МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний технічний університет

«Харківський політехнічний інститут»

Навчально-науковий інститут комп’ютерного моделювання, прикладної фізики та математики

Кафедра динаміки та міцності машин

Звіт

про виконання

Комп’ютерного практикуму №6

по курсу «Комп’ютерної мережі"

з теми "Динамічна маршрутизація на протоколах RIP і OSPF"

Виконав:

студент групи ІКМ-220б

Пономаренко О.В.

Викладач:

доцент кафедри ДММ

Трубаєв О.І.

Харків 2022

**Завдання лабораторної роботи**

**Завдання №1.** Налаштування протоколу RIP версії 2 для мережі з 6 пристроїв

**Завдання №2.** Приклад конфігурування протоколу OSPF для 4-х пристроїв

**Завдання №3.** Налаштування маршрутизації по протоколу OSPF для 6 пристроїв

**Теоретичні відомості**

**Маршрутизація** – процес визначення в мережі найкращого шляху, по якому пакет може досягти адресата. Динамічна маршрутизація може бути здійснена з використанням одного і більше протоколів (RIP v2, OSPF та ін.).

**Динамічна маршрутизація** - вид маршрутизації, при якому таблиця маршрутизації заповнюється і оновлюється автоматично за допомогою одного або декількох протоколів маршрутизації (RIP, OSPF, EIGRP, BGP). Кожен протокол маршрутизації використовує свою систему оцінки маршрутів (метрику).

**Маршрут до мереж призначення будується на основі таких критеріїв:**

* кількість ретрансляційних переходів;
* пропускна здатність каналу зв'язку;
* затримки передачі даних та ін.

Маршрутизатори обмінюються один з одним інформацією про маршрути за допомогою службових пакетів по протоколу UDP. Такий обмін інформацією збільшує наявність додаткового трафіку в мережі і навантаження на цю мережу. Можлива також ситуація, при якій таблиці маршрутизації на роутерах не встигають узгоджуватися між собою, що може спричинити появу помилкових маршрутів і втрату даних.

**Протоколи маршрутизації діляться на три типи:**

* дистанційно векторні протоколи (RIP);
* протоколи з відстеженням стану каналів (OSPF);
* змішані протоколи (EIGRP)та ін.

***Протокол RIP***

**RIP** - протокол дистанційно-векторної маршрутизації, який використовує для знаходження оптимального шляху алгоритм Беллмана-Форда. Алгоритм маршрутизації RIP - один з найбільш простих протоколів маршрутизації. Кожні 30 секунд він передає в мережу свою таблицю маршрутизації. Основна відмінність протоколів в

тому, що RIPv2 (на відміну від RIPv1) може працювати по мультикасту, тобто розсилаючи на мультикаст адреси. Максимальна кількість "хопів" (кроків до місця призначення), розміщених в RIP1, дорівнює 15 (метрика 15). Обмеження в 15 хопів не дає застосувати RIP у великих мережах, тому протокол найбільш поширений в невеликих комп'ютерних мережах. Друга версія протоколу - протокол RIP2 було розроблено в 1994 році і є покращеною версією першого. У цьому протоколі підвищена безпека за рахунок введення додаткової маршрутної інформації. Принцип дистанційно-векторного протоколу: кожен маршрутизатор, який використовує протокол RIP періодично широкомовно розсилає своїм сусідам спеціальний пакет-вектор, що містить відстані (вимірюються в метриці) від даного маршрутизатора до всіх відомих йому мереж.

Маршрутизатор який отримав такий вектор, нарощує компоненти вектора на величину відстані від себе до даного сусіда і доповнює вектор інформацією про відомих безпосередньо йому самому мережах або мережах, про які йому повідомили інші маршрутизатори. Додатковий вектор маршрутизатор розсилає всім своїм сусідам.

Маршрутизатор обирає з декількох альтернативних маршрутів маршрут з найменшим значенням метрики, а маршрутизатор, який передав інформацію по такому маршруту позначається як наступний (next hop). Протокол непридатний для роботи в великих мережах, так як засмічує мережу інтенсивним трафіком, а вузли мережі оперують тільки векторами-відстаней, не маючі точної інформації про стан каналів і топології мережі. Сьогодні навіть в невеликих мережах протокол витісняється переважаючими його по можливостях протоколами EIGRP и OSPF.

***Протокол OSPF***

Алгоритм роботи протоколу динамічної маршрутизації OSPF заснований на використанні усіма маршрутизаторами єдиної бази даних, яка описує, з якими мережами пов'язаний кожен маршрутизатор. Описуючи кожен зв'язок, маршрутизатори пов'язують з нею метрику - значення, що характеризує "якість" каналу зв'язку. Це дозволяє маршрутизаторам OSPF (на відміну від RIP, де всі канали рівнозначні) враховувати реальну пропускну здатність каналу і виявляти найкращі маршрути. Важливою особливістю протоколу OSPF є те, що використовується групова, а не широкомовна розсилка (як в RIP), тобто, навантаження каналів менше.

**OSPF (Open Shortest Path First)** - протокол динамічної маршрутизації, заснований на технології відстеження стану каналу link-state (LSA). Заснований на алгоритмі для пошуку найкоротшого шляху. Відстеження стану каналу вимагає відправки оголошень про стан каналу (LSA) на активні інтерфейси всіх доступних маршрутизаторів зони. У цих оголошеннях міститься опис усіх каналів маршрутизатора і вартість кожного каналу.

LSA повідомлення відправляються, тільки якщо відбулися які-небудь зміни в мережі, але раз в 30 хвилин LSA повідомлення відправляються в примусовому порядку. Протокол реалізує поділ автономної системи на зони (areas). Використання зон дозволяє знизити навантаження на мережу і процесори маршрутизаторів і зменшити розмір таблиць маршрутизації.

**Опис роботи протоколу**: усі маршрутизатори обмінюються спеціаль-

ними Hello-пакетами через всі інтерфейси, на яких активований протокол OSPF. Таким чином, визначаються маршрутизатори-сусіди, що розділяють загальний канал передачі даних. Надалі hello-пакети надсилаються з інтервалом раз в 30 секунд. Маршрутизатори намагаються перейти в стан сусідства зі своїми сусідами. Перехід в даний стан визначається типом маршрутизаторів і типом мережі, по якій відбувається обмін hello-пакетами, за зонною ознакою.

Пара маршрутизаторів в стані сусідства синхронізує між собою базу даних стану каналів. Кожен маршрутизатор посилає оголошення про стан каналу своїм сусідам, а кожен який отримав таке оголошення записує інформацію в базу даних стану каналів і розсилає копію оголошення іншим своїм сусідам.

При розсилці оголошень по зоні, всі маршрутизатори будують ідентичну базу даних стану каналів. Кожен маршрутизатор використовує алгоритм SPF для обчислення графа (дерева найкоротшого шляху) без петель. Кожен маршрутизатор будує власну маршрутизацію, грунтуючись на побудованому дереві найкоротшого шляху.

***Пряма і зворотна маска***

В обладнанні Cisco іноді доводиться використовувати зворотний маску, тобто не звичну 255.255.255.0 (**Subnet mask - пряма маска**), а 0.0.0.255 (**Wildcard mask - зворотна маска**). Зворотна маска використовується в листах допуску (access list) і при описі мереж в протоколі OSPF. Пряма маска використовується у всіх інших випадках.

Відмінність масок полягає також в тому, що пряма маска оперує мережами, а зворотна - хостами. За допомогою зворотної маски можна, наприклад, виділити в усіх підмережах хости з конкретною адресою і дозволити їм доступ в Інтернет. Так, як найчастіше за все в локальних мережах використовують адреси типу 192.168.1.0 з маскою 255.255.255.0, то найпоширеніша Wildcard mask (шаблонна маска або зворотна маска, або інверсна маска) - маска 0.0.0.255. **Шаблонна маска (wildcard mask)** - маска, яка вказує на кількість хостів мережі.

Є доповненням для маски підмережі. Обчислюється за формулою для кожного з октетів маски підмережі як 255-маска\_підмережі. Наприклад, для мережі 192.168.1.0 і маскою підмережі 255.255.255.242 шаблонна маска буде виглядати як 0.0.0.13. Шаблонна маска використовується в налаштуванні деяких протоколів маршрутизації, а також є зручним параметром обмежень в списках доступу. [1]

**Loopback**, або **«внутрішня петля»**, відноситься до маршрутизації електронних сигналів, цифрових потоків даних або інших рухомих сутностей назад до джерела без спеціального оброблення чи модифікування. Це в першу чергу засіб тестування передавання чи транспортної інфраструктури.

Існує багато прикладних застосувань. Це може бути канал зв'язку лише з однієї комунікаційної кінцевої точки. Будь-яке повідомлення, передане по такому [каналу](https://uk.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB_%D0%B7%D0%B2%27%D1%8F%D0%B7%D0%BA%D1%83), відразу отримує лише той самий канал. У телекомунікаціях, пристрої «внутрішньої петлі» виконують передавальні тести ліній доступу з [комутаційного центру](https://uk.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D1%87%D0%BD%D0%B0_%D1%82%D0%B5%D0%BB%D0%B5%D1%84%D0%BE%D0%BD%D0%BD%D0%B0_%D1%81%D1%82%D0%B0%D0%BD%D1%86%D1%96%D1%8F" \o "Автоматична телефонна станція), що, як правило, не потребує підтримки персоналу з боку обслуговуваного терміналу. На основі петлі існує метод тестування між станціями, не обов'язково сусідніми, де дві лінії використовуються, — тест проводять на одній станції, а дві лінії з'єднані між собою на дальній станції. [Патч-корд](https://uk.wikipedia.org/wiki/%D0%9F%D0%B0%D1%82%D1%87-%D0%BA%D0%BE%D1%80%D0%B4" \o "Патч-корд) може також виконувати функції «внутрішньої петлі».

У системі (як-от [модем](https://uk.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BC)), яка задіює двоспрямоване аналогово-цифрове перетворення, розрізняють **аналогову «внутрішню петлю»**, де аналоговий сигнал повертається назад безпосередньо, та **цифрову «внутрішню петлю»**, де сигнал обробляється в цифровій формі перш, ніж повторно перетворюється на аналоговий сигнал і повертається до джерела. [2]

**Хід роботи**

**Завдання №1.**

Створюємо та налаштовуємо мережу по прикладу з лабораторної роботи (рис. 1)

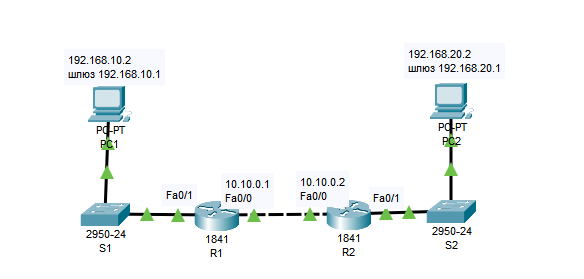


Рисунок 1 - Мережа завдання 1

Для початку налаштуємо ip адреси наших роутер використовуючи вже відомі нам команди з 5 лабороторної роботи (рис. 2)

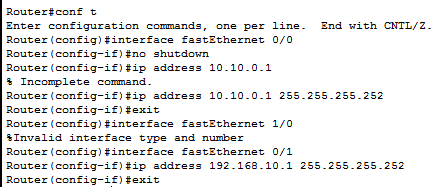


Рисунок 2 – встановлення ip адрес для першого роутера

Далі після того як ми зробили вище вказані маніпуляції з двома роутерами нам потрібно налаштувати на них rip протоколи (рис. 3)

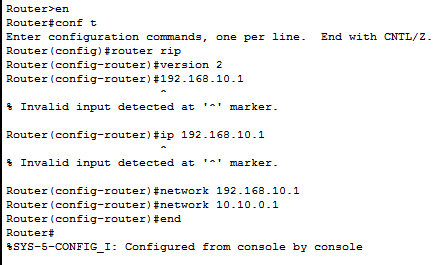


Рисунок 3 - налаштування RIP протоколу на першому роутері

Тепер якщо ми подивимося конфігурації RIP протоколів роутерів, то побачимо, що в нас з’явилися такі ip адреси мереж: 10.0.0.0, 192.168.10.0, 192.168.20.0 (рис. 4, 5)

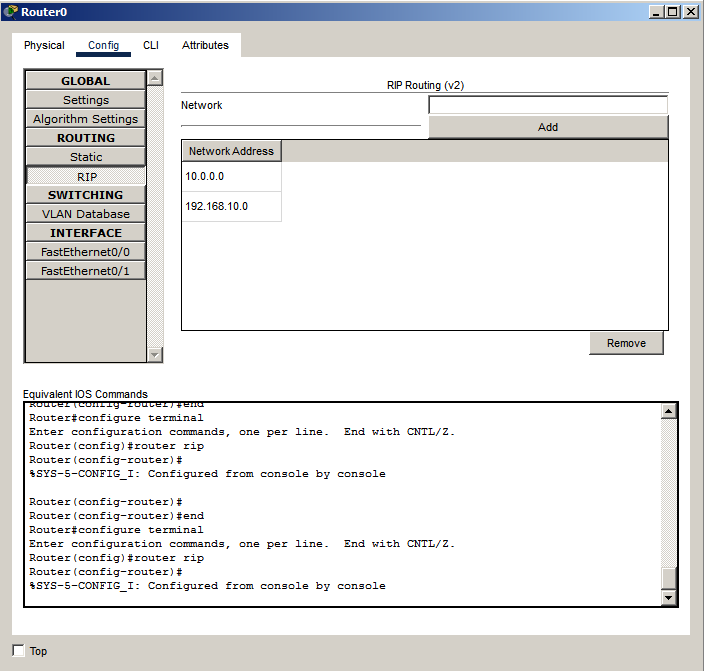


Рисунок 4 - конфігурація RIP на першому роутері

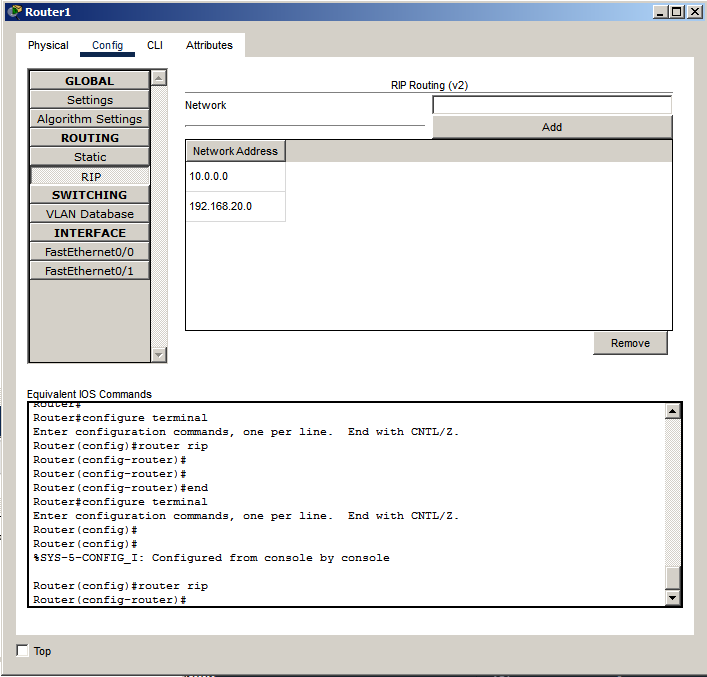


Рисунок 5 - конфігурація RIP на другому роутері

Також можемо перевірити RIP з’єднання за допомогою команди *show ip route rip* (рис. 6)

B:\KPI\computer-network-labs\lab6\task1\checking_R1_route_ip.PNG

Рисунок 6 - Таблиця маршрутизації R1

Також можна пінганути інший комп’ютер, щоб остаточно переконатися в тому, що вони можуть “*спілкуватися між собою”* (рис. 7)

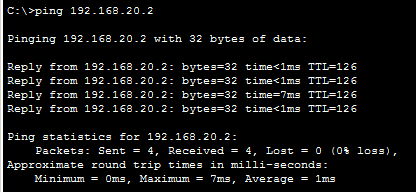


Рисунок 7 - пінгування другого комп'ютера

**Завдання №2.**

Створюємо та налаштовуємо мережу по прикладу з лабораторної роботи (рис. 8)

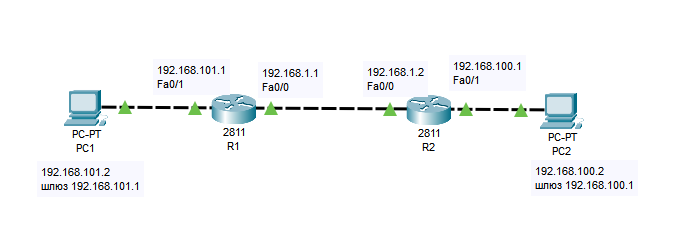


Рисунок 8 -Мережа завдання 2

**Налаштування роутерів**

Для початку ми встановимо ip адреси для портів роутерів, так само як зробили це в попередньому завданні.

Далі виконаємо конфігурування OSFP протоколу на обох роутерах (рис. 9, 10)

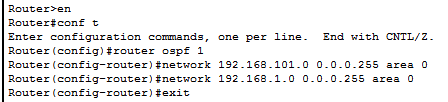


Рисунок 9 – конфігурація для першого роутера

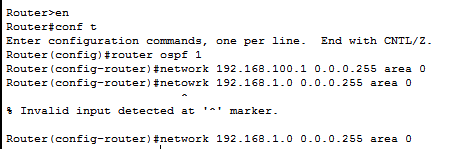


Рисунок 10 - конфігорування другого роутера

**Перевірка результату**

Зараз ми повинні перевірити доступність другого комп’ютера з першого виконавши пінгування (рис. 11)

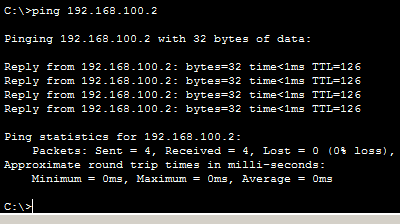


Рисунок 11 - пінгування другого комп'ютера

**Завдання №3.**

Створюємо та налаштовуємо мережу по прикладу з лабораторної роботи (рис. 12)

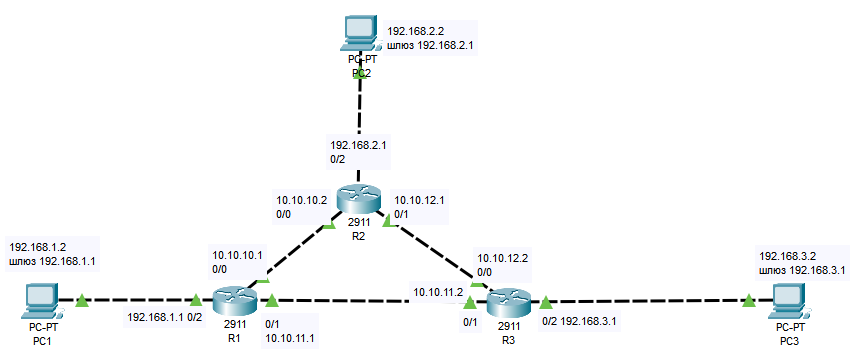


Рисунок 12 - Мережа завдання 3

Знову ж таки спочатку прописуємо ip адреси та маски підмереж всім хостам та перейдемо до налаштування самих роутерів.

Відкриємо перший роутер та налаштуємо на ньому loopback інтерфейс для прискорення пошуку шляху, реально ця адреса не існує (рис. 13)

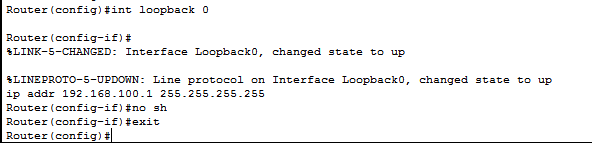


Рисунок 13 - налаштування loopback інтерфейсу для R1

Тепер коли ми це зробили, треба налаштувати сам OSPF протокол на першому роутері (рис. 14)

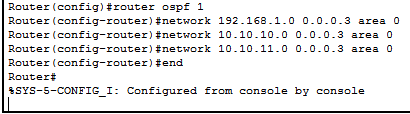


Рисунок 14 - налаштування OSPF протоколу на R1

Далі всі ті ж самі дії, що ми зробили на першому роутері, треба повторити на другому та третьому, змінюючи тільки ip адреси.

Коли ми це зробили ми можемо ввести команду *sh ip route* та побачити список знайдених мереж (рис. 15)

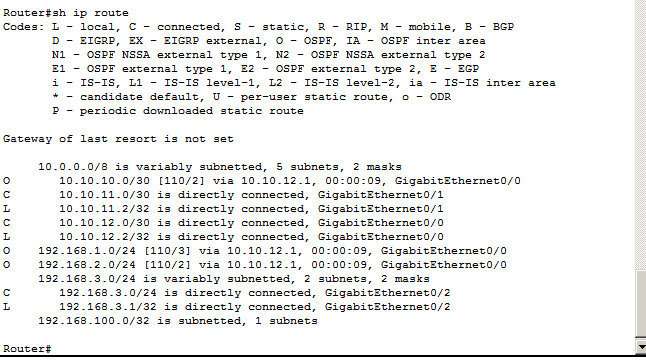


Рисунок 15 - виводимо список знайдених мереж

Після цього пінгуємо якийсь комп’ютер та впевнюємось, що все працює справно (рис. 16)

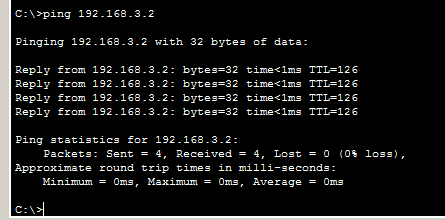


Рисунок 16 - пінгуємо третій комп'ютер

**Висновки**

Отже, виконуючи даний комп’ютерний практикум я навчився налаштовувати мережі таким чином, щоб була динамічна маршрутизація, використовуючи RIP та OSPF протоколи.

**Список джерел**

1. Комп’ютерний практикум № 6.
2. https://uk.wikipedia.org/wiki/Loopback