МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Факультет електроніки та інформаційних технологій

Кафедра комп’ютерних наук

Кваліфікаційна робота бакалавра

КОМП'ЮТЕРНИЙ ДОДАТОК ДЛЯ АВТОМАТИЗОВАНОЇ КОНФІГУРАЦІЇ МЕРЕЖ НА ОСНОВІ БАГАТОПРОТОЛЬНОЇ КОМУТАЦІЇ ЗА МІТКАМИ

Студент гр. ІН-82 Богдан АНАШКІН

Науковий керівник Дмитро ВЕЛИКОДНИЙ

старший викладач кафедри
комп’ютерних наук, к.ф.-м.н.

Завідувач випускаючої кафедри Анатолій ДОВБИШ

доктор технічних наук,професор.

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 Анашкіна Б. А.

Тема: «Комп'ютерний додаток для автоматизованої конфігурації мереж на основі багатопротольної комутації за мітками»

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 _____ Анашкін Б.А.

РЕФЕРАТ

Записка: 53 стор., 29 рис., 1 додаток, 20 джерел.

Об’єкт дослідження – мережі на основі багатопротольної комутації за мітками.

Мета роботи – Розробити комп'ютерний додаток для автоматизованої конфігурації мереж на основі багатопротольної комутації за мітками

Методи дослідження – методи збору та аналізу даних.

Результати – Розроблений комп'ютерний додаток для автоматизованої конфігурації мереж на основі багатопротольної комутації за мітками. Додаток розроблений за допомогою мови програмування C#, компілятор Microsoft Visual Studio Community 2022 (64-разрядная версия) – Current, версія 17.2.3

МЕРЕЖА, IP-АДРЕСА, C#, МАРШРУТИЗАЦІЯ, MPLS.

Зміст

Вступ

З початку виникнення комп'ютерних мереж спричинило великий прорив у передачі повідомлень на далекі відстані. Передача даних вже з тих пір є головною причиною виникнення різноманітних мереж та їх розвитку. У той час у сучасному світі мережі вже давно стали одним із ключових пунктів у її структурі будь-яких компаній. У цей час не існує організації, яка зможе повноцінно здійснювати та функціонувати свою діяльність без побудованої комп’ютерної мережі, яка може безвідказно фунціанувати. Деякі продвинуті користувачі можуть користуватися і інтегрованими сервісними мережами, і віртуальними приватними мережами (VPN), і безліч інших спеціальних послуг.

Поява саме таких технологій як ATM та Free Relay, які були розроблені в 90-ті роки, зробили прорив у передачі пакетів. З’явилися засоби забезпечення обслуговування такі як DiffServ та IntServ, протоколи маршрутизації та резервування. Проте всі вони програють у таких параметрах як затримка, джиттер, перевантаження і т.п., багатопротокольній комутації по мітках MPLS.

MPLS є універсальним розв’язанням проблем якості обслуговування (QoS), які стоять перед пакетними мережами на сьогоднішній день. На цей час MPSL має багато переваг, а саме: швидкість передачі даних, оптимізацію розподілу трафіку, масштабованість та ефективну маршрутизацію в пакетних мережах IP.

Але як саме зрозуміти технологію, якщо налаштування може визвати проблеми, і при неправильному налаштуванню системи може виникнути бажання, що технологія важка, та потребує багато матеріалу, та високому вмінню користування невідомими програмами.

Тому для того щоб, краще зрозуміти налаштування буде розроблений додаток для налаштування MPLS мережі у програмі GNS3.

ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

1.1 Динамічна маршрутизація. Основні алгоритми

Маршрутизація (*routing*) можна назвати ключовою функцією мережного рівня EMBBC. Хоча при цьому розуміється, перш за все, процес визначення в телекомунікаційній мережі одного або декілька шляхів (маршрутів), оптимальних у рамках обраних параметрів, між заданою множиною мережних вузлів. Таким чином, *шлях* (*маршрут*) — це буде послідовністю мережних вузлів і трактів передачі, які з'єднують саме задану пару вузлів мережі**[1]**

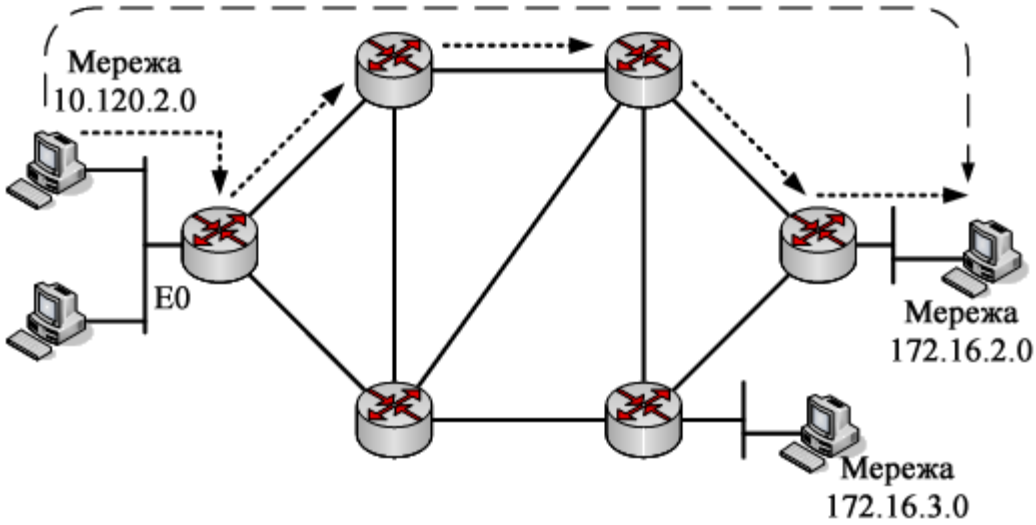

Рисунок 1.1 – Приклади шляху в мережі

Основним завданням мереж є транспортування інформації з персональних комп'ютерів до комп'ютерного-реципієнта, тобто у більшості випадків для цього потрібно зробити кілька відправлень.Тоді постає проблема вибору шляху, яка буде вирішуватися за допомогою алгоритмів маршрутизації. Але, якщо транспортування даних здійснюється дейтрограммами, то тоді для кожної з них ця проблема буде вирішується незалежно. Звідси слідує: при використанні віртуальних каналів вибір шляху буде проводиться на етапі утворення цього каналу.Отже, перший варіант буде реалізуватися в Інтернеті з його IP -дейтрограммами, а другий в ISDN.

Алгоритм маршрутизації має цілком певні властивості: стабільність, простота, надійність, правильність та оптимальність. Остання властивість може не настільки прозора, як на перший погляд здається, хоча все залежить від того, які або які параметри були оптимізовані. Припустимо, що потік даних між двома комп'ютерами, які підключеним через концентратор дуже високий, що матиме відчутний вплив на швидкість обміну між двома комп'ютерами, але цей факт досить складно визначити, будучи впевненими в правильності налаштування системи, але зовні це проявиться лише як збільшення затримки та зменшення пропускної здатності розділу інших комп’ютерів, які входять в мережу

Тоді ключовим параметром оптимізації може бути мінімальна затримка доставки пакету, максимальна пропускна здатність каналу, мінімальна ціна шляху, максимальна надійність на відказ мережі або мінімальна ймовірність помилки.

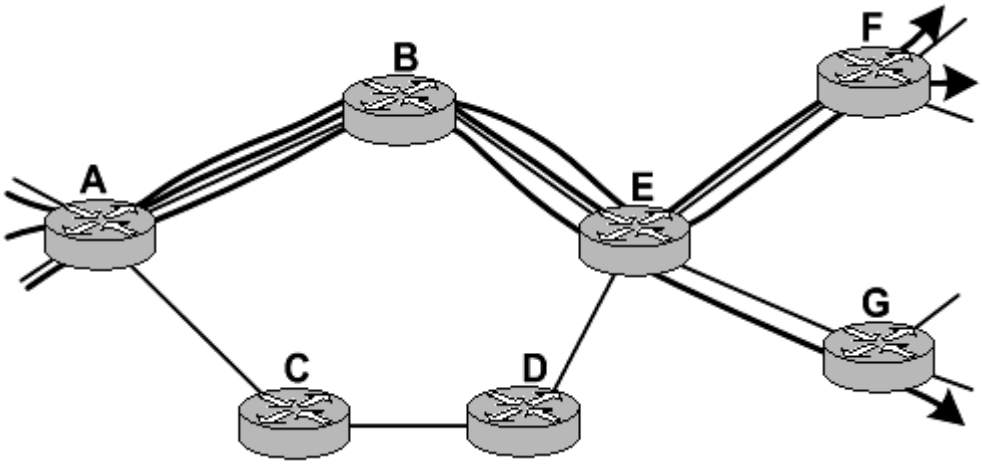

Рисунок 1.2 – Шляхи маршрутизації

Алгоритми маршрутизації бувають адаптивними та неадаптивними: Адаптивна маршрутизація передбачає пристосування алгоритму маршрутизації до реального стану мережі.

Зараз використовуються наступні основні методи адаптивної маршрутизації [2]:

1. Маршрутизація за досвідом. Пакет коли проходить певну кількість каналів, збільшує власний лічильник. Транзитні пакети надсилаються у випадкові канали. Під час цієї інформації в мережі створюється таблиця, для найближчих вузлів від конкретного адресата;
2. Метод якнайшвидшого передавання. В цьому методі буде використовуватися глобальна інформація про те, у якій наявності та довжину черг до вихідних каналів;
3. Локально-адаптивна маршрутизація. Мета цього методу є вибір напряму передавання, який здійснюється на підставі локальної інформації про наявність та довжину черг до вихідних каналів;
4. Розподілена маршрутизація. У методології зберігаються таблиці маршрутизації, в яких вказані маршрути до кожного з адресатів з мінімальною затримкою. Спочатку таблиці будуються на підставі теоретичних обчислень за відомою топологією, а потім ці дані поновлюються з використанням спостережень. В мережі при цьому завжди існує трафік маршрутизації (до 50% трафіку);
5. Централізована маршрутизація. Формуватися таблиця маршрутизації буде на сервері домена і вже через деякий час передаватися на всі вузли. Таблиця маршрутизації будується на основі інформації, яку передають вузли;
6. Гібридна маршрутизація. Цей метод є комбінацією методів локально-адаптивної і централізованої маршрутизації. Рішення про напрям передавання приймається на основі порівняння оцінок за обома варіантами.

Але також існують інші алгоритми маршрутизації, якими зазвичай користуються при статичному налаштуванні мережі. Такі методи будуть називаютися - неадаптивними. Вони називаються так тому, що під час завантаження мережі в маршрутизатори буде завантажуватися інформація про

маршрутизацію . Але звідси слідує, що ці алгоритми не приймають рішень щодо маршрутизації на основі топології мережі чи трафіку. Тому під час налаштування можуть виникати деякі проблеми.

Крім того, флудинг та випадкові блукання - це дві класифікації неадаптивних алгоритмів. Бо час флудингу кожен вхідний пакет надсилається на всі вихідні лінії, за винятком тієї, з якою він поступив. Одна з проблем полягає в тому, що вузол може отримати кілька копій певного пакету. У разі випадкового блукання пакет надсилається одному зі своїх сусідів випадковим чином. Звідси можна дійти висновку, що це ефективний алгоритм, оскільки він ідеально використовує альтернативні маршрути.

Наслідком цього, можна виділити різницю між адаптивними та неадаптивними методами маршрутизації

- Адаптивні алгоритми маршрутизації - це алгоритми, засновані на даних про дані, що відображають поточні умови трафіку.
- Адаптивні алгоритми маршрутизації використовуються для динамічної маршрутизації. У свою чергу алгоритми неадаптивної маршрутизації - це алгоритми, які звертаються до статичних таблиць, щоб визначити, в якому носі відправити пакет. Тому саме адаптивний алгоритм буде основною.

У свою чергу[3]:

- Неадаптивні алгоритми можуть використовуються в статичній маршрутизації. І будуть використовуватися при настроюванні локальних мереж.
- Саме в алгоритмах неадаптивної маршрутизації основою для маршрутизації є – статичні таблиці.
- Неадаптивні алгоритми є легшими та простішими, під час налаштування мережі

Тоді можна дійти висновку, що при розробці системи потрібно використовувати обидва алгоритми маршрутизації

У свою чергу протоколом маршрутизації, називають такий протокол, який може підтримувати мережеві протоколи та надавати механізми обміну маршрутною інформацією.

Звідси слідує, що критерієм вибору для того або іншого шляху між певною парою вузлів мережі є максимум або від його ваги, вартості, яка подана у вигляді суми цієї ваги або вартості трактів передачі, який цей шлях утворює. Можна також називати цю вагу, вартість – довжиною нашого шляху. А сама ця довжина називатися може у термінах протоколів маршрутизації – метрика протоколів маршрутизації(routing metric). В існуючих протоколах маршрутизації використовується широкий перелік метрик залежно від особливостей маршрутної задачі, яку потібно вирішити, та які характеризують різні властивості того чи іншого тракту передачі, його пропускну здатність, завантаженість, надійність, фізичну довжину та вартість.

1.2 Поняття про алгоритм маршрутизаці

Протокол маршрутизації вказує яким чином маршрутизатори можуть обмінюватися інформацією між собою для того, щоб обирати маршрути між будь-якими двома вузлів на комп’ютерна мережа. Маршрутизатори в основному виконують функцію переадресації в Інтернеті, тобто пакети даних передаються через мережу Інтернет, а саме від маршрутизатора до маршрутизатора, поки вони не досягнуть комп'ютера, на який був відправлений запит. Маршрутизація алгоритми визначають конкретний вибір маршруту. Але маршрутизатор має тільки інформацію про ті підключені мережі, які знаходяться поруч з ним

Протокол маршрутизації буде обмінюватися цією інформацією спочатку серед ті маршрутизатори, які знаходяться поруч з ним, а потім надсилати пакети всім у мережі. Таким чином, маршрутизатори в основному будуть отримувати інформацію про топологію мережі. Здатність протоколів

маршрутизації динамічно пристосовуватися до мінливих умов, таких як відключені лінії передачі даних та комп’ютери та маршрутизація даних навколо перешкод, є тим, що надає Інтернету надійність і високу доступність.

Петля маршруту - це поширена проблема в комп'ютерних мережах. Це відбувається, коли обчислений шлях до певного пункту призначення містить цикл через неточні таблиці маршрутизації, тому пакети даних, призначені для цього пункту призначення, будуть зосереджені нескінченно, поки вони зрештою не будуть відкинуті. Особливо це стосується ранніх протоколів віддаленої маршрутизації, таких як протокол інформації про маршрут (RIP), який схильний до здуття живота.

У протоколах, заснованих на технології моніторингу стану каналу, таких як протокол динамічної маршрутизації (OSPF) та протокол маршрутизації проміжних систем (ICC), петлі маршрутизації все ще можуть виникати, але вони короткочасні , оскільки вони зникають, як тільки інформація про інформацію про нову топологію розподіляється по мережі, і всі маршрутизатори синхронізують свої бази даних каналу[5]. Це має додаткову перевагу запобігання проблемам із циклами протоколу маршрутизації.

Хоча під час вибору протоколу маршрутизації (routing protocols) — це досить складне завдання та потребує багато часу. Під час розв’язання слід враховувати такі основні фактори:

- Враховується кількість мережних вузлів і трактів передачі, порядок їхнього з’єднання, а також планове зростання або зміну її структури;
- Характер і обсяг мережного трафіка;
- Вимоги до якості обслуговування;
- Підтримки масок змінної довжини (VLSM).
- Підтримуваний рівень безпеки та надійності;

Хоча існує багато типів протоколів маршрутизації, на ньому широко використовуються три основні класи IP-мережі:

- Протоколи внутрішніх шлюзів тип 1(Протоколи маршрутизації стану зв'язку).
- Протоколи внутрішніх шлюзів тип 2, протоколи маршрутизації відстані-вектора, як от Протокол маршрутизації інформації.
- Зовнішні протоколи шлюзу - це протоколи маршрутизації, що використовуються на Інтернет для обміну інформацією про маршрутизацію між Автономні системи, як от Протокол прикордонних шлюзів (BGP), а протокол маршрутизації вектор-шлях.

Протоколи маршрутизації стану зв'язку є одним з двох основних класів протоколи маршрутизації використовується в комутація пакетів мережі для комп’ютерні комунікації, інша істота протоколи маршрутизації відстані-вектора. Приклади протоколів маршрутизації стану каналів зв'язку включають Спочатку відкрийте найкоротший шлях (OSPF) та Проміжна система до проміжної системи (Є-Є).

Саме протокол стану зв'язку може виконуватися кожним комутаційний вузол в мережі. Це ознає, що вузли, які готові пересилати пакети до мережі Інтернет вони будуть називатися маршрутизатори. Хоча основна концепція маршрутизації стану зв'язку полягає в тому, що кожен вузол в мережі конструює карту підключення до мережі. Ця карта має у вигляд графіку, в яких вузли підключені до яких інших вузлів. Потім кожен вузол самостійно обчислює наступний найкращий логічний шлях від нього до кожного можливого пункту призначення в мережі. Потім кожна колекція найкращих шляхів формуватиме кожен вузол таблиця маршрутизації.

А протокол маршрутизації такі як відстань-вектор в мережі передачі даних може визначати найкращий маршрут для пакетів даних на основі відстані. Протоколи маршрутизації виконують розрахунок векторної відстані вимірюють відстань кількістю маршрутизатори пакет повинен пройти, один

маршрутизатор вважається одним кроком. Щоб визначити найкращий маршрут по мережі, маршрутизатори, на яких реалізований протокол векторної відстані, обмінюються інформацією між собою, як правило таблиці маршрутизації плюс кількість переходів для мереж призначення та, можливо, іншої інформації про дорожній рух. Протоколи маршрутизації відстані-вектора також вимагають, щоб маршрутизатор інформував своїх сусідів топологія мережі періодично змінюється.

Протоколи маршрутизації відстані-вектор використовують Алгоритм Беллмана – Форда для розрахунку найкращого маршруту. Інший спосіб розрахунку найкращого маршруту через мережу заснований на вартості лінії зв'язку та реалізований через протоколи маршрутизації стану зв'язку.

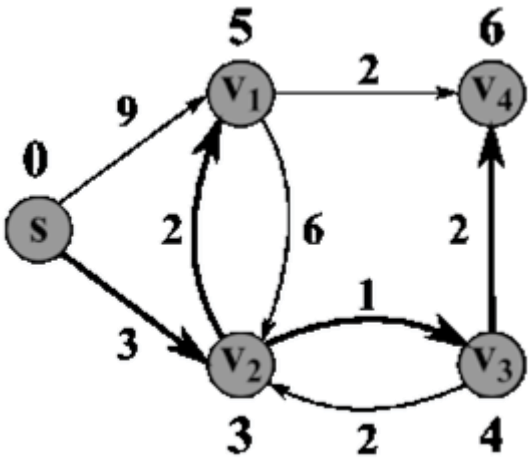

Рисунок 1.3 – Алгоритм Беллмана — Форда

Термін вектор відстані відноситься саме до того факту, що протокол може маніпулювати векторами (масивами) відстаней до інших таких же вузлів мережі. Алгоритм вектора відстані був оригінальним АРПАНЕТ алгоритм маршрутизації і був реалізований більш широко в локальні мережі за допомогою Протокол маршрутизації інформації (RIP)[8].

1.3 Протокол EIGRP

Протокол зовнішніх шлюзів (EGP) - це протокол для обміну інформацією про маршрутизацію між двома сусідніми хостами шлюзу (кожен

із яких має власний маршрутизатор) у мережі автономних систем. EGP використовується між хостами в Інтернеті для обміну інформацією таблиці маршрутизації. Таблиця маршрутизації містить список відомих маршрутизаторів, адреси, на які вони можуть потрапити, і метрику витрат, пов'язану із шляхом до кожного маршрутизатора, щоб було обрано найкращий доступний маршрут. Кожен маршрутизатор опитує свого сусіда з інтервалом від 120 до 480 секунд, і сусід відповідає, надіславши свою повну таблицю маршрутизації. EGP-2 - це остання версія EGP.

Перевагами протоколу EIGRP відносно простих дистанційно-векторних протоколів є[10,11]:

1. Швидка конвергенція. Саме на маршрутизаторах протоколу EIGRP конвергенція буде відбуватися значно швидше, оскільки вона може базуватися на сучасному алгоритмі дифузії поновлень маршрутизації DUAL (Diffusing Update Algorithm) [11]. Цей алгоритм прибирає петлі у кожний момент часу на всьому маршруті та додатково дозволяє усім маршрутизаторам, які належать до даної топології, виконати одночасну синхронізацію.
2. Ефективне використання смуги пропускання. По-перше, протокол EIGRP використовує розсилання часткових, обмежених за обсягом поновлень маршрутизації, і як наслідок цього забезпечується мінімальне використання такими поновленнями смуги пропускання. Маршрутизатори EIGRP зазвичай розсилають часткові та поетапні поновлення маршрутизації, а не повні таблиці маршрутизації. Цей процес аналогічний роботі протоколу OSPF, однак на відміну від нього, маршрутизатори протоколу EIGRP розсилають ці часткові поновлення не всім маршрутизаторам даної області, а лише тим, яким вони дійсно потрібні. Такі поновлення зазвичай називаються обмеженими. По-друге, у протоколі EIGRP замість регулярного розсилання поновлень

маршрутизації маршрутизатори підтримують постійний контакт один з одним шляхом розсилання невеликих пакетів вітання.

3. Підтримка масок підмереж змінної довжини VLSM (Variable-Length Subnet Mask) і безкласової міждоменної маршрутизації CIDR (Classless Interdomain Routing). Відмінність протоколу від IGRP, EIGRP забезпечує повну підтримку безкласового IP завдяки обміну масками підмереж у повідомленнях поновлення маршрутів. Це може дозволити мережевим проектувальникам максимально використовувати адресний простір.
4. Використання складної та гнучкої метрики маршрутів. Метрика протоколу EIGRP може враховувати одразу чотири показники , а саме: час затримки, завантаженість, пропускна спроможність та надійність каналу. При цьому адміністратор може задавати значимість кожного з цих показників.
5. підтримка декількох протоколів мережевого рівня;

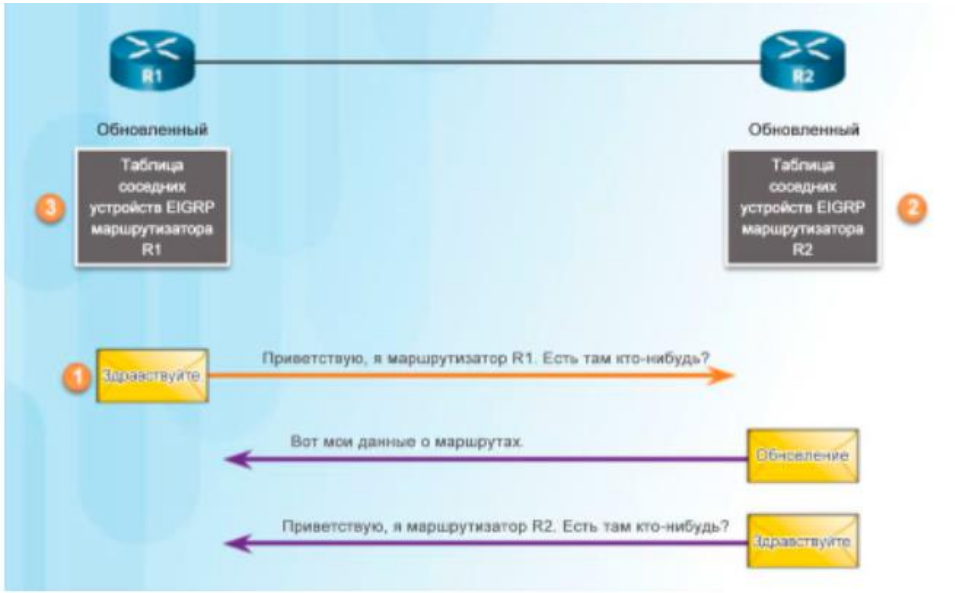

Рисунок 1.4 – Принцип роботи EIGRP

Алгоритм визначення маршруту базується на алгоритмі Дейкстри пошуку в глибину на графі. EIGRP обчислює і враховує 5 параметрів для кожної ділянки маршруту між вузлами мережі[12]:

- Total Delay – Загальна затримка передачі (з точністю до мікросекунди);

- Minimum Bandwidth – Мінімальна пропускна спроможність (в Кб/с – кілобіт/секунду);

- Reliability – Надійнсть (оцінка від 1 до 255; 255 найбільш надійно);

- Load – Завантаження (оцінка від 1 до 255; 255 найбільш завантажено);

- Maximum Transmission Unit (MTU) (не враховується при обчисленні оптимального маршруту, береться до уваги окремо) – максимальний розмір блоку, що можливо передати по ділянці маршруту

Протокол EIGRP використовує метрику довжиною 32 біта. Максимальна кількість переходів для протоколу EIGRP дорівнює 224 (наприклад, для протоколу RIP кількість переходів становить всього 16), чого цілком достатньо для підтримки навіть найбільших сучасних мереж [8].

Feasible Successor(можливий наступник) – скороченно: FS, це сусідній маршрутизатор, який має резервний маршрут без петель до тієї ж мережі, що й у наступника, і який задовольняє умову здійсненності (Feasibility Condition, FC).

Протокол EIGRP може використовувати багато нових технологій, кожен з яких може поліпшувати операційну ефективність, та підвищує швидкість конвергенції та розширює набір функцій протоколу IGRP та інших протоколів маршрутизації. Ці технології можна поділити на такі чотири категорії [9]:

- виявлення сусідніх пристроїв і відновлення загубленого з ними зв’язку;

- надійний транспортний протокол (Reliable Transport Protocol);

- алгоритм DUAL кінцевих станів машини;

- модулі конкретних протоколів.

Маршрутизатори EIGRP формуючи відношення суміжності можуть одержувати можливості: по-перше виявляти маршрутизатори, які раніше були недосяжні. По-друге ідентифікувати маршрутизатори, які стали недосяжними

або нероботоздатними. По-третє це динамічно дізнаватися про нові маршрути, що з’являються у мережі.

Протокол транспортного рівня моделі OSI, що використовується як для надійної, так і ненадійної доставки повідомлень, що стосуються протоколу маршрутизації EIGRP. EIGRP не може користуватися розповсюдженими протоколами надійної та ненадійної доставки TCP і UDP, оскільки останній дозволяють працювати тільки з IP на мережевому рівні, тоді як EIGRP розроблявся як протокол, здатний працювати з багатьма протоколами мережного рівня. Тому для доставки повідомлень EIGRP використовується спеціально створений для нього RTP. Надійна доставка повідомлень має на увазі наявність підтверджень від отримувача, ненадійна – ні. Наприклад, EIGRP відправляє оновлення маршрутів надійно, з підтвердженням, у той час як HELLO-пакети відправляються за допомогою RTP ненадійно і не вимагають підтвердження доставки[13].

1.4 Протокол RIP

Протокол RIP (Routing Information Protocol - протокол маршрутної інформації) є внутрішнім та дистанційно-векторного типу протоколом маршрутизації. Цей протокол зазвичай можуть використовувати в невеликих мережах.

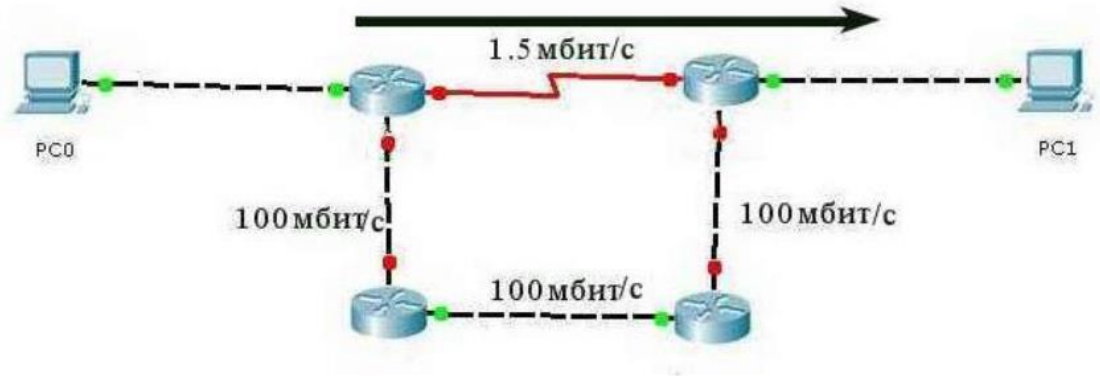

Рисунок 1.5 – Налаштування RIP

RIP протокол, який може оперувати хопами як метрикою маршрутизації. При цьому максимальна кількість хопів, які може дозволити RIP — 15 (метрика 16 буде означати «нескінченно велику метрику», це значить те, що це недосяжний сегмент мережі).У той час кожен RIP-маршрутизатор має за правило сповіщати мережу про свою повну таблицю маршрутизації кожні 30 секунд. Але існує одна проблема, маршрутизатор буде генерувати досить багато трафіку на низькошвидкісних лініях зв'язку. RIP працює на мережевому рівні стека TCP/IP, при цьому використовуючи UDP порт 520.

Етап 1 - створення мінімальної таблиці. У кожному маршрутизаторі зазвичай створюється програмним забезпеченням стека TCP/IP мінімальна таблиця маршрутизації, у якій враховуються тільки безпосередньо під'єднані мережі.

Етап 2 – розсилка мінімальної таблиці сусідам. Після того, як створенна мінімальна таблиця маршрутизатор починає розсилати своїм сусідам повідомлення протоколу RIP. Повідомлення, які передаються в дейтаграмах UDP, включають IP-адресу і відстань до кожної мережі від початкового маршрутизатора.

Етап 3 - отримання RIP-повідомлень від сусідів та обробка отриманої інформації. Маршрутизатор після того, як отримає повідомлення від сусідніх маршрутизаторів може збільшує кожне поле своєї метрики на 1 і запам'ятовувати, через який порт і від якого маршрутизатора отримана інформація, після чого порівнює значення зі своєю таблицею.

Етап 4 – розсилання нової таблиці сусідам. Після конфігурування таблиці маршрутизації, пристрій знову надсилає всім своїм сусідам таблицю. У ній зазвичай не тільки зберігається інформація про ті мережі, до яких маршрутизатор може бути підключений безпосередньо, але й про віддалені, про які він міг дізнатися від сусідніх маршрутизаторів на другому етапі.

Етап 5 - отримання таблиць та обробка отриманої інформації. Тут повторюється третій єтап – маршрутизатор знову отримує таблицю та порівнює зі своєю, вносячи певні зміни.

Отже можна дійти такого висновку, що протокол Rip має такі характеристики:

- за замовчуванням при відновленні маршрутизації пристроєм розсилаються широкомовні пакети кожні 30 секунд.

- в якості метрики при виборі маршруту використовується кількість переходів (хопів);

- якщо кількість переходів стає довше 15, тоді пакет буде відкидається;

- є дистанційно-векторним протоколом маршрутизації;

Незважаючи на те що протокол RIP відомий своїм марнотратним використанням широкомовного режиму, він дуже ефективний при частих змінах мережі, а також в тих випадках, коли топологія віддалених мереж невідома. Однак після збою каналу він може сповільнити стабілізацію системи. Проте про протоколі RIP продовжує використовуватися, тому що він простий, легкий у реалізації і не вимагає складного конфігурації. Таким чином, чутки про смерть протоколу RIP виявилися занадто перебільшеними. Протокол RIP широко використовується на платформах, які не використовують операційну систему UNIX. Багато пристроїв, включаючи мережеві принтери і мережні керуючі SNMP-компоненти, здатні приймати RIP-повідомлення, дізнаючись про можливі мережевих шлюзах. Таким чином, протокол RIP вважається "найменшим спільним знаменником" протоколів маршрутизації. Як правило, він при змінюється для маршрутизації в межах локальної мережі, тоді як глобальну маршру тизації здійснюють більш потужні протоколи[14].

1.5 Протокол OSPF

Протокол динамічної маршрутизації OSPF (англійська - це відкрита найкоротший шлях), заснований на технології моніторингу каналів

(технологія посилань) та використання алгоритму Дейкстри для пошуку найкоротшої доріжки.

Протокол OSPF, поряд з IS-E, належить до класу маршрутизації стану посилань. Принципи цього класу полягають у тому, що в пам’яті маршрутизатора, крім усіх оптимальних маршрутів у віддалених мережах, повинна бути повна мережа, в тому числі з поточними зв'язками між іншими маршрутизаторами. OSPF спочатку був створений як відкритий протокол, який зробив його найпоширенішим серед протоколів маршрутизації. Його алгоритм дозволяє легко побудувати склянку протоколів для OSPF[15].

Протокол OSPF(Open Shortest Path First - вибір найкоротшого шляху першим) в основному розбиває процедуру побудови таблиці маршрутизації на два єтапи. Тобто до першого єтапу можна відносити побудова та підтримка бази даних про стан зв’язків мережі, до другого вже можна відносити - генерація таблиці маршрутизації та знаходження оптимальних маршрутів. Зв’язки мережі представлені у вигляді графа, в якому вершинами графа є маршрутизатори і підмережі, а ребрами - зв’язки між ними. Кожен маршрутизатор може обмінюватися зі своїми сусідами тією інформацією про графа мережі, яку він має до даного моменту. Але важливо пам’ятати, що маршрутизатори не модифікують інформацію, як це відбувається в дистанційно-векторних протоколах, а вони передають її в незмінному вигляді.

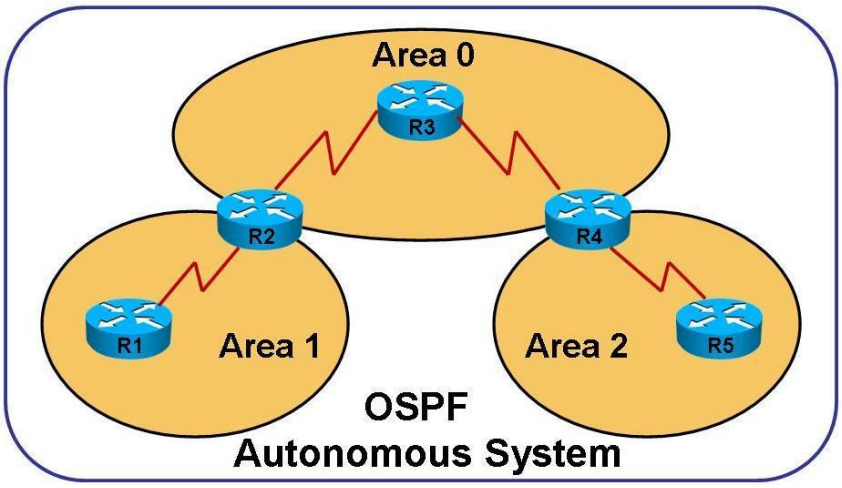

Рисунок 1.6 – Робота протоколу OSPF

Робота протоколу OSPF побудовано відповідно до наступного алгоритму:

1.Маршрутизатори обмінюються невеликими привітними пакетами.

2.Після обміну між ними встановлено сусідство. Кожен з маршрутизаторів додає до спеціального місцевого столу сусідів.

3.Маршрутизатори збирають стан своїх зв’язків із сусідами (посиланнями). Посилання включають ідентифікатор маршрутизатора та сусіда, мережу та префікс, тип мережі та метрику (вартість посилання). Після збору умов маршрутизатор утворює пакет LSA (посилання на державну рекламу).

4.LSA надсилається кожному сусіду, який передає пакет далі через мережу.

5.Отримавши пакет LSA, кожен маршрутизатор додає інформацію, що міститься в ньому, до локальної LSDB (база даних стану посилань).

6.Таблиця LSDB накопичує дані про всі пари маршрутизаторів у мережі.

7.На основі накопичених даних побудована повна мережа мережі, яка включає всі поточні маршрутизатори та утворені з'єднання між ними.

8.Використовуючи карту, кожен маршрутизатор шукає найкоротші маршрути до всіх мереж і формує від них таблицю маршрутизації.

Враховуючи ресурсномісткий та складний принцип OSPF, кожен маршрутизатор вимагає значної кількості оперативної пам’яті та досить високої продуктивності.

Пакет OSPF розміщений у пакеті IP з багаторазовою адресою одержувача. Відправник в ньому відповідає адресі маршрутизатора. Пакет розміщується в багаторазовому кадрі, наприклад, в Ethernet. При формуванні списків контролю доступу слід мати на увазі, що OSPF інкапсульований безпосередньо в IP, а не в UDP або TCP.

Маршрутизатори OSPF можуть використовувати п’ять різних типів пакетів для того, щоб ідентифікувати своїх сусідів та для оновлення інформації про маршрутизацію канального рівня [14]:

- Hello - періодично надсилається на пошук сусідів.
- Database Description DBD - використовується для управління синхронізацією LSDB у сусідів.
- Link state requestLSR - запит від LSA про маршрутизатор, виконаний насильно. Він використовується у випадках, коли маршрутизатор вмикається лише, і він повинен визначити мережу зв'язку, а також якщо у нього є мережа, і вам потрібно знайти альтернативні маршрути.
- Link state update LSU - містить дані про стан відносин з маршрутом.
- Link State Acknowledgment LSAck - підтверджуючий пакет, який відповідає у відповідь на інші типи.

Другий метод передбачає призначення значення адміністратором на основі власного визначення якості посилання. Цей варіант використовується у випадках, коли якість посилання визначається не лише його швидкістю. Включення метрики може бути завищена за посиланням, на якому помилки виявляються частіше, ніж інші, або здійснюється трафік. Цей метод застосовується в мережах, де встановлюються маршрутизатори різних виробників [15].

Переваги OSPF у порівнянні з EIGRP: сприяє створенню ієрархічних проектів мереж; має менш складну метрику порівняно із складеною метрикою EIGRP; не схильний до проблем, пов'язаних з постійним перебуванням маршруту в активному стані; не залежить від виробника конкретного продукту.

1.5 Технологія MPLS

1.5.1 Основні поняття технології

Багатопротокольна комутація міток (MPLS) - це метод маршрутизації в телекомунікаційних мережах, який здійснює маршрутизацію даних від одного вузла до іншого на основі міток короткого шляху, а не довгих мережевих адрес, що дозволяє уникнути складних пошуків у таблиці маршрутизації та

прискорює потоки трафіку При розробці технології визначили три основні елементи MPLS.

По-перше, це FEC – клас переадресації еквівалентності або клас еквівалентності переадресації;

По-друге, це компонент LSR – Lable Switching маршрутизатор, тобто маршрутизатор перемикання міток;

По-третє це буде LSP. Це мітка комутованого шляху або як ще називають шлях перемикання міток. Цей пункт буде стосуватися FEC.

Рисунок 1.7 – Заголовок MPLS

Весь заголовок MPLS – це 32 біти. Формат полів та їх довжина фіксовані. Часто весь заголовок називають міткою, хоча це не зовсім і правильно. Заголовок пакета буде містить зазвичай більше інформації, ніж потрібно для вибору певного маршрутизатора. При цьому можна організувати вибір простіше, для цього потрібно всього-то виконати дві функції. Одна з них – це поділити весь набір пакетів, що будуть надходити, на класи, які будуть називатися переадресаційними класами еквівалентності (FEC). При використанні багатопротокольної комутації міток MPLS пакет присвоюється лише певному класу FEC. При цьому FEC буде присвоюється мітка, а саме ідентифікатор певної фіксованої довжини, який зазвичай передається разом з пакетом. Після того він пересилається до наступного маршрутизатора. Але зрозуміти мережевий маршрутизатор MPLS куди пересилати пакет, може після того, як створить таблицю. Ця таблиця буде називається інформаційною базою міток LIB, яка містить набір використаних міток та для кожної з них окремо є прив'язка "мітка FEC".

Пакети одного FEC отримують однакові позначки. Тобто, проміжні LSR є молотковими, що для всього транзитного трафіку лише перемикає позначки. І вся інтелектуальна робота виконує Ingress LSR[16]:

LIB - Інформаційна база етикетки - таблиця позначок. Аналог таблиці маршрутизації (ребер) в IP. Це вказує на кожен вхідний позначку, що робити з пакетом - змініть позначку або видалити її та в який інтерфейс відправити.

LFIB - інформаційна база переадресації міток - за аналогією з FIB - це база позначок, до яких звертається мережевий процесор. Після отримання нового пакету не потрібно звертатися до процесора та робити пошук у таблиці знаків - все вже під рукою.

LIB - Інформаційна база етикетки - таблиця позначок. Аналог таблиці маршрутизації (ребер) в IP. Це вказує на кожен вхідний позначку, що робити з пакетом - змініть позначку або видалити її та в який інтерфейс відправити.

LFIB - інформаційна база переадресації міток - за аналогією з FIB - це база позначок, до яких звертається мережевий процесор. Після отримання нового пакету не потрібно звертатися до процесора та робити пошук у таблиці знаків - все вже під рукою.

Спочатку потрібно зрозуміти, що у традиційних мережах IP, в основному в загальному випадку, маршрутизація пакетів буде здійснюється на основі IP адреси призначення (destination IP address). Тоді як кожний маршрутизатор у мережі отримує інформацію про те, через який інтерфейс і якому сусідові необхідно перенаправляти Ip-пакет, що прийшов. Але завдяки мультипротокольній комутації буде запропонований інший підхід, а саме по мітках. Це значить те, що кожному Ip-Пакету буде призначаєтися якась довільно задана мітка. Мітка - це елемент фіксованої довжини, який використовується для локальної ідентифікації класу еквівалентності пересилання FEC. Довжина мітки — 32 біта (4 байти): 12 біт — заголовок і 20 біт — значення мітки. Заголовок мітки складається з трьох полів: 3-бітове поле

Exp, яке може бути використане для вказівки класу обслуговування, S-біт атрибута "нижнього" стека та 8-бітний TTL (Time-to-Live) поле. 20-бітове поле мітки містить значення MPLS-мітки, яке може бути будь-яким числом в діапазоні від 0 до , за винятком значень резерву:

1: Мітка Router Alert Label - аналог опції Router Alert в IP - може бути будь-де, крім дна стека. Коли пакет приходить з такою міткою, він може бути переданий локальному модулю, а далі він комутується відповідно до мітки, яка була нижчою — реальною транспортною, при цьому наверх стеку знову має бути додана мітка 1.

2: IPv6 Explicit NULL Label - те саме, що й 0, тільки з поправкою на версію протоколу IP.

3: Implicit Null. Фіктивна мітка, яка використовується для оптимізації процесу передачі пакету MPLS Egress LSR. Ця мітка може анонсуватись, але ніколи не використовується в заголовку MPLS реально. Розглянемо її пізніше.

4-15: Зарезервовані.

Існує три базові протоколи для поширення міток — LDP, RSVP-TE та MBGP.

Якщо коротко, то LDP це буде найпростіший і найзрозуміліший спосіб — спирається на маршрутну інформацію вузлів. RSVP-TE - це розвиток колись розробленого, але непопулярного протоколу RSVP - використовується в MPLS-TE для побудови LSP, що задовольняють певним умовам. Для його роботи необхідні IGP, що підтримують Traffic Engineering (OSPF, ISIS).

MBGP — близький родич BGP, але це протокол із трохи іншої історії, він передає мітки для інших цілей. Тому і стоїть він осторонь LDP та RSVP-TE.

1.5.2 Методи розповсюдження міток

Перший очевидний факт це те, що мітки розповсюджуються в напрямку від одержувача трафіку до відправника, а точніше від Egress LER до Ingress LER. Перший неочевидний факт - MPLS Downstream - це від відправника до одержувача, а Upstream від одержувача до відправника. Отже можно визначити це так: LSP «зростає» з FEC вгору до Ingress LER, як дерево, а трафік «спускається» до одержувача по LSP, як дощова вода по гілках. Тобто мітки розповсюджуються назустріч трафіку. Сам механізм поширення міток залежить від протоколу, налаштувань і виробника.

DU против DoD

По-перше, маршрутизатор може поширювати мітки всім своїм сусідам відразу ж і без зайвих питань, а може видавати за запитом від вищих. Перший режим називається DU - Downstream Unsolicited. Як тільки LSR дізнається про FEC, він розсилає всім своїм MPLS-сусідам мітки для цього FEC.

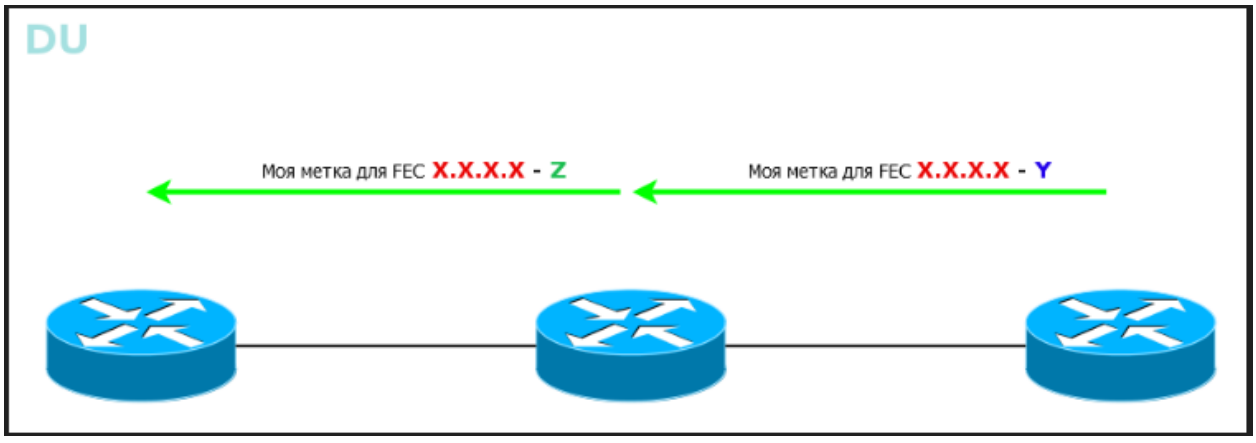

Рисунок 1.8 – Принцип роботи Downstream Unsolicited

Другий режим - DoD - Downstream-on-Demand. LSR знає FEC, у нього є сусіди, але поки вони не запитають, яка для цього FEC мітка, LSR зберігає мовчання.

Цей спосіб зручний, коли LSP пред'являються якісь вимоги, наприклад, по ширині смуги. Навіщо слати мітку просто так, якщо вона одразу ж буде відкинута? Краще вищестоящий LSR запитає у нижчестоящого: мені потрібна від тебе мітка для цього FEC - а той цю мітку дає.

Рисунок 1.9 – Принцип роботи Downstream-on-Demand

Режим виділення міток специфічний для інтерфейсу та визначається в момент встановлення з'єднання. У мережі можуть бути використані обидва способи, але на одній лінії сусіди повинні домовитися тільки про один конкретний.

Також існує режим утримання міток:

Liberal Label Retention Mode – мітки зберігаються. У випадку, коли R3 стане наступним кроком (наприклад, проблеми з основним шляхом), трафік буде перенаправлено швидше, тому що позначка вже є. Тобто швидкість реакції вища, але велика кількість використаних міток.

Conservative Label Retention Mode – зайва мітка відкидається відразу, як вона отримана. Це дозволяє скоротити кількість використовуваних міток, але і MPLS зреагує повільніше у разі аварії.

1.5.3 Протоколи розповсюдження міток

Протокол розповсюдження міток (LDP) може використовувати для встановлення транспортних LSP MPLS, саме тоді, коли розробка трафіку не потрібна. Він встановлює LSP, які слідують вже існуючій таблиці маршрутизації IP, і особливо це добре підходить для встановлення цілої сітки LSP між усіма маршрутизаторами в мережі.

LDP може працювати в багатьох режимах, щоб задовольнити різні вимоги; однак найпоширенішим є режим небажаного використання, який встановлює повну мережу тунелів між маршрутизаторами[20]:

- У режимі запиту вхідний маршрутизатор надсилає запит мітки LDP до маршрутизатора наступного стрибка, як визначено з його таблиці маршрутизації IP. Цей запит пересилається через мережу поетапно кожним маршрутизатором. Як тільки запит досягає вихідного маршрутизатора, генерується повідомлення про повернення. Це повідомлення підтверджує LSP і повідомляє кожному маршрутизатору відображення міток для використання для кожного посилання для цього LSP.
- У непотрібному режимі вихідні маршрутизатори передають зіставлення міток для кожного зовнішнього посилання всім своїм сусідам. Ці трансляції розповсюджуються по кожному каналу мережі, поки не досягнуть вхідних маршрутизаторів. На кожному переході вони повідомляють висхідному маршрутизатору про відображення міток для використання для кожного зовнішнього каналу, і, переповнюючи мережу, вони встановлюють LSP між усіма зовнішніми каналами.

RSVP-TE в основному використовується для встановлення транспортних LSP MPLS, саме тоді, коли існують вимоги до інженерії руху. Він використовується для забезпечення QoS. Ще одною з особливостей є

балансування навантаження по ядру мережі, а також включає можливість керувати повністю оптичними мережами.

RSVP дозволяє використовувати вихідну маршрутизацію, коли вхідний маршрутизатор визначає повний шлях через мережу. Вхідний маршрутизатор може використовувати калькулятор обмеженого найкоротшого шляху спочатку (CSPF), щоб визначити шлях до місця призначення, забезпечуючи виконання будь-яких вимог QoS та Shared Risk Link Group (SRLG). Отриманий шлях потім використовується для встановлення LSP. Оптичні розширення RSVP включають можливість передавати оптичні довжини хвилі та спільні ризикові групи каналів, а також пропускну здатність, затримку та інші характеристики каналу.

Основною перевагою LDP перед RSVP є простота налаштування повної сітки тунелів за допомогою небажаного режиму, тому він найчастіше використовується в цьому режимі для налаштування базової сітки тунелів, необхідної для VPN рівня 2 і рівня 3.

В технології MPLS передача та управління трафіку буде відбувається саме за рахунок технології Traffic Engineering, яка буде здійснювати передачу трафіку по каналах по найбільш оптимальним маршрутом. Обмеження є тільки завдяки технології CSPF (Constrained Shortest Path First), яка може вибрати шляхи не тільки користуючись критерієм, заснованому на його оптимальній довжині маршруту , але також враховувати завантаження маршрутів. При використовувані протоколів RSVP-TE, вони дозволятимуть резервувати смуги пропускання в мережі.

Один із плюсів технології MPLS це захист від збоїв який залежить від попереднього розрахунку шляхів резервного копіювання для збоїв каналу або вузла. Якщо є збій у мережі, то автоматично може відбутися розрахунок найкращого шляху, але це можливо при наявності необхідного шляху. Шляхи

резервного копіювання, які зазвичай попередньо запрограмовані в FIB маршрутизатора та очікують активації, вони можуть активуватися за мілісекунду після виявлення збою.

З точки зору усіх користувачів безперечними перевагами MPLS є істотне підвищення якості роботи (QoS) та також значно спрощена побудова захисту доступу до VPN (Virtual Private Network). Під час використання MPLS відпадає необхідність у інших підвищених заходах безпеки та додатковому шифруванні. До того ж по мережі, які побудовані основі MPLS, можуть передаватися будь-які дані, оскільки вміст пакета залишається незмінним протягом всього шляху, в ньому можуть замінюватися лише позначки. Як наслідок, користувачі можуть передавати з CHC, SPX/IPX-, IP-пакети з невирішеними адресами, кадри Frame Relay або комірки ATM і багато іншого. Однак фіксованому шляху MPLS надається у вигляді частини інтерфейсу IP, тому для його використання не доведеться робити ніяких спеціальних дій з налаштування.[17].

1.6 Постановка задачі

Постановку задачі можна сформувати наступним чином:

1. Налаштувати схему мережі з використанням технології MPLS у симуляторі GNS3.
2. Проаналізувати тастворити десктопний додаток використовуючи мову програмування C#.

Налаштування Технології

2.1 Налаштування схеми за допомогою протоколу EIGRP

У програмі для симуляції GNS3 робимо таку схему:

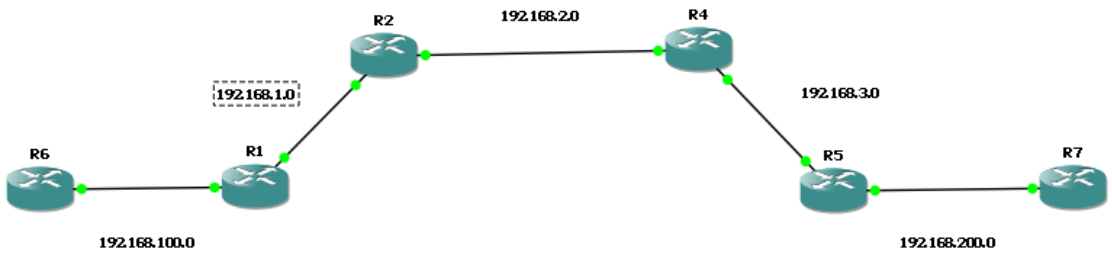

Рисунок 2.1 – Топологія мережі

Отже, тестова схема складається з 7 роутерів. Для налаштування схеми необхідно ввести такі команди на роутері див. Додаток А:

Приклад для R1:

Conf t – Перехід до режиму конфігурації

Int fa 0/0 – Перехід на інтерфейс Fa 0/0

Ip add 192.168.100.3 255.255.255.0 – Задання адреси та маски

No sh – Вмикання інтерфейсу

Ex

Int fa 0/1

Ip add 192.168.1.2 255.255.255.0

No sh

Ex

Тобто зараз відбулося налаштування портів, а саме кожен отримав особисту ip адресу. А налаштування протоколу EIGRP відбувається наступним чином:

Router eigrp 200 – Налаштування протоколу eigrp

Network 192.168.1.0 0.0.0.255 – Сусідня мережа з зворотньою маскою

Network 192.168.100.0 0.0.0.255

Після налаштування одного роутера потрібно налаштувати інші роутери. Для цього див. Додаток А.

Після всього налаштування доречно перевірити нашу мережу на працездатність, для цього ввести на роутері R1 команду: *ping 192.168.3.3.* Якщо налаштування вірні, то повинно бути так, як на рисунку:

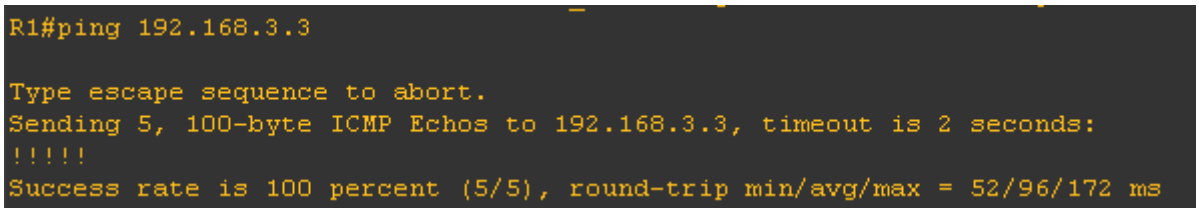

Рисунок 2.2 – Командна строка R1

Це значить те, що наша з роутеру R1 до роутера R5 надходять пакети ICMP

2.2 Налаштування MPLS

Для налаштування MPLS необхідно для кожного роутера прописати наступні команди:

Ip cef - Вмикаємо Cisco Express Forwarding – технологія швидкої комутації пакетів.

Mpls ip - Вмикаємо глобально процес комутації по мітках

mpls label protocol ldp - Обираємо протокол, по якому будуть обмінюватися мітками LSR (ELSR) між собою (є ще TDP, він є пропрієтарним)

mpls ldp router-id loopback 0 - Визначаємо, який інтерфейс (IP-адреса) береться в якості ID роутера в процесі MPLS.

int fa 0/0

mpls ip - Вмикаємо MPLS на інтерфейсі.

mpls mtu 1512 - Збільшуємо розмір mtu для запобігання фрагментації фреймів.

exit

int fa 0/1

mpls ip

mpls mtu 1512

exit

Якщо все вийшло без помилок то при перевірці командою sh mpls forwarding-table, мережа повинна працювати.

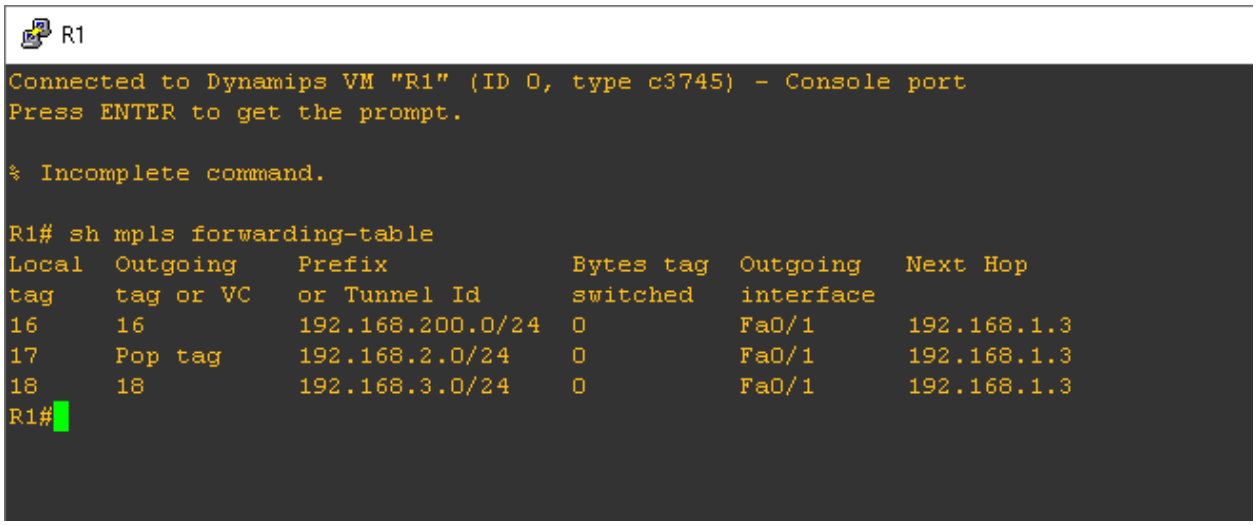

Рисунок 2.3 – Результат команди sh mpls forwarding-table

Далі потрібно ввести команду sh mpls ldp neighbor, для перевірки сусідів.

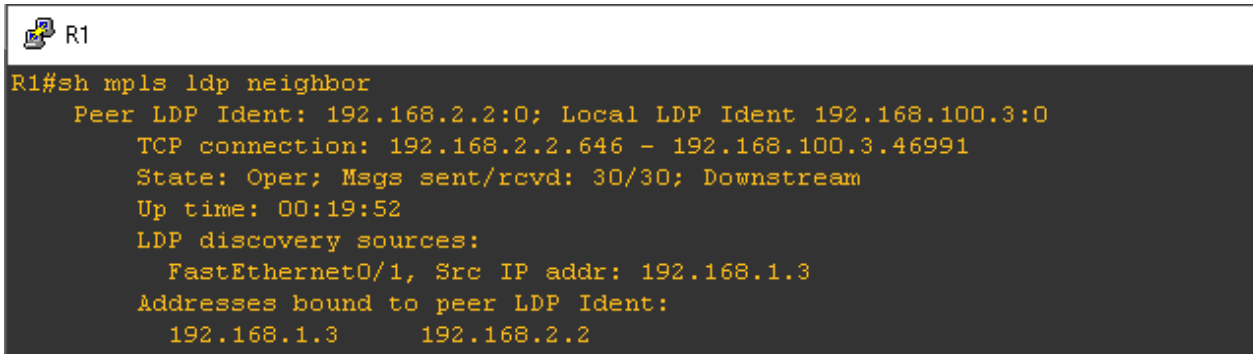

Рисунок 2.4 – Результат команди sh mpls ldp neighbor

Після цього можна побачити, що показує для роутера R1 показує сусіда R2.

Але для фінальної перевірки скористаємося програмою Wireshark. Wireshark-це головний і широко використовуваний протокол мережевого протоколу. Це дозволяє бачити, що відбувається у вашій мережі на мікроскопічному рівні, і це фактично (і часто де-юре) стандарт у багатьох комерційних та некомерційних підприємствах, державних установ та навчальних закладів. Розробка Wireshark процвітає завдяки добровольчим внескам експертів з мережі по всьому світу і є продовженням проекту, розпочатий Джеральдом Комбсом у 1998 році.[18]

Відправляємо пакет від роутера R6 до роутера R7

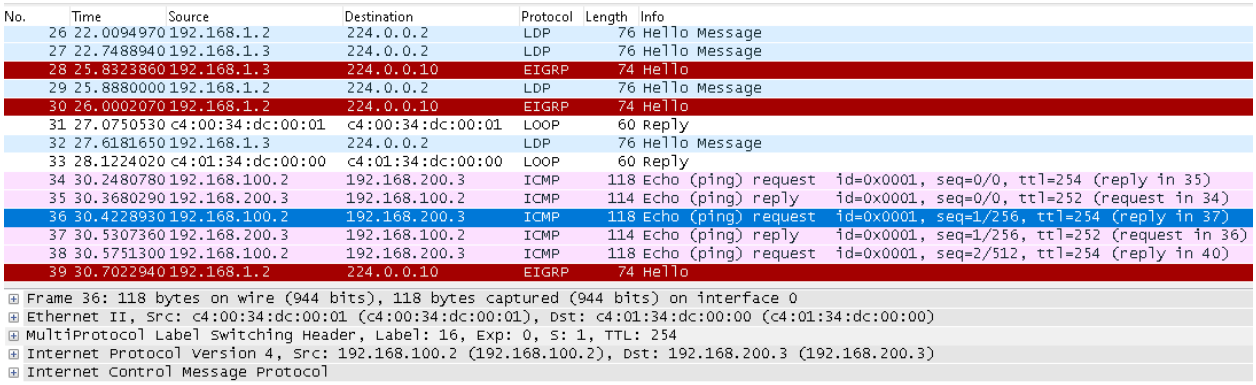

Рисунок 2.5 – Результат перехоплення пакету

Отже на рисунку 0.0 можна побачити пакет на якому є MultiProtocol Label Switchigh Header. Після цього остаточно зрозуміло, що мережа працює

Розробка комп'ютерний додатку

3.1 Розробка інтерфейсу додатку

Для того, щоб розробити додаток мною було використано Microsoft Visual Studio. Було обрано саме це середовище розробки, бо по-перше цей інтегроване середовище розробки безкоштовне. По-друге має простий для використання інтерфейс. По-третє в мережі можна знайти значну кількість матеріалу для написання багатьох програм. Під час налаштування були виявлені процеси, які можна спростити за допомогою додатку

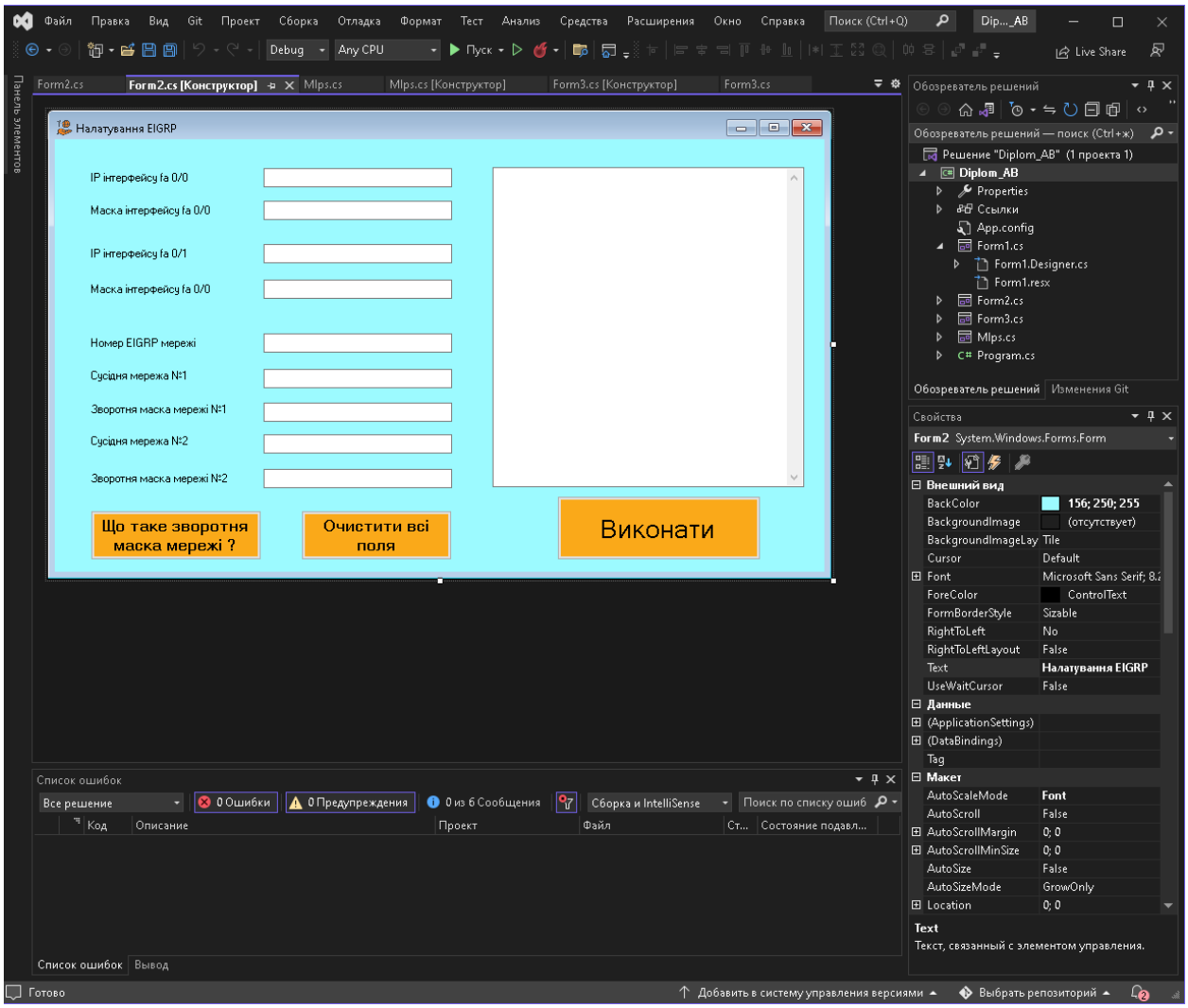

Рисунок 3.1 – Вигляд додатку в Microsoft Visual Studio

Відкривши додаток можна побачити дві активні кнопки, які допоможуть налаштувати мережу MPLS.

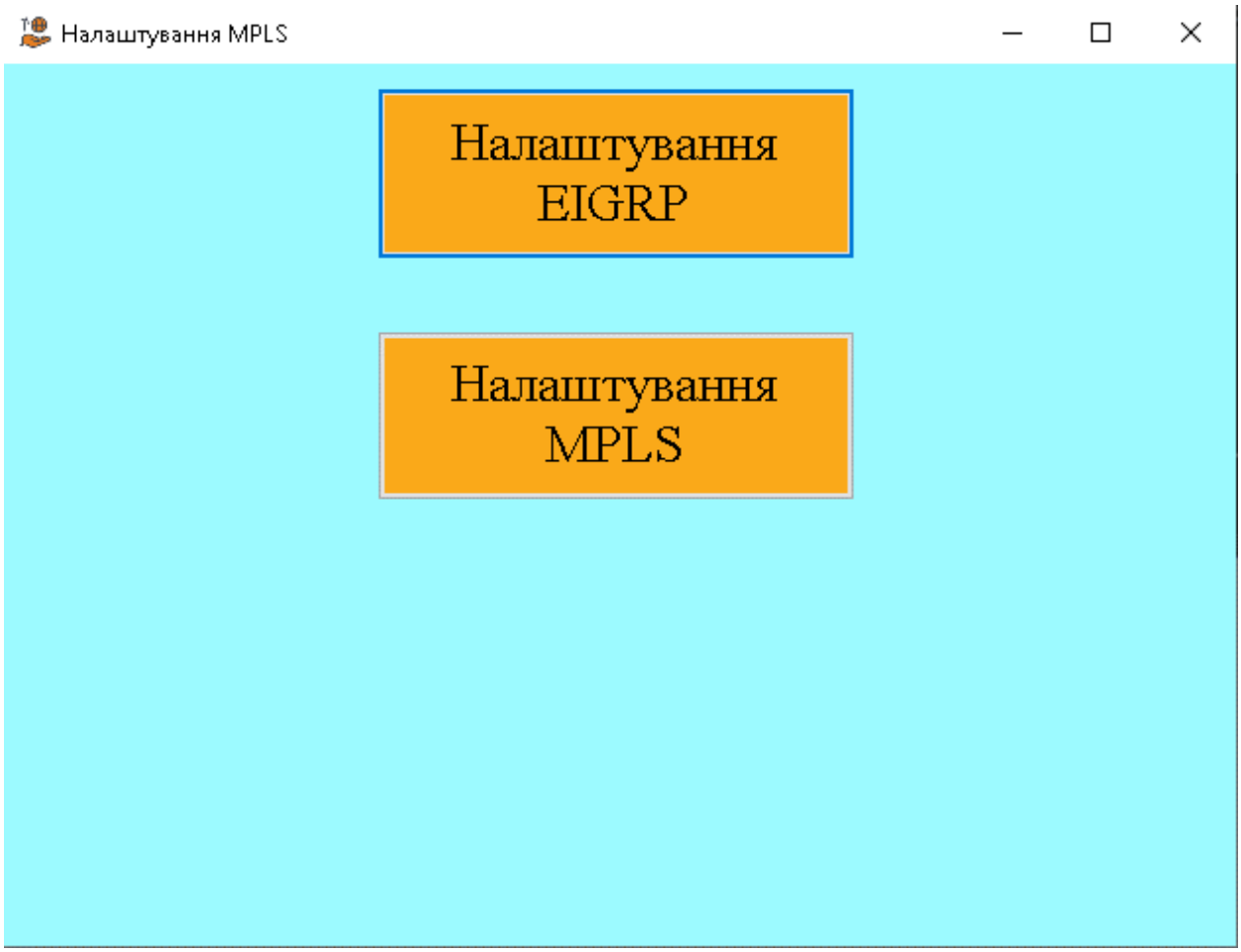

Рисунок 3.2 – Головне меню додатку

При натисканні на «Налаштування EIGRP» користувачу буде доступне поле з налаштуванням IP-адреси роутера та протоколу EIGRP

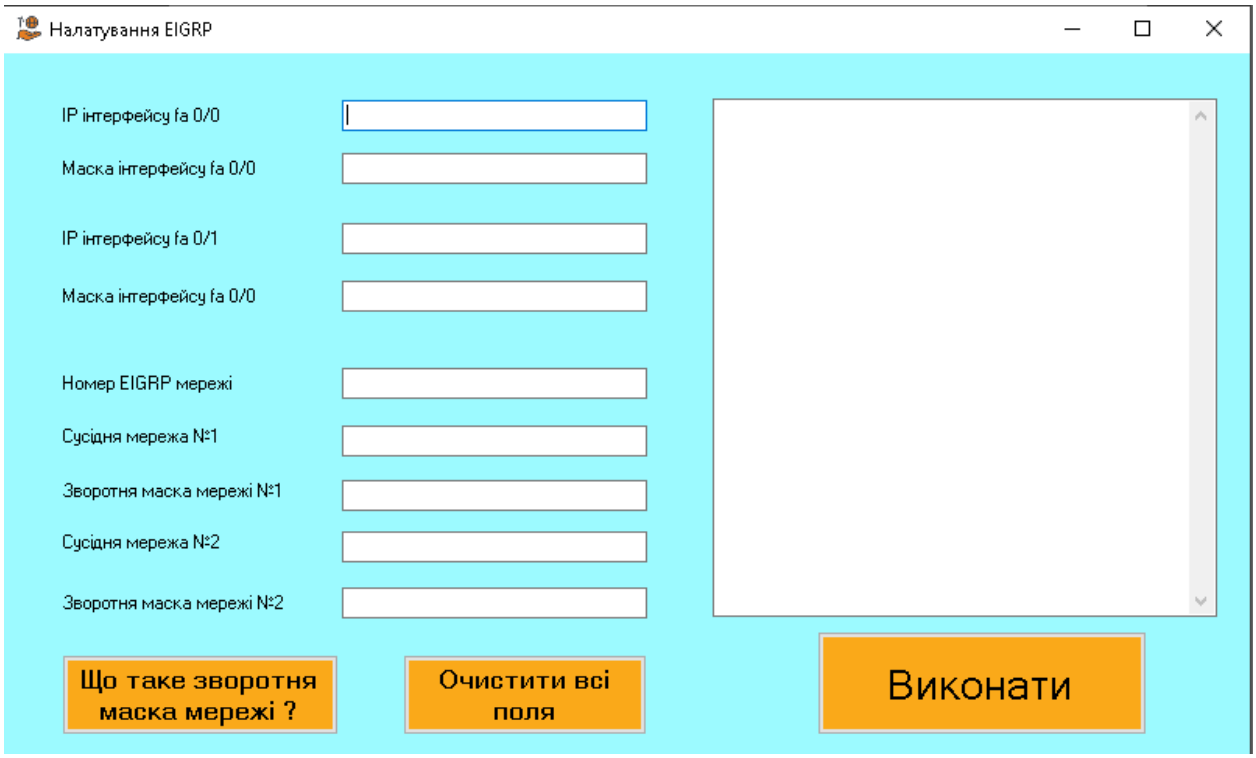

Рисунок 3.3 – Меню налаштування EIGRP

На рисунку 3.3 можна побачити поля для вводу ip-адрес, та масок для кожного інтерфейсу а також поля для налаштування EIGRP, а саме поля для сусідніх мереж , зворотніх масок цих мереж та номер мережі EIGRP.

Також є окреме вікно для налаштування MPLS. В ньому записано команду для налаштування мережі MPLS

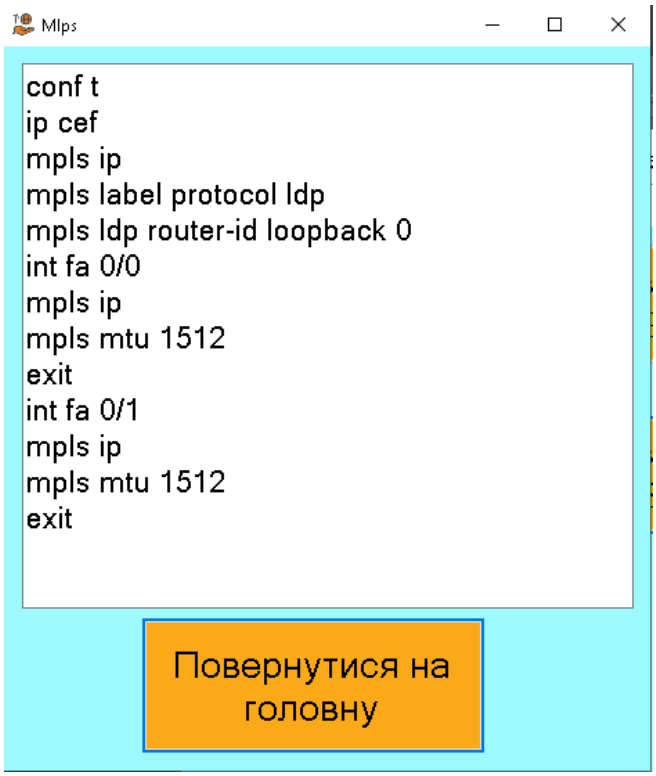

Рисунок 3.4 – Налаштування MPLS

3.2 Опис функціоналу додатка

Користувач має ввести ip-адреси для роутера який зараз налаштовується

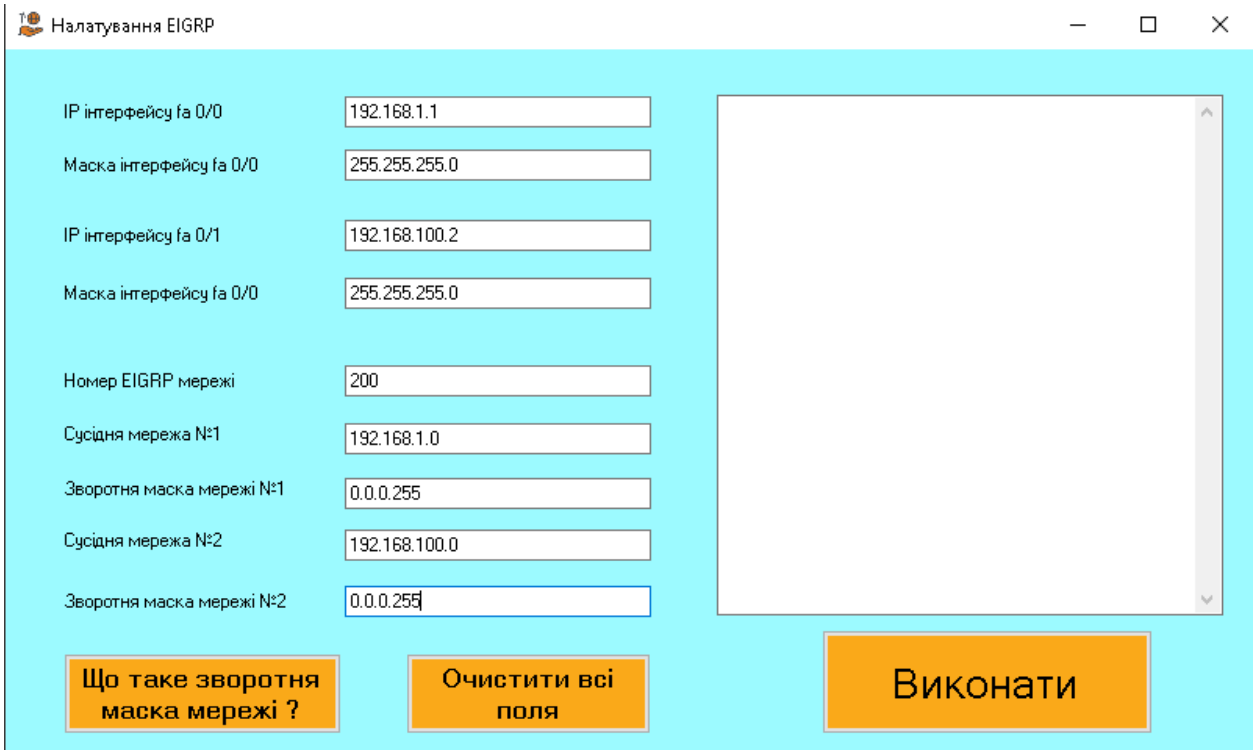

Рисунок 3.5 – Заповнення полей для вводу

Якщо користувач не знає або забув, що таке зворотня маска його мережі знизу є кнопка, яка видасть підказку, як заповнити поле зворотньої маски мережі

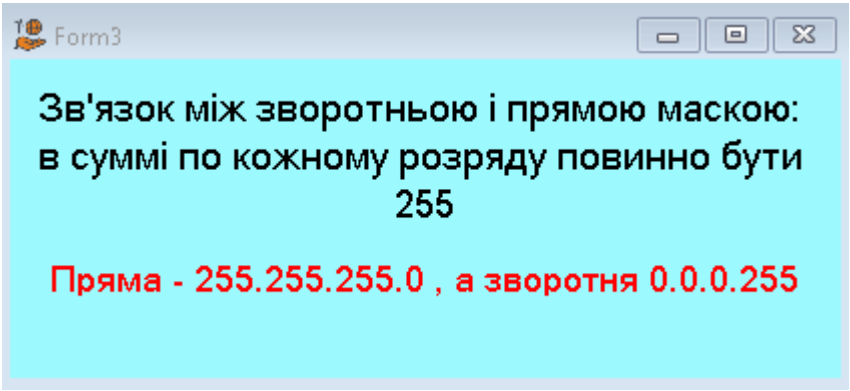

Рисунок 3.6 – Зворотня маска мережі

Після натисканні кнопки «Виконати» в поле, яке знаходиться у правій частині додатку буде надана інструкція для налаштування роутера.

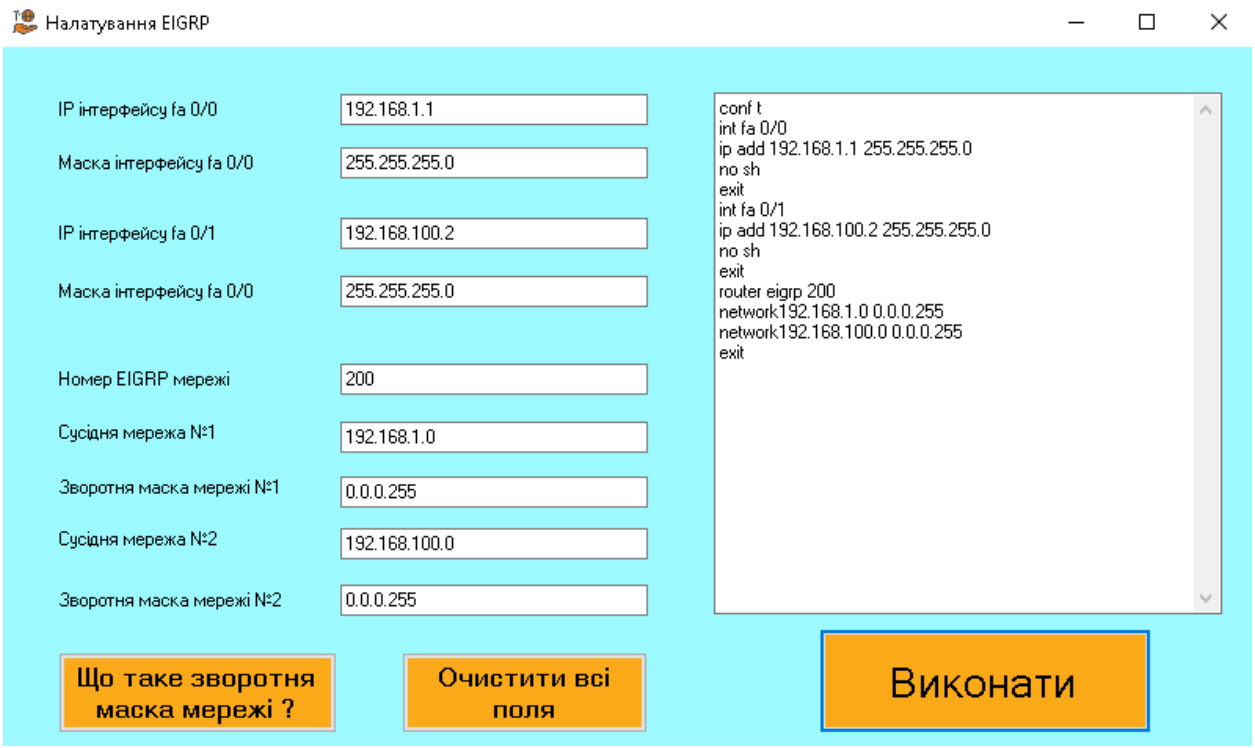

Рисунок 3.7 – Результат роботи додатку

Також, якщо користувач хоче змінити дані, це можна зробити без проблем. Це буде також корисно, якщо була помічена помилка. Для того, щоб швидко очистити поля, можна використовувати кнопку «Очистити усі поля»

Також якщо потрібна швидка інструкція для налаштування мережі, додатком буде запропоновано випадково згенеровано мережа. Для цього потрібно натиснути на «Виконати»

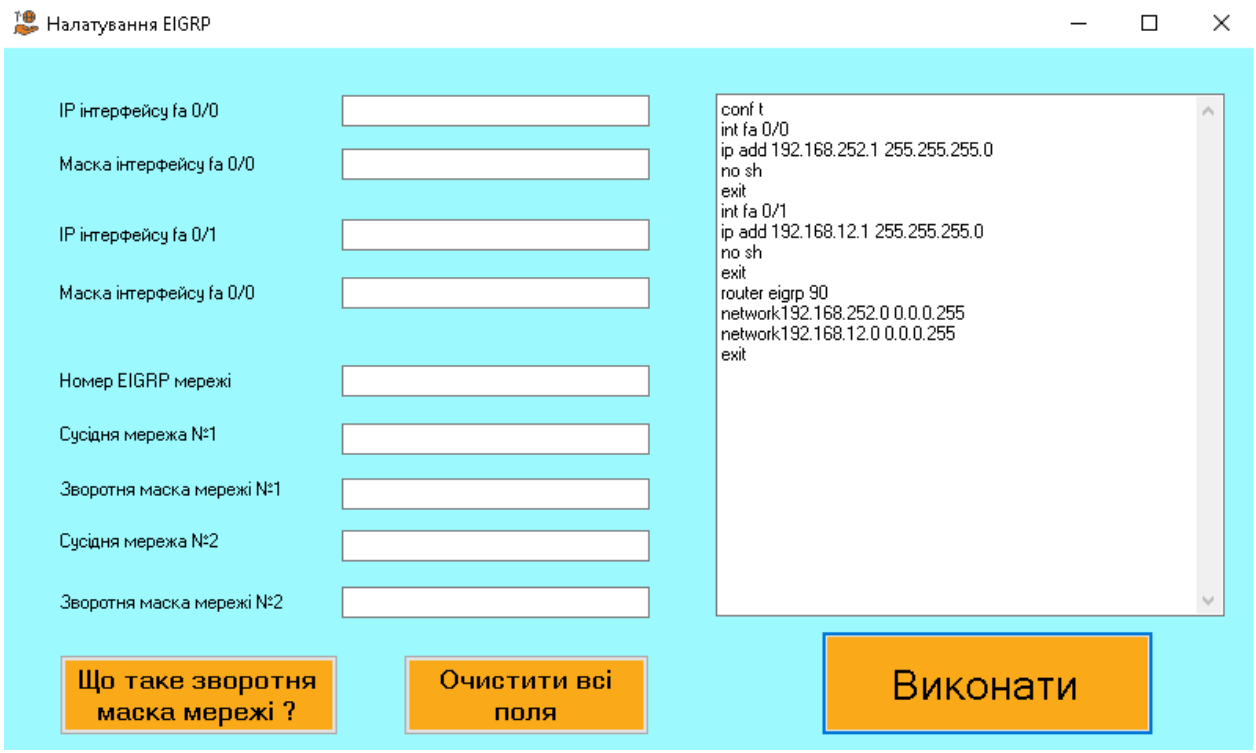

Рисунок 3.8 – Випадково згенеровано мережа

3.3 Тестування додатку

Робимо тестову мережу

Рисунок 3.9 – Тестова мережа

Для перевірки додатку роутер R15 налаштуємо випадково(додатком), а все інше за допомогою додатку

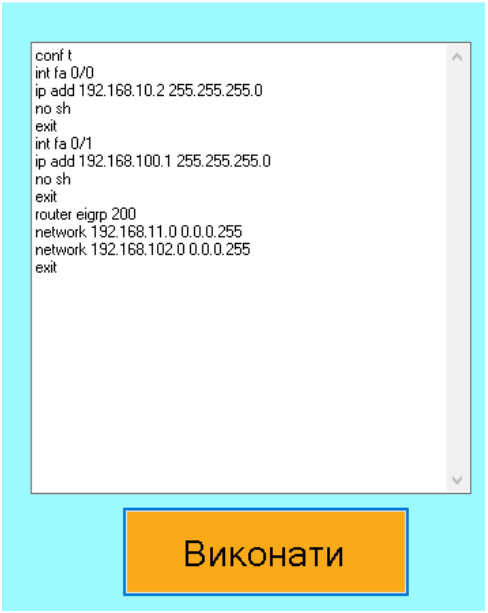

Рисунок 3.10 – Код для R15

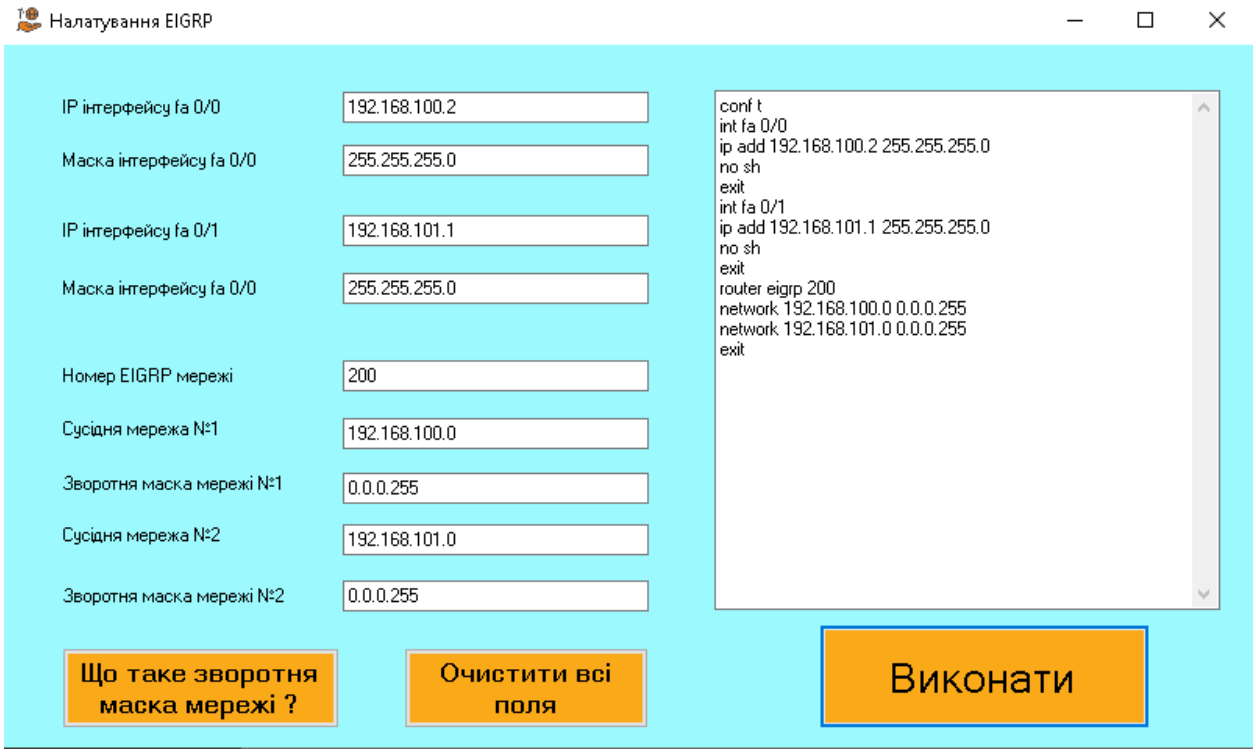

Рисунок 3.11 – Налаштування роутеру

Налаштовуємо кожен роутер та вводимо команди з додатку:

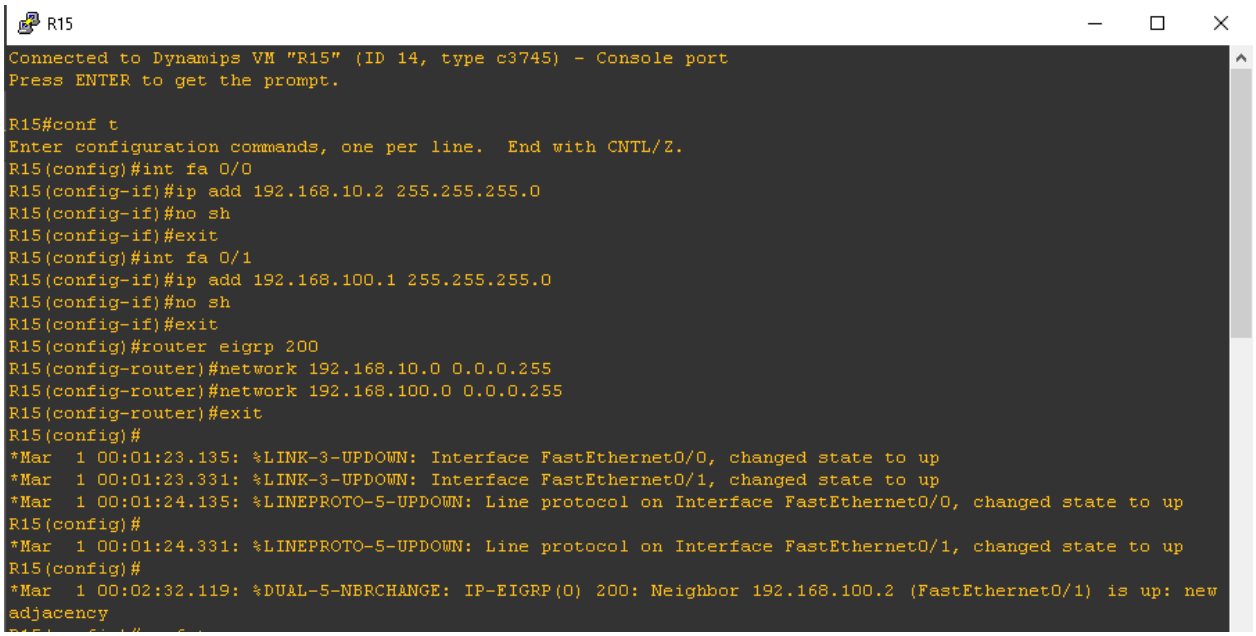

Рисунок 3.12 – Налаштування Ip та EIGRP

```
R15(config)#ip cef
R15(config)#mpls ip
R15(config)#mpls label protocol ldp
R15(config)#mpls ldp router-id loopback 0
R15(config)#int fa 0/0
R15(config-if)#mpls ip
R15(config-if)#mpls mtu 1512
R15(config-if)#exit
R15(config)#int fa 0/1
R15(config-if)#mpls ip
R15(config-if)#mpls mtu 1512
R15(config-if)#exit
R15(config)#
*Mar  1 00:06:49.343: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R15(config)#
*Mar  1 00:06:52.859: %LDP-5-NBRCHG: LDP Neighbor 192.168.101.1:0 (1) is UP
R15(config)#exit
```

Рисунок 3.13 – Налаштування MPLS

Далі вводимо команди для перевірки таблиці маршрутизації та наявність сусіда для роутера R15

```
R15#sh mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     17          192.168.11.0/24  0          Fa0/1       192.168.100.2
17     18          192.168.102.0/24 0          Fa0/1       192.168.100.2
18     Pop tag     192.168.101.0/24 0          Fa0/1       192.168.100.2
```

Рисунок 3.14 – Результат команди sh mpls forwarding-table

```
R15#sh mpls ldp neighbor
    Peer LDP Ident: 192.168.101.1:0; Local LDP Ident 192.168.100.1:0
        TCP connection: 192.168.101.1.28422 - 192.168.100.1.646
        State: Oper; Msgs sent/rcvd: 22/22; Downstream
        Up time: 00:12:30
        LDP discovery sources:
          FastEthernet0/1, Src IP addr: 192.168.100.2
        Addresses bound to peer LDP Ident:
          192.168.100.2   192.168.101.1
```

Рисунок 3.15 – Результат команди sh mpls ldp neighbor

Тоді можна аналізувати таблицю маршрутизації за рисунком - 3.14. Перший роутер з міткою 16 передає на другий роутер мітку 17. На роутері це 2 (другий рядок) локальна мітка 17, це та яку передав першій роутер, а вихідна мітка «Pop tag» це буде означати, що роутер повинен зняти мітку. Проаналізувавши цю таблицю можно побачити, що MPLS налаштована вірно.

Висновок

У ході виконання роботи було з’ясовано принцип роботи алгоритмів маршрутизації. Також був з’ясований принцип роботи багатопротокольної комутації міток (MPLS).

MPLS мережа може легко змінюватись, тобто додавати або віднімати кількість роутерів у мережі. Ця мережа є протокольно-незалежною, це значить, що може використовувати більшість протоколів. У MPLS мережі до звичайного пакета додається спеціальна мітка.

Була побудована схема мережі MPLS у емуляторі GNS3. Був виконаний аналіз схеми та розроблений десктопний додаток для полегшаного налаштування мережі MPLS, з використанням протоколу динамічної маршрутизації EIGRP та накладання мережі MPLS . Під час налаштування мережі був використаний додаток, тобто був проведений тест. Після всіх налаштувань, схема запрацювала правильно.

Користуватися додатком просто та зручно, що скорочує час на побудову та налаштування схеми.

Список літератури

1. Маршрутизація: мета, основні задачі й протоколи. [Електронний ресурс] - http://www.znanius.com/3820.html
2. Адаптивні методи маршрутизації. [Електронний ресурс] - https://wiki.cuspu.edu.ua/index.php/Методи_маршрутизації#:~:text=Адаптивна%20маршрутизація%20передбачає%20пристосування%20алгоритму,наступні%20основні%20методи%20адаптивної%20маршрутизації%3A&text=маршрутизація%20за%20досвідом.
3. Різниця між адаптивними та неадаптивними алгоритмами маршрутизації. [Електронний ресурс] - https://raznisa.ru/raznica-mezhdu-adaptivnymi-i-neadaptivnymi-algoritmami-marshrutizacii/
4. Протоколи маршрутизації (огляд, таблиці маршрутизації, вектор відстані). [Електронний ресурс] - https://www.opennet.ru/docs/RUS/inet_book/4/44/rut_4411.html
5. Х. Хаю, М.А. Орлова, Л.І. Абросимов (2022). " АЛГЕБРАИЧЕСКАЯ МЕТОДОЛОГИЯ МОДЕЛИРОВАНИЯ БЕСЦИКЛОВОЙ МАРШРУТИЗАЦИИ
6. Демичев М.С., Гаипов К.Э. — Алгоритм поиска беспетельных маршрутов // Программные системы и вычислительные методы. - 2020. - № 4. - С. 10 - 25. DOI: 10.7256/2454-0714.2020.4.33605 URL: https ://nbpubMLcom/fcary_read_article.php?id=33605
7. Бобынцев , Д. О. Основы администрирования информационных систем : учебное пособие / Д . О. Бобынцев [и др .] . - Москва ; Берлин : Директ - Медиа , 2021. - 200 с .
8. Протокол маршрутизації відстані-вектора [Електронний ресурс] - https://uk.upwiki.one/wiki/Distance-vector_routing_protocol
9. Комп’ютерні мережі. Огляд протоколу EIGRP [Електронний ресурс] - http://posibnyky.vntu.edu.ua/kom_m/4.8.1.html

10. Подройко Е.В., Лисецкий Ю.М., 2020 ISSN 1028-9763. Математичні машини і системи, 2020, № 2
11. Макаренко С.И. Усовершенствованный протокол маршрутизации ЕЮЯР, обеспечивающий повышенную устойчивость сетей связи // Труды учебных заведений связи. 2018. Т. 4. № 3. С. 65-73.
12. Протоколи внутрішньодоменної маршрутизації [Електронний ресурс] - http://wordpress-zl.hol.es/%D0%BF%D0%B2%D0%BC/
13. Протокол транспортного рівня моделі. [Електронний ресурс] - http://ciscotips.ru/rtp-term
14. Що забезпечує протокол маршрутизації. [Електронний ресурс] - https://crashbox.ru/work-in-the-system/what-the-routing-protocol-provides-routing-protocols-rip-ospf-bgp/
15. Протокол маршрутизації OSPF. [Електронний ресурс] - https://www.smart-soft.ru/blog/protokol_marshrutizatsii_ospf/
16. Базовий MPLS. Термінологія [Електронний ресурс] - https://linkmeup.gitbook.io/sdsm/10.-base-mpls/02.-glossary
17. Технологія MPLS. [Електронний ресурс] - https://wiki.cuspu.edu.ua/index.php/Технологія_MPLS
18. About Wireshark. [Електронний ресурс] - https://www.wireshark.org
19. Протоколb маршрутизації. [Електронний ресурс] - https://uk.upwiki.one/wiki/Routing_protocol
20. What is Label Distribution Protocol Електронний ресурс] - https://www.metaswitch.com/knowledge-center/reference/what-is-label-distribution-protocol-ldp

Додатки

Додаток А

R1

```
conf t
int fa 0/0
ip add 192.168.100.3 255.255.255.0
no sh
exit
int fa 0/1
ip add 192.168.1.2 255.255.255.0
no sh
exit
router eigrp 200
network 192.168.100.0 0.0.0.255
network 192.168.1.0 0.0.0.255
exit
conf t
ip cef
mpls ip
mpls label protocol ldp
mpls ldp router-id loopback 0
int fa 0/0
mpls ip
mpls mtu 1512
exit
int fa 0/1
mpls ip
mpls mtu 1512
```

```
exit
R2
conf t
int fa 0/0
ip add 192.168.1.3 255.255.255.0
no sh
exit
int fa 0/1
ip add 192.168.2.2 255.255.255.0
no sh
exit
router eigrp 200
network 192.168.2.0 0.0.0.255
network 192.168.1.0 0.0.0.255
exit
conf t
ip cef
mpls ip
mpls label protocol ldp
mpls ldp router-id loopback 0
int fa 0/0
mpls ip
mpls mtu 1512
exit
int fa 0/1
mpls ip
mpls mtu 1512
exit
R4
conf t
```

```
int fa 0/0
ip add 192.168.2.3 255.255.255.0
no sh
exit
int fa 0/1
ip add 192.168.3.2 255.255.255.0
no sh
exit
router eigrp 200
network 192.168.2.0 0.0.0.255
network 192.168.3.0 0.0.0.255
exit
conf t
ip cef
mpls ip
mpls label protocol ldp
mpls ldp router-id loopback 0
int fa 0/0
mpls ip
mpls mtu 1512
exit
int fa 0/1
mpls ip
mpls mtu 1512
exit
```

R5

```
conf t
int fa 0/0
ip add 192.168.3.3 255.255.255.0
no sh

exit
int fa 0/1
ip add 192.168.200.2 255.255.255.0
no sh
exit
router eigrp 200
network 192.168.200.0 0.0.0.255
network 192.168.3.0 0.0.0.255
exit
conf t
ip cef
mpls ip
mpls label protocol ldp
mpls ldp router-id loopback 0
int fa 0/0
mpls ip
mpls mtu 1512
exit
```

int fa 0/1

mpls ip

mpls mtu 1512

exit

R6

conf t

int fa 0/1

ip add 192.168.100.2 255.255.255.0

no sh

exit

router eigrp 200

network 192.168.100.0 0.0.0.255

exit

R7

conf t

int fa 0/0

ip add 192.168.200.3 255.255.255.0

no sh

exit

router eigrp 200

network 192.168.200.0 0.0.0.255

network 192.168.100.0 0.0.0.255

exit