Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)

Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(освітньо-кваліфікаційний рівень)

ГЮИК.ХХХХХХ.001ПЗ
(позначення документа)

Дослідження процесів відмовостійкості в програмно-конфігурованих системах
(тема)

Виконав: студент 2 курсу, групи ІКІм-19-1
спеціальності 172 Телекомінікації та радіотехніка
(Код і повна назва спеціальності)
освітньої програми Інфокомунікаційна інженерія
(повна назва освітньої програми)

Алексін В.В.
(прізвище, ініціали)

Керівник зав. кафедри ІКІ імені В.В. Поповського

Лемешко О.В.
(посада,прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2020р.

Атестаційна робота не містить

відомостей, що заборонені

до відкритого друку

Студент гр. ІКІм-19-1 Алексін В.В.

Керівник зав.каф. Лемешко О.В.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
Освітній рівень другий (магістерський)
Спеціальність 172 Телекомунікації і радіотехніка
Освітня програма Інфокомунікаційної інженерії

ЗАТВЕРДЖУЮ
Зав. кафедри _____
(підпис)
«____» _____2020р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студенту Алексіну Владиславу Володимировичу .
(прізвище, ім'я, по-батькові)

1. Тема роботи: Дослідження процесів відмовостійкості в програмно-конфігурованих системах.
затверджена наказом по університету від «20 » жовтня 2020р. №1396Ст
2. Термін здачі студентом роботи 15.12.2020р.
3.Вихідні дані до роботи: математичної моделі щодо реалізації відмовостікої маршрутизації з підтримкою балансування навантаження.
4. Перелік питань, які потрібно опрацювати в ході роботи:
1) Аналіз відомих технологічних та теоретичних рішень щодо проблеми відмовостійкості в телекомунікаційних системах.
2) Моделювання та дослідження процесів відмовостійкості в середовищі Matlab.
3) Дослідження процесів відмовостійкості в програмно-конфігурованих системах.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, плакатів):
Демонстраційний матеріал у вигляді ppt-презенації; структурна схема телекомунікаційної мережі для розробки математичної моделі, для досліження відмовостійкої маршрутизації; структурні схеми телекомунікаційної мережі, для дослідження протоколі відмовостійкої маршрутизації.

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по-батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	Завідувач кафедри Лемешко О.В.		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	01.09.2020	Виконано
2	Збір матеріалів для дослідження	05.10.2020	Виконано
3	Розробка 1 розділу	30.10.2020	Виконано
4	Розробка 2 розділу	10.11.2020	Виконано
5	Розробка 3 розділу	25.11.2020	Виконано
6	Оформлення пояснювальної записки	15.12.2020	Виконано
7	Оформлення слайдів та презентації	15.12.2020	Виконано

Дата видачі завдання___ 01 вересня 2020 року_____

Студент _____ Алексін В.В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ зав.каф Лемешко О.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 3 розділа; 82 сторінок; 55 рисунка; 1 таблиця; 19 посилань.

ПОТІК, ВІДМОВОСТІЙКІСТЬ, БАЛАНСУВАННЯ, МАРШРУТИЗАЦІЯ, МОДЕЛЬ, ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА.

Об’єкт дослідження – процеси відмовостійкості в програмно-конфігурованих системах.

Предмет дослідження – методи і засоби, моделі реалізації задачі щодо відмовостійкості та маршрутизації з балансуванням навантаження в програмно-конфігурованих системах.

Мета роботи – підвищення продуктивності та масштабованості ТКМ на основі вдосконалення потокових моделей та програмних засобів забезпечення відмовостійкості та маршрутизації з балансуванням навантаження.

Методи досліження – формалізація та порівняння, математичне програмування.

Особливу роль в архітектурі забезпечення якості обслуговування (Quality of Service, QoS) грає забезпечення та підтримання відмовостійкості.

Основні рішення пробеми відмовостійкості:

- Забезпечення та підтримка відмовостійкості шлюза за замовчуванням;
- Забезпечення та підтримка відмовостійкої маршрутизації, бажано з балансуванням навантаження;
- Резервування основних елементів мережі (маршрутизаторів, шлюзів, каналів зв’язку, вузлів та ін).

Сучасні протоколи марутизації з кожной новой реалізацією доповнюються функціоналом підвищення відмовостійкості рішень, відображеням цього є поява таких концепцій, як Fast ReRoute в мережах MPLS (Multiprotocol Label Switching), а також Fault-Tolerant Routing і IP resiliency Technology в IP – мережах.

У магістерській атестаційній роботі було об’єднано разом транспортний рівень та рівень доступа в одну мережу, для реалізації комплексного захисту мережі від різного роду пошкоджень та раціонального розподілу ресурсів.

Проведено дослідження протоколів захисту шлюзу за замовчуванням, таких як: HSRP та GLBP на симуляційному обладнанні PT та GNS3. Також проведено аналіз переваг та недоліків, як обраної та вдосконаленої структури мережі так і математичної моделі та досліджених протоколів захисту шлюза за замовчуванням.

Обрано та вдосконалено математичну модель для дослідження відмовостійкої маршрутизації та підтримки балансування навантаження.

ABSTRACT

Explanatory note: 3 section; 82 pages; 55 drawing; 1 table; 19 links.

FLOW, FAILURE RESISTANCE, BALANCE, ROUTING, MODEL, TELECOMMUNICATION NETWORK.

The object of research - fault tolerance processes in software-configured systems.

The subject of research - methods and tools, models for the implementation of the problem of fault tolerance and routing with load balancing in software-configured systems.

The purpose of the work is to increase the productivity and scalability of TCM based on the improvement of flow models and software to ensure fault tolerance and routing with load balancing.

Research methods - formalization and comparison, mathematical programming.

A special role in the architecture of quality of service (Quality of Service, QoS) is played by ensuring and maintaining fault tolerance.

The main solutions to the problem of fault tolerance:

- Ensuring and maintaining the default gateway fault tolerance;

- Providing and supporting fault-tolerant routing, preferably with load balancing;

- Redundancy of basic network elements (routers, gateways, communication channels, nodes, etc.).

Modern maruting protocols with each new implementation are complemented by functionality to increase the resilience of solutions, a reflection of which is the emergence of concepts such as Fast ReRoute in MPLS (Multiprotocol Label Switching), as well as Fault-Tolerant Routing and IP resiliency Technology in IP networks.

In the master's attestation work, the transport level and the access level were combined into one network, for the implementation of comprehensive protection of the network from various types of damage and rational allocation of resources.

The study of default gateway protection protocols, such as: HSRP and GLBP on PT and GNS3 simulation equipment, was performed. An analysis of the advantages and disadvantages of both the selected and improved network structure and the mathematical model and investigated default gateway protection protocols was also

performed. A mathematical model for fault-tolerant routing research and load balancing support has been selected and improved.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦ І ТЕРМІНІВ

ОС – Операційна система;

ТКМ – Телекомунікаційна мережа;

Fast Convergence – швидка збіжність;

Fault-tolerant routing – відмовостійка маршрутизація;

FRR – Fast ReRoute – швидка перемаршрутизація;

GLBP – Gateway Load Balancing Protocol – протокол балансування навнтаженням шлюзу за замовчуванням;

HSRP – Hot Standby Router Protocol – протокол резервування для забезпечення відмовостійкості шлюза за замовчуванням;

IP – Internet Protocol – міжмережевий протокол;

CARP – Common Address Redundancy Protocol – протокол надмірності загальной адреси;

MPLS – Multiprotocol Label Switching – багатопротокольна комутація по мітках;

TE – Traffic Engineering;

QoS – Quality of Service – якість обслуговування;

VRRR – Virtual Router Redundancy Protocol – протокол резервування віртуальних маршрутизаторів;

NGN – Next Generation Network – мережа наступного покоління;

IPTV – телебачення по інтернет протоколу;

MAC – Media Access Control – управління доступом до середовища;

GNS3 – Graphical Network Simulator – графічний симулятор мережі;

STP – Spanning Tree Protocol – протокол остового дерева;

PAgP – Port Aggregation Protocol – протокол агрегування портів;

ECMP – Equal-Cost Multi-Path – Багатошляхова маршрутизація з рівною вартістю;

LACP – Link Aggregation Control Protocol – протокол агрегування каналів;

IRDP – ICMP Router Discovery Protocol – інтернет протокол знаходження маршрутизаторів;

FHRP – First Hop Redundancy Protocol – протокол резервування першого переход

ВСТУП

Ускладнення в області телекомунікаційних технологій призводить до того, що все більш ретельні вимоги ставляться до якості обслуговування мереж, до можливості їх збільшення, до якості обробки трафіка, об’єм якого не перестає зростати. Відомо, що фундаментом у забезпеченні заданих значень таких важливих показників якості обслуговування (Quality of Service, QoS), як середня затримка, джиттер, рівень втрат пакетів і швидкість їх передачі відводиться протоколам маршрутизації разом з протоколами захисту шлюзу за замовчуванням [1].

Найважливішими факторами, які є необхідними для реалізації відмовостійкості в IP мережах:

- маршрутизація (вибір маршрута пакетів та його зміна вразі виникнення перешкод);

- захист елементів мережі від можливого перевантаження (превентивний та пост-фактум).

В основу IP маршрутизації було положено достатньо можливостей для рішення задач пов’язаних з проблемою відмовостійкості. Таким чином є можливість відновити маршрут передачі даних після, практично, будь-якої відмови мережевих елементів.

Однак на даний момент, немає жодної практичної реалізації маршрутизації, яка б мала змогу це зробити протягом прийнятого інтервалу часу, так як реконфігурація мережі може зайняти більше часу, ніж десяті частки секунди, які зазвичай є прийнятним для користувача інтервалом часу. Затримки викликані тим, що було здійснено недостатня кількість контрольних повідомлень і того факту, що завжди певне число мережевих вузлів повинно бути поінформовано про те, що стався збій в мережі, і ці вузли повинні зробити певні контрзаходи, для чого потрібен час. Незважаючі на те, що розрив з'єднання на кілька секунд є абсолютно прийнятним для з'єднання термінал - термінал, це істотно обмежує використання людиною існуючих IP мереж для зв'язку в режимі реального часу [2].

У зв'язку з цим виникає необхідність в розробці актуальних алгоритмів маршрутизації, що забезпечують більш надійну передачу пакетів даних. Також повинно хвилювати збільшення доступності шлюзу за замовчуванням та його

захист, так як в наслідок його перевантаження та/або його не працездатності мережа буде працювати не корректно чи не буде працювати взагалі.

Задачі маршрутизації виконують дуже важливі функції в забезпеченні якості обслуговування в сучасних телекомунікаційних системах, які переважно функціонують на основі таких технологій як IP та MPLS.

Важливо те, що основним джерелом погіршення якості обслуговування є перевантаження елементів мережі. На жаль, більшість протоколів маршрутизації забезпечують перерахунок маршрутів з періодом у десятки секунд та не забезпечують оперативного реагування на перевантаження мережі. Тому для більш швидкого оперативного реагування на можливі відмови в обслуговуванні пакетів, які викликані перевантаженням каналів і чергами маршрутизаторів, все частіше використовуються засоби відмовостійкої маршрутизації, такі як Fast ReRoute, Fast IGP/BGP Convergence і т.д.

При цьому дуже важливо, щоб маршрутний протокол задовольняв ряду важливих вимог: забезпечував реалізацію різних схем резервування ресурсів і елементів мережі: захист каналу, вузла, маршруту, шлюзу; був адаптований під одно/багато шляхову стратегію маршрутизації, а також наряду з розрахунком самих маршрутів визначав порядок розподілу по них мережевого трафіка [2].

На жаль, відомі технологічні та протокольні рішення в цій області не забезпечують задоволення перерахованих вимог в належному обсязі. Тому багато передових концепцій і технологій, такі як Traffic Engineering (TE), Fast ReRoute та ін., не можуть повною мірою реалізувати потенціал закладених в них можливостей.

Причина цього багато в чому полягає в недосконалості математичних моделей і методів, закладених в протоколи маршрутизації, механізми управління чергами та ін. В сучасних маршрутних протоколах переважно використовуються графові моделі і методи пошуку найкоротшого шляху (мультишляху), в рамках яких досить складно, а в більшості випадків і неможливо врахувати вимоги системного характеру, що пред'являються до рішень по багатоадресної і відмовостійкої маршрутизації [3].

Тому основною задачою в даній магістерській роботі буде:

– аналіз математичних алгоритмів побудованих на основі потокових моделей;

– спроба вдосконалення методів та моделей побудованих на основі потокових моделей;

– дослідження проблем відмовостійкості програмно-конфігурованих систем та спроба вирішення проблем відмовостійкості, за допомогою протоколів збільшення доступності та захисту шлюзів за замовчуванням та інших протоколів відмовостійкої маршрутизації на основі роботи з симуляційним обладнанням;

– Комплексне рішення задач відмовостійкості на основі алгоритмічной та програмной реалізації для обох рівнів одночастно.

Окремі результати магістерської атестаційної роботи доповідалися на наступних конференціях:

– «Відмовостійка маршрутизація з підтримкой балансування навантаження» представлена на 23-й Міжнародном молодіжном форумі «Радіоелектроніка та молодь у XXI столітті»-2019. 6-7с.
– «Аналіз методів дослідження відмовостійкої маршрутизації в SDN-мережах» представлена на 24-й Міжнародном молодіжном форумі «Радіоелектроніка та молодь у XXI столітті»-2020. 28-29с.
– «Дослідження та аналіз процесів відмовостійкості в програмно-конфігурованих» представлена на Шостій міжнародній науково-технічній конференції «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв’язку».

1 АНАЛІЗ ВІДОМИХ ТЕХНОЛОГІЧНИХ ТА ТЕОРЕТИЧНИХ РІШЕНЬ ЩОДО ПРОБЛЕМИ ВІДМОВОСТІЙКОСТІ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

1.1 Актуальність проблеми відмовостійкості в телекомунікаційних мережах

Одною з головних особливостей сучасних телекомунікаційних мереж (ТКМ), що складають основу глобальної інформаційної інфраструктури, є підтримка мультисервісності. Ця особливість є ключовою при реалізації концепції побудови мереж наступного покоління (Next Generation Network, NGN). Важливу роль в архітектурі забезпечення якості обслуговування (Quality of Service, QoS) з «кінця в кінець» (end-to-end) при впровадженні мультимедіа-сервісів відводиться засобам широкомовної (broadcast) і багатоадресної (multicast) маршрутизації, які практично завжди використовуються при передачі трафіка таких додатків як IPTV, дистанційного навчання, реплікації баз даних та інформації веб-сайтів, розсилки корпоративної інформації та ін., відсоток якого в спектрі надаваних послуг постійно зростає [4].

Тому для забезпечення якості обслуговування та взагалі підтримки корректної роботи телекомунікаційних мереж на даний момент розроблено безліч можливих варіантів рішення цих проблем. Основне завдання полягає в тому, які концепції вибрати і як їх вдосконалити та об’єднати. Рішенням проблем відмовостійкості в тій чі іншій мірі можуть послужити наступні варіанти:

1. Апаратні рішення – введення надмірності, резервування елементів мережі.
2. Програмні рішення:

– Протоколи канального рівня (протоколи остовного дерева + протоколи агрегування каналу);

– Протоколи мережного рівня (протоколи забезпечення відмовостійкості шлюзу + швидка перемаршрутизація FRR).

Поява таких концепцій, як Fast ReRoute в мережах MPLS (Multiprotocol Label Switching), а також Fault-Tolerant Routing і IP resiliency technology в IP-мережах свідчить про те, що сучастні протоколи маршрутизації постійно вдосконалюються, а саме головне доповнюються рішеннями проблем пов’язаних з відмовостійкостю.

Відмовостійкість визначається кількістю одиничних відмов складових частин (елементів) системи, після настання яких зберігається працездатність системи в цілому. Базовий рівень відмовостійкості має на увазі захист від відмови одного будь-якого елементу. Тому основний спосіб підвищення відмовостійкості це надмірність. Найбільш ефективно надмірність реалізується апаратно, шляхом резервування [5].

Властивість відмовостійкість пов'язано з наступними технічними характеристиками:

- коефіцієнт готовності, який показує, яку частку часу від загального терміну служби система знаходиться в робочому стані;

- показники надійності системи, що визначають ймовірність безвідмовної роботи або ймовірності певних видів відмов системи або її елементів за певний період часу.

Відмовостійка архітектура з точки зору інженерії - це спосіб побудови відмовостійких систем, які зберігають працездатність (можливо, з пониженням ефективності) при відмовах елементів. Термін часто використовується в створенні комп'ютерних систем, які продовжують працювати з можливим зменшенням пропускної здатності або збільшенням часу відгуку в разі відмови частини елементів системи (проблем з апаратною або програмною частиною).

Відмовостійкість шлюзів інтернет і віддаленого доступу – дані ключові вузли необхідно зберігати на апаратних професійних рішеннях з можливістю об'єднання обох пристроїв в відмовостійкий кластер. Така архітектура зможе забезпечити стабільність зв'язку Компанії з простором Інтернет, з'єднання з філіями і безперервний доступ до внутрішніх і зовнішніх ключових сервісів [6].

Після проведеного аналізу можна сформулювати наступні вимоги, які є ключовими та першочергово висуваються до рішень щодо відмовостійкості в IP/MPLS-мережах, без врахування топологічних змін мережі:

– узгоджене рішення окремих задач для розрахунку шляхів і розподілу по ним призначених для користувача потоків;

– реалізація функцій балансування навантаження по множині шляхів;

– підтримка якості обслуговування, в т.ч. по множині показників;

– адаптивна реалізація схем по резервуванню ресурсів (захисту вузла, каналу, маршруту, і їх пропускної спроможності);

– запобігання перевантаження елементів мережі (маршрутизаторів, каналів зв'язку і шляхів в цілому) в ході реалізації запропонованих маршрутних рішень;

– висока масштабованість результуючих рішень, під якою в даному випадку розуміють здатність технологій і протоколів управління виконувати покладені на них функції без істотного зниження ефективності своєї роботи в умовах зростання розміру мережі – числа маршрутизаторів і каналів зв'язку, кількості потоків та розширення переліку показників QoS;

– збільшення доступності та захист шлюзу за замовчуванням.

Можливість реалізації рішень пов’язнаних з відмовостійкостю закладені майже в кожний рівень моделі взаємодії відкритих систем OSI, наприклад:

- Фізичний рівень – введення надмірності(дублювання елементів мережі, схеми резервування каналів зв’язку 1+1,1:1,1:N,N:M).
- Канальний рівень – протоколи агрегування каналів EtherChannel, протоколи остового дерева STP.
- Мережний рівень – схеми захисту елементів мережі FRR, протоколи резервування першого переходу FHRP і т.д.

Необхідно розуміти, що вирішити повноцінно задачу відмовостійкості досить складно, це потребує реалізації методів та засобів на всіх рівнях моделі OSI причому погоджено и комплексно.

1.2 Аналіз існуючих рішень стосовно відмовостійкості в програмно-конфігурованих системах

Відомо, що основні причини, які призводять до виникнення проблем пов’язаних з відмовостійкістю, це або відмова одного з компонентів мережі, або перевантаження мережевого обладнання.

Проблема з перевантаженням телекомунікаційних мереж виникає, через зростання продуктивності сучасних ТКМ. Це призводить до неминучої втрати великих об’ємів даних, що значно вплине на значення показників якості обслуговування. Оскільки, більшість втрат виникає на мережному та транспортному рівні, то з’явились наступні засоби та технології підвищення відмовостійкості, котрі в свою чергу засновані на технологіях IP (Internet Protocol) та MPLS (Multiprotocol Label Switching). До таких технологій відносять наступні:

– швидка протокольна збіжність (Fast IGP/BGP Convergence);

– відмовостійка маршрутизація (Fault-tolerant routing);

– швидка перемаршрутизація (Fast ReRoute, FRR).

Спочатку необхідно відмітити і те, що шляхи також класифікуються. Шляхи, які використовуються у багатошляховій маршрутизації, можна поділити на класи. Насамперед потрібно виділити такий клас, як шляхи, що не перетинаються, під якими розуміють маршрути тільки зі спільними вузлами відправник-отримувач. Якщо шляхи містять хоча б один спільний вузол та (або) канал, то їх називають такими, що перетинаються. Причому якщо шляхи мають спільні вузли, то їх називають шляхами, що перетинаються за вузлами, а якщо спільні канали – шляхами, що перетинаються за каналами (рис. 1.1) [7].

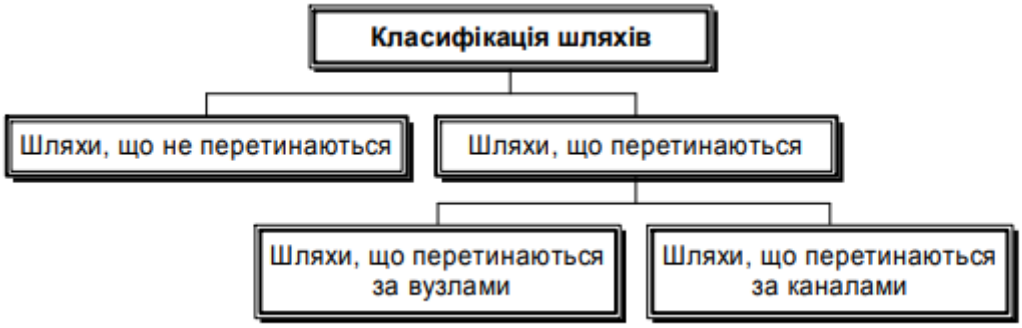


Рисунок 1.1 – Класифікація шляхів при багатошляховій маршрутизації

Наведені технології IP / MPLS-мереж, як і більшість рішень, пов'язаних з підвищенням надійності, засновані на реалізації різних схем резервування шляхів [8]:

1. Схема M:N, при якій створюється M резервних шляхів для N основних шляхів. Резервні шляхи можуть бути використані для передачі фонових потоків, що робить більш ефективним використання вільного мережевого ресурсу. При аварії запитується резервний маршрут і фоновий трафік витісняється.

2. Схема 1:N, при якій створюється один резервний шлях для N основних шляхів. Резервний шлях можна використовувати, як і для балансування навантаження, тобто додаткова можливість частково оптимізувати мережу, або в разі відмови елементу мережі чі всього шляху в цілому перейти на резервний шлях.

3. Схема 1:1, для кожного працюючого маршруту створюється резервний шлях, який повинен містити проблемний елемент мережі (канал або вузол), який зазвичай входить в основний шлях.

В рамках технології Fast IGP/BGP convergence забезпечується виконання всіх умов, пов’язаних з мінімізацією часу реакції мережі на можливі неполадки її елементів. Цей процес синхронізації таблиць маршрутизації після зміни топології мережі називається збіжністю мережі (network convergence).

Процес збіжності мережі включає в себе наступні дії:

– виявлення аварії в мережі;

– передача інформації про аварію, тобто поширення LSA по топології мережі;

– обчислення найкоротших шляхів на всіх маршрутизаторах при отриманні нової інформації про стан ТКМ;

– оновлення маршрутних таблиць на всіх маршрутизаторах в мережі.

Для критично важливих ділянок комп'ютерних мереж необхідно прогнозувати можливий час простою, щоб в подальшому мінімізувати цей показник. Один з підходів передбачає аналіз потенційних точок відмови на маршруті з'єднання серверів і користувачів, тобто окремих компонентів системи (комутаторів, маршрутизаторів, точок доступу), збій яких може позначитися на готовності всієї системи в цілому. Після виявлення потенційного місця відмови, необхідно провести аналіз ризиків з урахуванням витрат на підтримку працездатності системи. Можна виділити наступні стратегії поведінки щодо поліпшення відмовостійкості системи:

– застосування «холодного» резерву (компоненти, які служать для швидкої заміни вийшов з ладу елемента);

– застосування «гарячого» резерву (компоненти, які знаходяться в роботі і готові взяти на себе функції вийшов з ладу елемента в будь-який момент).

При конфігуруванні роботи комп'ютерної мережі з використанням надмірності досягається відмовостійкість і збільшується пропускна здатність з'єднання. Існують алгоритми, що дозволяють будувати відмовостійкі комп'ютерні мережі з використанням дублювання елементів системи.

З точки зору базової архітектури IP-мереж все активне мережеве обладнання працює на канальному і мережевому рівнях моделі OSI, і саме вони визначають надійність і відмовостійкість комп'ютерних мереж в цілому. На рис.1.2 приведена класифікаційна схема методів і протоколів забезпечення відмовостійкості комп'ютерних мереж на різних мережевих рівнях [9]:

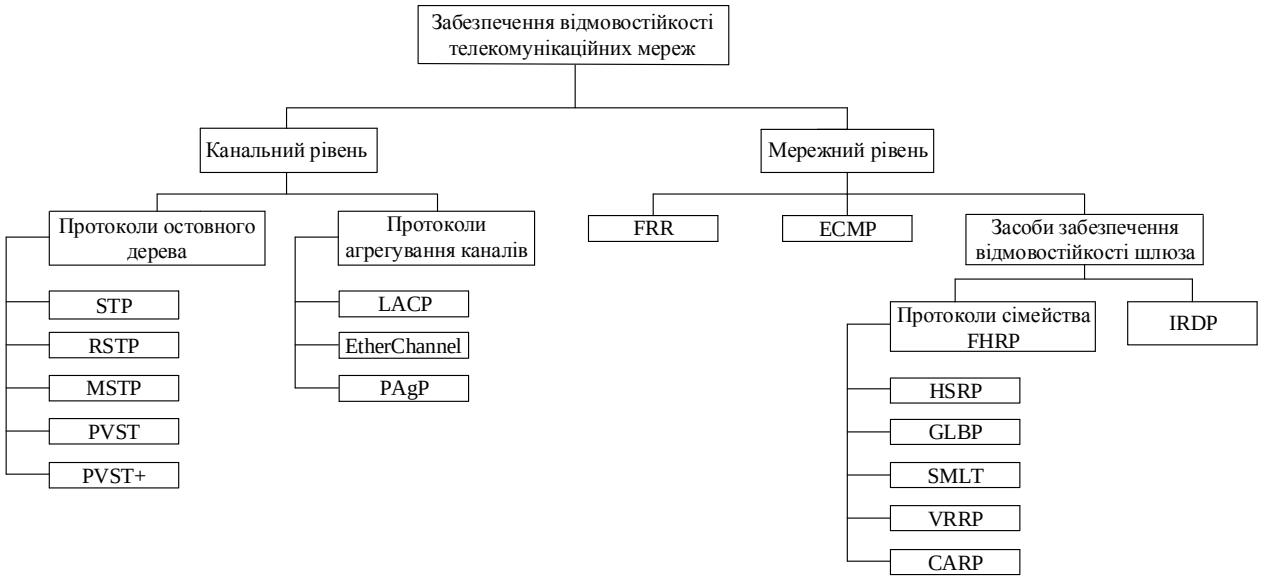


Рисунок 1.2 – Класифікація протоколів, що забезпечують відмовостійкість телекомунікаційних мереж

Як видно з рис.1.2, протоколи забезпечення відмовостійкості на канальному рівні діляться на дві великі групи - протоколи остовного дерева і протоколи агрегування каналів. Протоколи мережевого рівня в свою чергу діляться на протоколи, що забезпечують відмовостійкість шлюзу, ECMP і FRR.

В рамках даної роботи необхідно детально розглянути:

– схеми захисту FRR;

– зміна таймерів на маршрутизаторів(прискорення оновлення/перерахунку маршрутиних таблиць);

– протоколи сімейства FHRP.

Саме ці засоби підвищення відмовостійкості краще інших дають можливість найбільш якісно реалізувати та дослідити явище відмовостійкої маршрутизації разом з балансуванням навантаження та захистом шлюзу.

Спочатко коротко розглянемо про проектування відмовостійкості на канальному рівні, далі детальніше про мережний рівень.

У ЛВС потенційними точка відмови є мережева карта і канал зв'язку. Резервування даних елементів в комп'ютерних мережах реалізується декількома протоколами. На канальному рівні резервуються фізичні з'єднання між пристроями і самі пристрої, що досягається за рахунок протоколів агрегування каналів (Link aggregation) і протоколів остовного дерева (STP).

Протокол агрегування каналів описаний в стандарті IEEE 802.3ad і IEEE 802.1aq Link Aggregation Control Protocol (LACP). LACP підтримує множинні паралельні з'єднання типу комутатор-комутатор і сервер-комутатор. Даний стандарт називають також NIC Teaming (Сполучення адаптерів), Port Trunking (транкінг портів), NIC Bonding (Склейка адаптерів) і Link Bonding (зв'язування каналів). Деякі з виробників мережевого устаткування для своїх продуктів використовують закриті / патентовані технології, а не стандарт в чистому вигляді, наприклад, Cisco використовує EtherChannel, а також протокол PAgP.

Протокол забезпечує «гаряче» резервування ліній зв'язку, збільшення ширини смуги пропускання між пристроями мережі шляхом агрегування каналів (в ідеальних умовах об'єднана ширина пропускання може досягти суми смуг агрегованих каналів), а також балансування навантаження по декількох паралельних з'єднань, тим самим підвищуючи надійність мережі в цілому. У разі резервування ліній зв'язку при відмові одного з агрегіруемих каналів, трафік без переривання пересилається через що залишилися агреговані канали зв'язку, а після відновлення відмовив каналу зв'язку - автоматично включає його в роботу.

На рис.1.3 зображена типова схема використання даної технології при резервуванні та агрегації каналів зв'язку між комутаторами в ЛВС.

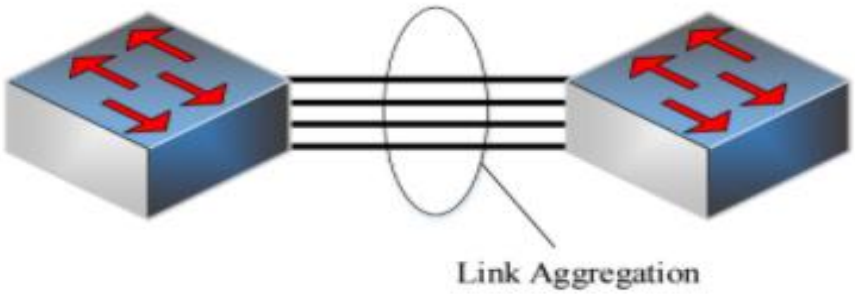


Рисунок 1.3 – Агрегування каналів між комутаторами

У цьому прикладі чотири порти одного комутатора підключені до чотирьох портыв іншого комутатора. У драйвері NIC підтримується статичний режим LACP, а комутатор об'єднує смугу пропускання чотирьох портів таким чином, щоб ефективна смуга пропускання дорівнювала сумі швидкостей всіх мережевих карт. Трафік по всім чотирьом з'єднанням балансується по навантаженню, і, коли відбувається збій одного з'єднання, алгоритм балансування навантаження перерозподіляє її по залишилися з'єднанням. Дана технологія дозволяє збільшити

відмовостійкість з'єднань між вузлами та виконати балансування навантаження, проте вона не забезпечує відмовостійкість у разі виходу з ладу комутатора.

Spanning Tree Protocol (STP, протокол остовного дерева) описаний в стандарті IEEE 802.1d. STP дозволяє створювати мережеві топології з надлишковими зв'язками і комутаторами для забезпечення відмовостійкості на канальному рівні. Протокол вирішує задачу надмірності шляхом усунення петель і блокування надлишкових з'єднань між комутаторами. Необхідність усунення петель обумовлена широкомовними штормами між комутаторами, що знаходяться в одному широкомовному домені [10].

Протокол STP будує дерево зв'язку без петель між усіма комутаторами ЛВС, дозволяючи динамічно блокувати необхідні порти і, при необхідності, також динамічно перебудовувати дерево зв'язку. Таким чином, при відмові комутатора або каналу зв'язку, відбувається перестроювання дерева, що забезпечує відмовостійкість всієї ЛВС. В Нині існують швидші реалізації даного алгоритму, які знайшли своє відображення в протоколах RSTP, а також в MSTP, в якому будується дерево для кожного VLAN, налаштованого в ЛВС. Пропрієтарними версіями протоколу STP є PVST і PVST +.

На рис. 1.4 зображений сегмент мережі, в якому відбувається резервування комутаторів за допомогою протоколу STP:

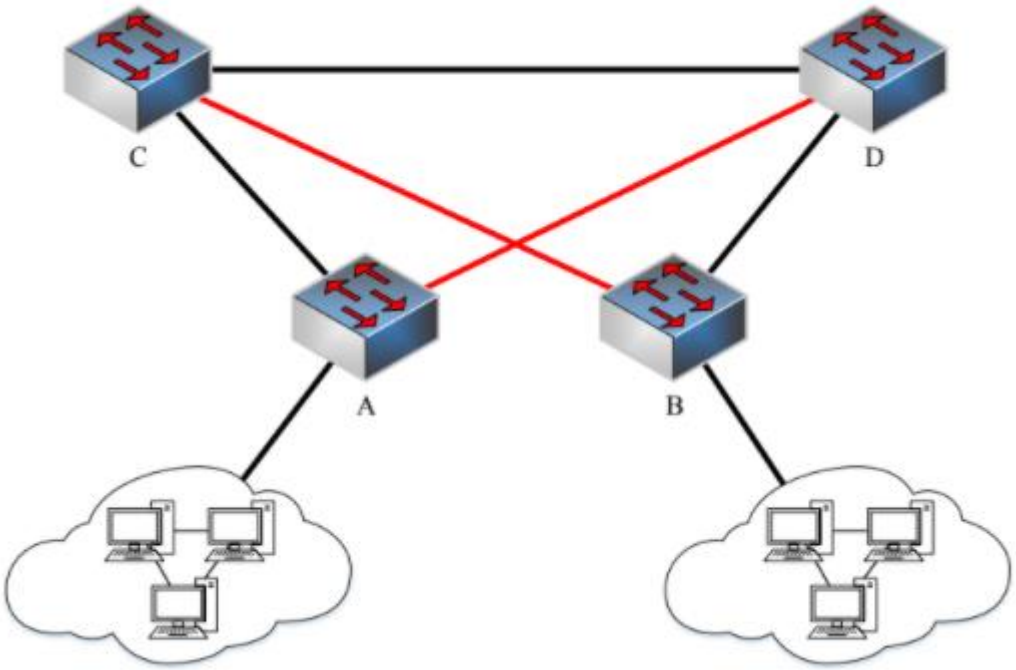


Рисунок 1.4 – Резервування комутаторів з використанням протокола STP

В даному прикладі резервуються робота комутаторів C і D. Протокол STP відпрацьовує так, що блокує порти, що з'єднують безпосередньо A з D і B з C (на малюнку дані зв'язку виділені червоним кольором). При відмові комутатора C або D, протокол STP перебудує дерево і трафік піде через інший комутатор, реалізуючи тим самим відмовостійкість даної схеми.

Протоколи динамічної маршрутизації (RIP, OSPF, IS-IS, BGP і т.д.) по факту є протоколами, що забезпечують відмовостійкість на мережевому рівні, так як ці протоколи збільшують доступність мережі. Основне їхнє завдання – це передача пакетів по оптимальним маршрутом, а в разі відмови перейти на інший маршрут. Також для оптимізації роботи мережі на мережевому рівні можливе використання таких протоколів як Equal Cost Multi-Path (ECMP) і протоколів сімейства Frist Hop Redundancy Protocol (FHRP), які забезпечують балансування навантаження між декількома маршрутами в мережі і високу доступність шлюзів, заданих за замовчуванням, шляхом їх дублювання і спільної роботи, а також гарантують дуже швидке час відновлення в разі аварій [11].

Одним з найбільш ефективних способів підвищення надійності мережі є створення структур з дублюванням. На практиці використовується кілька різновидів схем дублювання: організація паралельних з'єднань, установка двох або більше центральних маршрутизаторів/комутаторів, побудова розподіленої магістралі.

На даний момент більшість великих ЛВС будуються за схемою з маршрутизаторами/L3-комутаторами в центрі, які виконують роль шлюзів, заданих за замовчуванням. У таких ЛВС зазвичай організовуються віртуальні мережі з маршрутизацією, передбачені надлишкові зв'язку між пристроями, встановлений резервний центральний комутатор. В такому випадку на канальному рівні комп'ютерної мережі слабким місцем буде саме маршрутизатор / L3-комутатор. У разі виходу його з ладу можливо кілька варіантів розвитку подій, що вимагають втручання системного адміністратора: налаштування робочих станцій на роботу з іншим маршрутизатором в якості шлюзу за замовчуванням або установка додаткового маршрутизатора. Для збільшення відмовостійкості такої мережі використовують два шлюзу.

На рис. 1.5 зображена схема з резервуванням маршрутизатора:

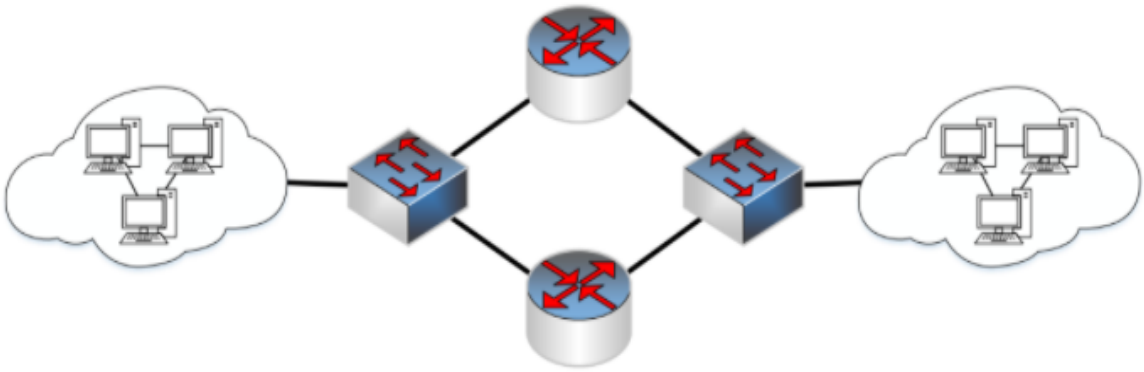


Рисунок 1.5 – Схема резервування маршрутизатора

Протоколи сімейства FHRP дозволяють забезпечувати клієнтів відмовостійким шлюзом. Сенс роботи даних протоколів полягає в тому, щоб дозволити кільком мережевим пристроям використовувати один адрес (в загальному випадку - адрес шлюзу), забезпечуючи тим самим відмовостійкість для клієнтів. В даному прикладі один мережевий адреса використовуватимуть два маршрутизатора, що утворюють групу і є по суті одним віртуальним маршрутизатором, відмовостійкість якого вище, ніж відмовостійкість кожного фізичного маршрутизатора, що становить дану групу [12].

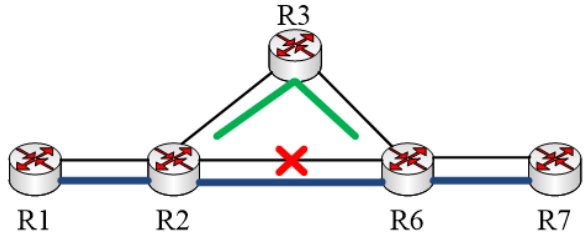
Протокол IRDP описаний в стандарті RFC 1256. Даний протокол реалізує алгоритм оповіщення клієнтів про присутність маршрутизатора в мережі самостійно або за запитом клієнтів. Таким чином, IRDP дозволяє клієнтам знаходити і призначати шлюзи, задані за замовчуванням. Мінус даного протоколу випливає з необхідності клієнтам самим призначати адреси шлюзів, отримані за допомогою даного протоколу, а також можливість їх динамічного перемикання, що передбачає необхідність його підтримки з боку клієнтів.

Протокол ECMP описаний в стандарті RFC 2992. Даний протокол працює з протоколами динамічної маршрутизації як внутрішнього (IGP), так і зовнішнього (EGP) шлюзу. Він дозволяє призначати в системі кілька рівнозначних маршрутів для передачі трафіку. Таким чином, ECMP дозволяє рівномірно розподілити потік даних через кілька мережевих з'єднань, а в разі відмови провести перемикання з непрацюючого маршруту на працюючий, забезпечуючи тим самим відмовостійкість на мережевому рівні.

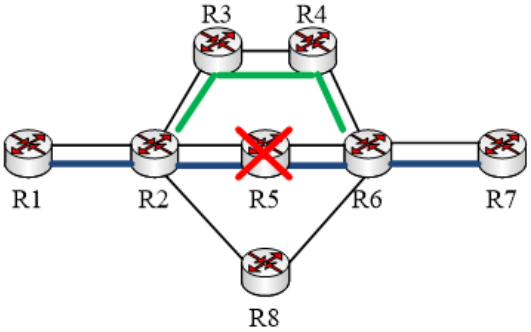
Швидка перемаршрутізація (Fast Re-Route, FRR) забезпечує відмовостійкість в MPLS-мережах шляхом побудови обхідного маршруту для

трафіку, якщо виявляється проблема на робочому маршруті. Перемикання займає близько 50 мс. FRR використовує заздалегідь розраховані маршрути, тобто, маршрутизатора потрібно всього лише використовувати нову мітку і направити трафік на інший порт. Принцип MPLS FRR заснований на тому, що якась проміжна топологія використовується як засіб резервування мережі. Недолік використання MPLS FRR полягає в тому, що алгоритм, що дозволяє обмежити тривалість операцій відновлення 50 мс, не є детерминистским: така операція відновлення має локальний характер, і, як тільки відбувається відмова, всій мережі може заново знадобитися перерахунок маршрутів, крім того для забезпечення додаткової відмовостійкості мережі будуть потрібні додаткові вельми дорогі порти маршрутизаторів IP / MPLS [13].

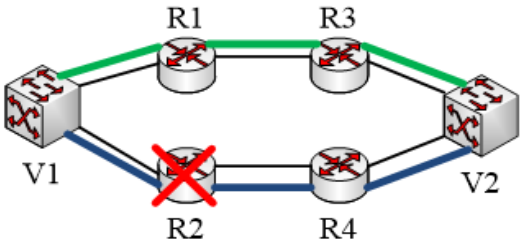
На рис. 1.6 наведено схеми захисту швидкої перемаршрутизації для елементів досліджуваної мережі.



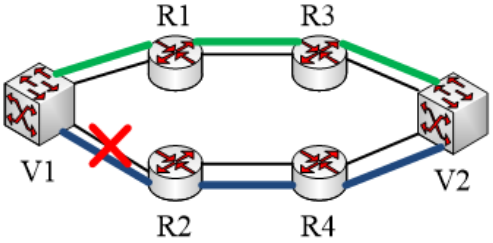
а) Схема захисту з‘єднання(каналу зв’язку)



б) Схема захисту сегменту(вузла)



в) Схема захисту шляху



г) Схема захисту шлюзу

Рисунок 1.6 – Схеми захисту швидкої перемаршрутизації для елементів досліджуваної мережі

1.3 Переваги і недоліки існуючих протоколів захисту шлюзу за замовчуванням

Технологія відмовостійкої маршрутизації направлена на збільшення доступності шлюзу за замовчуванням і включає в себе такі протоколи [14]:

1. Протокол маршрутизації «гарячого» резерву HSRP (Hot Standby Router Protocol) був розроблений компанією Cisco Systems. На даний момент в якості основного стандарту, описує даний протокол, прийнятий документ RFC 2281, написаний представниками Cisco Systems і Juniper Networks.

Протокол HSRP вирішує завдання доступності та відмовостійкості шлюзу, заданого за замовчуванням. Досягається це за рахунок використання у двох і більше маршрутизаторів або комутаторів третього рівня одної IP-адреси і MAC-адреси так званого віртуального маршрутизатора. Така група маршрутизаторів / L3-комутаторів називається HSRP-групою. При цьому клієнти мережі працюють з віртуальним маршрутизатором, а протокол в свою чергу працює з фізичними пристроями HSRP-групи, забезпечуючи таким чином прозору реалізацію отказоустойчивого шлюзу для клієнтів. Для реалізації доступності та відмовостійкості шлюзу алгоритм вводить поняття активного і резервного маршрутизаторів, а також групи резервування. Для коректного та своєчасного перемикання на резервний шлюз використовується два види таймерів: таймер вітання, протягом якого маршрутизатори і L3-комутатори з однієї групи резервування очікують пакета вітання від активного вузла і таймер утримання, після закінчення якого резервний маршрутизатор посилає пакет з повідомленням про відмову активного маршрутизатора і бере на себе його роль.

2. Протокол VRRP (Virtual Router Redundancy Protocol), як і решта протоколів сімейства FHRP призначений для збільшення доступності маршрутизаторів виконуючих роль шлюзу. Це досягається шляхом об'єднання групи маршрутизаторів в один віртуальний маршрутизатор та призначення їм загальної IP-адреси, яка і буде використовуватися як шлюз за замовчуванням для комп'ютерів в мережі.

Фактично, віртуальний маршрутизатор – це група інтерфейсів маршрутизаторів, які знаходяться в одній мережі і розділяють VRID (Virtual Router Identifier) і віртуальну IP-адресу. VRRP – маршрутизатор може перебувати в декількох віртуальних маршрутизаторах, кожен з унікальною комбінацією VRID/I - адресу. Відповідності між VRID та IP-адресою повинні бути однаковими

на всіх маршрутизаторах в одній мережі. У будь-який момент часу тільки один з фізичних маршрутизаторів виконує маршрутизацію трафіку, тобто, стає VRRP Master router, інші маршрутизатори в групі стають VRRP Backup router.

Вибір головного віртуального маршрутизатора проводиться автоматично, ним стає маршрутизатор з найбільшим пріорітетом. Взагалі на процес вибору можна вплинути двома способами. По-перше, якщо в як адресу віртуального маршрутизатора вказати адресу інтерфейсу маршрутизатора, то цей пристрій буде головним за замовчуванням. По друге, при налаштуванні VRRP для кожного маршрутизатора обов'язково вказується пріоритет, і пристрій з найвищим пріоритетом стає головним. Тобто, якщо поточний VRRP Master router стає недоступним, то його роль бере на себе один з VRRP Backup маршрутизаторів, той у якого найвищий пріоритет. Завдання пріоритету дозволяє визначити більш пріоритетні шляхи адміністративно. Backup – маршрутизатор не буде намагатися перехопити на себе роль Master-маршрутизатора, якщо тільки у нього не вищий пріоритет, ніж у поточного Master-маршрутизатора. VRRP дозволяє адміністративно заборонити перехоплення ролі Master-маршрутизатора. Виключення з цього правила – це VRRP – маршрутизатор завжди буде ставати Master, якщо він власник IP-адреси, що привласнена віртуальному маршрутизатору. У кожному віртуальному маршрутизаторі тільки Master відправляє періодичні VRRP - оголошення на зарезервовану групову адресу. На канальному рівні в якості MAC-адреси відправника VRRP - оголошень використовується віртуальна MAC- адреса.

Під час своєї роботи VRRP - маршрутизатор може перебувати в трьох станах: ініціалізація, яке настає відразу після завершення налаштування протоколу, головний віртуальний маршрутизатор і підлеглий віртуальний маршрутизатор. На стадії ініціалізації відбувається вибір головного віртуального маршрутизатора з групи.

Використання протоколу VRRP для підвищення надійності комп'ютерних мереж є ефективним. Протокол простий в налаштуванні, а сама настройка зводиться до формування віртуальних маршрутизаторів. При відмові головного віртуального маршрутизатора відбувається автоматичний перехід (без ручного конфігурації і зміни налаштувань) на підлеглий віртуальний маршрутизатор і мережу продовжує функціонувати в штатному режимі.

Якщо поточний VRRP Master router стає недоступним, то його роль бере на себе один з VRRP Backup маршрутизаторів, той у якого найвищий пріоритет.

Завдання пріоритету дозволяє визначити більш пріоритетні шляхи адміністративно. Backup – маршрутизатор не буде намагатися перехопити на себе роль Master-маршрутизатора, якщо тільки у нього не вищий пріоритет, ніж у поточного Master-маршрутизатора. VRRP дозволяє адміністративно заборонити перехоплення ролі Master-маршрутизатора. Виключення з цього правила – це VRRP – маршрутизатор завжди буде ставати Master, якщо він власник IP- адреси, що привласнена віртуальному маршрутизатору. У кожному віртуальному маршрутизаторі тільки Master відправляє періодичні VRRP - оголошення на зарезервовану групову адресу. На канальному рівні в якості MAC-адреси відправника VRRP - оголошень використовується віртуальна MAC- адреса.

3. Протокол GLBP (Gateway Load Balancing Protocol) працює аналогічно, але не ідентично іншим протоколам резервування шлюзу, таким як HSRP і VRRP. Ці протоколи дозволяють декільком маршрутизаторам брати участь у сконфігурованій віртуальній групі маршрутизаторів із загальною віртуальною IP-адресою. Один член групи вибирається активним маршрутизатором, в той час як інші залишаються неактивними доти, поки не відбудеться збій з активним маршрутизатором. При цьому ці резервні маршрутизатори володіють ресурсами, які майже не використовуються протягом усього часу експлуатації цієї системи. GLBP забезпечує розподіл навантаження на кілька маршрутизаторів використовуючи одну віртуальну IP-адресу та кілька віртуальних MAC-адресів. Кожний хост налаштований з однаковою віртуальною IP-адресою і всі маршрутизатори у віртуальній групі беруть участь у передачі пакетів. Маршрутизатори відправляють один одному повідомлення hello кожні 3 секунди.

4. Протокол CARP створювався командою OpenBSD як вільна альтернатива протоколам HSRP і VRRP. Розробка даного протоколу була завершена в жовтні 2003 року.

Протокол CARP (Common Address Redundancy Protocol) мережевий протокол, основним завданням якого є використання однієї IP-адреси кількома хостами в межах сегмента мережі. CARP є вільною, безпечною (в тій мірі, в якій взагалі можна говорити про безпеку протоколу ARP) альтернативою протоколам VRRP і HSRP. CARP дозволяє виділити групу хостів у тій частині мережі і призначити їй один IP-адреса. Така група називається «redundancy group» (група надмірності). В межах цієї групи один з вузлів стає «головним», а решта позначаються як «резервні». У кожен момент часу майстер-хост відповідає на ARP-запити до призначеного IP-адресою і обробляє трафік, що йде до цією

адресою. Кожен хост одночасно може належати до декількох груп.

Характеристики протоколів наведено в табл.1.1

Таблиця 1.1 – Характеристика протоколів захисту шлюзу за замовчуванням

Характе-ристика	HSRP	VRRP	GLBP	CARP
Застосування	Cisco Proprietary	IEEE Standard	Cisco Proprietary	Not a standard (BSD based OC)
Стандарт	RFC 2281	RFC 5798	Ні	Ні
Рівень моделі OSI	Мережний	Мережний	Мережний	Мережний
Балансування навантаження	Не підтримується	Підтримується	Підтримується	Підтримується
IPv6	Підтримується	Підтримується	Підтримується	Підтримується
Переваги	– легка конфігурація; – низьке навантаження мережі службовим трафіком.	– спрощене управління мережею; – висока адаптованість; – низьке навантеження мережі службовим трафіком; – балансування навантаження; – мінімізація обчислювальних витрат.	– ефективне використання мережних ресурсів; – висока доступність; – автоматичне балансування навантаження; – низькі витрати на адміністрування; – ефективне проектування рівня доступа.	– відкрита альтернатива HSRP та VRRP; – резервування для брандмауерів та маршрутизаторів; – балансування навантаження.
Недоліки	– неефективний для передачі трафіку реального часу; – слабкий рівень безпеки;	– слабкий рівень безпеки (не включає жодного типу аутентифікації).	– пропрієтарний протокол Cisco; – висока складність управління мережею.	– несумісність з існуючими стандартами; – слабкий рівень безпеки.

Майже всі сучасні протоколи підтримують функцію багатошляхової маршрутизації. В результаті власних практичних досліджень та аналізу результатів багатьох інших наукових досліджень, можна відмітити, що дійсно багатошляхова маршрутизація завдяки забезпеченню балансування навантаження одночасно за множиною шляхів сприяє поліпшенню показників QoS. Важливе місце з позиції застосування багатошляхової маршрутизації відводиться також сфері підвищення відмовостійкості та безпеки ТКМ, в якій традиційно використовується маршрутизація за множиною шляхів, що не перетинаються, в яких спільними є тільки вузли – відправник та отримувач пакетів. Використання маршрутів, що не перетинаються, гарантує, що вихід з ладу або компрометація одного з елементів мережі (вузла або каналу) не спричинять значних пошкоджень телекомунікаційної мережі або ж зловмисник скомпрометує лише один, а не декілька маршрутів, що в свою чергу не дає йому значної можливості керувати мережею, як у разі маршрутизації за шляхами, що перетинаються. Однак реалізація багатошляхової маршрутизації за шляхами, що не перетинаються, завдяки відмові у використанні мережевого ресурсу, що є спільним для множини шляхів, як правило, негативно позначається на продуктивності ТКМ та рівні якості обслуговування в мережі загалом.

Пошук компромісу в питанні забезпечення відмовостійкості та безпеки, з одного боку, та якості обслуговування, з іншого, привів до того, що в деяких важливих випадках вимоги щодо перетинання використовуваних шляхів можна дещо знизити, і використовувати шляхи, які допускають перетин, наприклад, лише за вузлами ТКМ. У таких маршрутах спільними є не тільки вузли відправник та отримувач, але й деякі транзитні вузли, проте вони не містять спільних каналів зв’язку. Це актуально в умовах, коли місцем відмов є, наприклад, радіоканал, причому експлуатаційна надійність вузла, що функціонує на базі сучасного комутаційного обладнання, може відповідати коефіцієнту готовності 0,99999. Інший приклад полягає в тім, що радіоканал безпроводової ТКМ також є основним джерелом компрометації переданих даних на фізичному рівні OSI. Тобто саме в таких випадках, коли до відмов та/або компрометації схильні саме канали зв’язку, а не вузли ТКМ, доцільно використовувати маршрути, що перетинаються лише за вузлами, в такому випадку відбувається підвищення продуктивності мережі із забезпеченням того самого рівня відмовостійкості або безпеки, що й у разі задіяння маршрутів, які не перетинаються [15].

Для розрахунку шляхів у багатошляховій маршрутизації переважно використовуються графокомбінаторні моделі та алгоритми, до переваг яких зазвичай зараховують невисоку обчислювальну складність і високу масштабованість. Прикладом цьому можуть бути модифікації алгоритму Дійкстри, які покладено в основу протоколів багатошляхової маршрутизації SMR (Split Multipath Routing) і AODVM (AODV-Multipath), що використовуються в безпроводових ТКМ, а також за безпечної маршрутизації в MANET згідно з протоколом SPREAD (Secure Protocol for REliable dAta Delivery). Незважаючи на зазначені переваги, графокомбінаторні рішення мають і важливі недоліки. До них належать, насамперед, відсутність використання характеристик потоків пакетів, які передаються, що ускладнює роботу засобів боротьби з перевантаженням каналів зв'язку ТКМ, а також складність розрахунку і регулювання кількості використовуваних шляхів. У зв'язку з цим все більше уваги приділяють використанню потокових моделей, у межах яких характеристики трафіку, що передається в мережі, враховуються повніше порівняно з графокомбінаторними моделями [16].

Висновки по розділу: на даний момент, рішення в цій області, як протокольні так і технологічні не можуть забезпечити перерахованих вище вимог в повному обсязі. Оскільки в сучасних маршрутних протоколах використовуються методи пошуку найкоротшого шляху/мультишляху та графові моделі, то в більшості випадків неможливо враховувати вимоги, що висуваються до рішень відмовостійкості, в частності до рішень відмовостійкої маршрутизації.

Через недосконаліть цих математичних моделей та методів, неможливо врахувати повністю всіх характеристик мережі, що не дозволяє в повній мірі керувати процесом боротьби з перевантаженням каналів зв'язку, ускладнюється реалізація схем захисту елементів мережі в цілому, підвищення рівня відмовостійкості маршрутних рішень в такому випадку практично не можливо.

Є можливості підвищення відмовостійкості за рахунок введення надмірності, але в такому разі з'являється ряд додаткових недоліків, які нівелюють переваги цього вибору. Зокрема, це підвищення вартості мережі в кілька разів, ускладення структури мережі, збільшення витрат на обслуговування мережі та ін.

Отже необхідно шукати інші варіанти рішення проблем пов'язаних з відмовостійкостю, які були знайдені в результаті проведеного аналізу засобів забезпечення відмовостійкості, можна сказати що можливості для реалізації цих

засобів закладені в кожном рівні моделі взаїмодії відкритих систем. Серед них є, як і унікальні рішення для реалізації відмовостійкості так і опосередковані, але головне те, що при грамотному виборі цих можливостей та при правильному комплексному впровадженні можна досягнути очікуваних результатів. А саме були обрані протоколи сімейства FHRP, які на даний момент є одним із найкращих рішень проблем, пов’язаних з рішенням відмовостйкої маршрутизації, комплексно з механізмом FRR швидкой перемашрутизацією.

Конфігурування та реалізація на практиці найкращого по результатам аналізу та дослідження протоколів захисту шлюзу за замовчуванням разом з засобами швидкої перемаршрутизації FRR наведені в наступних розділах.

Враховуючи все вище сказане наша наукова та практична задача, пов’язана з вибором та вдосконаленням нової математичної моделі багатошляхової маршрутизації, в основі б якої лежала потокова модель і яка б дозволяла реалізувати можливость маршрутим не перетинатися одне з одним за вузлами і каналами. Такі моделі можуть бути покладені в основу відповідних маршрутних протоколів для забезпечення заданого рівня якості обслуговування, підвищення безпеки даних, що передаються, а також підвищення відмовостійкості й ефективного використання мережевих ресурсів.

‘

2 МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ ПРОЦЕСІВ ВІДМОВОСТІЙКОСТІ В СЕРЕДОВИЩІ MATLAB

2.1 Опис обраної математичної моделі відмовостійкої маршрутизації з балансуванням навантаження

Для підвищення оперативності реагування на можливі відмови в обслуговуваннні пакетів, викликані перевантаженням каналів і черг маршрутизаторів, все частіше використовується засоби відмовостійкої маршрутизації. При цьому важливо, щоб протокол маршрутизації забезпечував різноманітні схеми резурвування ресурсів та елементів мережі: захисту каналу,вузла,шляху, та навіть шлюзу. У зв'язку з цим будемо використовувати модель, яка дозволяє реалізувати наведені схеми резервування. В рамках цієї моделі умови збереження потоку на вузлах і в мережі в цілому та умови запобігання перевантаженню каналів зв'язку будуть доповнені в рамках захисту шлюзу [17].

На сьогоднішній день відомо два основних типа моделей маршрутизації: графові та потокові. Для графових моделей характерно те, що вони враховують лише топологію ТКМ. Для даних моделей задачею маршрутизації є пошук одного найкоротшого шляху (за кількістю переприйомів) на графі – для одношляхової маршрутизації, а також мультишляху – для багато шляхової маршрутизації. Графові моделі (алгоритм Дейкстри та Белмана-Форда) покладені в основу роботи сучасних протоколів маршрутизації таких як OSPF, IS-IS, RIP, IGRP.

Для потокових моделей характерне те, що вони можуть враховувати не тільки структуру мережі, а також параметри каналів зв'язку та потоків трафіка , які ними передаються. Завдяки використанню потокових моделей, можна більш ефективно вирішувати задачі що до балансування навантаження у ТКМ [18].

Структура ТКМ для моделі с багатошляховою маршрутизацією описується за допомогою спрямованого графу G = (M, L).

При цьому M = R∪V – множина вершин графа, що включає в себе дві підмножини:

$R = \{R_i; i = 1, m\}$ – множина вузлів (кількість маршрутизаторів у телеуомунікаційній мережі),

$V = \{V_j;\ j = \overline{1,m}\}$ – множина вершин, що моделють мережі доступа (МД) ТКМ.

В свою чергу множина *R* також включає в себе дві підмножини:

R^+ – множина вершин, що моделюють пригранічні таршрутизатори транспортної мережі, тобто маршрутизатори до яких можуть бути підключені мережі доступу, де $m^+ = \left|R^+\right|$ – загальне число пригранічних маршрутизаторів в ТМ;

R^- – множина вершин що, моделють транзитні маршрутизатори транспортної де $m^- = \left|R^-\right|$ – загальна кількість транзитних маршрутизаторів в ТМ.

Підмножиною множини R^+ є множина R_j^+, що моделює ті пригранічні маршрутизатори, а точніще їх інтерфейси, які утворюють віртуальний маршрутизатор для j – ї мережі доступу, що описується вершиною .

Тоді $m_j^+ = R_j^+$ – загальне число пригранічних маршрутизаторів, що утворюють віртуальний маршрутизатор для *j* – ї мережі доступу. В нашому випадку це маршрутизатори R1,R3,R4,R6.

Таким чином, множини R_j^+ і ($j = \overline{1,v}$) можуть перетинатися, тому що інтерфейси одного і того ж пригранічного маршрутизатора можуть входити до складу різних віртуальних маршрутизаторів.

В свою чергу множина дуг L = E∪W вихідного графа G, включає в себе також дві підмножени:

$E = \{E_{i,j}; i, j = \overline{1,m}, i \neq j\}$ – множина каналів зв'язку транспортної мережі;

$W = \{\mathrm{W}_{i,j}; i, j = \overline{1,v}, \mathrm{j} = \overline{1,m}\}$ – множина ліній доступу, що з'єднують мережі доступу та пригранічні маршрутизатори транспортної мережі.

Кожна дуга $(i, j) \in \mathrm{E}$ зважується параметром $c_{i,j}$, який характеризує пропускну здатність каналу зв'язку, що моделюється.

Запропонована структура ТКС у вигляді графа (рис. 2.1) має 6 вузлів (маршрутизаторів) та 8 дуг (каналів зв'язку), в розривах яких вказані їх пропускні спроможності (1 / с), а також має 2 мережі доступа V1 і V2.

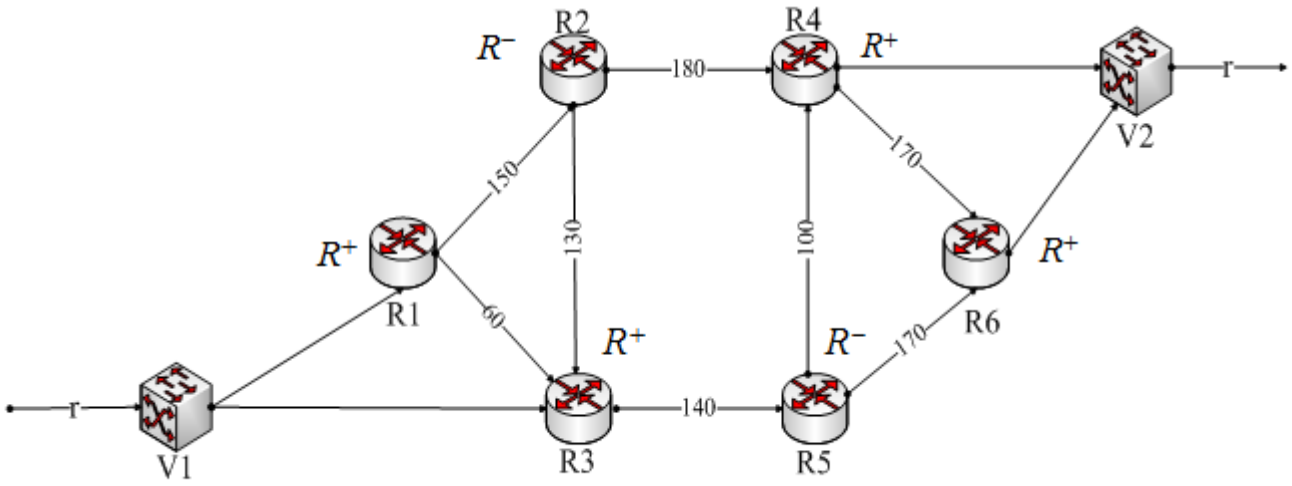


Рисунок 2.1 – Структура ТКС з заданими пропускними здатностями каналів зв’язку

Нехай кожному k-му потокому з множини K, що надходять на приграничні маршрутизатори від мереж доступу, зіставляється ряд параметрів:

r^k – середня інтенсивність пакетів k-го потоку в (1/с);

V_s^k – мережа доступу, яка виступає джерелом k – го потоку;

V_d^k – мережа доступу, яка виступає отримувачем k – го потоку при $k \in K$, де K – множина потоків в мережі.

Тоді в результаті розв’язання задачі відмовостійкої маршрутизації в ТКМ за допомогою пропонованої моделі необхідно розрахувати три типи керуючих змінних, які віднесені до основного маршруту:

– $x_{i,j}^k$ – маршрутна змінна, що характеризує частку k – го потоку в каналі зв’язку ТМ, представленого дугою $E_{i,j}$;

– $y_{i,j}^k$ – змінна доступа, що характеризує частку k – го потоку, що протікає в лінії доступу, представленій дугою $W_{i,j}$, тобто від мережі доступа V_j до приграничного маршрутизатора транспортної мережі;

– $z_{i,j}^k$ – змінна доступу, що характеризує частку k – го потоку, що протікає в лінії доступу, представленій дугою $W_{j,i}$, тобто від приграничного маршрутизатора до мережі доступа V_j.

У ході рішення задачі одноадресної маршрутизації розрахувати множину змінних $x_{i,j}^k$, кожна з яких характеризує долю інтенсивності *k*-го потоку в каналі зв'язку, представленого дугою $E_{i,j} \in E$, і що входить в основний маршрут. Кількість маршрутних змінних $x_{i,j}^k$ відповідає добутку $|K| \cdot |E|$, тоді як загальна кількість змінних доступу кількість змінних доступу $y_{i,j}^k$ і $z_{i,j}^k$ визначається як $v \cdot m^+ \cdot |K|$.

Керуючою зміною є величина $x_{i,j}^k$, яка характеризує частку k-го трафіка в каналі зв'язку між *i*-м та *j*-м вузлами. Відповідно до фізики багатошляхової та одношляхової маршрутизації на зміні $x_{i,j}^k$ накладаються такі обмеження:

$$0 \le x_{i,j}^k \le 1, \tag{2.1}$$

$$x_{i,j}^k \in \{0; 1\}. \tag{2.2}$$

На керуючі змінні згідно з їх фізичним змістом накладається ряд обмежень. При підключенні в даний момент часу мережі доступу лише до одного інтерфейсу віртуального маршрутизатора, як це реалізовано, наприклад, в протоколі HSRP на змінні доступу накладаються обмеження виду:

$$\begin{cases} y_{i,j}^k \in \{0; 1\}; \\ \sum\limits_{j:R_j \in R_i^+} y_{i,j}^k = 1; \end{cases} \text{ та } \begin{cases} z_{j,i}^k \in \{0; 1\}; \\ \sum\limits_{j:R_j \in R_i^+} z_{j,i}^k = 1. \end{cases} \tag{2.3}$$

При можливості балансування трафіка за всіма доступними інтерфейсами віртуального маршрутизатора так, як це реалізовано в протоколах VRRP, GLBP і CARP умови (2.3) замінюються на нерівності:

$$0 \le y_{i,j}^k \le 1 \text{ та } 0 \le z_{i,j}^k \le 1. \tag{2.4}$$

Крім того, на додаток до (2.4) мають місце такі умови:

$$\begin{cases} \sum_{R_j \epsilon R_p^+} y_{p,j}^k = 1, V_p = V_s^k; \\ \sum_{R_j \epsilon R_h^+} z_{j,h}^k = 1, V_h = V_d^k. \end{cases} \quad (2.5)$$

Ці умови вводяться для того, щоб не допустити втрат пакетів на ділянках «мережа доступу – віртуальний маршрутизатор ТМ» і «віртуальний маршрутизатор ТМ – мережа доступу» (2.5).

Фізичний зміст змінних обмежень (2.1-2.2) визначає можливість розгалуження потоку за шляхами мережі, тобто трафік може передаватися як одним, так і множиною шляхів. У ході розв'язання маршрутних задач необхідно не допустити втрати пакетів на мережевих вузлах та у мережі в цілому. Для цього необхідно забезпечити виконання умови збереження потоку:

$$\begin{cases} \sum_{j:(i,j)\in E} x_{ij}^k - \sum_{j:(j,i)\in E} x_{ji}^k = 0, & k \in K, i \neq s_k, t_k; \\ \sum_{j:(i,j)\in E} x_{ij}^k - \sum_{j:(j,i)\in E} x_{ji}^k = 1, & k \in K, i = s_k; \\ \sum_{j:(i,j)\in E} x_{ij}^k - \sum_{j:(j,i)\in E} x_{ji}^k = -1, & k \in K, i = t_k. \end{cases} \quad (2.6)$$

Для забезпечення узгодженості при розрахунку керуючих змінних, що відповідають за реалізацію відмовостійкої маршрутизації, важливо виконати дещо видозмінені у порівнянні з (2.6) умови збереження потоку:

$$\begin{cases} \sum_{j:(i,j)\in E} x_{ij}^k - \sum_{j:(j,i)\in E} x_{ji}^k = \sum_{j:(j,i)\in E} y_{ij}^k; k \epsilon K, R_i \epsilon R^+, V_p = V_s^k; \\ \sum_{j:(i,j)\in E} x_{ij}^k - \sum_{j:(j,i)\in E} x_{ji}^k = 0;\ k \epsilon K, R_i \epsilon R^-; \\ \sum_{j:(i,j)\in E} x_{ij}^k - \sum_{j:(j,i)\in E} x_{ji}^k = \sum_{j:(j,i)\in E} -z_{ij}^k; k \epsilon K, R_i \epsilon R^+, V_h = V_d^k. \end{cases} \quad (2.7)$$

В (2.7) індекс *j* вказує номер вхідного або вихідного інтерфейсу *i* –го маршрутизатора, через який *k* -й потік відповідно надходить або відправляється через маршрутизатор. Умови (2.7) гарантують відсутність втрат пакетів на маршрутизаторах ТМ та в комунікаційній системі в цілому, а також те, що потік будь-якого користувача з МД приймається та обслуговується ТМ.

Для забезпечення відмовостійкості ТКМ в цілому, в якій МД з ТМ з'єднані через певний віртуальний інтерфейс/інтерфейси маршрутизатора, вводяться додаткові керуючі змінні, які визначають резервний шлях для тих самих відправника та одержувача. З математичної точки зору необхідно розрахувати наступні додаткові керуючі змінні:

– $x_{i,j}^k$ – маршрутна змінна, що характеризує частку *k* – го потоку в каналі зв'язку $E_{i,j}$ резервного шляху для ТМ;

– $y_{i,j}^k$ – змінна доступа, що характеризує частку *k* – го потоку, що протікає в резервній лінії доступу $W_{i,j}$;

– $z_{i,j}^k$ – змінна доступу, що характеризує частку *k* – го потоку, що протікає в резервній лінії доступу $W_{j,i}$.

Як і у випадку формування основного маршруту, змінні доступу для резервного шляху обмежені умовами, аналогічними до (2.3) та (2.5). Крім того, ті самі умови (2.4)-(2.5) відповідно повинні запобігати втратам пакетів і забезпечити збереження потоку в транспортній мережі для резервного шляху.

Для запобігання можливого перевантаження каналів зв'язку ТМ вводяться умови (2.9).

Для реалізації схеми захисту шлюзу за замовчуванням з можливістю балансування навантаження за всіма доступними інтерфейсами віртуального маршрутизатора в модель вводяться такі нелінійні умови:

$$\sum_{i:V_i \in V} y_{i,j}^k \bar{y}_{i,j}^k + \sum_{n:E_{j,n} \in E} x_{j,n}^k \bar{x}_{j,n}^k = 0, R_j \in R^+. \qquad (2.8)$$

Якщо ці умови виконуються, це гарантує, що приграничний маршрутизатор *Rj* (тобто всі інцидентні до цього вузла канали зв'язку і лінії доступу) використовується або основним, або резервним шляхом.

У запропонованій моделі отримані також наступні лінійні умови при здійсненні підключення мережі доступу лише до одного інтерфейсу віртуального маршрутизатора (тобто без балансування навантаження):

$$\begin{cases} x_{j,n}^k + \bar{x}_{j,n}^k \le 1; \\ y_{i,j}^k + \bar{y}_{i,j}^k \le 1; \\ z_{i,j}^k + \bar{z}_{i,j}^k \le 1. \end{cases} \quad (2.9)$$

Виконання умов (2.9) гарантує, що приграничний маршрутизатор *Rj* буде використано лише в одному шляху – основному або резервному.

Крім умов збереження потоку (2.7) необхідно виконати умови запобігання перевантаженню каналів зв'язку:

$$r_k \cdot x_{i,j}^k \le c_{i,j}, (i,j) \in E, i \ne j. \quad (2.10)$$

Для запобігання перетину основного та резервного маршрутів необхідно виконати такі умови:

– при захисті (i, j) – каналу

$$x_{i,j}^k \bar{x}_{i,j}^k = 0; \quad (2.11)$$

– при захисті i - го вузла

$$\sum_{i:(i,j)\in E} x_{i,j}^k \bar{x}_{i,j}^k = 0; \quad (2.12)$$

– при захисті шляху

$$\sum_{(i,j)\in E} x_{i,j}^k \bar{x}_{i,j}^k = 0; \quad (2.13)$$

– при захисті шляху(мультишляху) з умовою заборони перетинання основного та резервного маршрутів по каналам зв'язку:

$$\sum_{i:(i,j)\in E} x_{i,j}^{k}\bar{x}_{i,j}^{k} = 0; \qquad (2.14)$$

За критерій оптимальності отримуваних рішень щодо відмовостійкої маршрутизації пропонується вибрати мінімум наступної цільової функції:

$$F = \sum_{k\in K}\sum_{E_{i,j}\in E} c_{i,j}^{k}x_{i,j}^{k} + \sum_{k\in K}\sum_{E_{i,j}\in E} \bar{c}_{i,j}^{k}\bar{x}_{i,j}^{k} + \sum_{k\in K}\sum_{W_{i,j}\in W} f_{i,j}^{o}y_{i,j}^{k} + \sum_{k\in K}\sum_{W_{i,j}\in W} \bar{f}_{j,i}^{o}\bar{y}_{i,j}^{k} + \sum_{k\in K}\sum_{W_{i,j}\in W} f_{j,i}^{p}z_{j,i}^{k} + \sum_{k\in K}\sum_{W_{i,j}\in W} \bar{f}_{j,i}^{p}\bar{z}_{j,i}^{k} \to min \qquad (2.15)$$

де $c_{i,j}^{k}$ та $\bar{c}_{i,j}^{k}$ - метрики каналів зв'язку, які використовуються при обчисленні основного та резервного шляхів відповідно в ТМ;

Вагові коефіцієнти $f_{i,j}^{o}$ і $f_{i,j}^{p}$, у свою чергу, являють собою набір метрик доступу для k -го потоку, який визначає умовну вартість підключення МД до приграничного маршрутизатора при виборі шлюзу за замовчуванням;

В якості метрики було обрано кількість переприйомів (метрика протоколу маршрутизації RIP).

Вагові коефіцієнти $\bar{f}_{i,j}^{o}$ і $\bar{f}_{i,j}^{p}$ мають той самий фізичний зміст, але для резервних ліній доступу. Вибір цих показників в запропонованому рішенні визначається за допомогою зворотних функцій коефіцієнтів готовності ліній доступу.

2.2 Реалізація задачі у середовищі Matlab

Намагаємося сформулювати оптимізаційну задачу через клас лінійного програмування. А саме треба запрограмувати математичну модель так, щоб здійснювався захист будь-якого елементу мережі (шлюзу, каналу, вузла, шляху/мультишляху), враховуючи те, що резервний маршрут не повинен перетинатися з основним і не повинен мати спільних елементів мережі окрім вузла-відправника і вузла-одержувача, які являються мережами доступу V1 і V2.

Окрім того, при реалізації одношляхової маршрутизації маршрутні змінні будуть носити булевий характер, в зв'язку з чим оптимізаційна задача вже буде ставитися до підкласу задач змішаного цілочисельного нелінійного програмування (Mixed Integer Noninear Programming, MINLP).

Для рішення сформульованої оптимізаційної задачі відмовостійкої маршрутизації використаємо середовище MatLab, а саме пакет Optimization Toolbox. При цьому для рішення задач лінійної оптимізації використаємо програму «linprog» та «linprog».

Реалізація задачі в середовищі Matlab для одношляхової маршрутизації наведено на рис. 2.2-2.4.

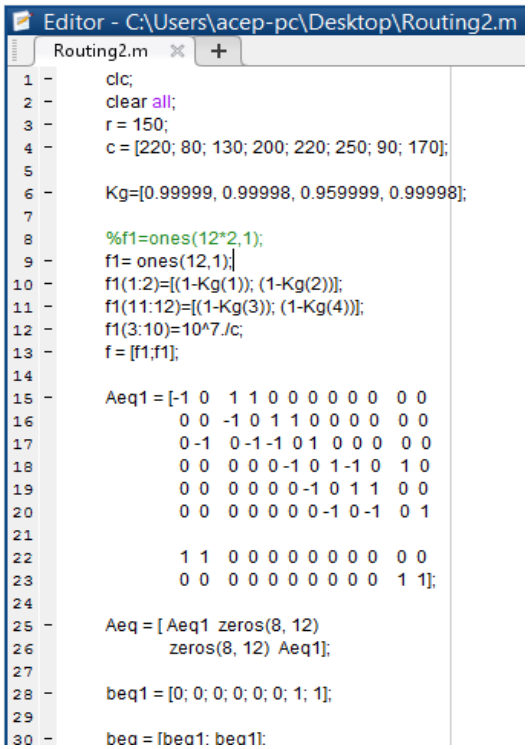


Рисунок 2.2 – Фрагмент программи в середовищі Matlab для одношляхової маршрутизації (частина 1)

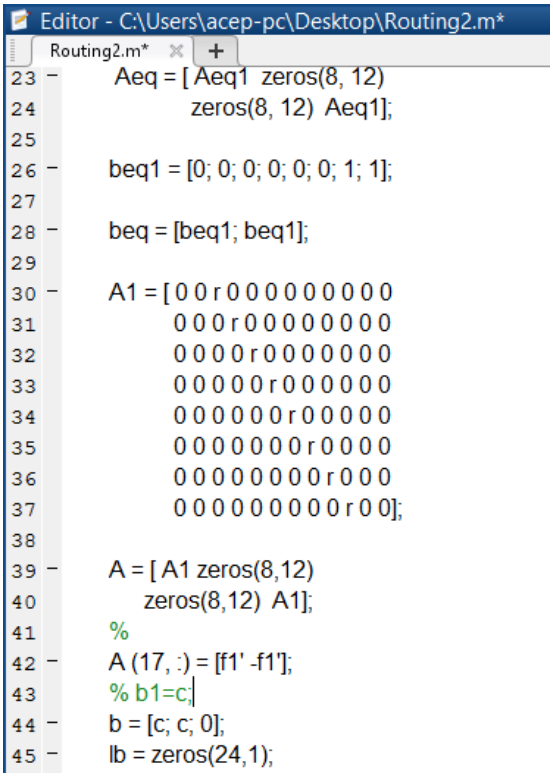


Рисунок 2.3 – Фрагмент программи в середовищі Matlab для одношляхової маршрутизації (частина 2)

```
ub = ones(24,1);
ub(2+12)=0;
%  ub(8+8)=0;
% x0 = ones(24,1);
 [x, fval] = linprog (f,A,b, Aeq,beq,lb,ub);
 intcon=1:1:24;
 %[x, fval]=intlinprog (f,intcon,A,b, Aeq,beq,lb,ub)
  fval;
 y = r * x;
  yy(1,1:12) = x(1:12);
  yy(2,1:12) = x(13:24);
yy'
```

Рисунок 2.4 – Фрагмент программи в середовищі Matlab для одношляхової маршрутизації (частина 3)

Реалізація задачі в середовищі Matlab для багатошляхової маршрутизації з підтримкой балансування навантаження наведено на рис. 2.5-2.7.

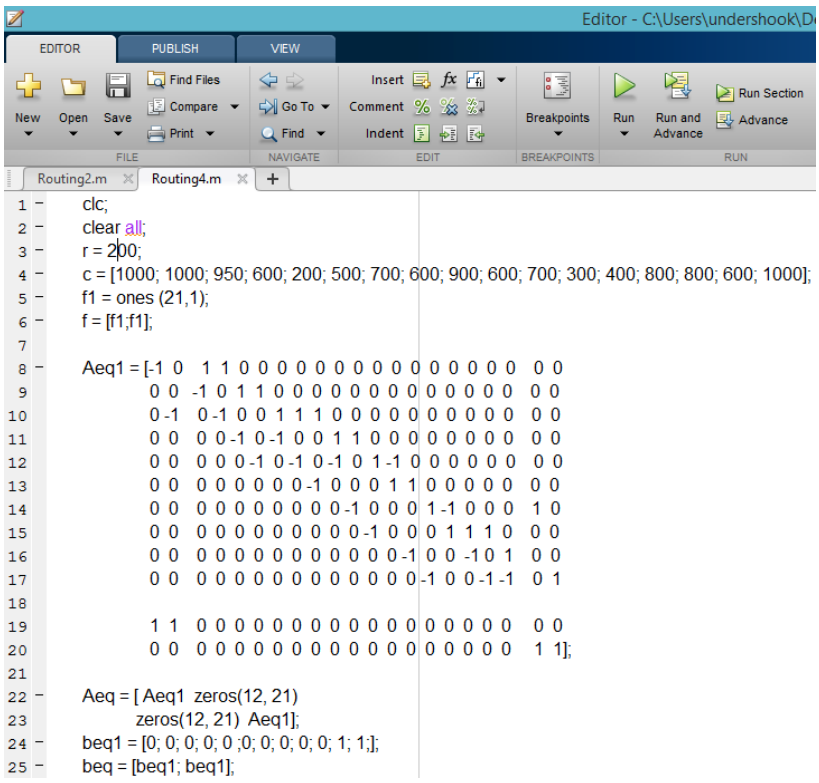


Рисунок 2.5 – Фрагмент программи в середовищі Matlab для багатошляхової маршрутизації з підтримкой балансування навантаження (частина 1)

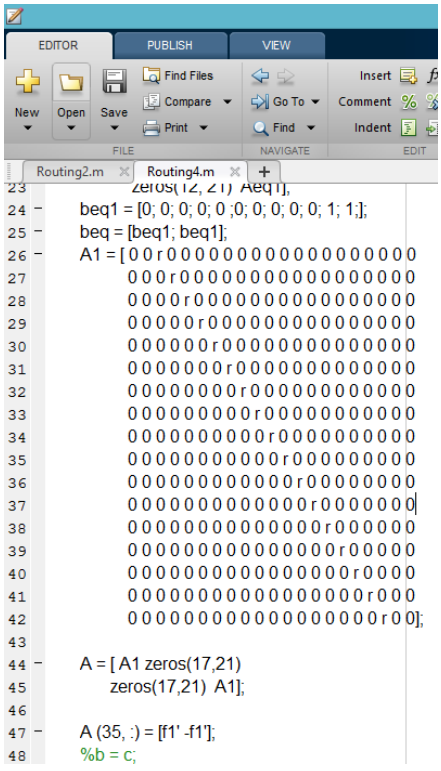


Рисунок 2.6 – Фрагмент программи в середовищі Matlab для багатошляхової маршрутизації з підтримкой балансування навантаження (частина 2)

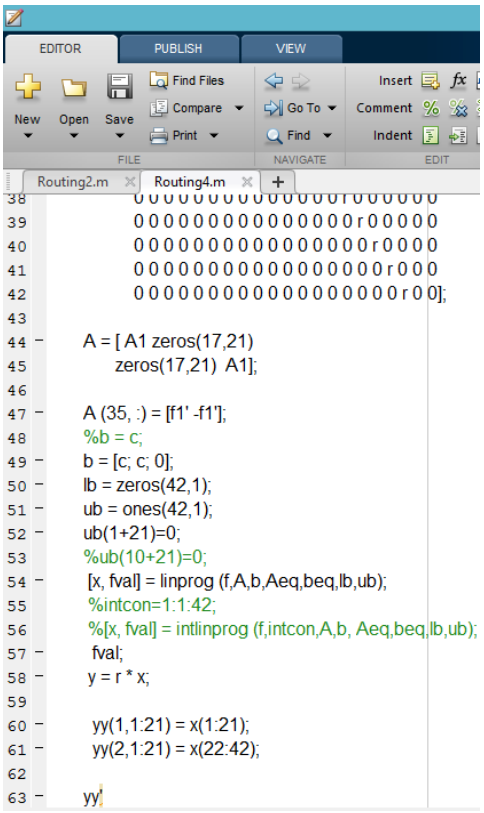


Рисунок 2.7 – Фрагмент программи в середовищі Matlab для багатошляхової маршрутизації з підтримкой балансування навантаження (частина 3)

2.3 Результати дослідження відмовостійкої маршрутизації

Проведемо розрахунки для кількох схем захисту елементів мережі: захисту каналу, захисту вузла, захисту усього шляху/мультишляху, захисту шлюзу. Представимо отримані результати розрахунків у вигляді графо-потокової моделі.

На рис 2.8-2.9 представлено результат реалізації схеми захисту канала R2 → R4 для одношляхової маршрутизації.

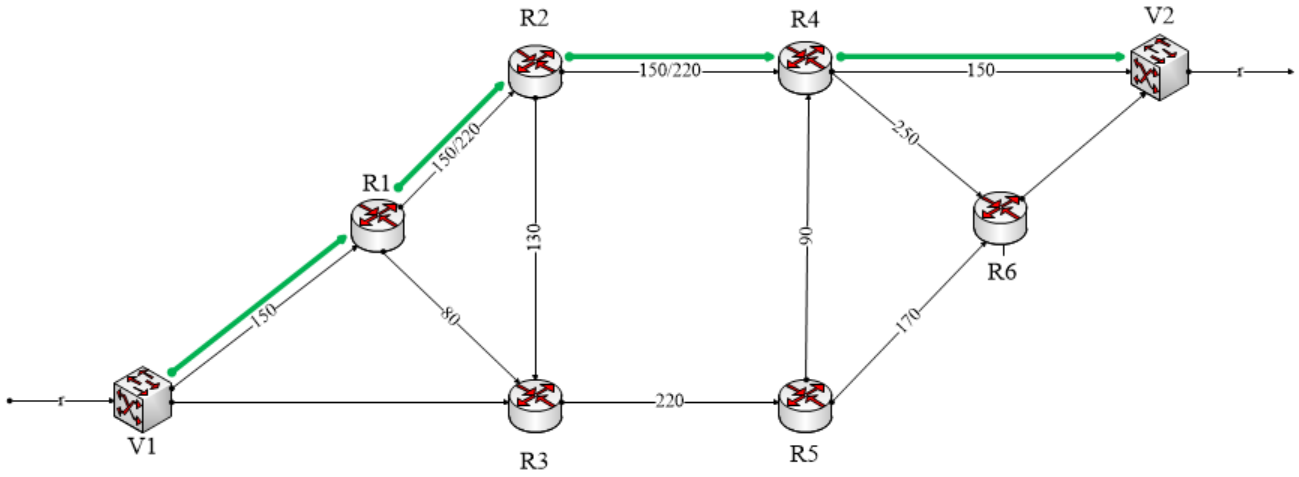


Рисунок 2.8 – Основний маршрут при реалізації схеми захисту канала R2 → R4 при одношляховій маршрутизації

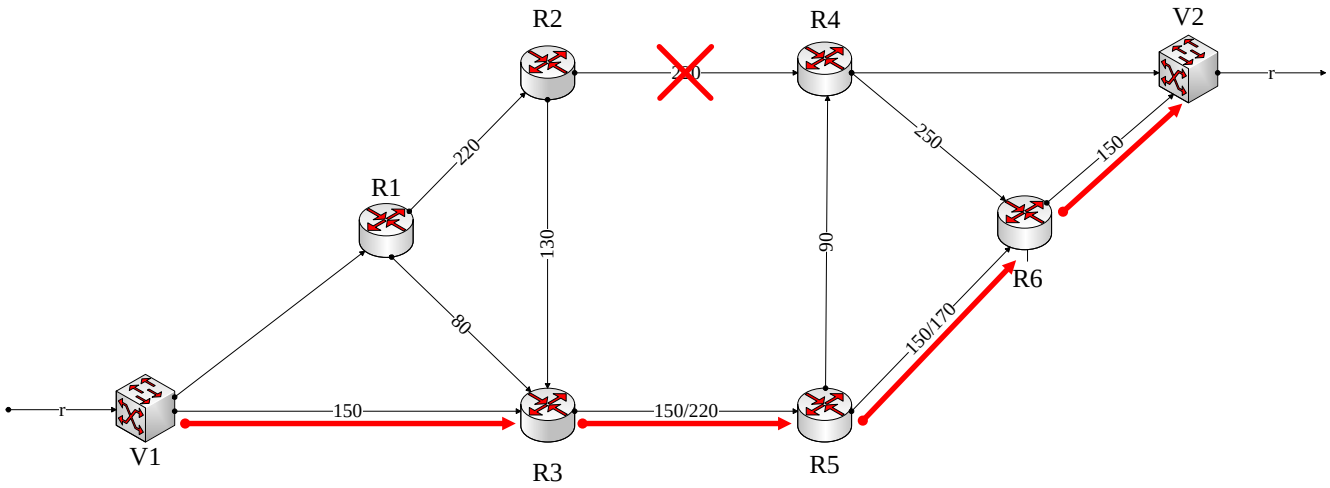


Рисунок 2.9 – Резервний маршрут при реалізації схеми захисту канала R2 → R4 при одношляховій маршрутизації

В такому випадку маршрути проходять через наступні вузли:

– V1 → R1 → R2 → R4 → V2 – Основний маршрут;

– V1 → R3 → R5 → R6 → V2 – Резервний маршрут.

Отже, при формуванні резервного маршруту канал R2 → R4 використано не було, а це означає, що умова захисту цього каналу було виконано.

На рис 2.10-2.11 зображено результат реалізації схеми захисту вузла R4 для одношляхової маршрутизації.

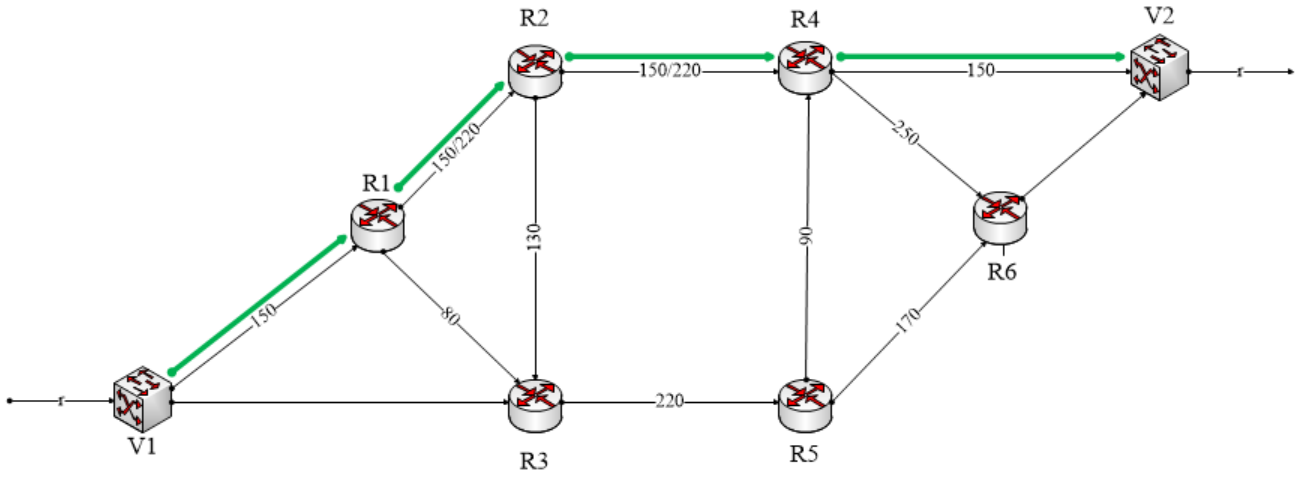


Рисунок 2.10 – Основний маршрут при реалізації схеми захисту вузла R4 для одношляхової маршрутизації

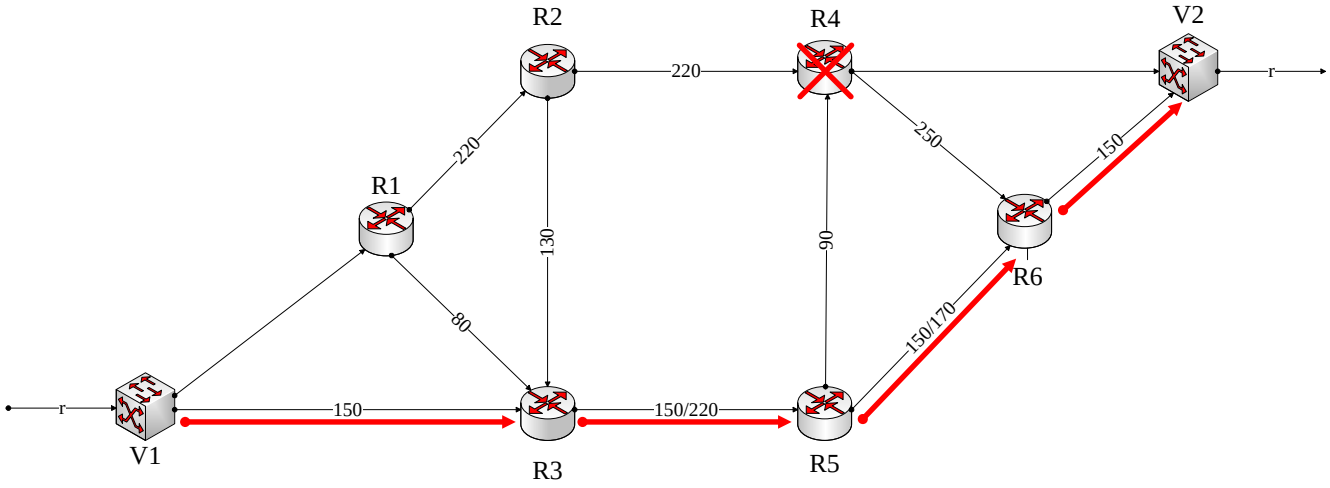


Рисунок 2.11 – Резервний маршрут при реалізації схеми захисту вузла R4 при одношляхової маршрутизації

В такому випадку маршрути проходять через наступні вузли:

– V1 → R1 → R2 → R4 → V2 – Основний маршрут;

– V1 → R3 → R5 → R6 → V2 – Резервний маршрут;

Отже, при формуванні резервного маршруту вузол R4 не використовували, а це означає, що умову захисту цього вузла було виконано.

На рис 2.12-2.13 представлено результат реалізації схеми захисту шлюзу на маршрутизаторі R1 для одношляхової маршрутизації.

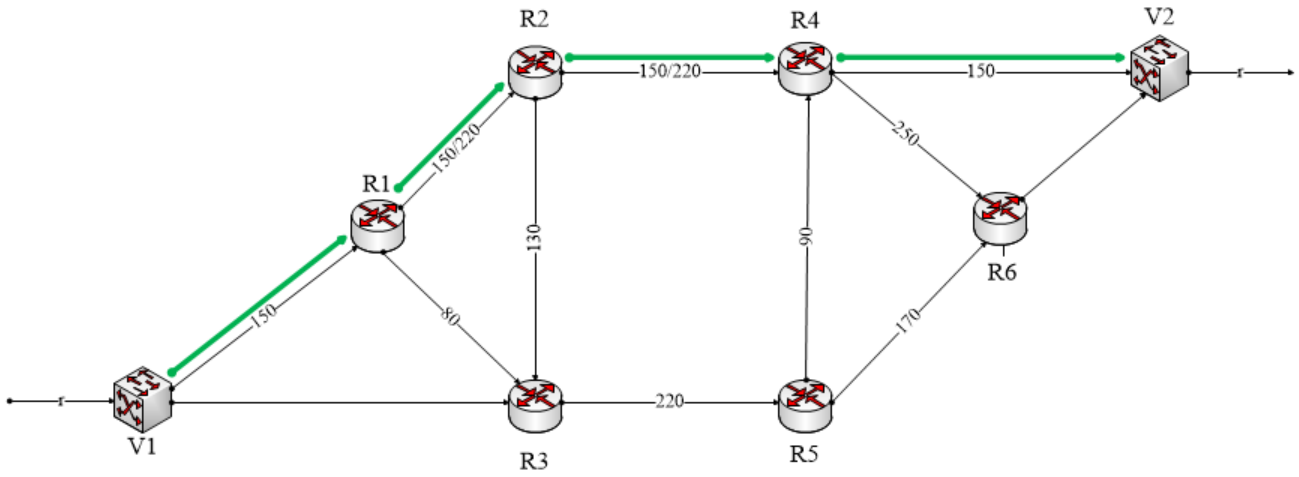


Рисунок 2.12 – Основний маршрут при реалізації схеми захисту шлюза на маршрутизаторі R1 для одношляхової маршрутизації

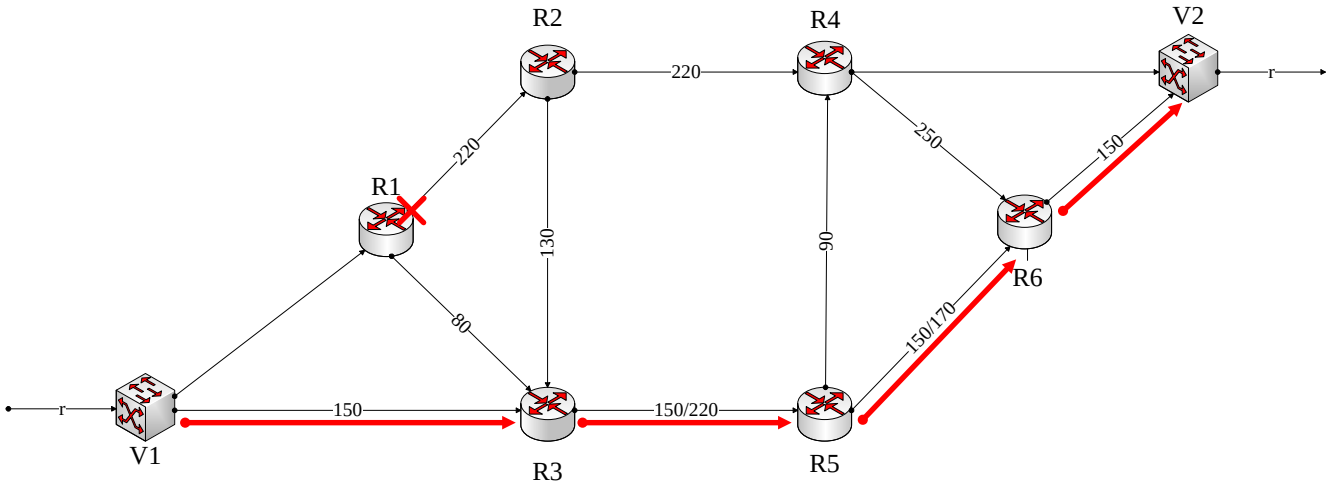


Рисунок 2.13 – Резервний маршрут при реалізації схеми захисту шлюза на маршрутизаторі R1 для одношляхової маршрутизації

В такому випадку маршрути проходять через наступні вузли:

– V1 → R1 → R2 → R4 → V2 – Основний маршрут;

– V1 → R3 → R5 → R6 → V2 – Резервний маршрут.

Отже, при формуванні резервного маршруту вузол R1 не використовували, а це означає, що умову захисту цього вузла було виконано.

На рис 2.14-2.15 показано результат реалізації схеми захисту канала R4 → R7 для багатошляхової маршрутизації з балансуванням.

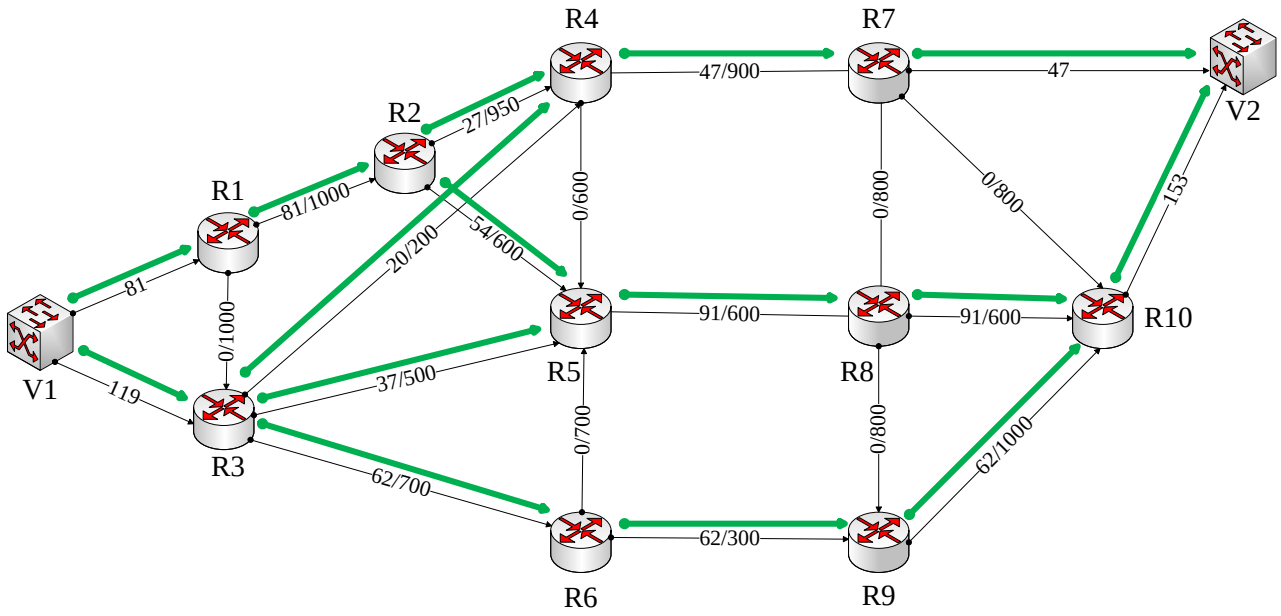


Рисунок 2.14 – Розподіл основного маршруту при реалізації схеми захисту каналу R4 → R7 для багатошляхової маршрутизації з балансуванням

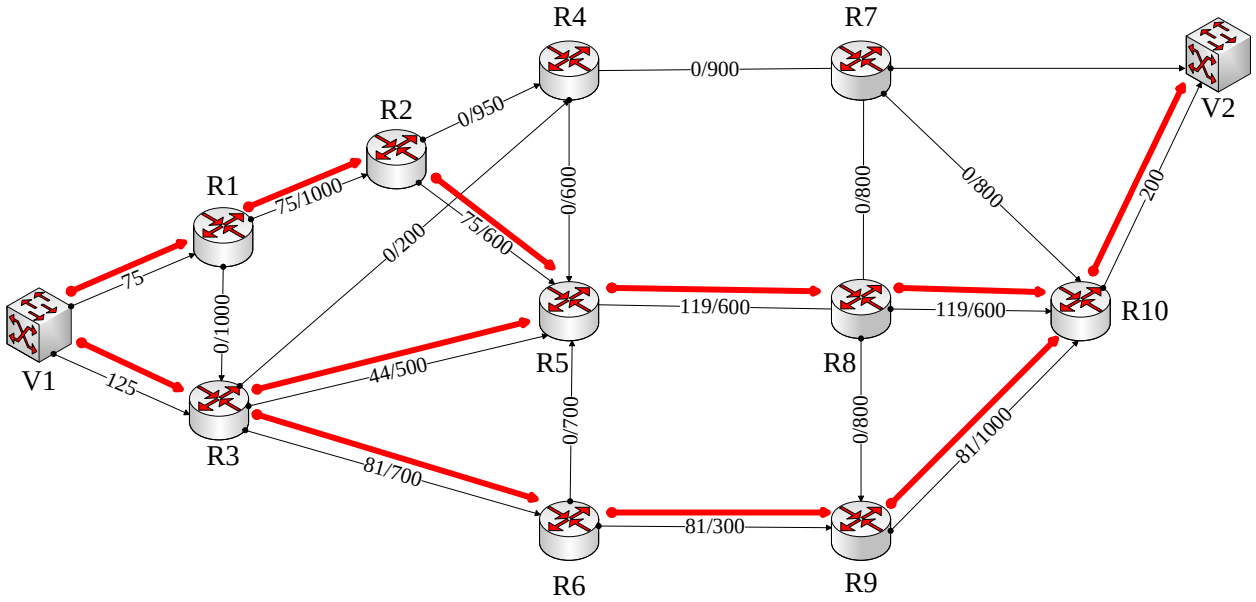


Рисунок 2.15 – Розподіл резервного маршруту при реалізації схеми захисту каналу R4 → R7 для багатошляхової маршрутизації з балансуванням

В такому випадку маршрути проходять через наступні вузли:

– V1 → R1 → R2 → R4 → R7 → V2 – 1-й шлях основного маршруту мультишляху;

– V1 → R1 → R2 → R5 → R8 → R10 → V2 – 3-й шлях основного маршруту мультишляху;

– V1 → R3 → R4 → R7 → V2 – 3-й шлях основного маршруту мультишляху;

– V1 → R3 → R5 → R8 → R10 → V2 – 4-й шлях основного маршруту мультишляху;

– V1 → R3 → R6 → R9 → R10 → V2 – 5-й шлях основного маршруту мультишляху;

– V1 → R1 → R2 → R5 → R8 → R10 → V2 – 1-й шлях резервного маршруту мультишляху;

– V1 → R3 → R5 → R8 → R10 → V2 – 2-й шлях резервного маршруту мультишляху;

– V1 → R3 → R6 → R9 → R10 →V2 – 3-й шлях резервного маршруту мультишляху;

Отже, при формуванні резервного маршруту канал R2 → R4 використано не було, а це означає, що умова захисту цього каналу було виконано.

На рис 2.16-2.17 представлено результат реалізації схеми захисту вузла R4 для багатошляхової маршрутизації з балансуванням.

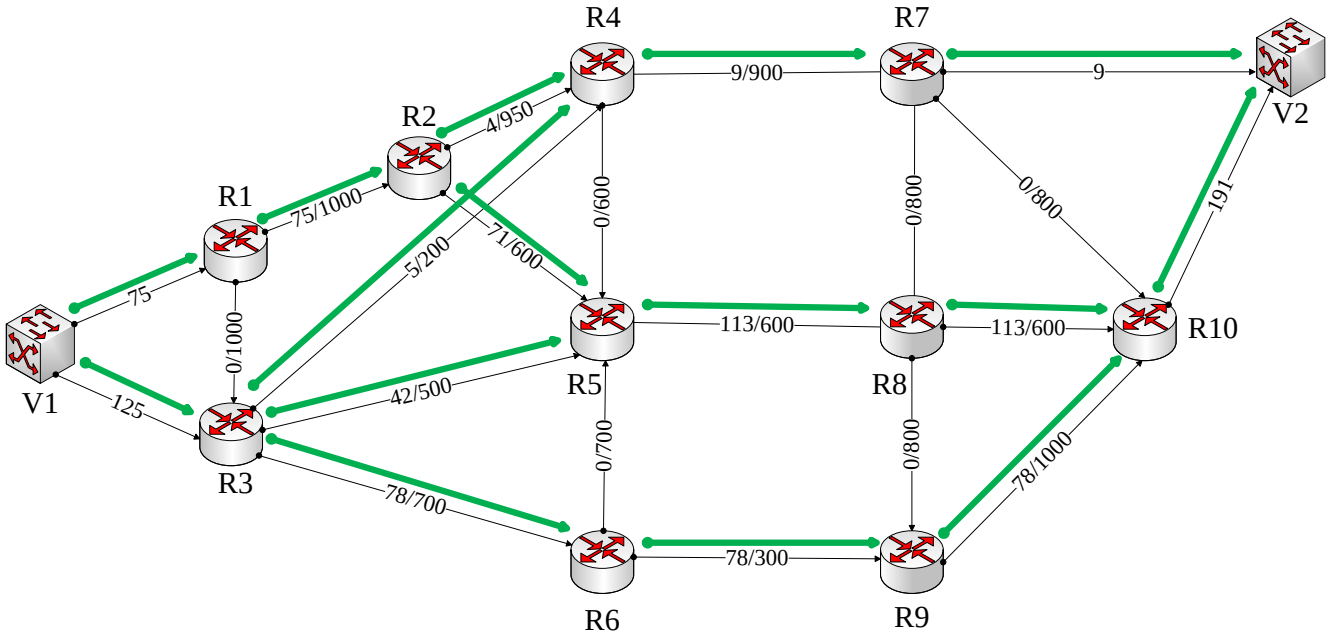


Рисунок 2.16 – Розподіл основного маршруту при реалізації схеми захисту вузла R4 для багатошляхової маршрутизації з балансуванням

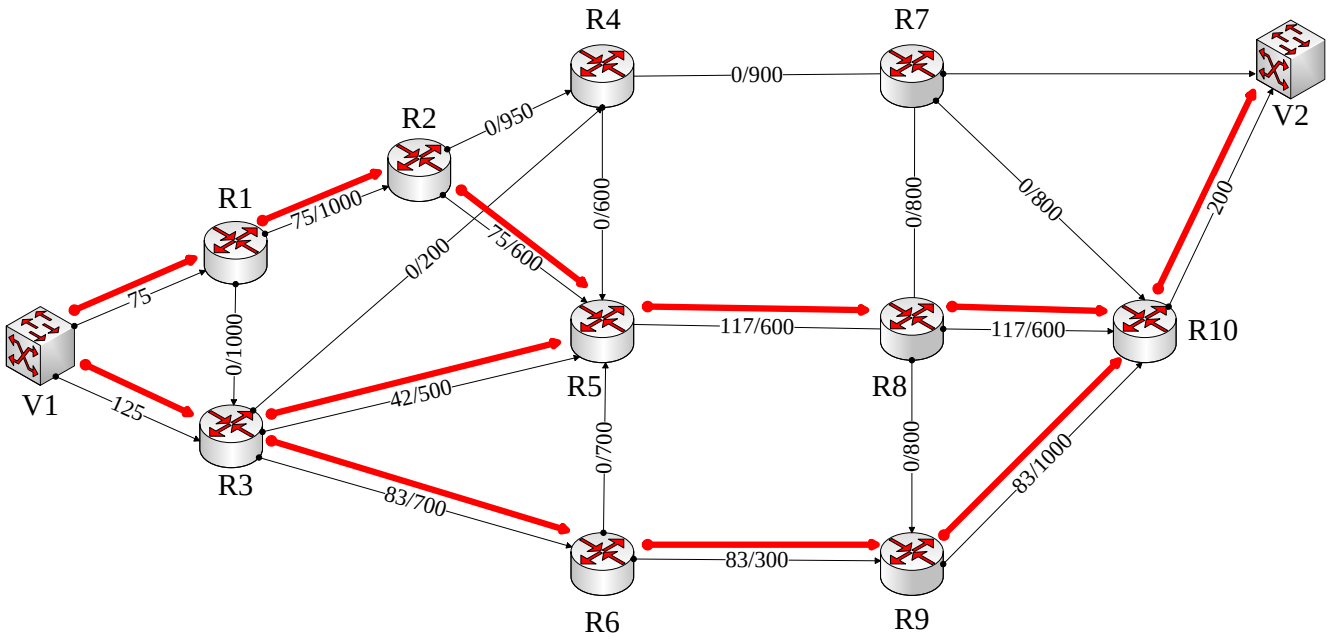


Рисунок 2.17 – Розподіл резервного маршруту при реалізації схеми захисту вузла R4 для багатошляхової маршрутизації з балансуванням

В такому випадку маршрути проходять через наступні вузли:

– V1 → R1 → R2 → R4 → R7 → V2 – 1-й шлях основного маршруту мультишляху;

– V1 → R1 → R2 → R5 → R8 → R10 → V2 – 2-й шлях основного маршруту мультишляху;

– V1 → R3 → R4 → R7 → V2 – 3-й шлях основного маршруту мультишляху;

– V1 → R3 → R5 → R8 → R10 → V2 – 4-й шлях основного маршруту мультишляху;

– V1 → R3 → R6 → R9 → R10 → V2 – 5-й шлях основного маршруту мультишляху;

– V1 → R1 → R2 → R5 → R8 → R10 → V2 – 1-й шлях резервного маршруту мультишляху;

– V1 → R3 → R5 → R8 → R10 → V2 – 2-й шлях резервного маршруту мультишляху;

– V1 → R3 → R6 → R9 → R10 → V2 – 3-й шлях резервного маршруту мультишляху;

Отже, при формуванні резервного маршруту вузол R4 не використовується (суміжні вузли не передають на нього пакети), що говорити про те, що умова його захисту була виконана.

На рис 2.18 зображено результат реалізації схеми захисту шляху з урахуванням умови, що основний та резервний маршрути не мають пересікатися по каналам (2.14).

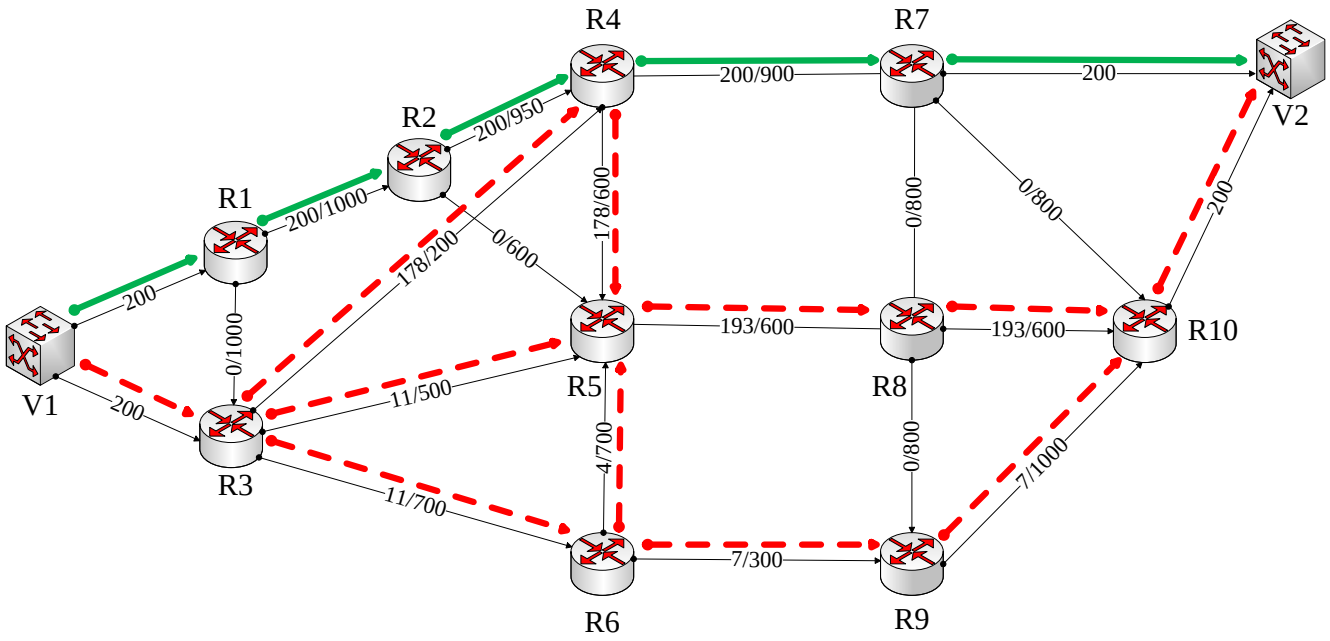


Рисунок 2.18 – Розподіл маршрутів при реалізації схеми захисту шляху (без перетинання по каналам) для багатошляхової маршрутизації з балансуванням

В такому випадку маршрути проходять через наступні вузли:

– V1 → R1 → R2 → R4 → R7 → V2 – Основний маршрут;

– V1 → R3 → R4 → R5 → R8 → R10 → V2 – 1-й шлях резервного маршруту мультишляху;

– V1 → R3 → R5 → R8 → R9 → R10 → V2 – 2-й шлях резервного маршруту мультишляху;

– V1 → R3 → R6 → R5 → R8 → R10 → V2 – 3-й шлях резервного маршруту мультишляху;

– V1 → R3 → R6 → R9 → R10 → V2 – 4-й шлях резервного маршруту мультишляху;

Резервний маршрут не включає в себе жодного каналу зв'язку основного маршруту. Основний і резервний маршрут мають спільний вузол R4, але оскільки умови того, щоб маршрути не можуть пересікатися по вузлам не було, то це говорить про те, що задачу виконано.

На рис 2.19 зображено результат реалізації схеми захисту шляху з урахуванням умови, що основний та резервний маршрути не повинні мати спільних елементів мережі (каналів і вузлів), окрім вузла-відправника та вузла-одержувача (2.14).

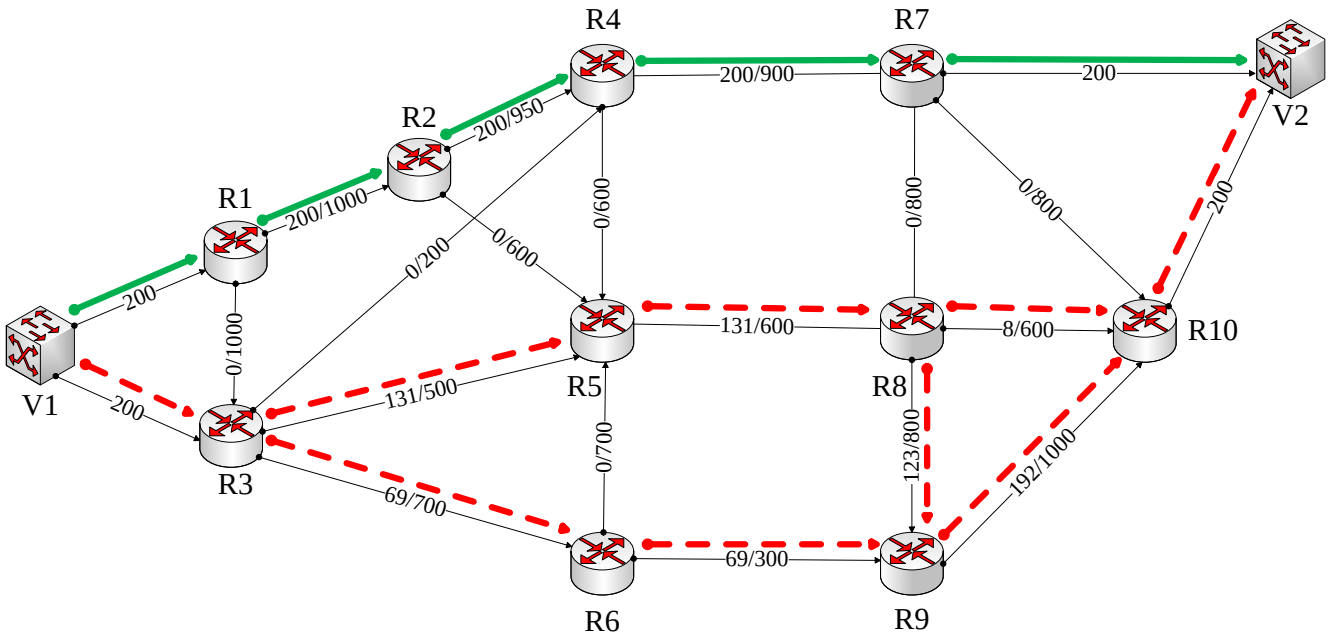


Рисунок 2.19 – Розподіл маршрутів при реалізації схеми захисту шляху (без перетинання по каналам та вузлам) для багатошляхової маршрутизації з балансуванням

В такому випадку маршрути проходять через наступні вузли:

– V1 → R1 → R2 → R4 → R7 → V2 – Основний маршрут;

– V1 → R3 → R5 → R8 → R10 → V2 – 1-й шлях резервного маршруту мультишляху;

– V1 → R3 → R5 → R8 → R9 → R10 → V2 – 2-й шлях резервного маршруту мультишляху;

– V1 → R3 → R6 → R9 → R10 → V2 – 3-й шлях резервного маршруту мультишляху;

Отже, можна помітити що, весь основний маршрут захищено і резервний маршрут не включає в себе жодного його елементу.

На рис 2.20-2.21 зображено результат реалізації схеми захисту шлюза за замовчуванням для багатошляхової маршрутизації з балансуванням. Захищаємо шлюз V1.

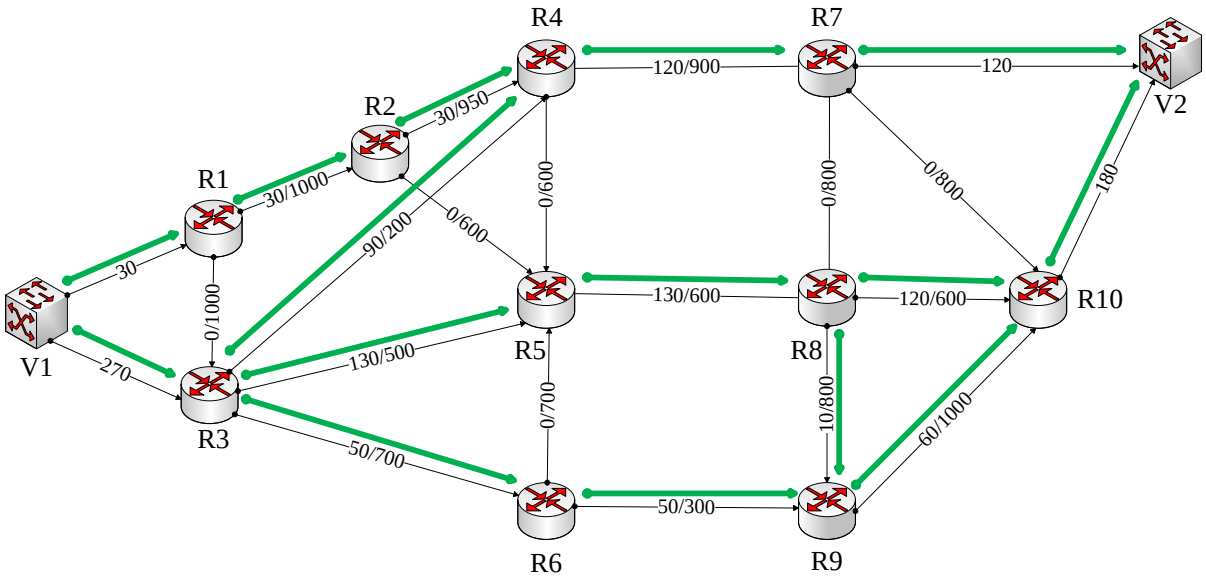


Рисунок 2.20 – Основний маршрут при реалізації схеми захисту шлюзу за замовчувнням для багатошляхової маршрутизації з балансуванням

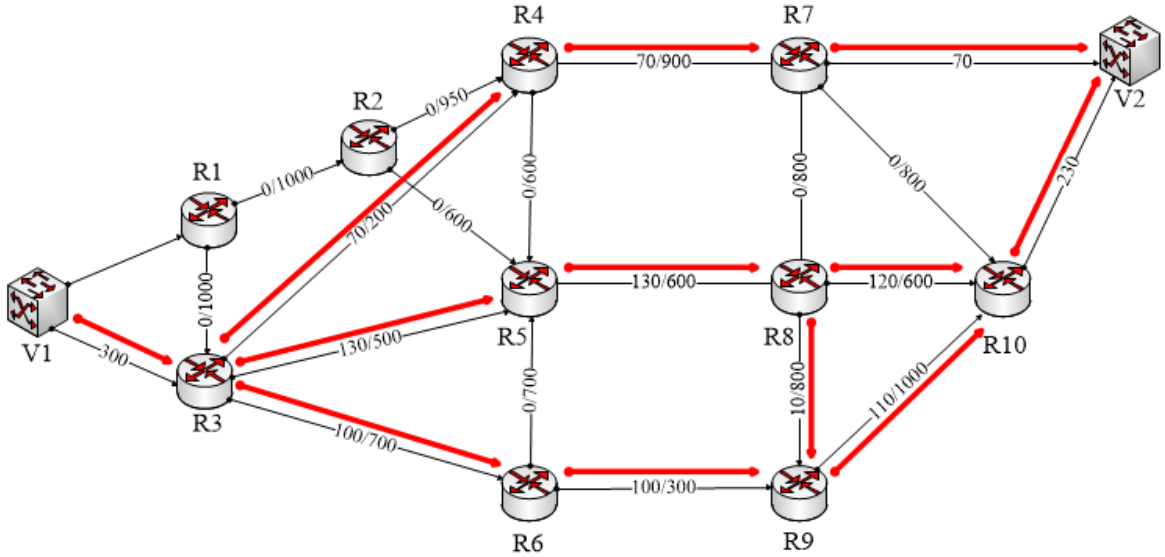


Рисунок 2.21 – Резервний маршрут при реалізації схеми захисту шлюзу за замовчувнням для багатошляхової маршрутизації з балансуванням

В такому випадку маршрути проходять через наступні вузли:

– V1 → R1 → R2 → R4 → R7 → V2 – 1-й шлях основного маршруту мультишляху;

– V1 → R3 → R4 → R7 → V2 – 2-й шлях основного маршруту мультишляху;

– V1 → R3 → R5 → R8 → R10 → V2 – 3-й шлях основного маршруту мультишляху;

– V1 → R3 → R5 → R8 → R9 → R10 → V2 – 4-й шлях основного маршруту мультишляху;

– V1 → R3 → R6 → R9 → R10 → V2 – 5-й шлях основного маршруту мультишляху;

– V1 → R3 → R4 → R7 → V2 – 1-й шлях резервного маршруту мультишляху;

– V1 → R3 → R5 → R8 → R10 → V2 – 2-й шлях резервного маршруту мультишляху;

– V1 → R3 → R5 → R8 → R9 → R10 →V2 – 3-й шлях резервного маршруту мультишляху;

– V1 → R3 → R6 → R9 → R10 → V2 – 4-й шлях резервного маршруту мультишляху;

Отже, можна помітити що, мережа доступа V1 не приймає участі у передачі пакетів на свої суміжні вузли, а це означає, що задачу по захисту шлюзу було виконано.

Представлені схеми захисту елементів мережі дійсно забезпечують покращення надійності мережі. Чим більше елементів мережі захищено (вузол,канал,шлюз,маршрут в цілому), тим більша надійність, адже ймовірність втрати пакетів суттєво зменшується. Але такі рішення відмовостійкої маршрутизації несуть за собою ряд недоліків. Це пов’язано з тим, що використання резервних шляхів так чи інакше потребує додаткового мереженого ресурсу (канального чи буферного) і вони не можуть використовуватися іншими потоками. А це в свою чергу суттєво впливає на продуктивність мережі, а також на її вартість. Таким чином, необхідно ускладнювати математичну модель, щоб ефективно використовувати канали зв’язку, та намагатися повніше враховувати параметри потоків, для раціонального використовування і без того обмеженого ресурса.

Висновки по розділу: в даному розділі було описано математичну, потокову модель, розроблена на основі графікомбінаторних моделей з метою удосконалення алгоритмів та механізмів відмовостійкої маршрутизації. В ході проведення досліджень були отримані результати, які представлені на рис.2.2-2.21 і направлені на відображення роботи одношляхової/багатошляхової відмовостійкої маршрутизації з балансуванням та без балансування навантаження. Результати досліджень не показують всіх необхідних моментів для детального дослідження, так як моделювання показує тільки загальний принцип обраної моделі. Тому в наступному розділі проводяться дослідження протоколів FHRP, а саме HSRP та GLBP, які хоть і побудовані на вище указаних графікомбінаторних моделях, але на основі їх аналізу та практичних дослідженнях можна детально показати переваги та недоліки потокової моделі.

3. ДОСЛІДЖЕННЯ ПРОЦЕСІВ ВІДМОВОСТІЙКОСТІ В ПРОГРАМНО-КОНФІГУРОВАНИХ СИСТЕМАХ

Дослідження протоколів сімейства FHRP, проводилося на основі симуляційного обладнання.

- Graphical Network Simulator – це графічний симулятор мережі, який дозволяє змоделювати віртуальну мережу з маршрутизаторів і віртуальних машин. У відмінності з Cisco Packet Tracer має ряд цікавих особливостей, одна з яких, це можливість з'єднання проектованої топології з реальною мережею. Це дає просто унікальну можливість перевірити на практиці будь-який проект, без використання реального обладнання. Використання WireShark дозволяє провести моніторинг трафіку всередині проектованої топології, що дає додаткову інформацію для розуміння досліджуваних технологій [16].

3.1 Дослідження та аналіз роботи протоколу HSRP на симуляційном обладнанні GNS3

Схема для дослідження протоколу HSRP наведена на рис.3.1.

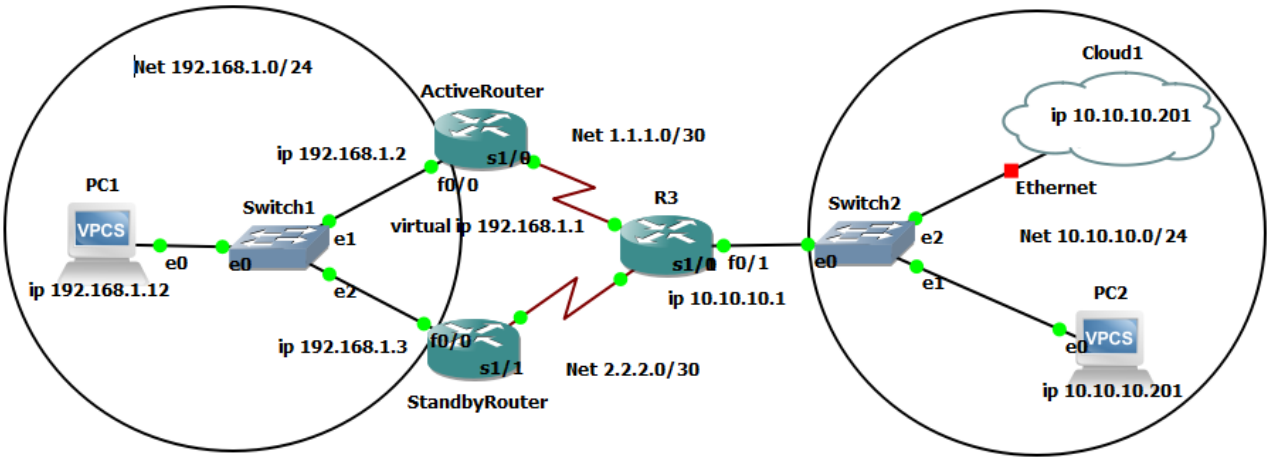


Рисунок 3.1 – Схема для дослідження протоколу HSRP

Для дослідження будемо використовувати 3 маршрутизатори Cisco, комутатори Cisco Catalyst 2960, 6 кабелів Ethernet та 2 ПК з ОС Windows.

Перевірки будемо робити шляхом аналізу мережної доступності з локального комп'ютера (192.168.1.12) до сервера (10.10.10.201) при повному відключенні Active_Router і при відключенні інтерфейсу на R3, що дивиться в бік Active_Router.

Конфігурація інтерфейсів та протоколу HSRP для ActiveRouter наведена на рис.3.2.

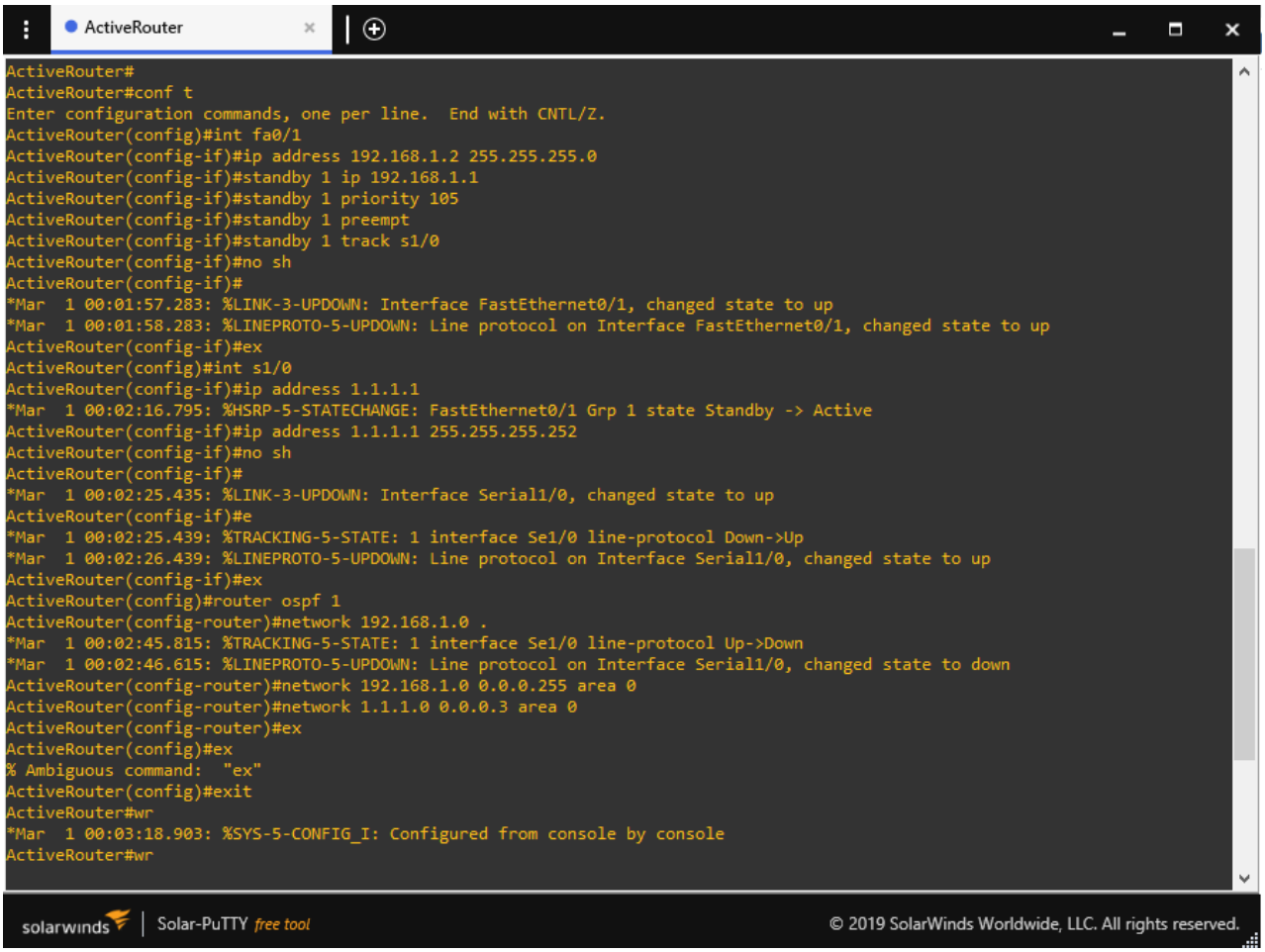


Рисунок 3.2 – Конфігурація інтерфейсів та протоколу HSRP для ActiveRouter

На рис.3.3 наведена аналогічна конфігурація для StandbyRouter.

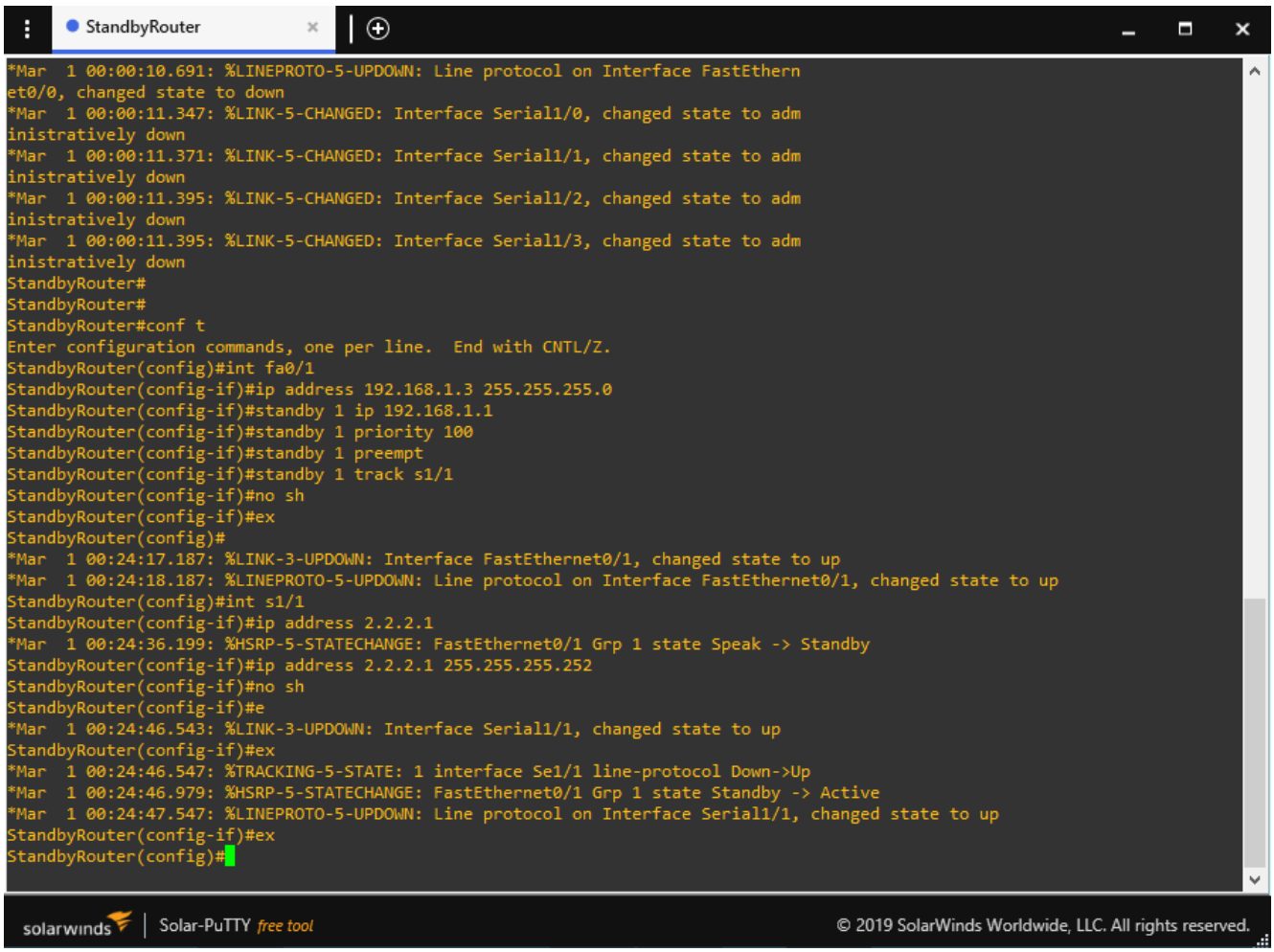


Рисунок 3.3 – Конфігурація інтерфейсів та протоколу HSRP для StandbyRouter

Далі необхідно перевірити правильність налаштування протоколу HSRP та конфігурацію інтерфейсів на маршрутизаторах.

На рис.3.4 наведено перевірка налаштування інтерфейсів та протоколу HSRP на маршрутизаторі ActiveRouter за допомогою команд «Ping» та «Show standby».

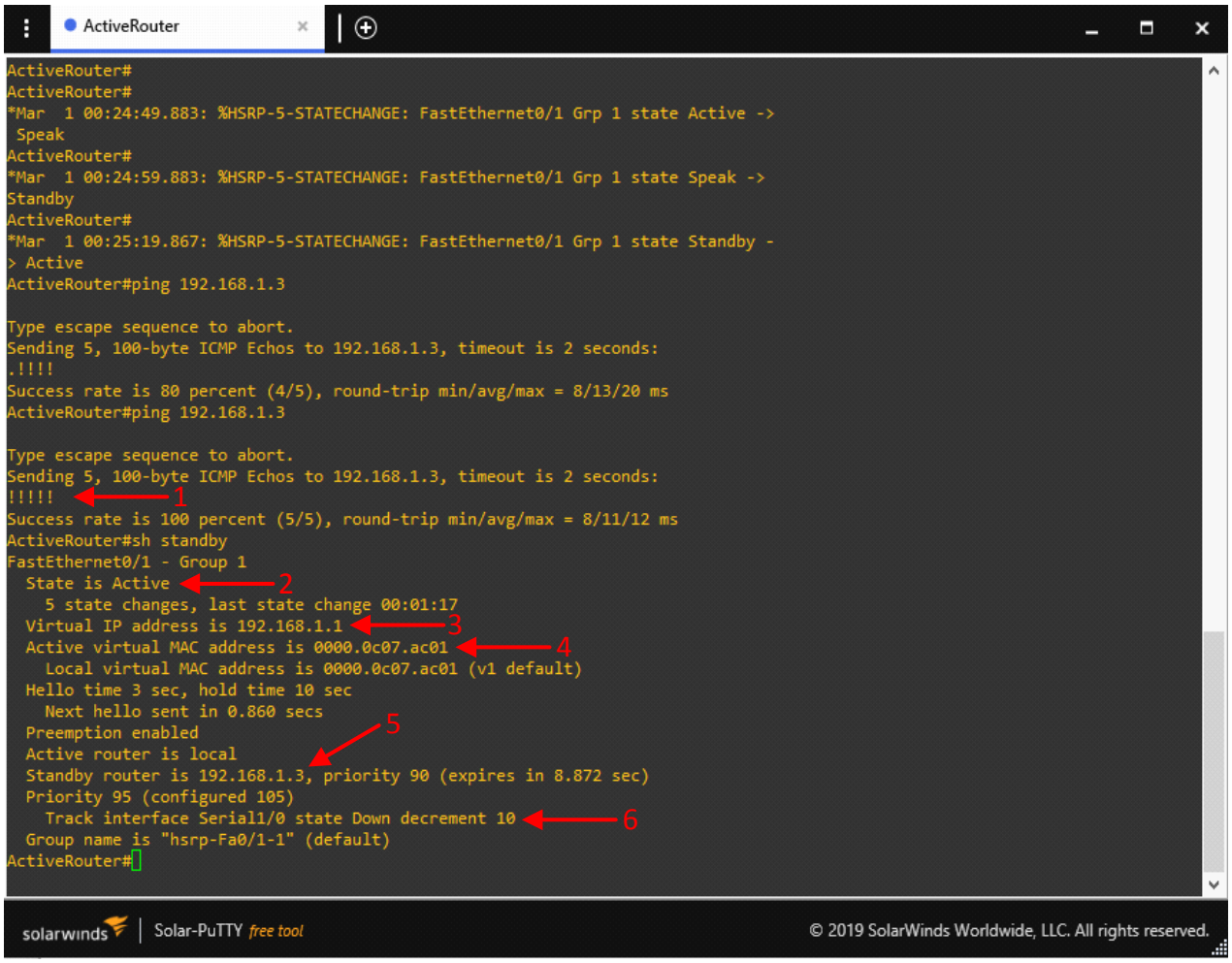


Рисунок 3.4 – Перевірка налаштування інтерфейсів та протоколу HSRP на маршрутизаторі ActiveRouter

На рис. 3.4 наведені такі позначення:

1 – мережева доступність з Standby_Router присутня;

2 – наш роутер має статус Active;

3 – налаштований віртуальний адрес;

4 – віртуальний MAC адрес за замовчуванням;

5 –Standby роутер має IP, налаштоване вище;

6 – контроль інтерфейса serial 1/0 увімкнений.

Перевірка налаштування інтерфейсів та протоколу HSRP на маршрутизаторі StandbyRouter за допомогою команд «Ping» та «Show standby» наведено на рис3.5.

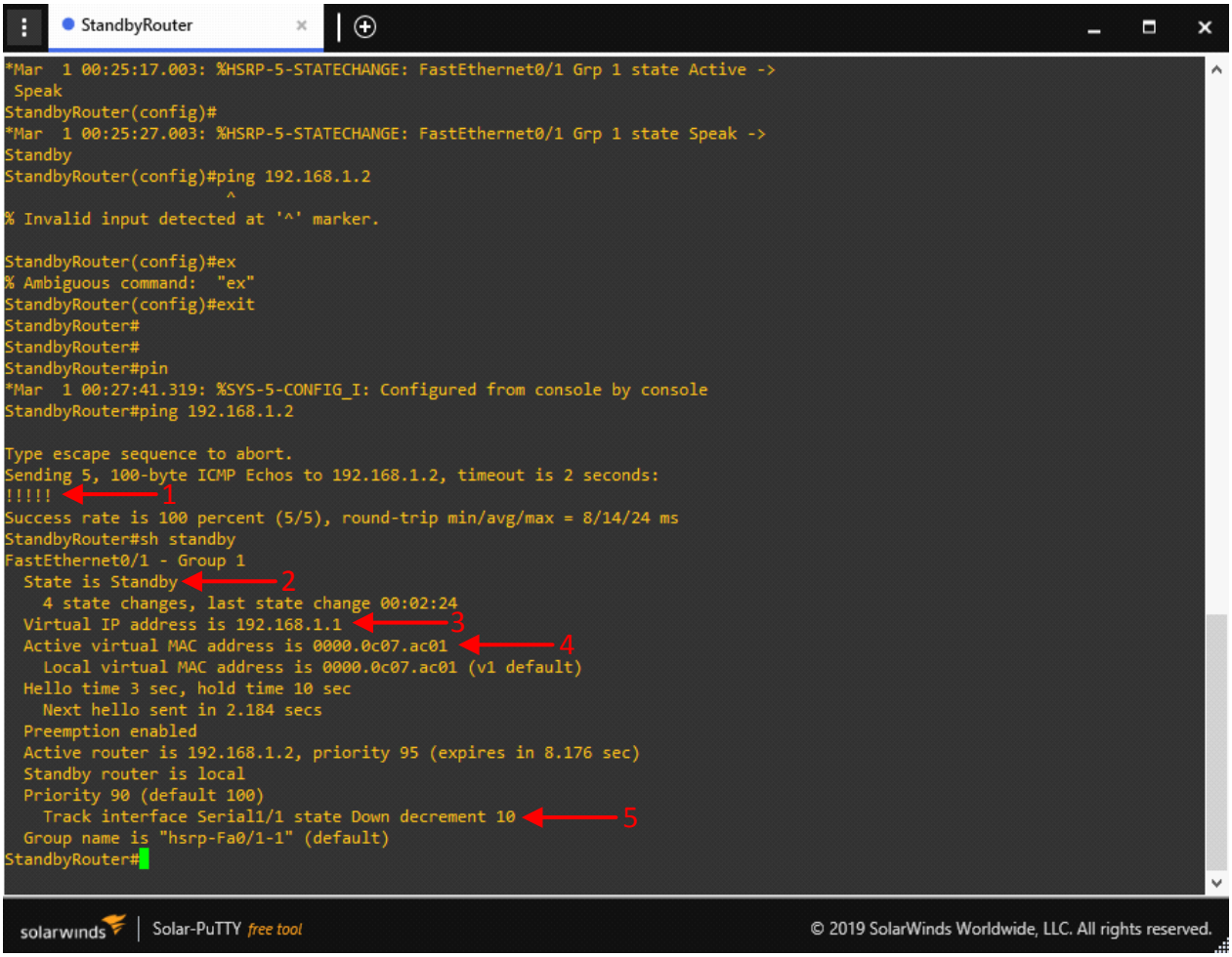


Рисунок 3.5 – Перевірка налаштування інтерфейсів та протоколу HSRP на маршрутизаторі StandbyRouter

На рис. 3.5 наведені такі позначення:

1 – мережева доступність з ActiveRouter присутня;

2 – наш роутер має статус Standby;

3 – налаштований віртуальний адрес;

4 – віртуальний MAC адрес за замовчуванням;

5 – контроль інтерфейса serial 1/1 увімкнений.

З рис.3.4-3.5 видно, що мережева доступність присутня та що конфігурація протоколу HSRP виконана успішно. Також можна помітити, що пріоритети на роутерах відрізняються від тих що за замовчуванням. Це пов'язано з тим, що інтерфейси serial у нас зараз не працюють і, так як у нас налаштований їх контроль (track), то автоматично знижується пріоритет у роутерів (на 10 за замовчуванням). На цьому заснований принцип відмовостійкості при відмові

зовнішніх інтерфейсів. Іншими словами, якщо у роутера в стані Active щось трапиться з інтерфейсом, який «знаходиться під наглядом», то HSRP знизить його пріоритет на задане число, і він стане Standby.

Взагалі, якщо налаштована динамічна маршрутизація, то команда «track» не потрібна, вона налаштовується при статичной маршрутизації для відслідковування стану інтерфейсів і вразі відмови одного з них вручну переключитися на інший маршрут, в даному випадка переключення на резервний маршрут відбувається автоматично.

Налаштування маршрутизатора R3 наведено на рис.3.6.

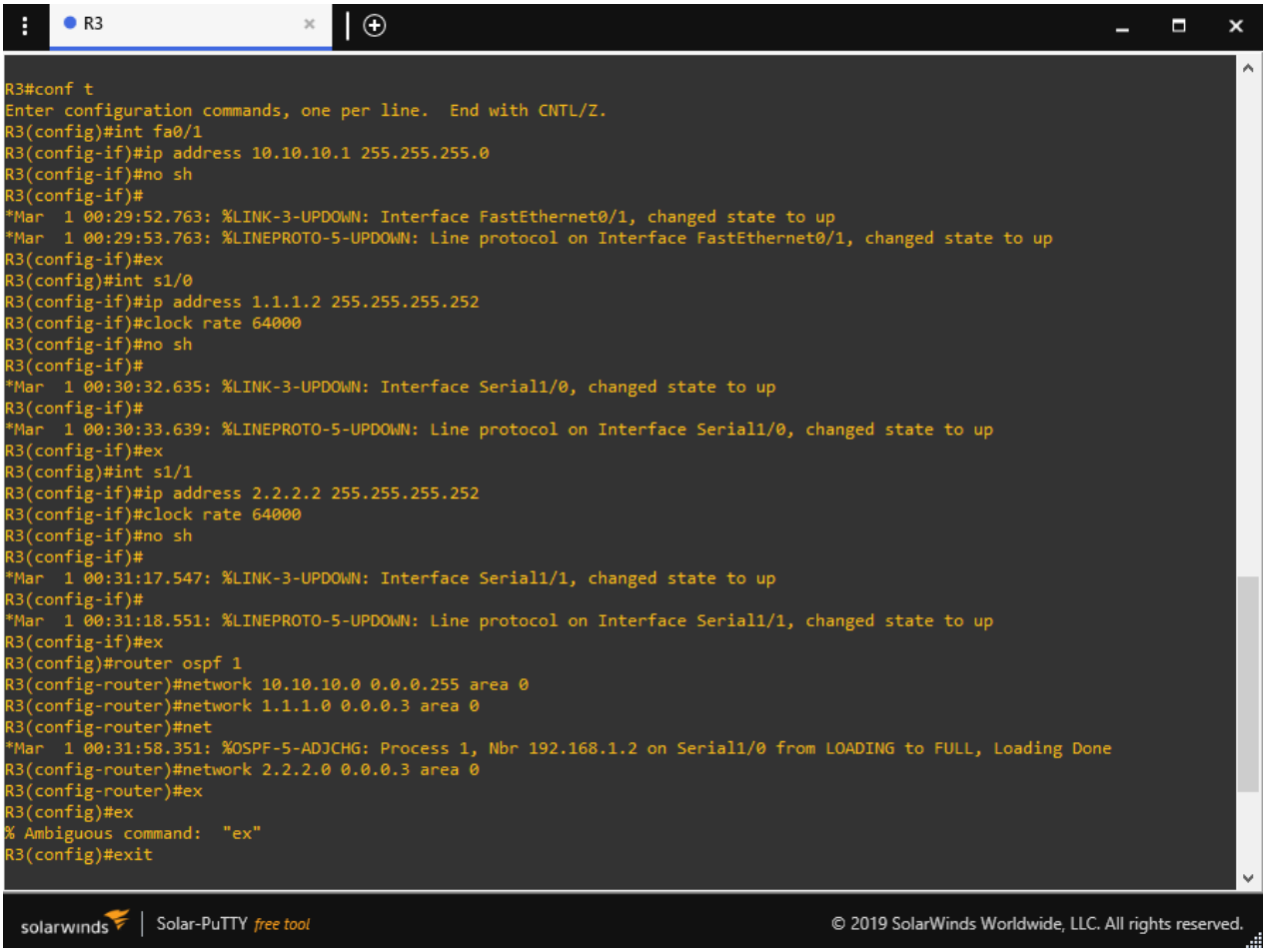


Рисунок 3.6 – Конфігурація інтерфейсів та динамічної маршрутизації OSPF на маршрутизаторі R3

Спочатку перед перевіркою працездатності мережі необхідно налаштувати так звану «вартість шляху», для того щоб в таблиці маршрутизації не було двох одинакових маршрутів.

Конфігурація вартості шляху наведено на рис.3.7.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int s1/1
R3(config-if)#ip ospf cost 120
R3(config-if)#exit
R3(config)#exit
R3#we
*Mar  1 00:38:23.855: %SYS-5-CONFIG_I: Configured from console by console
R3#wr
Building configuration...
[OK]
```

Рисунок 3.7 – Налаштування вартості шляху для інтерфейса s1/1 на маршрутизаторі R3

Перевірка таблиць маршрутизації та перевірка мережевої доступності на маршрутизаторі R3 наведено на рис.3.8.

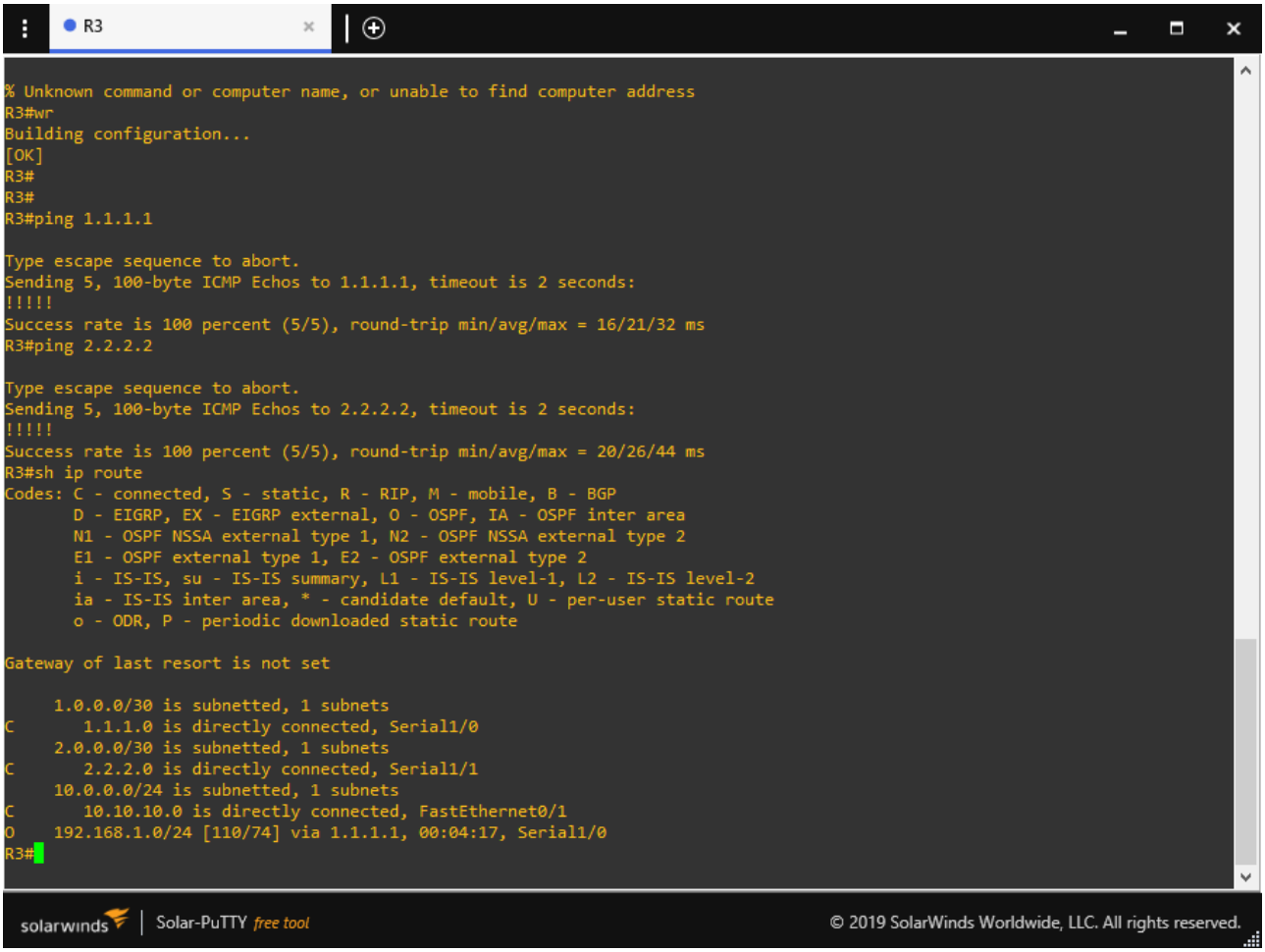


Рисунок 3.8 – Перевірка таблиць маршрутизації та перевірка мережевої доступності на маршрутизаторі R3

Як видно з рис 3.8 наданий момент є тільки один маршрут, причому основний маршрут, а не резервний бо проходить через інтерфейс активного роутера s1/0.

Перевірка проходження трафіку по основному маршруту наведено на рис. 3.9-3.10.

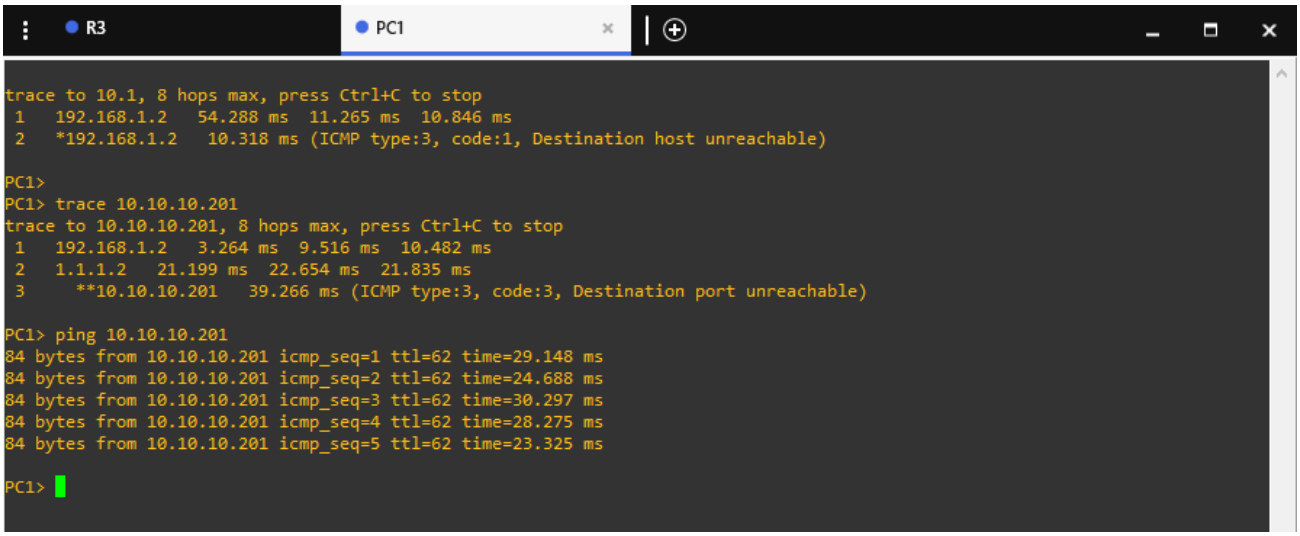


Рисунок 3.9 – Перевірка проходження трафіку по основному маршруту з PC1 до PC2 за допомогою команди «ping» і «traceroute»

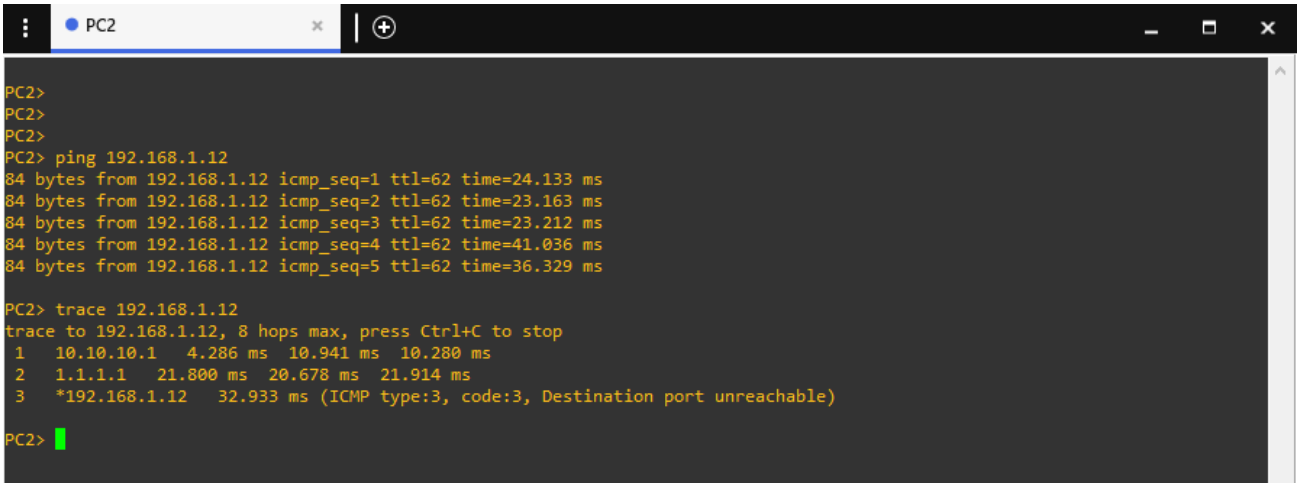


Рисунок 3.10 – Перевірка проходження трафіку по основному маршруту з PC2 до PC1 за допомогою команди «ping» і «traceroute»

Тепер коли всі умовності дотримані відключаємо інтерфейс s1/0 активного роутера для перевірки роботи відмовостійкої маршрутизації.

На рис.3.11-3.12 наведено перевірку стану Active та Standby роутера після відключення інтерфейсу s1/0.

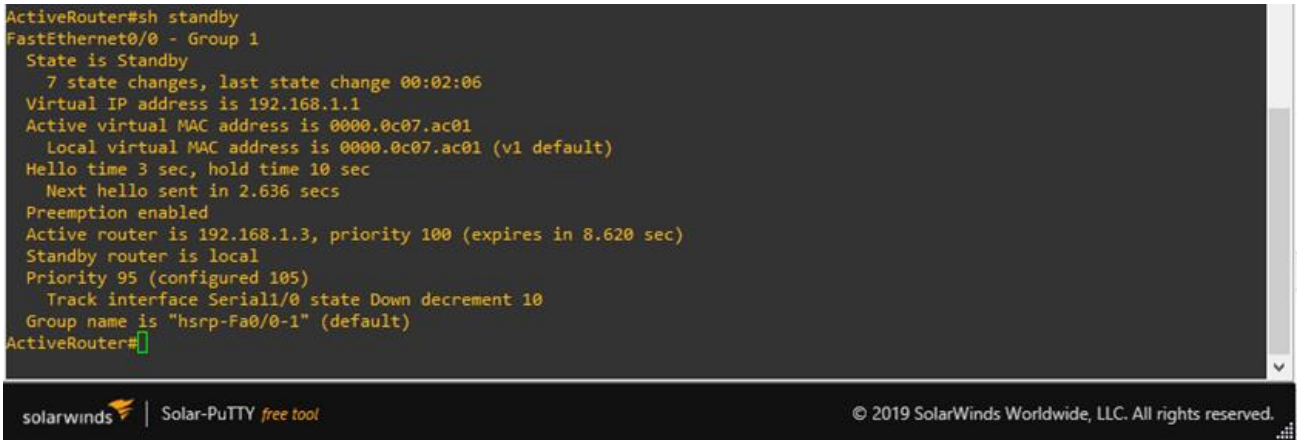


Рисунок 3.11 – Перевірка стану ActiveRouter за допомогою команди «show standby»

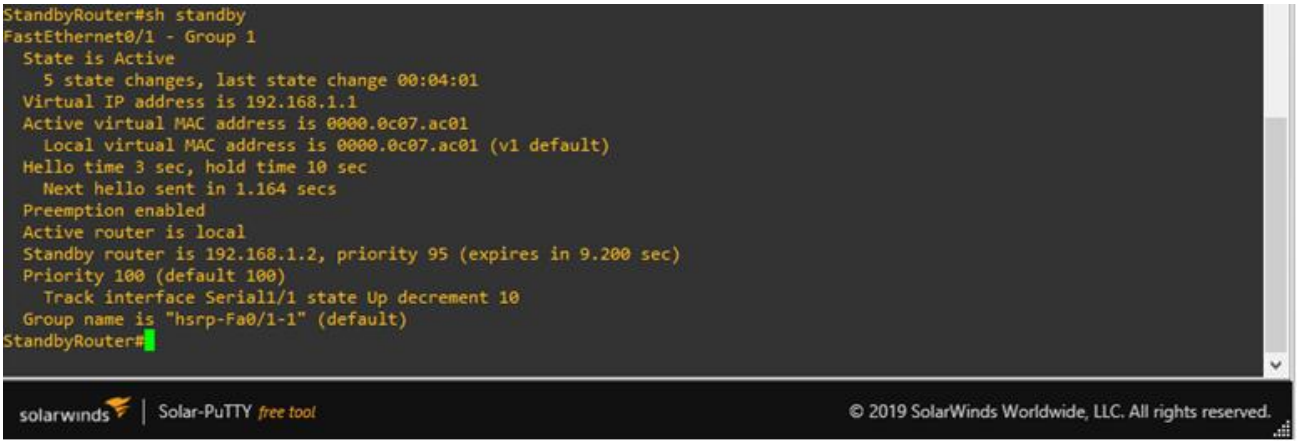


Рисунок 3.12 – Перевірка стану StandbyRouter за допомогою команди «show standby»

Як видно з рис. 3.11-3.12 стан роутерів змінився, а саме вони помінялись містами, тепер активний це Standby, а той що був в режимі очікування став Active.

Тепер необхідно здійснити перевірку проходження трафіку по мережі, для визначення наявності резервного маршруту.

Перевірку проходження трафіку по резервному маршруту наведено на рис. 3.13-3.14.

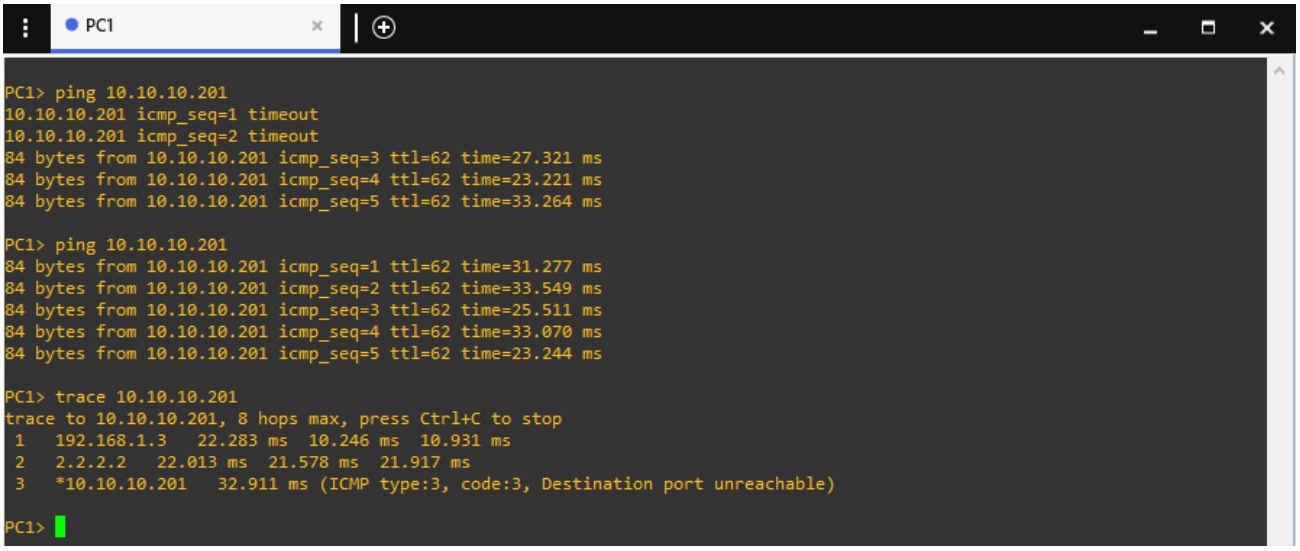


Рисунок 3.13 – Перевірка проходження трафіку по резервного маршруту з PC1 до PC2 за допомогою команди «ping» і «traceroute»

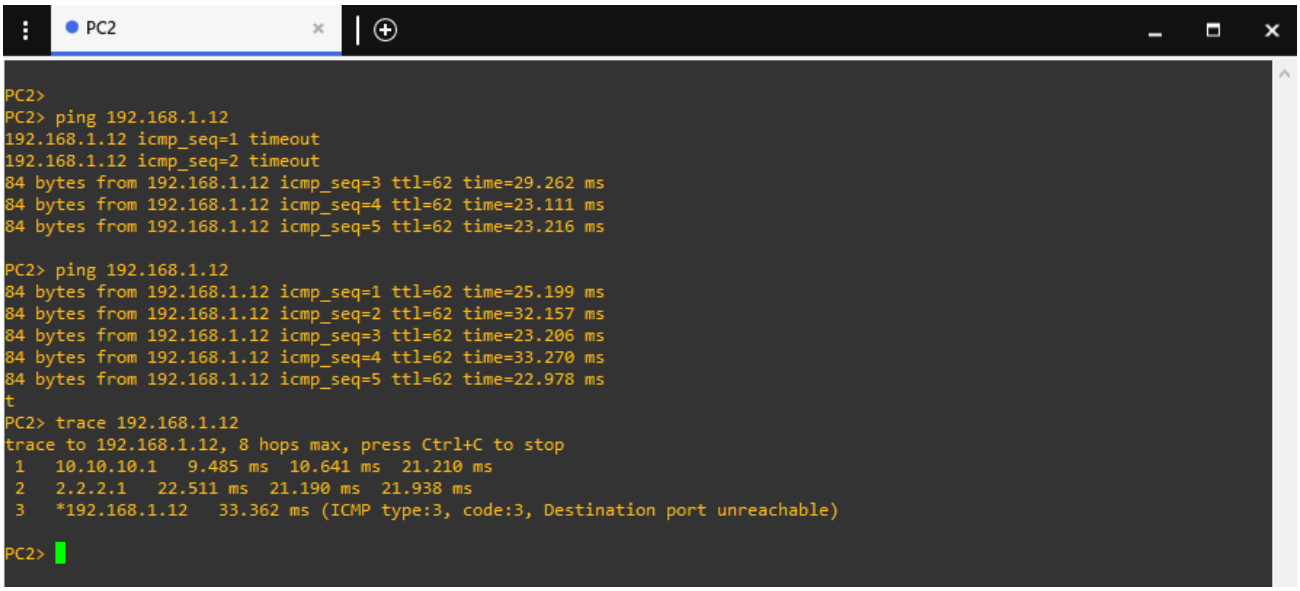


Рисунок 3.14 – Перевірка проходження трафіку по резервного маршруту з PC2 до PC1 за допомогою команди «ping» і «traceroute»

Як видно з рис.3.13-3.14 резевування маршрутів виконано успішно, також бачімо, що деякі «пінги» були втрачені, для того щоб зменшити кількість втрат треба змінувати таймери HSRP, які за замовчуванням встановлюються відповідно на 3 та 10 секунд, це означає, що пакет «Hello» надсилається між пристроями

групи очікування HSRP кожні 3 секунди, а пристрій очікування стає активним, коли Hello-пакет не отримано протягом 10 секунд.

Тепер перейдемо до аналізу трафіку, що проходив по досліджуваним маршрутам. Аналіз трафіку будемо здійснювати за допомогою программи Wireshark.

На рис. 3.15 наведено аналіз трафіку резервного маршруту на ділянці e0 – fa0/1, тобто на ділянці вихідний інтерфейс комутатора – вхідний інтерфейс маршрутизатора, що знаходиться в стані Active.

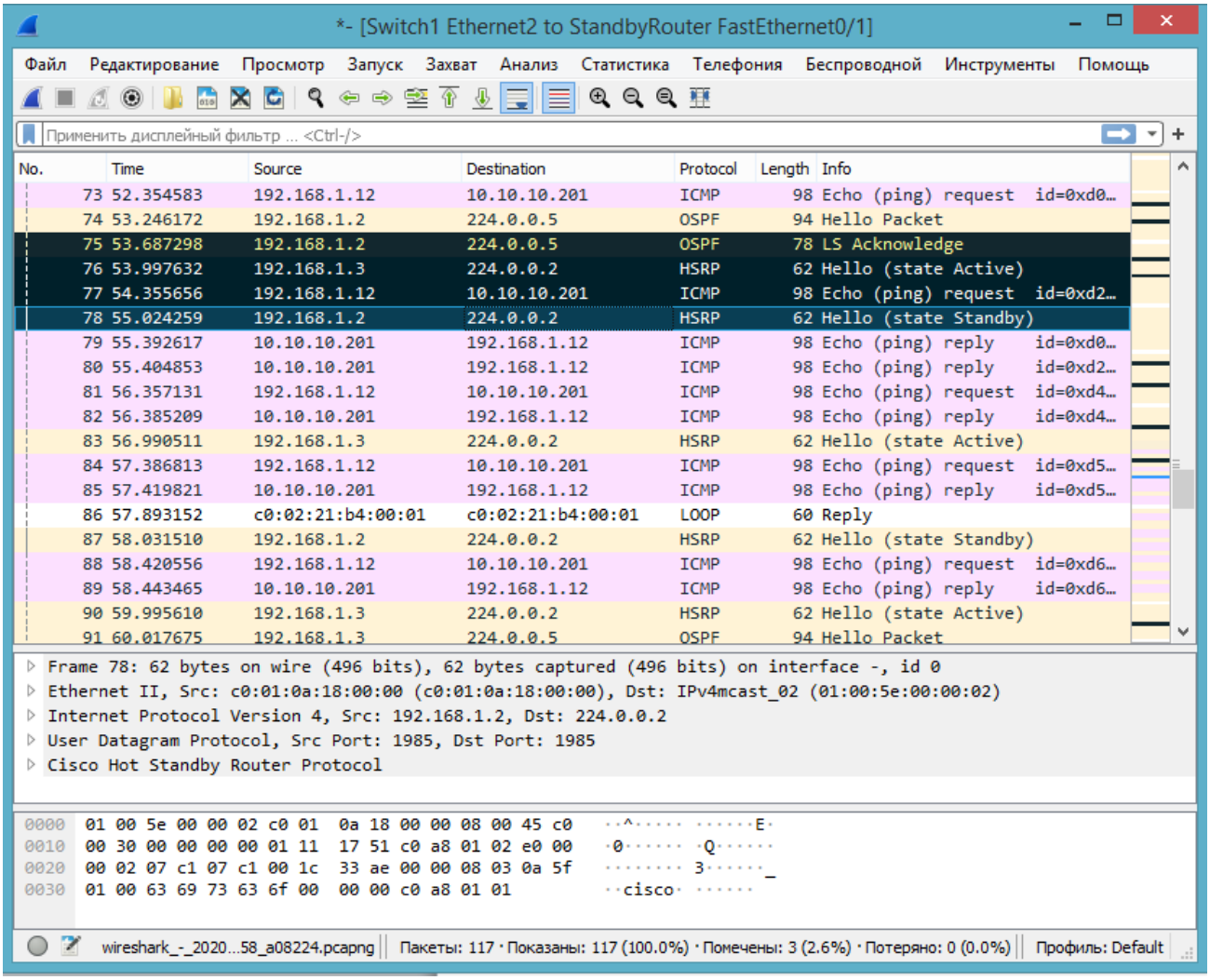


Рисунок 3.15 – Аналіз трафіку резервного маршруту на ділянці e0 – fa0/1

Виходячи з рис.3.15 можна побачати який трафік проходить, через резервний шлях. Напрклад, адреса призначення 224.0.0.2 – це адреса багатоадресної передачі, маршрутизатори HSRP з тієї ж групи надсилають

багатоадресні повідомлення привітання іншим шлюзам, щоб повідомляти членів групи про основний шлях та поточний стан кожного маршрутизатора (активного чи режиму очікування). Інтерфейс з активним станом використовується для переадресації трафіку.

Щоб спостерігати за поведінкою мережі та роботою HSRP, створюється навмисний збій, який вимикає активний маршрутизатор або його інтерфейс. HSRP проходить процес ініціалізації, щоб визначити, який маршрутизатор повинен взяти на себе роль Active, коли активний маршрутизатор R1 стане недоступним. Виділені потоки на рис.3.15 відображають зміну станів з активного на очікування, а також проходження ехо-запитів при використані команди «ping». Можна побачити, що в даний момент StandbyRouter з IP-адресою інтерфейсу 192.168.1.3 став Active, а ActiveRouter з IP-адресою інтерфейсу 192.168.1.2 в свою чергу тепер Standby. Таким чином видно, що відмовостійка машрутизація повноцінно працює на протоколі HSRP.

3.2 Дослідження та аналіз роботи протоколу GLBP на симуляційном обладнанні GNS3

Схема для дослідження протоколу HSRP наведена на рис.3.16.

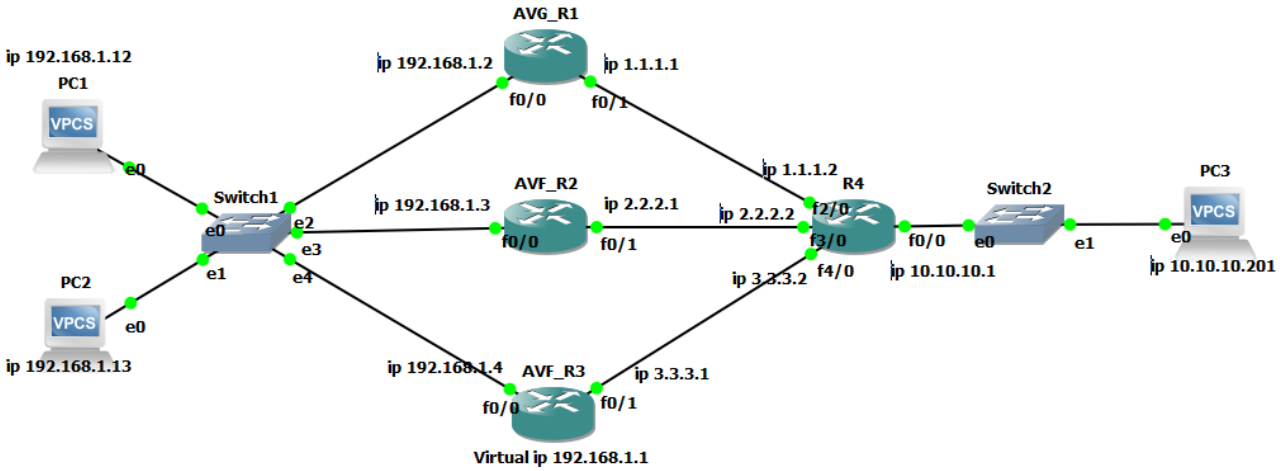


Рисунок 3.16 – Схема для дослідження протоколу GLBP

На рисунках 3.17-3.18 відображено проходження трафіка по маршрутам з балансуванням навантаження за допомогою команди «traceroute»(в gns3 – trace) та «ping».

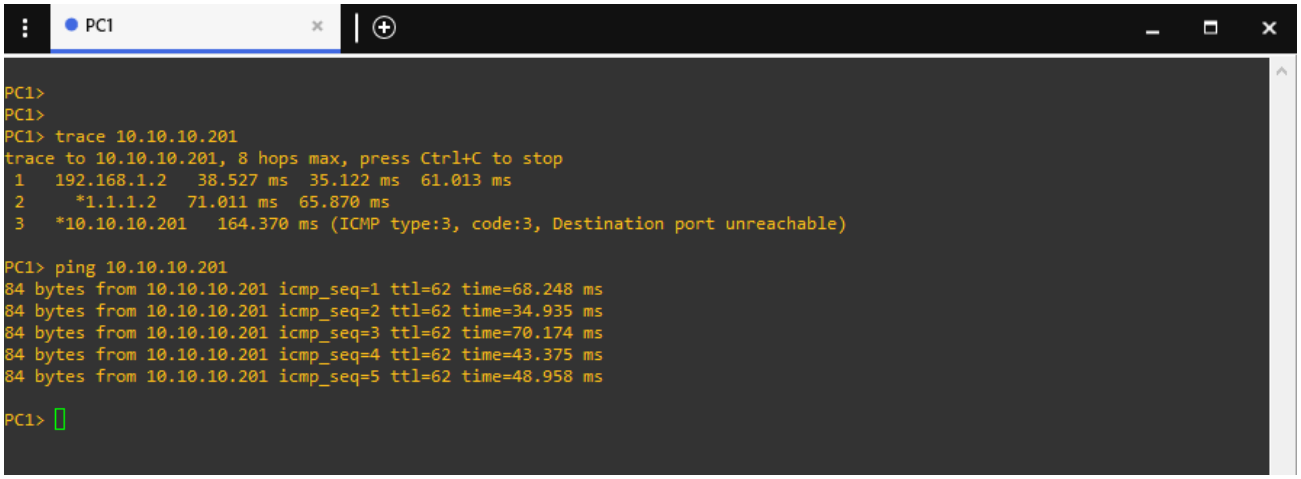


Рисунок 3.17 – Трасування маршруту та перевірка мережевої доступності за допомоги команд «trace» та «ping» з PC1 – PC3

Рисунок 3.18 – Трасування маршруту та перевірка мережевої доступності за допомоги команд «trace» та «ping» з PC2 – PC3

Як видно з рис.3.17-3.18 трафік з різних терміналів проходить через декілька маршрутів, саме так реалізовується балансування навантаження при використанні режиму «Round-Robin» на протоколі GLBP. Сенс його заключається в тому, що трафік рівномірно проходить через мережу по різним маршрутам.

На рис.3.19 наведено стан протоколу GLBP на маршрутизаторі AVG_R1.

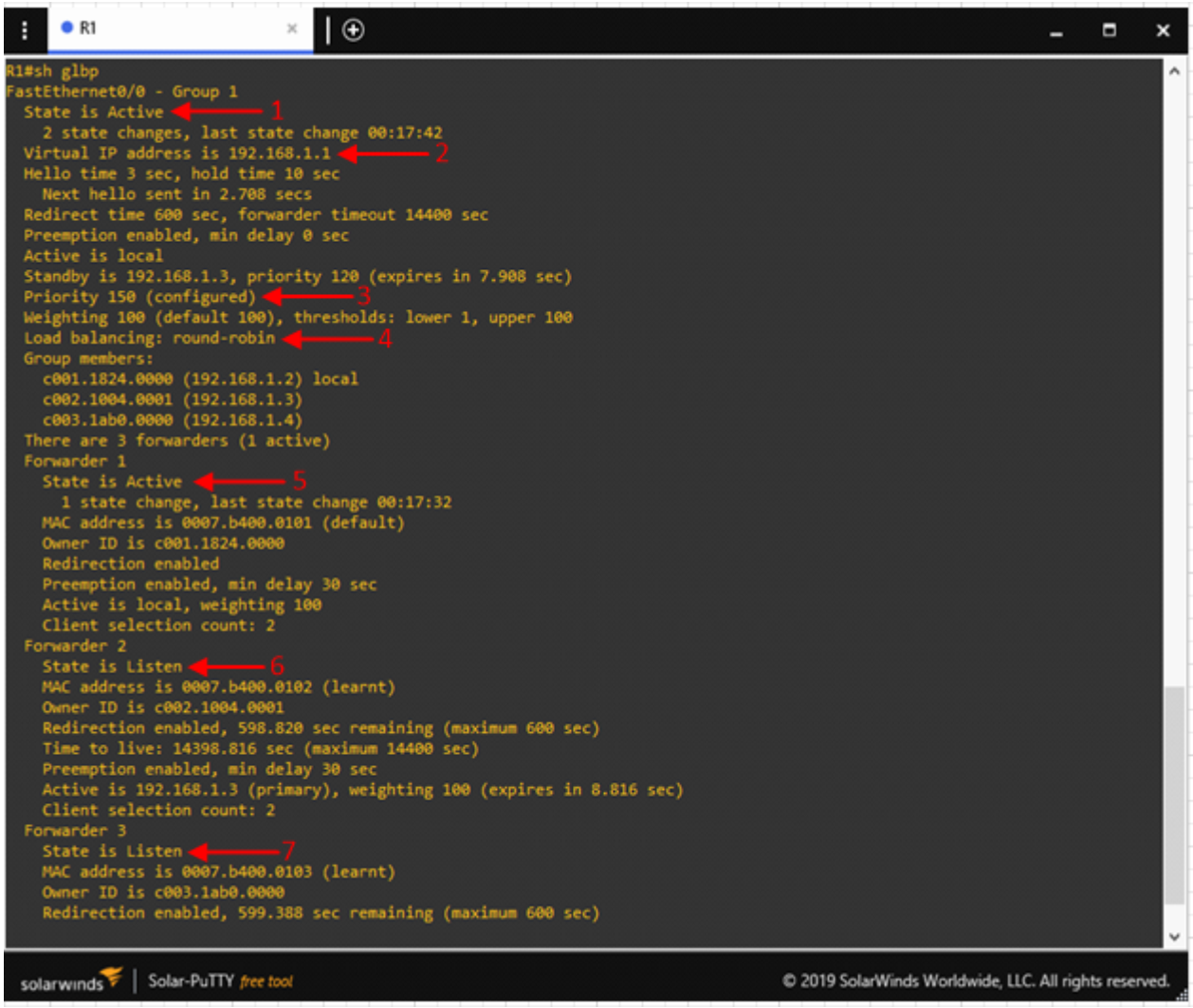


Рисунок 3.19 – Перевірка стану протокола GLBP за допомогою команди «Show GLBP»

На рис. 3.19 наведені такі позначення:

1 – Роутер AVG_R1 має статус «Active»;

2 – налаштований віртуальний адрес;

3 – налаштований пріорітет для виборів AVG;

4 – режим балансування навантаження;

5 – Forwarder AVG_R1 має налаштований статус «Active», як для AVG та і AVF;

6 – AVF_R2 має статус «Listen»;

7 – AVF_R3 має статус «Listen»;

GLBP налаштований таким чином, що трафік який виходить з терміналів-клієнтів через мережу може бути спільним для кількох маршрутизаторів, тим самим справедливо розподіляючи навантаження трафіку між доступними маршрутизаторами. Це було виявлено та доведено за допомогою наведених вище рисунків, які показують шлях різних перевірених трафіків ICMP.

Якщо пріоритети не вказані за замовчуванням для певних маршрутизаторів, ці маршрутизатори стають активними. База даних GLBP ідентифікує два маршрутизатори, які активно маршрутизують пакети, в той час як резервний маршрутизатор прослуховує будь-які вимоги або вимоги щодо надсилання пакетів.

AVG (Active Virtual Gateway) – активний маршрутизатор, який займається роздачею MAC-адрес пристроїв. Керівник над маршрутизаторами в мережі GLBP. Це роль диспетчера, який вказує пристрої, що будуть розподіляти трафік по засобу роздачі їм MAC-адрес, коли приходить ARP-запит. Тобто IP адреса у всіх буде єдина, а ось MAC-адреси будуть різні [19].

AVF (Active Virtual Forwarder) – активний маршрутизатор, який пропускає через себе трафік. Маршрутизатор AVG може бути тільки один, а от маршутизаторів AVF можеть бути всі інші, при цьому AVG може бути і AVF одночасно.

Рис.3.20 показує, що всі маршрутизатори активні та беруть участь у маршрутизації трафіку.

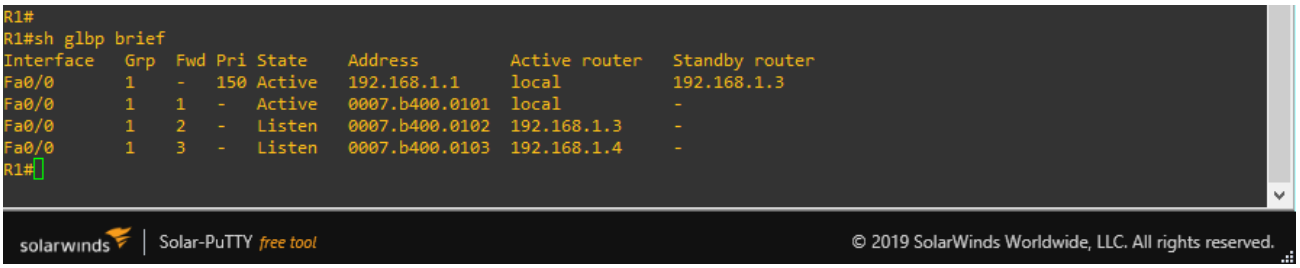


Рисунок 3.20 – Перевірка стану маршрутизаторів за допомогою команди «Show glbp brief»

На маршрутизаторі AVG_R1, який є активним маршрутизатором, видно, що інші маршрутизатори перебувають у режимі прослуховування та очікування. GLBP управляє надмірністю віртуального шлюзу так само, як і HSRP.

Перед відключеням одного з маршрутів для перевірки працездатності протоколу GLBP на можливість реалізації відмовостійкої маршрутизації необхідно перевірити наявність та кількість маршрутів. На рис.3.21 – Наведено перевірку активних маршрутів на маршрутизаторі R4.

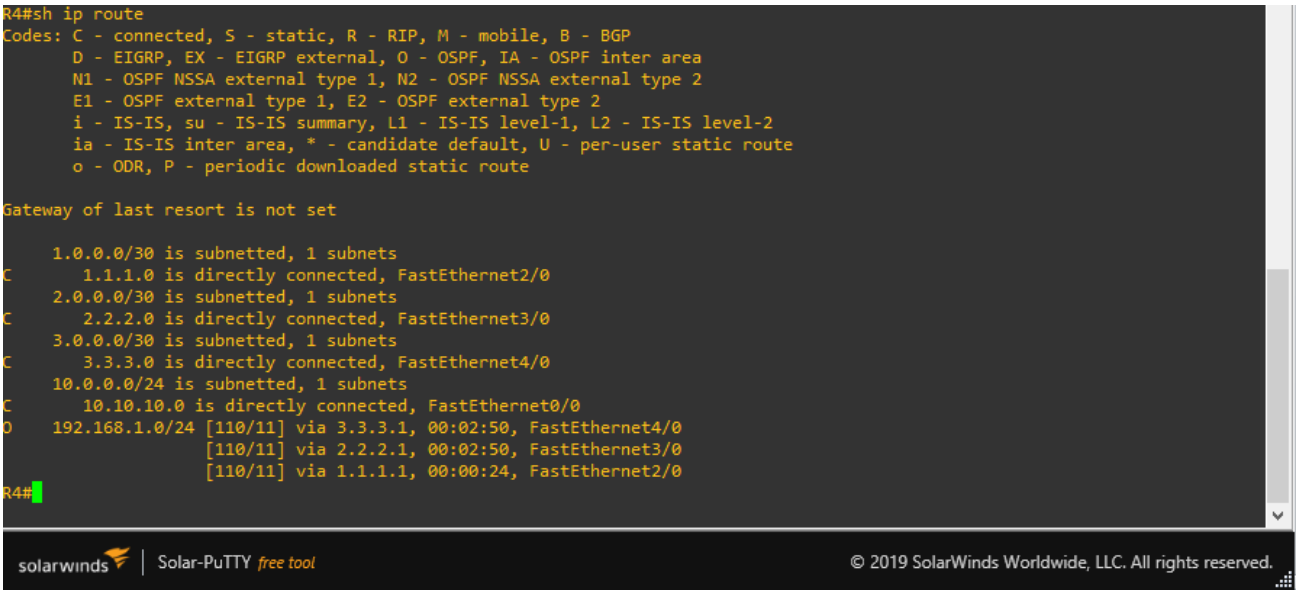


Рисунок 3.21 – Перевірка маршрутної таблиці на маршрутизаторі R4 за допомогою команди «Show ip route»

Тепер перевіримо реакцію мережі на винекнення відмови. В даному випадку вимкнемо інтерфейс f0/1, який в свою чергу є шлюзом від AVG_R1.

На рис.3.22 – Наведено імітацію винекнення відмови на основі виходу з ладу інтерфейсу f0/1 маршрутизатора AVG_R1.

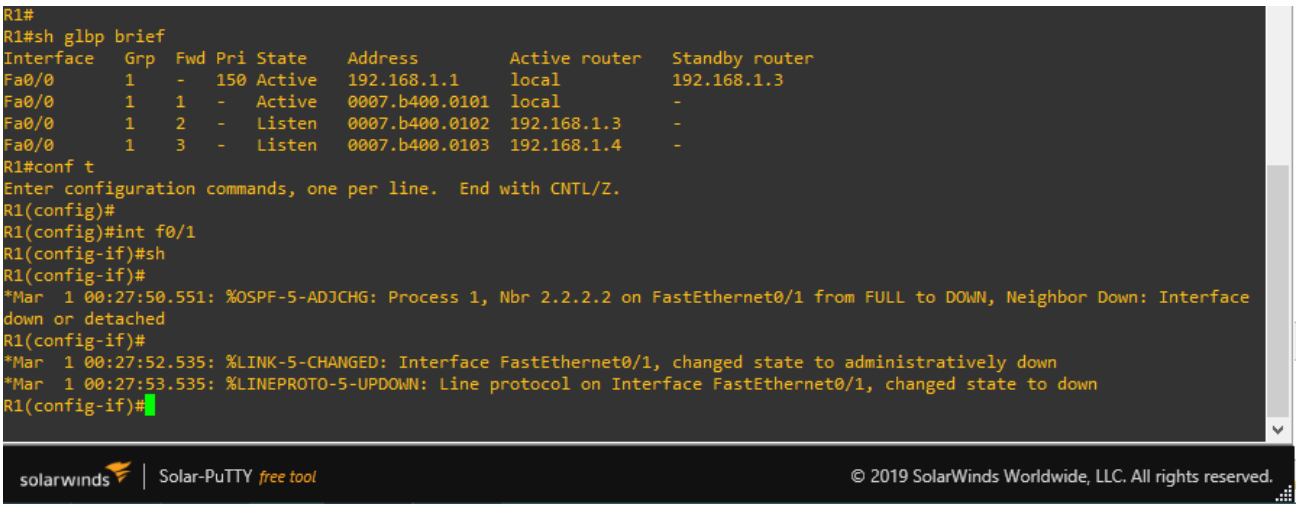


Рисунок 3.22 – Вимкнення інтерфейсу f0/1 за допомогою команди «shutdown»

На рис.3.23-3.24 – наведено перевірку проходження трафіку через мережу після відключення інтерфейсу f0/1 маршрутизатора AVG_R1 з терміналів PC1 та PC2.

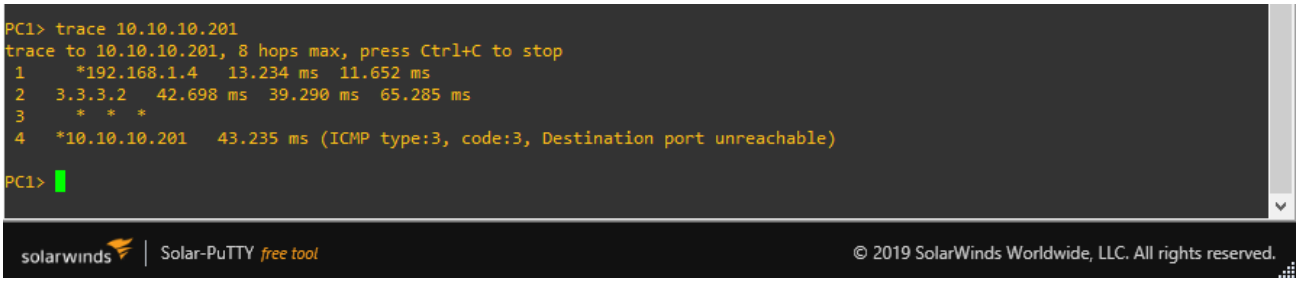


Рисунок 3.23 – Перевіркв проходження трафіку через мережу після відключення інтерфейсу f0/1 маршрутизатора AVG_R1 з PC2 – PC3

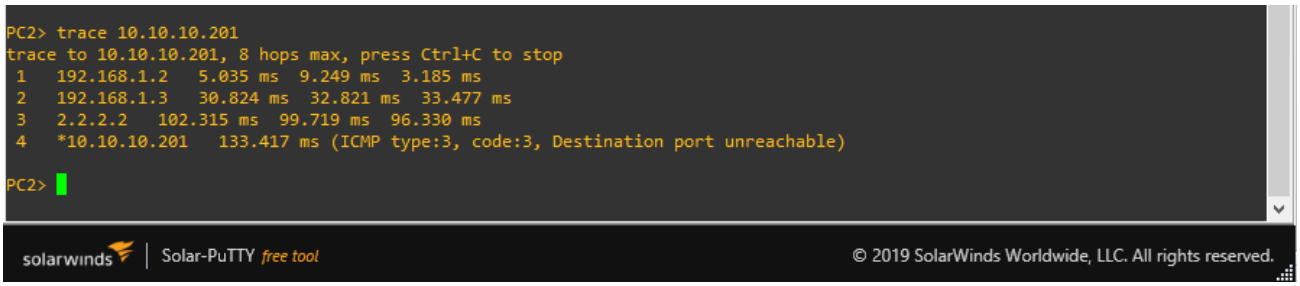


Рисунок 3.24 – Перевіркв проходження трафіку через мережу після відключення інтерфейсу f0/1 маршрутизатора AVG_R1 з PC1 – PC3

Як видно з рис.3.23-3.24 маршрутизація трафіку в мережі змінилась, балансування при цьому залишилося.

Перевіримо активні, діючі маршрути. Перевірка маршрутної таблиці наведено на рис.3.25.

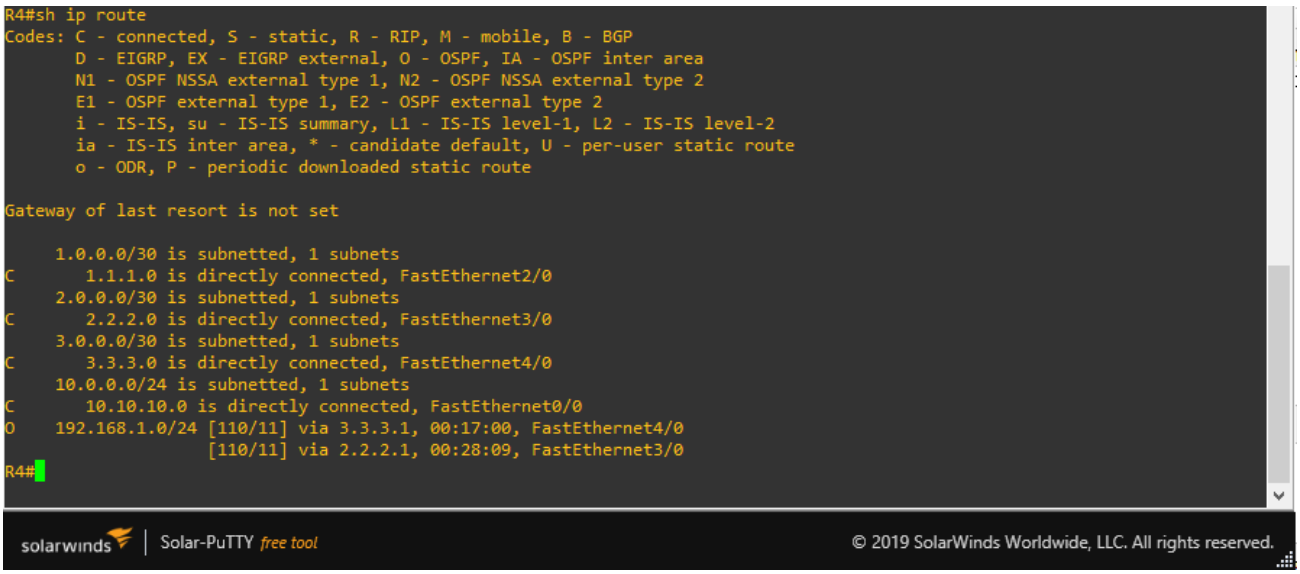


Рисунок 3.25 – Перевірка маршрутної таблиці на маршрутизаторі R4

Як видно з рис.3.25 замість 3-х активних маршрутів, залишилось 2 активних маршрутів. Навіть в такому випадку зберігається балансування, а через деякий час, а саме Hold time – 10 секунд, роль AVG буде присвоїна іншому маршрутизатор, а якщо, точніше то всі активні пристрої обмінюються кожні 3 секунди Hello-пакетами. Резервні роутери теж приймають пакети і чекають свого часу. Якщо через 3 секунди пакет-Hello не буде отриманий, то запуститься Dead таймер, який дорівнює 10 с. В якості резервного (Standby) маршрутизатора вибирається один з AVF. Коли Standby шлюз стає Active, то знову вибирається Standby.. Саме цей час, є часом простою мережі, за цей період трафік навіть при балансуванні буде втрачатися, щоб зменшити цей час необхідно конфігурувати таймер протоколу під кожну ситуацію окремо, так як в такому випадку відбувається перевантаження мережі службовим трафіком.

3.3 Результати дослідження та порівняння працездатності роботи протоколів HSRP та GLBP

Протоколи сімейства FHRP та механізми на основі, яких вони працюють, різняться за складністю та виконують різні завдання на основі сценарію, який необхідний для забезпечення оптимальної роботи. Порівняння між запропонованими протоколами відмовостійкої маршрутизації проводиться для таких параметрів продуктивності, як падіння пакетів та частково часу конвергенції. Оцінки виконуються теоретично і демонструються за допомогою реальних моделювань.

HSRP дозволяює багатьом пристроям брати участь у віртуальній групі пристроїв, налаштованій на віртуальну IP-адресу. Один з учасників обраний активним пристроєм для переадресації пакетів, відправлених на віртуальну IP-адресу групи. Інші пристрої в групі не беруть участі в процесі переадресації пакетів, якщо активний пристрій не виходить з ладу. Таким чином, пропускна здатність не використовується. GLBP виконує для користувача ту саму функцію надмірності, що і HSRP. Протокол GLBP залежить від того, скільки маршрутизаторів налаштовано на одну групу. Налаштовані маршрутизатори GLBP постійно перенаправляють трафік, створюючи ідеальний сценарій для мережевого середовища.

В результаті проведення моделювання цих протоколів можна зробити висновок, що протокол HSRP не може виконати балансування навантаження, оскільки він передає обов'язки активного резервного маршрутизатора лише у випадку відмови, а трафік балансування навантаження через два канали з використанням двох HSRP-маршрутизаторів, як топологія, з якою ми працювали з однією групою HSRP, неможливі. Однак є можливість збалансувати навантаження за допомогою HSRP, якщо виконати балансування навантаження, налаштувавши кілька груп HSRP, щоб мати кілька адрес віртуального маршрутизатора, для цього необхідні додаткові конфігурації. В результаті отримуємо балансування навантаження, але через додаткові конфігурації робить його дещо трудомістким, більш-менш фіксованим або статичним.

Тому був розроблений протокол GLBP, який долає ряд обмежень існуючих протоколів маршрутизації.

GLBP забезпечує відмовостійку маршрутизацію з балансуванням навантаження для багатьох пристроїв (шлюзів) з використанням однієї віртуальної IP-адреси та декількох віртуальних MAC-адрес. Трафік розподіляється порівну в групі GLBP, а не контролюється одним пристроєм, поки

інші пристрої залишаються в режимі простою (не працюють на даний момент чи не працюють, але мають можливість).

Кожен термінал сконфігурований на одну і ту ж віртуальну IP-адресу, і всі пристрої в групі віртуальних пристроїв беруть участь у переадресації пакетів. Учасники GLBP спілкуються між собою за допомогою Hello-пакетів, тобто спеціальних привітних повідомлень, що надсилаються кожні 3 секунди на адресу багатоадресної передачі (джерело-адресат).

Аналіз результатів пінгу під час навмисного збою, виконаного за сценаріями HSRP та GLBP. Приклад та оцінка параметру зниження продуктивності, зокрема втрати пакетів зображена на рис.3.26-3.28.

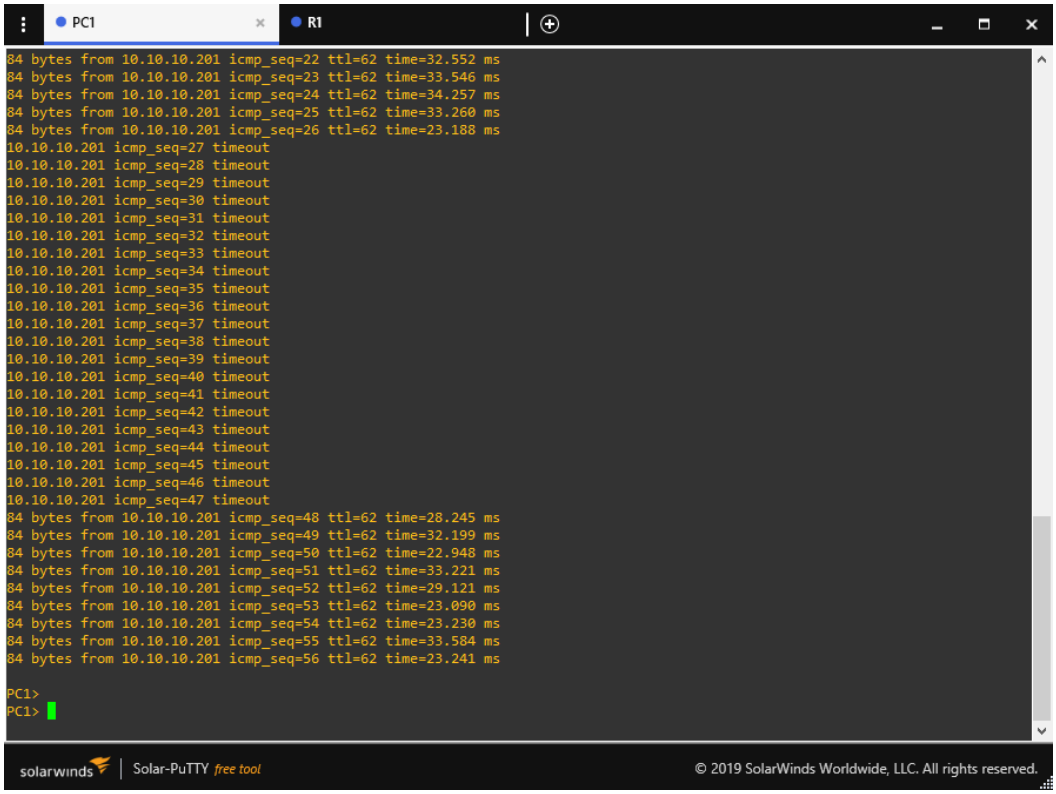


Рисунок 3.26 – Перевірка проходження пакетів з PC1 – PC2 для протоколу HSRP в момент відключення основного маршруту

В процесі проходження пакетів по основному маршруту було проведено імітацію збою на основі відключення інтерфейсу(шлюзу) на основному маршруті, внаслідок цього відбулась втрата пакетів, яка не припиниться до того моменту,

коли несправність даного елементу мережі буде усунена, або ж раніше відбудеться перенаправлення трафіку через резервний маршрут.

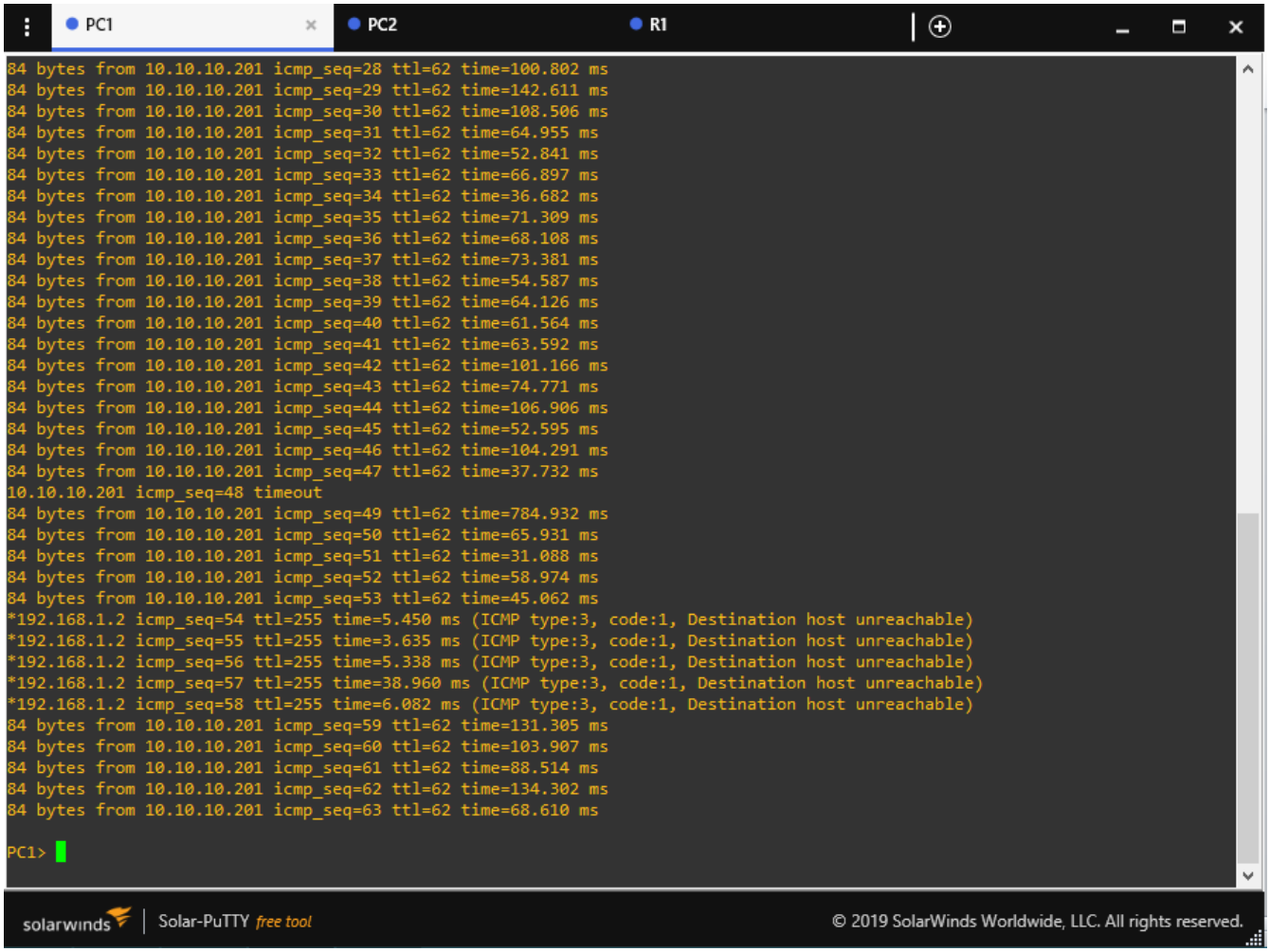


Рисунок 3.27 – Перевірка проходження пакетів з PC1 – PC3 для протоколу GLBP в момент відключення основного маршруту

Рисунок 3.28 – Перевірка проходження пакетів з PC2 – PC3 для протоколу GLBP в момент відключення основного маршруту

Як видно з рис.3.27-3.28 кількість втрачених пакетів при використані протоколу GLBP значно менше в порівні з протоколом HSRP. Такий результат спостерігається за рахунок рівномірного балансування навантаження GLBP. В разі використання протоколу HSRP внаслідок відмови, необхідно усунути відмову та переключити трафік на резервний шлях, на все це витрачається певний час, а отже і втрачаються пакети, одночасно при використанні протоколу GLBP, у випадку відмови основного маршруту, маршрутизатори все ще активні та зберігають переадресацію пакетів. В ідеальних умовах пакети за рахунок балансування трафіку по альтернативним маршрутам не втрачаються зовсім, але втрата 3-х пакетів при використанні GLBP в порівні з втратою 20 пакетів при використанні HSRP, це суттєва різниця, яка й відображає головну перевагу

протоколу GLBP – оптимальне розподілення мережевих ресурсів, на основі чого можна майже повністю нівелювати втрату пакетів при маршрутизації.

Стостовно протокольной збіжності, то фактичний час конвергенції залежить від таймерів, налаштованих для групи, і, можливо, від конвергенції протоколу маршрутизації. Наприклад час привітання HSRP встановлено за замовчуванням на 3 секунди, а таймер часу утримання – 10 секунд. Дані таймери відповідають за конвергенцію. На основі теоретичних та практичних досліджень можна зробити висновок, що взалежності від сценарію таймери потрібно змінювати, наприклад час привітання потрібно змінити на 1 секунду, для того щоб збіжність займала менше 3 секунд. В свою чергу, це призводить до зменшення втрати пакетів, але до збільшення навантаження службовим трафіком.

В результаті проведення теоретичного аналізу та практичних досліджень можна зробити висновок, що найкращим та самим ефективним на даний момент протоколом відмовостійкої маршрутизації, є протокол GLBP. Звичайно, що є і інші засоби та методи, за допомогою яких можна досягти подібних результатів, але практика показує, що вони мають принципово більше недоліків чим GLBP, основним недоліком якого, висока складність управління мережею.

ВИСНОВКИ

Оскільки вимоги щодо якості обслуговування дедалі зростають, пропорційно цьому зростають і вимоги до маршрутизації. Протоколи маршрутизації повинні окрім проведення розрахунків оптимальних маршрутів передачі пакетів та визначитя порядку розподілу трафіку по ним, ще й забезпечувати швидку конфігурацію мережі, відмовостійкість з резервуванням канального та буферного ресурсу та можливість масштабованості мережі. У зв'язку з цим, в роботі був проведений аналіз таких рішень відмовостійкої маршрутизації, як:

– швидка протокольна збіжність (Fast IGP/BGP Convergence);

– відмовостійка маршрутизація (Fault-tolerant routing);

– швидка перемаршрутизація (Fast ReRoute, FRR).

Детально було досліджено рішення відмовостійкої маршрутизації і розглянуто схеми захисту каналу, вузла та шляху/мультишляху, шлюзу мережі. Також було досліджено та порівняно роботу протоколів збільшення доступності шлюзу за замовчуванням, зокрема протоколів HSRP та GLBP на симуляційному обладнанні.

В результаті проведення дослідження протоколів сімейства FHRP, які направлені на реалізацію відмовостійкості, було виявлено, що протокол HSRP не задовольняє всіх вимог, що висуваються до рішень відмовостійкої маршрутизації, тому що забезпечує лише резервування основного шляху і не вирішує проблеми пов'язані з перевантаженням мережі, що є одной з основних причин винекнення відмов в сучасних ТКМ, знову ж за рахунок зростаючих вимог до якості обслуговування.

Більш повніше ці вимоги врахувалися при розробці протоколу GLBP, який окрім можливості рівномірного балансування навантаження, що в свою чергу дозволяє більш оптимально розподіляти мережеві ресурси та недопускає перевантажень, а отже і значних втрат пакетів, також має можливість ще й інші режими роботи, такі як «зважений», при якому можна вручну розподіляти потік не 50/50, як при рівномірному розподілені, а й використовувати інші співвідношення і все це на фоні лише одного суттєвого недоліка, як висока складність керування мережею.

Взагалі сучасні протоколи маршрутизації, які основані на відносно застарілих моделях та механізмах в умовах швидко зростаючого трафіку, а отже і зростаючих вимог якості обслуговування не можуть забезпечити повністю всіх рішень, щодо відмовостійкої маршрутизації. На даний момент можна ще знайти компроміс на основі комбінування тих чи інших рішень, а ще є проблеми з безпекою, тому потрібно використовувати принципово нові концепції, якою є використання потокової моделі, можливість враховувати більше вихідних параметрів, зокрема наприклад пропускні здатності мережі, дає в перспективі більш гнучкі варіанти для розвитку рішень для реалізації відмовостійкої маршрутизації.

Ріст ефективності технологічних рішень відмовостійкої маршрутизації, направлених на покращення відмовостійкості в ТКМ, багато в чому залежить від достовірності та адекватності математичних моделей і методів, котрі закладаються в основу відповідного протоколу маршрутизації. Описана та досліджена математична модель дійсно забезпечує адекватне рішення задачі відмовостійкої маршрутизації, але також є й недоліки, які можуть негативно сказатися на продуктивності мережі. В першу чергу, це стосується погіршення загальної продуктивності ТКМ, оскільки використання резервних шляхів так чи інакше пов'язане з залученням додаткового мережевого ресурсу (канального і буферного), який з цієї причини не може бути використаний іншими потоками.

З іншого боку, необхідність розрахунку на ряду з основними маршрутами ще і множини резервних шляхів пов'язане з підвищенням обчислювального навантаження на маршрутизатори ТКМ, а також необхідністю підтримки маршрутних таблиць підвищеної розмірності.

При цьому основні і резервні шляхи необхідно не тільки розрахувати, але ще і підтримувати в активному стані. В цілому перераховані фактори негативно позначаються і на масштабованості рішень, пов'язаних з відмовостійкої маршрутизацією. Особливо це критично для ТКМ великої розмірності і з розгалуженою мережевою структурою, що призводить в результаті до розрахунку шляхів з великим числом каналів зв'язку і маршрутизаторів.

Перераховані недоліки є загальними практично для всіх технологій, пов'язаних з підвищенням надійності мережі в цілому, і є своєрідною «платою» за забезпечення заданого рівня відмовостійкості кінцевих рішень. Для мінімізації даних недоліків бажано, щоб в результаті проведених розрахунків резервний шлях якомога менше відрізнявся за складом каналів і вузлів від основного – в

ідеалі лише на проблемний елемент мережі, що підлягає подальшого захисту. Це має сприяти тому, що резервування підлягатимуть мінімальні обсяги пропускної здатності каналів мережі. Крім того, тоді в вузлах мережі для кожного потоку можуть зберігатися вже не дві маршрутних таблиці (для основного та резервного шляху), а одна, але з мінімально необхідними коригуваннями, що стосуються відмінностей основного і резервного шляхів. Це позитивно позначиться на продуктивності мережі та показниках якості обслуговування в цілому.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Вегешна Ш. Качество обслуживания в сетях IP / Ш. Вегешна. – Москва: Издательский дом “Вильямс”, 2003. – 368 с.

2. Лемешко А.В. Модель отказоустойчивой маршрутизации многоадресных и широковещательных потоков в MPLS-сети / А.В. Лемешко, К.М. Арус // Системи обробки інформації. – 2013. – Вип. 9. – С. 160-163. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2013_9_34

3. Лемешко А. В. Повышение масштабируемости и производительности решений по отказоустойчивой маршрутизации в телекоммуникационных сетях / А. В. Лемешко, А. С. Еременко, Н. Тарики, К. М. Арус // Системи обробки інформації. - 2016. - Вип. 1. - С. 152-156. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2016_1_34

4. Mauthe A., Hutchison D., Cetinkaya E.K., Ganchev I., Rak J., Sterbenz J.P., Gunkelk M., Smith P., Gomes T. Disaster-resilient communication networks: Principles and best practices. Resilient Networks Design and Modeling (RNDM) 2016: Proceedings of the 8th International Workshop. Halmstad, Sweden, 13-15 September, 2016. IEEE, 2016. P. 1-10. DOI: 10.1109/RNDM.2016.7608262.

5. White R., Tantsura J. E. Navigating Network Complexity: Next-generation routing with SDN, service virtualization, and service chaining. AddisonWesley Professional, 2015. 320 p.

6. Beshley M., Klymash M., Strykhalyuk B., Shpur O., Bugil B., Kagalo I. SOA quality management subsystem on the basis of load balancing method using fuzzy sets. International Journal of Computer Science and Software Engineering (IJCSSE). 2015. January 15. Vol. 44, No. 1. P. 10-21.

7. Модель маршрутизації у телекомунікаційній мережі з використанням шляхів, що перетинаються за вузлами / О. С. Єременко, Д. В. Андрушко // Вісник Національного університету "Львівська політехніка". Радіоелектроніка та телекомунікації. - 2015. - № 818. - С. 181-188. - Режим доступу: http://nbuv.gov.ua/UJRN/VNULPPT_2015_818_27

8. Janevski T. NGN Architectures, Protocols and Services. 1st Edition. Wiley, 2014. 366 p.

9. Choras M., Kozik R., Bruna M.P.T., Yautsiukhin A., Churchill A., Maciejewska I., Eguinoa I., Jomni A. Comprehensive approach to increase cyber security and resilience. Availability, Reliability and Security (ARES) 2015: Proceedings

of the 10th International Conference. Toulouse, France, 24-27 August, 2015. IEEE, 2015. P. 686-692. DOI: 10.1109/ARES.2015.30

10. Misra S., Goswami S. Network Routing: Fundamentals, Applications, and Emerging Technologies 1st Edition. Wiley, 2017. 536 p.

11. Таненбаум Е. Компьютерные сети / Е. Таненбаум. – Санкт-Петербург, 2012. – 960 с.

12. Гольдштейн А. Б. Технология и протоколы MPLS / А. Б. Гольдштейн, Б. С. Гольдштейн. – Санкт Петербург: БХВ, 2005. – 304 с.

13. Остерлох Х. Маршрутизация в IP-сетях. Принципы, протоколы, настройка. / Х. Остерлох. – Санкт-Петербург: BHV, 2002. – 512 с.

14. Rak J. Resilient Routing in Communication Networks (Computer Communications and Networks), 1st edition. Springer, 2015. 181 p.

15. Лемешко О. В., Євсєєва О. Ю. Конспект лекцій з дисципліни «Алгоритми управління та адаптації в ТКС» для студентів денної форми навчання спеціальності 7.092401 – Телекомунікаційні системи та мережі. Харків: ХНУРЕ, 2008. 164 с.

16. Mauthe A., Hutchison D., Cetinkaya E.K., Ganchev I., Rak J., Sterbenz J.P., Gunkelk M., Smith P., Gomes T. Disaster-resilient communication networks: Principles and best practices. Resilient Networks Design and Modeling (RNDM) 2016: Proceedings of the 8th International Workshop. Halmstad, Sweden, 13-15 September, 2016. IEEE, 2016. P. 1-10. DOI: 10.1109/RNDM.2016.7608262.

17. Телекомунікаційні системи та мережі. Структура та основні функції [Електронний ресурс] / В. В. Поповський та ін. Т. 1. Харків: СМІТ, 2011. Режим доступу: http://www.znanius.com/3534.html.

18. Lemeshko O. V., Arous K. M., Yeremenko O. S. Fault-Tolerant Unicast, Multicast and Broadcast Routing Flow-based Models. Scholars Journal of Engineering and Technology (SJET). 2015. Vol. 3, Issue 4A. P. 343–350.

19. Medhi D., Ramasamy K. Network Routing, Second Edition: Algorithms, Protocols, and Architectures (The Morgan Kaufmann Series in Networking) 2nd Edition. Cambridge, MA, USA: Elsevier Inc., 2018. 1018 p.