МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему:

«Віртуальні локальні мережі VLAN в малих локальних та побутових мережах SOHO»

Завідувач

випускаючої кафедри **Довбиш А.С.**

Керівник роботи **Великодний Д.В.**

Студента групи ІК.мз – 91с **Кулеба В.В.**

СУМИ 2020

Сумський державний університет

(назва вузу)

Факультет *ЕЛІТ* Кафедра *Комп'ютерних наук*

Спеціальність *«Інформатика»*

Затверджую:

зав.кафедрою _____

_____

"_____" _____ 20___р.

ЗАВДАННЯ

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТОВІ

Кулебі Віктору Вікторовичу

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) *Віртуальні локальні марежі VLAN в малих локальних та побутових мережах SOHO*

затверджую наказом по інституту від "____" _____ 20 ___ р. № _____

2. Термін здачі студентом закінченого проекту (роботи) _____

3. Вхідні данні до проекту (роботи) _____

_____

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)
1) Огляд існуючих рішень. Постановка задачі. 2) Огляд Cisco Packet Tracer та Cisco IOS як програмного середовища симуляції VLAN. 3) Моделювання, побудова, та тестування різних типів VLAN у мережах SOHO

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

6. Консультанти до проекту (роботи), із значенням розділів проекту, що стосується їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання
_____

Керівник _____

Завдання прийняв до виконання _____

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломного проекту (роботи)	Термін виконання проекту (роботи)	Примітка
11	*Огляд існуючих рішень щодо VLAN. Постановка задачі*	07.08-07.09	
32	*Огляд Cisco Packet Tracer та Cisco IOS як програмного середовища симуляції VLAN*	10.10-20.10	
43	Розробка інформаційного та програмного забезпечення системи управління мережевими сервісами	20.10-20.11	
54	Оформлення пояснювальної записки	21.11-23.11	

Студент – дипломник _____

Керівник проекту _____

РЕФЕРАТ

Записка: 88 стор., 90 рис., 5 табл., 1 додаток, 41 джерело.

Мета роботи – дослідження теоретичних основ, методів і засобів побудови віртуальних локальних мереж у малих та побутових локальних мережах.

Об'єктом дослідження є віртуальні локальні комп'ютерні мережі VLAN.

Предметом дослідження є внутрімережевий трафік VLAN, транкування портів та каналів, процес інкапсуляції кадрів, а також маршрутизація трафіку між VLAN.

Методи досліджень. Для вирішення поставлених задач використано методи системного аналізу та програмної симуляції.

Результати – спроектовано та розгорнуто різні типи віртуальних локальних мереж на різних мережевих вузлах. Мережі побудовані у програмному симуляторі Cisco Packet Tracer з використанням команд консолі CLI.

VIRTUAL LOCAL AREA NETWORK, SMALL OFFICE HOME OFFICE NETWORK, ПРОГРАМНИЙ СИМУЛЯТОР CISCO PACKET TRACER, КОМАНДИ CISCO IOS, ПРОГРАМНА СИМУЛЯЦІЯ VLAN.

ЗМІСТ

ВСТУП……...….....….4

1 ВІРТУАЛЬНІ МЕРЕЖІ VLAN……..……..…..…….....5

1.1 Особливості віртуальніх локальних мереж та їх призначення..... 5

1.2 Необхідність VLAN для малих локальних та побутових мереж та їх переваги.…7

1.3 Класифікація віртуальних локальних мереж.....9

1.4 Тегування (маркування) кадрів в мережах VLAN.....12

1.5 Магістральні (транкові) порти (Trunk Links) та порти доступу (Access Links) в мережах VLAN.....15

1.6 Магістралі віртуальних мереж VLAN.....19

1.7 Маршрутизація між VLAN.....23

1.8 Постановка задачі.....28

2 CISCO PACKET TRACER ЯК ПРОГРАМНЕ СЕРЕДОВИЩЕ СИМУЛЯЦІЇ VLAN У МАЛИХ ЛОКАЛЬНИХ ТА ОФІСНИХ МЕРЕЖАХ 29

2.1 Призначення та переваги Cisco Packet Tracer.....29

2.2 Інтерфейс Cisco Packet Tracer.....21

2.3 Операційна система Cisco IOS та її команди.....41

3 ПОБУДОВА ТА ТЕСТУВАННЯ РІЗНИХ ТИПІВ VLAN В МЕРЕЖАХ SOHO.....54

3.1 VLAN в мережі SOHO на двох комутаторах, з однією міжкомутаторною магістраллю.....54

3.2 VLAN у мережі SOHO на одному комутаторі й маршрутизаторі…….....60

3.3 Мережа SOHO з віртуальними мережами на комутаторі третього рівня та маршрутизаторі з IP-телефонією.....71

ВИСНОВКИ.....87

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....88

ДОДАТОК.....92

Додаток А.....92

ВСТУП

Ще до карантину й локдауну, спричиненими ковід-19, відсоток т.з. домашніх офісів (*Small office Home office, SOHO*) у США складав близько 50% від усіх компаній. Звичайно ж, доля робітників й компаній, що належать до сектору SOHO, різко зросла в умовах ковід-19, і ця тенденція буде й далі рости й поширюватися завдяки перш за все економічним перевагам такого формату.

Малі локальні та побутові мережі (SOHO networks) обслуговують вищезазначений сектор бізнесу, з'єднуючи комп'ютери (як правило від 1 до 10) та інші пристрої в єдину телекомунікаційну мережу.

Серед вимог, що їх висувають до мереж SOHO (окрім суто технічних), на першому плані будуть: економічність, простота конфігурування, масштабованість, безпека.

З точки зору телекомунікаційних технологій мережа SOHO представляє собою не що інше, як локальну мережу, тобто LAN, і здебільшого базується на технологіях Ethernet та Wi-Fi, з усіма недоліками: порушення вимог до безпеки й конфіденційності даних в спільному комунікаційному середовищі; ризик перевантаження й обвалення мережі як загального широкомовного домена; негнучкий, неефективній розподіл ресурсів незалежно від трафіку; зниження реальної швидкості передачі даних в сильно завантаженій мережі, аж до її повної зупинки, через конфлікти в середовищі передачі даних.

Існують різні способи вирішення цих недоліків, які можна поділити на фізичні (або апаратні) й логічні. Приклад фізичного рішення – придбання дорогого спеціального обладнання (розумних комутаторів) або використання окремих комутаторів для утворення різних доменних групп.

Але ці ж самі проблеми можна вирішити набагато простіше й ефективніше за допомогою логічних засобів, головним з яких є віртуальні локальні мережі, VLAN.

1 ВІРТУАЛЬНІ МЕРЕЖІ VLAN

1.1 Особливості віртуальніх локальних мереж та їх призначення

Віртуальною локальною мережею VLAN (Virtual Local Area Network) прийнято називати логічно сгруповані вузли мережі, кадри яких є ізольованими від інших вузлів тієї ж фізичної мережі [3].

Віртуальні локальні мережі не є стандартизованими й потребують використання програмного забезпечення виробника (правила побудови віртуальних локальних мереж за стандартом IEEE 802.1Q не залежать від протоколу канального рівня, тому не відносяться до налаштувань комутатора). [5]

У локальних мережах, що включають комутуючі пристрої, використання технології віртуальних мереж являє собою спосіб об'єднання користувачів в робочі групи незалежно від їх географічної позиції (рис 1.1).

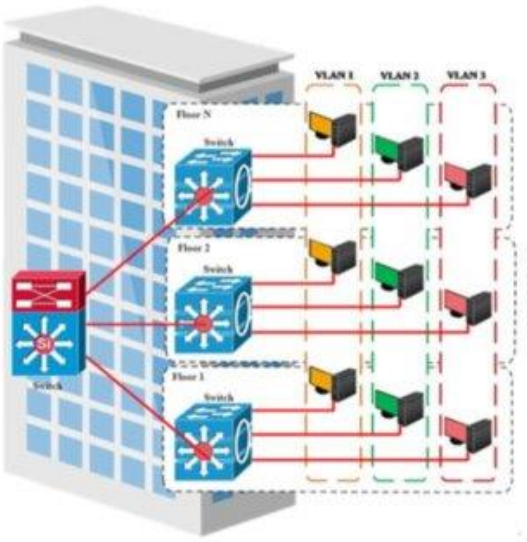

Рисунок 1.1 – VLAN об’єднують користувачів незалежно від географічної позиції та підключених портів комутатора/комутаторів [4]

Пристрої в мережах VLAN працюють таким чином, ніби знаходяться у власній незалежній мережі, навіть якщо поділяють загальну фізичну інфраструктуру з іншими VLAN. Будь-який комутаційний порт може належати будь-якій мережі VLAN. Пакети одноадресної, багатоадресної та широкомовної розсилки пересилаються і розсилаються тільки на термінальні пристрої в межах вихідної

мережі VLAN цих пакетів [5]. Мережа VLAN є ізольованим широкомовним доменом (рис. 1.2).

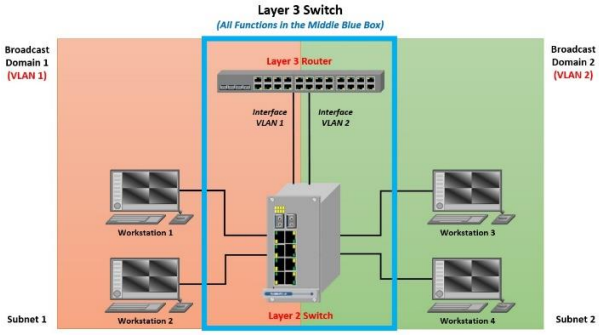

Рисунок 1.2 – Кожна VLAN являє собою окремий широкомовний домен [5]

Сегментація у віртуальній мережі і в фізичній локальної мережі розрізняються тим, що віртуальні мережі функціонують на 2-ми 3-му рівнях еталонної моделі OSI, а обмін інформацією між віртуальними мережами забезпечується маршрутизацією 3-го рівня [11] – пакети, адресовані пристроям, які не належать до VLAN, повинні пересилатися через пристрій, що підтримує маршрутизацію, тобто маршрутизатор (рис. 1.3).

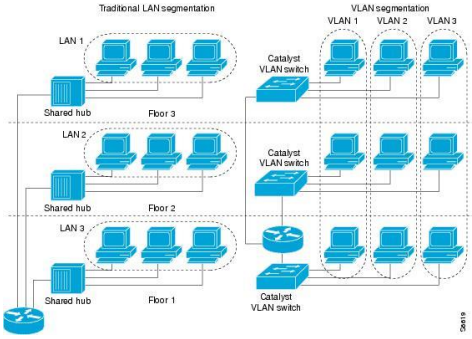

Рисунок 1.3. Різниця між традиційною сегментацією LAN та VLAN-сегментацією [11]

Комп’ютер може входити до складу кількох VLAN, утворюючи точку перетину віртуальнх мереж. [18]

Обгрунтуємо необхідність віртуальних мереж для SOHO LAN.

1.2 Необхідність VLAN для малих локальних та побутових мереж та їх переваги

➢ **Необхідність VLAN для безпеки мережі.** Класична мережа Ethernet це фізичне середовище спільної комунікаії. При цьому за допомогою спеціального ПЗ можна перехопити конфіденційні повідомлення, паролі, і т.д. Часто сегментувати таку мережу фізично немає змоги через географічні та інші обмеження. За допомогою віртуальних локальних мереж можна об'єднати всіх користувачів за рівнем доступа, правами, обов'язками, належністю до певного відділу й т.д. незалежно від місця їх знаходження. VLAN утворюють додатковий рівень безпеки, передаючи трафік в межах однієї віртуальної мережі. Якщо фрейми є одноадресними, вони будуть відправлятися тільки на один заданий порт призначення, а не всім користувачам, тобто комутатор з налаштуваннями VLAN фільтрує трафік [1].

➢ **Необхідність VLAN у боротьбі з засиллям широкомовного трафіку.** Широкомовні повідомлення надсилають усім вузлам мережі єдиного домену, які мусять їх обробляти. Наприклад, в протоколах TCP/IP такі повідомлення використовують для протокола ARP, оновлення таблиць маршрутизації. В залежності від апаратного забезпечення широкомовні повідомлення можуть в більшій чи меншій мірі послаблювати виробничу здатність робочих станцій – процесор перериває своє функціонування, припиняючи виконання додатків для користувача. Якщо це стає реальною проблемою (широкомовний шторм, що може паралізувати мережу), її можно вирішити, сегментуючи мережу на дрібніші широкомовні домени [17].

➢ **Необхідность VLAN для покращення пропускної здібності.** При безпосередньому підключенні користувачів до одного сегменту вони колективно використовують його пропускну здібність. Логічно, що середнє значення пропускної здібності буде мати зворотню залежність від кількості користувачів. Віртуальні локальні мережі забезпечують користувачам більшу пропускну здатність, ніж у умовах спільного комунікаційного середовища. Кожна станція

VLAN приймає той трафік, який їй належить, використовуючи пропускну здібність в повній мірі. Тому в комутованій мережі є можливим паралельне передавання даних в межах одного широкомовного домену [1].

➢ **Необхідність VLAN для боротьби з затримками даних.** При передаванні даних через транзитні сегменти, коли фрейми проходять через маршрутизатори, перекидування їх з вхідного порту на вихідний займає більший час, ніж прохождення через порти комутаторів. Об'єднання в функціонально однорідні логічні групи видаляє необхідність транзиту пакетів через маршрутизатори й вивільняють багато часу, особливо в випадку протоколів з відправкою підтвердження (send acknowledge) [3].

➢ **Необхідність VLAN для спрощення списків доступу.** Списки контроля доступу є способом контролю трафіку в мережі. Вони дають можливість різних рівней деталізаціїї керування доступом (від індивідуальних користувачів до всіх користувачів мережі або мереж) в цілях безпеки, або керування пропускною здібністю. Складання списків – це клопітка й масштабна робота, що займає багато часу й потребує ресурсів. Технологія VLAN суттєво спрощує завдання побудови списків доступу, адже локальні мережі можно вважати групами користувачів з однаковими правами доступу [2].

Отже, VLAN надають локальним мережам суттєві переваги, що важко переоцінити [1]:

1. Безпека. Трафік логичних груп повністю відокремлений від решти мережі, що сприяє захисту конфіденційної інформації через обмеження витоку вразливих даних.

2. Регулювання обсягу доменів широкомовної розсилки. Розподіл мережі на VLAN зменшує кількість термінальних пристроїв в домені широкомовної розсилки.

3. Продуктивність. Зменшуються затримки даних. Поділ суцільних мереж другого рівня OSI на логічні групи (широкомовні домени) обмежує зайвий мережевий трафік, підвищуючи продуктивність.

4. Економія. Відпадає необхідність в дорогому обладнанні, технічних апгрейдах мережевої інфраструктури завдяки більш ефективному використанню наявної смуги пропускання та висхідних каналів.

5. Розподіл ресурсів. Користувачі з однотипними вимогами до мережі використовують ту ж саму мережу VLAN й одні види трафику (еластичний чи real-time).

6. Керування мережею. Спрощується складання списків доступу. Якщо в мережу підключається новий комутатор, до нього застосовуються вже готові налаштування. Назва VLAN, як правило, несе в собі інформацію про її функціональне призначення.

1.3 Класифікація віртуальних локальних мереж

У сучасних мережах використовується різноманітні VLAN. Типи VLAN можуть визначатися за різними критеріями, серед яких: класи трафіку, гнучкість, особливості кадрів, функції, і т.д. Розглянемо найсуттєвіші з них.

Дефолтні та назначені VLAN

За можливістю конфігурації віртуальні мережі можна поділити на VLAN за замовчуванням та назначені VLAN.

Дефолтні VLAN. Після першого завантаження комутатора всі його порти стають частиною VLAN по дефолту. Порти комутатора в межах VLAN за замовчуванням належать до одного широкомовного домену. Тобто будь-яке обладнання, підключене до будь-якого порту комутатора, може й буде обмінюватися даними з іншими пристроями на інших портах цього комутатора. Для комутаторів Cisco мережею VLAN за замовчуванням призначена VLAN 1. VLAN 1 підтримує всі функції будь-якої мережі VLAN, але її не можна видалити або навіть перейменувати. По дефолту весь керуючий трафік 2-го рівня пов'язаний з мережею VLAN 1 [12].

Назначені VLAN. Вони конфігуруються адміністратором, який дає їм назви. Їх можна перейменовувати та видаляти.

Різновиди VLAN за типами трафіку (керуюча VLAN, VLAN даних, голосова VLAN)

*VLAN даних***.** Віртуальна локальна мережа даних призначена й налаштовна виключно для передачі трафіку, що його генерує користувач. VLAN даних не розрахована на передачу трафіку керування або голосового трафіку. Сепарація голосового й керуючого трафіку від даних користувача – це best practice. Мережі даних використовуються для функціональної сегментації мережі на групи користувачів або пристроїв [1].

Керуюча VLAN. Це будь-яка мережа VLAN, налаштована для доступу до функцій управління комутатора. Мережа VLAN 1 (принаймі в Cisco) є керуючою VLAN по дефолту. Щоб створити керуючу віртуальну мережу, треба призначити IP-адресу й маску підмережі віртуальному інтерфейсу комутатора (SVI) даної VLAN. Після цього комутатором можна керувати за за допомогою таких протоколів, як HTTP, Telnet, SSH або SNMP. Що стосується кількості керуючих мереж, сучасні комутатори можуть підтримувати більше одного інтерфейсу SVI. Але ж, хоча комутатор може підтримувати більш ніж одну керуючу VLAN, на практиці це майже не реалізується, бо збільшує вразливість до мережевих атак. Окрім цього, з точки зору мереж SOHO LAN в цьому немає практичної потреби [16].

Голосова мережа VLAN. Для підтримки передачі real-time голосового трафіку по IP (VoIP) потрібна окрема мережа VLAN. Це викликано високими вимогами для пропускання VoIP-трафіку [18]:

• гарантована смуга пропускання, щоб забезпечити високу якість голосової передачі;

• пріоритетність передачі у порівнянні з іншими типами мережевого трафіку;

• можливість маршрутизації для обходу перевантажених відрізків;

• затримка менше ніж 150 мс (по всій мережі).

Тобто вся мережа мусить бути заранше спроектована для підтримки VoIP-трафіку (рис. 1.4).

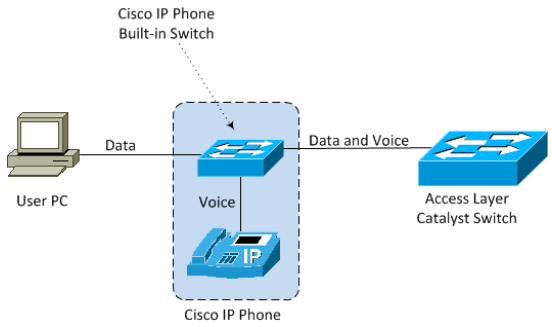

Рисунок 1.4 – Відокремлення голосового трафіку від трафіку даних [16]

Статичні й динамічні VLAN

З точки зору того, на якій основі будуються VLAN і, відповідно, наскількі гнучкими вони є, розрізняють статичні й динамічні віртуальні мережі.

Статичні віртуальні мережі. Статичні VLAN зазвичай будуються на основі одного комутатора. Кожен з портів комутатора призначають певній мережі, і це призначення залишається незмінним (для змін треба конфігурувати порти вручну). Це так званий механізм групування в мережі портів. Кадр, що належить до певної мережі, ніколи не потрапить до порту іншої віртуальної мережі. Теоретично порт можна приписати декільком віртуальним мережам, але на практиці це навряд чи реалізується – втрачається сенс сегментації на віртуальні мережі. У даному сценарію віртуальних локальних мереж не може бути більше, ніж портів у комутатора [1].

Але ця техніка погано пристосована до використання у віртуальних мережах на базі двох комутаторів. Якщо вузли однієї окремої мережі під'єднані до портів різних комутаторів, ще пару портів треба виділити для з'єднання саміх комутаторів. Тобто для з'єднання комутаторів між собою треба стільки ж портів, скільки VLAN вони підтримують (не кажучи вже про порти для під'єднання віртуальних мереж). А ще додаткові порти комутатора знадобляться для підключення до маршрутизатора, тому в мережах, що базуються на кількох комутаторах, портів може просто не вистачати.

Динамічні віртуальні мережі. Динамічні VLAN здійснюють автоматичний моніторінг того, які вузли призначають до яких віртуальних мереж. За умови

використання інтелектуального ПЗ мережевого керування можно формувати динамічні віртуальні мережі на основі MAC-адрес, протоколів, або навіть додатків. В цьому випадку найчастіше апаратна адреса користувача прописується в централізованому управлінні віртуальною мережею. Якщо користувач з даною апаратною адресою переміститься в інший сегмент мережі, база даних відшукає цю адресу й сконфігурує порт для потрібної VLAN, новий порт комутатора буде автоматично приписаний до тієї ж самої віртуальної мережі. Попереднє створення бази даних треба виконувати вручну. Адміністратор позначає всі апаратні адреси (що внесені у таблиці кожного комутатора) віртуальними номерами. Групування певних MAC-адрес у віртуальну адресу виключає необхідність поєднувати їх кількома портами. MAC-адреса фактично стає міткою віртуальної мережі [1].

VLAN з тегованими та та нетегованими кадрами

За особливостями кадрів можна розрізняти VLAN з тегованим (маркованим) та не-тегованим (немаркованим) трафіком.

1.4 Тегування (маркування) кадрів в мережах VLAN

Тегований трафік – різновид динамічної VLAN, в якій використовується інформація про приналежність до певної мережі, що вбудована в кадр.

Тегування може відбуватися за різними протоколами. Для порівняння розглянемо пропраєтарний протокол міжкомутаторного каналу (InterSwitch Link - ISL) від Cisco та універсальний стандарт IEEE 802.1q. Використання ISL зараз не схвалюється навіть самим виробником, і ми будемо розбирати його з точки зору історичної цікавості, і на його тлі буде розглянутий найпопулярніший стандарт IEEE 802.1q.

Протокол міжкомутаційного каналу (InterSwitch Link, ISL)

ISL - це метод власного тегування, який підтримується лише на обладнанні Cisco за допомогою швидких та гігабітних ліній Ethernet. Розмір кадру ISL починається від 94 байт і збільшується до 1548 байт за рахунок накладних витрат (додаткових полів), які протокол розміщує в тому кадрі, що він тегує (рис. 1.5).

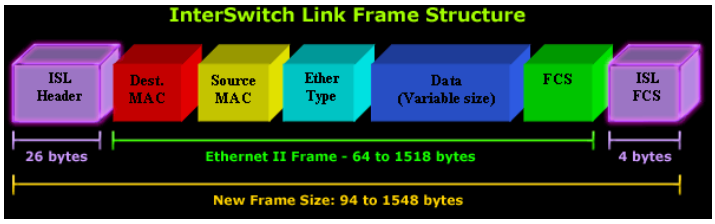

Рисунок 1.5 – Структура кадру ISL [21]

У схемі нас цікавить перш за все ISL Header та контрольна сума ISL Frame Check Sequence (FCS). Решта показаного кадру Ethernet - це стандартний фрейм Ethernet II [21].

Заголовок ISL. ISL Header (рис 1.6) – поле з 26 байт, що містить всю необхідну інформацію про VLAN (як і слід було очікувати), щоб дозволити просування кадру по магістральній лінії та знайти маршрут до місця призначення.

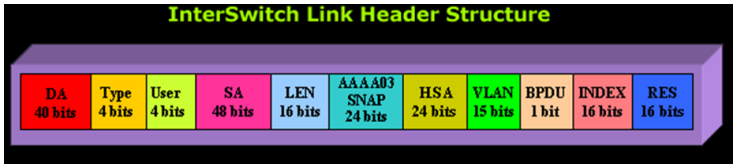

Рисунок 1.6 – Структура заголовку ISL [21]

Як видно, заголовок ISL складається з досить багатьох полів (11), але лише декілька з цих полів суттєво важливі.

Стандарт тегування IEEE 802.1q

Як вже згадувалося, метод тегування IEEE 802.1q є найпопулярнішим, оскільки він дозволяє інтегрувати пристрої, що підтримують VLAN, від усіх постачальників, які підтримують протокол. Механізм тегування IEEE 802.1q здається досить простим та ефективним завдяки 4-байтовому полю накладних витрат між адресою джерела та полем Тип (Type) у кадрі Ethernet II (рис. 1.7)

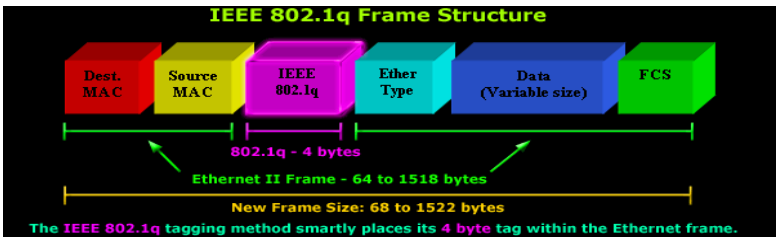

Рисунок 1.7 – Кадр з тегом IEEE 802.1q [19]

Процес вставки тегу 802.1q в кадр Ethernet II призводить до того, що оригінальне поле Check Check Sequence (FCS) стає недійсним, оскільки змінюється кадр. Отже, набуває актуальності перерахування FCS на основі нового кадру, що тепер містить поле IEEE 802.1q. Цей процес автоматично виконується комутатором безпосередньо перед тим, як він відправляє кадр по магістральній лінії зв'язку [19]. Тут зосередимося на рожевому блоці, позначеному як заголовок IEEE 802.1q.

Заголовок IEEE 802.1q. Як зазначалося, заголовок 802.1q має довжину лише 4 байти або 32 біти, тоді як у цьому просторі вміщається вся інформація, необхідна для успішної ідентифікації VLAN кадру та забезпечення його надходження до правильного пункту призначення. Діаграма нижче аналізує всі поля, що містяться в заголовку 802.1q (рис 1.8).

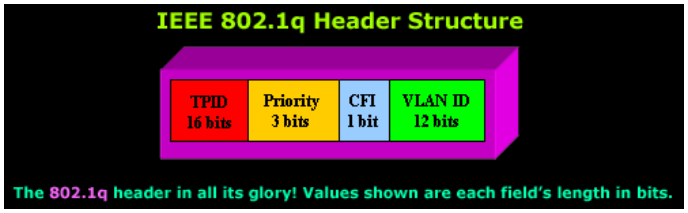

Рисунок 1.8– Структура заголовку IEEE 802.1q [19]

Структура досить проста, оскільки маємо лише 4 поля в порівнянні з 11 ISL.

Поле ідентифікатора протоколу тегів (TPID). Поле TPID має довжину 16 біт зі значенням 0x8100. Він використовується для ідентифікації кадру з тегами IEEE 802.1q.

Наступні три поля, Priority, CFI та VLAN ID, також відомі як поле TCI (Tag Control Information) і часто представлені у вигляді одного поля (поле TCI).

Поле пріоритету (Priority). Поле Priority має лише 3 біти, але воно використовується для встановлення пріоритетності даних, які несе цей кадр. Пріоритетність даних дозволяє нам надати особливий пріоритет сервісам, чутливим до затримки часу, таким як Voice Over IP (VoIP), над звичайними даними.

Поле Priority має приблизно 3 біти, що дозволяє в цілому 2 в третьому ступіні = 8 різних пріоритетів для кожного кадру, тобто від нуля (0) до семи (7) включно.

Поле індикатору канонічного формату (CFI, Canonical Format Indicator). Поле CFI має лише 1 біт. Якщо встановлено на "1", це означає, що MAC-адреса має неканонічний формат, інакше "0" означає, що це канонічний формат. Для комутаторів Ethernet це поле завжди встановлюється на нуль (0). Поле CFI в основному використовується з міркувань сумісності між мережами Ethernet та Token Ring. У тому випадку, коли кадр надходить на порт Ethernet, а прапорець CFI встановлюється на один (1), тоді цей кадр не повинен пересилатися [19], оскільки він був отриманий на будь-який непозначений порт (порт доступу Link).

Поле ідентифікатора віртуальної локальної мережі (VLAN ID, Virtual Local Area Network Identifier). Поле ідентифікатора VLAN ID є, мабуть, найважливішим з усіх, оскільки він дозволяє визначити, до якої VLAN належить кадр, даючи можливість комутаційному комутатору вирішувати, з яких портів кадр може виходити залежно від конфігурації комутатора.

Метод тегування IEEE 802.1q підтримує до 4096 різних VLAN. Це число походить від 12-розрядного поля ідентифікатора VLAN і це 2 в дванадцятому ступіні = 4096, тобто з VLAN 0 на VLAN 4095 включно.

Теговані та не-теговані кадри будуть по-різному оброблятися портами VLAN в залежності від їх призначення.

1.5 Магістральні (транкові) порти (Trunk Links) та порти доступу (Access Links) в мережах VLAN

Trunk Links

Порти комутаторів, які використовують для VLAN з тегованим трафіком на основі стандарту IEEE 802.1q, називають магістральними або транковими (Trunk).

Це теговані/марковані порти. Вони призначені для передачі кадрів Ethernet, що вміщують службові поля з інформацією про віртуальну мережу (відповідно до стандарту IEEE 802.1q), від декількох VLAN. Це уможливлює з'єднання комутаторів мережі тільки одним трактом передачі (що неможливо у VLAN на основі портів). Ще раз хочеться наголосити, що транковий канал призначений для

передачі пакетів для будь-якої VLAN. Магістральні порти зазвичай знаходяться в з'єднаннях між комутаторами [22]. Ці порти можуть нести пакети з усіх доступних VLAN, оскільки VLAN охоплює кілька комутаторів (рис. 1.9).

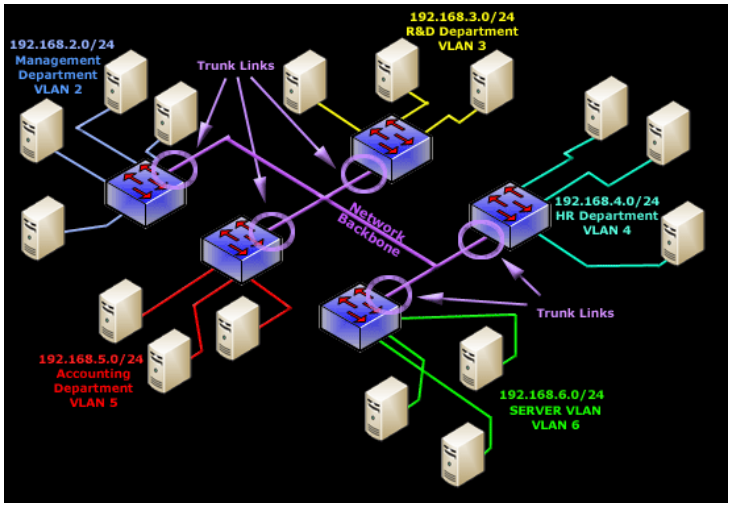

Рисунок 1.9 – Магістральні (транкові) порти між VLAN [22]

Access Links

Для роботи комутатора з несумісним обладнанням,за стандартом IEEE 802.1q, передбачаються порти доступу (Access Link) – нетаговані (немарковані) порти.

Такі порти доступу можуть бути використані для побудови статичних віртуальних мереж за механізмом розподілу портів.

Порти доступу - це найпоширеніший тип на будь-якому комутаторі VLAN. Усі хости мережі підключаються до портів доступу комутатора, щоб отримати доступ до локальної мережі (рис. 1.10). Ці звичайні порти, які можна знайти на кожному комутаторі, але налаштовані спеціально, завдяки чому можна підключити до них комп’ютер і отримати доступ до мережі. Слід зазначити, що термін „Access Link” описує налаштований порт – це означає, що наведені вище порти можуть бути налаштовані за іншим типом – як магістральні [22]. Налаштовуючи порти на комутаторі для роботи в якості Access Link, ми зазвичай налаштовуємо лише одну VLAN на порт, тобто VLAN, до якого пристрій буде мати доступ.

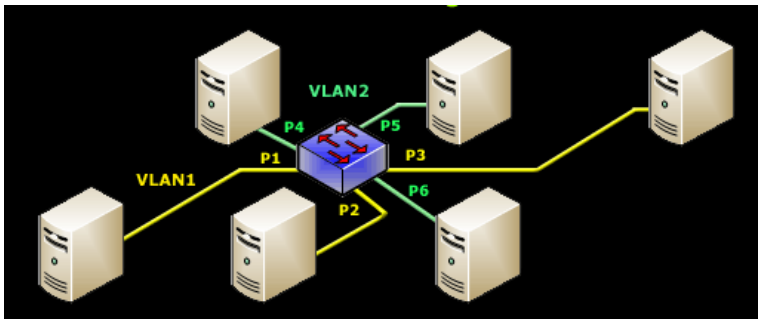

Рисунок 1.10 – Підключення Access Link для доступу до локальної мережі [22]

Важливо відзначити, що будь-який пристрій, підключений до каналу доступу, не знає про VLAN, призначену порту. Пристрій просто припускає, що він є частиною одного домену мовлення, як це відбувається з будь-яким звичайним комутатором. Під час передачі даних будь-яка інформація про VLAN або дані з інших VLAN видаляються, тому одержувач не має про них інформації [18].

Коли мова йде про різницю між Access Link та Trunk Link, треба розрізняти фізичні порти й сконфігуровані.

Зазвичай фізичні гігабітні порти налаштовуються як магістральні, підключаючи комутатор до магістральної мережі зі швидкістю 1 гігабіт, тоді як порти Access Link підключаються на 100 Мбіт (рис. 1.11, рис.1.12).

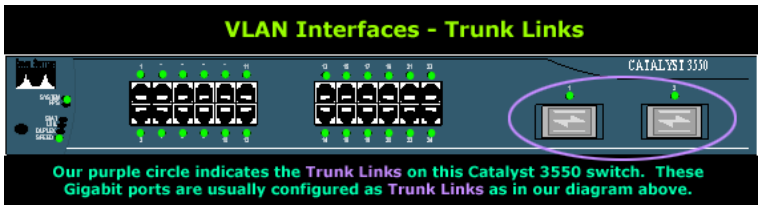

Рисунок 1.11 – Гігабітні порти зазвичай налаштовуються як транкові [22]

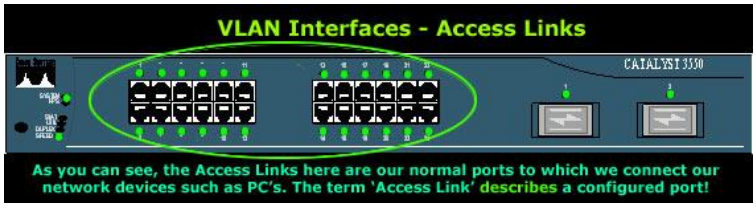

Рисунок 1.12 – 100 Мегабітні порти зазвичай налаштовуються як порти доступу [22]

Крім того, треба зазначити, що для того, щоб порт або лінія функціонували як магістральна лінія, обов'язково потрібно, щоб вони працювали зі швидкістю мінімум 100 Мбіт або більше. Порт, що працює на швидкості 10 Мбіт, не може працювати як магістральна лінія, і це логічно, оскільки транкова лінія завжди використовується для підключення до магістральної мережі, що мусить працювати зі швидкістю більшою, ніж швидкість Access Link [22].

На малюнках фізичних портів вище показані порти, що зазвичай налаштовано як порт доступу або в 95% всіх комутаторів. Залежно від потреб, може знадобитися сконфігурувати 100 Мбіт порт як Trunk Link, і в цьому випадку він, очевидно, вже не називається портом Access Link, а буде називатися Trunk Link [22].

Native VLAN

Стандарт IEEE 802.1q також передбачає передачу кадрів від портів, що не є включеними до жодної VLAN. Це відбувається через тракти передач із магістральними портами (тегованими/маркованими). У цьому сценарії кадри від портів, що не належать до жодної віртуальної мережі, за замовчуванням призначаються до так званої нативної VLAN (Native VLAN), ідентифікатор якої по дефолту є 1. Як правило, Native VLAN використовується для передачі інформації керування комутаторами та маршрутизаторами, а також керування протоколами: STP (Spanning Tree Protocol), VTP (VLAN Trunking Protocol), CDP (Cisco Discovery Protocol) та ін [13].

Мережі Native VLAN визначаються в специфікації IEEE 802.1Q для того, щоб забезпечити зворотю сумісність з нетегованим трафіком (який є більш характерним для застарілих типів локальних мереж). Мережі Native VLAN виступають загальним ідентифікатором на протилежних кінцях транкового канала.

✓ *Теговані кадри в мережі Native VLAN.* Деякі пристрої, що підтримують транкінг, додають тег VLAN в пакети VLAN з нетегованим трафіком (IP-телефони, сервери, маршрутизатори і комутатори не від Cisco). Керуючий трафік, що відправляється в мережі Native VLAN, не слід тегувати. Якщо транковий порт 802.1Q отримає тегований кадр з таким же ідентифікатором VLAN, як у мережі

VLAN з нетегованим трафіком, цей кадр буде відкинуто. Отже, під час налаштування порту комутатора треба налаштувати пристрій таким чином, щоб він не відправляв тегованих кадри по мережі Native VLAN [13].

✓ *Нетеговані кадри в мережі Native VLAN.* Коли транковий порт комутатора Cisco отримує нетеговані кадри (що не мусить бути проблемою в правильно сконфігурованій віртуальній мережі), він пересилає ці кадри в мережу Native VLAN. Якщо жодний пристрій не є пов'язаним з мережею Native VLAN, а також немає інших транкових портів (що також часто трапляється), то кадр відкидається. Мережею native VLAN за замовчуванням є мережа VLAN 1. Тому найкраща практика – налаштувати невикористану віртуальну мережу як Native VLAN) [13].

1.6 Магістралі віртуальних мереж (Trunks)

Магістральний канал, або транк, з точки зору VLAN – це канал з типологією «точка-точка» між двома сегментними вузлами, що підтримує більше однієї віртуальної мережі. Транк віртуальних мереж розповсюджує VLAN по всій мережі вищого щабелю. Зокрема обладнання Cisco підтримує стандарт IEEE 802.1Q для координації магістральних каналів в Fast Ethernet, Gigabit Ethernet і 10-Gigabit Ethernet [20].

Використання магістральних каналів в мережах VLAN не завжди є мандаторним, але відмова від них суттєво обмежує можливості VLAN. Транки віртуальних мереж забезпечують поширення всього трафіку VLAN між комутаторами. В результаті вузли, що підключені до різних комутаторів, але належать до одніє віртуальної мережі, можуть обмінюватися даними без допомоги маршрутизатора [18].

Магістральний канал віртуальних мереж не належить до будь-якої мережі VLAN (рис. 1.13), а функціонує як канал зв'язку між комутаторами і маршрутизаторами для багатьох VLAN. Транк може також з'єднувати мережеві пристрої (за умови, що вони мають адаптер з підтримкою 802.1Q) [18].

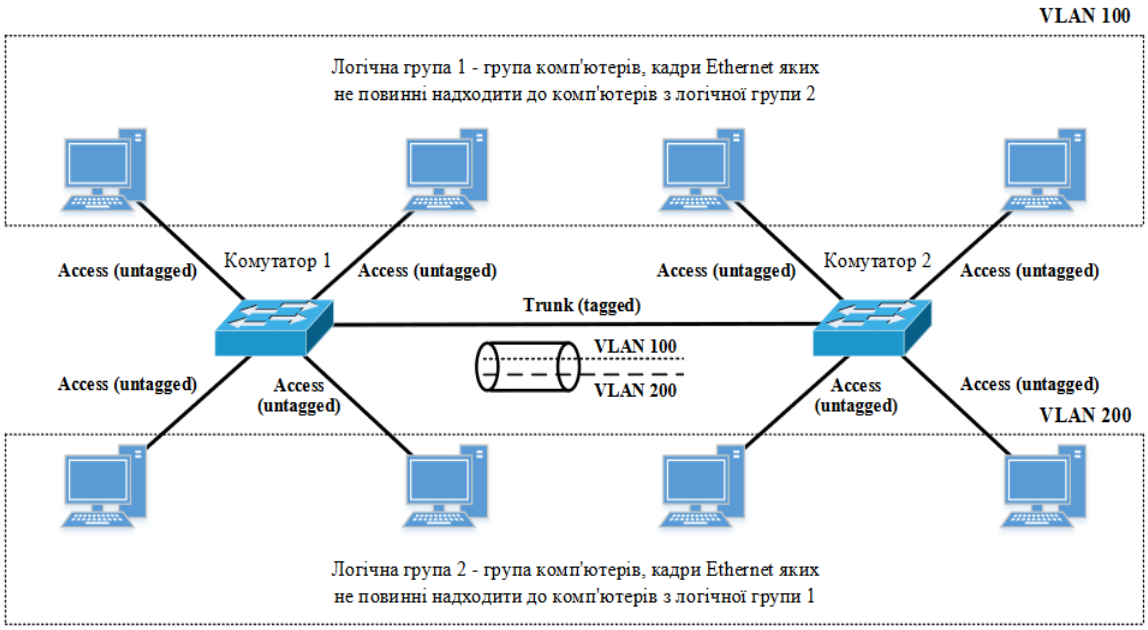

Рисунок 1.13. Магістральний (транковий) канал віртуальних мереж

При створенні магістральних каналів можуть виникати проблеми з застарілим обладнянням або пропраєтарними протоколами. Зокрема, в мережі Ethernet для формування магістральних каналів можуть застосовуватися як мінімум порти Fast Ethernet або Gigabit Ethernet. Крім того, для тегування кадрів віртуальної локальної мережі потрібно внести зміни у кадр Ethernet, а це означає, що тегування кадрів VLAN мусять підтримувати всі комутатори, які беруть участь у цьому. Перш за все, треба визначитися з тим, який протокол буде застосовуватися: протокол міжкомутаторного каналу (Inter Switch Link - ISL), пропраєтарний протокол компанії Cisco, універсальний IEEE 802.lq (що підтримувється усіма компаніями), чи, знову ж таки, новий пропраєтарний протокол Cisco, що зветься протоколом динамічного формування магістральних каналів (DTP) [35].

Якщо в якості методу розмітки кадрів застосовується стандарт IEEE 802.1q, то з'являється можливість забезпечити взаємодію обладнання різних постачальників, а також зберегти стандартний формат фрейму Ethernet, що дозволяє як і раніше використовувати комутатори, які не підтримують IEEE 802.lq, для перенаправлення кадрів без помилок. При використанні стандарту IEEE 802. lq просто вводяться

невеликі зміни в стандартний кадр Ethernet, щоб він міг передавати інформацію розмітки віртуальної локальної мережі. Такий спосіб застосування розмітки є зручним, якщо в мережі необхідно розширити сегмент з використанням недорогого (або несучасного) комутатора. Стандарт IEEE 802.1q підтримується також комутаторами інших постачальників, тому він може застосовуватися і в організаціях, в яких відсутнє мережеве обладнання Cisco. Стандарт IEEE 802.1q передбачає додавання до початкового кадру всього лише чотирьох байтів (порівняно з 11 ISL), тому, крім усього іншого, цей протокол є надзвичайно ефективним. Єдиним реальним недоліком використання методу тегування на основі IEEE 802.1q є те, що він не підтримується в комутаторах Cisco застарілих моделей, і навіть якщо і підтримується, то можливість застосування автоматичного узгодження магістральних портів залежить від конкретної версії програмного забезпечення комутатора.

При автоматичному узгодженні використовується протокол динамічного формування магістральних каналів (Dynamic Trunking Protocol, DTP) – новіший пропраєтарний протокол Cisco. Звичайно ж, такий сегмент VLAN не може бути розширеним за допомогою застарілих комутаторів Cisco або комутаторів інших виробників [35].

Оскільки методи тегування ISL та IEEE 802.lq разглядалися вище, доцільно окремо розглянути протокол DTP.

Протокол динамічного формування магістральних каналів (Dynamic Trunking Protocol, DTP)

DTP це пропраєтарний мережевий протокол канального рівня, розроблений компанією Cisco для реалізації транкінгу в мережі VLAN між двома комутаторами і для інкапсуляції кадрів. Також DTP є таким протоколом , що дозволяє комутаторам динамічно визначати, чи сусідній комутатор є налаштованим для створення магістралі між портами комутаторів, і який протокол використовувати (802.1Q або ISL)

Узгодження характеристик магістральних каналів з використанням динамічного протоколу ISL (Dynamic ISL – DISL) або динамічного протоколу формування магістральних каналів (DTP) дозволяє двом з'єднаним між собою портам узгодити рішення про те, чи стануть вони стати портами магістрального каналу. При такому узгодженні адміністратору не треба налаштовувати конфігурацію з обох сторін магістрального каналу і досить виконати настройку тільки з одного боку. Порт, що знаходиться на іншому кінці каналу, може сконфігурувати необхідні параметри автоматично. [14]

Існують наступні налаштування режиму порту комутатора:

- Switchport mode access (доступ до режиму комутації): Переводить інтерфейс (порт доступу) у постійний режим без зв’язку та веде переговори щодо перетворення лінії зв’язку у не-зв’язану. Інтерфейс стає інтерфейсом, що не перебуває в мережі, незалежно від того, чи є сусідній інтерфейс магістральним інтерфейсом чи ні.
- Switchport mode dynamic auto (режим динамічного автоматичного переключення). Робить інтерфейс здатним перетворити лінію зв'язку в магістраль. Інтерфейс стає магістральним інтерфейсом, якщо для сусіднього інтерфейсу встановлено магістральний або бажаний режим. Типовим режимом комутаційного режиму для нових інтерфейсів комутатора Ethernet Cisco є динамічний автоматичний режим. Якщо два комутатори Cisco залишатимуться з загальним типовим налаштуванням автоматичного, магістраль ніколи не буде формуватися.
- Switchport mode dynamic desirable (бажаний динамічний режим комутаційного режиму). Заставляє інтерфейс активно намагатися перетворити лінію зв'язку в магістральну. Інтерфейс стає магістральним інтерфейсом, якщо для сусіднього інтерфейсу встановлено магістральний, бажаний або автоматичний режим. Це режим комутації за замовчуванням на комутаторах Catalyst 2950 та 3550.
- Switchport mode trunk (комутатор магістрального режиму). Переводить інтерфейс у режим постійного транкінгу та веде переговори про перетворення

сусідньої лінію зв'язку в магістраль. Інтерфейс стає інтерфейсом магістралі, навіть якщо сусідній інтерфейс не є інтерфейсом магістралі.

- Switchport nonegotiate (без переговорів). Заважає інтерфейсу генерувати кадри DTP. Цю команду можна використовувати лише тоді, коли режим перемикання інтерфейсу є доступом або транком. Треба вручну налаштувати сусідній інтерфейс як інтерфейс зовнішньої лінії, щоб встановити магістральну лінію.

1.7 Маршрутизація між VLAN

Мережі VLAN використовуються для сегментації комутованих мереж. Комутатори 2-го рівня можна налаштувати для роботи з більш ніж 4 тисячами мереж VLAN. Мережа VLAN - це домен широкомовного розсилання, тому комп'ютери в різних мережах VLAN не можуть обмінюватися даними без допомоги пристроїв маршрутизації. Можливості протоколів IPv4 та IPv6 на комутаторах 2-го рівня лімітовані, тому що ці пристрої не можуть виконувати функцію динамічної маршрутизації. Хоча комутатори 2-го рівня володіють розширеними функціями IP, наприклад можливістю виконувати статичну маршрутизацію, цього недостатньо для обслуговування такого великого числа мереж VLAN.

Будь-який пристрій, що підтримує маршрутизацію 3-го рівня, наприклад маршрутизатор або багаторівневий комутатор, можна використовувати для виконання основних функцій маршрутизації. Незалежно від пристрою, процес пересилання мережевого трафіку з однієї VLAN в іншу з використанням маршрутизації називають маршрутизацією між VLAN.

Існують різні варіанти маршрутизації між мережами VLAN, які можно поділити на 2 групи:

1) апаратні методи маршрутизації між VLAN (використання маршрутизатора з двома інтерфейсами Ethernet та використання сервера з двома мережевими картами).

2) логічні методи маршрутизації між VLAN (конфігурація ROS (Router-on-a-stick) та комутація 3-го рівня з використанням SVI).

Апаратні методи маршрутизації між VLAN:

Використання маршрутизаторів з двома інтерфейсами Ethernet (рис. 1.14)

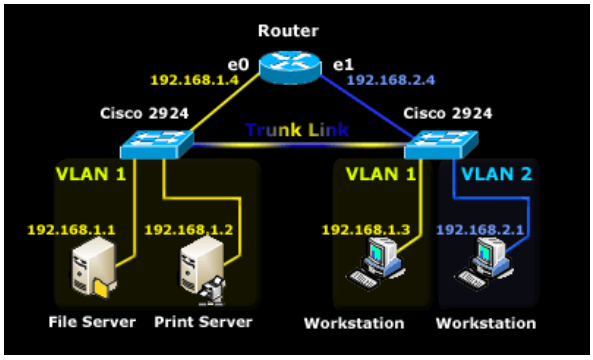

Рисунок 1.14 – Використання маршрутизаторів з двома інтерфейсами Ethernet [20]

Колись це був один з кращих і найшвидших методів маршрутизації пакетів між VLAN. Налаштування досить просте й включає маршрутизатор з двома інтерфейсами Ethernet, як показано на схемі, що під'єднується до обох VLAN з відповідною IP-адресою, призначеною кожному інтерфейсу. Маршрутизація IP, звичайно, включена на маршрутизаторі, і є можливість застосовувати списки доступу в тому випадку, коли потрібно обмежити доступ до мережі між VLAN.

Крім того, кожен хост (сервери та робочі станції) повинен або використовувати інтерфейс маршрутизатора, підключений до їх мережі, як дефолтний шлюз, або потрібно створити запис маршруту, щоб переконатися, що вони використовують маршрутизатор як шлюз до іншої VLAN. Однак цей сценарій є досі дорогим для реалізації, оскільки нам потрібен спеціальний маршрутизатор для маршрутизації пакетів між VLAN, і він також обмежений перспективою розширення.

У випадку, коли існує більше двох VLAN, будуть потрібні додаткові інтерфейси Ethernet, тому в основному ідея полягає в тому, що потрібен окремий

інтерфейс Ethernet на маршрутизаторі, який буде підключатися до кожної VLAN [20].

На завершення цього сценарію, коли мережа розширюється і створюється більше VLAN, вона дуже швидко стає складною і дорогою, тому це рішення виявиться недостатнім для покриття майбутнього зростання.

Використання серверів з двома мережевими картами (рис. 1.15)

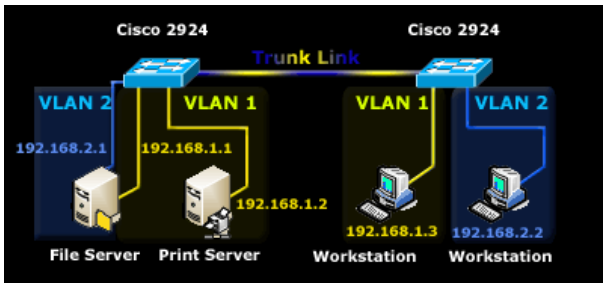

Рисунок 1.15 – Використання маршрутизаторів з двома мереживими картами [20]

Це налаштування одного із серверів для здійснення маршрутизації між двома VLAN, що зменшує загальну вартість, оскільки спеціальне обладнання не потрібно.

Для того, щоб сервер виконував маршрутизацію, йому потрібно більше однієї мережевих карти - по одній для кожної VLAN, та призначені відповідні IP-адреси. Після цього все, що потрібно зробити, це включити IP-маршрутизацію на сервері. Нарешті, кожна робоча станція повинна використовувати сервер або як шлюз, або слід створити запис маршруту, щоб вони знали, як дістатися до іншої мережі. У цій конфігурації немає нічого особливого, вона проста, дешева, і вона робить свою роботу, якщо не потрібно мати багато VLAN [20].

Логічні методи маршрутизації між VLAN:

Маршрутизація між мережами VLAN з використанням методу router-on-a-stick (рис. 1.16)

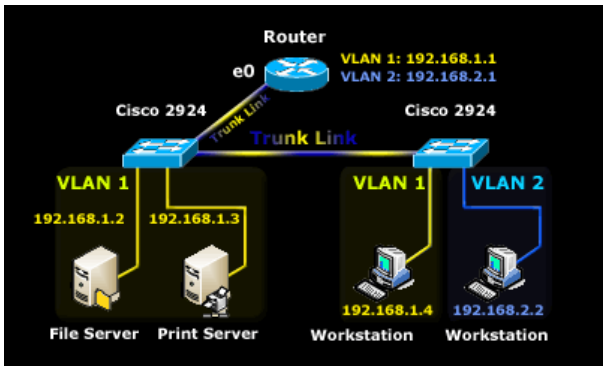

Рисунок 1.16 – Маршрутизація між мережами VLAN з використанням методу router-on-a-stick [20]

На відміну від методу маршрутизації між VLAN, який потребує кількох фізичних інтерфейсів маршрутизатора і комутатора, метод маршрутизації між VLAN router-on-a-stick цього не вимагає. Замість цього на деяких маршрутизаторах програмне забезпечення дозволяє налаштовувати інтерфейс маршрутизатора в якості транка. Це означає, що для маршрутизації пакетів між декількома VLAN на маршрутизаторі і комутаторі потрібен лише один фізичний інтерфейс. Тобто один фізичний інтерфейс маршрутизує трафік між кількома VLAN. Інтерфейс маршрутизатора налаштовується для роботи в якості магістрального каналу й підключається до порту комутатора, який налаштований в транковому режимі. Маршрутизатор виконує маршрутизацію між VLAN, приймаючи на магістральному інтерфейсі трафік з тегом VLAN, що надходить від суміжного комутатора, і потім за допомогою субінтерфейсів перерозподіляє його між VLAN. Вже після цього цей маршрутизований трафік надсилається з цього ж фізичного інтерфейсу з міткою VLAN для відповідної віртуальної мережі призначення [20].

Субінтерфейси - це програмні віртуальні інтерфейси, пов'язані з одним фізичним інтерфейсом. Субінтерфейси налаштовуються в програмному забезпеченні маршрутизатора, і кожному субінтерфейсу призначаються IP-адреса і VLAN. Для полегшення логічної маршрутизації субінтерфейси налаштовуються для різних підмереж, відповідних призначеним ним VLAN. Після прийняття рішення про маршрутизацію на основі мережі призначення VLAN кадрів даним

присвоюються мітки VLAN, після чого вони відправляються назад на фізичний інтерфейс.

Комутація 3-го рівня з використанням SVI (рис. 1.17)

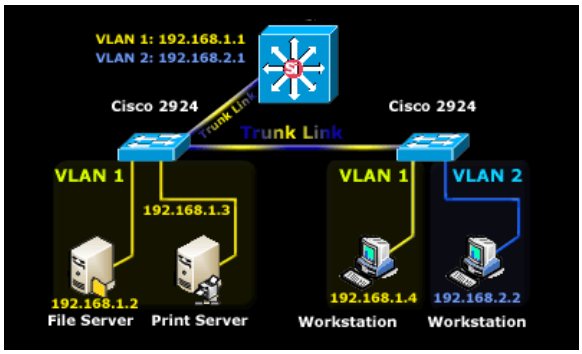

Рисунок 1.17 – Маршрутизація 3-го рівня з використанням SVI [21]

SVI (Switch Virtual Interface) - це віртуальний інтерфейс, що не не має виділених фізичних портів і налаштовується в багаторівневому комутаторі. Інтерфейс SVI можна створити для будь-якої мережі VLAN, що існує на комутаторі. Інтерфейс SVI може виконувати ті ж функції для мережі VLAN, що й інтерфейс маршрутизатора. Крім того, його можна налаштовувати так само, як інтерфейс маршрутизатора (тобто з IP-адресою, вхідними та вихідними списками, і т.д.). Інтерфейс SVI для мережі VLAN забезпечує обробку пакетів 3-го рівня у напрямку до або з портів комутатора, пов'язаних з цією VLAN [21].

По дефолту інтерфейс SVI створюється для мережі VLAN за замовчуванням, для можливості віддаленого керування комутатором. Додаткові інтерфейси SVI необхідно створювати окремо [21].

Інтерфейс SVI виконує наступні функції: забезпечує шлюз мережі VLAN для маршрутизації трафіку (в обидва напрямки), утворює IP-з'єднання 3-го рівня на комутаторі, підтримує конфігурацію протоколу маршрутизації та режиму моста.

Він має багато переваг: є набагато швидшим, не потребує зовнішніх каналів, не обмежується одним каналом, має коротші затримки [21].

1.8 Постановка задачі

Проаналізувавши існуючі рішення щодо віртуальних мереж VLAN, сформулюємо мету наукової роботи наступним чином: змоделювати, створити, та протестувати мережі SOHO з віртуальними локальними мережами, що можуть будуватися системними адміністраторами-початківцями або навіть користувачами з базовими навичками телекомунікацій та досвідом роботи з мережевими симуляторами. Створення і тестування мереж має проходити в безкоштовному та популярному мережевому симуляторі Cisco Packet Tracer за допомогою командного рядку у консолі CLI та екранних форм (для чого, відповідно, треба зробити огляд симулятора Cisco Packet Tracer та підібрати необхідне обладнання та команди).

Треба зібрати три мережі SOHO, що базуються на різних типах мережевого обладнання та, відповідно, з кількома типами віртуальних мереж, щоб задовольнити різний попит в залежності до наявного обладнання та завдань:

1) Мережу SOHO на двох комутаторах, з статичною IP-адресацію, певними порти комутаторів приписаними до відповідних VLAN і двостороннім транковим каналои між комутаторами.

2) Мережу SOHO на одному комутаторі і маршрутизаторі, з магістральною лінією зв’язку між комутатором і маршрутизатором, а також DHCP на маршрутизаторі замість статичної IP-адресації.

3) Повноцінну й сучасну мережу SOHO на комутаторі третього рівня з IP-телефонією, DHCP-сервером та Wi-Fi мережею

2 CISCO PACKET TRACER ЯК ПРОГРАМНЕ СЕРЕДОВИЩЕ СИМУЛЯЦІЇ VLAN В МАЛИХ ЛОКАЛЬНИХ ТА ПОБУТОВИХ МЕРЕЖАХ

2.1 Призначення та переваги Cisco Packet Tracer

Packet Tracer (PT) є офіційним програмним симулятором від Cisco Systems, Inc., іконічного розробника й виробника мережевого обладнання, програмного забезпечення, телекомунікаційного обладнання та ін. Він був створений у вересні 2000 року.

Cisco Packet Tracer є гнучкою й водночас потужною інтерактивною середою з поняттями та протоколами (таблиця 2.1) для моделювання та конфігурування мереж, тестування мереж, виявлення неполадок в мережах та знаходження оптимальних шляхів їх корегування; також для віртуального налаштовування фізичних інтерфейсів телекомунікаційного обладнання Cisco. Інтерактивний симулятор відтворює прадоподібне відчуття роботи в реальній мережі, що може складатися з десятків або навідь сотень пристроїв. [31]

Packet Tracer дозволяє будувати будь-які моделі мереж на обладнанні Cisco, анімувати дію мереж, додавати пакети даних, слідкувати за появою та зміною параметрів IP-пакетів під час їх проходження через мережеві вузли, заміряти їх швидкість, коментувати створені мережі та зберігати їх. За допомогою симулятора можна у сповільненому темпі слідкувати за такими подіями в мережі, що в реальному часі відбуваються в мілісекунди. [32]

Налаштування залежать від типу пристроїв й можуть виконуватися:

- За допомогою графічного інтерфейсу користувача GUI
- За допомогою команд інтерфейсу операційної системи Cisco IOS (у командному рядку консолі Command Line Interface – CLI).
- Як через графічний інтерфейс, так і командами операційної системи Cisco IOS.

Cisco Packet Tracer також можна використовувати як мережевий додаток – щоб симулювати віртуальні мережі через реальні (в т.ч. Інтернет). Можна налаштувати Cisco Packet Tracer для роботи з багатьма користувачами незалежно від місця їх географічного перебування, щоб вони працювали над однією мережевою топологією. Командна робота, ігри та змагання в Cisco Packet Tracer широко використовуються для навчання. [31]

Симулятор надає користувачу два типи робочого простору: логічний та фізичний. Cisco Packet Tracer дає можливість будування физичних моделей мереж – користувач може накласти схему мережі на креслення реальнії будівлі, комплекса будівель та міста. Це дозволяє спроектувати кабельну систему, розмістити пристрої в певних приміщеннях, врахувати фізичні й географічні обмеження (довжина кабелів, зона дії кабелів, покриття бездротових мереж) [32].

Cisco Packet Tracer має простий інтерфейс, що є інтуітивно зрозумілим для користувача. Тут немає складних налаштувань й багаторівневих дерев меню, що робить цей інструмент ідеальним для початківців й студентів. Водночас, експерти також використовують Cisco Packet Tracer для проектування, моделювання й тестування суперскладних, розгорнутих мереж.

Робота з програмою сприяє розвитку таких якостей, як швидкість прийняття рішень, креативний підхід до вирішення проблем та критичне мислення.

Важливої перевагою Cisco Packet Tracer є можливість безкоштовно завантажити цю програму. Для цього треба зареєструватися студентом Cisco Network Academy (щоб скачати актуальну версію), або ж можна скачати один з чисельних дистрибутивів (наприклад, застарілу «студентську» версію 6.2)

Нарешті, Cisco Packet Tracer можна встановлювати на найбільш популярних платформах.

Симуляція, візуализация, режим багатьох користувачів, можливості проектування, платформенна універсальність, доступність та багата палітра налаштувать роблять Cisco Packet Tracer чи не найпопулярнішім мережевим симулятором у світі.

Cisco Packet Tracer підтримує різноманітні протоколи (табл. 2.1) [32]:

Таблиця 2.1. Протоколи, що підтримуються в Cisco Packet Tracer [32]

Рівень	**Протоколи що підтримуються Cisco Packet Tracer**
Прикладний	FTP , SMTP, POP3, HTTP, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, ISR VOIP, SCCP config and calls ISR command support, Call Manager Express
Траспортний	TCP and UDP, TCP Nagle Algorithm & IP Fragmentation, RTP
Мережевий	BGP, IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, RIPv1/v2/ng, MultiArea OSPF, OSPFv3, EIGRP, EIGRPv6, Static Routing, Route Redistribution, Multilayer Switching, L3 QoS, NAT, CBAL, Zone-based policy firewall and Intrusion Protection System on the ISR, GRE VPN, IPSec VPN, HSRP, CEF
Канальний	(802.3), 802.11, HDLC, Frame Relay, PPP, PPPoE, STP, RSTP, VTP, DTP, CDP, 802.1q, PAgP, L2 QoS, SLARP, Simple WEP, WPA, EAP, VLANs, CSMA/CD, Etherchannel, DSL, ¾ G network support

2.2 Інтерфейс Cisco Packet Tracer

Головне вікно Cisco Packet Tracer можно умовно розподілити на кілька зон в залежності від функцій (рис. 2.1). Найбільшою зоною, як бачимо, є робочий простір, навколо якого групуються допоміжні кнопки, інструменти, і т.ін.

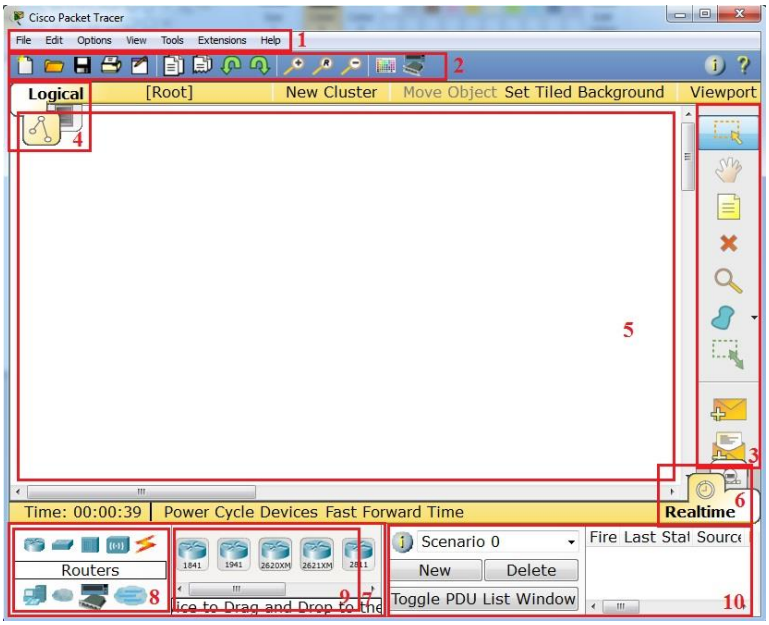

Рисунок 2.1. Головне вікно Cisco Packet Tracer

Опис компонентів головного вікна симулятора та їх можливостей дано нижче, у таблиці 2.2.

Таблиця 2.2. Компоненти головного вікна симулятора Cisco Packet Tracer та їх призначення

№	*Назва*	*Опис*
1.	**Панель Меню**	Ця панель вміщує меню File (Файл), Edit (Правка), Options (Параметри), View (Вид), Tools (Інструменти), Extensions (Розширення) та Help (Справка). Включає такі команди, як Open (Відкрити), Save (Зберегти), Save as Pkz (Зберегти як Pkz), Print (Печать) та Preferences (Налаштування).
2.	**Панель основних команд**	На цій панели розміщено кнопки-іконки до команд File (Файл) та Edit (Правка). Також тут розміщені кнопки Copy (Копіювати), Paste (Вставити), Undo (Відмінити), Redo (Повторити), Zoom (Збільшити), Drawing Palette (Палітра малювання) та Custom Devices Dialog (Вікно пристроїв

		користувача устройств). Справа розміщена кнопка Network Information (Інформація про мережу).
3.	**Панель інструментів**	Ця панель надає доступ до основних інструментів: Select (Вибрати), Move Layout (Пемістити шар), Place Note (Зробити нотатку), Delete (Видалити), Inspect (Перевірити), Resize Shape (Змінити розмір форми), Add Simple PDU (Додати простий PDU) и Add Complex PDU (Додати складний PDU).
4.	**Логічний/ фізичний простір та панель навігації**	Можна переключатися між фізичним простором та логічним простором. В логічному просторі також можна повернутися на попередній рівень у кластері та використовувати такі функції, як New Cluster (Створити кластер), Move Object (Перемістити),Set Tiled Background (Задати фон), та Viewport (Вікно просмотру). В фізичному робочому просторі цей розділ дозволяє навігувати крізь фізичні локації, а також використовувати функції New City (Нове місто), New Building (Нова будівля), New Closet (Нова стійка), Move Object (Перемістити), Set Background (Задати фон), вмикати Grid (Сітку), та входити в Working Closet (Робоча стійка).
5.	**Робочий простір**	Простір, безпосередньо в якому будується мережа, спостерігається симуляція й збирається статистика.
6.	**Панель перемикання режиму реального часу/режим у симуляції симуляции**	Дозволяє переходи між режимами реального часу та симуляції. Також включає в себе кнопки Power Cycle Device (Скинути по живленню), Fast Forward Time (Прискорити час), Play Control (Керування відтворенням) та кнопку включення Event List (Список подій) в режимі симуляції. Також має годинника, що вказую час у різних режимах.

7.	**Компоненти мережі**	Дозволяє вибирати обладнання та з'єднання для подальшого використання у робочому просторі. Включає в себе такі розділи, як Device-Type Selection (Вибір видів обладнання) та Device-Specific Selection (Вибір пристроїв).
8.	**Вибір видів обладнання**	Включає в себе різноманітні види пристроїв та наявні типи з'єднань між ними. Зміст розділу Device-Specific Selection (Вибір пристроїв) змінюється в залежності від типу обраного пристрою.
9.	**Вибір пристроїв**	Дозволяє обирати конкретні моделі пристроїв та з'єднань для подальшого переміщення на робочий простір.
10.	**Пакети користувача**	Це вікно керує пакетами, що циркулюють в мережі під час симуляції.

Обладнання та лінії зв'язку в Cisco Packet Tracer

Маршрутизатори (рис 2.2) – мережеве обладнання, що використовується для пошуку та побудування оптимального маршруту передачі даних на основі спеціальних алгоритмів маршрутизації – наприклад, вибір маршрутів з оптимальною вартістю або найменшою кількістю транзитних узлов.

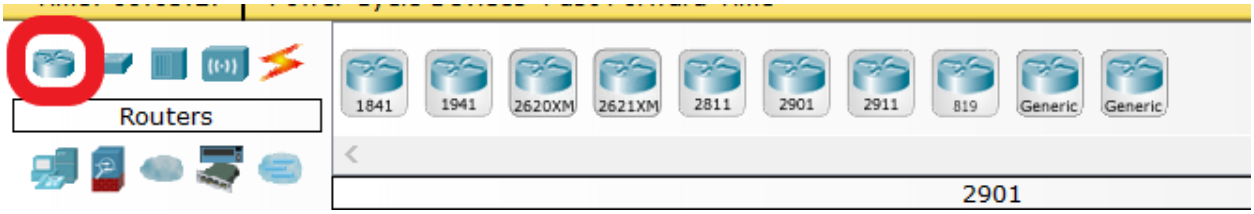

Рисунок 2.2 – Маршрутизатори Cisco Packet Tracer

В Cisco PT доступні такі типи маршрутизаторів:

o Cisco 1841. Маршрутизатор з інтегрованими сервісами (Інтегрований сервісний маршрутизатор, ISR) має два порта Fast Ethernet і два вільних слота для підключення інтегральних карт для високошвидкісного WAN-з'єднання.

o Cisco 1941. Ця модель подібна до попередньої лише з тим, що відрізняється, що працює під управлінням 15 версій Cisco IOS. Також має два порта Gigabit Ethernet.

o Cisco 2620XM. Цей мультисервісний маршрутизатор має один порт Fast Ethernet, два слоти для встановлення WAN-інтерфейсів карток та слот для AIM.

o Cisco 2621XM. Даний маршрутизатор подібний попередньому, за виключенням наявності двох портів Fast Ethernet.

o Cisco 2811. Маршрутизатор з інтегрованими сервісами має два порта Fast Ethernet, чотири слоти WIC та два слоти AIM.

o Cisco 2901. Цей маршрутизатор має два порта Gigabit Ethernet, чотири слоти WIC й два слоти для DSP.

o Cisco 2911. Даний маршрутизатор має три порта Gigabit Ethernet, а в іншому повторює характеристики попереднього пристрою. Функціонує під управлінням 15 версії Cisco IOS.

o Генетичний маршрутизатор-PT. Маршрутизатор з налаштуванням під користувачем. Має 10 слотів і кілька спеціальних модулів, назва яких починається з PT.

Комутатори (рис 2.3) – пристрої, що працюють на канальному рівні моделі OSI. Вони призначені для об'єднання кількох вузлів в межах одного або більше сегментів мереж. Пакети комутаторів передаються на основі внутрішніх таблиць комутацій, відповідно трафік йде лише на ту MAC-адресу за призначенням, і не повторюється на всіх портах (як у випадку з концентраторами).

Рисунок 2.3 – Комутатори Cisco Packet Tracer

Коммутатор (раніше називався багатопортовим мостом) з'єднує кілька пристроїв в мережу, при цьому кожний порт комутатора є колізійним доменом. Наступні комутатори доступні в Cisco PT:

✓ Cisco 2950-24. Керований комутатор з підтримкою 24 портів Fast Ethernet.

✓ Cisco 2950T-24. Цей комутатор, що належить до родини інтелектуальних комутаторів Catalyst 2950, має 24 порта швидкого Ethernet й два гігабітних порти Ethernet з підтримкою модулів GBIC (Gigabit Interface Converter).

✓ Комутатор 2960. Порти доступу Ethernet: 48 x FE RJ-45. Порти агрегації Ethernet: 2 x GE RJ-45 combo SFP. Універсальні порти Ethernet: 2 x SFP

✓ Коммутатор 3560 24-PS. Catalyst 3560 – серія комутаторів Ethernet з фіксованою конфігурацією, що підтримує стандарт IEEE 802.3af (Power over Ethernet), а також Cisco Inline Power (передстандартний PoE). Коммутатори серії призначені для застосування на рівні доступу. Catalyst 3560 ідеально підходить організаціям, що використовують мережеву інфраструктуру для впровадження нових продуктів, наприклад IP телефонів, системного управління будівлею, відеокамер та т. д. Серія 3560 включає стомегабітні та гігабітні комутатори. Стомегабітні моделі мають 24 або 48 мідних портів Fast Ethernet, а також 2 або 4 SFP-порта Gigabit Ethernet відповідно для створених з'єднань. За допомогою технології IEEE 802.3af можна забезпечити електропостачання різних мережевих пристроїв (безпровідні точки доступу, IP-телефони, відеокамери) безпосередньо через мережеве підключення (що особливо зручно, коли підключити їх до електричної мережі проблематично) [28].

Концентратор (рис 2.4) повторює пакет, прийнятий одним портом, на всіх інших портах.

Рисунок 2.4 – Концентратори Cisco Packet Tracer

Концентратор це застаріле обладнання, яке цікаве з історичної точки зори й для вивчення таких явищ, як широкомовний шторм та ін.

Бездротове обладнання. Включає в себе точки доступу, що реалізують бездротові технології Wi-Fi та мережі на їх основі, а також стильникові вежі та сервери (рис. 2.5).

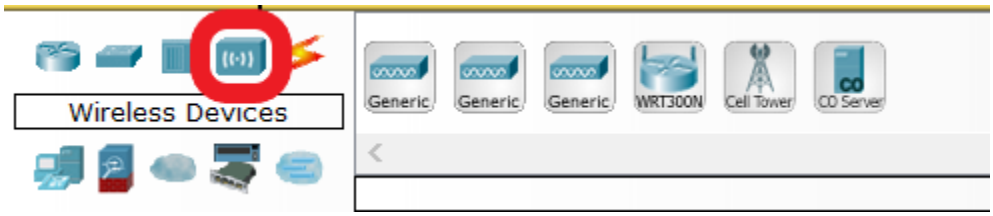

Рисунок 2.5 – Бездротове обладнання Cisco Packet Tracer

Лінії зв'язку (рис. 2.6). За допомогою цих компонентів створюються з'єднання окремих вузлів в єдину схему. Packet Tracer підтримує широкий діапазон мережевих ліній зв'язку (див. Табл. 2.1). При цьому кожен тип кабелю може бути приєднаним лише до певних типів інтерфейсів.

Рисунок 2.6 – Лінії зв'язку Cisco Packet Tracer

Більш детальний опис ліній зв'язку приведено нижче, у таблиці 2.3

Таблиця 2.3 Лінії зв'язку Cisco Packet Tracer

Типи кабелів	*Опис*
Консоль	Консольне з'єднання може бути встановлене між ПК і маршрутизаторами або комутаторами. Потрібно виконати деякі вимоги щодо роботи консольного сеансу з ПК: швидкість з'єднання з обох сторін мусить бути однаковою, має бути 7 біт даних (або 8 біт) для окремих сторін, контроль четності повинен

	бути однаковим, 2 або 1 стопових біта (но вони не зобов'язані бути однорідними), а потік даних для окремих сторін може бути чим завгодно.
Прямий мідний кабель 	Цей тип кабелю є стандартним середовищем з'єднання Ethernet для пристроїв, що функціонують на різних рівнях OSI (напр. комутатор - маршрутизатор). Він повинен бути з'єднаний з наступними типами портів: 10 Мбіт (Ethernet), 100 Мбіт/с (швидкий Ethernet) й 1000 Мбіт/с (гігабітний Ethernet).
Мідний кросовер 	Такий тип кабелю є середовищем з'єднання Ethernet для пристроїв, що працюють на однакових рівнях OSI (комутатор – комутатор; маршрутизатор - маршрутизатор). Він може бути під'єднаним до таких портів: 10 Мбіт (Ethernet), 100 Мбіт/с (швидкий Ethernet) й 1000 Мбіт/с (гігабітний Ethernet).
Оптика 	Використовується для з'єднань між оптичними портами (100 Мбіт / с або 1000 Мбіт / с)
Телефонний 	З'єднання через телефонну лінію може здійснюватися лише між пристроями, що мають модемні порти. Стандартне представлення модемних з'єднань - це кінцевий пристрій (наприклад, ПК), що дзвонить в мережеву хмаринку.
Коаксіальний 	Коаксіальна середа використовується для з'єднань між коаксіальними портами – такими як кабельний модем, що є з'єднаним з хмаринкою Packet Tracer.

Серійний DCE  **Серійний DTE** 	З’єднання через послідовні порти, які часто використовуються для зв'язку між WAN. Для налаштування таких з'єднань необхідно встановити синхронізацію на стороні DCE-пристроїв. Синхронізація DTE виконується за вибором. Сторону DCE можна визначити за маленькою іконкою "годиннику" поруч із портом. При виборі типу з'єднань Serial DCE, перший пристрій, до якого застосовується з'єднання, стає DCE-пристроєм, а друге автоматично стане DTE. Можливо й зворітне розташування сторон, якщо вибраний тип з'єднання – послідовний DTE.
Консольний кабель-концентратор 	Консольні кабелі-концентратори використовуються для підключення сервера доступу або сервера терміналів до кожного з інших маршрутизаторів та портів консолі комутаторів

Термінальні пристрої (рис. 2.7). Включають таке обладнання, як ПК, ноутбуки, сервери, телефони, телевізори, смарт-пристрої та навість сніфери.

Рисунок 2.7 – Термінальні пристроої Cisco Packet Tracer

Засоби міжмережевої безпеки (рис. 2.8). Включає міжмережевий екран ASA 5505

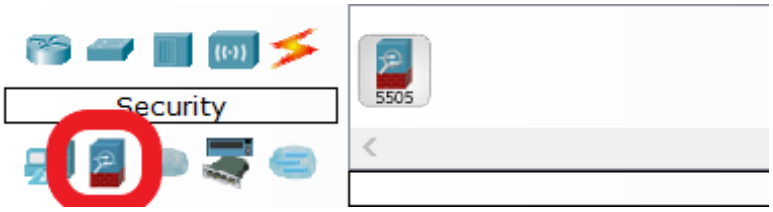

Рисунок 2.8 – Лінії зв'язку Cisco Packet Tracer

Емуляція мережі Інтернет (рис. 2.9). Включає DSL модем та хмаринки Інтернет

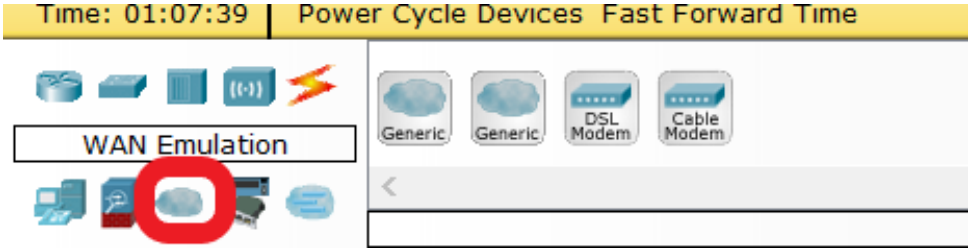

Рисунок 2.9 – Емуляція мережі Інтернет в Cisco Packet Tracer

Пристрої користувача (рис. 2.10) та *хмаринка для режиму багатьох користувачів*

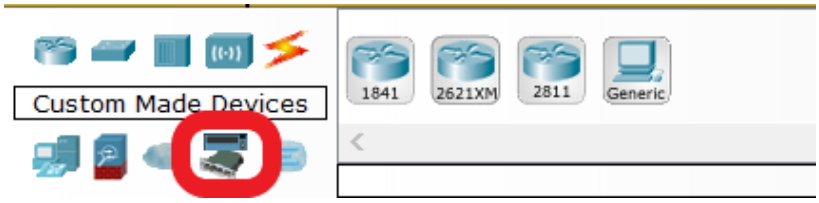

Рисунок 2.10 – Пристрої користувача в Cisco Packet Tracer

Пристрої користувача дозволяють кастомізувати обладнання для індивідуальних цілей, що їх не передбачили в загальних пристроях. Це включає особливий набор модулів і, відповідно, більш гнучкі можливості конфігурування.

Хмаринка для режиму багатьох користувачів (рис.2.11) дозволяє спільне керування мережею та навіть мережеві ігри.

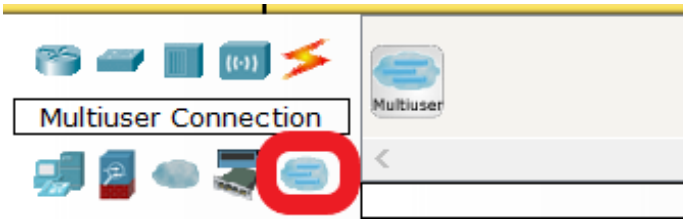

Рисунок 2.11 – Хмаринка для режиму багатьох користувачів в Cisco Packet Tracer

2.3 Операційна система Cisco IOS та її команди

Вважається, що успіх продуктів Cisco Systems та їх домінування на ринку мережевого обладнання та програмного забезпечення багато в чому пояснюються вдалою операційною системою IOS (Internetwork Operating System). Хоча IOS в першу чергу була розроблена для керування мережевим обладнанням, вона є повноцінною операційною системою – потужною але гнучкою. Командний рядок оболонки IOS і сьогодні перевершує можливості операційної середи багатьох операційних середовищ, які керуються меню користувача, і командний рядок IOS навіть зараз не сприймається як анахронізм (хоча зараз можна керувати IOS через WEB-браузери) [29].

Cisco IOS, реалізована на маршрутизаторах й комутаторах Cisco, забезпечує такі функції [26]:

- Мережева та міжмережева безпека;
- IP-адресація віртуальних та фізичних інтерфейсів;
- Можлівість налаштування інтерфейсів для оптимізації підключення певної середи передачі даних;
- Маршрутизація;
- Налаштування технологій якості обслуговування (QoS);
- Підтримка технологій керування мережею.

Кожна з функцій або служб має набір певних команд, що дозволяють їх активувати та конфігурувати.

Доступ до сервісів, що їх пропонує Cisco IOS, загалом реалізується через інтерфейс командного рядка (CLI).

Cisco IOS спроектована як ієрархічна модульна операційна система. Вона вміщає кілька різних режимів роботи, кожен з яких має свій власний простір (рис. 2.12) [23].

Ці режими включають в себе:

- Виконавчий режим користувача
- Привілейований виконавчий режим
- Глобальний режим конфігурації
- Інші специфічні режими конфігурації

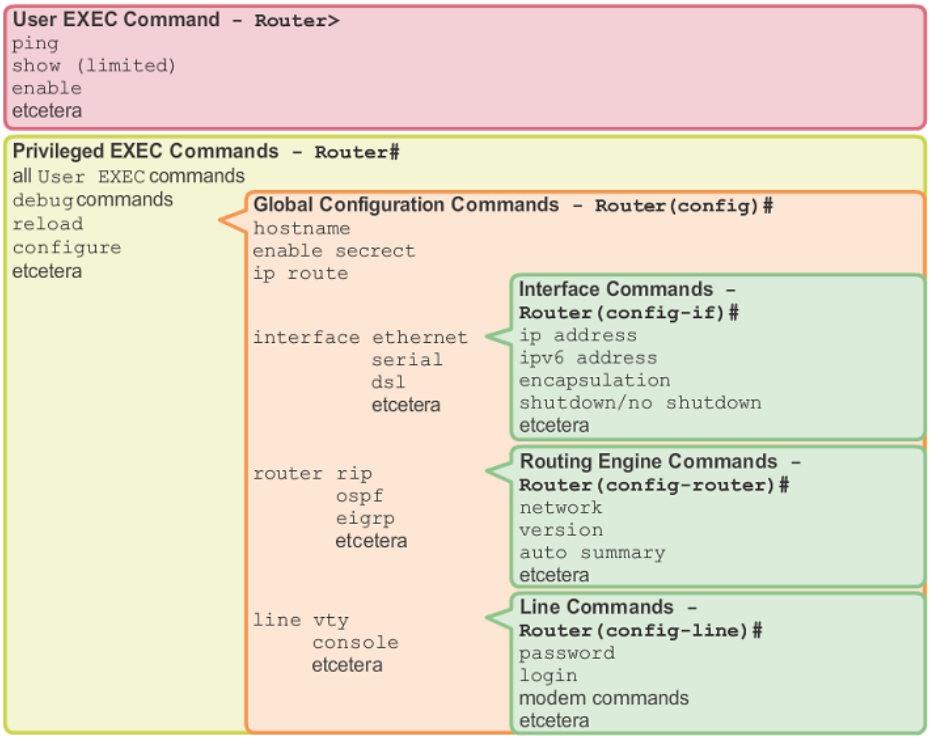

Рисунок 2.12 – Командні режими роботи в Cisco Packet Tracer та їх ієрархія [26]

Кожен режим використовується для виконання певних завдань і має певний набір команд, які доступні у відповідному режимі. Наприклад, щоб настроїти інтерфейс маршрутизатора, користувач повинен увійти в режим конфігурації інтерфейсу. Всі настройки, які вводяться в режимі конфігурації інтерфейсу, застосовуються тільки до цього інтерфейсу.

Деякі команди доступні всім користувачам; інші можуть бути виконані тільки після входу в режим, в якому ця команда доступна. Кожен режим відрізняється відповідної підказкою, і доступні тільки ті команди, які дозволені для цього режиму. Ієрархічна модальна структура може бути налаштована для забезпечення безпеки. Різна аутентифікація може використовуватися для кожного ієрархічного режиму. Це контролює рівень доступу, який можна надати мережевого персоналу.

Виконавчий режим користувача EXEC

Після реєстрації в маршрутизаторі користувач входить в призначений для користувача режим команд EXEC (крім тих випадків, коли по системним налаштуванням користувач відразу входить в привілейований режим EXEC). Зазвичай при реєстрації потрібно ввести ім'я користувача і пароль. Максимальна кількість спроб - три рази, після чого в доступі буде відмовлено. Команди EXEC, доступні на призначеному для користувача рівні, доступні і на вищому, привілейованому рівні. Команди EXEC дозволяють підключитися до віддалених пристроїв, тимчасово змінити параметри абонентської лінії, виконати основні тести, а також отримати відомості про систему [25].

Привілейований режим EXEC

Багато команд привілейованого режиму EXEC конфігурують робочі параметри, тому доступ привілейованого рівня повинен бути захищений паролем. Набір привілейованих команд EXEC включає команди призначеного для режиму користувача EXEC. Привілейований режим EXEC забезпечує доступ до режимів конфігурації за допомогою команди configure і включає команди розширеного тестування, наприклад, debug [25].

Запрошення привілейованого режиму EXEC складається з імені пристрою як вузла мережі, за яким слід знак решітки (#). Привілейований режим EXEC часто називають "режим enable", так як для входу використовується команда enable.

Якщо в системі встановлено пароль, з'явиться запит на введення пароля. Пароль не відображається на екрані і вводиться з урахуванням регістру символів. Якщо пароль привілейованого режиму не був встановлений, то вхід в привілейований режим EXEC можливий тільки з консолі маршрутизатора. Системний адміністратор може встановлювати паролі за допомогою відповідних команд [26].

Режим глобальної конфігурації

Це конфігурація характеристик або функціональних можливостей, системи в цілому. Режим глобальної конфігурації використовується для конфігурації всієї системи або для переходу в спеціальні режими конфігурації - наприклад, щоб настроїти такі специфічні елементи, як інтерфейси або субінтерфейси. При введенні команди змінюють поточну конфігурацію - зміни конфігурації вступають в силу при кожному натисканні клавіші Enter (якщо команда правильна). З режиму глобальної конфігурації можна перейти в безліч режимів конфігурації, специфічних для конкретного протоколу або платформи [25].

Режим конфігурації інтерфейсу

Прикладом специфічного режиму конфігурації, в який можна перейти з режиму глобальної конфігурації, виступає режим конфігурації інтерфейсу. Він дозволяє включити або змінити безліч функціональних можливостей конкретного інтерфейсу. Команди конфігурації інтерфейсу змінюють функціонування інтерфейсу. Командам конфігурації інтерфейсу завжди передує команда режиму глобальної конфігурації interface - щоб визначити тип інтерфейсу [25].

Режим конфігурації субінтерфейсу

З режиму конфігурації інтерфейсу можна перейти в режим конфігурації субінтерфейса. Режим конфігурації субінтерфейса знаходиться в ієрархічному підпорядкуванні до режиму конфігурації інтерфейсу. В режимі конфігурації

субінтерфейса можна задавати параметри безлічі віртуальних інтерфейсів (субінтерфейсов) на одному фізичному інтерфейсі. Різних протоколах субінтерфейси представляються як окремі фізичні інтерфейси. І навпаки, субінтерфейси підтримують множинну инкапсуляцию протоколів в один фізичний інтерфейс [26]. Вижимка про режими конфігурування та команди доступу та виходу приведена нижче у таблиці 2.4.

Таблиця 2.4. Зведени дані щодо режимів конфігурування [26]

Режим конфігурування	*Спосіб доступу*	*Запрошення (?)*	*Спосіб виходу*
Загальний режим користувача EXEC	Вхід в систему	***Router>***	Команда ***logout***.
Привілейований режим EXEC	В загальному режимі користувача EXEC використовується команда EXEC ***enable***.	***Router#***	Щоб вийти в загальний режим користувача EXEC, використовується команда ***disable***. Щоб увійти в режим глобальної конфигурації – команда привілегійованого режиму EXEC ***configure terminal*** .
Глобальна конфігурация	В привілейованому режимі EXEC використовуєтьс я ***configure terminal.***	***Router(config)#***	Щоб вийти в привілейований режим EXEC – команда ***end*** або Ctrl-Z. Для переходу в режим конфігурування интерфейсу потрібна команда ***interface***.

Конфігурування інтерфейсу	В режимі глобального конфігурування треба вказати інтерфейс в команді ***interface***.	***Router(config-if)#***	Для виходу в режим глобального конфігурування – команда ***exit***. Для виходу в привілейований режим EXEC – команда ***end*** або Ctrl-Z. Для переходу в режим конфігурування интерфейсу субінтерфейса треба вказати субінтерфейс після команди ***interface***.
Конфігурування субінтерфейсу	В режимі конфігурування інтерфейсу треба субінтерфейс в команді ***interface***. (залежить від платформи.)	***Router(config-subif)#***	Для виходу в режим глобального конфігурування –команда ***exit***. Для виходу в привілейований режим EXEC треба ввести команду ***end*** або Ctrl-Z.

Команди IOS рахують на сотні, і супроводжувальної інструкціїї не завжди вистачає, щоб засвоїти їх в повному обсязі. Дочерня компанія Cisco, видавництво Cisco Press, навіть випускає серію *Cisco IOS Reference Library* для допомоги системним адміністраторам.

Тому ми повинні вибрати ті комплекси команд, які знадобляться для поставлених раніше задач:

- Навігація між режимами
- Налаштування інтерфейсів
- Налаштування віртуальних мереж
- Налаштування транкових каналів

- Налаштування DHCP
- Перевірка налаштувань

Отже, для конфігурування віртуальних локальних мереж та магістральних каналів вибираємо основні команди, що приведені нижче, у таблиці 2.5.

Таблиця 2.5. Основні команди Cisco IOS, необхідні для налаштування віртуальних локальних мереж в малих офісних та домашніх мережах [33], [34]

Задача	***Команда***
Налаштування VLAN	
Увійти в режим *enable*	*Switch> enable*
Увійти в режим глобальної конфігурації	*Switch# configure terminal*
Створити VLAN з валідним ID та перйти в режим конфігурації VLAN	*Switch(config)# vlan vlan-id*
Вказати унікальне ім'я для ідентифікації VLAN	*Switch(config-vlan)# name vlan-name*
Повернутися в привілейований режим EXEC	*Switch(config-vlan)# end*
Увійти в режим глобальної конфігурації	*Switch# configure terminal*
Створити VLAN з валідним ID	*Switch(config)# vlan vlan-id*
Вказати унікальне ім'я для ідентифікації VLAN	*Switch(config-vlan)# name vlan-name*
Повернутися в привілейований режим EXEC	*Switch(config-vlan)# end*
Увійти в режим глобальної конфігурації	*Switch# configure terminal*
Увійти в режим конфігурації інтерфейсу	*Switch(config)# interface interface-id*

Налаштувати порт на режим access	*Switch(config-if)# switchport mode access*
Присвоїти порт VLAN'у.	*Switch(config-if)# switchport access vlan vlan-id*
Повернутися в привілейований режим EXEC	*Switch(config-if)# end*
Відобразити ім'я, статус та порти VLAN по одній VLAN на рядок	*Switch# brief*
Відобразити інформацію про певний номер VLAN ID. Для vlan-id діапазон від 1 до 4094	*Switch# id vlan-id*
Відобразити інформацію про певне ім'я VLAN. Vlan-name – рядок ASCII від 1 до 32 символів.	*Switch# name vlan-name*
Видалити VLAN	*Switch# no vlan vlan-id*
Відобразити загальну інформацію про VLAN	*Switch# summary*
Налаштування магістрального каналу	
Увійти в режим глобальної конфігурації	*Switch# configure terminal*
Увійти в режим конфігурації інтерфейсу	*Switch(config)# interface interface-id*
Встановити порт в режим постійного транкінгу	*Switch(config-if)# switchport mode trunk*
Встановити для native VLAN значення, що відрізняється від VLAN 1	*Switch(config-if)# switchport trunk native vlan vlan-id*
Вказати список VLAN, дозволених для транка	*Switch(config-if)# switchport trunk allowed vlan vlan-list*

Повернутися в привілейований режим EXEC	*Switch(config-if)# end*
Перевірити налаштування TRUNK	*Switch# show interfaces interface-ID switchport*
Скинути налаштування TRUNK до дефолтних	*Switch# no switchport trunk allowed vlan*
Налаштування маршрутизатора в мережі з VLAN	
Увійти в режим *enable*	*Router> enable*
Увійти в режим глобальної конфігурації	*Router# configure terminal*
Увійти в режим конфігурації інтерфейсу	*Router(config)#interface fa 0/0*
Підняти інтерфейс	*Router(config-if)#no shutdown*
Задати субінтерфейс для відповідної VLAN	*Router(config)#interface fa0/0.10*
Налаштувати інкапсуляцію за стандартом 802.1q	*Router(config-subif)#encapsulation dot1q 10*
Задати IP-адресу та маску підмережі для субінтерфейсу	*Router(config-subif)#ip address 192.168.10.1 255.255.255.0*
Повернутися в режим інтерфейсу	*Router(config-subif)#exit*
Повернутися в режим глобальної конфігурації	*Router(config-if)# exit*
Показати налаштування магістралі	*Switch#show trunk*
Показати налаштування інтерфейсів	*Router#show ip interfaces*
Показати налаштування інтерфейсів	*Router#show ip interfaces brief*
Показати маршрутизацію між VLAN	*Router#show ip route*
Налаштування маршрутизатора як DHCP сервера в мережі з VLAN	

Увійти в режим *enable*	*Router> enable*
Увійти в режим глобальної конфігурації	*Router# configure terminal*
Виключити статичні адреси (адреси субінтерфейсів)	*Router#ip dhcp excluded-address 192.168.10.1 255.255.255.0*
Увійти в режим конфігурування DHCP та створити пул адрес для термінальних пристроїв відповідної VLAN	*Router(config)#ip dhcp pool lan-10*
Приписати мережу VLAN	*Router(dhcp-config)#network 192.168.10.0 255.255.255.0*
Визначити маршрутизатор по замовчуванню для даної мережі VLAN	*Router(dhcp-config)#default-router 192.168.10.252*
Повернутися в режим глобальної конфігурації	*Router(dhcp-config)#exit*
Вийти з режиму глобальної конфігурації	*Router(config)#exit*
Побачити налаштування пулів IP-адрес	*Router#show running-config*
Побачити автоматично роздані IP-адреси та MAC-адреси відповідних пристроїв	*Router#show ip dhcp binding*
Записати налаштування в пам’ять	*Router#write memory*
Налаштування маршрутизатора як VLAN сервера	
Увійти в режим *enable*	*Router> enable*
Увійти в режим глобальної конфігурації	*Router# configure terminal*
Увійти в режим конфігурації інтерфейсу	*Router(config)#interface fa 0/0*

Підняти інтерфейс	*Router(config-if)#no shutdown*
Задати субінтерфейс для відповідної VLAN	*Router(config)#interface fa 0/0.10*
Налаштувати інкапсуляцію за стандартом 802.1q	*Router(config-subif)#encapsulation dot1q vlan-id*
Задати IP-адресу та маску підмережі для субінтерфейсу	*Router(config-subif)#ip address 192.168.10.1 255.255.255.0*
Задати helper-address	*Router(config-subif)#ip helper-address 10.10.120.100*
Повернутися в режим інтерфейсу	*Router(config-subif)#exit*
Повернутися в режим глобальної конфігурації	*Router(config-if)# exit*
Вийти з режиму глобальної конфігурації	*Router(config)#exit*
Побачити налаштування	*Router#show run*
Налаштування магістрального каналу від комутатора L3 до маршрутизатора	
Увійти в режим *enable*	*Switch> enable*
Увійти в режим глобальної конфігурації	*Switch# configure terminal*
Увійти в режим конфігурації інтерфейсу	*Router(config)#interface gi 0/1*
Налаштувати інкапсуляцію за стандартом 802.1q	*Router(config-subif)#switchport trunk encapsulation dot1q 10*
Налаштувати постійний транковий режим	*Router(config-subif)#switchport mode trunk*
Повернутися в режим інтерфейсу	*Router(config-subif)#exit*

Повернутися в режим глобальної конфігурації	*Router(config-if)# exit*
Вийти з режиму глобальної конфігурації	*Router(config)#exit*
Налаштування access-портів комутатора для комп'ютера та телефона	
Увійти в режим *enable*	*Switch> enable*
Увійти в режим глобальної конфігурації	*Switch# configure terminal*
Увійти в режим конфігурації інтерфейсу	*Router(config)#interface fa 0/1*
Налаштування access-портів комутатора для комп'ютера	*Switch(config-if)# switchport access vlan vlan-id*
Налаштування access-портів комутатора для комп'ютера	*Switch(config-if)# switchport access voice vlan vlan-id*
Повернутися в режим інтерфейсу	*Router(config-subif)#exit*
Повернутися в режим глобальної конфігурації	*Router(config-if)# exit*
Вийти з режиму глобальної конфігурації	*Router(config)#exit*
Налаштування телефонного сервісу та розподілення телефонних номерів	
Увійти в режим *enable*	*Switch> enable*
Увійти в режим глобальної конфігурації	*Switch# configure terminal*
Увійти в режим конфігурації телефонії	*Router(config)#telephony-service*
Задати максимальну кількість телефонних номерів	*Router(config-telephony)#max-dn 144*
Задати максимальну кількість телефонів	*Router(config-telephony)#max-ephones 42*

Задати IP-адресу що буде джерелом для голосової мережі	*Router(config-telephony)#ip source-address 10.10.110.1 port 2000*
Назначити автоматичне розподілення телефонних номерів	*Router(config-telephony)#auto assign 1 to 144*
Повернутися в режим глобальної конфігурації	*Router(config-telephony)#exit*
Призначити порядковий номер телефонному апарату (по черзі підключення)	*Router(config)#ephone-dn 1*
Призначити телефонний номер для телефону, що підключиться першим	*Router(config-ephone-dn)#number 54001*
Вийти з режиму глобальної конфігурації	*Router(config)#exit*
Записати налаштування в пам’ять	*Router#write memory*

Наступний етап -- практичне розгортання мереж SOHO з різними типами обладнання та різними віртуальними мережами відповідно поставленій задачі, починаючи з більш простих мереж і закінчуючи повноцінною мережею з IP-телефонією та Wi-Fi.

3 ПОБУДОВА ТА ТЕСТУВАННЯ РІЗНИХ ТИПІВ VLAN В МЕРЕЖАХ SOHO

3.1 VLAN в мережі SOHO на двох комутаторах, з однією міжкомутаторною магістраллю.

Модель майбутньої мережі з VLAN на двох комутаторах представлена на рис. 3.1:

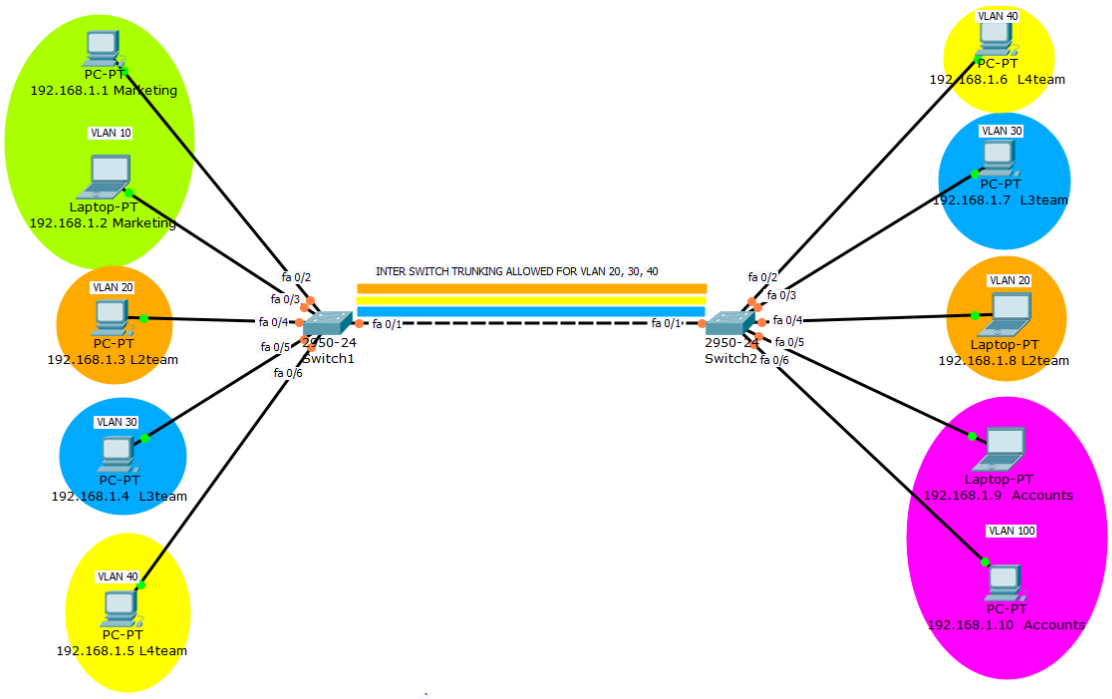

Рисунок 3.1 – Модель мережі на двох комутаторах

Збираємо мережу на двох комутаторах 2950-24.

До комутатору Switch1 під'єднуємо (використовуємо прямий мідний кабель):

ПК 192.168.1.1 з VLAN Marketing (VLAN 10) – інтерфейс fa 0/2,

ноутбук 192.168.1.2 Marketing (VLAN 10) – інтерфейс fa 0/3,

ПК 192.168.1.3 L2team (VLAN 20) – інтерфейс fa 0/4,

ПК 192.168.1.4 L3team (VLAN 30) – інтерфейс fa 0/5, та

ПК 192.168.1.5 L4team (VLAN 40) – інтерфейс fa 0/6.

До комутатору Switch2 під'єднуємо (використовуємо прямий мідний кабель):

ПК 192.168.1.6 L4team (VLAN 40) – інтерфейс fa 0/2,

ПК 192.168.1.7 L3team (VLAN 30) – інтерфейс fa 0/3,

ноутбук 192.168.1.8 L2team (VLAN 20) – інтерфейс fa 0/4,

ноутбук 192.168.1.9 Accounts (VLAN 100) – інтерфейс fa 0/5, та

ПК 192.168.1.10 Accounts (VLAN 100) – інтерфейс fa 0/6.

З'єднуємо комутатори між собою (використовуємо мідний кросовер): інтерфейс fa 0/1 та інтерфейс fa 0/1

Призначаємо статичні адреси термінальним пристроям через екранні форми:

Заходимо на кожен кінцевий пристрій, навігуємо на вкладку Desktop, обираємо опцію IP Configuration (рис. 3.2) та призначаємо IP-адреси від 192.168.1.1 до 192.168.1.10 та маску підмережі 255.255.255.0, починаючи зліва зверху.

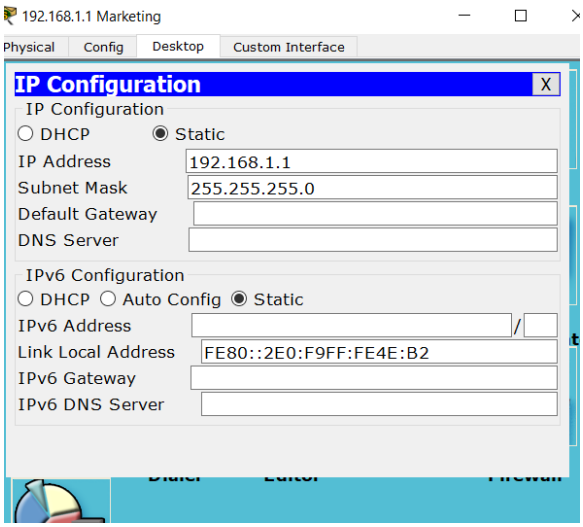

Рисунок 3.2 – приклад призначенння статичних IP-адресів термінальним пристроям через екранні форми

Таким чином, всі термінальні пристрої знаходяться в одній локальній мережі 192.168.1.0 255.255.255.0

Використовуючи інструмент Place Note (Нотатки) задаємо назви термінальних пристроїв, вказуючи IP-адреси та функціональні групи, до яких вони належать.

Використовуючи інструменти малювання, графічно визначаємо віртуальні мережі еліпсами різних кольорів та надписуємо еліпси в залежності від належності до певної VLAN, використовуючи інструмент Place Note.

Також надписуємо віртуальні мережі, трафік яких дозволений у транковому каналі.

Налаштовуємо комутатори.

Оголошуємо віртуальні мережі та даємо їм імена на кожному комутаторі:

Заходимо на Switch1:

Switch> enable (заходимо у режим enable)

Switch# configure terminal (заходимо у режим глобальної конфігурації)

Switch(config)# vlan 10 (заходимо у режим конфігурації vlan)

Switch(config-vlan)# name marketing (даємо ім’я vlan)

Таким же чином налаштовуємо інші Vlan

Таким же чином налаштовуємо Switch 2.

Призначаємо порти доступу на обох комутаторах та призначаємо віртуальні мережі портам комутаторів.

Заходимо на Switch1:

Switch(config)# interface fa 0/2 (входимо в режим конфігурації інтерфейса)

Switch(config-if)# switchport mode access (налаштуємо доступ)

Switch(config-if)# switchport access vlan 10 (приписуємо vlan до інтерфейсу)

Таким же чином налаштовуємо інші порти.

За цим же зразком проводимо конфігурування Switch 2:

Конфігуруємо інтерфейс fa 0/1 як магістральну лінію на кожному комутаторі та дозволяємо трафік всіх VLAN крім 10 та 100.

Заходимо на Switch1:

Switch(config)# interface fa 0/1 (входимо в режим інтерфейса)

Switch(config-if)# switchport mode trunk (задаємо транковий режим)

Switch(config-if)# switchport trunk allowed vlan 20, 30, 40 (дозволяємо vlan)

Switch(config-if)#exit (виходимо в попередній режим)

Switch(config)#exit (виходимо в попередній режим)

Перевіримо налаштування (рис 3.3):

Switch#show run

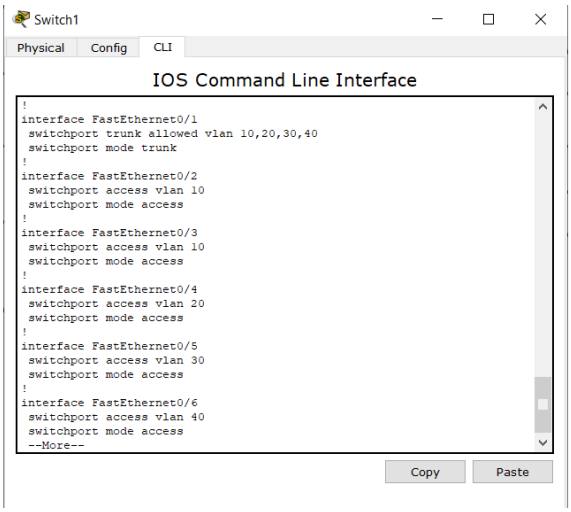

Рисунок 3.3 – Результат налаштувань на комутаторі Switch1

Таким же чином налаштовуємо Switch2.

Налаштування правильні. Зібрану мережу модна побачити на рис 3.4:

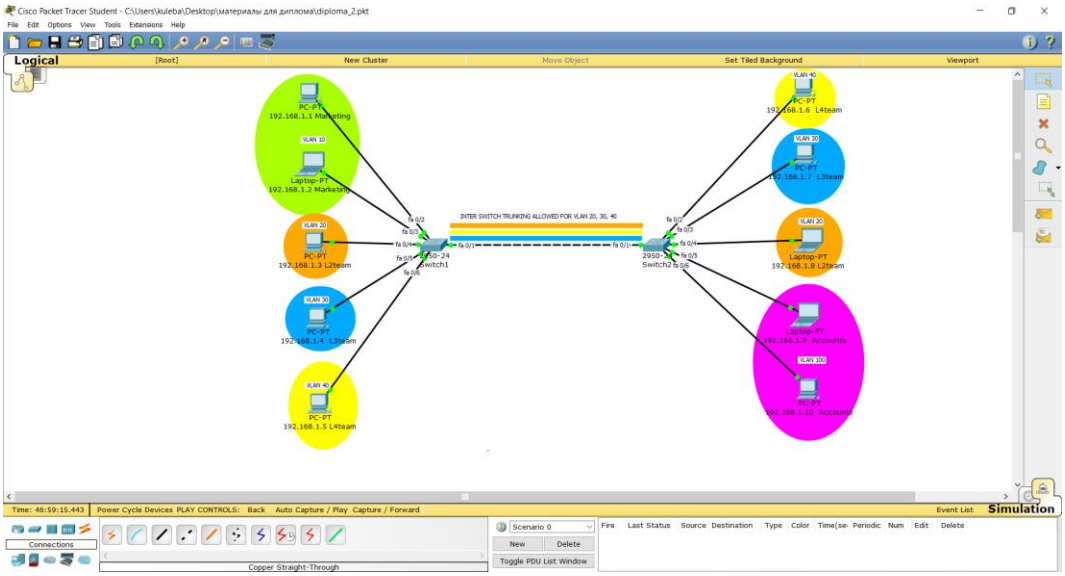

Рисунок 3.4 – Результат розгортання мережі на двох комутаторах

Подивимось, як просуваються пакети в мережі в режимі симуляції. На вихідному термінальному пристрої пакет ще не інкапсульований (рис 3.5), він має

тільки заголовок Ethernet II на поверхневому рівні (Out Layer) 2 рівня OSI, ми також бачимо IP-заголовок 3 рівня OSI на вихідному термінальному пристрої.

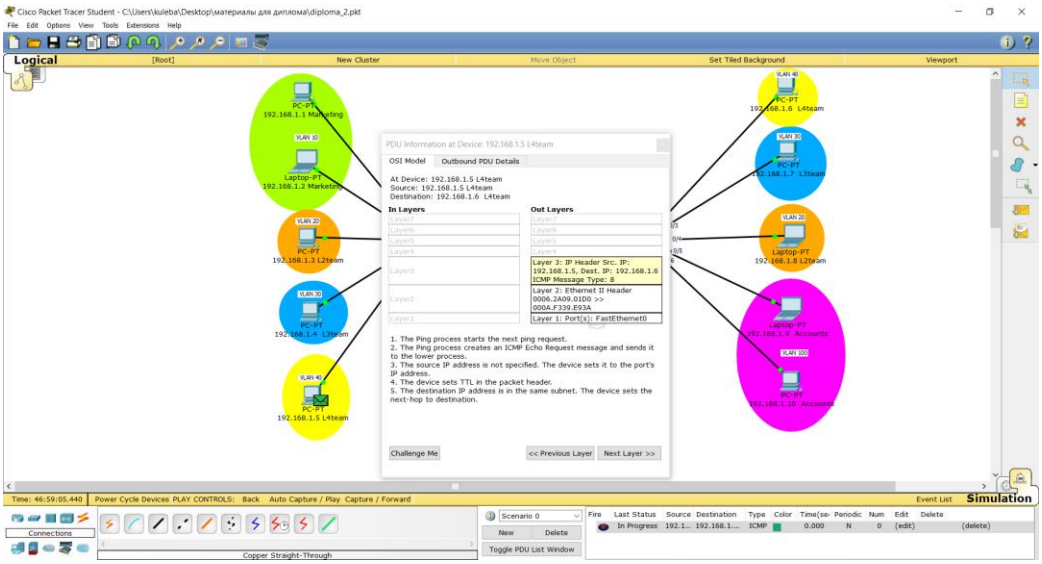

Рисунок 3.5 – Зміст пакету, що перехоплений на вихідному термінальному пристрої перед комутатором

На першому комутаторі Switch 1 (рис 3.6) після інкапсуляції з’являється поверхневий заголовок 802.1q (заголовок Ethernet II опиняється на внутрішньому рівні In Layer):

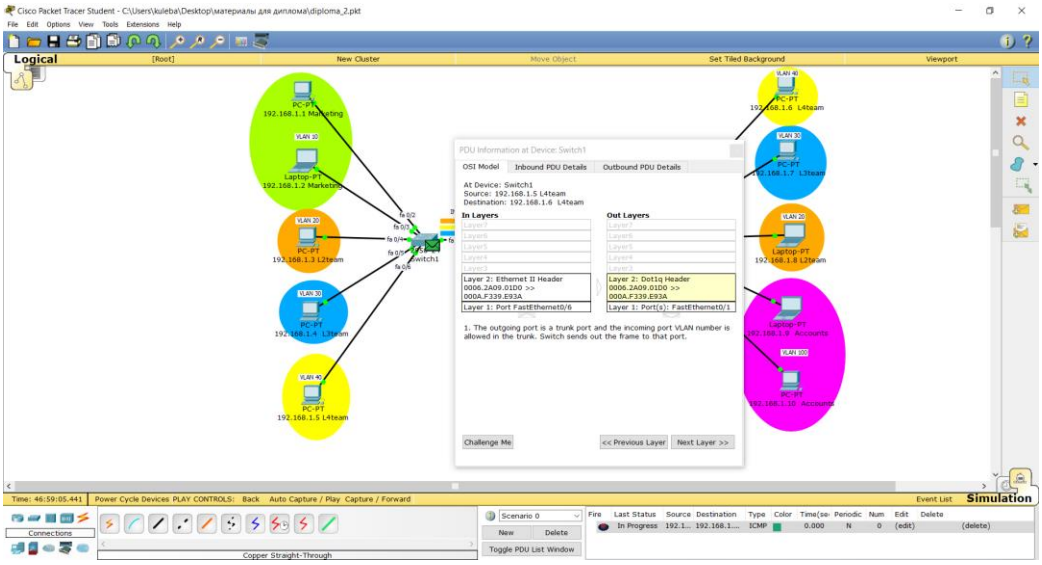

Рисунок 3.6 – Структура пакету, що перехоплений на комутаторі Switch 1 перед просуванням магістраллю

На вхідному комутаторі Switch 2 (рис. 3.7) заголовки міняються місцями: заголовок 802.1q опиняється на In Layer, Ethernet II на Out Layer), заголовка 3 рівня OSI на комутаторі бути не може.

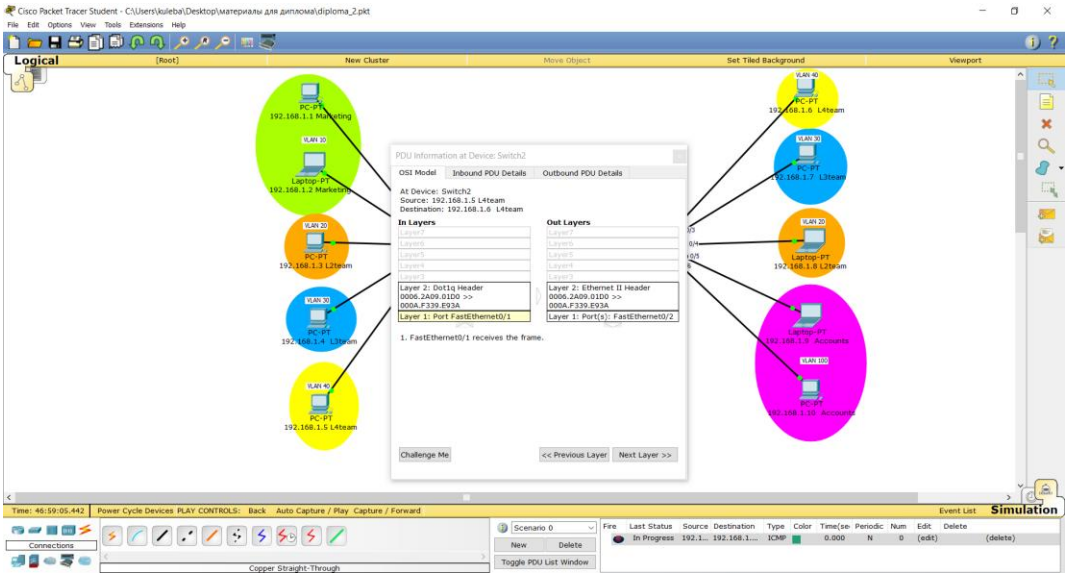

Рисунок 3.7 – Структура пакету, перехопленого на вхідному комутаторі після просування магістраллю

Пакет прибуває до термінального пристрою з IP-заголовками рівню 3, на другому рівні заголовки Ethernet II після декапсуляції (рис. 3.8).

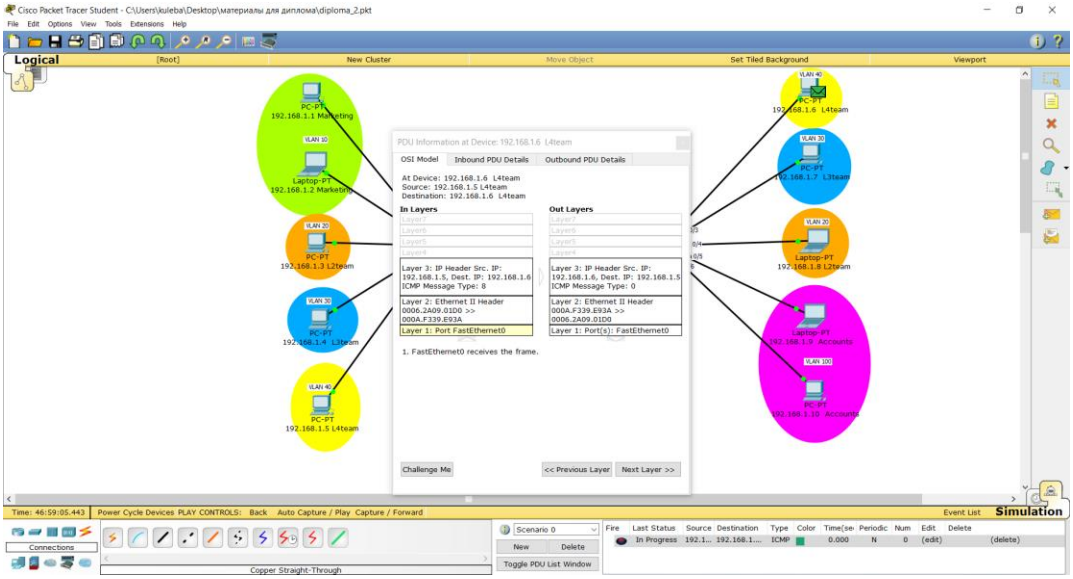

Рисунок 3.8 – Структура пакету, перехопленого на вхідному кінцевому пристрої

У режимі реального часу перевіряємо трафік усередені віртуальних мереж та між ними.

Пакет з 192.168.1.2 Marketing до 192.168.1.2 Marketing *Success*

Пакет з 192.168.1.2 Marketing до 192.168.1.3 L2team *Failure*

Пакет з 192.168.1.5 L4team до 192.168.1.6 L4team *Success*

Пакет з 192.168.1.8 L2team до 192.168.1.3 L2team *Success*

Пакет з 192.168.1.9 Accounts до 192.168.1.10 Accounts *Success*

Пакет з 192.168.1.9 Accounts до 192.168.1.2 Marketing *Failure*

Отже мережа працює правильно, фільтруючи транковий трафік згідно налаштувань.

3.2 VLAN у мережі SOHO на одному комутаторі й маршрутизаторі

Мережа буде мати топологію, як зображено на рис. 3.9:

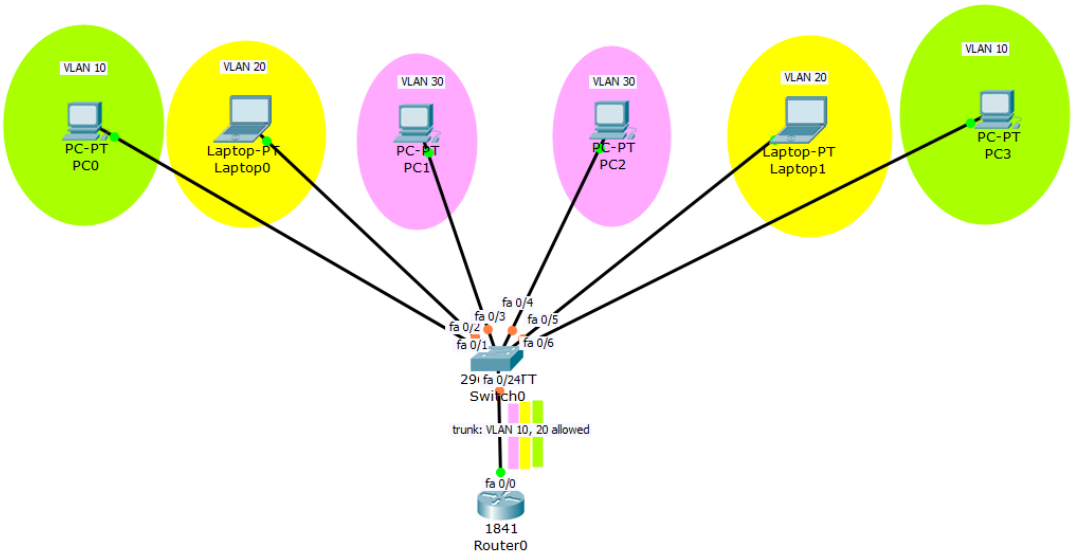

Рисунок 3.9 – Модель мережі з VLAN на одному комутаторі та маршрутизаторі.

До порту fa 0/0 маршрутизотору 1841 під’єднуємо порт fa 0/24 комутатора 2950-24 (використовуємо мідний кросовер).

До інтерфейсів комутатора Switch0 приєднуємо термінальні пристрої, зліва направо (використовуємо прямий мідний кабель):

Інтерфейс fa 0/1 – PC0 (VLAN 10)

Інтерфейс fa 0/2 – Laptop0 (VLAN 20)

Інтерфейс fa 0/3 – PC1 (VLAN 30)

Інтерфейс fa 0/4 – PC2 (VLAN 30)

Інтерфейс fa 0/5 – Laptop1 (VLAN 20)

Інтерфейс fa 0/6 – PC2 (VLAN 10)

Використовуючи інструменти малювання, графічно визначаємо віртуальні мережі еліпсами різних кольорів та надписуємо еліпси в залежності від належності до певної VLAN, використовуючи інструмент Place Note.

Також надписуємо віртуальні мережі, трафік яких дозволений у транковому каналі – всі віртуальні мережі.

Налаштовуємо комутатор: оголошуємо VLAN 10, 20, 30 за допомогою команд, що ми вже описували для попередньої мережі.

Призначаємо порти доступу на комутаторі та приписуємо їм відповідні віртуальні мережі – ці команди також ідентичні тим, що використовувалися на даному етапі в попередній схемі.

Switch#show run (перевіряємо налаштування портів доступу на комутаторі – рис. 3.10).

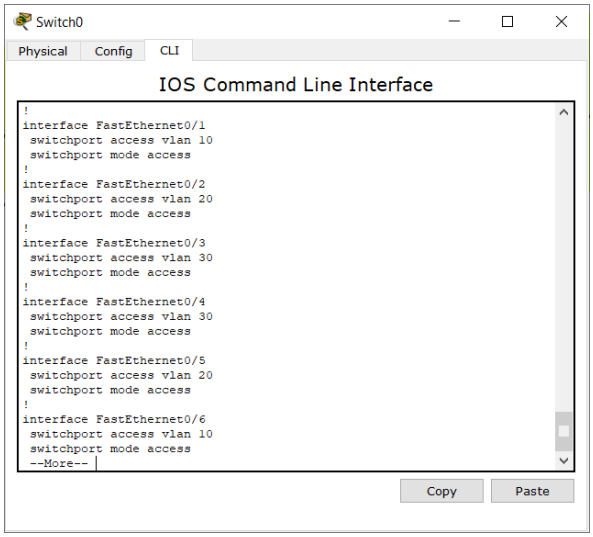

Рисунок 3.10 – Результат налаштування портів доступу на комутаторі

Налаштовуємо транковий режим від комутатора до маршрутизатора, як у попередній схемі, але з тією різницею, що ми дозволяємо трафік усіх віртуальних мереж:

Switch(config-if)# switchport trunk allowed vlan all

Перевіряємо налаштування транку на комутаторі (рис. 3.10):

Switch#show run

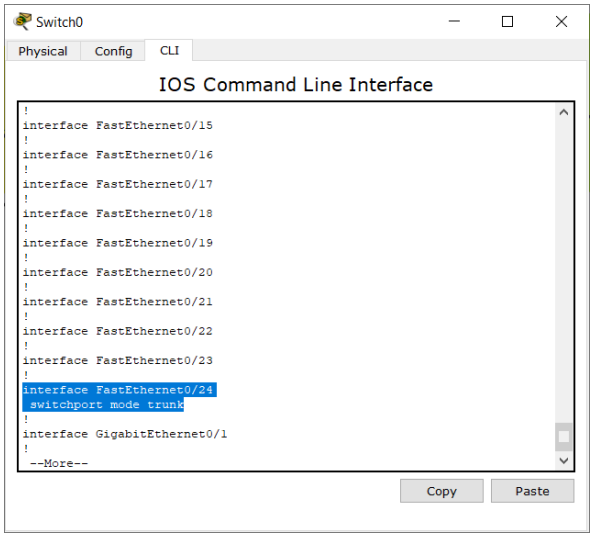

Рисунок 3.11 – Результат налаштування транку на комутаторі

Налаштовуємо маршрутизотор. Створюємо 3 субінтерфейси для кожної віртуальної мережі на маршрутизаторі, призначаємо інкапсуляцію для відповідних

віртуальних мереж в залежності від інтерфейсу, призначаємо IP-адреси для кожного субінтерфейсу.

Router(config)#interface fa 0/0 (входимо в режим інтерфейсу)

Router(config-if)#no shutdown (піднімаємо інтерфейс)

Router(config)#interface fa0/0.10 (входимо в режим субінтерфейсу)

Router(config-subif)#encapsulation dot1q 10 (призначаємо інкапсуляцію)

Router(config-subif)#ip address 110.110.10.110 255.255.255.0 (призначаємо IP-адресу субінтерфейсу)

Таким же чином налаштовуємо інші субінтерфейси.

Перевіряємо налаштування за допомогою *sh run.*

Далі Виключаємо статичні IP-адреси (адреси субінтерфейсів маршрутизатора, що ми призначили раніше) та конфігуруємо 3 пула DHCP для віртуальних мереж 110.110.10.0, 120.120.20.0, та 130.130.30.0.

Router(config)#ip dhcp excluded-address 110.110.10.110

За цією ж схемою виключаємо адреси інших субінтерфейсів.

Приписуємо пул адрес певній мережі:

Router(config)#ip dhcp pool lan-10

Router(dhcp-config)#network 110.110.10.0 255.255.255.0 (визначаємо мережу для пула)

Router(dhcp-config)#default-router 110.110.10.110 (визначаємо дефолтний роутер)

І таким чином для всіх інших мереж.

Перевіряємо налаштування (рис. 3.12):

Router#show run:

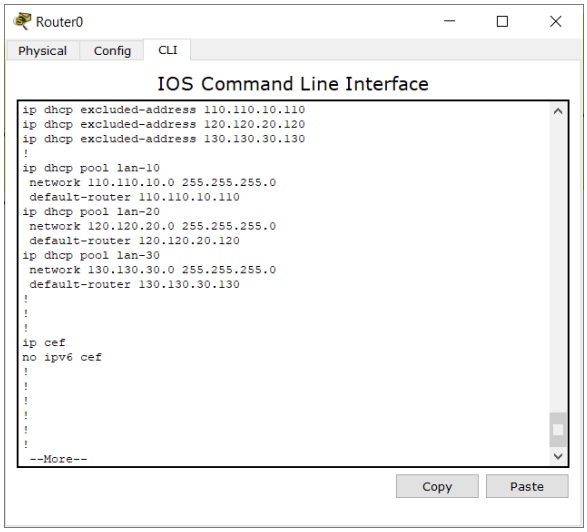

Рисунок 3.12 – Результат налаштувань *dhcp pool*

Налаштування правильні, тому записуємо їх у пам’ять:

Router#write memory

На термінальних пристроях вмикаємо режим DHCP через екранні форми (рис. 3.13).

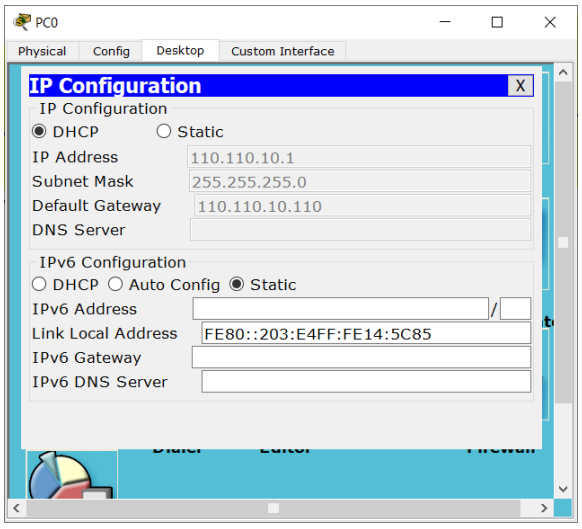

Рисунок 3.13 – Результат налаштування режиму DHCP на кінцевих пристроях через екранні форми.

Подивимося автоматично розподілені IP-адреси та MAC-адреси відповідних термінальних пристроїв (рис. 3.14):

Router#show ip dhcp binding

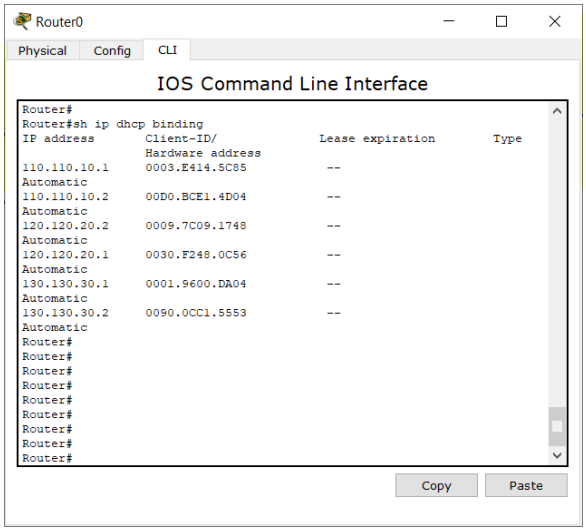

Рисунок 3.14 – Результат автоматичного розподілення IP-адреси та MAC-адреси термінальних пристроїв

Отже, маємо три пари IP-адрес, по дві адреси з кожної віртуальної мережі. Якщо ми перевіримо IP-адреси всіх термінальних пристроїв через екранні форми, побачимо таку картину:

Інтерфейс fa 0/1 – PC0 (VLAN 10) 110.110.10.1/24

Інтерфейс fa 0/2 – Laptop0 (VLAN 20) 120.120.20.1/24

Інтерфейс fa 0/3 – PC1 (VLAN 30) 130.130.30.2/24

Інтерфейс fa 0/4 – PC2 (VLAN 30) 130.130.30.1/24

Інтерфейс fa 0/5 – Laptop1 (VLAN 20) 120.120.20.2/24

Інтерфейс fa 0/6 – PC2 (VLAN 10) 110.110.10.2/24

Таким чином, розподіл IP-адрес правильний, він відповідає приналежності інтерфейсів комутатора та термінальних пристроїв до призначених віртуальних мереж.

Тестуємо мережу у режимі симуляції.

Якщо ми пересилаємо пакети у межах однії віртуальної мережі (наприклад, з VLAN 10 до VLAN 10, з VLAN 20 до VLAN 20, з VLAN 30 до VLAN 30), то ми помітимо, що маршрутизатор не бере участі у розподілі трафіку (рис 3.15-3.17), для цього достатньо комутатору. З таким же успіхом можемо «вбити» маршрутизатор

або перервати лінію зв’язку меж комутатором та маршрутизатором, нічого не зміниться.

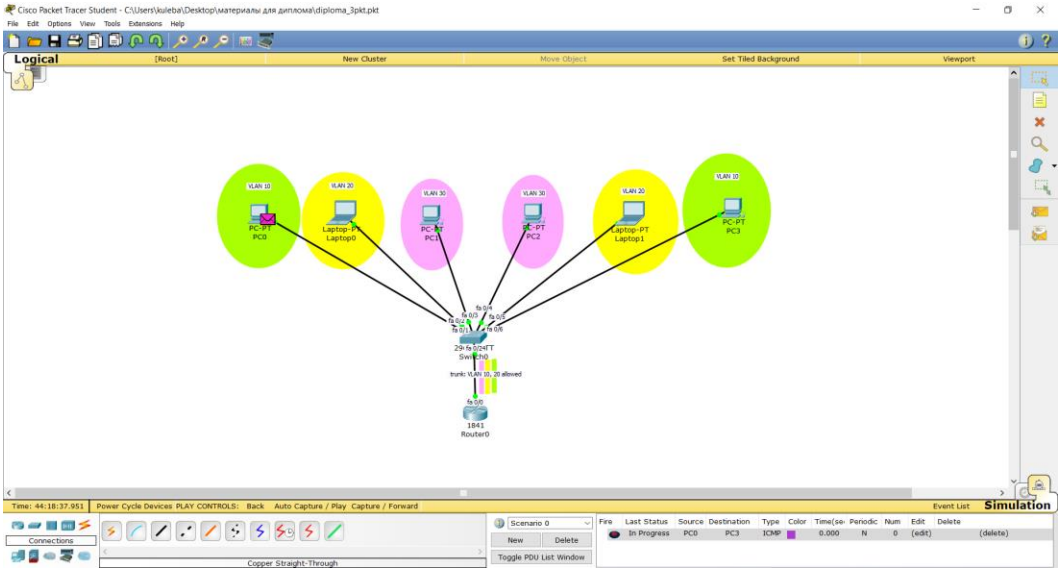

Рисунок 3.15 – Позиція пакету на вихідному термінальному пристрої (трафік в межах однієї VLAN)

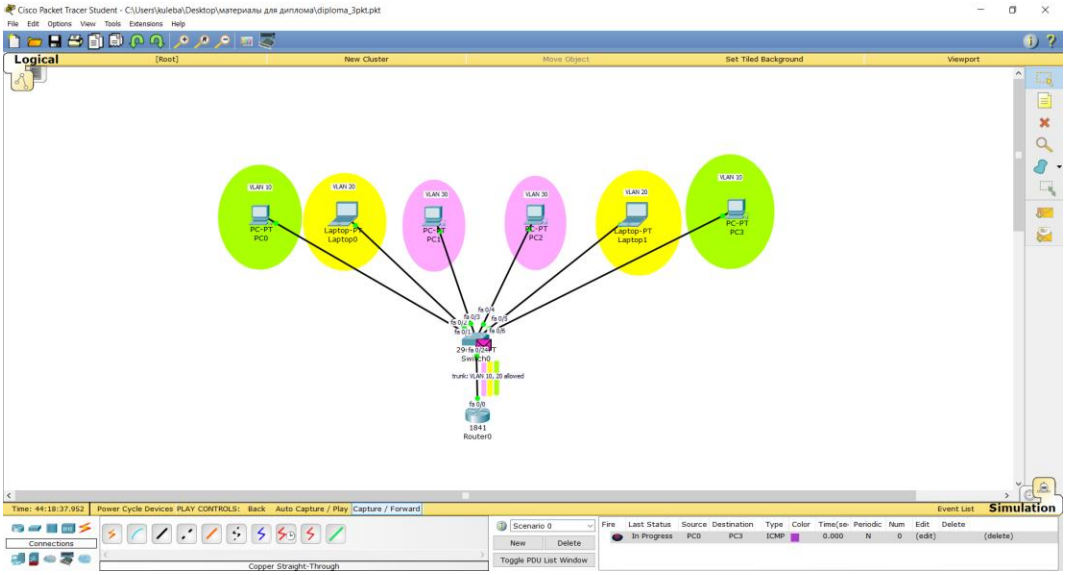

Рисунок 3.16 – Позиція пакету на комутаторі (трафік в межах однієї VLAN)

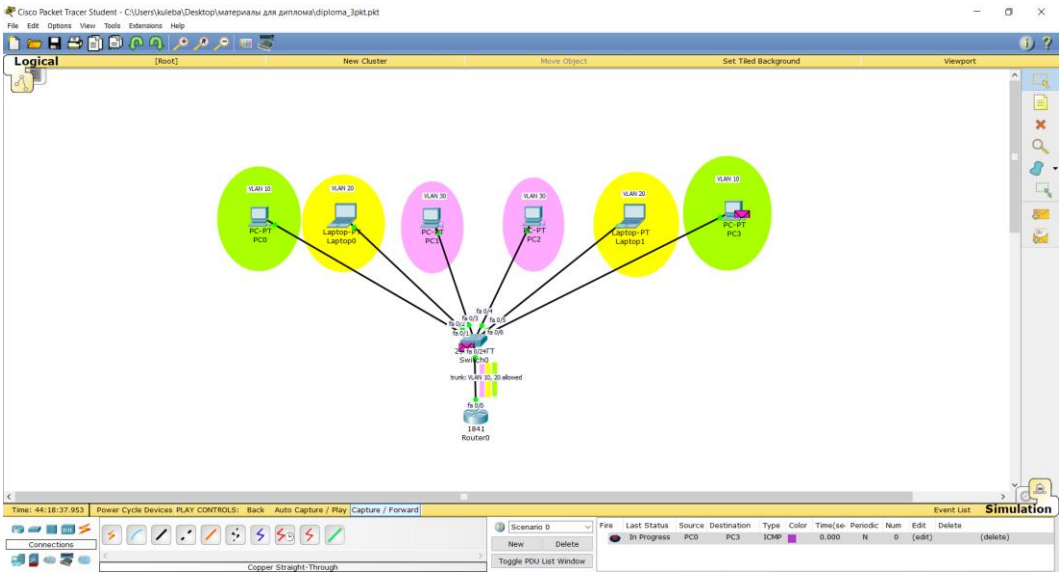

Рисунок 3.17 – Позиція пакету на вхідному кінцевому пристрої (трафік в межах однієї VLAN)

Якщо ми перехопимо пакети (рис. 3.18-3.20), ми побачимо тільки Ethernet II заголовки як на термінальних пристроях, так і на комутаторі (також IP-заголовки на термінальних пристроях).

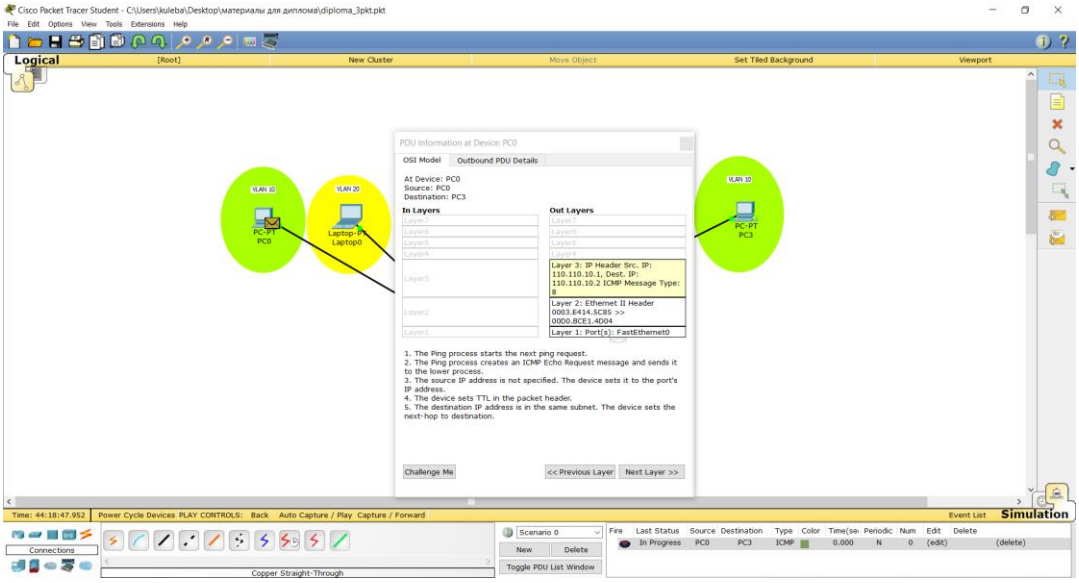

Рисунок 3.18 – Структура пакету, що перехоплений на вихідному термінальному пристрої (трафік в межах однієї VLAN)

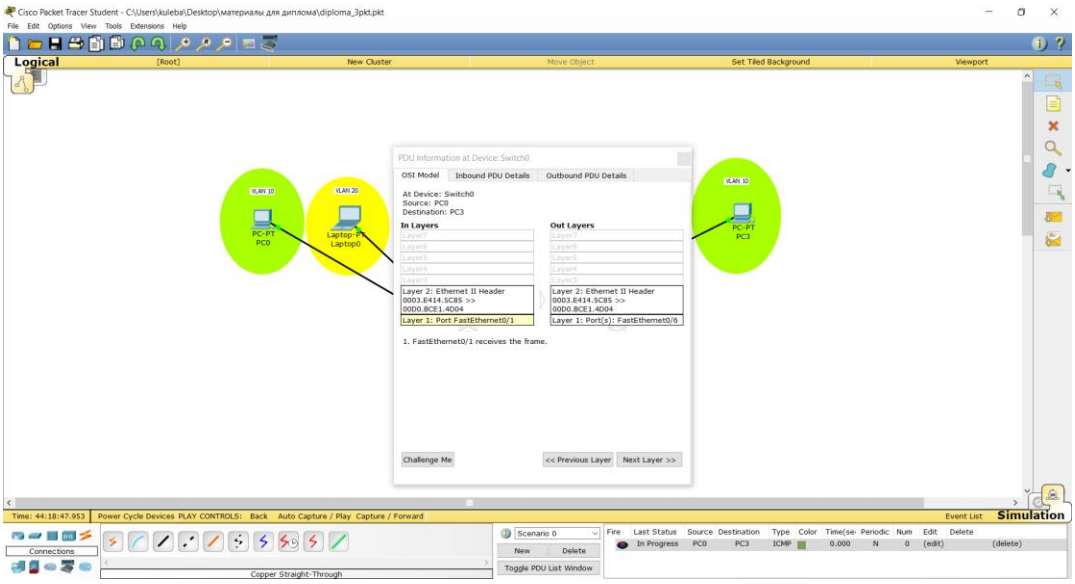

Рисунок 3.19 – Зміст пакету, що перехоплений на комутаторі (трафік в межах однієї VLAN)

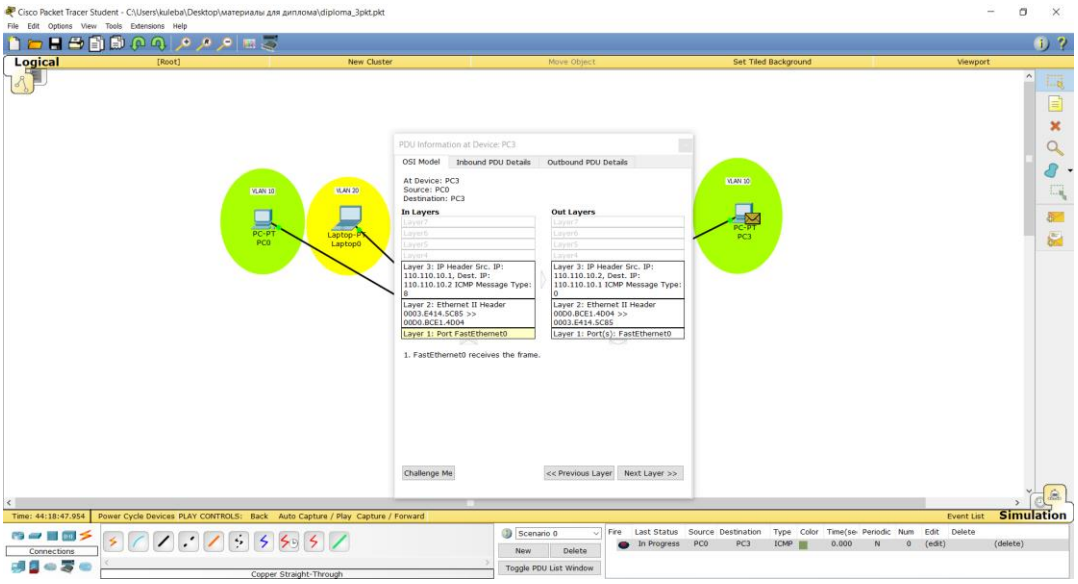

Рисунок 3.20 – Зміст пакету, що перехоплений на вхідному кінцевому пристрої (трафік в межах однієї VLAN)

Тепер перехопимо пакети під час передачі пакетів з однієї віртуальної мережі в іншу.

Відмінним буде те, що залучається магістральний канал й пакет потрапляє на маршрутизатор для інкапсуляції (рис. 3.21): ми побачимо це, якщо перехопимо пакет на маршрутизаторі.

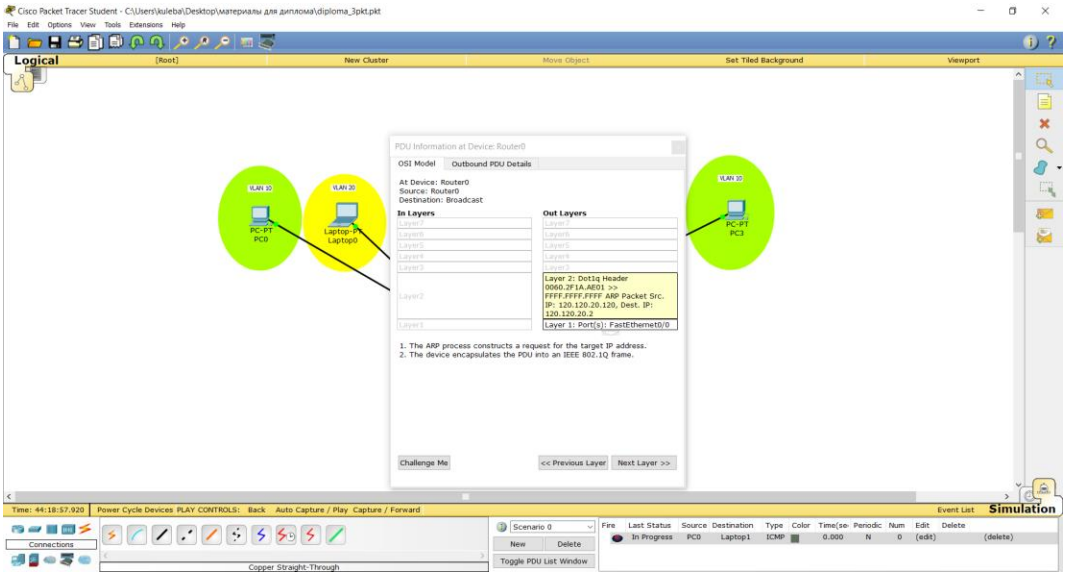

Рисунок 3.21 – Структура пакету, що перехоплений на маршрутизаторі (трафік між різними VLAN)

З цього моменту структура пакету буде мінятися так, як ми вже описували для попередньої моделі мережі (рис. 3.22).

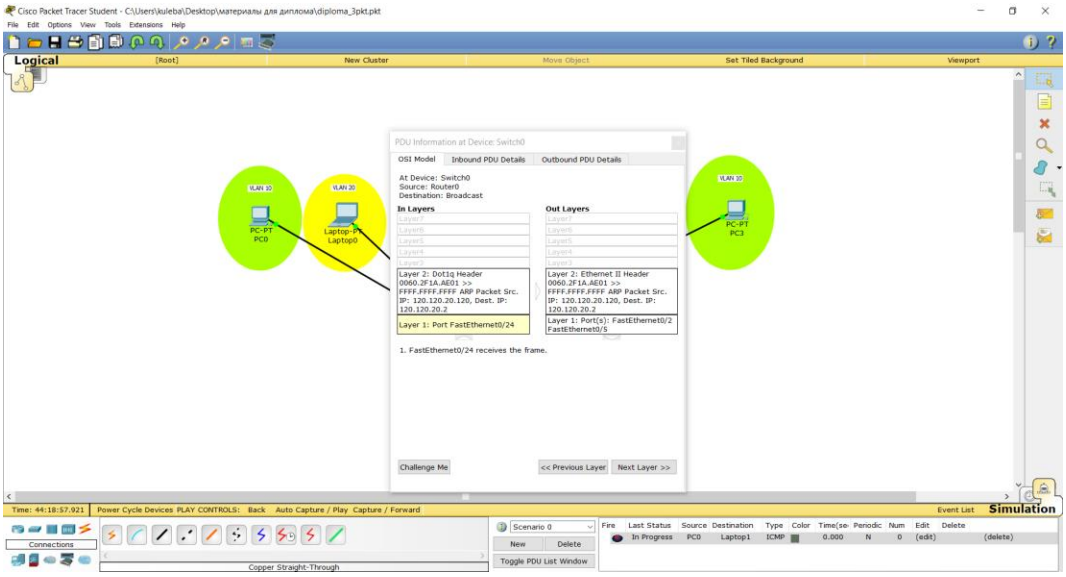

Рисунок 3.22 – Структура пакету, що перехоплений на вхідному кінцевому пристрої (трафік між різними VLAN)

При цьому ми бачимо, що пакет передається потрібному термінальному пристрою вхідної віртуальної мережі, і не передається іншому пристрою з тієї ж мережі (рис. 3.23-3.24).

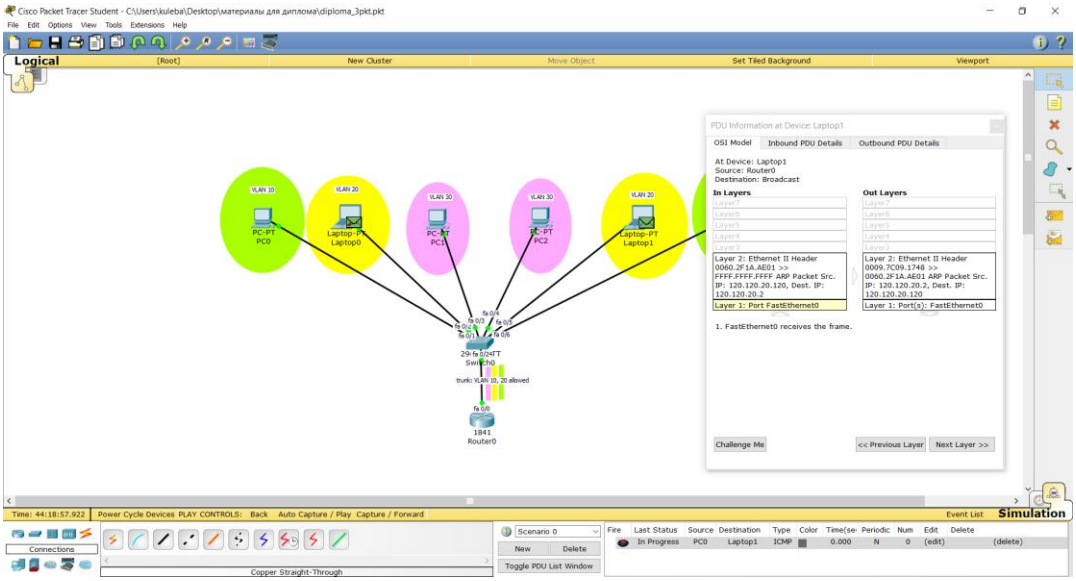

Рисунок 3.23 – Структура пакету, що передається потрібному термінальному пристрою

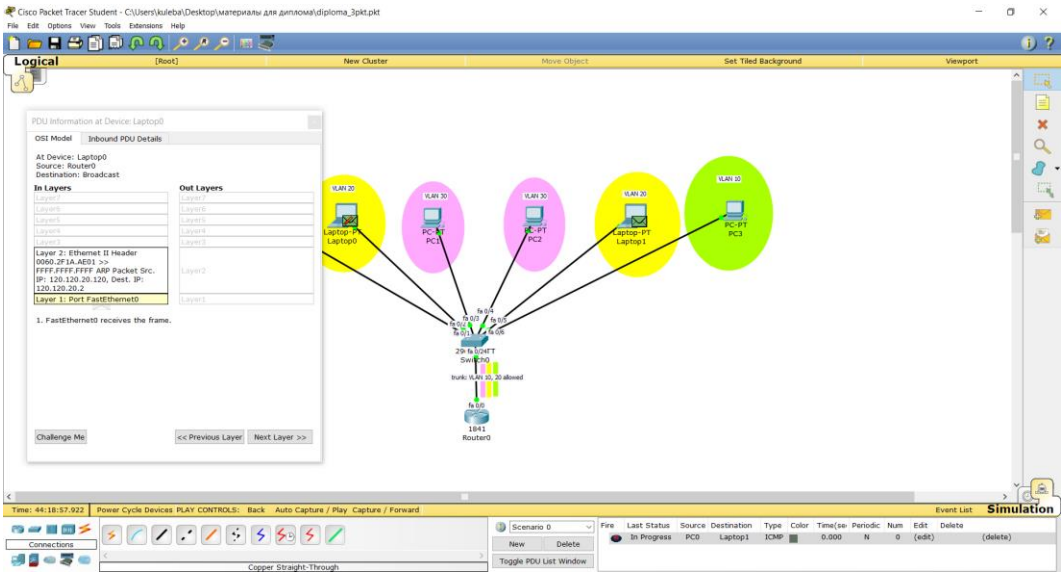

Рисунок 3.24 – Структура пакету, що не не приходить до іншого термінального пристроя в тій самій мережі

Оскільки магістраль в мережі відкрита для всіх VLAN, у користувачів має бути можливість пересилати пакети з будь-якого термінального пристрою на будь-який термінальний пристрій. Перевіримо це в режимі реального часу:

Пакет з PC0 (VLAN 10) до Laptop0 (VLAN 20) *Success*

Пакет з PC0 (VLAN 10) до Laptop1 (VLAN 20) *Success*

Пакет з PC0 (VLAN 10) до PC1 (VLAN 30) *Success*

Пакет з PC0 (VLAN 10) до PC1 (VLAN 30) *Success*

Пакет з PC1 (VLAN 30) до Laptop1 (VLAN 20) *Success*

Пакет з PC0 (VLAN 10) до PC1 (VLAN 30) *Success*

Пакет з PC2 (VLAN 30) до PC0 (VLAN 10) *Success*

Отже мережа зібрана правильно й функціонує відповідно до налаштувань.

3.3 Мережа SOHO з віртуальними мережами на комутаторі третього рівня та маршрутизаторі з IP-телефонією.

Змоделюємо дану мережу згідно схемі, що представлена на рис. 3.25:

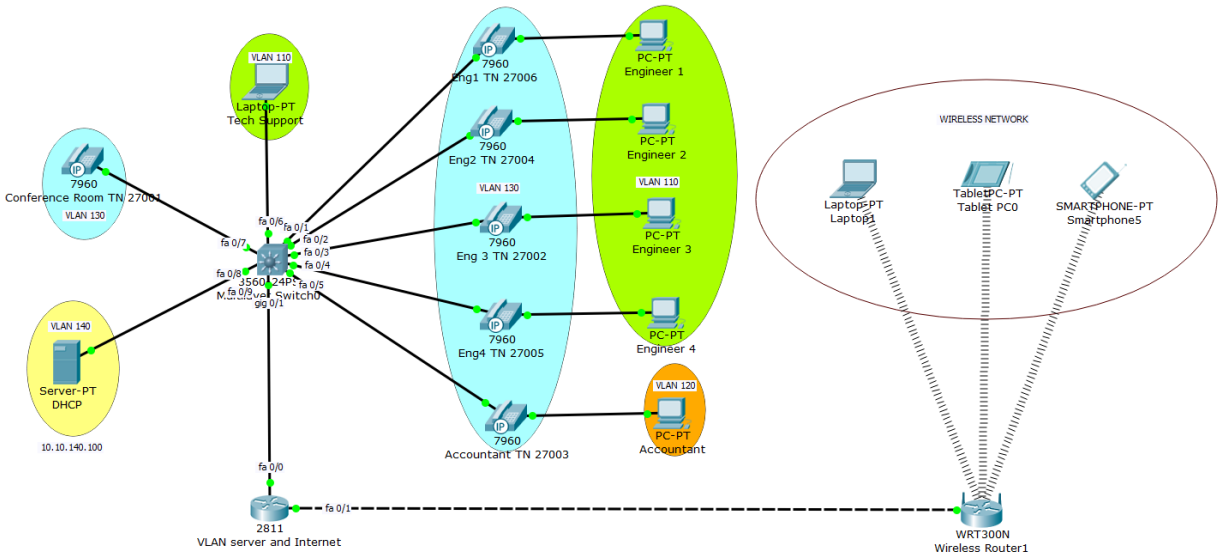

Рисунок 3.25 – Проект мережі на комутаторі третього рівня з IP-телефонією та Wi-Fi

З’єднуємо Multilayer Switch0 3650-24PS з термінальними пристроями у зіркову топологію (використовуємо прямий мідний кабель):

Інтерфейс fa 0/1 – ПК Engineer 1 (через IP-телефон Eng1 TN 27006, Vlan 130), Vlan 110.

Інтерфейс fa 0/2 – ПК Engineer 2 (через IP-телефон Eng2 TN 27004, Vlan 130), Vlan 110.

Інтерфейс fa 0/3 – ПК Engineer 3 (через IP-телефон Eng3 TN 27002, Vlan 130), Vlan 110.

Інтерфейс fa 0/4 – ПК Engineer 4 (через IP-телефон Eng4 TN 27005, Vlan 130), Vlan 110.

Інтерфейс fa 0/5 – ПК Accountant (через IP-телефон Accountant TN 27003), Vlan 120.

Інтерфейс fa 0/6 – Laptop PT Tech Support, Vlan 110.

Інтерфейс fa 0/7 – IP-телефон Conference room 27001, Vlan 130.

Інтерфейс fa 0/8 – Server PT DHCP, Vlan 140.

Інтерфейс gig 0/1– маршрутизатор 2811 (VLAN server).

З'єднуємо маршрутизатор 2811 з бездротовим маршрутизатором WRT 300N (використовуємо мідний кросовер): інтерфейс fa 0/1 – інтерфейс Internet 0/0.

Використовуючи інструмент Place Note (Нотатки) задаємо назви термінальних пристроїв, вказуючи IP-адреси та функціональні групи, до яких вони належать.

Використовуючи інструменти малювання, графічно визначаємо віртуальні мережі еліпсами різних кольорів та надписуємо еліпси в залежності від приналежності до певної VLAN, використовуючи інструмент Place Note.

Налаштовуємо VLAN сервер на маршрутизаторі (піднімаємо інтерфейс, призначаємо субінтерфейси, приписуємо їм IP-адреси, визначаємо *ip helper-address (крім сервера DHCP),* інкапсуляцію 802.1q) як у попередній мережі.

Налаштовуємо комутатор третього рівня: оголошуємо віртуальні мережі, призначаємо порти доступу, конфігуруємо транковий порт від комутатора до маршрутизатора.

Оголошуємо віртуальні мережі та іменуємо їх на комутаторах, як у першій та другій схемах.

Призначаємо порти доступу аналогічно до попередніх мереж.

Перевіряємо конфігурацію VLAN (рис. 3.26):

Switch# sh vlan brief

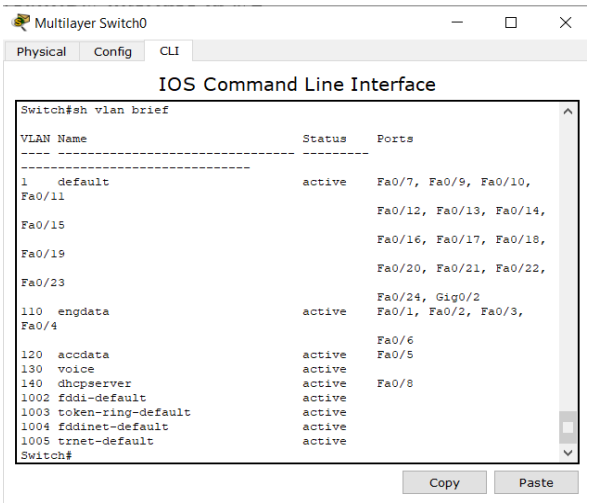

Рисунок 3.26 – Результат конфігурування віртуальних мереж

Порти комутатора налаштовані правильно відповідно до віртуальних мереж.

Налаштовуємо магістральний порт від комутатора до маршрутизатора аналогічно попередній мережі з одним комутатором і маршрутизатором.

Перевіряємо налаштування транкінгу (рис 3.27):

Switch# sh run

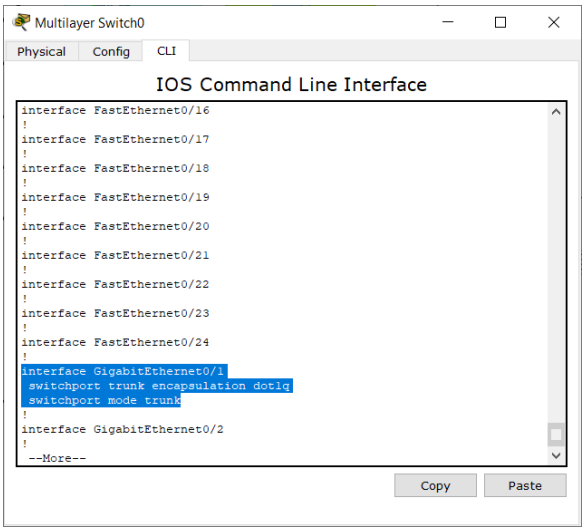

Рисунок 3.27 – Результат налаштування транкінгу на комутаторі

Налаштовуємо DHCP сервер (рис. 3.28) через екранні форми (на сервері Services → DHCP):

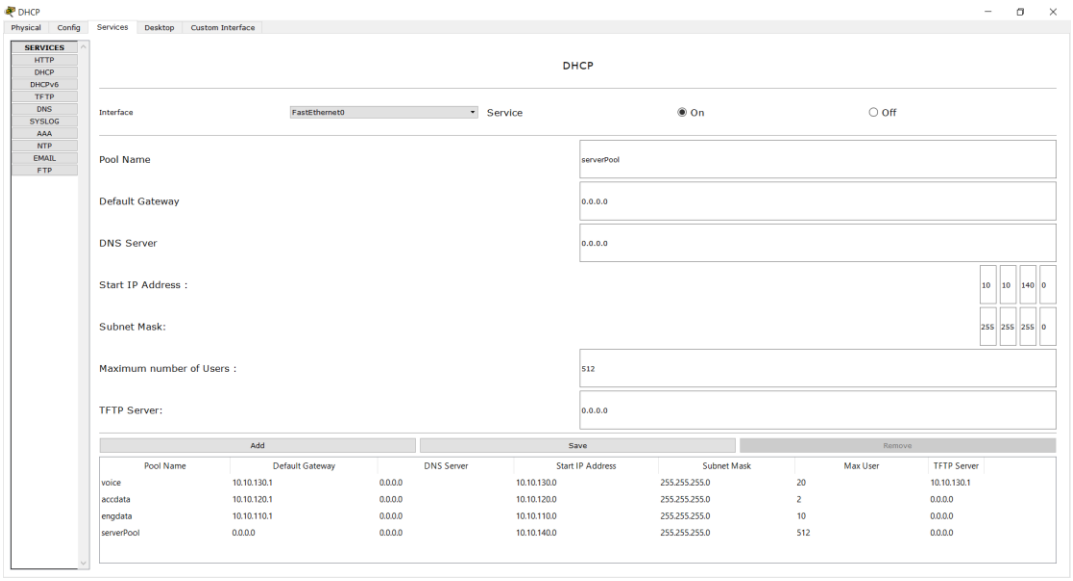

Рисунок 3.28 – Результати налаштування DHCP сервера через екранні форми

Для кожної віртуальної мережі додаємо ім’я пулу, призначаємо дефолтний шлюз (IP субінтерфейсу), стартову IP-адресу, маску підмережі, а для голосової віртуальної мережі – ще й TFTP сервер.

Перевіряємо доступність IP-адрес (10.10.110.1, 10.10.120.1, 10.10.130.1) за допомогою утіліти ping (рис.3.29-3.31):

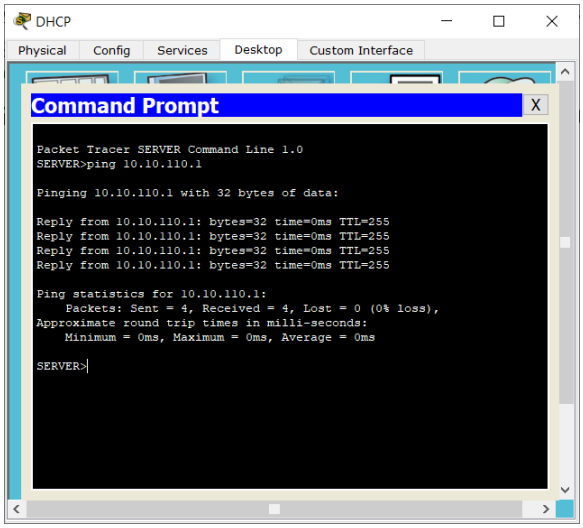

Рисунок 3.29 – Результат перевірки доступності 10.10.110.1

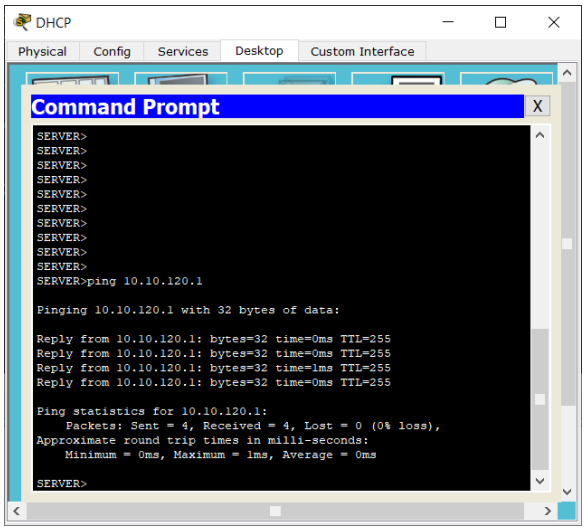

Рисунок 3.30 – Результат перевірки доступності 10.10.120.1

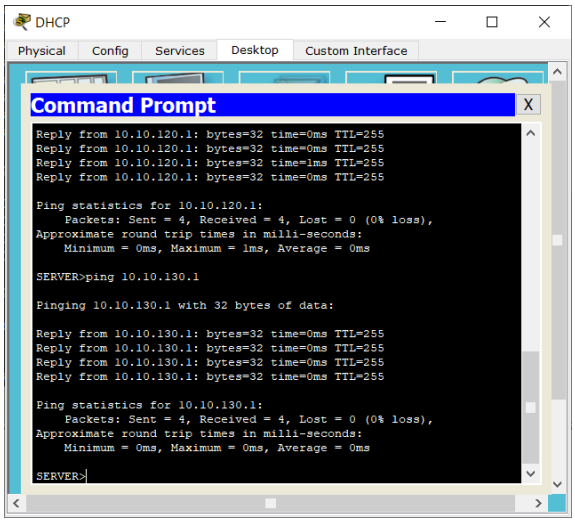

Рисунок 3.31 – Результат перевірки доступності 10.10.130.1

Як бачимо, всі вузли пінгуються, DHCP сервер налаштований правильно.

Далі приписуємо порти на комутаторі відповідним VLAN (одній голосовій VLAN якщо це один телефон, одній VLAN даних якщо це ПК або ноутбук, та двом VLAN – даних та голосу – якщо ПК або ноутбук підключається через IP-телефон).

Switch(config)#int fa 0/1 (заходимо в режим інтерфейсу)

Switch(config-if)#switchport access vlan 110 (призначаємо мережу даних)

Switch(config-if)#switchport voice vlan 130 (призначаємо мережу голосу)

Проводимо подібні налаштування для інших інтерфейсів і віртуальних мереж.

Перевіряємо конфігурацію портів доступу (рис. 3.32):

```
.
interface FastEthernet0/1
 switchport access vlan 110
 switchport voice vlan 130
!
interface FastEthernet0/2
 switchport access vlan 110
 switchport voice vlan 130
!
interface FastEthernet0/3
 switchport access vlan 110
 switchport voice vlan 130
!
interface FastEthernet0/4
 switchport access vlan 110
 switchport voice vlan 130
!
interface FastEthernet0/5
 switchport access vlan 120
 switchport voice vlan 130
!
interface FastEthernet0/6
 switchport access vlan 110
!
interface FastEthernet0/7
 switchport voice vlan 130
!
interface FastEthernet0/8
 switchport access vlan 140
!
```

Рисунок 3.33 Результати перевірки портів доступу

Як бачимо, порти доступу налаштовані правильно.

Далі конфігуруємо сервіси IP-телефонії та розподіл телефонних номерів на маршрутизаторі.

Router(config)#telephony-service (входимо в режим налаштування телефонного сервісу)

Router(config-telephony)#max-dn 144 (задаємо максимальну кількість телефонних номерів)

Router(config-telephony)#max-ephones 20 (задаємо максимальну кількість телефонних пристроїв)

Router(config-telephony)#ip source-address 10.10.130.1 port 2000 (задаємо IP-адресу джерело)

Router(config-telephony)#auto assign 1 to 144 (задаємо автоматичний розподіл номерів)

Router(config-telephony)#exit (виходимо у попередній режим)

Router(config-telephony)#exit (виходимо у попередній режим)

Router(config)#ephone-dn 1 (входимо у режим конфігурації телефону)

Router(config-ephone-dn)#number 27001 (задаємо номер)

Аналогічні налаштування проводимо для інших телефонних пристроїв та номерів.

Після цього підключаємо телефони до мережі енергопостачання. Телефонні номери будуть роздаватися по черзі підключення. Щоб підключити телефонний апарат до мережі енергопостачання в Cisco Packet Tracer, треба зайти на вкладку фізичного інтерфейсу телефону й мишкою перетащити силовий кабель до гнізда (рис. 3.34).

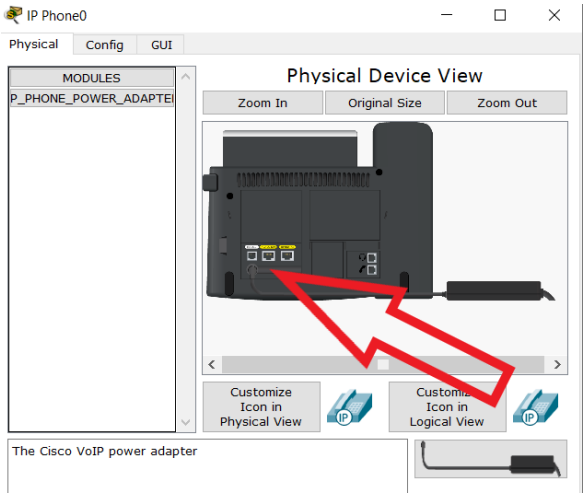

Рисунок 3.34 – Підключення телефонного аппарату до мережі живлення

Спробуємо поздвонити з одного телефонного апарату на інший.

Використовуючи GUI, знімаємо слухавку з телефону 27006 та дзвонимо на номер 27003 (рис. 3.35). Йде сигнал виклику, визначається номер, з якого дзвонять (рис. 3.36). Отже телефонний сервіс налаштований правильно.

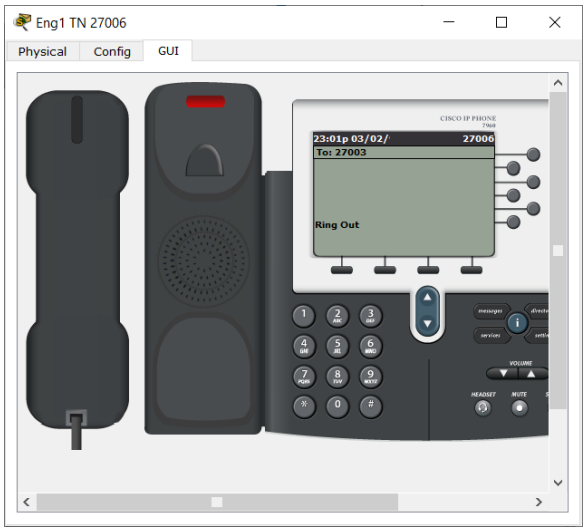

Рисунок 3.35 – Графічна фіксація вхідного в GUI

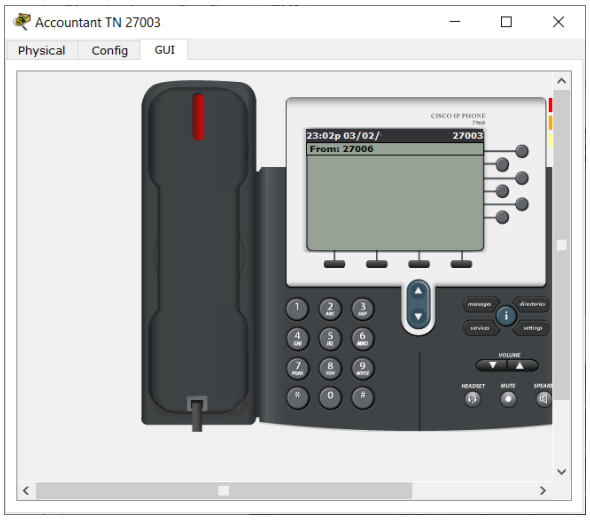

Рисунок 3.36 – Графічна фіксація вихідного звонка в GUI

Налаштовуємо точку доступу й Wi-Fi мережу для приватного користування працівників.

Піднімаємо інтерфейс fa 0/1 на маршрутизаторі та призначаємо IP-адресу 190.190.1.1 255.255.255.0. Він буде відігравати роль Інтернет порту для точки доступу.

Router(config)#interface fa 0/1

Router(config-if)#no shutdown

Router(config-subif)#ip address 190.190.1.1 255.255.255.0

Налаштовуємо порт LAN на бездротовому маршрутизаторі (рис. 3.35), що буде роздавати мережу бездротовим з'єднанням. Робимо це за допомогою графічного інтерфейса. IP-адресою для Wi-Fi буде 192.168.0.1/24

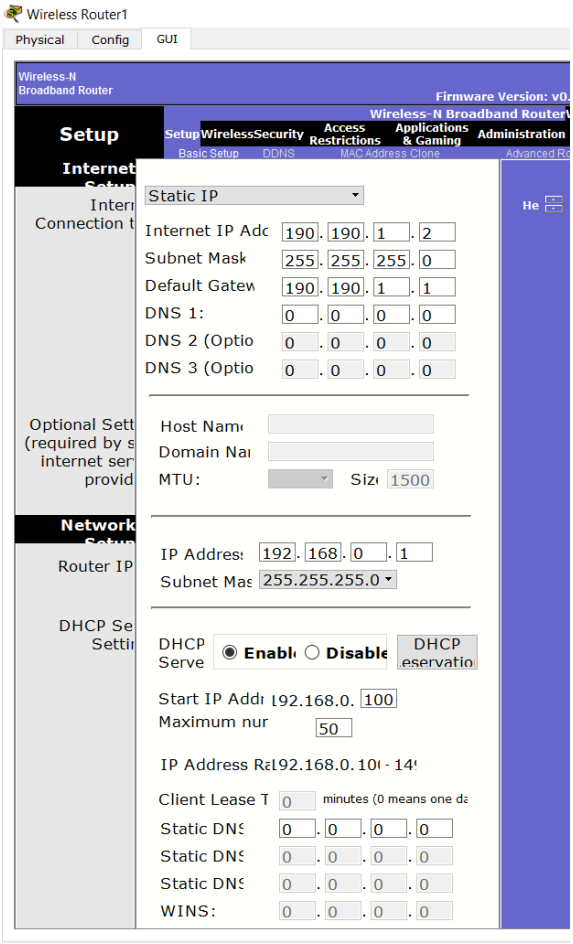

Рисунок 3.37 – Результати налаштування порта LAN на бездротовому маршрутизаторі через GUI

Налаштовуємо параметри Wireless (рис. 3.38)

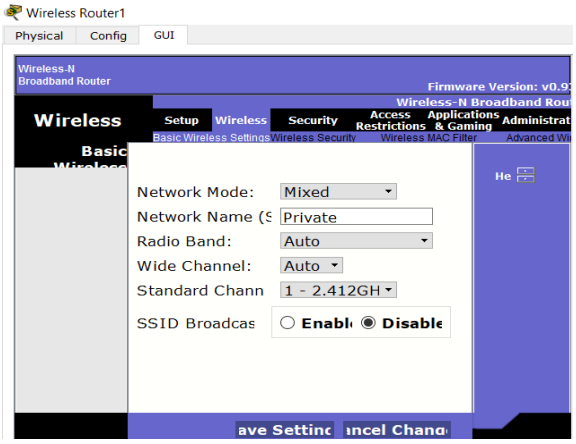

Рисунок 3.39 – Результати налаштування Wireless через GUI

Задаємо режим безпеки (WPA2) та пароль доступу *superpuper* (рис. 3.40):

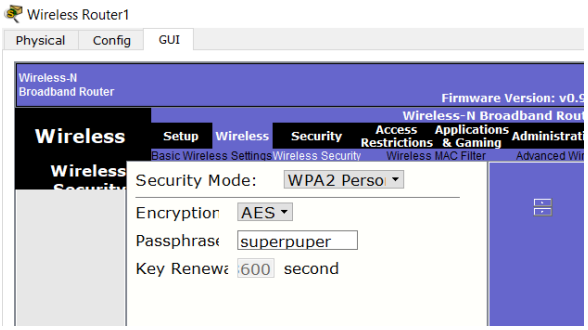

Рисунок 3.40 – Результати налаштування режиму безпеки та паролю через GUI

Додаємо кінцеві пристрої користувачів для мережі Wi-Fi: ноутбук, планшет, та смартфон.

Щоб підключити ноутбук до мережі Wi-Fi, треба спочатку вимкнути ноутбук, видалити модуль, взявши його мишкою та кинувши на панель модулів (рис. 3.38), і у вільний слот перетащити Wi-Fi модуль (рис. 3.39).

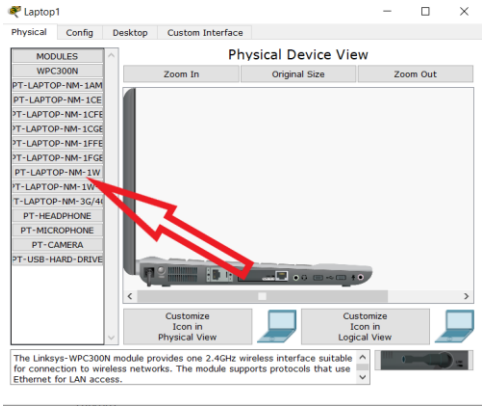

Рисунок 3.41 – Звільнити слот

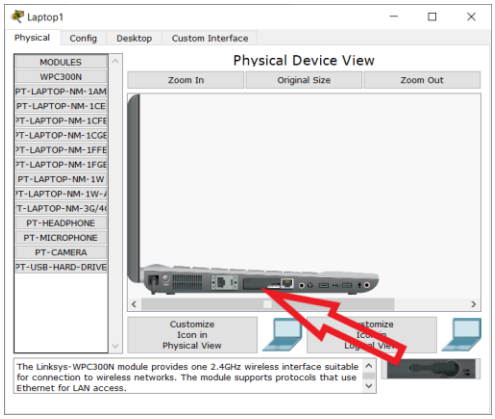

Рисунок 3.42 – Вставити бездротовий модуль у слот

Потім на кінцевих пристроях користувачів для мережі Wi-Fi треба налаштувати параметри відповідно до налаштувань точки доступу та ввести пароль (рис. 3.43).

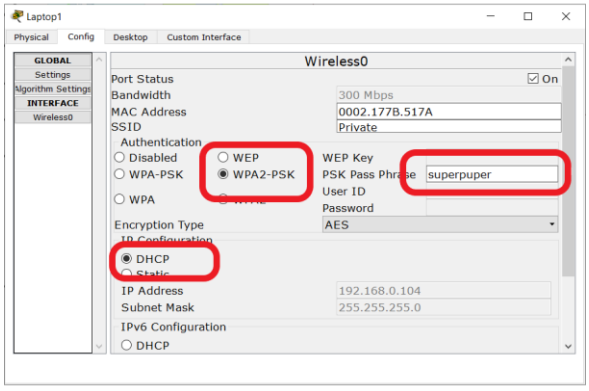

Рисунок 3.43 – Результати налаштування кінцевих пристроїв для мережі Wi-Fi

Ми бачимо, що бездротове з’єднання встановлено (рис. 3.44):

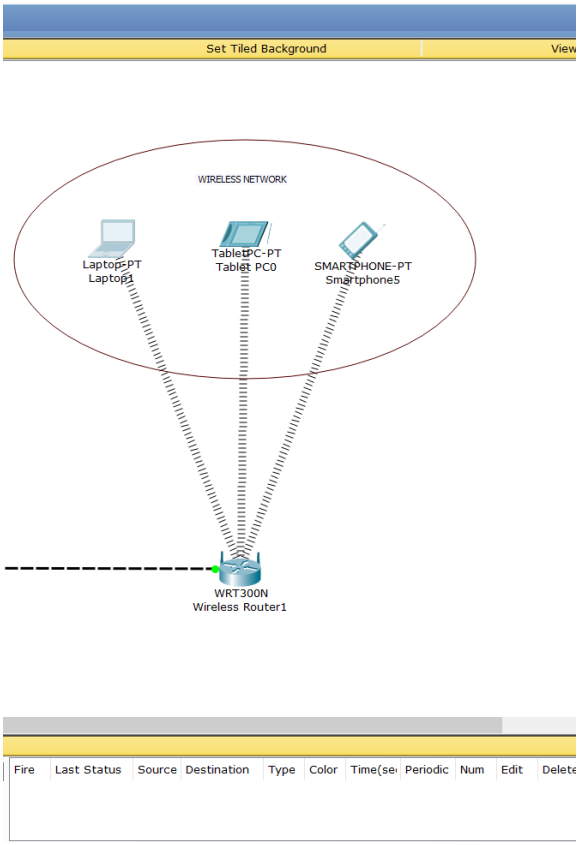

Рисунок 3.44 – Графічна маніфестація функціонального бездротового з’єднання у Cisco Packet Tracer

Протестуємо з’єднання за допомогою утіліти ping – наприклад, з ноутбуку на порт маршрутизатора fa 0/1 (рис. 3.45):

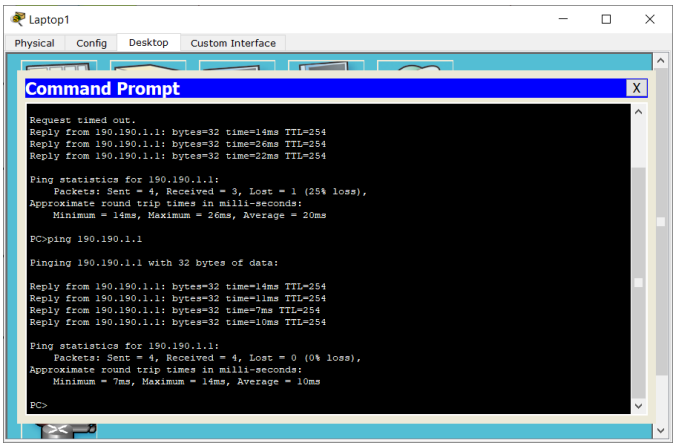

Рисунок 3.45 – Результат пінгу інтерфейса маршрутизатора

Пінг пройшов, отже бездротова мережа побудована правильно.

Скріншот повністю зібраної мережі представлений на (рис. 3.46).

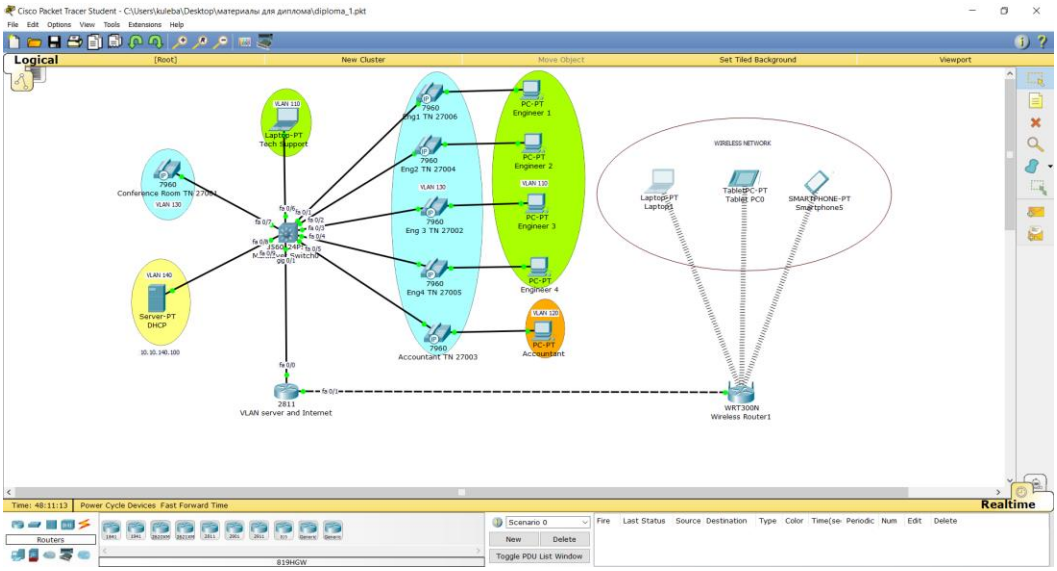

Рисунок 3.47 – Повністю зібрана мережа на комутаторі третього рівня

Протестуємо зібрану мережу. Теоретично, як і в попередній мережі, пакети, що йдуть до термінального пристрою своєї VLAN, не будуть потрапляти на маршрутизатор (крім ARP пакетів), а будут оброблятися на рівні комутатора. Якщо ж пакети будуть пересилатися з однієї VLAN на іншу, вони будуть оброблятися маршрутизатором.

Перевіримо це, перехоплюючи пакети в режимі симуляції.

Перешлемо пакет з ПК Engineer 4 на ПК Engineer 3 в одній мережі VLAN 110.

Пакет просувається з вихідного термінального пристрою, потрапляє на комутатор, і з комутатора – на вхідний термінальний пристрій. Перехоплюємо пакет на комутаторі (рис. 3.48). Бачимо тільки Ethernet II заголовки на In Layer та Out Layer.

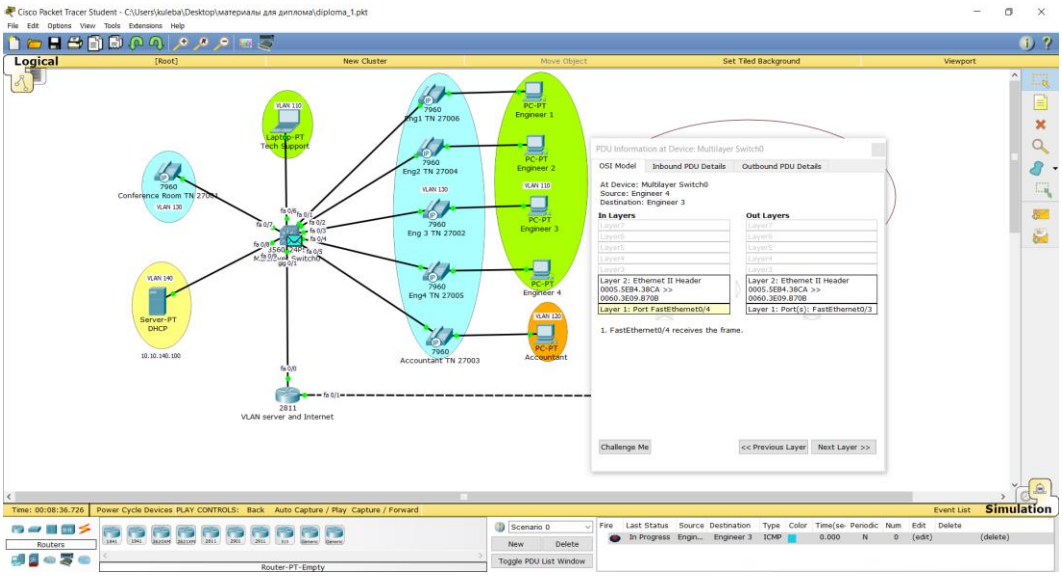

Рисунок 3.48 – Пакет в мережах однієї VLAN, перехоплений на комутаторі

Тепер перешлемо пакет з ПК Accountant (VLAN 120) на ПК Engineer 4 в мережі VLAN 110.

Пакет просувається з вихідного термінального пристрою, потрапляє на комутатор L3, з комутатора – на маршутизатор, потім знову на комутатор L3 і на вхідний термінальний пристрій.

Перехоплюємо пакет на комутаторі (рис. 3.49).

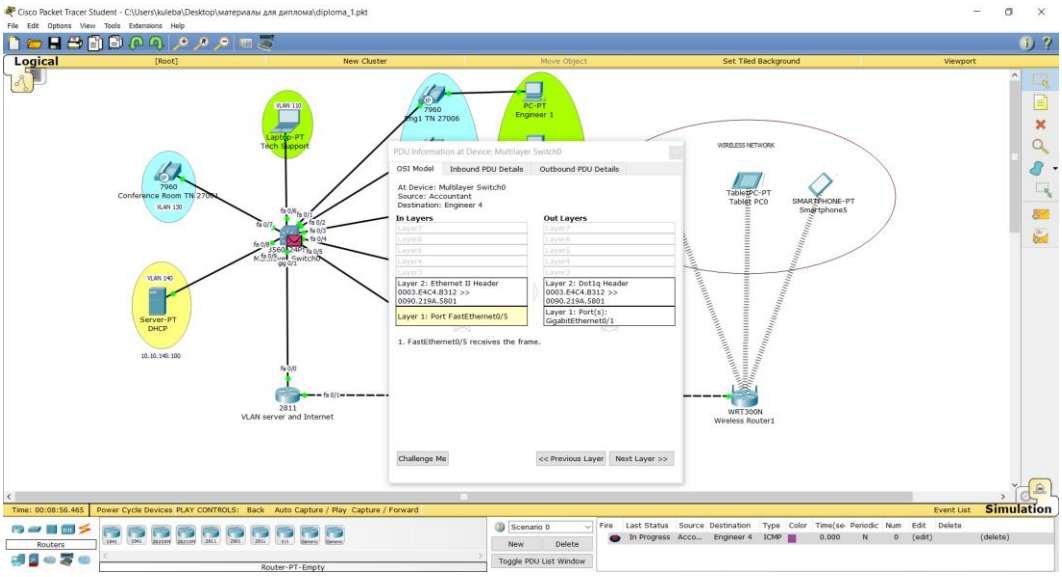

Рисунок 3.49 – Структура пакету, що перехоплений між різними VLAN на комутаторі (вхід до транку)

Як бачимо, після виходу з віртуальної мережі 120 пакет включає Ethernet II заголовок на In Layer та Dot1q на Out Layer.

Далі пакет просувається на маршрутизатор і на цьому етапі відбувається інкапсуляція (рис. 3.50), пакет має 2 заголовка Dot1q на In Layer та на Out Layer на другому рівні.

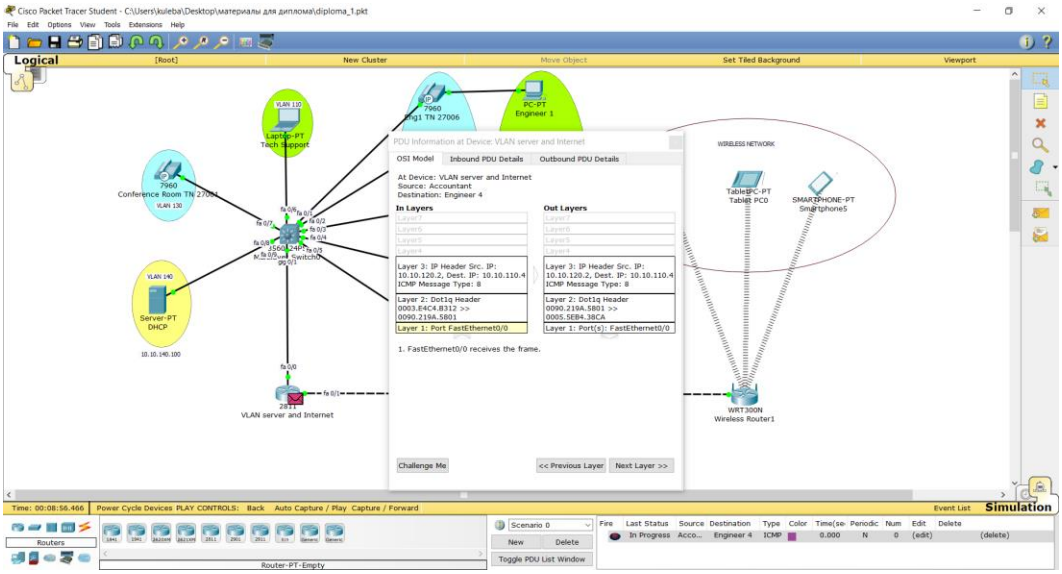

Рисунок 3.50 – Інкапсуляція пакету на маршрутизаторі

Після цього пакет повертається на комутатор і обробляється для входу в віртуальну мережу 110 на інтерфейсі fa 0/4. Бачимо, що заголовки міняються місцями порівняно з позицією входу до транку: Ethernet II заголовок на Out Layer та Dot1q на In Layer (рис. 3.51).

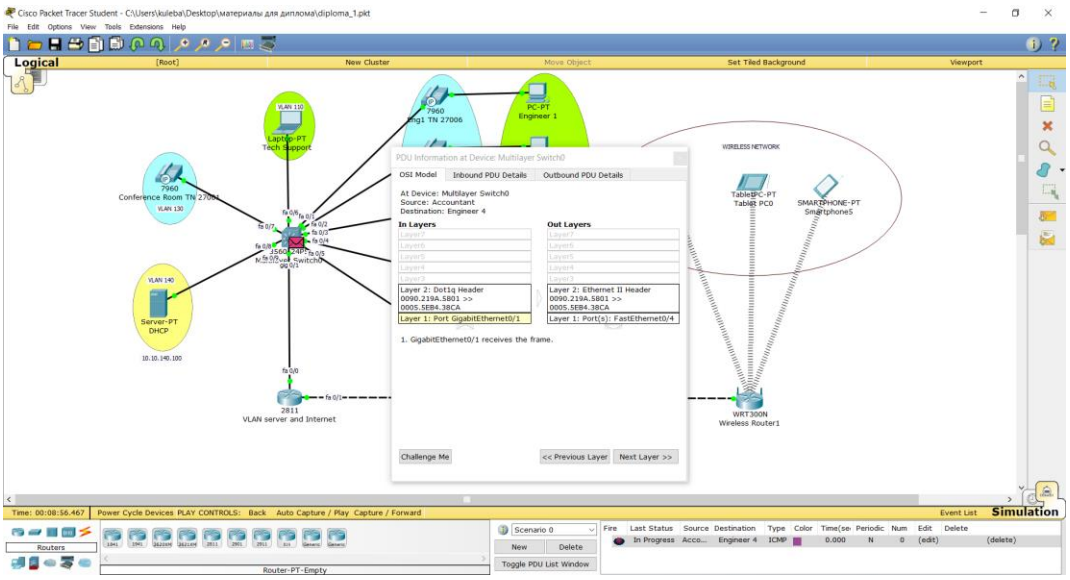

Рисунок 3.51 – Обробка пакету для входу в іншу мережу VLAN

Отже, мережа функціонує правильно, комутатор L3 обробляє й пересилає пакети в межах однієї мережі VLAN, а при переході з однієї VLAN до іншої пакети через транковий канал потрапляють на маршрутизатор для інкапсуляції.

ВИСНОВКИ

Висновки до наукової роботи можна сформулювати наступним чином:

Було з’ясовано, що віртуальні локальні мережі є логічним засобом розбиття одного широкомовного домену на кілька ізольованих доменів з угрупуванням віртуальних мереж незалежно від географічного розташування та портів підключення. VLAN є надійним й водночас бюджетним рішенням для забезпечення безпеки мережі, регулювання широкомовного трафіку, покращення пропускної здібності, покращення продуктивності мережі, розподілу ресурсів, та керування мережею. Типи VLAN можуть розрізнятися за класами трафіку, гнучкістю, особливостями кадрів, функціями, і т.д. Трафік між віртуальними мережами забезпечуються функцією транкінга. Маршрутизація між VLAN може реалізуватися апаратними методами (застарілі), або логічними.

Необхідність проектувати, моделювати й тестувати мережі перед їх фізичною реалізацією спричинила до розробки мережевих симуляторів, найпопулярнішим серед яких є Cisco Packet Tracer. Це безкоштовная програма з режимом симуляції та анімації, з можливістю накладувати логічні мережі на фізичні моделі і проектувати реальні мережі, беручі до уваги фізичні й географічні обмеження. Операційна система Cisco IOS є гнучкою й водночас потужною. Вона реалізується на вузлах мережі, забезпечуючи безпеку, IP-адресацію, маршрутизацію, QoS, та підтримку технологій керування мережею, здебільшого через консоль команд.

З використанням набутих теоретичних знань та практичних навичок були змодельовані, розгорнуті й протестовані мережі SOHO з різними типами VLAN. Опис команд і послідовність операцій у третьому розділі та додатку може стати практичним посібником для використання VLAN в малих та побутових мережах для користувачів, що будуть виступати в ролі системних адміністраторів, а також базою для лабораторних робіт для навчання студентів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гергель А.В. Компьютерные сети и сетевые технологии. Учеб. метод. пособие. — Н. Новгород: Изд-во ННГУ, 2007 – 107 с.

2. Компьютерные сети. Принципы, технологии, протоколы: Учебник для 2-е изд. / В.Г. Олифер, Н.А. Олифер. — СПб.: Питер, 2004. — 864 с.

3. П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. «Телекомунікаційні та інформаційні мережі». – Київ: САММІТ-Книга, 2010 – 708 с.

4. Design a VLAN (Virtual Local Area Network) Based Network [Електронний ресурс] - https://www.researchgate.net/publication/341979907_Design_a_VLAN_Virtual_Local_Area_Network_Based_Network

5. Introduction to VLAN [Електронний ресурс] - https://www.amgsystems.com/news-and-media/technical-bulletins/introduction-to-vlan

6. What is SOHO and which SOHO network is to choose? [Електронний ресурс] - https://haticexinterior.com/what-is-soho-and-which-soho-network-is-to-choose/

7. A Small Office/Home Office (SOHO) Network Topology [Електронний ресурс] - https://computernetworkingsimplified.wordpress.com/2013/06/07/how-will-a-typical-small-officehome-office-soho-lan-look-like/

8. SOHO network: Requirements, planning and implementation [Електронний ресурс] - https://www.examcollection.com/certification-training/network-plus-soho-network-requirements-planning-and-implementation.html

9. Understanding Home and SOHO Networks [Електронний ресурс] - http://etutorials.org/Networking/beginners+guide+to+wi-fi+wireless+networking/Part+I+Why+Wi-Fi/Chapter+4.+Networking+Without+Wires/Understanding+Home+and+SOHO+Networks/

10. https://www.fundera.com/ [Електронний ресурс]

11. Cisco Library, CiscoSystem // Cisco Easy Virtual Network [Електронний ресурс] - www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/easy-virtual-network-evn/aag_75118.p

12. Основы компьютерных сетей. Тема №6. Понятие VLAN, Trunk и протоколы VTP и DTP [Електронний ресурс] - https://habr.com/ru/post/319080/

13. Как работает Cisco Native VLAN [Електронний ресурс] - https://www.youtube.com/watch?v=3Xk8BQKnjVY

14. Настройка VLAN на оборудовании Cisco [Електронний ресурс] - https://www.youtube.com/watch?v=AWCagiMb5iw

15. VLAN для чайников [Електронний ресурс] - https://asp24.ru/novichkam/vlan-dlya-chaynikov/

16. VLAN [Електронний ресурс] - https://lanmarket.ua/entsiklopediya/telekommunikatsionnye-tekhnologii/vlan.html

17. Другие преимущества VLAN [Електронний ресурс] - http://citforum.ru/nets/autotracker/glava5.shtml

18. Виртуальные Локальные Сети: VLAN [Електронний ресурс] - http://network.xsp.ru/3_6.php

19. VLANS - IEEE 802.1Q TRUNK LINK PROTOCOL ANALYSIS [Електронний ресурс] - http://www.firewall.cx/networking-topics/vlan-networks/221-vlan-8021q-analysis.html

20. INTERVLAN ROUTING - ROUTING BETWEEN VLAN NETWORKS [Електронний ресурс] - http://www.firewall.cx/networking-topics/vlan-networks/222-intervlan-routing.html

21. VLAN INTERSWITCH LINK (ISL) PROTOCOL ANALYSIS [Електронний ресурс] - http://www.firewall.cx/networking-topics/vlan-networks/220-vlan-isl-analysis.html

22. VLANS - ACCESS & TRUNK LINKS [Електронний ресурс] - http://www.firewall.cx/networking-topics/vlan-networks/218-vlan-access-trunk-links.html

23. Основные команды по настройке и эксплуатации маршрутизаторов Cisco [Електронний ресурс] - https://www.opennet.ru/docs/RUS/cisco_basic/

24. Навигация по операционной системе IOS [Електронний ресурс] - http://ccna.mpei.ac.ru/IntroductionToNetworkTech/course/module2/2.1.3.1/2.1.3.1.html

25. Использование интерфейса командной строки Cisco IOS [Електронний ресурс] - https://www.cisco.com/c/ru_ru/td/docs/ios/fundamentals/configuration/guide/12_4/cf_12_4_book/cf_cli-basics.html

26. Режимы Cisco IOS [Електронний ресурс] - http://datanets.ru/rezhimy-cisco-ios.html

27. Структура операционной системы Cisco IOS [Електронний ресурс] - https://sites.google.com/site/kfgnb0101/home/Doc/cisco/struktura-operacionnoj-sistemy-cisco-ios

28. Коммутатор Cisco L2 (WS-C3560-24PS-S) [Електронний ресурс] - https://setevuha.ua/cisco-ws-c3560-24ps-s.html

29. Структура та компоненти CISCO IOS [Електронний ресурс] - https://studfile.net/preview/5208999/

30. Настольные Fast Ethernet коммутаторы Cisco Catalyst 2950 [Електронний ресурс] - http://telenetwork.narod.ru/Doc/Cisco/hardware/cat2950.html

31. Методичка Cisco Packet Tracer http://dvboyarkin.ru/wp-content/uploads/2015/05/1.Metodichka_Cisco_Packet_Tracer.pdf

32. ЛАБОРАТОРНАЯ РАБОТА № 1 «ЗНАКОМСТВО СО СРЕДОЙ МОДЕЛИРОВАНИЯ CISCO PACKET TRACER» Автор: С.Н. Мамойленко Новосибирск – 2016 [Електронний ресурс] - https://ita.sibsutis.ru/sites/csc.sibsutis.ru/files/courses/network/lab01.pdf

33. Команды Cisco: описание, возможности, инструкции по работе. [Електронний ресурс] - https://ruud.ru/it/46745-komandy-cisco-opisanie-vozmozhnosti-instrukciya-po-rabote/

34. Cisco Cheat Sheets [Електронний ресурс] - https://cheatography.com/tag/cisco/

35. VLAN в Cisco [Електронний ресурс] - https://linkas.ru/articles/vlan-v-cisco/

36. Конфигурация изолированных частных VLAN на коммутаторах [Електронний ресурс] - http://www.akvilona.ru/serv/cisco/a_vlan.htm

37. Как настроить VLAN'ы на коммутаторах Cisco Catalyst [Електронний ресурс] - https://community.cisco.com/t5/%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F-%D0%B8-%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%86%D0%B8%D1%8F/%D0%BA%D0%B0%D0%BA-%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B8%D1%82%D1%8C-vlan-%D1%8B-%D0%BD%D0%B0-%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%82%D0%BE%D1%80%D0%B0%D1%85-cisco-catalyst/ta-p/3145627

38. НАСТРОЙКА VLAN НА МАРШРУТИЗАТОРЕ CISCO [Електронний ресурс] - https://deltaconfig.ru/cisco-router-on-a-stick/

39. Intervlan routing. Design variations. [Електронний ресурс] - https://www.youtube.com/watch?v=Z4yn4BuDK3Q&feature=emb_logo

40. Настройка VLAN на Cisco [Електронний ресурс] - https://network.msk.ru/blog/nastroyka-vlan-cisco

41. Настройка маршрутизации InterVLAN и транкинга ISL/802.1Q на коммутаторах Catalyst 2900XL/3500XL/2940/2950/2970 с использованием внешнего маршрутизатора [Електронний ресурс] - https://www.cisco.com/c/ru_ru/support/docs/lan-switching/inter-vlan-routing/14976-50.html

ДОДАТОК

Додаток А

VLAN в мережі SOHO на двох комутаторах, з однією міжкомутаторною магістраллю.

Switch1:

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name marketing
Switch(config)# vlan 20
Switch(config-vlan)# name L2team
Switch(config)# vlan 30
Switch(config-vlan)# name L3team
Switch(config)# vlan 40
Switch(config-vlan)# name L4team
Switch(config)# vlan 100
Switch(config-vlan)# name accounts
Switch(config-vlan)# exit
```

Switch 2:

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name marketing
Switch(config)# vlan 20
Switch(config-vlan)# name L2team
Switch(config)# vlan 20
Switch(config-vlan)# name L2team
Switch(config)# vlan 30
Switch(config-vlan)# name L3team
Switch(config)# vlan 40
Switch(config-vlan)# name L4team
```

Switch1

```
Switch(config)# interface fa 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config)# interface fa 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config)# interface fa 0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config)# interface fa 0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 30
Switch(config)# interface fa 0/6
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 40
```

Switch 2

```
Switch(config)# interface fa 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 40
Switch(config)# interface fa 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 30
Switch(config)# interface fa 0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config)# interface fa 0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config)# interface fa 0/6
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
```

Switch1:

```
Switch(config)# interface fa 0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 20, 30, 40
Switch(config-if)#exit
Switch(config)#exit
Switch#show run
```

Switch2

```
Switch(config)# interface fa 0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 20, 30, 40
Switch(config-if)#exit
Switch(config)#exit
Switch#show run
```

VLAN у мережі SOHO на одному комутаторі й маршрутизаторі

Switch

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config)# vlan 20
Switch(config)# vlan 30
Switch(config-vlan)# exit
Switch(config)# interface fa 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config)# interface fa 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config)# interface fa 0/3
Switch(config-if)# switchport mode access
```

```
Switch(config-if)# switchport access vlan 30
Switch(config)# interface fa 0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 30
Switch(config)# interface fa 0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config)# interface fa 0/6
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)#exit
Switch(config)#exit
Switch#show run
Switch>en
Switch(config)# interface fa 0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)#exit
Switch(config)#exit
Switch#show run
```

Router

```
Router> enable
Router# configure terminal
Router(config)#interface fa 0/0
Router(config-if)#no shutdown
Router(config)#interface fa0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 110.110.10.110 255.255.255.0
Router(config-subif)#exit
Router(config-if)# exit
Router(config)#interface fa0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 120.120.20.120 255.255.255.0
```

```
Router(config-subif)#exit
Router(config-if)# exit
Router(config)#interface fa0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 130.130.30.130 255.255.255.0
Router(config-subif)#exit
Router(config-if)# exit
Router(config)#ip dhcp excluded-address 110.110.10.110
Router(config)#ip dhcp excluded-address 120.120.20.120
Router(config)#ip dhcp excluded-address 130.130.30.130
Router(config)#ip dhcp pool lan-10
Router(dhcp-config)#network 110.110.10.0 255.255.255.0
Router(dhcp-config)#default-router 110.110.10.110
Router(dhcp-config)#exit
Router(config)#ip dhcp pool lan-20
Router(dhcp-config)#network 120.120.20.0 255.255.255.0
Router(dhcp-config)#default-router 120.120.20.120
Router(dhcp-config)#exit
Router(config)#ip dhcp pool lan-20
Router(dhcp-config)#network 130.130.30.0 255.255.255.0
Router(dhcp-config)#default-router 130.130.30.130
Router(dhcp-config)#exit
Router(config)#exit
Router#show run:
Router#write memory
Router#show ip dhcp binding
```

Мережа SOHO з віртуальними мережами на комутаторі третього рівня та маршрутизаторі з IP-телефонією.

Router

```
Router> enable
Router# configure terminal
Router(config)#interface fa 0/0
Router(config-if)#no shutdown
```

```
Router(config)#interface fa0/0.110
Router(config-subif)#encapsulation dot1q 110
Router(config-subif)#ip address 10.10.110.1 255.255.255.0
Router(config-subif)# ip helper-address 10.10.140.100
Router(config)#interface fa0/0.120
Router(config-subif)#encapsulation dot1q 120
Router(config-subif)#ip address 10.10.120.1 255.255.255.0
Router(config-subif)# ip helper-address 10.10.140.100
Router(config)#interface fa0/0.130
Router(config-subif)#encapsulation dot1q 130
Router(config-subif)#ip address 10.10.130.1 255.255.255.0
Router(config-subif)# ip helper-address 10.10.130.100
Router(config)#interface fa0/0.140
Router(config-subif)#encapsulation dot1q 140
Router(config-subif)#ip address 10.10.140.1 255.255.255.0
Router(config-subif)#exit
Router(config)#exit
```

Switch

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 110
Switch(config)# name engdata
Switch(config)# vlan 120
Switch(config)# name accdata
Switch(config)# vlan 130
Switch(config)# name voice
Switch(config)# vlan 140
Switch(config)# name dhcpserver
Switch(config-vlan)# exit
Switch(config)# exit
Switch(config)# interface fa 0/1-4
```

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 110
Switch(config)# interface fa 0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 120
Switch(config)# interface fa 0/8
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 140
Switch# sh vlan brief
Switch(config)# interface gig 0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch# sh run
Switch> enable
Switch# configure terminal
Switch(config)#int fa 0/1
Switch(config-if)#switchport access vlan 110
Switch(config-if)#switchport voice vlan 130
Switch(config)#int fa 0/2
Switch(config-if)#switchport access vlan 110
Switch(config-if)#switchport voice vlan 130
Switch(config)#int fa 0/3
Switch(config-if)#switchport access vlan 110
Switch(config-if)#switchport voice vlan 130
Switch(config)#int fa 0/4
Switch(config-if)#switchport access vlan 110
Switch(config-if)#switchport voice vlan 130
Switch(config)#int fa 0/5
Switch(config-if)#switchport access vlan 120
Switch(config-if)#switchport voice vlan 130
Switch(config)#int fa 0/6
Switch(config-if)#switchport access vlan 110
Switch(config)#int fa 0/7
Switch(config-if)#switchport voice vlan 130
Switch(config)#int fa 0/8
```

Router

```
Router(config)#telephony-service
Router(config-telephony)#max-dn 144
Router(config-telephony)#max-ephones 20
Router(config-telephony)#ip source-address 10.10.130.1 port 2000
Router(config-telephony)#auto assign 1 to 144
Router(config-telephony)#exit
Router(config-telephony)#exit
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 27001
Router(config-ephone-dn)#ephone-dn 2
Router(config-ephone-dn)#number 27002
Router(config-ephone-dn)#ephone-dn 3
Router(config-ephone-dn)#number 27003
Router(config-ephone-dn)#ephone-dn 4
Router(config-ephone-dn)#number 27004
Router(config-ephone-dn)#ephone-dn 5
Router(config-ephone-dn)#number 27005
Router(config-ephone-dn)# exit
Router(config)# exit
Router# exit
Router> enable
Router# configure terminal
Router(config)#interface fa 0/1
Router(config-if)#no shutdown
Router(config-subif)#ip address 190.190.1.1 255.255.255.0
Router(config-subif)#exit
Router(config-if)# exit
```