НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ

КАФЕДРА СИСТЕМНОГО ПРОГРАМУВАННЯ І
СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ

«На правах рукопису»
УДК 004.7

«До захисту допущено»

в.о. завідувача кафедри СПСКС

_____ Віталій РОМАНКЕВИЧ_

"_ __"_____2020р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 123 Комп'ютерна інженерія
Комп'ютерні системи та компоненти

на тему: «Спосіб підвищення ефективності вибору шляху при груповій маршрутизації»

Виконала: студентка ІІ курсу, групи КВ-81мн
Войтенко Єлизавета Дмитрівна _____
(підпис)

Науковий керівник доц. каф. СПСКС к.т.н., доцент Орлова М.М. _____
(підпис)

Рецензент доцент каф., к.т.н. Щербина О.А. _____ _____

Консультант з нормо контролю доцент, с.н.с., к.т.н. Боярінова Ю.Є. _____
_____
(підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студентка _____
(підпис)

Київ – 2020 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет прикладної математики

Кафедра системного програмування і спеціалізованих комп'ютерних систем

Рівень вищої освіти – другий (магістерський)
за освітньо-науковою програмою
Спеціальність 123 Комп'ютерна інженерія
Комп'ютерні системи та компоненти

ЗАТВЕРДЖУЮ
Завідувач кафедри СПСКС

_____ Володимир ТАРАСЕНКО_
(підпис) (ініціали, прізвище)

"___"_____2018р.

ЗАВДАННЯ
на магістерську дисертацію студентці
Войтенко Єлизаветі Дмитрівні
(прізвище, ім'я, по батькові)

1. Тема дисертації «Спосіб підвищення ефективності вибору шляху при груповій маршрутизації»,
науковий керівник дисертації доц. каф. СПСКС к.т.н., доцент Орлова М.М,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від « 07 » квітня 2020 р. № 963-С

2. Термін подання студентом дисертації 13 травня 2020 р._____

3. Об'єкт дослідження: процес та принципи функціонування протоколу групової маршрутизації BGP.

4. Предмет дослідження: програмна реалізація розробленого способу підвищення ефективності пошуку шляху при груповій маршрутизації.

5. Перелік завдань, які потрібно розробити: провести аналіз сучасної проблеми пошуку оптимального шляху при груповій маршрутизації, вивчити існуючі методики вирішення цієї проблеми, розробити модифіковану імітаційної моделі, розробити власний спосіб на основі проведених досліджень.

6. Перелік ілюстративного матеріалу: плакати (6), презентація _____
_____

7. Перелік публікацій (мінімальна кількість):

Одна стаття у науковому фаховому виданні.

Участь у науковій конференції.

8. Дата видачі завдання 5 вересня 2018 р. _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1.	Ґрунтовне ознайомлення з предметною галуззю	05.11.2018	
2.	Визначення структури магістерської дисертації; вивчення літератури, пошук додаткової літератури, патентний пошук	22.04.2018	
3.	Робота над першим розділом магістерської дисертації; структуризація теоретичного матеріалу	30.09.2019	
4.	Робота над тезами доповіді за проміжними етапами розробки додаткового програмного забезпечення (модифікована імітаційна модель)	07.10.2019	
5.	Проведення наукового дослідження; робота над другим розділом магістерської дисертації	10.02.2020	
6.	Робота над статтею для фахового видання за результатами проведеного наукового дослідження	13.03.2020	
7.	Проведення наукового дослідження; робота над третім розділом магістерської дисертації	17.04.2020	
8.	Оформлення текстової і графічної частини магістерської дисертації	24.04.2020	
9.	Попередній розгляд магістерської дисертації на кафедрі	13.05.2020	

Студентка _____ Єлизавета ВОЙТЕНКО

Науковий керівник дисертації _____ Марія ОРЛОВА

РЕФЕРАТ

Актуальність теми. Кожен день все більше використовується мережа Інтернет для обміну інформацією, що в значній мірі є можливим завдяки функціонуванню протоколу BGP (Border Gateway Protocol), як єдиного протоколу зовнішньої групової маршрутизації між окремими мережами. Через швидкий приріст кількості користувачів та збільшення об’ємів інформації, що передається, знов і знов піднімається питання про підвищення ефективності та оптимізацію пошуку шляху для передачі даних при такій маршрутизації.

Мета роботи: підвищення ефективності пошуку шляху передачі даних при груповій маршрутизації та розробка й оптимізація способу перерозподілу навантаження каналів зв’язку з використанням програмного контролера.

Для досягнення поставленої мети в роботі вирішуються наступні завдання.

1. Аналіз існуючих методик покращення критеріїв пошуку ефективного шляху при груповій маршрутизації.
2. Дослідження проблеми пошуку оптимального шляху при груповій маршрутизації.
3. Розробка модифікованої імітаційної моделі.
4. Розробка способу підвищення ефективності пошуку шляху при груповій маршрутизації з використанням програмного контролера, що базується на контролі і перерозподілі навантаження каналів зв’язку.

Об’єктом дослідження є процес та принципи функціонування протоколу групової маршрутизації BGP.

Предметом дослідження є спосіб підвищення ефективності пошуку шляху при груповій маршрутизації, що базується на контролі і перерозподілі навантаження каналів зв'язку.

Методи дослідження. В роботі використовуються методи оптимізації, методи моделювання комп'ютерних мереж.

Наукова новизна одержаних результатів полягає в наступному:

1. Проаналізовано основні методики покращення критеріїв пошуку ефективного шляху при груповій маршрутизації.
2. Запропоновано спосіб з використанням програмного контролеру для підвищення ефективності пошуку маршруту через примусовий перерозподіл трафіку за наявними посиланнями на основі використання або затримки посилань.
3. Розроблена модифікована імітаційна модель для проведення безпечних тестувань та збору тестових даних.

Практична цінність одержаних результатів полягає в тому, що запропонований спосіб підвищує показники ефективності пошуку шляху при груповій маршрутизації за часовим критерієм, що дозволяє отримати виграш у середньому до 3,5% у порівнянні з вже існуючими аналогами і при цьому він не має впливу на безпеку функціонування мережі та протоколу, з якими працює.

Апробація роботи. Основні положення і результати роботи були представлені та обговорювались на XIV всеукраїнській науково-методичній конференції «Проблеми охорони праці, промислової та цивільної безпеки 2018», XII науковій конференції молодих вчених «Прикладна математика та комп'ютинг» ПМК-2019 (Київ, 13-15 листопада 2019 р.).

Публікації. За результатами магістерської дисертації було опубліковано 3 наукові роботи, з них 1 стаття у науковому фаховому виданні України (у виданні, що реферується наукометричною базою) та 2 тези доповідей. Науковий журнал «Комп'ютерні-інтегровані технології: освіта, наука, виробництво» – Луцьк, 2020. Випуск №39.

Структура та обсяг роботи. Магістерська дисертація складається з вступу, трьох розділів, висновків та додатків.

У вступі надано загальну характеристику проблематики ефективності групової маршрутизації, сформульовано мету дослідження, показано практичну цінність роботи.

У першому розділі надано детальне обґрунтування актуальності напрямку досліджень, виконано оцінку поточного стану в даній сфері, представлено теоретичний огляд особливостей функціонування BGP.

У другому розділі проаналізовано критерії оптимізації пошуку шляху, досліджено методи покращення цих критеріїв; розглянуто вимоги до імітаційної моделі, для тестування способу підвищення ефективності пошуку шляху.

У третьому розділі розроблено та описано програмний контролер для підвищення ефективності шляху при груповій маршрутизації, представлена порівняльна характеристика запропонованого способу з вже існуючими.

У висновках проаналізовано отримані результати роботи.

Робота виконана на 81 аркуші, містить 3 додатки та посилання на список використаних літературних джерел з 37 найменувань. У роботі наведено 21 рисунків та 4 таблиці.

Ключові слова: Border Gateway Protocol, BGPSEC, оптимізація маршрутизації, групова маршрутизація, імітаційна модель.

ABSTRACT

Actuality of the theme. Every day, the Internet is increasingly used to exchange information, which is largely possible due to the functioning of the BGP protocol (Border Gateway Protocol), as a single protocol for external group routing between individual networks. Due to the rapid increase in the number of users and the increase in the amount of information transmitted, the question of improving the efficiency and optimization of finding a way to transmit data with such routing is raised again and again.

The goal of the work: increase the efficiency of data path retrieval in group routing and develop and optimize the method of load redistribution of communication channels using a software controller.

To achieve this goal, the following tasks are solved in the work.

1. Analysis of existing methods for improving the criteria for finding an effective way for group routing.
2. Research of a problem of search of an optimum way at group routing.
3. Development of a modified simulation model.
4. Development of a method to increase the efficiency of path finding in group routing using a software controller based on control and redistribution of communication channels.

The object of the research is the process and principles of operation of the BGP group routing protocol.

The subject of the research is way to increase the efficiency of path finding in group routing, based on the control and redistribution of communication channels.

Research methods. Optimization methods, network modeling methods are used in the work.

The scientific novelty of the obtained results is as follows:

1. The main methods of improving the criteria for finding an effective way for group routing are analyzed.
2. The method using a software controller to increase the efficiency of route search through forced redistribution of traffic on existing links based on the use or delay of links is proposed.
3. Developed a modified simulation model for safe testing and collection of test data.

The practical value of the obtained results is that the proposed method increases the efficiency of finding a path with group routing by time criterion, which allows you to gain an average of up to 3.5% compared to existing counterparts and it does not affect the safety of operation the network and protocol it works with.

Approbation of work. The main provisions and results of the work were presented and discussed at the XIV All-Ukrainian scientific-methodical conference "Problems of labor protection, industrial and civil safety 2018", XII scientific conference of young scientists "Applied Mathematics and Computing" PMK-2019 (Kyiv, 13-15 November 2019).

Publications. According to the results of the master's dissertation, 3 scientific works were published, including 1 article in the scientific professional publication of Ukraine (in the publication, which is referenced by the scientometric base) and 2 abstracts. Scientific journal "Computer-integrated technologies: education, science, production" - Lutsk, 2020. Issue №39.Structure and scope of work.

The master's thesis consists of an introduction, three sections, conclusions and appendices.

The introduction gives a general description of the problems of the efficiency of group routing, formulated the purpose of the study, shows the practical value of the work.

The first section provides a detailed justification for the relevance of the research direction, assesses the current state of affairs in this field, presents a theoretical overview of the features of BGP functioning.

In the second section the criteria of optimization of search of a way are analyzed, methods of improvement of these criteria are investigated; the requirements to the simulation model for testing the way to increase the efficiency of the path search are considered.

The third section develops and describes a software controller to improve the efficiency of the path in group routing, presents a comparative characteristic of the proposed method with existing ones.

The conclusions are analyzed the results of work.

The work is done on 81 sheets, contains 3 attachments and a link to the list of used literary sources of 37 titles. The paper presents 21 figures and 4 tables.

Keywords: Border Gateway Protocol, BGPSEC, routing optimization, group routing, simulation model.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ, СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ

BGP – англ. Border Gateway Protocol, укр. протокол граничного шлюзу – протокол зовнішньої маршрутизації, що використовується для зв’язку між автономними системами в мережі Інтернет.

EBGP – англ. exterior BGP, укр. зовнішній BGP – протокол BGP, що працює між автономними системами; eBGP-сусіди повинні бути безпосередньо пов'язані за замовчуванням.

EGP – англ. Exterior Gateway Protocol, укр. протокол зовнішнього шлюзу – протокол зовнішньої маршрутизації, що використовувався для обміну даними між декількома автономними системами; був замінений протоколом BGP.

IBGP – англ. interior BGP, укр. внутрішній BGP – протокол BGP, що працює всередині автономної системи; iBGP-сусіди не обов'язково повинні бути безпосередньо пов'язані.

IETF – англ. Internet Engineering Task Force, укр. Інженерна Рада мережі Інтернет – відкрита міжнародна спілка проектувальників, учених, мережевих операторів та провайдерів, яке займається розвитком протоколів і архітектури мережі Інтернет.

MRAI-таймер – англ. Minimum Route Advertisement Interval timer, укр. таймер мінімального інтервалу оголошення маршруту – це таймер зі значенням за замовчуванням 30 секунд, який змушує маршрутизатори BGP чекати хоча б таку кількість часу, перш ніж надсилати оголошення повторно за тим же самим префіксом.

QoS – англ. Quality of Service, укр. якість обслуговування – набір методів для управління ресурсами пакетних мереж.

RFC – англ. Request for Comments, укр. запит на обговорення – серія пронумерованих інформаційних документів мережі Інтернет, що містить технічні специфікації та стандарти.

RFC4271 – документ, в якому прописана специфікація (стандарт) четвертої, на момент написання статті останньої, версії протоколу BGP.

SDN – англ. Software-defined Networking, укр. програмно-конфігурована мережа – комп'ютерна мережа для передачі даних, що має відділений від модулів передачі даних програмно реалізований рівень управління мережею.

SLA – англ. Service Level Agreement, укр. угода про рівень обслуговування – угода про характеристики наданих послуг та їх необхідний рівень між постачальником цих послуг та користувачем.

SPVP – англ. Simple Path Vector Protocol, укр. протокол простого векторного шляху – це модифікована версія протоколу BGP, яка фіксує основну семантику BGP шляхом вилучення всіх несуттєвих деталей для підвищення рівня безпеки через підвищення ефективності вибору шляху.

SSLD – англ. Sender Side Loop Detection, укр. виявлення бічної петлі відправника – методика підвищення ефективності пошуку шляху при груповій маршрутизації, що базується на додаткових перевірках на наявність одержувача повідомлення в маршруті, що оголошується, перед відправленням повідомлення про новий використовуваний маршрут сусіду.

Update-повідомлення – повідомлення протоколу BGP, що призначене для оголошення та видалення маршрутів по мережевим префіксам; після встановлення з'єднання пересилаються всі маршрути, які маршрутизатор хоче оголосити сусідові, надалі пересилаються тільки дані про додані або видалені маршрути по міру їх появи.

АС – укр. автономна система, англ. Autonomous System – система IP-мереж та маршрутизаторів, керованих одним або більшою кількістю постачальників, що мають єдину політику маршрутизації з мережею Інтернет.

Імітаційна модель – програмний модуль, що імітує функціонування мережі та протоколу для маршрутизації всередині неї, і використовується для моделювання певних ситуацій та тестування способів покращення маршрутизації без можливої шкоди робочим мережам та їх користувачам.

Перехідні петлі – англ. transient loops – явище, що є характерним для класу маршрутно-векторних протоколів маршрутизації та полягає в тому, що після зникнення маршруту до одного з префіксів протокол може перебрати велику кількість недійсних альтернативних маршрутів в процесі пошуку оптимального шляху до того, як прийти до стабільного маршруту.

Сусіди – англ. peers – будь-які два маршрутизатори, між якими відкрито TCP-з'єднання для обміну інформацією про маршрутизації.

ВСТУП

На теперішньому етапі взаємин між людьми та технологіями передачі даних за допомогою різноманітних комп'ютерних мереж зовсім звичайна і для багатьох повсякденна справа. Однак, через дуже швидкісний приріст користувачів, який передбачає й збільшення кількості об'єднаних груп маршрутизаторів, а також через зростання вимог до критеріїв якості передачі даних постало питання про способи підвищення ефективності маршрутизації.

Досягти оптимізації вибору шляху – це мета, яка була важливою для інженерів-розробників ще на ранніх стадіях користування комп'ютерними технологіями та вона ж не втрачає своєї актуальності та перспективності можливих досліджень навіть зараз. Важливим моментом при ознайомленні з цим питанням є прийняття до уваги того, що вже понад чверть століття фактично єдиним масово використовуваним протоколом, що диктує правила при зовнішній груповій маршрутизації є протокол BGP (Border Gateway Protocol). Він був вперше запропонований в 1989 році, та за цей чималий термін майже не зазнав якихось суттєвих перетворень, хоча вже вийшла і була введена в експлуатацію четверта версія протоколу, що лише свідчить про його фундаментальність. Це стандартний протокол маршрутизації в мережі Інтернет, який використовується в якості магістральної технології для задач логічної маршрутизації для забезпечення глобального зв'язку в світі.

Проте, навіть зважаючи на цей факт, чимала кількість людей веде свою науково-дослідницьку діяльність у напрямку пошуку можливостей розробки методів, способів та/або методологій, які можна впровадити для підвищення ефективності вибору шляху при груповій маршрутизації. До цього можна додати й те, що для тестування цих варіантів потрібно провести суттєву підготовку, в тому числі підібрати чи то навіть розробити спеціальні імітаційні моделі, які

моделюють певні алгоритми поведінки мережі за певних потрібних умов. Хоча існують і такі моделі, що знаходяться у відносно вільному доступі, зазвичай вони вузькоспрямовані, тому підходять не для всіх тестувань розробок.

В магістерській дисертації розглянутий спосіб покращення ефективності пошуку шляху при груповій маршрутизації, розроблена на базі проведених досліджень та вже наявних аналогів імітаційна модель, яка дозволяє протестувати отримані результати на практиці без ризиків створення проблем для звичайних користувачів.

1 АНАЛІЗ ПРОБЛЕМИ ТА ОБҐРУНТУВАННЯ ТЕМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИБОРУ ШЛЯХУ

1.1 Аналітичний огляд проблеми пошуку оптимального шляху при груповій маршрутизації

В повсякденному застосуванні часто ставиться завдання прокладення маршрутів між різними точками, для з’єднання їх між собою. В першу чергу важливо просто знайти маршрут між двома чи більшою кількістю модулів. Якщо дана задача є можливою до виконання, то на наступному етапі за мету береться оптимізація цього маршруту за деякими параметрами.

У комп’ютерних мережах теж існує потреба з’єднувати різновіддалені точки між собою, іноді навіть складається потреба в груповому з’єднанні, тобто прокладанні маршрутів між групами модулів, або від одного модуля до групи чи навпаки. Під пошуком оптимального шляху в комп’ютерних мережах слід розуміти зменшення інтервалу часу для приведення таблиці маршрутизації в коректний (функціонально робочий) стан.

При маршрутизації в мережі немає ризиків, що інформація сама по собі «заблукає» чи «вирішить піти в іншу сторону», як це може бути з кур’єром у звичайному житті. Проте проблема з людським фактором залишається, і дані можуть бути відправлені за неправильно визначеним шляхом. Наприклад, через перевантажений вузол чи відсутню адресу. Ще гіршим є варіанти з витоком маршрутів (в англомовній термінології route leaks), коли у мережі з’являється анонс з кращим префіксом, але далекий від потрібного напрямку.

Також окремо треба виділити ситуацію в груповій маршрутизації з утворенням перехідних петель (в англомовній літературі transient loops). Це явище є особливістю при пошуку оптимального шляху, що є характерним для класу маршрутно-векторних протоколів маршрутизації. Воно базується на тому, що після зникнення маршруту до одного з префіксів протокол може перебрати велику кількість недійсних альтернативних маршрутів в процесі

пошуку оптимального шляху до того, як зійтися до стабільного маршруту. Перебір таких альтернативних маршрутів призводить до утворення «уявних» циклів маршрутизації, що і називається перехідними петлями.

Для поставленої задачі найбільш цікавим є розгляд проблематики саме зі сторони перехідних петель, тому далі буде наведений більш детальний опис та аналіз їх функціонування.

На рисунку 1.1 представлений процес формування перехідної петлі для мережі з невеликою кількістю маршрутизаторів, а саме з 6.

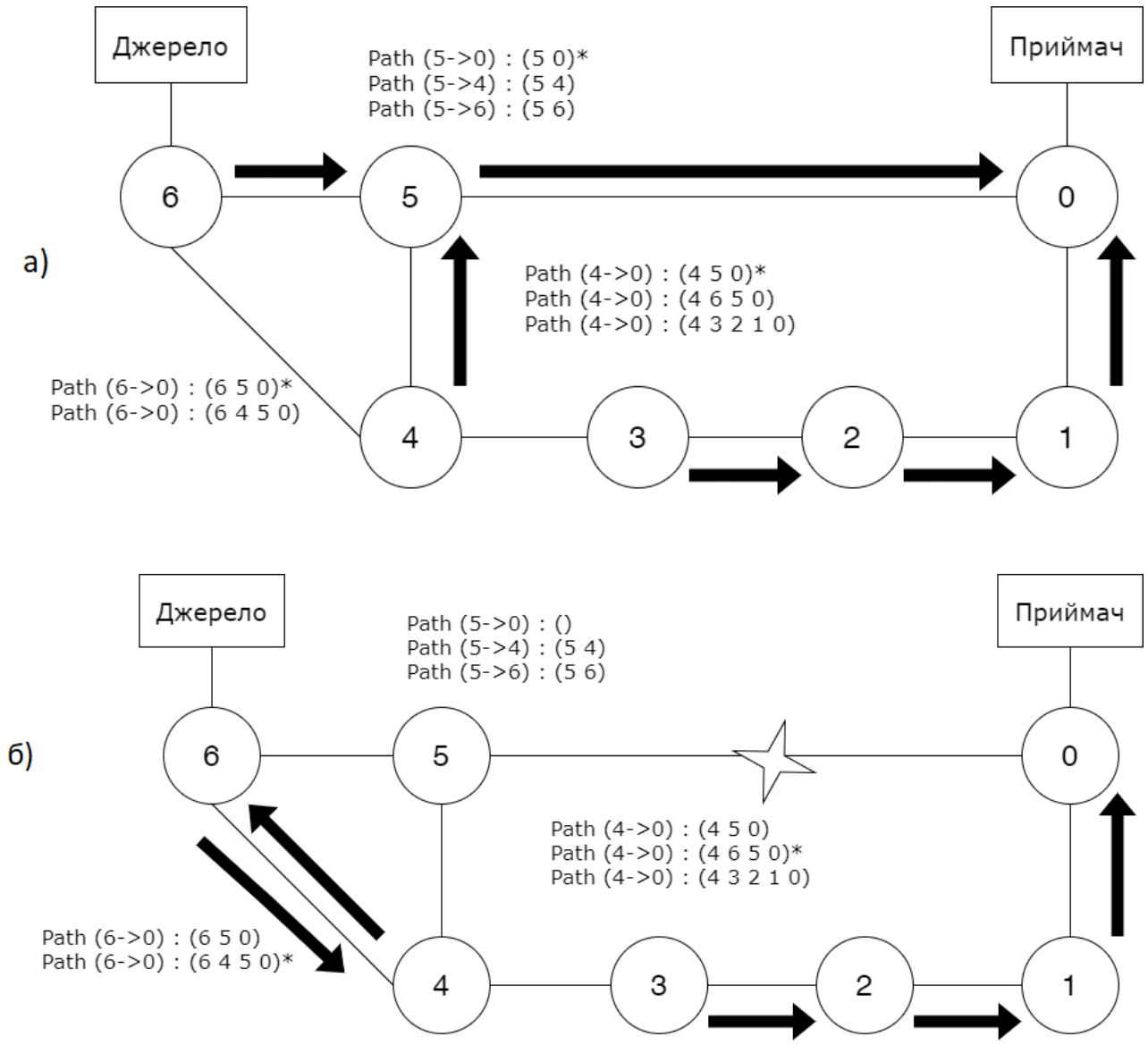

Рисунок 1.1 – Модель формування transient loop: а) коректний випадок: б) некоректний пошук шляху при розриві зв’язку (5-0)

У ситуації, що зображена на рисунку, пакети повинні маршрутизуватися з вузла 6 в вузол 0. На початку найкращим шляхом до вузла 0 з вузла 6 буде маршрут (6-5-0), якщо брати за критерій оцінки кількість хопів (проміжних ділянок). Крім того вузол 6 зберігає інформацію про маршрут (6-4-5-0), проте в початковий момент часу даний маршрут не є тим, якому віддається перевага. Для наочності на рисунку 1.1 а) ще описані маршрути до вузла 0 з вузлів 5 і 6, бажані маршрути відзначені «*».

Розглянемо ситуацію, в якій лінія зв'язку між вузлами 5 і 0 обривається (рис. 1.1 б), про що вузол 5 сповіщає своїх сусідів (вузли 4 і 6) за допомогою спеціальних повідомлень. Отримавши дані повідомлення, вузли 6 і 4 видаляють зі своїх таблиць маршрутизації маршрути, які були отримані ними від вузла 5 (4-5-0, 6-5-0) і розсилають своїм сусідам повідомлення про видалення цих маршрутів, після чого переходять на наступні бажані маршрути (6-4-5-0, 4-6-5-0) і посилають сусіднім маршрутизаторам повідомлення про нові доступні маршрути до вузла 0.

Таким чином, в той час як обидва вузла 4 і 6 знають, що не можуть маршрутизувати пакети до вузла 0 безпосередньо через вузол 5, вони не знають, що нові обрані ними маршрути також недійсні. В даному випадку цикл швидко знаходиться, коли вузли 4 і 6 отримують спеціальні повідомлення один від одного про видалення маршрутів 4-5-0 та 6-5-0. Новим маршрутом, для якого віддається перевага, для вузла 4 стає маршрут (4-3-2-1-0), про який вузол 4 повідомляє вузли 5 і 6. І ось в нас знову є коректна таблиця маршрутизації.

На практиці такі цикли мають істотно більший розмір, а таймер MRAI (Minimum Route Advertisement Interval) таймер перешкоджає швидкому поширенню спеціальних повідомлень. Раніше вже було доведено, що внаслідок цього час пошуку оптимального шляху в даній мережі при маршрутизації протоколу BGP при видаленні маршруту в графі BGP маршрутизаторів час пошуку оптимального шляху протоколу в даній мережі

пропорційний значенню MRAI таймера та Гамільтоновому шляху в графі, що містить маршрутизатор, маршрут до якого видалявся [37].

Стандартних засобів протоколу групової маршрутизації BGP недостатньо для швидкого виявлення перехідних петель в процесі збіжності протоколу. Хоча з часу впровадження протоколу було запропоновано декілька методик для боротьби з утворенням перехідних петель та прискоренню часу оптимального шляху при груповій маршрутизації протоколу.

Були виділені наступні дві задачі, пов’язані з дослідженням пошуку оптимального шляху при груповій маршрутизації протоколу BGP та його різноманітних модифікацій.

1. Визначення, чи є проблема «відкладеного пошуку» суттєвою для заданої топології.
2. Визначення набору застосовуваних методик, які дозволять мінімізувати час пошуку оптимального шляху при груповій маршрутизації (кількість переданих повідомлень оновлення), при цьому задовольняючи обмеженням на величину накладних витрат, пов'язаних із застосуванням даних методик.

Обидві задачі зводяться до оцінки часу пошуку оптимального шляху при груповій маршрутизації та кількості переданих повідомлень про оновлення для заданої мережі автономних систем.

Для вирішення задачі пошуку оптимального шляху при груповій маршрутизації вже були створені різні методи, методології та способи. Їх ефективність, класифікація та недоліки розглядаються в наступному розділі. Незважаючи на все різноманіття можливих варіантів рішень, усі вони проходять один і той самий шлях до реалізації.

Спочатку обирається напрям та головна міні-проблема для дослідження, проводиться збір даних за заданим напрямом, чому так вже спробували, чому випробуваний підхід не став широковживаним. Далі створюється власна стратегія, «вихід» із ситуації і реалізується на практиці. Однак, просто взяти і впровадити свій винахід до однієї чи декількох автономних систем, що мають

доступ до мережі Інтернет, ризиковано [14]. Тому для тестувань та випробувань використовують імітаційні моделі, що дозволяють відтворити поведінку протоколу в різних ситуаціях, при цьому не нашкодивши іншим звичайним користувачам мережі Інтернет. Після довгого й різностороннього тестування та виправлення недоліків, можна представляти до розгляду Інженерній Раді Інтернету IETF (Internet Engineering Task Force), яка після схвалення може відправити на обмежене використання. Це такий період, коли мережевий винахід випробовують на повноцінній, але обмеженій мережі. Пройшовши такий шлях, рішення проблеми може бути офіційно впроваджене в широкий доступ. Є ще короткий шлях, замість звернення до IETF викласти в вільний доступ. Такий варіант не є офіційним, але може допомогти в майбутніх дослідженнях.

1.2 Визначення поняття автономної системи в зовнішній груповій маршрутизації

Перш ніж переходити до самого протоколу BGP, потрібно чітко окреслити поняття автономної системи (АС). Це система IP-мереж та маршрутизаторів, керованих одним або більшою кількістю постачальників, що мають єдину політику маршрутизації з мережею Інтернет [36]. Підкреслюю, що дане визначення є дійсним лише у рамках, які мають відношення до протоколу BGP.

Автономні системи можна розділити на три наступні категорії, залежно від їх з'єднань з іншими АС і режиму роботи:

1. Багатоінтерфейсна (multihomed) АС – це АС, яка має зв’язок з декількома Інтернет-провайдерами, що дозволяє цій АС доступ до Інтернету у випадку, коли стається розірвання з’єднання з основним

провайдером. Такий тип АС не підтримує передачу транзитного трафіку інших АС через свої ресурси.

2. Обмежена (stub) АС – це АС, яка має лише одне підключення до іншої однієї АС. Згідно з деякими опублікованими науковими дослідженнями [3] такий спосіб користування АС не є бажаним за тієї причини, що тоді мережа повністю підпадає під опіку одного Інтернет-провайдера, а значить відпадає потреба в унікальній ідентифікації на рівні мережі АС.
3. Транзитна (transit) АС – це АС, яка в основному є проміжним пунктом для трафіку сусідів поміж АС. Тобто для якихось двох мереж, яким необхідно налагодити зв’язок між собою, третя (транзитна) АС є дозволеним проміжним пунктом в передачі даних.

До 2007 року були можливі тільки 16-бітні номера АС, тобто всього було доступно 65536 номерів, де 0 і 65535 – зарезервовані [27]. Номери в інтервалі від 64512 до 65534 призначалися для приватних АС, що не маршрутизуються глобально – аналог приватних IP-адрес. Інтервал 64496-64511 відводився для використання в прикладах і документації. Зараз можливе використання 32-бітних номерів АС [28].

На момент написання даного тексту в світі існує лише 100 338 АС, з них в Україні – 2448, що дозволяє Україні зайняти 9 місце з 242 у світі за кількістю АС [32]. Хоча ще 5 років тому Україна знаходилась на третьому місці, поступаючись лише РФ та США. Це свідчить про дійсно швидкий розвиток мережі Інтернет та зацікавленості користувачів в її безпечній та налагодженій роботі.

Всередині АС є внутрішні маршрутизатори та граничні. Внутрішні потрібні для зв’язку всередині однієї АС, і вони не мають прямого доступу назовні, а граничні використовуються для зв’язку між АС. Тобто, як показано на рисунку 1.2, всередині однієї АС, яка позначається блакитною областю, маршрутизатори вільно обмінюються даними між собою через внутрішній протокол (синій пунктир), а щоб переслати трафік за межі власної АС,

потрібно використати протокол для зовнішньої маршрутизації і тільки через граничний маршрутизатор (червоний пунктир).

Саме через таке розмежування між функціями маршрутизаторів BGP і отримав свою назву – протокол граничного шлюзу.

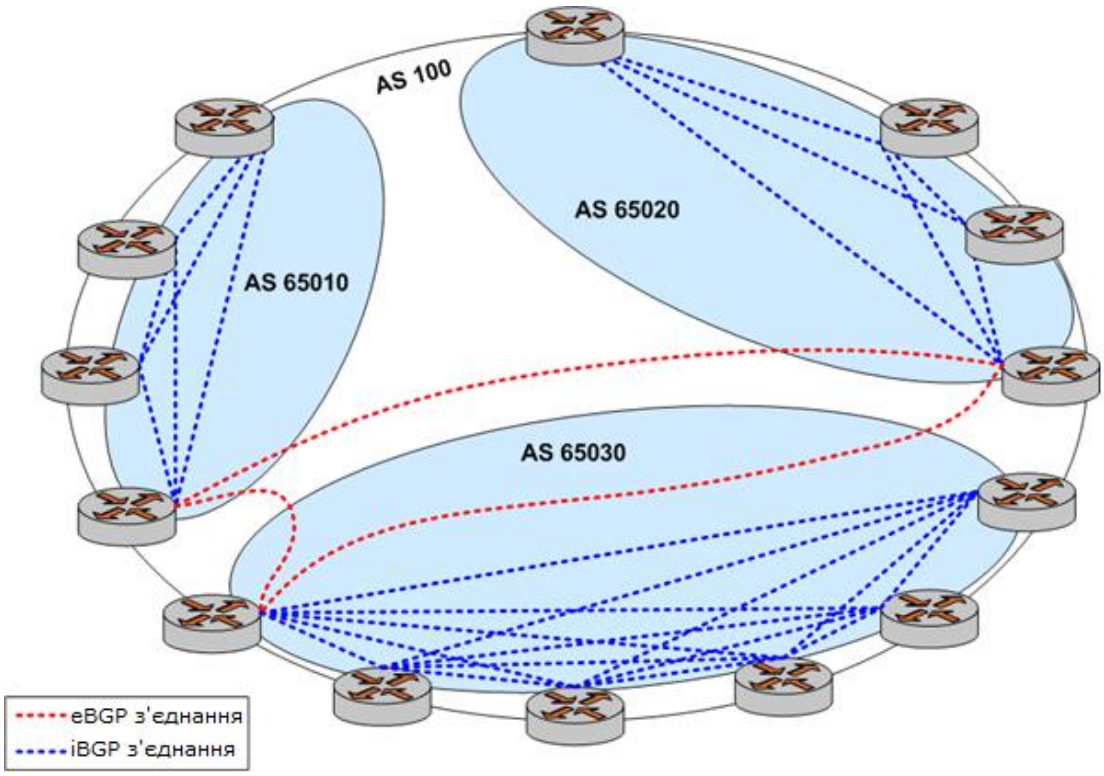

Рисунок 1.2 – Приклад взаємодії автономних систем

1.3 Протокол маршрутизації BGP

Принциповою відмінністю зовнішньої маршрутизації від внутрішньої є наявність політики маршрутизації, тобто при розрахунку маршруту розглядається не тільки метрика, заснована на довжині шляху, а й політичні та економічні міркування. Ця обставина не дозволяє адаптувати під завдання зовнішньої маршрутизації протоколи внутрішньої маршрутизації, застосувавши їх до графа автономних систем.

Для вирішення завдання зовнішньої маршрутизації й був розроблений протокол BGP, який спочатку мав стати лише тимчасовим рішенням для тестового використання, щоб потім усе найкраще з нього перенести на протокол зовнішнього шлюзу EGP (Exterior Gateway Protocol). Однак, «багато тимчасових рішень залишаються з нами на дуже довгий термін, а надійні довгострокові рішення так ніколи і не створюються», як відмітив один з винахідників BGP Яков Рехтер, який переконався в цьому на власному досвіді [29]. Використовувана в даний момент версія цього протоколу має номер чотири, відповідний стандарт – RFC4271 [20].

Як вже було сказано раніше в більш загальній формі, принцип взаємодії протоколу BGP між різними АС та всередині однієї АС відрізняється. Якщо маршрутизатори належать одній автономній системі, то вони працюють за протоколом Internal BGP (IBGP), а якщо вони знаходяться в різних АС, то працюють відповідно до протоколу External BGP (EBGP). Однак, треба зазначити, що це стосується лише передачі трафіку для мережі Інтренет, адже всередині однієї АС може передаватися також і внутрішній трафік за правилами якогось іншого протоколу внутрішньої маршрутизації.

На фундаментальному рівні BGP допомагає маршрутизаторам приймати рішення про те, куди слід направляти гігантські потоки даних (поточний розмір таблиці для IPv4 понад дев’ятсот тисяч маршрутів, а для IPv6 – трохи за 100 тисяч, рис. 1.3 [4]), що передаються через величезну комунікаційну мережу, яка вістить значну кількість ліній зв'язку, що перетинаються між собою. При майже нескінченному числі можливих шляхів – як прямих та швидких, так і заплутаних та повільних – BGP надає маршрутизаторам інформацію, потрібну їм для вибору шляху, незважаючи на те, що загальною карти мережі Інтернет немає і відсутній авторитетний вузол, який би відповідав за підбір напрямків для трафіку.

Створення протоколу BGP, робота якого заснована на тому, що окремі мережі безперервно обмінюються інформацією про доступні канали передачі даних, допомогло мережі Інтернет продовжити своє зростання та стати по-

справжньому глобальним механізмом, що працює з величезними об’ємами трафіку. Однак BGP також дозволяє майже кожному, в кого є доступ до ліній зв'язку й необхідні навички, перехоплювати ті ж самі величезні обсяги даних.

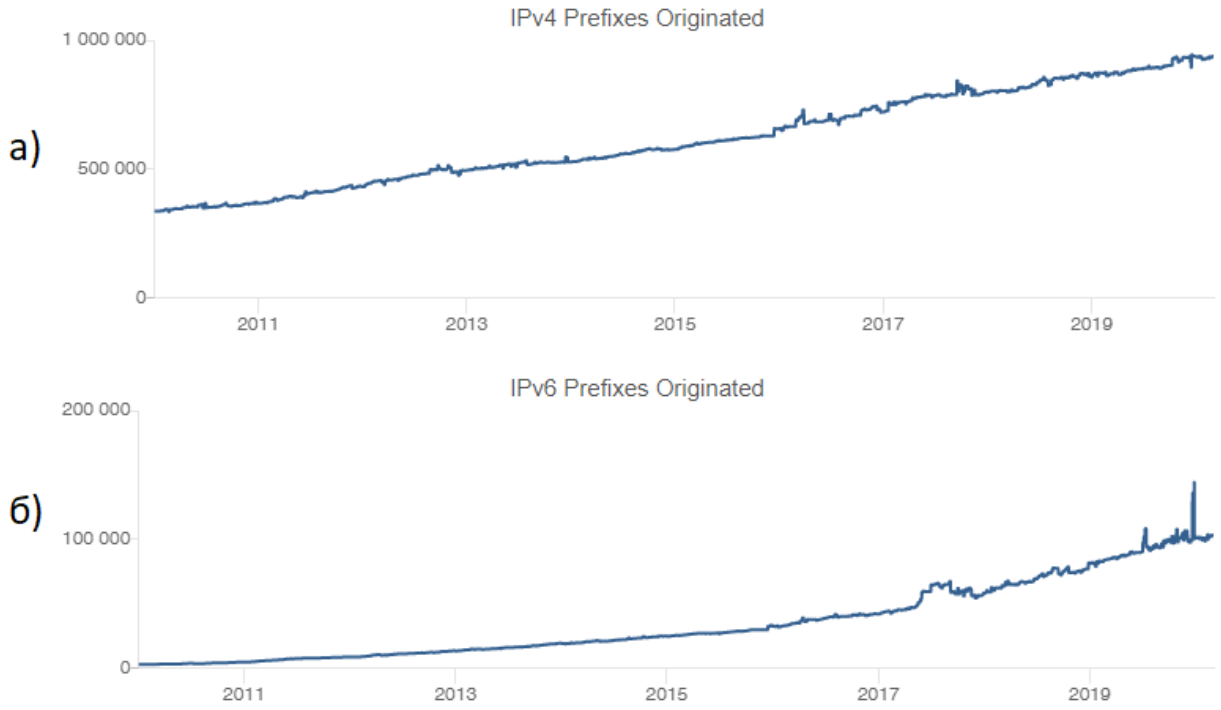

Рисунок 1.3 – Статистика за останні 10 років (абсциса) по приросту префіксів (ордината): а) IPv4; б) IPv6

Головна причина цього полягає в тому, що протокол BGP, як і багато інших ключових систем в мережі Інтернет, довіряє користувачам. Це цілком доречний принцип в менших мережах, але в глобальному масштабі він відкриває широкі можливості для атак різного типу.

1.3.1 Види повідомлень BGP та їх основні атрибути

Маршрутизатори, що використовують протокол BGP, обмінюються інформацією про доступність мереж. Разом з інформацією про мережі

передаються різні атрибути цих мереж, за допомогою яких BGP обирає найкращий маршрут і налаштовуються політики маршрутизації.

Для обміну інформацією між АС в протоколі BGP існує чотири типи сервісних повідомлень:

- OPEN – надсилається після встановлення TCP-з'єднання; відповіддю на OPEN є повідомлення KEEPALIVE, якщо друга сторона згодна встановити BGP-з'єднання, в іншому випадку надсилається повідомлення NOTIFICATION з кодом помилки, і з'єднання розривається; при цьому маршрутизатори, які встановили BGP з'єднання, називаються BGP-сусідами;
- KEEPLALIVE – повідомлення, призначене для підтвердження згоди встановити BGP з'єднання, а також для моніторингу активності відкритого з'єднання: для цього BGP-сусіди обмінюються KEEPALIVE-повідомленнями через певні інтервали часу;
- UPDATE – повідомлення, що призначене для оголошення та видалення маршрутів по мережевим префіксам; після встановлення з'єднання за допомогою повідомлень UPDATE пересилаються всі маршрути, які маршрутизатор хоче оголосити сусідові (full update), після чого пересилаються тільки дані про додані або видалені маршрути по міру їх появи (partial update);
- NOTIFICATION – повідомлення цього типу використовується для інформування BGP-сусіда про причини закриття з'єднання; після відправки цього повідомлення відправник розриває BGP-з'єднання [16].

Як вже було сказано, BGP-повідомлення типу UPDATE використовуються для передачі маршрутної інформації між BGP-сусідами. Цей тип повідомлення дозволяє оголошувати про один новий маршрут та про недоступність групи старих маршрутів в межах одного повідомлення. У UPDATE повідомленнях передбачені наступні атрибути шляху:

- ORIGIN – стандартний обов'язковий атрибут, який визначає походження шляхової інформації; у даного атрибута маршруту існує три можливих значення:
    - IGP – якщо власником префіксу є АС, якій належить розглянутий маршрутизатор;
    - EGP – якщо власником префіксу є АС, якій не належить розглянутий маршрутизатор;
    - INCOMPLETE – якщо власник префіксу невідомий;
- AS_PATH – стандартний обов'язковий атрибут, який складений з сукупності сегментів шляху; атрибут визначає автономні системи, через які доставлена маршрутна інформація;
- NEXT_HOP – стандартний обов'язковий атрибут, який визначає IP-адресу граничного маршрутизатора, який повинен розглядатися як мета наступного кроку на шляху до точки призначення;
- MULTI_EXIT_DISC – опціональний неперехідній атрибут, який представляє собою натуральне число; величина цього атрибута може використовуватися при виборі одного з декількох шляхів до сусідньої АС;
- LOCAL_PREF – опціональний атрибут, який використовується BGP маршрутизатором, щоб повідомити своїм BGP-сусідам у своїй власній АС ступінь переваги оголошеного маршруту;
- ATOMIC_AGGREGATE – стандартний атрибут, який використовується для інформування BGP-сусідів про вибір маршруту, що забезпечує доступ до більш широкого списку адрес [24].

За існуючими статистичними даними, для визначення найкращого маршруту, більшість адміністраторів АС використовують метрику, що базується на довжині атрибута AS_PATH [26].

Це один з основних атрибутів, який передається з інформацією про маршрут. Інформація, що в ньому мітиться, дозволяє протоколу BGP

визначати де знаходиться мережа відносно інших автономних систем, видаляти петлі при маршрутизації, а також може бути використана під час налаштування політик.

Атрибути протоколу BGP поділяються на групи загальновідомих обов'язкових та дискреційних. Загальновідомі обов'язкові, що повинні мітитися в кожному повідомленні Update та повинні підтримуватися кожною реалізацією програмного забезпечення протоколу BGP, - це AS-PATH, ORIGIN та NEXT-HOP.

Дискреційний атрибут може з'являтися, а може й ні, у кожному повідомленні UPDATE, але вони все одно повинні підтримуватися. До таких атрибутів відносять LOCAL-PREF, MULTI_EXIT_DISC та ATOMIC-AGGREGATE. Хоча останній за початковим задумом відносився до обов'язкових атрибутів, але з часом втратив свою необхідність.

1.3.2 Особливості функціонування протоколу маршрутизації BGP

Маршрутизація, як і будь-який інший процес, здійснюється крок за кроком від однієї АС до іншої, відповідно до тих політик, які в них налаштовані. Всі політики BGP налаштовуються, в основному, по відношенню до зовнішніх АС. Тобто, йдеться про правила взаємодії з ними.

Розглянемо більш детально порядок дій BGP маршрутизатора при отриманні та подальшому анонсування маршруту.

Кожен граничний BGP маршрутизатор використовує три бази даних: Adj-RIBsIn, Loc-RIB і Adj-RIBsOut, в яких містяться відповідно маршрути, отримані від BGP-сусідів, маршрути, які використовуються самим маршрутизатором та маршрути, які оголошуються BGP-сусідам.

На кожному маршрутизаторі, що використовує BGP, налаштовуються дві політики маршрутизації: політика прийому маршрутів та політика анонсування маршрутів.

Для обробки маршрутів в названих вище базах даних, маршрутизатор виконує процедуру BGP-рішення, в якій можна виділити наступні три фази (рис. 1.4).

1. Маршрути, отримані від BGP-сусідів, записуються в базу даних Adj-RIBsIn. Відповідно до політики прийому для кожного маршруту в Adj-RIBsIn обчислюється пріоритет. В результаті деякі маршрути можуть бути відфільтровані (відкинуті, видалені з подальшого розгляду).

2. Далі для кожного префіксу з усіх наявних варіантів маршрутів вибирається маршрут з найбільшим пріоритетом, який визначається в процесі порівняння атрибутів маршруту. Порівняння атрибутів маршруту проводиться послідовно до виявлення першої нерівності:

- якщо NEXT_HOP маршруту не доступний, маршрут ігнорується;
- LOCAL_PREFERENCE – маршрут з більшим значенням атрибута LOCAL_PREFERENCE є кращим;
- AS_PATH – маршрут з більш коротким атрибутом AS_PATH є кращим;
- ORIGIN – маршрут зі значенням, що дорівнює IGP, є кращим, далі пріоритет віддається значенням EGP;
- MED – маршрут з меншим значенням атрибута MED є кращим;
- NEXT_HOP – маршрут з більшим значенням атрибута NEXT_HOP є кращим;
- ROUTER_ID – унікальний ідентифікатор BGP маршрутизатора; маршрут з меншим значенням даного атрибута є кращим;

3. Коротко описати завдання третьої фази можна так – відбір маршрутів для анонсування BGP-сусідам. З бази маршрутів, що використовуються самим маршрутизатором LocRIB, обираються маршрути, що відповідають політиці

анонсування, а результат розміщують в базі маршрутів для оголошення BGP-сусідам Adj-RIBsOut, вміст якої потім і розсилається BGP-сусідам. Для кожного BGP-сусіда може бути реалізована своя політика анонсування маршрутів.

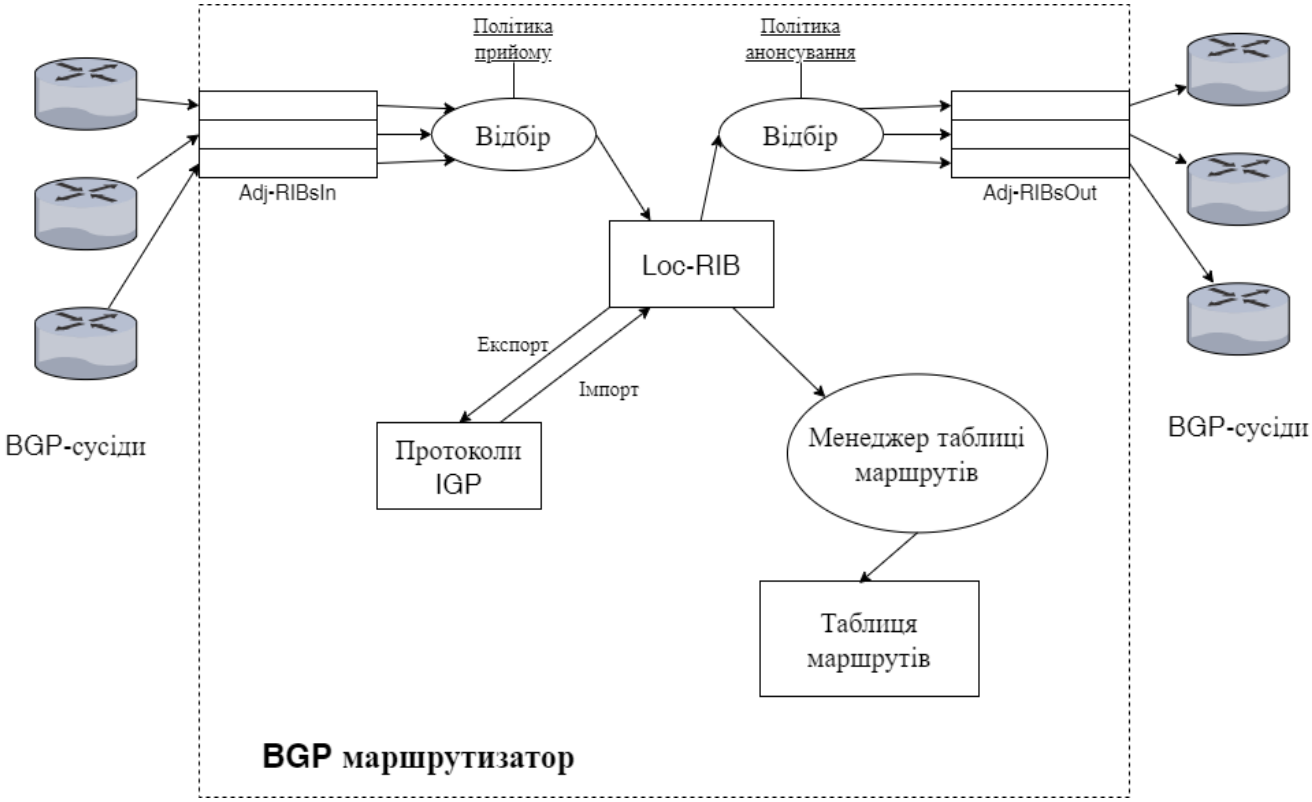

Рисунок 1.4 – Схема роботи BGP-маршрутизатора

Важливою властивістю процесу вибору та анонсування маршрутів є те, що BGP маршрутизатор оголошує тільки ті маршрути, які він сам використовує. Ця обставина є наслідком загальної IP-маршрутизації: при виборі маршруту для дейтаграми враховується тільки адреса одержувача. Таким чином, якщо маршрутизатор сам використовує один маршрут до префікса I, а сусідові оголосив інший, то дейтаграми від сусіда все одно будуть пересилатися до префікса I тим самим маршрутом, який використовує сам маршрутизатор, оскільки адреса відправника при виборі маршруту IP-модулем не розглядається.

Висновки до розділу 1

В даному розділі розглянута та проаналізована проблема пошуку оптимального шляху при груповій маршрутизації. Показана важливість даного питання та виявлені складові частини даної проблеми. Обґрунтовано причини виникнення даної проблеми та виділено дві основні задачі, на які спираються дослідження пошуку оптимального шляху при груповій маршрутизації протоколу BGP.

Викладено основний порядок дій, від визначення основного напряму до впровадження готового рішення, який потрібно реалізувати при розробці розширення для вирішення поставленої задачі з пошуку оптимального шляху при груповій маршрутизації. Доведено, що через те, що цей шлях є досить довгий та з великою кількістю умов, не всі рішення доведено до офіційного введення в загальну експлуатацію.

Представлено та розглянуто основні поняття, пов’язані з протоколом групової зовнішньої маршрутизації BGP, такі як автономна система, атрибути, види повідомлень, політик тощо. Спираючись на статистику приросту кількості автономних систем та префіксів мережі Інтернет, обґрунтована актуальність вибраної тематики.

2 ОПТИМІЗАЦІЯ ЕФЕКТИВНОГО ШЛЯХУ ПРИ ГРУПОВІЙ МАРШРУТИЗАЦІЇ

2.1 Методики покращення критеріїв пошуку ефективного шляху при груповій маршрутизації

Перш ніж розроблювати власний спосіб з підвищення ефективності потрібно розібрати та проаналізувати вже існуючі. Як і сам протокол BGP мав стати лише випробувальною тимчасовою версією EGP, в який би перейшли всі позитивні сторони тестового протоколу без перенесення виявлених недоліків, так і розроблений в даній дисертації спосіб повинен навчитися у своїх попередників історіям успіху та поразок і на них будувати свій шлях до досягнення поставленої мети.

Звісно ж за стільки років існування протоколу з’явився чималий обсяг різноманітніших рішень проблем оптимізації маршрутів і щоб розглянути їх усі не вистачить і декількох років. Тому, для прискорення аналізу і уникнення марнування часу на варіанти не гідні суттєвої уваги, були обрані найбільш успішні та вживанні методики з різною направленістю досліджень.

Всього для огляду було обрано сім методик:

- Sender Side Loop Detection (SSLD) [1];
- Ghost Flushing [5];
- Consistency assertions [17];
- Forwarding edge numbers [7];
- Differentiated BGP Update Processing [25];
- динамічно змінний MRAI таймер [21];
- перестановка Update повідомлень в черзі [21].

Розглянемо основні принципи та ідеї, що реалізовані в кожній методиці.

Перша методика SSLD базується на виявленні бічної петлі відправника. Перед відправленням повідомлення про новий використовуваний маршрут

сусідньому BGP-маршрутизатору відправник перевіряє, чи не присутній одержувач повідомлення в маршруті, що оголошується. Якщо таке припущення є істинним, то відправник видаляє цей маршрут, посилає всім сусідам спеціальне повідомлення про видалення даного маршруту та запускає ще раз процедуру вибору пріоритетного маршруту.

Наприклад, при розгляді описаної в п.1.1 (рис. 1.1) ситуації роутер 4 при отриманні від роутера 5 повідомлення про видалення маршруту (5-0) в звичайній ситуації обере новий бажаний маршрут (4-6-5-0) та відправить його своїм сусідам, хоча ми зрозуміло, що такий маршрут буде хибним і призведе до некоректної роботи системи. Однак, при використанні механізму SSLD перед оголошенням даного маршруту роутеру 5 маршрутизатор під номером 4 помітить, що роутер 5 присутній в новому маршруті, що відправляється, а це в свою чергу свідчить про появу циклу. Тоді роутер 4 замість повідомлення про оголошення нового маршруту, надішле повідомлення про його видалення й відразу перемкнеться на наступний бажаний маршрут.

Авторами методики Ghost Flushing були запропоновані дві модифікації протоколу BGP, застосування яких може бути поєднане: ghost flushing rule та ghost buster rule.

У методиці використовується поняття ghost information, під яким розуміється зберігання в базах даних недійсних на даний момент маршрутів. Прикладом ghost information служить наявність в базі даних маршрутизатора 4 (в прикладі розглянутому в п.1.1) маршруту (4-6-5-0) після видалення маршруту (5-0). Ghost information може поширюватися в мережі BGP маршрутизаторів за допомогою передачі BGP Update-повідомлень.

Ідея методики - прискорити зникнення ghost information з баз даних маршрутизаторів за допомогою генерації наборів спеціальних анулюючих повідомлень.

Ghost Flushing rule. Для швидкого видалення ghost information кожен маршрутизатор намагається якомога швидше повідомити сусідні маршрутизатори якщо шлях, який він до цього анонсував став недійсним.

Це робиться за рахунок наступної модифікації протоколу: коли шлях до маршруту заміщається на довший, та значення таймера MRAI не закінчилось з часу останньої передачі Update-повідомлення, то потрібно послати спеціальне повідомлення про анулювання маршруту усім сусідам. Таким чином якщо раніше оголошений даним маршрутизатором маршрут стане недійсним і при цьому не можна ще відправити нове Update повідомлення, то буде сгененеровано набір спецальних повідомлень про анулювання маршруту, щоб припинити використання недійсного маршруту сусідніми маршрутизаторами. Для топології повнозв'язного графа авторами методики були доведені наступні леми:

Лема 1. Час пошуку ефективного шляху маршрутизації протоколу BGP із застосуванням правила Ghost flushing rule при події видалення маршруту дорівнює добутку числа вершин графа на час передачі BGP повідомлення між двома маршрутизаторами.

Лема 2. Кількість повідомлень про оновлення та ануляцію маршруту, що генеруються в процесі пошуку оптимального шляху для протоколу BGP із застосуванням правила Ghost Flushing rule становить подвійний добуток з попередньої леми 1, помножений ще на кількість дуг в графі.

Ghost Buster rule. Мета даного правила домогтися при його застосуванні поверх правила Ghost flushing rule часу збіжності протоколу не O (n), а O (d), де d – діаметр графа, а n – число вершин графа.

Це досягається за рахунок внесення додаткових затримок при відправці Update повідомлень за допомогою наступної модифікації протоколу: маршрутизатор відправляє Update повідомлення про новий маршрут свого сусіда тільки якщо він отримав повідомлення про цей маршрут delta секунд тому. В іншому випадку він відкладає відправку повідомлення, поки не пройде інтервал часу delta. Авторами методики була доведена наступна лема:

Лемма 1. При застосуванні Ghost buster rule час збіжності протоколу після видалення маршруту складе добуток часу передачі BGP повідомлення між двома маршрутизаторами та діаметру графа при коефіцієнті K, де K – сума

проміжку часу delta та часу передачі BGP повідомлення між двома маршрутизаторами, поділена на цей самий час передачі BGP повідомлення між двома маршрутизаторами.

Ідея методики Consistency assertions полягає в тому, щоб ввести в експлуатацію визначення протоколу SPVP (Simple Path Vector Protocol). При виконанні протоколу SVPV протоколі кожен маршрутизатор вибирає тільки один з усіх можливих шляхів до потрібного префіксу й оголошує його іншим маршрутизаторам в мережі. Для такого протоколу можна ввести поняття «консистентних маршрутів» (consistency paths).

Розглянемо два маршрути до префіксу D: (N1, D) = (N1, A, B, C, D), (N2, D) = (N2, X, B, Y, Z, D). З маршруту (N1, D), випливає, що (B, D) = (B, C, D), а з маршруту (N2, D) слід взяти до уваги, що (B, D) = (B, Y, Z, D). Але з визначення SPVP слід пам’ятати, що в кожен момент часу може існувати тільки один маршрут (B, D). Таким чином можна зробити висновок, що один з маршрутів (N1, D), (N2, D) є недійсним. Автори методики [5] формалізують цей факт шляхом введення наступних визначень:

$$path(N_1, D) = path(N_1, P_1, P_2, \dots, P_n, D) = path(N_1, P_i) + path_{N_1}(P_i, D)$$

Визначення 1. Маршрут (N1, D) є коректними, порожній шлях завжди є коректним.

Визначення 2. Маршрути (N1, D) та (N2, D) є консистентними, якщо виконується одна з умов:

- два порожніх маршрути є консистентними;
- два непустих маршрути, які не містять однакових маршрутизаторів є консистентними;
- порожній маршрут консистентний на непустому маршруті;
- два непустих маршрути, які містять однаковий маршрутизатор P є консистентними, якщо $path_{N_1}(P, D) = path_{N_2}(P, D)$

Авторами методики доводиться наступна теорема:

Теорема 1. Якщо два маршрути є коректними, то вони є консистентними. Якщо маршрути (N1, D) і (N2, D) не є консистентні, і N2 міститься в (N1, D), то маршрут (N2, D) визнається недійсними. Недійсні шляхи заборонено вибирати в якості бажаних. На цій основі вводяться два правила:

1) якщо в останньому повідомленні N_{last} видаляє свій маршрут до префікса D (N_{last}, D), тоді визнати всі маршрути, в яких присутня N_{last} недійсними;
2) якщо в останньому повідомленні $N_{changed}$ оголошує новий маршрут до D, то:

   2.1) якщо $N_{change} \in path(N_i, D)$ та $path_{N_i} \neq path(N_{change}, D)$, тоді визнати маршрут (Ni, D) недійсним;

   2.2) якщо $N_i \in path(N_{change}, D)$та $path_{N_{change}}(N_i, D) \neq path(N_i, D)$, тоді визнати маршрут ($N_{change}$,$D$) недійсним.

Крім того розглядаються й відмінності моделі SPVP від реальної роботи протоколу BGP, адже це різні протоколи, що мають різну специфікацію:

- одна й та ж сама АС за допомогою декількох iBGP маршрутизаторів може оголошувати декілька маршрутів до одного й того ж самого префіксу з метою розподілу навантаження; пропонована модифікація описаних правил – розбиття однієї АС на кілька логічних АС для кожного префіксу, до якого відбувається адресація, та застосування правил окремо для декількох АС;
- в моделі протоколу SPVP порожній шлях вважається коректним, оскильки свідчить про фізичну недоступність цільового префіксу, а ось у BGP видалення маршруту може статися внаслідок зміни політики маршрутизації; пропонована модифікація правил – використовувати правила тільки для анулюючих повідомлень, пов'язаних з фізичною недоступності цільового префіксу;

- при обриві внутрішніх ліній зв'язку АС може бути розділена на кілька незалежних частин, які будуть обирати різні маршрути до цільового префіксу; пропонована модифікація – вважати видалення маршрутів внаслідок розбиття АС впливом політик маршрутизації і не застосовувати до них правила фільтрації.

Наступною розглянемо методику Forwarding edge numbers. Причина утворення transient loops, або перебору всіх доступних шляхів до цільового префіксу – анулюючі повідомлення, які надходять і містять недостатньо інформації для визначення точної причини недоступності того чи іншого шляху. Наведемо кілька прикладів для топології, зображеної на рис. 2.1.

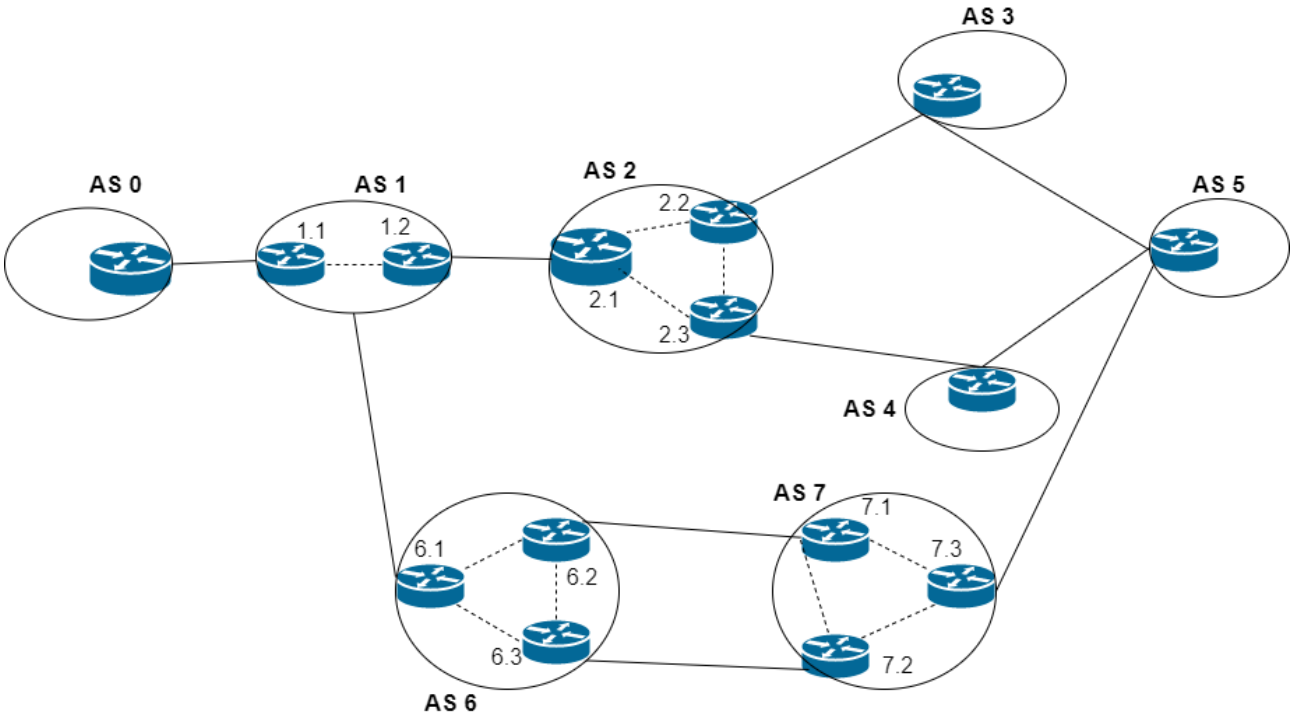

Рисунок 2.1 – Приклад топології при Forwarding edge numbers

При розриві зв'язку між AC0 і AC1 AC 5 для видалення маршрутів (3210), (4210) і (7610) треба буде отримати 3 відповідних повідомлення про видалення. При обриві каналу зв'язку між маршрутизаторами 6.1 і 6.2 маршрутизатор 6.2 згенерує анулююче повідомлення про видалення маршруту

(610) в напрямку AC7, що в кінцевому підсумку призведе до видалення маршруту (7610) з таблиці AC5.

З точки зору авторів методики необхідний механізм, що дозволяє розрізняти BGP повідомлення про оновлення та про анулювання маршруту, що відправляються різним сусідам BGP маршрутизатора. Пропонується використання так званих «лічильників напрямків» (forward edge sequence number). Для кожної AC X та сусідньої з нею AC Y зв'язується унікальний «головний лічильник напрямку». Для позначення використовується запис (X: Y, n). Значення головного лічильника напрямку змінюється для AC X при відновленні зв'язку між X і Y. Коли AC X оголошує маршрут для AC Y, вона додає до цього маршруту значення лічильника напрямку, який асоційований з X і Y. Таким чином, кожен маршрут, який передається в мережі маршрутизаторів має асоційований з ним список лічильників напрямку (у вигляді трійок значень (X: Y, n)). Якщо дві сусідні AC взаємодіють через кілька граничних маршрутизаторів, то з кожною сесією між двома граничними маршрутизаторами зв'язується «додатковий лічильник напрямку». Правила зміни додаткового лічильника збігаються з правилом зміни головного лічильника, але додатковий лічильник передається між граничними маршрутизаторами сусідніх AC та між внутрішніми маршрутизаторами. Розглянемо як формуються і обробляються BGP повідомлення про оновлення та анулювання маршруту при використанні такої методики.

При генерації спеціального повідомлення про видалення маршруту до повідомлення прикріплюється асоційований з ним список головних лічильників напрямку, а також при необхідності – список додаткових лічильників. Одержувач повідомлення формує на його основі своє повідомлення про оновлення (чи видалення маршруту) і прикріплює до нього в незміненому вигляді вихідне повідомлення. Таким чином кожен маршрутизатор при отриманні нового такого повідомлення володіє більш повною інформацією про вихідне місце та причини появи цього повідомлення. Розглянемо описані раніше приклади:

- при розриві лінії зв'язку між АС 0 та АС 1 буде згенеровано анулююче повідомлення, яке буде містити трійку (0: 1, n), де n – відповідний лічильник напрямку; АС 5 при отриманні першої ж копії цього повідомлення перевірить, які маршрути в його базі даних залежать від цього лічильника напрямків та видалить відразу три недійсних маршрути (3210), (4210), (7610);
- при обриві лінії зв'язку між 6.2 та 7.1 – в цьому випадку маршрут не буде видалений оскільки в таблицях маршрутів АС6 та АС7 міститься два маршрути (7610) з однаковим списком головних лічильників напрямків, але з відмінними списками додаткових лічильників напрямків.

У Differentiated BGP Update Processing всі передані BGP повідомлення про оновлення та анулювання маршрутів можна класифікувати за ступенем важливості для одержувача інформації, що передається в повідомленні інформації. Наприклад, якщо передане анулююче повідомлення видаляє вторинний маршрут, то пріоритет його доставки нижче, ніж у анулюючого повідомлення, що видаляє поточний найкращий маршрут.

Пропонується використовувати два різних MRAI таймера для класів високопріоритетних та фонових BGP повідомлень. BGP повідомлення про оновлення та/чи видалення будь-якого маршруту класифікуються з точки зору одержувача повідомлення, при цьому для класифікації вводиться поняття «префіксне дерево маршруту» (per-prefix forwarding path tree).

Префіксне дерево маршруту будується для кожного префіксу. Коренем дерева є сам префікс, а його безпосередні сусіди є вузлами дерева першого рівня. У загальному випадку після завершення процесу збіжності пакети даних, що йдуть до цільового префіксу подорожують по дереву від листя до кореня. На підставі введеного визначення автори методики будують наступну класифікацію (рис.2.2).

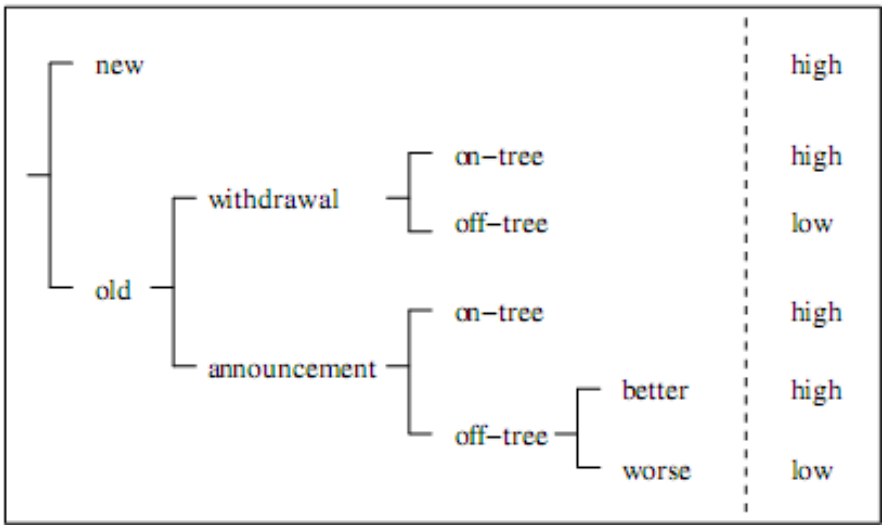

Рисунок 2.1 – Класифікація префіксного дереву маршруту

Основна проблема – класифікація BGP повідомлень будується з точки зору одержувача, а пріоритетизація повідомлень повинна проводитися відправником. Автори методики пропонують наступну схему – для всіх повідомлень про видалення маршруту обчислення пріоритетів не проводиться, для кожного Update повідомлення про префікс X, перевіряється, чи є в таблиці відправника запис про маршрут до даного префіксу від передбачуваного одержувача. Якщо запис в таблиці маршрутів присутній, то Update повідомлення вважається низькопріоритетним (off-tree), інакше – високопріоритетним (new або on-tree).

В такому випадку пропонується два способи налаштування MRAI таймерів:

- для високопріоритетних повідомлень значення таймера дорівнює стандартному, для низькопріоритетних повідомлень значення таймера більше стандартного – даний спосіб зменшує кількість переданих повідомлень;
- для високопріоритетних повідомлень значення таймера менше стандартного, для низькопріоритетних повідомлень значення таймера дорівнює стандартному, що зменшує загальний час пошуку оптимального шляху в мережі маршрутизаторів.

Друга пропозиція авторів методики – альтернативний спосіб вибору нового пріоритетного маршруту після приходу повідомлення про видалення старого: новий обраний маршрут – це найкоротший маршрут з маршрутів, що максимально відрізняються від видаленого маршруту.

Даний алгоритм вибору нового маршруту запобігає поширенню недійсних маршрутів, що мають більш короткий атрибут AS_PATH, ніж зберігається в мережі дійсних маршрутів. Реалізація даної методики досягається за рахунок введення для кожного маршруту в таблиці BGP маршрутизатора його стану. При отриманні нового маршруту йому присвоюється «стабільний» стан. При видаленні маршруту або при його заміні на менш бажаний маршрут, його стан змінюється на «нестабільний». При цьому для маршруту, що знаходиться в стані «нестабільний», застосовується особлива процедура вибору найкращого маршруту. З кожним маршрутом пов'язаний свій таймер, який запускається при зміні стану маршруту на «нестабільний». Після закінчення таймера стан маршруту змінюється на «стабільний». При видаленні або зміні на менш бажаний маршрут вже нестабільного маршруту асоційований з ним таймер перезапускається.

В дослідженні [25] було показано, що для кожної топології BGP маршрутизаторів існує оптимальне значення MRAI таймера, при якому досягається мінімальний час збіжності протоколу BGP в даній топології для випадку видалення маршруту до одиночного префіксу. При цьому дане оптимальне значення залежить від різних характеристик топології.

Автори ідеї про динамічно змінний MRAI таймер висловили припущення, що поточне значення MRAI таймера за замовчуванням в 30 секунд є занадто завищеними. При цьому було висловлено припущення, що оптимальне значення MRAI таймера залежить від кількості сусідів маршрутизатора, чим більше сусідів у маршрутизатора – тим більше повинно бути значення MRAI таймера. Автори методики провели ряд експериментів зі значеннями MRAI таймера в 0.5, 1.25 і 2.25 секунд, розглянувши при цьому випадки масових вилучень маршрутів до різних префіксів (рис. 2.3).

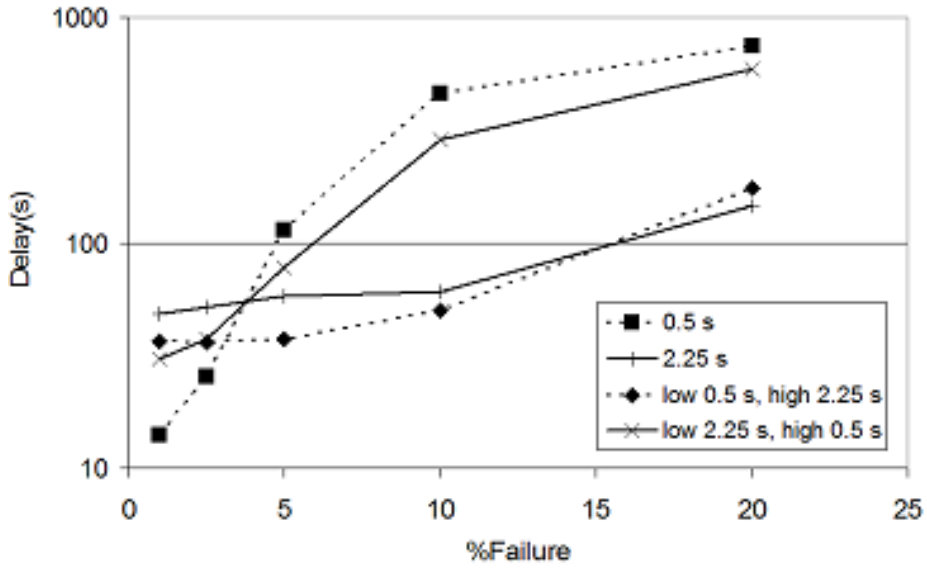

Рисунок 2.3 – Залежність затримок від кількості вилучених маршрутів при різних значення MRAI таймеру

З результатів експериментів були зроблені висновки, що при малому масштабі вилучень префіксів оптимальним є найменше значення MRAI таймера, а для великих масштабів – оптимальна схема з різним значенням MRAI таймера для різної кількості сусідів маршрутизатора.

Для застосування отриманих результатів на практиці була запропонована схема динамічного зміни значення MRAI таймера. Розрізняють три рівні значень MRAI таймера (наприклад, 0.5, 1.25. 2.25 секунд), значення таймера змінюється в залежності від довжини черги вхідних повідомлень про оновлення/видалення маршруту. Результати роботи такої схеми наведені на рис.2.4

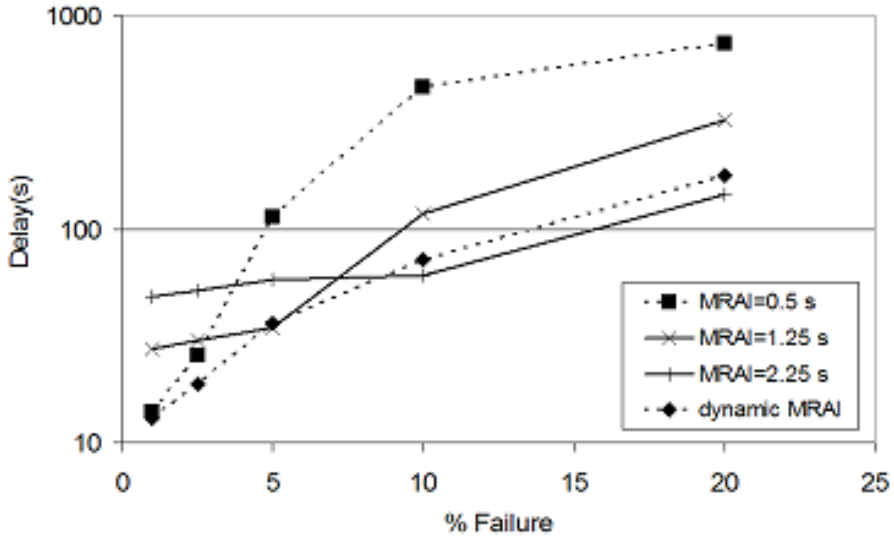

Рисунок 2.4 – Залежність затримок від кількості вилучених маршрутів при використанні динамічно змінного MRAI таймеру

І остання методика – перестановка Update повідомлень в черзі. Нехай в черзі з 4 BGP повідомлень на маршрутизаторі повідомлення 1 та 3 послідовно оновлюють маршрут до префікса X, а повідомлення 2 та 4 оновлюють маршрут до префікса Y. Уявімо ситуацію, в якій MRAI таймер закінчується після обробки повідомлення 2, але до завершення обробки повідомлення 3. В такому випадку після повторного закінчення таймера маршрутизатор в цілому відправить не менше 4 Update повідомлень – по два повідомлення для кожного префікса X та Y. Якщо б повідомлення були розташовані по іншому (повідомлення щодо префікса X – 1 і 2), то тоді було б відправлено тільки 2 Update повідомлення.

Запропонована авторами методика полягає в наступному: для кожного вхідного повідомлення про оновлення або ж видалення маршруту кешується в спеціальну чергу цільової префікс цього повідомлення. Для кожного префікса обробляються відразу всі повідомлення в черзі. Результати застосування даної методики представлені на рис. 2.5.

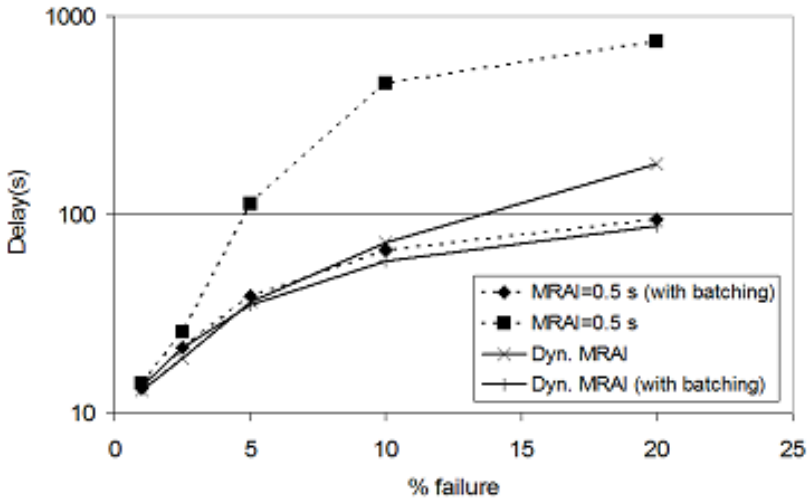

Рисунок 2.5 – Залежність затримок від кількості вилучених маршрутів при перестановок повідомлень у черзі

Розглянувши усі сім методик можна підвести підсумок за декількома критеріями, що представлено у порівняльній таблиці 2.1.

Таблиця 2.1 – Порівняльна таблиця методик оптимізації ефективного шляху

Назва методики	Зміни в протоколі маршрутизації	Ускладнення логіки протоколу	Теоретичні результати	Враху-вання iBGP	Результати експериментів
1	2	3	4	5	6
SSLD	процедура відправлення повідомлень про оновлення та видалення маршрутів; процедура прийняття BGP рішення	незначне	немає	не важливо	незначне зменшення часу пошуку оптимального шляху; для ряду топологій зменшення кількості переданих повідомлень аж до 50%.

Продовження таблиці 2.1

1	2	3	4	5	6
Ghost Flushing	процедура обробки вхідних повідомлень; процедура прийняття BGP рішення, процедура відправки BGP повідомлень;	незначне	доведені теоретичні оцінки часу пошуку оптималь-ного шляху і кількості переданих повідомлень	ні	значне зменшення часу пошуку оптимального шляху
Consistency Assertions	формат BGP Update повідомлень, процедура прийняття BGP рішень,	значне за рахунок того, що приділяєть ся дуже велика увага деталям	немає, через занадто детальний розгляд протоколу	так	значне зменшення часу пошуку оптимального шляху, середнє зменшення кількості переданих Update повідомлень
Forwarding edge numbers	формат BGP повідомлень про оновлення та видалення, процедура прийняття BGP рішення, отримання / відправлення BGP повідомлень	значне	є	так	значне зменшення часу пошуку оптимального шляху та кількості переданих повідомлень

Продовження таблиці 2.1

1	2	3	4	5	6
Differentia-ted BGP Update Processing	процедура прийняття BGP рішення, процедура відправки / отримання BGP повідомлень	при реалізації усіх пропозицій – досить значне	немає	ні	значне зменшення часу пошуку оптимального шляху і кількості переданих повідомлень
Динамічно змінний MRAI таймер	процедура відправлення / отримання BGP повідомлень	незначне	немає	не важливо	значне зменшення часу пошуку оптимального шляху
Переста-новка BGP повідом-лень у черзі	процедура отримання BGP повідомлень	незначне	немає	не важливо	значне зменшення часу пошуку оптимального шляху

Всі раніше згадані методики намагалися вирішити проблему, використовуючи один із наступних підходів:

a. Змінення існуючого протоколу BGP, що в свою чергу призводить до збільшення накладних витрат на протокол, що впливає на продуктивність, і крім того його практично неможливо реалізувати через неможливість змінити діюче середовище Інтернету.
b. Використання програмно-конфігурованої мережі SDN (Software Defined Network), проте використання SDN потребує, щоб усі маршрутизатори та комутатори через Інтернет підтримували технологію SDN, що не може бути реалізовано у реальному середовищі мережі Інтернет. Крім того, маршрутизатори та

комутатори в трафіку повинні знаходитися під управлінням одного адміністратора, щоб отримувати зміни потоку трафіку від того ж контролера SDN.

Відповідно, розроблений спосіб базується на контролері, який розроблений таким чином, що ключовою особливістю запропонованого механізму є те, що він може бути реалізований в реальному часі для вирішення проблеми підвищення ефективності вибору маршруту та перерозподілу трафіку без внесення будь-яких змін як до протоколу BGP, так і без втручання у вже запущені та функціонуючі Інтернет-інфраструктури.

2.2 Модифікована імітаційна модель протоколу BGP

Такий глибокий аналіз потрібен не лише для того, щоб розібрати помилки попередніх розробок, а й для того, щоб визначити особливості та вимоги до не менш важливого за розробку самого способу оптимізації елементу – імітаційної моделі.

Зазвичай імітаційна модель будується не з нуля. Існують готові імітаційні моделі основних елементів мереж: найбільш поширених типів маршрутизаторів, каналів зв'язку, методів доступу, протоколів, тощо. Ці моделі окремих елементів мережі створюються на підставі різних даних: результатів тестових випробувань реальних пристроїв, аналізу принципів їх роботи, аналітичних співвідношень. В результаті створюється бібліотека типових елементів мережі, які можна налаштовувати за допомогою заздалегідь передбачених в моделях параметрів.

Системи імітаційного моделювання зазвичай включають також набір засобів для підготовки початкових даних про досліджувану мережі - попередньої обробки даних про топологію мережі та виміряному трафіку. Ці засоби можуть бути корисні, якщо мережа, що моделюється, являє собою

варіант існуючої мережі і є можливість провести в ній вимірювання трафіку та інших параметрів, потрібних для моделювання. Крім того, система забезпечується засобами для статистичної обробки отриманих результатів моделювання.

В окремій публікації [34] вже описувалася модифікована імітаційна модель зовнішньої групової маршрутизації, тому тут наведемо стислий виклад інформації.

Звісно існує декілька майже універсальних варіантів у вільному доступі, однак жоден з них не підійшов за усім переліком критеріїв для тестування розробленого способу.

Функціональними вимогами до розробленої модифікованої імітаційної моделі є:

- повнота моделювання політик, а також алгоритмів прийняття рішень;
- моделювання чотирьох видів BGP повідомлень (глибоке відтворення механізмів Update повідомлень);
- відтворення механізмів з'єднання, роз'єднання та розриву зв'язку;
- масштабування мережі;
- відтворення архітектури iBGP;
- наявність прогнозування роботи таймеру MRAI та його затримок;
- режим сценарних подій [34].

Усе разом це має суттєвий вплив на те, які методики можна протестувати за допомогою імітаційної моделі. Оскільки для розробленого способу використовувалися як база сім інших методик і з ними ж він порівнюється, то модифікована імітаційна модель повинна однаково гарно працювати для кожного з варіантів.

Як вже в попередньому розділі було згадано, Update повідомлення відіграють не останню роль у роботі протоколу при пошуку оптимального шляху маршрутизації. Якраз ці повідомлення несуть відповідальність за

передачу інформації між сусідніми станціями про доступні чи видалені маршрути.

В одному з наукових досліджень [35] навіть була доведена залежність потенційного обсягу масштабування мережі в імітаційних моделях від детальності моделювання атрибутів саме Update-повідомлень та від формату їх передачі. Тому для того, щоб добитися більшого рівня масштабування всередині розробленої модифікованої імітаційної моделі передача повідомлень організована у вигляді об'єктів.

Встановлення з'єднання, як і його розрив (чи примусове роз'єднання) є ключовою частиною в передачі інформації, в тому числі і про маршрути її передачі. Якщо не промоделювати якийсь з цих процесів, то може вийти ситуація, коли з'єднання розірвано, але передавач про це не знає та продовжує передавати інформацію. Більш того, без реалізації механізмів з'єднання-роз'єднання користувач імітаційної моделі не зможе досить чітко протестувати ситуації з видаленням маршрутів. Для цього його прийдеться або вручну видаляти маршрутизатори не зупиняючи модель, що може призвести до краху системи чи витоку маршрутів, що є достатньо серйозними наслідками, або ж для кожної зміни конфігурації потрібно буде призупиняти систему, щоб вносити до неї виправлення, що теж не є оптимістичним варіантом.

Іншим критерієм масштабування є наявність декількох маршрутизаторів всередині однієї АС. Це звичайна ситуація, яку, однак, творці імітаційних моделей часто оминають. Такий простий варіант неможливий для розробленої імітаційної моделі як мінімум через наявність Consistency Assertions у розглянутих методиках. Та і без неї цей пункт є дуже важливим, хоч і не найпопулярнішим серед розробників.

Більш повна варіативність представлення топології мережі в межах модифікованої імітаційної моделі організована за рахунок відхилення від розповсюдженої тенденції представлення АС одним єдиним об'єктом. В

розробленому варіанті реалізації кожен наявний в мережі маршрутизатор представляє собою окремий об’єкт [34].

Додатково були розроблені та введені в модифіковану імітаційну модель різні механізми передачі даних для випадків «зовнішнього» (external) зв’язку між маршрутизаторами, коли з’єднуються об’єкти з різних АС, та «внутрішнього» (internal), коли з’єднання йде між маршрутизаторами всередині однієї АС.

Моделювання роботи таймеру MRAI та затримок, що викликані ним, стало обов’язковим пунктом через Update повідомлення. Доведено, що робота таймеру мінімального інтервалу оголошення маршрутів має високий вплив на кількість повідомлень про оновлення маршруту, що мають генеруватися. А це в свою чергу має вплив на часовий критерій визначення оптимального шляху маршрутизації та кількість службової і повної інформації, що передається.

В інтересах подальшого порівняльного аналізу існуючих методик та розробленого способу та щоб полегшити задачу тестування в однакових умовах, в розробленій модифікованій імітаційній моделі є можливість роботи в режимі сценарних подій. Це означає, що є можливість зберегти до чотирьох варіантів сценаріїв (кількість маршрутизаторів, їх зв’язки, навантаження на мережу, налаштування MRAI і тому подібне) для дослідження поведінки моделі при однакових подіях. Це дозволяє не тільки промоделювати однакові умови для різних методик, а також і зібрати статистичні дані при багаторазовому повторному запуску одного й того самого сценарію.

Для оцінки ефективності роботи способів пошуку ефективного шляху маршрутизації в запропонованій модифікованій імітаційній моделі був обраний часовий критерій. Користувач при тестуванні може на свій розсуд обрати один з двох режимів:

1) вимірювання часу власне визначення оптимального шляху з конкретної початкової точки до іншої конкретної кінцевої;

2) вимірювання кінцевого часу пошуку всіх найкращих шляхів, від кожного модуля до кожного, всередині заданої топології мережі [34].

Розроблена модифікована імітаційна модель складається з таких частин:

- модуль передачі BGP-повідомлень;
- модуль BGP рішень;
- модуль збору даних.

В свою чергу до задач модуля передачі BGP-повідомлень входить:

- конфігурація модуля BGP рішень;
- моделювання передачі BGP-повідомлень між BGP маршрутизаторами;
- моделювання подій видалення та оголошення маршрутів;
- моделювання затримок при передачі Update-повідомлень між BGP маршрутизаторами.

Головними функціями модуля BGP рішень є:

- моделювання процесу вибору маршруту;
- моделювання політик маршрутизації;
- агрегація BGP повідомлень.

Модуль збору даних відповідальний за:

- збір даних з внутрішніх таймерів;
- збір інформації про маршрутизацію;
- надання статистики трафіку, в тому числі провідна пропускна здатність користувачів або який відсоток трафіку вони використовують;
- виведення даних в окремий файл.

На рис. 2.6 приведена загальна схема роботи описаної модифікованої імітаційної моделі.

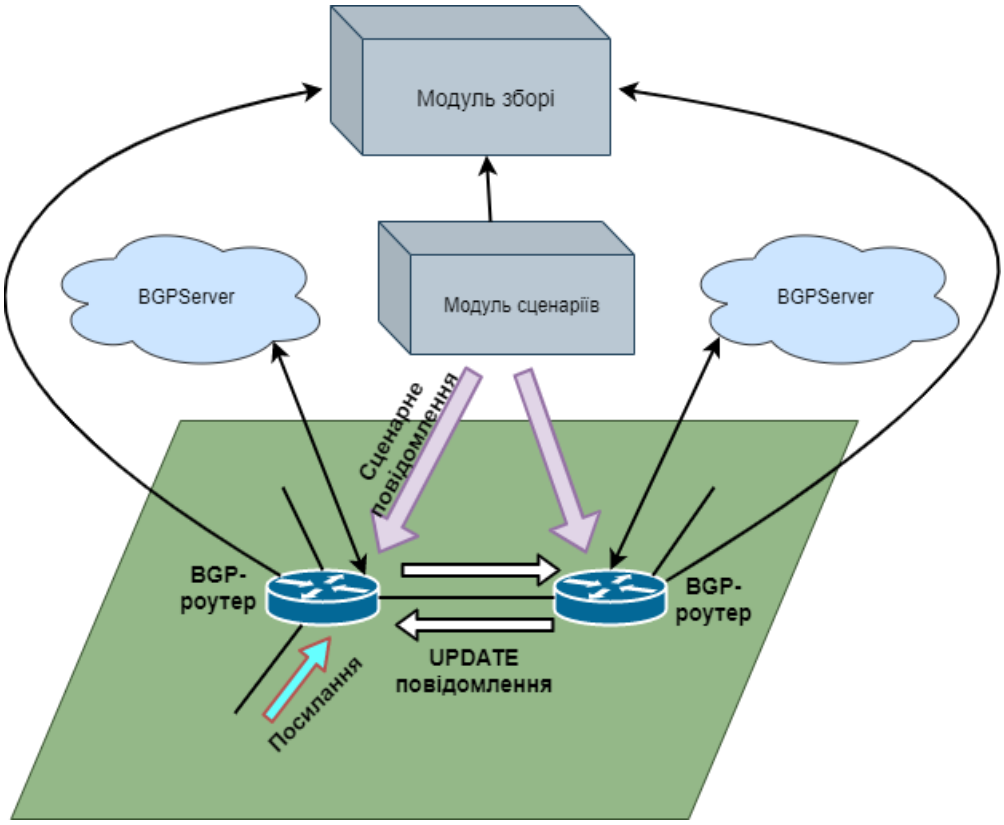

Рисунок 2.6 – Загальна схема роботи модифікованої імітаційної моделі

Висновки до розділу 2

В розділі проведено аналіз та опис основних сімох методик оптимізації ефективного шляху при груповій маршрутизації – SSLD, Ghost Flushing, Consistency assertions, Forwarding edge numbers, Differentiated BGP Update Processing, динамічно змінний MRAI таймер та перестановка Update повідомлень в черзі. Проаналізовано їх основні ідеї, проведено теоретичні та експериментальні дослідження, результати яких представлені в порівняльній таблиці.

Базуючись на описаному розборі існуючих методів виділено два основні підходи для вирішення проблеми підвищення ефективності пошуку шляху при груповій маршрутизації. Описані та проаналізовані їх головні недоліки та обґрунтовано напрям їх вирішення в запропонованому способі за допомогою програмного контролера, який буде функціонувати в реальному часі без критичного втручання в сам протокол маршрутизації BGP та інфраструктуру мережі.

Крім того, обґрунтована необхідність розробки власної імітаційної моделі. Обґрунтовані основні функціональні вимоги, що пред’являються до її модифікації. Описані ключові відмінності від існуючих аналогів та причини внесення конкретних змін у порівнянні з аналогічними варіантами імітаційних моделей.

3 ПРОГРАМНИЙ КОНТРОЛЕР ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИБОРУ ШЛЯХУ

В первинному вигляді мережі Інтернет існував лише один шлях між двома АС і її структура мала дещо ієрархічний вигляд. З часом структура стає більш плоскою, що призводить до появи більшої кількості шляхів між кожною парою АС. Однак протокол BGP, як домінуючий міжмережний протокол, не може скористатися наявністю безлічі шляхів для збільшення пропускної спроможності мережі в цілому. Натомість сьогодні BGP-маршрутизатори використовують лише єдиний за замовчуванням шлях, який при перевантаженості призводить до зниження продуктивності, не реагуючи на «затори» та бурхливий трафік. Надмірне використання або перевантаженість певного шляху, впливає на пропускну спроможність як цього каналу, так і мережі в цілому. У такому випадку інтернет-додатки зазнають великої затримки, що в свою чергу має вплив на якість обслуговування або може призвести до збою сеансу між джерелом та пунктом призначення.

У звичайній роботі протоколу BGP, лише після завершення обчислення найкращого шляху, можна виміряти та посилити такі параметри роботи мережі, як затримка, пропускна спроможність, втрата пакету та інші. Відсутність більш широкого сповіщення про ефективність роботи в мережі Інтернет та труднощі для впровадження проактивних вимірювань віднесли Інтернет до класу мереж, важких для впровадження таких факторів продуктивності, як використання каналів зв'язку та затримка у прийнятті рішень про маршрутизацію.

Найбільш вживаний метод виправлення таких недоліків – множинна адресація, що використовує одночасно декілька посилань на мережу Інтернет від різних постачальників послуг мережі Інтернет. Задля взяття під контроль надмірності посилань, протокол маршрутизації BGP використовується для розподілу трафіку по цих кількох посиланнях, але не автоматично. Остання

версія протоколу BGP не має прямої реалізації, яка підтримує будь-яку якість обслуговування QoS (Quality of Service), і вона не може задовольнити угоду про рівень обслуговування, що важливо для користувачів. Більшість пристроїв переадресації трафіку IP мають власне програмне забезпечення для площини управління з вузьким уявленням про можливості глобального шляху до IP-мережі призначення та відсутністю інформації про обрані найкращі характеристики якості обслуговування (QoS).

Тому запропоновано програмний контролер, як ефективне рішення цієї проблеми, яке дозволяє при цьому уникнути проблем методик, що були розглянуті в попередньому розділі. Для більш точної конкретизації задачі запропонованого контролера до нього були сформульовані та пред’явлені пред’явлені такі вимоги:

- доступність мережі та послуг має бути на 100% в режимі роботи;
- додержання затримки в межах допустимого діапазону;
- зберігання використання посилань нижче заздалегідь визначених рівнів фіксації;
- забезпечення ефективного/правильного використання наявних Інтернет-ресурсів.

3.1 Принцип роботи програмного контролера

Програмний контролер був розроблений та впроваджений для підвищення параметрів роботи мережі наступним чином:

- впровадження розробленого контролеру для управління протоколу BGP на основі параметрів продуктивності мережі, таких як використання зв'язку та затримка без будь-яких змін самого протоколу або працюючого Інтернет-середовища;

- перерозподіл трафіку на основі використання посилань на доступні багатоходові посилання для перевантажених посилань, що пропонує оптимальне управління пропускною спроможністю для підвищення продуктивності мережі та досягнення необхідної Угоди про рівень обслуговування SLA (Service Level Agreement);
- зменшення затримки передачі від одного крайнього маршрутизатора до іншого для програм, залежних від часу, через переключення програми на інше багатоходове посилання з доступною пропускною спроможністю;
- оброблення оновлення маршруту протоколу BGP автоматично та динамічно на основі показників продуктивності мережі та необхідних витрат.

Запропонований спосіб управління та підвищення ефективності пошуку шляху при груповій маршрутизації в мережі Інтернет через протокол BGP використовує програмний контролер, який був розроблений та введений у багатоходову мережу з протоколом BGP, для організації примусового перерозподілу трафіку за наявними посиланнями на основі використання зв'язку, затримки або будь-яких інших параметрів роботи мережі, які можуть бути виміряні, наприклад, кількість втрачених пакетів.

В даному випадку дослідження було зосереджене на використанні посилань, оскільки перевантаженість зв’язку призводить до втрати пакету та високого рівня затримок. Втрати пакетів також можуть бути наслідком несправних пристроїв або кабелів, а це вже не може бути вирішено програмним методом.

Запропонований програмний контролер може використовуватися для автоматичного примушування політик протоколу BGP на підприємстві або маршрутизаторах провайдера реорганізуватися для того, щоб обробляти трафік на основі використання посилання, і ця дія буде здійснена, якщо використання посилання досягне завчасно заданого значення.

Запропонований спосіб був розроблений на основі концепції програмно визначеної мережі SDN, в якій існує контролер, що керує мережевими комутаторами і контролює рух потоків через ці комутатори за допомогою відкритого протоколу слідування.

Використання SDN було описано, як одна з двох основних методик вирішення проблеми підвищення ефективності пошуку маршруту, в другому розділі. Однак, запропонований спосіб не йде по шляху, що був запропонований в описаних в тому розділі методів і використовує лише ідею, що лягла в основу функціонування мереж SDN, а не самі мережі даного типу.

Для нормального функціонування мережі SDN необхідно, щоб усі маршрутизатори та комутатори підтримували SDN та знаходилися під однаковим адмініструванням, тоді як використаний програмний контролер реалізований без будь-яких змін в системі міждоменних маршрутизацій, та лише коригує атрибути протоколу BGP для зміни маршрутів трафіку, і відповідно використання каналів зв'язку теж змінено.

Тобто програмний контролер вбудований у мережу групової маршрутизації й просто збирає показники продуктивності цієї мережі з різних інструментів, щоб надіслати нову політику маршрутизації через сеанси інших протоколів інтерфейсу через мережу на маршрутизатор, не запускаючи сам протокол BGP. І відповідно ніякий трафік не буде прийнятий або направлений цьому маршрутизатору, уникаючи будь-якого погіршення продуктивності та не створюючи ніяких накладних витрат на мережу чи загроз безпеці у разі впровадження контролеру. Та, у винятковому випадку, коли з роботою програмного контролера щось піде не так, протокол BGP повернеться до свого нормального функціонування. Що дозволяє, теоретично, пропустити етап тестування на імітаційній моделі, як засобі захисту мережі та її користувачів від помилок в роботі протоколу BGP. В такому випадку за імітаційною моделлю закріплюється роль засобу тестування та порівняння параметрів в безпечних та однакових штучних умовах.

Запропонований програмний контролер був розроблений з використанням різних програмних пакетів, а також використовує декілька програмних пакетів для розгортання маршрутизаторів, контролю за використанням трафіку, розрахунком використання трафіку і, звісно, примусового впливу на політику маршрутизатора.

Для розробки використовувалась мова програмування Python, як набір реалізацій протоколу клієнт-сервер, що працює в інтеграції з мовою C та містить сторонні інструменти та бібліотеки, які ідеально підходять для прототипування та розгортання мережевих додатків. Інтерпретація часу виконання Python різко скорочує інтервал від модифікації до виконання, що є значною перевагою, коли більшість змін є поступовими, а більшість проблем виникає під час виконання, як у нашому випадку. Чистий синтаксис цієї мови програмування, динамічне введення тексту, інтегрована обробка винятків та об'єктні засоби зробили його широко використовуваною інтерпретованою мовою [10].

3.2 Опис основних компонентів програмного контролера

На рис. 3.1 показано, що для функціонування запропонованого способу підвищення ефективності пошуку шляху при груповій мережі, потрібно лише два елементи – мережа Інтернет і розроблений програмний контролер.

Для повноти випробувань використовувалась змодельована мережа, яка була розділена на три секції: підприємство, Інтернет-провайдери та Інтернет-користувачі, як показано на рис. 3.1 в виділеній прямокутній області.

Секція підприємства представляє сервісну частину, де він пропонує різні послуги мережі Інтернет для користувачів. Підприємство використовує три BGP-мультихомедіальні канали з пропускною здатністю 10 Мбіт/с, щоб підтримувати надійність сервісу, доступність і поза курсом SLA.

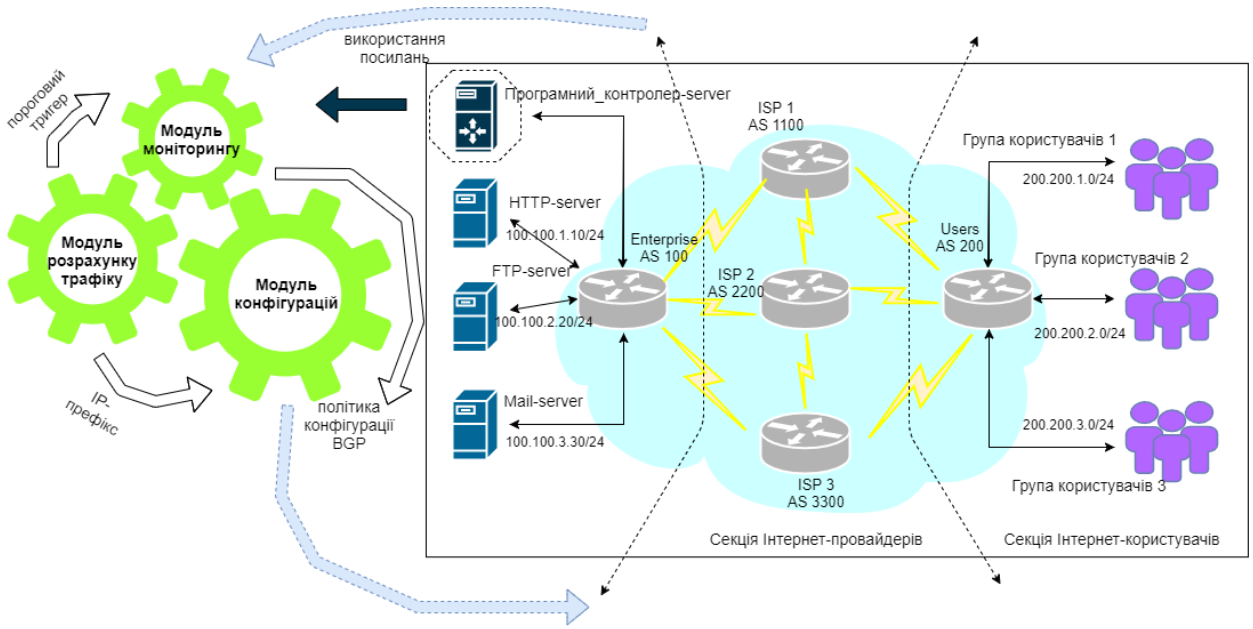

Рисунок 3.1 – Компоненти програмного контролера

Секція Інтернет-провайдерів представляє провайдерів 1-го або 2-го рівня, де Інтернет-трафік проходить через їх мережі від Інтернет-користувачів до підприємства та навпаки.

Секція Інтернет-користувачів представляє постачальника послуг рівня 3, який пропонує доступ до мережі Інтернет для користувачів, щоб вони мали змогу задовольняти потребу в використанні мережі Інтернет для власних цілей.

IP-префікси призначені для кожної секції і відповідно конфігурація протоколу BGP застосовується до кожного маршрутизатора в мережі, щоб зробити можливим доступ потоку трафіку з секції Інтернет-користувачів мати доступ до служб у секції підприємства.

Інтернет-мережа представляє послуги, користувачів, трафік та маршрутизатори. Маршрутизатори BGP – це найважливіша частина і для тестувань використовувалися мережеве обладнання виробництва TP-Link та Cisco.

Інтернет-сервіси, такі як HTTP та FTP, були представлені машиною CentOS Linux із включеними відповідними послугами та налаштовані на прослуховування та відповідь на запити користувачів мережі Інтернет [22].

Користувачі мережі Інтернет та Інтернет-провайдери були представлені такими самими машинами, що використовувалися для генерування трафіку по мережі та з налаштованою роботою демона Quagga з налаштованим пакетом для моніторингу посилань, щоб миттєво отримати кожну статистику використання посилань та створити базу даних про використання зв’язків.

Ця мережева модель представляє сценарій мережі в режимі реального часу із з'єднаннями між користувачами, підприємствами та провайдерами.

Сам програмний контролер складається з трьох модулів:

- модуль моніторингу зв’язку;
- модуль розрахунку трафіку;
- модуль конфігурації.

3.2.1 Модуль моніторингу зв’язку

Як зрозуміло з назви, цей модуль зосереджений на моніторингу зв’язку між маршрутизаторами, оцінці перевантаженості посилань та є тригером для роботи основного механізму програмного контролера.

Даний модуль функціонує наступним чином.

1. Він контролює використання кожного посилання, періодично перевіряючи журнал моніторингу посилань на машинах Інтернет-провайдера.
2. Спеціально налаштований пакет інструментів на машинах провайдера опитує кожен інтерфейс маршрутизатора, використовуючи протокол управління мережевими пристроями для отримання статистики використання та відповідно оновлює кожен файл журналу посилань кожні 5 хвилин.

3. Кожен запис у файлі журналу має часову відмітку, і модуль моніторингу відслідковує оновлення файлів журналу, щоб перевірити, чи досягнуто завчасно задане порогове значення.
4. Коли порогове значення буде досягнуто, модуль продовжить перевірку журналу і ще 5 разів поспіль підтверджує, що порогове значення було досягнуто і використання посилання постійно перевищує поріг.
5. Раніше згадані багаторазові перевірки дії на використання посилань застосовуються для уникнення нестабільності мережі, коли збільшення використання може бути миттєвим, а потім знову повертається до свого нормального рівня, і відповідно не потребує перерозподілу трафіку.
6. Модуль розрахунку трафіку програмного контролера ініціюється на підставі підтвердження того, що використання каналу зв'язку перевищило порогове значення, як показано на попередньому кроці.
7. Значення порогу для кожної ланки визначатиметься на основі послуг, пропонованих за цим посиланням, та необхідного рівня SLA.

3.2.2 Модуль розрахунку трафіку

Після підтвердження від модулю моніторингу зв’язку про перевищення лімітного значення використання якогось каналу зв’язку в справу включається модуль розрахунку (обчислення) трафіку.

Свою назву отримав через те, що працює з інформацією про трафік IP, оброблює, аналізує та сортує її. В ідеальному випадку робота програмного контролера в мережі з частково перевантаженими каналами закінчується на цьому модулі, але якщо всі доступні канали перевантажені, то модуль

розрахунку трафіку стає підготовчим етапом перед впровадженням в роботу третього і останнього модуля.

Модуль розрахунку трафіка працює за наступними етапами.

1. Він спрацьовує лише в тих випадках, коли буде досягнуто попередньо визначений поріг.
2. Для цього модуля ми отримуємо статистику трафіку на основі звітів щодо експорту інформації від протоколу, призначеному для збору інформації про трафік IP (NetFlow або IPFIX).
3. Модуль розрахунку трафіку проаналізує звіт протоколу з попереднього кроку та сформує таблицю використання префіксних пар у порядку зменшення від найвищого префікса використання до найнижчого.
4. Після визначення префіксних пар вибору, відповідна пара буде обрана для перенаправлення трафіку через інше посилання на основі наявної пропускної спроможності за іншими посиланнями.
5. Нарешті, якщо немає пропускної здатності, він надсилає сигнал адміністратору мережі, інакше модуль конфігурації протоколу BGP буде ініційований.

3.2.3 Модуль конфігурації

Даний модуль є останньою спробою підвищення ефективності пошуку шляху. Він дуже тісно пов’язаний з роботою самого протоколу BGP та впливає на конфігурації, що обираються в протоколі для майбутньої маршрутизації.

Його роботу неможливо описати без повторного опису порядку маршрутизації в протоколі BGP, тому наступний порядок роботи відображає

не лише роботу модуля програмного контролера, а й перелік дій протоколу маршрутизації.

a. Протокол BGP базує свої рішення щодо маршрутизації на основі атрибутів.
b. Політика протоколу BGP може бути застосована для управління як вхідним, так і вихідним трафіком, і відповідно механізм управління програмного контролера може бути розгорнутий в обох сценаріях.
c. Атрибут протоколу BGP AS-Path зазвичай використовується для управління вхідним трафіком за допомогою техніки попереднього передбачення шляху між АС, а атрибут Local-Pref в свою чергу, використовується для управління вихідним трафіком.
d. Попередньо шлях маршрутизації створюється таким чином, щоб BGP-маршрутизатори формували якнайдовший шлях з номерів АС, а потім перевага віддається найкоротшим доступним шляхам до обраної АС.
e. Атрибут Local-Pref протоколу BGP використовується для вибору вихідного трафіку, де кращим вважається маршрут з найвищим значенням атрибуту.
f. Модуль конфігурації програмного контролера вибирає відповідну політику протоколу BGP, яка буде застосована для перестановки вибраного префікса через нове посилання шляхом коригування вищевказаних атрибутів протоколу BGP.
g. Перш ніж застосувати нову конфігурацію, перевіряється таймер перевищення часу затримки, щоб уникнути завеликої затримки за зменшення маршруту.
h. Затримка за зменшення маршруту використовується, щоб допомогти постачальникам послуг запобігти впливу проблем маршрутизатора або ланцюга одного клієнта на стабільність мережі провайдера шляхом виведення проблемних BGP-маршрутів.

і. Затримка зменшення маршруту може бути застосована за рахунок декількох оновлень маршрутизації, які викликані декількома змінами конфігурації або посилань, щоб в модулі конфігурації був застосований таймер затримки.

3.2.4 Узагальнений процес взаємодії між модулями

Процес роботи програмного контролера та внутрішньої взаємодії його модулів можна описати таким чином:

1) робота циклу модуля моніторингу, якщо поріг використання не досягнуто, перевірте журнал посилань;
2) ініціація модуля розрахунку трафіку;
3) отримання статистики від протоколу, призначеному для збору інформації про трафік IP для цільового посилання;
4) обчислення трафіку за кожним префіксом;
5) створення таблиці використання префіксально-пропускної спроможності;
6) обрання пари з найвищим префіксом використання та пропускної спроможності;
7) перевірка журналу посилань для інших посилань на наявність пропускної спроможності; якщо немає пропускної спроможності, тоді поверніться до 6 та виберіть другу найвищу пару пропускної спроможності префіксу та повторіть 7, якщо все одно немає доступної пропускної спроможності, тоді надіслати сигнал тривоги;
8) звернення до модуля конфігурації та видача нового маршруту;
9) перевірка таймеру затримки, якщо його значення незадовільне, тоді зачекайте та перевірте ще раз, в іншому випадку надіслати конфігурацію, скинути таймер та повернутися до 1.

Процес роботи програмного контролера показаний на рис. 3.2 у вигляді діаграми системних потоків для представлення згаданих раніше етапів, а також роботи трьох модулів.

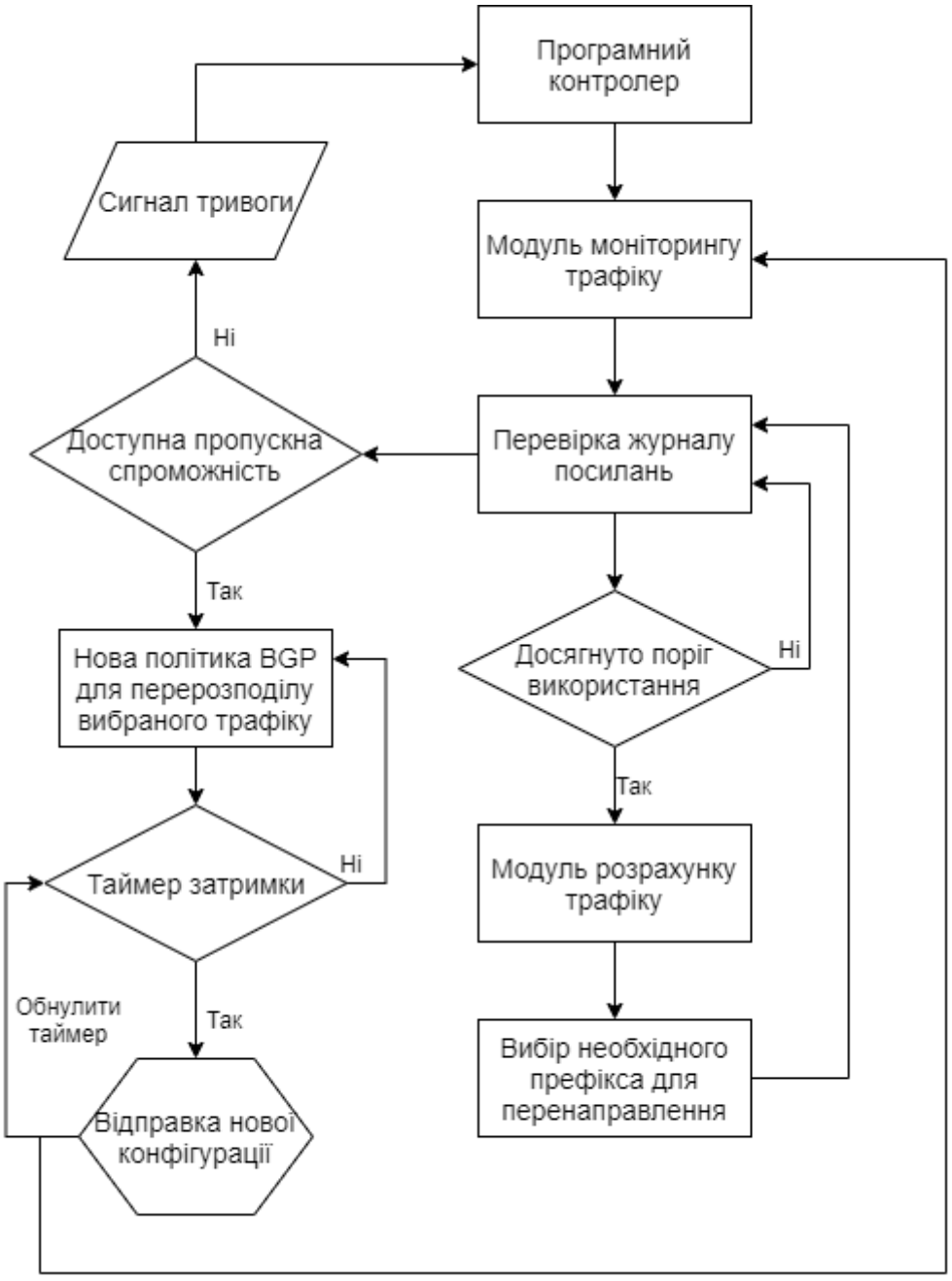

Рисунок 3.2 – Процес роботи механізму управління протоколом BGP через програмний контролер

3.3 Аналіз отриманих результатів тестування програмного контролера

Використання посилання має значний вплив на затримку та джітер параметрів роботи мережі, особливо коли посилання стає максимально використаним або ж навіть надмірно використаним.

У звичайній BGP-операції трафік може збільшуватися, поки посилання не перестане використовуватись. Це у випадку, якщо не буде зроблено жодних дій для перерозподілу трафіку в будь-якій іншій лінії зв'язку, що має доступну пропускну спроможність, і відповідно затримка та джітер будуть збільшені та вплинуть на пропоновані послуги.

У наступному експерименті продуктивність мережі буде вимірюватися з затримкою від початкового маршрутизатора до кінцевого та джітером понад 10 Мбіт/с, а моделювання виконано за допомогою модифікованої імітаційної моделі. Продуктивність порівнюється для різних навантажень трафіку з 50, 75, 100 та 120 відсотків пропускної спроможності каналу, щоб зосередити увагу на впливі надлишкового використання зв'язку на продуктивність мережі.

На рис. 3.3 видно, що для навантажень трафіку посилання 50% і 75% затримка коливається від 1 мс до 2 мс, а для 100% вона збільшується до приблизно 3,5 с, коли посилання використовується на максимальну пропускну спроможність, і, нарешті, коли зв'язок перевикористовується при навантаженні в 120% затримка значно зросла і досягає 22,5 с, що означає, що досягнуто неприйнятного рівня обслуговування, тобто не виконується SLA.

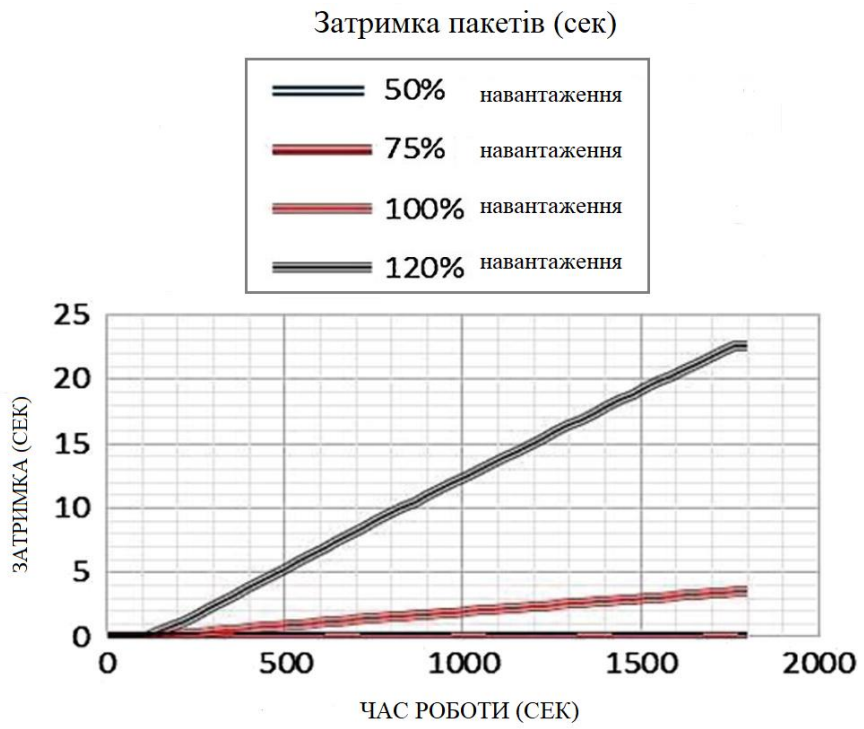

Рисунок 3.3 – Затримка пакетів від початкового маршрутизатора до кінцевого

На рис. 3.4 видно, що для навантажень у 50%, 75% та 100% джітер коливається приблизно від 0 до 3 мс, але при надмірному використанні зв'язку, тобто при навантаженні в 120% він досягає 246 мс.

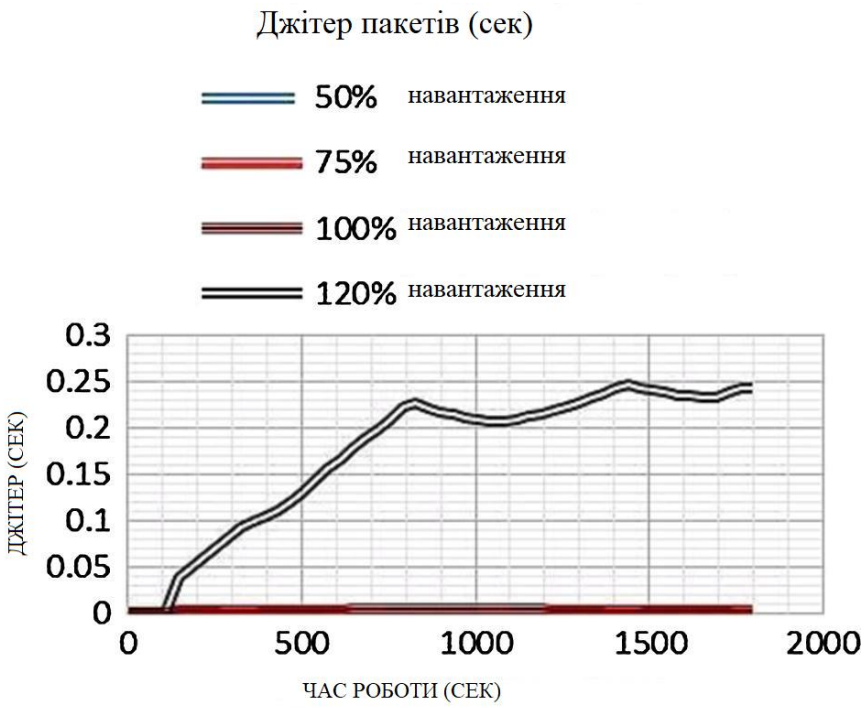

Рисунок 3.4 – Джітер пакетів

Як показано в даному експерименті, трафік в каналі зв'язку повинен утримуватися в межах пропускної спроможності каналу і зв'язок не повинен бути використаний надмірно. Саме для даних цілей програмний контролер і впроваджено – для перерозподілу трафіку і збереження навантаження на трафік в межах пропускної спроможності.

Вимоги до мережі, представлені затримкою, джітером та втратою пакетів для деяких служб, показані в таблиці 3.1, яка демонструє, як на ці служби впливатиме надмірне використання посилань.

Таблиця 3.1 – Вимоги до голосової та відеомережі

	Одностороння затримка	Джітер	Втрата
Загальний екран	<1000 мс	<100 мс	<0.05%
Відео-конференції	<150 мс	<30 мс	<0,10%
IP-телефонія	<150 мс	<30 мс	<0,10%

В цьому випадку програмний контролер буде розгорнуто на підприємстві для підтримування використання корпоративних Інтернет посилань на рівні 90% пропускної спроможності лінії зв'язку і підтримки підприємством запропонованої якості послуг або його SLA.

Перше Інтернет-з'єднання підприємства, підключене до ISP1, має початкове навантаження трафіку близько 4 Мбіт/с, а потім починає збільшуватися, досягаючи приблизно 9,5 Мбіт/с, як показано на рис. 3.5.

Друге Інтернет-посилання підприємства, підключене до ISP2 та налаштоване в якості резервного посилання для першого та третього посилання з нульовим навантаженням трафіку, як показано на рис. 3.6.

Третє Інтернет-посилання підприємства підключено до ISP3 та має близько 5 Мбіт/с навантаження трафіку, як показано на рис. 3.7.

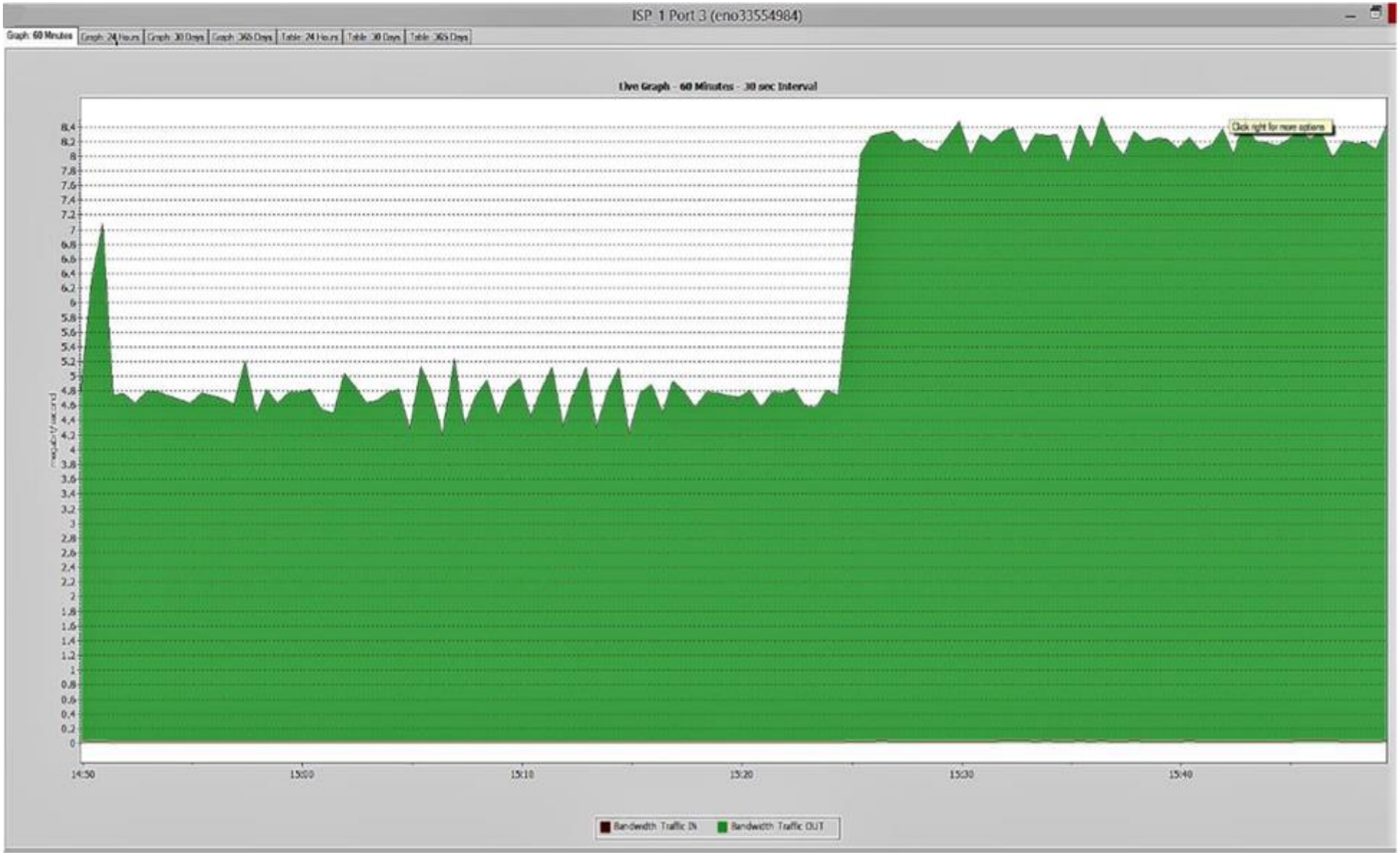

Рисунок 3.5 – Початкове навантаження трафіку ISP1

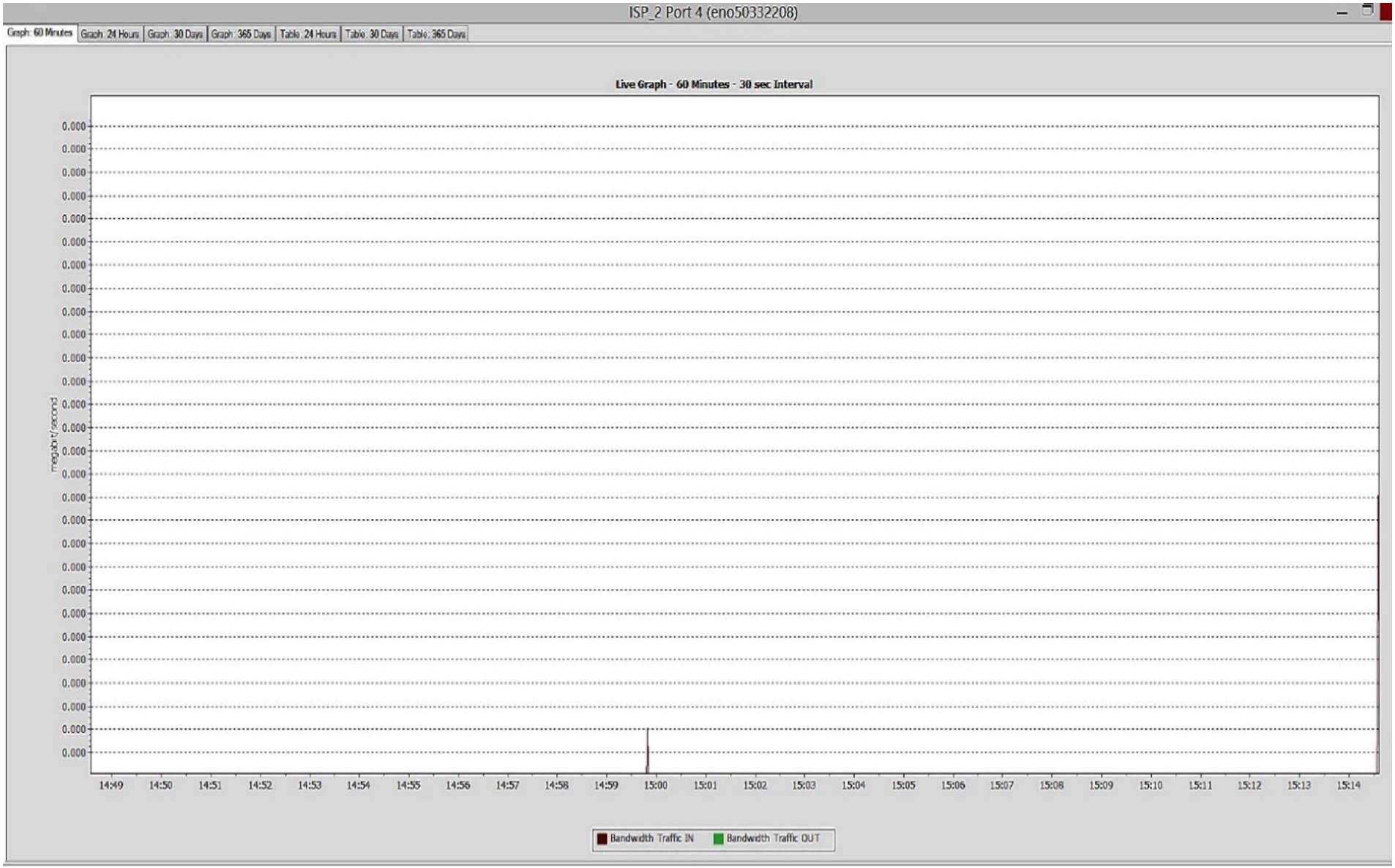

Рисунок 3.6 – Початкове навантаження трафіку ISP2

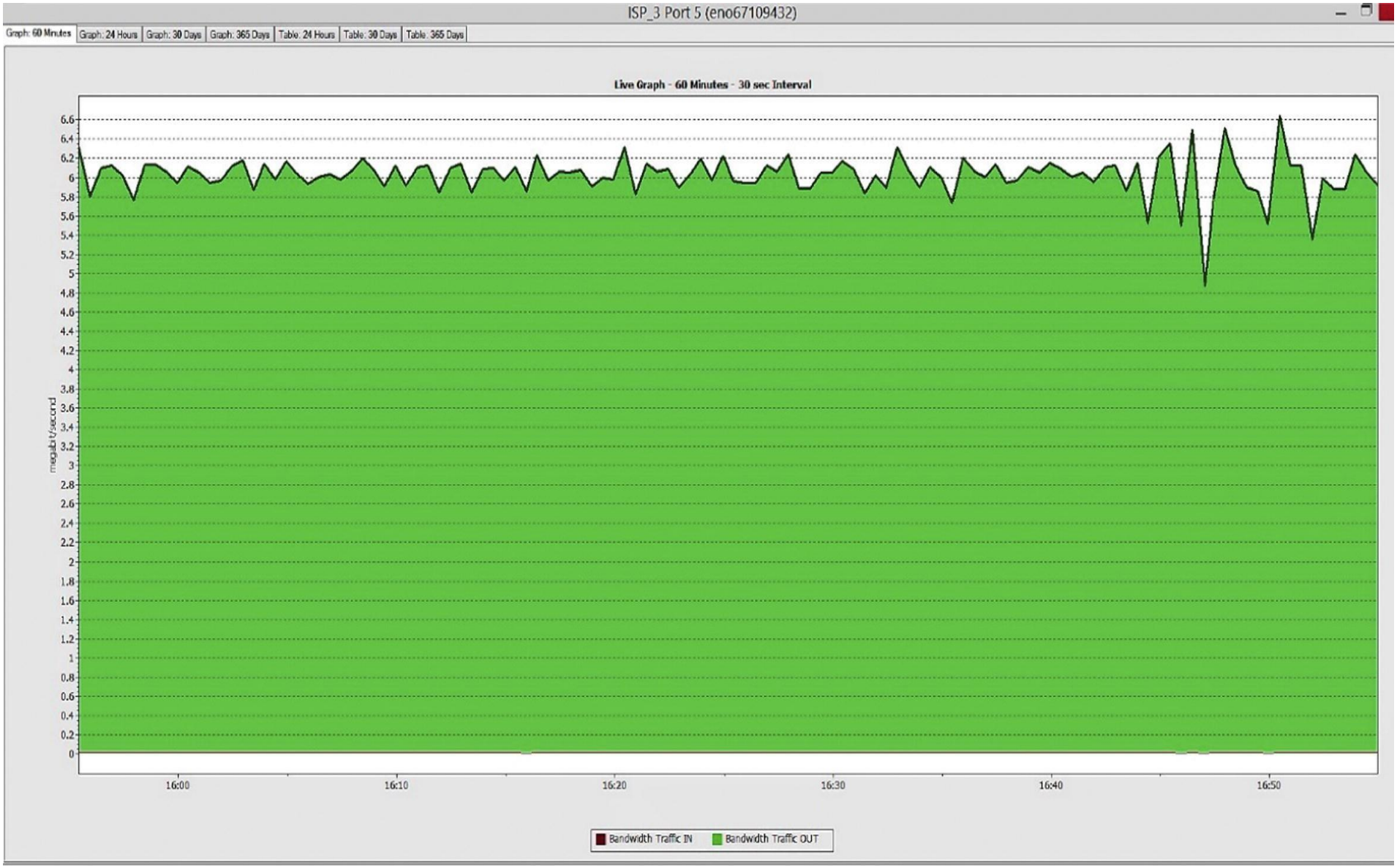

Рисунок 3.7 – Початкове навантаження трафіку ISP3

Усі графіки використання посилань отримані з інструменту моніторингу зв'язків, який відстежує використання корпоративних зв’язків. У звичайному режимі роботи підприємства навантаження на перше Інтернет-з'єднання буде збільшуватися до тих пір, поки не з'явиться негативний вплив на послуги підприємства, пропоновані через це посилання, за причини повного або надмірного використання каналу зв'язку.

У разі розгортання програмного контролера, коли використання першого з'єднання збільшується та перевищує 90% пропускної спроможності зв'язку (9,5 Мбіт/с, як показано на рис. 3.5), модуль розрахунку трафіку програмного контролера запускається і обирає необхідний IP-префікс для перенаправлення, а також обирає 2-е Інтернет-з'єднання підприємства для переведення цієї кількості трафіку, оскільки це посилання з меншим завантаженням трафіку та має доступну пропускну спроможність для розміщення перерозподіленого трафіку.

На рис. 3.8 показана різниця в конфігурації BGP-маршрутизатора підприємства до і після того, як модуль конфігурації програмного контролера надіслав нові BGP-політики для перерозподілу трафіку, де шість маршрутних карт були налаштовані по дві на кожне посилання та застосовані для здійснення необхідного перерозподілу трафіку на доступні Інтернет-посилання.

Після застосування перерозподіленої політики маршрутизації BGP, трафік через перше Інтернет-з'єднання зменшився до приблизно 4 Мбіт/с, як показано на рис. 3.9, виділення за допомогою еліпса та стрілки вказують на момент зміни трафіку на графіку.

Початкова конфігурація	Перерозподілена конфігурація
router bgp 100 no synchronization bgp router-id 100.100.3.1 network 100.100.1.0 mask 255.255.255.0 network 100.100.2.0 mask 255.255.255.0 network 100.100.3.0 mask 255.255.255.0 neighbor 10.10.1.1 remote-as 1100 neighbor 10.10.1.1 ebgp-multihop 255 neighbor 10.10.1.1 soft-reconfiguration inbound neighbor 10.10.1.1 route-map ISP1-out in neighbor 10.10.1.5 remote-as 2200 neighbor 10.10.1.5 ebgp-multihop 255 neighbor 10.10.1.5 soft-reconfiguration inbound neighbor 10.10.1.5 route-map ISP1-in out neighbor 10.10.1.9 remote-as 3300 neighbor 10.10.1.9 ebgp-multihop 255 neighbor 10.10.1.9 soft-reconfiguration inbound neighbor 10.10.1.9 route-map ISP1-in out no auto-summary !	router bgp 100 no synchronization bgp router-id 100.100.3.1 network 100.100.1.0 mask 255.255.255.0 network 100.100.2.0 mask 255.255.255.0 network 100.100.3.0 mask 255.255.255.0 neighbor 10.10.1.1 remote-as 1100 neighbor 10.10.1.1 ebgp-multihop 255 neighbor 10.10.1.1 soft-reconfiguration inbound **neighbor 10.10.1.1 route-map ISP11 in** **neighbor 10.10.1.1 route-map ISP1 out** neighbor 10.10.1.5 remote-as 2200 neighbor 10.10.1.5 ebgp-multihop 255 neighbor 10.10.1.5 soft-reconfiguration inbound **neighbor 10.10.1.5 route-map ISP22 in** **neighbor 10.10.1.5 route-map ISP2 out** neighbor 10.1 0.1.9 remote-as 3300 neighbor 10.10.1.9 ebgp-multihop 255 neighbor 10.10.1.9 soft-reconfiguration inbound **neighbor 10.10.1.9 route-map ISP33 in** **neighbor 10.10.1.9 route-map ISP3 out** no auto-summary !

Рисунок 3.8 – Конфігурація BGP-маршрутизаторів підприємства

Зменшене навантаження трафіку на першому з'єднанні підприємства миттєво відобразилося й на другому Інтернет-з'єднанні підприємства, і його навантаження на трафік стає приблизно 6 Мбіт/с, як показано на рис. 3.10. Тоді, відповідно, використання першого Інтернет-з'єднання підприємства зберігається на рівні до 90% пропускної спроможності зв'язку і таким чином підприємство може підтримувати запропонований рівень обслуговування SLA.

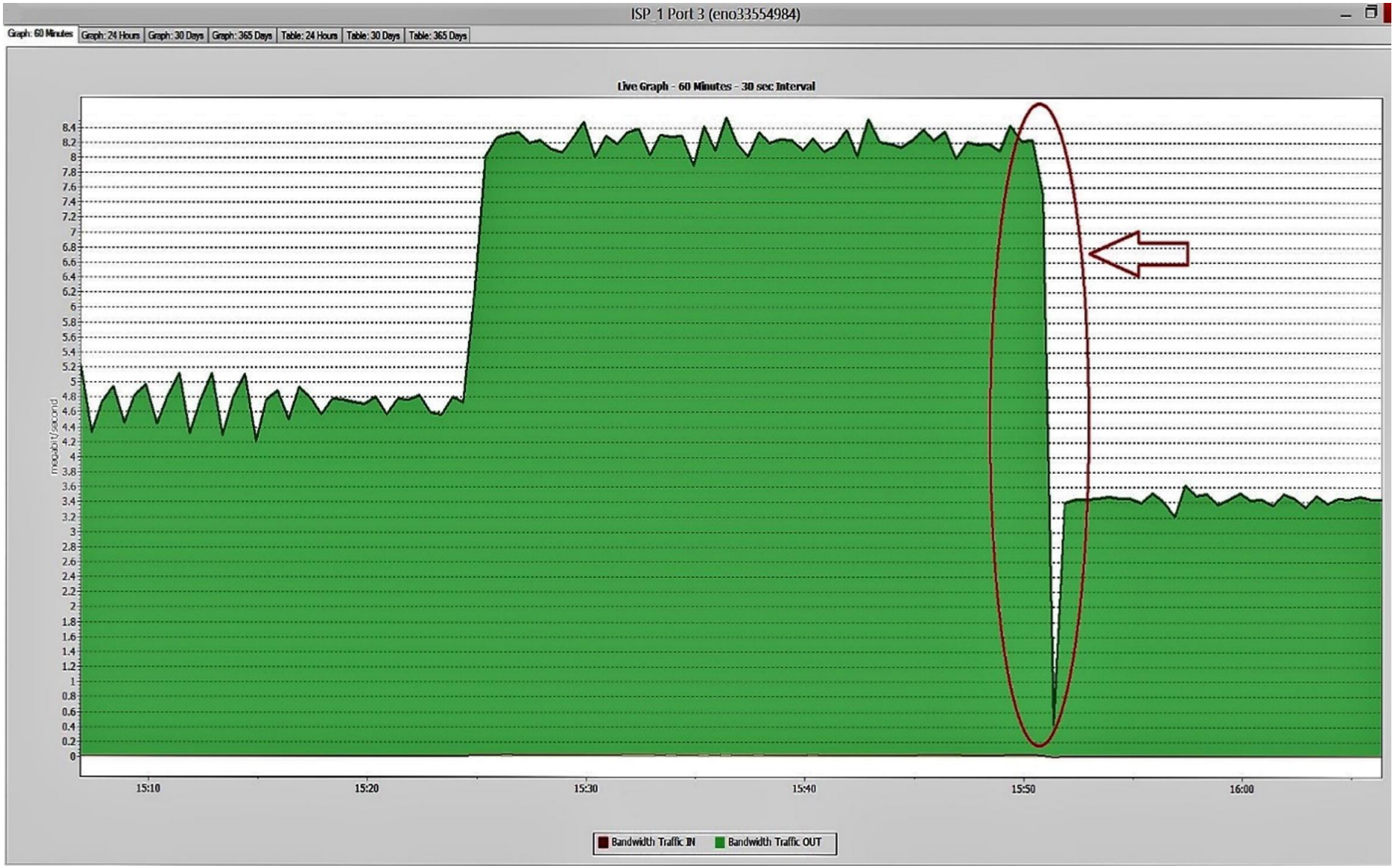

Рисунок 3.9 – Перерозподілене навантаження трафіку ISP1

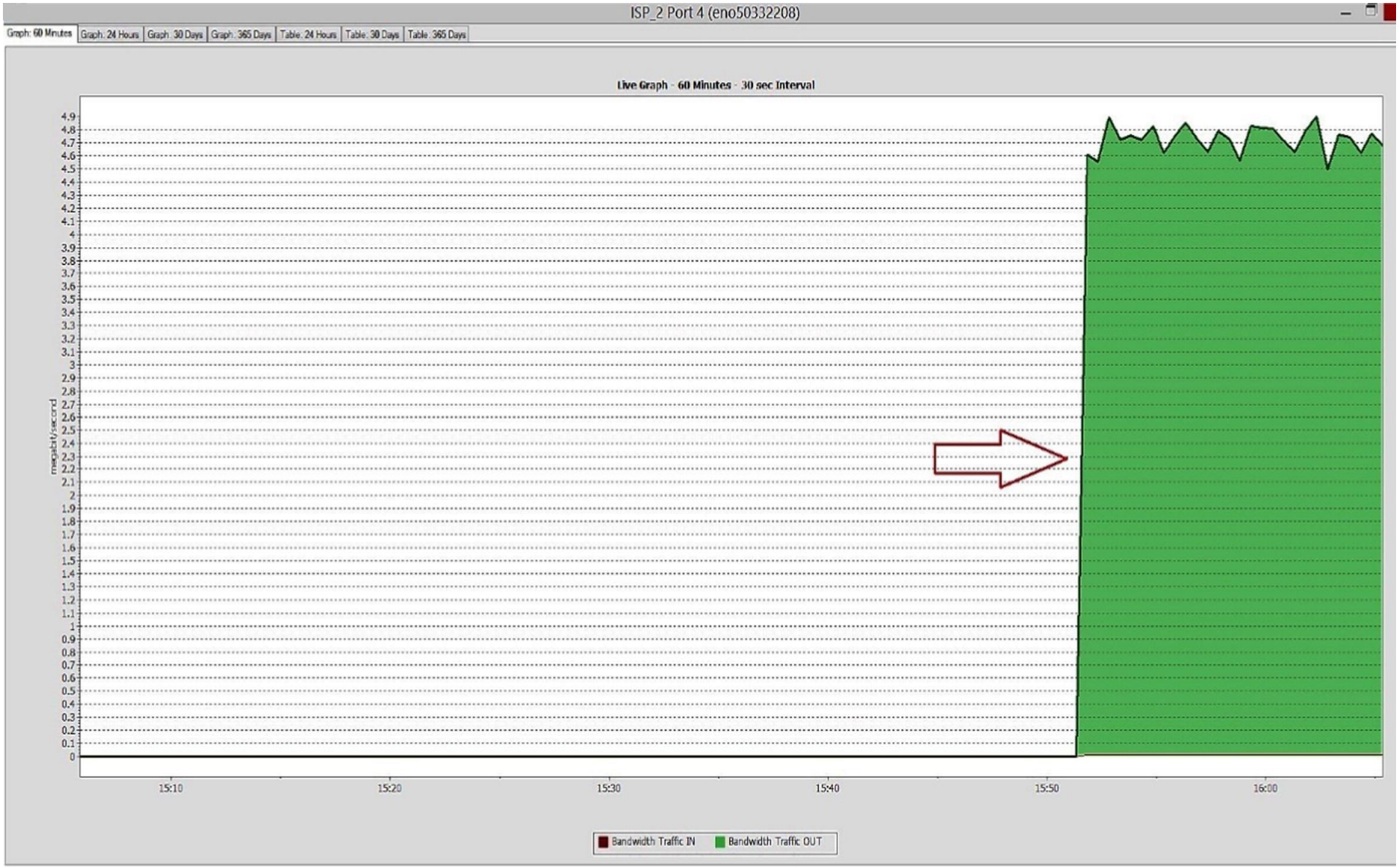

Рисунок 3.9 – Перерозподілене навантаження трафіку ISP2

Попередній експеримент показує, що програмний контролер підвищив затримку та джітер параметрів роботи мережі та пропонує належне використання наявних Інтернет-посилань порівняно з нормальною роботою протоколу BGP.

У таблиці 3.2 показано значне підвищення в параметрах продуктивності затримки та джітера при використанні програмного контролера порівняно з нормальною роботою протоколу BGP, коли при нормальній роботі навантаження трафіку може бути збільшено до 100% пропускної спроможності та перевищити пропускну спроможність зв'язку, що призводить до неприйнятних значень затримки та джітеру, що відповідно впливає на будь-яку пропоновану послугу через це посилання. Тоді як при застосуванні програмного контролера утримується навантаження трафіку в межах пропускної спроможності посилання та зберігається значення затримки та джітеру у прийнятних діапазонах і відповідно підтримується рівень продуктивності мережі для послуг, що пропонуються.

Таблиця 3.2 – Порівняння параметрів продуктивності зв'язку

Завантаженість протоколу	Затримка	Джітер
BGP (100% навантаження)	> 3000 мс	> 3 мс
BGP (> 100% навантаження)	> 3500 мс	> 240 мс
Програмний контролер (<100% навантаження)	< 3 мс	< 1 мс

У таблиці 3.3 показано навантаження на трафік через посилання провайдерів для нормальної роботи протоколу BPG порівняно з використанням програмного контролера, коли в звичайній операції BGP трафік збільшується при з'єднанні ISP1, тоді як посилання ISP2 не має трафіку, і всі послуги, пропоновані в каналі ISP1, будуть впливати коли посилання буде максимально навантажене або перенавантажене. В той самий час при застосуванні програмного контролера трафік посилання ISP1 буде

перерозподілений, коли буде досягнуто попередньо визначений поріг, і відповідно, посилання ISP2 отримає деякий об'єм трафіку ISP1 для підтримки ефективності послуг.

Таблиця 3.3 – Завантаженість Інтернет-з’єднань

	ISP1	ISP2	ISP3
Чистий BGP	> 9.5 Мбіт/с	0	< 5 Мбіт/с
Програмний контролер	< 4 Мбіт/с	< 5 Мбіт/с	< 6 Мбіт/с

Одним з тестів було порівняння ефективності за часовим критерієм пошуку шляху для різної кількості маршрутизаторів при додаванні нового BGP-сусіда в мережу, представлену повнозв’язним графом, для різних методів (рис. 3.10)

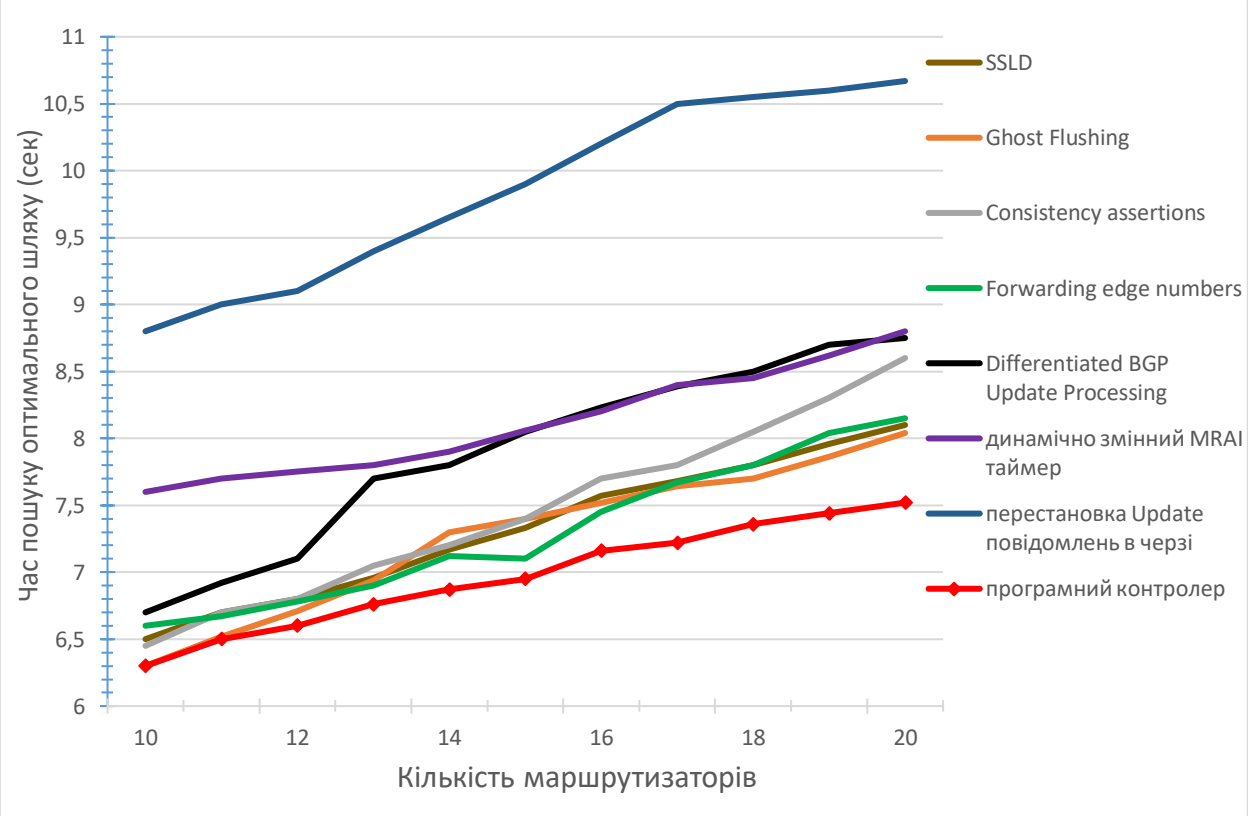

Рисунок 3.10 – Графік залежності часу пошуку оптимального шляху від кількості маршрутизаторів в мережі для різних методів

З даного графіку видно, що програмний контролер отримує деякий виграш в часі у порівнянні з вибраними методами. Видно, що залежність носить лінійний характер і чим більше маршрутизаторів, тим рівніше стає лінія і тим більше стає відрив від конкурентів. Звісно на такій невеликій кількості не всі методи можуть показати себе у всій своїй силі, але такого тесту достатньо для первісного порівняння їх можливостей.

Впроваджений програмний контролер видає нову політику BGP-маршрутизації у разі перевикористання зв'язку або використання зв’язку при досягненні заздалегідь визначеного значення для підтримки рівня обслуговування (SLA), і відповідно BGP-маршрутизатори надсилатимуть повідомлення про оновлення своїм сусідам для оновлення своїх таблиць маршрутизації. В такому випадку ефективність мережі може постраждати через наступні фактори:

- багаторазові зміни мережі через оновлення маршруту або несправність зв’язку призводять до великої кількості BGP Update-повідомлень, що в свою чергу може призвести до нестабільності мережі та відповідно до погіршення продуктивності через одну з наступних причин:
    - сповільнення конвергенції протоколу BGP; у випадку, коли за час конвергенції береться час, який необхідний BGP-маршрутизатору для початку переадресації пакетів після того, як трапився збій або зміна пошуку шляху, доки цей маршрутизатор отримує повідомлення про оновлення, трафік не буде переданий, тому збільшення часу конвергенції знизить продуктивність мережі;
    - штрафне числове значення затримки за демпфірування маршруту може бути застосоване Інтернет-провайдером до BGP-сусіда через множинні оновлення маршрутизації, отримані внаслідок багаторазових змін конфігурації або

нестабільності зв’язку, для уникнення проблеми нестабільності мережі;

- великий вплив BGP Update-повідомлень на деякі сервіси, що працюють переважно або тільки у режимі реального часу, наприклад, голос через IP (VOIP) і ситуації, коли відбувається оновлення, а якість голосу падає до незадовільного рівня чи виклик не може бути виконаний для кожного абонента протягом часу, необхідного маршрутизатору для пошуку оптимального шляху;
- використання техніки попереднього планування шляху маршрутизації, яка є популярною для управління вхідного трафіку протоколу BGP та використовується програмним контролером для контролю вхідного трафіку, але вибір маршруту на основі довжини шляху AS-Path не гарантується на 100%, а також це може спричинити появу петель маршрутизації, щоб мінімізувати цей мережний ризик, можна зробити одне з наступних:
    - адміністратор мережі може просто перевірити свою довжину шляху префіксів, звернувшись до серверів загальнодоступних маршрутів, і належно вирішує необхідну довжину шляху для гарантування, що нова політика маршрутизації, видана програмним контролером, буде ефективною і програмний контролер буде ініціалізований цими значеннями, що відповідають кожному префіксу;
    - незважаючи на те, що підхід використання техніки попереднього планування шляху маршрутизації широко практикується багатьма АС, але все ж існують дослідження, які пропонують використовувати алгоритми, щоб дозволити більш надійне використання планування маршруту, наприклад, алгоритм для обчислення оптимальних стратегій прокладення шляху, заданого декількома сусідніми посиланнями [31], і

відповідно програмний контролер може один з таких алгоритмів.

Програмний контролер містить таймер затримки, який перевіряється, перш ніж застосовувати будь-яку нову BGP-конфігурацію для контролю та запобігання повідомлень про постійне оновлення, і, відповідно, уникати як повільної конвергенції, так і зі штрафним числовим значенням затримки за демпфірування маршруту.

Також розроблений програмний контролер може вплинути на якість голосових дзвінків, бо максимальне або надмірне навантаження на зв'язок має аналогічний до вищезгаданих BGP Update-повідомлень вплив на передачу аудіо-трафіку в режимі реального часу. Цей ефект буде безперервним, доки ситуація з непомірним навантаженням не вирішиться, що займає час більший, ніж потрібно BGP-маршрутизатору для пошуку оптимального шляху. А значить, що при перерозподілі навантажень ця проблема більше не буде виникати без додаткових дій зі сторони.

Крім того підвищиться продуктивність, знову ж таки через пропозицію вирішення проблеми перевантаженості зв’язку, а її ефективність полягає в тому, що час погіршення якості обслуговування (деградації) послуги не перевищить час конвергенції, який може підтримуватися на настільки низькому рівні, наскільки це можливо за допомогою застосування послідовної конфігурації протоколу BGP.

Окрім особливостей впливу виконання програмного контролера на ефективність роботи існує і сторона безпеки функціонування, яку не можна скидати з рахунку. Протокол BGP має ряд вразливостей з самого початку, які не можуть бути вирішені в самому протоколі через великий шанс перенавантаження його і як наслідок суттєвого сповільнення його функціонування [33].

Протокол BGP покладається на TCP як на свій транспортний протокол, тому він сприйнятливий до тих самих атак, які спрямовані на будь-який інший

протокол на основі TCP, а також тому, що протокол BGP є застосунком, вразливим до різних загроз і найбільш популярні атаками є:

- атака маніпуляції з BGP-маршрутом, що відбувається коли вміст таблиці маршрутизації змінюється зловмисним пристроєм, який може запобігти досягненню трафіку кінцевої точки призначення без будь-якого підтвердження чи повідомлення; для зменшення впливу такої атаки зазвичай використовують механізм аутентифікації сусідів MD5, щоб гарантувати, що тільки авторизовані сусіди можуть встановити це відношення BGP-сусідства, і щоб інформація про маршрути обміну між цими двома пристроями не була змінена або замінена;
- атака BGP Denial of Service (DoS), що виникає, коли небажаний трафік відправляється зловмисником до жертви у спробі використання всіх наявних ресурсів BGP-мережі або центрального процесору жертв, що призводить до нестачі ресурсів для дійсної обробки трафіку протоколу BGP; для пом'якшення наслідків впливу даного різновиду атак застосовується перевірка безпеки атрибуту TTL (Time-to-Live), для налаштованого зовнішнього сеансу eBGP, TTL заголовка IP-адреси для всіх пакетів сусіднього сеансу встановлюється на 1, що перешкоджає встановленню сеансу eBGP за межі одного хопу, але не працює для iBGP;
- атака викрадення BGP-маршруту (Route Hijacking), що відбувається, коли зловмисник спеціально оголошує префікси жертви для перенаправлення деякого або всього трафіку до себе з непередбачуваною метою; для мінімізації шкоди застосовується аутентифікація BGP-сусіда за допомогою MD5 або TTL, окрім деяких інших дій конфігурації, таких як налаштування максимальних префіксів, фільтрація префіксів за допомогою списків префіксів або списків доступу до AC та змісту атрибуту AS-Path з обмеженням

довжини для забезпечення отримання інформації про маршрути від надійних сусідів.

В програмному контролері дані проблеми загрози безпеки захисту розглянуті в превентивно-уникаючому аспекті:

- сам програмний контролер не запускає протокол BGP і не має активних BGP-сеансів з BGP-маршрутизаторами в мережі, він функціонує окремо від мережі і не може вплинути на неї, якщо атака буде направлена на нього;
- за задумом програмний контролер підключається до приватної мережі підприємства або Інтернет-провайдера і це означає, що він не буде відкритий в мережі Інтернет задля уникнення DDoS-атаки або піддавання компрометації та буде використовуватися лише для зміни таблиць маршрутизації та пересилання трафіку на інші напрямки;
- програмний контролер має можливість спілкуватися з BGP-маршрутизаторами для надсилання нової конфігурації політики протоколу BGP по захищеному каналу на базі каналу IPSEC, щоб додати ще один рівень захисту.

Висновки до розділу 3

В даному розділі розглянута концепція роботи розробленого програмного контролера з описом основних відмінностей від вже існуючих аналогів, описана структура рішення та його основні модулі. Робота кожного модуля розглянута окремо, після чого описана їх взаємодія між собою та з зовнішніми елементами мережі Інтернет. Також представлено засоби, які використовувалися для створення конкретних елементів реалізації рішення проблеми підвищення ефективності пошуку шляху при BGP-маршрутизації.

Представлені графіки функціонування програмного контролера при вирішенні конкретної проблеми з перенавантаженням каналу та як вони змінюються на кожному етапі роботи. Експериментально доведена теоретична ефективність перерозподілу трафіку по завантаженості каналів та вплив даного явища на затримку пакетів та джітер. Крім того проведено порівняння роботи запропонованого програмного контролера з вже існуючими методами підвищення ефективності пошуку шляху з досить непоганим результатом на користь саме програмного контролера.

До того ж обґрунтовано переваги програмного контролера зі сторони відсутності впливу на рівень безпеки BGP-маршрутизації та зі сторони підвищення якості зв’язку за рахунок видачі нової політики при досягненні максимального чи навіть надмірного використання каналу зв’язку.

ЗАГАЛЬНІ ВИСНОВКИ

В роботі проаналізовано принципи функціонування протоколу BGP, як головного протоколу групової маршрутизації між автономними системами в мережі Інтернет. Ґрунтуючись на статистичних даних про приріст кількості автономних систем у світі, а значить і Інтернет-префіксів, підтверджена актуальність проблеми створення способів підвищення ефективності пошуку шляху при такій маршрутизації та розглянуто порядок дій для впровадження розробленого способу у роботу мережі.

Крім того розглянуто основні методики оптимізації пошуку ефективного шляху, розібрані їх основні концепції та представлена порівняльна характеристика на основі теоретичних та експериментальних даних. На основі цих даних виділені два підходи до розгляду проблеми, на які спираються обрані рішення. Аргументовано створення власної імітаційної моделі для проведення тестування, збору даних та створення статистики по роботі як вже існуючих аналогів, так і запропонованого способу. Представлено головні відмінності у порівняні з найчастіше вживаними імітаційними моделями та охарактеризовано причини впровадження конкретних змін.

В результаті запропоновано власний спосіб підвищення ефективності пошуку шляху з використанням програмного контролера, в основу якого лягла ідея перерозподілу трафіку з максимально навантажених або перевантажених каналів зв’язку на ті, де пропускна спроможність дозволяє підвищити рівень навантаження без втрат швидкості та якості подання послуг.

Розроблений контролер складається з трьох модулів: моніторингу зв’язку, розрахунку трафіку та конфігурації. Розписані алгоритми взаємодії модулів між собою та з зовнішніми елементами мережі, представлений порядок дій всередині

програмного контролера від запуску і до отримання результатів з описанням причин наявності кожного кроку та його мети.

Однією з ключових особливостей, яку пропонує розроблений спосіб є більш прискіпливий підхід до поводження з Інтернет-трафіком для автоматичного перерозподілу трафіку через багатопоточні з'єднання на основі використання посилань, що не призводить до якихось змін або порушень для існуючої системи мережі Інтернет.

Результатом впровадження програмного контролера є підвищення загальної продуктивності мережі BGP, що виражається в :

- більш ефективному використанні наявної пропускної спроможності по відношенню до існуючих посилань;
- підтримці трафіку в межах пропускної здатності;
- підтримці параметрів продуктивності мережі в допустимих діапазонах;
- підвищенні продуктивності та надійності за допомогою оптимізації в реальному часі для всього IP-трафіку;
- забезпеченні надійної якості маршрутизації без надмірних технічних ресурсів;
- підтримці угоди про рівень обслуговування трафіків підприємства або Інтернет-провайдера.

До того ж при порівнянні результатів роботи запропонованого способу із розглянутими вже впровадженими методиками підвищення ефективності пошуку шляху були отримані позитивні результати, що говорить про конкурентоздатність розробленого програмного контролера.

Також необхідно зазначити відсутність впливу впровадження програмного контролера в роботу мережі та на її безпеку через те, що він не сам запускає протокол BGP і не бере прямої участі в активному сеансі з маршрутизаторами.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Abuzneid A., Stark B. J. Improving BGP Convergence Time via MRAI Timer. Novel Algorithms and Techniques in Telecommunications and Networking. 2010. P. 105-110. URL: https://link.springer.com/chapter/10.1007/978-90-481-3662-9_17 (дата звернення: 07.12.2018).
2. Arins A. Latency factor in worldwide IP routed networks. 2014 IEEE 2nd Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Vilnius, 2014. P. 1-4.
3. ASN Resource guide. APNIC Internet Archive : URL: https://web.archive.org/web/20071231160539/http://www.apnic.net/services/asn_guide.html (дата звернення: 17.09.2019).
4. BGP Prefix Report. Hurricane Electric Internet services : URL: https://bgp.he.net/report/prefixes (дата звернення: 01.03.2020).
5. Brembler-Barr A., Afek Y., Shwarz S. Improved BGP Convergence via Ghost Flushing. IEEE Journal on Selected Areas in Communications. 2005. P. 1933-1948.
6. Butler K., Farley T., Mcdaniel P., Rexford J. A Survey of BGP Security Issues and Solutions. Proceedings of the IEEE. 2010. Vol. 98. Issue 1. P. 100-122.
7. Chandrashekar J., Duan Z., Zhang Z., Krasky J. Limiting Path Exploration in BGP. INFOCOM. 2005. Vol. 5. P. 2337-2348.
8. Fujinoki H. Analysis on ideal network structures to improve reliability by multi-path and multi-homing BGP routing in the Internet.
9. Goodell G., Aiello W., Griffin T., Ioannidis J., Mcdaniel P. D. Working around BGP: An Incremental Approach to Improving Security and Accuracy in Interdomain Routing. ISOC Symposium on Network and Distributed Systems Security. 2003. Vol. 23. P. 317-329.

10. Gordon M. An introduction to network programming the Python way. IEEE Distributed Systems Online. 2005. №10. Vol. 6. P. 5–7.
11. Griffin T. G., Premore B. J. An Experimental Analysis of BGP Convergence Times. Proceedings of the Ninth International Conference on Network Protocols. 2001. P. 53. URL: https://ieeexplore.ieee.org/document/992760 (дата звернення: 08.12.2018).
12. Houle J.D., Ramakrishnan K.K., Sadhvani R., Yuksel M., Kalyanaraman S. The Evolving Internet - Traffic, Engineering, and Roles. The 35th TPRC Research Conference on Communication, Information and Internet Policy, Arlington, 15 August 2007. Palatijn : TPRC, 2007. P. 1-23.
13. Khan A., Kim H., Kwon T., Choi Y. A comparative Study on IP Prefixes and their Origin ASes in BGP and the IRR. ACM SIGCOMM Computer Communication Review. 2013. Vol. 43. Issue 3. P. 16-24. URL: https://dl.acm.org/doi/10.1145/2500098.2500101 (дата звернення 12.04.2019).
14. Mahajan R., Wetherall D., Anderson T. Understanding BGP misconfiguration. ACM SIGCOMM Computer Communication Review. 2002. Vol. 32. P. 3-16. URL: https://dl.acm.org/doi/10.1145/633025.633027 (дата звернення: 20.11.2019).
15. Moubarak M. T., Elbayoumy A. D., Megahed M. H. Design and implementation of BGP novel control mechanism (BGP-NCM) based on network performance parameters. Ain Shams Engineering Journal. 2018. Vol. 9. Issue 4. P. 2079-2091. URL: https://www.sciencedirect.com/science/article/pii/S2090447917300345#t0005 (дата звернення: 07.12.2019).
16. Nordström O., Dovrolis C. Beware of BGP attacks. ACM SIGCOMM Computer Communication Review. 2004. Vol. 34. Issue 2. P. 1-8. URL: https://dl.acm.org/doi/10.1145/997150.997152 (дата звернення: 10.11.2019).

17. Pei D., Zhao X., Wang L., Massey D., Mankey A. Improving BGP Convergence through Consistency Assertions. INFOCOM. 2002. Vol. 2. P. 902-911.
18. RFC 1965. Autonomous System Confederations for BGP. [Чинний від 1996-06-01] : URL: https://tools.ietf.org/html/rfc1965 (дата звернення: 17.06.2018). 6 p. (Інформація та документація).
19. RFC 3682. The Generalized TTL Security Mechanism (GTSM). [Чинний від 2004-02-01] : URL: https://tools.ietf.org/html/rfc3682 (дата звернення: 19.12.2019). 11 p. (Інформація та документація).
20. RFC 4271. A Border Gateway Protocol 4 (BGP-4). [Чинний від 2006-01-01] : URL: https://tools.ietf.org/html/rfc4271 (дата звернення: 17.06.2018). 104 p. (Інформація та документація).
21. Sahoo A., Kant K., Mohapatra P. Improving BGP Convergence Delay for Large-Scale Failures. Dependable Systems and Networks. 2006. P. 323-332.
22. Schroder C. Linux Networking Cookbook. Nuove : O'Reilly Media. 2007. 632 p.
23. Siraj S., Gupta A., Badgujar R. Network simulation tools survey. Int J Adv Res Comput Commun Eng. 2012. Vol.1. P. 199-206.
24. Smith B. R., Garcia-Luna-Aceves J. J. Securing the border gateway routing protocol. Global Telecommunications Conference «GLOBECOM '96». 22-24 November 1996. P. 81 - 85. URL: https://ieeexplore.ieee.org/document/586129 (дата звернення: 10.10.2019).
25. Sun W., Mao M., Shin K. G. Differentiated BGP Update Processing for Improved Routing Convergence. Proceedings of the Proceedings of the IEEE. 2006. P. 280-289.
26. Tangmunarunkit H., Govindan R., Shenker S. Internet Path Inflation due to Policy Routing. Scalability and Traffic Control in IP Networks. 2001. P.188-195.

27. The 16-bit AS Number Report : URL: https://www.potaroo.net/tools/asn16/ (дата звернення: 01.03.2020).
28. The 32-bit AS Number Report : URL: https://www.potaroo.net/tools/asn32/ (дата звернення: 01.03.2020).
29. Timberg C. Нет ничего более постоянного, чем временное. The Washington Post, 2003. №05. URL: https://bitnovosti.com/2015/10/18/net-of-insecurity-part-2/ (дата звернення: 17.10.2018).
30. Ultra Modern Telecommunications & Workshops. 2009. P. 1-6.
31. Wang J., Chiu D., Lui J., Chang R.K.C. Inter-as inbound traffic engineering via ASPP. Transactions on Network and Service Management. 2007. Vol. 4. P. 62-70. URL: https://ieeexplore.ieee.org/document/4275035 (дата звернення: 10.09.2019).
32. World Report. Hurricane Electric Internet services : URL: https://bgp.he.net/report/world (дата звернення: 17.09.2019).
33. Войтенко Є. Д., Орлова М. М. Аналіз вразливості безпеки функціонування BGP та причин складності боротьби з ними. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2020. №39 С. 85-90.
34. Войтенко Є. Д., Орлова М. М. Модифікована імітаційна модель зовнішньої групової маршрутизації. Збірник тез доповідей Дванадцятої наукової конференції «Прикладна математика та комп’ютинг ПМК 2019», 13–15 листопада 2019 р. Київ : КПІ, 2019. С. 236–239.
35. Войтенко Є. Д. Способи захисту від DDOS атак засобами BGP. Збірник тез доповідей Дев'ятнадцятої всеукраїнської науково-методичної конференції «Проблеми охорони праці, промислової та цивільної безпеки 2018», 12-14 листопада 2018 р. Київ : КПІ, 2018. С. 64-66. URL: http://confopcb.iee.kpi.ua/proc/article/download/149166/148274 (дата звернення: 21.11.2018).

36. Кораблин А, Глюков М. Базис сетей. BGP и IP SLA. LinkMeUp СДСМ. 2012. №8. URL: https://2ip.ua/ua/blog/as (дата звернення: 20.11.2019).
37. Шукайло А. Е. Исследование проблем сходимости протокола BGP : дис. на здобуття наук. ступеня магістра : 05.05.2011 / Московский Государственный Университет им. М.В. Ломоносова, Москва, 2011.