МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему:

«Технологія VLAN як механізм для організації керованості та безпеки у локальних мережах»

Завідувач

випускаючої кафедри **Довбиш А.С.**

Керівник роботи **Великодний Д.В.**

Студентки групи ІК.мз – 92с **Ротаренко С.Ю.**

СУМИ 2021

Сумський державний університет

(назва вузу)

Факультет *ЕлІТ* Кафедра *Комп'ютерних наук*

Спеціальність *«Інформаційно-комунікаційні технології»*

Затверджую:

зав.кафедрою _____

_____

"_____" _____ 20___р.

ЗАВДАННЯ

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТОВІ

Ротаренко Світлані Юріївні

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) *Технологія VLAN як механізм для організації керованості та безбеки у локальних мережах*

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) Аналіз віртуальних локальних мереж. 3) Інформаційне та програмне забезпечення налаштування технології VLAN

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
1	*Огляд існуючих рішень. Постановка задачі*		
2	*Аналіз віртуальних локальних мереж*		
3	Інформаційне та програмне забезпечення налаштування технології VLAN		
4	Оформлення пояснювальної записки		

Студент – дипломник _____

Керівник проекту _____

РЕФЕРАТ

Записка: 52 сторінки, 25 рисунків, 20 джерел.

Мета роботи – дослідження теоретичних основ, методів і засобів побудови віртуальних локальних мереж.

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

Предметом дослідження є внутрімережевий трафік VLAN, маршрутизація трафіку між VLAN.

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

Результати – змодельована та протестована мережа у програмному симуляторі Cisco Packet Tracer з використанням команд консолі CLI.

VIRTUAL LOCAL AREA NETWORK, ETHERTNET, ПРОГРАМНИЙ СИМУЛЯТОР CISCO PACKET TRACER, SPANNING TREE PROTOCOL, OSI.

ЗМІСТ

ВСТУП

Віртуальні мережі (VLAN) в даний час входять в число найважливіших стратегічних напрямків майже всіх найбільших виробників мережевого устаткування.

Складно назвати точний час появи концепції "віртуальних мереж" в тому вигляді, в якому вона існує на сьогоднішній день, але можна сказати, що це сталося, коли інтелектуальність вироблених комутаторів почала зростати.

Традиційна мережа з роздільним середовищем передачі не могла надати велику смугу пропускання, яка була необхідна потужності процесорів робочих станцій, що постійно збільшувалася і появі мультимедійних додатків та додатків клієнт-сервер. Саме ці передумови спонукали проектувальників до створення різних технологій для захисту та поділу інформації всередині мережі. Однією з таких технологій і є віртуальна локальна мережа - VLAN.

VLAN (англ. Virtual Local Area Network – віртуальна локальна комп'ютерна мережа) - є групою клієнтів (пристроїв) з певним набором необхідних параметрів мережі, що взаємодіють так, ніби вони прикріплені до одного домену, незалежно від їх фізичного розташування.

До переваг віртуальної локальної мережі в порівнянні з іншими LAN можна віднести:

- гнучкий поділ пристроїв на групи: одному VLAN відповідає одна підмережа. Комп'ютери, що розташовуються в різних VLAN, ізольовані один від одного;

- скорочення широкомовного трафіку в мережі: кожен VLAN визначає окремий широкомовний домен. Широкомовний трафік не буде транслюватися між різними VLAN;

- скорочення числа обладнання та мережевого кабелю: немає необхідності купувати і встановлювати комутатор і прокладку мережевого кабелю.

Наукова робота присвячена аналізу віртуальних локальних мереж та дослідженню безпеки при їх організації.

1 ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

1.1 Принцип побудови сучасних локальних мереж. Базова концепція комутації в локальних мережах.

З моменту створення перших локальних мереж, була розроблена велика кількість самих різних мережевих технологій, але, незважаючи на це, велике поширення змогли отримати лише деякі з них. Це, в першу чергу, пов'язано з високим рівнем стандартизації принципів організації мереж і з підтримкою їх відомими компаніями. Але при всьому цьому, стандартні мережі не завжди володіють найкращими характеристиками і можуть забезпечити найбільш сприятливі режими обміну. Але основними і великими перевагами технологій є великі обсяги випуску їх апаратури і її невисока вартість. Важливим фактором також є те, що розробники програмних засобів, перш за все, звертають увагу на найпоширеніші мережі. Внаслідок цього, користувач, який вибирає стандартні мережі, володіє повною гарантією взаємосумісності апаратури і програм. В даний момент поступове зменшення кількості типів, які використовують мережі, стає тенденцією. Причина криється в тому, що для збільшення швидкості передачі в локальних мережах до 100 і навіть до 1000 Мбіт/с також потрібне застосування самих новітніх технологій та здійснення досить дорогих наукових досліджень. Зрозуміло, це можуть дозволити собі тільки найбільші фірми, що підтримують свої стандартні мережі і їх більш досконалі різновиди.

Найбільш поширеною серед стандартних мереж стала мережа під назвою Ethernet. Першим варіантом технології Ethernet була фізична шинна топологія, в основі якої лежав коаксіальний кабель. Наступним не менше поширеним варіантом технології став стандарт 10BASET, який завдяки тому, що проблеми, що виникли в одному кабелі, не впливали на всю решту мережу (що є характерною ситуацією для мереж 10BASE2 і 10BASE5 з топологією розділяється шини) був набагато надійніше. В технології 10BASET була використана неекранована кручена пара, яка була набагато дешевше, ніж коаксіальний кабель [1]. Більш того, завдяки тому, що багато організацій

використовували виту пару для телефонії, стандарт 10BASET в короткі терміни став розумною альтернативою Ethernet мереж стандартів 10BASE2 і 10BASE5. Типові топології для мережі стандарту 10BASE2 і мережі 10BASET з використанням концентратора показані на рисунку 1.1.

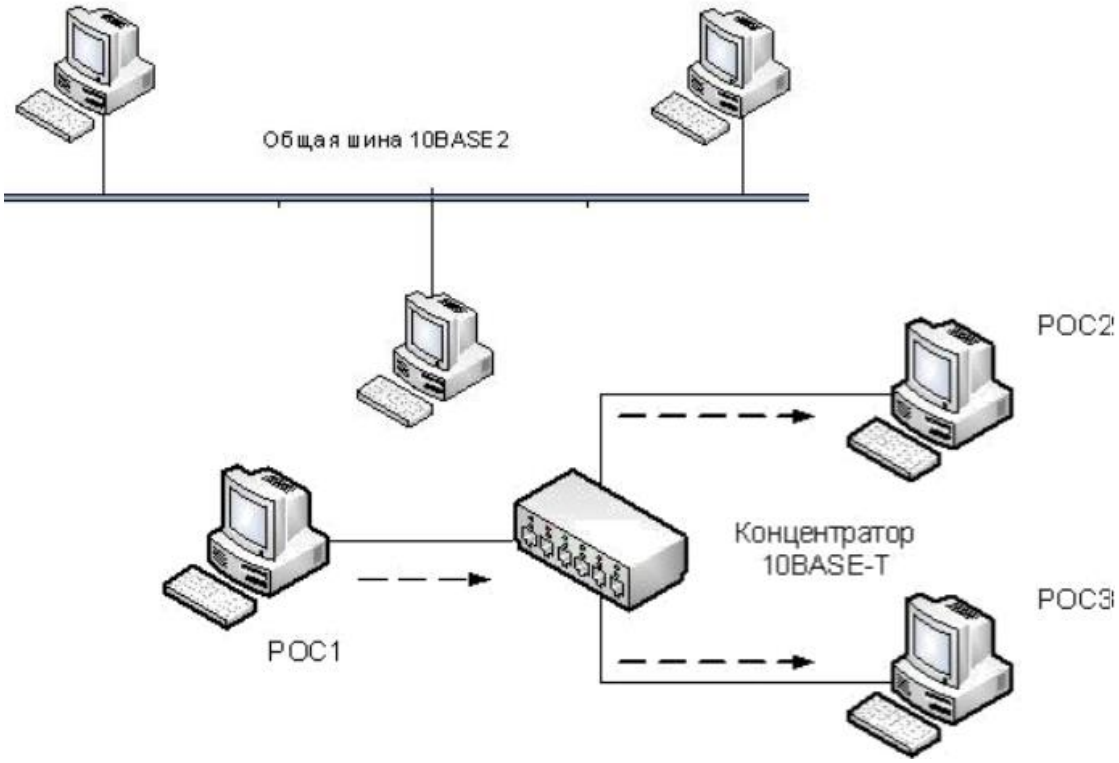

Рисунок 1.1 - Фізичні топології для мережі 10BASE2 і мережі 10BASE-T з використанням концентратора [1]

Проте, незважаючи на те, що технологія 10BASET була значним просуванням у еволюції мережевих технологій, вона все ж мала декілька значних недоліків, які пов'язані із застосуванням концентраторів:

- фрейм, який передається будь-яким наявним пристроєм, може стати причиною колізії в мережі, за умови, якщо він "зіткнеться" з фреймом, переданим від іншого пристрою, який знаходиться в тому ж самому сегменті;

- тільки один пристрій з усіх наявних має можливість передавати кадр в один часовий проміжок, іншими словами пристрої в одному сегменті працюють в режимі конкуренції і розділяють загальну смугу пропускання (в 10 Мбіт/с);

- широкомовні фрейми, які відправляються одним пристроєм, будуть отримані і оброблені усіма пристроями, які знаходяться в даній локальній мережі [2].

У той час, коли три стандарти Ethernet, які були описані вище, були розроблені, смуга пропускання в 10 Мбіт, яку вони поділяли, здавалася гігантською величиною! До появи локальної мережі (LAN), для роботи дуже часто застосовувалися простіші термінали, які підключалися до центрального серверу в мережі за допомогою каналу в 56 Кбіт/с. Після розробки технології 10BASET Ethernet, її швидкість виявилася дивовижною для того часу.

Через деякий час, продуктивність Ethernet мереж стала поступово знижуватися. Розробники програмного забезпечення почали створювати додатки, які використовували досить таки велику смугу пропускання в локальній мережі. У локальних мережах стали з'являтися такі проблеми, як затори трафіку, так як пристрої в одному і тому ж сегменті Ethernet були нездатні передавати більше ніж 10 Мбіт / с потоків даних, крім цього вони ще й поділяли цю смугу пропускання між собою. В результаті збільшення обсягів трафіку стало виникати велика кількість колізій в локальних мережах.

1.2 Методи комутації. Переваги і недоліки механізмів комутації в мережах LAN

При прийнятті рішення про передачу фрейму, комутатор може скористатися одним з механізмів передачі, які будуть розглянуті далі. Велика частина пристроїв на даний момент застосовує метод комутації з буферизацією фреймів (англ. Store and forward), але, незважаючи на це, всі розглянуті далі методи внутрішньої обробки потоків даних реалізовані і застосовуються в різних пристроях.

Велика частина прозорих мостів і комутаторів в даний час використовує метод комутації з буферизацією фреймів (англ. Store and forwar dprocessing). В даному методі, перш ніж почати передачу першого біта фрейму через вихідний

інтерфейс, пристрій повинен отримати фрейм повністю. Відомі ще два методу внутрішньої обробки фреймів: наскрізна комутація (англ. Cutthrough) і бесфрагментная комутація (англ. Fragment free). Завдяки тому, що MAC адресу одержувача розташовується на початку Ethernet заголовка, комутатор може почати пересилання ще до того, як він отримає весь фрейм. Наскрізна і бесфрагментная комутації працюють за таким принципом, тобто передача починається задовго до того, як буде отримано весь фрейм, з цього випливає, що час обробки та передачі (тобто затримка, delay) значно зменшується [2].

Метод наскрізної комутації (англ. Cutthrough) полягає в тому, що пристрій починає пересилання фрейму відразу ж після прийняття тієї частини заголовку, яка містить адресу призначення. Особливістю даного методу комутації є те, що він значно знижує затримку в мережі, але має недолік у вигляді поширення помилок в мережі. В результаті того, що контрольна сума фрейма (англ. Frame check sequence FCS) розташовується в Ethernet кінцевик, перед початком пересилання, комутатор не має можливості визначити, чи є які-небудь помилки у фреймі. При використанні даного методу комутації, важливо враховувати дві основні особливості: затримка за рахунок обробки фреймів пристроєм помітно знижується, але результатом цього є подальша передача фрейму з наявними помилками.

Метод бесфрагментной комутації (англ. Fragment freep rocessing) працює за тим же принципом, що і метод наскрізної комутації, але відрізняється значно меншим числом помилок, що передаються через пристрій. Відмінною особливістю технології CSMA/CD (англ. Carrier Sense Multiple Access With Collision Detection - множинний доступ з контролем несучої і виявленням колізій) є те, що велика кількість колізій існують на перших 64 бітах фрейма. Подібність бесфрагментной комутації і наскрізний комутації полягає в тому, що в бесфрагментной комутації передача починається тільки після отримання 64 байтів передається фрейма. Затримка через обробку фрейма комутатором в такому випадку значно зменшується, в порівнянні з методом комутації з

буферизацією, але при цьому буде перевищувати час затримки наскрізного методу. Кількість помилок, яке надсилається пристроєм, також буде значно менше, ніж в методі комутації з буферизацією.

В даний час велика частина робочих станцій підключені до мережі за допомогою з'єднань зі швидкістю 100 Мбіт/с, вищі канали зазвичай працюють на швидкості 1 Гбіт/с, в комутаторах застосовуються спеціалізовані мікросхеми (англ. Application Specific Integrated Circuits, ASIC), які працюють на дуже високій швидкості і призначені для апаратної обробки потоків даних. Отже, в нинішніх комутаторах здебільшого застосовується метод комутації з буферизацією фреймів, так як на таких швидкостях передачі даних помітного зменшення затримки не відбувається.

Внутрішні механізми обробки фреймів в комутаторах значно відрізняються в залежності від виробників, але, незважаючи на це, всі методи можна звести до трьох основних або до деяких їх похідних, які були описані вище.

У комутаторах також є велика кількість додаткових функцій, які відсутні в застарілих пристроях для локальних мереж (LAN), наприклад, концентратори і мости. Основні переваги комутаторів перераховані далі.

У випадках, коли до порту комутатора підключається всього одне мережеве пристрій, він виконує мікросегментацію мережі і надає виділену смугу пропускання для пристрою.

Комутатори дають можливість здійснити пересилку множинних одночасних потоків даних між пристроями, які підключені до різних інтерфейсів.

У випадках, коли до порту комутатора підключається тільки одне мережеве пристрій, який працює в дуплексному режимі, ефективна смуга пропускання збільшується вдвічі.

Комутатори мають можливість виконувати узгодження швидкості, що означає, що пристрої, які підключені через різні за швидкістю технології Ethernet, здатні взаємодіяти через комутатор, але не через концентратор.

1.3 Широкомовний домен і домен колізій

Два значущих принципу сегментації локальних комп'ютерних мереж можуть бути описані двома термінами: домен колізій (англ. Collision domain) і широкомовний домен (англ. Broadcast domain).

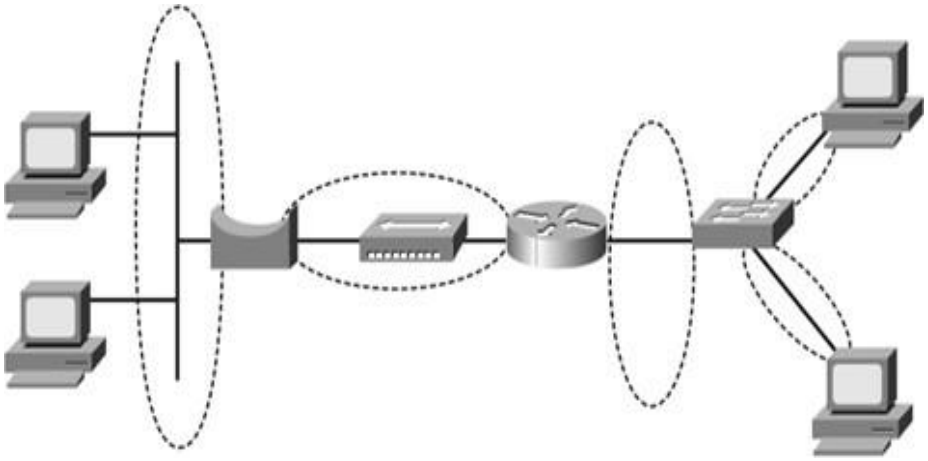

Рисунок 1.2 - Домени колізій [1]

Домени колізій.

Домен колізій є набором інтерфейсів локальної мережі, фрейми даних інтерфейсів мають можливість вступати в колізії між собою, але це не відноситься до фреймів від інших пристроїв в мережі. На рисунку 1.2 можна побачити ілюстрацію доменів колізій.

Комутатор, який зображений на правій стороні схеми, поділяє локальну мережу на окремі домени колізій на кожному порту. Відповідно, маршрутизатор і міст поділяють мережу на окремі домени колізій. З усіх присутніх на схемі пристроїв тільки концентратор, який зображений в центрі схеми мережі, не створює безліч роздільних доменів колізій для кожного інтерфейсу. Це пристрій виконує функцію повторення фреймів на всіх своїх портах без буферизації і затримки фрейму перед передачею в завантажений сегмент мережі.

Широкомовний домен.

Термін широкомовний домен (англ. Broadcast domain) застосовується для опису певної ділянки мережі, на якому можуть поширюватися широкомовні фрейми. Широкомовний домен складається з набору пристроїв, який забезпечує

отримання та обробку широкомовного повідомлення усіма пристроями у випадках, коли один пристрій передає дане широковещательное повідомлення. Зокрема, в результаті того, що комутатори передають все широкомовні і многоадресатние повідомлення через всі свої порти, комутатор створює єдиний широкомовний домен. В якості бар'єру між широкомовними фреймами виступають маршрутизатори, їх функцією є не пропускати фрейми через себе. На рисунку 1.3 проілюстровані кордону широкомовних доменів для схеми мережі, показаної на рисунку 1.2.

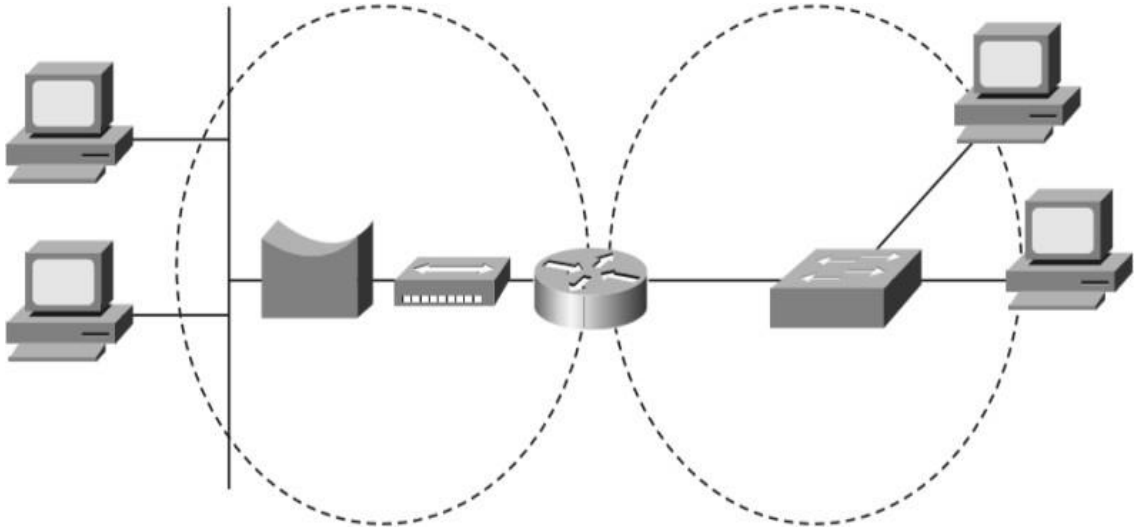

Рисунок 1.3 - Широкомовні домени [1]

Широкомовне повідомлення, яке було відправлено одним пристроєм в широкомовному домені, не передається пристроям в іншому широкомовному домені. У прикладі, показаному на рисунку 1.3, є два широкомовних домену, тобто маршрутизатор не передаватиме широкомовні фрейми, відправлені комп'ютером, який зображений на схемі зліва, в мережевий сегмент, який проілюстрований на схемі справа.

1.4 Використання технології VLAN для ефективної організації роботи підприємств

Спочатку комутатори не мали можливості забезпечувати створення віртуальних локальних мереж, оскільки вони застосовувалися для

безпосередньої пересилання фреймів між пристроями. В результаті того, що концентратори колективного доступу до середовища передачі даних були не в змозі справлятися з збільшуються запитами на розширення пропускної здатності мережі в зв'язку з застосуванням додаток клієнт-сервер, які забезпечували графічний інтерфейс користувачів (GUI), ринок комутаторів швидко розширювався.

Комутатор працює з кадрами "інтелектуально", тобто він зчитує MAC адресу надходить, або входить, кадру і зберігає отриману інформацію в таблиці комутації. Таблиця комутації містить MAC адреси мережі і номера портів, які пов'язані з ними. Після створення такої таблиці, комутатори перевіряють кожен кадр, який був занесений в пам'ять, і записують нові адреси, які відсутні в таблиці. Як приклад на рисунку 1.4 показана таблиця комутації комутатора [5].

```
Cat5500> show cam dynamic
VLAN        Destination MAC          Destination Ports or VCs
----------  -----------------------  ------------------------
1           00-60-2f-9d-a9-00        3/1
1           00-b0-2f-9d-b1-00        3/5
1           00-60-2f-86-ad-00        5/12
1           00-c0-0c-0a-bd-4b        4/10
Cat5500>
```

Рисунок 1.4 - Таблиця комутації [5]

У міру того, як технології поліпшувалися і захоплювали ринок, стали з'являтися віртуальні локальні мережі - VLAN.

В даний час в число найважливіших стратегічних напрямків майже всіх найбільших виробників мережевого устаткування входять віртуальні мережі (VLAN). Вказати точний час появи концепції "віртуальних мереж" в тому вигляді, в якому вона існує зараз складно, але можна сказати, що це сталося, коли інтелектуальність вироблених комутаторів почала зростати буквально з кожним дня.

VLAN (від англ. Virtual Local Area Network) - топологічна, або віртуальна, локальна мережа. VLAN - це логічне комбінування деякого числа кінцевих станцій в одному сегменті (широкомовному домені) на канальному рівні, навіть якщо вони фізично підключені до різних комутаторів. VLAN дозволяє повністю ізолювати трафік групи вузлів від решти мережі [2].

Технологія віртуальних локальних мереж є дуже затребуваною, завдяки ряду переваг:

1) VLAN допомагає структурувати мережу - можливість виділення в окрему мережу відділу організації або групи комп'ютерів (наприклад, сегмента серверів, звичайних користувачів, ip-телефонів, ip-відеокамер і т.д), використовуючи загальний комутатор (рис.1.5);

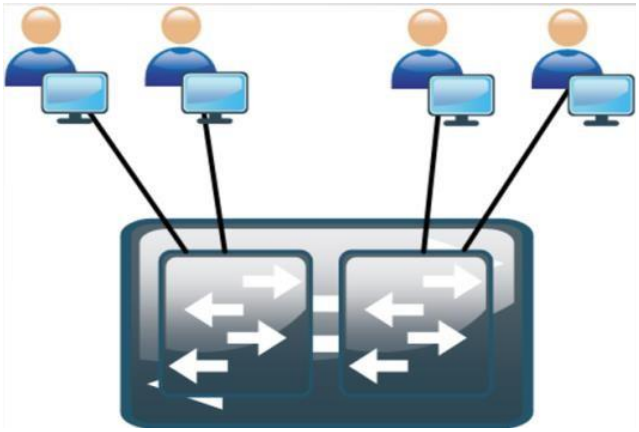

Рисунок 1.5 - Структурування мережі за допомогою загального комутатора при організації VLAN

2) VLAN використовується для забезпечення безпеки - наприклад, при поділі мережі гостьових користувачів і мережі серверів, зловмисники не будуть мати доступ в інший сегмент мережі, так як користувачі різних сегментів можуть взаємодіяти тільки на мережевому рівні, тобто за допомогою маршрутизатора;

3) VLAN використовується для об'єднання користувачів на канальному рівні, навіть при підключенні до різних фізичних комутаторів. Завдяки даній технології, немає необхідності в протягуванні кабелю від користувача до потрібного світча, досить, link-а між комутаторами (рис.1.6).

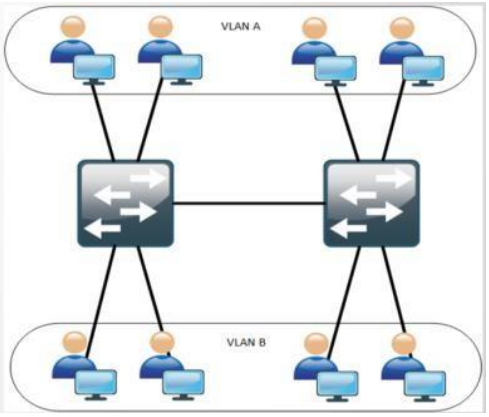

Рисунок 1.6 - Об'єднання користувачів на канальному рівні при організації VLAN

4) VLAN зменшує кількість широкомовного трафіка. Кожен VLAN - це окремий широкомовний домен, всередині якого передаються широкомовні кадри. Створення додаткових VLAN-ів на комутаторі означає розбиття комутатора на кілька широкомовних доменів, завдяки чому, при генеруванні широковещательного запиту користувачем, даний запит отримають тільки користувачі даного широковещательного домену.

У комутаторах можуть використовуватися три типи VLAN:

- VLAN на базі портів;
- VLAN на базі MAC-адрес;
- VLAN на основі міток в додатковому полі кадру - стандарт IEEE 802.1Q.

Організація VLAN на базі портів і MAC адрес, є застарілою і не рекомендується для застосування в сучасних реалізаціях віртуальних мереж.

Стандарт IEEE 802.1Q визначає зміни в структурі кадру Ethernet, що дозволяють передавати інформацію про VLAN по мережі. З точки зору зручності і гнучкості налаштувань, VLAN на основі міток є найкращим рішенням. Його основні переваги - це гнучкість і зручність в налаштуванні і зміні - додавання міток дозволяє VLAN поширюватися через безліч 802.1Q-сумісних комутаторів по одній фізичній з'єднанню. VLAN 802.1Q дозволяє VLAN працювати з комутаторами і мережевимиадаптерами серверів і робочих станцій, що не

розпізнають мітки. В силу зазначених властивостей, VLAN на базі тегів використовуються на практиці набагато частіше за інших типів.

З використанням VLAN, один комутатор має можливість створити два широкомовних домену. Комутатор VLAN також здатний налаштувати частина інтерфейсів на один широкомовний домен, а частина на інший, в результаті чого, буде створено два широкомовних домени. Дані індивідуальні широкомовні домени, які були створені комутатором, і є віртуальними локальними мережами (англ. Virtual LAN - VLAN).

1.5 Постановка задачі

Як вже було сказано раніше, VLAN (англ. Virtual Local Area Network, Віртуальна Локальна Мережа) - це група пристроїв, яка взаємодіє безпосередньо на канальному рівні, незважаючи на те, що на фізичному рівні всі ці пристрої підключені до різних комутаторів. До переваг віртуальної локальної мережі в порівнянні з іншими LAN можна віднести:

- гнучкий поділ пристроїв на групи: тобто, одному VLAN відповідає одна підмережа. Комп'ютери, які розташовуються в різних VLAN, будуть ізольовані один від одного.

- скорочення широкомовного трафіка в мережі: кожен VLAN визначає окремий широкомовний домен. Широкомовний трафік не буде транслюватися між різними VLAN.

- скорочення числа обладнання та мережевого кабелю: при створенні нової віртуальної локальної мережі немає необхідності купувати і встановлювати комутатор і прокладку мережевого кабелю.

Проаналізувавши існуючі рішення щодо віртуальних мереж VLAN, можно сформулювати мету наукової роботи наступним чином: провести аналіз роботи віртуальних локальних мереж та зробити висновки щодо безпеки при їх організаціїї. Для цього необхідно виконати наступні завдання:

- зробити загальний огляд побудови сучасних локальних мереж;

- розглянути основні причини і переваги створення віртуальних локальних мереж;

- проаналізувати основні функції та призначення VLAN;

- ознайомитися із типами та протоколами VLAN;

- розглянути приклади організації VLAN;

- змоделювати мережу VLAN в середовищі Cisco Packet Tracer та протестувати на предмет розподілу трафіку в даній мережі.

2 2 АНАЛІЗ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ

2.1 Функції і призначення VLAN

Основним призначенням технології VLAN є полегшення процесу ізолювання мереж, які згодом будуть пов'язані маршрутизаторами, що реалізують один з протоколів мережевого рівня, наприклад, IP. Даний вид організації мережі дозволяє забезпечувати досить потужні бар'єри на шляху помилкового трафіку, при його передачі з однієї мережі в іншу. На даний момент можна вважати, що кожна велика мережа повинна мати маршрутизатори, так як в противному випадку потоки помилкових кадрів, наприклад, широкомовних, можуть час від часу «затоплювати» всю мережу через комутатори, тим самим приводячи мережу в неробочий стан. Технологія віртуальних мереж дозволяє організувати основу для побудови великої мережі, яка пов'язана маршрутизаторами, так як комутатори дають можливість створювати повністю ізольовані сегменти програмним шляхом, тобто без використання фізичної комутації. До винаходу технології VLAN з метою створення окремої мережі застосовувалися сегменти коаксіального кабелю, які були фізично ізольовані один від одного або сегменти, який будувалися на повторителях і мостах і не були пов'язані один з одним. Після чого дані мережі з'єднувалися маршрутизаторами в єдину складову мережу.

Під зміною складу сегментів (наприклад, перехід користувача з однієї мережі в іншу або поділ більших сегментів) в даному випадку розуміється фізична перекомутація роз'ємів, які перебувають на передніх панелях повторювачів або в кросових панелях, а це в свою чергу не практично в великих мережах, так як має на увазі велику кількість фізичної роботи і досить високу ймовірність помилки. З цієї причини, щоб виключити фізичну перекомутацію роз'ємів, почали використовувати багатосегментні концентратори, це, в свою чергу, дозволило програмувати склад розділяється сегмента без фізичної перекоммутации. Тим не менше, використання концентраторів для зміни складу сегментів створює значні обмеження для структури мережі - число сегментів такого повторювача досить мало, через що неможливо надати кожному вузлу свій сегмент, як це відбувається при використанні комутатора. Крім цього, в даному випадку всім процесом передачі даних між сегментами керуватимуть маршрутизатори, а комутатори, маючи високу продуктивність, будуть "байдикувати". З цієї причини мережі, які побудовані за допомогою повторювачів з конфігураційної комутацією, все ще працюють на основі дроблення середовища передачі даних між великим числом вузлів і мають значно меншу продуктивність у порівнянні з мережами, які побудовані на основі комутаторів. Застосування технології віртуальних мереж в комутаторах дозволяє вирішити два завдання:

- підвищення продуктивності в кожній з віртуальних мереж, так як комутатор передає кадри в подібній мережі тільки вузлу призначення;

- ізоляція мереж друг від друга керувати правами доступу користувачів і створення захисних бар'єрів на шляху широкомовних штормів [4].

Для з'єднання віртуальних мереж в єдину загальну мережу необхідно використання мережевого рівня. Мережевий рівень може бути реалізований в окремому маршрутизаторі, а також має можливість працювати в складі програмного забезпечення комутатора, який в такому випадку є комбінованим пристроєм - так званим комутатором 3-го рівня. Технологія освіти і роботи

віртуальних мереж з використанням комутаторів достатню кількість часу була стандартизована, незважаючи на те, що була реалізована в дуже широкому спектрі моделей комутаторів різних виробників. Але ситуація змінилася після прийняття в 1998 році стандарту IEEE 802.1Q, який має можливість визначати основні правила побудови віртуальних локальних мереж, що не залежать від протоколу канального рівня, який підтримується комутатором. Через пізню появи стандарту на VLAN великі виробники комутаторів створили свої технології віртуальних мереж, які були несумісні з технологіями інших виробників. З цієї причини, незважаючи на появу стандарту, дуже часто можна спостерігати таку ситуацію, коли віртуальні мережі, які створені на комутаторах одного виробника, які не розпізнаються і не підтримуються комутаторами іншого виробника.

2.2 Створення VLAN на основі одного комутатора

Для створення віртуальних мереж на основі одного комутатора найчастіше застосовується спосіб групування в мережі портів комутатора, при якому кожен порт зараховується певної віртуальної мережі. Широкомовний кадр, що надійшов від порту, який відноситься, наприклад, до віртуальної мережі 1, ніколи не буде відправлений порту, який не перебуває у даній віртуальної мережі. Порт також можна віднести до кількох віртуальних мереж, але на практиці цей спосіб використовується рідко, так як зникає ефект повної ізоляції мереж.

Найбільш логічним і поширеним способом створення VLAN є групування портів для одного комутатора, так як віртуальних мереж, побудованих на основі одного комутатора, не може бути більше, ніж портів. У випадках, коли до одного порту приєднаний сегмент, який створений на основі повторювача, недоцільно підключати вузли даного сегмента до різним віртуальним мережам, так як в будь-якому випадку трафік цих вузлів залишиться загальним. Для утворення віртуальних мереж на основі групування портів досить зарахувати кожен порт до однієї з декількох уже названих віртуальних мереж, тобто від користувача не

потрібно великого обсягу ручної роботи. Найчастіше цей процес проводиться з використанням спеціальної програми, яка додається до комутатора. Адміністратор утворює віртуальні мережі за допомогою переміщення мишкою графічних символів портів на графічні символи мереж.

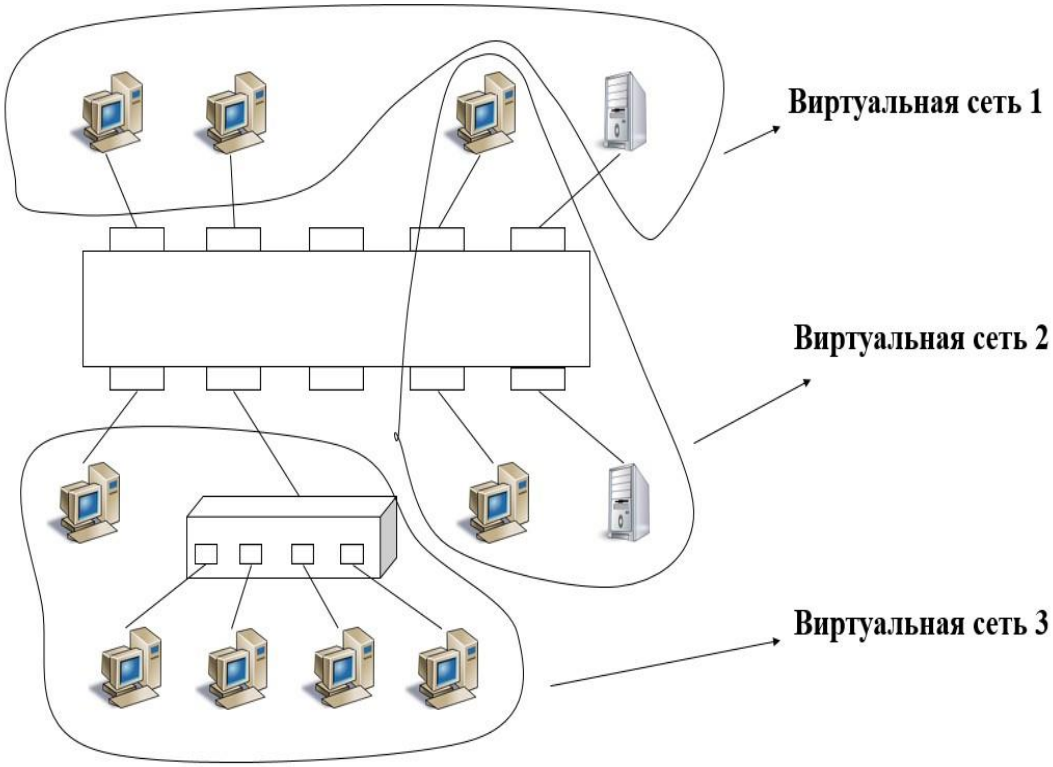

Рисунок 2.1 - Побудова VLAN на основі одного комутатора способом угруповання портів [2]

Наступним способом створення віртуальних мереж після угруповання портів є групування MAC-адрес. Кожен MAC-адреса, прийнятий комутатором, зараховується будь-якої віртуальної мережі. У випадках, коли в мережі існує велика кількість вузлів, даний спосіб вимагає виконання безлічі ручної роботи від адміністратора. Але при утворенні віртуальних мереж на основі декількох комутаторів даний спосіб є більш зручним, ніж спосіб групування портів.

2.2.1 Створення VLAN на основі декількох комутаторів

Створення мережі VLAN на основі одного комутатора не вимагає багато чого: досить налаштувати кожен порт таким чином, щоб задати йому номер

VLAN, в якій він знаходиться. У випадках, коли присутні більше одного комутатора необхідно брати до уваги і інші додаткові способи перенаправлення трафіку між ними.

При використанні мережі VLAN в мережах з деякою кількістю пов'язаних між собою комутаторів, на каналах зв'язку, які знаходяться між ними, використовується магістральний з'єднання VLAN (англ. VLAN trunking). Магістральний з'єднання VLAN передбачає застосування комутаторами процесу призначення тегів VLAN (англ. VLAN tagging), при якому перед початком передачі фрейму через магістральний канал комутатор доповнює даний фрейм іншим заголовком. Даний додатковий заголовок складається з поля ідентифікатора VLAN (англ. VLAN ID), який дає можливість передавальному комутатора зіставляти фрейм з певною мережею VLAN, а приймає комутатора визначити, до якої саме VLAN відноситься цей фрейм [5].

На рисунку 2.2 можна побачити приклад двох мереж VLAN з декількома комутаторами, однак, без використання магістрального з'єднання. В даному випадку застосовуються дві мережі VLAN: VLAN 10 і VLAN 20. Кожній з мереж VLAN належить по два порти на кожному комутаторі, отже, кожна мережа VLAN присутній в обох комутаторах. Для перенаправлення трафіку мережі VLAN 10 між двома комутаторами, до яких вона належить, дана схема передбачає присутність каналу зв'язку між ними, який в повному обсязі розташовується в мережі VLAN 10. Точно також, для забезпечення трафіку

мережі VLAN 20 між комутаторами знаходиться другий канал зв'язку, вже повністю знаходиться в мережі VLAN 20.

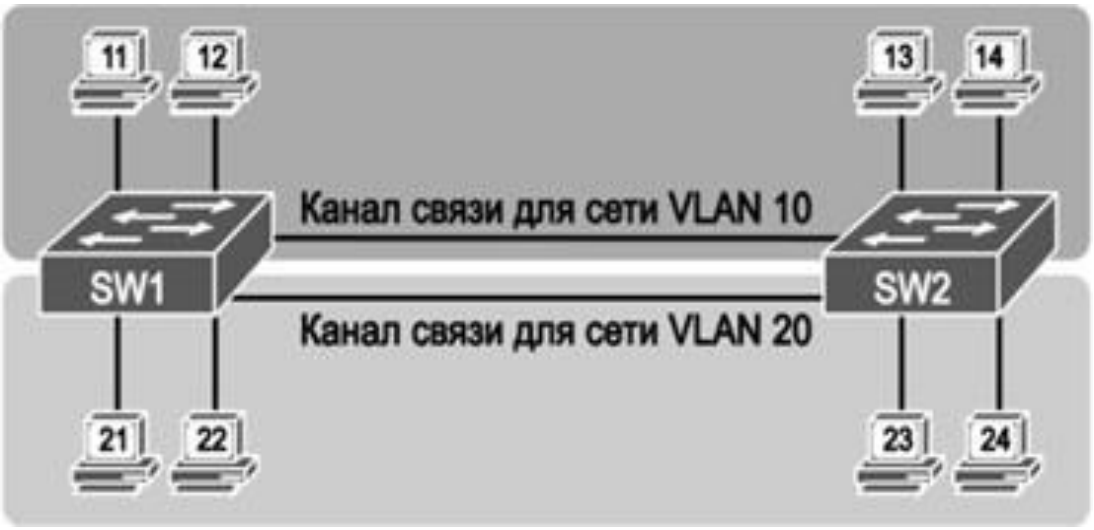

Рисунок 2.2 - Мережі VLAN при присутності декількох комутаторів, однак без магістрального з'єднання [2]

Комп'ютер ПК11 (що знаходиться в мережі VLAN 10) в повній мірі має можливість передати кадр комп'ютера ПК14. Фрейм попрямує на комутатор SW1, після чого через канал зв'язку (призначений для VLAN 10) попрямує на комутатор SW2. Однак, незважаючи на те, що дана схема працює, її масштабування є нелегким завданням. Для роботи кожної мережі VLAN необхідний окремий фізичний канал зв'язку між комутаторами. Наприклад, при необхідності наявності 10 або 20 мереж VLAN, необхідно розташувати між комутаторами 10 або 20 каналів зв'язку і застосувати для них 10 або 20 портів на кожному комутаторі.

2.2.2 Концепції призначення тегів

Магістральний з'єднання VLAN утворює між комутаторами один канал зв'язку, який може підтримувати таку кількість мереж VLAN, яка необхідна. Для комутаторів даний магістральний канал буде являтся частиною всіх VLAN. Але незважаючи на це, трафік в магістральному каналі VLAN буде роздільним, і фрейми VLAN 10 ніяк не зможуть потрапити на пристрої VLAN 20 (і навпаки), так як, проходячи через магістральний канал, кожен фрейм позначений номером

VLAN. На рисунку 2.3 можна побачити схему мережі з одним фізичним каналом зв'язку між двома комутаторами.

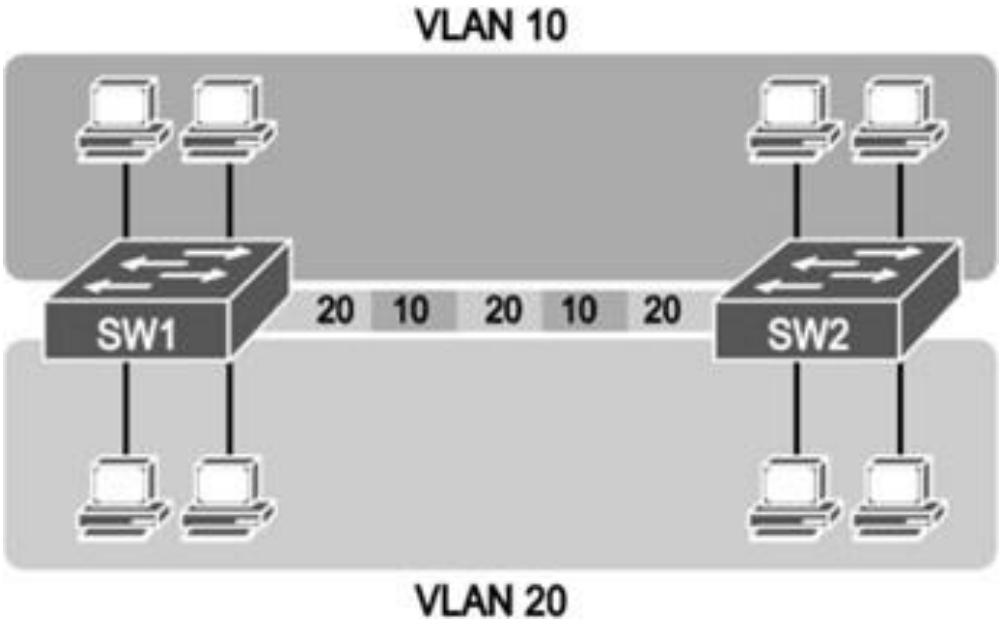

Рисунок 2.3 - Мережі VLAN з декількома комутаторами і магістральним з'єднанням [2]

Магістральний з'єднання дає можливість комутаторів переслати фрейми деякої кількості мереж VLAN по одному фізичному каналу завдяки доповнює фрейм Ethernet невеликим заголовком. Приклад, який можна побачити на рисунку 2.4 показує пересилання комп'ютером ПК11 широковещательного фрейму на інтерфейсі Fa0/1 (етап 1). Для здійснення лавинної розсилки комутатора SW1 необхідно перенаправити широкомовний фрейм на комутатор SW2. Але при цьому комутатор SW1 зобов'язаний якимось способом повідомити комутатора SW2, що даний фрейм належить мережі VLAN 10, для того, щоб після його прийняття призвести лавинную розсилку тільки в мережі VLAN 10, а не VLAN 20. Як можна побачити на етапі 2, перед пересиланням фрейму комутатор SW1 доповнив вихідний фрейм Ethernet заголовком VLAN, в якому вказується інформація про те, до якої VLAN належить даний фрейм (в даному випадку VLAN 10).

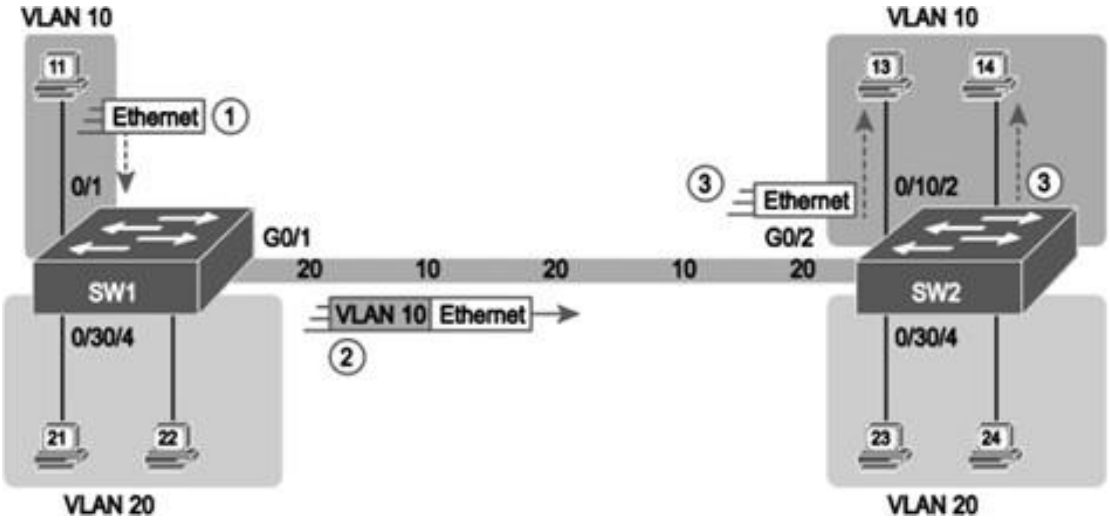

Рисунок 2.4 - Магістральне з'єднання VLAN між двома комутаторами [2]

Після отримання комутатором SW2 даного фрейму, він отримує інформацію про те, що фрейм відноситься до мережі VLAN 10. Після чого комутатор SW2 прибирає заголовок VLAN і пересилає початковий фрейм по інтерфейсу до VLAN 10 (етап 3). Як інший приклад можна розглянути випадок, коли комп'ютер ПК21 (що знаходиться в мережі VLAN 20) передає широкомовний фрейм. Комутатор SW1 передає даний фрейм через порт Fa0/4 (так як цей порт належить мережі VLAN 20) і порт Gi0/1 (так як це магістральний канал, що означає, що він підтримує кілька різних мереж VLAN).

Комутатор SW1 доповнює фрейм заголовком магістралі, який складається з ідентифікатора VLAN 20. Визначивши, що фрейм належить мережі VLAN 20, комутатор SW2 прибирає магістральний заголовок і пересилає його тільки на порти Fa0/3 і Fa0/4, так як вони належать мережі VLAN 20, але не на порти Fa0/1 і Fa0/2, так як вони належать мережі VLAN 10.

2.3 Протоколи VLAN

2.3.1 Протокол VLAN Trunking - VTP

У випадках, коли в мережі є чимале число комутаторів, налаштування всіх наявних VLAN на кожному з комутаторів є досить нелегкою. Саме тому був створений магістральний (транкінгового) протокол віртуальних мереж VTP (VLAN Trunking Protocol). Протокол VTP є протокол локальної обчислювальної мережі, який призначений для обміну даними про VLAN.

Протокол створення магістральних каналів віртуальної локальної мережі (VTP) має на увазі зручне доповнення до засобів управління віртуальними локальними мережами. Він дає можливість в автоматичному режимі встановлювати віртуальні локальні мережі відразу деякого числа комутаторів в мережі [2].

Для того, щоб можна було розглянути зручність застосування даного протоколу, потрібно уявити себе на місці адміністратора у великій неоднорідною мережі. Припустимо, що в даній мережі міститься 500 комутаторів і більше 100 віртуальних локальних мереж. Щоб віртуальні локальні мережі могли обмінюватися інформацією по магістральних каналів відповідно до їх визначеннями, необхідно, щоб номери віртуальних локальних мереж були однаковими у всіх комутаторах, які беруть участь у формуванні даних мереж на підприємстві. Також, потрібно пам'ятати для чого призначені певні віртуальні локальні мережі, наприклад, "дана мережа - призначена для вищого керівництва, дана - для звичайних службовців" і т.д. Навіть такі типові характеристики дають можливість зрозуміти, які труднощі можуть виникнути при налаштуванні конфігурації віртуальних локальних мереж в такій великій мережі. Наприклад, уявіть собі, що може статися якщо користувальницький порт буде поміщений не в ту віртуальну локальну мережу, в яку потрібно, через те, що хтось помилково ввів параметр VLAN 151 замість VLAN 115?

З метою вирішення даної проблеми програмне забезпечення протоколу VTP дозволяє в автоматичному режимі привести в дію ухвали віртуальних локальних мереж від імені адміністратора, це, в свою чергу, дає можливість встановити на одному комутаторі імена та номери віртуальних локальних мереж, після чого, поширити ці дані по всьому підприємству. Важливо пам'ятати, що програмне забезпечення VTP не поширюється по всьому комутаторів дані про те, до якої віртуальної локальної мережі відноситься певний пристрій (так як, в більшості мереж ці дії можуть призвести до руйнівних наслідків); на інші комутатори передаються тільки визначення (ім'я, номер та інші основні дані).

Щоб досягти цієї мети програмне забезпечення VTP в першу чергу (після введення протоколу VTP в дію) анонсує дані про конфігурацію віртуальної локальної мережі через все магістральні порти. Отже, що знаходяться поруч комутатори отримують інформацію про наявність в топології віртуальних локальних мереж і про їх конфігурації. Після цього, дані комутатори поширюють дані про віртуальних локальних мережах по підключеним до них комутаторів і т.д.

Програмне забезпечення VTP працює в комутаторі в трьох режимах: клієнтському, серверному і прозорому.

Клієнтський режим. В даному режимі комутатор здійснює прийом і передачу анонсів VTP, що відносяться до його домену управління. Після чого, комутатор доповнює свою конфігурацію віртуальної локальної мережі змінами. У той час, як комутатор знаходиться в клієнтському режимі, будь-які зміни в конфігурацію віртуальної локальної мережі не можуть бути внесені. З цієї причини, зміни в конфігурацію віртуальної локальної мережі комутатора, який знаходиться в клієнтському режимі, можна внести з використанням протоколу VTP.

Серверний режим. В даному режимі комутатор теж проводить прийом і передачу анонсів VTP, але крім цього також створює нові анонси. Даний режим дає можливість виробляти модифікацію даних віртуальної локальної мережі

безпосередньо в самому комутаторі, а також може здійснювати додавання і видалення віртуальних локальних мереж з домену управління. Модифікація конфігурації заходів домену управління сприяє оновленню номера версії конфігурації (а також номери версії бази даних VTP). Подібне оновлення змушує все знаходяться в домені управління комутатори оновити свої конфігурації VTP з урахуванням нових даних. Слід зазначити, що в кожному домені управління необхідна наявність одного-двох серверів VTP; крім цього, потрібно уважно контролювати дотримання прав на модифікацію конфігурації даних комутаторів. Інакше, можуть виникнути помилки, які згодом будуть поширяться по всьому домену управління.

Прозорий режим. Даний режим дозволяє перенаправляти дані, але інформація про конфігурацію віртуальних локальних мереж, яка знаходиться в даних анонсах, ігноруються. В даному режимі дозволяється здійснювати зміни конфігурації віртуальних локальних мереж в комутаторі, але подібні зміни в конфігурації будуть ставитися тільки до даного локального комутатора [6].

2.3.2 Протокол Spanning-Tree - STP

Одним з поширених способів захисту мережі від обриву кабелю є утворення резервних з'єднань. Але, при резервуванні з'єднань виникає комутаційна петля, показана на рисунку 2.3. В результаті утворення петлі, що пересилаються по мережі пакети будуть зациклюватися. З цієї причини в сучасні комутатори вже вбудовано захист від зациклення пакетів, що блокує пересилання інформації по резервним лініях до того моменту, поки основні лінії зв'язку є працездатними.

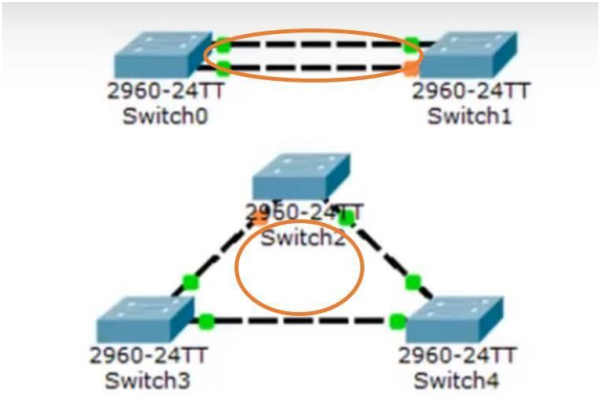

Рисунок 2.3 - комутаційні петлі

Освіта комутаційних петель призводить до утворення наступних проблем, які, в свою чергу, можуть привести до непрацездатності всієї мережі:

1) широкомовні шторми,

2) множинні копії кадрів,

3) множинні петлі.

З метою запобігання виникнення даних петель комутатори застосовують протокол основного дерева (англ. Spanning Tree Protocol - STP) - мережевий протокол, який працює на другому рівні OSI.

Головне завданням протоколу STP є приведення мережі Ethernet з множинними зв'язками до деревоподібної топології. Це здійснюється за допомогою автоматичного блокування надлишкових зв'язків. Час збіжності (тобто перемикання на резервний канал) становить 30-50 секунд. Але це вважається досить великим числом, з цієї причини, крім протоколу STP, існують альтернативні протоколи: RSTP, MSTP (час збіжності яких становить менше секунди).

Принцип дії протоколу складається з 3 етапів:

1) В мережі вибирається один кореневий комутатор (англ. Root Bridge).

Порти кореневого комутатора стають призначеними і переходять в стан передачі, тобто вони мають можливість приймати і передавати пакети. (Рис. 2.4)

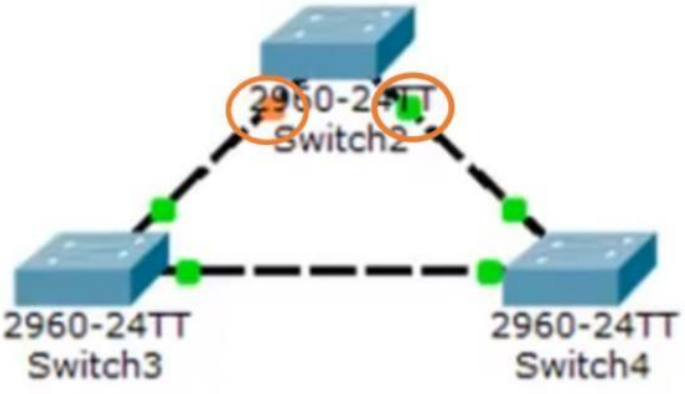

Рисунок 2.4 - Призначені порти кореневого комутатора

2) Після цього, відбувається вибір кореневого порту на некореневим комутаторі. В цьому випадку, кореневої порт вибирається залежно від вартості шляху від некорневого комутатора до кореневого. Вартість шляху можна розрахувати, використовуючи пропускну здатність каналу. Тобто, чим більше пропускна здатність, тим менше вартість.

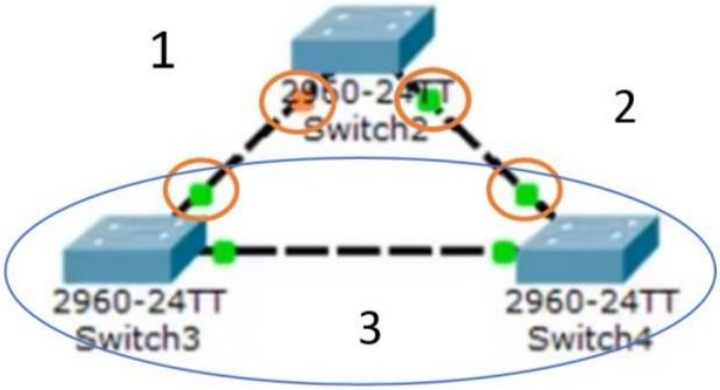

Рисунок 2.5 - Кореневі порти некореневих комутаторів

Наприклад, при пропускній здатності каналів під номерами 2 і 3 були 100 Мбіт/с, а каналу під номером 1 - 10 Мбіт/с, то для Switch3 кореневих портом був би другий порт, тому, що його пропускна здатність більше пропускної здатності інших портів.

3) Далі, вибирається призначений порт. У кожному сегменті (тобто проліт між комутаторами) протокол STP утворює один порт, який призначений для зв'язку з цим сегментом. Призначений порт вибирається на Switch-і, що має найменшу вартість шляху до кореневого комутатора. Призначений порт переходить в стан передачі. У нашому випадку - це порт на Switch4 (рис.2.6)

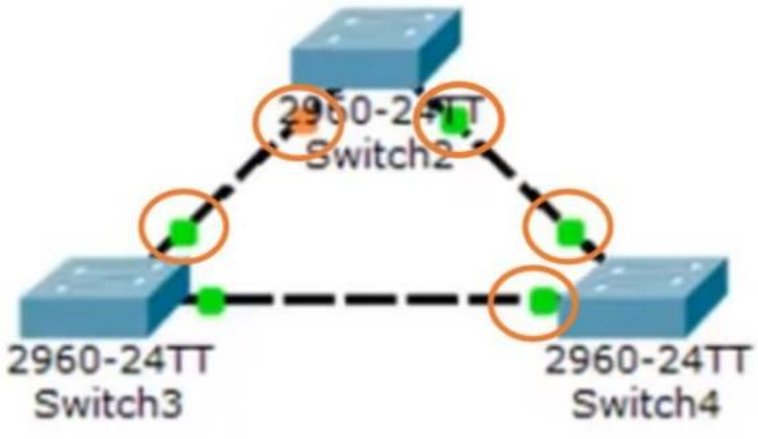

Рисунок 2.6 - Призначений порт

Вибір кореневого комутатора відбувається наступним чином. Протокол STP ґрунтується на числі BID (англ. Bridge ID). Даний параметр є об'єднанням пріоритету комутатора і його MAC-адреси. Оскільки на всіх комутаторах пріоритет однаковий, то кореневих комутатором автоматично стане комутатор з найменшим MAC-адресою. Таким же чином здійснюється вибір призначеного порту, якщо у двох комутаторів однакові вартості шляху до кореневого.

Стану портів можуть бути наступні:

- блокування (blocking),
- прослуховування (listening),
- навчання (learning)
- передача (forwarding).

1. Blocking - це стан всіх портів за замовчуванням, при якому фрейми не відсилаються портами. Після включення комутатора, всі порти знаходяться в даному стані.

2. Listening - це стан, який йде після стану blocking. В даному випадку порт комутатора теж не передає фрейми, але бере участь у процесі spanning-tree для вирішення, чи є необхідність продовження для передачі фреймів.

3. Learning - це стан, наступне за станом listening. В цьому випадку, порт комутатора не передати фрейми, а готується до переходу в наступне – стан forwarding.

4. Forwarding - це стан після стану learning. В даному випадку, порт комутатора може передавати фрейми і продовжувати брати участь в процесі spanning-tree. Цей стан необхідно для нормального функціонування пристроїв.

2.3.3 VLAN на базі міток - стандарт IEEE 802.1Q

У випадках, коли застосовується додаткове поле з інформацією про номер віртуальної мережі, воно застосовується тільки у випадках, коли кадр пересилається від комутатора до комутатора, а при пересиланні кадру кінцевому вузлу воно віддаляється. Спільно з цим трансформується протокол взаємодії "комутатор-комутатор", а програмне і апаратне забезпечення кінцевих вузлів не змінюється. Існує велика кількість прикладів подібних фірмових протоколів, але їх загальним недоліком є те, що інші виробники не підтримують дані протоколи.

Компанія Cisco запропонувала ідею застосування заголовка протоколу

802.10 як типове доповнення до кадрів будь-яких протоколів локальних мереж. Даний заголовок протоколу використовується для підтримки функцій безпеки обчислювальних мереж. Сама компанія Cisco застосовує цю технологію в тих випадках, коли комутатори зв'язуються один з одним за допомогою протоколу FDDI. Але, незважаючи на це, дана ініціатива не отримала підтримку інших провідних виробників комутаторів.

Новий стандарт IEEE 802.1Q призначений для встановлення будь-яких змін в структурі кадру Ethernet, які дають можливість пересилати дані про VLAN по

мережі. Стандарт IEEE 802.1p визначає спосіб встановлення пріоритету кадру, який працює на основі застосування нових полів, визначених у стандарті IEEE 802.1Q. Кадр Ethernet доповнюється двома байтами.

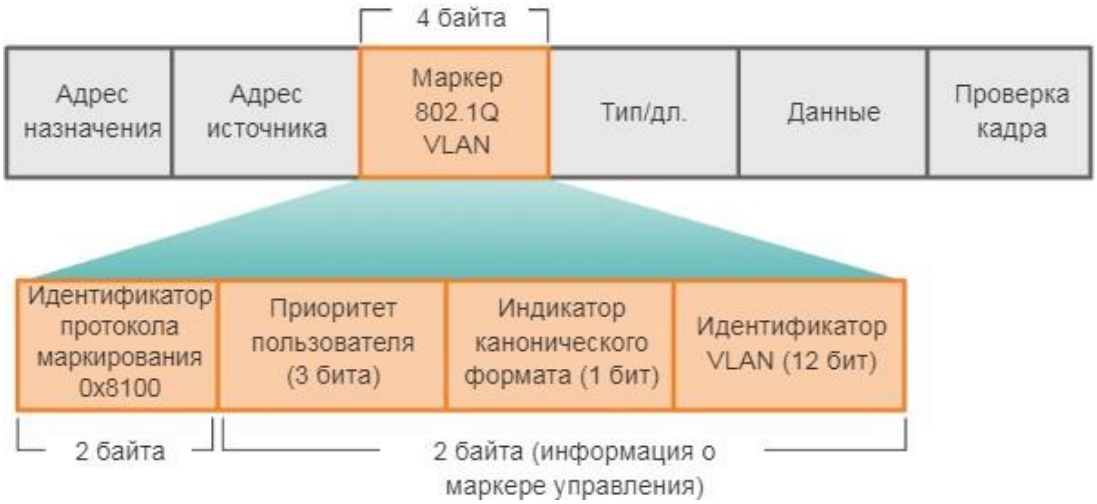

Рисунок 2.7 - Додаткові 4 байта дозволяють використовувати технології QoS і VLAN [7]

Дані 16 біт містять дані про те, до якої VLAN належить кадр Ethernet і про його пріоритет. Говорячи конкретніше, три біта дозволяють кодувати до восьми рівнів пріоритету, 12 біт дають можливість розрізняти трафік до 4096 VLAN, а один біт зарезервований для позначення кадрів мереж інших типів (наприклад, TokenRing, FDDI), які пересилаються по магістралі Ethernet. Слід зазначити, що додаток максимального розміру кадру Ethernet двома байтами призводить до утворення недоліків в роботі великої кількості комутаторів, які призначені для обробки кадрів Ethernet апаратно. З метою уникнення таких проблем, фахівці зі стандартизації подали ідею зменшити на два байта максимальний розмір корисного навантаження в кадрі. Специфікація IEEE 802.1p, яка утворюється в рамках процесу стандартизації 802.1Q, встановлює спосіб пересилання даних про пріоритет мережевого трафіку [4].

Стандарт 802.1p призначений для специфікації алгоритму зміни порядку позиціонування пакетів в чергах, з використанням якого можна забезпечити доставку чутливого до тимчасових затримок трафіку в необхідний час. Крім встановлення пріоритетів, стандарт 802.1p також призначений для введення значимого протоколу GARP (англ. Generic Attributes Registration Protocol) з двома спеціальними його реалізаціями. Першою спеціалізацією є протокол GMRP (англ. GARP Multicast Registration Protocol), які дає можливість автоматизованого

робочого місця здійснювати запит на приєднання до домену групового розсилання повідомлень. Концепція, яка підтримує даний протокол має назву приєднання, яке ініціюється "листям". Протокол GMRP дає можливість пересилати трафік тільки в ті порти, з яких надійшов запит на груповий трафік. Друга реалізація GARP має назву - протокол GVRP (англ. GARP VLAN Registration Protocol), який схожий з протоколом GMRP. Але, незважаючи на це, при роботі з даного протоколу, робоча станція замість запиту на приєднання до домену групового розсилання повідомлень відправляє запит на доступ до однієї з наявних VLAN [1].

З метою узгодження роботи пристроїв, які підтримують формат кадру 802.1 Q, з тими пристроями, які не підтримують даний формат, творці стандарту порекомендували розділити весь трафік в мережі на наступні типи:

- трафік вхідного порту;
- внутрішній трафік;
- трафік вихідного порту.

Трафік вхідного порту (англ. Ingress Port). Кожен кадр, який надходить в коммутируемую мережу і направляється від маршрутизатора або від робочої станції, має певний порт-джерело. За допомогою його номера комутатор повинен вирішити прийняти (або відкинути) даний кадру і передавати його в певну VLAN. Дане рішення, яке приймається в певній логічній точці мережі, забезпечує співіснування абсолютно різних видів VLAN. Отримавши кадр, комутатор додає йому "ярлик" (англ. Tag) VLAN. Після того, як кадр з доданим "ярликом" VLAN потрапляє в мережу, він стає частиною проходить (англ. Progress), або внутрішнього трафіку.

Внутрішній трафік (англ. ProgressTraffic). Кадр з доданим "ярликом" комутується тим же способом, що і кадр без "ярлика". Рішення про те, до якої VLAN належить даний кадр приймаються в прикордонних елементах мережі і інші мережеві пристрої відносяться "нейтрально" до того, яким способом даний кадр виявився в мережі. В результаті того, що максимальний розмір кадру

Ethernet не змінився, пакети всіх VLAN здатні бути оброблені традиційними комутаторами і маршрутизаторами внутрішньої частини мережі.

Трафік вихідного порту (англ. EgressPort). При необхідності виявитися в межсетевом маршрутизаторі або в кінцевої робочої станції, кадру необхідно потрапити за кордону комутованої мережі. Вихідний пристрій мережі приймає рішення про те, якого порту (або портам) необхідно переслати пакет і чи потрібно видаляти з нього службові дані, які передбачені стандартом 802.1Q. Суть полягає в тому, що типові робочі станції не завжди "визнають" дані про VLAN за стандартом 802.1Q, але сервера, який обслуговує декілька підмереж використовуючи єдиний інтерфейс, необхідно використовувати ці дані [6].

Умовний розподіл трафіку на внутрішній, а також вхідного і вихідного портів дає можливість постачальникам нестандартних реалізацій VLAN утворювати шлюзи для їх стикування з VLAN, які відповідають стандарту 802.1Q.

2.3.4 Використання мережевого протоколу

При застосуванні даного методу комутаторів для створення віртуальної мережі необхідно підтримувати будь-якої мережевий протокол. Подібні комутатори мають назву комутаторів 3-го рівня, у зв'язку з тим, що дані комутатори містять в собі як функції комутації, так і маршрутизації.

Об'єднання комутації і маршрутизації є зручним для створення віртуальних мереж в результаті того, що в даному випадку немає необхідності у введенні додаткових полів в кадри, плюс до цього адміністратору немає необхідності повторювати одну і ту ж операція на канальному і мережевому рівнях, так як він може встановити мережі тільки один раз. До якої віртуальної мережі належить певний кінцевий вузол, визначається стандартним методом встановлення мережевої адреси.

Але, незважаючи на це, застосування мережевого протоколу для створення віртуальних мереж не дозволяє застосовувати його звичайними комутаторами, за

винятком комутаторів 3-го рівня. Це є значним мінусом. Тому, найзручнішим і гнучким способом вважається створення віртуальних локальних мереж з використанням стандартів 802.1 Q/p з подальшим їх відображенням на "традиційні мережі" в комутаторах 3-го рівня або маршрутизаторах.

3 ІНФОРМАЦІЙНЕ ТА ПРОРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ ТЕХНОЛОГІЇ VLAN

3.1 Результати моделювання мережі в середовищі Cisco Packet Tracer та налаштування VLAN

Модель майбутньої мережі з VLAN на шести комутаторах 2950-24 та одному роутері 2811 представлена на рис. 3.1:

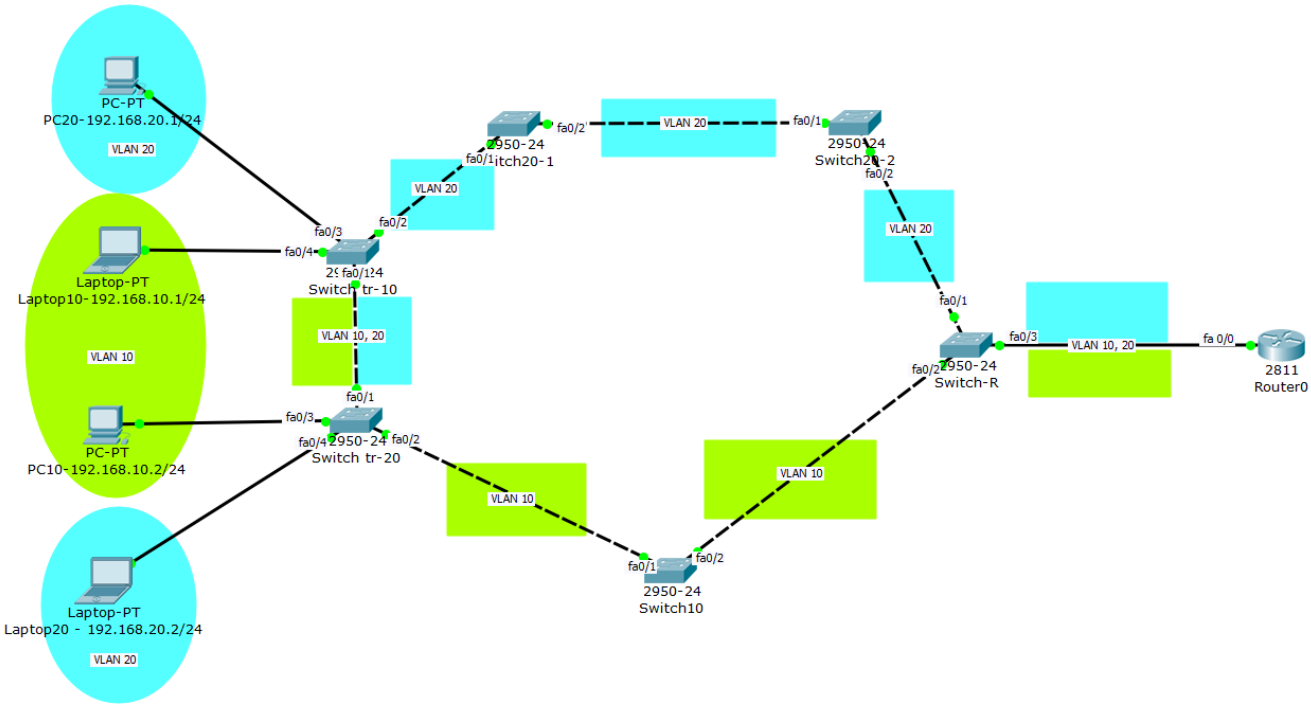

Рисунок 3.1 – Модель мережі на шести комутаторах і одному роутері

Мережа включає сім магістральних каналів – шість між комутаторами, один – між комутатором та маршрутизатором.

Верхньою гілкою будуть просуватися пакети, що належать до віртуальної локальної мережі 20, нижньою – пакети, що належать до віртуальної локальної мережі 10.

Два магістральних канали будуть уможливлювати просування пакетів з обох віртуальних мереж, 10 та 20 (це транковий канал між комутатором та маршрутизатором та канал між комутаторами Switch tr-10 та Switch tr-20).

Розмістимо вузли мережі – шість комутаторів 2950-24 – на робочому просторі, будуючи кільцеву топологію.

Використовуючи інструмент Place Note (Нотатки) задаємо назви комутаторів в залежності до віртуальних мереж, до яких вони будуть відноситися, а також виділячи комутатори з налаштуваннями транкових каналів.

З'єднуємо їх між собою (використовуємо мідний кросовер):

Switch tr-10 інтерфейс fa 0/1 до Switch tr-20 інтерфейс fa 0/1 (комутатори Switch tr-10 та Switch tr-20 будуть з'єднані транковим каналом),

Switch tr-10 інтерфейс fa0/2 до Switch 20-1 інтерфейс fa 0/1,

Switch 20-1 інтерфейс fa 0/2 до Switch 20-2 інтерфейс fa 0/1,

Switch 20-2 інтерфейс fa 0/2 до Switch-R інтерфейс fa 0/1,

Switch tr-20 інтерфейс fa 0/2 до Switch 10 інтерфейс fa 0/1,

Switch 10 інтерфейс fa 0/1 до Switch-R інтерфейс fa 0/2.

Додаємо маршрутизатор 2811 Router0 та під'єднуємо Switch-R інтерфейс fa 0/3 до Router0 інтерфейс fa 0/0 (використовуємо прямий мідний кабель).

Канал між Switch-R та маршрутизатором буде магістральним.

Додаємо на робочий простір чотири термінальні пристрої, два PC та два ноутбуки, та під'єднуємо один PC та один ноутбук до Switch tr-10 (інтерфейс fa 0/3 та інтерфейс fa 0/4 відповідно), потім повторюємо те ж саме для Switch tr-20.

Використовуючи інструмент Place Note, задаємо назви термінальним пристроям в залежності до віртуальних мереж, до яких вони будуть відноситися.

Таким чином, маємо PC10 та Laptop10 (для мережі 192.168.10.0/24) та PC20 та Laptop20 (для мережі 192.168.20.0/24).

Також надписуємо IP-адреси термінальних пристроїв.

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 транкових каналах (між Switch tr-20 та Switch tr-10, а також між Switch-R та Router0) – це будуть віртуальні мережі 10 та 20.

Призначаємо статичні адреси термінальним пристроям через екранні форми:

Заходимо на кожен кінцевий пристрій, навігуємо на вкладку Desktop, обираємо опцію IP Configuration (рис.) та призначаємо IP-адреси (рис. 3.2):

192.168.10.1 для PC10,

192.168.10.2 для Laptop10,

192.168.20.1 для PC20,

192.168.20.2 для Laptop20,

Маска підмережі буде однаковою для всіх термінальних пристроїв – 255.255.255.0

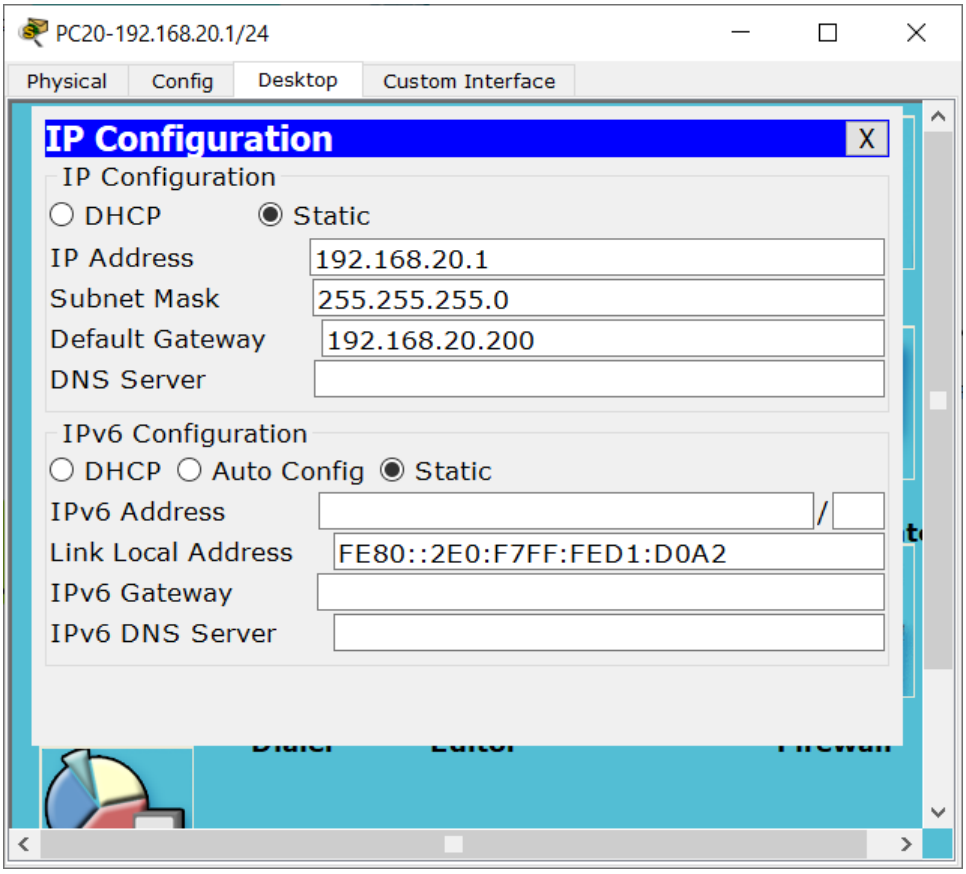

Рисунок 3.2 – приклад призначеннння статичних IP-адресів термінальним пристроям через екранні форми

Також призначаємо дефолтні шлюзи: 192.168.20.200 для термінальних пристроїв, що входять до віртуальної мережі 20 та 192.168.10.100 для термінальних пристроїв, що входять до віртуальної мережі 10.

Налаштовуємо Switch tr-10

Заходимо у режим enable

Switch>en

Заходимо у режим глобальної конфігурації

Switch#conf t

Switch(config)#

Заходимо у режим конфігурації vlan та оголошуємо номер віртуальної мережі 10:

Switch(config)#vlan 10

Даємо ім’я віртуальній мережі:

Switch(config-vlan)#name vlanten

Таким же чином налаштовуємо комутатор для віртуальної мережі 20:

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name vlantwenty

Виходимо з режиму конфігурації VLAN:

Switch(config-vlan)#exit

Призначаємо порти доступу для окремих віртуальних мереж.

Интерфейс fa 0/3 буде портом доступу:

Switch(config)#int fa0/3

Switch(config-if)#switchport mode access

Приписуємо його до мережі 20:

Switch(config-if)#switchport access vlan 20

Таким же чином призначаємо порт fa 0/4 для мережі 10:

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Призначаємо інтерфейс fa 0/1 транковим портом:

Switch(config-if)#int fa0/1

Switch(config-if)#switchport mode trunk

Дозволяємо рух пакетів усіх віртуальних локальних мереж для цього інтерфейса:

Switch(config-if)#

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

А ось для інтерфейса fa0/2 дозволено буде тільки пакети з мережі 20:

Switch(config-if)#int fa0/2

Switch(config-if)#switchport mode trunk

Switch(config-if)#

Switch(config-if)#switchport trunk allowed vlan 20

Switch(config-if)#

Виходимо з режиму конфігурації інтерфейсів:

Switch(config-if)#exit

Виходимо з режиму глобальної конфігурації:

Switch(config)#exit

Перевіряємо налаштування портів та віртуальних локальних мереж на комутаторі (рис. 3.3):

Switch#sh run

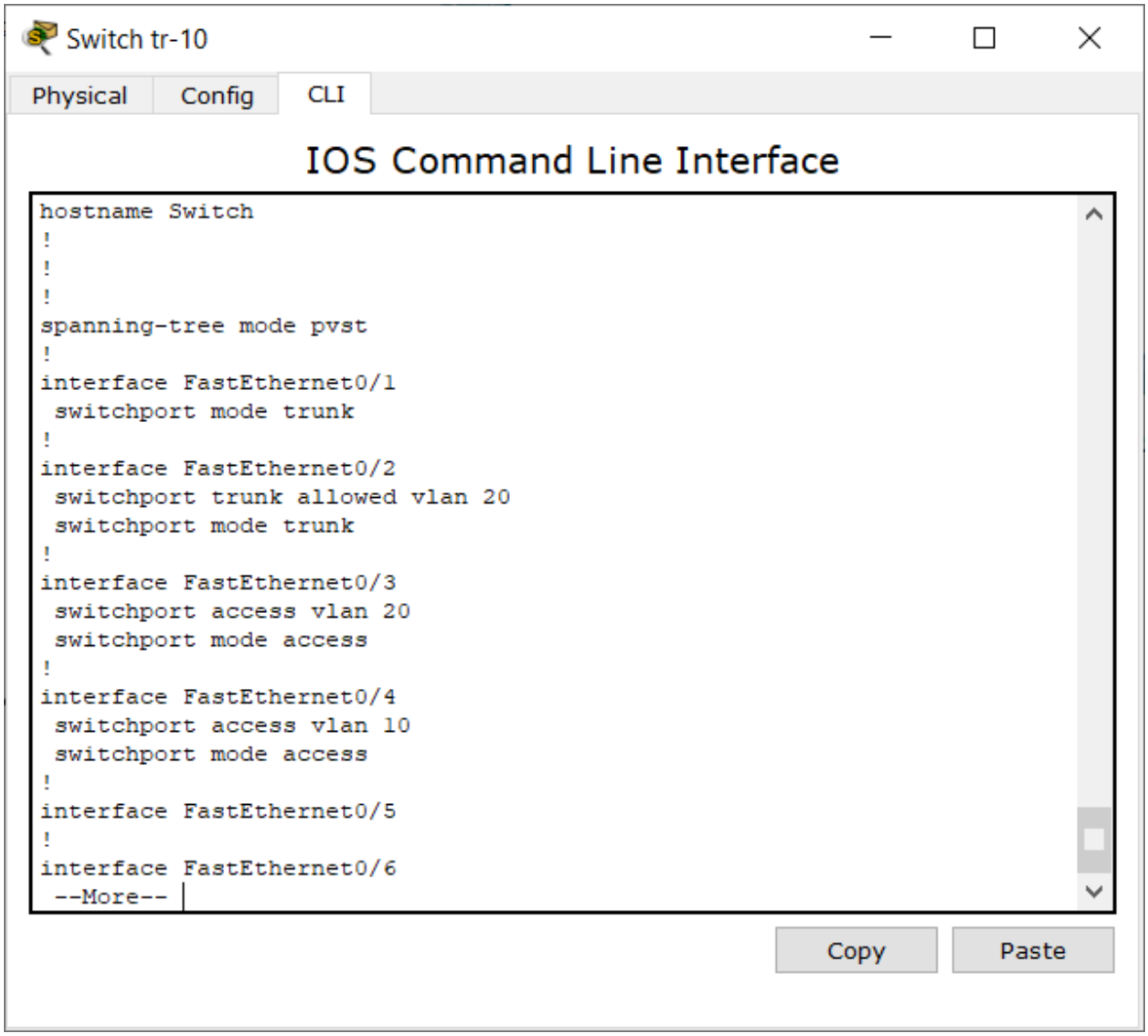

Рисунок 3.3 – результат перевірки конфігурації інтерфейсів та призначених віртуальних мереж

Аналогічним чином налаштовуємо Switch tr-20 та інші комутатори. Звісно ж, Switch20-1, Switch20-2 та Switch10 не будуть мати портів доступу, бо до них не під'єднані ніякі термінальні пристрої. Для транкових портів на комутаторах Switch20-1, Switch20-2 дозволяємо тільки VLAN 20, для транкових портів Switch10 дозволяємо тільки VLAN 10.

Що стосується комутатора Switch-R, дозволяємо VLAN 20 для інтерфейса 0/1, VLAN 10 для інтерфейса 0/2, та всі віртуальні мережі для інтерфейса 0/3.

Переходимо до налаштувань маршрутизатора.

Заходимо у режим enable:

Router>en

Заходимо у режим глобальної конфігурації:

Router#conf t

Заходимо у режим налаштування інтерфейсу:

Router(config)#int fa 0/0

Піднімаємо інтерфейс:

Router(config-if)#no sh

Входимо в режим конфігурації суб-інтерфейсів та призначаємо суб-інтерфейс для віртуальної локальної мережі 10:

Router(config-if)#int fa 0/0.10

Router(config-subif)#

Призначаємо інкапсуляцію для VLAN 10:

Router(config-subif)#encapsulation dot1q 10

Призначаємо IP-адресу для суб-інтерфейсу fa 0/0.10 – це буде шлюз за замовчуванням для віртуальної локальної мережі 10:

Router(config-subif)#ip address 192.168.10.100 255.255.255.0

Виходимо з режиму конфігурації суб-інтерфейсів:

Router(config-subif)#exit

Аналогічним чином призначаємо суб-інтерфейс для віртуальної локальної мережі 20, Призначаємо інкапсуляцію для VLAN 20, призначаємо IP-адресу для суб-інтерфейсу fa 0/0.20 – це буде шлюз за замовчуванням для віртуальної локальної мережі 20

Виходимо з режиму глобальної конфігурації:

Router(config)#exit

Перевіряємо налаштування суб-інтерфейсів, інкапсуляцію, та IP-адреси шлюзів:

Router #sh run

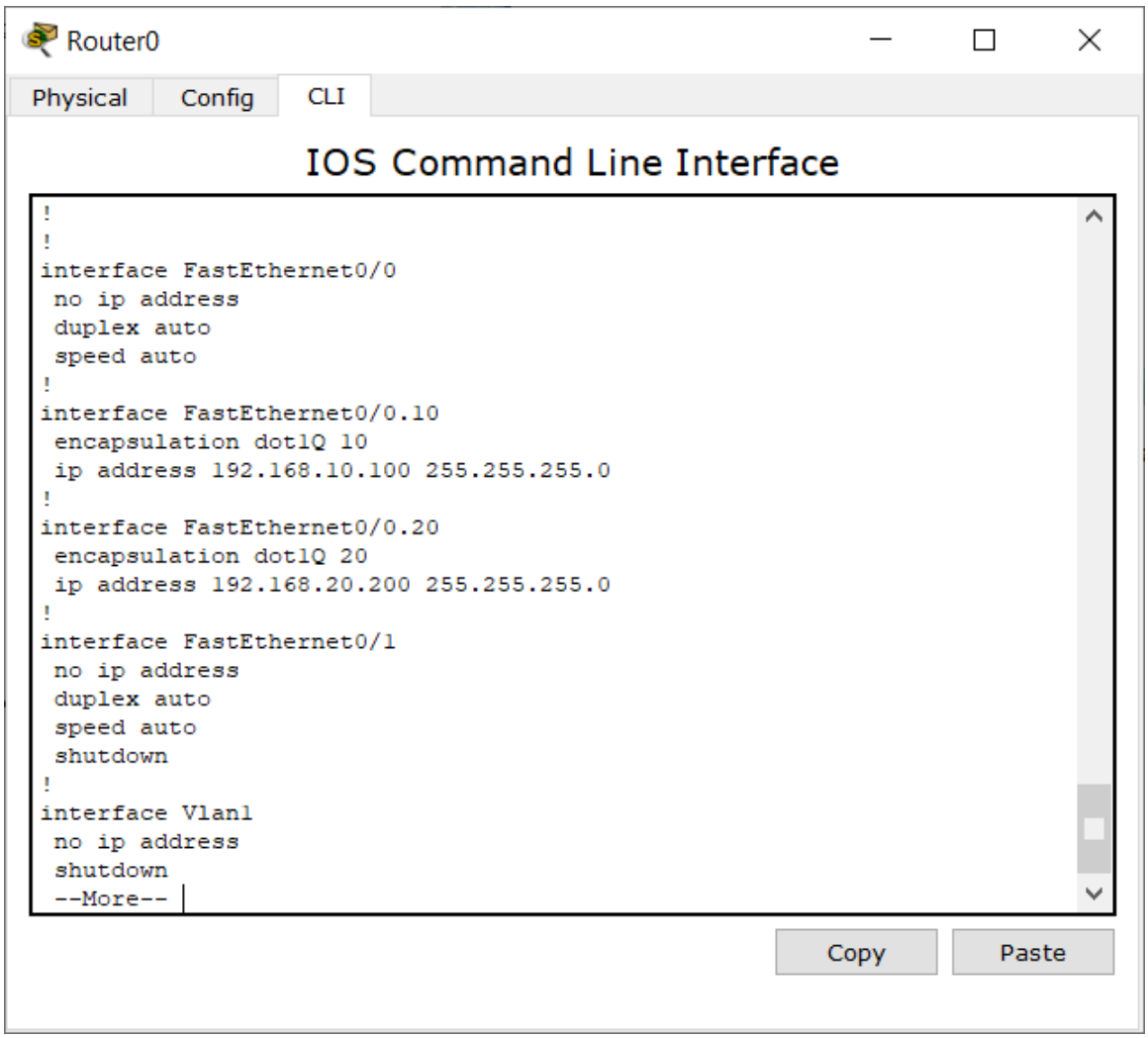

Рисунок 3.4 – результат перевірки конфігурації суб-інтерфейсів та IP-адрес дефолтних шлюзів на маршрутизаторі

3.2 Тестування комп'ютерної мережі з підтримкою VLAN

Перш за все переконаємося, що пакети, що надходять з будь-якого термінального пристрою, надходять будь-якому іншому пристрою, незалежно від приналежності пристрою до віртуальної локальної мережі.

Після побудови ARP-таблиць всі пакети надходять до адресатів – успішний статус незалежно від приналежності вхідних та вихідних пристроїв до віртуальних мереж (рис. 3.5).

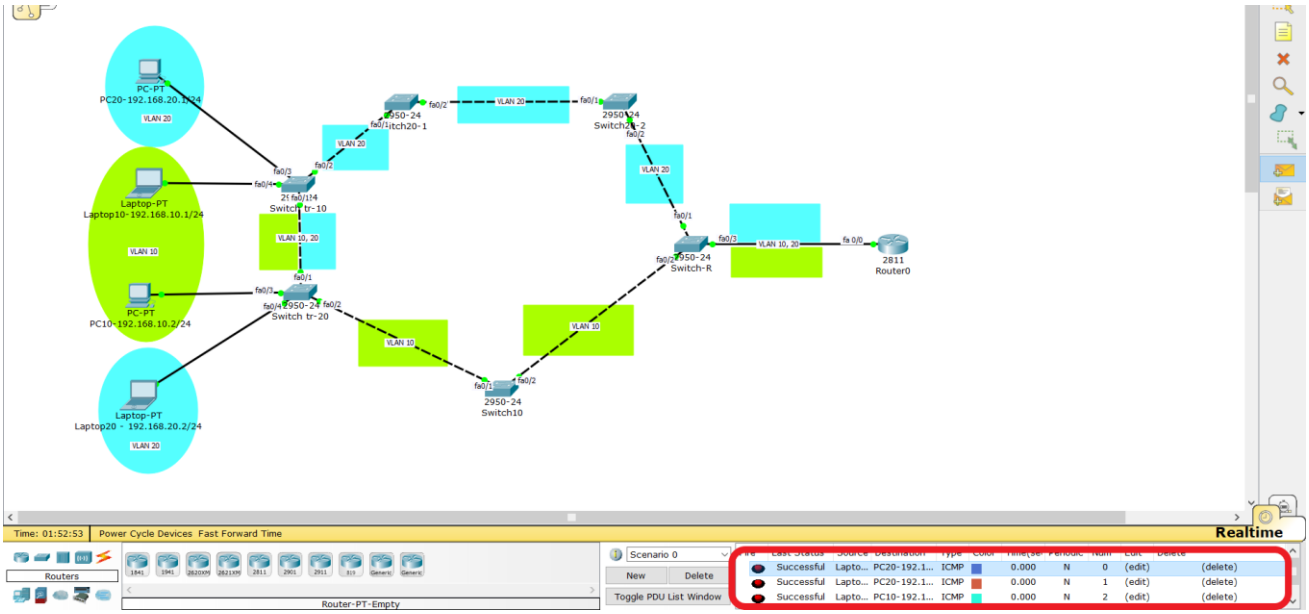

Рисунок 3.5 – результат тестування мережі у реальному часі

Тепер протестуємо мережу в режимі симуляції, перехоплюючи пакети.

Сценарій 1. Теоретично, при просуванні пакетів в межах однієї віртуальної локальної мережі буде задіяно тільки один магістральний канал – лінія зв’язку між комутаторами Switch tr-20 та Switch tr-10.

В режимі симуляції, як і було передбачено, ICMP пакет, надісланий з PC10 до Laptop10 (тобто в межах VLAN 10), просувається таким маршрутом:

З PC10 до порту fa 0/3 комутатора Switch tr-20, потім через порт fa 0/1 комутатора Switch tr-20 до магістрального каналу, через магістральний канал до

інтерфейсу fa 0/1 на комутаторі Switch tr-10, що перекидає його на свій порт fa 0/4 та відправляє адресатові, Laptop10.

Транкові порти інших комутаторів та, тим паче, суб-інтерфейси маршрутизатора при цьому не є задіяними, бо в цьому немає потреби.

Перехопимо пакети на вхідному та виходному комутаторах та дослідимо їх структуру.

На вихідному комутаторі Switch tr-20 на вкладці Inbound можна бачити заголовок Ethernet II (рис. 3.6) – це логічно, бо пакет прибув з термінального пристрою:

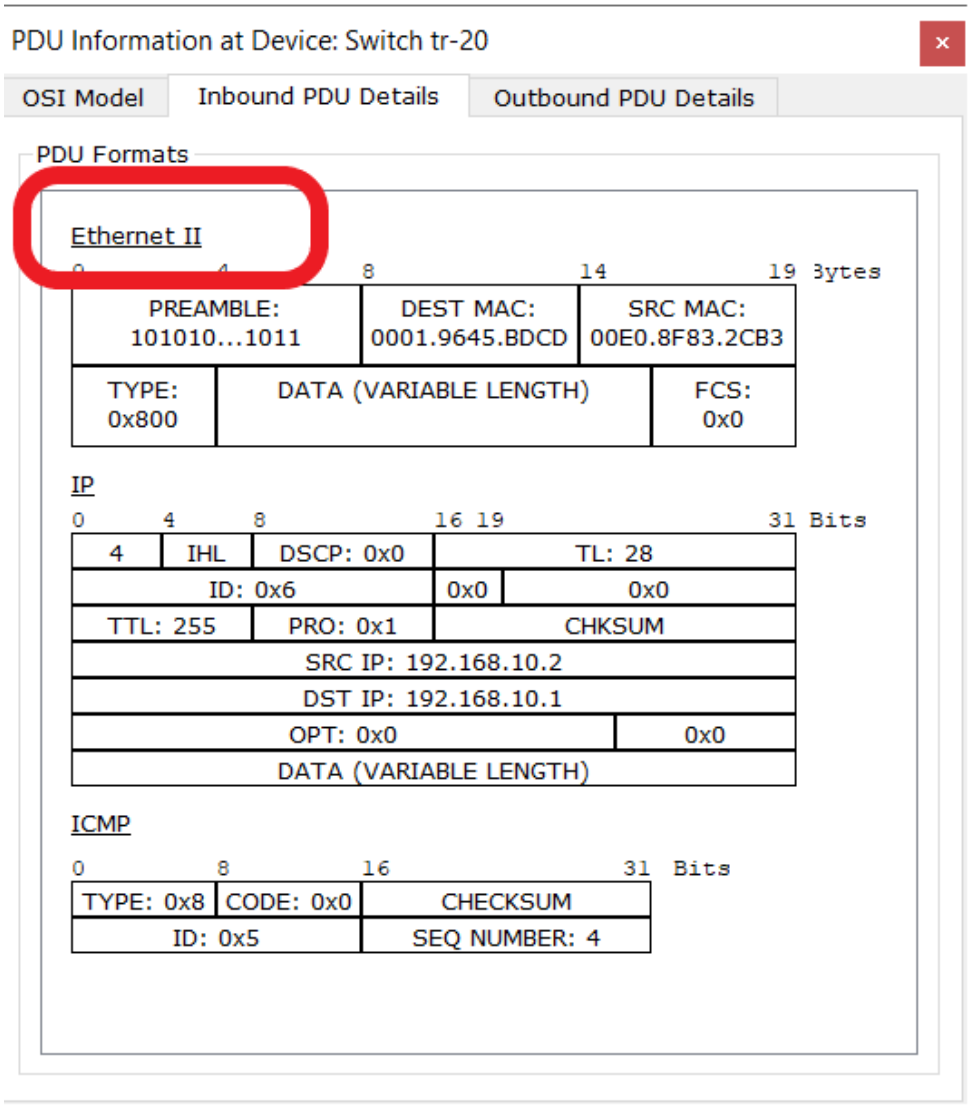

Рисунок 3.6 – Inbound структура пакета на комутаторі перед просуванням у транковому каналі

На вкладці Outbound можна бачити, що пакет підготовлений до просування магістральним каналом, тобто інкапсульований (рис. 3.7), мітка віртуальної мережі в полі TCI (Tag Control Information) показана у шістнадцатичному форматі A, що відповідає 10 у десятичному форматі:

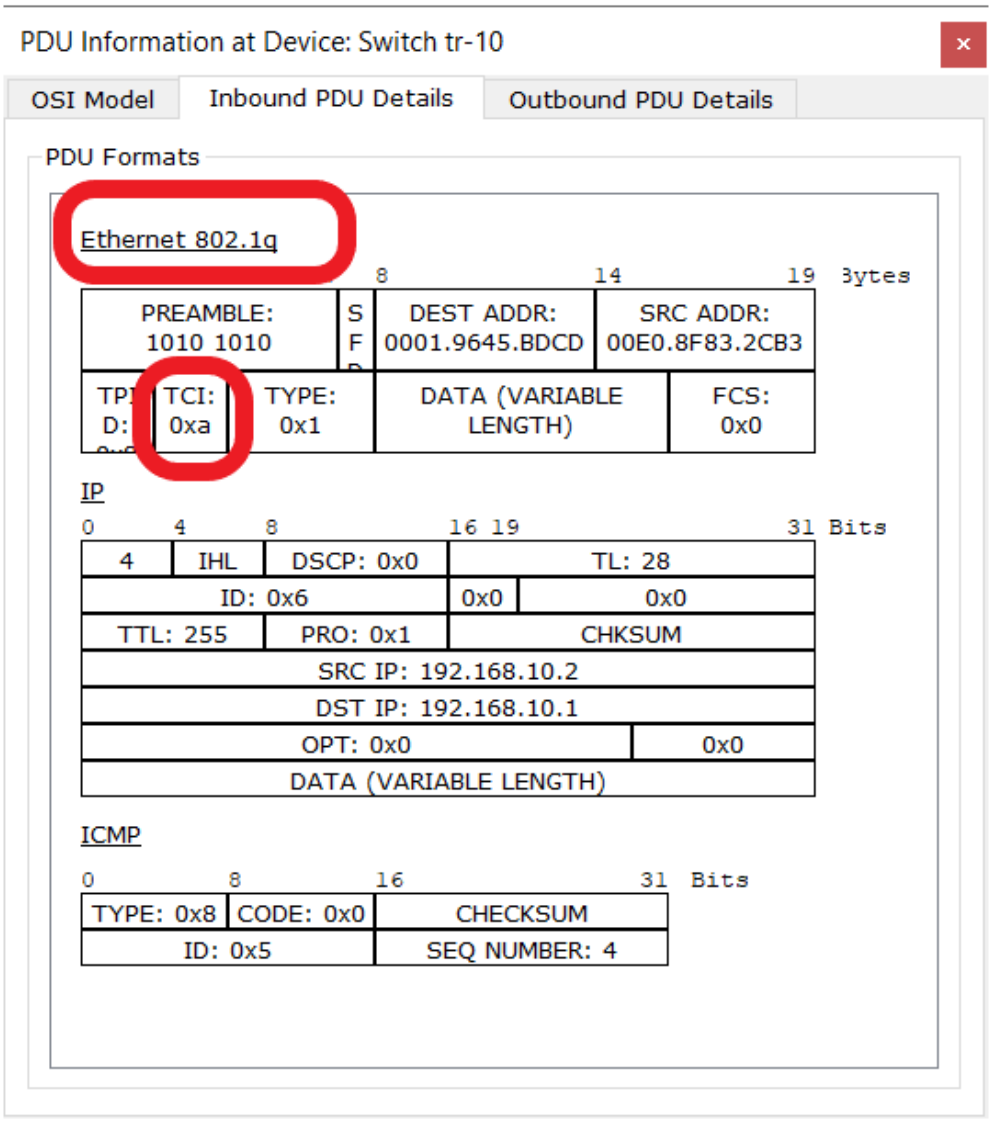

Рисунок 3.7 – Outbound структура пакета на комутаторі перед просуванням у транковому каналі

Після проходження пакетом транкового каналу структура пакету зміниться за дзеркальним принципом: на вхідному комутаторі Switch tr-10 на вкладці Outbound можна бачити інкапсульований пакет з міткою віртуальної мережі, а на вкладці Inbound – заголовок Ethernet II для відправлення на інтерфейс термінального пристрою.

Отже, мережа функціонує правильно, згідно теоретичним принципам.

Сценарій 2. Теоретично, при просуванні пакетів з однієї віртуальної локальної мережі до іншої буде задіяно магістральні канали проміжних вузлів мережі, тобто комутаторів між термінальними пристроями та маршрутизатором.

При цьому не обійтися між допомоги маршрутизатора для здійснення між-VLAN маршрутизації.

Також, згідно з налаштуваннями, пакети будут просуватися до маршрутизатора та від маршрутизатора тільки тими гілками, в яких дозволена відповідна віртуальна мережа.

Тобто, пакет з термінального пристрою, що належить до мережі 10, буде просуватися до маршрутизатора нижньою гілкою; а з маршрутизатора пакет, що призначається VLAN 20, буде просуватися до термінального пристрою верхньою гілкою.

Отже, перешлемо пакет з Laptop20 (VLAN 20) до PC10 (VLAN 20).

Пакет просувається таким маршрутом: Laptop20 → int fa 0/4 Switch tr-20 → int fa 0/1 Switch tr-10 → int fa 0/2 Switch tr-10 → int fa 0/1 Switch20-1→ int fa 0/2 Switch20-1→ int fa 0/1 Switch20-2 → int fa 0/2 Switch20-2 → int fa 0/1 Switch-R → int fa 0/3 Switch-R → int fa 0/0 Router0 → int fa 0/3 Switch-R → int fa 0/2 Switch-R → int fa 0/2 Switch 10 → int fa 0/1 Switch 10 → int fa 0/2 Switch tr-20 → int fa 0/3 Switch tr-20 → PC10 (рис 3.8).

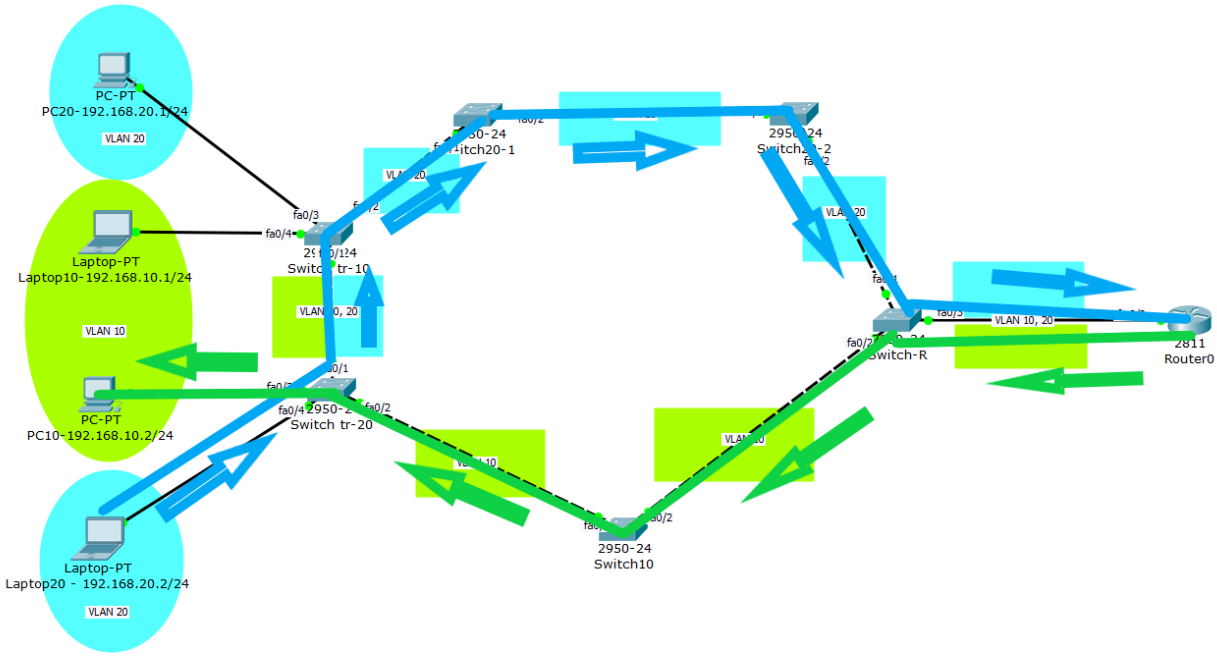

Рисунок 3.8 – Графічна репрезентація маршруту просування пакету з VLAN 20 до VLAN 10

Пакет, перехоплений після прибуття з термінального пристрою до вхідного комутатора, буде мати структуру, ідентичну структурі пакета на такому ж етапі у попередньому сценарії, тому не будемо розглядати структуру пакету повторно.

Дослідимо структуру пакету, перехопленого на проміжному вузлі мережі, тобто на комутаторі, між двома інтер-комутаторними транками. Теоретично, на обох вкладках, Inbound та Outbound, ми побачимо інкапсульований пакет з міткою віртуальної мережі. Наприклад, на проміжному комутаторі Switch20-1 це буде мітка віртуальної мережі 20 (рис. 3.9):

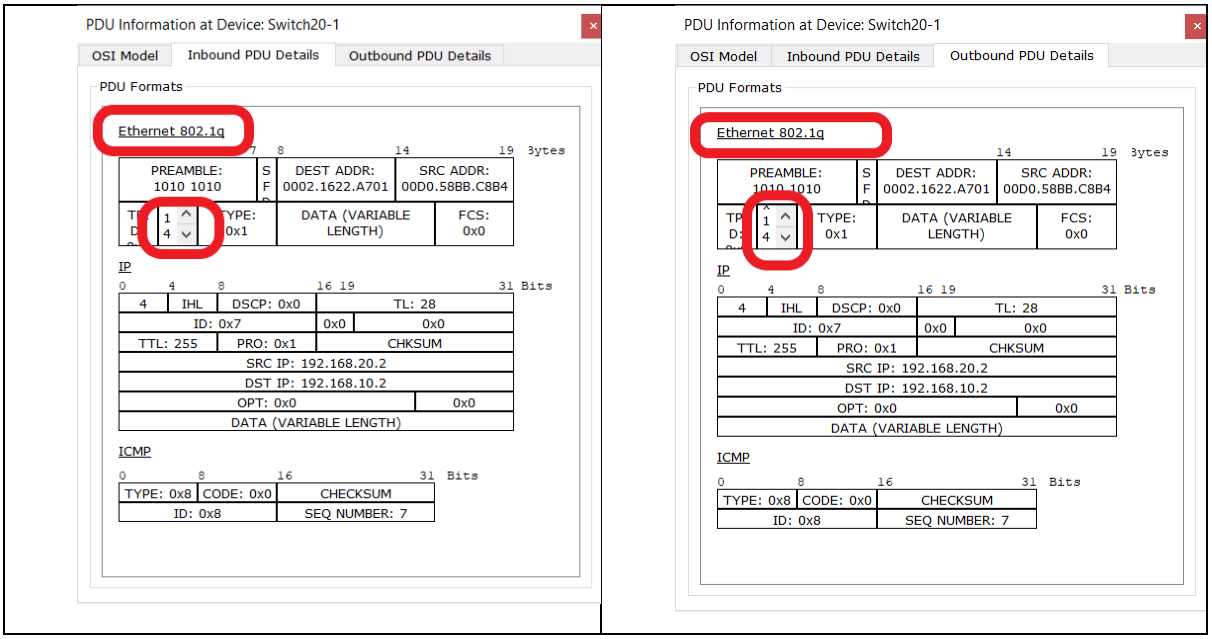

Рисунок 3.9 – Структура пакету, перехопленого на проміжному вузлі мережі VLAN 20

Отже, як можно бачити на скиншоті, мітка в шестнадцатичному форматі є 14, що відповідає мітці 20 в десятичному форматі ($4x16^0+4x16^1=4+16=20$). Значить, на даному етапі мережа функціонує правильно, згідно теоретичним положенням.

Дослідимо структуру пакету, перехопленого на маршрутизаторі. Як на Inbound, так і на Outbound, ми побачимо інкапсульований пакет 802.1Q, але мітки віртуальних мереж будуть різними на Inbound, та на Outbound вкладках: мітка VLAN 20 (14) на Inbound та мітка VLAN 10 (A) на Outbound (рис. 3.10).

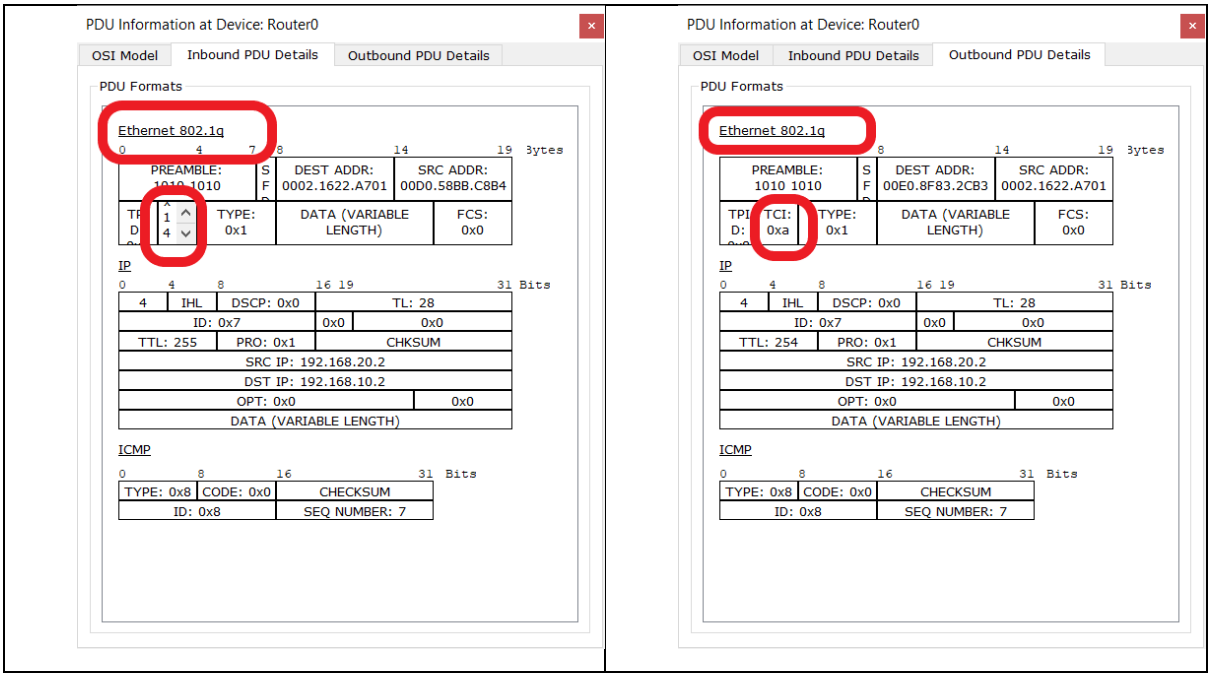

Рисунок 3.10 – Структура пакету, перехопленого на маршрутизаторі

На зворотньому маршруті від маршрутизатора до термінального пристрою структура пакету буде подібною структурі пакету, перехопленого на проміжному вузлі мережі іншої гілки – з єдиною різніцею в тому, що мітка віртуальної мережі в полі TCI буде не 20 (14), а 10 (A), бо пакет просуватиметься нижньою гілкою.

Отже, мережа повністю зібрана, сконфігурована й функціонує абсолютно правильно.

ВИСНОВКИ

Підводячи підсумки виконаної роботи, в якості головних результатів слід виділити наступні.

Віртуальні локальні мережі були створені для вирішення питання розподілу повноважень та впровадження політик безпеки без використання дорогих рішень та приладів. VLAN дозволяє розділяти користувачів не за їх територіальною приналежністю, а за логічним розподілом функцій та призначення.

У роботі були розглянуті передумови впровадження технології віртуальних локальних мереж, протоколи і методи реалізації віртуальних локальних мереж. Технологія віртуальних локальних мереж є дуже затребуваною, завдяки ряду переваг:

1) VLAN допомагає структурувати мережу;

2) використовується для забезпечення безпеки;

3) використовується для об'єднання користувачів на канальному рівні;

4) VLAN зменшує кількість широкомовного трафіку.

За допомогою програми Cisco Packet Tracer був показаний процес створення мережі VLAN на шести комутаторах та одному роутері.

Підсумовуючи вищесказане, можна відзначити, що всі поставлені завдання, а також основна мета роботи - провести аналіз роботи віртуальних локальних мереж, їх моделювання та тестування виконані.

СПИСОК ЛІТЕРАТУРИ

1. Бодчер Р. Программа сетевой академии Cisco CCNA [3-е изд.] : [пер. с англ.]/ Рональд Бодчер, К. Р. Киркендаль. – М. : изд. Дом “Вильямс”, 2005. – 1186 с.

2. Олифер Виктор, Олифер Наталья «Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание» Питер, 2020 год, 1008 стр., ISBN 978-5-4461-1426-9; (PDF) [Електронний ресурс] - https://www.htbook.ru/kompjutery_i_seti/setevye_tekhnologii/kompyuternye-seti-principy-tehnologii-protokoly

3. Амато Вито. Основы организации сетей Cisco, том 1. М.: Издательский дом "Вильяме", 2004. – 512с.

4. Телекомунікаційні системи та мережі. Структура й основні функції. Том 1 [Електронний ресурс] - http://www.znanius.com/3820.html

5. Учебное пособие: Коммутаторы локальных сетей D-Link. Москва, 2006 – 156 с

6. Основы компьютерных сетей: учеб. пособие / Под ред. Л.Г. Гагариной. – М.: Форум»: ИНФРА-М, 2012. – 272 с.

7. Остерлох Х. Маршрутизация в IP-сетях. Принципы, протоколы, настройка: Пер. с англ. / В. Плешаков. – СПб.: ООО «ДиаСофтЮП», 2010. – 512 с.

8. Олифер В.Г. Протокол межсетевого взаимодействия IP [Электронный ресурс]/ В.Г. Олифер, Н.А. Олифер. – [Електронний ресурс] http://citforum.ru/nets/protocols2/index.shtml

9. Пакет К. Создание масштабируемых сетей CISCO / К. Пакет, Д. Тир : [пер. с англ.] – М.: Изд. дом “Вильямс”, 2002. – 792 с.

10. Хилл Б. Полный справочник по CISCO / Хилл Б. : [пер. с англ.] – М. : изд. дом “Вильямс”, 2004. – 1088 с

11. Бородко А.В., Кукунин Д.С. Учебное пособие по дисциплине КСПД. Часть 1 / ГОУВПО СПбГУТ. – СПб, 2013 – 195 с

12. Ethernet [Електронний ресурс] - http://zaycev.me/Downloads/Ethernet.pdf

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

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

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

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

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

18. 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

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

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