мережа Ethernet не відрізняється ні рекордними характеристиками, ні оптимальними алгоритмами, вона поступається за рядом параметрів іншим стандартним мережам. Але завдяки потужній підтримці, найвищому рівню стандартизації, величезним обсягам випуску технічних засобів мережі Ethernet

набули величезної популярності, вистіснивши такі застарілі технології, як Arcnet, FDDI і Token ring.

ЛІТЕРАТУРА:

1. Батаєв О.П. Теорія електричного зв'язку: навчальний посібник / О.П. Батаєв, І.В. Ковтун, Н.А. Корольова. - Харків: Українська державний університет залізничного транспорту, 2010. - 650с.

2. Жураковський Б.Ю. Комп'ютерні мережі: навчальний посібник / Б.Ю. Жураковський, І.О. Зенів. - Київ: КПІ ім. Ігоря Сікорського, 2020. - 328с.

3. Борисова Л.В. Основи побудови телекомкнікаційних систем та мереж: конспект лекцій / Л.В. Борисова. - Харків: Національний університет цивільного захисту України, 2017 – 205с.

STUDY OF THE "ETHERNET" PROTOCOL AND ITS POSSIBILITIES IN BUILDING COMPUTER NETWORKS

A. M. Silvestrov, Doctor of Science, Professor,

T.Y. Miroshnychenko, Master's student.

National University «Yuri Kondratyuk Poltava Polytechnic»