НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

До захисту допущено:
Завідувач кафедри
_____ Леонід УРИВСЬКИЙ
«___»_____20__ р.

Дипломна робота
на здобуття ступеня бакалавра
за освітньо-професійною програмою "Телекомунікаційні системи та мережі"
спеціальності 172 "Телекомунікації та радіотехніка»
на тему: "Дослідження технології перерозподілу маршрутної інформації у корпоративній IP-мережі на базі маршрутизаторів Cisco"

Виконав:
студент III курсу, групи ТС-п81
Шевчук Андрій Борисович _____
Керівник:
Ст. викладач кафедри ТС, к.т.н.,
Новіков Валерій Іванович _____
Рецензент:
Професор кафедри ТК, д.т.н. професор,
Лисенко Олександр Іванович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2021 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Леонід УРИВСЬКИЙ
«___»_____20__ р.

ЗАВДАННЯ

на дипломну роботу студенту

Шевчук Андрій Борисович

1. Тема роботи "Дослідження технології перерозподілу маршрутної інформації у корпоративній IP-мережі на базі маршрутизаторів Cisco", керівник роботи Новіков Валерій Іванович, старший викладач кафедри телекомунікаційних систем, к.т.н., затверджені наказом по університету від "14" квітня 2021 р. № 1007-с

2. Термін подання студентом роботи 11.06.2021 р.

3. Вихідні дані до роботи: Матеріали щодо технології перерозподілу маршрутної інформації, покроковий план написання дипломної роботи.

4. Зміст роботи: Обґрунтування актуальності теми. Розгляд та детальний аналіз протоколів перерозподілу маршрутизації. Розгляд роботи протоколів взаємодії при взаємній роботі та окремо. Моделювання фрагменту прототипу мережі та покроковий опис виконання алгоритму.

5. Перелік ілюстративного матеріалу - презентація Power Point (10 слайдів)

6. Дата видачі завдання 01.03.2020 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1.	Отримання завдання	01.03.2021	
2.	Робота над 1 розділом	15.03.2021	
3.	Робота над 2 розділом	30.03.2021	
4.	Робота над 3 розділом	20.04.2021	
5.	Робота над вступною частиною	10.05.2021	
6.	Робота над висновками	20.05.2021	
7.	Робота над оформленням	01.06.2021	
8.	Подання роботи на кафедру	11.06.2021	

Студент Андрій Шевчук

Керівник Валерій Новіков

АНОТАЦІЯ

Текстова частина дипломної роботи: 88 с., 28 рисунків, 12 таблиць, 11 лістингів, 15 джерел.

Мета роботи: дослідити технологію перерозподілу маршрутної інформації, розглянути протоколи маршрутизації RIP, OSPF та EIGRP. Проаналізувати функціонал та характеристики Cisco Packet Tracer та Graphical Network Simulator-3. Розробити практичний розділ у вигляді лабораторної роботи.

Проаналізувати роботу корпоративної IP-мережі, перевірити правильність функціонування протоколів перерозподілу маршрутної інформації.

RIP, OSPF, EIGRP, CISCO PACKET TRACER, GRAPHICAL NETWORK SIMULATOR-3, ПЕРЕРОЗПОДІЛ МАРШРУТНОЇ ІНФОРМАЦІЇ, МАРШРУТИЗАЦІЯ, КОРПОРАТИВНА IP-МЕРЕЖА

ABSTRACT

The purpose of the work is to research the technology of redistribution of route information, consider routing protocols RIP, OSPF та EIGRP. Analyze the functionality and characteristics of Cisco Packet Tracer and Graphical Network Simulator-3. Develop a practical section in the form of laboratory work.

The present paper concentrates on analyzing of the corporate IP-network, check the correct operation of the protocols for redistribution of route information.

RIP, OSPF, EIGRP, CISCO PACKET TRACER, GRAPHICAL NETWORK SIMULATOR-3, REDISTRIBUTION OF ROUTE INFORMATION, ROUTING, CORPORATE IP NETWORK

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 9
ВСТУП 11
1 АНАЛІЗ СПОСОБІВ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ПЕРЕРОЗПОДІЛУ МАРШРУТНОЇ ІНФОРМАЦІЇ У КОРПОРАТИВНІЙ IP-МЕРЕЖІ 14
1.1 Аналіз технології перерозподілу маршрутної інформації 14
1.1.1 Поняття перерозподілу маршрутної інформації 14
1.1.2 Поняття метричного домену 15
1.1.3 Маршрутні петлі 17
1.2 Аналіз спільної роботи декількох протоколів маршрутизації 28
1.2.1 Спільна робота протоколів маршрутизації без перерозподілу 28
1.2.2 Налаштування базового перерозподілу маршрутної інформації 34
1.2.3 Налаштування перерозподілу маршрутної інформації з приєднаних і статичних маршрутів 38
1.2.4 Налаштування перерозподілу маршрутної інформації в протокол RIP . 42
1.2.5 Налаштування перерозподілу маршрутної інформації в протокол EIGRP 44
1.2.6 Налаштування перерозподілу маршрутної інформації в протокол OSPF 46
1.3 Висновки до розділу 1 47
2 АНАЛІЗ ЗАСОБІВ МОДЕЛЮВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ IP-МЕРЕЖ 49
2.1 Використання програми Cisco Packet Tracer для моделювання роботи телекомунікаційних IP-мереж 49
2.1.1 Основи використання симулятора мереж Cisco Packet Tracer 49
2.1.2 Характеристика Cisco Packet Tracer 50
2.1.3 Інтерфейс Cisco Packet Tracer 55
2.2 Використання програми Graphical Network Simulator-3 для моделювання роботи телекомунікаційних IP-мереж 58
2.2.1 Теоретичні відомості про програму GNS3 58

2.2.2 Характеристики GNS3 58
2.3 Порівняльний аналіз засобів моделювання 60
2.3.1 Переваги та недоліки Cisco Packet Tracer 60
2.3.2 Переваги та недоліки GNS3 61
2.3.3 Вибір засобів моделювання для дослідження технології перерозподілу маршрутної інформації у корпоративній IP-мережі 63
2.4 Висновки до розділу 2 64
3 РОЗРОБКА ЛАБОРАТОРНОЇ РОБОТИ З ДИСЦИПЛІНИ ТЕХНОЛОГІЇ ТА ЗАСОБИ МІЖМЕРЕЖЕВОЇ ВЗАЄМОДІЇ "ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ ПЕРЕРОЗПОДІЛУ МАРШРУТІВ НА БАЗІ МАРШРУТИЗАТОРІВ CISCO" 65
3.1 Короткі теоретичні відомості 65
3.1.1 Початкові поняття 65
3.1.2 Метрика 66
3.1.3 Адміністративна відстань (AD) 67
3.2 Перерозподіл маршрутів 68
3.2.1 Налагодження редистрибуції (перерозподілу) маршрутів 68
3.2.2 Перерозподіл маршрутів в RIP 70
3.2.3 Перерозподіл маршрутів в OSPF 71
3.2.4 Перерозподіл маршрутів в EIGRP 71
3.3 Налагодження функціонування мережі з використанням перерозподілу маршрутів між протоколами 72
3.3.1 Налагодження мережі між протоколами RIP та OSPF 72
3.3.2 Налагодження мережі між протоколами OSPF та EIGRP 77
3.3.3 Приклад налагодження функціонування мережі з використанням перерозподілу маршрутів між протоколами RIP та EIGRP 78
3.3.4 Приклад налагодження функціонування мережі з використанням перерозподілу маршрутів між протоколу EIGRP та статичної маршрутизації 79

3.3.5 Приклад налагодження функціонування мережі з використанням перерозподілу маршрутів між статичної маршрутизації та протоколом маршрутизації RIP 81
3.3.6 Приклад налагодження функціонування мережі з використанням перерозподілу маршрутів між статичної маршрутизації та протоколом маршрутизації OSPF 81
3.4 Створення та налаштування прототипу фрагменту мережі з підтримкою перерозподілу маршрутної інформації 82
3.5 Висновки до розділу 3 85
ВИСНОВКИ 86
ПЕРЕЛІК ПОСИЛАНЬ 87

ПЕРЕЛІК СКОРОЧЕНЬ

ARP	Address Resolution Protocol — протокол визначення адреси
BGP	Border Gateway Protocol – протокол граничного шлюзу
CDP	Cisco Discovery Protocol- протокол, що дає можливість знаходити підключене мережеве обладнання
CCNA	Cisco Certified Network Associate - Сертифікація рівня спеціаліст
CCNP	Cisco Certified Network Professional - Професійні сертифікації
Cisco ASA	Cisco Adaptive Security Appliances - Прилади адаптивної безпеки
DCE	Data Communication Equipment - обладнання провайдера, яке оприділяє швидкість каналу, передає данні від обладнання клієнта
DHCP	Dynamic Host Configuration Protocol — протокол динамічної конфігурації вузла
DTE	Data Terminal Equipment - клієнтське обладнання, яке зазвичай є комп'ютером або маршрутизатором
EIGRP	Enhanced Interior Gateway Routing Protocol) — протокол, що використовує механізм DUAL для вибору найкоротшого маршруту
GNS	Graphical Network Simulator — асинхронний спосіб передачі даних
GUI	Graphical user interface- Дружній графічний інтерфейс
ICMP	Internet Control Message Protocol — протокол міжмережевих керуючих повідомлень
IOS	Internetwork Operating System — Міжмережева Операційна Система
OSI	Open Systems Interconnect — взаємодія відкритих систем

OSPF	Open Shortest Path First — протокол пошуку першого найкоротшого шляху
RIP	Routing Information Protocol — протокол маршрутної інформації
TCP	Transmission Control Protocol — протокол управління передачею
UDP	User Datagram Protocol — протокол дейтаграм користувача
VM	Virtual Machine - віртуальна машина
WAN	Wide Area Network — глобальна обчислювальна мережа

ВСТУП

Перерозподіл маршрутної інформації (route redistribution) – це передача маршрутів, вивчених за допомогою одного протоколу маршрутизації, в інший протокол маршрутизації. Часто в корпоративної мережі передачі даних виникають ситуації, коли на одному маршрутизаторі необхідно використати декілька протоколів маршрутизації. Найбільш поширеними причинами є:

- Об'єднання двох мереж передачі даних, а маршрутизація в них забезпечується за допомогою різних протоколів маршрутизації.

Якщо одна з мереж передачі даних перед об'єднанням повністю не перекладається на протокол маршрутизації, використовуваний в іншій мережі, то в цій ситуації, принаймні, на граничних маршрутизаторах об'єднуваних мереж передачі даних мають бути запущені обидва протоколи маршрутизації. Для забезпечення зв'язку між цими мережами, пограничні маршрутизатори повинні проводити перетворення маршрутної інформації між двома протоколами маршрутизації.

- Мережа передачі даних перекладається з одного протоколу маршрутизації на інший. Якщо міграція не робитися на усіх маршрутизаторах одночасно, то на деяких ключових маршрутизаторах обидва протоколи маршрутизації повинні співіснувати певний час, яке знадобиться для повного переходу на новий протокол маршрутизації. В цьому випадку, щоб забезпечити зв'язок між частиною мережі, яка вже була переведена на новий протокол маршрутизації, і частиною, де це ще не зроблено, ключові маршрутизатори повинні не лише дозволяти співіснувати обом протоколам маршрутизації, але також і виконувати перетворення маршрутної інформації між цими протоколами маршрутизації.

- В мережі передачі даних можуть існувати сервера або робітники станції, яким необхідно брати участь в процесі динамічної маршрутизації, без оголошення власної маршрутної інформації. Прикладом подібній ситуації

можуть виступати сервера під управлінням ОС Unix або Windows, які використовують протокол маршрутизації RIP, а мережу передачі даних реалізована на маршрутизаторах Cisco, на яких запущений протокол маршрутизації EIGRP. У такій ситуації маршрутизатори, які підключені до сегментів мережі, в яких є інтелектуальні хости, повинні конвертувати маршрутну інформацію протоколу EIGRP в протокол RIP.

Існує значно більше випадків, що вимагають роботи декількох протоколів маршрутизації на одному маршрутизаторі. Не вдаючись до подробиць кожної з таких ситуацій, очевидно, що усі вони накладають одну вимогу: окрім простого співіснування, протоколи маршрутизації повинні обмінюватися маршрутною інформацією.

Простого виконання декількох протоколів маршрутизації на одному і тому ж маршрутизаторі недостатньо для обміну маршрутною інформацією між цими протоколами.

Маршрутизатори автоматично не здійснюють обмін маршрутної інформації між протоколами маршрутизації запущеними на них. Причина цього полягає в тому, що декілька протоколів маршрутизації, навіть будучи присутнім на одному маршрутизаторі, можуть виконувати різні завдання.

Отже, обмін маршрутною інформацією між ними може бути небажаний.

Іншою причиною того, що декілька протоколів маршрутизації запущені на одному маршрутизаторі не обмінюються маршрутною інформацією автоматично, являється те, що різні протоколи маршрутизації по різному розраховують метрики маршрутів, внаслідок чого ці метрики несумісні. Наприклад, протоколом RIP як метрика використовується кількість переходів до мережі одержувача, тоді як протокол EIGRP використовує комбіновану метрику. Метрика є одним з найважливіших параметрів маршруту що розглядаються протоколом маршрутизації при побудові таблиці маршрутизації. Оскільки метрики несумісні, не існує простого способу адекватно перетворювати метрики маршрутів розрахованих різними

протоколами маршрутизації. Неадекватне перетворення може з великою вірогідністю привести до виникнення маршрутних петель.

Джерела маршрутної інформації не обмежуються динамічними протоколами маршрутизації. Вони також включають статичні і приєднані маршрути. Проте статичні і приєднані маршрути можуть бути лише джерелом маршрутної інформації для перерозподілу. З очевидних причин перерозподіл не може робитися в статичні і приєднані маршрути. Дипломну роботу присвячено дослідженню технології перерозподілу маршрутної інформації у корпоративної IP-мережі на базі маршрутизаторів Cisco.

1 АНАЛІЗ СПОСОБІВ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ПЕРЕРОЗПОДІЛУ МАРШРУТНОЇ ІНФОРМАЦІЇ У КОРПОРАТИВНІЙ IP-МЕРЕЖІ

1.1 Аналіз технології перерозподілу маршрутної інформації

1.1.1 Поняття перерозподілу маршрутної інформації

Процес перетворення маршрутної інформації між різними її джерелами називається перерозподілом маршрутної інформації (routing information redistribution) чи просто перерозподілом. Включення перерозподілу на маршрутизаторі зазвичай припускає вказівку трьох наступних компонентів:

- Джерела маршрутної інформації, яка має бути перерозподілена.
- Одержувача маршрутної інформації у вигляді протоколу маршрутизації, в який перерозподіляється маршрутна інформація.
- Метрик, які повинні використовуватися протоколом маршрутизації при оголошенні в домен маршрутизації динамічного протоколу перерозподіленої маршрутної інформації.

Останній компонент зводитися, як правило, до вказівки одній або декількох фіксованих метрик, які повинні використовуватися протоколом маршрутизації при оголошенні перерозподіленою маршрутною інформацією.

Якщо вказана лише одна метрика, протокол маршрутизації буде використати її для усіх мереж одержувачів, що перерозподіляються, а якщо вказано декілька, протокол маршрутизації використовує кожну з них для індивідуальної підмножини мереж одержувачів, що перерозподіляються, відповідно до окремо вказаних правил.

Перерозподіл маршрутної інформації необов'язково повинен бути двостороннім. Якщо інформація одного протоколу маршрутизації перерозподіляється в іншому, інформація останнього не обов'язково повинна перерозподілятися в перший. Можливо, в деяких випадках і бажаний перерозподіл маршрутної інформації тільки з одного протоколу у іншій, але не навпаки.

Як приклад можна розглянути таку ситуацію. У мережі передачі даних є область, в якій маршрутизація здійснюється при допомозі застарілого мережевого устаткування, на якому не може бути розгорнутий основний протокол маршрутизації вживаний в корпоративній мережі передачі даних. У цій ситуації маршрутна інформація повинна бути перерозподілена з цього сегменту в загальний домен маршрутизації, а зворотний перерозподіл може привести до перевантаження маршрутною інформацією мережевого устаткування розташованого усередині цієї області. У даному випадку забезпечення маршрутною інформацією про зовнішні мережі одержувачах маршрутизаторів усередині області, може бути виконано поширенням маршруту за умовчанням на граничний маршрутизатор області який має повну маршрутну інформацію.

1.1.2 Поняття метричного домену

Різні протоколи маршрутизації використовують різні алгоритми розрахунку метрик. Незалежно від конкретного алгоритму розрахунку метрики усіх протоколів маршрутизації мають одну загальну властивість

- вони збільшуються зі збільшенням кількості переходів на шляху від мережі одержувача.

Формульно накопичувальний характер метрики можна описати виразом (1.1).

$$\forall\, d \text{ і } d' \quad \text{,якщо} \quad d'>d, \quad M(d')>M(d) \qquad (1.1)$$

де d і d' - кількість переходів на шляху від мережі одержувача

M (x) - функція метрики.

Враховуючи цю загальну властивість метрик протоколів маршрутизації визначимо метричний домен протоколу маршрутизації як частину мережі передачі даних, в якій метрики протоколу маршрутизації відображають відстань до мережі одержувача, і задовольняють вираз (1.1). Метрики розраховуються відповідно до алгоритму, наказаного запущеного на

маршрутизаторах протоколом маршрутизації. Іншими словами, будь-хто маршрутизатор в межах метричного домена протоколу маршрутизації розраховує метрики маршрутів до мереж одержувачів, що знаходяться в межах метричного домена, відповідно до алгоритму, наказаного протоколом маршрутизації. Якщо маршрутизатор використовує будь-який інший алгоритм для розрахунку метрики маршруту до мережі одержувача, то цей маршрутизатор знаходиться за межами метричного домена, якому належить мережа отримувач.

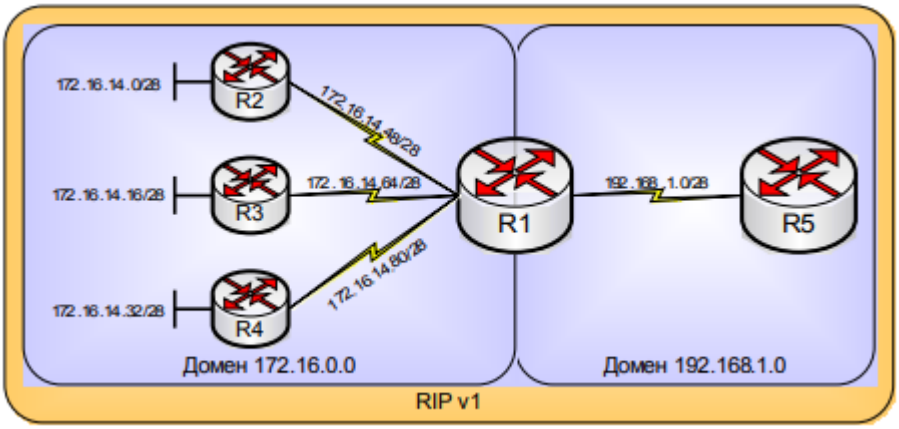

Рисунок 1.1 - Приклад метричного домена [1]

Прикладом метричного домена (Рис. 1.1) протоколу RIP v1 є безперервна група сегментів, підмережі яких належать одній і тій же класовій мережі. Межа такого метричного домена для протоколу

RIP пролягає по маршрутизатору R1, який, крім того, має підключення до сегменту, що належить іншій класовій мережі.

Як ми знаємо, при формуванні маршрутних оновлень протоколом RIP, які мають бути відправлені, через інтерфейси, що належать іншій класовій мережі, маршрутизатор робить автоматичне підсумовування маршрутів до маршруту на класову мережу, метрику якого встановлює рівною 1, відкидаючи тим самим накопичену інформацію про метрики приватних маршрутів. Очевидно, що будь-який маршрутизатор, який не належить

класовій мережі 172.16.0.0, може отримувати тільки сумарний маршрут на класову мережу, а не приватні маршрути до мереж одержувачів. Такі маршрутизатори сприйматимуть будь-яку мережу одержувач в межах цього метричного домена з однією метрикою - тій, яка є у них для цій класовій мережі. Маршрутизатори належать іншою класовою мережі більше не обчислюють метрики маршрутів, до мереж одержувачів в межах цього метричного домена відповідно з алгоритмом протоколу RIP, тобто такі маршрутизатори знаходяться за межами метричного домена 172.16.0.0.

Наведений вище приклад є природною межею метричного домена, обумовлену підсумовуванням маршрутів до мереж одержувачів на межі класової мережі.

Межа метричного домена також створюється на маршрутизаторах тих, що виконують, перерозподіл маршрутної інформації, який замінює накопичені метрики однією або декількома фіксованими метриками.

Залежно від протоколу маршрутизації, перерозподіл може, супроводжуватися або не супроводжуватися підсумовуванням маршрутів. Якщо воно супроводжуються підсумовуванням, отримана межа метричного домена не відрізняється від природної межі. У зворотному випадку межа носить повністю штучний характер - приватні маршрути перетинають межу не зміненим, але їх метрики замінюються на фіксовану величину.

Штучні межі метричних доменів можуть негативно впливати на роботу мережі передачі даних, створюючи маршрутні петлі.

1.1.3 Маршрутні петлі

Маршрутні петлі (routing loops) є маршрутами в мережі передачі даних, які приводять на один і той же маршрутизатор більше одного разу. Маршрутні петлі украй не бажані, оскільки трафіку доводиться долати додатковий шлях лише для того, щоб прибути на той же самий маршрутизатор. Це у свою чергу призводить до затримки трафіку, або навіть

до повної неможливості його доставки мережам одержувачам. Маршрутні петлі піддають мережу передачі даних надмірному навантаженню і призводять до величезної кількості операцій по обробці трафіку, що поступає, на причетних маршрутизаторах.

Маршрутні петлі можуть бути класифіковані як:

Короткоживучі маршрутні петлі - петлі існуючі нетривалий час, зазвичай не більше пари хвилин.

Довгоживучі маршрутні петлі - петлі існуючі тривалий час, від декількох хвилин до безкінечності.

Виникнення короткоживучих маршрутних петель обумовлене процесами, що відбуваються під час сходження мережі, після тих, що сталися в ній змін. Час можливого існування таких маршрутних петель залежить від швидкості сходження мережі і від протоколу маршрутизації вживаного в мережі передачі даних. Короткоживучі маршрутні петлі мають можливість самознищуватися за певний, не тривалий період часу.

Виникнення довгоживучих маршрутних петель обумовлене помилками в налаштуванні процесу маршрутизації усередині домена маршрутизації.

Зазвичай довгоживучі маршрутні петлі не зникають, якщо не прийняти заходів до усунення тих помилок в процесі маршрутизації, які привели до їх виникненя. Довгоживучі маршрутні петлі можуть бути як постійні, так і періодичними. Постійні маршрутні петлі існують весь час, тоді як періодичні проходять через цикли, зникаючи і з'являючись знову.

Протоколи маршрутизації розробляються такими, що самостабілізуються. Тоді як тимчасова нестабільність, що викликається змінами в типології мережі передачі даних і часто супроводжується короткоживучими маршрутними петлями, часто неминуча. Протоколи маршрутизації долають нестабільність і встановлюють маршрутизацію без петель. Жоден протокол маршрутизації не спроектований так, щоб дозволити довгоживучим маршрутним петлям утворитися в який-небудь момент роботи.

Усі протоколи маршрутизації базуються на математичних моделях, для яких доведено, що вони не викликають появу довгоживучих маршрутних петель. Більшість цих математичних моделей забезпечують функціонування без утворення петель, за допомогою дотримання умови, що метрики, пов'язані з місцями призначення, ростуть з додаванням кожного додаткового переходу на шляху до місця призначення.

Формально можна описати, що якщо маршрутизатор R1 вибирає маршрут до мережі одержувача D, який проходить через маршрутизатор R2, то M1>M2, де M1 і M2 є метриками маршруту до мережі одержувача D маршрутизаторів R1 і R2 відповідно. Іншими словами, чим далі місце призначення, тим більше метрика. Якщо це допущення дотримується, маршрутна петля утворитися не може.

Доводиться це просто. Вважатимемо, що в мережі передачі даних N усі маршрутизатори вибирають маршрути до мереж одержувачам на основі вищезгаданого допущення. Припустимо, що петля існує і є маршрутизатор R1, маршрут, що встановив, до мережі одержувачеві D через маршрутизатор R2, який у свою чергу встановив маршрут до D через маршрутизатор R3, і так далі до маршрутизатора Rn, що встановив маршрут до D через маршрутизатор R1. Така ситуація показана на рис. 1.2.

Допущення дотримується, отже, метрики усіх маршрутів повинні відповідати нерівності (1.2).

$$M1 > M2 > M3,\ Mn - 2 > Mn - 1 > Mn > M1 \qquad (1.2)$$

Нерівність (1.2) зводиться до M1 > M1. Отже, наша початкова передумова про те, що петля може існувати навіть у тому випадку, якщо усі маршрутизатори дотримуються прийнятого допущення, невірна.

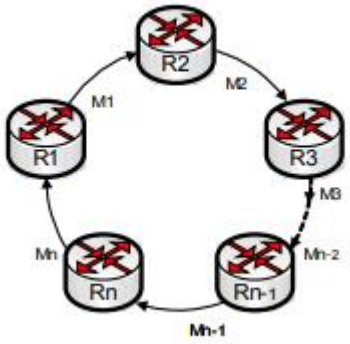

Рисунок 1.2 - Припущення про утворення маршрутної петлі [1]

Маршрутні петлі не виникають в мережі передачі даних, в якій маршрутизація підтримується засобами одного протоколу маршрутизації, поки не порушені обмеження протоколу, такі як максимальна кількість переходів, в маршруті до мережі одержувачеві, а мережеве устаткування і його програмне забезпечення працюють в нормальному режимі. У випадку якщо маршрутизація в мережі передачі даних підтримується за допомогою більш ніж одного протоколу маршрутизації або комбінації статичної і динамічної маршрутизації, виникає можливість виникнення маршрутних петель. Ця можливість збільшується при перерозподілі маршрутної інформації між протоколами маршрутизації. Оскільки в процесі перерозподілу об'єднуються домени окремих протоколів маршрутизації, тоді як метричні домени залишаються окремими. Мережі одержувачі, що знаходяться в межах одного домена протоколу маршрутизації, стають доступними з домена іншого протоколу маршрутизації з однією і тією ж метрикою.

Розглянемо односторонній перерозподіл маршрутної інформації. На рис. 1.3 показана мережа передачі даних, в якій потенційним джерелом маршрутних петель може бути одна точка одностороннього перерозподілу маршрутної інформації.

Маршрутизатор R1 оголошує мережі одержувачі, наявні в частині мережі передачі даний N1 з використанням протоколу маршрутизації RP1

маршрутизатора R2, який потім перерозподіляє ці мережі одержувачі в протокол маршрутизації RP2. Маршрутизатор R2 оголошує перерозподілені мережі одержувачі своїм сусідам, що знаходяться в частині мережі передачі даних N2. Адміністративна відстань протоколу маршрутизації RP1 рівна A1 а адміністративна відстань протоколу маршрутизації RP2 рівна A2. Адміністративні відстані такі, що A2<A1.

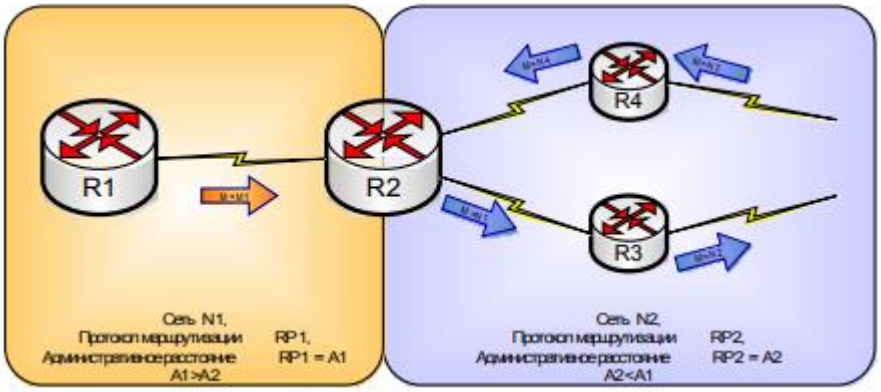

Рисунок 1.3 – Утворення маршрутної петлі при односторонньому перерозподілі маршрутної інформації [1]

Стрілки всередині N2 показують потік маршрутних оновлень, який, якщо має місце, призводить до утворення маршрутної петлі для мереж одержувачів з N1 усередині N2.

Спочатку обговоримо сценарій, що призводить до маршрутних петель, а потім причини, що викликають запуск такого сценарію.

Маршрутизатор R1 відправляє маршрутне оновлення, що містять мережі одержувачі, розташовані в N1, маршрутизатору R2. Маршрутизатор R2 отримує маршрутне оновлення, встановлює маршрут до оголошених мереж одержувачів і робить перерозподіл отриманим маршрутним інформації в протокол маршрутизації RP2, засобами якого потім оголошує ці мережі одержувачі своїм сусідам в N2.

Припустимо, що сусід R3 отримує маршрутне оновлення маршрутизатора R2 і встановлює свої маршрути до оголошених мереж

одержувачам через R2. Після цього маршрутизатор R3 сам починає оголошувати дані мережі одержувачі своїм сусідам. Зрештою це маршрутне оновлення поступає на маршрутизатор R4, який після установки маршрутів до цим мережам одержувачам, починає оголошувати їх засобами протоколу маршрутизації RP2 маршрутизатору R2.

Тепер маршрутизатор R2 повинен замінити існуючі у нього маршрути до цих мереж одержувачам, що вказують на маршрутизатор R1, на нові маршрути, що вказують на R4. Оскільки маршрутизатор R1 оголосив їх засобами протоколу маршрутизації RP1, тоді як маршрутизатор R4 оголошує їх засобами PR2, адміністративна відстань якого менше ніж у PR1.

У цього сценарію є невелике упущення: маршрутизатор R2 повинен оголосити мережі одержувачі, отримані їм від маршрутизатора R1 усім своїм сусідам практично одночасно. Тобто маршрутизатор R4 отримати перше маршрутне оновлення, що містять ці мережі одержувачі, від маршрутизатора R2, після чого він повинен встановити свої маршрути до мереж одержувачів в N1 через маршрутизатор R2. З цієї миті він повинен відхиляти усі інші маршрутні оновлення, якщо вони мають метрику, велику метрики маршрутів, що пролягають через маршрутизатор R2. Незважаючи на це упущення, цей сценарій цілком реальний і може настати, особливо якщо цьому сприятимуть деякі додаткові чинники.

- Маршрутизатор R2 може не відправити маршрутне оновлення всім своїм сусідам одночасно. Він може запланувати спочатку відправку маршрутній інформації маршрутизатору R3 і тільки після цього маршрутизатору R4. Якщо проміжок часу між передачею маршрутних оновлень маршрутизаторам R3 і R4 досить великий, маршрутизатор R4 може отримати маршрутне оновлення від іншого сусіда, в цьому випадку він оголосить мережі одержувачі з N1 маршрутизатору R2, що приведе до установки для них неправдивих маршрутів.

- Вартість каналу зв'язку між маршрутизаторами R2 і R4 настільки велика, що маршрутизатор перемкнутися на який-небудь інший маршрут

навіть якщо він перед цим встановив маршрут до мереж одержувачів в N1 через маршрутизатор R2. Якщо це станеться, маршрутизатор зробить оголошення мереж одержувачів маршрутизатору R2, що приведе до видалення істинних і установки неправдивих маршрутів маршрутизатором R2.

- Якщо в якийсь момент часу після первинного оголошення маршрутній інформації про мережі одержувача розташованих в N1, станеться тимчасове відключення каналу зв'язку між маршрутизаторами R2 і R4 маршрутизатор R4 встановить маршрути до N1 через іншого сусіда. При відновленні каналу зв'язку маршрутизатор R4 зробить оголошення маршрутній інформації маршрутизатору R2, що приведе до виникнення маршрутної петлі. Це найбільш вірогідні чинники, які сприяють виникненню маршрутних петель.

Незалежно від того, які обставини привели до перемикання маршрутів маршрутизатором R2, далі події розвиватимуться таким чином:

1. Після зміни маршрутизатором R2 напряму маршрутів до мереж одержувачам їх N1, він перестає використовувати при оголошенні цих мереж метрику призначену при перерозподілі, а замість неї використовує метрику яку він отримав від маршрутизатора R4, збільшену на вартість каналу зв'язку до маршрутизатора R4. Ця метрика вища, ніж метрика отримана при перерозподілі, оскільки вона є цією початковою метрикою, збільшеною на вартість каналів зв'язку між маршрутизаторами R3 і R4.

2. Коли маршрутизатор R3 виявить збільшення метрики, що оголошується маршрутизатором R2, він заморожує свої маршрути, і починає оголошувати ці мережі одержувачі з метрикою, рівні й нескінченності.

3.З цієї миті події можуть розвиватися різними шляхами кожен з яких приведе до того, що маршрутизатори R4 iR2 заморозять неправдиві маршрути.

4. Коли період заморожування на маршрутизаторі R2 пройде, маршрутизатор зможе відновити правильні маршрути до мереж одержувачів

розташованих за маршрутизатором R1, які незабаром після цього можуть бути знову витіснені неправдивими маршрутами. Якщо правильні маршрути витісняються, то повторюється описаний процес, який може тривати нескінченно довго.

Описана конфігурація мережі схильна до виникнення маршрутних петель. Наступні чинники ще більше погіршують негативний ефект описаних маршрутних петель:

- Такі петлі можуть виникати не відразу. Замість цього вони можуть бути викликані якою-небудь подією. Очевидно, що це може статися в найменш очікуваний момент.

- Ці петлі можуть періодично виникати або нескінченно, або обмежена кількість разів. Діагностика періодичних маршрутних петель більше складне завдання, ніж діагностика постійних.

Розглянемо двобічний перерозподіл маршрутної інформації. На відміну від випадку з одностороннім перерозподілом маршрутної інформації, що призводить до утворення періодичних маршрутних петель, двобічний перерозподіл маршрутної інформації зазвичай призводить до виникнення постійних маршрутних петель. Розглянемо мережу, показану на рис. 1.4.

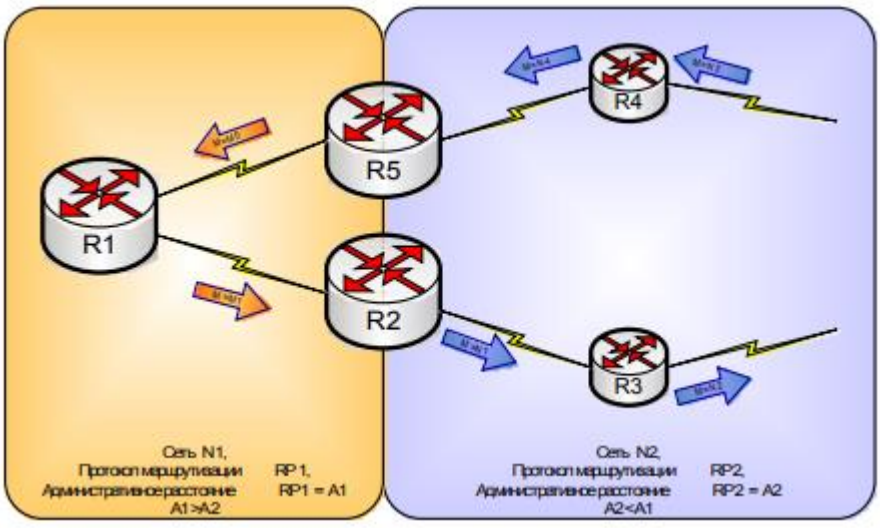

Рисунок 1.4 – Утворення маршрутної петлі при двосторонньому перерозподілі маршрутної інформації [1]

Ця мережа аналогічна мережі розглянутою раніше на Рисунку 1.3, за винятком того, що маршрутизатори R2 і R5 виконують двобічний перерозподіл між протоколами маршрутизації RP1 і RP2.

Припустимо, маршрутизатор R1 відправляє маршрутне оновлення, одержувачі, що містять мережі, в межах N1, маршрутизатору R2. Як і раніше, маршрутизатор R2 отримує це оновлення, встановлює маршрути до цих мереж одержувачам, робить перерозподіл отриманої маршрутної інформації в протокол маршрутизації RP2 і починає оголошувати перерозподілені маршрути своїм сусідам по RP2. Сусіди R2 після отримання оновлень від маршрутизатора R2, починають у свою чергу оголошувати отриману маршрутну інформацію своїм сусідам. У кінцевому підсумку це маршрутне оновлення поступає на маршрутизатор R4, який після занесення у свою таблицю маршрутизації отриманих маршрутів починає оголошувати цю маршрутну інформацію маршрутизатору R5.

Маршрутизатор R5 заносить отриману інформацію в таблицю маршрутизації, а потім робить її перерозподіл назад в протокол маршрутизації RP1 і починає оголошувати цю маршрутну інформацію в мережі N1.

У нашому випадку ці маршрутні оновлення поступлять на маршрутизатор R1. Якщо метрика перерозподілу, з якою маршрутизатор R5 зробив перерозподіл маршрутної інформації в RP1, менше метрики, з якою маршрутизатор R1 спочатку дізнався про ці мережі-одержувачі, він відкине правильні маршрути і занесе у свою таблицю маршрутизації неправдиві маршрути через R5.

Наскільки ймовірно, що події розвиватимуться так, як було описано? Відповідь така: дуже ймовірно. На відміну від сценарію з однією точкою перерозподілу, цей сценарій немає згаданого раніше упущення.

Подальший розвиток подій повністю відрізняється від того, що відбувалося в схемі з однією точкою перерозподілу. Після того, як маршрутизатор R1 встановить неправдиві маршрути до мереж-одержувачів,

розташовані в N1 через маршрутизатор R5, він змінить метрики, з якими він раніше оголошував ці мережі маршрутизатору R2. Ймовірно, що ці нові метрики будуть менше за коректних, як мінімум для частини найбільш віддалених мереж одержувачів. Отже, маршрутизатор R2 цього разу стане отримувати маршрутні оновлення від маршрутизатора R1 з меншими метриками.

Маршрутизатор R2 визнає ці зміни в мережі сприятливими, і не стане заморожувати маршрути до мереж одержувачів з N1 через маршрутизатор R1.

Але оскільки маршрутизатор R2 робить перерозподіл отриманої від R1 маршрутної інформації в N2 з фіксованою метрикою, то він не стане робити розсилку оновлень маршрутної інформації своїх сусідів по протоколу маршрутизації RP2. На цьому завершується процес обміну змінами в маршрутній інформації. Мережа передачі даних переходить в стабільний стан, в якому утворена маршрутна петля існуватиме невизначено довгий час.

На рис. 1.5 показана загальна схема мережі, яка схильна до утворення маршрутної петлі, викликаної двома точками перерозподілу маршрутної інформації.

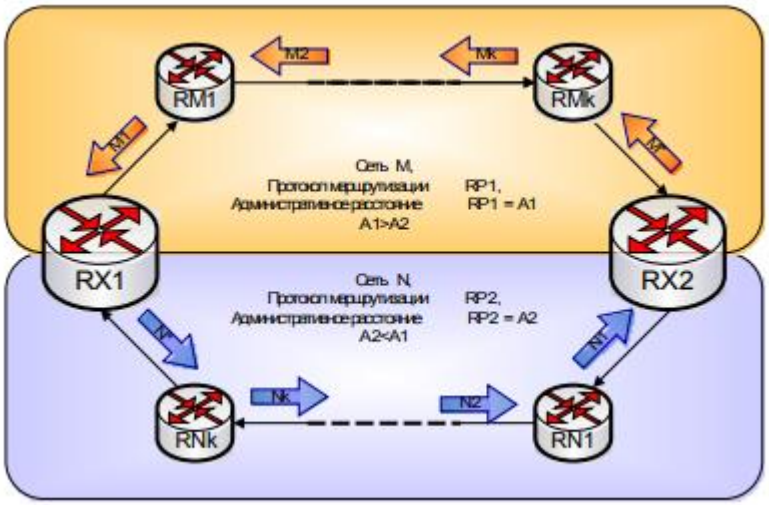

Рисунок 1.5 – Утворення маршрутних петель у 2-х доменах маршрутизації [1]

Метрики протоколів маршрутизації RP1 і RP2 обчислюються з використанням різних алгоритмів, тому вони позначаються різними буквами - M і N. Точки перерозподілу маршрутизатори RX1 і RX2 оголошують мережі-одержувачі з фіксованою метрикою перерозподілу N* і M* відповідно. Маршрутизатори RX1 і RX2 встановили свої маршрути до мереж-одержувачів в M і N з метриками M0 і N0. Необхідно звернути увагу на те, що маршрутизатори RX1 і RX2 оголошують мережі одержувачі в один домен маршрутизації, тоді як їх маршрути до цих мереж-одержувачів вказують в інший домен маршрутизації.

Маршрутизатори в кожному домені встановили маршрути, які вказують на відповідну точку перерозподілу маршрутної інформації, - або маршрутизатор RX1, або RX2.

Маршрутизатор RX2 робить перерозподіл маршрутної інформації протоколу маршрутизації RP2 про мережі-одержувачі з N в домен маршрутизації M протоколу маршрутизації RP1 з метрикою M*. Далі ця інформація поширюється по домену маршрутизації M, у результаті поступаючи на маршрутизатор RM1, який оголошує її маршрутизатору RX1.

Маршрутизатор RX1 у свою чергу робить її перерозподіл назад в домен маршрутизації RP2 з метрикою N*, тим самим, відкидаючи накопичену протоколом RP2 маршрутну інформацію про мережі-одержувачі в домені N, і утворюючи маршрутну петлю.

З маршрутною інформацією домена маршрутизації M після її перерозподілу в домен маршрутизації N виконуються такі ж дії.

Далі проведемо аналіз протоколів маршрутизації, що схильні до утворення маршрутних петель. Вище описані сценарії утворення маршрутних петель, описувалися на прикладах класичних дистанційно-векторних алгоритмів маршрутизації. Проте це не означає, що подібні сценарії з невеликими змінами не можуть бути застосовані в протоколах маршрутизації за станом каналів зв'язку.

Навіть при тому, що маршрутизаторам із запущеним протоколом маршрутизації за станом каналу відома точна топологія усієї мережі передачі даних домена маршрутизації, якому належить маршрутизатор, їм не відома топологічна інформація про зовнішні місця призначення. Протоколи маршрутизації за станом каналів зв'язку обробляють інформацію про зовнішні мережі-одержувачі подібно до того, як це роблять дистанційно-векторні протоколи маршрутизації. Отже, вони в тому ж ступені схильні до утворення маршрутних петель при перерозподілі маршрутної інформації.

1.2 Аналіз спільної роботи декількох протоколів маршрутизації

1.2.1 Спільна робота протоколів маршрутизації без перерозподілу

Очевидно, що нічого не заважає запустити два і більше протоколи маршрутизації на одному і тому ж маршрутизаторі. В деяких випадках це може здатися непоганою ідеєю. Наприклад, при плануванні переходу з одного протоколу маршрутизації на інший, потрібно включити новий протокол маршрутизації в "тіньовому режимі", тобто встановити адміністративну відстань більшу, ніж у основного протоколу маршрутизації.

Хоча ідея здається непоганою, вона навряд чи життєздатна, якщо в якості нового протоколу маршрутизації вибраний дистанційно-векторний протокол.

Насправді дистанційно-векторні протоколи маршрутизації можуть оголошувати тільки ті мережі-одержувачі, які були успішно внесені ними у свою таблицю маршрутизації. У описаній ситуації, навмисно зроблено так щоб маршрути нового протоколу маршрутизації не потрапляли в таблицю маршрутизації, отже, маршрутизатори не зможуть обмінюватися маршрутною інформацією по новому протоколу маршрутизації, оскільки джерелом при обміні маршрутною інформацією є таблиця маршрутизації.

Може здатися, що протокол EIGRP не дотримується описане обмеження, оскільки, на відміну від класичних дистанційно-векторних

протоколів маршрутизації, в протоколі EIGRP, є таблиця топології, в якій є вся необхідна інформація для побудови таблиці маршрутизації.

Розглянемо, наскільки сильно відрізняється поведінка протоколу EIGRP від інших дистанційно-векторних протоколів маршрутизації в запропонованій ситуації. Для цього скористаємося мережею передачі даних зображеної на рис. 1.6

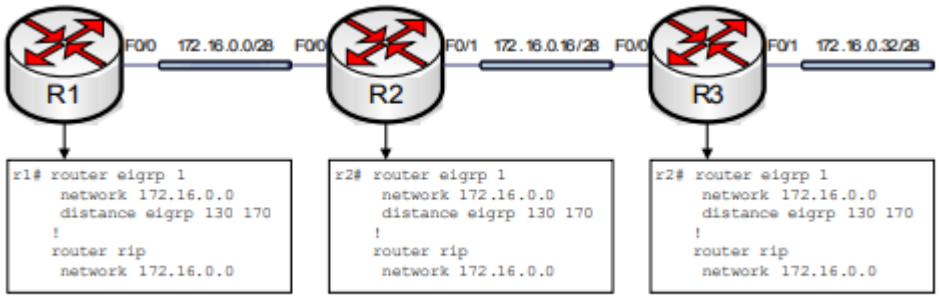

Рисунок 1.6 - Спільна робота двох протоколів маршрутизації без перерозподілу маршрутної інформації [1]

На усіх маршрутизаторах тих, що входять в мережу передачі даних паралельно запущено два протоколи маршрутизації - це протоколи RIP і EIGRP. Необхідно звернути увагу на те що, усі маршрутизатори мають у своїй конфігурації рядок distance eigrp 130 170, яка встановлює адміністративну відстань протоколу EIGRP рівним 130, що більше адміністративної відстані протоколу RIP, рівного 120.

Розглянемо таблицю маршрутизації маршрутизатора R1, показану в лістингу 1.1.

Лістинг 1.1 - Таблиця маршрутизації маршрутизатора R1

```
r1#show ip route
     172.16.0.0/28 is subnetted, 3 subnets
R       172.16.0.32 [120/2] via 172.16.0.1, 00:00:18, FastEthernet0/0
R       172.16.0.16 [120/1] via 172.16.0.1, 00:00:18, FastEthernet0/0
C       172.16.0.0 is directly connected, FastEthernet0/0
```

Як і очікувалося, в таблиці маршрутизації відсутні маршрути, отримані за допомогою протоколу EIGRP.

Тепер розглянемо таблицю топології маршрутизатора R1, вона представлена в лістингу 1.2.

Лістинг 1.2 - Таблиця топології маршрутизатора R1

```
Router#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(172.16.0.2)

P 172.16.0.16/28, 0 successors, FD is Inaccessible
        via 172.16.0.1 (30720/28160), FastEthernet0/0
P 172.16.0.0/28, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
```

Таблиця топології містить тільки два записи, одну про безпосередньо підключеній мережі 172.16.0.0/28, і одну, отриману від сусіднього маршрутизатора R2, 172.16.0.16/28. Про інші мережі тих, що знаходяться в домені маршрутизації EIGRP, записи в таблиці топології відсутні.

Як видно з прикладу 17.2 маршрутизатор R2 оголошує мережу 172.16.0.16/28 маршрутизатору R1, з метрикою не рівної нескінченності. Проте маршрутизатор R1, позначає цей запис як недоступну, оскільки процесу маршрутизації EIGRP не вдалося помістити цей маршрут в таблицю маршрутизації, оскільки там вже є присутнім маршрут до цієї мережі з меншою адміністративною відстанню, отриманий від протоколу RIP.

Процеси EIGRP запущені на інших маршрутизаторах поступають так само. Вони позначають як недоступні усі мережі, отримані в маршрутних оновленнях, що поступили від сусідніх маршрутизаторів. Оскільки мережі одержувачі недоступні, маршрутизатори не стануть їх оголошувати своїм сусідам.

Цей приклад наочно ілюструє, що незалежно від наявності таблиці топології в протоколі EIGRP його дистанційно-векторна природа не дозволяє використати наявну інформацію.

Якщо видалити команду distance eigrp 130 170 з конфігурації маршрутизатора R1, то він використовуватиме адміністративну відстань призначену протоколу EIGRP за умовчанням і рівне 90. Отже, протокол EIGRP в даному випадку зможе встановлювати маршрути в таблицю маршрутизації.

Чи станеться це насправді? У лістингу 1.3 наводиться таблиця маршрутизації побудована маршрутизатором R1, після того, як на ньому була відновлена за замовчуванням адміністративна відстань протоколу EIGRP.

Дійсно в таблиці маршрутизації з'явився один маршрут, отриманий по протоколу EIGRP. Цей маршрут відноситься до єдиної мережі одержувачеві, що знаходився в таблиці топології маршрутизатора R1 з лістингу 1.2. Цікавою особливістю цієї мережі одержувача є те що вона розташована рівно в одному переході від маршрутизатора R1. Проте для мереж одержувачів розташованих далі одного переходу в таблицю маршрутизації досі вказані маршрути протоколу RIP.

Лістинг 1.3 - Таблиця маршрутизації маршрутизатора R1 після відновлення адміністративної відстані протоколу EIGRP

```
r1#show ip route
     172.16.0.0/28 is subnetted, 3 subnets
R       172.16.0.32 [120/2] via 172.16.0.1, 00:00:15, FastEthernet0/0
D       172.16.0.16 [90/30720] via 172.16.0.1, 00:00:16, FastEthernet0/0
C       172.16.0.0 is directly connected, FastEthernet0/0
```

Це не дивно, оскільки на маршрутизаторі R2 і далі процес маршрутизації EIGRP досі має більшу адміністративну відстань, ніж процес маршрутизації RIP. Отже, маршрутизатор R2 оголошує за допомогою протоколу EIGRP тільки безпосередньо підключені до нього мережі одержувачі, які у кращому разі розташовані в одному переході від маршрутизатора R1.

Якщо подивитися таблицю топології маршрутизатора R1 (Лістинг 1.4) можна побачити, що запис про мережу 172.16.0.16 більше не помічена як недоступна.

Лістинг 1.4 - Таблиця топології маршрутизатора R1 після відновлення адміністративної відстані протоколу EIGRP

```
show ip eigrp topology
P 172.16.0.16/28, 1 successors, FD is 30720
        via 172.16.0.1 (30720/28160), FastEthernet0/0
P 172.16.0.0/28, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
```

Це пов'язано з тим, що тепер у протоколу маршрутизації EIGRP запущеного на маршрутизаторі R1, менша адміністративна відстань, чим у протоколу RIP, і він може занести в таблицю маршрутизації відомі йому маршрути.

З розглянутого прикладу можна зробити висновок про те, що хоча ідея запуску в тіньовому режимі протоколу маршрутизації EIGRP, виглядає досить привабливою, вона не приносить бажаного результату, що відповідає загальному правилу дистанційно векторних протоколів маршрутизації.

Тепер розглянемо приклад для мережі передачі даних, показаної на рис. 1.6, але з вибраним в якості тіньового протоколу маршрутизації протоколом OSPF.

Для запуску протоколу OSPF в тіньовому режимі використовується команда distance ospf intra - area 130, що встановлює адміністративну відстань внутрішньозональних маршрутів більшим, ніж адміністративна відстань маршрутів отриманих по протоколу RIP. Після запуску протоколу маршрутизації OSPF в тіньовому режимі на усіх маршрутизаторах представленої мережі передачі даних, необхідно подивитися таблицю топології мережі передачі даних побудовану протоколом OSPF (Лістинг 1.5).

Лістинг 1.5 - Таблиця топології мережі передачі даних побудована протоколом OSPF

```
r1#show ip ospf database

            OSPF Router with ID (172.16.0.2) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.0.2      172.16.0.2      270         0x80000002 0x0047EF 1
172.16.0.17     172.16.0.17     271         0x80000001 0x009BD2 2
172.16.0.33     172.16.0.33     271         0x80000002 0x006396 2

                Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.0.0      172.16.0.2      270         0x80000001 0x0075C9
172.16.0.16     172.16.0.17     272         0x80000001 0x00519F
172.16.0.32     172.16.0.33     271         0x80000001 0x0001CA
```

З лістингу видно, що в таблиці топології побудованої протоколом OSPF, є присутніми записи про усі маршрутизатори і мережі одержувачах розташованих в даній мережі передачі даних.

Видалимо з налаштування процесу маршрутизації OSPF команду distance ospf intra - area 130, повернувши тим самим адміністративну відстань протоколу OSPF використовувану за замовчуванням і рівну 110.

Подивимося, як зміниться таблиця маршрутизації (Лістинг 1.6).

Лістинг 1.6 - Таблиця маршрутизації маршрутизатора R1 після відновлення адміністративної відстані протоколу OSPF

```
r1#show ip route
     172.16.0.0/28 is subnetted, 3 subnets
O       172.16.0.32 [110/3] via 172.16.0.1, 00:00:10, FastEthernet0/0
O       172.16.0.16 [110/2] via 172.16.0.1, 00:00:10, FastEthernet0/0
C       172.16.0.0 is directly connected, FastEthernet0/0
```

Слід звернути увагу, що маршрути, отримані по протоколу OSPF, повністю замінили в таблиці маршрутизації маршрути протоколу RIP. Це відбувається, тому що протокол OSPF, має повну топологічну інформацію про усю мережу передачі даних, в якій він працює, по цій інформації кожен

маршрутизатор може самостійно розрахувати маршрути до усіх мереж одержувачів розташованих в мережі передачі даних.

Після розгляду цього прикладу можна зробити висновок, що запуск протоколу маршрутизації за станом каналів зв'язку в тіньовому режимі дає бажаний результат, і тому таку можливість варто розглядати як попередній етап в проектах переходу з одного протоколу маршрутизації на інший.

До запуску протоколу маршрутизації OSPF в тіньовому режимі слідує підходити дуже обережно, уважно перевіривши конфігурацію процесу маршрутизації OSPF перед установкою його адміністративної відстані меншим, ніж у використовуваного протоколу маршрутизації і розглянувши всі можливі сценарії розвитку подій в мережі передачі даних після зміни адміністративної відстані.

При необхідності переходу на новий протокол маршрутизації в корпоративній мережі передачі даних слід розглядати в першу чергу перехід саме на протокол OSPF.

Нині протокол OSPF вважається, перспективнішим рішенням для використання в середніх і великих корпоративних мережах передачі даних. У нього безліч плюсів в порівнянні з іншими, поширеними нині, внутрішніми протоколами маршрутизації, головні з яких це: відкрита специфікація, ієрархічна архітектура, а так само значно кращі тимчасові параметри виявлення і обробки змін в топології мережі передачі даних.

1.2.2 Налаштування базового перерозподілу маршрутної інформації

Перед налаштуванням перерозподілу маршрутної інформації між її джерелами необхідно визначити:

Джерело маршрутної інформації - в якості джерела маршрутної інформації можуть виступати динамічні протоколи маршрутизації, статичні і приєднані маршрути;

Одержувач маршрутної інформації - в якості одержувача маршрутної інформації можуть виступати тільки протоколи динамічної маршрутизації;

Напрям перерозподілу - перерозподіл маршрутної інформації може бути як одностороннім, так і двостороннім, якщо перерозподіл здійснюється між двома динамічними протоколами маршрутизації.

Механізм перерозподілу маршрутної інформації включається при допомозі команди redistribute. Синтаксис команди redistribute залежить від джерела маршрутної інформації, загальний синтаксис команди наводиться в лістингу 1.7.

Лістинг 1.7 - Синтаксис команди redistribute

```
(config-router)#redistribute protocol [metric metric-value][tag tag-value]
[route-map map-tag]
(config-router)# no redistribute protocol [metric metric-value][tag tag-value]
[route-map map-tag]
```

Опис параметрів команди redistribute наводитися в таблиці 1.1.

Таблиця 1.1 - Параметри команди redistribute

Параметр	Опис
Protocol	Джерело маршрутної інформації.
Metric *metric-value*	Метрика призначена для перерозподілених маршрутів.
Tag*rag-value*	Ярлик призначений для використання при контролі перерозподілу маршрутів.
Route-map*map-tag*	Ім’я маршрутної карти, яке використовується при перерозподілі.

Найбільш поширені види джерел маршрутної інформації наводяться в таблиці 1.2.

Таблиця 1.2 - Найбільш поширені джерела маршрутної інформації.

Джерело маршрутної інформації	Опис
connected	Перерозподіл безпосередньо підключених до маршрутизатора мереж.
static	Перерозподіл статичних маршрутів налаштованих на маршрутизаторі
rip	Перерозподіл маршрутної інформації з протоколу RIP
eigrp	Перерозподіл маршрутної інформації з протоколу EIGRP
ospf	Перерозподіл маршрутної інформації з протоколу OSPF.
bgp	Перерозподіл маршрутної інформації з протоколу BGP.

Розглянемо метрику, що привласнюється маршрутам, що перерозподіляються. Не обов'язкове ключове слово metric команди redistribute, задає метрику, що привласнюється отриманим при перерозподілі маршрутам. Значення метрики залежить від протоколу маршрутизації, в який робитиметься перерозподіл маршрутної інформації. Для протоколу RIP і OSPF метрика задається одним числом з можливого для протоколу діапазону метрик. Для протоколу RIP таким діапазоном є діапазон від 1 до 15, а для протоколу OSPF, необхідне значення метрики можна розрахувати по формулі (1.3), де як пропускна спроможність каналу зв'язку використовується величина, підібрана з потреб конкретної мережі передачі даних.

Метрика протоколу OSPF розраховується за формулою:

$$Metric = 108/BW \quad (1.3)$$

де BW – ширина смуги пропускання каналу зв’язку.

Протокол EIGRP для розрахунку вартості маршрутів використовує комбіновану метрику, що обчислюється по п'яти компонентах, які вказуються по порядку. Це пропускна спроможність, вимірювана в Кбит/з, затримка, надійність, завантаження і значення MTU. Кожен їх цих

параметрів, так само як і для протоколу OSPF, виставляється виходячи з потреб конкретної мережі передачі даних.

Для маршрутів що перерозподіляються в протокол маршрутизації BGP, в якості BGP метрики використовується числова метрика протоколу маршрутизації, з якого робився перерозподіл.

Ще одним способом призначення метрики що усім, що перерозподіляється в протокол маршрутизації маршрутам з різних джерел являється призначення метрики за умовчанням, за допомогою команди default - metric. Синтаксис команди наводиться в лістингу 1.8

Лістинг 1.8 - Синтаксис команди default – metric

```
(config-router)# default-metric metric-value [bandwidth delay reliability
loading mtu]
(config-router)# no default-metric metric-value [bandwidth delay reliability
loading mtu]
```

Опис параметрів команди default - metric наводитися в таблиці 1.3.

Таблиця 1.3 - Параметри команди default – metric

Параметр	Опис
Metric-value	Метрика призначена за замовчуванням для всіх перерозподілених маршрутів.
Bandwidth	Значення пропускної здатності каналу зв’язку. Використовується для розрахунку комбінованої метрики EIGRP.
delay	Значення затримки каналу зв’язку. Використовується для розрахунку комбінованої метрики EIGRP.
Reliability	Значення надійності каналу зв’язку. Використовується для розрахунку комбінованої метрики EIGRP
loading	Значення загрузки каналу зв’язку. Використовується для розрахунку комбінованої метрики EIGRP
mtu	Значення MTU каналу зв’язку. Використовується для розрахунку комбінованої метрики EIGRP

Якщо не було використано ні ключове слово metric в команді redistribute, ні команду default-metric, то перерозподіленим маршрутам привласнюються метрики, встановлені за умовчанням для перерозподілених в цей протокол маршрутизації маршрутів. Значення метрик за замовчуванням для перерозподілених маршрутів наводиться в таблиці 1.4.

Таблиця 1.4 - Метрики маршрутів використовувані за замовчуванням при перерозподілі маршрутної інформації

Отримувач маршрутної інформації	Метрика за замовчуванням
RIP	Нескінченність
EIGRP	Нескінченність
OSPF	20
BGP	Вихідна метрика маршруту

1.2.3 Налаштування перерозподілу маршрутної інформації з приєднаних і статичних маршрутів

Приклад налаштування перерозподілу маршрутної інформації з приєднаних і статичних маршрутів наводиться на рис. 1.7.

Перерозподіл маршрутної інформації з приєднаних і статичних маршрутів в динамічні протоколи маршрутизації здійснюється за допомогою команд redistributeconnected і redistributestatic відповідно.

Синтаксис команд відповідає загальному синтаксису команди redistribute описаному в лістингу 1.7.

Після застосування команд redistributeconnected і redistributestatic на маршрутизаторах R1 і R2 в їх таблицях маршрутизації з'явилися маршрути протоколу RIP до безпосередньо підключених до їх сусідів мереж, хоча команд network що описують ці мережі в конфігурації процесу маршрутизації RIP немає.

Варто також звернути увагу на те, що в конфігурації маршрутизатора R2, відсутня команда redistributestatic, проте в таблиці маршрутизації

маршрутизатора R1, знаходиться мережа 172.16.1.0/24. Це пов'язано з тим, що в протоколі маршрутизації RIP механізм перерозподілу маршрутної інформації включається автоматично для статичних маршрутів, у яких в якості точки призначення вказується не IP адреса, а безпосередньо підключений інтерфейс, а також IP адреса мережі одержувача належить мережам, описаним в одній з команд network процесу маршрутизації RIP.

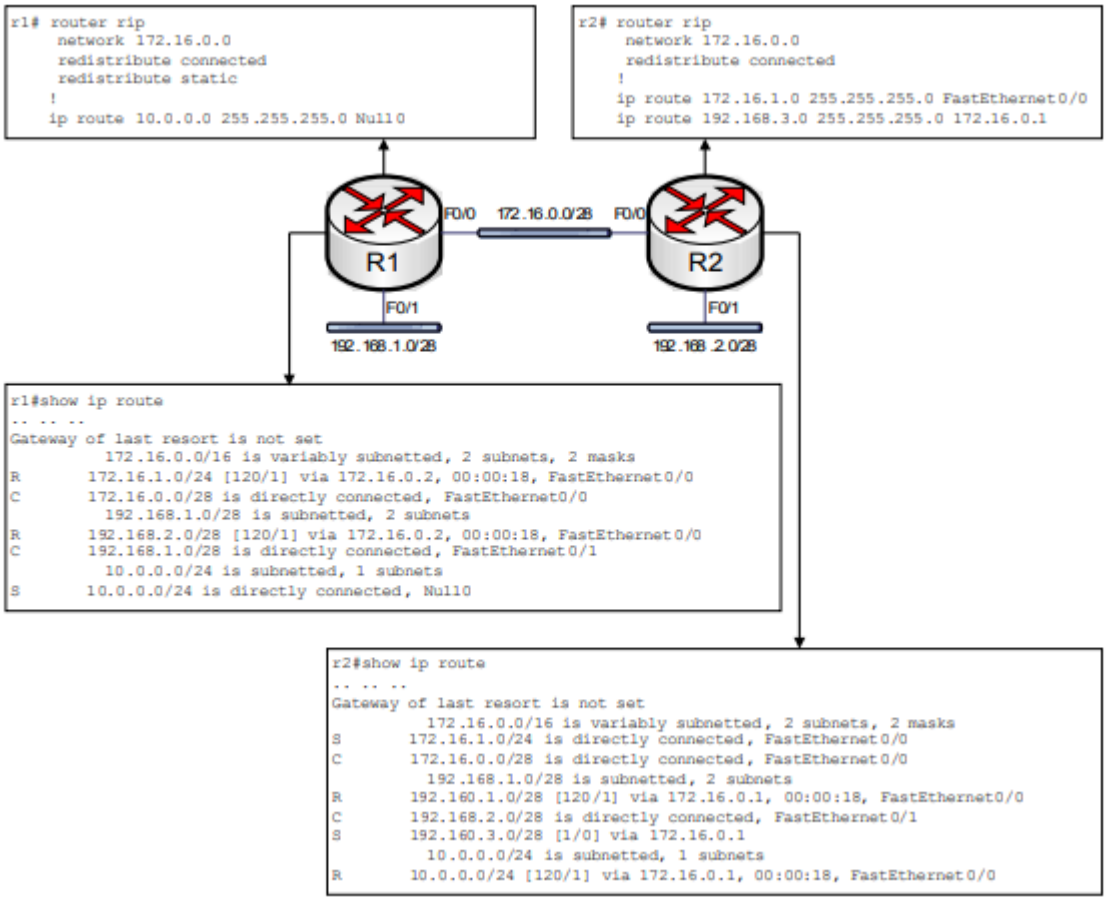

Рисунок 1.7 - Перерозподіл приєднаних і статичних маршрутів в протокол RIP [1]

Розглянутий механізм поширення інформації про безпосередньо підключені до маршрутизатора мережі-одержувача в динамічний протокол маршрутизації, може здатися, досить зручним, з точки зору внесення змін до конфігурації процесу маршрутизації таких протоколів як EIGRP або OSPF. Адже досить один раз використати команду redistribute connected при

налаштуванні процесу маршрутизації і надалі не треба описувати в процесі маршрутизації нові мережі, що налаштовуються на маршрутизатор і видаляти невживані за допомогою команд network.

Варто відмітити, що практика такого використання команди redistribute connected широко поширена в корпоративних мережах передачі даних. Проте таке поширення інформації про безпосередньо підключені мережі в протоколи маршрутизації EIGRP і OSPF являється абсолютно неправильним.

Як згадувалося раніше, в протоколі маршрутизації EIGRP, введено розділення внутрішніх і зовнішніх маршрутів по адміністративній відстані.

Внутрішні маршрути протоколу EIGRP мають адміністративну відстань рівна 90, що дозволяє їм вигравати практично у будь-яких інших динамічних протоколів маршрутизації, тоді як для зовнішніх маршрутів протокол EIGRP за умовчанням встановлює адміністративну відстань рівним 170 (Рис. 1.8). Це призводить до того, що зовнішні маршрути протоколу EIGRP навпаки програють усім іншим динамічним протоколам маршрутизації. Отже ця ситуація потенційно може призводити до виникненню маршрутних петель в домені маршрутизації EIGRP.

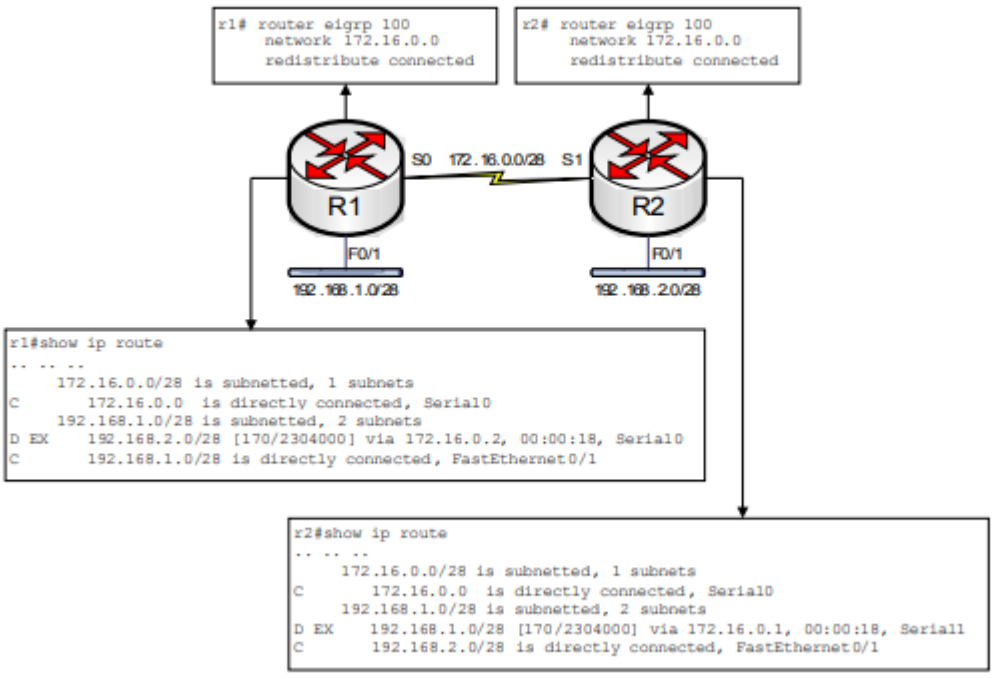

Рисунок 1.8 - Перерозподіл приєднаних маршрутів у протокол EIGRP [1]

Приклад використання команди redistribute в протоколі OSPF приводиться на рис. 1.9.

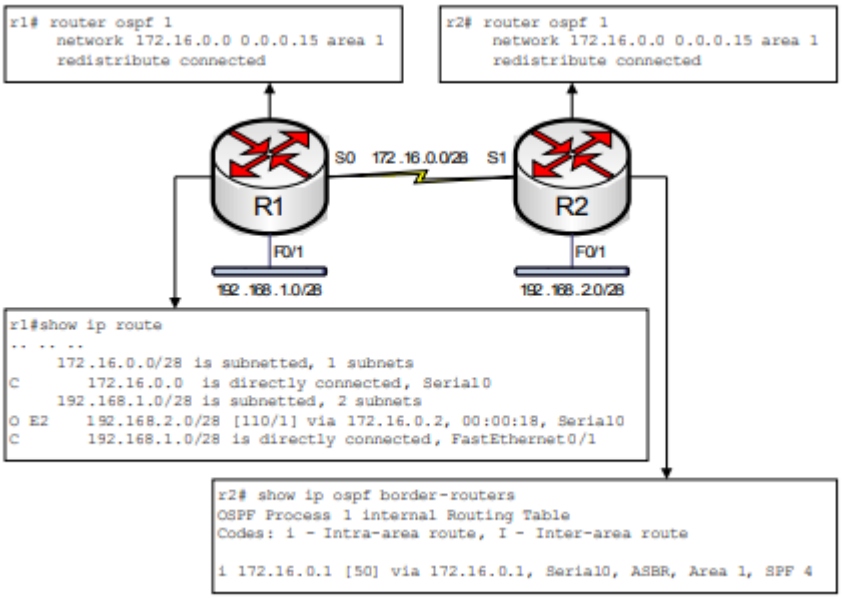

Рисунок 1.9 - Перерозподіл приєднаних маршрутів у протокол OSPF [1]

Після використання цієї команди в налаштуванні процесу маршрутизації OSPF, маршрутизатор стає ASBR маршрутизатором, і робить поширення, отриманих так само маршрутів за допомогою LSA повідомлень 5 типу. Як відомо поширення даних LSA робиться без змін по усьому обміну маршрутизації OSPF. Крім того, в протоколі OSPF є заборона на розміщення ASBR маршрутизаторів в тупикових зонах.

Як відомо при перерозподілі протокол OSPF для перерозподілених в нього маршрутів, за умовчанням встановлює другий тип зовнішнього маршруту, а це означає, що метрика цього маршруту не змінюється при поширенні маршруту усередині домена маршрутизації OSPF. Цей факт може призводити до побудови неоптимальних або навіть неправильних таблиць маршрутизації в мережах передачі даних із складною топологічною структурою, в якій застосовуються канали зв'язку з різними величинами пропускної спроможності.

З вищесказаного можна зробити висновок, що в протоколах маршрутизації EIGRP і OSPF перерозподіл з приєднаних і статичних маршрутів, можна використати в обмежених масштабах і тільки як тимчасове рішення.

1.2.4 Налаштування перерозподілу маршрутної інформації в протокол RIP

Перерозподіл маршрутної інформації в протокол маршрутизації RIP здійснюється за допомогою команди redistribute, синтаксис якої наводиться в лістингу 1.9.

Лістинг 1.9 - Синтаксис команди redistribute (RIP)

```
(config-router)#redistribute protocol [process-id] [as-number] [metric metric-
value] [match route-type] [tag tag-value] [route-map map-tag]
(config-router)# no redistribute protocol [process-id] [as-number] [metric
metric-value] [match route-type] [tag tag-value] [route-map map-tag]
```

Опис параметрів команди redistribute (RIP) наводитися в таблиці 1.5.

Таблиця 1.5 - Параметри команди redistribute (RIP)

Параметр	Опис
protocol	Джерело маршрутної інформації.
Process-id	Ідентифікатор процесу маршрутизації. Використовується при перерозподілі з протоколу OSPF.
As-number	Номер автономної системи. Використовується при перерозподілу з протоколів EIGRP або BGP.
Metric metric-value	Метрика призначена для перерозподілу маршрутів.

Продовження таблиці 1.5

Match route-type	Тип перерозподілених маршрутів. Може приймати значення: External 1 - Зовнішній маршрут 1 типу; External 2 - Зовнішній маршрут 2 типу. Параметр застосовується при перерозподілу з протоколу OSPF.
Tag tag-value	Ярлик призначений для використання при контролі перерозподілу маршрутів.
Route-map map-tag	Ім'я маршрутної карти яка використовується при перерозподілу.

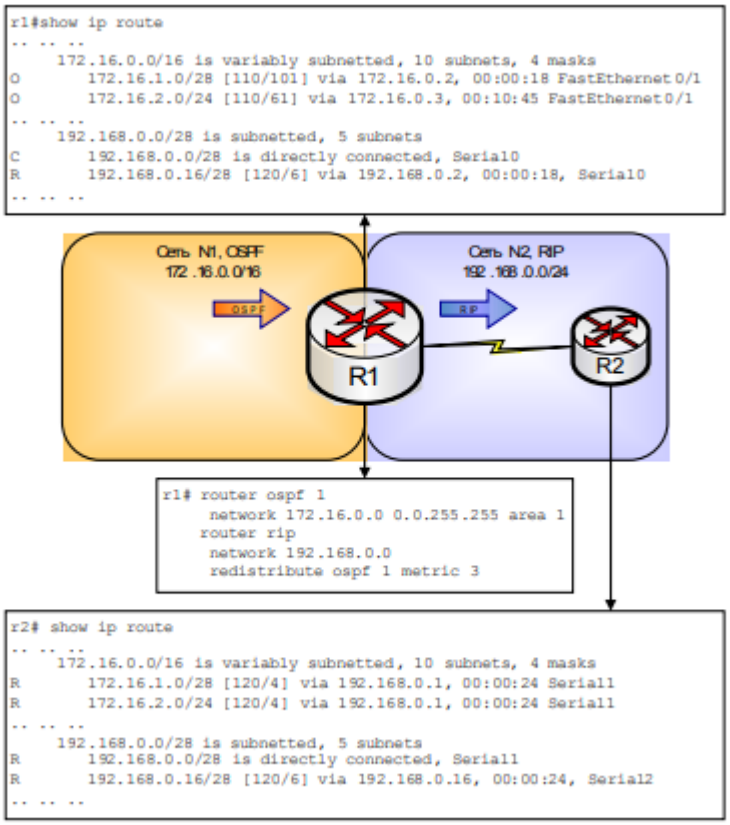

Рисунок 1.10 - Перерозподіл маршрутної інформації у протокол RIP [1]

На рис. 1.10 наводиться приклад налаштування перерозподілу маршрутної інформації в протокол RIP з протоколу OSPF.

На маршрутизаторі R1 запущені два протоколи маршрутизації : протоколи OSPF і RIP. Маршрутизатор R1 робить перерозподіл маршрутній

інформації з N1 в N2, і встановлює метрику для перерозподілених маршрутів в протокол RIP, рівну 3 переходам. Оскільки в команді redistribute не вказані типи маршрутів протоколу OSPF, які мають бути перерозподілені в протокол RIP, буде зроблено перерозподіл усіх маршрутів усіх типів з протоколу OSPF.

Маршрутизатор R2 отримує маршрути до мереж одержувачів з N1 як внутрішні маршрути протоколу RIP.

З наведеного прикладу видно, що протокол RIP не робить розділення маршрутів внутрішні, включені в процес маршрутизації при допомозі команд network, і зовнішні, отримані при перерозподілі маршрутній інформації із зовнішніх джерел.

1.2.5 Налаштування перерозподілу маршрутної інформації в протокол EIGRP

Перерозподіл маршрутної інформації в протокол маршрутизації EIGRP здійснюється за допомогою команди redistribute, синтаксис якої наводиться в лістингу 1.10.

Лістинг 1.10 - Синтаксис команди redistribute (EIGRP)

```
(config-router)#redistribute protocol [process-id] [as-number] [metric metric-
value] [match route-type] [metric metric-value][tag tag-value] [route-map map-
tag]
(config-router)# no redistribute protocol [process-id] [as-number] [metric
metric-value] [match route-type] [metric metric-value][tag tag-value] [route-
map map-tag]
```

У синтаксисі команди redistribute (EIGRP) є присутнім параметр as-number, цей параметр застосовується не лише при перерозподілі маршрутній інформації з протоколу BGP, але і з екземпляра протоколу EIGRP запущеного в іншій автономній системі.

На рис. 1.11 наводиться приклад налаштування перерозподілу маршрутної інформації в протокол EIGRP з протоколу RIP.

На маршрутизаторі R1 запущені два протоколи маршрутизації : протоколи RIP і EIGRP. Маршрутизатор R1 робить перерозподіл маршрутній інформації з N1 в N2. Необхідно звернути увагу на те що при виконання перерозподілу маршрутизатор R1, не встановлює фіксовану метрику, як це було в протоколі RIP, а фіксовано задає п'ять змінних, по яких протокол EIGRP відповідно до свого алгоритму зможе розрахувати метрику для перерозподілених маршрутів.

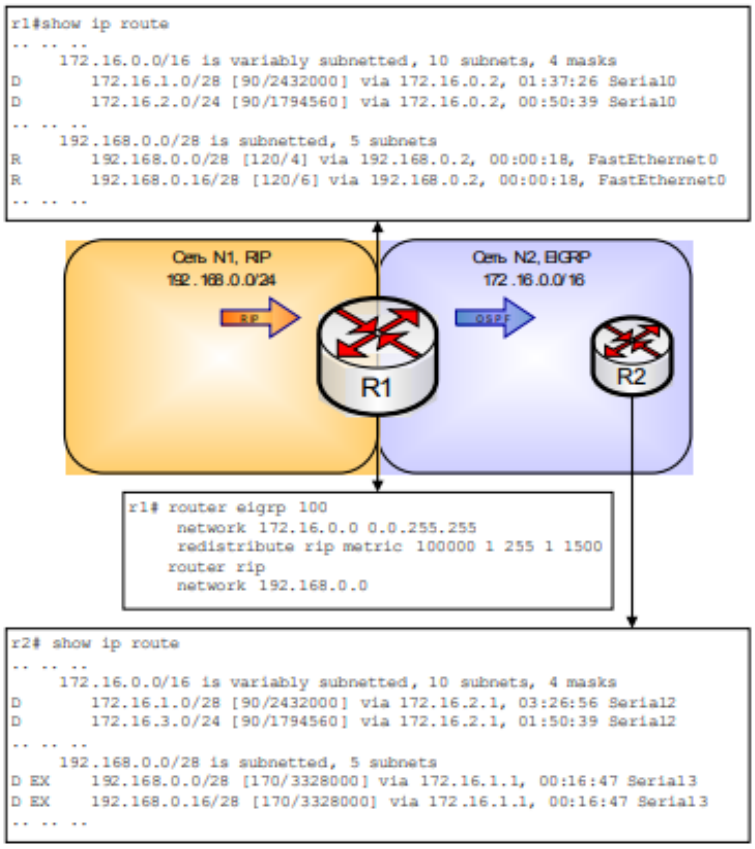

Рисунок 1.11 – Перерозподіл маршрутної інформації у протокол EIGRP [1]

Маршрутизатор R2 отримує маршрути до мереж одержувачів з N1 як зовнішні маршрути протоколу EIGRP, про це свідчить адміністративна відстань, рівна 170 і ярлик "EX", що вказує на механізм отримання маршруту, як зовнішнього маршруту протоколу EIGRP.

1.2.6 Налаштування перерозподілу маршрутної інформації в протокол OSPF

Перерозподіл маршрутної інформації в протокол маршрутизації OSPF здійснюється за допомогою команди redistribute, синтаксис якої наводиться в лістингу 1.11. У таблиці 1.6 наводяться описи часткових параметрів команди redistribute (OSPF).

Лістинг 1.11 - Синтаксис команди redistribute (OSPF)

```
(config-router)#redistribute protocol [process-id] [as-number] [metric metric-
value] [metric-type type-value] [match route-type] [metric metric-value][tag
tag-value] [route-map map-tag] [subnets]
(config-router)# no redistribute protocol [process-id] [as-number] [metric
metric-value] [metric-type type-value] [match route-type] [metric metric-
value][tag tag-value] [route-map map-tag] [subnets]
```

Таблиця 1.6 – Часткові параметри команди redistribute (OSPF)

Параметр	Опис
Metric-type *type-value*	Тип зовнішнього маршруту OSPF, яким буде присвоєно перерозподіл маршрутам. За замовчуванням тип 2.
subnets	Виробляти перерозподіл маршрутів до підмереж. Якщо даний параметр не використовується, в протокол OSPF перерозподіляються лише маршрути до класових мереж.

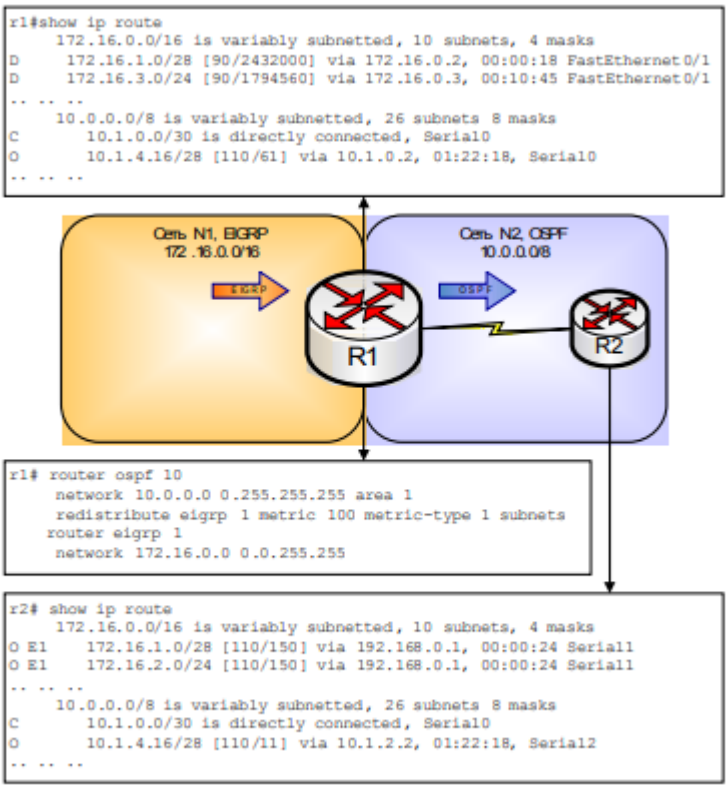

Рисунок 1.12 - Перерозподіл маршрутної інформації у протокол OSPF [1]

На рис. 1.12 наводиться приклад налаштування перерозподілу маршрут утвореної інформації в протокол OSPF з протоколу EIGRP.

На маршрутизаторі R1 запущені обидва протоколи маршрутизації : протоколи EIGRP і OSPF. Маршрутизатор R1 робить перерозподіл повній маршрутній інформації з N1 в N2, встановлює метрику для перерозподілених маршрутів в протокол OSPF, рівну 100, а також призначає 1 тип зовнішніх маршрутів для маршрутної інформації, що перерозподіляється. Це означає, що метрика перерозподілених маршрутів в домені маршрутизації OSPF змінюватиметься у міру поширення зовнішніх маршрутів по домену OSPF.

1.3 Висновки до розділу 1

- В ході роботи над розділом розглянуто поняття перерозподілу маршрутної інформації;

- Розглянуто протоколи (RIP, OSPF, EIGRP) перерозподілу маршрутної інформації;

-Розглянуто спільну робота двох протоколів маршрутизації без перерозподілу та з перерозподілом маршрутної інформації.

2 АНАЛІЗ ЗАСОБІВ МОДЕЛЮВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ IP-МЕРЕЖ

2.1 Використання програми Cisco Packet Tracer для моделювання роботи телекомунікаційних IP-мереж

2.1.1 Основи використання симулятора мереж Cisco Packet Tracer

Cisco Packet Tracer є відмінним інструментом моделювання та візуалізації мережі, корисним для навчання як студентів, так і досвідчених користувачів, у яких під рукою немає фізичного обладнання компанії Cisco. Програма-симулятор дозволяє налаштовувати (віртуально) різноманітне телекомунікаційне обладнання фірми Cisco (комутатори, маршрутизатори, ip-телефони, шлюзи, сервера, міжмережеві екрани Cisco ASA і багато іншого). Інтерфейс простий і зрозумілий, і ви зможете створити і настроїти прості мережі в Packet Tracer навіть якщо не володієте глибокими знаннями в мережевих технологіях або обладнанні Cisco. Багато хто використовує ці програми для проектування і моделювання мереж, навчання студентів, підготовці до сертифікаційних іспитів CCNA/CCNP, отримання практичних навичок пошуку та усунення проблем в мережах на обладнанні Cisco.

Щоб освоїти основи використання Cisco Packet Tracer, потрібно ознайомитися з інтерфейсом програми.

Інтерфейс програми дуже простий, немає складних налаштувань, елементів управління і розгалужених меню, що приємно дивує користувачів.

- Верх вікна програми виконаний в класичному стилі, в якому немає нічого зайвого (базові функції операції з файлами, скасування дії, масштабування, збереження, копіювання).

- У правій частині вікна зібрані функції для позначок, виділення областей, видалення і переміщення об'єктів.

- У нижній частині розміщена основні інструменти Cisco Packet Tracer, які використовуються для створення вашої мережі. У лівому нижньому кутку програми містяться різні види мережевого обладнання (комутатори,

маршрутизатори, телефони, шлюзи, сервера, хаби, бездротові джерела, пристрої захисту мережі, емуляція WAN-з'єднання, комп'ютери, принтери, телевізори, мобільні телефони та багато іншого). При постійному використанні програми Cisco Packet Tracer, часто використовувані пристрою запам'ятовуються і відображаються в спеціальній папці (Custom Made Devices).

2.1.2 Характеристика Cisco Packet Tracer

Cisco Packet Tracer розроблений компанією Cisco і рекомендований для використання при вивченні телекомунікаційних мереж і мережевого устаткування, а також для проведення уроків з лабораторних робіт у закладах вищої освіти.

Основні можливості Packet Tracer:

• Дружній графічний інтерфейс (GUI), що сприяє кращому розумінню організації мережі, принципів роботи пристрою;

• Можливість змоделювати логічну топологію: робочий простір для того, щоб створити мережі будь-якого розміру на CCNA-рівні складності;

• Моделювання в режимі real-time (реального часу);

• Режим симуляції;

• Багатомовність інтерфейсу програми: що дозволяє вивчати програму на своїй рідній мові.

• Вдосконалене зображення мережевого обладнання зі здатністю додавати/видаляти різні компоненти;

• наявність Activity Wizard дозволяє мережевим інженерам, студентам і викладачам створювати шаблони мереж і використовувати їх в подальшому.

• проектування фізичної топології: доступна взаємодія з фізичними пристроями, використовуючи такі поняття як місто, будівля, стійка і т.д .;

Широкий діапазон можливостей даного ПЗ дозволяє мережевим інженерам: конфігурувати, налагоджувати і будувати обчислювальну

мережу. Також даний продукт незамінний в навчальному процесі, оскільки дає наочне відображення роботи мережі, що підвищує освоєння матеріалу учнями.

Емулятор мережі дозволяє мережевим інженерам проектувати мережі будь-якої складності, створюючи і відправляючи різні пакети даних, зберігати і коментувати свою роботу. Фахівці можуть вивчати і використовувати такі мережеві пристрої, як комутатори другого і третього рівнів, робочі станції, визначати типи зв'язків між ними і з'єднувати їх.

На заключному етапі, після того як мережа спроектована, фахівець може приступати до конфігурації обраних пристроїв за допомогою термінального доступу або командного рядка (Рис 2.1.)

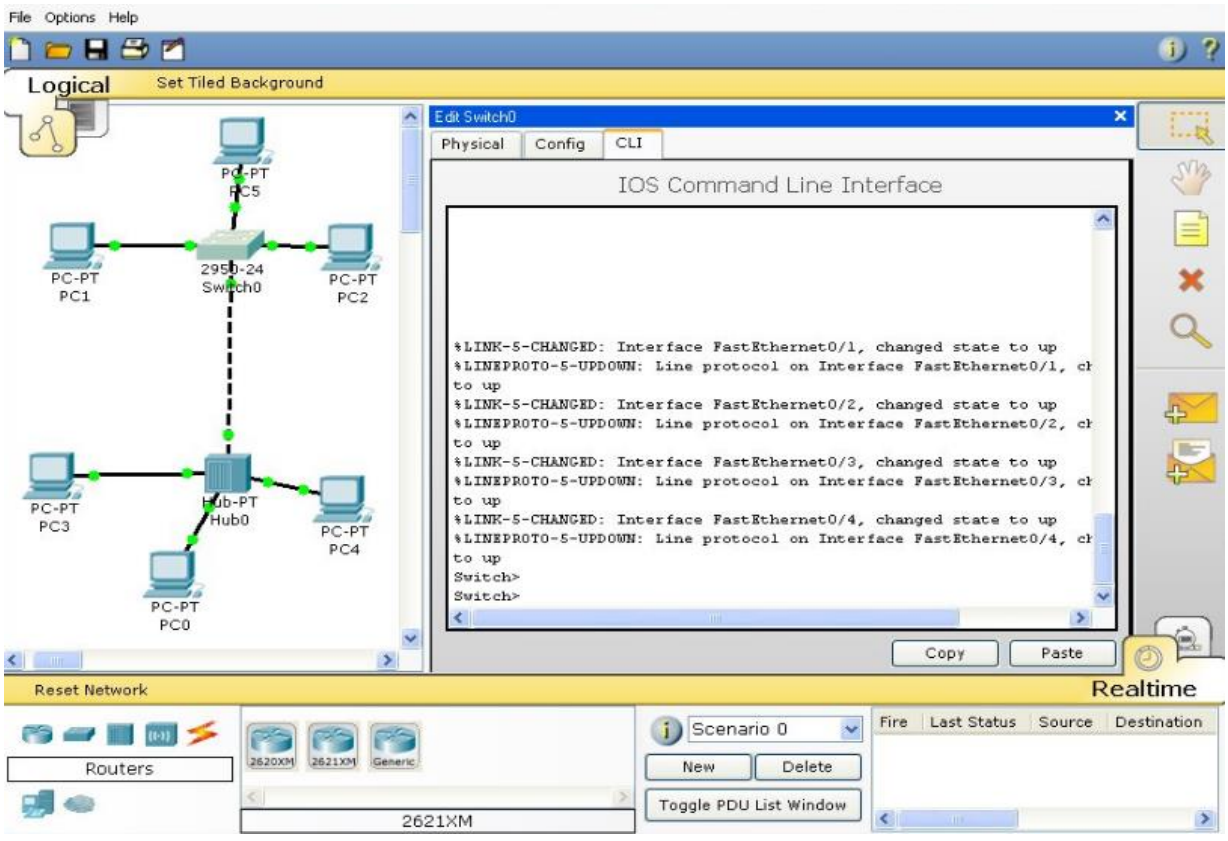

Рисунок 2.1 - Cisco Packet Tracer

Однією з найважливіших особливостей даного симулятора є наявність в ньому "Режиму симуляції" (Рис. 2.2). В даному режимі всі пакети, що пересилаються всередині мережі, відображаються в графічному вигляді. Ця

можливість дозволяє мережевим фахівцям наочно продемонструвати, яким інтерфейсом в даний момент переміщається пакет, який протокол використовується і т.д.

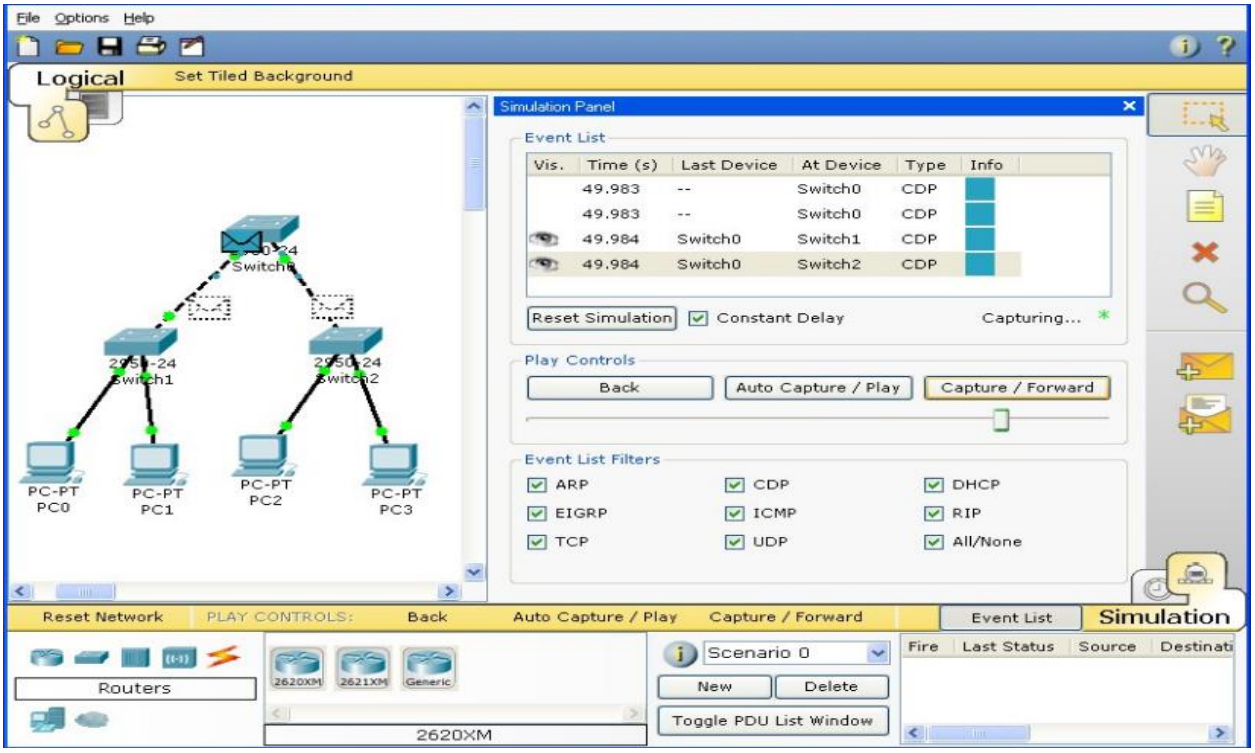

Рисунок 2.2 - "Режим симуляції" в Cisco Packet Tracer

Однак, це не всі переваги Packet Tracer: в меню "Режим симуляції" мережеві інженери можуть не тільки відслідковувати використовувані протоколи, а й бачити, на якому з семи рівнів моделі OSI даний протокол задіяний (Рис. 2.3).

Така, на перший погляд, простота і наочність робить практичні заняття надзвичайно корисними, поєднуючи в них як вивчення матеріалу, так і його закріплення.

Packet Tracer здатний моделювати велику кількість пристроїв різного призначення, а так само чимало різних типів зв'язків, що дозволяє проектувати мережі будь-якого розміру на високому рівні складності.

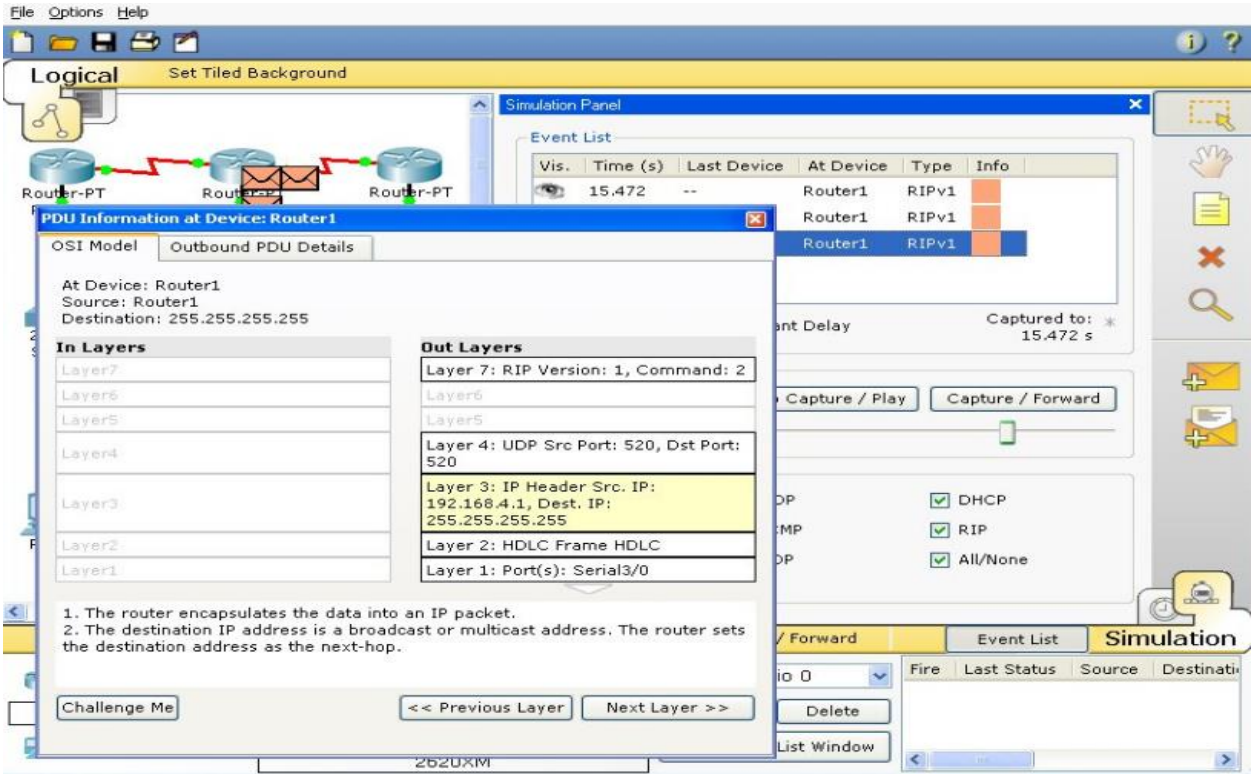

Рисунок 2.3 - Аналіз семирівневої моделі OSI в Cisco Packet Tracer

Пристрої, які моделюються:

- Комутатори третього рівня:
  - Router 2620 XM;
  - Router 2621 XM;
  - Router-PT.
- Комутатори другого рівня:
  - Switch 2950-24;
  - Switch 2950T;
  - Switch-PT;
  - з'єднання типу "міст" Bridge-PT.
- Мережеві концентратори:
  - Hub-PT;
  - повторювач Repeater-PT.
- Кінцеві пристрої:
  - робоча станція PC-PT;
  - сервер Server-PT;

    - принтер Printer-PT.
- Бездротові пристрої:
    - точка доступу AccessPoint-PT.
- Глобальна мережа WAN.

Типи звязків:

- консоль;
- телефонна лінія;
- мідний кабель без перехрещування (прямий кабель);
- мідний кабель з перехрещуванням (крос-кабель);
- Serial DCE;
- Serial DTE.
- волоконно-оптичний кабель;

Так само доцільно навести ті протоколи, які студент може відстежувати:

- EIGRP;
- ARP;
- CDP;
- ICMP;
- RIP;
- DHCP;
- TCP;
- UDP.

2.1.3 Інтерфейс Cisco Packet Tracer

Інтерфейс програми Cisco Packet Tracer наведений нижче (рис. 2.4.).

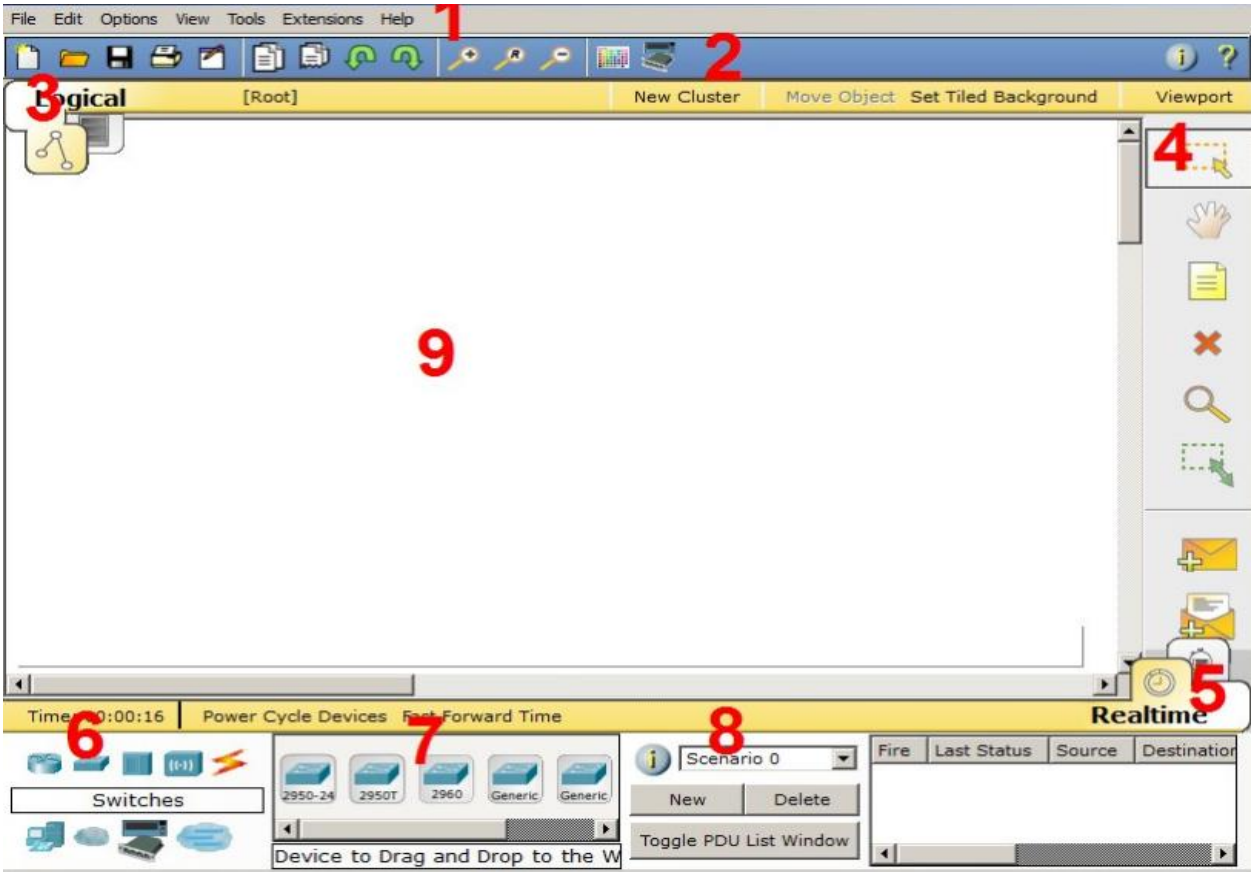

Рисунок 2.4 - Інтерфейс програми Cisco Packet Tracer

1. Головне меню програми;
2. Панель інструментів - дублює певні пункти меню;
3. Перемикач між логічною і фізичною організацією;
4. Додаткова панель інструментів: інструменти виділення, видалення, переміщення, масштабування об'єктів, а також формування незалежних пакетів;
5. Перемикач між режимом симуляції і режимом (Real-Time);
6. Панель ліній зв'язку і груп кінцевих пристроїв;
7. Безпосередньо кінцеві пристрої - тут містяться найрізноманітніші комутатори, вузли, точки доступу, провідники;

8. Панель створення користувацьких сценаріїв;

9. Робочий простір.

Більшу частину цього вікна займає робоча область, в якій можна розміщувати різні мережеві пристрої, з'єднувати їх різними способами і як наслідок отримувати найрізноманітніші мережеві топології.

Зверху, над робочою областю, розташована головна панель програми (Рис. 2.5) і її меню. Меню дозволяє виконувати збереження, завантаження мережевих топологій, налаштування симуляції, а також багато інших функцій. Головна панель містить на найбільш часто використовувані функції меню.

Рисунок 2.5 - Головна панель Packet Tracer

Праворуч від робочої області, розташована бічна панель, де знаходиться ряд кнопок, які відповідають за переміщення полотна робочої області, видалення об'єктів і т.д.

Знизу, під робочою областю, розташована панель обладнання (Рис. 2.6).

Дана панель містить в своїй лівій частині типи доступних пристроїв, а в правій частині доступні моделі. При наведенні на кожен з пристроїв, в прямокутнику, що знаходиться в центрі між ними буде відображатися його тип. Типи пристроїв, найбільш часто використовувані в лабораторних роботах Packet Tracer, представлені нижче (Рис. 2.7).

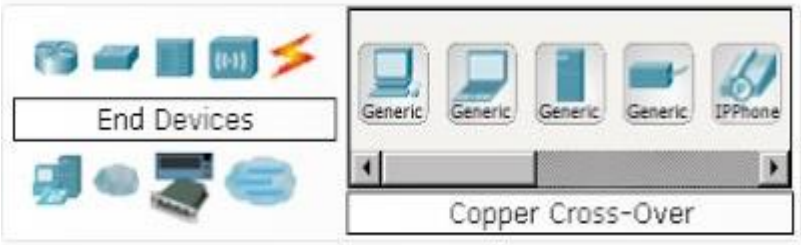

Рисунок 2.6 - Панель обладнання Packet Tracer

Рисунок 2.7 - Основні типи пристроїв

Не має сенсу розглядати конкретні моделі пристроїв кожного типу. Окремого розгляду заслуговують типи з'єднань. Найбільш часто використовувані з них (розгляд типів підключень йде зліва направо, відповідно до наведеного на Рис. 2.8).

Рисунок 2.8 - Типи з'єднань в Packet Tracer

• Автоматичний тип - при даному типі з'єднання Packet Tracer автоматично вибирає найкращий тип з'єднання для обраних пристроїв

• Консоль - консольні з'єднання

• Мідь Пряме - з'єднання мідним кабелем типу вита пара, обидва кінці кабелю обтиснуті в однаковій розкладці. Підійде для наступних з'єднань: комутатор - комп'ютер, комутатор - комутатор, комутатор - маршрутизатор.

• Мідь кросовер - з'єднання мідним кабелем типу вита пара, кінці кабелю обтиснуті як кросовер. Підійде для з'єднання двох комп'ютерів.

• Оптика - необхідно для з'єднання пристроїв, що мають оптичні інтерфейси за допомогою оптичного кабелю.

• Телефонний кабель - звичайний телефонний кабель.

• Коаксіальний кабель - слугує для з'єднання пристроїв за допомогою коаксіального кабелю.

2.2 Використання програми Graphical Network Simulator-3 для моделювання роботи телекомунікаційних IP-мереж

2.2.1 Теоретичні відомості про програму GNS3

Графічний мережевий симулятор (GNS3) - це безкоштовний інтерфейс клієнт-сервер з відкритим вихідним кодом для емуляції і віртуалізації мережі. Графічний емулятор, який дозволяє моделювати складні мережі. GNS3 підтримує великий обсяг віртуальних мережевих пристроїв від різних постачальників мережевого обладнання за рахунок використання пристроїв, які є простими в імпорті шаблонами. Його платформа побудована на основі Python. Для забезпечення повної емуляції, GNS3 тісно пов'язаний з наступними компонентами:

– PEM емулятор брандмауера CiscoPIX на основі Qemu;

– Dynagen – текстовий інтерфейс для Dynamips;

– Dynamips – ядро програми, що дозволяє емулювати CiscoIOS.

2.2.2 Характеристики GNS3

GNS3 є чудовим інструментом для реалізації лабораторних робіт Cisco, і слугує як для мережевих інженерів та адміністраторів, так і для людей, які бажають пройти сертифікацію CCNA, CCNP, CCIP і CCIE, JNCIA, JNCIS, JNCIE. Також дане програмне забезпечення може бути використано

для знайомства з Cisco IOS, Juniper, JUNOS, а також для налаштування і подальшої установки конфігурацій на реальні фізичні пристрої. GNS3 має ряд переваг в якості безкоштовного емулятора мережі з відкритим вихідним кодом.

Відкритий вихідний код емулятора можна переглянути на GitHub безкоштовно. Якщо користувач виявляє помилку в програмному забезпеченні, він може повідомити про це спільноті або самому розробнику. Може спробувати відтворити помилку, виправити її і відправити змінений вихідний код для поліпшення програмного забезпечення.

Емулятор дозволяє створити модель комп'ютера або іншого пристрою і запускати всередині оригінальне програмне забезпечення. Емулюються всі доступні компоненти пристрою, в тому числі, пристрої вводу/виводу, пам'ять і процесор.

Оскільки GNS3 є клієнт-серверним додатком, рекомендується розгортати віртуальну машину GNS3 VM (Virtual Machine) в якості сервера. Потім можна встановити клієнтську програму GNS3 на локальному комп'ютері і підключитися до сервера віртуальної машини GNS3. Після установки можна створювати мережеві топології за допомогою клієнтської частини ПО, які будуть виконуватися на сервері.

У випадку з Cisco, емулятор створює модель маршрутизатора і запускає всередині реальну операційну систему Cisco IOS. Таким чином ми отримуємо повнофункціональний маршрутизатор. Тобто запустивши маршрутизатор Cisco, ми отримаємо у доступі практично всі функції, які працюють на реальному маршрутизаторі (у Cisco Packet Tracer значна частина функціоналу недоступна, тому що це лише симулятор).

У GNS3 кожен віртуальний мережевий пристрій можна запускати і зупиняти незалежно від інших віртуальних пристроїв.

Емулятор не тільки підтримує Ethernet-з'єднання між мережевими пристроями, але і дозволяє встановлювати послідовні з'єднання між пристроями, що підтримують відповідні модулі.

Також у GNS3 можна додати повноцінний комп'ютер з Windows або Ubuntu. При цьому Windows Server або RedHat можна використовувати в схемі за допомогою технологій віртуалізації (VirtualBox або VMWare) або підключивши GNS3 до реальної мережі. Таким чином можна перевірити встановлений VPN, аутентифікацію користувачів через сервер та використовувати справжній браузер при підключенні до Інтернету.

2.3 Порівняльний аналіз засобів моделювання

2.3.1 Переваги та недоліки Cisco Packet Tracer

Packet Tracer має ряд переваг:

- Для роботи необхідно створити безкоштовний обліковий запис Cisco Networking Academy.
- Працює на більшості операційних систем.
- Має велику різноманітність пристроїв для симуляції.
- Надає безліч варіантів підключення мережевих пристроїв.
- Пропонує різні методи підключення та налаштування пристроїв.
- Працює в режимі реального часу.
- Є можливість налаштувати, перевірити і усунути неполадки на мережевих пристроях через вкладку CLI.
- Дозволяє створювати свої завдання за допомогою функції майстра завдань.

Основні недоліки програми:

- Все що виходить за рамки курсу CCNA, організувати в даному симуляторі неможливо
- При створенні завдання користувачем необхідно зберегти його у вигляді файлу, який необхідно поширити серед усіх зацікавлених сторін. Відсутність централізованого методу розподілу призводить до деяких проблем. Це є одним з недоліків програми.

- Все ПЗ має помилки, і Packet Tracer не є винятком. Помилки Packet Tracer, як правило, більш помітні (ще один недолік), ніж в інших симуляторах або емуляторах, можливо, через його популярність і широке використання.

- Є, по суті, симулятором, не підтримує повну віртуалізацію і запуск в віртуальних машинах, не працює з реальними прошивками пристроїв.

Незважаючи на недоліки, Cisco Packet Tracer залишається «золотим стандартом» симуляторів віртуальних мереж. Хоча це і безкоштовне програмне забезпечення, він пропонує багатофункціональне середовище для експериментів з великою кількістю типів мережевих пристроїв, платформ і з'єднань. Крім того, моделювання програмного забезпечення IOS Cisco показує найбільш близьку поведінку до реальних мережевих пристроїв, і його вбудований термінальний клієнт дуже схожий на реальний.

Packet Tracer - це потужний інструмент моделювання мереж, створений Cisco, за допомогою якого можна застосувати знання і навички в реальних умовах. Чудова можливість отримати практичний досвід побудови простих і складних мереж, що включають різні пристрої, а не тільки маршрутизатори і комутатори. Створення взаємопов'язаних рішень для розумних міст, будинків і підприємств.

Використання Cisco Packet Tracer як навчального середовища для навчальних курсів, дистанційного навчання, професійної підготовки, планування роботи або просто для розваги – це чудова можливість підвищити рівень своїх знань та умінь в сфері телекомунікацій.

2.3.2 Переваги та недоліки GNS3

Відсутність можливості повноцінної симуляції комутаторів Cisco другого рівня - є недоліком даного програмного забезпечення. У такому випадку застосовують вже відомий симулятор CPT для виконання лабораторних робіт з використанням комутаторів другого рівня.

До складу GNS3 не входять образи junos/Ios/pix/asa/ips, оскільки вони є частиною комерційних продуктів відповідних компаній та не мають жодного прямого відношення до проекту GNS3. Але це не є проблемою , так як знайти потрібний образ вже не складає труднощів.

Ще один важливий недолік - дуже високі вимоги до системних ресурсів. Однак це не проблема GNS3, а проблема пристроїв, що запускаються в ньому та потребують дуже багато ресурсів. GNS3 на відміну від Cisco Packet Tracer працює з реальними прошивками пристроїв. Наприклад, для запуску Cisco ASA потрібен 1Гб оперативної пам'яті. А якщо необхідно зібрати кластер? А якщо в схемі присутній Cisco IPS, якому потрібен ще 1Гб? А якщо в топологію необхідно додати ще пару серверів?

Тому на сьогоднішній день, мінімальні системні вимоги для GNS3 це 4Гб оперативної пам'яті. Але краще мати 8Гб, якщо ви плануєте збирати схеми корпоративних мереж.

Не зважаючи на недоліки, однією з найцікавіших особливостей GNS3 є можливість з'єднання топології мережі, що проектується з реальною мережею. Це надає унікальну можливість перевірити на практиці будь-який проект, без використання "живого" устаткування. А застосування Wireshark створює можливість провести моніторинг трафіку усередині топології мережі, що проектується.

До загальних переваг даного продукту відносять:

- Можливість створення складних топологій мережі високої якості
- Емуляція багатьох Cisco IOS маршрутизаторів (IPS, PIX та ASA брендмауери, JUNOS)
- Моделювання Ethernet, ATM та Frame Relay перемикачів
- Підключення модельованої мережі в реальну мережу.
- Захват пакетів з допомогою утиліти Wiresherk

До недоліків GNS3 слід віднести

- Сильне навантаження на CPU комп'ютера (близько 10 маршрутизаторів на 1 середній ПК)

- Слабка робота з L2 мережами (можна доповнити іншим ПЗ - VDE)

- Головним недоліком GNS3 є факт необхідності створювати свої власні програмні образи мережевих пристроїв для емуляції. Це не вина GNS3. Інтегрування образів програмного забезпечення Cisco IOS в GNS3 було б незаконним. Наявність цих образів є важливим фактором, і це необхідно враховувати перед розгортанням GNS3 для особистого або комерційного використання.

GNS3 має співтовариство розробників і користувачів, головна перевага якого - позитивний зворотний зв'язок, створеної групою однодумців, які хочуть допомогти іншим вчитися, працювати.

Емулятор має хорошу документацію з ілюстраціями для початківців користувачів або при необхідності керівництва по розширеній конфігурації.

За своєю суттю GNS3 - це емулятор муршрутизатора, тому йому для повноцінної роботи (розрахунку/ моделювання мережі) потрібні образи комутаторів (IOS). В свою чергу образи IOS можна скачати з сайту Cisco (для зареєстрованих користувачів і акаунтів з необхідними правами). Після налаштування програми і створення лабораторної мережі ПК з GNS можна підключати до реальної мережі.

Якщо Cisco Packet Tracer є «золотим стандартом» в симуляторах віртуальних мереж, то GNS3 - в емуляторах віртуальних мереж. Спільнота GNS3 з відкритим вихідним кодом створила багатофункціональне, добре документоване програмне забезпечення, яке є повністю безкоштовним. Незважаючи на виконання традицій моделі серверного/клієнтського додатку, серверний компонент простий в розгортанні, налаштуванні і обслуговуванні.

2.3.3 Вибір засобів моделювання для дослідження технології перерозподілу маршрутної інформації у корпоративній IP-мережі

Для вибору правильного засобу моделювання проведено порівняльний аналіз двох програм.

Обидві прорграми підтримують технологію перерозподілу маршрутної інформації, але в ході аналізу обрано емулятор GNS-3, не зважаючи на його велику потребу в ресурсах системи, він має більший функціонал, ніж у CPT, підтримуючи більше протоколів перерозподілу маршртуної інформації.

2.4 Висновки до розділу 2

- Проведено аналіз програми Cisco Packet Tracer;
- Проведено аналіз програми Graphical Network Simulator-3;
- Після порівняльного аналізу двох програм, обрано Graphical Network Simulator-3 в якості програми для подальшого виконання роботи, в зв'язку з більш потужною функціональною базою.

3 РОЗРОБКА ЛАБОРАТОРНОЇ РОБОТИ З ДИСЦИПЛІНИ ТЕХНОЛОГІЇ ТА ЗАСОБИ МІЖМЕРЕЖЕВОЇ ВЗАЄМОДІЇ "ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ ПЕРЕРОЗПОДІЛУ МАРШРУТІВ НА БАЗІ МАРШРУТИЗАТОРІВ CISCO"

3.1 Короткі теоретичні відомості

3.1.1 Початкові поняття

Застосування протоколу маршрутизації для оголошення маршрутів, що визначаються іншими способами (наприклад, іншим протоколом маршрутизації, статичними маршрутами або маршрутами з прямим підключенням), називається перерозподілом. Хоча у всій об'єднаній IP-мережі бажано використовувати єдиний протокол маршрутизації, з ряду причин часто використовується багатопротокольна маршрутизація: наприклад, при злитті компаній, у випадку, якщо декількома підрозділами управляють кілька мережевих адміністраторів, або в середовищах, де використовуються компоненти від різних постачальників. При проектуванні мережі часто використовуються різні протоколи маршрутизації. У будь-якому випадку, наявність середовища з кількома протоколами робить передбачає перерозподіл маршрутів.

Редистрибуція, перерозподіл маршрутів (route redistribution) - передача маршрутів, вивчених за допомогою одного протоколу маршрутизації, в інший протокол маршрутизації. Крім того, статичні маршрути або безпосередньо приєднані мережі, також можуть бути перерозподілені і, після цього, будуть передаватися за допомогою відповідного протоколу маршрутизації.

Перерозподіл маршрутів можливо тільки між протоколами, які підтримують один і той же стек протоколів.

Маршрутизатор, на якому виконується редистрибуція називається граничним. На цьому маршрутизаторі повинні бути налаштовані два протоколи маршрутизації.

Для того щоб перерозподілити маршрути з одного джерела в інший, повинна бути як мінімум одна точка де вони перерозподіляються. Тобто, має бути маршрутизатор, який це виконує. Наприклад, якщо перерозподіляються маршрути протоколу OSPF в маршрути EIGRP, то на такому маршрутизаторі повинні бути налаштовані обидва протоколи, а потім правила перерозподілу маршрутів з одного протоколу в інший.

Якщо налаштовано перерозподіл маршрутів з певного протоколу маршрутизації, то маршрутизатор перерозподілить:

- маршрути в таблиці маршрутизації, які були вивчені по цьому протоколу;

- всі connected маршрути, які вказані в команді network цього протоколу.

Для різних протоколів перерозподіл маршрутів налаштовується по-різному. Наприклад, для одних протоколів зазначення метрики маршруту обов'язкове, а для інших немає.

3.1.2 Метрика

При перерозподілі одного протоколу в інший слід пам'ятати, що метрики кожного протоколу відіграють важливу роль у перерозподілі. Кожен протокол використовує різні метрики. Наприклад, метрика протоколу RIP заснована на кількості переходів, однак протоколи IGRP і EIGRP використовують складову метрику залежно від пропускної здатності, затримки, надійності, завантаження і максимального розміру переданого блоку даних (MTU), де пропускна здатність і затримка є єдиними параметрами, використовуваними за замовчуванням. У процесі перерозподілу маршрутів необхідно визначити метрику, зрозумілу приймаючому протоколу. Є два методи визначення метрик при перерозподілі маршрутів:

- визначити метрику тільки для конкретного перерозподілу;

- використовувати одну і ту ж метрику за замовчуванням для всього перерозподілу (використання команди default-metric спрощує завдання, тому що в цьому випадку не потрібно визначати метрику окремо для кожного перерозподілу).

Варіанти задання початкової метрики у порядку зменшення пріоритету (якщо метрика вказана кількома методами, то буде використовуватися метрика з вищим пріоритетом):

- у route map вказати метрику командою set metric;

- задати metric в команді redistribute;

- налаштування default-metric в режимі настройки протоколу маршрутизації. Значення по замовчуванню початкової метрики для перерозподілу маршрутів в різних протоколах представлено в таблиці 3.1.

Таблиця 3.1 - Значення по замовчуванню початкової метрики

Протокол	Початкова метрика по замовчуванню
OSPF	20 для всіх крім BGP, для BGP 1
RIP	Нескінченність
EIGRP	Нескінченність
BGP	IGP metric
IS-IS	0

3.1.3 Адміністративна відстань (AD)

Якщо маршрутизатор використовує більше одного протоколу маршрутизації і визначає маршрут до одного і того ж місця призначення з допомогою обох протоколів, який з маршрутів має бути визнаний кращим? Кожен протокол використовує свій тип метрики для визначення кращого маршруту. Порівняння маршрутів з різними типами метрик неможливо. Адміністративні відстані вирішують цю проблему. Адміністративні відстані

призначаються джерелам маршрутів, з тим щоб маршрут від найбільш переважного джерела був обраний в якості кращого.

Адміністративні відстані допомагають вибрати маршрут серед різних протоколів маршрутизації, але можуть призвести до проблемам при перерозподілі. Серед цих проблем можуть бути петлі маршрутизації, проблеми збіжності і неефективна маршрутизація. Значення адміністративної відстані для різних джерел інформації про маршрути представлена в таблиці 3.2.

Таблиця 3.2 – Значення AD для різних джерел інформації про маршрути

Протокол	Значення	Протокол	Значення
Connecred interface	0	OSPF	110
Статичний маршрут	1	IS-IS	115
Статичний маршрут EIGRP	5	RIP	120
External BGP	20	ODR	160
EIGRP	90	External EIGRP	170
IGRP	100	Internal BGP	200

3.2 Перерозподіл маршрутів

3.2.1 Налагодження редистрибуції (перерозподілу) маршрутів

Команда, виконання якої необхідно для мінімального налагодження фунціонування перерозподілу маршрутів, є команда "redistribute". По замовчування перерозподіл відключений. Для відключення процесу перерозподілу маршрутів використовується команда "no redistribute протокол".

Дана команда дозволяє перерозподіляти маршрути з одного протоколу маршрутизації на другий, а також перерозподіл статичних маршрутів на протокол маршрутизації.

Синтаксис команди redistribute:

redistribute {протокол | static} [metric значення] [metric-type тип] [match] <route-type> [route-map карта] [weight вага] [subnets]

- protocol – протокол, маршрути якого перерозподіляються. Якщо для протоколу потребується вказати ідентифікатор процесу або автономной системи, то необхідно вказати дані параметри. Допустимі значення: bgp, igrp, eigrp, isis, ospf, rip. Також можливий перерозподіл статичних маршрутів.

- metric значення – необов'язковий аргумент. Це ключове слово задає значення метрики для перерозподіленого маршрута. Метрику по замовчуванню необхідно визначати для більшинства варіантів перерозподілу. Виключенням із даного правила являються статичні маршрути та перерозподіл маршрутів з протокола IGRP на протокол EIGRP.

- metric-type тип - необов'язковий аргумент. Дане ключове слово відноситься тільки до протоколів OSPF та IS-IS. У випадку протоколу OSPF воно дозволяє визначити два значення типу метрики: 1 (внутрішній маршрут типу 1) і 2 (внутрішній маршрут типу 2). Тип по замовчуванню для OSPF – це тип 2. У випадку IS-IS можливі варіанти: internal (значення метрики менше 63) і external (значення метрики більше 63, але менше 128). Тип метрики по замовчуванню для IS-IS – internal.

- match <route-type> - необов'язковий аргумент. Команда для перерозподілу маршрутів OSPF в інші протоколи. Дозволяє вказати тип маршрутів OSPF, які будуть перерозподіляться: external 1, external 2, internal, nssa-external.

- route-map карта - необов'язковий аргумент. Дане ключове слово дозволяє застосовувати до маршрутів фільтр маршрутної карти перед тим, як вони будуть перерозподілені.

- weight вага - необов'язковий аргумент. Дане ключове слово призначене тільки для протоколу BGP. Воно дозволяє призначити перерозподіленому маршруту вагу протоколу BGP.

- subnets - необов’язковий аргумент. Використовується при перерозподілі маршрутів на протокол OSPF. Коли дане ключове слово присутнє, воно заставляє OSPF приймати всі маршрути підмереж. Якщо його немає, протокол OSPF перерозподіляє тільки маршрути, зоною охоплення яких не являються підмережі.

Синтаксис команди default-metric, що виконує задання початкової метрики за допомогою default-metric для всіх перерозподілених маршрутів:

R(config-router)# default-metric <metric-value>, де <metric-value> - значення метрики.

3.2.2 Перерозподіл маршрутів в RIP

Синтаксис команди:

R(config-router)# redistribute <protocol> [process-id] [match <route-type>] [metric <metric-value>] [route-map <map-tag>]

Параметри команди redistribute:

- <protocol>- протокол, маршрути якого перерозподіляються в RIP

- match <route-type>- команда для перерозподілу маршрутів OSPF в інші протоколи. Дозволяє вказати тип маршрутів OSPF, які будуть перерозподілені:

– external 1

– external 2

– internal

– nssa – external

- metric <metric-value> - метрика, яка буде використовуватися для перерозподілених маршрутів. По замовчуванню дорівнює 0, це призводить до того, що маршрут не буде перерозподіляється.

- route - map <map-tag> - вказує на карту маршруту, яка використовується для фільтрації маршрутів, які будуть перерозподілені на RIP.

3.2.3 Перерозподіл маршрутів в OSPF

Синтаксис команди:

R(config-router)# redistribute <protocol> [process-id] [metric <metric-value>] [metric-type <type-value>] [route-map <map-tag>] [subnets] [tag <tag-value>]

Параметри команди redistribute:

- <protocol> - протокол, маршрути якого перерозподіляються в OSPF

- metric <metric-value> - метрика, яка буде використовуватися для перерозподілених маршрутів. По замовчуванню дорівнює 20.

- metric-type <type-value> - дозволяє вказати в який тип маршрутів OSPF будуть перерозподілені маршрути іншого протоколу :

– 1 - external type 1

– 2 - external type 2 . Значення за замовчуванням

- route-map <map-tag> - вказує на карту маршруту, яка використовується для фільтрації маршрутів, які будуть перерозподілені в OSPF

- subnets - вказує, що маршрути розбиті на підмережі також повинні перерозподілятися. За замовчуванням такі маршрути не перерозподіляються

- tag <tag-value> - 32-бітове значення, яке приєднується до кожного зовнішнього маршруту. OSPF цей параметр не використовує, але він може використовуватися ASBR при передачі інформації між автономними системами.

3.2.4 Перерозподіл маршрутів в EIGRP

Синтаксис команди:

R(config-router)# redistribute <protocol> [process-id] [match <route-type>] [metric <metric-value>] [route-map <map-tag>]

Параметри команди redistribute:

- <protocol> - протокол, маршрути якого перерозподіляються в EIGRP

- match <route-type> - команда для перерозподілу маршрутів OSPF в інші протоколи. Дозволяє вказати тип маршрутів OSPF, які будуть перерозподілені:

– external 1

– external 2

– internal

– nssa – external

- metric <metric-value> - метрика, яка буде використовуватися для перерозподілених маршрутів. Типово дорівнює 0, це призводить до того, що маршрут не перерозподіляється. Виняток - перерозподіл з EIGRP.

- route-map <map-tag> - вказує на карту маршруту, яка використовується для фільтрації маршрутів , які будуть перерозподілені в EIGRP.

При розподілі з одного процесу EIGRP в інший процес EIGRP, метрика маршрутів зберігається. У цьому випадку можна не задавати початкову метрику.

При розподілі з інших протоколів метрику задавати обов'язково.

3.3 Налагодження функціонування мережі з використанням перерозподілу маршрутів між протоколами

3.3.1 Налагодження мережі між протоколами RIP та OSPF

Варто звернути увагу на специфіку налагодження перерозподілу маршрутів для мережі, яка зображена на рис. 3.1. Параметри адресації цієї мережі наведені в таблиці 3.3.

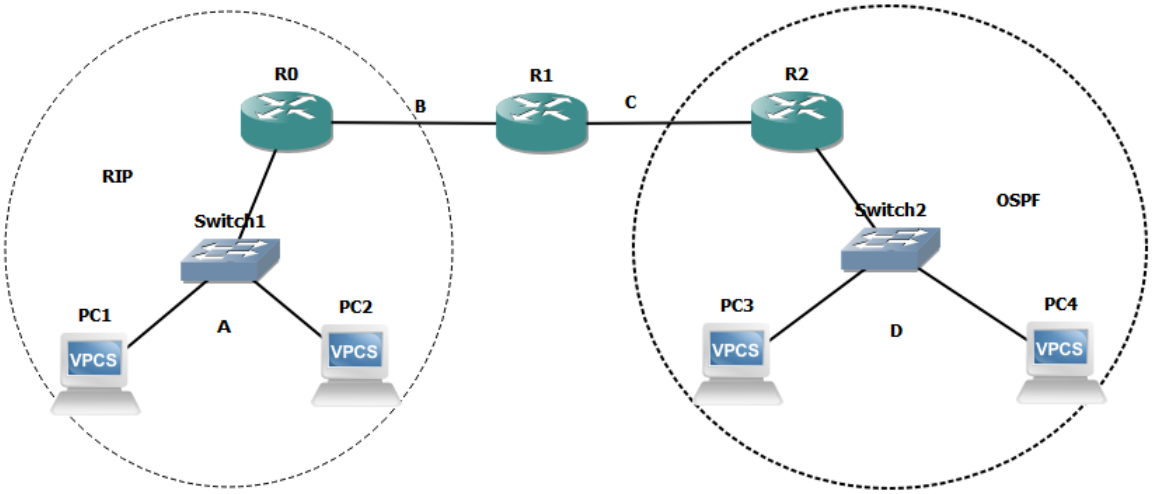

Рисунок 3.1 – Приклад мережі

Таблиця 3.3 – Параметри адресації мережі

Підмережа\Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	-	195.4.1.0	255.255.255.0	/24
Підмережа B	-	196.4.1.0	255.255.255.0	/24
Підмережа C	-	197.4.1.0	255.255.255.0	/24
Підмережа D	-	198.4.1.0	255.255.255.0	/24
Маршрутизатор R0	Інтерфейс f0/0	196.4.1.1	255.255.255.0	/24
	Інтерфейс f1/0	195.4.1.1	255.255.255.0	/24
Маршрутизатор R1	Інтерфейс f0/0	196.4.1.2	255.255.255.0	/24
	Інтерфейс f1/0	197.4.1.1	255.255.255.0	/24
Маршрутизатор R2	Інтерфейс f0/0	197.4.1.2	255.255.255.0	/24
	Інтерфейс f1/0	198.4.1.1	255.255.255.0	/24
Робоча станція PC1	Мережний адаптер	195.4.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	195.4.1.1	-	-
Робоча станція PC2	Мережний адаптер	195.4.1.3	255.255.255.0	/24
	Шлюз за замовчуванням	195.4.1.1	-	-
Робоча станція PC3	Мережний адаптер	198.4.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	198.4.1.1	-	-
Робоча станція PC4	Мережний адаптер	198.4.1.3	255.255.255.0	/24
	Шлюз за замовчуванням	198.4.1.1	-	-

Команди, які використовуються на маршрутизаторах для налагодження адресації:

```
Router>enable
Router#configure terminal
Router(config)#hostname R0
R0(config)#interface f0/0
R0(config-if)#ip address 196.4.1.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#exit
R0(config)# interface f1/0
R0(config-if)#ip address 195.4.1.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#exit
    . . .
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#interface f0/0
R1(config-if)#ip address 196.4.1.2 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)# interface f1/0
R1(config-if)#ip address 197.4.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
    . . .
Router>enable
Router#configure terminal
Router(config)#hostname R2
R2(config)#interface f0/0
R2(config-if)#ip address 197.4.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)# interface f1/0
R2(config-if)#ip address 198.4.1.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
```

Команди для налагодження роботи протоколу RIP та OSPF на відповідних маршрутизаторах мережі:

```
R0>enable
R0#configure terminal
R0(config)#router rip
R0(config-router)#network 195.4.1.0
R0(config-router)#network 196.4.1.0
R0(config-router)#exit
. . .
R2>enable
R2#configure terminal
R2(config)#router ospf 1
R2(config-router)#network 197.4.1.0 0.0.0.255 area 0
R2(config-router)#network 198.4.1.0 0.0.0.255 area 0
R2(config-router)#exit
```

Команди для налагодження роботи перерозподілу маршрутів на відповідному маршрутизаторі:

```
R1>enable
R1#configure terminal
R1(config)# router rip
R1(config-router)#network 196.4.1.0
R1(config-router)#network 197.4.1.0
R1(config-router)# redistribute ospf 1 metric 1 match external 1
R1(config-router)#exit

R1(config)# router ospf 1
R1(config-router)#network 196.4.1.0 0.0.0.255 area 0
R1(config-router)#network 197.4.1.0 0.0.0.255 area 0
R1(config-router)# redistribute rip metric 10 metric-type 2 subnets
R1(config-router)#exit
```

Діагностика функціонування протоколу маршрутизації RIP та OSPF на маршрутизаторі Cisco

Команди, що застосовуються для діагностики функціонування протоколу RIP на маршрутизаторі Cisco: show ip route, show ip protocols, show ip rip database, debug ip rip, undebug ip all.

Основними командами, для початкової діагностики виконання протоколу OSPF у мережі з однією областю, є команди show ip route, show ip protocols, show ip ospf, show ip ospf database, show ip ospf neighbor, debug ip ospf events, debug ip ospf packet, debug ip ospf hello. Результат команди show ip route представлено на рис. 3.2.

Команда show ip route дозволяє побачити маршрутну інформацію маршрутизатора. Літерою O позначений маршрут, який отримано за допомогою протоколу OSPF, а літерою R - маршрут, який отримано за допомогою протоколу RIP.

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    195.4.1.0/24 [120/1] via 196.4.1.1, 00:00:02, FastEthernet0/0
C    196.4.1.0/24 is directly connected, FastEthernet0/0
C    197.4.1.0/24 is directly connected, FastEthernet1/0
O    198.4.1.0/24 [110/2] via 197.4.1.2, 00:00:09, FastEthernet1/0
```

Рисунок 3.2 – Результат команди show ip route

Команда show ip rip database показує, які маршрути перерозподілені з протоколу OSPF. Результат команди представлено на рис. 3.3.

```
Router#sh ip rip database
195.4.1.0/24    auto-summary
195.4.1.0/24
    [1] via 196.4.1.1, 00:00:14, FastEthernet0/0
196.4.1.0/24    auto-summary
196.4.1.0/24    directly connected, FastEthernet0/0
197.4.1.0/24    auto-summary
197.4.1.0/24    directly connected, FastEthernet1/0
198.4.1.0/24    auto-summary
198.4.1.0/24    redistributed
    [3] via 197.4.1.2, 00:01:39, FastEthernet1/0
```

Рисунок 3.3 – Результат команди show ip rip database

3.3.2 Налагодження мережі між протоколами OSPF та EIGRP

Специфіка налагодження перерозподілу маршрутів мережі, зображеній на рис. 3.4, буде наведена нижче. Параметри адресації мережі наведені в таблиці 3.3.

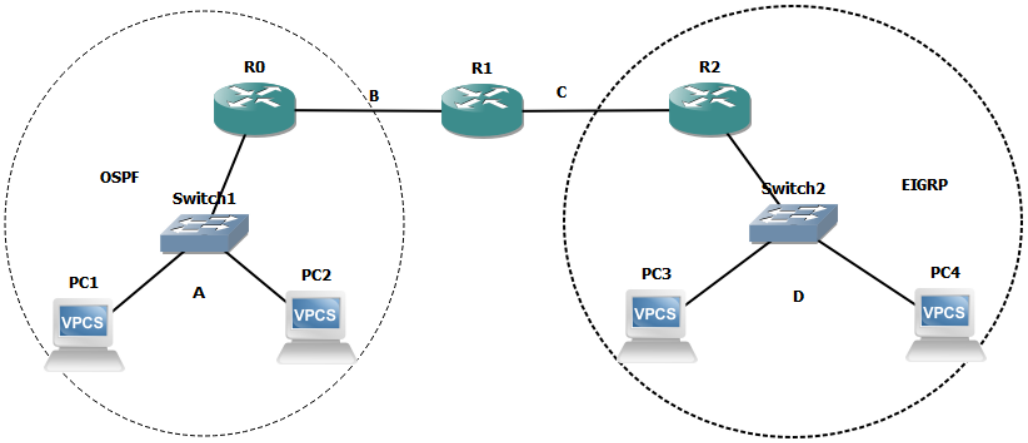

Рисунок 3.4 – Приклад мережі

Налаштування функціонування протоколів перерозподілу маршрутної інформації в мережі відбувається аналогічно минулому прикладу, з мінімальною зміною параметрів. Команди налаштування наведені вище, тому перейдемо відразу до діагностики роботи протоколів перерозподілу маршрутизації.

Діагностика функціонування протоколу маршрутизації OSPF та EIGRP на маршрутизаторі Cisco

Для діагностики роботи протоколу EIGRP на маршрутизаторі Cisco необхідно застосувати такі команди: show ip route, show ip protocols, show ip eigrp interfaces, show ip eigrp neighbors, show ip eigrp neighbor detail, show ip eigrp topology, show ip eigrp traffic, debug eigrp fsm, debug eigrp packets, undebug all.

Початкова діагностика роботи протоколу OSPF, який працює у мережі з однією областю, характеризується командами show ip route, show ip

protocols, show ip ospf, show ip ospf database, show ip ospf neighbor, debug ip ospf events, debug ip ospf packet, debug ip ospf hello.

Результат команди show ip route представлено на рис. 3.5.

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    195.4.1.0/24 [110/2] via 196.4.1.1, 00:00:48, FastEthernet0/0
C    196.4.1.0/24 is directly connected, FastEthernet0/0
     197.4.1.0/24 is variably subnetted, 2 subnets, 2 masks
D       197.4.1.0/24 is a summary, 00:01:38, Null0
C       197.4.1.0/30 is directly connected, Serial0/0
D    198.4.1.0/24 [90/20514560] via 197.4.1.2, 00:01:30, Serial0/0
```

Рисунок 3.5 – Результат роботи команди show ip route

Show ip route - команда, яка показує маршрутну інформацію маршрутизатора. Літерою O позначається маршрут, який отримано за допомогою протоколу OSPF. Маршрут, який отримано за допомогою протоколу EIGRP, позначається літерою E.

3.3.3 Приклад налагодження функціонування мережі з використанням перерозподілу маршрутів між протоколами RIP та EIGRP

Розглянемо специфіку налагодження перерозподілу маршрутів для мережі, яка зображена на рис. 3.6. Параметри адресації мережі наведені у таблиці 3.3. Команди, які виконуються на маршрутизаторах для налагодження адресації, команди для налагодження роботи протоколів на відповідних маршрутизаторах мережі та команди діагностики роботи протоколів маршрутизації наведені вище.

Команди для налагодження роботи перерозподілу маршрутів на відповідному маршрутизаторі:

R1>enable

```
R1#configure terminal
R1(config)# router rip
R1(config-router)#network 196.4.1.0
R1(config-router)#network 197.4.1.0
R1(config-router)# redistribute eigrp 1 metric 1
R1(config-router)#exit
```

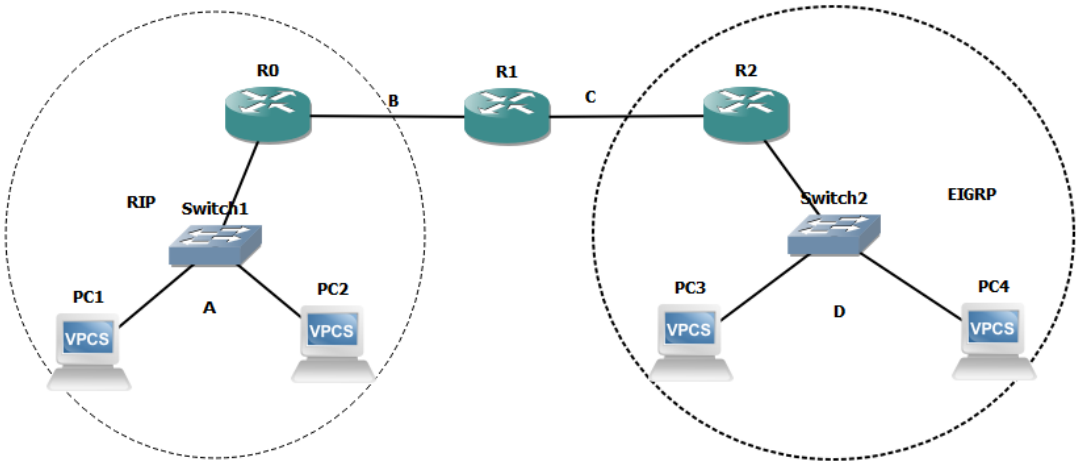

Рисунок 3.6 – Приклад мережі

```
R1(config)# router eigrp 1
R1(config-router)#network 196.4.1.0
R1(config-router)#network 197.4.1.0
R1(config-router)# redistribute rip metric 19 100 255 255 296
R1(config-router)#exit
```

3.3.4 Приклад налагодження функціонування мережі з використанням перерозподілу маршрутів між протоколу EIGRP та статичної маршрутизації

Розглянемо специфіку налагодження перерозподілу маршрутів для мережі, яка зображена на рис. 3.7. Параметри адресації мережі наведені у таблиці 3.3.

Команди для налагодження наведені вище, послідовність дій аналогічна попереднім налаштуванням.

Діагностика роботи протоколу маршрутизації EIGRP та статичної маршрутизації на маршрутизаторі Cisco

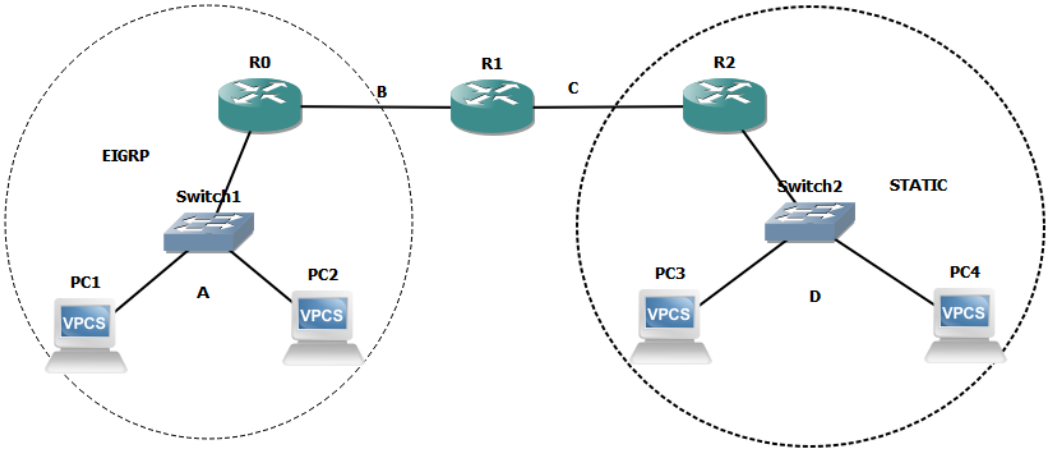

Рисунок 3.7 – Приклад мережі

Для діагностики роботи протоколу EIGRP на маршрутизаторі Cisco застосовуються наступні команди: show ip route, show ip protocols, show ip eigrp interfaces, show ip eigrp neighbors, show ip eigrp neighbor detail, show ip eigrp topology, show ip eigrp traffic, debug eigrp fsm, debug eigrp packets, undebug all.

Основними командами, які необхідні для початкової діагностики роботи статичної маршрутизації у мережі, є команди show ip route.

Результат виконання команди show ip route на маршрутизаторах представлено на рис. 3.7.

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    195.4.1.0/24 is directly connected, FastEthernet1/0
C    196.4.1.0/24 is directly connected, FastEthernet0/0
D    197.4.1.0/24 [90/30720] via 196.4.1.2, 00:06:41, FastEthernet0/0
D EX 198.4.1.0/24 [170/2588160] via 196.4.1.2, 00:06:41, FastEthernet0/0
```

Рисунок 3.8 – Результат виконання команди show ip route

3.3.5 Приклад налагодження функціонування мережі з використанням перерозподілу маршрутів між статичної маршрутизації та протоколом маршрутизації RIP

Розглянемо специфіку налагодження перерозподілу маршрутів для мережі, яка зображена на рис. 3.7. Параметри адресації мережі наведені у таблиці 3.3. Команди, які виконуються на маршрутизаторах для налагодження адресації, команди для налагодження роботи протоколів на відповіднихмаршрутизаторах мережі та команди діагностики роботи протоколів маршрутизації наведені вище. Команди для налагодження роботи перерозподілу маршрутів на відповідному маршрутизаторі:

```
R1>enable
R1#configure terminal
R1(config)# router rip
R1(config-router)#network 196.4.1.0
R1(config-router)#network 197.4.1.0
R1(config-router)# redistribute static metric 1
R1(config-router)# exit
R1(config)#ip route 195.4.1.0 255.255.255.0 196.4.1.1
R1(config)# ip route 198.4.1.0 255.255.255.0 197.4.1.2
```

3.3.6 Приклад налагодження функціонування мережі з використанням перерозподілу маршрутів між статичної маршрутизації та протоколом маршрутизації OSPF

Розглянемо специфіку налагодження перерозподілу маршрутів для мережі, яка зображена на рис. 3.7. Параметри адресації мережі наведені у таблиці 3. Команди, які потрібно виконати на маршрутизаторах для налагодження адресації, команди для налагодження роботи протоколів на відповідних маршрутизаторах мережі та команди діагностики роботи протоколів маршрутизації наведені вище. Команди для налагодження роботи перерозподілу маршрутів на відповідному маршрутизаторі:

```
R1>enable
```

```
R1#configure terminal
R1(config)# router ospf 1
R1(config-router)#network 196.4.1.0 0.0.0.255 area 0
R1(config-router)#network 197.4.1.0 0.0.0.255 area 0
R1(config-router)# redistribute static metric 10 metric-type 1 subnets
R1(config-router)# exit
R1(config)#ip route 195.4.1.0 255.255.255.0 196.4.1.1
R1(config)# ip route 198.4.1.0 255.255.255.0 197.4.1.2
```

3.4 Створення та налаштування прототипу фрагменту мережі з підтримкою перерозподілу маршрутної інформації

1. У середовищі програмного симулятора/емулятора створено проект мережі, який представлений на рис. 3.9. Даний прототип мережі можна використовувати для виконання лабораторних робіт при вивчені протоколів перерозподілу маршрутної інформації в мережах. Використано маршрутизатори моделі 2620. Для з'єднання маршрутизаторів між собою використано дані, які приведені в таблиці 3.6. Для підключення локальних мереж використано інтерфейси Fast Ethernet.

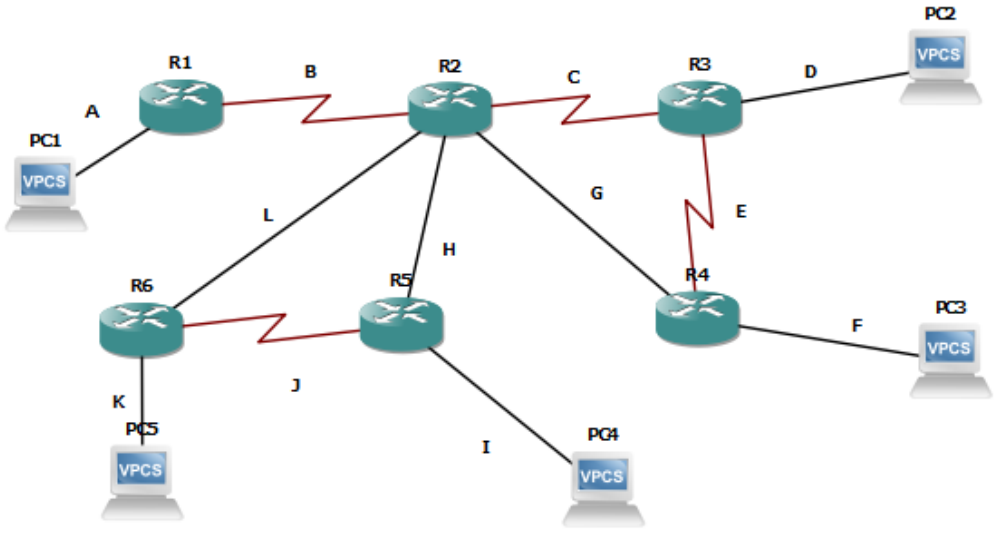

Рисунок 3.9 – Проект мережі

2. Для мережі, схема якої наведена на рисунку 3.9 з урахуванням даних таблиці 3.5, здійснити розрахунок параметрів адресації мережі та інтерфейсів пристроїв. Дані розрахунку подати у вигляді таблиці.

Таблиця 3.5 – Дані для адресації підмереж

Підмережа	IP-адреса	Підмережа	IP-адреса	Підмережа	IP-адреса	Підмережа	IP-адреса
A	195.G.N.0	D	198.G.N.0	G	201.G.N.0	J	204.G.N.0
B	196.G.N.0	E	199.G.N.0	H	202.G.N.0	K	205.G.N.0
C	197.G.N.0	F	200.G.N.0	I	203.G.N.0	L	206.G.N.0

Примітка: G двозначний номер групи, N – номер варіанта студента за списком групи.

3. Налагодити адресацію інтерфейсів робочих станцій та маршрутизаторів згідно з даними розрахунку. Під час вибору врахувати, що IP-адреса шлюзу за замовчуванням для робочої станції відповідає IP-адресі інтерфейсу маршрутизатора, до якого підключена локальна мережа. Перевірити їх доступність за допомогою команди ping для відповідних ділянок мереж.

4. Налагодити функціонування протоколу маршрутизації (з урахуванням даних таблиці 3.7) на кожному з маршрутизаторів мережі. Провести перевірку зв’язку між вузлами відповідних мереж.

5. Налагодити перерозподіл маршрутів (редистрибуцію) на відповідному маршрутизаторі мережі з урахуванням самостійного обрання параметрів редистрибуції.

6. Виконати операцію дослідження особливостей отримання службової та діагностичної інформації виконання протоколів за допомогою відповідних команд.

7. Провести перевірку зв’язку між вузлами різних мереж.

Таблиця 3.6 Данні для з’єднання маршрутизаторів між собою

№ варіанту	Канал B bandwidth	Канал C bandwidth	Канал E bandwidth	Канал G bandwidth	Канал H bandwidth	Канал J bandwidth	Канал L bandwidth
1	Serial	FE	Serial	FE	Serial	FE	Serial
	64	128	192	256	320	384	448
2	FE	Serial	FE	Serial	FE	Serial	Serial
	128	192	256	320	384	448	512
3	Serial	FE		Serial	Serial	Serial	FE
	192	256	320	384	448	512	576
4	FE	Serial	Serial	FE	Serial	FE	Serial
	256	320	384	448	512	576	640
5	Serial	Serial	FE	FE	FE	Serial	Serial
	320	384	448	512	576	640	704
6	Serial	FE	Serial	FE	Serial	Serial	FE
	384	448	512	576	640	704	768
7	Serial	FE	Serial	FE	FE	Serial	Serial
	448	512	576	640	704	768	832
8	Serial	Serial	FE	FE	Serial	FE	Serial
	512	576	640	704	768	832	896
9	FE	FE	Serial	FE	Serial	Serial	Serial
	576	640	704	768	832	896	960
10	FE	Serial	FE	Serial	Serial	Serial	FE
	640	704	768	832	896	960	1024
11	Serial	FE	Serial	Serial	Serial	FE	FE
	704	768	832	896	960	1024	1088
12	Serial	FE	FE	FE	Serial	Serial	Serial
	768	832	896	960	1024	1088	1152
13	FE	FE	FE	Serial	Serial	Serial	Serial
	832	896	960	1024	1088	1152	1216
14	FE	Serial	Serial	Serial	FE	Serial	Serial
	896	960	1024	1088	1152	1216	12
15	Serial	FE	Serial	FE	FE	Serial	Serial
	960	1024	1088	1152	1216	1280	1344
16	Serial	Serial	FE	Serial	FE	FE	FE
	1024	1088	1152	1216	1280	1344	64
17	Serial	FE	FE	Serial	FE	Serial	Serial
	1088	1152	1216	1280	1344	1408	96
18	Serial	FE	Serial	Serial	FE	FE	Serial
	1152	1216	1280	32	64	96	128
19	Serial	FE	Serial	FE	Serial	FE	Serial
	1216	1280	1344	64	96	1238	160
20	Serial	Serial	FE	Serial	Serial	FE	FE
	1280	1344	1408	96	128	160	192

Таблиця 3.7 – Протокол маршрутизації для відповідної мережі

№ варіанта	WAN 1	WAN 2	WAN 3
1	RIP	OSPF	EIGRP
2	EIGRP	OSPF	RIP
3	OSPF	RIP	EIGRP
4	RIP	EIGRP	OSPF
5	EIGRP	RIP	OSPF
6	OSPF	EIGRP	RIP
7	Static	RIP	OSPF
8	RIP	Static	OSPF
9	RIP	OSPF	Static
10	Static	OSPF	RIP
11	EIGRP	Static	RIP
12	OSPF	RIP	Static
13	RIP	EIGRP	Static
14	Static	OSPF	EIGRP
15	OSPF	Static	RIP
16	Static	RIP	EIGRP
17	EIGRP	OSPF	Static
18	OSPF	Static	EIGRP
19	Static	EIGRP	RIP
20	RIP	Static	EIGRP

3.5 Висновки до розділу 3

- Розділ розкриває застосування теоретичних знань для розвитку практичних навичок;

- Покрокова інструкція дозволяє швидко та без зайвих зусиль налаштувати обладнання для роботи мережі;

- Кожен студент отримує своє унікальне завдання, що дозволяє розвинути особисті знання і уміння.

ВИСНОВКИ

В дипломній роботі досліджено процес маршрутизації та перерозподілу маршрутної інформації в корпоративних мережах на маршрутизаторах компанії Cisco. З цього можна зробити наступні висновки:

- Детально розглянуто поняття перерозподілу маршрутної інформації;

- Для перерозподілу маршрутної інформації використовуються певні протоколи - RIP, OSPF, EIGRP;

- Проаналізовано спільну робота двох протоколів маршрутизації без перерозподілу та з перерозподілом маршрутної інформації та наведенно відповідні результати.

- Порівняно симулятор Cisco Packet Tracer з емулятором Graphical Network Simulator-3, їх характеристики, та обрано програму для подальшого виконання роботи.

- Graphical Network Simulator-3 - "золота середина" для моделювання мереж, їх аналізу та налаштування, має потужну функціональну базу і достатньо зручний в роботі, не зважаючи на його недоліки;

- Заключний розділ розкриває застосування теоретичних знань для розвитку практичних навичок - покрокова інструкція дозволяє швидко та без зайвих зусиль налаштувати обладнання для роботи мережі, а кожен студент отримує своє унікальне завдання, що дозволяє розвинути особисті знання і уміння.

- Диломна робота в повній мірі розкриває актуальність питань розглянутих на початку та засоби їх реалізації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Дибров М.В. МАРШРУТИЗАТОРЫ**:** Учебное пособие. Красноярск, 2008. 389 с.

2. Золотухин М.С., Симонова Е.С. СЕТЕВЫЕ СИМУЛЯТОРЫ И ЭМУЛЯТОРЫ ОБОРУДОВАНИЯ CISCO // Современные наукоемкие технологии. – 2020. – № 7. – С. 57-61

3. Попов С., Баутин А. Cisco Packet Tracer для всех. OmniScriptum Publishing KS., 2018. 300 с.

4. Имитированные Cisco, идентичные натуральным. [Электронный ресурс]. URL: https://habr.com/ru/post/494504.

5. Обзор эмуляторов и симуляторов оборудования Cisco. [Электронный ресурс]. URL: http://nyukers.blogspot.com/2015/05/cisco.html#axzz6OwUa1rbH.

6. RFC 1584. Moy J. / Multicast Extensions to OSPF / J. Moy. – Network Working Group, 1994. – 102 p.

7. RFC 2453. Malkin G. / RIP Version 2 / G. Malkin. – Network Working Group, 1998. – 39 p.

8. Остерлох, Х. Маршрутизация в IP сетях. Принципы, протоколы, настойка: Пер. с англ. / Хифер Остерлох – СПб.: ООО «ДиаСофтЮП», 2002. – 512 с.

9. Руденко, И. Маршрутизаторы CISCO для IP–сетей. Пер. с англ. / И. Руденко, Tsunami Computing. – М.: КУДИЦ–ОБРАЗ, 2003. – 656 с.

10. https://www.gotoadm.ru/gns-3-planirovanie-seti/

11. https://sysadmin.ru/articles/osnovy-raboty-s-cisco-packet-tracer

12. https://winitpro.ru/index.php/2019/06/05/ispolzovanie-simulyatora-setej-cisco-packet-tracer/

13. https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer

14. https://www.netacad.com/ru/courses/packet-tracer

15.https://readera.org/dostoinstva-i-nedostatki-ispolzovanija-cisco-packet-tracer-v-postroenii-140107731