Лабораторна робота № 6

Увага! Теоретичні дані по OSPF та EIGRP вчать усі стеднти!
Практично реалізують: OSPF – непарні варіанти, EIGRP – парні варіанти!

Тема: настроювання, та дослідження роботи протоколів OSPF та EIGRP.
Мета: на прикладі невеликої КМ навчитись настроювати протоколи маршрутизації OSPF та EIGRP, а також шукати та виправляти помилки в OSPF- та та EIGRP- конфігурації.

Теоретичні відомості (OSPF)

1 Загальні відомості та термінологія протоколу OSPF

Протокол OSPF (Open Shortest Path First) є протоколом маршрутизації за станом каналів, що базується на відкритих стандартах. Він описаний в декількох стандартах інженерної групи Internet (Internet Engineering Task Force – IETF), останнім з яких є стандарт RFC 2328. Термін „відкритий" в протоколі OSPF означає його доступність всім користувам .

Протокол OSPF це надійний, масштабованим та ефективний протокол, який може бути використаний в окремій зоні у невеликих КМ і в кількох зонах для великих КМ. Маршрутизація OSPF може бути розширена на великі мережі за умови, що під час проектування КМ використовувались ієрархічні принципи її побудови, які полягають у під'єднанні кількох зон до зони розподілення (нульової зони), яку також називають магістраллю. Таке проектування дозволяє здійснювати повний контроль над повідомленнями про оновлення маршрутів. Задання зон зменшує об'єм службового навантаження маршрутизації, прискорює збіжність, обмежує можливу нестабільність мережі однією зоною та підвищує продуктивність мережі.

Протокол OSPF функціонує не так як дистанційно-векторні протоколи. Маршрутизатори ідентифікують сусідні маршрутизатори та обмінюються з ними інформацією. У протокола OSPF є свій набір термінів (рис. 1.

Інформація, зібрана від сусідніх маршрутизаторів OSPF не є повною ТМ. Кожен OSPF-маршрутизатор повідомляє своїм сусідам про стан своїх зв'язків або каналів. Ця інформація розповсюджується методом лавинного розсилання. Під цим поняттям розуміється відправлення однієї та тієї ж інформації з усіх портів, за виключенням того, на який вона надійшла. Маршрутизатор OSPF оголошує стан своїх каналів та передає далі отриману ним інформацію про стани каналів інших маршрутизаторів.

Маршрутизатори в зоні 1 обробляють цю інформацію та будують свою топологічну БД, яку називають також БД стану каналів. Всі маршрутизатори в одній OSPF-зоні мають одну й ту ж БД стану каналів. Автономна система може бути розділена на ряд зон, що представляють собою групи зв'язних (неперервних) мереж і під'єднаних до них пристроїв. Маршрутизатори з кількома інтерфейсами можуть бути учасниками кількох зон – їх називають граничними маршрутизаторами зон (Area Border Routers). Вони підтримують окремі топологічні БД для кожної зони.

Після цього кожен маршрутизатор застосовує алгоритм вибору найкоротшого шляху SPF, який також називають алгоритмом Дейкстри, до своєї бази даних. Ці обчислення визначають найкращий шлях до пункту призначення. Алгоритм SPF додає вартості (оцінки) для окремих переходів, які зазвичай базуються на ширині смуги пропускання. Мінімальна оцінка маршруту додається до ТМ, що також називається таблицею пересилання.

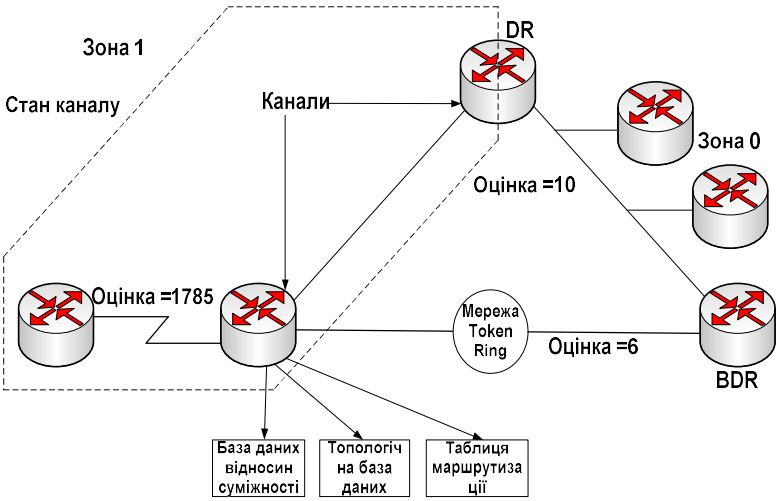


Рисунок 1 – Термінологія протокола OSPF

OSPF-маршрутизатори записують інформацію про своїх сусідів в ТСП. Для зменшення об'єму інформації, якою обмінюються сусідні пристрої в одній мережі, маршрутизатори OSPF обирають *призначений маршрутизатор (Designated Router, DR)* та *резервний призначений маршрутизатор (Backup Designated Router, BDR)*, які служать точками централізації при обміні інформацією маршрутизації.

OSPF-маршрутизатори встановлюють зв'язки або стани (states) зі своїми сусідами для ефективного сумісного використання інформації канального рівня.

2 Стани протокола OSPF

Маршрутизатори OSPF використовують п'ять різних типів пакетів для ідентифікації своїх сусідів та оновлення інформації маршрутизації канального рівня. У таблиці 1 описані типи пакетів протокола OSPF. Ці п'ять типів пакетів дозволяють протоколу OSPF здійснювати різноманітні та складні типи зв'язків.

Таблиця 1 – Типи пакетів протокола OSPF

Тип пакета протоколу OSPF	Опис
Тип 1 – Hello	Використовується для створення та підтримки таблиці сусідніх пристроїв
Тип 2 – Пакет опису бази даних (Database description packet, DBD)	Описує вміст бази даних стану каналів OSPF-маршрутизатора
Тип 3 – Запит інформації про стан каналів (link-state requests – LSR)	Здійснює запит окремих фрагментів бази даних стану каналів маршрутизатора
Тип 4 – Оновлення стану каналів (Link-state update, LSU)	Передає повідомлення про стан каналів (link-state advertisements, LSA) сусіднім маршрутизаторам
Тип 5 – Підтвердження отримання повідомлення про стан каналів (Link-state acknowledgement, LSAck)	Підтверджує отримання від сусіднього пристрою повідомлення LSA

Ключовим фактором при проектуванні OSPF-мереж та при усуненні помилок в них є розуміння зв'язків або станів, які виникають між OSPF-маршрутизаторами. Інтерфейси OSPF-маршрутизаторів можуть знаходитися в одному з наведених нижче семи станів. Зв'язки між сусідніми маршрутизаторами послідовно проходять ці стани зверху вниз:

- Вимкнений стан (Down State)
- Ініціалізація (Init State)
- Двохстороннє з'єднання (Two-way)
- ExStart
- Обмін (Exchange)
- Завантаження (Loading)
- Стан встановлення повного зв'язку між сусідніми (суміжними) пристроями (Full adjacency)

Вимкнений стан

Вимкнений стан має місце, коли обмін інформацією між сусідніми пристроями не відбувався. Маршрутизатори очікують переходу в наступний стан – стан ініціалізації

Стан ініціалізації

В стані ініціалізації OSPF-маршрутизатори регулярно (зазвичай 10 секунд) відсилають пакети першого типу (Hello) для встановлення зв'язку з сусідніми маршрутизаторами. Коли деякий інтерфейс отримує перший Hello-пакет, відповідний маршрутизатор переходить в стан ініціалізації. Це означає, що маршрутизатору відомо про наявність у нього сусіднього пристрою і він чекає переходу зв'язку з ним в наступний стан.

Існує два типи зв'язку між маршрутизаторами: двохсторонній зв'язок та стан повного зв'язку сусідніх пристроїв, хоча між цими двома станами і знаходяться декілька проміжних станів. Перед тим, як стане можливим встановлення будь-якого типу зв'язку, маршрутизатор повинен отримати від свого сусіда повідомлення Hello.

Стан двохстороннього зв'язку

Кожен OSPF-маршрутизатор намагається встановити з усіма своїми сусідами по мережі OSPF стан двохстороннього зв'язку або двонаправленого зв'язку, використовуючи для цього пакети Hello, які зокрема містять список відомих відправнику сусідніх OSPF-маршрутизаторів.

Маршрутизатор переходить в стан двохстороннього зв'язку в момент, коли бачить себе в пакеті Hello, отриманому від сусіднього пристрою. Тобто, коли перший маршрутизатор взнає, що другий маршрутизатор знає про нього, він оголошує наявність стану двохстороннього зв'язку між ними.

Стан двохстороннього зв'язку є базовим станом двох сусідніх пристроїв протоколу OSPF, однак в ньому ще не відбувається сумісне використання інформації маршрутизації. Для того, щоб дізнатись про стан каналів інших маршрутизаторів і врешті решт створити ТМ, кожен OSPF-маршрутизатор повинен утворити хоча б одне з'єднання (стан суміжності) з сусіднім пристроєм. Стан суміжності це більш тісний зв'язок між OSPF-маршрутизаторами, що включає в себе ряд послідовних станів, які базуються не лише на Hello-повідомленнях, а й інших чотирьох типах OSPF-пакетів. Маршрутизатори, які намагаються стати суміжними обмінюються інформацією ще до того, як буде повністю встановлено стан суміжності. Першим етапом встановлення стану повної суміжності є стан ExStart.

Стан ExStart

У технічному аспекті в момент коли маршрутизатор та його сусідній пристрій входять у стан ExStart, їх зв'язок характеризується як стан суміжності, однак в дійсності ці пристрої ще не є повністю суміжними. Стан ExStart встановлюється за допомогою пакетів опису бази даних (DBD). Для обговорення того, який маршрутизатор в даному з'єднанні буде головним (master), а який підлеглим (slave), маршрутизатори використовують пакети Hello, а для обміну вмістом БД використовуються пакети DBD (рис. 2).

Маршрутизатор з максимальним значенням OSPF-ідентифікатора (ID) стає головним. Коли два сусідніх маршрутизатора визначають свої ролі як головного та підлеглого, вони входять у стан обміну (Exchange) та починають надсилати один одному інформацію маршрутизації.

Стан обміну

У стані обміну сусідні маршрутизатори використовують пакети DBD для відправлення один одному своєї інформації про стан каналів, як показано на рис. 2. Іншими словами, маршрутизатори описують один одному свої БД стану каналів. При цьому маршрутизатори порівнюють отриману інформацію з тією, що міститься в їх власних БД стану каналів. Якщо будь-який з маршрутизаторів отримує інформацію про канал, яка відсутня в його БД – він запитує у сусіднього маршрутизатора повне оновлення. Повний обмін інформації відбувається в стані завантаження (Loading).

Стан завантаження

Після того, як обидва маршрутизатора описали один одному свої БД, вони можуть запитати більш повну інформацію, використовуючи пакети запиту стану каналів (LSR). Коли маршрутизатор отримує запит LSR, він відповідає відправкою оновлення маршрутизації, використовуючи пакет оновлення стану каналів (LSU). Ці LSU-пакети містять оголошення актуального стану каналів (LSA), які складають сутність протоколів маршрутизації стану каналів. Як показано на рис. 2, підтвердження отримання LSU-пакетів здійснюється за допомогою пакетів підтвердження стану каналів (LSAck).

Стан повної суміжності

Після того, як повністю реалізований стан завантаження, маршрутизатори повністю суміжні. Кожен маршрутизатор підтримує свій список суміжних сусідніх маршрутизаторів (БД суміжних пристроїв).

У табл. 2 перераховано важливі бази даних протоколу OSPF.

Таблиця 2 – Бази даних протоколу OSPF

База даних	Опис
База даних суміжних пристроїв	Список усіх сусідніх пристроїв, з якими даний маршрутизатор встановив двосторонні зв'язки.
База даних стану каналів або топологічна база даних (Link State Data Base)	Інформація про всі маршрутизатори мережі. Ця база даних відображає поточну мережеву топологію. Всі маршрутизатори однієї і тієї ж області мають ідентичні бази даних канального рівня.
База даних пересилання або таблиця маршрутизації (Routing Table)	Список маршрутів, що генерується при виконанні алгоритму над топологічною базою даних. Таблиця маршрутизації кожного маршрутизатора унікальна та містить інформацію про те, яким чином і за якими маршрутами слід направляти пакети, призначені іншим маршрутизаторам.

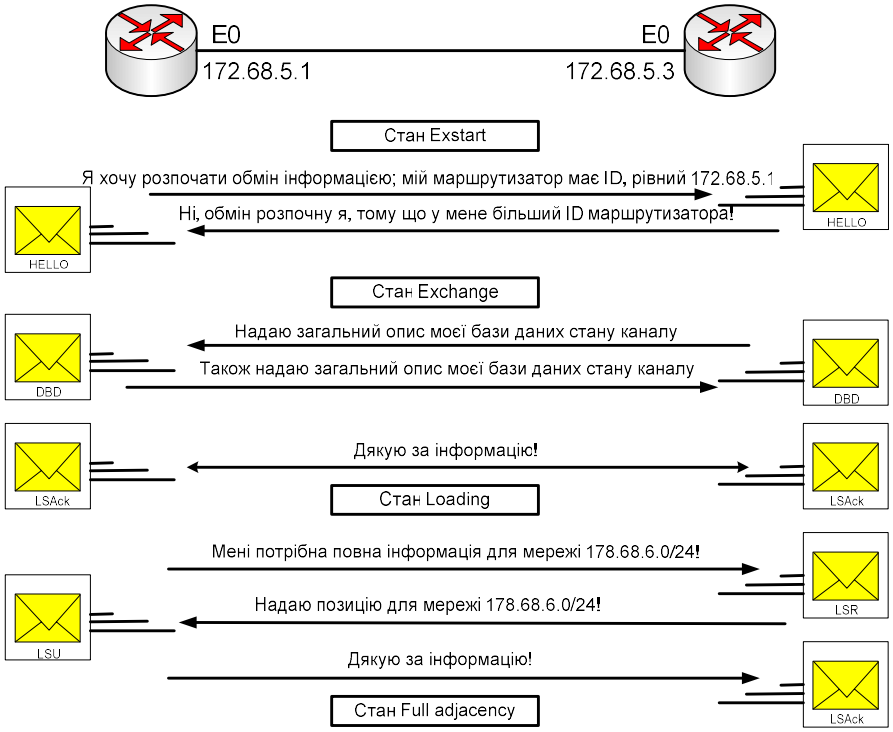


Рисунок 2 – Виявлення маршрутизатора по протоколу OSPF

3 Основи функціонування протоколу OSPF

Для визначення найкращого шляху до пункту призначення протокол OSPF використовує алгоритм вибору найкоротшого маршруту (тобто маршруту з найменшою оцінкою). Цей алгоритм було розроблено голандським комп'ютерним спеціалістом Дейкстра (Dijkstra) та опубліковано у 1959 році. В цьому алгоритмі КМ розглядається як множина вузлів, що з'єднані між собою каналами типу „точка-точка". Кожному каналу присвоюється деяке значення оцінки, а кожному вузлу – деяке ім'я. Кожен вузол має повну БД всіх каналів, тому всім вузлам відома вся інформація про фізичну топологію мережі. Після цього алгоритм вибору найкоротшого шляху обчислює вільну від петель топологію, використовуючи даний вузол як початкову точки та послідовно аналізуючи його інформацію про суміжні вузли.

Для того, щоб сумісно використовувати інформацію про маршрутизацію, OSPF-маршрутизатори повинні встановити зв'язок з сусіднам. Кожен маршрутизатор намагається встановити відношення суміжності або сусідства хоча б з одним маршрутизатором кожної IP-мережі, до якої під'єднані усі його порти. Деякі маршрутизатори можуть намагатися встановити відношення суміжності з усіма сусідніми маршрутизаторами, в той час як інші – тільки з одним або двома. OSPF-маршрутизатори визначають, з якими іншими маршрутизаторами їм слід встановити відношення суміжності, на основі типу мережі, яка їх поєднує.

Після того, як між сусідніми пристроями встановлені відношення суміжності, між ними

відбувається обмін інформацією про стан каналу. Як показано на рис. 3, і перераховано в наведеному нижче списку, інтерфейси OSPF-маршрутизаторів розпізнають три типи мереж.

- Широкомовні мережі множинного доступу.
- Неширокомовні мережі множинного доступу (nonbroadcast multi-access – NBMA).
- Мережі з каналами типу „точка-точка” .

Мережевий адміністратор може сконфігурувати на будь-якому типі інтерфейсу і четвертий тип мереж – мережа типу „точка-декілька точок”. У табл. 3 наведені типи OSPF-мереж. В мережі *множинного доступу* (*multiaccess network*) неможливо заздалегідь знати, скільки маршрутизаторів буде з’єднано. В мережах типу „*точка-точка*” (*point-to-point*) можуть бути з’єднані тільки два маршрутизатори. Якщо всі маршрутизатори встановлять відношення суміжності з усіма іншими і будуть обмінюватися інформацією про стан каналів, то об’єм службових повідомлень стане занадто великим. Як згадувалось вище проблема великого об’єму службових повідомлень, може бути вирішена вибором призначеного маршрутизатора.

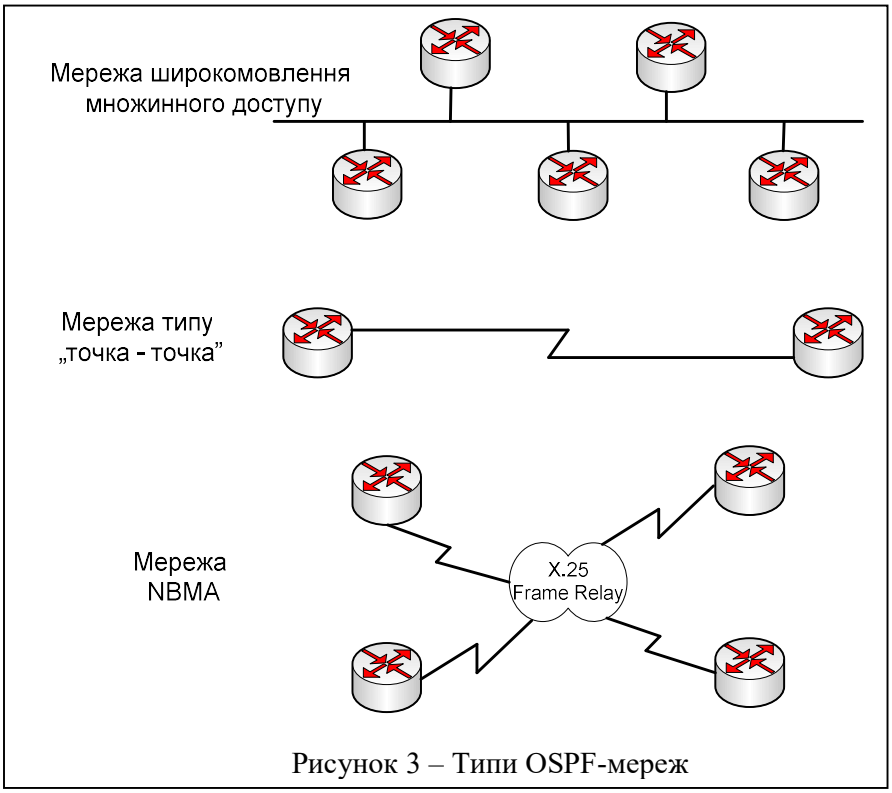


Рисунок 3 – Типи OSPF-мереж

Цей призначений маршрутизатор (DR) стає суміжним пристроєм для всіх маршрутизаторів широкомовного сегмента. Всі інші маршрутизатори цього сегмента надсилають інформацію про стан каналу до DR, який стає джерелом інформації для даного сегмента і розсилає інформацію про стан каналів всім іншим маршрутизаторам сегмента, використовуючи адресу багатоадресного розсилання 224.0.0.5 для всіх OSPF-маршрутизаторів. Незважаючи на підвищення ефективності роботи КМ, яке забезпечується використанням DR, в даному підході є й недолік – призначений маршрутизатор представляє собою точку, від якої залежить робота всього сегмента і у випадку виходу його з ладу весь сегмент припиняє працювати. Тому вибирається також резервний призначений маршрутизатор (BDR), який приймає на себе виконання функцій призначеного маршрутизатора у випадку відмови останнього. На рис. 4 наведено маршрутизатори DR та BDR, що отримують повідомлення LSA. Для того, щоб обоє маршрутизатори DR та BDR отримували всі повідомлення про стан каналу, які надсилаються в сегмент, використовується адреса багатоадресого розсилання 224.0.0.6.

Таблиця 3 – Типи мереж OSPF

Тип мережі	Характеристики, що визначаються	Чи є вибір DR-маршрутизатора?
Широкомовний множинний доступ	Ethernet, Token Ring, FDDI	Так
Неширокомовний множинний доступ	Frame Relay, X.25, SMDS	Так
„Точка-точка”	PPP, HDLC	Ні
„Точка-декілька точок”	Конфігурується мережевим адміністратором	Ні

Зазначимо, що маршрутизатор стає DR, якщо він має найвищий (найбільший) пріоритет інтерфейса (OSPF interface priority), маршрутизатор з другим за величиною пріоритетом стає BDR. Якщо значення цих пріоритетів однакові (а за замовчанням вони однакові і дорівнюють одиниці) – то до уваги береться ідентифікатора маршрутизатора (Router ID). Маршрутизотор з найбільшим значенням ID стає DR, а з другим за величиною пріоритетом – BDR. Ідентифікатором маршрутизатора стає найбільша IP-адреса Loopback-інтерфейса, або, якщо Loopback-інтерфейс не налаштований – найбільша IP-адреса потра маршрутизатора.

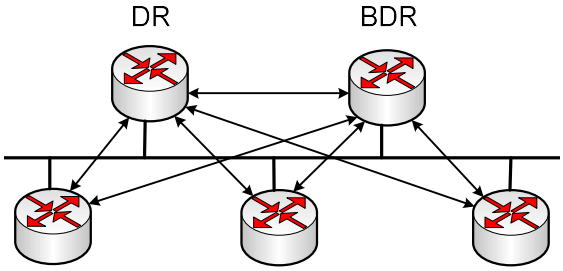


Рисунок 4 – Маршрутизатори DR та BDR отримують повідомлення LSA

У мережах типу „точка-точка” існує лише два вузла і тому маршрутизатори DR та BDR не обираються. Обидва маршрутизатори з’єднання „точка-точка” є повністю суміжними пристроями.

Для визначення кращого маршруту протокол OSPF використовує оцінку як метрику, яка обчислюється за виразом:

$$10^8/(\text{ширина смуги пропускання інтерфейсу}).$$

Для того, щоб протокол OSPF правильно обчислював характеристики маршрутів, необхідно, щоб усі інтерфейси, під’єднані до будь-якого каналу, домовились про його оцінку. Ця оцінка може бути змінена для того, щоб здійснити вплив на результат обчислення протоколом OSPF його оцінки. Найбільш типовою ситуацією, в якій потрібно змінювати оцінку, є використання маршрутизаторів від різних виробників. Це пов’язано з тим, що оцінки каналу, зроблені різними пристроями, можуть бути різними.

У таблиці 4 наведені стандартні оцінки каналів. Зазначимо, що, у випадку, коли маршрут до пункта призначення проходить через кілька сегментів – оцінка маршрута дорівнюватиме сумі оцінок цих сегментів.

Таблиця 4 – Деякі стандартні оцінки протоколу OSPF

Середовище передавання	Оцінка
Послідовний канал 56 Кбіт/с	1785
Послідовний канал 64 Кбіт/с	1562
T1 (Послідовний канал 1,544 Мбіт/с)	64
E1 (Послідовний канал 2,048 Мбіт/с)	48
Мережа Ethernet 10 Мбіт/с	10
Мережа Token Ring 16 Мбіт/с	6
100 Mbps Fast Ethernet, FDDI	1

4 Конфігурування протоколу OSPF

Для того, щоб увійти в режим настроювання протоколу OSPF слід ввести команду:

`Router(Config)# router ospf process-id`,

де `process-id` – номер у діапазоні 1 – 65535, який має локальне значення і на відміну відміну від EIGRP, не повинен збігатися на всіх маршрутизаторах мережі, в якій настроюється протокол OSPF. При цьому маршрутизатори мережі будуть бачити один одного і обмінюватись OSPF-анонсами.

Далі на кожному маршрутизаторі слід виконати команду

`Router(config-router)#network net-addr wildcard-mask area a-id`,

де `net-addr` – IP-адреса мережі або підмережі, яка безпосередньо під’єднана до даного маршрутизатора (в кожній команді `network` вказується по одній такій мережі); `wildcard-mask` – шаблонна маска (на відміну від протоколу EIGRP є обов’язковою), яка в даному випадку вказує на ті розряди IP-адреси, які слід порівняти з шаблоном (шаблонна маска може бути отримана шляхом інвертування двійкових розрядів звичайної маски підмережі); `a-id` – ідентифікатор зони OSPF, в цій зоні всі OSPF-маршрутизатори обмінюються інформацією між собою і володіють однаковою базою даних link-state databases. Всі маршрутизаторі в одній зоні повинні мати однакове значення

a-id. Хоча це значення може бути довільне, прийнято використовувати 0, якщо є лише одна зона OSPF. В подальшому, при додаванні нових зон нульова зона є магістральною (backbone area).

Дана команда виконує такі функції:

- всі інтерфейси маршрутизатора які мають адреси, що належать мережам вказаним командами network беруть участь у надсиланні та отриманні OSPF-анонсів;
- ці мережі (підмережі) будуть включені в OSPF-анонси.

Так, наприклад, для мережі, наведеної на рис. 5, для маршрутизатора R1 команди настроювання протоколу OSPF будуть

```
R1(config)#router ospf 1
R1(config-router)# network 172.16.1.16 0.0.0.15 area 0
R1(config-router)# network 192.168.10.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0;
```

для маршрутизатора R2

```
R2(config)#router ospf 1
R2(config-router)# network 10.10.10.0 0.0.0.255 area 0
R2(config-router)# network 192.168.10.0 0.0.0.3 area 0
R2(config-router)# network 192.168.10.8 0.0.0.3 area 0;
```

для маршрутизатора R3

```
R3(config)#router ospf 1
R3(config-router)# network 172.16.1.32 0.0.0.7 area 0
R3(config-router)# network 192.168.10.4 0.0.0.3 area 0
R3(config-router)# network 192.168.10.8 0.0.0.3 area 0.
```

Після виконання цих команд ТМ будуть:

для маршрутизатора R1

```
   10.0.0.0/24 is subnetted, 1 subnets
O 10.10.10.0 [110/65] via 192.168.10.2, 00:00:37, Serial0/0/0
  172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.16/28 is directly connected, FastEthernet0/0
O 172.16.1.32/29 [110/65] via 192.168.10.6, 00:01:58, Serial0/0/1
   192.168.10.0/30 is subnetted, 3 subnets
C 192.168.10.0 is directly connected, Serial0/0/0
C 192.168.10.4 is directly connected, Serial0/0/1
O 192.168.10.8 [110/128] via 192.168.10.6, 00:02:52, Serial0/0/1
               [110/128] via 192.168.10.2, 00:00:13, Serial0/0/0
```

для маршрутизатора R2

```
   10.0.0.0/24 is subnetted, 1 subnets
C 10.10.10.0 is directly connected, FastEthernet0/0
  172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O 172.16.1.16/28 [110/65] via 192.168.10.1, 00:01:28, Serial0/0/0
O 172.16.1.32/29 [110/65] via 192.168.10.10, 00:00:54, Serial0/0/1
   192.168.10.0/30 is subnetted, 3 subnets
C 192.168.10.0 is directly connected, Serial0/0/0
O 192.168.10.4 [110/128] via 192.168.10.1, 00:01:28, Serial0/0/0
               [110/128] via 192.168.10.10, 00:00:54, Serial0/0/1
C 192.168.10.8 is directly connected, Serial0/0/1
```

для маршрутизатора R3

```
   10.0.0.0/24 is subnetted, 1 subnets
O 10.10.10.0 [110/65] via 192.168.10.9, 00:01:20, Serial0/0/1
  172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O 172.16.1.16/28 [110/65] via 192.168.10.5, 00:04:07, Serial0/0/0
C 172.16.1.32/29 is directly connected, FastEthernet0/0
   192.168.10.0/30 is subnetted, 3 subnets
O 192.168.10.0 [110/128] via 192.168.10.5, 00:04:07, Serial0/0/0
               [110/128] via 192.168.10.9, 00:01:20, Serial0/0/1
C 192.168.10.4 is directly connected, Serial0/0/0
```

```
C 192.168.10.8 is directly connected, Serial0/0/1
```

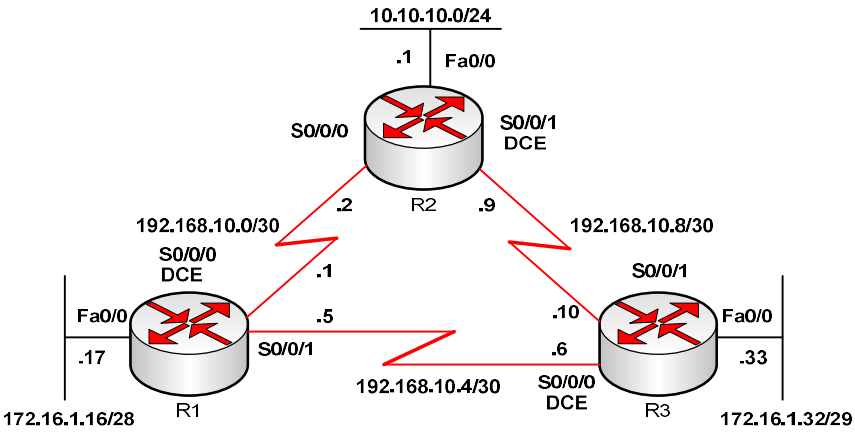


Рисунок 5 – Структура мережі для настроювання протоколу OSPF

Літерами "O" в ТМ починаються маршрути отримані за протоколом OSPF. Розглянемо, наприклад, перший рядок ТМ маршрутизатора R1

```
O 10.10.10.0 [110/65] via 192.168.10.2, 00:00:37, Serial0/0/0.
```

Отже, тут 10.10.10.0 – адреса мережі призначення; [110/65] – адміністративна відстань протоколу OSPF і через слеш – метрика маршута; адреса порта наступного транзитного вузла на шляху до мережі призначення, 00:00:37 – час існування даного маршруту; Serial0/0/0 – локальний інтерфейс, через який слід надсилати пакети до мережі призначення.

Останній запис маршруту ТМ маршрутизатора R1 має вигляд

```
O 192.168.10.8 [110/128] via 192.168.10.6, 00:02:52, Serial0/0/1
               [110/128] via 192.168.10.2, 00:00:13, Serial0/0/0
```

Це означає, що до мережі `192.168.10.8` є два еквівалентні маршрути з метрикою 128, через потри маршрутизаторів R3 та R2 відповідно.

Обчислення метрики

Як зазначалось вище, метрика маршрута у протоколі OSPF обчислюється як сумарна оцінка каналів цього маршрута від джерела до пункта призначення. Так, наприклад, метрика маршрута від маршрутизатора R1 до мережі 10.10.10.0 буде 64+1=65, де 64 – оцінка каналу між R1 та R2 з пропускною спроможністю 1,544 Мбіт/с (див. табл. 4), а 1 – оцінка каналу від R2 до мережі 10.10.10.0/24. Аналогічно, метрика маршрута від маршрутизатора R1 до мережі 192.168.10.8 буде 64+64=128.

Подивитись пропускну спроможність інтерфейсу маршрутизатора можна за допомогою команди `show interfaces int num` (де – ім'я та номер інтерфейса відповідно).

Нижче наведено результати виконання цієї команди для деяких інтерфейсів маршрутизаторів R1 та R2 (на прикладах виведено лише один рядок, який містить інформацію стосовно пропускної спроможності – Bw).

```
R1#show interfaces serial 0/0/0
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
R2#show interfaces serial 0/0/0
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
R2#show interfaces fastEthernet 0/0
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
R2#show interfaces serial 0/0/1
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec.
```

Слід звернути увагу на те, що під час конфігурування OSPF не слід покладатись на значення смуги пропускання послідовних каналів за замовчанням, оскільки ці значення можуть не відповідати тим, що потрібні і бути не тими, що ви передбачаєте. Для задання потрібного значення

смуги пропускання слід скористатись командою

```
Router(config-if)#bandwidth bandwidth-kbps.
```

Можна також скористатись командою `ip ospf cost cost_value` (де cost_value – оцінка маршрута) і задати вже саму оцінку канала маршрута. Наприклад, команда `R1(config-if)#ip ospf cost 1562` еквівалетна команді `R1(config-if)#bandwidth 64`, за виключенням того, що в першому випадку обчислення вартості виконавти не слід.

Анонсування маршруту за замовчанням та статичного маршруту

Аналогічно протоколу RIP, для анонсування маршрута за замовчанням OSPF потребує задання команди `default-information originate` в режимі конфігурування протоколу OSPF. Такий анонсований маршрут в ТМ інших OSPF-маршрутизаторів буде починатись з сиволів O*E2 (або O*E1).

Настроїмо на маршрутизаторі R1 Loopback 1 з IP-адресою 172.30.1.1, задамо маршрут за замовчанням до цього інтерфейсу та вкажимо маршрутизатору на анонсування цього маршрута:

```
R1(config)#interface loopback 1
R1(config-if)#ip add 172.30.1.1 255.255.255.252
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 1
R1(config)#router ospf 1
R1(config-router)#default-information originate
```

Тепер маршрут за замовчанням анонсуватиметься до маршрутизаторів R2, R3. В ТМ маршрутизатора R1 з'явиться запис

```
S* 0.0.0.0/0 is directly connected, Loopback1,
```

а в ТМ маршрутизатора R3 –

```
O*E2 0.0.0.0/0 [110/1] via 192.168.10.5, 00:00:20, Serial0/0/0
```

Анонсування статичних маршрутів можна задати за допомогою команди `redistribute static` в режимі конфігурування протоколу OSPF.

Конфігурування аутентифікації в протоколі OSPF

Рівень безпеки мережі підвищується, якщо відомо, що маршрутна інформація поступила з конкретного джерела. Протокол OSPF дозволяє маршрутизаторам виконувати взаємну аутентифікацію. За замовчанням маршрутизатор покладається на те, що:

- інформація про маршрути поступає від того маршрутизатора, який повинен її надсилати;
- в процесі передачі ця інформація не була спотворена.

Для гарантування цього, на маршрутизаторах однієї зони може бути сконфігурована взаємна аутентифікація.

Аутентифікація є іншим типом конфігурування окремих інтерфейсів. Кожному OSPF-інтерфейсу маршрутизатора може бути заданий відмінний від інших ключ аутентифікації, який виконує функції пароля для маршрутизаторів OSPF однієї і тієї ж зони. Для конфігурування OSPF-аутентифікації використовується команда

```
Router(config-if)#ip ospf authentication-key password.
```

Після конфігурування паролю, в зоні можна увімкнути функцію аутентифікації за допомогою команди

```
Router(config-router)#area num authentication [message-digest],
```

яка повинна бути виконана на всіх маршрутизаторах, що беруть участь в аутентифікації. Хоча ключове слово message-digest необов'язкове, рекомендується завжди використовувати його в даній команді, оскільки за замовчанням паролі аутентифікації пересилаються відкритим текстом. При використанні ключового слова message-digest замість пароля пересилається дайджест повідомлення (хеш пароля). Якщо у одержувача сконфігуровано відповідний ключ аутентифікації, то потенційний зловмисник не зможе зрозуміти смисл цього дайджеста.

Якщо вибрана аутентифікація з використанням дайджеста повідомлення, то ключ аутентифікації не використовується. Натомість на інтерфейсі OSPF-маршрутизатора повинен бути сконфігурований ключ дайджеста повідомлення за допомогою команди

```
Router(config-if)#ip ospf message-digest-key key-id
                  md5 [encryption-type] password
```

Аутентифікація MD5 створює дайджест повідомлення, який є кодованими даними, створеними на базі пароля і вмісту пакету. Маршрутизатор-одержувач використовує для відновлення дайджеста спільно використовуваний пароль і цей пакет. Якщо дайджести збігаються – маршрутизатор вважає, що джерелу пакету можна довіряти і вміст пакету не був спотворений (підроблений) в процесі передачі.

Конфігурування таймерів протоколу OSPF

В деяких випадках необхідно прискорення сповіщення маршрутизаторів мережі про збої в роботі каналів. У протоколі OSPF з цією метою використовуються таймери.

Нагадаємо, що для того, щоб OSPF-маршрутизатори могли обмінюватися інформацією, вони повинні мати однакові інтервали розсилання повідомлень Hello і критичні інтервали. За замовчанням критичний інтервал має значення в чотири рази більше, ніж інтервал розсилання повідомлень Hello. Це означає, що маршрутизатор має можливість чотири рази надіслати повідомлення Hello до того, як він буде оголошений непрацездатним. У широкомовних мережах OSPF за замовчанням інтервал повідомлень Hello дорівнює 10 секунд, а інтервал критичних повідомлень – 40 секунд. У нешироковомовних мережах OSPF ці інтервали дорівнюють 30 і 120 секунд відповідно. Ці стандартні значення забезпечують ефективне функціонування протоколу OSPF, тому їх не рекомендується змінювати. Мережевий адміністратор може змінити ці значення, проте для цього слід мати достатні підстави вважати, що таке зміна підвищить ефективність роботи мережі. При конфігурування таймерів необхідно стежити, щоб у всіх маршрутизаторів ці значення збігались. При конфігурації на інтерфейсі інтервалів Hello і критичного використовуються команди:

```
Router(config-if)# ip ospf hello-interval seconds,
Router(config-if)# ip ospf dead-interval seconds.
```

Конфігурування пріоритета інтерфейса для протоколу OSPF

Таке конфігурування дозволяє мереженому адміністратору впливати на процес вибору маршрутизаторів DR та BDR и виконується за допомогою команди

```
Router(config-if)#ip ospf priority num,
```

де num – число з діапазону 0 – 255, яке і визначає цей пріоритет.

5 Тестування протоколу OSPF

Команда `show ip route` дозволяє проглянути ТМ маршрутизтора.

Команда `show ip protocols` показує протоколи мереженого рівня, які працюють на маршрутизаторі. Для протоколу OSPF вона дозволяє побачити ідентифікатор маршрутизотора (router ID). В деяких версіях IOS номер показано не буде, тоді його можна проглянути за командами `show ip ospf` або `show ip ospf interface`. Остання команда дозволяє також подивитись значення таймерів протоколу OSPF та значення оцінки відповідного інтерфейсу [5, 15].

Команда `show ip ospf neighbor` показує сусідні OSPF-маршрутизатори, які знаходяться у сусідських відношеннях з даним маршрутизатором. З цієї таблиці можна дізнатись, зокрема, про ідентифікатори сусідніх маршрутизаторів (поле Neighbor ID); значення пріоритету інтерфейса маршрутизатора (Pri) – використовується в процесі вибору DR та BDR; стан інтерфейсу для протоколу OSPF (State). Наприклад, стан Full означає, що ці маршрутизатори мають ідентичні топологічні бази даних; час, що буде чекати маршрутизатор на отримання пакету Hello, перш ніж об'явити, що даний сусідній пристрій зник (Dead Time); IP-адресу інтерфейсу сусіднього маршрутизатора, до якого безпосередньо під'єднано даний маршрутизатор (Address); локальний інтерфейс, через який маршрутизатор встанови дані сусідські відносини (Interface). Є також модифікація цієї команди яка дозволяє отримати детальнішу інформацію про сусудів – `show ip ospf neighbor detail`.

Наприклад, для нашого випадку (рис. 5) таблиці сусідів будуть:

для маршрутизатора R1

```
Neighbor ID     Pri State   Dead Time Address       Interface
192.168.10.9    0   FULL/ - 00:00:35  192.168.10.2  Serial0/0/0
192.168.10.10   0   FULL/ - 00:00:35  192.168.10.6  Serial0/0/1;
```

для маршрутизатора R2

```
Neighbor ID     Pri State   Dead Time Address       Interface
```

```
192.168.10.5    0   FULL/ -  00:00:32  192.168.10.1   Serial0/0/0
192.168.10.10   0   FULL/ -  00:00:35  192.168.10.10  Serial0/0/1;
```
для маршрутизатора R3
```
Neighbor ID     Pri State    Dead Time Address        Interface
192.168.10.5    0   FULL/ -  00:00:36  192.168.10.5   Serial0/0/0
192.168.10.9    0   FULL/ -  00:00:35  192.168.10.9   Serial0/0/1,
```
що свідчить про те, що кожен маршрутизотор знаходиться в сусідських відносинах з двома іншими маршрутизаторами мережі.

Зауважимо, що два маршрутизатора не можуть сформувати сусідских відносин, якщо: на інтерфейсах маршрутизаторів, що з'єднані маски підмереж різні (це говорить про те, що ці інтерфейси знаходяться в окремих мережах); OSPF Hello інтервал і/або час життя (Dead Timers) на цих маршрутизаторах різні; типи мереж OSPF різні; під час настроювання протоколу OSPF виконано неправильні і/або некоректні команди.

Команда `show ip ospf database` – відображає вміст топологічної бази даних. Команда `clear ip route *` – очищує всю ТМ. Команда `clear ip route a.b.c.d` – вилучає з ТМ лише маршрут, задний адресою a.b.c.d. Команди групи `debug ip ospf` – виконують відлагодження операцій протоколу OSPF.

ЗАВДАННЯ

1. a. Настройте протокол OSPF на маршрутизаторах R2 – R6 мережі, наведеної на рис. 6, попередньо виконавши визначення IP-адрес для кожного її сегменту згідно даних, наведених у табл. 5 (маски підмереж повинні бути оптимальними). При цьому для мереж Net 1 – Net 9 використайте IP-адреси мережі 10.0.0.0/8, для мереж Net 10 – Net 12 – 172.16.0.0/16, а для Net 13, Net 14 – 193.18.24.0/24. Також врахуйте, що:

- маршрутизатор R2 повинен анонсувати лише мережі Net 10 – Net 12; - на маршрутизаторі R2 повинен бути прописаний шлях за замовчанням до маршрутизатора R1; - на маршрутизаторі R2 повинен бути прописаний статичний маршрут до Loopback 1, що піднятий на маршрутизаторі R7. Адреса для Loopback 1: 192.168.3.15/24.

b. Настройте аутентифікацію на кожному маршрутизаторі мережі.

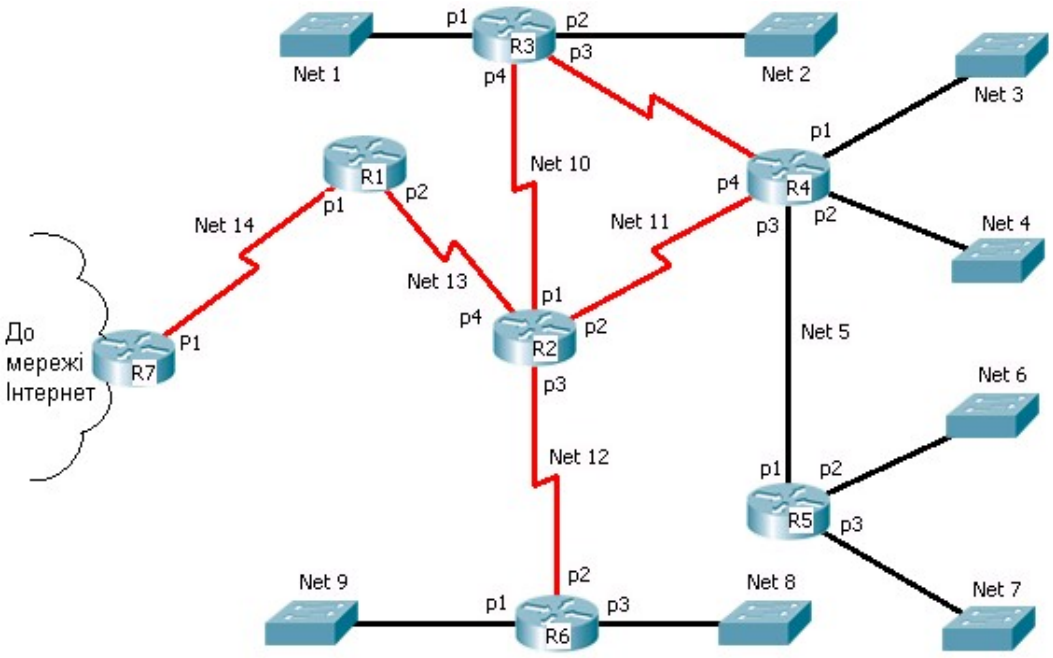


Рисунок 6 – Структура комп'ютерної мережі завдання № 1

Таблиця 5 – Варіанти до завдання № 1

№ вар.	Кількість вузлів у мережах								
	Net 1	Net 2	Net 3	Net 4	Net 5	Net 6	Net 7	Net 8	Net 9
1	120	60	16	10	130	60	64	80	70
2	15	85	23	18	128	10	58	20	28
3	125	37	24	12	50	54	30	10	16
4	10	60	50	17	256	40	13	10	100
5	8	4	28	70	120	64	14	6	70
6	6	64	16	32	40	30	14	14	5
7	16	4	100	27	20	40	13	10	8
8	14	20	70	30	28	70	20	14	14
9	36	33	5	9	16	32	8	5	37
10	90	30	8	20	100	27	54	4	40
11	35	12	14	23	60	30	2	16	24
12	78	256	37	15	128	10	58	32	50
13	70	30	40	10	57	33	55	2	28
14	12	125	24	37	115	45	4	10	16
15	17	10	50	60	128	2	16	23	100
16	70	8	28	4	10	50	37	17	70
17	32	6	16	64	125	37	24	12	37
18	27	16	100	4	10	60	50	17	40
19	30	14	70	20	8	4	28	70	24
20	9	36	5	128	6	64	16	32	50
21	20	90	8	30	16	4	100	27	28
22	23	35	14	12	14	20	70	30	16
23	15	78	37	15	36	33	5	9	100
24	10	70	40	30	264	30	8	20	70
25	115	45	4	10	35	12	14	23	5
26	50	2	14	23	78	15	37	15	100
27	10	50	37	17	70	30	40	10	70
28	125	37	24	12	100	28	150	200	5
29	10	60	50	17	60	16	256	128	8
30	8	4	28	70	12	100	200	264	14

Таблиця 6 – Варіанти до завдання № 2

№ вар.	RS	DN	Номер варіанта з		№ вар.	RS	DN	Номер варіанта з	
			табл. 7	табл. 8				табл. 7	табл. 8
1	R1	Net 7	1	1	16	R1	Net 7	4	3
2	R1	Net 5	2	1	17	R1	Net 5	5	3
3	R1	Net 4	3	1	18	R1	Net 4	6	3
4	R1	Net 8	4	1	19	R1	Net 8	1	4
5	R2	Net 1	5	1	20	R2	Net 1	2	4
6	R2	Net 3	6	1	21	R2	Net 3	3	4
7	R2	Net 7	1	2	22	R2	Net 7	4	4
8	R2	Net 8	2	2	23	R2	Net 8	5	4
9	R2	Net 4	3	2	24	R2	Net 4	6	4
10	R2	Net 8	4	2	25	R2	Net 8	1	5
11	R3	Net 7	5	2	26	R3	Net 7	2	5
12	R3	Net 5	6	2	27	R3	Net 5	3	5
13	R7	Net 1	1	3	28	R7	Net 1	4	5
14	R7	Net 3	2	3	29	R7	Net 3	5	5
15	R7	Net 5	3	3	30	R7	Net 5	6	5

2. Вкажіть оптимальний маршрут для протоколу OSPF з точки зору маршрутизатора RS до мережі DN (рис. 7). Обчисліть значення метрики цього маршруту. Варіанти завдань наведено у табл. 6.

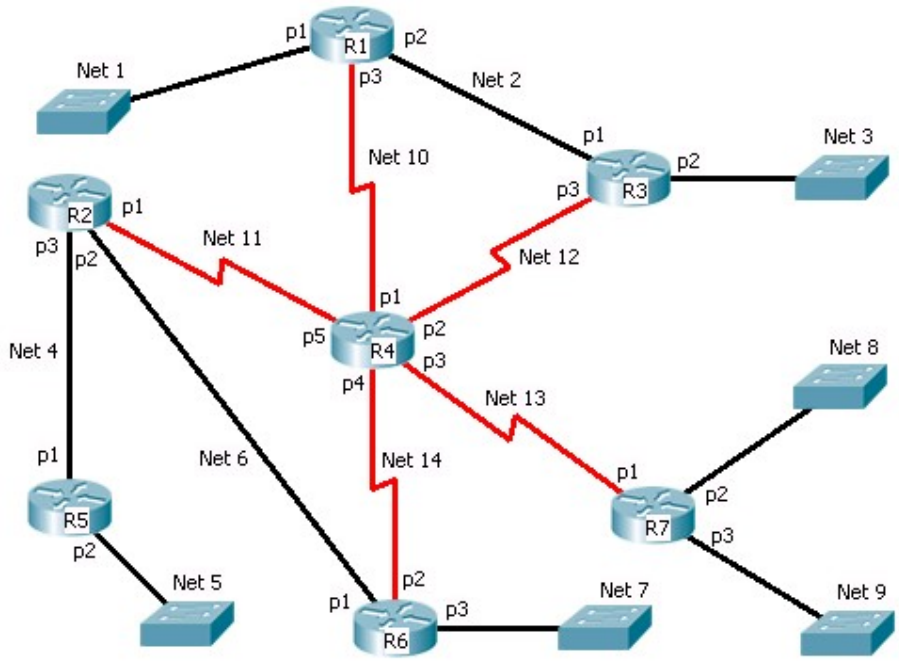


Рисунок 7 – Комп'ютерна мережа для завдання № 2

Таблиця 7 – Значення пропускної спроможності послідовних каналів

№ варіанта	Значення пропускної спроможності мережі (Мбіт/с)				
	Net 10	Net 11	Net 12	Net 13	Net 14
1	1024	128	1024	1024	512
2	256	512	1544	64	128
3	512	1024	1544	512	256
4	64	128	512	128	1024
5	128	64	256	256	64
6	1024	512	512	1544	1024

Таблиця 8 – Значення пропускної спроможності каналів LAN

№ вар.	Значення пропускної спроможності мережі (Мбіт/с)								
	Net 1	Net 2	Net 3	Net 4	Net 5	Net 6	Net 7	Net 8	Net 9
1	100	100	1000	10	10	100	10	100	100
2	1000	10	100	100	10	100	10	100	100
3	10	1000	10	1000	100	100	100	100	100
4	1000	100	100	100	1000	10	1000	100	100
5	1000	100	100	100	100	100	1000	10	100

Контрольні питання

1. Поясніть з якою метою використовується метрика маршруту і на основі яких параметрів вона обчислюється.
2. Поясніть що таке статична та динамічна маршрутизація.
3. Назвіть дві основні категорії алгоритмів динамічної маршрутизації. Наведіть приклади протоколів, що використовують дані алгоритми.
4. Поясніть різницю між внутрішніми і зовнішніми протоколами маршрутизації та наведіть приклади таких протоколів. Наведіть порівняльний аналіз цих видів маршрутизацій.
5. Наведіть порівняння протоколів динамічної маршрутизації.
6. Поясніть основні відмінності між алгоритмами маршрутизації DVA та LSA.
7. Наведіть команди настроювання статичного маршруту та маршруту за замовчанням.

8. Поясніть яку роль грає маршрут за замовчанням? В яких випадках він використовується?
9. Наведіть загальну характеристику протоколу OSPF. Які переваги та недоліки протоколу OSPF ви знаєте?
10. Наведіть термінологію протоколу OSPF.
11. Поясніть призначення топологічної бази даних та бази даних відносин суміжності протоколу OSPF.
12. Поясніть для яких типів мереж відбувається вибір маршрутизаторів DR та BDR у протоколі OSPF і яку роль вони виконують.
13. На власному прикладі покажіть процес вибору маршрутизаторів DR та BDR.
14. Охарактеризуйте основні типи пакетів OSPF.
15. Дайте стислу характеристику станів інтерфейсів OSPF-маршрутизаторів.
16. Наведіть основні команди тестування конфігурування протоколу OSPF та поясніть їх призначення.

1.1 Огляд протоколу EIGRP

Дистанційно-векторний протокол маршрутизації EIGRP (Enhanced Interior Gateway Routing Protocol) був розроблений та реалізований фірмою Cisco у 1992 р. Він є суттєвим вдосконаленням свого попередника – протоколу маршрутизації IGRP, який сьогодні фактично не використовується.

Переваги використання протоколу EIGRP.

Перевагами протоколу EIGRP відносно простих дистанційно-векторних протоколів є:

- *Швидка конвергенція*. На маршрутизаторах протоколу EIGRP конвергенція відбувається значно швидше, оскільки вона базується на сучасному алгоритмі дифузії поновлень маршрутизації DUAL (Diffusing Update Algorithm). Цей алгоритм гарантує відсутність петель у кожний момент часу на всьому маршруті та дозволяє усім маршрутизаторам, що належать до даної топології, виконати одночасну синхронізацію. Крім того, якщо у традиційних дистанційно-векторних протоколів певний маршрут став недоступним – маршрутизатори повинні чекати чергового періодичного поновлення, а протокол EIGRP буде при цьому використовувати резервний шлях (якщо такий існує).
- *Ефективне використання смуги пропускання*. По-перше, протокол EIGRP використовує розсилання часткових, обмежених за обсягом поновлень (Partial, bounded updates) маршрутизації, і як наслідок цього забезпечується мінімальне використання такими поновленнями смуги пропускання в умовах стабільної роботи мережі. Маршрутизатори EIGRP як правило розсилають часткові, поетапні поновлення маршрутизації, а не повні таблиці маршрутизації. Цей процес аналогічний роботі протоколу OSPF, однак на відміну від нього, маршрутизатори протоколу EIGRP розсилають ці часткові поновлення не всім маршрутизаторам даної області, лише тим, яким вони дійсно потрібні. Саме тому такі поновлення називаються обмеженими. По-друге, у протоколі EIGRP замість регулярного розсилання поновлень маршрутизації маршрутизатори підтримують постійний контакт один з одним шляхом розсилання невеликих пакетів вітання. Хоча пакети вітання розсилаються регулярно, внаслідок невеликого розміру вони досить незначно використовують смугу пропускання (на відміну від протоколів RIP та IGRP, які розсилають сусіднім пристроям свою повну таблицю маршрутизації кожні 30 або 90 секунд, відповідно).
- *Підтримка масок підмереж змінної довжини VLSM* (Variable-Length Subnet Mask) *і безкласової міжоменної маршрутизації CIDR* (Classless Interdomain Routing). На відміну від протоколу IGRP, EIGRP забезпечує повну підтримку безкласового IP шляхом обміну масками підмереж у повідомленнях поновлення маршрутів. Це дозволяє мережевим проектувальникам максимально використовувати адресний простір
- *Підтримка декількох протоколів мережевого рівня*. Протокол EIGRP підтримує протоколи IP, IPX та AppleTalk шляхом використання залежних від протоколу модулів (protocol-dependent module, PDM).
- *Використання складної та гнучкої метрики маршрутів*. Метрика протоколу EIGRP, на відміну від багатьох інших протоколів маршрутизації (крім протоколу IGRP), може враховувати одразу чотири показники (пропускна спроможність, час затримки, завантаженість та надійність каналу). При цьому адміністратор може задавати значимість кожного з цих показників.

Доцільно зауважити, що у деяких джерелах EIGRP називають гібридним протоколом маршрутизації, який поєднує кращі риси дистанційно-векторних алгоритмів і алгоритмів маршрутизації за станом каналу. Так, наприклад, протокол EIGRP використовує такі функції протоколу OSPF, як часткові поновлення маршрутів та виявлення сусідніх пристроїв. Але слід пам'ятати, що у технічному аспекті протокол EIGRP є суто ДВП.

1.2 Обчислення метрики протоколу EIGRP

Протокол EIGRP використовує метрику довжиною 32 біта, яка обчислюється за формулою:

$$M_{EIGRP} = \left(K_1 \cdot \left\lfloor \frac{10^7}{Bw} \right\rfloor \cdot 256 + \frac{K_2 \cdot \left\lfloor \frac{10^7}{Bw} \right\rfloor \cdot 256}{256 - Ld} + K_3 \cdot \frac{Dl}{10} \cdot 256 \right) \cdot \frac{K_5}{Rl + K_4}, \quad (1)$$

де Bw – найменша смуга пропускання каналу на шляху між відправником та отримувачем у КБіт/с; Dl – сумарна затримка каналів передачі даних між відправником та отримувачем в мкс. Затримка

визначається типом ЛЗ з'єднання (значення затримок для різних типів ліній зв'язку наведено у таблиці 1); Ld – максимальна завантаженість каналу між відправником та отримувачем; Rl – найнижча надійність каналу маршруту між відправником та отримувачем (характеризує як часто у каналі виникають помилки передавання даних); K_1 – K_5 – вагові коефіцієнти. Позначення $\lfloor X \rfloor$ у даному випадку означає – ціла частина від числа X.

Таблиця 1 – Значення затримки залежно від середовища передавання

Середовище передавання	Значення затримки (мкс)	Середовище передавання	Значення затримки (мкс)
Fast Ethernet	100	1544 K	20000
FDDI	100	1024 K	20000
100M ATM	100	512 K	20000
Ethernet	10000	64 K	20000

Значення Bw та Dl – це статичні величини, а Ld та Rl – вимірюються динамічно протягом 5 хвилин (для визначення відповідних середніх значень і уникнення впливу, наприклад, миттєвих заторів та помилок каналу).

Значення надійності може бути у діапазоні від 1 до 255, де 1 – відповідає мінімальній надійності, а 255 – максимальній. Надійність виражається у вигляді дробі Rl/255. Так, 255/255 – означає надійність 100%, а 250/255 – 98%

Значення завантаженості також може бути у діапазоні від 1 до 255, де 1 – відповідає мінімальній завантаженості, а 255 – максимальній. Як і надійність, завантаженість також виражається у вигляді дробі Ld/255. Так, наприклад, 51/255 – означає 20% завантаженість, а 255/255 – що дана лінія повністю завантажена.

Зауважимо, що за замовчанням значення коефіцієнтів такі: $K_1 = K_3 = 1$, $K_2 = K_4 = K_5 = 0$ і формула для обчислення метрики має вигляд:

$$M_{EIGRP}^{def} = \left(K_1 \cdot \left\lfloor \frac{10^7}{Bw} \right\rfloor + K_3 \cdot \frac{Dl}{10} \right) \cdot 256 \cdot \quad (2)$$

Оскільки до складу метрики в даному випадку входять лише статичні величини, не буде виконуватись частих перерахунків даних топологічної таблиці.

Зазначимо, що максимальна кількість переходів для протоколу EIGRP дорівнює 224 (наприклад, для протоколу RIP кількість переходів становить усього 16), чого цілком достатньо для підтримки навіть самих великих сучасних мереж.

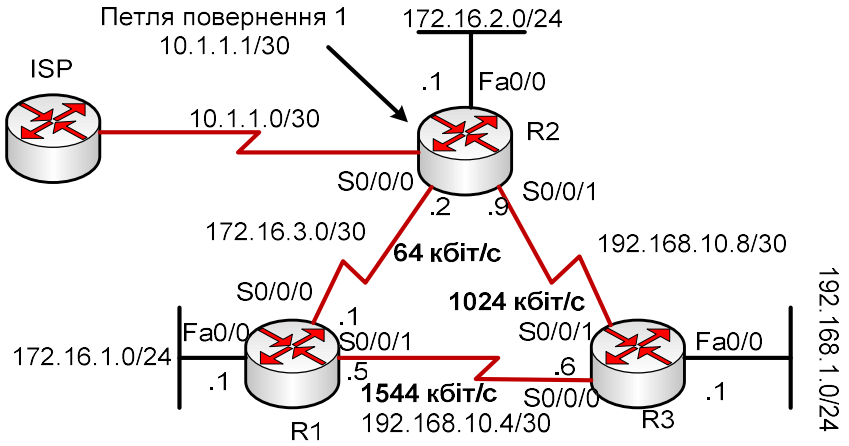
Розглянемо приклад обчислення метрики. Подивимось на приклад невеликої КМ (рис. 1.1.а) та зміст ТМ маршрутизатора R2 (рис. 1.1.б). ТМ містить маршрути до всіх, відомих для R2 пунктів призначення. Літери „C" і „D" в лівих позиціях рядків таблиці означає джерело отримання даного рядка. Так, літера „C" означає безпосередньо під'єднані мережі, а літера „D" – що даний рядок отриманий за допомогою протоколу EIGRP. Розглянемо останній рядок ТМ:

```
D 192.168.1.0/24 [90/3014400] via 192.168.10.10 00:00:09, Serial0/0/1.
```

Тут після літери „D" йдуть: IP-адреса пункту призначення; у квадратних дужках адміністративна відстань (90) і через слеш метрика маршрута (3014400); IP-адреса інтерфейса наступного вузла на шляху до пункта призначення (192.168.10.10); скільки часу існує цей рядок (9 сек.) та локальний вихідний інтерфейс, через який можна досягнути пункт призначення (Serial0/0/1). Обчислимо значення метрики.

Для визначення метрики згідно (2) слід визначити найменшу смугу пропускання каналу уздовж маршруту від джерела до пункта призначення та знайти сумарну затримку. Найменша смуга пропускання 1024 Кбіт/с (оскільки оптимальний маршрут від R2 до мережі 192.168.1.0 проходить через R3, а смуга пропускання каналу від R2 до R1 складає всього 64 Кбіт/с). Сумарна затримка шляху складає 20000 + 100 = 20100 мкс (див. табл. 1). Отже, враховуючи сказане остаточне шукане значення складе:

$$M_{EIGRP}^{def} = \left(1 \cdot \left\lfloor \frac{10^7}{1024} \right\rfloor + 1 \cdot \frac{20100}{10} \right) \cdot 256 = (9765 + 2010) \cdot 256 = 3014400$$



а)

```
R2# show ip route
<частина виведення пропушена>
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D 192.168.10.0/24 is a summary, 00:00:9, Null0
D 192.168.10.4/30 [90/21024000] via 192.168.10.10, 00:00:9, Serial0/0/1
C 192.168.10.8/30 is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D 172.16.0.0/16 is a summary, 00:00:9, Null0
D 172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:9, Serial0/0/0
C 172.16.2.0/24 is directly connected, Fastethernet0/0
C 172.16.3.0/30 is directly connected, Serial0/0/0
      10.0.0.0/30 is subnetted, 1 subnets
C 10.1.1.0/30 is directly connected, loopback1
D 192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:9, Serial0/0/1
```

б)

Рисунок 1.1 – а) невелика комп'ютерна мережа, б) ТМ маршрутизатора R2

Далі зупинемось детальніше на сутності роботи протоколу EIGRP, але для цього перш за все слід познайомитись з його основною термінологією.

1.3 Термінологія протоколу EIGRP

Протокол EIGRP у своїй роботі використовує дані трьох таблиць: *маршрутизації*, *сусідніх пристроїв* та *топології*. Ці таблиці ще називають базами даних протоколу. Призначення ТМ нам вже відоме. Тому розглянемо призначення двох інших таблиць.

Таблиця сусідніх пристроїв

Кожний маршрутизатор EIGRP підтримує таблицю сусідніх пристроїв (neighbor table), в якій перераховані суміжні маршрутизатори. Для кожного протоколу (наприклад, IP, IPX), що підтримується протоколом EIGRP, є своя таблиця сусідніх пристроїв (ТСП). При виявленні нових сусідніх пристроїв їх адреси та інтерфейси заносяться у ці таблиці. Проглянути зміст ТСП можна за командою show ip eigrp neighbors).

При відправленні пакета привітання сусідній пристрій повідомляє час утримання, що вказує, як довго маршрутизатор розглядає свій сусідній пристрій як досяжний та працездатний. Якщо за період утримання від маршрутизатора не надійшов пакет привітання, то вважається, що час утримання вичерпано. В такому випадку алгоритм DUAL (цей алгоритм ми розглянемо пізніше) інформується про зміну топології і повинен знову обчислити параметри нової топології.

ТСП має, зокрема, такі поля.

- *Порядковий номер* (Н) запису по мірі навчання даного пристрою стосовно сусідніх пристроїв.
- *Адреса сусіднього пристрою* (Neighbor Address) – адреса мережевого рівня сусіднього пристрою.
- *Інтерфейс* (Interface) – локальний інтерфейс, через який було отимано пакет Hello від сусіднього пристрою.

- *Час утримання* (Hold Time) – часовий інтервал, після закінчення якого, у випадку відсутності будь-яких повідомлень від сусіднього пристрою, канал розглядається як непрацездатний. При отриманні ж будь-якого пакету протоколу EIGRP, таймер приймає початкове значення.
- Доступний час (Uptime) – час, що минув з моменту додавання даного сусіднього пристрою у ТСП.
- *Таймер циклу обміну повідомленнями* (Smooth Round-Trip Timer – SRTT) – середній час, потрібний для того, щоб надіслати пакет сусідньому пристрою та одержати від нього відповідний пакет. Цей таймер визначає інтервал повторного передавання (Retransmit Interval – RTI).
- *Час ретрансляції* (Retransmission Timeout – RTO) – час в мілісекундах, протягом якого програмне забезпечення очікує моменту повторного пересилання пакету з черги повторного розсилання.
- *Лічильник черги* (Queue Count – Q Cnt) – число пакетів які перебувають у черзі очікуючи передавання. Якщо це значення постійно більше нуля – ймовірно маршрутизатор зазнає переповнення. Нульове значення свідчить, що пакетів протоколу EIGRP у черзі немає.
- *Послідовний номер* (Sequence Number – Seq No) – номер останнього пакета, отриманого від даного сусіднього пристрою. Протокол EIGRP використовує це поле для підтвердження отримання пакету, переданого сусіднім пристроєм, та для ідентифікації пакетів, що передані з порушенням порядку. ТСП забезпечує надійне та впорядковане доставлення пакетів.

Наприклад, ТСП для маршрутизатора R2 (рис. 1.1.а) має вигляд

```
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
  H Address       Interface  Hold  Uptime  SRTT  RTO   Q   Seq
                             (sec)         (ms)       Cnt  Num
  1 192.168.10.10 Ser0/0/1    10  00:01:44  20   200   0    7
  0 172.16.3.1    Ser0/0/0    10  00:03:27  25   200   0    12
```

Топологічна таблиця

Топологічна таблиця (topology table) містить всі ТМ протоколу EIGRP, наявні на пристроях даної автономної системи (проглянути зміст топологічної таблиці можна за командою show ip eigrp topology). Алгоритм DUAL отримує інформацію з ТСП і топологічної таблиці (ТТ) та обчислює маршрути з найменшою оцінкою до кожного пункту призначення. Завдяки цьому маршрутизатори протоколу EIGRP можуть швидко визначити альтернативні маршрути та використати їх у разі потреби. Первинний маршрут (successor) записується у ТМ, а його копія – у ТТ. Усі маршрутизатори EIGRP підтримують ТТ для кожного сконфігурованого мережевого протоколу. У цій таблиці містяться маршрути до усіх пунктів призначення, які стали відомі маршрутизатору.

ТТ має такі поля.

- *Передбачувана відстань* (Feasible Distance – FD) – це найменша обчислена метрика до кожного пункту призначення. У прикладі 1.1 показано ТТ для маршрутизатора R2, з прикладу, наведеного на рис. 1.1. Тут передбачувана відстань, наприклад до мережі 192.168.1.0 становить 3014400, на що вказує запис „FD is 3014400".
- *Джерело маршруту* (Route Source) – це ідентифікаційний номер маршрутизатора, який анонсував цей маршрут. Дане поле заповнюється лише тільки для маршрутів, які стали відомі ззовні від інших мереж протоколу EIGRP. У прикладі 1.1, джерелами маршруту до мережі 192.168.1.0 є 192.168.10.10 та 172.16.3.1, про що свідчать записи „via 192.168.10.10" та „via 172.16.3.1" відповідно.
- *Повідомлена відстань* (Reported Distance – RD) або об'явлена відстань (Advertised Distance – AD) – це значення відстані, яке сусідній маршрутизатор повідомляє конкретному одержувачу. У прикладі 1.1 повідомлена відстань до мережі 192.168.1.0 дорівнює 28160, на що вказує значення поля RD (3014400/28160).

Інформація про інтерфейс (Interface Information) – це номер інтерфейсу, через який можна досягти пункту призначення. З прикладу 1.1 видно, що мережу 192.168.10.10 можна досягнути через інтерфейс Serial0/0/1 (via 192.168.10.10 (3014400/28160), Serial0/0/1), а можна резервним шляхом через Serial0/0/0 (via 172.16.3.1 (410240000/2172416), Serial0/0/0)

- *Статус маршруту* (Route Status) – може бути пасивний або активний. Пасивні (Passive – P) –

це стійкі та готові до використання маршрути, активні (Active – A) це ті, для яких алгоритм DUAL продовжує процес перерахування маршруту. Протокол EIGRP сортує записи ТТ так, щоб первинні маршрути знаходились у її верхній частині, а за ними йшли резервні. У нижній частині цієї таблиці розташовуються маршрути, які алгоритм DUAL розглядає як можливі петлі маршрутизації.

```
R2# show  ip  eigrp  topology
IP-EIGRP Topology Table  AS(1)/ID 10.1.1.1
Codes: P - Passive, A - Active, U - Update,
Q - Query, R - Reply, r - Reply Status s – sia Status
P 192.168.10.4/30, 1 successors, FD is 3523840
   via 192.168.10.10 (3523840/2169856), Serial0/0/1
   via 172.16.3.1 (410240000/2169856), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 3014400
   via 192.168.10.10 (3014400/28160), Serial0/0/1
   via 172.16.3.1 (410240000/2172416), Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
   via connected Serial0/0/1
P 172.16.1.0/24, 1 successors, FD is 3526400
   via 192.168.10.10 (3526400/2172416), Serial0/0/1
   via 172.16.3.1 (40514560/28160), Serial0/0/0
P 172.16.2.0/24, 1 successors, FD is 28160
   via connected FastEthernet 0/0
P 172.16.3.0/30, 1 successors, FD is 40512000
```

Приклад 1.1 – Топологічна таблиця протоколу EIGRP

Первинні маршрути

Первинним називається маршрут обраний у якості основного для досягнення певного пункту призначення. Цей маршрут визначається алгоритмом DUAL на основі інформації з ТСП і ТТ, і вноситься до ТМ. Для кожного конкретного маршруту може бути до чотирьох первинних маршрутів. Вони можуть мати як рівні, так і нерівні оцінки й розглядаються як найкращі вільні від петель маршрути до даного пункту призначення.

Резервні маршрути

Потенційно первинний (Feasible Successor – FS) – це резервний маршрут. Такі маршрути встановлюються одночасно з первинними, однак зберігаються тільки у ТТ. Одночасно можуть зберігатися кілька резервних маршрутів. Наявність резервного маршруту для досягнення одержувача не є обов'язковою.

Маршрутизатор розглядає пристрої на резервному маршруті як сусідні в спадному напрямку (він вважає, що вони перебувають ближче до пункту призначення, ніж сам). Вони виражають анонсовану сусіднім маршрутизатором оцінку маршруту до пункту призначення. Якщо первинний маршрут стає недійсним, то маршрутизатор шукає резервний і підвищує його статус до первинного. Резервний маршрут до пункту призначення повинен мати менше значення FD, ніж значення RD даного первинного маршруту.

Якщо резервний маршрут не був установлений на основі наявної інформації, то маршрутизатор надає йому статус активного (Active) і надсилає пакети запитів усім сусіднім пристроям для перерахування топології. Після одержання відповідей на ці запити маршрутизатор може на їх основі установити нові первинні або резервні маршрути. Після цього маршрутизатор надає маршруту статус пасивного (Passive).

Вибір первинного та резервних маршрутів

Розглянемо питання визначення маршрутизатором первинних та резервних маршрутів. Нехай в ТМ маршрутизатора RTA є маршрут до мережі Network Z через маршрутизатор RTB (рис. 1.2). З погляду маршрутизатора RTA маршрутизатор RTB перебуває на поточному первинному маршруті до мережі Network Z, тому RTA надсилає пакети, призначені для мережі Network Z у

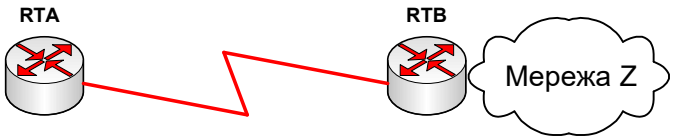


Рисунок 1.2 – Первинний маршрут протоколу EIGRP

напрямку RTB. Маршрутизатор RTA повинен мати принаймні один первинний маршрут до Network Z для того, щоб алгоритм DUAL міг внести його в ТМ.

Якщо деякий маршрутизатор RTC, який з'єднаний з RTA аналогічно маршрутизатору RTB і повідомляє RTA про наявність у нього маршруту до мережі Network Z з такою ж метрикою, як і у маршрутизатора RTB, то RTA також розглядає RTC як первинний маршрут і алгоритм DUAL установлює другий маршрут до мережі Network Z через RTC (рис. 1.3).

Кожен сусідній пристрій маршрутизатора RTA, що анонсує вільний від петель маршрут до мережі Network Z (однак з FD, більшою ніж метрика найкращого маршруту й меншою ніж його RD), ідентифікується у ТТ, як той, що знаходиться на резервному маршруті. Маршрутизатор розглядає свої пристрої на резервних маршрутах як сусідні пристрої, що перебувають у низхідному напрямку, тобто розташовані ближче до одержувача, чим він сам. Якщо з будь-яких причин первинний маршрут не може виконувати свої функції, то алгоритм DUAL може швидко знайти резервний на основі даних ТТ й встановити новий маршрут до пункту призначення. Якщо ж такий резервний маршрут відсутній, то алгоритм DUAL переводить маршрут в активний стан і запрошує допомоги у сусідів у знаходженні нового, вільного від петель маршруту. Сусідні маршрутизатори зобов'язані відповісти на цей запит. Якщо в сусіднього маршрутизатора є такий маршрут (маршрути), то надсилається інформація про нього (них). Інакше сусідній маршрутизатор повідомляє про відсутність маршруту до цього пункту призначення.

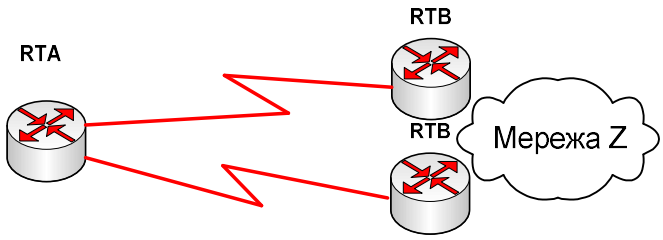


Рисунок 1.3 – Первинні маршрути протоколу EIGRP

Надлишкова кількість перерахувань маршрутів свідчить про нестабільну роботу мережі й знижує її продуктивність. Для запобігання проблем, пов'язаних з конвергенцією, алгоритм DUAL перед виконанням перерахування завжди намагається знайти резервний маршрут. Якщо такий є, то алгоритм DUAL може встановити новий маршрут без перерахування.

Застарівання активних маршрутів Якщо один або більше маршрутизаторів, яким був розісланий запит, не відповідає протягом активного часу (180 секунд), то маршрут (або кілька маршрутів) переводиться у стан „за стрівання" (stuck in active), В цьому випадку протокол EIGRP виключає зі своєї ТСП маршрутизатори, що не відповіли на запит і реєструє в системному журналі повідомлення про помилку „stuck in active" для маршрутів, які були активними.

Створення тегів для маршрутів

У ТТ може бути записана додаткова інформація про кожний маршрут. Протокол EIGRP класифікує маршрути як внутрішні або зовнішні. Внутрішніми називаються маршрути усередині даної автономної системи протоколу EIGRP, а зовнішніми – ті, що беруть свій початок поза даною автономною системою. Маршрути, отримані або перерозподілені від інших протоколів маршрутизації вважаються зовнішніми.

Як тег, маршруту може бути присвоєне значення від 0 до 255. Всі зовнішні маршрути заносяться в ТТ і їм призначається тег, що містить таку інформацію: ідентифікаційний номер маршрутизатора EIGRP, що поширив маршрут у мережу EIGRP; Номер АС одержувача; протокол, використовуваний у зовнішній мережі; оцінка або метрика, отримана від зовнішнього протоколу; конфігурований тег адміністратора.

Для завдання строгої і точної політики маршрутизації рекомендується скористатися функцією задання маршрутам тегів і, особливо, тегів адміністратора. Останнім може бути будь-яке число від 0 до 255. По суті це звичайний тег, що можна використовувати для реалізації спеціальної стратегії маршрутизації. Зовнішні маршрути можуть прийматися, відкидатися або поширюватися на основі кожного з тегів маршруту, в тому числі й тегу адміністратора. Оскільки користувач може задати тег адміністратора будь-яким зручним для нього способом, функція задання тегів маршрутам надає більшу гнучкість під час керуванні мережею. Це виявляється особливо корисним у тих випадках, коли мережа протоколу EIGRP взаємодіє з мережею протоколу граничного шлюзу, що базується на використанні політик.

4.8.4 Функції і технології протоколу EIGRP

Протокол EIGRP використовує багато нових технологій, кожен з яких поліпшує операційну ефективність, підвищує швидкість конвергенції та розширює набір функцій протоколу IGRP та інших протоколів маршрутизації. Ці технології можна поділити на такі чотири категорії.

- Виявлення сусідніх пристроїв і відновлення загубленого з ними зв'язку.
- Надійний транспортний протокол (Reliable Transport Protocol).
- Алгоритм DUAL кінцевих станів машини.
- Модулі конкретних протоколів.

Розглянемо детальніше кожну з цих технологій.

Виявлення сусідніх пристроїв і відновлення втраченого з ними зв'язку

Звичайні прості дистанційно-векторні маршрутизатори не встановлюють зв'язків зі своїми сусідами. На відміну від них маршрутизатори протоколу EIGRP встановлюють зв'язки зі своїми сусідніми пристроями. На рис. 1.4 проілюстровано процес встановлення зв'язків між суміжними пристроями протоколу EIGRP.

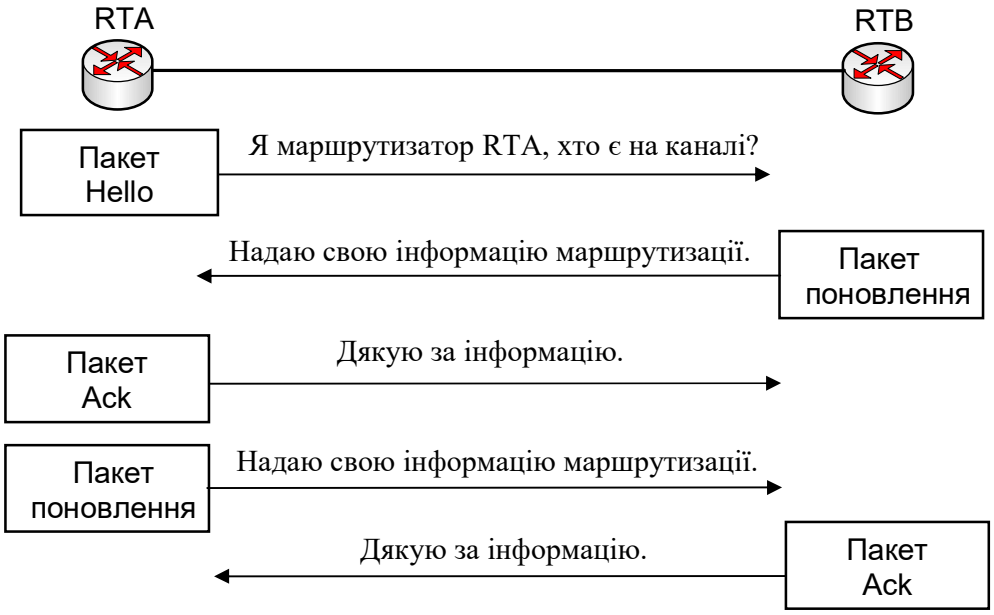


Рисунок 1.4 – Обмін інформацією сусідніх маршрутизаторів EIGRP

Маршрутизатори EIGRP встановлюють відносини суміжності із сусідніми маршрутизаторами шляхом розсилання невеликих пакетів-вітань. Ці пакети за замовчанням розсилаються кожні 5 секунд на каналах з великою смугою пропускання й кожні 60 секунд на низькошвидкісних багаточкових каналах. Маршрутизатор EIGRP припускає, що поки від відомих йому сусідніх пристроїв надходять пакети вітання, ці пристрої та відповідні маршрути залишаються діючими.

Формуючи відносини суміжності маршрутизатори EIGRP одержують можливості: динамічно дізнаватися про нові маршрути, що з'являються у мережі; ідентифікувати маршрутизатори, які стали недосяжними або непрацездатними; виявляти маршрутизатори, які раніше були недосяжні.

Надійний транспортний протокол

Надійний транспортний протокол (Reliable Transport Protocol, RTP) – це протокол транспортного рівня, який може гарантувати впорядковане доставлення пакетів EIGRP всім сусідам. У мережах IP-протоколу для впорядкування і своєчасного доставлення пакетів використовується протокол TCP. Однак протокол EIGRP незалежний від використовуваного мережевого протоколу і не використовує протокол TCP/IP для обміну інформацією маршрутизації (як це роблять протоколи RIP, IGRP, OSPF). Для реалізації такої незалежності від IP, протокол EIGRP використовує свій фірмовий транспортний протокол для гарантованого доставлення інформації.

EIGRP може активізувати протокол RTP для забезпечення служби надійної або негарантованої доставки залежно від конкретної ситуації. Наприклад, пакети вітання не потребують додаткового навантаження на мережу, за рахунок гарантованого доставлення, оскільки вони розсилаються часто

і їх розмір повинен бути невеликим. Проте гарантоване доставлення інформації про маршрути може прискорити конвергенцію, оскільки маршрутизатори EIGRP не очікують завершення часу таймера до повторного передавання. Використання надійного транспортного протоколу дозволяє протоколу EIGRP одночасно здійснювати багатоадресне та одноадресне розсилання, що забезпечує максимальну ефективність.

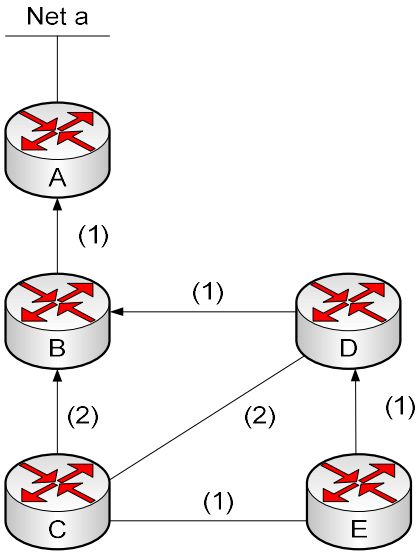
Машина кінцевих станів алгоритму DUAL

Головним компонентом протоколу EIGRP є алгоритм обчислення маршрутів. Повна назва цієї технології – абстрактна машина кінцевих станів (finite-state machine, FSM) алгоритму DUAL. Вона визначає набір можливих станів, через які можна пройти, які події викликають ці стани, а які є результатом цих станів. FSM містить всі логічні операції, необхідні для обчислення й порівняння маршрутів у мережі протоколу EIGRP.

Алгоритм DUAL стежить за всіма маршрутами, анонсованими сусідніми пристроями й використовує складену (композитну) метрику для кожного маршруту. Він гарантує, що кожний маршрут не містить петель. Після відповідних обчислень алгоритм DUAL заносить маршрути з найменшими оцінками в ТМ (тобто первинні маршрути), а їх копії – у ТТ.

Протокол зберігає важливу маршрутну й топологічну інформацію в ТСП і ТТ, які надають алгоритму DUAL маршрутну інформацію у випадку порушень у роботі мережі. Використовуючи інформацію цих таблиць DUAL може при необхідності швидко знаходити альтернативні маршрути: якщо будь-який канал стає непрацездатним, то він шукає у ТТ. альтернативний (потенційно первинний або резервний) маршрут.

Пакети, надіслані у мережу-одержувач, негайно надсилаються за резервним маршрутом, що у цей момент одержує статус первинного, як показано на рис. 1.5. Тут маршрутизатор D втрачає прямий зв'язок з маршрутизатором B і не має ідентифікованого первинного маршруту. Ймовірна відстань FD (обчислена оцінка) для маршруту від маршрутизатора D до маршрутизатора A дорівнює 2, а анонсована відстань через маршрутизатор C дорівнює 3. Оскільки значення RD менше, ніж метрика найкращого маршруту, але більше ніж відстань FD, жоден резервний маршрут не заноситься у ТТ. Маршрутизатор C має ідентифікований резервний маршрут, так само як і маршрутизатор E, оскільки маршрут вільний від петель, а відстань RD до маршрутизатора наступного переходу менша, ніж відстань FD для первинного маршруту. Кінцевий результат роботи алгоритму DUAL наведено на рис. 1.5,б. Детально процес конвергенції наведений у [15].

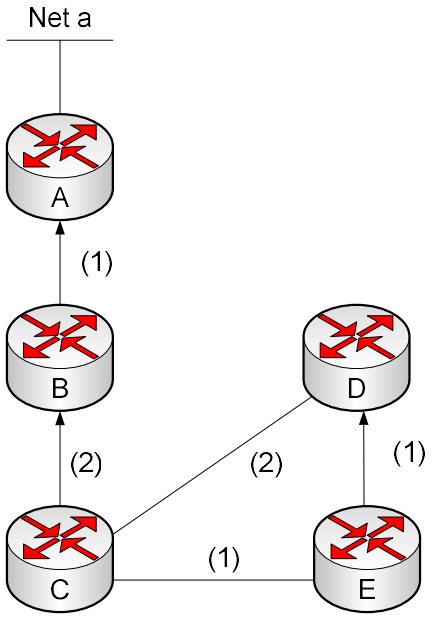


а)

C	EIGRP	FD	RD	Топологія
Net a		3		(FD)
	Через B	3	1	(Наступник)
	Через D	4	2	(FS)
	Через E	4	3	

D	EIGRP	FD	RD	Топологія
Net a		2		(FD)
	Через C	2	1	(Наступник)
	Через E	5	3	(Наступник)

E	EIGRP	FD	RD	Топологія
Net a		3		(FD)
	Через D	3	2	(Наступник)
	Через C	4	3	



C	EIGRP	FD	RD	Топологія
Net a		3		(FD)
	Через B Через D Через E	3	1	(Наступник)

D	EIGRP	FD	RD	Топологія
Net a		5		(FD)
	Через C Через E	5 5	3 4	(Наступник) (Наступник)

E	EIGRP	FD	RD	Топологія
Net a		4		(FD)
	Через C Через D	4	3	(Наступник)

б)

Рисунок 1.5 – Приклад результату роботи алгоритму DUAL: а) мережа до порушення прямого зв'язку між маршрутизаторами D і B; б) мережа після такого порушення.

Модулі PDM

Однією з привабливих якостей EIGRP є його модульна структура, що забезпечує максимальний рівень масштабованості та адаптованості. Підтримка різних мережевих протоколів (IP, IPX, AppleTalk), реалізована в протоколі EIGRP за допомогою модулів PDM. Фактично EIGRP може бути легко адаптований до нових або модифікованих мережевих протоколів (наприклад, IPv6) шляхом додавання нового модуля PDM. На рис. 1.6 показана загальна схема роботи модуля PDM.

а)

Кожний модуль PDM відповідає за виконання всіх функцій, пов'язаних з відповідним мережним протоколом. Зокрема, модуль IP-EIGRP відповідає за виконання таких функцій:

- відправлення та одержання інформації протоколу EIGRP, що містить дані протоколу IP;
- повідомлення алгоритму DUAL про одержання нової інформації, що стосується IP-маршругизації;
- підтримка результатів прийнятих алгоритмом DUAL рішень про маршрутизацію в таблиці IP-маршрутизації;
- подальше поширення інформації про маршрути, яка стала відома іншим протоколам маршрутизації, що підтримують IP.

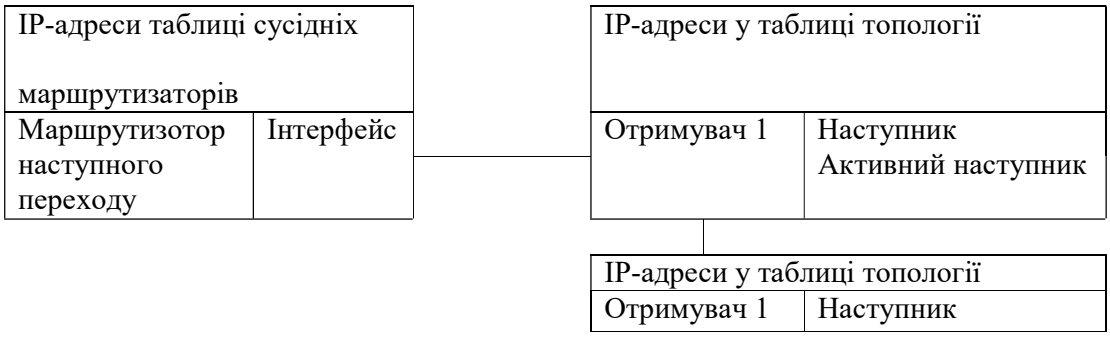


Рисунок 1.6 – Модулі PDM протоколу EIGRP

1.5 Типи пакетів протоколу EIGRP

Протокол EIGRP використовує кілька різних типів пакетів для підтримки різних своїх таблиць і встановлення складних (комплексних) зв'язків із сусідніми маршрутизаторами. Нижче наведено

п’ять типів пакетів протоколу EIGRP:

1) пакети вітання (Hello);
2) пакети підтвердження (Acknowledgment);
3) пакети відновлення маршрутів (Update);
4) пакети запитів (Query);
5) пакети відповідей на запити (Reply).

Розглянемо кожен з цих типів пакетів.

Пакети вітання

Протокол EIGRP використовує пакети вітання для виявлення сусідніх маршрутизаторів, їх тестування та повторного виявлення після збоїв. Повторне виявлення відбувається в тому випадку, якщо маршрутизатори не одержують один від одного пакетів вітання протягом часу утримання, але пізніше поновлюють зв’язок.

Маршрутизатори EIGRP розсилають пакети вітання з фіксованим інтервалом (задається у файлі конфігурації), який називається *інтервалом розсилання вітання* (hello interval). Прийнятий за замовчанням інтервал вітання залежить від ширини полоси пропускання інтерфейсу, як показано в табл. 1.2. Для відправлення пакетів вітання протокол EIGRP використовує багатоадресне розсилання.

Нагадаємо, що маршрутизатор протоколу EIGRP зберігає інформацію про сусідні пристрої у ТСП. В ній для кожного сусіднього пристрою є поле послідовного номера, у якому записується номер останнього отриманого від цього пристрою пакета протоколу EIGRP. Іншим полем ТСП є поле часу утримання, в якому записується час одержання останнього пакета. Для того, щоб у сусіднього маршрутизатора зберігався статус пасивного (досяжного і працездатного), необхідно, щоб за час утримання від нього надійшов хоча б один пакет. В протилежному випадку протокол EIGRP розглядає цей сусідній маршрутизатор як непрацездатний і алгоритм DUAL починає перераховувати ТМ. Стандартно час утримання втричі більше інтервалу вітань, однак адміністратор може сконфігурувати обидва таймери.

Таблиця 1.2 – Інтервали розсилання пакетів привітання

Ширина смуги пропускання	Тип каналу	Інтервал привітання за замовчанням	Час утримання за замовчанням
≤ 1,544 Мбіт/с	Протокол Multipoint Frame Relay	60 секунд	180 секунд
> 1,544 Мбіт/с	Линия T1, з’єднання "точка -точка"	5 секунд	15 секунд

У протоколі EIGRP (на відміну від OSPF) для здійснення зв’язку відсутня умова рівності значень інтервалів вітання й блокування на сусідніх маршрутизаторах. При цьому останні дізнаються про інтервали таймерів з пакетами вітання і використовують дану інформацію для встановлення стійкого зв’язку незважаючи на різні інтервали таймерів.

Пакети вітання завжди розсилаються методом негарантованого доставлення і не вимагають підтвердження.

Пакети підтвердження

Маршрутизатор EIGRP використовує пакети підтвердження для того, щоб повідомити інші маршрутизатори про одержання ним пакета EIGRP протягом сеансу „надійного” обміну даними. Надійний транспортний протокол може забезпечити надійний зв’язок між вузлами EIGRP. Для забезпечення гаратированого доставлення, вузол що приймає повинен підтвердити отримання повідомлення від джерела. Для цього використовуються пакети підтвердження (які можна назвати пакетами вітання „без даних”), На відміну від багатоадресних пакетів вітання, ці пакети є одноадресними. Підтвердження також може бути здійснене шляхом суміщення передачі прямих і зворотних пакетів інших типів пакетів EIGRP, таких як пакети відповідей на запити.

Пакети відновлень маршрутів

Пакети відновлень маршрутів використовуються в тих випадках, коли маршрутизатор виявляє новий сусідній пристрій. Тоді маршрутизатор EIGRP надсилає одноадресні пакети відновлення маршрутів цьому новому сусідньому пристрою для того, щоб він міг додати цю інформацію у свою

ТТ. Зауважимо, що для передавання новому сусідньому пристрою всієї топологічної інформації може знадобитись більше одного пакета.

Пакети відновлення використовуються також коли маршрутизатор виявляє зміну топології мережі, тоді він надсилає багатоадресні пакети відновлення усім своїм сусідам, попереджаючи їх про таку зміну. Всі пакети відновлення розсилаються методом гарантованого доставлення.

Пакети запитів і відповідей на запити

Маршрутизатор протоколу EIGRP використовує пакети запитів щоразу, коли йому потрібна конкретна інформація від будь-якого зі своїх сусідніх пристроїв. Пакет відповіді використовується для відповіді на запит.

Якщо у маршрутизатора EIGRP зникає первинний маршрут і він не може знайти резервного, то алгоритм DUAL переводить маршрут в активний стан. Після цього маршрутизатор виконує багатоадресне розсилання запиту всім своїм сусідам для знаходження первинного маршруту. Сусідні пристрої повинні надіслати відповіді на запити, в яких або надається інформація про первинний маршрут, або повідомляється про відсутність у них такої інформації.

Запити можуть бути як багато- так і одноадресними, у той час як відповіді на запити завжди є одноадресними. Обидва типи пакетів розсилаються методом гарантованого доставлення.

1.6 Конвергенція протоколу EIGRP

Алгоритм DUAL забезпечує дуже швидку конвергенцію протоколу EIGRP. Для кращого розуміння процесу конвергенції з використанням DUAL, розглянемо схему, наведену на рис. 1.7 [5]. Маршрутизатор RTA може одержати доступ до мережі Network w через три різних маршрутизатори: RTX, RTY або RTZ. Для спрощення обчислень композитна метрика протоколу EIGRP замінена оцінкою для каналу. ТТ маршрутизатора RTA містить список всіх маршрутів, анонсованих сусідніми з ним пристроями.

Як показано у табл. 1.3, маршрутизатор RTA зберігає для кожної мережі реальну (обчислену) оцінку доступу до цієї мережі, а також анонсовану оцінку (повідомлену відстань) від свого сусіднього пристрою.

Спочатку RTY є первинним маршрутом до Network w, оскільки має найменшу обчислену оцінку. Найменша обчислена метрика RTA до Network w (передбачувана відстанню FD до Network w) дорівнює 31.

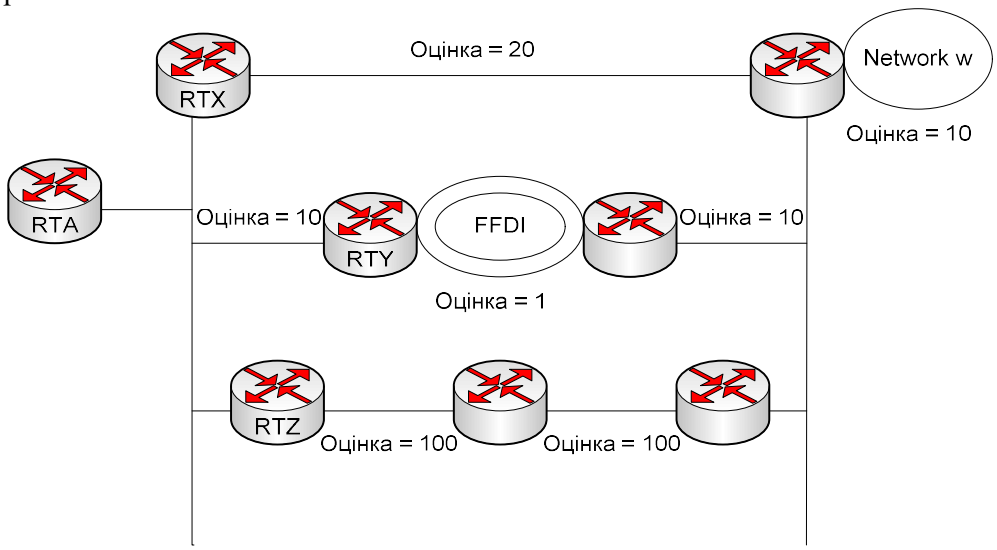


Рисунок 1.7 – Конвергенція протоколу EIGRP.

Таблиця 1.3 – Композитна метрика

Сусідній Пристрій	Обчислена оцінка маршрута (FD) до мережі Network w	Повідомлена відстань (RD) до мережі Network w
RTY	31	21
RTZ	230	220
RTX	40	30

Для вибору резервного маршруту, який би став первинним до Network w, маршрутизатор RTA виконує процес, що складається з трьох етапів.

Етап 1. Визначається, які сусідні пристрої мають відстань RD до Network w, меншу відстані FD для RTA до Network w. Це відстань FD дорівнює 31; RD для RTX дорівнює 30, а RD для RTZ дорівнює 220. Таким чином, RD для RTX менше поточного FD, у той час як RD для RTZ більше поточного FD.

Етап 2. Визначається мінімальна обчислена оцінка до Network w з доступних маршрутів, що залишились. Обчислена оцінка маршруту через RTX дорівнює 40, а через RTZ дорівнює 230. Таким чином, RTX забезпечує найменшу обчислену оцінку.

Етап 3. Визначається, чи задовольняють маршрутизатори критеріям першого та другого етапів. Маршрутизатор RTX задовольняє й тим, і іншим, тому він є резервним маршрутом.

Якщо маршрутизатор RTY стає непрацездатним, то маршрутизатор RTA негайно переходить до використання маршрутизатора RTX (резервного маршруту) для пересилання пакетів у Network w. Здатність здійснювати негайне переключення на резервний маршрут є основною передумовою дуже швидкої конвергенції протоколу EIGRP.

Чи може RTZ бути резервним маршрутом? Використовуючи вищенаведений триетапний процес, RTA з'ясовує, що RTZ анонсує оцінку 220, яка не менша, ніж відстань FD для RTA (дорівнює 31). Отже, RTZ не може бути резервним маршрутом (поки ще). Відстань FD може змінитись тільки під час переходу з активного у пасивний стан, а цей перехід поки ще не відбувся, тому ця відстань залишається рівною 31. До цього моменту, оскільки для Network w ще не відбувся перехід в активний стан, алгоритм DUAL здійснює процес, який називається локальним обчисленням.

Маршрутизатор RTA не може знайти резервних маршрутів, тому він в кінцевому підсумку переходить від пасивного до активного стану для мережі Network w і запитує свої сусідні пристрої про цю мережу. Даний процес називається обчисленням дифузії (diffusing computation). При переході мережі Network w у активний стан ця відстань FD перевстановлюється, що дозволяє RTA в остаточному підсумку прийняти RTZ як первинний маршрут до мережі Network w.

Тепер знову повернемось до прикладу КМ, наведеної на рис. 1.1,а. та ТМ маршрутизатора R2 (рис. 1.1,б.). Якщо вийде з ладу безпосередній зв'язок між R2 та R3 чи є резервний шлях в ТТ маршрутизатора R2 до мережі 192.168.1.0? Так, є, оскільки метрика маршрута від R1 до мережі 192.168.1.0 складає 2172416, що менше ніж метрика маршрута від R2 до мережі 192.168.1.0, яка дорівнює 3014400 (наявність резервного шляху можна проглянути за допомогою введення на R2 команди `show ip eigrp topology` – приклад 1.2.). При невиконанні даної умови резервного шляху від до мережі R2 до мережі 192.168.1.0 не було б і тоді, був би потрібен перерахунок. В даному ж випадку перерахунку не потрібно і при виході з ладу основного шляху зразу ж відбудеться використання резервного.

```
R2# show ip eigrp topology
 <частина результатів виведення опущена>
                . . .
P 192.168.1.0/24, 1 successors, FD is 3014400
   via 192.168.10.10 (3014400/28160) Serial0/0/1
   via 172.16.3.1 (41026560/2172416) Serial0/0/1
<частина результатів виведення опущена>
```

Приклад 1.2 – Основний та резервний шляхи до мережі 192.168.1.0

1.7 Конфігування протоколу EIGRP для IP

Незважаючи на складність алгоритму DUAL, конфігурування протоколу EIGRP виявляється відносно простою. Розглянемо процес конфігурування на невеликому прикладі (рис. 1.8).

Для того, щоб сконфігурувати EIGRP для протоколу IP слід виконати такі етапи.

Етап 1. Для включення протоколу EIGRP і визначення автономної системи треба виконати команду

`Router(config)# router eigrp autonomous-system-number`,

де параметр autonomous-system-number – це ідентифікатор АС, який вказує на всі маршрутизатори, що належать даній об'єднаній мережі. Це значення повинне відповідати усім маршрутизаторам в цій об'єднаній мережі. Наприклад, для маршрутизатора A дана команда може бути

`Router_A(config)# router eigrp 13`.

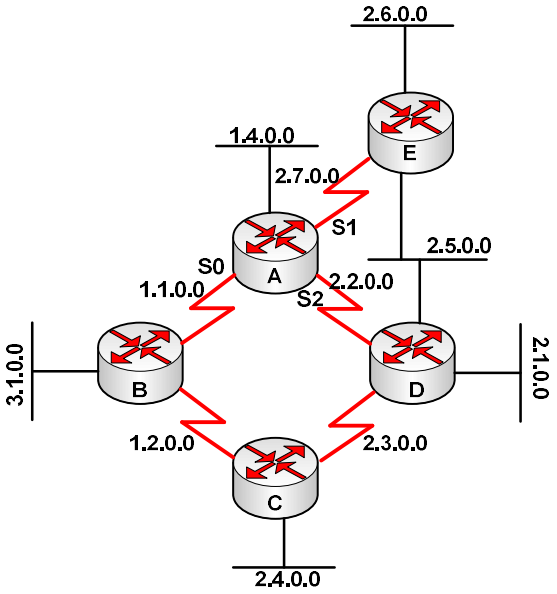


Рисунок 1.8 – Конфігурування EIGRP для протоколу IP

Етап 2. Вказати, які мережі належать до даної АС EIGRP на локальному маршрутизаторі за допомогою команди

`Router(config-router)# network network-number`,

де параметр network-number – це номер мережі. Дана команда задає які інтерфейси даного маршрутизатора беруть участь у роботі протоколу EIGRP і які мережі ним анонсуються. Номер мережі вказується з врахуванням класу IP-адреси. Наприклад, мережі 2.2.0.0 і 2.7.0.0 вводяться за допомогою команди `Router_A(config-router)# network 2.0.0.0`, оскільки вони є підмережами мережі 2.0.0.0.

Команда network конфігурує тільки приєднані мережі. Наприклад, мережа 3.1.0.0 не приєднана безпосередньо до маршрутизатора A. Отже вона не є частиною конфігурації маршрутизатора A.

Якщо треба вказати для протоколу EIGRP лише окремі підмережі, варто скористатись командою

`Router(config-router)# network network-number wildcard mask`,

де wildcard mask – інвертована маска, тобто 32-бітне число яке можна отримати шляхом інвертування маски підмережі. Біти інвертованої маски вказують будуть чи не будуть перевірятись відповідні біти IP-адреси. Там, де біти інвертованої маски нульові – відповідний біт IP-адреси повинен бути перевірений, а де одиничні – ні. Наприклад, якщо для протоколу EIGRP треба вказати тільки підмережу 2.2.0.0 слід ввести команду `Router_A(config-router)# network 2.2.0.0 0.0.255.255`.

Доцільно зауважити, що ряд ОС дозволяють замість інвертованої маски вводити звичайну маску підмережі. Проте, перш ніж використовувати таку можливість, слід дізнатись, чи підтримує це дана версія ОС.

Етап 3. Під час конфігурування послідовних каналів, що використовують протокол EIGRP важливо задати смугу пропускання на даному інтерфейсі. Якщо вона для таких інтерфейсів не змінена, то протокол EIGRP приймає для смуги пропускання значення за замовчанням (замість справжньої ширини смуги пропускання). Якщо канал має меншу швидкість, то маршрутизатор може бути не в змозі виконати конвергенцію, або може відбутись втрата змін маршрутизації, або обрано неоптимальний маршрут. Значення смуги пропускання конфігурується за командою

`Router(config-if)# bandwidth kilobits`.

Команда для завдання смуги пропускання є єдиною, яка використовується в процесі маршрутизації і повинна бути встановлена відповідності до швидкості каналу для даного інтерфейсу.

Етап 4. Рекомендується також додавати в конфігурацію кожного маршрутизатора E1GRP команду

`Router(config-if)# eigrp log-neighbor-changes`.

Ця команда дозволяє записати в системний журнал зміни в станах суміжності (сусідніх пристроїв) для аналізу стійкості системи маршрутизації й допомагає виявляти проблеми, що виникають.

Конфігування смуги пропускання у мережах NBMA

При проектуванні протоколу EIGRP у середовищі нешироковомовної мережі множинного доступу (nonbroadcasl multiaccess – NBMA), такий як мережа Frame Relay, необхідно дотримуватися таких правил:

- швидкість передачі даних протоколу EIGRP не повинна перевищувати узгодженої швидкості передачі інформації (committed information rate – CIR віртуального каналу (virtual circuit –VC);
- агрегований (сукупний) обсяг даних протоколу EIGRP no усім віртуальним каналам не повинен перевищувати швидкість каналу на інтерфейсі;
- смуга пропускання, виділена протоколу EIGRP на кожному каналі VC повинна бути однаковою в обох напрямках.

При правильному розумінні цих правил і виконання їх протокол E1GRP ефективно працює в середовищі розподіленої мережі WAN. Якщо при конфігурування протоколу EIGRP у мережі WAN не вжито відповідних заходів, то потоки даних EIGRP можуть викликати переповнення.

Конфігурування смуги пропускання в багатоточковій мережі

Завдання під час конфігування команди bandwidth у середовищі NBMA залежить від того, як спроектовані віртуальні канати VC.

Якщо у багато точковій конфігурації послідовний канал має багато каналів VC і усі ці канали рівномірно спільно використовують смугу пропускання, то в команді bandwidth повинна бути задана смуга пропускання, яка дорівнює сумі всіх швидкостей CIR. Наприклад, у мережі на рис. 1.9 швидкість CIR кожного каналу VC дорівнює 56 Кбіт/с. Оскільки є чотири канали VC, смуга пропускання повинна бути встановлена рівною 224 (4·56).

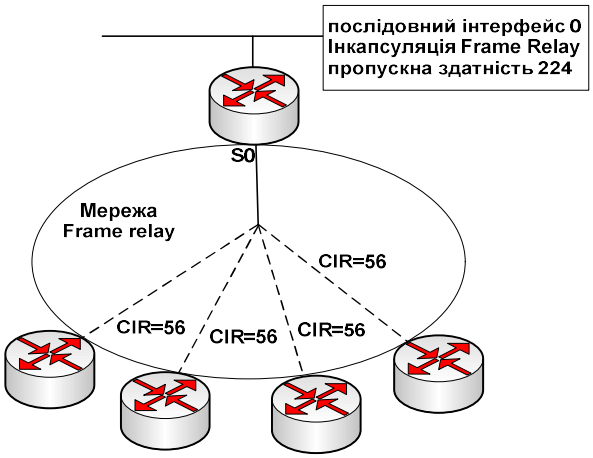


Рисунок 1.9 – Конфігурування EIGRP у багатоточковій мережі WAN

Конфігурування смуги пропускання в гібридній багатоточковій мережі

Якщо у багатоточковій мережі канали VC мають різні швидкості передавання, то потрібно дещо складніше конфігурування. При цьому можуть бути застосовані два нижченаведені основні підходи.

1. *Вибрати найменшу для всіх каналів швидкість CIR і помножити її на кількість віртуальних каналів* (рис. 1.10). Такий підхід застосований до фізичного інтерфейсу. Його недолік полягає в тому, що канали з великою смугою пропускання можуть виявитися недозавантаженими.

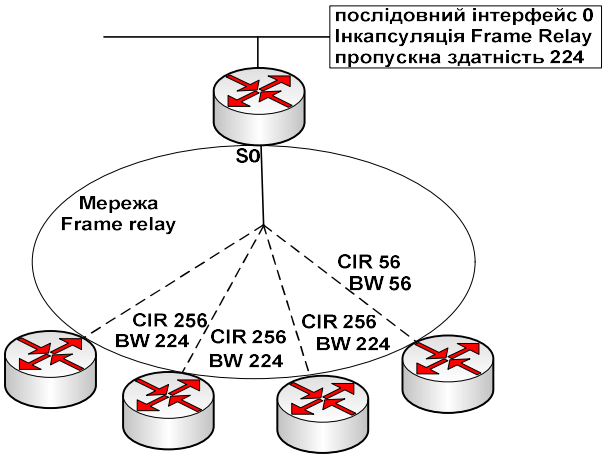


Рисунок 1.10 – Конфігурування EIGRP у багатоточковій гібридній мережі WAN

2. *Використання підінтерфейсів*. Команда bandwidth може бути сконфігурована на кожному під інтерфейсі, що дозволяє використовувати різні швидкості на кожному каналі VC. В цьому випадку підінтерфейси конфігуруються для каналів з різними швидкостями CIR. Канали, що мають одну й ту ж сконфігуровану швидкість CIR представляються як єдиний пі-дінтерфейс зі смугою пропускання, що відповідає сукупної швидкості CIR всіх каналів. На рис. 1.11 три віртуальних канали VC мають однакову CIR, що дорівнює 256 Кбіт/с. Вони групуються разом як один багатоточковий послідовний інтерфейс serial 0.1. Єдиний канал VC, що залишається, має меншу

CIR (яка дорівнює 56), може бути визначений як послідовний під-інтерфейс типу „точка-точка” – serial 0.2.

Використання команди ip bandwidth-percent

Команда `ip bandwidth-percent` задає у відсотковому відношенні частина смуги пропускання, яку протокол EIGRP може використовувати на деякому інтерфейсі. За замовчанням протокол EIGRP може використовувати до 50% смуги пропускання інтерфейсу для обміну інформацією маршрутизації. При обчисленні цієї процентної частини команда `ip bandwidth-percent` використовує значення, встановлене командою `bandwidth`. Команду `ip bandwidth-percent` слід використовувати в тих випадках, коли встановлена для каналу смуга пропускання не відповідає його справжній швидкості. Значення смуги пропускання може бути штучно занижено з різних причинах, зокрема, для керування метрикою маршрутизації або для того, щоб відрегулювати надлишкове навантаження у багатоточковій конфігурації протоколу Frame Relay. Незалежно від причини заниження, треба сконфігурувати EIGRP так, щоб замінити штучно занижену смугу пропускання на більш високе значення за допомогою команди ip bandwidth-percent. У деяких випадках значення, що задається цією командою, може навіть перевищувати 100% .

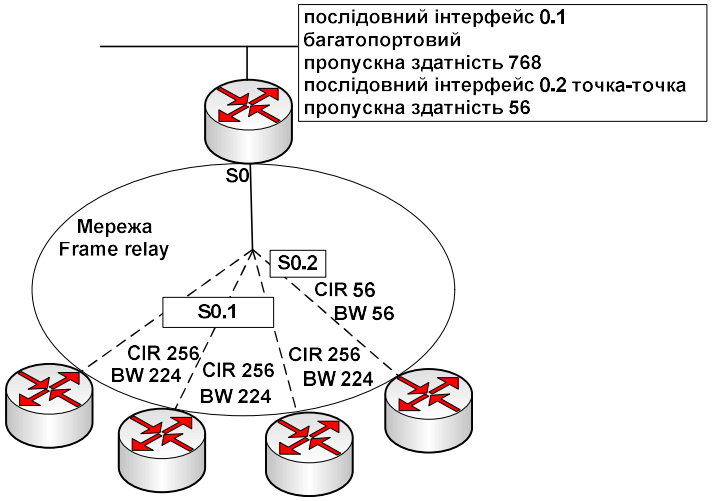


Рисунок 1.11 – Конфігурування EIGRP у багатоточковій гібридній мережі WAN (кращий варіант)

Наприклад, припустимо, що реальна смуга пропускання послідовного каналу маршрутизатора дорівнює 64 Кбіт/с, однак її значення штучно занижене до 32 Кбит/с. На рис. 1.12 показано як слід змінити функціонування протоколу EIGRP так, щоб він обмежував обсяг потоків даних протоколу маршрутизації реальною смугою пропускання послідовного інтерфейсу. У наведеному прикладі конфігурації для процеса EIGRP, який функціонує для автономної системи 24, смуга пропускання у відсотках для послідовного інтерфейсу serial 0 встановлюється рівною 100%. Оскільки 100% від 32 Кбіт/с дорівнює 32 Кбіт/с, протоколу EIGRP надається можливість використовувати половину реальної смуги пропускання, яка дорівнює 64 Кбіт/с.

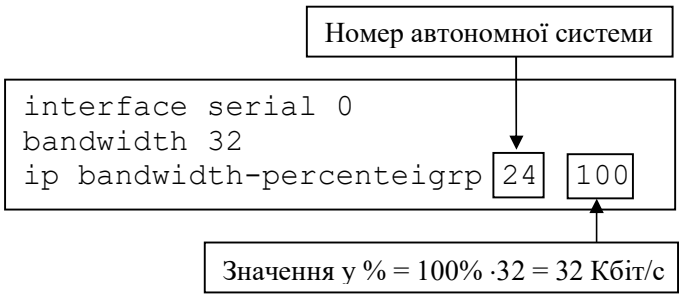


Рисунок 1.12 – Застосування команди ip bandwidth-percent для EIGRP.

Конфігурування узагальнення маршрутів протоколу EIGRP

Протокол EIGRP автоматично узагальнює маршрути на границі мережі, що використовує IP-адреси з класами (тобто на границі мережі, у якій мережева адреса містить у собі клас адреси). Це означає, що, незважаючи на те, що маршрутизатор RTC під’єднаний тільки до під мережі 2.1.1.0, він об’являє, що під’єднаний до всієї мережі 2.0.0.0 класу А. У більшості випадків автоматичне узагальнення корисно, оскільки дозволяє зробити ТМ максимально компактними (рис. 1.13).

Однак за деяких обставин автоматичне узагальнення може виявитись небажаним. Якщо в

Рисунок 1.13 – Автоматичне узагальнення маршрутів в EIGRP

мережі є підмережі, які не є безперервними (як, наприклад, на рис. 1.14), то для правильної роботи механізму маршрутизації автоматичне узагальнення необхідно відключити (інакше маршрутизатор RTD не прийматиме маршута до мережі 2.0.0.0/8, що під’єднана до RTC, оскільки він сам безпосередньо під’єднаний до мережі 2.0.0.0/8). Для такого відключення використовується команда `Router(config-router)#no auto-summary`.

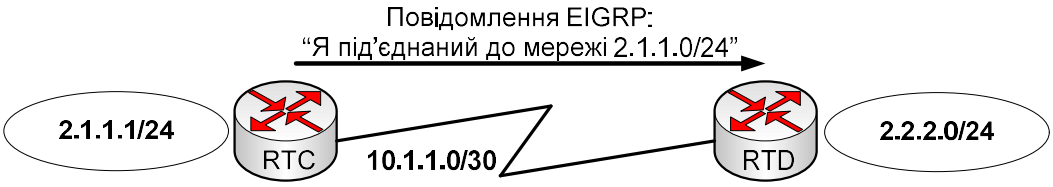


Рисунок 1.14 – Автоматичне узагальнення маршрутів протоколу EIGRP у мережі з розривами

При використанні протоколу EIGRP можна вручну сконфігурувати префікс, який буде використовуватись як узагальнена адреса. Ручне конфігуруванн узагальнення маршрутів здійснюється окремо для кожного інтерфейсу, тому першим повинен бути вбраний інтерфейс, що розповсюджує узагальнення маршрутів. Після цього узагальнена адреса може бути визначена за допомогою команди

```
Router(config-if)#ip summary-address eigrp autonomous-
system-number ip-address mask administrative-distance.
```

Узагальнені маршрути протоколу EIGRP за замовчанням мають адміністративну відстань, що дорівнює 5. Однак це значення може бути змінене під час конфігурування на будь-яке значення від 1 до 255.

Маршрутизатор RTC, наведений на рис. 1.14, може бути сконфігурований з використанням команд, наведених у прикладі 1.3.

```
RTC(config)# router eigrp 9
RTC(config-router)#no auto-summary
RTC(config-router)#exit
RTC(config)#interface serial0
RTC(config-if)#ip summary-address eigrp 9 2.1.0.0 255.255.0.0
```

Приклад 1.3 – Ручне узагальнення маршрутів

В результаті виконання команд цього прикладу, RTC додасть до таблиці маршрут `D 2.1.0.0/16 is a summary, 00:00:22, Null0`. Узагальнений маршрут має як джерело не реальний інтерфейс, а Null0, оскільки цей маршрут використовується тільки для цілей анонсування і не представляє маршруту, який маршрутизатор RTC може обрати для досягнення цієї мережі. В RTC цей маршрут має адміністративну відстань, яка дорівнює 5.

Для маршрутизатора RTD на рис. 1.13. узагальнення маршрутів не має значення, однак він приймає цей маршрут і призначає йому адміністративну відстань „нормального” маршруту EIGRP (стандартно 90), У конфігурації для маршрутизатора RTC автоматичне узагальнення маршрутів

відключено командою `no auto-summary`. Якби воно відключено не було, то маршрутизатор RTD отримав би два маршрути: сконфігурований вручну узагальнена адреса (2.1.0.0/16) і призначений автоматично, що використовує класи адреса (2.0.0.0/8). У більшості випадків під час ручного узагальнення слід використовувати команду `no auto-summary`.

Конфігурування аутентифікації у протоколі EIGRP

Для підвищення рівня безпеки протоколу EIGRP на маршрутизаторах слід настроїти аутентифікацію. Така настройка складається з двох кроків.

1. Створити ключову послідовність (key chain), яку будуть використовувати усі маршрутизатори Вашої мережі за допомогою команд, наведених у перших трьох рядках прикладу 1.4. Ці команди створюють ключ, що має ім'я MY_KEY, задають номер ключа (1) та значення рядка ключа (CISCO).
2. Дозволити антентифікацію за алгоритмом MD5 на відповідному інтерфейсі (інтерфейсах) маршрутизатора (останні три рядки прикладу 1.4).
3.

```
Router(config)# key chain MY_KEY
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string CISCO
Router(config-keychain-key)# exit
Router(config-keychain)# exit
Router(config)# interface serial0/0/0
Router(config-if)# ip autentification mode eigrp 1 md5
Router(config-if)# ip autentification key-chain eigrp 1 MY_KEY
```

Приклад 1.4 – Настроювання аутентифікації протоколу EIGRP

1.8 Тестування базової конфігурації протоколу EIGRP

Основні варіанти команди show, що можуть бути використані для тестування роботи протоколу EIGRP зі стислими описами їх функцій наведені у таблиці 1.4.

Функція IOS Cisco debug також надає корисні команди моніторингу протоколу EIGRP (табл. 1.5).

Таблиця 1.4 – Основні команди Show протоколу EIGRP

Команда	Опис
`show ip eigrp neighbors [type number] [details]`	Відображає таблицю сусідніх пристроїв протоколу EIGRP. Опції type і number використовуються для вказання інтерфейсу. Ключове слово details розширює виведення.
`show ip eigrp interfaces [type number] [as-number] [details]`	Відображає інформацію протоколу EIGRP для кожного інтерфейсу. Необов'язкові ключові слова обмежують виведення конкретним інтерфейсом або автономною системою. Ключове слово details розширює виведення.
`show ip eigrp topology [as-number]|[[ip-address] mask]`	Відображає всі допустимі резервні маршрути ТТ протоколу EIGRP. Необов'язкові ключові слова можуть використовуватись для фільтрації виведення на основі номера автономної системи або конкретної мережевої адреси.
`show ip eigrp topology [active|pending|zero-successors]`	Залежно від використаного ключового слова відображає всі маршрути у ТТ, які є активними, готуються до перерахування, або не мають первинних маршрутів.
`show ip eigrp topology all-links`	Відображає не тільки резервні маршрути, а й усі маршрути топології мережі протоколу EIGRP.
`Show ip eigrp traffic [as-number]`	Відображає число відправлених і отриманих пакетів протоколу EIGRP. Виведення команди може бути відфільтровано шляхом задання необов'язкового номера автономної системи.

Таблиця 1.5 – Основні команди відлагодження протоколу EIGRP

Команда	Опис
`debug eigrp fsm`	Дозволяє спостерігати роботу резервного маршруту протоколу EIGRP і перевірити, що процес маршрутизації встановлює і вилучає поновлення маршрутів.
`debug eigrp packet`	Відображає передавання і отримання пакетів протоколу EIGRP. Цими пакетами можуть бути пакети вітання, поновлення маршрутів, запиту або відповіді на запит. У виведенні відображаються послідовні номери і номери підтверджень, використовувані алгоритмом надійного транспортування протоколу EIGRP.

ЗАВДАННЯ

1. a. Настройте на маршрутизатора R2 – R6 мережі, наведеної на рис. 1.15 протокол EIGRP, попередньо виконавши визначення IP-адрес для кожного її сегменту згідно даних, наведених у табл. 1.6 (маски підмереж повинні бути оптимальними). При цьому для мереж Net 1 – Net 7 використайте IP-адреси мережі 172.16.0.0/16, для мереж Net 8 – Net 11 – 10.0.0.0/8, а для Net 12, Net 13 – 202.180.4.0/24. Також врахуйте, що:

- маршрутизатор R2 повинен анонсувати лише мережі Net 8 – Net 11;
- на маршрутизаторі R2 повинен бути прописаний шлях за замовчанням до маршрутизатора R1;
- на маршрутизаторі R2 повинен бути прописаний статичний маршрут до Loopback 1, що піднятий на маршрутизаторі R7. Адреса для Loopback 1: 192.168.3.15/24.

Поясніть, як буде працювати алгоритм EIGRP у нашій мережі, якщо на кожному EIGRP-маршрутизаторі виконати команду: 1) auto-summary; 2) no auto-summary.

b. Настройте аутентифікацію на на всіх EIGRP-маршрутизаторах.

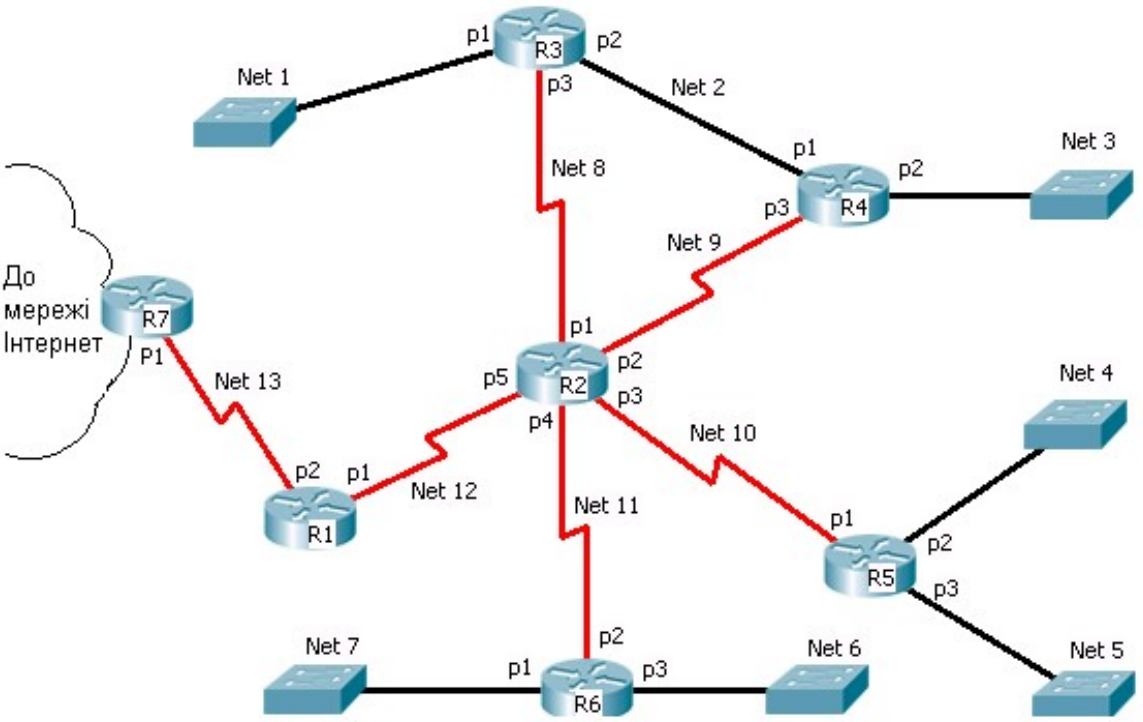


Рисунок 1.15 – Комп'ютерна мережа до завдання № 1

Таблиця 1.6 – Варіанти до завдання №1

№ варіанта	Кількість вузлів у мережах						
	Net 1	Net 2	Net 3	Net 4	Net 5	Net 6	Net 7
1	17	70	28	37	50	4	10
2	12	37	16	24	37	64	125
3	17	40	100	50	60	4	10
4	70	24	70	28	4	20	8
5	32	50	5	16	64	128	6
6	27	28	8	100	4	30	16
7	30	16	14	70	20	12	14
8	9	100	37	5	33	15	36
9	20	70	40	8	30	30	264
10	23	5	4	14	12	10	35
11	15	100	14	37	15	23	78
12	10	70	37	40	30	17	70
13	200	5	24	150	28	12	100
14	128	8	50	256	16	17	60
15	264	14	28	200	100	70	12
16	80	70	16	64	60	10	130
17	20	28	23	58	10	18	128
18	10	16	24	30	54	12	50
19	10	100	50	13	40	17	256
20	6	70	28	14	64	70	120
21	14	5	16	14	30	32	40
22	10	8	100	13	40	27	20
23	14	14	70	20	70	30	28
24	5	37	5	8	32	9	16
25	4	40	8	54	27	20	100
26	16	24	14	2	30	23	60
27	32	50	37	58	10	15	128
28	2	28	40	55	33	10	57
29	10	16	24	4	45	37	115
30	23	100	50	16	2	60	128

2. Вкажіть оптимальний маршрут для EIGRP з т. зору RS до мережі DN (рис. 1.15). Обчисліть значення його метрики. Варіанти завдань наведено у табл. 1.7. Час затримки каналів зв'язку, залежно від їх пропускної спроможності наведено у табл. 1.10.

Таблиця 1.7 – Варіанти до завдання № 2

№ вар.	RS	DN	№ вавріанта з		№ вар.	RS	DN	№ вавріанта з	
			табл. 1.8	табл. 1.9				табл. 1.8	табл. 1.9
1	R1	Net 7	1	1	16	R1	Net 7	4	3
2	R1	Net 5	2	1	17	R1	Net 5	5	3
3	R1	Net 4	3	1	18	R1	Net 4	6	3
4	R1	Net 8	4	1	19	R1	Net 8	1	4
5	R2	Net 1	5	1	20	R2	Net 1	2	4
6	R2	Net 3	6	1	21	R2	Net 3	3	4
7	R2	Net 7	1	2	22	R2	Net 7	4	4
8	R2	Net 8	2	2	23	R2	Net 8	5	4
9	R2	Net 4	3	2	24	R2	Net 4	6	4
10	R2	Net 8	4	2	25	R2	Net 8	1	5
11	R3	Net 7	5	2	26	R3	Net 7	2	5
12	R3	Net 5	6	2	27	R3	Net 5	3	5
13	R7	Net 1	1	3	28	R7	Net 1	4	5
14	R7	Net 3	2	3	29	R7	Net 3	5	5
15	R7	Net 5	3	3	30	R7	Net 5	6	5

Таблиця 1.8 – Значення пропускної спроможності послідовних каналів.

№ варіанта	Значення пропускної спроможності мережі (Мбіт/с)				
	Net 10	Net 11	Net 12	Net 13	Net 14
1	64	1024	1024	64	256
2	128	256	1544	512	512
3	256	512	512	256	256
4	128	1024	64	1544	64
5	1024	1544	1024	1024	512
6	64	256	64	64	128

Таблиця 1.9 – Значення пропускної спроможності каналів LAN.

№	Значення пропускної спроможності мережі (Мбіт/с)								
вар.	Net 1	Net 2	Net 3	Net 4	Net 5	Net 6	Net 7	Net 8	Net 9
1	1000	10	100	10	10	100	100	100	1000
2	100	10	100	100	10	100	100	100	1000
3	100	100	100	1000	100	100	1000	100	1000
4	100	1000	10	100	1000	10	100	100	1000
5	100	100	100	100	100	100	100	10	1000

Таблиця 1.10 – Значення затримки каналів зв'язку

Значення пропускної спроможності (Кбіт/с)	Значення затримки (мкс)
64	20000
128	20000
256	20000
512	20000
1024	20000
1544	20000
10000	1000
100000	100
1000000	10

Контрольні запитання

1. Поясніть з якою метою використовується метрика маршрута і на основі яких параметрів вона обчислюється.
2. Поясніть що таке статична та динамічна маршрутизація.
3. Назвіть дві основні категорії алгоритмів динамічної маршрутизації. Наведіть приклади протоколів, що використовують дані алгоритми.
4. Поясніть різницю між внутрішніми і зовнішніми протоколами маршрутизації та наведіть приклади таких протоколів. Наведіть порівняльний аналіз цих видів маршрутизацій.
5. Наведіть порівняння протоколів динамічної маршрутизації.
6. Поясніть основні відмінності між алгоритмами маршрутизації DVA та LSA.
7. Наведіть команди настроювання статичного маршруту та маршруту за замовчанням.
8. Поясніть яку роль грає маршрут за замовчанням? В яких випадках він використовується?
9. Наведіть загальну характеристику протоколу EIGRP, а також його переваги та недоліки.
10. Наведіть загальну формулу обчислення метрики протоколу EIGRP. Порівняйте її з метриками протоколів RIP та OSPF.
11. Наведіть основну термінологію протоколу EIGRP.
12. Які три таблиці використовуються у протоколі EIGRP? Наведіть призначення цих таблиць.
13. Поясніть які маршрути є первинними а які резервними. Чи до кожного пункта призначення існують такі маршрути? Відповідь обгрунтуйте.
14. Наведіть основні технології протоколу EIGRP.
15. Стисло охарактеризуйте та наведіть приклад роботи алгоритму DUAL.
16. Поясніть як у протоколі EIGRP відбувається адаптування під зміни структури мережі.

17. Які типи пакетів протоколу EIGRP Ви знаєте? Поясніть призначення цих пакетів.
18. За рахунок чого час конвергенції для протоколу EIGRP достатньо малий?
19. Наведіть основні етапи конфігурування протоколу EIGRP з відповідними командами.
20. Поясніть як виконується конфігурування смуги пропускання в гібридній багато точковій мережі для протоколу EIGRP.
21. Поясніть як виконується автоматичне узагальнення маршрутів у протоколі EIGRP. Наведіть команду, яка дозволяє вимкнути та увімкнути таке узагальнення.
22. Наведіть команди конфігурування аутентифікації у протоколі EIGRP.
23. Наведіть кілька команд тестування базової конфігурації протоколу EIGRP з відповідними поясненнями.

Зміст звіту

1. Короткі теоретичні відомості.
2. Виконання варіанта завдання, що виданий викладачем. У звіті навести зокрема скріншоти таблиць маршрутизаторів
3. Висновки.