**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**

**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**КАФЕДРА КОМП’ЮТЕРНОЇ ІНЖЕНЕРІЇ**

## КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«ВИКОРИСТАННЯ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ В МЕРЕЖАХ OSPF ТА BGP З МЕТОЮ ПІДВИЩЕННЯ ЇХ МАСШТАБОВАНОСТІ ТА ПРОДУКТИВНОСТІ»**

на здобуття освітнього ступеня магістра

зі спеціальності 123 Комп’ютерна інженерія

*(код, найменування спеціальності)*

освітньо-професійної програми

*(назва)*

*Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(підпис)*  *(ім’я, ПРІЗВИЩЕ здобувача)*

Виконав: здобувач вищої освіти гр. КСДМ-62

Підгулько Г.Г.

(Ім’я, ПРІЗВИЩЕ)

Керівник: к.т.н. доцент Торошанко Я.І.

*науковий ступінь,* (Ім’я, ПРІЗВИЩЕ)

*вчене звання*

Рецензент:

*науковий ступінь,* (Ім’я, ПРІЗВИЩЕ)

*вчене звання*

**Київ 2023**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**

**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**Навчально-науковий інститут інформаційних технологій**

# 

# Кафедра Комп’ютерної інженерії

Ступінь вищої освіти «Магістр»

Спеціальність

Освітньо-професійна програма **123 «**Комп’ютерна інженерія»

# ЗАТВЕРДЖУЮ

Завідувач кафедрою Комп’ютерної інженерії

Н.О. Лащевська Ім’я, ПРІЗВИЩЕ

“\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_ 2023 р.

## ЗАВДАННЯ

### НА кваліфікаційну РОБОТУ

### Підгулько Георгію Георгійовичу

*(прізвище, ім’я, по батькові здобувача)*

1.Тема кваліфікаційної роботи Використання протоколів маршрутизації в мережах OSPF та BGP з метою підвищення їх масштабованості та продуктивності

керівник кваліфікаційної роботик.т.н. доцент Торошанко Я.І.

(ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «\_\_\_\_» \_\_\_\_\_\_\_\_ 2023 р. № \_\_\_\_

2. Строк подання кваліфікаційної роботи «\_\_\_\_» \_\_\_\_\_\_\_\_ 2023 р.

3. Вихідні дані до кваліфікаційної роботи:

3.2 Інтернет-ресурси стосовно параметрів якості корпоративних комп’ютерних мереж;

3.3 Технічна документація стосовно апаратно-програмного забезпечення щодо моделювання протоколів маршрутизації OSPF та BGP;

3.4 Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити:

4.1Методи маршрутизації у комп’ютерних мережах;

4.2 Порівняння протоколів динамічної маршрутизації у комп’ютерній мережі;

4.3 Заходи для удосконалення протоколу маршрутизації OSPF;

4.4 Підвищення продуктивності протоколу маршрутизації BGP.

5. Перелік графічного матеріалу: *презентація*

6. Дата видачі завдання «\_\_\_\_» \_\_\_\_\_\_\_\_ 2023 р.

#### КАЛЕНДАРНИЙ ПЛАН

|  |  |  |  |
| --- | --- | --- | --- |
| №  з/п | Назва етапів  кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
| 1 | Підбір науково-технічної літератури |  |  |
| 2 | Методи маршрутизації у ком’ютерних мережах |  |  |
| 3 | Порівняння протоколів динамічної маршрутизації у ком’ютерній мережі |  |  |
| 4 | Заходи для удосконалення протоколу маршрутизації OSPF |  |  |
| 5 | Підвищення продуктивності протоколу маршрутизації BGP |  |  |
| 6 | Вступ, висновки, реферат |  |  |
| 7 | Розробка обов’язкових демонстраційних матеріалів |  |  |
| 8 | Попередній захист роботи |  |  |

Здобувач вищої освіти \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Підгулько Г.Г.

*( підпис ) (Ім’я, ПРІЗВИЩЕ)*

Керівник

кваліфікаційної роботи\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Торошанко Я.І.

*( підпис ) (Ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 77 стор., 2 табл., 32 рис., 22 джерел.

*Мета роботи* - Розробка та аналіз методів підвищення масштабованості та продуктивності протоколів OSPF та BGP з метою забезпечення ефективного та стабільного функціонування комп’ютерних мереж.

*Об’єкт дослідження* – комп’ютерні мережі.

*Предмет дослідження* – протоколи маршрутизації OSPF та BGP.

*Короткий зміст роботи:*

В роботі розглянуто основні характеристики та методи маршрутизації у – комп’ютерних мережах, наведено огляд протоколів динамічної маршрутизації. Проведено детальний аналіз протоколів маршрутизації OSPF та BGP та оцінювання їх продуктивності. Проаналізовано продуктивність обчислень DSPF з використанням методів оптимізації низького рівня; представлено відносну продуктивність алгоритмів DSPF і ISPF інтернет трафіку, методи аналізу та класифікації. Запропоновано заходи для удосконалення протоколу маршрутизації OSPF та підвищення продуктивності протоколу маршрутизації BGP.

КОРПОРАТИВНІ МЕРЕЖІ, ПРОТОКОЛИ СТАТИЧНОЇ МАРШРУТИЗЦІЇ, ПРОТОКОЛИ СТАТИЧНОЇ МАРШРУТИЗЦІЇ, OSPF, BGP

## ABSTRACT

Text part of the master's qualification work:

77 pages, 32 pictures, 2 table, 22 sources.

The purpose of the work - Development and analysis of methods for increasing the scalability and performance of the OSPF and BGP protocols in order to ensure the efficient and stable functioning of computer networks.

The object of research is computer networks.

The subject of research is OSPF and BGP routing protocols.

Summary of the work:

The paper considers the main characteristics and methods of routing in computer networks, provides an overview of dynamic routing protocols. Detailed analysis of OSPF and BGP routing protocols and evaluation of their performance was carried out. The performance of DSPF calculations using low-level optimization methods was analyzed; the relative performance of DSPF and ISPF Internet traffic algorithms, methods of analysis and classification are presented. Measures are proposed to improve the OSPF routing protocol and increase the performance of the BGP routing protocol.

KEYWORDS:

CORPORATE NETWORKS, STATIC ROUTING PROTOCOLS, STATIC ROUTING PROTOCOLS, OSPF, BGP

**ЗМІСТ**

Стор.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Вступ**........................................................................................................................... | | | 9 | |
| **1** | **М МЕТОДИ МАРШРУТИЗАЦІЇ У КОМП’ЮТЕРНИХ МЕРЕЖАХ**........... | | 11 | |
|  | 1.1 | Важливі концептуальні поняття щодо маршрутизації та метрик……... | 12 |
|  |  | 1.1.1 Параметри метрики…………………………………………………. | 12 |
|  | 1.2 | Класифікація протоколів маршрутизації………………….…………….. | 13 |
|  | 1.3 | Статична та динамічна маршрутизація………………………………….. | 14 |
|  | 1.4 | Протоколи класової маршрутизації та безкласової маршрутизації…... | 15 |
|  |  | 1.4.1 Класова маршрутизація…………………………………………….. | 16 |
|  |  | 1.4.2 Безкласова маршрутизація…………………………………………. | 17 |
|  | 1.5 | Маршрутизація на основі стану каналів………………………………… | 17 |
|  |  | 1.5.1 Характеристики протоколу на основі стану каналів……………... | 19 |
|  |  | 1.5.2 Методи маршрутизації на основі стану каналів…………………... | 19 |
|  |  | 1.5.3 Сильні та слабкі сторони маршрутизації на основі стану каналів. | 20 |
|  | 1.6 | Дистанційно-векторна маршрутизація…………………………………... | 20 |
|  |  | 1.6.1 Характеристики дистанційно-векторної маршрутизації…………. | 22 |
|  |  | 1.6.2 Плюси і мінуси дистанційно-векторної маршрутизації………….. | 22 |
| **2** | **1 ПОРІВНЯННЯ ПРОТОКОЛІВ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ**  **КОМП’ЮТЕРНІЙ МЕРЕЖІ**………………………………………………... | | 24 | |
|  | 2.1 | Вимоги корпоративної мережі до протоколу маршрутизації………….. | 24 |
|  | 2.2 | Основні критерії порівняння протоколів маршрутизації………………. | 25 |
|  | 2.3 | Коротка характеристика найбільш поширених протоколів маршрутизації……………………………………………………………... | 29 |
|  | 2.4 | Порівняльна характеристика протоколів маршрутизації OSPF і BGP… | 38 |
| **3** | **ЗАХОДИ ДЛЯ УДОСКОНАЛЕННЯ ПРОТОКОЛУ МАРШРУТИЗАЦІЇ OSPF**……………………...……………………………… | | 42 | |
|  | 3.1 | Алгоритм функціонування протоколу OSPF…………………………… | 43 |
|  | 3.2 | Алгоритм ISPF…………………………………………………………….. | 45 |
|  | 3.3 | Структура системи оцінювання продуктивності OSPF………………… | 46 |
|  | 3.4 | Характеристика продуктивності алгоритму DSPF……………………... | 47 |
|  | 3.5 | Оптимізація за допомогою алгоритму ISPF……………………………... | 52 |
| **4** | **ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ПРОТОКОЛУ МАРШРУТИЗАЦІЇ BGP**………………………………………………………. | | 55 | |
|  | 4.1 | Архітектура однокрокової маршрутизації………………………………. | 57 |
|  | 4.2 | Краща конвергенція маршрутизації……………………………………… | 58 |
|  | 4.3 | Результати моделювання…………………………………………………. | 59 |
|  | 4.4 | Багатокрокова міждоменна маршрутизація……………………………... | 63 |
|  |  | 4.4.1 Перетворення багатокрокової маршрутизації на масштабовану… | 64 |
|  |  | 4.4.2 Маршрутизація наступного переходу для сусідів………………… | 65 |
|  | 4.5 | Захист системи маршрутизації…………………………………………… | 67 |
|  |  | 4.5.1 Зменшена поверхня атаки…………………………………………... | 67 |
|  |  | 4.5.2 Модель загроз, менш вразлива до помилок конфігурації ………... | 68 |
|  |  | 4.5.3 Наскрізні механізми безпеки……………………………………….. | 68 |
|  | 4.6 | Управління трафіком……………………………………………………… | 70 |
|  |  | 4.6.1 Маршрутизація, орієнтована на продуктивність ………………... | 70 |
|  |  | 4.6.2 Розробка міждоменного трафіку…………………………………… | 72 |
|  | **ВисновкИ**.......................................................................................................... | | 74 | |  |  |
|  | **Перелік посилань**....................................................................................... | | 76 | |  |  |
|  | **ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ**................................................................. | | 78 | |  |  |

**ВСТУП**

Стабільність мережі та час конвергенції все частіше стають критичними параметрами загальної продуктивності мережі. Тому дуже важливо порівняти продуктивність протоколів маршрутизації, щоб зрозуміти проблеми конвергенції та майбутні потреби. Корпоративні мережі потребують кращої продуктивності мережі зі стабільним зв’язком із віддаленими філіями. Для підключення віддалених відділень необхідна наявність резервного каналу на випадок збою зв’язку. Постачальники Інтернет-послуг (ISP) не можуть гарантувати мережеве підключення без помилок або збоїв зв’язку. Щоб уникнути простою мережі, підприємство використовує резервну лінію зв’язку, бажано з іншим провайдером Інтернету з можливістю резервної лінії зв’язку для своєї мережі.

Маршрутизація є важливим компонентом комунікаційних мереж; без нього дані залишалися б обмеженими підмережею, з якої вони походять. Тому необхідно вибрати відповідні протоколи маршрутизації для кращого та надійного зв’язку в будь-якій інфраструктурі. Існують різні протоколи з унікальною архітектурою та алгоритмами маршрутизації, які використовуються для надійного та швидкого зв’язку з різними функціями та рівнями продуктивності.

Для безпечної та масштабованої комунікаційної інфраструктури необхідний вибір відповідних протоколів маршрутизації, які можуть запропонувати необхідні результати. У корпоративній мережі дані переміщуються між локальними мережами та глобальними мережами через різні мережеві топології та обробляються різними протоколами як усередині, так і за межами різних автономних систем. Таким чином, вибір найбільш відповідних протоколів зв’язку має вирішальне значення для створення безпечної та масштабованої платформи зв’язку, що є критичним аспектом у побудові та підтримці ефективних мереж зв’язку, особливо з огляду на динамічний характер Інтернет-з’єднань та взаємодії автономних мереж

На сьогоднішній день важко знайти компанію, яка не мала б мережевої інфраструктури. Практично всі сучасні мережі маршрутизуються. Зі зростанням розмірів мережі компанії для підтримки її нормальної працездатності мережевому адміністратору доводиться переходити від статичної маршрутизації до динамічної і, отже, до використання одного з протоколів динамічної маршрутизації.

Ефективність протоколу маршрутизації при прокладанні шляху даних має вирішальне значення для досягнення високої продуктивності доставки даних у мережі. Протоколи маршрутизації оновлюють свої таблиці маршрутизації у відповідь на зміни мережі. Наприклад, збої зв’язку або маршрутизатора в мережі можуть змінити оптимальні маршрути до певних місць призначення. Будь-якому протоколу маршрутизації потрібен деякий час для обчислення нових стабільних оптимальних маршрутів після зміни мережі, а маршрути, що використовуються в проміжний період, можуть бути неоптимальними або навіть нефункціональними. Процес пошуку нових оптимальних маршрутів після зміни мережі називається конвергенцією [6]. Час конвергенції протоколу маршрутизації має бути коротким, щоб уникнути втрат пакетів через часові чорні діри маршрутизації, які можуть виникнути, коли під час маршрутизації за часом використовується нефункціональний маршрут сходиться до нових стабільних оптимальних маршрутів. Протоколи маршрутизації з коротким часом конвергенції важливі для побудови високопродуктивних стабільних мереж.

Оскільки вибір протоколу істотно впливає на ефективність і надійність роботи мережі організації загалом, він має бути добре обґрунтованим.

Метою магістерської роботи є дослідження та аналіз проблеми, з якою стикаються корпоративні мережі у разі збою зв’язку, і які протоколи маршрутизації вони повинні використовувати, щоб мінімізувати мережеву затримку, тремтіння, час конвергенції та час конвергенції після відмови для кращої продуктивності мережі, коли як внутрішні, так і зовнішні протоколи маршрутизації використовуються через безпечне мережеве з’єднання.

Також в роботі наведено обґрунтування підвищення продуктивності протоколів OSPF та BGP у корпоративних мережах.

**1 МЕТОДИ МАРШРУТИЗАЦІЇ У КОМП’ЮТЕРНИХ МЕРЕЖАХ**

У корпоративних мережах протоколи маршрутизації зазвичай передають

інформацію про маршрутизацію пакетів між взаємопов’язаними вузлами

Усі протоколи маршрутизації повинні мати такі цілі:

1. Комунікація між різними маршрутизаторами, розташованими в різних місцях.

2. Приймання правильних та ефективних рішень щодо маршрутизації.

3. Обмін інформацією між роутерами сусідів.

4. Створення безпомилкових таблиць маршрутизації.

5. Вивчення існуючих маршрутів.

Маршрутизатори використовуються для передачі данх між різними підмережами і обміну інформацією про маршрути між ними. Основна концепція «протоколів маршрутизації» полягає в створенні найкращого можливого шляху передачі інформації від одного кінця до іншого, щоб знайти найкращий маршрут від джерела до місця призначення. Протоколи маршрутизації побудовані на основі різних властивостей. Для маршрутизації на основі IP динамічні протоколи IGP можна класифікувати як [1]:

- Link State Routing Protocols;

- протоколи дистанційної векторної маршрутизації;

- гібридні протоколи.

Основні характеристик протоколів маршрутизації наступні:

- *найбільш оптимальні маршрути.* Однією з характеристик протоколів маршрутизації є пошук найкращого оптимального маршруту для передачі інформації Він може бути одним із найменших або з найменших шляхів на ситуацію;

- *найшвидша конвергенція*. У між маршрутному зв'язку час зв'язку має бути невеликим, тому інформацію про маршрутизатори можна легко підтвердити.

- *параметри безпеки*. Протокол забезпечує безпечну передачу даних від джерела до місця призначення;

- *уникнення петель*. Loop free використовується для визначення ефективної пропускної здатності мережі шляхом створення впевненості в тому, що в мережі немає петель, оскільки петлі не тільки сповільнюють, але також ускладнюють розрахунок ефективної пропускної здатності.

**1.1 Важливі концептуальні поняття щодо маршрутизації та метрик**

Метрику можна просто визначити як критерій прийняття рішень будь-якого протоколу маршрутизації, на основі якого він приймає рішення щодо маршрутизації. Всі протоколи мають різні критерії для визначення найкращого маршруту. Наприклад, у випадку RIP метрикою є підрахунок стрибків, EIGRP використовує складену метрику, яка є комбінацією різних атрибутів, таких як навантаження, надійність, MTU, смуга пропускання та затримка. Метрикою OSPF є витрати на пропускну здатність.

Метрики зазвичай визначають найкращий можливий шлях у випадку, коли для одного і того самого вузла призначення є доступним більше ніж один шлях. Існують різні способи обчислення найкращого шляху і показників для кожного протоколу маршрутизації.

**1.1.1 Параметри метрики**

Кожен протокол маршрутизації використовує метрику для вимірювання та ранжирування маршрутів на основі маршрутизації: від найкращого до гіршого від найбільш бажаного до найменш бажаного. Різні протоколи маршрутизації використовують різні методи маршрутизації та параметри для вимірювання різних метрик [1].

Зазвичай використовуються наступні метрики для визначення найкращих шляхів за допомогою будь-якого протоколу маршрутизації:

- затримка: визначає кількість часу, необхідного для подорожі від однієї точки до іншої. Вона залежить від різних параметрів, наприклад; використання пропускної здатності каналу, фізичної відстані і черги порту;

- вартість: може базуватися на будь-якій окремій метриці або комбінації метрик, яку можна визначити за найкоротшою відстанню або маршрутом з найменшим трафіком. Вона нормально керується адміністраторами мережі;

- навантаження: обчислюється трафіком на конкретних вузлах. Протокол маршрутизації зазвичай використовує навантаження для розрахунку найкращого маршруту;

- підрахунок стрибків: підраховує кількість маршрутизаторів, через які має пройти пакет, щоб досягти місця призначення;

- пропускна здатність: також відіграє важливу роль в ідентифікації шляху, яка зазвичай спонукає до вибору каналу з високою пропускною здатністю замість низької продуктивності;

- надійність: можна розрахувати, посилаючись на попередні несправності або кількість попередніх помилок.

**1.2 Класифікація протоколів маршрутизації**

Протоколи маршрутизації можна класифікувати на дві основні категорії: статичний маршрут і динамічний маршрут. Статичні маршрути налаштовуються адміністратором мережі. Адміністративні дистанції статичних маршрутів завжди дорівнюють 1, що означає, що в мережі є статичний маршрут і, крім того, інші протоколи динамічної маршрутизації також використовуються для вибору шляху, при якому статичний маршрут завжди вважатись найкращим маршрутом, оскільки він має меншу адміністративну відстань порівняно з будь-яким протоколом маршрутизації. Динамічні маршрути – це маршрути, вибрані за допомогою протоколу маршрутизації. Динамічні маршрути можна розділити на дві основні категорії:

- протоколи внутрішньої маршрутизації між шлюзами;

- протоколи зовнішньої маршрутизації між шлюзами.

Протоколи внутрішньої маршрутизації між шлюзами використовуються для вибору маршруту в межах автономної системи, серед яких найпопулярнішими протоколами IGP є RIP, OSPF, IS-IS і EIGRP. Кожен з протоколів маршрутизації має власні метричні та адміністративні відстані. Протоколи зовнішньої маршрутизації між шлюзами використовуються для маршрутизації між різними автономними системами; основним прикладом протоколів зовнішньої маршрутизації між шлюзами є протоколи пограничної маршрутизації між шлюзами. Протоколи маршрутизації можна класифікувати таким чином, як представлено на рис. 1.1.

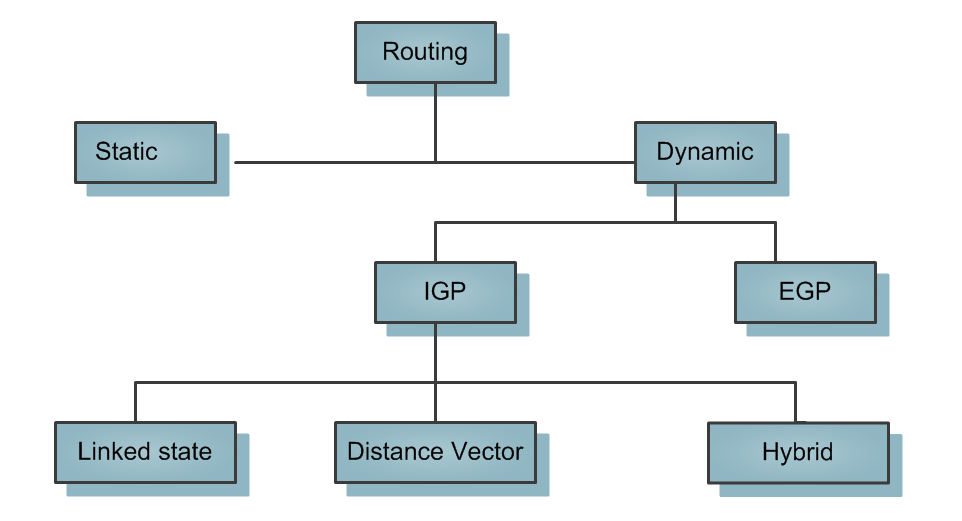


Рисунок1.1 –Приклад класифікації протоколів маршрутизації

**1.3 Статична та динамічна маршрутизація**

У статичній маршрутизації адміністратор мережі налаштовує всі маршрути вручну. Отже, для кожного нового додавання адміністратор мережі повинен додати новий запис маршрутизації. . Щоразу, коли в мережі додається новий маршрут або вузол, це потрібно ввести вручну, і якщо вузол потрібно видалити, це також потрібно зробити вручну. Зазвичай статична маршрутизація використовується для невеликих мереж. При статичній маршрутизації, мережа має більший контроль над мережею. Статична маршрутизація є простою для налаштування та менше використовує процесор та пам’ять, що є одним із основних переваг, але проблема виникає, коли відбувається зміна топології та переналаштування маршруту вручну, що іноді стає дуже проблематичним і це є недоліком статичної маршрутизації. У статичній маршрутизації адміністратор мережі має набагато більше контролю і розуміння мережі, оскільки він вручну встановлює шлях і знає, який шлях надійніший і який шлях вибрати для конкретного типу трафіку. Тоді як поряд з багатьма перевагами протокол динамічної маршрутизації має також певну проблема: у динамічній маршрутизації таблиці маршрутизації формуються динамічно на основі протоколу маршрутизації та алгоритмів розрахунку його шляху. Головним недоліком протоколів динамічної маршрутизації є те, що вони займають більш інтенсивно процесор та пам'ять [2].

Протоколи динамічної маршрутизації мають власні методи та методику встановлення найкращого шляху. Зазвичай поєднані статичні і гібридні протоколи дистанційно-векторної маршрутизації зберігають таблицю топології, в якій усі можливі шляхи до пунктів призначення, що є величезною перевагою будь-якого адміністратора мережі, яку можна використовувати за допомогою протоколу динамічної маршрутизації.

**1.4 Протоколи класової маршрутизації та безкласової маршрутизації**

На основі маски підмережі протоколи маршрутизації розділені на два протоколи маршрутизації, такі як:

- протоколи безкласової маршрутизації;

- протоколи класової маршрутизації.

**1.4.1 Класова маршрутизація**

Існує три основні класи IP-адрес:

1. Клас А з діапазоном від 1-126. У класі A фіксується один октет для частини мережі, де три частини фіксуються для частини хосту. Маска підмережі класу А становить 255.0.0.0.

2. Клас Б з діапазоном від 128-191. У класі B встановлено два октети для частини мережі та два октети зарезервовані для частини хосту. Маска підмережі класу B становить 255.255.0.0.

3. Клас С з діапазоном від 192-223. У класі C три октети зарезервовані для частини мережі і лише один октет зарезервовано для частин хосту.

На рисунку 1.2 зображено приклад мережі, у якій розгорнуто маршрутизацію класів з однаковою мережевою маскою в усіх мережевих розташуваннях.

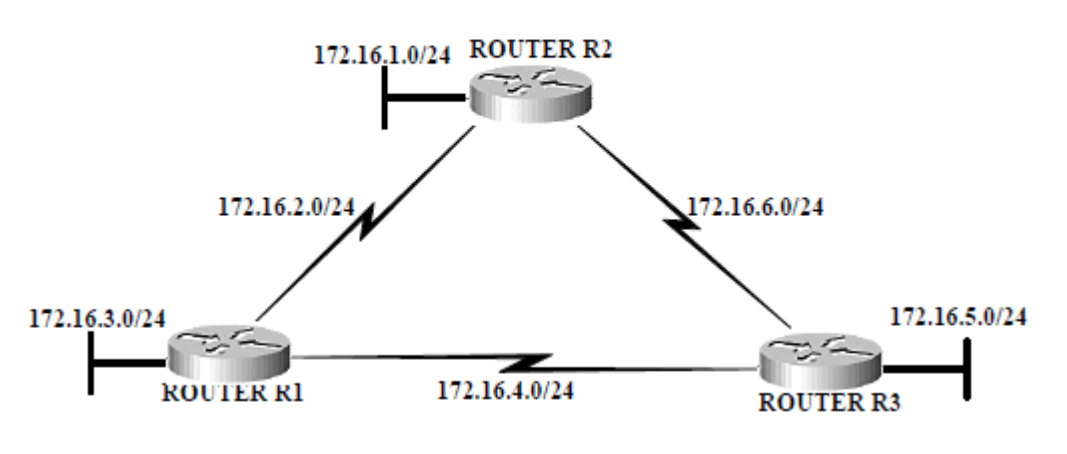


Рисунок 1.2 – Мережа, розгорнута за допомогою класової маршрутизації і маски підмережі

Маршрутизатори використовують ту саму маску підмережі, щоб зрозуміти мережеву адресу, безпосередньо пов’язану з інтерфейсом основної мережі. Коли роутер не пов’язаний безпосередньо з інтерфейсом тієї самої основної мережі, він застосовує класову маска підмережі для маршруту [2]. Протоколи класової маршрутизації мають багато недоліків та не використовуються широко в сучасних мережах:

Ці протоколи не підтримують маски підмережі змінної довжини (VLSM).

Вони не можуть підтримувати розривні мережі.

Ці протоколи не можуть закріпити оновлення маршрутизації. протокол не можна використовувати в мережах з підмережами.

**1.4.2 Безкласова маршрутизація**

Оскільки є обмеження щодо адрес IPV4, тому є багато причин для цього обмеження. Крім того, комерційні класи не є безкоштовними, і кожен, хто користується цими адресами, повинні платити за це. Тому комусь буде дуже важко мати публічні адреси в кожному з розташувань таких, як розподіл адрес IPV4.

В даний час найкращою властивістю будь-якого протоколу маршрутизації є підтримка маскування підмережі змінної довжини. На рисунку 1.3 зображено безкласову мережу, розгорнуту за допомогою маскування підмережі змінної довжини в кожній локації.

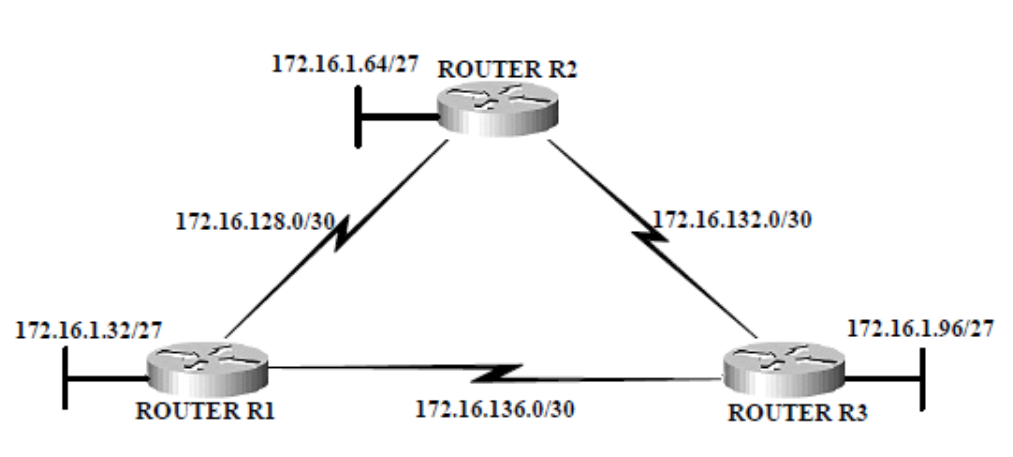


Рисунок 1.3 – Мережа, розгорнута за протоколом безкласової маршрутизації

**1.5 Маршрутизація на основі стану каналів**

Необхідність подолання проблеми з протоколом дистанційної векторної маршрутизації спонукала розробку протоколу маршрутизації на основі стану каналів. Протоколи маршрутизації на основі стану каналів мають такі функції:

- швидка реакція на зміни в мережі замість періодичних оновлень;

- використання активованих оновлень у випадку протоколу маршрутизації з урахуванням стану каналів;

- швидка реакція на будь-яку зміну мережі;

- самовідновлення на мережевому маршруті не працює.

Протокол маршрутизації на основі стану каналів надсилає оновлення лише за будь-яких змін, відбуваються в мережі таким чином, не використовуючи пропускну здатність без потреби. Коли відбувається зміна статусу будь-якого каналу, надсилається оголошення, яке називається повідомленням про стан каналу.

За допомогою повідомленням про стан каналу інформація обмінюється між усіма вузлами. Кожне повідомленням про стан каналу містить інформацію про сусідній пристрій. Будь-яка зміна в каналі повідомляється через повідомлення про стан каналу LSA шляхом лавинної розсилки. Усі вузли можуть підтримувати одну базу даних для всіх маршрутів, відому як таблиця топології. Ці бази даних надають послідовну інформацію про вартість каналу в мережі. Таким чином формується таблиця маршрутизації [3].

Це таблиця маршрутизації, яка містить інформацію про вартість каналу, їхні шляхи та щодо всіх сусідніх вузлів. Для обчислення шлях і вартості для кожного каналу використовується алгоритм Дейкстра. Вартість каналу встановлюється оператором мережі та а представлена як вага або довжина цього конкретного каналу. Балансування продуктивності навантаження досягається після призначення вартості каналу. Тому переповненість ресурсів каналів мережі можна уникнути. Тому оператори мережі можуть змінити маршрутизацію, змінивши вартість каналу. Зазвичай витрати на канал залишаються зі значеннями за замовчуванням, і рекомендується змінити реверс каналу, потім розподілити вагу на каналі. Хоча протоколи на основі стану каналу мають кращу еластичність, вони складні порівняно з протоколами DV. Алгоритм маршрутизації на основі стану каналу представлено на рис.1.4.

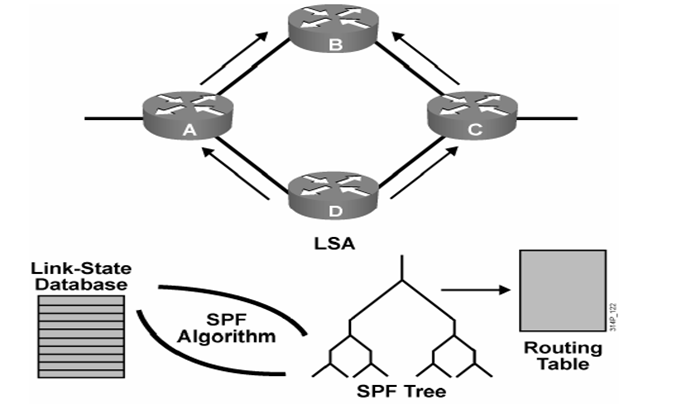
****

Рисунок 1.4 – Алгоритм маршрутизації на основі стану каналу

Існують два протоколи маршрутизації на основі стану каналів: OSPF та інтегрований ISIS. Протоколи маршрутизації на основі стану каналів використовують алгоритм SPF (Shortest Path First Algorithm), відомий як алгоритм Дейкстра. Однак протокол IS-IS використовує лише SPF.

**1.5.1 Характеристики протоколу на основі стану каналів**

Протокол на основі стану каналів має такі характеристики:

- кожен маршрутизатор має ідентичну базу даних;

- забезпечує ієрархічну структуру;

- включає та підтримує кілька шляхів у таблиці топології до місця призначення;

- ефективна та швидка конвергенція без петель;

- має набагато точніші показники.

**1.5.2 Методи маршрутизації на основі стану каналів**

Маршрутизація на онові стану каналів складається з наступних етапів [3]:

- кожен маршрутизатор отримує інформацію про безпосередньо підключені сусідні мережі і їх безпосередньо зв'язані канали;

- кожен маршрутизатор зберігає інформацію про пакет стану каналу, отриманий від свого сусіднього маршрутизатора;

- кожен маршрутизатор встановлює шлях мінімальної вартості для топології мережі;

- кожен маршрутизатор повинен мати з’єднання з безпосередньо підключеним сусіднім маршрутизатором, що належить мережам, і це зазвичай виконується через обмін пакетами ARP;

- кожен маршрутизатор повинен надсилати інформацію про стан каналу.

**1.5.3 Сильні та слабкі сторони маршрутизації на основі стану каналів**

У протоколах маршрутизації на основі стану каналів маршрутизатори обчислюють маршрути автономно, а також є автономними від розрахунку проміжних маршрутизаторів. Сильні сторони протоколів маршрутизації на основі стану каналів полягають в наступному:

- вони швидко реагують на будь-які зміни підключення;

- розмір пакету дуже малий.

Основними недоліками протоколів маршрутизації на основі стану каналів є:

- інтенсивне використання пам'яті;

- складне налаштування розуміння;

- використання складного алгоритму;

- використання більш інтенсивного процесора

-зазвичай невдалий через гнучкість змін каналів.

**1.6 Дистанційно-векторна маршрутизація**

Основним прикладом протоколів дистанційного вектору або маршрутизації є протокол маршрутної інформації (RIP). Протокол дистанційно-векторної маршрутизації, як випливає з назви, розглядає два основні параметри для визначення найкращого маршруту: це відстань і вектор. Дистанційні засоби «Наскільки далеко» та «Вектор» означають, у якому напрямку. RIP версії 1 і RIP версії 2 використовують алгоритм Беллмана-Форда. Адміністративна відстань RIP становить 120. Адміністративна відстань – це ступінь надійності будь-яких протоколів маршрутизації [4].

Чим меншою буде адміністративна відстань, тим більшою буде надійність протоколів маршрутизації. Метрикою протоколів інформації про маршрутизацію є «підрахунок переходів». Метрика є критерієм прийняття рішень будь-якого протоколу маршрутизації. RIP зазвичай використовується для менших мереж, а його межа стрибків становить 15.

Маршрутизатори, що використовують метод вектору відстані, мають лише інформацію, яку передають сусідньому маршрутизатору. Протоколи маршрутизації на основі вектору відстані використовують періодичні оновлення замість активованого оновлення.

Протокол дистанційно-векторної маршрутизації має багато проблем. Однією з проблем, пов’язаних з протоколом маршрутизації на основі вектору відстані, полягає в тому, що маршрутизатор не обізнаний про повну топологію.

Нижче на рисунку 1.5 показано, як маршрути вивчаються протоколами дистанційної - векторної маршрутизації та дає змогу набагато легше зрозуміти проблеми, пов’язані з протоколами маршрутизації на основі вектору відстані, такі як розщеплений горизонт, псування маршруту тощо.

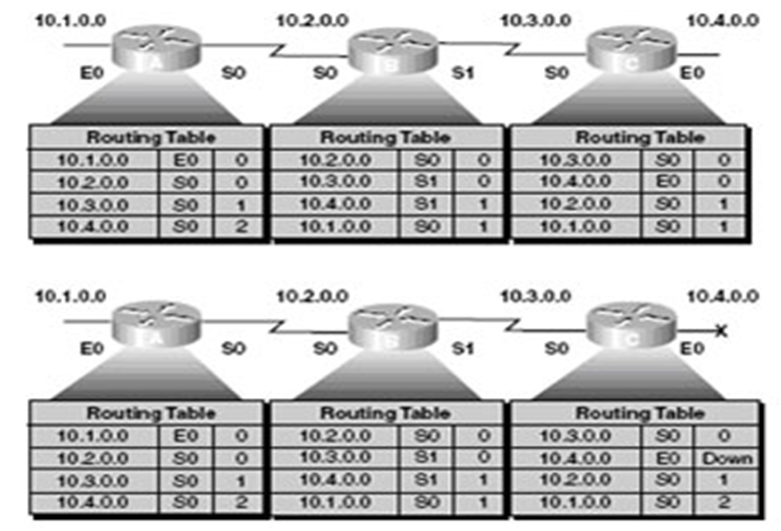


Рисунок 1.5 – Маршрутизація на основі вектору відстані

**1.6.1 Характеристики дистанційно-векторної маршрутизації**

Характеристики протоколу дистанційно-векторної маршрутизації є наступними [4]:

- протокол дистанційно-векторної маршрутизації визначає свою власну таблицю маршрутизації, де знаходяться всі сусідні маршрутизатори безпосередньо з’єднані з таблицею протягом постійного періоду;

- нову інформацію слід розміщувати в кожній таблиці маршрутизації миттєво, коли маршрути становляться недоступними;

- протоколи дистанційно-векторної маршрутизації прості й ефективні в невеликих мережах і, отже, потребують невеликого управління;

- маршрутизація на основі вектору відстані в основному базується на векторі кількості переходів;

- алгоритм «Вектор відстані» є ітераційним.

**1.6.2 Плюси і мінуси** **дистанційно-векторної маршрутизації**

Перевагами протоколів дистанційно-векторної маршрутизації є:

- протоколи дистанційно-векторної маршрутизації не використовують складних алгоритмів і працюють дуже ефективно для невеликих мереж;

- дистанційну-векторну маршрутизацію легко реалізувати;

- використовують менше пам'яті та процесора порівняно з протоколами маршрутизації на основі стану каналів.

Протокол дистанційно-векторної маршрутизації має багато проблем. Такі проблеми як псування маршруту, розділений горизонт, рахування до нескінченності та петлі маршрутизації є головними недоліками дистанційно-векторної маршрутизації. Дистанційно-векторна маршрутизація використовує алгоритми Беллмана-Форда, які не є ефективними алгоритмами.

Деякі з найпопулярніших проблем дистанційно-векторної маршрутизації наступні:

- можливість утворення петель маршрутизації;

- використання періодичних оновлень потребує часу для конвергенції;

- протоколи дистанційно-векторної маршрутизації мають ліміт переходів;

- алгоритм Беллмана-Форда не використовує розширені показники, такі як протоколи пов’язаного стану.

**2 ПОРІВНЯННЯ ПРОТОКОЛІВ** **ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ**

**У КОМП’ЮТЕРНІЙ МЕРЕЖІ**

В цьому розділі розкрито найбільш суттєві критерії порівняння протоколів та фактори, що впливають на їх вибір у корпоративній мережі, а також наведено коротку порівняльну характеристику протоколів та деякі загальні рекомендації щодо їх застосування

**2.1 Вимоги корпоративної мережі до протоколу маршрутизації**

Як відомо, протоколи динамічної маршрутизації дозволяють маршрутизаторам IP-мереж автоматично створювати таблиці оптимальних (за обраним критерієм) маршрутів і динамічно змінювати їх відповідно до змін топології мережі. Вибір протоколу маршрутизації багато в чому залежить від наступних факторів [5]:

- топологія та складність мережі. Необхідно передбачити наявність резервних ліній зв'язку в мережі, що забезпечує її надійне функціонування (наявність серверів і сегментів мережі) у разі збоїв мережевого обладнання та магістральних ліній зв'язку. Наприклад, при деревоподібній топології мережі з так званим «кореневим маршрутизатором» можливості динамічної маршрутизації зведені до мінімуму;

- розмір мережі та необхідність подальшого масштабування. Можливості деяких протоколів у цьому відношенні обмежені;

- чисте навантаження. Для мереж з високим коефіцієнтом завантаження ліній зв'язку важлива здатність протоколу перерозподіляти потоки даних;

- вимоги до надійності мережі. Дозволений термін простою або нестабільності в роботі мережі внаслідок виходу з ладу її вузлів залежить від виду діяльності організації і визначається можливими фінансовими втратами або небезпекою порушення виробничого циклу;

- вимоги до захисту інформації в мережі. Вимоги визначаються ступенем ризику, пов'язаного з потраплянням інформації про адреси та маршрути в мережі до рук зловмисників, що особливо важливо для мереж, які мають зовнішні канали зв'язку;

- необхідність підключення маршрутизованого сегмента до вже існуючої мережі. В цьому випадку слід звернути увагу на сумісність протоколів маршрутизації та засобів їх реалізації;

- можливість організації програмних маршрутизаторів. При малому трафіку в мережі або окремих її ділянках висока продуктивність від маршрутизаторів не потрібна. У таких випадках може бути економніше використовувати комп’ютер загального призначення з кількома мережевими картами та програмним забезпеченням із функціями протоколу маршрутизації замість апаратного маршрутизатора. Однак не всі протоколи маршрутизації мають відповідне програмне забезпечення, а кількість споживаних обчислювальних ресурсів комп'ютера залежить від складності протоколів;

- кваліфікація та суб'єктивні переваги обслуговуючого персоналу. Складність налаштування маршрутизаторів і адміністрування мережі при використанні різних протоколів істотно відрізняється. Якщо необхідні можливості є в декількох протоколах, важливо враховувати зручність і досвід роботи з одним з протоколів адміністратора мережі.

**2.2 Основні критерії порівняння протоколів маршрутизації**

У конкретній мережі необхідно провести порівняльний аналіз найбільш відомих протоколів динамічної маршрутизації.

Протоколи маршрутизації поділяються на два основні класи: протоколи внутрішніх шлюзів (Interior Gateway Protocols - IGP) і протоколи зовнішніх шлюзів (Exterior Gateway Protocols - EGP). Протоколи класу IGP призначені для обміну інформацією про мережі та підмережі між внутрішніми маршрутизаторами однієї автономної системи (autonomous system - AS), та між маршрутизаторами під одним адміністративним контролем, які використовують той самий протокол маршрутизації. Такими мережами можуть бути мережі інтернет-провайдерів, великих урядових і дослідницьких організацій, приватних бізнес-концернів. Протоколи EGP призначені для обміну інформацією про маршрутизацію між прикордонними маршрутизаторами різних автономних систем. Домінуючим EGP-протоколом на сьогодні є протокол граничної маршрутизації версії 4 - BGP-4). Цей протокол використовується для обміну інформацією про маршрут між AS мережі Інтернет.

За способом розподілу маршрутної інформації протоколи IGP поділяються на дистанційно-векторні та стани каналів зв'язку. У методі вектору відстані кожен маршрутизатор періодично надсилає оновлення всієї або частини своєї таблиці маршрутизації сусіднім маршрутизаторам. Оскільки інформація про маршрути поширюється по всій мережі, кожен маршрутизатор може розраховувати відстань від нього до всіх мереж і підмереж внутрішньо фірмової мережі. Найпоширенішими протоколами цього типу є RIP (Routing Information Protocol) і IGRP (Interior Gateway Routing Protocol). У методиці обліку стану каналів зв'язку, кожен маршрутизатор корпоративної мережі надсилає інформацію про прямі підключення до мереж і маршрутизаторів іншим маршрутизаторам. На основі отриманої інформації про всі локальні з'єднання в мережі кожен маршрутизатор здатний побудувати весь свій топологічний граф, а потім заповнити його таблицю складним алгоритмом вибору найкоротшого шляху (Shortest Path First - SPF).

Найвідомішими протоколами цього типу є OSPF (Open Shortest Path First) і IS-IS (Intermediate System to Intermediate System). Існують також гібридні протоколи, які поєднують переваги обох методів розподілу маршрутної інформації. Прикладом гібридного протоколу є EIGRP (Enhanced Interior Gateway Routing Protocol) [5].

Протоколи на основі методу вектору відстані вимагають менше обчислювальних ресурсів маршрутизатора, ніж протоколи зі збереженням стану з їх складними алгоритмами SPF. З іншого боку, протоколи зі збереженням стану займають меншу пропускну здатність мережі (за винятком початкової фази вивчення топології мережі), оскільки вони передають лише інформацію про зміни, а не всю таблицю маршрутизації, що особливо важливо для великих мереж.

Інші критерії для порівняння протоколів динамічної маршрутизації включають:

- швидкість сходження. Ця характеристика протоколу визначає тривалість інтервалу часу можливої ​​нестабільної роботи мережі, протягом якого протокол виявляє недоступний маршрут, вибирає новий маршрут і поширює нову інформацію по мережі. Швидкість реакції на зміни в топології мережі особливо важлива при підтримці критично важливих додатків, які вимагають високого ступеня доступності мережі. Протоколи на основі методу вектору відстані вимагають більше часу для конвергенції, ніж протоколи зі збереженням стану, оскільки інформація про новий маршрут передається від одного маршрутизатора до іншого опосередковано без вказівки джерела її походження в процесі періодичних трансляцій;

- можливість врахувати різні характеристики маршруту в метриці (критерії) для вибору найбільш раціонального маршруту. Показники можна розрахувати на основі однієї або кількох характеристик маршруту. До найбільш часто використовуваних характеристик маршруту відносяться: кількість переходів (проміжних маршрутів на шляху); пропускна здатність каналів зв'язку; затримка пакета в дорозі; надійність (частота помилок у каналах зв'язку); Load (завантаженість маршрутизаторів і каналів зв'язку); Ціна (довільне значення, яке призначає адміністратор на основі як вищезазначених, так і інших міркувань, наприклад, фінансових). Метрики, розраховані на основі кількох показників, забезпечують велику гнучкість при виборі маршруту. Можливості протоколу підтримувати декілька метрик одночасно дозволяють задовольнити потреби QoS-трафіку (якості обслуговування) різних програм;

- можливість балансування навантаження між кількома маршрутами. Можливість зберігати в таблицях маршрутизації кілька маршрутів до однієї мережі (з однаковими або навіть різними показниками) дозволяє маршрутизатору зменшити навантаження на лінії зв'язку шляхом поперемінної відправки пакетів по кожному з маршрутів. Слід зазначити, що балансування навантаження може викликати проблеми у випадках, коли програма використовує протоколи дейтаграм канального та транспортного рівнів, які не нумерують і, отже, не змінюють порядок пакетів, як, наприклад, транспортний протокол із встановленням Union. TSR.

- можливість комбінування маршрутів на ділянках, що перекриваються. Наявність цієї функції сприяє зниженню відносної складності великої мережі, зменшенню кількості записів у таблицях маршрутизаторів і прискоренню пошуку в них. Агрегація маршрутів вимагає, щоб протокол маршрутизації підтримував маски підмережі змінної довжини та міг поширювати інформацію про маску мережі разом із інформацією про мережевий маршрут;

- максимальна кількість маршрутизаторів у мережі визначає її можливості масштабування. Це обмеження опосередковано пов'язане з іншими характеристиками протоколу маршрутизації, які впливають на його здатність працювати у великій мережі (наприклад, швидкість конвергенції, частка пропускної здатності мережі, необхідна для передачі службових повідомлень протоколу);

- необхідність попередньої логічної підготовки мережі. Деякі протоколи маршрутизації для досягнення відповідного рівня масштабування (зменшення споживання обчислювальних ресурсів маршрутизаторів і пропускної здатності мережі) мають на увазі виділення логічних областей в мережі і з'єднань між ними. Використання таких протоколів може вимагати серйозної розробки проекту мережі (його топології та схем адресації);

- забезпечення безпеки під час обміну маршрутною інформацією. Якщо мережа підтримує обмін інформацією про маршрутизацію між підмережами, з’єднаними глобальним зв’язком, така інформація, потрапляючи в руки зловмисників, може становити загрозу безпеці мережі. У таких випадках підтримка протоколу маршрутизації для методів автентифікації джерела та шифрування інформації маршрутизації стає важливою;

- наявність програмного забезпечення (ПЗ) для реалізації протоколу маршрутизації. Проколи можуть бути відкритими і підтримуватися різними виробниками апаратних маршрутизаторів і програмного забезпечення для універсальних комп'ютерів, і можуть бути закриті і реалізовані тільки певними організаціями;

- перспективність — реалізація протоколу перспективних напрямків (наприклад, протоколу IP6, підтримка трафік інжинірингу).

**2.3 Коротка характеристика найбільш поширених протоколів маршрутизації**

Нижче наведено такі найбільш поширені протоколи маршрутизації:

- **RIP**. Протокол RIP на основі алгоритму вектору відстані в більшості реалізацій використовує найпростішу метрику - кількість проміжних маршрутизаторів до мережі призначення. Його трафік стабілізується та швидко відправляє передачу пакета по іншому з'єднанню, переконавшись про низький рівень мережі. Для того, щоб отримати позитивні результати; дослідники (Fulkerson, 1962, і Bellman, 1957) запропонували періодично оновлювати таблицю маршрутизації кожним маршрутизатором. Кожен маршрутизатор відправляє всю радикальну інформацію у таблиці маршрутизації на сусідні маршрутизатори. Для оновлення таблиці маршрутизації в кожному маршрутизаторі, коли вектор відстані отримує дані від сусіднього маршрутизатора, протокол шукатиме зміни у порівнянні з попереднім вектором відстані. З цієї причини в результаті покращилсь маршрутизація за допомогою таймерів та процесу оновлення маршрутизації, так як топологія оновлює таблицю маршрутизації з використанням таймерів [6].

Переваги статичної маршрутизації з використанням RIP прості, але оновлення не оновлюються вручну, коли змінюється структура. Основною перевагою цього протоколу є простота налаштування, яка не потребує висококваліфікованого обслуговуючого персоналу. Цей протокол відкритий і підтримується практично всіма виробниками мережевого обладнання. Існують також реалізації цього протоколу в програмному забезпеченні (наприклад, для Unix-подібних ОС - пакети Zebra, Kawaga тощо) і підтримка у низці ОС (наприклад, в Windows, починаючи з Windows NT Server, Unix-подібних , Cisco IOS). Основними недоліками цього протоколу є: повільна конвергенція та великий обсяг службового трафіку (для адаптації до змін топології мережі маршрутизатори періодично надсилають повні копії своїх таблиць). Це обмежує сферу застосування цього протоколу. Протокол використовується для мереж з числом маршрутизаторів не більше п'ятнадцяти .У RIP версії 2 додана підтримка маски змінної довжини, багатоадресної розсилки (multicasting) замість широкомовної розсилки, а також заходи безпеки при обміні інформацією про маршрутизацію у вигляді аутентифікації ключа MD5 і clear. На рис. 2.1 показаний приклад корпоративної мережі на основі протоколу RIP.

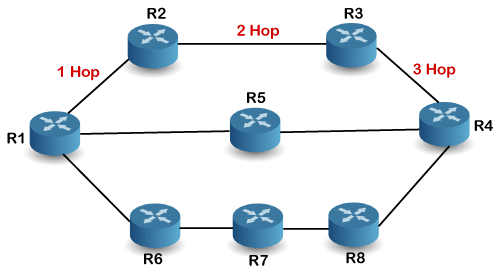


Рисунок 2.1 - Приклад корпоративної мережі за протоколом RIP

Протокол досить поширений у невеликих локальних мережах, що не прагнуть до розширення, з невисокими вимогами до надійності мережі та відсутністю кваліфікованого персоналу мережевих адміністраторів. У новій версії Riping організована підтримка протоколу IPv6;

**- IGRP**. Векторний протокол замкнутої відстані IGRP від ​​Cisco Systems був розроблений для усунення багатьох недоліків RIP і мав на меті забезпечити кращу підтримку великих мереж (до 255 маршрутизаторів), які містять канали зв’язку з різною пропускною здатністю та характеристиками затримки. Протокол використовує комбінацію показників, які включають затримку, пропускну здатність, надійність і завантаження маршруту. Коефіцієнти ваги, які визначають внесок характеристик в результуючу метрику, встановлюються користувачем, забезпечуючи гнучку адаптацію до дуже конкретних завдань. Індикатори затримки та пропускної здатності попередньо налаштовані для кожного посилання, а показники надійності та навантаження можна розрахувати в процесі обробки реального мережевого трафіку. Щоб підтримувати вимоги QOS різних додатків, можна підготувати кілька таблиць маршрутизації на основі метрик з різними ваговими значеннями [6].

За замовчуванням IGRP є набором метрик секторної затримки та мінімальної пропускної здатності сегмента (тобто максимальна кількість переходів до 255 (за замовчуванням 100), а оновлення маршрутів оголошуються кожні 1,5 хвилини). Для IGRP у мережах зв'язку зарезервовано Протокол № 9.

Оскільки IGRP є безкласовим протоколом, який не містить поле маски підмережі, маршрутизатор припускає, що всі адреси підмережі меншого класу A, B і мережі C мають однакову маску підмережі. Це не стосується безкласових протоколів маршрутизації, які можуть використовувати маски підмережі різної довжини.

Протокол IGRP забезпечує більш швидку конвергенцію, ніж RIP, завдяки використанню пакетів оновлення з миттєвим розподілом (інформація про зміни в мережі надсилається, як тільки вона стає доступною, не чекаючи часу наступного оновлення). Цей протокол підтримує балансування навантаження між кількома маршрутами, навіть якщо їхні показники не збігаються, але знаходяться в межах певного діапазону показників найкращого маршруту. При цьому співвідношення обсягів даних, що надсилаються по кожному шляху даних, буде пропорційним співвідношенню їх метрик. На рисунку 2.2 наведено приклад корпоративної мережі з застосуванням протоколу IGRP.

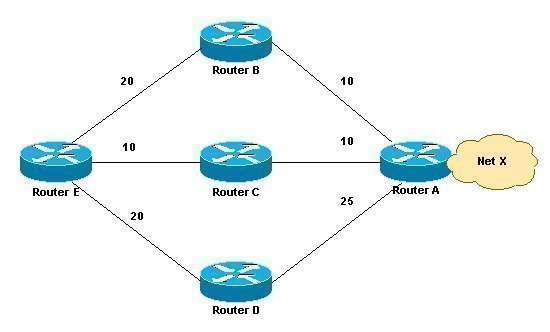


Рисунок 2.2 - Приклад корпоративної мережі з застосуванням протоколу IGRP

До недоліків протоколу можна віднести відсутність підтримки масок підмереж змінної довжини та можливості об'єднання маршрутів. Періодичні трансляції інформації про маршрутизацію на сусідні маршрутизатори залишаються широкомовними. Заходи безпеки обмежені. Під час обміну інформацією про маршрут відсутні засоби автентифікації. Непрямим засобом захисту є можливість приймати повідомлення про оновлення маршруту лише від маршрутизаторів, які маршрутизатор визначає як «сусідів», а також можливість вносити зміни в конфігурацію маршрутизатора лише на основі пароля, який зберігається в зашифрованому вигляді. Цей протокол сумісний з RIP;

- **EIGRP**. Протокол Cisco Systems EIGRP є вдосконаленою версією оригінального протоколу IGRP. Протокол є гібридним і оснований на алгоритмі дифузійного оновлення (DUAL). Він поєднує в собі найкращі сторони дистанційно-векторних протоколів (простота алгоритму вибору оптимального маршруту) і протоколів стану каналів зв'язку (швидка конвергенція та економія пропускної здатності мережі за рахунок повідомлень лише про стан з'єднань та їх зміну). Усі трансляції протоколу є багатоадресними або одноадресними. Таким чином, інформація надсилається лише для змін і лише тим маршрутизаторам, яких вони стосуються. Для збільшення масштабу протоколу в нього додана підтримка масок підмережі змінної довжини і можливість комбінування маршрутів. Маршрути поділяються на внутрішні та зовнішні - отримані з інших протоколів маршрутизації або записані в таблицю статично [7].

Протокол IGRP був створений у 1992 році, який був розширений вектором відстані. IGRP і EIGRP налаштовані на маршрутизаторах Cisco та мають власне Cisco. EIGRP може динамічно виявляти маршрутизатори, підключений безпосередньо до мережі. Enhanced Interior Gateway Routing Protocol не залежить від періодичних оновлень, оскільки конвергенції в топології, але створює схему з оголошеннями про зміни в топології. Дані присутні як у протоколах для вектору відстані. Структурна схема обробляється для визначення найбільш прийнятного способу для кожної мережі призначення. Розширений внутрішній протокол маршрутизації шлюзу реалізує алгоритм під назвою (DUAL) Deployment Update Algorithm. На рисунку 2.3 наведено приклад корпоративної мережі на основі протоколу EIGRP.

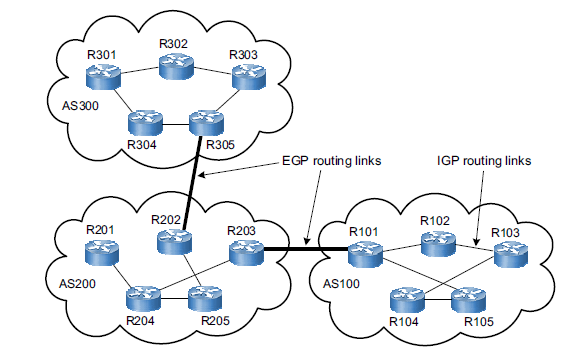


Рисунок 2.3 - Приклад корпоративної мережі за протоколом EIGRP

Останні версії EIGRP містять заходи безпеки, які запобігають додаванню зловмисниками записів до таблиці маршрутизації та автентифікації ключа MD5. Крім того, зараз розробляється підтримка IPv6 для EIGRP, тому цей протокол продовжуватиме розвиватися. Основним недоліком EIGRP, як і його попередника, є його закритість і реалізація тільки на обладнанні Cisco Systems. Цей протокол добре сумісний з IGRP і RIP;

- **OSPF**. Найбільш універсальним і гнучким протоколом динамічної маршрутизації в корпоративних мережах на сьогоднішній день є Open Shortest Path First Protocol (OSPF). Спочатку протокол призначався для роботи у великих мережах (до 65 536 маршрутизаторів) зі складною топологією. Він оснований на алгоритмі стану каналів зв'язку і має високу стійкість до змін топології мережі і швидку конвергенцію. При виборі маршруту використовується показник пропускної здатності складної мережі (тобто передача даних на найшвидші канали зв'язку).

SPF — це інженерна робоча група Інтернету (IETF), розроблена робочою групою IGP [8]. Ця група була створена в 1988 році для розробки IGP на основі вперше використаного алгоритму найкоротшого шляху.

Кожен маршрутизатор підключається до іншого маршрутизатора поруч із ним, вибіркове затоплення надсилатиме ці пакети туди, куди вони передаються на маршрутизатор призначення та оновлюють їхню таблицю маршрутизації

за допомогою внутрішньої продуктивності синхронізації кожні 30 хвилин.

Протокол може підтримувати різні вимоги QoS IP-пакетів (пропускна здатність, затримка та надійність), будуючи окрему таблицю маршрутизації для кожної з цих метрик.

Цей протокол має й інші переваги, корисні у великих сучасних мережах. Вони включають можливість балансування навантаження між каналами з однаковими метриками та засобами аутентифікації як за незашифрованим паролем, так і за зашифрованим (шляхом додавання ключа та тіла пакету до дайджест-пакету за алгоритмом MD5). Нумерація пакетів виключає їх повторення і тим самим можливість повторних атак. Відкритість протоколу обумовлює його підтримку практично всіма виробниками мережевого обладнання, впровадження в програмне забезпечення для всіх популярних ОС (наприклад, для Unix-подібних ОС - пакети Zebra, Kawaga і т.д.), а також пряму інтеграцію з рядом ОС (наприклад, Windows 2000 Server і вище, OpenBSD, Cisco IOS, Solaris 10 тощо).

Серед недоліків протоколу можна заначити високу обчислювальну складність і, отже, високі вимоги до ресурсів маршрутизатора. Обчислювальна складність OSPF зростає зі збільшенням розміру мережі. Тому для підвищення масштабованості протоколу використовується поділ мережі на логічні області, з'єднані магістральною областю. Внутрішня топологічна інформація між регіонами не надається. Для зменшення розміру таблиць маршрутизації і зниження службового трафіку при оновленні топологічної інформації передбачена можливість об'єднання декількох мережевих адрес в одну при наявності у них загального префіксу і заміни широкомовних трансляцій на багатоадресну [8].

На рис. 2.4 наведено приклад корпоративної мережі з використанням протоколу OSPF.

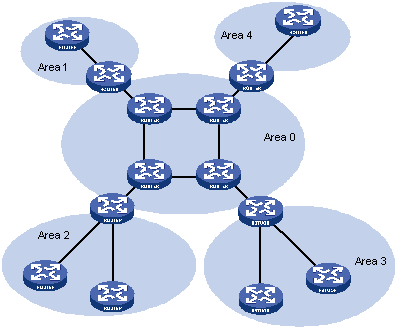


Рисунок 2.4 - Приклад корпоративної мережі з застосуванням протоколу OSPF

Щоб зберегти IP-адреси в з’єднаннях «точка-точка» між маршрутизаторами, немає необхідності призначати адреси кінцевим точкам. Ціною за ці переваги є складність конфігурації та необхідність ретельного планування мережі для її оптимальної роботи (розбивка на зони, вибір магістралі, розподіл функцій між маршрутизаторами з урахуванням їх обчислювальної потужності: загальні, виділені в зону, граничні тощо).

Перспективними особливостями OSPF слід назвати підтримку протоколу IPv6 і можливість вибору маршруту на основі поточного коефіцієнта завантаження каналів зв'язку (розширена версія OSPF отримала назву Constrained Shortest Path First - SSPF). Цей протокол сумісний з RIP;

- **IS-IS.** Протокол IS-IS оснований на алгоритмі стану каналу і є попередником OSPF. В даний час цей протокол рідко використовується в корпоративних мережах. Це пояснюється повною перевагою перед ним протоколу OSPF, який, по суті, є вдосконаленим IS-IS. На рис. 2.5 наведено приклад корпоративної мережі з використанням протоколу IS-IS.

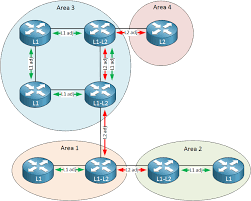


Рисунок 2.5 - Приклад корпоративної мережі з застосуванням протоколу IS-IS

До недоліків протоколу належить його нездатність підтримувати маски підмереж змінної довжиною, об'єднанням маршрутів, а також широкомовним характер розсилок сусіднім маршрутизаторам.

Все це негативно позначається на швидкості конвергенції, завантаженості маршрутизаторів і завантаженості ліній зв'язку;

- **БГП-4.** Протокол BGP був розроблений як зовнішній протокол для організації маршрутизації між автономними системами в глобальній мережі Інтернет (максимальна кількість маршрутизаторів 65534 між AS). Зараз в Інтернеті використовується версія 4 протоколу BGP-4. Хоча цей протокол відноситься до зовнішніх протоколів маршрутизації, іноді він також використовується для внутрішньої маршрутизації [9].

BGP — це протокол, орієнтований на вектор відстані. Однак, на відміну від RIP і IGRP, BGP не вимагає періодичного оновлення всієї таблиці маршрутизації. Повні таблиці обмінюються між маршрутизаторами лише тоді, коли вони спочатку підключені. Потім надсилаються лише повідомлення про оновлення таблиці, і лише маршрутизаторам, які явно визначені як сусіди. Одне оновлення BGP-4 може оголосити один новий маршрут або скасування кількох застарілих маршрутів. Все це сприяє зниженню трафіку служби.

Метрика BGP — це довільна кількість одиниць, яка характеризує ступінь переваги певного маршруту та встановлюється адміністратором мережі, в основному на основі договірних і фінансових переваг, можливо, з урахуванням інших факторів (за замовчуванням на основі мінімальної кількості проміжних AS). Різні маршрутизатори можуть використовувати різні політики маршрутизації. Хоча BGP підтримує таблицю маршрутизації всіх можливих шляхів до певної мережі, він рекламує лише оптимальні маршрути у своїх повідомленнях про налаштування. Наявність альтернативних маршрутів в таблиці прискорює реакцію маршрутизатора на інформацію про недоступність основного шляху і навіть дозволяє підтримувати балансування навантаження. Оскільки протокол орієнтований на обмін даними між різними AS, де під час вибору маршрутів зазвичай переважають не технічні, а політичні міркування, процес балансування навантаження передбачає змістовний розподіл маршрутів між альтернативними каналами шляхом налаштування відповідних параметрів цього протоколу.

Повідомлення BGP-4 про коригування містять послідовність AS, через яку можна досягти вказаної мережі, її IP-адреси та довжини маски префіксу (підтримується лише безкласова адресація SDR).

Цей протокол дозволяє комбінувати маршрути. Список AS використовується для поліпшення конвергенції, швидкість якої не висока [10].

Для забезпечення безпеки можна використовувати різні методи автентифікації маршрутизатора. Цей протокол сумісний з RIP і OSPF. На рис. 2.6 наведено приклад корпоративної мережі з використанням протоколу BGP.

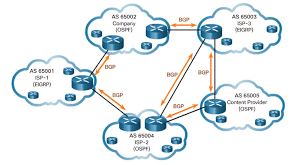


Рисунок 2.6 - Приклад корпоративної мережі з використанням протоколу BGP

**2.4 Порівняльна характеристика протоколів маршрутизації OSPF і BGP**

Протокол OSPF — це тип ієрархічної топології або структури мережі. OSPF віддає перевагу найшвидшому шляху, а не найкоротшому. У Open Shortest Path First використовується Інтернет-протокол. Він використовує алгоритм маршрутизації стану зв’язку (LSR) для своєї функціональності.

OSPF — це внутрішній протокол шлюзу (IGP), за допомогою якого маршрутизатори з’єднують мережі за допомогою Інтернет-протоколу (IP). Це протокол маршрутизатора, який використовується для пошуку найкращого шляху для пакетів, коли вони одночасно проходять через набір підключених мереж. Головним недоліком OSPF є те, що він складніший за інші протоколи. На рис.2.7 представлено структуру мережі за протоколом OSPF.

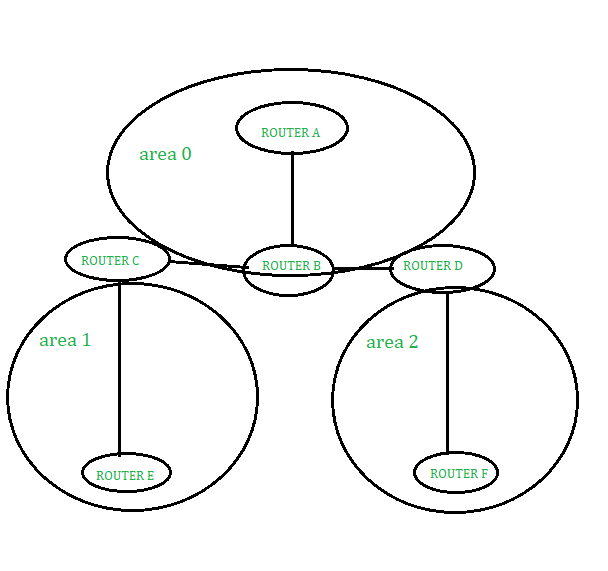


Рисунок 2.7 - Структура мережі за протоколом OSPF

Протокол BGP – це тип сітчастої топології або структури Протокол граничного шлюзу віддає перевагу найкращому шляху. У протоколі граничного шлюзу використовується протокол керування передачею. Основна відмінність між OSPF (Open Shortest Path First) і BGP (Border Gateway Protocol) полягає в тому, що Open Shortest Path First є протоколом маршрутизації всередині домену, тоді як Border Gateway Protocol є протоколом маршрутизації між доменами.

Наприклад, якщо користувач з Індії завантажує веб-сайт із вихідними серверами в Сінгапурі, то цей протокол BGP є таким протоколом, який забезпечує швидке та ефективне спілкування. Іншим прикладом є те, що якщо хтось надсилає будь-які дані через Інтернет, протокол BGP відповідає за весь доступний шлях, яким дані можуть переміщатися. На рис.2.8 представлено структуру мережі за протоколом BGP.

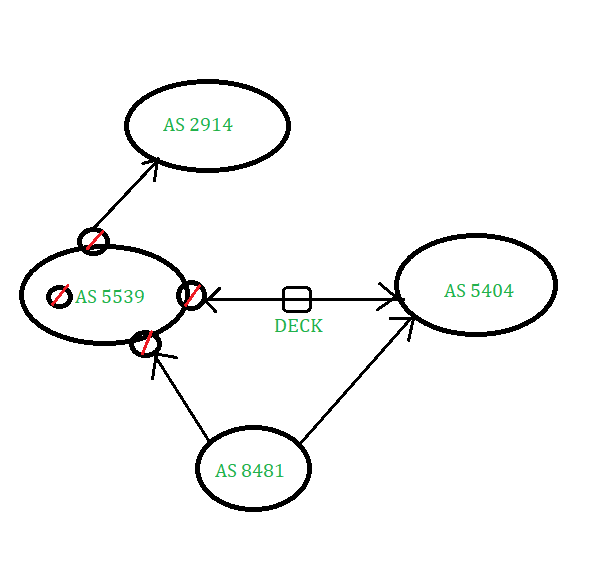


Рисунок 2.8 - Структура мережі за протоколом BGP (тут усі префікси приймаються в AS5539, який позначається значенням спільноти:

5539:500 = клієнт, 5539:100 = піринг (decix), 5539:250 = вгору (NTT)

Також відмінність між OSPF і BGP полягає в тому, що OSPF — це внутрішньо доменний протокол маршрутизації, який використовує маршрутизацію стану зв’язку, і операція маршрутизації виконується всередині автономної системи, тоді як BGP — це між доменний протокол маршрутизації, який використовує векторну маршрутизацію шляху, з маршрутизацією операції, що виконуються між двома автономними системами.

В таблиці 2.1 підсумовано відмінності між протоколами OSPF і BGP.

Таблиця 2.1 – Відмінності між протоколами OSPF і BGP

|  |  |  |  |
| --- | --- | --- | --- |
| №  за/п | Характеристики протоколів OSPF і BGP | OSPF | BGP |
| 1 | Протокол шлюзу | Протокол внутрішнього шлюзу | Протокол зовнішнього шлюзу |
| 2 | Реалізація | Легка | Складна |
| 3 | Конвергенція | Швидка | Повільна |
| 4 | Структура | Можливість проектування ієрархічної мережі | Сітчаста |
| 5 | Потреба в ресурсах | Пам’ять і інтенсивні обчислення | Масштабування пам’яті та процесора краще в BGP, хоча воно залежить від розміру таблиці маршрутизації |
| 6 | Розмір мереж | Використовується переважно в мережі меншого масштабу, якою можна керувати централізовано | Переважно використовується у великих мережах, таких як Інтернет |
| 7 | Функція | Найшвидший маршрут має перевагу над найкоротшим | Найкращий шлях визначається для датаграми |
| 8 | Використаний алгоритм | Алгоритм Дейкстри | Алгоритм найкращого шляху |
| 9 | Протокол | IP | TCP |

Деякі інші відмінності між OSPF і BGP включають наступні:

- конфігурація: OSPF легко налаштувати, тоді як конфігурація BGP є набагато складнішою;

- швидкість конвергенції: OSPF може швидше досягти конвергенції (часу, який маршрутизатор потребує для обміну й оновлення останньої інформації про маршрутизацію). Навпаки, BGP має повільну швидкість конвергенції;

- топологія чи структура мережі: OSPF — це тип ієрархічної топології або дизайну мережі, тоді як BGP — тип сітчастої топології або структури мережі;

- вимоги до ресурсів: OSPF потребує інтенсивного використання пам’яті та ресурсів ЦП. З іншого боку, з BGP розмір таблиці маршрутизації визначає необхідні ресурси пристрою.

- масштаб: BGP є більш гнучким і масштабованим, ніж OSPF, і він також використовується у більшій мережі.

- бажаний шлях: OSPF використовується для визначення найшвидшого маршруту, тоді як BGP наголошує на визначенні найкращого шляху.

- протокол: в OSPF використовується Інтернет-протокол. У BGP використовується протокол керування передачею.

**3 ЗАХОДИ ДЛЯ УДОСКОНАЛЕННЯ ПРОТОКОЛУ МАРШРУТИЗАЦІЇ OSPF**

Open Shortest Path First (OSPF) — це популярний протокол внутрішнього шлюзу, який широко використовується у великих доменах IP-маршрутизації. Нещодавні дослідження показали, що час, який витрачається на локальні обчислення SPF, необхідно контролювати, щоб досягти часу конвергенції в мілісекундах. У цій роботі представлено досвід авторів у вимірюванні та покращенні продуктивності програмного забезпечення протоколу маршрутизації OSPF. По-перше, було розглянуто структуру характеристики продуктивності багаторазового використання для дослідження продуктивності маршрутизації, яка дозволила б виконувати відтворювані експерименти в контрольованому середовищі з різними мережевими топологіями та навантаженнями. Потім було представлено відносну продуктивність кількох оптимізацій низького рівня, запропонованих для оптимізації коду обчислення маршруту та структур даних. Нарешті, представлено переваги продуктивності оптимізації на рівні алгоритму за допомогою інкрементального алгоритму найкоротшого шляху (ISPF). Можна досягти суттєвого підвищення продуктивності за допомогою ISPF, краще ніж це що можливо за допомогою методів оптимізації коду та використання ефективних структур даних для реалізації алгоритму SPF (DSPF) Дейкстри.

Open Shortest Path First (OSPF) — це протокол маршрутизації за принципом вибору найкоротшого шляху, який є більш надійним і менш інтенсивним у смузі пропускання, ніж протоколи маршрутизації за вектором відстані, такі як RIP [6], і широко використовується у великих доменах IP-маршрутизації. Але він також вимагає значної потужності процесора та пам’яті, щоб підтримувати базу даних про стан каналів в актуальному режимі. Недавні дослідження [11] показали, що час, який споживають локальні обчислення SPF за протоколом маршрутизації за принципом вибору найкоротшого шляху OSPF, необхідно контролювати, щоб досягти часу конвергенції в мілісекундах.

У цьому розділі представлено структуру для вимірювання продуктивності протоколу маршрутизації OSPF. Головну увагу зосереджено на вимірюванні накладних витрат, пов’язаних з обчисленням таблиці маршрутизації, яке, як відомо, є однією з найбільш інтенсивних операцій на ЦП у маршрутизаторах на основі OSPF. Алгоритм Дейкстри «Спочатку за найкоротшим шляхом» (DSPF) [11] є стандартом де-факто, який використовується майже в усіх комерційних реалізаціях OSPF для обчислення таблиці маршрутизації. Було розроблено набір тестів для аналізу та характеристики продуктивності алгоритму DSPF у програмному забезпеченні маршрутизації OSPF університету Меріленда (UMD) відповідно до специфікацій IETF. Потім було оцінено відносну вигоду від використання деяких методів оптимізації коду разом із використанням більш ефективних структур даних для покращення його продуктивності. та оцінено переваги ISPF. було чітко продемонстровано, що оптимізація на рівні алгоритму за допомогою ISPF перевершує оптимізацію низького рівня.

**3.1 Алгоритм функціонування протоколу OSPF**

Open Shortest Path First (OSPF) — це динамічний ієрархічний протокол маршрутизації за станом зв’язку, призначений для використання в автономній системі (AS). Він використовує алгоритм DSPF для розрахунку таблиці маршрутизації. OSPF поділяє домен на дворівневу ієрархію областей, де корінь є магістральною областю, що з’єднує всі інші області на другому рівні. Кожен маршрутизатор у зоні OSPF підтримує синхронізовану топологічну базу даних, яка називається базою даних про стан зв’язку, яка містить топологію мережі як карту взаємозв’язку маршрутизаторів усередині області. Оголошення про стан зв’язку (LSA) описує стан інтерфейсу рекламного маршрутизатора до каналу зв’язку, який є основною одиницею інформації, що передається через мережу та зберігається в базі даних стану зв’язку. Усі бази даних про стан зв’язку в області синхронізуються за допомогою процедури, що називається надійним перетоком [12]. На рис. 3.1 представлено приклад фізичного вигляду зони OSPF. А на рис. 3.2 представлено дерево DSPF, створене маршрутизатором 1.

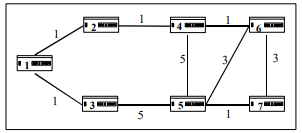


Рисунок 3.1 - Приклад фізичного вигляду зони OSPF

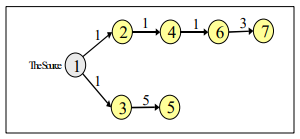


Рисунок 3.2 - Дерево DSPF, створене маршрутизатором 1

Кожен маршрутизатор створює таблицю маршрутизації зі своєї бази даних про стан каналів, обчислюючи найкоротші шляхи до всіх можливих пунктів призначення за допомогою алгоритму SPF. Алгоритм підтримує список кандидатів вузлів, які є потенційними кандидатами для додавання до першого дерева найкоротшого шляху (SPF-дерева) на кожній ітерації. Вона починається з додавання вихідного маршрутизатора (маршрутизатора, який виконує обчислення) до SPF-дерева, а також усіх сусідів вихідного маршрутизатора до списку кандидатів, включаючи вартість каналів із сусідами. Маршрутизатор у списку кандидатів з найменшою відстанню до джерела видаляється зі списку та додається до SPF-дерева. Потім усі сусіди цього маршрутизатора перевіряються на можливість включення до списку кандидатів, якщо вони виявлені вперше або покращено вартість їх найкоротшого шляху. Алгоритм повторює список кандидатів і завершує роботу, коли він стає порожнім. Ключовими операціями в реалізації алгоритму SPF є: (1) вставлення нового вузла до списку кандидатів у відсортованому порядку на основі відстані вузла до джерела та (2) отримання зі списку вузла з мінімальною відстанню до джерела. У цій статті терміни маршрутизатори та вузли використовуються як синоніми.

**3.2 Алгоритм ISPF**

Щоб уникнути повторного обчислення всієї таблиці маршрутизації в результаті зміни топології мережі McQuillan et. al. розробив більш ефективний варіант алгоритму DSPF, який отримав назву Інкрементний SPF (ISPF) [13]. Перш ніж обговорювати алгоритм ISPF, розглянемо приклад, який демонструє неефективність алгоритму SPF. На рисунку 3.2 показано SPF-дерево, обчислене R1 для області OSPF, показаної на рисунку 3.1. Розглянемо випадок, коли канал зв'язку між R4 і R5 не працює. Очевидно, що посилання не в SPF-дереві; тому його збій не змінює таблицю маршрутизації. Незважаючи на це, алгоритм DSPF вимагає повторного обчислення всієї таблиці маршрутизації, коли виявляється збій зв’язку, незалежно від релевантності чи впливу зміни на фактичне дерево SPF. Втрата часу та обчислювальних ресурсів на такі надлишкові обчислення уповільнює конвергенцію маршрутизації. Алгоритм ISPF уникає надлишкових обчислень шляхом визначення та повторного обчислення лише тих найкоротших шляхів, на які впливає зміна.

У цьому розділі ми пояснюємо алгоритм ISPF, розглядаючи два основні випадки зміни стану зв’язку. Для детального опису алгоритму дивіться посилання [13]. По-перше, давайте розглянемо випадок, коли вартість зв’язку від вузла A до вузла B збільшується на X. ISPF не перераховує таблицю маршрутизації, якщо посилання не було в SPF-дереві, оскільки збільшення вартості не змінить таблиця маршрутизації. Якби посилання було в SPF-дереві, тоді нова вартість могла б потенційно збільшити вартість найкоротшого шляху до вузла B, а також вартість найкоротших шляхів до вузлів, на шляхах яких лежить вузол B. Таким чином, тільки вузли в піддереві з корінням у B є кандидатами на зміну своїх позицій у SPF-дереві. Алгоритм ISPF спочатку ізолює всі вузли в піддереві з коренем B і збільшує вартість їхніх шляхів від джерела на X. Потім він намагається знайти коротший шлях до кожного вузла в піддереві через сусідній вузол, який не є частиною піддерево та додає вузол до списку кандидатів, якщо можна знайти новий коротший шлях. Після перевірки всіх вузлів у піддереві, якщо список кандидатів не порожній, викликається алгоритм DSPF, який приймає новий список кандидатів і попереднє дерево SPF як вхідні дані, щоб знайти найкращі можливі найкоротші шляхи для вузлів у списку та, можливо, інші вузли піддерева. На рисунку 3.3 показано зміни до SPF-дерево на рисунку 3.2, яке виникає, коли вартість зв’язку від маршрутизатора R4 до маршрутизатора R6 збільшується з 1 до 8. На рис. 3.4 представлено нове дерево SPF після змін.

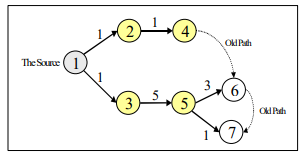


Рисунок 3.3 - Нове дерево SPF після топологічної зміни

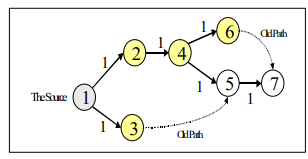


Рисунок 3.4 - Нове дерево SPF після змін

**3.3 Структура системи оцінювання продуктивності OSPF**

В роботі було розроблено експериментальну структуру характеристики продуктивності, яка дозволяє проводити відтворювані експерименти в контрольованому середовищі з можливістю змінювати топологію мережі, ступінь підключення та навантаження на маршрутизацію. На рисунку 3.5 показано систему оцінки продуктивності. Структура системи складається з таких компонентів:

1. Генератор топології мережі (TIERS) [2],

2. Симулятор протоколу маршрутизації OSPF (RPS),

3. Інструмент профілювання коду (QUANTIFY) [10]

4.Випробовуваний маршрутизатор (RUT), який в основному є інструментальним програмним забезпеченням маршрутизації UMD OSPF.

У запропонованій структурі TIERS використовується для генерації мережевих топологій, які відображають ієрархічну структуру домену та локальність у великих мережах та Інтернеті. Було використано RPS для моделювання логічних хмар OSPF і обміну пакетами OSPF з RUT. RPS діє як граничний маршрутизатор між змодельованою хмарою та RUT. RPS може імітувати декілька областей OSPF у кількох доменах маршрутизації. Таким чином, RUT вважає, що його підключено до реальної мережі OSPF. Ми пов’язуємо код OSPF RUT із QUANTIFY, щоб інструментувати об’єктний код і контролювати його виконання. QUANTIFY збирає дані про продуктивність під час виконання та створює профіль виконання, який показує, наприклад, час виконання різних функцій і частоту їх викликів. Профіль виконання можна використовувати, щоб знайти основні вузькі місця в коді та визначити, які частини потребують подальшого налаштування для покращення продуктивності.

**3.4 Характеристика продуктивності алгоритму DSPF**

У цьому підрозділі спочатку охарактеризовано продуктивність алгоритму DSPF, щоб визначити операції, головним чином відповідальні за його неефективність. Потім було оцінено покращення продуктивності шляхом запропонованої оптимізації у коді та структурах даних. Потім було проведено два різних експерименти, щоб дослідити вплив топології мережі на час виконання алгоритму.

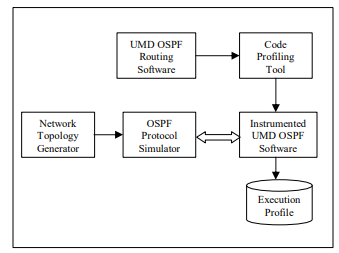


Рисунок 3.5 - Структура оцінювання продуктивності програмного забезпечення

Час конвергенції є основним показником продуктивності в цьому дослідженні, який визначається як час, потрібний RUT для перерахунку своєї таблиці маршрутизації в результаті зміни в області, до якої належить RUT. Це еквівалентно часу виконання алгоритму DSPF. Можна змоделювати топологічну зміну, піднявши або опустивши тракт, що запускає повторне обчислення всієї таблиці маршрутизації в DSPF. На рисунку 3.6 показано час виконання (вартість виконання) у порівнянні з кількістю вузлів, яка визначається як сума кількості маршрутизаторів і мереж усередині області. Він показує вплив рівня підключення на час виконання. Середня кількість трактів на маршрутизатор визначає середню здатність підключення маршрутизатора, яка показана на графіку, що відповідає кожній точці даних. На рисунку 3.7 показано вплив кількості маршрутизаторів у зоні на час виконання, де кількість маршрутизаторів показано на графіку. Можна зробити такі спостереження з графіків на рисунку 3.6, 3.7:

1. Час виконання DSPF прямо пропорційний кількості вузлів усередині області. Він погіршується зі збільшенням рівня підключення або збільшенням кількості маршрутизаторів.

2. Час виконання алгоритму значно змінюється в залежності від топології області з фіксованою кількістю вузлів. Наприклад, обчислення SPF займає 25 мс у зоні з 400 вузлами з 60 маршрутизаторами та рівнем підключення 26 (рисунок 3.6), тоді як це займає менше 13 мс у зоні з 400 вузлів із 150 маршрутизаторами та рівнем підключення. приблизно 6 (рисунок 3.7). Отже, можна зробити висновок, що рівень підключення в межах області має більший вплив на час конвергенції, ніж кількість маршрутизаторів у тій самій області.

3. Низький рівень зв’язку (розріджена область) демонструє лінійне зростання (рисунок 3.6), тоді як високий рівень зв’язку (щільна область) площа) демонструє квадратичне зростання часу виконання (рисунок 3.7). Результат відповідає складності алгоритму Дейкстри, описаному в літературі [14], яка має порядок *n*2 для щільних мереж і *n* log *n* для розріджених мереж, де *n* — кількість вузлів.

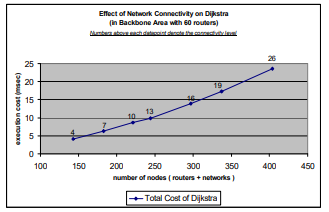


Рисунок 3.6 – Вплив мережевого підключення на алгоритм Дейкстри

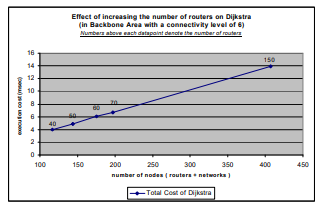


Рисунок 3.7 - Вплив кількості маршрутизаторів на алгоритм Дейкстри

На рисунку 3.8 та 3.9 зображено час виконання дев'яти найдорожчих функцій в алгоритмі. Це показує, що cl\_enq і findLSA є двома найдорожчими функціями, які можна оптимізувати для скорочення часу конвергенції. cl\_enq використовується для вставки нового вузла в список кандидатів, тоді як findLSA використовується для пошуку вузла з певним ідентифікатором стану посилання в базі даних стану посилання. Було також виявлено, що вартість виконання вставки нового вузла в список кандидатів сильно змінюється, головним чином через використання неефективної структури даних (відсортований список посилань) для списку кандидатів. Функція cl\_enq виконує лінійний пошук у пов’язаному списку під час вставки нового вузла. Ми можемо оптимізувати функцію cl\_enq, використовуючи більш ефективну структуру даних, таку як бінарне дерево пошуку або бінарну купу, для реалізації списку кандидатів.

На рисунку 3.10 показано підвищення продуктивності алгоритму DSPF в результаті використання більш ефективної структури даних. У результаті детального аналізу ми також виявили, що висока частота викликів функції findLSA робить її одним із найдорожчих компонентів у DSPF. Функція findLSA викликається кілька разів, щоб обчислити покажчики на сусідні вузли. Ми реалізували більш ефективну структуру даних для вузлів, яка полегшує кешування покажчиків на сусідні вузли. За допомогою кешування можна один раз обчислити вказівники на сусідні вузли та кешувати їх для наступних звернень, що зрештою зменшує частоту викликів findLSA. Можна спостерігати, що значний приріст продуктивності досягається шляхом кешування покажчиків на рисунку 3.11.

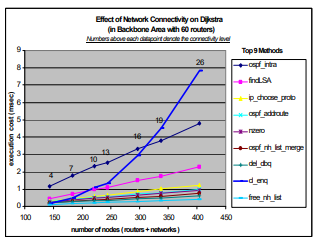


Рисунок 3.8: Вплив підключення до мережі на ефективність SPF



Рисунок 3.9 - Покращення продуктивності шляхом кешування покажчиків

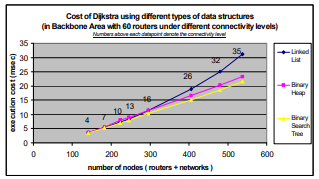


Рисунок 3.10 - Покращення продуктивності на використання більш ефективної структури даних

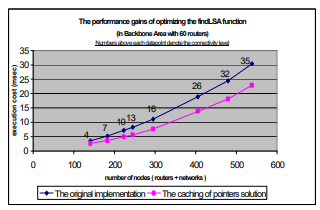


Рисунок 3.11 - Покращення продуктивності на кешування покажчиків

**3.5 Оптимізація за допомогою алгоритму ISPF**

На рисунку 3.12 показано діаграму потоку даних алгоритму ISPF. Він також показує основні компоненти реалізації ISPF.

Реалізація ISPF складається з чотирьох основних структурних блоків, а саме блоку приймання OSPF, детектора зміни топології, блок реалізації алгоритму ISPF і блок модифікованої реалізації DSPF. Приймання OSPF реалізує стандартну логіку обробки введення та перевірки помилок для пакетів OSPF. Детектор змін топології реалізує логіку, яка виявляє зміни в топології області. Він аналізує вхідні LSA і порівнює їх із попередньо встановленими LSA, якщо вони існують, у базі даних про стан зв’язку, створеній тим самим вузлом. Коли детектор зміни топології визначає точний тип зміни, він генерує нову подію зміни та додає це до списку подій зміни. Алгоритм ISPF проходить список подій змін і перевіряє кожну подію зміни. Він намагається визначити та оновити лише найкоротші маршрути, на які впливає топологічна зміна. Таблиця 3.1 показує події змін, оброблених ISPF.

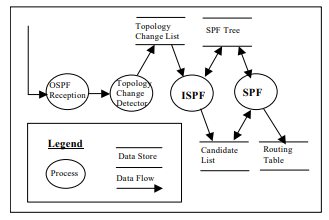


Рисунок 3.12 - Компоненти реалізації ISPF

Таблиця 3.1 - Типи подій топологічної зміни

|  |  |
| --- | --- |
| Назва події | Опис |
| NewNode | Надходження нового LSA, який раніше не був отриманий |
| LinkDown | Збій лінії зв'язку (або вузла) |
| LinkUp | Відновлення тракту (або вузла) |
| LinkCostIncrease | Вартість тракту зростає |
| LinkCostDecrease | Вартість тракту зменшується |
| AgedLSA | LSA вузла видляється (термін дії закінчується) |

Було трохи змінено реалізацію стандартного алгоритму DSPF, щоб оновити таблицю маршрутизації після того, як ISPF завершить обробку подій топологічної зміни. Стандартний алгоритм DSPF будує SPF-дерево з порожнього списку кандидатів, тоді як модифікована реалізація приймає як вхідні дані список кандидатів, сформований алгоритмом ISPF. Потім він виконує кроки обчислення DSPF для кожного з вузлів у списку кандидатів.

На рисунку 3.13 показано час виконання алгоритмів DSPF і ISPF для магістральних і кінцевих областей.

Час виконання алгоритму ISPF значно менший за час виконання алгоритму DSPF. DSPF показує лінійне зростання для низького рівня зв’язку в розрідженій області (як показано на рисунку 3.14), а квадратичне зростання для високого рівня зв’язку в щільній зоні (як показано на рисунку 3.13). З іншого боку, час виконання ISPF показує набагато повільніші темпи зростання.

Для такої ж кількості вузлів, час виконання DSPF значно змінюється залежно від топології області, тоді як вплив топології на час виконання ISPF менш очевидний.

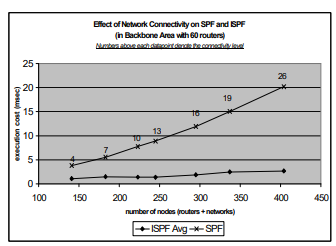


Рисунок 3.13 - Вплив підключення до мережі в магістральній зоні

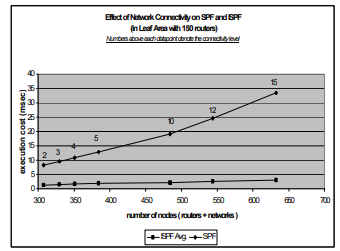


Рисунок 3.14 - Вплив підключення до мережі в листовій області

Отже. алгоритму DSPF потрібен фіксований проміжок часу, щоб виконати обчислення таблиці маршрутизації в області певного розміру та з’єднання, оскільки щоразу він обчислює повну таблицю маршрутизації. З іншого боку, час виконання ISPF змінюється пропорційно кількості найкоротших шляхів, на які впливає топологічна зміна.

**4 ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ПРОТОКОЛУ МАРШРУТИЗАЦІЇ BGP**

Протокол Border Gateway Protocol (BGP) об’єднує єдиний глобальний Інтернет із менших мереж із різними цілями політики. BGP страждає через низьку продуктивність мережі, а також уразливості безпеки, помилки конфігурації, помилки програмного забезпечення тощо. BGP не реагує на серйозні проблеми продуктивності та доступності в площині даних, які, насправді, часто абсолютно невидимі для протоколу маршрутизації. Коливання маршруту BGP можуть призвести до великої втрати пакетів, періодичної втрати зв’язку та збільшення затримки шляху.

Було запропоновано численні способи виправлення BGP. Ці пропозиції зазвичай діляться на дві категорії: (1) покращення BGP (наприклад, для покращення конвергенції [3, 4] і безпеки [5, 6]); і (2) альтернативні архітектури, які використовують «чистий підхід» до міждоменної маршрутизації [7–10]. Однак ці пропозиції стикаються з серйозними практичними перешкодами. З одного боку, вдосконалення BGP додають механізми до вже складного протоколу, що може створювати нові проблеми (наприклад, помилки конфігурації, проблеми конвергенції протоколів і нові вектори атак). З іншого боку, альтернативні архітектури важко, часто навіть неможливо, розгортати поступово.

В роботі представлено новий спосіб виправлення міждоменної маршрутизації. Для цього запропоновано нову архітектуру маршрутизації під назвою «маршрутизація наступного переходу», яка базується на двох керівних принципах:

1. Замість розширення або заміни BGP пропонується спрощення протоколу маршрутизації шляхом обмеження способу вибору та експорту маршрутів;

2. Вирішення таких питань, як продуктивність і безпека рівня даних поза межами протоколу маршрутизації. Аналіз протоколу маршрутизації BGP і моделювання показують, що маршрутизація наступного переходу значно покращує продуктивність без шкоди для інших глобальних цілей.

Конвергенція BGP надто повільна для інтерактивних програм. Технології зменшення затримки конвергенції вводять додаткові таймери та параметри конфігурації в програмне забезпечення маршрутизатора, погіршуючи і без того складну систему.

Така залежність є радше перешкодою, ніж допомогою для досягнення високої продуктивності мережі. Натомість пропонується маршрутизація наступного переходу, тобто ранжування та шляхи експорту AS виключно на основі AS наступного переходу на шляху до кожного префіксу призначення та застосування простого правила «послідовної фільтрації» [15] при експорті маршрутів. Було показано як аналітично, так і експериментально, що маршрутизація наступного переходу забезпечує значно кращу продуктивність мережі, ніж традиційна маршрутизація на основі шляхів у двох важливих аспектах:

**Краща конвергенція.** маршрутизація наступного переходу набагато швидше наближається до «стабільної» конфігурації маршрутизації, ніж звичайний BGP. Крім того, процес конвергенції передбачає набагато менше повідомлень про оновлення та пересилання змін. Результати моделювання показують, що наступна маршрутизація особливо ефективна для запобігання найсерйознішим проблемам конвергенції BGP. Результати моделювання свідчать про те, що маршрутизація наступного переходу може дозволити автономним системам відключити механізми для зменшення затримки конвергенції та обмеження швидкості надсилання повідомлень про оновлення.

**Більш відповідальна для багато шляхової маршрутизації.** Сучасні маршрутизатори BGP, вибирають один шлях для кожного пункту призначення, а не використовують різноманітність шляхів в Інтернеті. В цій роботі показано, що маршрутизація наступного переходу природно підтримує багато шляхову маршрутизацію, що призводить до багатьох переваг, наприклад, покращення доступності, кращого відновлення після збоїв, балансування навантаження, налаштованого вибору маршруту.

**Маршрутизація, орієнтована на продуктивність.** Сучасні маршрутизатори BGP віддають перевагу коротшим AS-PATH як непрямий спосіб покращити наскрізну продуктивність. Однак довжина AS-PATH лише слабко корелює із затримкою наскрізного розповсюдження та не відображає інших цікавих показників продуктивності, наприклад пропускної здатності, затримки та втрат [16]. Отже, BGP не в змозі впоратися з серйозними проблемами продуктивності та доступності в площині даних. Для досягнення високої продуктивності мережі вибір маршруту повинен базуватися на прямих спостереженнях за якістю шляху, а не на довжині AS-PATH.

Запропоновано використовувати два механізми: наскрізний моніторинг і багатокрокову маршрутизацію. Жоден із цих механізмів не передбачено сьогоднішнім BGP. Натомість AS має адаптувати рейтинги наступних переходів, а також спосіб розподілу трафіку між декількома «наступними переходами» на основі моніторингу якості шляху в площині даних. В роботі описано методи моніторингу ефективності маршруту для AS-заглушок, постачальників онлайн-послуг і транзитних провайдерів.

**4.1 Архітектура однокрокової маршрутизації**

Маршрутизатори BGP зазвичай отримують кілька маршрутів до одного пункту призначення. Маршрутизатор BGP використовує три кроки для обробки оголошень маршруту:

- політика імпорту визначає, які маршрути слід відфільтрувати (і, отже, вилучити з розгляду), і призначає «локальні переваги»;

- процес прийняття рішень вибирає найбільш бажаний маршрут;

- експортна політика визначає, які з сусідніх маршрутизаторів вивчають обраний маршрут.

Процес прийняття рішення складається з упорядкованого списку атрибутів, за якими порівнюються маршрути. Необхідно зосередитись на наступних важливих кроках у процесі прийняття рішень щодо BGP (повний список кроків див. [26]):

- віддавати перевагу вищим місцевим перевагам (LocalPref);

- віддавати перевагу коротшим маршрутам

• віддавати пріоритет старим маршрутам над новими.

Тепер необхідно визначити три правила маршрутизації наступного переходу.

Правило I: Використання наступного рейтингу. Необхідно налаштовувати рейтинги маршрутів лише на основі найближчої наступної AS на шляху до кожного пункту призначення. Допускається рівність у рейтингах наступних стрибків.

Правило II: Надання пріоритету поточному маршруту. Щоб звести до мінімуму дослідження шляху, коли постає вибір між «старим» (поточним) маршрутом і таким же хорошим (з точки зору наступного переходу) новим, необхідно повторно вибрати старий маршрут.

Правило III: Послідовне експортування [17]. Якщо маршрут P можна експортувати до сусідньої AS i, то такими повинні бути всі маршрути, які мають вищий рейтинг, ніж P.

**4.2 Краща конвергенція маршрутизації**

Інтуїтивно зрозуміло, що BGP може здійснювати конвергенцію з двох основних причин:

- невеликі та віддалені зміни маршрутизації можуть змусити AS вибрати новий наступний стрибок, таким чином призводячи до ланцюгової реакції наступних змін маршрутизації;

- невідповідності між ранжируванням шляхів і політикою експорту маршрутів можуть призвести до того, що AS від’єднає інші AS від пункту призначення під час вибору кращого маршруту для себе, що змусить їх шукати альтернативні маршрути.

Запропоновані правила маршрутизації наступного переходу запобігають таким сценаріям. Рейтинг наступного переходу гарантує, що зміни віддаленої маршрутизації не змушують AS змінювати свій наступний крок. Послідовний експорт гарантує, що під час покращення власного маршруту AS ніколи не відключатиме інші AS від пункту призначення..

**Метрики.** Для вимірювання ефективності під час процесу конвергенції застосовано три показники:

- кількість змін пересилання, тобто кількість разів, коли AS змінюють свій вибір наступного стрибка під час процесу конвергенції (сумується для всіх AS);

- кількість змін маршрутизації, тобто кількість змін маршрутів AS під час процесу конвергенції (сумована для всіх AS);

- кількість оновлень BGP, переданих під час процесу конвергенції (підсумовано для всіх AS).

**4.3 Результати моделювання**

Експерименти показують, що маршрутизація наступного переходу значно зменшує кількість повідомлень про оновлення, змін маршрутизації та змін пересилання за різних мережевих подій і точок огляду.

Для налаштування симуляції буловикористано Інтернет-топологію рівня AS Cyclops [17]. Кожна AS представлена одним маршрутизатором, а зв’язки між AS анотовані діловими відносинами. Топологія містить загальну кількість 33 976 AS, з них 4 670 незаглушених, тобто AS, які не мають власних клієнтів, а решта – заглушки. Топологія містить 54 786 посилань клієнт-постачальник і 43 888 однорангових посилань.

При оцінюванні протоколу BGP та PRR (Prefer Recent Route) на останньому етапі визначення зв’язків надається перевага поточному найкращому маршруту над новими маршрутами та маршрутизації наступного переходу. Для всіх цих протоколів дотримувались умови імпорту та експорту Gao-Rexford [17] (див. Додаток B), де AS надають пріоритет маршрутам, отриманим клієнтом, над маршрутами, отриманими одноранговими, а не маршрутами, отриманими постачальником. BGP і PRR віддають перевагу коротшим маршрутам перед довшими в кожній категорії (замовник/одноранговий/провайдер). Усі три протоколи відповідають вимогам узгодженого експорту. Порівняння трьох протоколів дозволяє кількісно оцінити важливість ранжування наступного стрибка (тільки в маршрутизації наступного стрибка) і пріоритеризації поточного маршруту (як у ранжуванні наступного стрибка, так і в PRR).

Під час дослідження було використано симулятор C-BGP [29], який обмежує швидкість оновлень, що надсилаються під час кожного сеансу. Хоча BGP RFC рекомендує стандартний MRAI 30 секунд [18], постачальники маршрутизаторів [18] і IETF виступають за використання набагато менших MRAI (наприклад, кілька секунд) або повне видалення таймера через вимоги до продуктивності інтерактивні програми. Таким чином, результати моделювання без налаштувань MRAI повинні бути розумною оцінкою змін пересилання, змін маршрутизації та повідомлень про оновлення BGP, оскільки Інтернет відходить від великих таймерів MRAI. Насправді експериментальні та теоретичні результати, наведені нижче, свідчать про те, що маршрутизація наступного переходу може дозволити AS повністю видалити таймер MRAI. Оскільки C-BGP не дає точних оцінок часу конвергенції, було представлено результати для цього показника.

На рисунку 4.1 зображено розподіл кількості повідомлень про оновлення, які бачать AS без заглушки.

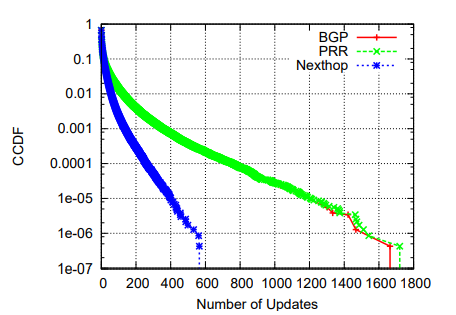


Рисунок 4.1 - Частка AS без заглушки. Які зазнають більше ніж x повідомлень про оновлення після збою зв’язку

Близько третини AS в Інтернеті не бачать жодних змін у маршрутизації після збою з’єднання. Для AS, які зазнають змін у маршрутизації, середня кількість оновлень, отриманих кожною AS, становить 11,7 для BGP, 11,8 для PRR і 8,0 для наступного переходу BGP. Оскільки після будь-якої події багато AS майже не впливають або не відчувають жодного ефекту, ми будуємо графік додаткової кумулятивної функції розподілу (CCDF), щоб зосередитися на AS, які отримують багато повідомлень про оновлення.

У BGP (верхня крива на рисунку 4.1) деякі AS без заглушки отримують тисячі повідомлень про оновлення. Цікаво, що більші AS із кращим зв’язком зазвичай отримують більше повідомлень про оновлення, імовірно тому, що у них набагато більше сусідів, які експортують маршрути до них. Найбільш уражена незаглушена AS отримує 1698 повідомлень про оновлення, а найбільш уражена заглушка отримує 244. PRR трохи зменшує це число (середня крива на рис. 4.1, яка здебільшого збігається з кривою BGP, за винятком хвоста), уникаючи непотрібного дослідження шляху. Маршрутизація наступного переходу призводить до значного покращення (нижня крива). Набагато менша кількість повідомлень про оновлення свідчить про те, що маршрутизація наступного переходу дозволить AS видалити таймер MRAI.

Як було зазначено раніше. протокол маршрутизації наступного переходу складається з трьох частин: рейтинг наступного переходу, перевага старому маршруту та послідовний експорт. Хоча етап узгодженого експорту застосовується в усіх протоколах BGP, PRR і наступного переходу, розрив між кривими BGP і PRR на рис. 4.1 показує незначні переваги кроку PRR у маршрутизації наступного переходу. Навпаки, розрив між кривими PRR і наступного переходу на малюнку чітко демонструє покращення за допомогою ранжирування наступного переходу.

Маршрутизація наступного переходу також значно зменшує кількість змін маршрутизації та пересилання для автономних систем без заглушки (див. рис. 4.2).

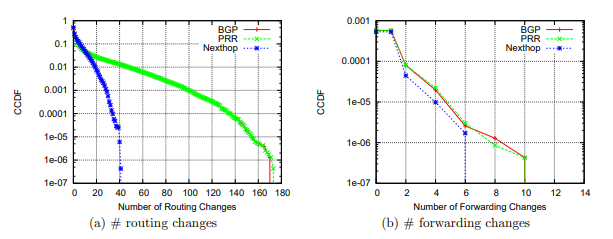


Рисунок 4.2 – Частка автономних систем без заглушки, які зазнають більше ніж x змін маршрутизації/пересилання після збою зв’язку

Для AS, які зазнають змін, середня кількість змін маршрутизації становить 4,99 для BGP, 5,03 для PRR і лише 3,95 для наступного переходу BGP. Ми отримуємо подібні результати для середньої кількості змін пересилання: 2,36 для BGP, 2,37 для PRR і 2,20 для наступного маршруту. Насправді жодна з незаглушених AS не зазнає більше шести змін пересилання під час маршрутизації наступного переходу для цих експериментів. На відміну від цього, AS зазнають до десяти змін пересилання, коли віддають перевагу коротшому AS-PATH замість того, щоб залишатися з тим самим AS наступного переходу, як у PRR.

На рисунку 4.3 зображено розподіл кількості повідомлень про оновлення та змін маршрутизації, як це видно на AS-заглушках. Зауважте, що маршрутизація наступного переходу знову приводить до значного покращення порівняно з BGP і PRR.

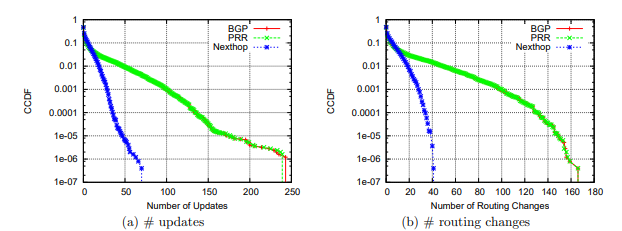


Рисунок 4.3 – Частка AS-заглушок, які мають більше ніж x повідомлень про оновлення/змін маршрутизації після збою зв’язку під час різноманітних заходів для заглушки AS.

Графіки CCDF, хоча й корисні для ілюстрації різноманітного досвіду AS під час конвергенції, є громіздкими для прямого порівняння протоколів за різними подіями та показниками конвергенції. Однак із таким спотвореним розподілом середнє значення та медіана не мають особливого значення. Таким чином, ми зосереджуємося на досвіді AS на позиції 0,1% на графіках CCDF, що дозволяє нам зосередитися на (не заглушках) AS, які найбільше страждають від збоїв з’єднання, не дозволяючи одній AS, що виділяється, спотворювати результати. Ми узагальнюємо дані в стовпчастих діаграмах на рисунку 5. Стовпчики для «Помилки з’єднання» відповідають положенню y = 0,001 на малюнках 3(a) і 4(a), відповідно. Ми не будуємо графік кількості змін переадресації, оскільки для більшості експериментів 0,1-процентиль AS зазнав щонайбільше однієї зміни переадресації. Ми отримуємо подібні результати, порівнюючи кількість повідомлень про оновлення та змін маршрутизації

Запропоновані правила маршрутизації наступного переходу передбачають існування стабільного стану в мережі [19], але це не гарантує конвергенції BGP до стабільного стану або що така конвергенція буде швидкою. Дійсно, навіть у природній «структурі Гао-Рексфорда», яка фіксує звичайні практики маршрутизації AS і де конвергенція BGP до стабільного стану гарантована, конвергенція може включати експоненціально багато змін пересилання, змін маршрутизації та BGP оновлення.

**4.4 Багатокрокова міждоменна маршрутизація**

Останнім часом спостерігається сплеск інтересу до багатокрокової міждоменної маршрутизації. В цьому підрозділі обговорюється, як маршрутизація наступного переходу може зробити багатокрокову маршрутизацію більш масштабованою та поступовою для розгортання. Потім розглядається застосування результатів щодо конвергенції та сумісності стимулів маршрутизації наступного переходу до конкретного налаштування багатокрокової маршрутизації.

**4.4.1 Перетворення багатокрокової маршрутизації на масштабовану**

На жаль, наївні схеми багатокрокової маршрутизації на основі BGP можуть бути немасштабованими через необхідність поширювати та зберігати декілька маршрутів.

Для топології на рис. 4.4 розглянемо простий багатокроковий протокол, де вузли повідомляють про всі доступні маршрути сусіднім вузлам. Зауважте, що AS *A* і *B*, кожна з яких має два маршрути до пункту призначення *D*, обидві оголосять два маршрути до AS *C*. AS *C* потім оголосить чотири маршрути до AS *D* і так далі. Це може легко призвести до вибуху стану та надмірної передачі повідомлень про оновлення.

Отже, маршрутизація наступного переходу більш піддається багатокроковому доступу, ніж маршрутизація на основі шляху. Ключове зауваження полягає в тому, що при маршрутизації наступного переходу вузлу не потрібно вивчати численні шляхи сусіднього вузла, а просто вивчати достатньо, щоб уникнути петель. Якщо AS *C* на рис. 4.4 має ранжування маршрутів наступного переходу, тоді, щоб дозволити *C* виявляти петлі, AS *A* (або *B*) може просто надіслати C (невпорядкований) список усіх AS, які проходять її (кілька) маршрутів. BGP дозволяє агрегувати маршрути в один такий AS-SET, який узагальнює атрибути AS-PATH усіх окремих маршрутів.

Таким чином, агрегація маршрутів BGP, яка використовується для забезпечення керованості таблиць маршрутизації BGP в інших контекстах, також може бути використана для значного зменшення вартості багатокрокової маршрутизації наступного переходу.

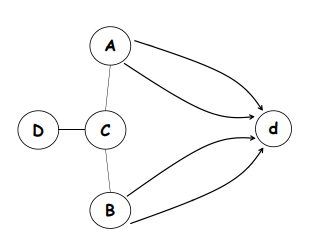


Рисунок 4.4 – AS *A* і *B* оголошують два маршрути до AS *C* і *C*  потім оголошує чотири маршрути до AS *D* і так далі. Очевидно, що це може призвести до вибуху стану.

**4.4.2 Маршрутизація наступного переходу для сусідів**

У той час як за BGP маршрутизатор обмежений вибором одного маршруту (для кожного префікса призначення), AS може захотіти вибрати різні маршрути для різних сусідніх AS з економічних міркувань (наприклад, ISP може пропонувати клієнтам різні послуги) або з експлуатаційних причин (наприклад, для підвищення стійкості до відмов [20). Специфічний для сусідів BGP є нещодавно запропонованим розширенням BGP що дозволяє маршрутизатору вибирати інший (єдиний) маршрут для кожного сусіда, тобто налаштовувати вибір маршруту для кожного сусіда. Дивно, але додаткова гнучкість у виборі маршруту за NS-BGP також покращує глобальну стабільність мережі.

Тепер ми покажемо, що теоретичний результат для конвергенції маршрутизації наступного переходу поширюється на NS-BGP. Зокрема, ми розглядаємо маршрутизацію наступного переходу за допомогою NS-BGP, тобто маршрутизацію за допомогою NS-BGP так, що (1) AS обмежено використанням лише рейтингу наступного переходу для вибору маршрутів для сусідніх AS (можливо, використовуючи різні рейтинги для різних сусідів); і (2) AS послідовно експортує по відношенню до кожної сусідньої AS. Рисунок 4.5 ілюструє маршрутизацію наступного переходу за допомогою NS-BGP.

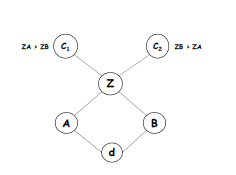


Рисунок 4.5 – NS-BGP із маршрутизацією наступного стрибка: *C*1 віддає перевагу *ZA* над *ZB* як перші два стрибки на шляху до *D*. *C*1 віддає перевагу *ZB* над *ZA* як перші два стрибки на шляху до *D.*. *Z* є провайдером Інтернету, який використовує NS-BGP, тому може використовувати рейтинг наступного переходу *A* > *B* для вибору маршрутів для *C*1 та рейтинг наступного переходу *B* > *A* для вибору маршрутів для *C*2

Отже, маршрутизація наступного переходу знижує бар’єр для втілення багатокрокової маршрутизації в реальність. Використання багатокрокової маршрутизації може дати такі переваги:

**Доступність.** Багатокрокова маршрутизація збільшує ймовірність того, що AS має принаймні один робочий шлях.

**Відновлення після відмови.** AS з декількома наступними переходами може миттєво реагувати на збій в одному вихідному каналі, надсилаючи трафік по іншому (і не чекати, доки протокол знову об’єднається).

**Балансування навантаження.** AS може мати кілька наступних переходів (з однаковими локальними перевагами) і вирішувати, чи і скільки трафіку направляти через кожен наступний крок (наприклад, на основі моніторингу площини даних). Звичайні методи, такі як хешування полів у IP-заголовку, можуть гарантувати, що пакети одного потоку проходять однаковий шлях, щоб запобігти доставці пакетів поза порядком.

**4.5 Захист системи** **маршрутизації**

Розглянемо три переваги маршрутизації наступного переходу перед маршрутизацією на основі шляху з BGP, які роблять деякі небезпечні атаки на BGP неефективними або менш шкідливими:

- значно зменшена поверхня атаки;

- покращена стійкість до помилок конфігурації;

- сумісність стимулів.

**4.5.1 Зменшена поверхня атаки**

Деякі з найнебезпечніших атак на BGP базуються на «брехні» про довжину шляху AS. Дійсно, AS може залучати багато трафіку, оголошуючи коротший маршрут, ніж той, який вона має насправді [21], таким чином запускаючи так звані атаки на чорну діру або перехоплення для втручання, скидання пакетів, підслуховування тощо.

Під час маршрутизації наступного переходу AS не враховує AS-PATH під час прийняття рішень щодо маршрутизації — за межами першого переходу, який неможливо підробити! — тому AS більше користі від таких атак.

Таким чином, маршрутизація наступного переходу значно зменшує поверхню атаки BGP. Насправді, єдині ефективні атаки на основі AS-PATH на маршрутизацію наступного переходу – це атаки, які запускають механізм виявлення циклу BGP (які, очевидно, також ефективні проти маршрутизації на основі шляху з BGP).

**4.5.2 Модель загроз, менш вразлива до помилок конфігурації**

Розглядається модель загроз, яка фіксує деякі типові помилки конфігурації. Сучасні мережі AS зазвичай складаються з комерційних маршрутизаторів, тому доцільно розглядати помилки конфігурації, які призводять AS (маршрутизатори) до ранжування та експорту маршрутів ненавмисним і небажаним способом (на відміну від запуску нового програмного забезпечення маршрутизатора). У запропонованій моделі загроз «супротивник» може вибрати одну AS *A*, а потім змінити політику маршрутизації цієї AS, тобто ранжування маршрутів *A* та правила експорту маршрутів. Тому накладаються обмеження на зміну зловмисником політики маршрутизації *A*.

Хоча існування стабільного стану не гарантує конвергенції протоколу до стабільного стану, розуміння того, коли стабільний стан взагалі існує в мережі, є важливим першим кроком на шляху до розуміння динаміки протоколів за наявності небажаної поведінки.

**4.5.3 Наскрізні механізми безпеки**

На сьогоднішній день AS може використовувати політики BGP, щоб уникнути шляхи, які проходять через небажані AS. Наприклад, уряд США може захотіти уникнути спрямування свого трафіку через інші країни. Подібним чином AS може уникати AS, які, як відомо, здійснюють цензуру, здійснюють прослуховування телефонних розмов або пропонують низьку продуктивність. Це досягається шляхом застосування регулярних виразів до AS-PATH, щоб призначити меншу перевагу маршрутам, які містять небажані AS, або повністю фільтруючи ці маршрути. За маршрутизації наступного переходу AS більше не може вказувати політики маршрутизації BGP, які уникають віддалених небажаних AS або країн, що роблять такі «політики уникнення AS» неможливими.

Хоча маршрутизація наступного переходу робить «політики уникнення AS» неможливими, можна зазначити, що такі політики не мають гарантій; AS-PATH перераховує послідовність AS, які розповсюджували оголошення BGP, а не шлях, який обов’язково проходять пакети даних (і вони можуть відрізнятися навіть із доброякісних причин). Необхідно зазначити, що покладатися на BGP для безпеки рівня даних є помилковим. Саме коли йдеться про такі питання, як конфіденційність і цілісність, не слід залишати це напризволяще або недовіряти. Ці гарантії повинні бути забезпечені іншими (наскрізними) способами, такими як шифрування та автентифікація, наприклад, використовуючи механізми в [22].

Було продемонстровано, що маршрутизація наступного переходу робить деякі небезпечні атаки проти BGP (майже всі атаки на основі AS-PATH, наприклад, атаки на скорочення шляху) неефективними, тоді як інші атаки роблять менш шкідливими або невигідними для зловмисника. Також було показано, як наскрізні механізми, які можна поступово розгортати, можна використовувати для покращення безпеки рівня даних. Поєднання цих заходів дозволить створити систему маршрутизації, яка є значно безпечнішою, ніж сьогоднішній BGP. Однак сама по собі маршрутизація наступного переходу не забезпечує повного захисту від усіх атак. Зокрема, маршрутизація наступного переходу все ще вразлива до атак «викрадення префіксів», коли зловмисник оголошує IP-префікс, яким він не володіє, а також до атак, які запускають механізм виявлення циклу BGP.

За останнє десятиліття стандарти та дослідницькі спільноти приклали багато зусиль, щоб захистити BGP від викрадення префіксів і більш складних атак. Нарешті ми стали свідками початкового розгортання

Інфраструктура відкритих ключів ресурсів (RPKI) — криптографічний корінь довіри для Інтернет-маршрутизації, який офіційно зіставляє AS з їхніми IP-префіксами та відкритими ключами. RPKI дозволить AS автентифікувати, що джерело оголошення маршруту справді володіє оголошеним префіксом — властивість, яка називається «автентифікація джерела». Крім того, існує багато дискусій щодо розгортання механізмів перевірки шляху на рівні AS (наприклад, S-BGP, soBGP, BGPsec), які дозволять AS перевірити, що оголошений маршрут дійсно існує (і було оголошено диктор), таким чином також запобігаючи атакам на механізм виявлення циклу BGP.

**4.6 Управління трафіком**

Сучасні маршрутизатори віддають перевагу коротшим AS-PATH як непрямому способу покращити наскрізну продуктивність і уникнути вибору резервних маршрутів. У цьому розділі ми обговорюємо, як мережеві оператори можуть більш природним чином досягати своїх цілей щодо керування трафіком, не покладаючись на AS-PATH. По-перше, ми обговорюємо, як ранжувати AS наступного переходу на основі вимірювань продуктивності наскрізного шляху. Потім ми обговорюємо, як оператори можуть збалансувати навантаження, ранжуючи AS наступного переходу на основі кожного префіксу та позначаючи шляхи резервного копіювання атрибутом спільноти BGP.

**4.6.1 Маршрутизація, орієнтована на продуктивність**

Маршрутизація наступного переходу може призвести до більш довгих шляхів, ніж звичайний BGP. Щоб зрозуміти вплив на довжину AS-PATH, ми аналізуємо відмінності в довжині шляху для різних AS у діапазоні події «T-up», «T-long» і «T-short». Експерименти показують, що більшість AS (68,7%–89,9%, залежно від події) мають однакову довжину AS-PATH під час маршрутизації BGP і наступного стрибка, а більшість інших AS мають лише один додатковий стрибок. Тим не менш, нетривіальна частина AS бачить ще довші шляхи. Хоча ці шляхи можуть працювати досить добре, деякі AS дійсно можуть мати гіршу продуктивність. Як наслідок, статичний рейтинг наступного стрибка не повинен бути єдиним фактором у прийнятті рішень щодо маршрутизації.

Враховуючи, що довжина AS-PATH лише слабко корелює з продуктивністю шляху, можна стверджувати, що маршрутизатори повинні приймати рішення на основі вимірювань якості шляху. Маршрутизатори можуть регулювати (i) рейтинг наступних AS і (ii) розподіл трафіку між кількома наступними AS з однаковим рангом на основі цікавих показників продуктивності (наприклад, пропускна спроможність, затримка або втрата). Різні типи AS можуть вибирати різні методи для моніторингу продуктивності шляху, наприклад:

**- Багатодоменні шлейфові AS:** багато багатодоменних шлейфових AS можуть застосовувати існуючі методи вимірювання для інтелектуального керування маршрутами, які підтримуються комерційними маршрутизаторами. Вимірювання продуктивності в обох напрямках відносно легко зібрати, оскільки заглушка AS бачить трафік як у прямому, так і в зворотному напрямках.

**- Постачальник онлайн-послуг:** Постачальники онлайн-послуг, такі як Google і Microsoft, можуть легко відстежувати наскрізну продуктивність своїх клієнтів (наприклад, реєструючи статистику RTT на рівні TCP на своїх серверах.

**- Постачальники транзитних послуг:** для постачальників транзитних послуг моніторинг продуктивності складніший, оскільки більшість трафіку не починається й не закінчується в їхніх мережах, а через асиметричну маршрутизацію вони можуть бачити один напрямок трафіку, але не бачити інший. Тим не менш, вимірювання пасивного потоку можна використовувати для визначення продуктивності. Транзитні постачальники також можуть вимірювати продуктивність безпосередньо, використовуючи вибірку на основі хешування для вибірки обох напрямків трафіку — для підмножини потоків, які проходять через AS в обох напрямках. Ця техніка також гарантує, що AS вимірює лише низхідну частину шляху до пункту призначення, а не частину між джерелом і ISP.

У всіх трьох випадках AS може вимірювати продуктивність кількох шляхів за допомогою «ін’єкції маршруту», щоб спрямувати невелику частину трафіку на кожен альтернативний шлях для постійного відстеження продуктивності. Крім того, AS можуть використовувати активне зондування t o відстежувати альтернативні шляхи, а не направляти «реальний» трафік клієнтів цими шляхами.

На основі вимірювань продуктивності AS може адаптувати спосіб спрямування трафіку через кілька наступних переходів. Розробка та аналіз ефективних методів адаптивного балансування навантаження є самостійною темою для досліджень. Нещодавні роботи показують, що справді можливо розробити стабільні та ефективні контролери для адаптації потоку трафіку за кількома шляхами [45–48].

**4.6.2 Розробка міждоменного трафіку**

Окрім вибору шляхів із хорошою продуктивністю, оператори покладаються на вибір міждоменного шляху, щоб збалансувати навантаження на свої мережеві посилання. Оператори розробляють трафік, вимірюючи обсяги трафіку та вибираючи шляхи, які оптимізують потік трафіку через різні канали зв’язку. Сьогодні деякі оператори використовують AS-PATH для допомоги в плануванні трафіку. Інші підходи (які не покладаються на AS-PATH) є більш прийнятними:

**Розробка вихідного трафіку:** оператори балансують навантаження на межі з’єднань з іншими AS, налаштовуючи політики, які призначають «локальні переваги» маршрутам BGP. Це все ще можливо при маршрутизації наступного переходу з обмеженням, що переваги залежать лише від безпосереднього сусіда, а не від наступних переходів у ASPATH. Таким чином, мережеві оператори не можуть використовувати «регулярні вирази» на AS-PATH, щоб (скажімо) спрямувати деякий трафік через альтернативну точку виходу на основі парної чи непарної другої AS на шляху. Політики, засновані на регулярних виразах, мабуть, досить незграбні і не можуть широко використовуватися на практиці. Натомість мережеві оператори можуть вибирати різні рейтинги наступного переходу для різних (груп) префіксів призначення як спосіб спрямувати частину трафіку іншими шляхами.

**Розробка вхідного трафіку:** контроль потоку вхідного трафіку, як відомо, важко, оскільки Інтернет-маршрутизація базується на пункті призначення. Сьогодні деякі AS використовують «попереднє AS» — штучне додавання додаткових переходів, щоб AS-PATH виглядав довшим — щоб зробити маршрути через них менш бажаними для інших. Це часто використовується як (дещо незграбний) спосіб позначення «резервного» маршруту. Зауважте, що маршрутизація наступного переходу, видаляючи довжину AS-PATH із процесу прийняття рішень, робить попередній AS неефективним. Натомість мережеві оператори можуть використовувати спільноти BGP для сигналізації про резервні маршрути до сусідніх AS [50]; якщо ці AS експортують «сигнал» своїм сусідам, інші AS також можуть надати нижчий рейтинг резервним шляхам. Можливо, що ще важливіше, моніторинг якості шляху дозволяє AS приймати рішення на основі продуктивності, що природно веде до рішень про маршрутизацію, які уникають надмірного навантаження на резервні канали з меншою пропускною здатністю. Тим не менш, як і з сучасним BGP, розробка вхідного трафіку залишається певною мірою «чорною магією».

Крім того, інженерія трафіку значно виграє від багатокрокової маршрутизації. Як було зазначено раніше, AS може легко розділити трафік на кілька наступних переходів, що ведуть до того самого пункту призначення; Налаштування частки трафіку, призначеної для кожного наступного переходу, є набагато більш детальним підходом до проектування трафіку, ніж вибір одного шляху для кожного префіксу призначення.

BGP страждає від багатьох серйозних проблем. Вважається, що спрощення BGP є привабливою альтернативою розширенню або заміні BGP. В роботі запропоновано наступну маршрутизацію — три прості обмеження щодо того, як маршрути вибираються та експортуються, у поєднанні із зовнішніми механізмами для моніторингу площини даних і безпеки. Маршрутизація наступного переходу надає AS достатню експресивність для реалізації своїх бізнес- та інженерних цілей, уникаючи при цьому деяких основних проблем BGP (наприклад, повільна конвергенція, велика площа атаки, стимули до «брехні», труднощі з підтримкою багатокрокової маршрутизації тощо).

**ВИСНОВКИ**

Аналіз протоколів маршрутизації у корпоративних мережах дозволяє зазначити, що існують дві категорії протоколів: протоколи статичної маршрутизації і протоколи динамічної маршрутизації, і що протоколи OSPF та BGP відносяться до протоколів динамічної маршрутизації.

OSPF — це протокол маршрутизації за станом з’єднання, який зазвичай використовує алгоритм SPF (DSPF) Дейкстри для обчислення повної таблиці маршрутизації в результаті будь-якої зміни стану з’єднання в мережі, що сповільнює конвергенцію маршрутизації. Визначено, що алгоритм DSPF, який використовується при розрахунку таблиці маршрутизації, має значний вплив на продуктивність маршрутизаторів OSPF. У цій роботі, по-перше, представлено систему оцінки ефективності маршрутизації, продемонстровано життєздатність структури, охарактеризувавши продуктивність DSPF і оцінивши відносну вигоду ISPF. По-друге, було вимірювано продуктивність DSPF за різної топології. Також охарактеризовано продуктивність OSPF і визначено функції, що викликають вузькі місця. Було показано, що завдяки оптимізації коду та ефективним структурам даних час виконання DSPF можна скоротити на 10-30%. По-третє, було вивчено вплив оптимізації на рівні алгоритму на час конвергенції. За допомогою масштабного моделювання було показано, що використання ISPF для оптимізації обчислення таблиці маршрутизації OSPF значно покращує продуктивність маршрутизаторів OSPF. Оптимізація обчислення таблиці маршрутизації покращує швидкість реагування та масштабованість механізму маршрутизації за рахунок скорочення часу конвергенції та зменшення потреби у більшій потужності ЦП у міру зростання мережі.

Стосовно протоколу BGP, аналіз, проведений в роботі, дозволяє зазначити, що сучасна система міждоменної маршрутизації не працює належним чином, оскільки протокол BGP конвергує повільно, вибирає шляхи без урахування продуктивності, не підтримує багатокрокову маршрутизацію та має численні вразливості безпеки. Замість того, щоб додавати механізми до вже складного протоколу або переробляти міждоменну маршрутизацію з нуля, запропоновано спростити BGP і вирішувати такі проблеми, як продуктивність поверхні даних поза межами протоколу маршрутизації. Було запропоновано перехід від сучасної маршрутизації на основі шляху до маршрутизації наступного переходу — рішення, які вибирають та експортують маршрути лише на основі сусіднього домену. Ґрунтуючись на теоретичних і експериментальних результатах, було показано, що маршрутизація наступного переходу дозволяє отримати значно кращу продуктивність мережі, ніж маршрутизація на основі шляхів, і особливо ефективна для запобігання найсерйознішим проблемам конвергенції BGP, поряд з іншими перевагами (включно з більшою придатністю до багатокрокової маршрутизації та зменшену поверхню атаки). Отже, результати дослідження показують, що маршрутизація наступного переходу забезпечує зменшення кількості повідомлень про оновлення та змін маршрутизації через низку мережевих подій. Ці результати також ілюструють, наскільки маршрутизація наступного переходу є особливо ефективною для запобігання найсерйознішим проблемам конвергенції, коли AS відчуває сотні змін маршрутизації та десятки змін пересилання. Це не тільки зменшує перебої в роботі даних, але й значно зменшує накладні витрати на розповсюдження повідомлень про оновлення BGP.

**ПЕРЕЛІК ПОСИЛАНЬ**

1. A. Shaikh, Experience in black-box OSPF measurement. Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement, 2021.

2. K.L. Calvert, et al., Modeling Internet Topology. IEEE Comm. Magazine, 2019.

3. E.W. Dijkstra, A Note on Two Problems in Connection with Graphs. Num. Math., Vol. 1, 2018.

4. H. El-Sayed, M. Ahmed, M. Jaseemuddin, Routing Software Performance Evaluation Framework. UAEU Tech Report, 2019.

5. J. McQuillan, I. Richer and E. C. Rosen, The New Routing Algorithm for the ARPANET. IEEE Transactions on Communications, COM-28(5); pp. 711- 719, May 2022.

6. J. Moy, OSPF: Anatomy of an Internet Routing Protocol. Addison-Wesley, February 2021.

7. J. Moy, OSPF Version 2. RFC 2328, April 2016.

8. V. Manral, R. White, and A. Shaikh, OSPF Benchmarking Terminology and Concepts, IETF Internet draft-ietf-bmwg-ospfconv-term-10.txt, June 2014

9. V. Manral, R. White, and A. Shaikh, Considerations When Using Basic OSPF Convergence Benchmarks. IETF Internet draft-ietf-bmwg-ospfconv-applicability07.txt, June 2015.

10. C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, “Delayed Internet routing convergence,” IEEE/ACM Trans. Networking, vol. 9, no. 3, pp. 293–306, 2021.

11. N. Kushman, S. Kandula, and D. Katabi, “Can you hear me now?! it must be BGP,” ACM SIGCOMM Computer Communications Review, Apr. 2017.

12. N. Kushman, S. Kandula, D. Katabi, and B. Maggs, “R-BGP: Staying connected in a connected world,” in Proc. USENIX NSDI, 2016.

13. P. B. Godfrey, M. Caesar, I. Haken, Y. Singer, S. Shenker, and I. Stoica, “Stabilizing route selection in BGP,” tech.rep., University of Illinois at Urbana-Champaign, Jan. 2020. http://hdl.handle.net/2142/14841.

14. S. Kent, C. Lynn, and K. Seo, “Secure border gateway protocol (S-BGP),” Journal on Selected Areas in Communications, no. 18(4), pp. 582–592, 2019.

15. K. Butler, T. Farley, P. McDaniel, and J. Rexford, “A survey of BGP security issues and solutions,” Proceedings of the IEEE, January 2022.

16. L. Subramanian, M. Caesar, C. T. Ee, M. Handley, M. Mao, S. Shenker, and I. Stoica, “HLP: A next generation inter-domain routing protocol,” in Proc. ACM SIGCOMM, pp. 13–24, ACM, 2015.

17. X. Yang, D. Clark, and A. W. Berger, “NIRA: A New Inter-domain Routing Architecture,” IEEE/ACM Trans. Networking, vol. 15, no. 4, pp. 775–788, 2017.

18. P. B. Godfrey, I. Ganichev, S. Shenker, and I. Stoica, “Pathlet routing,” in Proc. ACM SIGCOMM, 2019.

19. J. P. John, E. Katz-Bassett, A. Krishnamurthy, T. Anderson, and A. Venkatarmani, “Consensus routing: The Internet as a distributed system,” in Proc. Networked Systems Design and Implementation, Apr. 2022.

20. J. Feigenbaum, V. Ramachandran, and M. Schapira, “Incentive-compatible interdomain routing,” in Proc. ACM Electronic Commerce, pp. 130–139, 2021.

21. D. Wendlandt, I. Avramopoulos, D. Andersen, and J. Rexford, “Don’t secure routing protocols, secure data delivery,” in Proc. Hotnets V, 2016.

22. O. Nordstrom and C. Dovrolis, “Beware of BGP attacks,” ACM SIGCOMM Computer Communication Review, vol. 34, no. 2, pp. 1–8, 2020.

**ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ**