МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

Кваліфікаційна робота бакалавра

ГРАФІЧНИЙ ІНТЕРФЕЙС НАЛАШТУВАННЯ ОПЕРАТОРСЬКОЇ МЕРЕЖІ CARRIER ETHERNET ЗА СТАНДАРТОМ Q-IN-Q

Здобувач освіти гр. ІН – 82 Євгеній НАГОРНИЙ

Науковий керівник,
кандидат фізико-математичних наук,
старший викладач
кафедри комп'ютерних наук Дмитро ВЕЛИКОДНИЙ

Завідувач кафедри
доктор технічних наук, професор Анатолій ДОВБИШ

СУМИ 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра комп'ютерних наук

Затверджую_____
Зав. кафедрою Довбиш А.С.
“_____” _____2022 р.

ЗАВДАННЯ
до кваліфікаційної роботи бакалавра

Студента четвертого курсу, групи ІН-82 спеціальності «122 – Комп’ютерні науки» денної форми навчання Нагорного Є. М.

Тема: «Графічний інтерфейс налаштування операторської мережі Carrier Ethernet за стандартом Q-in-Q»

Затверджена наказом по СумДУ
№_____ від _____2022 р.

Зміст пояснювальної записки: 1) літературний огляд за обраною тематикою роботи; 2) постановка завдання та розробки; 3) практична реалізація.

Дата видачі завдання «_____»_____ 2022 р.
Керівник роботи _____ Великодний Д.В
Завдання прийняв до виконання _____ Нагорний Є.М.

РЕФЕРАТ

Записка: 48 стор., 42 рис., 1 додаток, 34 джерела.

Об’єкт дослідження – операторська мережа Carrier Ethernet за стандартом Q-in-Q.

Мета роботи – Розробити графічний інтерфейс для автоматизації налаштування конфігурації мереж на базі Carrier Ethernet за стандартом Q-in-Q.

Методи дослідження – збір та аналіз даних.

Результати – створений графічний інтерфейс для автоматизованої конфігурації мереж на основі Carrier Ethernet за стандартом Q-in-Q. Додаток розроблений за допомогою мови програмування JavaScript, компілятор Microsoft Visual Studio 2022 (64-розрядна версія) версія 17.2

МЕРЕЖА, IP-АДРЕСА, JS, ТУНЕЛЮВАННЯ, Q-IN-Q.

ЗМІСТ

ВСТУП

На сьогоднішній день розвиток комп’ютерних технологій йде семимильними кроками та збільшує свої оберти кожного дня. За останні 15 років, те що вважали унікальним та незамінним, стає некомпетентним в конкуренції з новітніми технологіями в своїй галузі.

Гарним прикладом є те, що абсолютно кожна компанія хоче мати свою надійну, швидку, масштабну та бюджетну мережу, яка може зв’язувати всі офіси з різних куточків світу. Для цих всіх пунктів необхідно мати знання і досвід в налаштуваннях мереж.

Зв'язок між офісами можливо проводити багатьма можливими технологіями, які дозволять уникати проблем, спрощувати налаштування, зменшити кількість обладнання, та їх ціну за пристрій та обслуговування.

Для цих всіх факторів процес розвитку мереж є створений стандарт Q-in-Q

Q-in-Q – це саме та технологія, якою користуються майже всі світові масштабні компанії. Але для її аналізу, редагування та налаштування потрібно мати знання та досвід в галузі комп’ютерно-інформаційних технологій.

Для досягнення даних вимог можуть бути використані графічні інтерфейси, які можуть допомогти отримати потрібні налаштування, з мінімальними витратами зусиль. Саме розробка інтерфейсу для налаштування мережі Carrier Ethernet за стандартом Q-in-Q і є основною метою даної роботи.

РОЗДІЛ 1 МЕРЕЖІ ОПЕРАТОРСЬКОГО КЛАСУ НА БАЗІ ТЕХНОЛОГІЇ CARRIER ETHERNET

1.1 Carrier Ethernet над MPLS

MPLS (Multiprotocol Label Switching) – технологія швидкої комутації пакетів у багатопротокольних мережах, заснована на використанні міток. MPLS розробляється і позиціонується як спосіб побудови високошвидкісних IP-магістралей, але область її застосування не обмежується протоколом IP, а поширюється на трафік будь-якого мережевого протоколу, що маршрутизується [1].

Сьогодні за допомогою MPLS можна вирішувати різні завдання:

• прискорювати просування пакетів за рахунок заміни на магістралі мережі маршрутизації на комутацію;

• вирішувати завдання Traffic Engineering, тобто конструювати шляху проходження трафіку через мережу таким чином, щоб домогтися максимально ефективного використання маршрутизаторів і каналів зв'язку;

• забезпечувати необхідні параметри якості обслуговування (QoS) за рахунок резервування пропускної здатності для трафіку, що проходить по шляхах MPLS;

• будувати масштабовані віртуальні приватні мережі (VPN) [2].

Щоб зрозуміти принцип роботи методики MPLS слід зазначити, що в традиційній IP-мережі кожному маршрутизатору доводиться виконувати пошук IP, шляхом постійного пошуку його в таблицях з пакетами даних з наступним пересиланням на наступний рівень, поки пакети даних не досягнуть потрібного пункту призначення. MPLS технологія привласнює мітку всім IP-пакетам, а тим часом вже маршрутизатори приймають рішення про передачу пакета далі на наступний пристрій завдяки потрібному значенню мітки. Мітка додається у складі MPLS заголовка, який додається

між заголовком кадру (другий рівень OSI) та заголовком пакета (третій рівень OSI) і, по суті, надалі йде їхнє накладання один на одного [4].

Наступний рисунок демонструє архітектуру мережі MPLS.

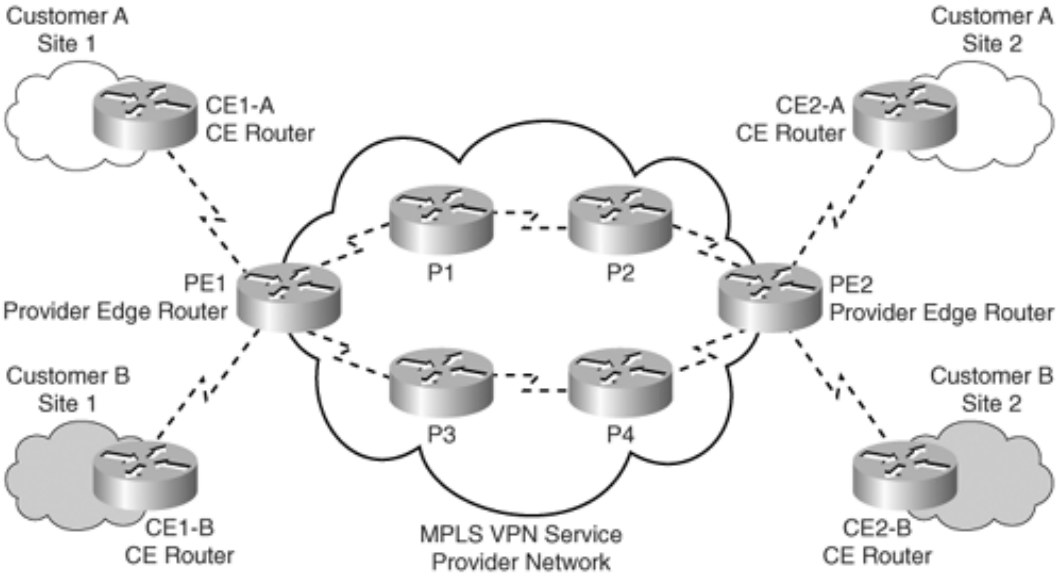

Рис. 1.1. Архітектура мережі MPLS [4]

Домен MPLS VPN, як і традиційний VPN, складається з мережі клієнта та мережі постачальника. Модель MPLS VPN дуже схожа на модель спеціального маршрутизатора PE в реалізації однорангового VPN. Однак замість розгортання окремого PE-маршрутизатора для кожного клієнта, клієнтський трафік ізольовано на одному PE-маршрутизаторі, який забезпечує підключення до мережі постачальника послуг для кількох клієнтів [4].

Технологія MPLS заснована на обробці заголовка MPLS , що додається до кожного пакета даних . Заголовок MPLS може складатися з о днієї або декількох " міток ". Декілька записів (міток) у заголовку MPLS н азиваються стеком міток . Кожен запис у стеку міток складається з наступн их чотирьох полів:

- значення мітки займає 20 біт ;
- поле класу трафіку необхідне для реалізації механізмів якості обслуг овування та явного повідомлення про перевантаження займає 3 біти;

- прапор дна стека; якщо прапор встановлений в 1 , це означає , що пот очна мітка остання в стеку ; _ займає 1 біт ;
- поле TTL, необхідно для запобігання петель MPLS комутації ; займає 8 біт [5].

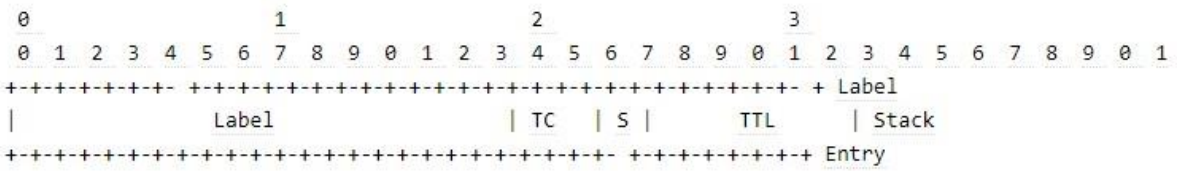

Рис. 1.2. Класичний формат мітки MPLS по регламенту RFC [5]

- Час життя (TTL). Це поле, що займає 8 бітів, дублює аналогічне пол е IP- пакета. Це необхідно для того, щоб пристрої LSR могли відкид ати заблукані»

  пакети тільки на підставі інформації, що міститься в заголовку MPL S, не звертаючись до заголовка IP.
- Клас послуги (Class of Service, CoS). Поле CoS, що займає 3 біти, спочатку було зарезервовано для розвитку технології, але останнім часом використовується в основному для вказівки класу трафіку, що потребує певного QoS.
- Ознака дна стека міток – S (1 біт).

  Розглянемо ситуацію, коли заголовок MPLS включає лише одну мітку [5].

Як очевидно з малюнка, технологія MPLS підтримує кілька типів кадрі в: PPP, Ethernet, Frame Relay і ATM. Це не означає, що під шаром MPLS п рацює абияка з перерахованих технологій, наприклад Ethernet. Це означа є, що в технології MPLS використовуються формати кадрівтехологій дл я розміщення в них пакету мережного рівня, яким майже сьогодні є IP- пакет.

Пакети, які мають один і той самий маршрут, поєднуються в класи, що надає можливість зменшити витрати ресурсів на їх обробку, через те, що маршрутизатору не потрібно аналізувати всі пакети, а лише один [23].

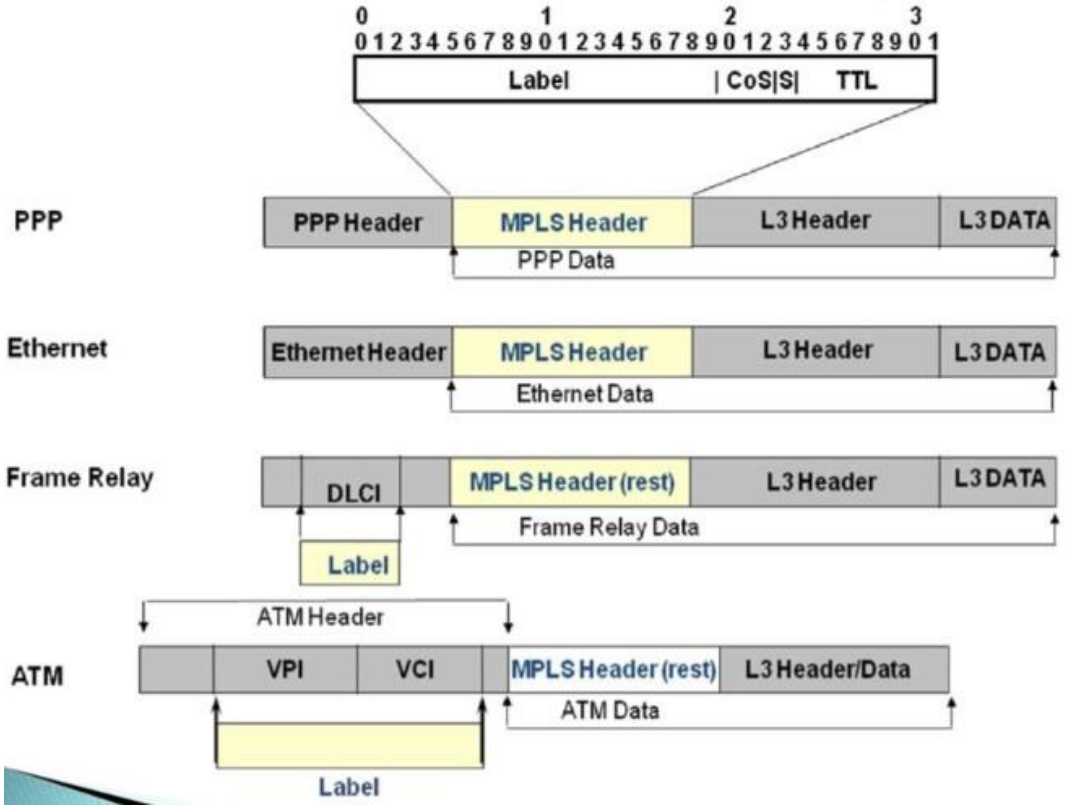

Рис. 1.3. Формати заголовків декількох різновидів технології MPLS [23]

Поява MPLS відкриває великі можливості для створення магістральних IP-мереж. Нова технологія може значно покращити існуючі способи їх створення: як за допомогою IP-маршрутизаторів, з'єднаних каналами «крапка-крапка», так і на базі транспортної мережі ATM, поверх якої працюють IP-маршрутизатори.

В обох випадках застосування MPLS дає значні переваги. У магістральній мережі ATM з'являється можливість одночасно надавати клієнтам як стандартні сервіси ATM, і широкий спектр послуг IP-мереж поруч із додатковими сервісами[25].

Транспортні позначки використовуються для передачі трафіку через мережу MPLS. Для них використовуються LDP і RSVP-TE. Сервісні мітки служать поділу різних сервісів. Тут входять в роль MBGP і відросток LDP - tLDP .

Зокрема MBGP дозволяє, наприклад, помітити, що ось такий маршрут належить такому-то VPN. Потім цей маршрут передає, як vpn-ipv4 family своєму сусідові з міткою, щоб той зміг потім відокремити мух від котлет. Щоб він міг відокремити, йому потрібно повідомити про відповідність мітки-FEC.

Обов'язковою умовою роботи всіх протоколів динамічного розподілу міток є базове налаштування IP-зв'язку. Тобто, на мережі повинні бути запущені IGP [27].

На зображеному нижче рисунку, показаний формат мітки MPLS.

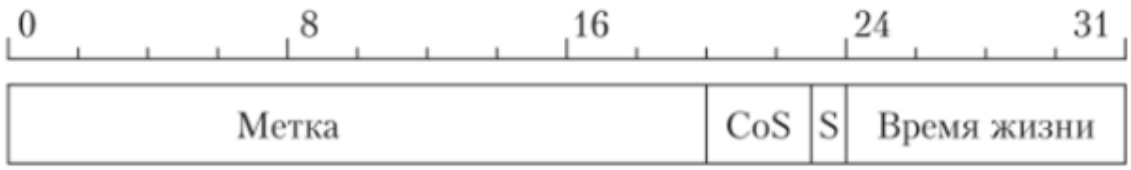

Рис. 1.4. Формат мітки MPLS [30]

MPLS-мітка передається у складі будь-якого пакета, причому спосіб її приєднання до пакету залежить від використовуваної технології канального рівня. MPLS-мітка додається між заголовком кадру (другий рівень ISO/OSI) і заголовком пакета (третій рівень моделі ISO/OSI) [27].

Рис. 1.5. Розташування MPLS мітки [30]

1.2 Стандарт IEEE 802.1ad – “Q-in-Q”

Q-in-Q або Double VLAN – це функція, яка підтримує інкапсуляцію тегів IEEE 802.1Q VLAN у теги другого рівня 802.1Q tag на провайдерських граничних комутаторах. За допомогою Double VLAN сервіс провайдер може використовувати унікальні VLAN) для надання послуг клієнтам, які мають кілька VLAN у своїх мережах. VLAN клієнта, або в цьому випадку

зберігаються і трафік від різних клієнтів сегментується навіть якщо він передається в тому самому VLAN[6].

На рисунку нижче зображено порівняння форматів пакетів

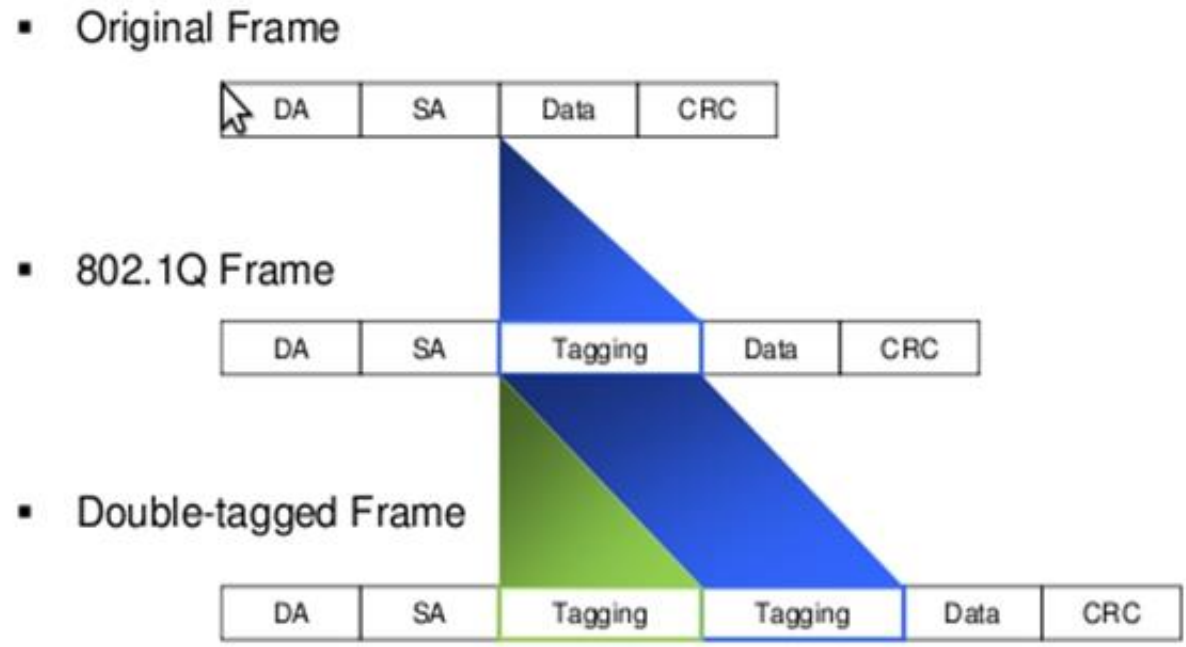

Рис. 1.6. Порівняння форматів пакетів [6]

Однією з переваг цього рішення є те, що його легко реалізувати, вам не потрібне дороге та ексклюзивне обладнання і нам не потрібно запускати будь-які протоколи маршрутизації між постачальником послуг і клієнтом (на відміну від MPLS VPN). З точки зору клієнта, це так само, ніби їхні сайти безпосередньо підключені до рівня 2 [7].

Приклад технології Q-in-Q можна відобразити таким способом.

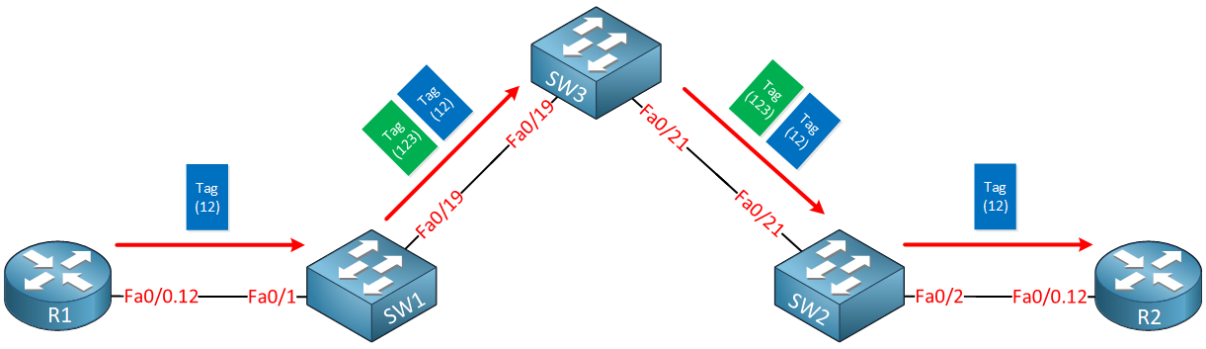

Рис. 1.7. Приклад технології Q-in-Q [7]

Кількість 802.1q VLAN = 4094. При використанні Double VLAN ми отримуємо 4094*4094 = 16,760,836 VLAN [6].

За винятком відсутності потреби узгодження тегів VLAN, дана технологія надає варіант збільшити у великій кількості VLAN в загалому.

QinQ робить структуру операторської мережі гнучкішою. Ви можете визначити для різних клієнтів різні зовнішні VLAN-теги, що передаються в операторській мережі, за якими в ній будуть застосовуватися різні політики QoS. Частина клієнтських потоків може зовсім не інкапсулюватися і передаватися в операторську мережу «як є» [9].

Формат кадру технології додає 32-бітове поле між вихідною MAC-адресою та полями EtherType вихідного кадру. Відповідно до 802.1Q мінімальний розмір кадру залишається 64 байт, але міст може збільшити мінімальний розмір кадру з 64 до 68 байтів при передачі. Це дозволяє легко вставляти мітку без додаткових відступів, а максимальний розмір кадру збільшений з 1518 до 1522 байтів. Два байти використовуються для ідентифікатора протоколу тега (TPID), два інших байти - для управління тегом (TCI). Поле TCI поділяється на PCP, DEI та VID [10].

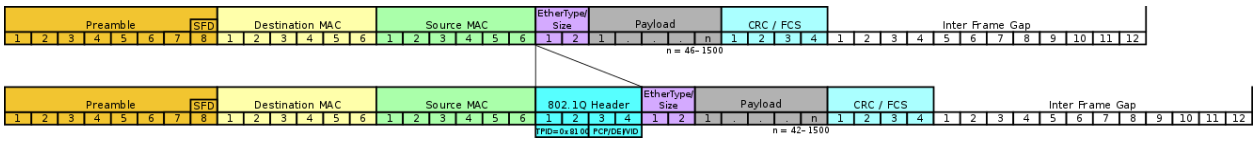

Рис. 1.8. Вставка тега 802.1Q у кадрі Ethernet [10]

Пакети QinQ мають фіксований формат. В основному пакет з тегом 802.11Q інкапсулюється в інший тег 802.1Q, від якого саме і походить назва «QinQ». Під час передачі пакети пересилаються на основі зовнішнього тегу VLAN у загальнодоступній мережі. Внутрішній тег VLAN приймається як дані, які також передаються в загальнодоступній мережі. У цій формі подвійного тега пакети QinQ мають на чотири байти більше, ніж звичайні пакети з тегами 802.1Q VLAN [10].

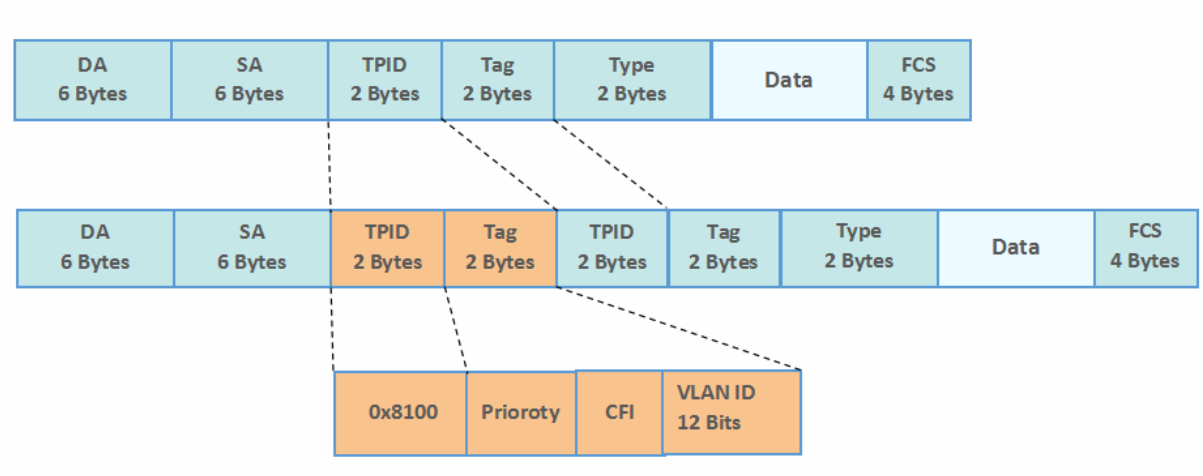

Рис. 1.9. Формат кадру Q-in-Q [10]

Тунелювання 802.1Q відмінно виконує свою роботу для комутації пакетів 2-го рівня, є несумісність між деякими функціями 2-го рівня та комутацією 3-го рівня.

- Тунельний порт не може бути маршрутизованим портом.
- IP-маршрутизація не підтримується у VLAN, яка містить порти 802.1Q. Пакети, отримані з тунельного порту, пересилаються лише на основі інформації рівня 2.
- Тунельні порти не підтримують списки контролю доступу IP
- Групи портів EtherChannel сумісні з тунельними портами, якщо конфігурація 802.1Q узгоджена з групою портів EtherChannel.
- Протокол агрегації портів , протокол керування агрегацією каналів і однонаправлене виявлення каналів (UDLD) підтримуються на тунельних портах 802.1Q.
- Протокол динамічної транкингу не сумісний з тунелюванням 802.1Q, оскільки необхідно вручну налаштувати асиметричні зв'язки з тунельними портами та портами магістралі.
- Виявлення петлі підтримується на тунельних портах 802.1Q.
- Коли порт налаштовано як тунельний порт 802.1Q, на інтерфейсі автоматично вмикається фільтрація блоку даних протоколу зв’язного мосту [11].

Q-in-Q VLAN Tag Termination просто додає ще один рівень тегу IEEE 802.1Q (так званий «тег метро» або«PE-VLAN») до пакетів із тегами 802.1Q, які надходять у мережу. Мета завершення тегу полягає в тому, щоб розширити простір VLAN шляхом тегування пакетів із тегами, створюючи кадр з подвійними тегами. Розширений простір VLAN дозволяє постачальнику послуг надавати певні послуги, наприклад, доступ до Інтернету в певних VLAN для певних клієнтів, і все ж дозволяє постачальнику послуг надавати інші види послуг для інших своїх клієнтів в інших мережах VLAN [12].

IEEE 802.1Q визначає протокол реєстрації кількох VLAN (MVRP), додаток протоколу множинної реєстрації , що дозволяє мостам узгоджувати набір VLAN, які будуть використовуватись за певним каналом. MVRP замінив повільніший протокол реєстрації GARP VLAN (GVRP) у 2007 році з поправкою IEEE 802.1ak-2007 [10].

Вихідні ідентифікатори VLAN 4096 на основі 802.1Q не можуть задовольнити цю потребу. QinQ може просто розширювати такі ідентифікатори, і в той же час він може використовувати різні VLAN, щоб розрізняти послуги оператора та різних клієнтів. Використання QinQ для надання доступу має такі переваги:

- може вирішити дефіцитну проблему ресурсів VLAN ID загальнодоступної мережі;
- Користувачі можуть планувати власний ідентифікатор VLAN у приватній мережі, не викликаючи конфліктів з ідентифікатором VLAN у загальнодоступній мережі;
- Забезпечити відносно просте рішення VPN рівня 2;
- Зробити мережу користувача більш незалежною. Коли постачальник послуг модернізує мережу, мережа користувача не потребує зміни вихідної конфігурації;
- Різні послуги можна розрізнити за VLAN ID різного рівня;

- QinQ може бути вкладений у кілька рівнів технічно без обмежень, обмежений лише довжиною повідомлення Ethernet, має гарну масштабованість [25].

QinQ можна реалізувати двома способами:

1. Базовий QinQ
   - Якщо отримано пакет із тегом VLAN, він стає пакетом із подвійними тегами.
   - Якщо отримане повідомлення не має тега VLAN, повідомлення стає повідомленням з тегом VLAN за промовчанням для порту.
2. Гнучкий QinQ
   - Додаючи різні теги зовнішньої VLAN до пакетів із різними внутрішніми ідентифікаторами VLAN.
   - Позначаючи пріоритет 802.1p зовнішньої VLAN відповідно до пріоритету 802.1p внутрішньої VLAN повідомлення та додаючи інші теги зовнішньої VLAN.

Завдяки використанню гнучкої технології QinQ, будучи здатним ізолювати мережі операторів та користувачів, він також може надавати багаті сервісні функції та гнучкіші мережеві можливості [28].

На наступних рисунках зображено приклад налаштування Q-in-Q в реалізації Port-based та Selective.

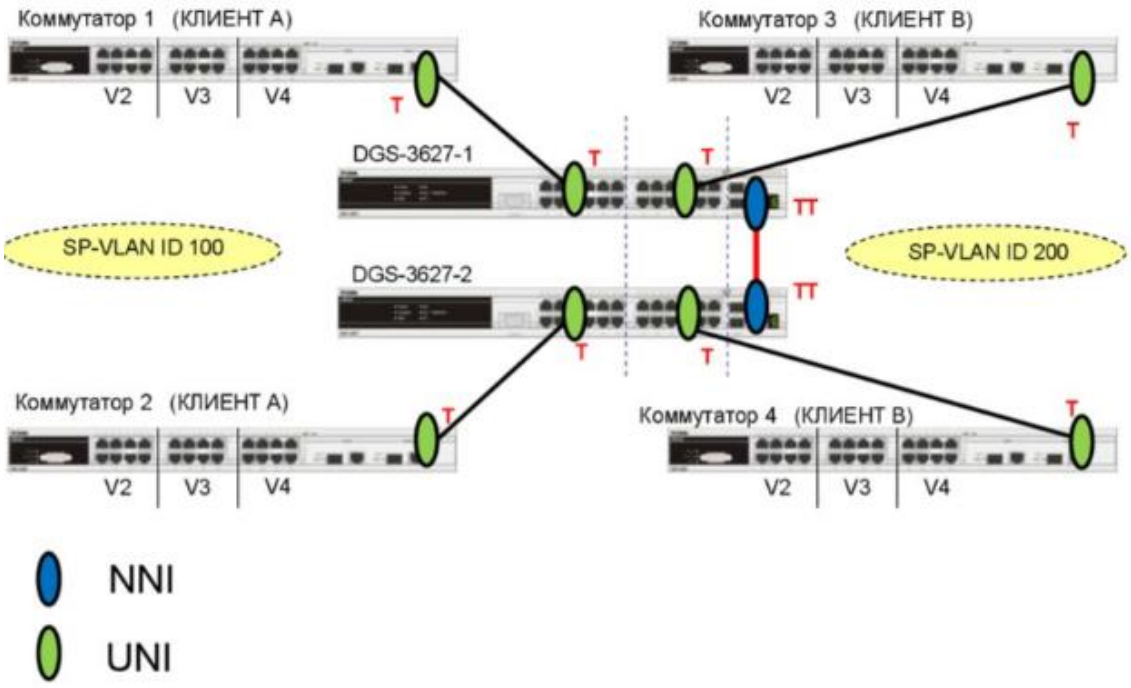

Рис. 1.10. Налаштування Q-in-Q у форматі Port-based [34]

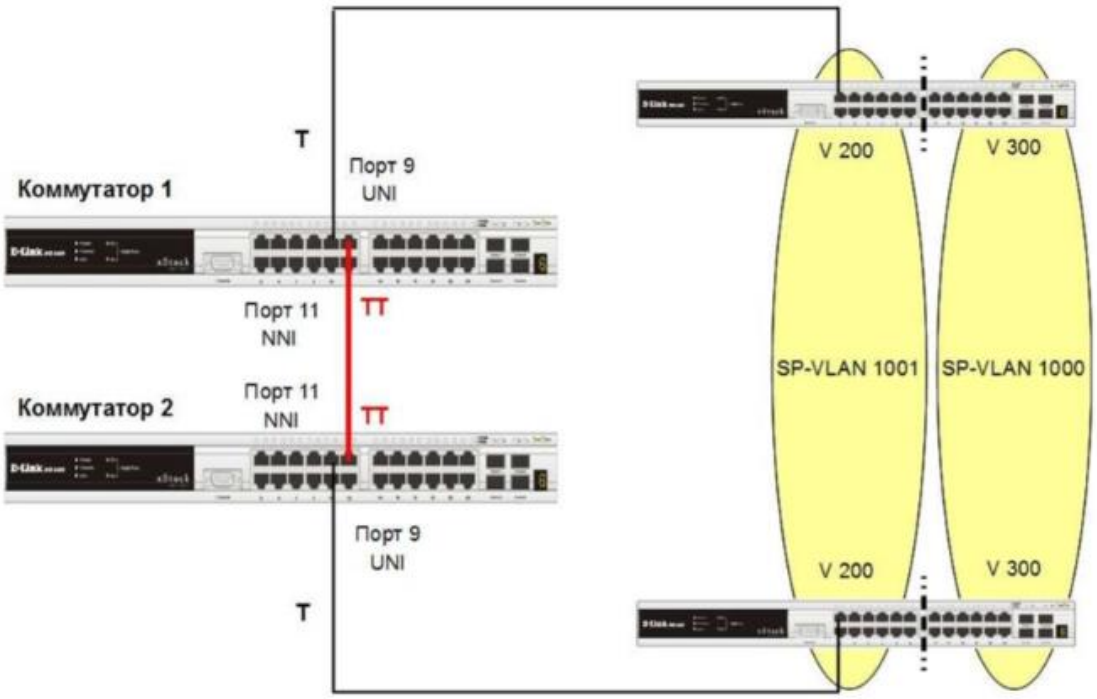

Рис. 1.11. Налаштування Q-in-Q у форматі Selective [34]

1.3 Стандарт IEEE 802.1ah – “Mac-in-Mac”.

Мости Provider Backbone Bridges (PBB ; відомий як «mac-in-mac») - це набір архітектури та протоколів для маршрутизації через мережу провайдера, що дає можливість з'єднувати кілька мереж Provider Bridge Network без втрат індивідуально визначених VLAN кожного клієнта. Спочатку він був створений Nortel, а потім передано до комітету IEEE 802.1 для стандартизації. Остаточний стандарт був схвалений IEEE у червні 2008 року як IEEE 802.1ah-2008 та був інтегрований у IEEE 802.1Q-2011 [13].

Основними концепціями технології на основі мережі є:

- мережа, яка використовує MAC-in-MAC, називається мережею магістрального мосту постачальника або мережею MAC-in-MAC. Для користувачів PBBN — це комутаційна мережа рівня 2, де з’єднання рівня 2 знаходяться між різними вузлами.
- мережа, що з'єднує PBBN з мережею клієнта, є мережею моста постачальника. Мережа клієнта може підключатися до PBBN безпосередньо або через PBN.
- опорний крайовий міст є граничним пристроєм у PBBN, як пристрій PE в мережі MPLS. BEB інкапсулює кадри з мережі клієнта за допомогою MAC-in-MAC або деінкапсулює кадри MAC-in-MAC з PBBN і пересилає їх до мережі клієнта.
- магістральний базовий міст є основним пристроєм у PBBN, як пристрій P у мережі MPLS. Він пересилає кадри MAC-in-MAC відповідно до їхніх B-MAC і B-VLAN [14].

На наступному рисунку показана типова мережа для технології Mac-in-Mac.

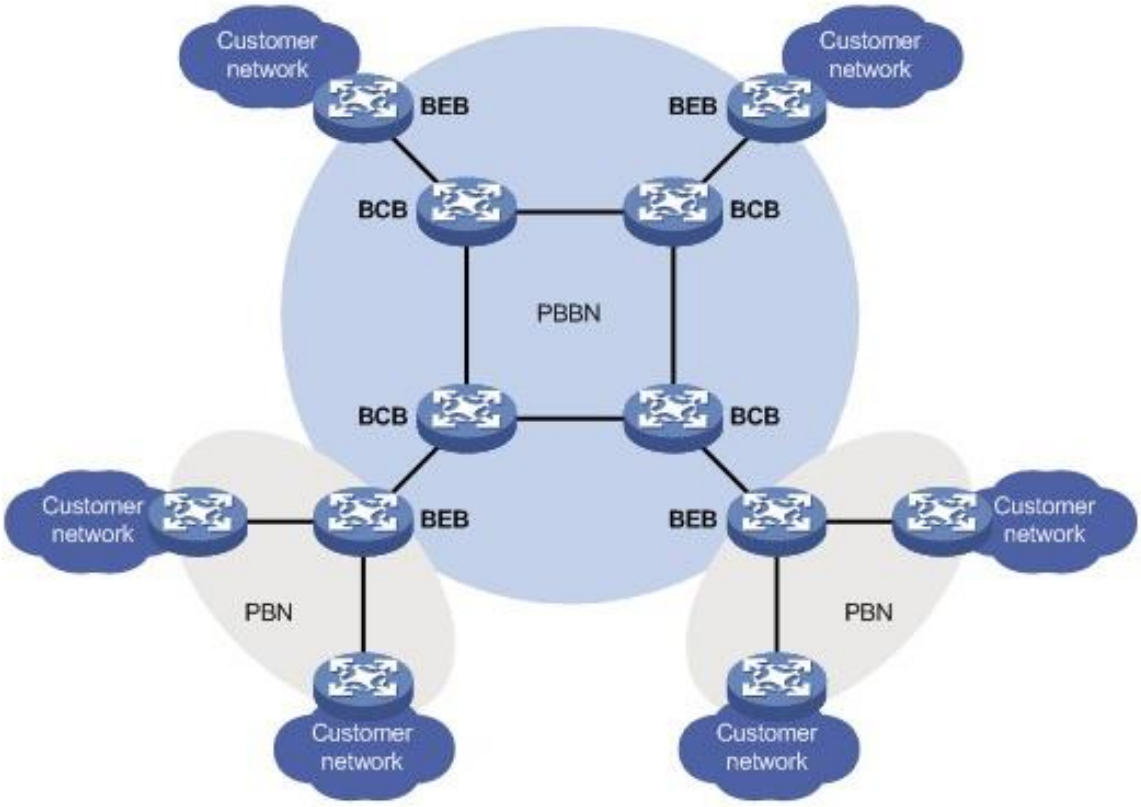

Рис. 1.12. Архітектура мережі Mac-in-Mac [14]

Передбачається, що мережа PBB провайдера приймає кадри від мереж PB (можливо іншого провайдера), які, у свою чергу, з'єднані з мережами користувача. У цьому випадку інтерфейси між мережею PBB та мережами PB звуться NNI (Network to Network Interface — інтерфейс «мережа-мережа»). У кадрах, що надходять на прикордонні комутатори мережі PBB є ідентифікатор S-VID, доданий вхідним прикордонним комутатором мережі PB (і не віддалений вихідним прикордонним комутатором мережі PB, так як таке видалення виконується для інтерфейсів UNI, але не для інтерфейсів NNI). Наявність ідентифікатор S-VID у вхідних кадрах не є необхідною умовою роботи мережі PBB, це лише можливий варіант; якщо мережа PBB безпосередньо з'єднує мережі користувачів, вхідні кадри поля S-VID не мають [15].

Іншим основним застосуванням 802.1ah Backbone Edge Bridges є зменшення кількості MAC-адрес, які необхідно вивчити в ядрі

мережі. Розмір таблиці MAC-адрес є основною проблемою для існуючих мереж VPLS, і використання інкапсуляції 802.1ah на кордоні з підключеною мережею доступу дуже ефективне для вирішення цієї проблеми [33].

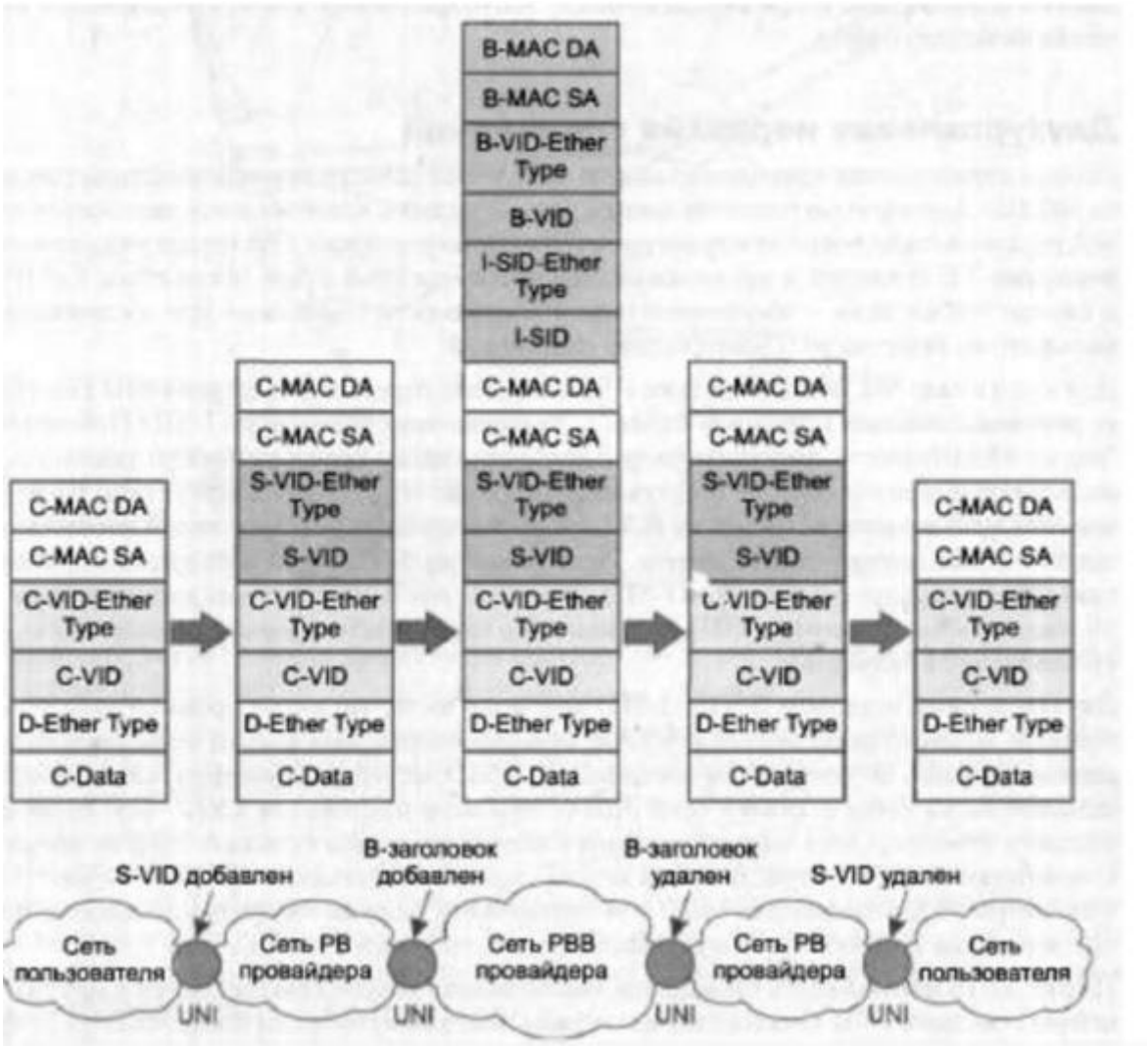

Рис. 1.13. Формат кадрів при інкапсуляції [15]

Ідея Mac-in-Mac полягає в тому, щоб запропонувати повне розділення доменів клієнтів та постачальників. Для цього був визначений новий заголовок Ethernet. Він може мати різні форми, але основними компонентами заголовка є основний компонент, який має:

- Магістральна адреса призначення (B-DA) (шість байтів);
- Адреса вихідної основи (B-SA) (шість байт);
- EtherType 0x88A8 (два байти);

- B-TAG / B-VID (два байти), це індикатор магістральної VLAN;

Інкапсуляція послуги, яка має:

- EtherType 0x88E7 (два байти);
- Прапори, що містять пріоритет, індикатор допустимого падіння (DEI) та індикацію відсутності адреси клієнта (NCA) (наприклад, кадри OAM).;
- I-SID, ідентифікатор служби (три байти);

Оригінальний кадр замовника:

- Адреса призначення клієнта (шість байт);
- Адреса джерела клієнта (шість байт);
- EtherType 0x8100 (два байти);
- Ідентифікатор VLAN клієнта (два байти);
- EtherType (наприклад, 0x0800);
- Корисне навантаження клієнта [16].

Коли IEEE 802.1ah налаштовано на мережі Ethernet через багатопротокольну комутацію міток (EoMPLS), канали Ethernet транспортуються як псевдодроти, використовуючи шляхи з комутацією міток MPLS (LSP) всередині тунелю MPLS. Щоб налаштувати MAC-in-MAC в мережах EoMPLS, ви повинні вказати параметри конфігурації EFP для входу в UNI, вказати параметри MAC-in-MAC та вказати параметри конфігурації віртуального інтерфейсу комутатора (SVI) на вихідному NNI. SVI являє собою VLAN портів комутатора, підключених до мосту через єдиний інтерфейс.

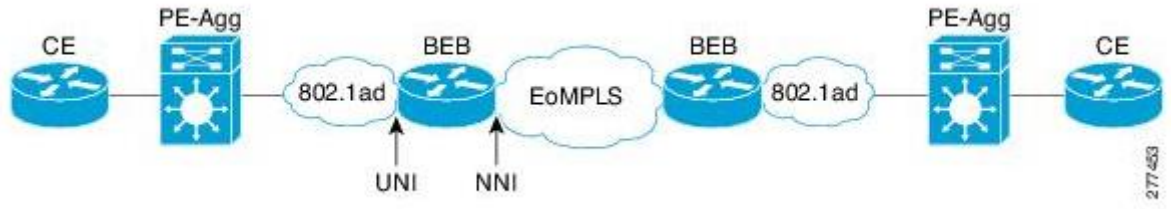

Рис. 1.14. Мережа Mac-in-Mac EoMPLS [32]

На рисунку що нижче, зображено перегляд мережі Mac-in-Mac:

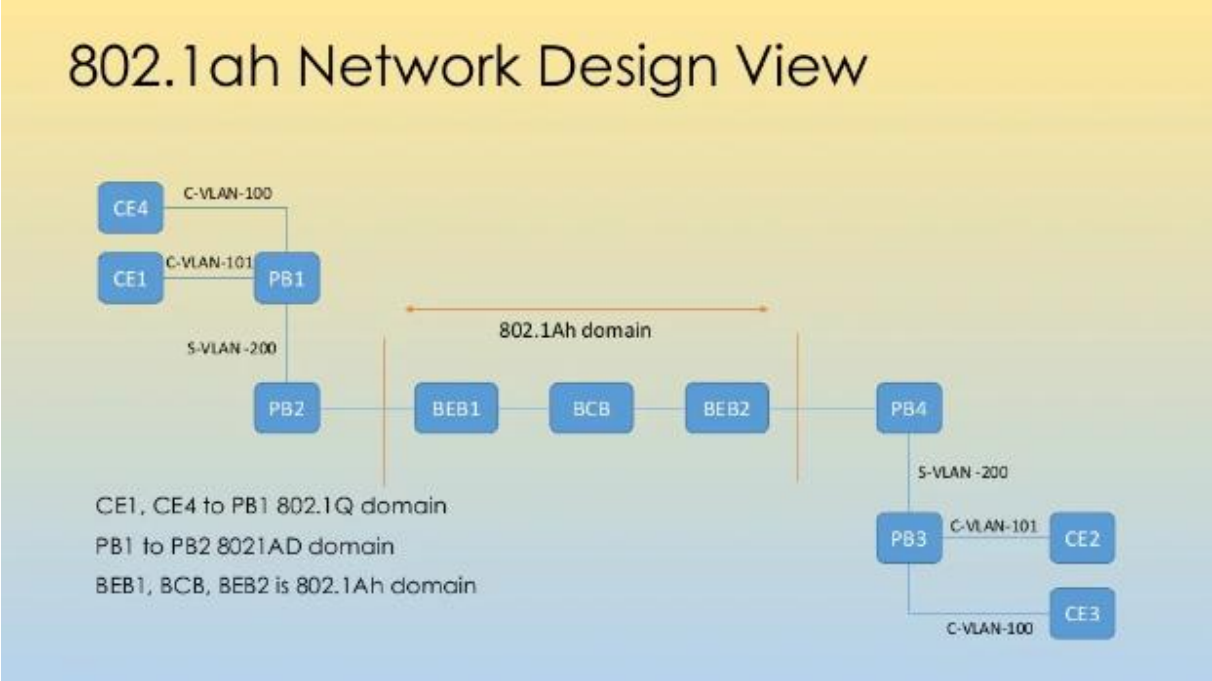

Рис. 1.15. Проєктування мережі 802.1ah [29]

1.4 L2VPN MPLS в Carrier Ethernet

L2VPN 2 забезпечує повний поділ між мережами постачальника та клієнта. Переваги VPN рівня 2 містять підтримку нестандартних транспортних протоколів та ізоляцію адресації з'єднань функціонування протоколу маршрутів між клієнтом та провайдером [17].

Існують різні види L2VPN, а саме:

- VLAN/QinQ - їх можна сюди віднести, оскільки основні вимоги VPN виконуються - організовується віртуальна мережа L2 між декількома точками, дані в якій ізольовані від інших. Насправді VLAN per-user організує Hub-n-Spoke VPN.
- L2TPv2/PPTP - застарілі та нудні речі.
- L2TPv3 разом із GRE мають проблеми з масштабуванням.
- VXLAN, EVPN - варіанти для ЦОД'ів.
- MPLS L2VPN – це набір різних технологій, транспортом для яких є MPLS LSP. Саме він зараз набув найширшого поширення в мережах провайдерів [19].

На малюнку нижче показано MPLS-базу провайдера, який надає послуги L2VPN.

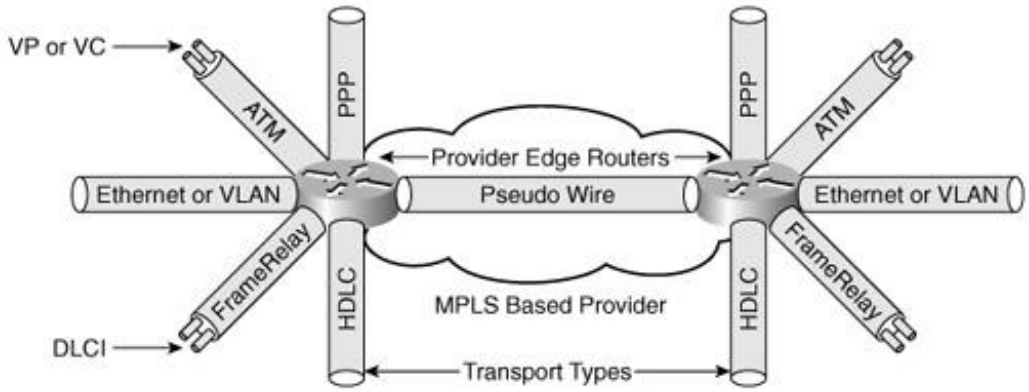

Рис. 1.16. L2VPN з боку провайдера [19]

Основна відмінність між L2VPN та L3VPN полягає у функції комутації та маршрутизації. Комутатор L2 працює тільки з MAC-адресами і не дбає про IP-адреси або будь-які елементи вищого рівня. Але комутатор L3 чи багаторівневий комутатор підтримує всі функції управління L2 [20].

Для побудови будь-якого L2VPN існують два концептуально різні підходи.

- Point-to-Point . Застосуємо до будь-яких типів протоколів канального рівня і в принципі повною мірою вичерпує всі сценарії застосування L2VPN. Підтримує всі мислимі та немислимі протоколи. Причому деякі ще й по-різному може реалізовувати .

  В основі лежить концепція PW – PseudoWire – псевдопровід.

Загальна назва послуги: VPWS - Virtual Private Wire Service [18].

- Point-to-Multipoint . Цей режим лише для Ethernet, оскільки лише в ньому фактично така потреба є. У цьому випадку у клієнта може бути три, п'ять, десять, сто та більше точок підключення і всі вони повинні передавати дані один одному, причому як одному конкретному філії, так і всім відразу. Це нагадує звичайний Ethernet-комутатор. Назва технології: VPLS - Virtual Private LAN Service [18].

Припустимо, ви приватний підприємець, у вас є офіс у м. Київ та м. Суми. Ви хочете об'єднати 2 мережі в 1 велику локальну мережу. З погляду вас (клієнта) дана послуга буде виглядати так, як показано на рисунку нижче [21].

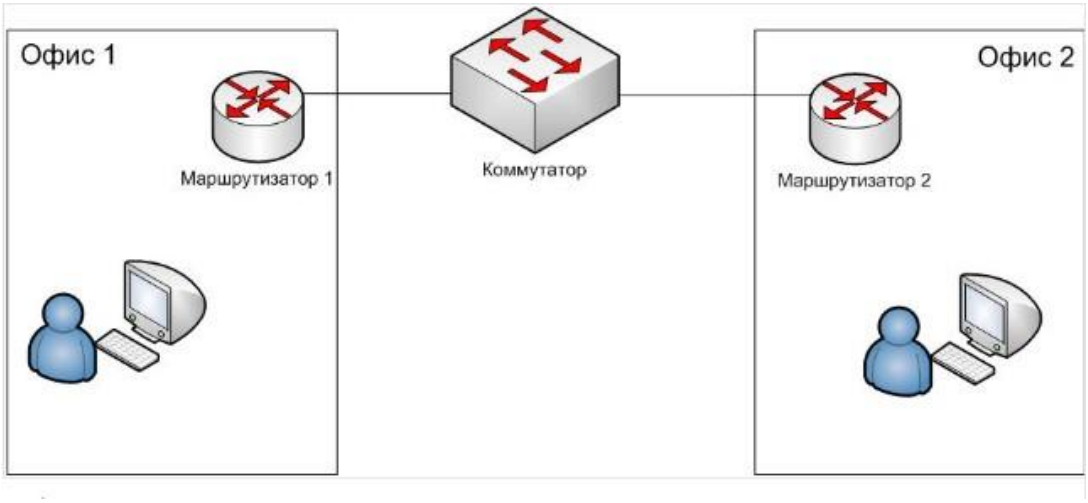

Рис. 1.17. Архітектура L2VPN мережі [21]

На малюнку що внизу, показано імена інтерфейсів, IP-адрес та протоколів, що використовуються в мережі провайдера. Також виділено end-to-end-характер адресації Carrier Ethernet та роботи стеку протоколів. На відміну від L3VPN, Carrier Ethernet пристрій працює в режимі opaque для мережі провайдера в L2VPN. Між двома пристроями та мережею Carrier Ethernet провайдера рівноправні зв'язку немає. В результаті очікується, що Carrier Ethernet пристрої сформують OSPF по всій мережі провайдера, а не до іншої [17].

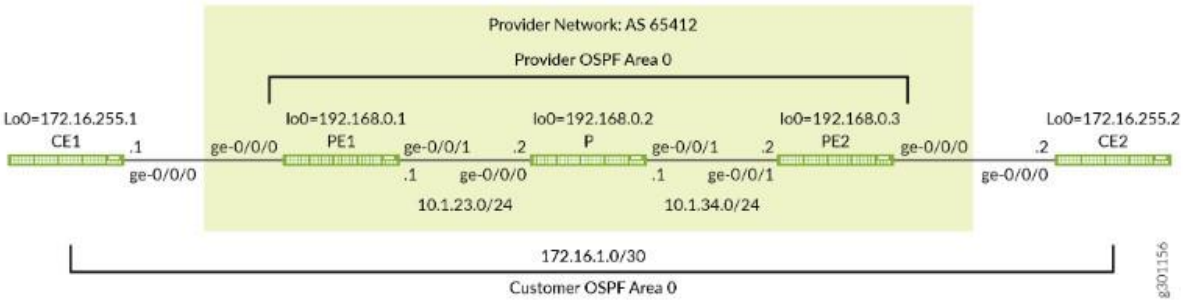

Рис. 1.18. MPLS L2VPN на основі багаторівневої мережі [17]

Послуга L2VPN є однією з найпопулярніших серед клієнтів провайдерів. Вона дуже проста і не вимагає налаштувань на обладнанні клієнта.

На рисунку нижче зображена структура кадру Ethernet, змінюючись при організації VLAN компанії та при організації тунелю на магістралі

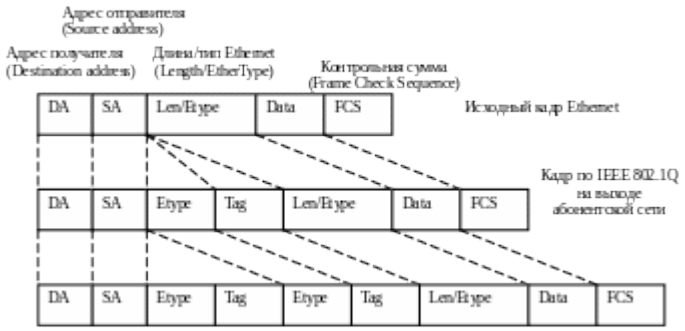

Рис. 1.19. Формат міток L2 VPN на VLAN [31]

Видно, що стандартний кадр Ethernet (верхня частина малюнка) під час створення VLAN за стандартом IEEE 802.1Q доповнюється двома полями: Etype (скорочення від EtherType) і Tag, де у першому полі вказується тип протоколу обробки кадру, тоді як у другому вноситься мітка (tag), що відповідає номеру VLAN усередині корпорації. На нижній частині малюнка показана структура кадру при тунелюванні, де значення тега відповідає номер тунельного порту.Таким чином, шляхом створення тунелів на магістралі, дані віртуальних локальних мереж різних компаній оброблятимуться окремо навіть за відповідних внутрішніх номерів [31].

Псевдодроти вимагають, щоб вхідні та вихідні пристрої PE використовували звичайні специфічні для служби методи для інкапсуляції даних рівня 2 клієнта. Вхідний PE інкапсулює дані відповідно до пропозиції проєкту , додає мітку віртуального каналу (VC) та тунельну мітку та пересилає пакет через LSP [33].

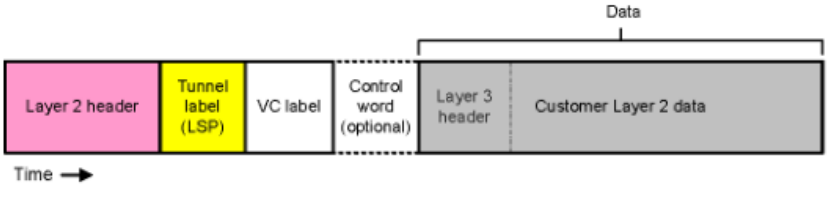

Рис. 1.20. Інкапсуляція даних відповідно проєкту [33]

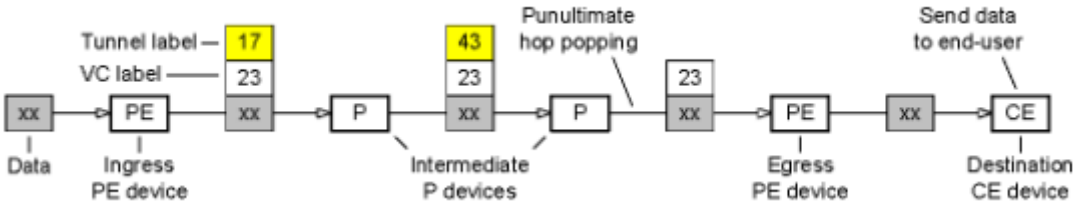

Рис. 1.21. Транспортування пакету L2 VPN через MPLS [33]

Коли пакет MPLS надходить до вихідного PE, вихідний PE використовує мітку VC для доставки даних на правильний пристрій CE з відповідною інкапсуляцією рівня 2 [33].

Переваги другого рівня VPN:

- прискорений обмін файлами та повідомленнями всередині мережі;
- висока безпека передачі;
- спільна робота над документами та базами даних;
- доступ до корпоративних інформаційних http - серверів;
- організація між офісами високоякісного відеозв'язку та відео трансляцій

Проте є недоліки. Так як. послуга є L2, то операторам зв'язку дуже складно відслідковувати проблеми на цій послузі і практично вони дізнаються про проблему від клієнта. По суті, клієнт сам бере на себе всю діагностику та роботу з провайдером, тому якщо існують якісь проблеми, то їх вирішення ускладнюється та затягується в часі [21].

Якщо ви маєте лише домен L2, ви можете перейти на L2. У чистому домені L2 - де хости пов'язані, комутатор L2 працюватиме добре. Зазвичай у топології мережі це називається рівнем доступу до мережі. Якщо вам потрібний комутатор для об'єднання кількох комутаторів доступу та маршрутизації між віртуальними локальними мережами, тоді потрібний комутатор L3 [20].

На рисунку відображена таблиця комутаторів, що надає змогу обрати необхідний комутатор в залежності від поставлених задач.

Рівень керування комутатора	Layer 2	Layer 2+	Layer 3
Функції комутації	MAC адреса	MAC адреса	IP апаратне перемикання адрес
802.1x, ACL, DHCP відстеження безпеки		✓	✓
Функція з'єднання сполучного дерева		✓	✓
VLAN маркування на основі IP адреси		✓	✓
Inter-VLAN		✓	✓

Рис. 1.22. Таблиця порівнянь комутаторів [20]

Також, на рисунку внизу представлена таблиця порівнянь L2 та L3 VPN, яка дозволяє розібратися в необхідності рівня VPN, в залежності від потреби.

ФІЛОСОФІЯ	VPN рівня 2 віртуалізують рівень каналу передачі даних (рівень 2), щоб географічно віддалені сайти виглядали так, ніби вони працюють в одній локальній мережі.	VPN рівня 3 віртуалізують мережевий рівень (рівень 3), щоб маршрутизувати мережі ваших клієнтів через загальнодоступну інфраструктуру, як-от Інтернет або магістраль постачальника послуг.
ПЕРЕСПЕРЕЖЕННЯ ТРАФІКУ	Пристрої постачальника пересилають трафік клієнтів на основі інформації рівня 2.	Пристрої постачальника пересилають трафік клієнтів на основі інформації рівня 3.
МАСШТАБОВАНІСТЬ	Як правило, VPN рівня 2 менш масштабовані, ніж VPN рівня 3.	Як правило, VPN рівня 3 більш масштабовані, ніж VPN рівня 2.
ЗВ'ЯЗНЕННЯ РІВЕНЬ 3	Клієнт здійснює підключення рівня 3 (IP) з віддаленими сайтами клієнтів, а не з постачальником послуг.	Клієнт створює підключення рівня 3 (IP) із периферійними пристроями сайтів провайдера.
УЧАСТВО ПОСТАВЩИКА ПОСЛУГ	Постачальник послуг не бере участі в IP-маршрутизації підмереж клієнта.	Постачальник послуг бере участь у IP-маршрутизації підмереж клієнта.
КОНТРОЛЬ МАРШРУТИЗАЦІЇ	Переважний підхід, коли клієнт хоче, щоб усе управління маршрутизацією та політикою було під його управлінським контролем.	Переважний підхід, коли клієнт може поділитися інформацією про маршрутизацію з постачальником послуг, а контроль політики не такий суворий.
ПРИКЛАДИ	LANE, IPLS, VPLS, EOMPLS, 802.1q Тунелювання	MPLS VPN, IPSEC P2P

Рис. 1.23. Таблиця відмінностей L2 і L3 VPN [24]

З точки зору мережевої безпеки, технології MPLS L2 VPN пропонують новий рівень захисту мережевого трафіку. Незважаючи на те, що пакети передаються по опорній мережі, що розділяється, через рознесення мережевих префіксів у різні маршрутні таблиці трафік однієї VPN-мережі виходить ізольованим в рамках кожного маршрутизатора — ще до застосування до нього (трафіку) правил просування пакетів і тим більше до реалізації правил традиційної бар'єрної, політики мережевої безпеки. В результаті атаки типу "відмова в обслуговуванні", а також атаки з використанням уразливостей прикладного ПЗ у принципі не можуть бути здійснені ззовні виділеної мережі MPLS VPN. Трафік такої атаки просто не дійде до мети [26].

1.5 Постановка задачі

При проведенні аналізу та збору інформації можна розпланувати етапи виконання практичних чистин кваліфікаційної роботи бакалавра.

1. В симуляторі GNS3 змоделювати, налаштувати та провести аналіз переміщення пакетів по мережі Carrier Ethernet за технологією Q-in-Q.
2. Створення графічного інтерфейсу Carrier Ethernet для оптимізації налаштування подібних мереж. Оптимізація необхідна для того, щоб не маючи відповідних навичок та досвіду в налаштуванні мереж, було можливим їх налаштування максимально просто та ефективно. Готовий графічний інтерфейс має бути зручним, зрозумілим, простим та легким для роботи з мережами.

РОЗДІЛ 2 МОДЕЛЮВАННЯ ТА НАЛАШТУВАННЯ МЕРЕЖІ В СИМУЛЯТОРІ CISCO PACKET TRACER

Моделювання комп'ютерних мереж являється основним напрямком дослідження та вдосконалення телекомунікаційних систем та технологій. Саме вони дають можливості в вивченні нових мереж, створенні нових, та їх тестуванні. Таким способом за допомогою моделювання в емуляторах стає реальним помічником в створенні масштабних мереж для різних компаній, які можуть знаходитися в різних точках світу.

Саме проектування мережі в емуляторах надає можливість оцінити кількість необхідного обладнання, яке, за нагоди, може стати потрібним в реальному житті для їх створення. Емуляція проектів мережі дає зможу проаналізувати стійкість до стресових навантажень, навантаження на мережу, проведення аналізу трафіку, та саме на аналізі робити корегування мереж.

Симулятори мереж надають змогу користувачам уникати багатьох помилок в реальності. В сучасному світі для компаній помилки можуть коштувати дорогоцінного часу та втрачених коштів. Одним з таких симуляторів є GNS3.

GNS3– це потужна програма моделювання мереж, яка дозволяє системним адміністраторам експериментувати з поведінкою мережі та оцінювати можливі сценарії розвитку подій. Цей інструмент доповнює фізичне обладнання, дозволяючи створювати мережі з практично необмеженою кількістю пристроїв, та допомагає отримати практичні навички конфігурування, пошуку та усунення проблем та виявлення пристроїв [22].

Цей емулятор є безоплатним, який можна завантажити з офіційного сайту, зареєструвавшись на ньому симулятор має свої переваги над конкурентами, а саме:

- Моделювання в режимі «реального часу»;

- Надання можливості створення логічних топологій;
- Приємний, дружній, та логічний графічний інтерфейс;
- Багатий на мови інтерфейс емулятора, що додає зручності в використанні;
- Створення шаблонів для використанні в майбутньому;
- Можливість доступного проектування фізичної топології, використовуючи різні поняття такі як офіс, будинок, місто і т.д.

Також, як майже в усіх симуляторів, незважаючи на всі плюси GNS3, є й недоліки:

- Першим, і на мою думку основним недоліком являються глюки емулятора, які можна усунути тільки перезавантаженням додатку. Найбільш популярним з них є мережевий протокол сполучного дерева (STP);
- Неповна емуляція IOS також є недоліком емулятора;
- Апаратна доступність. В GNS3, для його роботи потрібно мінімум 4Гб оперативної пам’яті, коли в свою чергу Cisco Packet Tracer може працювати з 2Гб.

З роками інтерфейс емулятор піддавався змінам, вдосконалювався, та ставав простішим, що в результаті надало для користувача простоту та ясність в використанні емулятора. Всі необхідні для використання інструменти стали згруповані, що навіть для того, хто перший раз запустив GNS3, зміг зрозуміти та почати роботу над моделюванням мережі.

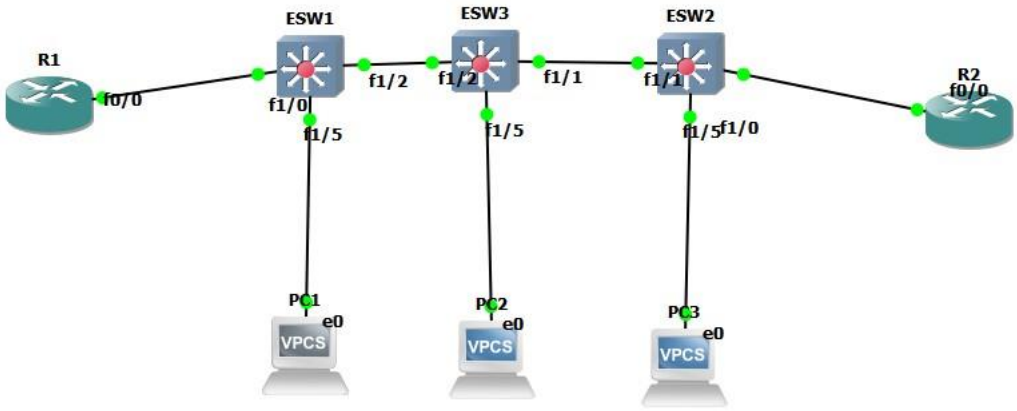

Рис. 2.1. Мережа Q-in-Q

Завдяки симулятору GNS3 була створена операторська мережа за стандартом Q-in-Q. Для неї в ході виконання дипломної роботи буде створено і налаштовано графічний інтерфейс для користувачів.

Для побудови мережі знадобилося обладнання:

1. 3 комутатори;
2. 3 комп’ютери;
3. 2 роутери.

2.1 Налаштування роутерів

Для правильного налаштування роутерів потрібно ввести команди, що зображені на рисунках нижче:

```
en
conf t
int fa 0/0
no sh
int fa 0/0.12
encapsulation dot1Q 12
ip address 192.168.12.1 255.255.255.0
```

Рис. 2.2. Налаштування роутера R1

```
en
conf t
int fa 0/0
no sh
int fa 0/0.12
encapsulation dot1Q 12
ip address 192.168.12.2 255.255.255.0
```

Рис. 2.3. Налаштування роутера R2

2.2 Налаштування комутаторів (switch-ів)

Від налаштування комутаторів залежить правильність роботи мережі. Для цього необхідно ввести відповідно для кожного роутера команди в консоль:

```
en
conf t
int fa 1/2
switchport trunk  encapsulation dot1q
switchport trunk allowed vlan all
switchport mode trunk
ex
vlan 123
name s-vid-123
Switch(config)#int fa 1/0
switchport access vlan 123
switchport mode dot1q-tunnel
```

Рис. 2.4. Налаштування комутатора SW1

```
en
conf t
int fa 1/1
switchport trunk  encapsulation dot1q
switchport trunk allowed vlan all
switchport mode trunk
ex
vlan 123
name s-vid-123
Switch(config)#int fa 1/0
switchport access vlan 123
switchport mode dot1q-tunnel
```

Рис. 2.5. Налаштування комутатора SW2

```
en
conf t
Int fa1/2
switchport trunk encapsulation dot1q
switchport mode trunk
int fa1/1
switchport trunk encapsulation dot1q
switchport mode trunk
ex
```

Рис. 2.6. Налаштування комутатора SW3

2.3 Аналіз мережевого трафіку

Проаналізувавши роботу мережі за допомогою влаштованого в симулятор GNS3 утиліти Wireshark, можна побачити, що дана мережа налаштована вірно, та технологія Q-in-Q повністю реалізована.

Wireshark дозволяє економити час на аналіз пакетів, який можна використати ефективно в іншому руслі роботи. Робота з програмою не створює проблем, є простою для користувачів, що надає можливість новачкам швидше здобувати навички.

Переглянувши через Wireshark на перехоплені пакети в мережі, можна побачити те, що команди спрацювали без помилок, та виконують свою основну функцію, яка є в Q-in-Q.

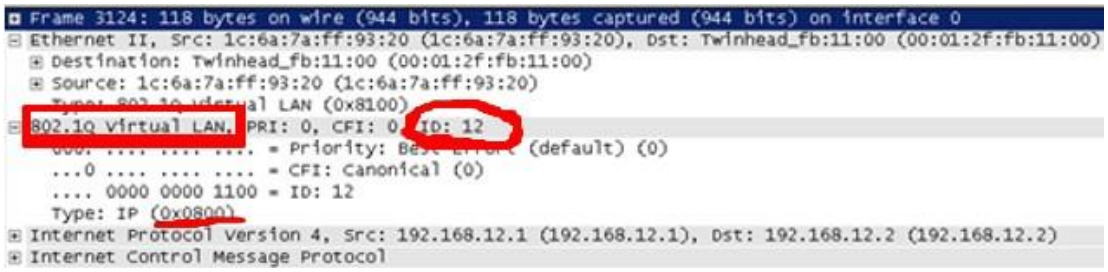

Рис. 2.7. Перехоплений кадр SW1

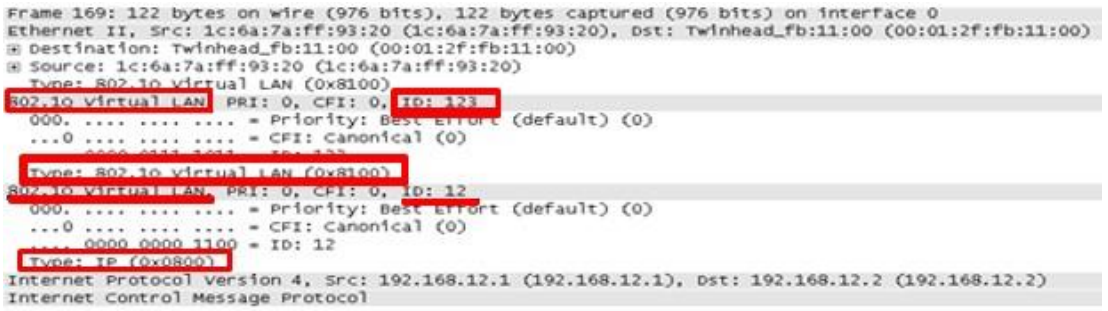

Рис. 2.8. Перехоплений кадр SW2

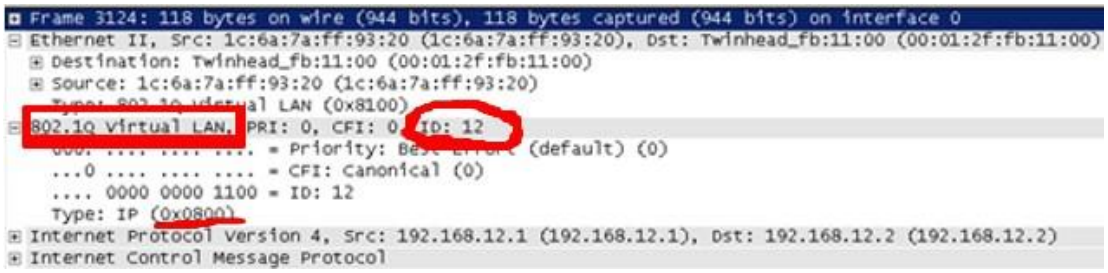

Рис. 2.9. Перехоплений кадр SW3

З рисунків 2.7-2.9 можна сказати, що після аналізу мережі все працює коректно, без нарікань та згідно з правилами технології. Саме правильне групування команд для кожної з частин мережі, надає змогу не робити стандартні помилки, які б можна було зробити, та збільшити час моделювання.

2.4 Побудова графічного інтерфейсу за допомогою мови програмування JavaScript

Основною метою бакалаврської дипломної роботи є графічний інтерфейс, для якого JavaScript, як мова програмування, є одним з основних в виконанні завдань такого плану.

JavaScript (JS) – це повноцінна мова програмування, яка застосовується до HTML документу і дає змогу забезпечити динамічну інтерактивність на веб-ресурсах.

Сама по собі мова програмування є гнучкою, та компактною в одному цілому. Багато інструментів написаних розробниками зверху JavaScript-у, які відкривають велику кількість функцій.

JS займає перше місце в топі мов програмування на Github, що викликає довірю у людей, які хочуть познайомитися ближче з програмуванням та веб-розробкою.

Один з найголовніших факторів під час вибору мови програмування – підтримка JS всіма популярними браузерами. Немалий пріоритет в виборі грав фактор того, що JavaScript відповідає за функціонал, оптимізацію, інтерактивність інтерфейсу, що й потрібно в рамках дипломної роботи.

Завдяки одній з найпопулярніших мов програмування, було побудовано графічний інтерфейс Carrier Ethernet за стандартом Q-in-Q. Завдяки полям можливо змінювати маски та IP-адреси не затруднюючись зі введенням в консоль. Ця функція надає новачкам, та тим, хто не знайомий з мережою, швидко і просто отримати необхідні значення.

РОЗДІЛ 3 СТВОРЕННЯ ГРАФІЧНОГО ІНТЕРФЕЙСУ ДЛЯ НАЛАШТУВАННЯ МЕРЕЖІ CARRIER ETHERNET ЗА СТАНДАРТОМ Q-IN-Q

В попередньому розділі в емуляторі GNS3 було створено модель мережі Carrier Ethernet за стандартом Q-in-Q.

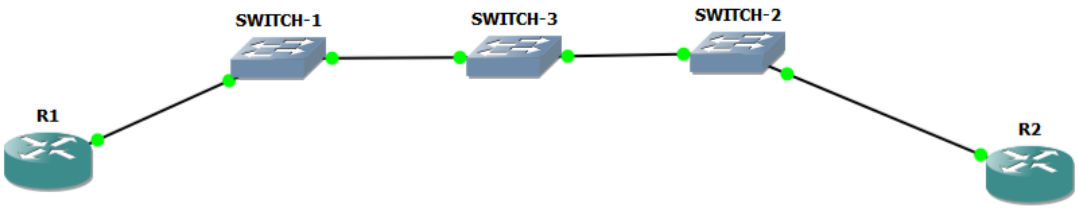

Рис. 3.1. Налаштування стандарту Q-in-Q

Найважчим в створенні мережі є налаштовування роутерів. Складними вони є через IP-адреси та маски, які змінюються від мережі до мережі. Консольні команди є важкими, що затруднює процес створення. Далеко не кожний новачок зможе успішно скласти схему мережі без складних команд роутерів. Для цього потрібно знати послідовність команд, та логіку їх роботи. А можна за допомогою графічного інтерфейсу це все зробити натиском декількох кнопок.

Налаштування комутаторів не беремо до функціоналу інтерфейсу через одноманітність команд для всіх комутаторів. Зі схеми видно, що роутер R1 та R2 однакової моделі, тобто, і налаштування їх однакове.

Графічний інтерфейс був розрозблений для двох роутерів, налаштування яких є змога отримати в окремому вікні після введення маски та IP-адреси.

Інтерфейс вийшов приємний для користувача, та водночас зрозумілий та простий, навіть для того, хто бачить його вперше.

Проєкт, який реалізований задля створення інтерфейсу можна буде переглянути в додатку дипломної роботи.

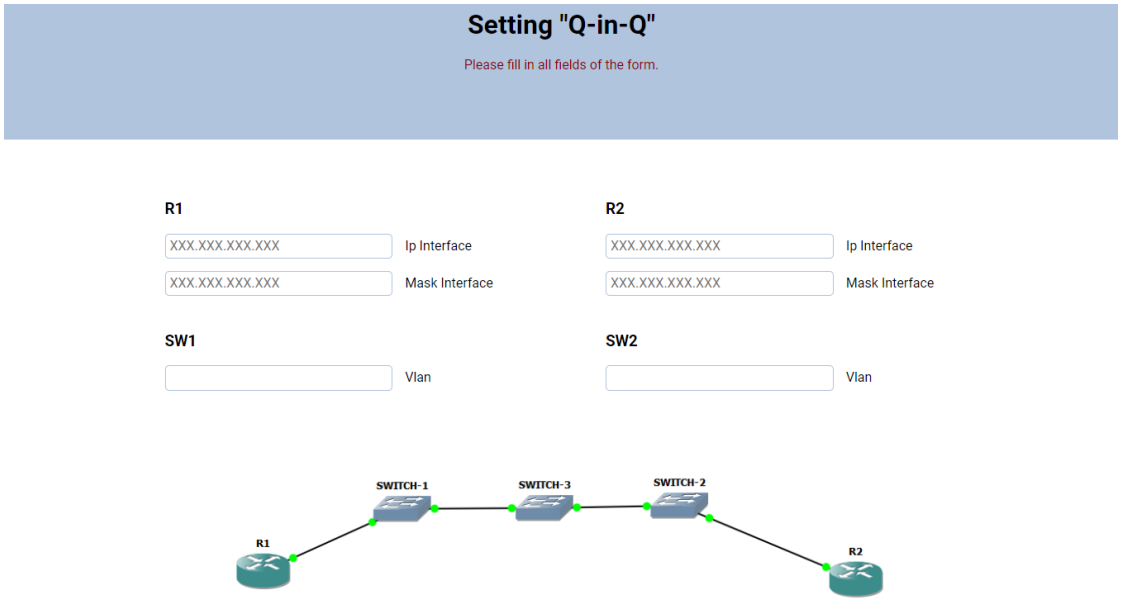

Рис. 3.2. Графічний інтерфейс технології Q-in-Q

На рисунку зображено 6 полів, по два на кожний роутер, а саме Mask Interface та IP Interface. Нижче від них розташовані ще два поля для нумерації VLAN. Зроблені поля для введення даних таким розміром, щоб показати пріоритетність введення значень.

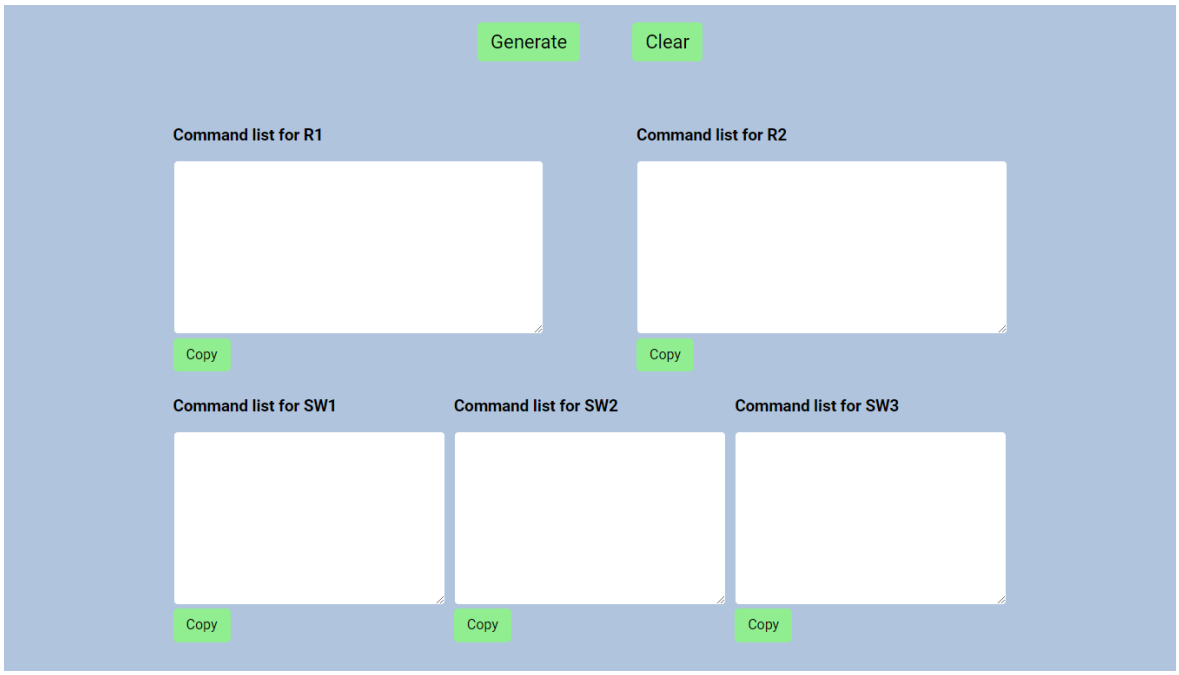

Рис. 3.3. Нижня частина графічного інтерфейсу

В нижній частині знаходять дві кнопки – Generate і Clear. Generate відповідає за генерацію команд після правильного введення в поля для значень, та Clear – очистку всіх полів.

Також необхідною складовою графічного інтерфейсу є валідаційна перевірка введених значень. Якщо значення буде перевищувати норму, або введення невірного формату значень в поля, то користувач інтерфейсу побачить вікно в якому буде вказана, де саме є помилка.

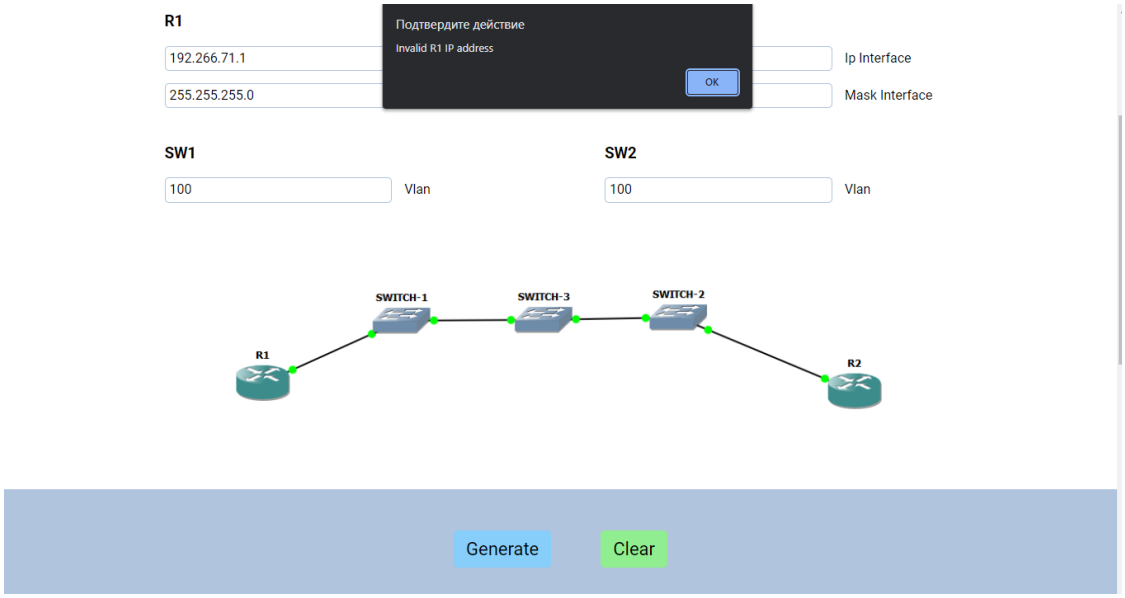

Рис. 3.4. Перевірка валідації на неправильну IP-адресу

Після коректного заповнення даними в поля, потрібно натиснути кнопку Generate.

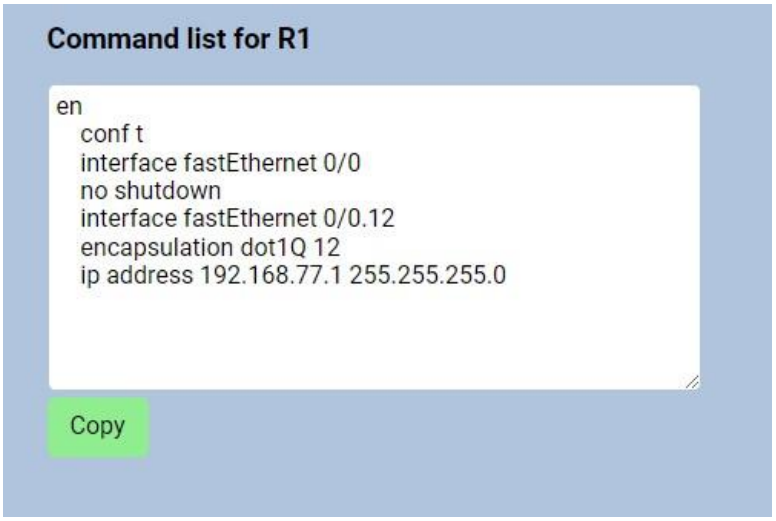

Рис. 3.5. Згенеровані команди для роутера R1

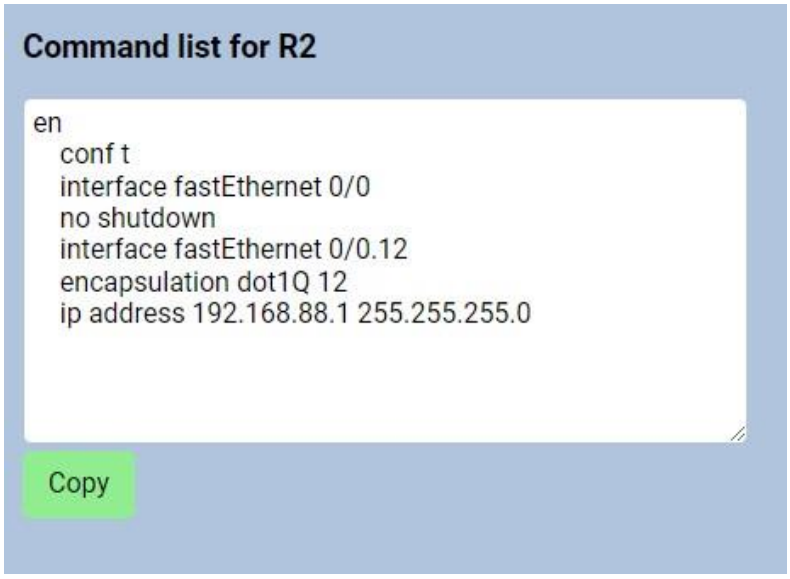

Рис. 3.6. Згенеровані команди для роутера R2

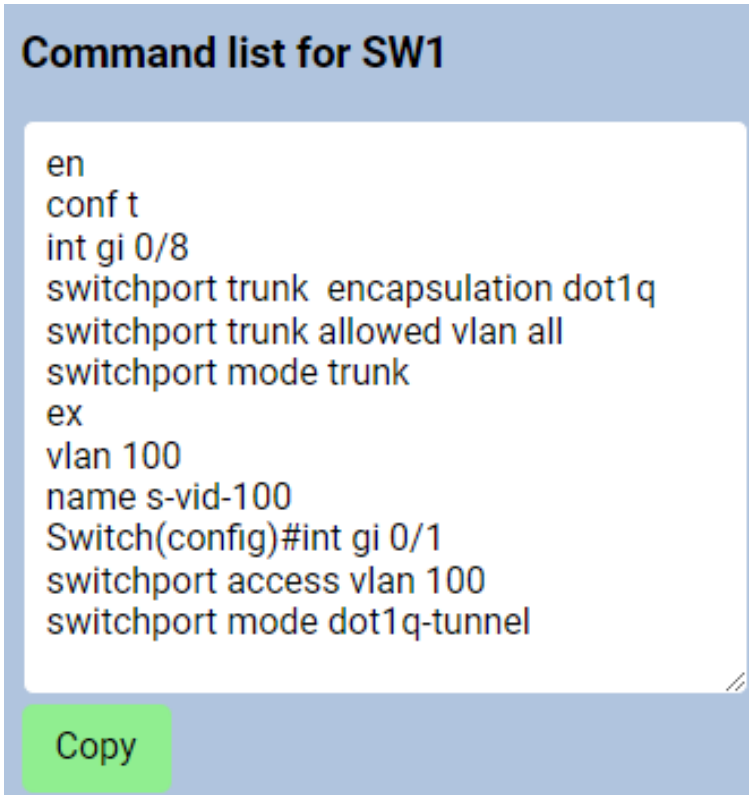

Рис. 3.7. Згенеровані команди для маршрутизатора SW1

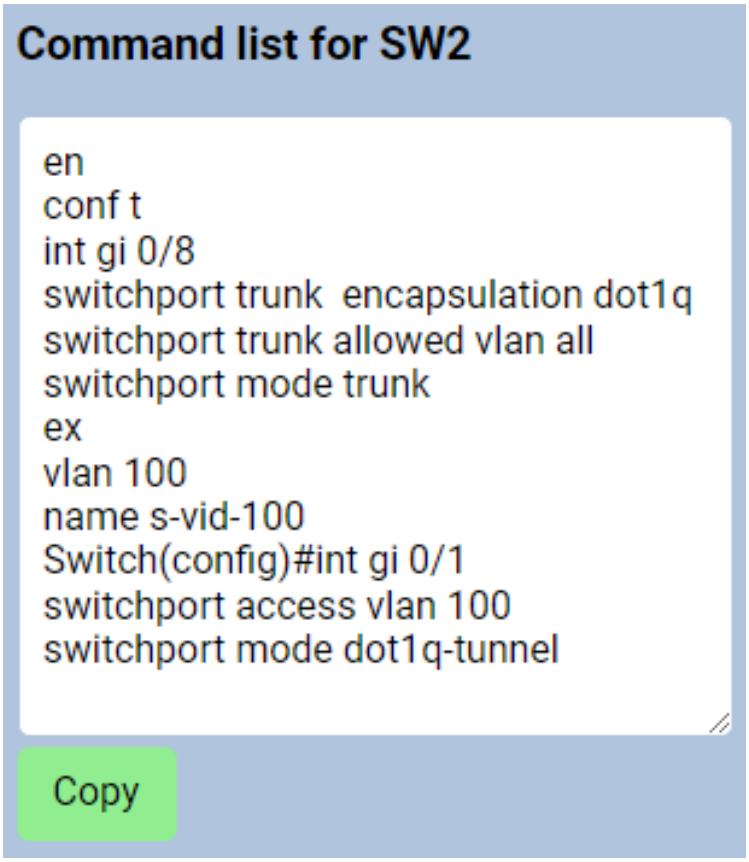

Рис. 3.8. Згенеровані команди для маршрутизатора SW2

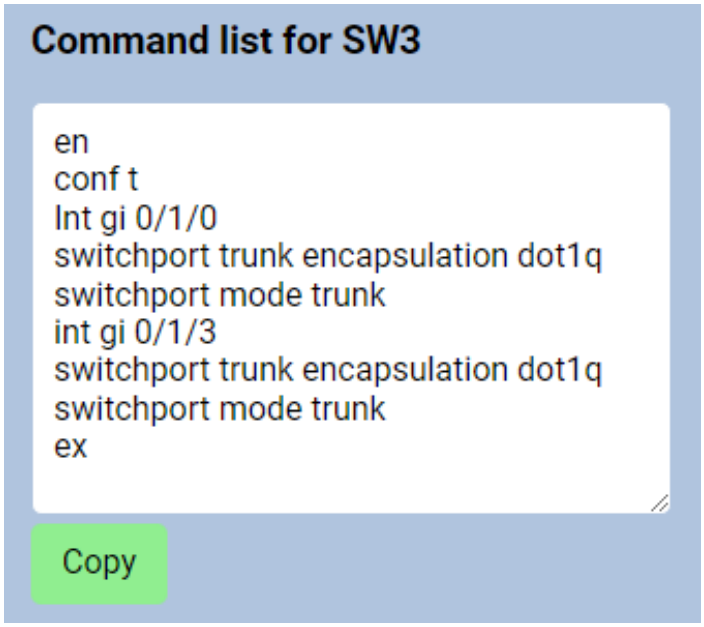

Рис. 3.9. Згенеровані команди для маршрутизатора SW3

З’явилися команди для роутерів, які вже можна використовувати для налаштовування мереж.

На рисунках вище зображені ще дві кнопки Copy, що надають можливості користувачу копіювати команди для кожного роутера окремо одним кліком миші.

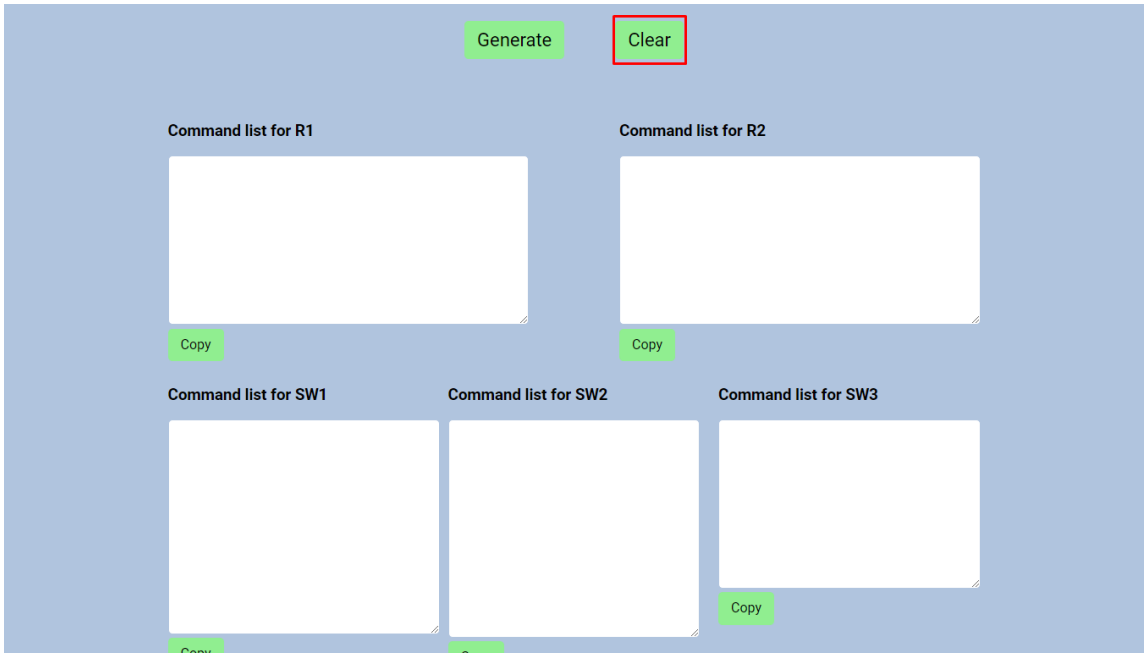

Рис. 3.10. Очищення полів від команд

На рисунку 3.10 зображено роботу кнопки Clear, в порівнянні з рисунком 3.5, що надає можливості користувачу безперервно підставляти адреси в поля, та копіювати команди.

Після копіювання команд роутерів та VLAN-ів можна спокійно вводити їх або ж в симуляторах, або вже на реальне обладнання. Також, якщо технологія Q-in-Q знадобиться не зараз, то скопійований текст можна зберегти на потрібні часи.

ВИСНОВОК

Технології, що розвиваються, надають можливості дізнаватися про нові варіанти вирішення задач легше, аніж в минулому. З часом мережі та технології будуть ставати все потужнішими, аніж раніше. Саме в процесі підготовки дипломної роботи, були розглянуті більш сучасні технології, ніж були в нещодавньому минулому.

З'ясовано ключові характеристики Carrier Ethernet, які були раніше, та основні, які застосовують на сьогоднішній день в різних підприємствах в різних куточках світу.

Було визначено що таке технологія Q-in-Q, її суть, переваги, та принцип роботи протоколу. Також були пояснені приклади кадрів в протоколі, їх види та варіанти використання.

В рамках роботи була створена базова архітектура VLAN на основі протоколу Q-in-Q, пояснення функцій, налаштування та переходи кадрів.

Реалізація протоколу була застосована в симуляторі GNS3. Серед популярних мережевих симуляторів являються UNetLab, Cisco Packet Tracer та Boson NetSlim. Кожен з них представляє доступ до основних методів мережевого обладнання таких як маршрутизатори та комутатори. Одним з їх недоліків вважається відсутність графічного інтерфейсу для налаштування динамічної маршрутизації, що для початківців затрудняє процес її конфігурування.

Розроблений даний інтерфейс дозволяє початківцям та новачкам успішно, та без помилок налаштовувати мережі за протоколом Q-in-Q, не вимагаючи на початку роботи знань команд конфігурації роутерів, а також дає можливість для автоматизації процесів роутерів, що спрощує роботу для користувача мережі. Даний приклад інтерфейсу та протоколу можливо використовувати як на симуляторах, так і на реальному обладнанні.

СПИСОК ЛІТЕРАТУРИ

1. Технология MPLS [Електронний ресурс] - Режим доступу до ресурсу:https://siblec.ru/telekommunikatsii/modelirovanie-setej-i-sistem-svyazi/6-tekhnologiya-mpls
2. КОМП'ЮТЕРНІ МЕРЕЖІ Частина 2 НАВЧАЛЬНИЙ ПОСІБНИК навчальний посібник для студентів спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології», спеціалізації «Інженерія програмного забезпечення інформаційно управляючих систем » та «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів КПІ ім. Ігоря Сікорського, 2020. – 372 с (335 с.)
3. MPLS - КАК РАБОТАЕТ И ЗАЧЕМ НУЖЕН? [Електронний ресурс] - Режим доступу до ресурсу:
https://wiki.merionet.ru/seti/25/mpls-kak-rabotaet-i-zachem-nuzhen/
4. MPLS VPN Architecture and Terminology [Електронний ресурс] – Режим доступу до ресурсу:https://flylib.com/books/en/2.686.1/mpls_vpn_architecture_and_terminology.html
5. MPLS [Електронний ресурс] – Режим доступу до ресурсу:https://dic.academic.ru/dic.nsf/ruwiki/104893
6. Что такое Double VLAN (Q-in-Q) и примеры настройки. [Електронний ресурс] – Режим доступу до ресурсу: https://www.dlink.ru/ru/faq/62/237.html
7. 802.1Q Tunneling (Q-in-Q) Configuration [Електронний ресурс] Режим доступу до ресурсу:https://networklessons.com/switching/802-1q-tunneling-q-q-configuration-example
8. IEEE 802.1Q Tunneling [Електронний ресурс] - Режим доступу до ресурсу:https://packetlife.net/blog/2010/jul/12/ieee-802-1q-tunneling/

9. Настройка Selective QinQ на управляемых коммутаторах Raisecom [Електронний ресурс] – Режим доступу до ресурсу:https://www.raisecom.su/articles/53482
10. QinQ vs VLAN vs VXLAN [Електронний ресурс] - Режим доступу до ресурсу: https://community.fs.com/blog/qinq-vs-vlan-vs-vxlan.html
11. Configuring 802.1Q and Layer 2 Protocol Tunneling [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/01xo/configuration/guide/tunnel.html#wp1026594
12. IEEE 802.1Q-in-Q VLAN Tag Termination [Електронний ресурс]- Режим доступу до ресурсу:https://www.cisco.com/en/US/docs/ios/lanswitch/configuration/guide/lsw_ieee_802.1q.html
13. Мосты Provider Backbone Bridges [Електронний ресурс] - Режим доступу до ресурсу: https://hmong.ru/wiki/IEEE_802.1ah
14. 04-Layer 2 - LAN Switching Configuration Guide [Електронний ресурс] – Режим доступу до ресурсу:http://www.h3c.com/en/d_201211/761546_294551_0.htm
15. Аппаратное и программное обеспечение ЭВМ и сетей [Електронний ресурс] - Режим доступу до ресурсу: https://ppt-online.org/850181
16. IEEE802.1ah-2008[Електронний ресурс] - Режим доступу до ресурсу:https://uk.upwiki.one/wiki/IEEE_802.1ah-2008#Description
17. VPN уровня 2 и Руководство пользователя VPLS для устройств маршрутов [Електронний ресурс] – Режим доступу до ресурсу:https://www.juniper.net/documentation/ru/ru/software/junos/vpn-l2/topics/example/mpls-ex-series-vpn-layer2.html
18. Сети для самых матёрых. Часть двенадцатая. MPLS L2VPN [Електронний ресурс] - Режим доступу до ресурсу: https://habr.com/ru/post/315028/

19. Introduction to Layer 2 VPNs [Електронний ресурс] - Режим доступу до ресурсу:https://flylib.com/books/en/2.686.1/introduction_to_layer_2_vpns.html
20. Управляемые коммутаторы: в чем разница между Layer2 и Layer3 [Електронний ресурс] – Режим доступу до ресурсу:https://ntema.com.ua/article/upravlyaemye-kommutatory-v-csem-raznica-mejdu-layer2-i-layer3
21. IT consultations.... L2VPN [Електронний ресурс]- Режим доступу до ресурсу:http://netwild.ru/l2vpn/
22. [Не только студентам] Лабораторная работа в Packet Tracer [Електронний ресурс] – Режим доступу до ресурсу:https://habr.com/ru/post/350720/
23. Технологія MPLS. Базові принципи та механізми. Протокол LDP. Моніторинг стану шляхів LSP. Інжиніринг трафіку в MPLS [Електронний ресурс] - Режим доступу до ресурсу: https://ppt-online.org/359126
24. VPN рівня 2 проти рівня 3 – знайте різницю [Електронний ресурс] - Режим доступу до ресурсу: https://ipwithease.com/layer-2-vs-layer-3-vpn/
25. MPLS сделает маршрутизаторы быстрыми [Електронний ресурс] – Режим доступу до ресурсу:https://compress.ru/article.aspx?id=10621
26. MPLS и безопасность [Електронний ресурс] - Режим доступу до ресурсу: http://www.ccc.ru/magazine/depot/04_13/0501.htm
27. Сети для самых маленьких. Часть десятая. Базовый MPLS [Електронний ресурс] – Режим доступу до ресурсу: https://linkmeup.ru/blog/1207/#PROTOCOLS
28. Основы QinQ [Електронний ресурс] – Режим доступу до ресурсу : https://russianblogs.com/article/7045742338/

29. 802.1ah Network & Packet: My view [Електронний ресурс] - Режим доступу до ресурсу:https://www.slideshare.net/DipankarShaw/8021ah-network-packet-my-view
30. Формат MPLS метки [Електронний ресурс] - Режим доступу до ресурсу: https://studme.org/189001/informatika/format_mpls_metki
31. Сети vpn mpls 2-го уровня (l2 vpn) [Електронний ресурс] - Режим доступу до ресурсу:https://studfile.net/preview/9319356/page:40/
32. IEEE 802.1ah on Provider Backbone Bridges [Електронний ресурс] – Режим доступу до ресурсу: https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/ios-xml/ios/cether/configuration/15-s/ce-15-s-book/ce-mac-evc-pbb.html.xml
33. Next-Generation Ethernet Encapsulation [Електронний ресурс] - Режим доступу до ресурсу:https://www.blog.adva.com/en/next-generation-ethernet-encapsulation
34. Функциональные возможности управляемых коммутаторов [Електронний ресурс] - Режим доступу до ресурсу: https://ppt-online.org/150628

ДОДАТОК

```
const r1Ip = document.body.querySelector('#r1-ip');
const r1Mask = document.body.querySelector('#r1-mask');

const r2Ip = document.body.querySelector('#r2-ip');
const r2Mask = document.body.querySelector('#r2-mask');

const r1Result = document.body.querySelector('#r1-result');
const r2Result = document.body.querySelector('#r2-result');

const generate = document.body.querySelector('#generate');
const clear = document.body.querySelector('#clear');

const r1Copy = document.body.querySelector('#r1-copy');
const r2Copy = document.body.querySelector('#r2-copy');

const inputReact = (event) => {
  event.target.value = event.target.value.replace(/[^\d.]/g, '');
};

const validate = (string) => {
  const numbers = string.split('.');
  if (numbers.length !== 4) return false;
  for (const number of numbers) {
    if (Number(number) > 256) return false;
  }
  return true;
};

generate.addEventListener('click', () => {
  if (!validate(r1Ip.value)) return alert('Invalid R1 IP address');
  if (!validate(r1Mask.value)) return alert('Invalid R1 Mask address');
  if (!validate(r2Ip.value)) return alert('Invalid R2 IP address');
  if (!validate(r2Mask.value)) return alert('Invalid R2 Mask address');

  const r1 = `en
    conf t
    interface fastEthernet 0/0
    no shutdown
    interface fastEthernet 0/0.12
    encapsulation dot1Q 12
    ip address ${r1Ip.value} ${r1Mask.value}`;

  const r2 = `en
```

```
    conf t
    interface fastEthernet 0/0
    no shutdown
    interface fastEthernet 0/0.12
    encapsulation dot1Q 12
    ip address ${r2Ip.value} ${r2Mask.value}`;

  r1Result.value = r1;
  r2Result.value = r2;
});

clear.addEventListener('click', () => {
  r1Result.value = '';
  r2Result.value = '';
});

r1Copy.addEventListener('click', () => {
  r1Result.select();
  document.execCommand('copy');
  alert('Copied the text: ' + r1Result.value);
});

r2Copy.addEventListener('click', () => {
  r2Result.select();
  document.execCommand('copy');
  alert('Copied the text: ' + r2Result.value);
});

r1Ip.addEventListener('input', inputReact);
r1Mask.addEventListener('input', inputReact);
r2Ip.addEventListener('input', inputReact);
r2Mask.addEventListener('input', inputReact);
```