

Виконав Плескач Роман Володимирович /
(ІПБ студента)

НУБІП України
КИЇВ – 2021

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ Завідувач кафедри Комп'ютерних
систем і мереж

д.т.н., професор Лахно В.А.
(вчене звання і ступінь) (підпис) (ініціали і прізвище)

«__» _____ 20__ року

ЗАВДАННЯ ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ РОБОТИ
СТУДЕНТА
Плескача Романа Володимировича

(прізвище, ім'я, по батькові)

Спеціальність 123 Комп'ютерна інженерія
(шифр і назва)

Освітня програма Комп'ютерні системи і мережі
(назва)

Орієнтація освітньої програми _____
(освітньо-професійна або освітньо-наукова)

Тема магістерської роботи: Дослідження векторного протоколу EIGRP при зміні
коефіцієнтів метрики, для оптимізації маршрутів

затверджена наказом ректора НУБіП від «23» жовтня 2020 р. № 1578 "С"

Термін подання завершеної роботи на кафедру _____
(рік, місяць, число)

Вихідні дані до магістерської роботи:

1. Завдання кафедри на виконання магістерської роботи
2. Наукова література з тематики магістерської роботи

НУБІП України

Перелік питань, що підлягають дослідженню.

1. Огляд проблематики
2. Проектування
3. Постановка експерименту

НУБІП України

Перелік графічного матеріалу Логічна схема мережі. Результати дослідження комбізованої метрики, при різних значеннях складових її коефіцієнтів

Дата видачі завдання “ ” 20 р.

НУБІП України

Керівник магістерської роботи

Блозва А.І.

(підпис)

(прізвище та ініціали)

Завдання прийняв до

(підпис)

виконання Плескач Р.В.

(прізвище та ініціали студента)

АНОТАЦІЯ

НУБІП України

В даний час у сучасних мережах при використанні алгоритмів маршрутизації виникає проблема у виборі найбільш підходящої метрики. Коли

алгоритм маршрутизації оновлює таблицю маршрутизації, його головною метою

є визначення найкращої інформації для вилучення до таблиці. Кожен алгоритм

маршрутизації інтерпретує поняття "найкраща" по-своєму. Для кожного шляху в

мережі алгоритм генерує число, яке називається метрикою. Як правило, що

менше величина цього числа, то краще шлях. Метрики можуть розраховуватися

з урахуванням однієї характеристики шляху. Поєднуючи кілька параметрів,

можна розраховувати і складніші метрики. При обчисленні значення метрики

використовують кілька характеристик шляху.

Метою даного проекту є покращення векторного протоколу EIGRP,

синтез і оптимізація отримання оптимального алгоритму маршрутизації, що

зводиться до задачі вибору метрики (об'єднання метрик). При цьому основними

вимогами до алгоритмів маршрутизації залишаються забезпечення якості

НУБІП України

доставки інформації з урахуванням завантаження каналів зв'язку і кількості переходів.

В роботі ставиться завдання дослідження різних

алгоритмів маршрутизації з метою вибору оптимального, за зазначеними критеріями.

Для досягнення поставленої мети, необхідно: мінімізувати вартісну функцію, під якою може розумітися будь-яка метрика (об'єднання метрик), яка використовується в алгоритмі маршрутизації. Для досягнення мети необхідно

розглянути алгоритми з різними комбінаціями метрик для зменшення їх вартісної функції.

ANNOTATION

Currently, in modern networks when using routing algorithms there is a problem in choosing the most appropriate metric. When a routing algorithm updates a routing table, its main goal is to determine the best information to include in the table. Each routing algorithm interprets the concept of "best" in its own way. For each path in the network, the algorithm generates a number called a metric. Generally, the smaller the value of this number, the better the path. Metrics can be calculated based on one characteristic of the path. Combining several parameters, you can calculate more

complex metrics. When calculating the value of the metric using several characteristics of the path

The aim of this project is to study the vector EIGRP protocol, synthesis and optimization of obtaining the optimal routing algorithm, which is reduced to the problem of metric selection (combination of metrics). The main requirements for routing algorithms are to ensure the quality of information delivery, taking into account the load of communication channels and the number of transitions.

The paper aims to study different routing algorithms in order to select the optimal one, according to these criteria.

НУБІП України

To achieve this goal, it is necessary to minimize the cost function, which can be understood as any metric (combination of metrics) used in the routing algorithm. To achieve this goal, it is necessary to consider algorithms with different combinations of metrics to reduce their cost function.

НУБІП України

ЗМІСТ

ЗМІСТ..... 5

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 7

НУБІП України

ВСТУП..... 8

1 ОГЛЯД ПРОБЛЕМАТИКИ МАРШРУТИЗАЦІЇ..... 10

1.1 Основні функції маршрутизаторів..... 10

НУБІП України

1.2 Адміністративна відстань..... 11

1.3 Метрики маршрутів..... 12

1.4 Побудова таблиці маршрутизації..... 14

1.5 Механізми маршрутизації..... 15

НУБІП України

1.6 Вартість маршруту..... 20

1.7 Протоколи сімейства IGP..... 20

1.9 Підсумок порівнянь..... 35

НУБІП України

2 ПРОЕКТУВАННЯ МЕРЕЖІ..... 37

2.1 Створення віртуальної машини..... 37

2.2 Встановлення EVE-NG..... 38

2.3 Налаштування правил Брандмауера GCP..... 39

НУБІП України

2.4 Налаштування мережі..... 40

3 ПОСТАНОВКА ЕКСПЕРИМЕНТУ..... 45

3.1 Дослідження композитної метрики, при різних значеннях складових її коефіцієнтів	45
---	----

3.2 Дослідження протоколу EIGRP з параметрами метрики за замовченням.....	49
---	----

3.3 Дослідження протоколу EIGRP з врахуванням параметру навантаження в метриці	51
--	----

3.4 Дослідження протоколу EIGRP з врахуванням параметру надійності в метриці	57
--	----

3.5 Дослідження протоколу EIGRP з врахуванням параметру MTU в метриці	58
---	----

ВИСНОВКИ	59
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ	61

ДОДАТОК А	62
-----------------	----

НУБІП України

НУБІП України

НУБІП України

НУБІП України

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AS (англ. Autonomous System) – автономна система.

DV (англ. Distance Vector) – дистанційно векторний протокол.

LS (англ. Link State) – протокол стану каналу зв'язку.

DND (англ. Dynamic neighbor discovery) – динамічне виявлення сусідів.

FD (англ. Feasible Distance) – можлива відстань.

RD (англ. Reported distance) – повідомлена відстань.

AD (англ. Advertised distance) – оголошена відстань.

НУБІП України

НУБІП України

НУБІП України

НУБІП України

ВСТУП

НУБІП України

Зазвичай порядок, у якому маршрутизатори спілкуються один з одним і

обмінюються інформацією, стає можливим завдяки протоколу маршрутизації.

Протокол маршрутизації також дозволяє маршрутизаторам вибирати маршрути між будь-якими двома вузлами комп'ютерної мережі. Алгоритми маршрутизації

відповідають за вибір найкращого шляху для зв'язку. Можна сказати, що

протокол маршрутизації – це мова, якою маршрутизатор розмовляє з іншими

маршрутизаторами, щоб обмінюватися інформацією про доступність і стан мережі [2]. Іноді люди часто плутають маршрутизацію з мостом. Основна

відмінність між маршрутизацією та мостом полягає в рівні, на якому вони

працюють.

У сучасних і майбутніх середовищах маршрутизації Enhanced Interior Gateway Routing Protocol (EIGRP) пропонує більші переваги та функції в порівнянні з історичними протоколами векторної маршрутизації, такими як

Routing Information Protocol версії 1 (RIPv1) і Interior Gateway Routing Protocol

(IGRP). Ці переваги включають швидку конвергенцію, менше використання пропускну здатності та підтримку балансування навантаження.

Enhanced Interior Gateway Routing Protocol (EIGRP) – це протокол

внутрішнього шлюзу, який підходить для багатьох різних топологій і носіїв. У

добре спроектованій мережі EIGRP добре масштабується і забезпечує надзвичайно швидкий час конвергенції з мінімальним мережевим трафіком.

Основними перевагами EIGRP є:

- дуже низьке використання мережевих ресурсів під час нормальної

роботи; тільки пакети вітання передаються в стабільній мережі;

- коли відбувається зміна, поширюються тільки зміни таблиці маршрутизації, не вся таблиця маршрутизації; це зменшує навантаження на

мережу, на яке впливає сам протокол маршрутизації;
- малий час конвергенції для змін в топології мережі (в деяких ситуаціях конвергенція може бути майже миттєвою).

EIGRP – це покращений дистанційно-векторний протокол, який обчислює найкоротший шлях призначення в рамках мережі за допомогою алгоритму дифузійного поновлення (DUAL) [7].

Поруч з перевагами EIGRP, слід відзначити, що він здійснює пошук одного найкращого маршруту з мінімальною метрикою, тобто є одношляховим, або здійснює балансування маршрутів у мережі з однаковою метрикою, що спричиняє максимальне використання знайденого найкращого або альтернативного шляху та його перевантаження, в той час як інші вузли (ресурси) мережі не будуть задіяні в процесі передачі трафіку. Такий підхід не дає можливості досягти стану повноцінної рівноваги, балансованого розподілу навантаження між всіма можливими альтернативними шляхами.

1 ОГЛЯД ПРОБЛЕМАТИКИ МАРШРУТИЗАЦІЇ

НУБІП України

1.1 Основні функції маршрутизаторів

Основним пристроєм, який відповідає за здійснення процесу маршрутизації, є маршрутизатор.

Маршрутизатор виконує дві ключові функції:

маршрутизація – підтримка таблиці маршрутизації та обмін інформацією про зміни в топології мережі з іншими маршрутизаторами. Ця функція реалізується за допомогою одного або кількох протоколів маршрутизації чи за допомогою статично налаштованих таблиць маршрутизації.

комутація – перенаправлення пакетів з вхідного інтерфейсу маршрутизатора на вихідний інтерфейс в залежності від таблиці маршрутизації. При необхідності маршрутизатор може зробити переупаковку IP пакета з одного виду пакетів канального рівня до іншого.

В даний час через поширення технології Ethernet на магістральних каналах передачі даних широке поширення отримали комутатори третього рівня. Такі комутатори, як і маршрутизатори будують таблиці маршрутизації та на їх основі здійснюють маршрутизацію мережного трафіку.

Необхідно розуміти, що у механізмі комутації пакетів маршрутизатором і комутатором третього рівня є серйозні відмінності. Маршрутизатор здійснює переупакування корисної інформації з поступаючих до нього пакетів різних протоколів другого рівня. Наприклад, з Ethernet в PPP або Frame Relay.

Комутатори третього рівня можуть лише переглядати інформацію мережевого рівня що знаходиться в пакетах, поступаючих на його інтерфейси. На основі отриманої інформації комутатор третього рівня комутує пакет на

вихідний інтерфейс. Комутатор третього рівня не здійснює переупаковування корисної інформації з поступаючих до нього пакетів. Отже, застосування комутаторів третього рівня можливе тільки в мережах Ethernet. Однак завдяки

високій продуктивності комутатори третього рівня здійснюють швидку маршрутизацію пакетів у мережах з пропускнуою здатністю каналів зв'язку до 1 Гбіт/с і вище. Протоколи маршрутизації та алгоритми роботи маршрутизації на маршрутизаторах та комутаторах третього рівня однакові. З цієї причини далі ми

будемо розуміти під маршрутизаторами як їх самих, так і комутатори третього рівня.

Алгоритми роботи маршрутизаторів можуть бути як статичними, так і динамічними.

При статичній маршрутизації конфігурування проводиться вручну.

При динамічній маршрутизації обміном інформації управляють протоколи маршрутизації, завдяки яким маршрутизатори можуть відстежувати топологію мережі та коригувати маршрути. І статична, і динамічна конфігурації,

а також їх комбінування переслідують одну і ту ж мету забезпечити обмін інформацією між віддаленими вузлами.

1.2 Адміністративна відстань

У процесі маршрутизації проводиться вибір оптимального маршруту до мережі одержувача. Оскільки одночасно на маршрутизаторі може бути запущено відразу кілька протоколів маршрутизації, необхідний метод вибору між маршрутами, одержаними від різних протоколів маршрутизації. У

маршрутизаторах для вибору маршрутів, отриманих від різних протоколів маршрутизації використовується концепція адміністративної відстані.

Адміністративна відстань сприймається як міра достовірності джерела інформації про маршрут. Це має сенс тоді, коли маршрутизатор має інформацію про маршрут до мережі одержувача від кількох протоколів маршрутизації.

Малі значення величини адміністративної відстані кращі від великих значень. Стандартні значення адміністративної відстані встановлюються такими, щоб значення, що вводяться вручну, були кращими за значення отримані автоматично, і протоколи маршрутизації з більш складними метриками були кращими за протоколи маршрутизації які мають прості метрики. У таблиці 1.1 представлені адміністративні відстані, які застосовуються у маршрутизаторах Cisco для різних протоколів маршрутизації.

Таблиця 1.1 – Адміністративна відстань в маршрутизаторах Cisco

Джерело інформації про маршрут	Стандартна адміністративна відстань
Пряме з'єднання	0
Статичний маршрут	1
Сумарний маршрут EIGRP	5
Зовнішній BGP	20
Внутрішній EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIPv1 RIPv2	120
Зовнішній EIGRP	170
Внутрішній BGP	200
Невідомий	255

1.3 Метрики маршрутів

Визначення того, який маршрут є найкращим шляхом до мережі одержувача, є особливістю притаманною будь-якому протоколу. Кожен протокол має власну міру того, що є найкращим. Маршрутизатори характеризують маршрут мережі за допомогою метрики маршруту.

Процес маршрутизації вибирає маршрут, що має найменше значення метрики. Метрики можуть бути обчислені на основі однієї чи кількох

характеристик. Найчастіше в алгоритмах маршрутизації використовуються такі параметри:

- ширина смуги пропускання являє собою засіб оцінки обсягу інформації, яка може бути передана каналом зв'язку;

- затримка – проміжок часу, необхідний для переміщення пакета по кожному з каналів зв'язку від відправника до одержувачу. Затримка залежить від пропускної спроможності проміжних каналів, розміру черг у портах маршрутизаторів, завантаження мережі та фізичної відстані;

- завантаження – середня завантаженість каналу зв'язку за одиницю часу;
- надійність – відносна кількість помилок на каналі зв'язку;
- кількість переходів – кількість маршрутизаторів, які повинен пройти пакет, перш ніж він досягне пункту призначення;

- вартість – значення, зазвичай обчислюється на основі пропускної спроможності, грошової вартості або інших одиниць вимірювання, що призначаються адміністратором.

В таблиці 1.2 показано загальні значення за замовчуванням для пропускної здатності та затримки на різних типах інтерфейсів маршрутизатора Cisco.

Таблиця 1.2 Загальні значення за замовчуванням інтерфейсів

Interface Type	Bandwidth, kbps	Delay, usec
Serial	1544	20000
Gigabit Ethernet	1000000	10
Fast Ethernet	100000	100
Ethernet	10000	1000

До пункту призначення може існувати безліч шляхів і всі вони можуть відображатися в таблиці маршрутизації. Якщо існує більш ніж один шлях до вузла одержувача, протокол маршрутизації повинен вибрати один шлях як найкращий і помістити його в таблицю маршрутизації. Однак багато протоколів маршрутизації підтримують механізм балансування навантаження, при якому в таблицю маршрутизації можуть бути записані декілька можливих маршрутів до вузла одержувача, і передача трафіку здійснюватиметься по кожному з маршрутів.

1.4 Побудова таблиці маршрутизації

Однією з основних задач маршрутизаторів є побудова таблиці маршрутизації з урахуванням даних отриманих від протоколів маршрутизації та налаштувань введених вручну.

Вибір маршруту для занесення до таблиці маршрутизації повинен ґрунтуватися по таких критеріях:

- доступність IP-адреси переходу. Процес маршрутизації полягає у послідовній передачі трафіку від відправника до одержувача. Маршрутизатор повинен знати IP адресу наступного маршрутизатора в ланцюжку передачі трафіку.

метрика маршруту. Якщо перехід можливий, протокол маршрутизації вибирає найкращий можливий маршрут передачі. Критерієм вибору маршруту є мінімальна метрика маршруту.

- префікс. Маршрутизатор розглядає довжину префікса

(маска підмережі), якщо є кілька маршрутів до мережі одержувача, але з різними префіксами, то в таблицю маршрутизації заносяться всі маршрути.

- адміністративна відстань маршруту. Якщо маршрутизатор має

більше одного маршруту до одержувача, критерієм вибору для занесення до

таблиці маршрутизації є мінімальна адміністративна відстань.

Після створення таблиці маршрутизації маршрутизатор повинен підтримувати її точну відповідність реальній топології мережі. Підтримка

таблиць маршрутизації здійснюється або адміністратором мережі вручну або за

допомогою динамічних протоколів маршрутизації. Незалежно від того, чи

маршрути конфігуруються вручну або за допомогою протоколів маршрутизації, точність відображення маршрутів є ключовим фактором у здатності маршрутизатора забезпечувати пересилання даних їй одержувачам.

1.5 Механізми маршрутизації

Існує кілька механізмів маршрутизації, які використовує маршрутизатор

для побудови і підтримки в актуальному стані своєї таблиці маршрутизації.

Зазвичай при побудові таблиці маршрутизації маршрутизатор застосовує комбінацію наступних методів маршрутизації:

- пряме з'єднання;

- статична маршрутизація;

- маршрутизація за замовчанням, - динамічна маршрутизація.

І хоча кожен із цих методів має свої переваги та недоліки, вони не є взаємовиключними.

Пряме з'єднання – це маршрут, який є локальним по відношенню до маршрутизатора. Якщо один з інтерфейсів маршрутизатора з'єднаний, з якоюсь мережею безпосередньо, то при отриманні пакета, адресованого такої підмережі, маршрутизатор відразу відправляє пакет на інтерфейс, до якого вона підключена, не використовуючи протоколи маршрутизації.

Прямі з'єднання завжди є найкращим способом маршрутизації. Оскільки маршрутизатору завжди відома безпосередньо приєднана до нього мережа, пакети, призначені для неї, направляються з перших рук, і маршрутизатор не покладається на інші засоби визначення маршрутів, наприклад на статичні або динамічні механізми маршрутизації.

Статичні маршрути – це маршрути до мереж одержувачів, які адміністратор мережі вручну вносить у таблицю маршрутизації.

Статичний маршрут визначає IP-адресу наступного сусіднього маршрутизатора або локальний вихідний інтерфейс, який використовується для направлення трафіку до певної мережі одержувача.

Як випливає із самої назви, статичний маршрут не може бути автоматично адаптований до змін у топології мережі. Якщо маршрутизатор або інтерфейс, визначений у маршруті, стають недоступними, маршрут до мережі одержувача стає недоступним.

Перевагою цього способу маршрутизації є те, що він виключає весь службовий трафік, пов'язаний із підтримкою та коригуванням маршрутів.

Статична маршрутизація може бути використана у таких ситуаціях:

- коли адміністратор потребує повний контроль маршрутів використовуваних маршрутизатором;
- коли необхідне резервування динамічних маршрутів;
- коли є мережі, які можна досягти єдиним можливим шляхом;

НУБІП УКРАЇНИ

коли небажано мати службовий трафік необхідний для оновлення таблиць маршрутизації, наприклад під час використання комутованих каналів зв'язку.

- коли використовуються застарілі маршрутизатори, які не мають необхідного рівня обчислювальних можливостей для підтримки динамічних протоколів маршрутизації.

Найкращою топологією для використання статичної маршрутизації є топологія «зірка». При даній топології маршрутизатори, підключені до центральної точки мережі, мають лише один маршрут для всього трафіку, який проходить через центральний вузол мережі. І один або два маршрутизатори в центральній частині мережі мають статичні маршрути до всіх віддалених вузлів.

Однак згодом така мережа може зрости до десятків і сотень маршрутизаторів із довільною кількістю підключених до них підмереж. Кількість статичних маршрутів у таблицях маршрутизації збільшуватиметься пропорційно до збільшення кількості маршрутизаторів у мережі. Щоразу при додаванні нової підмережі або маршрутизатора адміністратор повинен буде додавати нові маршрути до таблиць маршрутизації на всіх необхідних маршрутизаторах.

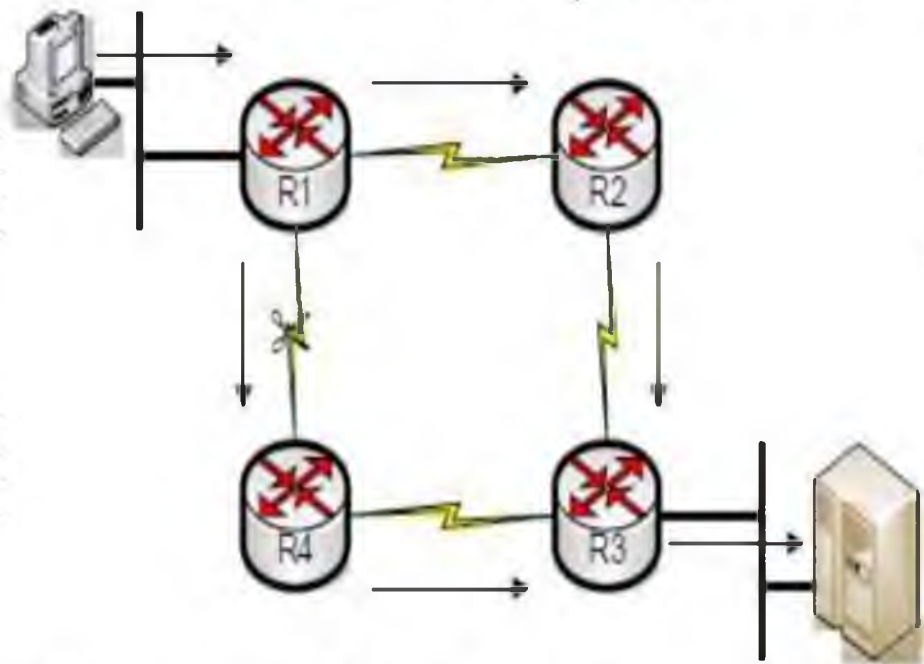
При такому підході може настати момент, коли більшу частину свого робочого часу адміністратор займатиметься підтримкою таблиць маршрутизації в мережі. І тут необхідно зробити вибір у бік використання динамічних протоколів маршрутизації.

Інший недолік статичної маршрутизації проявляється за зміни топології корпоративної мережі. При цьому адміністратор повинен вручну вносити всі зміни до таблиць маршрутизації маршрутизаторів, на які вплинули зміни у топології мережі.

Протоколи динамічної маршрутизації можуть автоматично відстежувати зміни у топології мережі.

При використанні протоколів динамічної маршрутизації адміністратор мережі конфігурує вибраний протокол на кожному маршрутизаторі в мережі. Після цього маршрутизатори починають обмін інформацією про відомі їм мережі та їх стани. Причому маршрутизатори обмінюються інформацією лише з тими маршрутизаторами, де запущено той самий протокол динамічної маршрутизації. Коли відбувається зміна топології мережі, інформація про ці зміни автоматично поширюється всім маршрутизаторам, і кожен маршрутизатор вносить необхідні зміни до своєї таблиці маршрутизації.

Показана на рисунку 1.1 мережа по-різному адаптується до змін топології, залежно від того, який тип маршрутизації використовується: динамічний чи статичний.



Рисунк 1.1 – Динамічний маршрут

Статична маршрутизація дозволяє переслати пакет з однієї мережі до іншої на основі вручну заданих маршрутів. У цьому прикладі маршрутизатор R1 завжди пересилає потоки даних, призначені маршрутизатору R3, через маршрутизатор R4. Маршрутизатор звертається до своєї таблиці маршрутизації і

Відповідно до інформації про статичному маршруті направляє пакет на вузол одержувач.

Якщо маршрут від маршрутизатора R1 до маршрутизатора R4 з якоїсь причини стає недоступним, маршрутизатор R1 не може передавати пакет маршрутизатору R4 по ньому. Відповідно, до повторного ручного конфігурування маршрутизатора R1 на передачу пакетів через маршрутизатор R2 зв'язок з мережею одержувачем буде неможливим.

Динамічна маршрутизація забезпечує більшу гнучкість. Відповідно до таблиці маршрутизації, створеної на маршрутизаторі R1, пакет може бути доставлений до пункту призначення за кращим маршрутом через маршрутизатор R4. Однак залишається доступним і другий шлях до пункту призначення через маршрутизатор R2. Коли маршрутизатор R1 дізнається, що канал до маршрутизатору R4 вийшов з ладу, він оновить свою таблицю маршрутизації, роблячи маршрут через маршрутизатор R2 кращим маршрутом до пункту призначення. У цьому випадку маршрутизатори продовжують пересилання пакетів резервного каналу.

Після того як маршрут між маршрутизаторами R1 та R4 відновиться, маршрутизатор R1 знову оновлює свою таблицю маршрутизації, віддаючи перевагу основному маршруту через маршрутизатор R4.

Протоколи динамічної маршрутизації можуть також для підвищення ефективності роботи мережі застосовувати механізм балансування навантаження по кількома маршрутами.

Успішне функціонування динамічної маршрутизації залежить від виконання маршрутизатором двох його основних функцій динамічної маршрутизації:

- підтримка таблиці маршрутизації в актуальному стані;
- своєчасне поширення інформації про відомі їм мережі та маршрути серед інших маршрутизаторів.

При поширенні інформації про мережі механізм динамічної маршрутизації використовує один з протоколів маршрутизації. Такий протокол визначає набір правил, що використовуються маршрутизатором при здійсненні зв'язку з сусідніми маршрутизаторами. Протокол маршрутизації визначає:

- яким чином поширюються оновлення маршрутів;
- яка інформація міститься в оновленнях;
- як часто розсилаються оновлення;
- яким чином виконується пошук одержувачів оновлень.

1.6 Вартість маршруту

Метрика маршруту або відстань до мережі також називається вартістю маршруту, одна з головних складових інформації, що передається між маршрутизаторами про відомі їм маршрути до мереж одержувачів. Кожен протокол маршрутизації має власні параметри та алгоритми розрахунку метрик маршрутів. В якості параметрів для розрахунку метрик маршрутів виступають: кількість переходів на шляху до мережі одержувача, швидкість передачі даних по каналу зв'язку або складніші метрики, в яких беруться до уваги відразу кілька характеристик маршруту.

Більшість протоколів маршрутизації ведуть бази даних про всі відомі їм мережі, а також про всі відомі маршрути до цих мереж. Якщо маршрутизатору відомо більше одного маршруту до мережі одержувача, він порівнює метрики цих маршрутів і передає в таблицю маршрутизації маршрут з найменшою метрикою.

1.7 Протоколи сімейства IGP

IGP-протоколи – вони ж Interior Gateway Protocols – умовний клас протоколів динамічної маршрутизації, що працюють у межах однієї автономної системи (AS). Дані протоколи передбачають несуперечливе настроювання всіх

учасників обміну маршрутною інформацією та єдину логіку архітектури мережі,

тому мають мінімальні засоби для обробки ситуацій, коли один із вузлів навмисно налаштований неправильно. Для IGP-протоколів характерно наявність автоматичного виявлення сусідніх пристроїв, які беруть участь у обміні

маршрутною інформацією, і навіть захист реалізований підписом службових

пакетів даних.

Протоколи динамічної маршрутизації поділяються на три категорії: дистанційно-векторні (DV), за станом каналу (LS) та гібридні протоколи.

Інформація про маршрути, що спільно використовується різними сегментами

мережі, визначається обраним протоколом маршрутизації, які зберігаються в

таблицях маршрутизації. Щоб підтримувати таблицю маршрутизації у актуальному стані, маршрутизатор повинен визначати найкращу інформацію для

зберігання. Кожен протокол визначає це з урахуванням певного критерію з

допомогою алгоритмів, які компілюють значення, відомі як метрики. Метрики

генеруються як мінімум з однієї характеристики мережі або частини з декількох

характеристик. Найбільш поширені вимірювання зазвичай включають кількість

переходів, затримку, смугу пропускання, навантаження, надійність (тобто

помилки в каналі), вартість тощо. Серед трьох типів протоколів маршрутизації:

найпростіший у налаштуванні – це дистанційно-векторний протокол, який використовує відстань та напрямок для пошуку найкращого шляху до місця призначення за допомогою алгоритму, що називається алгоритмом

Беллмана-Форда. Виявлення мережі досягається шляхом збору інформації

безпосередньо від підключених сусідніх маршрутизаторів, які у свою чергу,

могли отримувати інформацію від сусідніх маршрутизаторів. Для обміну

інформацією дистанційно-векторні протоколи використовують метод, відомий як

локальна трансляція. Вона надсилає дані на будь-який пристрій, підключений до інтерфейсу маршрутизатора. Дистанційно векторний протокол не дає про те, хто приймає та обробляє ці широкомовні повідомлення, і що вони періодичні за своїм підходом [1]. Ці протоколи розсилатимуть оновлення через регулярні

проміжки часу незалежно від того, чи відбулася зміна топології. Оскільки ці пакети регулярно проходять через мережу, то може генеруватися великий обсяг небажаного мережного трафіку. Приклади дистанційно векторних протоколів:

RIPv1, IGRP тощо.

1.7.1 RIP версії 1

RIP версії 1 – це протокол маршрутизації DV, який легко зрозуміти та розгорнути в AS. Хоча RIP замінений складнішими алгоритмами маршрутизації,

він все ще широко використовується в невеликих AS через свою простоту. Для

RIP не має формальної різниці між мережами та вузлами. Маршрутизатор зазвичай надає шлях, через який данина виходить з однієї мережі або AS і пересилається в іншу мережу. Таким чином, маршрутизатори повинні приймати рішення, якщо є можливість вибору пропонованого шляху пересилання.

Метрична система, що використовується в мережах RIP, – це лічильник переходів, який має максимальне значення 15 чи 16 [4]. Щоразу, коли маршрутизатор передає таблицю маршрутизації іншим маршрутизаторам, значення 1 додається до метрики всередині оновлення маршрутизації.

Максимальна кількість переходів призначена для вирішення проблеми петель маршрутизації. Петлі маршрутизації – це переважно плутанина в топології

мережі, яка виникає, коли таймери оновлення/старіння можуть бути неефективними. Якщо для лічильника стрибків встановлено значення 15, пакет

може бути переданий максимум через 15 маршрутизаторів, перш ніж буде

відкинуто, без нього пакети можуть передаватися нескінченно довго, доки не відбудеться збій у мережі або не відключаться маршрутизатори. RIP підтримує

до 6 шляхів з рівною вартістю до пункту призначення, це означає, що якщо пункт

призначення доступний різними маршрутами з однаковою кількістю переходів, маршрутизатор зберігатиме в пам'яті всі маршрути до шести (чотири за замовчуванням) [1]. Всі шляхи розміщуються в таблиці маршрутизаторів і

можуть використовуватися для балансування навантаження під час надсилання

даних. Основні особливості RIP можуть призводити до його недоліків, таких як великий інформаційний потік, неефективність системи показників і алгоритму класової маршрутизації.

1.7.2 Open Shortest Path First

Open Shortest Path First (OSPF) заснований на відкритих стандартах, має гарну сумісність із ширшим спектром обладнання і є поширеним протоколом маршрутизації у великих корпоративних мережах. Це протокол маршрутизації

LS, який використовує складнішу метричну систему для надання ефективних

рішень щодо виявлення шляхів у віддалених мережах. Вартість вимірювання

метрики розраховується шляхом зворотного перетворення пропускної спроможності каналів. По суті, швидше заслання дешевше. Шляхи з найменшою вартістю до віддалених мереж є найкращими маршрутами і зберігаються в

таблиці маршрутизації. OSPF може балансувати навантаження максимум по

шести каналах з рівною вартістю, хоча це може спричинити труднощі.

Послідовний інтерфейс маршрутизатора налаштований із тактовою частотою та смугою пропускання. Тактова частота – це швидкість, з якою дані можуть бути

надіслані за посланням, а смуга пропускання використовується протоколом

маршрутизації для розрахунку показників. За замовчуванням швидкість

послідовного інтерфейсу встановлена на 1544 Кбіт/с [2]. Існує потенційна небезпека цієї системи. Якщо для іншого каналу встановлені різні тактові

частоти, необхідно налаштувати смугу пропускання відповідним чином; в

іншому випадку OSPF розглядатиме обидві з'єднання як однакову швидкість, що

викликає проблеми з балансуванням навантаження [3]. Коли маршрутизаторам

необхідно часто запускати OSPF, цей процес виділяє багато ресурсів; ця

потенційна проблема може різко знизити швидкість мережевих послуг.

Між OSPF та RIP є кілька основних відмінностей. По-перше, порівняно з RIP, OSPF - це безкласовий протокол, який дозволяє використовувати різні маски підмережі, що, по суті, дає мережевим адміністраторам більшу гнучкість з IP-адресами та знижує втрати. По-друге, однією з привабливих переваг OSPF перед RIP є масштабованість. OSPF знає AS та області, а також може розуміти ієрархічну структуру маршрутизації. По-третє, як протокол LS, OSPF надсилає інформацію про оновлення тільки при зміні в мережі, а не надсилає періодичні оновлення через рівні проміжки часу, як у протоколах DV. Ця якість заощаджує використання смуги пропускання по всій мережі. По-четверте, хоча протокол RIP використовує широкомовну розсилку передачі інформації про маршрутизацію через мережу, що може викликати потенційні проблеми з перевантаженням мережі, OSPF використовує метод багатоадресної розсилки для зменшення мережевого трафіку, який використовує адреси, призначені для певних машин.

1.7.2.1 Пакети протоколу маршрутизації OSPF

Протокол OSPF інкапсулюється в IP, використовуючи ідентифікатор 89, не вимагає будь-якої додаткової фрагментації або складання пакетів - при виникненні такої необхідності використовується звичайна фрагментація та складання IP. Пакети протоколу OSPF мають такий формат, що великі блоки протокольної інформації можна легко розділити на дрібніші пакети. Рекомендується використовувати саме такий варіант, уникаючи можливості фрагментування IP.

Пакети протоколу маршрутизації завжди мають передаватися з нульовим значенням поля IP TOS. Якщо це можливо, пакети протоколів маршрутизації повинні мати перевагу в порівнянні зі звичайним трафіком даних IP як для прийому, так і при передачі.

Усі пакети протоколу OSPF використовують однотипні заголовки. Протокол OSPF Hello використовує пакети Hello для організації та підтримки сусідських відносин. Пакети Database Description (опис бази даних) і Link State

Request (запит стану каналу) служать для підтримки відносин суміжності.

Гарантований обмін оновленнями OSPF базується на обміні пакетами Link State Update (оновлення стану каналу) та Link State Acknowledgment (підтвердження прийому оновлення).

Кожен пакет Link State Update містить набір нових анонсів стану каналів (англ. link-state advertisement, LSA – оголошення про стан каналу) на один інтервал (англ. Hop) віддалених від пункту генерації анонсу. Один пакет Link State Update може містити анонси LSA від кількох маршрутизаторів. Кожний

запис LSA позначається ідентифікатором маршрутизатора, що створив анонс, і супроводжується контрольною сумою вмісту. У кожному запису LSA є поле типу; можливі варіанти цього поля описані у таблиці 1.2.

Пакети протоколу OSPF (за винятком пакетів Hello) передаються лише між суміжними маршрутизаторами. Це означає, що всі пакети протоколу OSPF

проходять лише один інтервал між маршрутизаторами, за винятком тих ситуацій, коли суміжність підтримується через віртуальні з'єднання (virtual adjacency).

IP-адреса відправника пакету OSPF є адресою одного із суміжних маршрутизаторів, а IP-адреса одержувача є адресою другого із суміжних маршрутизаторів або груповою IP-адресою.

Таблиця 1.3 – Типи анонсів LSA в OSPF

LSA	Опис
Router-LSA	Генеруються всіма маршрутизаторами. Цей тип LSA визначає стан інтерфейсів маршрутизатора в області. Анонс розсилається у лавинному режимі всередині області.

Network-LSA

Генерується виділеним маршрутизатором DR для широкомовних та NBMA-мереж. Цей тип LSA включає список маршрутизаторів, підключених до мережі.

Розсилається у лавинному режимі всередині області

Summary-LSA

Генерується граничними маршрутизаторами областей та розсилається в лавинному режимі в межах пов'язаної з LSA області. Кожен анонс summary-LSA описує маршрут до адресата поза даної області, але всередині даної AS (міждоменний маршрут). Тип 3 summary-LSA описує маршрути в мережі, а тип 4 - до граничних маршрутизаторів AS.

AS-external-LSA

Генерується граничними маршрутизаторами AS та розсилається по всій автономній системі. Кожен анонс AS-external-LSA описує маршрут до адресатів до іншого AS. Прийняті за замовчуванням маршрутизатори AS можуть описуватися в AS-external-LSA.

1.7.2.2 Переваги та недоліки протоколу OSPF

До основних переваг OSPF можна віднести наступне:

- Висока швидкість збіжності в порівнянні з протоколами, що

використовують дистанційно-векторну маршрутизацію;

- Підтримка мереж зі змінним розміром (робота з мережевими масками змінної довжини);

- оптимальне використання пропускнуєї спроможності (низький рівень службового трафіку) із побудовою дерева найкоротших шляхів. Таким чином, цей протокол можна використовувати навіть у дуже великих мережах (висока масштабованість).

Є також деякі недоліки:

складність OSPF, що вимагає грамотного планування, більш комплексного налаштування та адміністрування;

- Через використання алгоритму Дейкстри при побудові дерева найкоротших шляхів протокол не захищає мережу від перевантажень (відстеження завантаження каналу в динаміці не відбувається). Це вимагає реалізації додаткових методів зниження ймовірності перевантаження.

1.7.3 Enhanced Interior Gateway Routing Protocol

Enhanced Interior Gateway Routing Protocol (EIGRP) – це пропріетарний протокол Cisco, який поєднує переваги протоколів маршрутизації на основі стану каналу і векторної маршрутизації [2]. Основа EIGRP – це дистанційно векторний протокол маршрутизації, який має високий рівень передбачуваності. Порівняно з попередніми протоколами GRP, EIGRP можна легко налаштувати і адаптувати до широкого спектру мережевих топологій. EIGRP вважається розширеним дистанційно векторним протоколом через додавання кількох функцій стану каналу, таких як динамічне виявлення сусідів (DND). EIGRP також розглядається як покращений протокол IGRP внаслідок його стрімкої збіжності та постійної гарантованої топології без петель.

Для досягнення швидкої збіжності EIGRP використовує алгоритм оновлення відомий як алгоритм дифузного оновлення (DUAL). Зазвичай маршрутизатор, на якому запущено протокол EIGRP, зберігає таблиці маршрутизації своїх сусідів, щоб швидко адаптуватися до змін, які можуть бути внесені до мережі. Якщо в локальній таблиці маршрутизації немає відповідного маршруту або резервного маршруту, EIGRP повинен запросити своїх сусідів, щоб знайти альтернативний маршрут. Ці запити поширюються доти, доки не буде знайдено альтернативний маршрут або поки не буде визначено, що альтернативного маршруту не існує [2].

EIGRP оголошує маску підмережі для кожної мережі призначення. Цей атрибут робить його безкласовим протоколом маршрутизації. Це одна з функцій, яка дозволяє EIGRP підтримувати переривчасті підмережі та VLSM.

У процесі роботи замість періодичних оновлень EIGRP відправляє часткові оновлення. Ці оновлення надсилаються лише за зміни шляху або метрики маршруту. Ці оновлення містять інформацію про змінене посилання замість всієї таблиці маршрутизації. Передача цих часткових оновлень автоматично обмежується для маршрутизаторів, які потребують оновлення інформації. Ця характеристика забезпечує використання EIGRP значно меншої смуги пропускання ніж IGRP.

Механізм виявлення сусідів EIGRP дозволяє маршрутизаторам динамічно дізнаватися про інших маршрутизаторів у їх безпосередньо підключених мережах. Маршрутизатори також повинні виявляти, коли їхні сусіди стають недоступними чи непрацездатними. Цей процес досягається з низькими накладними витратами за рахунок періодичного надсилання невеликих вітальних пакетів. Поки маршрутизатор приймає вітальні пакети від сусіднього маршрутизатора, він припускає, що сусід працює, і вони можуть обмінюватися інформацією про маршрутизацію [2].

Маршрутизатори, на яких запущено протокол EIGRP, мають стати сусідами перед обміном інформацією про маршрутизацію. Для динамічного виявлення сусідів маршрутизатори EIGRP використовують групову адресу 224.0.0.10. Кожен маршрутизатор EIGRP зберігає інформацію про маршрутизацію та топології у трьох таблицях:

- таблиця сусідів, де зберігається інформація про сусідів EIGRP;
- таблиця топології, де зберігається інформація про маршрутизацію, отримана від сусідніх маршрутизаторів;
- таблиця маршрутизації, де зберігаються кращі маршрути.

Адміністративна відстань EIGRP становить 90, що менше адміністративної відстані RIP та адміністративної відстані OSPF, тому маршрути EIGRP будуть кращими за ці маршрути. EIGRP використовує надійний транспортний протокол (RTP) для надсилання повідомлень та обчислює його

метрику, використовуючи смугу пропускання, затримку, надійність та навантаження. За замовчанням при розрахунку метрики використовуються лише смуга пропускання та затримка, а надійність та навантаження дорівнюють нулю.

EIGRP використовує концепцію автономних систем. Автономна система – це набір маршрутизаторів із підтримкою EIGRP, які мають стати сусідами EIGRP.

На кожному маршрутизаторі всередині автономної системи має бути налаштований той самий номер автономної системи; інакше маршрутизатори не стануть сусідами.

Можлива відстань (FD) відноситься до метрики найкращого маршруту для досягнення мережі. Маршрутизатор буде вказано у таблиці маршрутизації.

Повідомлена відстань (RD) відноситься до метрики, оголошеної сусіднім маршрутизатором для певного маршруту. Іншими словами, це метрика маршруту, який використовується сусіднім маршрутизатором для досягнення мережі. Наприклад, EIGRP був налаштований на двох маршрутизаторах RT1 та RT2. Передбачається, що RT2 безпосередньо підключений до підмережі 10.0.1.0/24 і оголошує цю підмережу (10.0.1.0/24) EIGRP. Припускаючи також, що RT2 метрика для досягнення цієї підмережі становить 28160. Коли підмережа оголошується RT1, RT2 повідомляє RT1, що його метрика для досягнення 10.0.1.0/24 дорівнює 10. З точки зору RT1 ця метрика вважається повідомленою відстанню на цей маршрут. RT1 отримує оновлення та додає метрику сусіда до повідомленої відстані. Ця метрика називається можливою відстанню і зберігається у таблиці маршрутизації RT1[2].

Наступник – це маршрут із найкращою метрикою для досягнення пункту призначення. Цей маршрут зберігається у таблиці маршрутизації. Можливий наступник – це резервний шлях для досягнення того ж пункту призначення, який

можна використовувати негайно, якщо наступний маршрут не спрацює. Ці резервні маршрути зберігаються у таблиці топології. Щоб маршрут був обраний як можливий наступник, має бути виконана одна умова. Оголошена відстань

(AD) сусіда для маршруту повинна бути меншою за можливу відстань (FD) наступного сусіда.

Таблиця топології EIGRP містить усі вивчені маршрути до пункту призначення. У таблиці містяться всі маршрути, отримані від сусіда, наступники та можливі наступники для кожного маршруту, а також інтерфейси, якими були отримані оновлення. У таблиці також містяться всі локально підключені підмережі, що включені в процес EIGRP. Найкращі маршрути (наступники) з таблиці топології зберігаються в таблиці маршрутизації. Можливі наступники зберігаються лише у таблиці топології та можуть використовуватися негайно, якщо основний маршрут не працює.

EIGRP пропонує безліч переваг у порівнянні з іншими протоколами маршрутизації, включаючи такі:

- підтримка VLSM. EIGRP – це протокол безкласової маршрутизації, який містить маску підмережі маршруту у своєму оновленні;
- швидка збіжність. Використовуючи концепцію можливих наступників, визначену в DUAL, EIGRP може попередньо вибрати наступний шлях до пункту призначення. Це забезпечує дуже швидку збіжність при збої з'єднання;

- низьке завантаження ЦП при нормальній роботі каналом надсилаються лише «привіт» та часткові оновлення. Оновлення маршрутизації не розсилаються лавинною розсилкою та обробляються лише періодично;

- додаткові оновлення – EIGRP не надсилає повне оновлення маршрутизації; він надсилає лише інформацію про змінений маршрут;

- масштабованість – за рахунок використання VLSM та складної складової метрики мережі EIGRP можуть бути величезного розміру;

- просте налаштування – EIGRP підтримує ієрархічну структуру мережі,

але не вимагає строгих рекомендацій щодо налаштування, таких як ті, які необхідні для OSPF;

- автоматичне підсумовування маршруту – EIGRP виконуватиме автоматичне підсумовування за основними межами бітів;

- автентифікація маршруту MD5. Починаючи з версії програмного забезпечення Cisco IOS 11.3, EIGRP може бути налаштований для автентифікації пароля MD5 при оновленні маршруту

1.7.3.1 Пакети протоколу маршрутизації EIGRP

Протокол EIGRP використовує п'ять типів пакетів:

- HELLO/ACK (англ. Acknowledgment) – multicast-пакети, що відправляються для виявлення/відновлення сусіда, що не потребують підтвердження про отримання. Пакет HELLO, який не містить даних, також використовується як підтвердження. Пакет підтвердження ACK завжди надсилається в режимі одиночної відправки та містить ненульовий номер підтвердження;

- UPDATE. Пакети оновлень використовуються для передачі параметрів вузлів призначення. Коли виявляється новий сусід, йому надсилаються пакети UPDATE, щоб він міг створити свою таблицю топології. У цьому випадку пакети UPDATE надсилаються в режимі одиночної відправки. В інших випадках, наприклад, при зміні вартості зв'язку, такі пакети надсилаються в режимі multicast. Оновлення завжди передаються із підтвердженням;

- QUERY та REPLY. Пакети запитів (QUERY) та відповідей (REPLY) надсилаються, коли маршрути призначень переходять у активний стан. Пакети QUERY завжди надсилаються в режимі multicast, тільки якщо вони не

надсилаються у відповідь на отриманий запит. У цьому випадку запит надсилається в unicast режимі назад наступному елементу, який створив початковий запит. REPLY завжди посилаються у відповідь на QUERY, щоб сповістити запитувача про те, що переходити в активний стан не потрібно,

оскільки той, що відгукується, має можливі наступні елементи. Пакети REPLY надсилаються в режимі одиночної відправки запитувачу. Запити та відповіді передаються з підтвердженням;

- REQUEST-пакети використовуються для отримання специфічної (конкретної потрібної в даний момент) інформації від одного або декількох сусідів, які можуть передаватися в multicast- або unicast-режимах. Запити передаються із негарантованою доставкою.

1.7.3.2 Метрики EIGRP

EIGRP використовує метрики так само, як IGRP. Кожен маршрут таблиці маршрутів має пов'язану метрику. EIGRP використовує складову метрику так само, як IGRP, за винятком того, що вона модифікується множителем 256. Слід зазначити, що смуга пропускання, затримка, навантаження, надійність і MTU є допоміжними метриками. Як і IGRP, EIGRP вибирає маршрут, в першу чергу, на основі смуги пропускання та затримки або складової метрики з найменшим числовим значенням. Коли EIGRP обчислює цю метрику для маршруту, він називає її допустимою відстанню до маршруту. EIGRP обчислює допустиму відстань до всіх маршрутів у мережі. Метрика EIGRP заснована на 5 компонентах

[2]:

- bandwidth (*BW*) – найменша пропускна спроможність між вузлами джерелом та призначення. Пропускна спроможність виражається у кілобітах за секунду (Кбіт/с). Вона має бути статистично налаштована для точного представлення інтерфейсів, на яких працює EIGRP. Наприклад, пропускна спроможність для стандартного інтерфейсу 56 кбіт/с та для інтерфейсу T1

становить 1544 кбіт/с. Щоб точно налаштувати смугу пропускання, ми використовуємо команду інтерфейсу `bandwidth kbps`;

- `delay (DELAY)` – сумарний час затримки інтерфейсів по всьому

шляху. Затримка виражається у мікросекундах. Вона також має бути статистично

налаштована для точного представлення інтерфейсу, на якому працює EIGRP.

Затримку на інтерфейсі можна настроїти за допомогою команди інтерфейсу `delay time_in_micro-seconds`;

- `reliability (REL)` – найгірший показник надійності по всьому шляху

на підставі `keepalive`-повідомлень. Надійність – це число в діапазоні від 1 до 255,

де 255 – це 100-відсотково надійний маршрут, а 1 – ненадійний маршрут;

- `load (LOAD)` – найгірший показник завантаження каналу на всьому

шляху на підставі рівня передачі пакетів та налаштованої пропускної

спроможності на інтерфейсі. Навантаження – це число в діапазоні від 1 до 255,

яке показує вихідне навантаження інтерфейсу. Це значення динамічне, і його

можна переглянути за допомогою команди `show interfaces`. Значення 1 вказує на

мінімально завантажений маршрут, тоді як 255 вказує на 100% завантажений

маршрут,

- `MTU` – найменше MTU на всьому шляху. MTU включається до

оновлень EIGRP, але фактично не використовується для підрахунку метрики.

Максимальний блок передачі (MTU) – це найменше зареєстроване значення

MTU на шляху, зазвичай 1500. Показник затримки зазвичай використовується

для пропускної здатності, коли впливає на рішення щодо маршрутизації в IGRP

або EIGRP. Зміна пропускної здатності може вплинути на інші протоколи

маршрутизації, такі як OSPF. Зміна затримки впливає лише на IGRP і EIGRP.

EIGRP використовує композитну метрику, одержану з п'яти підметрик.

Коли EIGRP обчислює композитну метрику, він використовує формулу, яка

включає п'ять констант або значень «к». За замовчуванням для підрахунку

метрики використовуються BW та $DELAY$. Інші критерії не рекомендується використовувати, оскільки це призведе до частих перерахунків маршрутів. Встановлюючи K_2 , K_4 і K_5 на 0, по суті зводить нанівець підметрику навантаження, надійності та MTU.

Розрахунок композитної метрики маршрутизатором завжди буде дещо відрізняться від результату, коли вона розраховується вручну. Це пов'язано з тим, як маршрутизатор обробляє математичні операції з плаваючою комою, що призводить до невеликих розбіжностей округлення.

EIGRP підраховує метрику з використанням K -коefficientів, що передаються у пакетах HELLO. За замовчуванням значення coefficientів такі: $K_1 = K_3 = 1$, $K_2 = K_4 = K_5 = 0$.

Якщо $K_5 = 0$, то приватна при REL визначається як 1 [6].

Загальна метрика обчислюється за допомогою значень BW та $DELAY$. Використовується така формула для обчислення значення BW :

$$BW = \frac{256 \times 10^7}{BW_i} \quad (1.1)$$

де BW_i є найменшою пропускнуною спроможністю з усіх вихідних інтерфейсів на шляху до мережі призначення, представлена в кілобітах.

Формула для обчислення значення $DELAY$:

$$DELAY = 256 \times Delay_i \quad (1.2)$$

де $DELAY_i$ є сумою всіх затримок, сконфігурованих на вихідних інтерфейсах на шляху до мережі призначення, в десятках мікросекунд. Затримка, що показується командою `show ip eigrp topology` або `show interface` в Cisco IOS

(англ. Internetwork Operating System), зазначена в мікросекундах, відповідно це значення потрібно поділити на 10 перед використанням у цій формулі.

EIGRP використовує отримані значення під час підрахунку загальної метрики.

При обчисленні метрики, коли $K_5 = 0$ (значення за замовчанням), використовується формула:

$$CM = (K_1 \times BW + 256 \frac{K_2}{BW} + K_3 \times DELAY) \quad (1.3)$$

Якщо значення коефіцієнтів K_1, K_2, K_3, K_4, K_5 дорівнюють значенням за умовчанням, то формула перетворюється на таку:

$$CM = BW + DELAY \quad (1.4)$$

Якщо K_5 не дорівнює 0, то додатково виконується така операція:

$$CM = (K_1 \times BW + 256 \frac{K_2}{BW} + K_3 \times DELAY) \times K_5 \quad (1.5)$$

Таким чином, складова метрика EIGRP дозволяє ретельно (оптимально) налаштувати роботу мереж передачі даних.

1.9 Підсумок порівнянь

На основі наведених вище обговорень порівняння трьох протоколів маршрутизації підсумовані в таблиці 1.2.

Таблиця 1.4 – Порівняння RIP, OSPF і EIGRP

	RIP	OSPF	EIGRP
Категорія	DV	LS	Гібридний
Масштаб	Малі мережі	Корпоративні мережі	Середні
Маршрутизація	Класний механізм лічильника циклів маршрутизації	Безкласова	Безкласова 100% без петель
Метрика	Кількість стрибків	Обернена пропускна здатність посилення	Доступна пропускна здатність, затримка, навантаження, MTU і надійність зв'язку
Відкриття та оновлення	Періодичні оновлення	Багатоадресна передача кожного разу, коли вносяться зміни	DUAL Додаткове оновлення багатоадресної передачі

Продовження таблиці 1.4

	RIP	OSPF	EIGRP
Відновлення після збою	Повільна конвергенція	Як правило, швидше, ніж RIP	Алгоритм DUAL
Балансування навантаження	Підтримується лише на шляхах рівної вартості	Підтримується шість шляхів рівної вартості, але їх важко реалізувати	Підтримує шість шляхів рівної вартості, але зазвичай ігнорується через його складність і нестабільність

НУБІП України

2-ПРОЕКТУВАННЯ МЕРЕЖІ

2.1 Створення віртуальної машини

НУБІП України

В якості платформи для EVE-NG використовується Google Cloud. EVE-NG рекомендується розгортати в системі Ubuntu 16.04[5], тому

потрібно підготувати відповідне зображення Ubuntu. Для цього переходимо в

консоль проекту і вставляємо цю команду:

```
gcloud compute images create nested-ubuntu-xenial --source-image-family=ubuntu-1604-lts --source-image-project=ubuntu-os-cloud --licenses
```

<https://www.googleapis.com/compute/v1/projects/vm->

[options/global/licenses/enablevmx](https://www.googleapis.com/compute/v1/projects/vm-)

НУБІП України

Для створення віртуальної машини потрібно перейти в Navigation Menu/Compute Engine/VM Instances. Створюємо нову віртуальну машину:

- призначаємо назву для віртуальної машини;

- встановлюємо власний регіон і зону;

НУБІП України

- відредагуємо конфігурацію машини. Рекомендованими є процесори Intel Skylake або Cascade[5]. Тому виберемо: n1-standard-8 (8

vCPU, 30 GB memory);

НУБІП України

- вибираємо завантажувальний диск. Переходимо в Custom images, вибираємо свій проект, вибираємо зображення, яке створили і SSD диск об'ємом

50GB;

НУБІП України

- нижче дозволяємо HTTP трафік, тому що будемо використовувати EVE-NG без сертифіката SSL.

2.2 Встановлення EVE-NG

Для встановлення EVE-NG потрібно, від імені адміністратора виконати наступну команду: «`wget -O - http://www.eve-ng.net/repo/install-eve.sh | bash -i`».

Після встановлення необхідно перевірити оновлення в репозиторіях і перезавантажити віртуальну машину.

Після перезавантаження віртуальної машини з'явиться синій екран, показаний на рисунку 2.1. Натискаємо комбінацію клавіш `Ctrl + c` і вводимо команду `sudo -i` щоб стати адміністратором.

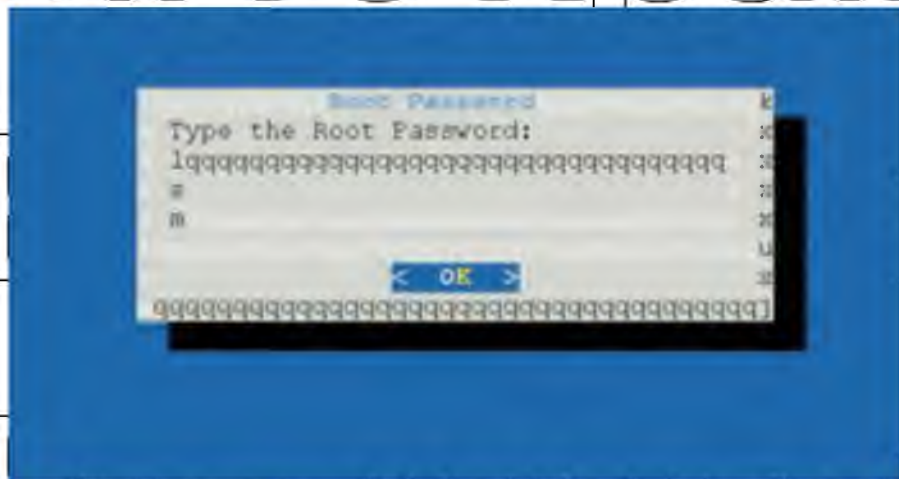


Рисунок 2.1 – Екран майстра IP

На момент налаштування IP адреси вибираємо DHCP (Рисунок 2.2). Після закінчення налаштування перезавантажимо віртуальну машину.

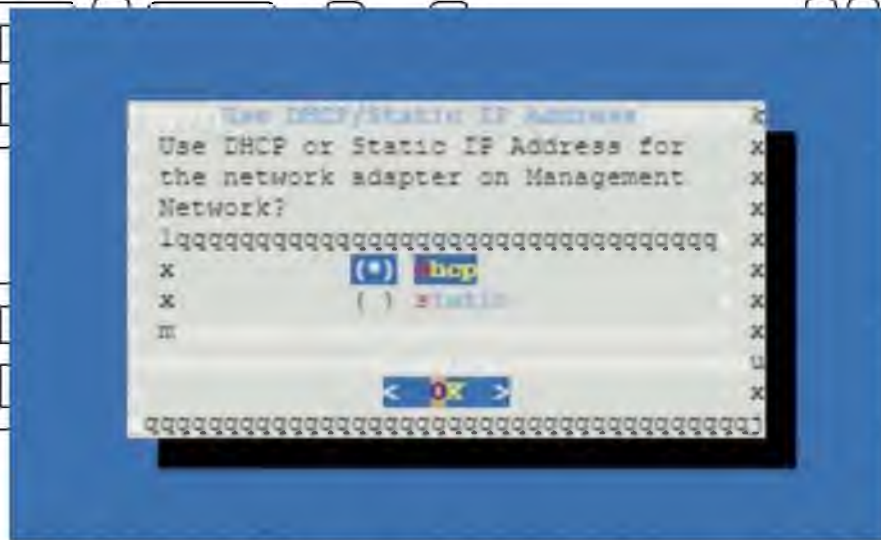


Рисунок 2.2 – Налаштування IP адресації

2.3 Налаштування правил Брандмауера GCP

За замовчуванням багато портів блокуються віртуальною машиною для зовнішнього доступу. Проблема в тому, що доступ до всіх пристроїв усередині лабораторних робіт надається по IP EVE-NG та порту пристрою.

Для створення правил брандмауера потрібно перейти в: [Navigation menu/VPC Network/Firewall rules](#). Дозволяємо доступ по будь-якому IP до портів з 0 по 65535 як показано на рисунку 2.3.

Direction of traffic ?

Ingress

Egress

Action on match ?

Allow

Deny

Targets

All instances in the network ?

Source filter

IP ranges ?

Source IP ranges *

0.0.0.0/0 ? for example, 0.0.0.0/0, 192.168.2.0/24 ?

Second source filter

None ?

Protocols and ports ?

Allow all

Specified protocols and ports

tcp : 0-65535

Рисунок 2.3 – Створення правила для брандмауєру

І створюємо ще одне таке правило, де замість Ingress ставимо Egress.

Тепер трафік може ходити в обидві сторони.

2.4 Налаштування мережі

Для дослідження маршрутизації було вирішено використовувати мережу
схема якої приведена на рисунку 2.4.

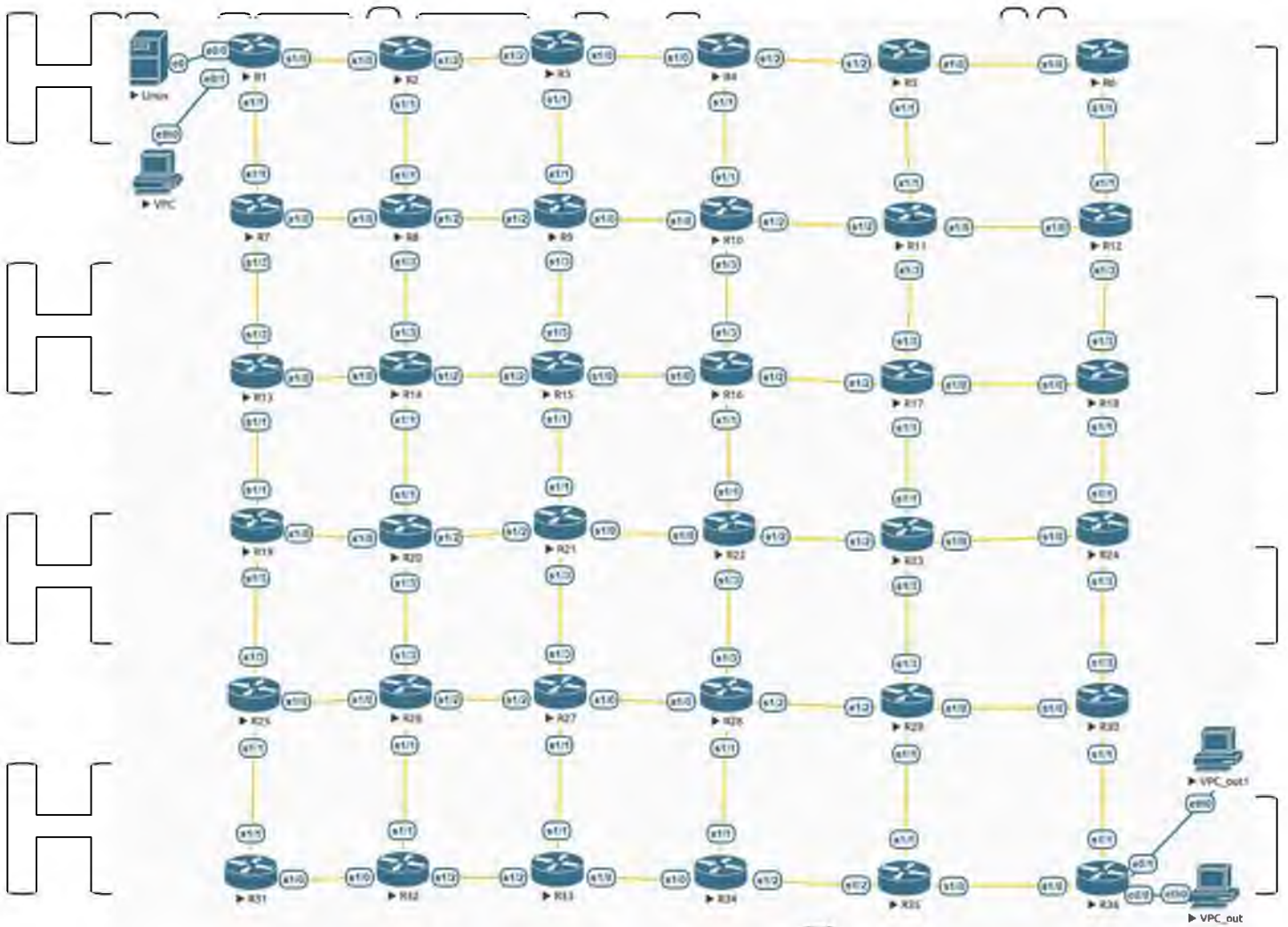


Рисунок 2.4 – Схема мережі для проведення дослідів

Схема адресації пристроїв приведена в таблиці 2.1

Таблиця 2.1 – Схема адресації пристроїв

Адреса підмережі	Інтерфейс 1	IP-адреса 1	Інтерфейс 2	IP-адреса 2
10.1.2.0/24	R1 s1/0	10.1.2.1	R2 s1/0	10.1.2.2
10.1.7.0/24	R1 s1/1	10.1.7.11	R7 s1/1	10.1.7.12
10.2.8.0/24	R2 s1/1	10.2.8.11	R8 s1/1	10.2.8.12
10.2.3.0/24	R2 s1/2	10.2.3.21	R3 s1/2	10.2.3.22
10.3.4.0/24	R3 s1/0	10.3.4.1	R4 s1/0	10.3.4.2
10.3.9.0/24	R3 s1/1	10.3.9.11	R9 s1/1	10.3.9.12

10.4.10.0/24	R4 s1/1	10.4.10.11	R10 s1/1	10.4.10.12
10.4.5.0/24	R4 s1/2	10.4.5.21	R5 s1/2	10.4.5.22
10.5.6.0/24	R5 s1/0	10.5.6.1	R6 s1/0	10.5.6.2
10.5.11.0/24	R5 s1/1	10.5.11.11	R11 s1/1	10.5.11.12
10.6.12.0/24	R6 s1/1	10.6.12.11	R12 s1/1	10.6.12.12
10.7.8.0/24	R7 s1/0	10.7.8.1	R8 s1/0	10.7.8.2
10.7.13.0/24	R7 s1/3	10.7.13.31	R13 s1/3	10.7.13.32
10.8.9.0/24	R8 s1/2	10.8.9.21	R9 s1/2	10.8.9.22
10.8.14.0/24	R8 s1/3	10.8.14.31	R14 s1/3	10.8.14.32
10.9.10.0/24	R9 s1/0	10.9.10.1	R10 s1/0	10.9.10.2
10.9.15.0/24	R9 s1/3	10.9.15.31	R15 s1/3	10.9.15.32
10.10.11.0/24	R10 s1/2	10.10.11.21	R11 s1/2	10.10.11.22
10.10.16.0/24	R10 s1/3	10.10.16.31	R16 s1/3	10.10.16.32
10.11.12.0/24	R11 s1/0	10.11.12.1	R12 s1/0	10.11.12.2
10.11.17.0/24	R11 s1/3	10.11.17.31	R17 s1/3	10.11.17.32
10.12.18.0/24	R12 s1/3	10.12.18.31	R18 s1/3	10.12.18.32
10.13.14.0/24	R13 s1/0	10.13.14.1	R14 s1/0	10.13.14.2
10.13.19.0/24	R13 s1/1	10.13.19.11	R19 s1/1	10.13.19.12
10.14.20.0/24	R14 s1/1	10.14.20.11	R20 s1/1	10.14.20.12
10.14.15.0/24	R14 s1/2	10.14.15.21	R15 s1/2	10.14.15.22

Продовження таблиці 2.1

Адреса підмережі	Інтерфейс 1	IP-адреса 1	Інтерфейс 2	IP-адреса 2
10.15.16.0/24	R15 s1/0	10.15.16.1	R16 s1/0	10.15.16.2
10.15.21.0/24	R15 s1/1	10.15.21.11	R21 s1/1	10.15.21.12
10.16.22.0/24	R16 s1/1	10.16.22.11	R22 s1/1	10.16.22.12
10.16.17.0/24	R16 s1/2	10.16.17.21	R17 s1/2	10.16.17.22
10.17.18.0/24	R17 s1/0	10.17.18.1	R18 s1/0	10.17.18.2

10.17.23.0/24	R17 s1/1	10.17.23.11	R23 s1/1	10.17.23.12
10.18.24.0/24	R18 s1/1	10.18.24.11	R24 s1/1	10.18.24.12
10.19.20.0/24	R19 s1/0	10.19.20.1	R20 s1/0	10.19.20.2
10.19.25.0/24	R19 s1/3	10.19.25.31	R25 s1/3	10.19.25.32
10.20.21.0/24	R20 s1/2	10.20.21.21	R21 s1/2	10.20.21.22
10.20.26.0/24	R20 s1/3	10.20.26.31	R26 s1/3	10.20.26.32
10.21.22.0/24	R21 s1/0	10.21.22.1	R22 s1/0	10.21.22.2
10.21.27.0/24	R21 s1/3	10.21.27.31	R27 s1/3	10.21.27.32
10.22.23.0/24	R22 s1/2	10.22.23.21	R23 s1/2	10.22.23.22
10.22.28.0/24	R22 s1/3	10.22.28.31	R28 s1/3	10.22.28.32
10.23.24.0/24	R23 s1/0	10.23.24.1	R24 s1/0	10.23.24.2
10.23.29.0/24	R23 s1/3	10.23.29.31	R29 s1/3	10.23.29.32
10.24.30.0/24	R24 s1/3	10.24.30.31	R30 s1/3	10.24.30.32
10.25.26.0/24	R25 s1/0	10.25.26.1	R26 s1/0	10.25.26.2
10.25.31.0/24	R25 s1/1	10.25.31.11	R31 s1/1	10.25.31.12
10.26.32.0/24	R26 s1/1	10.26.32.11	R32 s1/1	10.26.32.12
10.26.27.0/24	R26 s1/2	10.26.27.21	R27 s1/2	10.26.27.22
10.27.28.0/24	R27 s1/0	10.27.28.1	R28 s1/0	10.27.28.2
10.27.33.0/24	R27 s1/1	10.27.33.11	R33 s1/1	10.27.33.12
10.28.34.0/24	R28 s1/1	10.28.34.11	R34 s1/1	10.28.34.12
10.28.29.0/24	R28 s1/2	10.28.29.21	R29 s1/2	10.28.29.22
Продовження таблиці 2.1				
Адреса підмережі	Інтерфейс 1	IP-адреса 1	Інтерфейс 2	IP-адреса 2
10.29.30.0/24	R29 s1/0	10.29.30.1	R30 s1/0	10.29.30.2
10.29.35.0/24	R29 s1/1	10.29.35.11	R35 s1/1	10.29.35.12
10.30.36.0/24	R30 s1/1	10.30.36.11	R36 s1/1	10.30.36.12
10.31.32.0/24	R31 s1/0	10.31.32.1	R32 s1/0	10.31.32.2

10.32.33.0/24	R32 s1/2	10.32.33.21	R33 s1/2	10.32.33.22
10.33.34.0/24	R33 s1/0	10.33.34.1	R34 s1/0	10.33.34.2
10.34.35.0/24	R34 s1/2	10.34.35.21	R35 s1/2	10.34.35.22
10.35.36.0/24	R35 s1/0	10.35.36.1	R36 s1/0	10.35.36.2
192.168.10.0/24	R1 e0/0	192.168.1.1	Linux	192.168.1.2
192.168.11.0/24	R1 e0/1	192.168.11.1	VPC	192.168.11.2
192.168.36.0/24	R36 e0/0	192.168.36.1	VPC_out	192.168.36.2
192.168.136.0/24	R36 e0/1	192.168.136.1	VPC_out1	192.168.136.2

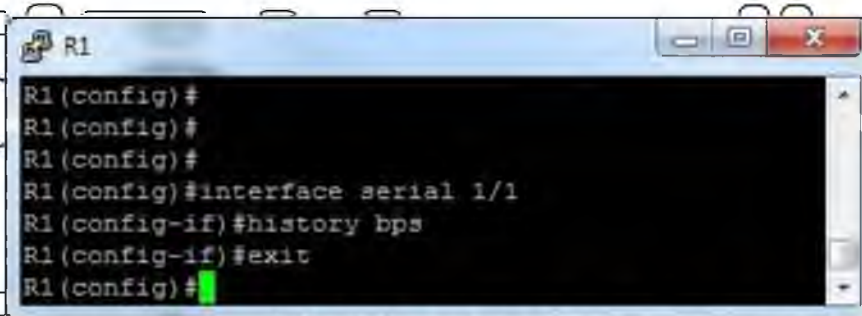
Лістинг конфігурації маршрутизаторів наведено в додатку А.

Для навантаження мережі запущено:

- `ping -f -s 9000 192.168.36.1` на вузлі Linux. Де параметр `-f` – режим флуду, у цьому режимі пакети передаються без затримок, а `-s 9000` – розмір одного пакету;
- `ping 192.168.136.1 -t -i 1` на вузлі VPC. Де параметр `-t` – режим для надсилання пакети безперервно, доки їх не перервати комбінацією `Ctrl+C`, а `-i 1` – кількість мілісекунд між відправкою кожного пакета.

Для перегляду шляху слідування пакетів використовується утиліта `tracert` за допомогою якої можна подивитися швидкість, на якій працював той чи інший порт маршрутизатора.

Для того, щоб маршрутизатор почав фіксувати навантаження на порт, необхідно на потрібному порту вказати логування швидкості графіку. Швидкість можна задати двома варіантами: пакети за секунду і кілобітах за секунду. На рисунку 2.5 показано налаштування фіксування швидкості на інтерфейсі в кілобітах за секунду.



```

R1
R1 (config)#
R1 (config)#
R1 (config)#
R1 (config)#interface serial 1/1
R1 (config-if)#history bps
R1 (config-if)#exit
R1 (config)#

```

Рисунок 2.5 – Налаштування логування швидкості трафіку

Було встановлено моніторинг на всіх портах маршрутизаторів.

Для перегляду навантаження за хвилину достатньо виконати наступну команду: `#show interface serial 1/1 history 60sec`

Інформація зберігається про останні 72 години навантаження. Також у запиті можна уточнити, яку інформацію нам хочеться побачити:

- 60min – остання година;
- 60sec – остання хвилина;
- 72hour – останні три дні;
- input – тільки вихідний графік;
- output – тільки вхідний графік.

3 ПОСТАНОВКА ЕКСПЕРИМЕНТУ

3.1 Дослідження композитної метрики, при різних значеннях складових її коефіцієнтів

Коефіцієнт K1 відповідає за включення метрики пропускну здатності в складову метрику. На рисунку 3.1 зображена зміна значення метрики в залежності від величини K1 з затримкою Serial і Ethernet інтерфейсів.

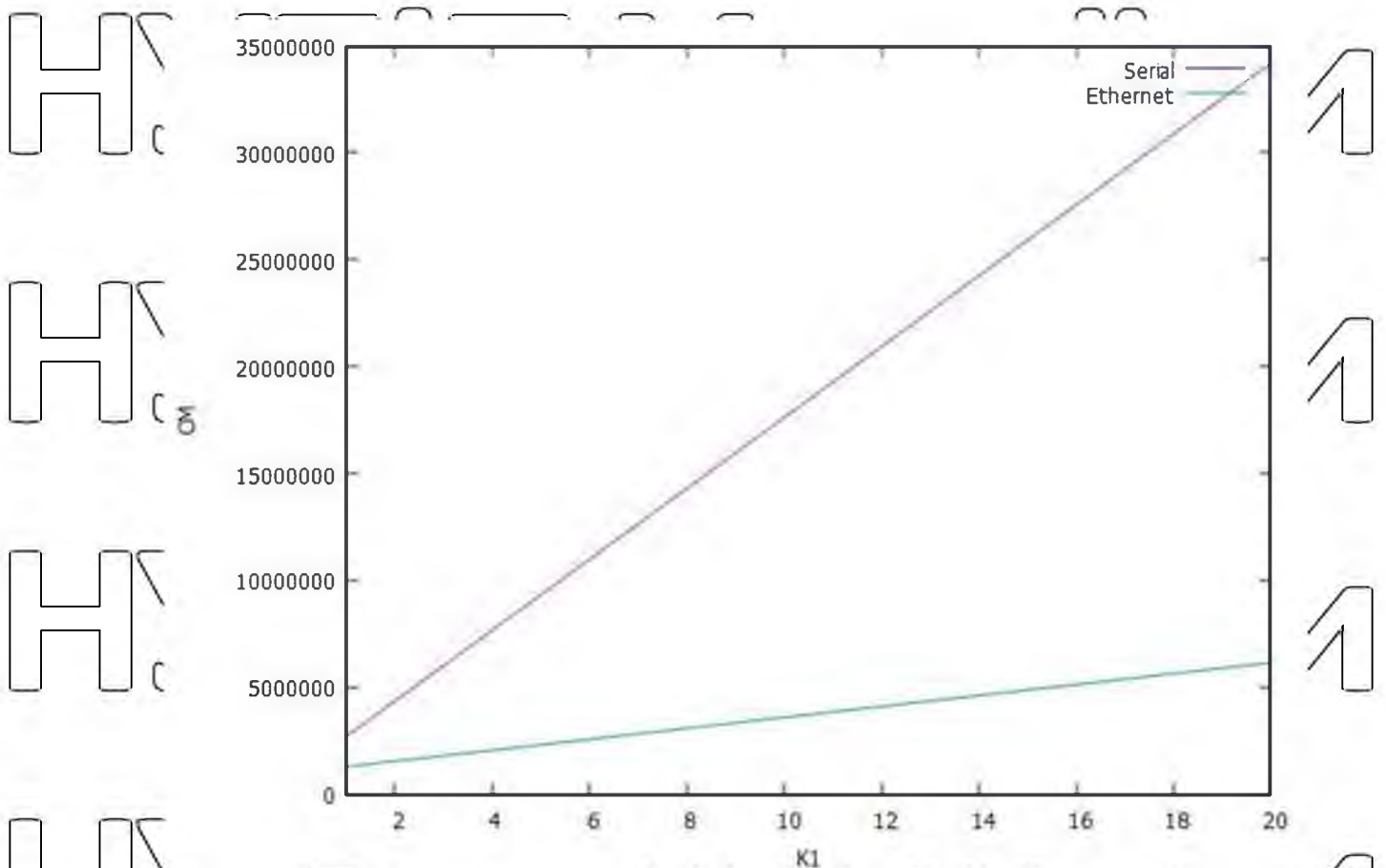


Рисунок 3.1 – Зміна величини метрики в залежності від величини K_1

Коефіцієнт K_2 відповідає за включення метрики навантаження в складову

метрику. На рисунку 3.2 зображена залежність композитної метрики від навантаження при різних значеннях коефіцієнта K_2 .

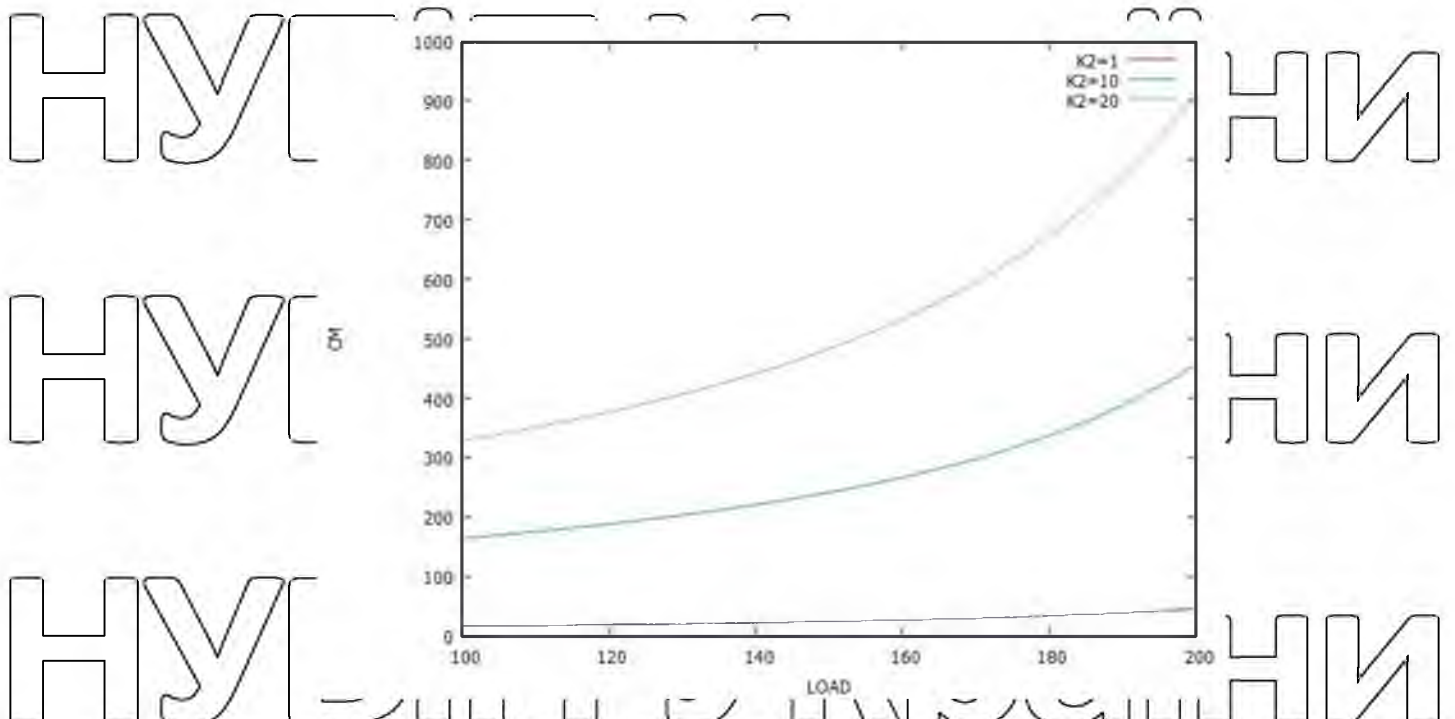


Рисунок 3.2 – Залежність величини складової метрики від навантаження

Коefіцієнт K_3 відповідає за ввіччєння метрики затримки в складову метрику. На рисунку 3.3 зображена залежність складової метрики від затримки при різних значєннях коefіцієнта K_3 .

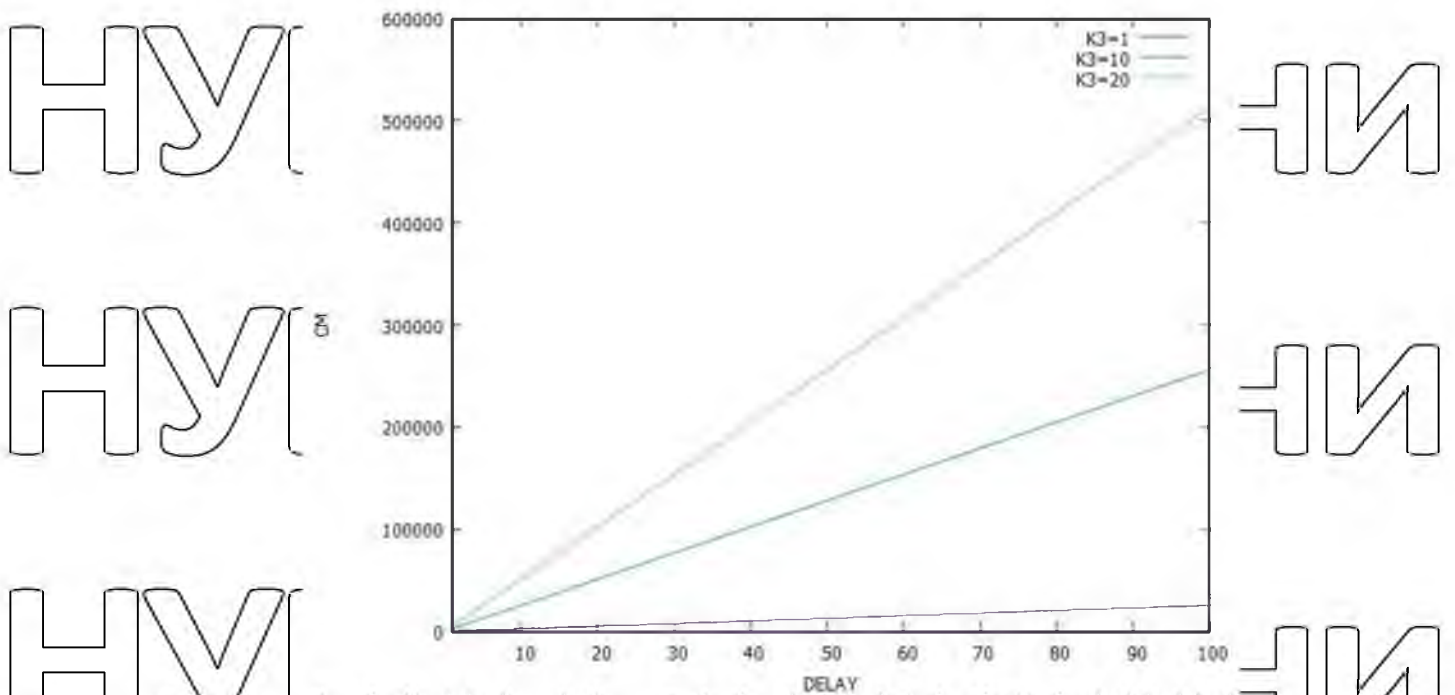


Рисунок 3.3 – Залежність величини складової метрики від затримки

Коефіцієнти K_4 і K_5 впливають на значення метрики надійності в складовій метриці. При чому щоб включити підрахунок метрики надійності коефіцієнт K_5 не повинен дорівнювати нулю. На рисунках 3.4 і 3.5 зображена

залежність величини складової метрики від значення надійності при різних значеннях K_4 і K_5 відповідно.

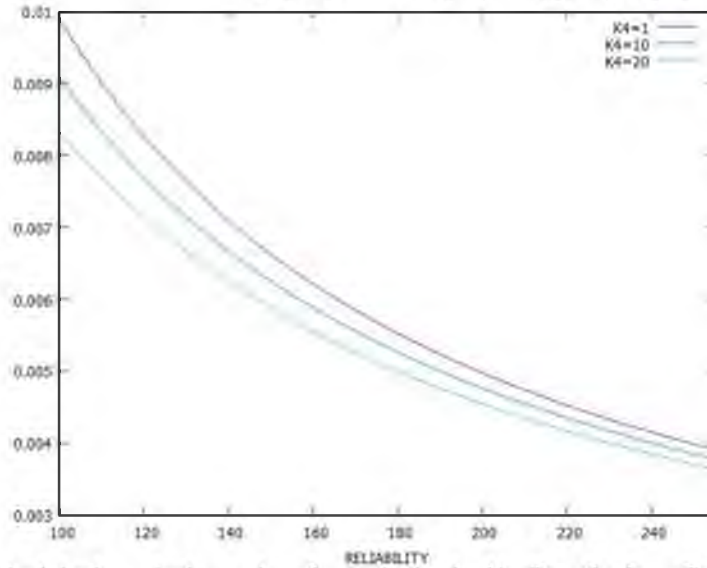


Рисунок 3.4 – Залежність величини складової метрики від надійності при різних значеннях K_4

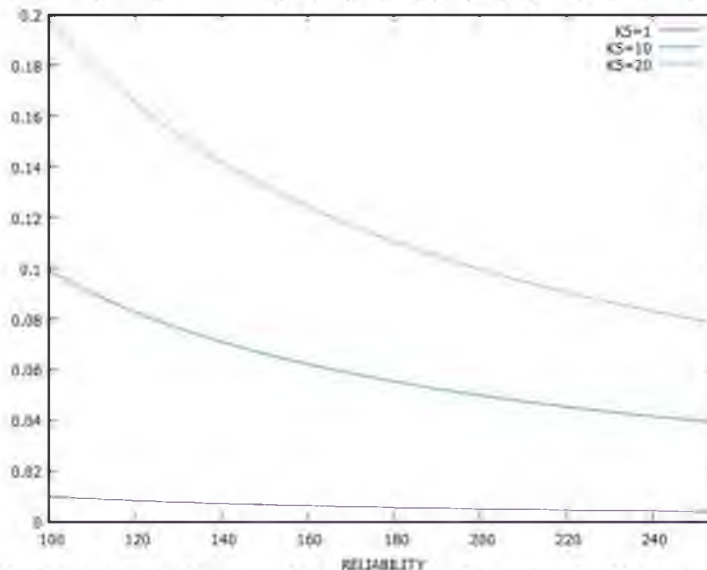


Рисунок 3.5 – Залежність величини складової метрики від надійності при різних значеннях K5

З отриманих графіків видно, що при зміні величин коефіцієнтів змінюється лише масштаб композитної метрики, а закон зміни зберігається.

Значить, якщо у всій системі використовувати однаковий масштаб коефіцієнтів, масштаб композитної метрики не зміниться. Отже, величина композитної метрики залежатиме переважно від параметрів мережі. Змінювати коефіцієнти у

більші та менші сторони має сенс при ручному налаштуванні окремих ділянок,

де є потреба змінювати напрямок трафіку. У разі збільшення коефіцієнтів K1, K2,

K3, K5 значення композитної метрики збільшується, зі збільшенням коефіцієнта

K4 значення композитної метрики зменшується.

3.2 Дослідження протоколу EIGRP з параметрами метрики за замовченням

За замовченням формула метрики EIGRP набуває такого вигляду:

$$CM = (BW \frac{10^7}{i} + Delay_i) \times 256 \quad (3.1)$$

З цієї формули і значень пропускної здатності і затримки приведених в таблиці 1.2 можна розрахувати значення метрики від маршрутизатора R1 до

мережі 192.168.36.0. З таблиці: Serial інтерфейс має пропускну здатність 1544

Кбіт/с а Ethernet має пропускну здатність 10000 Кбіт/с. Значення пропускної

спроможності, яке ми вводимо в нашу формулу обчислення метрики EIGRP – це

пропускну здатність найповільнішого каналу на шляху до цільової мережі, що

вимірюється в Кбіт/с. У нашому випадку це Serial інтерфейс, тобто ми говоримо,

що наш "найповільніший" зв'язок становить 1544 Кбіт/с. Наше значення

затримки може бути обчислено шляхом складання затримок вихідного інтерфейсу (виміряних у мікросекундах) та поділу на 10 (щоб дати нам значення, виміряне у десятках мікросекунд). Serial інтерфейс має затримку 20000

мікросекунд, а Ethernet має затримку 1000, що дає нам сумарну затримку $20000 \cdot 10 + 1000 = 201000$ мікросекунд. Однак ми хочемо, щоб наша одиниця

виміру була у десятках мікросекунд. Тому ми ділимо 201000 мікросекунд на 10, що дає нам 20100 десятків мікросекунд. Тепер у нас є два необхідні значення для

нашої формули: пропускна спроможність = 1544 Кбіт/с та затримка = 20100

десятки мікросекунд. Також слід відмітити що маршрутизатори Cisco не виконують розрахунки з плаваючою комою, тому для правильної калькуляції метрики на кожній стадії калькуляції необхідно округляти значення в меншу

сторону до цілого числа. Тепер додамо ці значення до нашої формули:

$$CM = \left(\frac{10^7}{1544} + 201000 \right) \times 256 = (6476 + 201000) \times 256 = 26576 \times 256 = 6803456$$

Теоретично в досліджуваній мережі є простір для балансування трафіку. А саме кожен можливий шлях від мережі 192.168.1.0 до мережі 192.168.36.0 має рівну вартість для EIGRP. На практиці ж балансування працює неоднозначно.

При створенні навантаження з вузла Linux за допомогою Bash сценарію зображеного на рисунку 3.6, пакети проходять тільки через інтерфейс serial 1/1 маршрутизатору R1.

```
#!/bin/bash until [ "$var1" = end ] do          cat
./512.txt >/dev/udp/192.168.136.1/8080        cat
./512.txt >/dev/udp/192.168.36.1/8080 done
```

exit 0

Рисунок 3.6 – Сценарій для навантаження маршрутизатора R36

Де 512.txt файл створений, для забезпечення максимального

навантаження на мережу, за допомогою команди: dd if=/dev/urandom of=./512.txt

bs=512 count=8.

Але при запуску модифікованого сценарію зображеного на рисунку 3.7, пакети завантажують обидва serial інтерфейси R36.

```
#!/bin/bash until [ "$var1" = end ] do
./512.txt >/dev/udp/192.168.136.1/8080
./512.txt >/dev/udp/192.168.36.1/8080
./512.txt >/dev/udp/10.25.31.12/8080
cat ./512.txt >/dev/udp/10.5.6.2/8080 done
exit 0
```

Рисунок 3.7 – Сценарій для навантаження маршрутизаторів R31 і R6

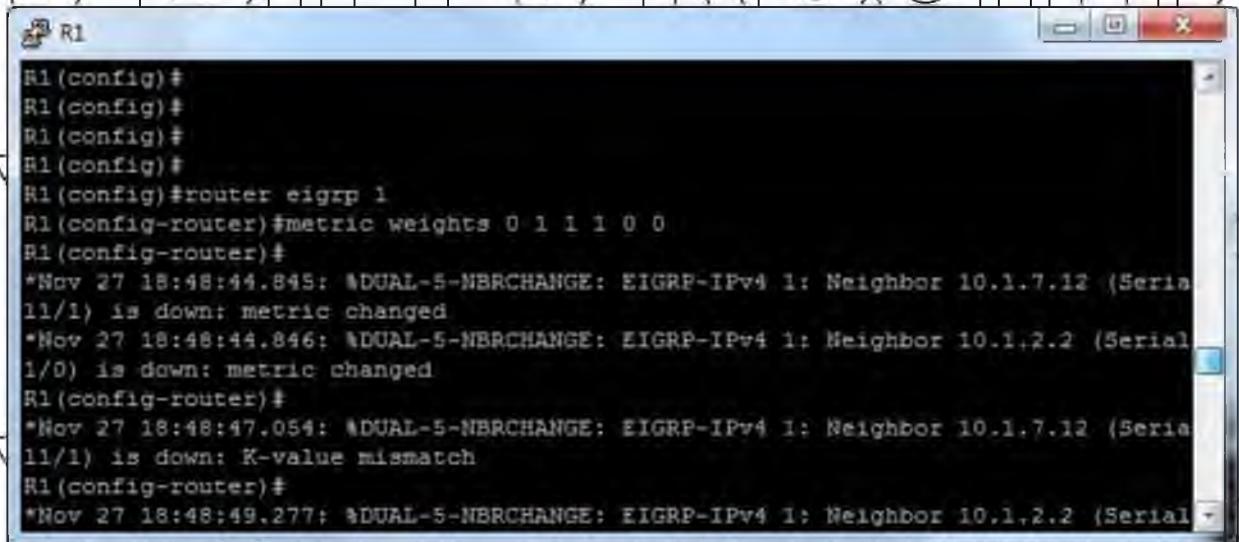
Також при створенні одночасно навантаження з мережі 192.168.1.0 в мережу 192.168.36.0 і навантаження з мережі 192.168.11.0 в мережу 192.168.136.0 дані проходять по одному маршруту.

Враховуючи результати проведених експериментів можна зробити висновок що EIGRP (з параметрами метрики за замовченням) якщо й робить балансування трафіку то робить він це випадково.

3.3 Дослідження протоколу EIGRP з врахуванням параметру

навантаження в метриці

Вивчаючи повну формулу розрахунку метрики EIGRP, можна помітити, що наявність ненульового значення K2 призведе до того, що EIGRP враховуватиме навантаження. Тому потрібно встановити K2 рівним 1, крім K1 і K3, які вже встановлені в 1 за замовчуванням. Значення K4 та K5 збережуться на рівні 0. На рисунку 3.8 показано, як можна налаштувати такий набір K-значень.



```

R1
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#router eigrp 1
R1(config-router)#metric weights 0 1 1 1 0 0
R1(config-router)#
*Nov 27 18:48:44.845: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.7.12 (Serial
11/1) is down: metric changed
*Nov 27 18:48:44.846: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.2.2 (Serial
1/0) is down: metric changed
R1(config-router)#
*Nov 27 18:48:47.054: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.7.12 (Serial
11/1) is down: K-value mismatch
R1(config-router)#
*Nov 27 18:48:49.277: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.2.2 (Serial

```

Рисунок 3.8 – Зміна коефіцієнтів метрики

Перший 0 у команді `metric weights 0 1 1 1 0 0`, показаній на рисунку 3.8, задає значення TOS, що дорівнює 0. Параметр TOS був призначений для маркування якості обслуговування (де TOS позначає тип службового байту в заголовку IPv4). Однак параметр TOS повинен дорівнювати 0. Насправді, якщо ввести число в діапазоні 1–8 і повернетеся назад, щоб вивчити свою поточну конфігурацію, можна виявити, що Cisco IOS змінила це значення на 0. Наступні п'ять чисел задають наші п'ять K-значень: $K1 = 1$, $K2 = 1$, $K3 = 1$, $K4 = 0$, $K5 = 0$.

Цей набір K-значень тепер враховуватиме не тільки пропускну здатність та затримку, але й навантаження під час розрахунку метрики. Проте є проблема. Звернувши увагу на пов'язаність консолі після нашої конфігурації. Ми виявимо, що наші сусідства були зруйновані, тому що маршрутизатор R1 тепер має інші

значення K , ніж всі інші маршрутизатори в мережі. Це означає, що сусіди EIGRP повинні мати відповідні K -значення і при зміні K -значень на одному EIGRP маршрутизаторі потрібно встановити ідентичний набір K -значень на кожному з його сусідів EIGRP.

Після додаткового врахування коефіцієнта K_2 , формула метрики набуває такого вигляду:

$$CM = \left(\frac{BW_i}{10^7} + \frac{BW_i \times (256 - LOAD) + Delay_i}{10^7} \right) \times 256 \quad (3.2)$$

LOAD в цій формулі значення динамічне, і змінюється від 1 до 255 в залежності від навантаження. Тому підставимо в цю формулу максимальне і мінімальне значення параметру навантаження:

$$CM_{min} = \left(\frac{10^7}{10^7} + \frac{10^7}{10^7} + 201000 \right) \times 256 =$$

$$= 6803456 + \frac{1544 \times (256 - 1)}{10^7 \times 256} = 6803456 + 6501 = 6809957$$

$$CM_{max} = \left(\frac{10^7}{1544} + \frac{10^7}{1544 \times (256 - 255)} + 201000 \right) \times 256 =$$

$$= 6803456 + 1544 \times (256 - 255) = 6803456 + 1658031 =$$

$$= 8461487$$

Різниця значення метрики між максимально і мінімально завантаженим каналом становить:

НУБІП України

$$CM_{max} - CM_{min} = 8461487 - 6809957 = 1658031$$

Враховуючи те що вартість додаткового переходу становить:

НУБІП України

$$DELAY = 256 \times Delay_i = 256 \times 20000 = 5120000$$

Де $DELAY_i$ – це затримка serial інтерфейсу в десятках мікросекунд

То при постійних змінах навантаження перерахунок показників за формулою 3.2 може призвести до випадкової зміни маршруту та втрати контролю над мережею передачі даних. Такий результат може призводити до відмови в обслуговуванні, що не може бути бажаною ситуацією.

Щоб запобігти створенню петель в досліджуваній мережі можна замінити значення коефіцієнта K_3 (який відповідає за затримку) на 255. Тоді вартість додаткового переходу становитиме:

НУБІП України

$$K_3 \times DELAY = K_3(256 \times Delay_i) = 255(256 \times 20000) = 130560000$$

При проведенні експериментів з мережею з врахуванням параметру навантаження виявилась одна особливість протоколу EIGRP. При створенні навантаження на інтерфейсі serial 1/1, що зображено на рисунку 3.9, перерахунок метрики не відбувається, рисунок 3.10.

НУБІП України

```

Serial1/0 is up, line protocol is up
Hardware is M4T
Internet address is 10.1.2.1/24
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, crc 16, loopback not set
Keepalive set (10 sec)
Restart-Delay is 0 secs
Last input 00:00:01, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 162 packets input, 14299 bytes, 0 no buffer
Received 55 broadcasts (0 IP multicasts)
 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
163 packets output, 16039 bytes, 0 underruns
 0 output errors, 0 collisions, 1 interface resets
 1 unknown protocol drops
 0 output buffer failures, 0 output buffers swapped out
 2 carrier transitions      DCD=up DSR=up DTR=up RTS=up CTS=up

Serial1/1 is up, line protocol is up
Hardware is M4T
Internet address is 10.1.7.11/24
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
  reliability 255/255, txload 193/255, rxload 1/255
Encapsulation HDLC, crc 16, loopback not set

```

Рисунок 3.9 – Навантаження на інтерфейс serial 1/1

```

D 192.168.36.0/24 [90/6809957] via 10.1.7.12, 00:08:31, Serial1/1
  [90/6809957] via 10.1.2.2, 00:08:31, Serial1/0

```

Рисунок 3.10 – Шляхи до мережі 192.168.36.0

На рисунках видно що при різних значеннях навантаження на інтерфейсах значення метрики не змінюється. Що на перший погляд дивно, але проаналізувавши маршрутну інформацію якою діляться маршрутизатори виявляється що EIGRP не враховує динаміку зміни метрики.

Пакети HELLO які розповсюджуються маршрутизатором по мережі за замовчування кожні 5 секунд передають значення констант K, інтервалу Hold, версії операційної системи та формату пакету протоколу EIGRP. А маршрутна інформація, в якій записано параметри підметрик, передається в пакетах Update, Query і Reply. І передаються вони при внесенні змін в зоні EIGRP.

Наприклад, після відключення одного з маршрутизаторів, параметр навантаження був врахований і всі шляхи через serial 0/1 на маршрутизаторі R1 було відкинуто так як навантаження на цьому інтерфейсі було більше. Таблиця

маршрутизації до відключення одного з маршрутизаторів і після показана на
 рисунку 3.11 і 3.12 відповідно.

```

C 10.1.2.0/24 is directly connected, Serial1/0
L 10.1.2.1/32 is directly connected, Serial1/0
C 10.1.7.0/24 is directly connected, Serial1/1
L 10.1.7.11/32 is directly connected, Serial1/1
D 10.2.3.0/24 [90/2688357] via 10.1.2.2, 00:27:09, Serial1/0
D 10.2.8.0/24 [90/2688357] via 10.1.2.2, 00:27:08, Serial1/0
D 10.3.4.0/24 [90/3200357] via 10.1.2.2, 00:27:09, Serial1/0
D 10.3.9.0/24 [90/3200357] via 10.1.2.2, 00:27:08, Serial1/0
D 10.4.5.0/24 [90/3712357] via 10.1.2.2, 00:27:08, Serial1/0
D 10.4.10.0/24 [90/3712357] via 10.1.2.2, 00:27:08, Serial1/0
D 10.5.6.0/24 [90/4224357] via 10.1.2.2, 00:27:09, Serial1/0
D 10.5.11.0/24 [90/4224357] via 10.1.2.2, 00:27:08, Serial1/0
D 10.6.12.0/24 [90/4736357] via 10.1.2.2, 00:27:08, Serial1/0
D 10.7.8.0/24 [90/2688357] via 10.1.7.12, 00:27:08, Serial1/1
D 10.7.13.0/24 [90/2688357] via 10.1.7.12, 00:27:08, Serial1/1
D 10.8.9.0/24 [90/3200357] via 10.1.7.12, 00:27:08, Serial1/1
  [90/3200357] via 10.1.2.2, 00:27:08, Serial1/0
D 10.8.14.0/24 [90/3200357] via 10.1.7.12, 00:27:08, Serial1/1
  [90/3200357] via 10.1.2.2, 00:27:08, Serial1/0
D 10.9.10.0/24 [90/3712357] via 10.1.7.12, 00:27:08, Serial1/1
  [90/3712357] via 10.1.2.2, 00:27:08, Serial1/0
  
```

Рисунок 3.11 – Таблиця маршрутизації до відключення R8

```

C 10.0.0.1/32 is directly connected, Loopback0
C 10.1.2.0/24 is directly connected, Serial1/0
L 10.1.2.1/32 is directly connected, Serial1/0
C 10.1.7.0/24 is directly connected, Serial1/1
L 10.1.7.11/32 is directly connected, Serial1/1
D 10.2.3.0/24 [90/2688357] via 10.1.2.2, 00:46:21, Serial1/0
D 10.2.8.0/24 [90/2688357] via 10.1.2.2, 00:46:20, Serial1/0
D 10.3.4.0/24 [90/3200357] via 10.1.2.2, 00:46:21, Serial1/0
D 10.3.9.0/24 [90/3200357] via 10.1.2.2, 00:46:20, Serial1/0
D 10.4.5.0/24 [90/3712357] via 10.1.2.2, 00:46:20, Serial1/0
D 10.4.10.0/24 [90/3712357] via 10.1.2.2, 00:46:20, Serial1/0
D 10.5.6.0/24 [90/4224357] via 10.1.2.2, 00:46:21, Serial1/0
D 10.5.11.0/24 [90/4224357] via 10.1.2.2, 00:46:20, Serial1/0
D 10.6.12.0/24 [90/4736357] via 10.1.2.2, 00:46:20, Serial1/0
D 10.7.8.0/24 [90/2688357] via 10.1.7.12, 00:46:20, Serial1/1
D 10.7.13.0/24 [90/2688357] via 10.1.7.12, 00:46:20, Serial1/1
D 10.8.9.0/24 [90/3200357] via 10.1.2.2, 00:00:08, Serial1/0
D 10.8.14.0/24 [90/3200357] via 10.1.2.2, 00:00:08, Serial1/0
D 10.9.10.0/24 [90/3712357] via 10.1.2.2, 00:00:08, Serial1/0
D 10.9.15.0/24 [90/3712357] via 10.1.2.2, 00:00:07, Serial1/0
D 10.10.11.0/24 [90/4224357] via 10.1.2.2, 00:00:08, Serial1/0
D 10.10.16.0/24 [90/4224357] via 10.1.2.2, 00:00:07, Serial1/0
D 10.11.12.0/24 [90/4736357] via 10.1.2.2, 00:00:08, Serial1/0
D 10.11.17.0/24 [90/4736357] via 10.1.2.2, 00:00:07, Serial1/0
D 10.12.18.0/24 [90/5248357] via 10.1.2.2, 00:00:07, Serial1/0
D 10.13.14.0/24 [90/3200357] via 10.1.7.12, 00:46:20, Serial1/1
  
```

Рисунок 3.12 – Таблиця маршрутизації після відключення R8

Враховуючи особливості передачі EIGRP параметрів метрики, можна стверджувати, що додавання параметру навантаження є нецільним.

3.4 Дослідження протоколу EIGRP з врахуванням параметру надійності в метриці

З повної формули розрахунку метрики EIGRP видно, що наявність ненульового значення K5 приведе до врахування метрики надійності в розрахунку маршруту. Змінивши стандартні значення коефіцієнтів встановленням K5 рівним 1, формула розрахунку метрики набуває такого вигляду:

$$CM = \left(BW \frac{10^7}{i} + Delay \right) \times 256 \times \frac{1}{reliability} \quad (3.3)$$

Надійність – це динамічна метрика інтерфейсу, яка оцінює надійність чи співвідношення між кількістю успішно прийнятих та всіма отриманими кадрами.

Коефіцієнт виражається як частка 255. Надійність 255 виражає 100-відсоткову надійність, надійність 230 виражає 90-відсоткову надійність, а надійність 26 виражає 10-відсоткову надійність. Тому підставимо в формулу максимальне і мінімальне значення параметру надійності:

$$CM_{min} = \left(\frac{10^7}{1544} + 201000 \right) \times 256 \times \frac{1}{1} = 6803456$$

$$CM_{max} = \left(\frac{10^7}{1544} + 201000 \right) \times 256 \times \frac{1}{255} = 26680$$

Показник надійності динамічно оновлюється IOS. Під час обчислення складеної метрики до місця призначення EIGRP враховує мінімальну надійність.

Це можна зробити, просто порівнявши надійність, оголошену сусіднім маршрутизатором, з надійністю інтерфейсу до оголошення сусіда, а також

обручи менше значення для об'єх. У цьому є істотний факт, що стосується обробки метрики надійності EIGRP. Коли EIGRP оголошує інформацію про надійність шляху, а також враховує це у складовій метриці, EIGRP не надсилає

жодних оновлень за будь-яких змін у надійності інтерфейсу. Коротше кажучи,

зміна надійності інтерфейсу не спричинить надсилання оновлень EIGRP.

Показник надійності маршруту – це знімок його поточної надійності при останньому оголошенні про нього.

3.5 Дослідження протоколу EIGRP з врахуванням параметру MTU в метриці

MTU означає максимальну одиницю передачі. Існує широко поширена

плутанина щодо компонента метрики MTU в EIGRP та використання

MTU. Як і у разі надійності та пропускної спроможності, EIGRP

оголошує мінімальний MTU на маршруті до пункту призначення. MTU

не використовується повністю, навіть якщо він передається у

повідомленні EIGRP у процесі вибору найкращого шляху. З повної

формули (1.5) розрахунку метрики EIGRP видно, що параметр

MTU неможливо включити до розрахунку композитної метрики.

НУБІП України

ВИСНОВКИ

В цій дипломній роботі описується дослідження векторного протоколу

EIGRP при зміні коефіцієнтів метрики, для оптимізації маршрутів.

У першому розділі було детально розглянуто проблематику маршрутизації, функції маршрутизаторів, метрики маршрутів, побудову таблиць маршрутизації, механізми маршрутизації і вартості маршрутів. Також було розглянуто протоколи сімейства IGP, такі як: RIP, OSPF, EIGRP, було розглянуто переваги та недоліки протоколів, пакети які вони розповсюджують, а також принципи побудови метрики. У кінці було проведено порівняння цих протоколів.

В другому розділі розглянутий один із способів розгортання платформи для проведення дослідів з віртуальним мережевим обладнанням. А саме: створення віртуальних машин в хмарному середовищі віртуалізації Google Cloud Platform, встановлення EVE-NG який являє собою віртуальне середовище наступного покоління, що дозволяє створити повноцінну віртуальну лабораторію з мережевим обладнанням та програмним забезпеченням провідних світових виробників, і було налаштовано правила брандмауера GCP для роботи з віртуальним обладнанням встановленим в EVE-NG. Також в цьому розділі була описана мережа в якій проводились дослідження, наведено логічну схему комп'ютерної мережі, схему адресації пристроїв в цій мережі, способи створення навантаження на мережу для перевірки маршрутизації та способ перевірки шляху слідування трафіку в комп'ютерній мережі.

Третій розділ присвячений постановці експерименту, висвітлено основні засади розрахунку протоколом EIGRP своєї композитної метрики, особливості вибору маршруту з однаковою вартістю композитної метрики, досліджено роботу протоколу з використанням параметрів K-коефіцієнтів за замовченням і

з зміненими цими параметрами. Була виявлена неможливість використання деяких параметрів, при розрахунку композитної метрики, які передаються в пакетах оновлень EIGRP.

У третьому розділі міститься безліч прихованих деталей про EIGRP.

Важливо знати ці метрики EIGRP до виконання налаштувань з ними. Цей розділ допомагає зрозуміти різні метрики, такі як пропускна здатність, затримка, навантаження, надійність, кількість переходів та максимальна одиниця передачі.

НУБІП України

НУБІП України

НУБІП України

НУБІП України

НУБІП України

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

НУБІП України

1. M. Sportack, "IP Routing Fundamentals," 2nd ed. California: Cisco Press.

1999.

НУБІП України

2. T. F. Johansson, "Bandwidth efficient AMR Operation for VoIP," IEEE Proceedings of the Workshop on Speech Coding, 2002.

3. C. Xianhui and J. C. Lee, "VoIP Performance over Different Interior

Gateway Protocols," International Journal of Communication Networks and Information Security (IJCNIS), 2009.

НУБІП України

4. J. C. Bolot, "Characterizing End-to-End Packet Delay and Loss in the Internet," ACM SIGCOMM, 1993.

5. Uldis Dzerkals, "EVE-NG Community Cookbook" Version 1.13

6. RFC 7868, Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP)

[Електронний ресурс] – Режим доступу до ресурсу:

<https://datatracker.ietf.org/doc/rfc7868/>

НУБІП України

7. Протокол EIGRP [Електронний ресурс] – Режим доступу до ресурсу:

https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routingprotocol-eigrp/16406-eigrp-toc.html

НУБІП України

8. Принципы работы протокола EIGRP [Електронний ресурс] – Режим

доступу до ресурсу: <https://habr.com/ru/post/420667/>

НУБІП України

9. Explain and Optimize EIGRP Metrics [Електронний ресурс] – Режим

доступу до ресурсу: <https://www.examcollection.com/certification-training/ccnptoptimize-eigrp-metrics.html>

10. Понимание EIGRP: обзор, базовая конфигурация и проверка

[Електронний ресурс] – Режим доступу до ресурсу:

<https://wiki.merionet.ru/seti/40/ponimanie-eigrp-obzor-bazovaya-konfiguraciya-iproverka/#>

НУБІП України

11. Enhanced Interior Gateway Routing Protocol (EIGRP) Informational RFC Frequently Asked Questions [Електронний ресурс] – Режим доступу до ресурсу:

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enhancedinterior-gateway-routing-protocol-eigrp/qa_C67-726299.html

12. Самойленко Н. EIGRP [Електронний ресурс] – Режим доступу до ресурсу: <http://xgu.ru/w/index.php?title=EIGRP&oldid=38608>

13. Burke A. Why Is Cisco Bothering with «Open» EIGRP? [Електронний ресурс] – Режим доступу до ресурсу: <http://pack-etpushers.net/why-is-ciscobothering-with-open-eigrp/>

14. Introduction to EIGRP [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gatewayrouting-protocol-eigrp/13669-1.html>

15. Enhanced Interior Gateway Routing Protocol (EIGRP) Informational RFC Frequently Asked Questions [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enhancedinterior-gateway-routing-protocol-eigrp/qa_C67-726299.html

ДОДАТОК А

Маршрутизатор R1

```
enable configure terminal hostname
R1 interface loopback 0 ip address
10.0.0.1 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.1.2.1 255.255.255.0 no
shutdown history bps exit interface
serial 1/1 ip address 10.1.7.11
255.255.255.0 no shutdown history bps
exit interface Ethernet 0/0 ip
address 192.168.1.1 255.255.255.0 no
shutdown history bps exit interface
Ethernet 0/1 ip address 192.168.11.1
255.255.255.0 no shutdown history
```

```
bps exit router eigrp 1 metric
weights 0 1 1 1 0 0 network
10.1.2.0 0.0.0.255 network 10.1.7.0
0.0.0.255 network 192.168.1.0
0.0.0.255 network 192.168.11.0
0.0.0.255 passive-interface
ethernet 0/0 passive-interface
ethernet 0/1
exit
end
copy running-config startup-config
Маршрутизатор
R2
```

```
enable configure terminal hostname
R2 interface loopback 0 ip address
10.0.0.2 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.1.2.2 255.255.255.0 no
shutdown history bps exit interface
```

```
serial 1/1 ip address 10.2.8.11
255.255.255.0 no shutdown history
bps exit interface serial 1/2 ip
address 10.2.3.21 255.255.255.0 no
shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0
```

```
network 10.1.2.0 0.0.0.255 network
10.2.3.0 0.0.0.255 network 10.2.8.0
0.0.0.255 exit end
copy running-config startup-config
```

Маршрутизатор R3

```
enable configure terminal hostname
R3 interface loopback 0 ip address
10.0.0.3 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.3.4.1 255.255.255.0 no
shutdown history bps exit interface
```

```
serial 1/1 ip address 10.3.9.11
255.255.255.0 no shutdown history
bps exit interface serial 1/2 ip
address 10.2.3.22 255.255.255.0 no
shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0
network 10.3.4.0 0.0.0.255 network
```

```
10.3.9.0 0.0.0.255 network 10.2.3.0
0.0.0.255 exit end
copy running-config startup-config
```

Маршрутизатор R4

```
enable configure terminal hostname
R4 interface loopback 0 ip address
10.0.0.4 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.3.4.2 255.255.255.0 no
shutdown history bps exit interface
```

```
serial 1/1 ip address 10.4.10.11
255.255.255.0 no shutdown history
bps exit interface serial 1/2 ip
address 10.4.5.21 255.255.255.0 no
shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0
network 10.3.4.0 0.0.0.255 network
10.4.10.0 0.0.0.255 network
10.4.5.0 0.0.0.255 exit end
copy running-config startup-config
```

Маршрутизатор

R5

```
enable configure terminal
hostname R5 interface loopback 0
ip address 10.0.0.5
255.255.255.255 no shutdown exit
ip routing interface serial 1/0 ip
```

```
address 10.5.6.1 255.255.255.0 no
shutdown history bps exit
interface serial 1/1 ip address
10.5.11.11 255.255.255.0 no
shutdown history bps exit
```

```
interface serial 1/2 ip address
10.4.5.22 255.255.255.0 no shutdown
history bps exit router eigrp 1
metric weights 0 1 1 1 0 0 network
10.5.6.0 0.0.0.255 network
10.5.11.0 0.0.0.255 network
10.4.5.0 0.0.0.255 exit end
```

```
copy running-config startup-config
```

Маршрутизатор

R6

```
enable configure terminal hostname
R6 interface loopback 0 ip address
10.0.0.6 255.255.255.255 no
shutdown exit ip routing interface
```

```
serial 1/0 ip address 10.3.6.2
255.255.255.0 no shutdown history
bps exit interface serial 1/1 ip
```

```

address 10.6.12.1 255.255.255.0 no
shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0
network 10.5.6.0 0.0.0.255

network 10.6.12.0 0.0.0.255

exit end

```

```

copy running-config startup-config
Маршрутизатор R7
enable configure terminal hostname
R7 interface loopback 0 ip address
10.0.0.7 255.255.255.255 no shutdown
exit ip routing interface serial 1/0

```

```

ip address 10.7.8.1 255.255.255.0 no
shutdown history bps exit interface
serial 1/1 ip address 10.1.7.12
255.255.255.0 no shutdown history
bps exit interface serial 1/3 ip
address 10.7.13.31 255.255.255.0 no
shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0
network 10.7.8.0 0.0.0.255 network
10.1.7.0 0.0.0.255 network 10.7.13.0
0.0.0.255 exit end
copy running-config startup-config

```

```

Маршрутизатор R8
enable configure
terminal hostname
R8 interface
loopback 0 ip
address 10.0.0.8
255.255.255.255 no
shutdown exit ip
routing interface
serial 1/0 ip
address 10.7.8.2
255.255.255.0 no
shutdown history
bps exit interface
serial 1/1 ip
address 10.2.8.12

```

```

address 10.7.8.2
255.255.255.0 no
shutdown history
bps exit interface
serial 1/1 ip
address 10.2.8.12

```

```

255.255.255.0 no
shutdown history
bps exit
interface serial
1/2 ip address
10.8.9.21

```

```

255.255.255.0 no
shutdown history
bps exit
interface serial
1/3 ip address
10.8.14.31

```

```

255.255.255.0 no
shutdown history
bps exit router
eigrp 1 metric
weights 0 1 1 1 0
0 network
10.7.8.0

```

```

0.0.0.255 network
10.2.8.0
0.0.0.255 network
10.8.9.0
0.0.0.255 network
10.8.14.0

```

```

0.0.0.255 exit
end
copy running-config startup-config

```

Маршрутизатор R9

```

enable configure
terminal hostname
R9 interface
loopback 0 ip
address 10.0.0.9
255.255.255.255 no

```

```

shutdown exit ip
routing interface
serial 1/0 ip
address 10.9.10.1

```



```

255.255.255.0 no
shutdown history bps
exit interface serial
1/1 ip address
10.3.9.12
255.255.255.0 no

```

```

shutdown history bps
exit interface serial
1/2 ip address
10.8.9.22
255.255.255.0 no
shutdown history bps

```

```

exit interface serial
1/3 ip address
10.9.15.31
255.255.255.0 no
shutdown history bps
exit router eigrp 1

```

```

metric weights 0 1 1 1
0 0 network 10.9.10.0
0.0.0.255 network
10.3.9.0 0.0.0.255
network 10.8.9.0
0.0.0.255 network

```

```

10.9.15.0 0.0.0.255
exit end
copy running-config startup-config

```

Маршрутизатор R10

```

enable configure terminal hostname
R10 interface loopback 0 ip address
10.0.0.10 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.9.10.2 255.255.255.0 no
shutdown history bps exit interface
serial 1/1 ip address 10.4.10.12
255.255.255.0 no shutdown history

```

```

bps exit interface serial 1/2 ip
address 10.10.11.21 255.255.255.0 no
shutdown history bps exit interface
serial 1/3 ip address 10.10.16.31

```

```

255.255.255.0 no shutdown history
bps exit router eigrp 1 metric
weights 0 1 1 1 0 0 network
10.9.10.0 0.0.0.255 network
10.4.10.0 0.0.0.255 network
10.10.11.0 0.0.0.255 network
10.10.16.0 0.0.0.255

```

```

exit end
copy running-config startup-config

```

Маршрутизатор R11

```

enable configure terminal hostname
R11 interface loopback 0 ip address
10.0.0.11 255.255.255.255 no

```

```

shutdown exit ip routing
interface serial 1/0 ip address
10.11.12.1 255.255.255.0 no
shutdown history bps exit

```

```

interface serial 1/1 ip address
10.5.11.12 255.255.255.0 no
shutdown history bps exit
interface serial 1/2 ip address
10.10.11.22 255.255.255.0 no
shutdown history bps exit

```

```

interface serial 1/3 ip address
10.11.17.31 255.255.255.0 no
shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0
network 10.11.12.0 0.0.0.255

```

```

network 10.5.11.0 0.0.0.255 network
10.10.11.0 0.0.0.255 network
10.11.17.0 0.0.0.255 exit end

```

```

copy running-config startup-config

```

Маршрутизатор R12

```

enable configure terminal hostname
R12 interface loopback 0 ip address
10.0.0.12 255.255.255.255 no

```

```

shutdown exit ip routing interface
serial 1/0 ip address 10.11.12.2

```

```

255.255.255.0 no shutdown history
bps exit interface serial 1/1 ip
address 10.6.12.12 255.255.255.0 no
shutdown history bps exit interface
serial 1/3 ip address 10.12.18.31
255.255.255.0 no shutdown history

```

```

bps exit router eigrp 1 metric
weights 0 1 1 1 0 0 network
10.11.12.0 0.0.0.255 network
10.6.12.0 0.0.0.255 network
10.12.18.0 0.0.0.255 exit end
copy running-config startup-config

```

Маршрутизатор R13

```

enable configure terminal hostname
R13 interface loopback 0 ip address
10.0.0.13 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.13.14.1 255.255.255.0

```

```

no shutdown history bps exit
interface serial 1/1 ip address
10.13.19.11 255.255.255.0 no shutdown
history bps exit

```

```

interface serial 1/3 ip address
10.7.13.32 255.255.255.0 no shutdown
history bps exit router eigrp 1
metric weights 0 1 1 1 0 0 network
10.13.14.0 0.0.0.255 network
10.13.19.0 0.0.0.255 network
10.7.13.0 0.0.0.255 exit end
copy running-config startup-config

```

Маршрутизатор R14

```

enable configure terminal hostname
R14 interface loopback 0 ip address
10.0.0.14 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.13.14.2 255.255.255.0

```

```

no shutdown history bps exit
interface serial 1/1 ip address
10.14.20.11 255.255.255.0 no shutdown
history bps exit interface serial 1/2

```

```

ip address 10.14.15.21
255.255.255.0 no shutdown history
bps exit interface serial 1/3 ip
address 10.8.14.32 255.255.255.0 no
shutdown

```

```

history bps exit router
eigrp 1 metric weights 0 1
1 1 0 0 network 10.13.14.0
0.0.0.255 network
10.14.20.0 0.0.0.255
network 10.14.15.0
0.0.0.255 network 10.8.14.0

```

```

0.0.0.255 exit end
copy running-config startup-config

```

Маршрутизатор R15

```

enable configure terminal hostname
R15 interface loopback 0 ip address
10.0.0.15 255.255.255.255 no
shutdown exit ip routing interface
serial 1/0 ip address 10.15.16.1
255.255.255.0 no shutdown history
bps exit interface serial 1/1 ip
address 10.15.21.11 255.255.255.0

```

```

no shutdown history bps exit
interface serial 1/2 ip address
10.14.15.22 255.255.255.0 no
shutdown history bps exit

```

```

interface serial 1/3 ip address
10.9.15.32 255.255.255.0 no
shutdown history bps exit

```

```

router eigrp 1 metric
weights 0 1 1 1 0 0 network
10.15.16.0 0.0.0.255
network 10.15.21.0

```

```

0.0.0.255 network
10.14.15.0 0.0.0.255
network 10.9.15.0 0.0.0.255
exit end

```

```

copy running-config startup-config

```

Маршрутизатор R16

```

enable configure terminal hostname
R16 interface loopback 0 ip address
10.0.0.16 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.15.16.2 255.255.255.0
no shutdown history bps exit
interface serial 1/1 ip address
10.18.22.11 255.255.255.0 no shutdown
history bps exit interface serial 1/2
ip address 10.16.17.21 255.255.255.0
no shutdown history bps exit
interface serial 1/3 ip address
10.10.16.32 255.255.255.0 no shutdown
history bps exit router eigrp 1
metric weights 0 1 1 1 0 0

```

```
network 10.15.16.0 0.0.0.255
```

```
network 10.16.22.0 0.0.0.255
```

```
network 10.16.17.0 0.0.0.255
```

```
network 10.10.16.0 0.0.0.255
```

```
exit end
```

```
copy running-config startup-config
```

Маршрутизатор R17

```

enable configure terminal hostname
R17 interface loopback 0 ip address
10.0.0.17 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.17.18.1 255.255.255.0
no shutdown history bps exit
interface serial 1/1 ip address
10.17.23.11 255.255.255.0 no shutdown
history bps exit interface serial 1/2
ip address 10.16.17.22 255.255.255.0
no shutdown history bps exit
interface serial 1/3 ip address
10.11.17.32 255.255.255.0 no shutdown
history bps exit router eigrp 1
metric weights 0 1 1 1 0 0 network
10.17.18.0 0.0.0.255 network
10.17.23.0 0.0.0.255

```

```
network 10.16.17.0
```

```
0.0.0.255 network
```

```
10.11.17.0 0.0.0.255 exit
```

```
end
```

```
copy running-config startup-config
```

Маршрутизатор**R18**

```

enable configure terminal hostname
R18 interface loopback 0 ip address
10.0.0.18 255.255.255.255 no
shutdown exit ip routing interface
serial 1/0 ip address 10.17.18.2
255.255.255.0 no shutdown history
bps exit interface serial 1/1 ip
address 10.18.24.11 255.255.255.0
no shutdown history bps exit
interface serial 1/3 ip address
10.12.18.32 255.255.255.0 no
shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0
network 10.17.18.0 0.0.0.255
network 10.18.24.0 0.0.0.255
network 10.12.18.0 0.0.0.255 exit
end

```

```
copy running-config startup-config
```

Маршрутизатор R19

```

enable configure terminal hostname
R19 interface loopback 0 ip address
10.0.0.19 255.255.255.255 no
shutdown exit ip routing interface
serial 1/0 ip address 10.19.20.1
255.255.255.0 no shutdown history
bps exit interface serial 1/1 ip
address 10.13.19.12 255.255.255.0
no shutdown history bps exit
interface serial 1/3 ip address
10.19.25.31 255.255.255.0 no

```

```

shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0
network 10.19.20.0 0.0.0.255 network
10.13.19.0 0.0.0.255 network
10.19.25.0 0.0.0.255 exit end
copy running-config startup-config

```

Маршрутизатор R20

```

enable configure terminal hostname
R20 interface loopback 0 ip address
10.0.0.20 255.255.255.255 no shutdown
exit

```

```

ip routing interface serial 1/0 ip
address 10.19.20.2 255.255.255.0 no
shutdown history bps exit interface
serial 1/1 ip address 10.14.20.12
255.255.255.0 no shutdown history
bps exit interface serial 1/2 ip
address 10.20.21.21 255.255.255.0 no

```

```

shutdown history bps exit interface
serial 1/3 ip address 10.20.26.31
255.255.255.0 no shutdown history
bps exit router eigrp 1 metric
weights 0 1 1 1 0 0 network
10.19.20.0 0.0.0.255 network

```

```

10.14.20.0 0.0.0.255 network
10.20.21.0 0.0.0.255 network
10.20.26.0 0.0.0.255 exit end
copy running-config startup-config

```

Маршрутизатор R21

```

enable configure terminal hostname
R21 interface loopback 0 ip address
10.0.0.21 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.21.22.1 255.255.255.0
no shutdown history bps exit

```

```

interface serial 1/1 ip address
10.15.21.12 255.255.255.0 no shutdown
history bps exit interface serial 1/2
ip address 10.20.21.22 255.255.255.0
no shutdown history bps exit

```

```

interface serial 1/3 ip address
10.21.27.31 255.255.255.0 no
shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0

```

```

network 10.21.22.0 0.0.0.255
network 10.15.21.0 0.0.0.255
network 10.20.21.0 0.0.0.255
network 10.21.27.0 0.0.0.255 exit
end
copy running-config startup-config

```

Маршрутизатор

R22

```

enable configure terminal hostname
R22 interface loopback 0 ip address
10.0.0.22 255.255.255.255 no
shutdown exit ip routing interface
serial 1/0 ip address 10.21.22.2
255.255.255.0 no shutdown

```

```

history bps exit interface serial
1/1 ip address 10.16.22.12
255.255.255.0 no shutdown history
bps exit interface serial 1/2 ip
address 10.22.23.21 255.255.255.0
no shutdown history bps exit

```

```

interface serial 1/3 ip address
10.22.28.31 255.255.255.0 no
shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0

```

```

network 10.21.22.0 0.0.0.255
network 10.16.22.0 0.0.0.255
network 10.22.23.0 0.0.0.255
network 10.22.28.0 0.0.0.255 exit
end
copy running-config startup-config

```

Маршрутизатор

R23

```

enable configure terminal hostname
R23 interface loopback 0 ip address
10.0.0.23 255.255.255.255 no

```

```
shutdown exit ip routing interface
serial 1/0 ip address 10.23.24.1
255.255.255.0 no shutdown history
bps exit
```

```
interface serial 1/1 ip address
10.17.23.12 255.255.255.0 no shutdown
history bps exit interface serial 1/2
ip address 10.22.23.22 255.255.255.0
no shutdown history bps exit
```

```
interface serial 1/3 ip address
10.23.29.31 255.255.255.0 no shutdown
history bps exit router eigrp 1
```

```
metric weights 0 1 1 0 0 network
10.23.24.0 0.0.0.255 network
10.17.23.0 0.0.0.255 network
10.22.23.0 0.0.0.255 network
```

```
10.23.29.0 0.0.0.255 exit end
copy running-config startup-config
```

Маршрутизатор R24

```
enable configure terminal hostname
R24 interface loopback 0 ip address
10.0.0.24 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.23.24.2 255.255.255.0
```

```
no shutdown history bps exit
interface serial 1/1 ip address
10.18.24.12 255.255.255.0 no shutdown
history bps exit interface serial 1/3
ip address 10.24.30.31 255.255.255.0
no shutdown history bps exit router
```

```
eigrp 1 metric weights 0 1 1 1 0 0
network 10.23.24.0 0.0.0.255 network
10.18.24.0 0.0.0.255 network
10.24.30.0 0.0.0.255 exit end
```

```
copy running-config startup-config
```

Маршрутизатор R25

```
enable configure terminal hostname
R25 interface loopback 0 ip address
10.0.0.25 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
```

```
ip address 10.25.26.1 255.255.255.0
no shutdown history bps exit
interface serial 1/1 ip address
10.25.31.11 255.255.255.0 no
```

```
shutdown history bps exit
interface serial 1/3 ip address
10.19.25.32 255.255.255.0 no
```

```
shutdown history bps exit
router eigrp 1 metric
weights 0 1 1 1 0 0 network
```

```
10.25.26.0 0.0.0.255
network 10.25.31.0
```

```
0.0.0.255 network
10.19.25.0 0.0.0.255 exit
```

```
end
copy running-config startup-config
```

Маршрутизатор

R26

```
enable configure terminal hostname
R26 interface loopback 0 ip address
10.0.0.26 255.255.255.255 no
```

```
shutdown exit ip routing interface
serial 1/0 ip address 10.25.26.2
255.255.255.0 no shutdown history
```

```
bps exit interface serial 1/1 ip
address 10.26.32.11 255.255.255.0
no shutdown history bps exit
```

```
interface serial 1/2 ip address
10.26.27.21 255.255.255.0 no
shutdown history bps exit
```

```
interface serial 1/3 ip address
10.20.26.32 255.255.255.0 no
shutdown history bps exit router
```

```
eigrp 1 metric weights 0 1 1 1 0 0
network 10.25.26.0 0.0.0.255
```

```
network 10.26.32.0
```

```
0.0.0.255 network
10.26.27.0 0.0.0.255
```

```
network 10.20.26.0
0.0.0.255 exit end
```

```
copy running-config startup-config
```

Маршрутизатор R27

```
enable configure terminal hostname
R27 interface loopback 0 ip address
10.0.0.27 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.27.28.1 255.255.255.0
no shutdown history bps exit
interface serial 1/1 ip address
10.27.33.11 255.255.255.0 no shutdown
history bps exit interface serial 1/2
ip address 10.26.27.22 255.255.255.0
```

```
no shutdown history bps exit
interface serial 1/3 ip address
10.21.27.32 255.255.255.0 no shutdown
history bps exit router eigrp 1
metric weights 0 1 1 1 0 0 network
10.27.28.0 0.0.0.255 network
```

```
10.27.33.0 0.0.0.255 network
10.26.27.0 0.0.0.255
network 10.21.27.0 0.0.0.255
exit end
```

```
copy running-config startup-config
```

Маршрутизатор R28

```
enable configure terminal hostname
R28 interface loopback 0 ip address
10.0.0.28 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.27.28.2 255.255.255.0
```

```
no shutdown history bps exit
interface serial 1/1 ip address
10.28.34.11 255.255.255.0 no shutdown
history bps exit interface serial 1/2
ip address 10.28.29.21 255.255.255.0
```

```
no shutdown history bps exit
interface serial 1/3 ip address
```

```
10.22.28.32 255.255.255.0 no shutdown
history bps exit router eigrp 1
metric weights 0 1 1 1 0 0 network
10.27.28.0 0.0.0.255 network
```

```
10.28.34.0 0.0.0.255 network
10.28.29.0 0.0.0.255 network
10.22.28.0 0.0.0.255 exit
```

```
end
```

```
copy running-config startup-config
```

Маршрутизатор

R29

```
enable configure terminal hostname
R29 interface loopback 0 ip address
10.0.0.29 255.255.255.255 no
shutdown exit ip routing interface
serial 1/0 ip address 10.29.30.1
```

```
255.255.255.0 no shutdown history
bps exit interface serial 1/1 ip
address 10.29.35.11 255.255.255.0
```

```
no shutdown history bps exit
interface serial 1/2 ip address
```

```
10.28.29.22 255.255.255.0 no
shutdown history bps exit
```

```
interface serial 1/3 ip address
10.23.29.32 255.255.255.0 no
```

```
shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0
```

```
network 10.29.30.0 0.0.0.255
network 10.29.35.0 0.0.0.255
```

```
network 10.28.29.0 0.0.0.255
network 10.28.29.0 0.0.0.255 exit
```

```
end
```

```
copy running-config startup-config
```

Маршрутизатор R30

```
enable configure terminal hostname
R30 interface loopback 0 ip address
```

```
10.0.0.30 255.255.255.255 no
shutdown exit ip routing interface
```

```
serial 1/0 ip address 10.29.30.2
255.255.255.0 no shutdown history
```

```
bps exit interface serial 1/1 ip
address 10.30.36.11 255.255.255.0
```

```
no shutdown history bps exit
interface serial 1/3 ip address
```

```

10.24.30.32 255.255.255.0 no shutdown
history bps exit router eigrp 1
metric weights 0 1 1 1 0 0 network
10.29.30.0 0.0.0.255 network
10.30.36.0 0.0.0.255 network
10.24.30.0 0.0.0.255 exit end

```

```

copy running-config startup-config
Маршрутизатор
R33

```

```

enable configure terminal hostname
R33 interface loopback 0 ip address
10.0.0.33 255.255.255.255 no

```

```

copy running-config startup-config
Маршрутизатор R31
enable configure terminal hostname
R31 interface loopback 0 ip address
10.0.0.31 255.255.255.255 no shutdown
exit

```

```

shutdown exit ip routing interface
serial 1/0 ip address 10.33.34.1
255.255.255.0 no shutdown history
bps exit interface serial 1/1 ip
address 10.27.33.12 255.255.255.0

```

```

ip routing interface serial 1/0 ip
address 10.31.32.1 255.255.255.0 no
shutdown history bps exit interface
serial 1/1 ip address 10.25.31.12
255.255.255.0 no shutdown history
bps exit router eigrp 1 metric

```

```

no shutdown history bps exit
interface serial 1/2 ip address
10.32.33.22 255.255.255.0 no
shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0
network 10.33.34.0 0.0.0.255
network 10.27.33.0 0.0.0.255

```

```

weights 0 1 1 1 0 0 network
10.31.32.0 0.0.0.255 network
10.25.31.0 0.0.0.255 exit end
copy running-config startup-config

```

```

network 10.32.33.0 0.0.0.255 exit
end
copy running-config startup-config

```

Маршрутизатор R32

```

enable configure terminal hostname
R32 interface loopback 0 ip address
10.0.0.32 255.255.255.255 no shutdown
exit ip routing interface serial 1/0
ip address 10.31.32.2 255.255.255.0
no shutdown history bps exit

```

Маршрутизатор

R34

```

enable configure terminal hostname
R34 interface loopback 0 ip address
10.0.0.34 255.255.255.255 no
shutdown exit ip routing interface
serial 1/0 ip address 10.33.34.2
255.255.255.0 no shutdown history

```

```

interface serial 1/1 ip address
10.26.32.12 255.255.255.0 no shutdown
history bps exit interface serial 1/2
ip address 10.32.33.21 255.255.255.0
no shutdown

```

```

bps exit interface serial 1/1 ip
address 10.28.34.12 255.255.255.0
no shutdown history bps exit
interface serial 1/2 ip address
10.34.35.21 255.255.255.0 no

```

```

history bps exit router eigrp
1 metric weights 0 1 1 1 0 0
network 10.31.32.0 0.0.0.255
network 10.26.32.0 0.0.0.255
network 10.32.33.0 0.0.0.255
exit end

```

```

shutdown history bps exit router
eigrp 1 metric weights 0 1 1 1 0 0
network 10.33.34.0 0.0.0.255
network 10.28.34.0 0.0.0.255

```

```

exit end

```

```
network 10.34.35.0 0.0.0.255 exit end
copy running-config startup-config
```

Маршрутизатор R35

```
enable configure
terminal hostname
```

```
R35 interface
```

```
loopback 0 ip address
10.0.0.36
255.255.255.255 no
shutdown exit ip
```

```
routing interface
```

```
serial 1/0 ip address
```

```
10.35.36.1
255.255.255.0 no
shutdown history bps
exit interface serial
```

```
1/1 ip address
```

```
10.29.35.12
```

```
255.255.255.0 no
shutdown history bps
exit interface serial
1/2 ip address
```

```
10.34.35.22
```

```
255.255.255.0 no
```

```
shutdown history bps
exit router eigrp 1
metric weights 0 1 1
1 0 0 network
```

```
10.35.36.0 0.0.0.255
```

```
network 10.29.35.0
```

```
0.0.0.255 network
```

```
10.34.35.0 0.0.0.255
```

```
exit end
```

```
copy running-config startup-config
```

Маршрутизатор R36

```
enable configure terminal hostname
```

```
R36 interface loopback 0 ip address
```

```
10.0.0.36 255.255.255.255 no shutdown
```

```
exit ip routing interface serial 1/0
```

```
ip address 10.35.36.2 255.255.255.0
no shutdown history bps
```

```
exit interface serial 1/1 ip address
10.30.36.12 255.255.255.0 no
```

```
shutdown history bps exit interface
```

```
Ethernet 0/0 ip address 192.168.36.1
```

```
255.255.255.0 no shutdown history
```

```
bps exit interface Ethernet 0/1
```

```
ip address 192.168.136.1
```

```
255.255.255.0 no shutdown
```

```
history bps exit router eigrp
```

```
1 metric weights 0 1 1 1 0 0
```

```
network 10.35.36.0 0.0.0.255
```

```
network 10.30.36.0 0.0.0.255
```

```
network 192.168.36.0 0.0.0.255
```

```
network 192.168.136.0
```

```
0.0.0.255 passive-interface
```

```
ethernet 0/0 passive-interface
```

```
ethernet 0/1 exit end
```

```
copy running-config startup-config
```