ПРОТОКОЛ IP.
СТАТИЧНА МАРШРУТИЗАЦІЯ
В IP-МЕРЕЖАХ

Навчальний посібник

Харків – 2017

Created by free version of DocuFreezer

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

ПРОТОКОЛ IP. СТАТИЧНА МАРШРУТИЗАЦІЯ В IP-МЕРЕЖАХ

Навчальний посібник

Харків – 2017

УДК 621.391(075.8)
ББК 32.81я73
П 775

Рекомендовано вченою радою Українського державного університету залізничного транспорту як навчальний посібник (витяг з протоколу № 6 від 13 вересня 2017 р.)

Рецензенти:

професори В. І. Барсов (НАУ «ХАІ»),
С. Г. Рассомахін (ХНУ ім. В. Н. Каразіна)

Авторський колектив:

Панченко С. В., Приходько С. І., Жученко О. С., Штомпель М. А.

П 775 Протокол IP: Статична маршрутизація в IP-мережах: Навч. посібник / С. В. Панченко, С. І. Приходько, О. С. Жученко та ін. - Харків: УкрДУЗТ, 2017. – 136 с., рис. 113, табл. 41.

ISBN 978-617-654-070-0

Навчальний матеріал, поданий у цьому навчальному посібнику, входить до відповідних підрозділів навчальних дисциплін «Телекомунікаційні та інформаційні мережі», «Телекомунікаційні та інформаційні мережі на залізничному транспорті», «Інтегральні цифрові мережі зв'язку», що викладаються на кафедрі «Транспортний зв'язок» Українського державного університету залізничного транспорту.

Навчальний посібник може бути використаний під час самостійної підготовки, при підготовці до певних контрольних заходів, у тому числі у формі тестового контролю, при виконанні контрольних, курсових і дипломних робіт (проектів), а також при викладанні окремих підрозділів інших навчальних дисциплін відповідно до навчальних програм. Крім теоретичного (лекційного) матеріалу, навчальний посібник містить рекомендації щодо виконання певних практичних завдань, у тому числі з застосуванням програмного середовища імітаційного моделювання, а також типові завдання для проведення тестового контролю знань, які можуть бути використані викладачем при розробленні комплексу питань для проведення поточного, модульного контролю та інших контрольних заходів.

Посібник призначений для студентів, які навчаються за денною, вечірньою, заочною (дистанційною), поєднаними формами навчання, і викладачів вищих навчальних закладів.

УДК 621.391(075.8)
ББК 32.81я73

ISBN 978-617-654-070-0

© Український державний університет залізничного транспорту, 2017.

Навчальний посібник

Панченко Сергій Володимирович,
Приходько Серій Іванович,
Жученко Олександр Сергійович
та ін.

ПРОТОКОЛ IP. СТАТИЧНА МАРШРУТИЗАЦІЯ В IP-МЕРЕЖАХ

Відповідальний за випуск Штомпель М. А.

Редактор Ібрагімова Н. В.

Підписано до друку 05.04.17 р.

Формат паперу 60х84 1/16. Папір писальний.

Умовн.-друк.арк. 9,0. Тираж 50. Замовлення №

Видавець та виготовлювач Українська державна академія залізничного транспорту,
61050, Харків-50, майдан Фейєрбаха, 7.
Свідоцтво суб'єкта видавничої справи ДК № 2874 від 12.06.2007 р.

Created by free version of DocuFreezer

ЗМІСТ

Вступ…… 5
1. Протокол IP…… 6
1.1. Формат IP-пакета…… 6
1.2. Фрагментація IP-пакетів…….. 9
1.3. Забезпечення якості обслуговування засобами протоколу IP……..... 15
2. Маршрутизація пакетів протоколу IP…….. 21
2.1. Загальні відомості про маршрутизацію пакетів протоколу IP……. 21
2.2. Приклад маршрутизації пакетів протоколу IP…… 24
2.3. Процедура пошуку маршруту в таблиці маршрутизації……. 29
2.4. Особливості таблиць маршрутизації маршрутизаторів Cisco…….. 31
3. Розроблення плану розподілу інформації для статичної маршрутизації в мережі на основі протоколу IP……. 34
3.1. Основні кроки розроблення плану розподілу інформації……... 34
3.2. Вихідні дані для розроблення плану розподілу інформації……... 35
3.3. Розбиття загального адресного простору IP-мережі на підмережі……... 36
3.4. Розподіл IP-адрес. Визначення мережевих параметрів обладнання…….. 40
3.5. Визначення метрик трактів……... 42
3.6. Утворення зваженого графа, відповідного. IP-мережі… 43
3.7. Визначення основних маршрутів…….. 44
3.8. Розроблення таблиць маршрутизації…… 58
3.9. Перевірка правильності розроблення плану розподілу інформації шляхом імітаційного моделювання в програмному середовищі Cisco Packet Tracer……..… 60
4. Основні команди командного рядка операційної системи Cisco IOS для конфігурування статичної маршрутизації…….. 66

5. Основи проведення дослідження статичної маршрутизації в IP-мережі у програмному середовищі Cisco Packet Tracer…….. 67
5.1. Створення імітаційної моделі IP-мережі та перевірка її роботи…….. 67
5.2. Дослідження імітаційної моделі IP-мережі в режимі візуального моделювання взаємодії мережевих компонентів та аналіз результатів моделювання……..... 79
5.2.1. Дослідження процесів передачі IP-пакета до порту маршрутизатора за участю протоколу ARP… 79
5.2.2. Дослідження маршутів передачі IP-пакетів……. 91
5.2.3. Дослідження альтернативних (резервних) маршутів передачі IP-пакетів…… 96
5.2.4. Дослідження маршутів передачі IP-пакетів за замовчуванням…….. 109
6. Варіанти завдань для розроблення плану розподілу інформації для статичної маршрутизації в мережі на основі протоколу IP…… 112
7. Типові завдання для проведення тестового контролю знань……. 122
Бібліографічний список……. 130
Додаток 1. Основні режими конфігурування пристроїв з операційною системою Cisco IOS…… 131
Додаток 2. Контекстна довідка в командному рядку операційної системи Cisco IOS……. 132
Додаток 3. Принципи визначення маршруту IP-пакета (команда tracert)……. 133
Додаток 4. Відповіді на тестові питання з розд. 7…….. 136

ВСТУП

На сьогодні в якості основного протоколу мережевого рівня використовується протокол IP (Internet Protocol, IP-протокол), який дозволяє створити єдину IP-мережу шляхом об'єднання окремих мереж (локальних) на основі різних технологій і протоколів фізичного й канального рівнів, за допомогою маршрутизаторів, що є вузлами IP-мережі та виконують маршрутизацію блоків протокольних даних IP-протоколу, які називають IP-пакетами.

У даному навчальному посібнику розглянуто формат IP-пакета і призначення його полів. Окрему увагу приділено таким властивостям протоколу IP, як фрагментація IP-пакетів і можливість забезпечення якості обслуговування на мережевому рівні шляхом урахування маршрутизаторами при обробці IP-пакетів їхніх відповідних службових полів. Докладно розглянуто принципи маршрутизації в мережах на основі протоколу IP, зокрема принципи статичної маршрутизації. Наводяться приклади маршрутизації в IP-мережі та принципи вибору маршруту маршрутизатором.

Навчальний посібник містить достатній обсяг теоретичних відомостей, необхідних у подальшому для вирішення практичних завдань.

Розділи навчального посібника, що містять варіанти завдань для розроблення плану розподілу інформації та рекомендації щодо проведення дослідження статичної маршрутизації в IP-мережі у програмному середовищі імітаційного моделювання, а також типові завдання для проведення тестового контролю знань, сприяють засвоєнню теоретичного матеріалу, дозволяють набути відповідні уміння і навички.

1. ПРОТОКОЛ IP

На сьогодні в якості основного протоколу мережевого рівня використовується протокол IP (Internet Protocol, IP-протокол), який дозволяє створити єдину IP-мережу шляхом об'єднання окремих (локальних) мереж, що використовують різні технології та протоколи на фізичному й канальному рівнях, за допомогою пристроїв третього рівня – маршрутизаторів і/або комутаторів третього рівня, що є вузлами IP-мережі, які виконують маршрутизацію блоків протокольних даних IP-протоколу − IP-пакетів.

Протокол IP здійснює передачу IP-пакетів без установлення з'єднання і є дейтаграмним протоколом, оскільки кожний IP-пакет обробляється у вузлах IP-мережі незалежно від інших пакетів. Протокол IP не забезпечує надійність доставки інформації, тому що він не має механізмів повторної передачі. IP-пакети можуть бути загублені, розмножені або отримані не в тому порядку, у якому вони були передані.

Важливою особливістю протоколу IP є можливість виконання динамічної фрагментації IP-пакетів (розбиття пакета на більш короткі пакети – фрагменти, які так само, як і вихідний пакет, мають власний заголовок і незалежно один від одного обробляються та передаються по мережі) вузлами IP-мережі при передачі даних між мережами з різними максимально припустимими значеннями довжин полів даних.

1.1. Формат IP-пакета

IP-пакет складається з заголовка та поля даних (рис. 1.1).

<table>
<tr><td>4 біти
Номер версії</td><td>4 біти
Довжина заголовка</td><td>8 бітів
Тип сервісу (ToS або DS)</td><td colspan="3">16 бітів
Загальна довжина</td></tr>
<tr><td colspan="3" rowspan="2">16 біт
Ідентифікатор пакета</td><td colspan="2">3 біти
Прапори</td><td rowspan="2">13 бітів
Зсув фрагменту</td></tr>
<tr><td>///</td><td>DF
MF</td></tr>
<tr><td colspan="2">8 бітів
Час життя</td><td>8 бітів
Протокол верхнього рівня</td><td colspan="3">16 бітів
Контрольна сума заголовка</td></tr>
<tr><td colspan="6">32 біти
IP-адреса джерела</td></tr>
<tr><td colspan="6">32 біти
IP-адреса призначення</td></tr>
<tr><td colspan="6">Параметри та вирівнювання</td></tr>
<tr><td colspan="6">Дані</td></tr>
</table>

Рис. 1.1. Формат пакета протоколу IP

Поле *номера версії* займає 4 бити й ідентифікує версію протоколу IP. Зараз скрізь використовується версія 4, хоча все частіше зустрічається і нова версія – 6.

Значення *довжини заголовка* IP-пакета також займає 4 біти й вимірюється в 32-бітових словах. Звичайно заголовок має довжину у 20 байтів (п'ять 32-бітових слів), але при додаванні деякої службової інформації це значення може бути збільшено за рахунок додаткових байтів у *полі параметрів*. Найбільша довжина заголовка становить 60 байтів.

Поле типу сервісу довжиною в один байт містить ознаки, які відображують вимоги до якості обслуговування пакета. Дане поле буде розглянуто окремо.

Поле *загальної довжини* займає 2 байти й характеризує загальну довжину пакета з урахуванням заголовка та поля даних. Максимальна довжина пакета обмежена розрядністю поля, що визначає цю величину, яка становить 65 535 байтів, але, як правило, настільки великі пакети не використовуються. При передачі по мережах різного типу довжина пакета вибирається з урахуванням максимальної довжини блока протокольних даних

(кадра) протоколу нижнього рівня, що несе IP-пакети. Якщо це кадри Ethernet, то вибираються пакети з максимальною довжиною 1500 байтів, що містяться в полі даних кадру Ethernet.

Ідентифікатор пакета займає 2 байти і використовується для розпізнавання пакетів, що утворювалися шляхом розподілу на частини (фрагментації) вихідного пакета. Усі частини (фрагменти) одного пакета повинні мати однакове значення цього поля.

Прапори займають 3 біти і містять ознаки, пов'язані з фрагментацією. Установлений в 1 біт DF (Do not Fragment − не фрагментувати) забороняє маршрутизатору фрагментувати даний пакет, а встановлений в 1 біт MF (More Fragments − більше фрагментів) говорить про те, що даний пакет є проміжним (не останнім) фрагментом. Біт, що залишився, − зарезервований.

Поле *зсуву фрагмента* займає 13 бітів і задає зсув у байтах поля даних цього фрагмента відносно початку поля даних вихідного нефрагментованого пакета. Використовується при збиранні/розбиранні фрагментів пакетів. Зсув має бути кратним 8 байтам.

Поле *часу життя* (Time To Live, TTL) займає один байт і використовується для задавання граничного строку, протягом якого пакет може переміщатися по мережі. Від значення часу життя, установленого джерелом пакета, віднімається одиниця щораз, як пакет проходить через маршрутизатор. Таким чином, час життя можна інтерпретувати як максимальну кількість транзитних вузлів, які дозволено пройти пакету. Якщо значення поля часу життя стає нульовим до того, як пакет досягає одержувача, пакет знищується.

Поле *протоколу верхнього рівня* займає один байт і містить ідентифікатор, що вказує, якому протоколу верхнього рівня належить інформація, розміщена в полі даних пакета. Наприклад, 6 означає, що в пакеті міститься повідомлення TCP, 17 − повідомлення UDP, 1 − повідомлення ICMP.

Контрольна сума заголовка займає 2 байти (16 бітів) і розраховується тільки за заголовком. Оскільки деякі поля заголовка змінюють своє значення в процесі передачі пакета по мережі (наприклад, поле часу життя), контрольна сума перевіряється й повторно розраховується на кожному

маршрутизаторі та кінцевому вузлі. Якщо контрольна сума неправильна, то пакет відкидається, як тільки виявляється помилка.

Поля IP-адреси відправника і одержувача мають однакову довжину − 32 біти.

Поле параметрів є необов'язковим і рідко використовується. Використовуючи поле параметрів, можна вказувати точний маршрут (здійснювати маршрутизацію від джерела), реєструвати прохідні пакетом маршрутизатори, поміщати дані системи безпеки або часові мітки. Оскільки кількість підполів у полі параметрів може бути довільною, то наприкінці заголовка має бути додано кілька нульових байтів для вирівнювання заголовка пакета по 32-бітній границі.

1.2 Фрагментація IP-пакетів

Протокол IP дозволяє забезпечити передачу даних між мережами з різними максимально припустимими значеннями довжин полів даних MTU (Maximum Transmission Unit − максимальна одиниця передачі) за рахунок розбиття пакета більшого розміру на більш короткі пакети – фрагменти, які так само, як і вихідний пакет, мають власний заголовок і незалежно один від одного обробляються й передаються по мережі.

Кінцеві вузли – відправники IP-пакетів, як правило, не використовують можливість фрагментації, оскільки задачу розбиття потоку байтів, формованого прикладним рівнем, на сегменти потрібного розміру виконують протоколи транспортного рівня (TCP, UDP).

Таким чином, фрагментація пакетів здійснюється, як правило, транзитними вузлами мережі – маршрутизаторами, комутаторами третього рівня у випадку, коли необхідно передати пакет з мережі з більшим значенням MTU у мережу з меншим значенням MTU. Зазначимо, що пакет може бути кілька разів піддаватися фрагментації яким-небудь із проміжних маршрутизаторів. Значення MTU різних технологій подано в табл. 1.1.

Таблиця 1.1

Значення MTU для різних технологій

Технологія	MTU, байт
DIX Ethernet	1500
Ethernet 802.3	1492
Token Ring (IBM, 16 Мбіт/с)	17 914
Token Ring (802.5, 4 Мбіт/с)	4464
FDDI	4352
X.25	576

Одержувач фрагмента використовує *ідентифікатор фрагмента* для того, щоб розпізнавати всі фрагменти одного пакета. При передачі пакета в полі ідентифікатора фрагмента встановлюється значення, яке має бути унікальним для даної пари відправника й одержувача протягом усього часу, поки даний пакет (або будь-який його фрагмент) може існувати в IP-мережі. Оскільки поле ідентифікатора допускає 65536 різних значень, часто ідентифікатори вибираються випадково, покладаючись на високу ймовірність того, що ідентифікатор виявиться унікальним протягом часу життя пакета.

Поле *зсуву фрагмента* надає одержувачеві пакета – кінцевому вузлу – інформацію про розміщення фрагмента у вихідному пакеті. Так, перший фрагмент буде мати в полі зсуву нульове значення. У пакеті, не розбитому на фрагменти, поле зсуву також має нульове значення. Зазначимо, що поле *зсуву фрагмента* має довжину тільки 13 бітів, що не дозволяє вказати в ньому значення більше $2^{13}-1$, тобто 8 191. При цьому довжина IP-пакета може мати значення аж до $2^{16}-1$, тобто 65 535 байтів. Із цієї причини зсув записується в поле *зсуву фрагмента* в кількості 8-байтових груп ($2^{16}/2^{13}=8$), а для одержання безпосереднього зсуву, вимірюваного в байтах, значення зсуву з поля зсуву фрагмента необхідно помножити на 8. Також це означає, що довжина всіх фрагментів, крім останнього, повинна бути кратною 8 байтам (і при цьому фрагмент повинен мати довжину менше, ніж значення MTU відповідної технології).

Прапор MF (More Fragments − більше фрагментів), установлений в одиницю, − ознака того, що фрагмент не є останнім. При передачі нефрагментованого пакета прапор MF установлюється в нуль.

Прапор DF (Do Not Fragment − не фрагментувати), установлений в одиницю, − ознака того, що даний пакет не підлягає фрагментації ні за яких умов. Якщо позначений у такий спосіб пакет не може дістатися одержувача без фрагментації, то такий пакет буде знищений.

Зазначимо, що процес фрагментації може змінити значення деяких полів заголовків IP у пакетах-фрагментах порівняно з заголовком IP вихідного пакета. Так, кожний фрагмент має власне значення контрольної суми заголовка, зсуву фрагмента й загальної довжини пакета. У всіх пакетах, крім останнього, прапор MF установлюється в одиницю, а в останньому фрагменті − у нуль.

Вміст поля даних кожного фрагмента формується в результаті поділу вмісту поля даних вихідного пакета. При цьому повинні бути виконано дві умови. По-перше, розмір фрагмента (заголовка в сумі з полем даних) не повинен перевищувати MTU технології нижчого рівня. По-друге, розмір поля даних кожного фрагмента, крім останнього, повинен бути кратним 8 байтам. Розмір останньої частини даних дорівнює отриманому залишку.

Збирання пакета з окремих фрагментів здійснюється тільки в кінцевому вузлі – вузлі призначення. Суть збирання полягає в розміщенні даних з кожного фрагмента в позицію, визначену зсувом, зазначеним у заголовку фрагмента. Ознакою закінчення збирання є відсутність незаповнених проміжків у полі даних і прибуття останнього фрагмента (з рівним нулю прапором MF). Якщо хоча б один фрагмент пакета буде загублений у мережі, відкинутий через наявність помилок у заголовку або ж минув час очікування пакета, то всі отримані раніше фрагменти вихідного пакета будуть відкинуті.

Розглянемо приклад вирішення завдання фрагментації IP-пакета. Нехай заголовок IP-пакета не містить поля з додатковими параметрами. Значення, записане в поле загальної довжини IP-пакета, становить 1520. Значення MTU (максимально допустиме значення довжини поля даних на канальному рівні), установлене на маршрутизаторі, становить 525.

1. Знайдемо довжину поля даних IP-пакета, враховуючи, що довжина заголовка пакета без додаткових параметрів і вирівнювання дорівнює 20 байтам (5 рядків по 4 байти):

довжина поля даних IP-пакета =

= загальна довжина IP-пакета − довжина заголовка IP-пакета =

= 1520 – 20 = 1500 байтів.

2. Враховуючи, що довжина поля даних фрагментів вихідного пакета, за винятком останнього, повинна бути кратна 8 байтам і, крім того, загальна довжина кожного фрагмента (з урахуванням довжини заголовка IP-пакета, яка становить 20 байтів) не повинна перевищувати значення MTU = 525, знайдемо один з варіантів, що задовольняє одночасно ці дві умови за такими формулами:

1) довжина полів даних усіх фрагментів, за винятком останнього, байт,

$$8 \cdot \left\lfloor \frac{\text{MTU - довжина заголовка IP - пакета}}{8} \right\rfloor,$$

де $\lfloor \bullet \rfloor$ − операція округлення до найближчого меншого цілого;

$$8 \cdot \left\lfloor \frac{525 - 20}{8} \right\rfloor = 504 \text{ байти};$$

2) кількість фрагментів

$$\text{кількість фрагментів} = \left\lceil \frac{\text{довжина поля даних IP - пакета}}{8 \cdot \left\lfloor \frac{\text{MTU - довжина заголовка IP - пакета}}{8} \right\rfloor} \right\rceil$$

де $\lceil \bullet \rceil$ − операція округлення до найближчого більшого цілого;

$$\text{кількість фрагментів} = \left\lceil \frac{1500}{8 \cdot \left\lfloor \frac{525 - 20}{8} \right\rfloor} \right\rceil = \left\lceil \frac{1500}{504} \right\rceil = 3;$$

3) довжина поля даних останнього фрагмента, байт,

довжина поля даних останнього фрагмента =

= довжина поля даних IP - пакета -

$$-\left(\text{кількість фрагментів} - 1\right)\cdot 8\cdot\left\lfloor\frac{\text{MTU} - \text{довжина заголовка IP - пакета}}{8}\right\rfloor,$$

$$\text{довжина поля даних останнього фрагмента} = 1500 - (3-1)\cdot 8\cdot\left\lfloor\frac{1520-20}{8}\right\rfloor =$$

$$= 1500 - 2\cdot 8\cdot 63 = 492 \text{ байти.}$$

Результати розрахунків параметрів фрагментів IP-пакета показано на рис. 1.2.

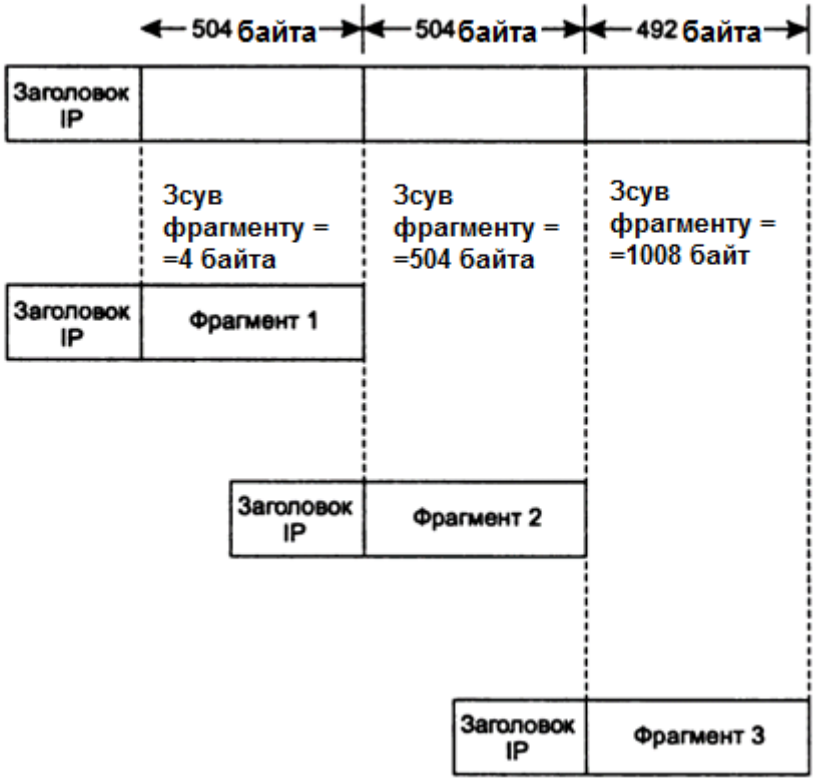


Рис. 1.2. Результати розрахунку параметрів фрагментів IP-пакета (приклад)

Кожний фрагмент забезпечується окремим заголовком протоколу IP. Поле ідентифікатора фрагмента повинне містити те значення, яке було у вихідному IP-пакеті (до фрагментації). Вміст цього поля ідентифікує фрагменти одного пакета. У табл. 1.2 показані прапори та значення зсуву фрагментів, установлені у відповідних полях фрагментів (зсув фрагментів визначається як

кількість 8-байтових груп, тому він знайдений як результат ділення зсуву в байтах на число 8, значення зсуву в першому фрагменті завжди дорівнює 0).

Таблиця 1.2

Значення деяких службових полів і прапорів фрагментів

Параметр	Фрагмент 1	Фрагмент 2	Фрагмент 3
Загальна довжина	504 байти	504 байти	492 байти
Ідентифікатор	5	5	5
Прапор DF	0	0	0
Прапор MF	1	1	0
Зсув фрагмента	0	63 блоки по 8 байтів (504 байти)	126 блоків по 8 байтів (1008 байтів)

На рис. 1.3 показаний результат фрагментації IP-пакета.

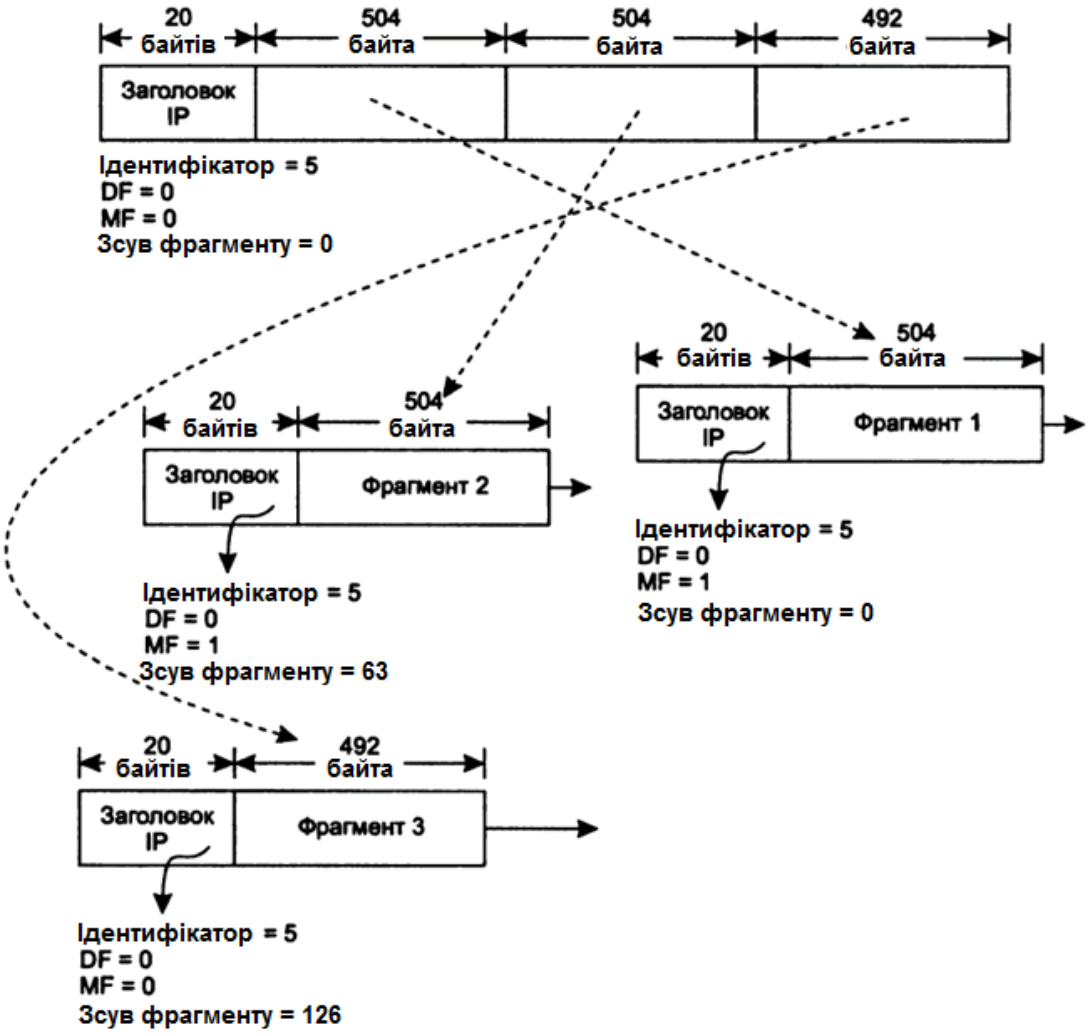


Рис. 1.3. Результат фрагментації IP-пакета (приклад)

1.3. Забезпечення якості обслуговування засобами протоколу IP

Протокол IP дозволяє забезпечити вимоги до якості обслуговування пакетів шляхом використання поля типу сервісу довжиною в один байт, яке містить ознаки, що відображують вимоги до якості обслуговування пакета. Слід зазначити, що назва й структура цього поля згодом зазнала ряд змін (рис. 1.4). Первісне поле мало назву Tos (Type of Service – тип сервісу), а потім було перейменовано в DS (Differentiated Services – диференційоване обслуговування).

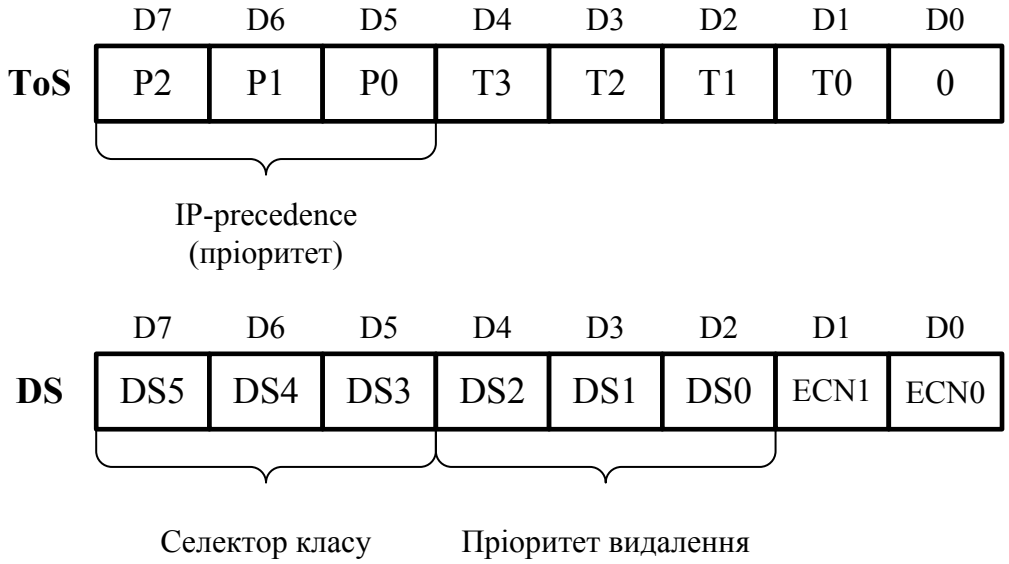


Рис. 1.4. Поле типу сервісу IP-пакета:
а – байт Tos відповідно до RFC 791 (1981 р.), RFC 1349 (1992 р.);
б – байт DS відповідно до RFC 2474 (1998 р.), RFC 3168 (2001 р.)

Три біти пріоритету (P2 – P0) байта ToS (рис. 1.4, а) можуть мати значення, показані в табл. 1.3, причому чим більше номер пріоритету, тим вище пріоритет пакета (0 – найнижчий пріоритет, 7 – найвищий пріоритет). Маршрутизатори й кінцеві вузли можуть брати до уваги пріоритет пакета й обробляти більш важливі пакети (з вищим пріоритетом) у першу чергу.

Біти T3 – T0 байта ToS (рис. 1.4, а) визначають прапори, які можуть бути виставлені для зазначення коду типу сервісу (критерію вибору маршруту). Інтерпретацію кодів наведено в табл. 1.4. Останній біт байта ToS (D0) має нульове значення.

Таблиця 1.3

Коди пріоритету поля ToS

Десяткова	Двійкова (біти P2 ÷ P0)	Опис
0	000	Routine − звичайний (установлений за замовчуванням)
1	001	Priority − підвищений
2	010	Immediate − високий
3	011	Flash − терміновий (відео й мова)
4	100	Flash override − терміновий зі скасуванням (відео)
5	101	Critical − критичний (IP-телефонія)
6	110	Internetwork control − міжмережеве керування
7	111	Network control − керування мережею

Таблиця 1.4

Коди типу сервісу (біти T3 ÷ T0 поля ToS)

Біти T3 ÷ T0 поля ToS	Опис
0000	Нормальний сервіс (за замовчуванням)
1000	Мінімальна затримка
0100	Максимальна пропускна здатність
0010	Максимальна надійність
0001	Мінімальні витрати

В RFC 2474 був переглянутий увесь октет ToS (рис. 1.4, б). Байт ToS був перейменований у поле Differentiated Services (DS). Перші 6 бітів одержали назву Differentiated Services Codepoint (DSCP − код диференційованого обслуговування), що дозволяє ввести в загальному випадку 64 коди (2^6) для зазначення вимог до якості обслуговування пакета. Зазначимо, що коди DSCP зворотно сумісні з кодами пріоритету поля ToS (IP precedence).

В RFC 3168 останні 2 біти (ECN1, ECN0) поля типу сервісу (рис. 1.4, б) одержали назву Explicit Congestion Notification (ECN − явне повідомлення про перевантаженість), що дозволяє маршрутизатору повідомити про виникнення перевантаження на маршруті іншим маршрутизаторам.

Мережеві вузли з підтримкою диференційованого обслуговування використовують поле DSCP у заголовку IP-пакета для визначення відповідної цьому пакету PHB-політики (Per-Hop Behaviors).

PHB-політика − це поведінка мережевого вузла при обслуговуванні пакетів з певним значенням коду диференційованого обслуговування DSCP. Усі пакети одного потоку зі специфічною вимогою до обслуговування несуть у собі одне й те саме значення коду DSCP.

Розглянемо застосування кодів DSCP для забезпечення певних вимог до якості обслуговування пакетів при реалізації відповідних PHB-політик. На сьогодні коди DSCP мають такий розподіл:

1) Default PHB – політика PHB за замовчуванням. Відповідний цій політиці код DCSP має вигляд 000 000 (стандартний код DCSP). Застосовується для передачі даних від вузлів, які не маркують пакети, однак надалі пакети можуть бути перемарковані іншими вузлами мережі;

2) Class Selector (CS) − селектор класу; установлює значення DSCP для сумісності з пріоритетом у поле ToS (IP precedence). Ці коди DCSP мають зворотну сумісність з кодами пріоритету (табл. 1.5);

Таблиця 1.5

Сумісність кодів DCSP з кодами пріоритету поля ToS

Код пріоритету поля Tos	Селектор класу поля DCSP
001	001 000
010	010 000
011	011 000
100	100 000
101	101 000
110	110 000
111	111 000

3) PHB-політика негайної передачі (Expedited Forwarding − EF); забезпечує (гарантує) низький рівень втрат пакетів, незначний джитер і малу затримку пакетів, а також гарантовану пропускну здатність. Як правило, застосовується для таких мережевих додатків, як передача голосу по мережах IP (IP-телефонії), додатків відеоконференцій, а також при наданні таких послуг, як передача інформації по віртуальних орендованих каналах, оскільки ця послуга забезпечує двоточкове з'єднання кінцевих вузлів домену. Подібний тип обслуговування досить часто називають послугою високого класу.

Пакети мають високий пріоритет у черзі (найвищий пріоритет можуть мати тільки пакети зі службовою інформацією для керування мережею, інтенсивністю яких у загальному випадку можна знехтувати) і будуть відкинуті тільки тоді, якщо весь тракт передачі буде повністю завантажений (потік пакетів може зайняти всю пропускну здатність тракту, при цьому пакети інших потоків будуть поміщені в чергу, а при повному заповненні черги − відкинуті). Існує можливість обмеження пропускної здатності для пакетів, обслуговування яких відповідає політиці негайної передачі. У цьому випадку частина пакетів буде відкинута так, щоб інтенсивність потоку пакетів відповідала виділеній для нього маршрутизатором пропускній здатності, що дозволить усунути блокування обслуговування пакетів інших потоків. Рекомендований для цієї політиці код DCSP має вигляд 101 110;

4) PHB-політика гарантованої доставки (Assured Forwarding − AF); визначає чотири рівні (класи) обслуговування (чотири пріоритети, які нижче від пріоритету, надаваного PHB-політикою негайної передачі), кожен з яких у свою чергу може бути охарактеризований трьома рівнями пріоритету відкидання пакетів при перевищенні виділеної пропускної здатності потоком пакетів відповідного класу (при перевантаженні). PHB-політика гарантованої передачі забезпечує гарантовану пропускну здатність, а також можливість використання додаткової пропускної здатності, якщо інші пакети не повністю використали виділену їм пропускну здатність. Цій PHB-політиці відповідають 12 кодів DSCP, представлених у табл. 1.6, з якої видно, що поле DSCP у цьому випадку має формат «xyzab0», де «xyz»

відповідають чотирьом класам (пріоритетам обслуговування) і можуть мати значення 001, 010, 011 або 100, а «ab» відповідають пріоритету відкидання пакетів і можуть мати значення 01, 10, 11. Останній біт поля DSCP – DS0 завжди має нульове значення.

Таблиця 1.6

Коди DSCP, що відповідають PHB-політиці гарантованої передачі AF

Пріоритет відкидання пакета	Пріоритет обробки пакета			
	AF клас 1	AF клас 2	AF клас 3	AF клас 4
низький (відкидається в третю чергу)	001 010 (AF11, DSCP 10)	010 010 (AF21, DSCP 18)	011 010 (AF31, DSCP 26)	100 010 (AF41, DSCP 34)
середній (відкидається в другу чергу)	001 100 (AF12, DSCP 12)	010 100 (AF22, DSCP 20)	011 100 (AF32, DSCP 28)	100 100 (AF42, DSCP 36)
високий (відкидається в першу чергу)	001 110 (AF13, DSCP 14)	010 110 (AF23, DSCP 22)	011 110 (AF33, DSCP 30)	100 110 (AF43, DSCP 38)

Рівень обслуговування, що відповідає PHB-політиці гарантованої доставки AF, поступається за якістю обслуговування рівню, забезпечуваному політикою негайної передачі EF, оскільки не гарантується низький рівень затримок пакетів. Але, незважаючи на це, рівень обслуговування, що відповідає PHB-політиці гарантованої доставки, є цілком прийнятним для більшості мережевих додатків, що використовують на транспортному рівні протокол TCP з метою гарантування доставки пакетів.

Зазначимо, що на практиці, як правило, пакети, що відповідають PHB-політиці негайної передачі EF, обслуговуються за пріоритетною схемою, але з обмеженням інтенсивності вхідного потоку. Пропускна здатність, що залишилася після обслуговування цих пакетів, розподіляється між пакетами, що відповідають PHB-політиці гарантованої доставки AF за допомогою алгоритму зваженого обслуговування,

що забезпечує гарантовану пропускну здатність, але не мінімізує затримку пакетів. Для кожного класу пріоритету обробки пакета (класи 1 − 4), відповідного PHB-політиці гарантованої доставки, утворюється власна черга пакетів, при цьому для кожного класу пріоритету обробки пакета можуть бути встановлені по три рівні пріоритету відкидання пакетів (низький, середній і високий).

Сумісність кодів DCSP з кодами пріоритету поля ToS (IP-precedence) і відповідність кодів DCSP політикам PHB наведена в табл. 1.7.

Таблиця 1.7

Сумісність кодів DCSP з кодами пріоритету поля ToS (IP-precedence) і відповідність кодів DCSP політикам PHB

Десяткове значення DSCP	Двійкове значення DSCP (DS5, DS4, DS3, DS2, DS1, DS0)	DSCP	Десяткове значення IP-precedence	Опис
0	000 000	BE	0	Routine (BE) – за замовчуванням
8	001 000	CS1	1	Priority
10	001 010	AF11		
12	001 100	AF12		
14	001 110	AF13		
16	010 000	CS2	2	Immediate
18	010 010	AF21		
20	010 100	AF22		
22	010 110	AF23		
24	011 000	CS3	3	Flash – відео й мова
26	011 010	AF31		
28	011 100	AF32		
30	011 110	AF33		
32	100 000	CS4	4	Flash override – відео
34	100 010	AF41		
36	100 100	AF42		
38	100 110	AF43		
46	101 110	EF	5	Critical – IP-телефонія
48	110 000	Зарезервовано	6	Internetwork control (Control)
56	111 000	Зарезервовано	7	Network control (Control)

2. МАРШРУТИЗАЦІЯ ПАКЕТІВ ПРОТОКОЛУ IP

2.1. Загальні відомості про маршрутизацію пакетів протоколу IP

Маршрутизація (routing) – це процес визначення маршруту передачі IP-пакета з однієї IP-мережі в іншу. Завдання маршрутизації вирішують як маршрутизатори, так і кінцеві вузли.

Маршрутизатор або шлюз – це вузол мережі з декількома IP-інтерфейсами (які мають MAC-адреси і IP-адреси), підключеними до різних IP-мереж, що здійснює на основі вирішення завдання маршрутизації транспортування IP-пакетів з однієї IP-мережі в іншу з метою доставки IP-пакета від відправника до одержувача. Маршрутизатор працює на третьому рівні семирівневої моделі, тому є пристроєм третього рівня.

Транспортування IP-пакетів в IP-мережах здійснюється на основі інформації про можливі маршрути маршрутизаторів, що містяться в таблицях маршрутизації маршрутизаторів, а також кінцеві вузли. Таким чином, таблиця маршрутизації – це база даних маршрутів, що зберігається в пам'яті всіх вузлів IP-мережі.

Записи в таблиці маршрутизації можуть бути створені трьома основними джерелами:

− програмним забезпеченням маршрутизатора (це записи про безпосередньо підключені мережі, інформація про які вводиться при ручному конфігуруванні інтерфейсів маршрутизаторів або кінцевих вузлів, а також записи про деякі особливі адреси призначення);

− адміністратором шляхом ручного конфігурування маршрутів;

− протоколами маршрутизації.

Розрізняють однокрокову й багатокрокову маршрутизацію. При однокроковій маршрутизації в процесі вибору маршруту визначається тільки наступний (найближчий) маршрутизатор, а не вся послідовність маршрутизаторів від початкового до кінцевого вузла. Однокрокова маршрутизація виконується за розподіленою схемою − кожний маршрутизатор відповідальний за вибір тільки одного кроку маршруту, а остаточний маршрут складається в результаті роботи всіх маршрутизаторів, через які проходить даний пакет.

При багатокроковій маршрутизації вузол-джерело задає в пакеті, що відправляється в мережу, повний маршрут його проходження через усі проміжні маршрутизатори. Багатокрокову маршрутизацію часто називають маршрутизацією від джерела (Source Routing). При використанні такої маршрутизації нема необхідності будувати й аналізувати таблиці маршрутизації в кожному маршрутизаторі, що прискорює проходження пакета по мережі, розвантажує маршрутизатори, але при цьому більше навантаження лягає на кінцеві вузли за рахунок необхідності визначати повний маршрут проходження пакетів. Зазначимо, що маршрутизація від джерела застосовується дуже рідко й надалі розглядатися не буде.

За способом заповнення таблиці маршрутизації маршрути поділяють на статичні й динамічні.

Статичні маршрути − це маршрути, які вносяться в таблицю маршрутизації вручну при конфігуруванні маршрутизатора.

Динамічні маршрути − це маршрути, які вносяться в таблицю маршрутизації за допомогою протоколів маршрутизації, які використовують для визначення маршрутів дані про топологію мережі та її стан. Результатом роботи протоколів маршрутизації є узгодження змісту таблиць маршрутизації взаємодіючих маршрутизаторів таким чином, щоб IP-пакет з однієї IP-мережі міг бути переданий у будь-яку іншу IP-мережу по маршруту з найменшою метрикою. Протоколи маршрутизації дозволяють оперативно вносити в таблиці маршрутизації дані про зміни зв'язків, що виникають у мережі.

Статична маршрутизація − вид маршрутизації, при якій маршрути вносяться в таблицю маршрутизації вручну при конфігуруванні маршрутизатора.

При динамічній маршрутизації маршрути вносяться в таблицю маршрутизації за допомогою протоколів маршрутизації.

До переваг статичної маршрутизації можна віднести:

− простоту настроювання в невеликих мережах;

− відсутність необхідності передачі службової інформації, на відміну від протоколів динамічної маршрутизації, і, як результат, відсутність додаткового навантаження на мережу.

До недоліків статичної маршрутизації можна віднести:

− складність масштабування. За необхідності зміни топології мережі, як правило, необхідне настроювання нових статичних маршрутів для всіх маршрутизаторів мережі. Трудомісткість корекції таблиць маршрутизації різко зростає при збільшенні кількості маршрутизаторів у мережі;

− неможливість визначення недоступності маршруту. Наприклад, при несправності (вимкненні) несуміжного маршрутизатора інші маршрутизатори можуть передавати IP-пакети по маршрутах, у які входить несправний (вимкнений) маршрутизатор, хоча насправді такі маршрути є недоступними.

При задаванні маршруту в таблиці маршрутизації, як правило, вказуються:

− номер IP-мережі призначення або IP-адреса вузла призначення (номер IP-мережі або IP-адреса вузла, куди повинен бути відправлений IP-пакет) і відповідна маска (маска мережі призначення при задаванні маршруту до мережі призначення або маска вигляду 255.255.255.255 при задаванні маршруту до вузла призначення); задавання адресою призначення IP-адреси певного вузла дозволяє задавати окремий маршрут проходження (специфічний маршрут) до конкретного вузла;

− IP-адреса суміжного маршрутизатора (шлюзу, наступного вузла), який буде здійснювати подальшу маршрутизацію (або вихідний порт маршрутизатора, на який повинен бути направлений IP-пакет);

− метрика маршруту, що характеризує міру переваги даного маршруту відповідно до заданого критерію, наприклад кількість маршрутизаторів, що входять у маршрут, пропускна здатність, затримка. Також у деяких маршрутизаторах у таблиці маршрутизації можуть міститися й інші додаткові умови, за якими вибирається маршрут. За наявності декількох маршрутів до однієї і тієї самої мережі маршрутизатори можуть вибирати маршрут з мінімальною метрикою.

Особливим маршрутом у таблиці маршрутизації є маршрут за замовчуванням, для якого адресою призначення та маскою є 0.0.0.0. Цей маршрут використовується в тому випадку, коли в таблиці маршрутизації відсутній запис про мережу або вузол призначення, куди необхідно направити IP-пакет. За відсутності

такого маршруту IP-пакети, адресовані в невідому мережу або невідомому вузлу призначення, будуть відкинуті. Зазначимо, що в таблицях маршрутизації кінцевих вузлів, що працюють у мережі з одним маршрутизатором, який, як правило, називають шлюзом, маршрут за замовчуванням є єдиним можливим маршрутом.

2.2. Приклад маршрутизації пакетів протоколу IP

Розглянемо процес маршрутизації на прикладі мережі, поданої на рис. 2.1. У цій мережі маршрутизатори поєднують IP-мережі, що мають умовні номери N 1, N 2, …, N 8, у загальну складену мережу.

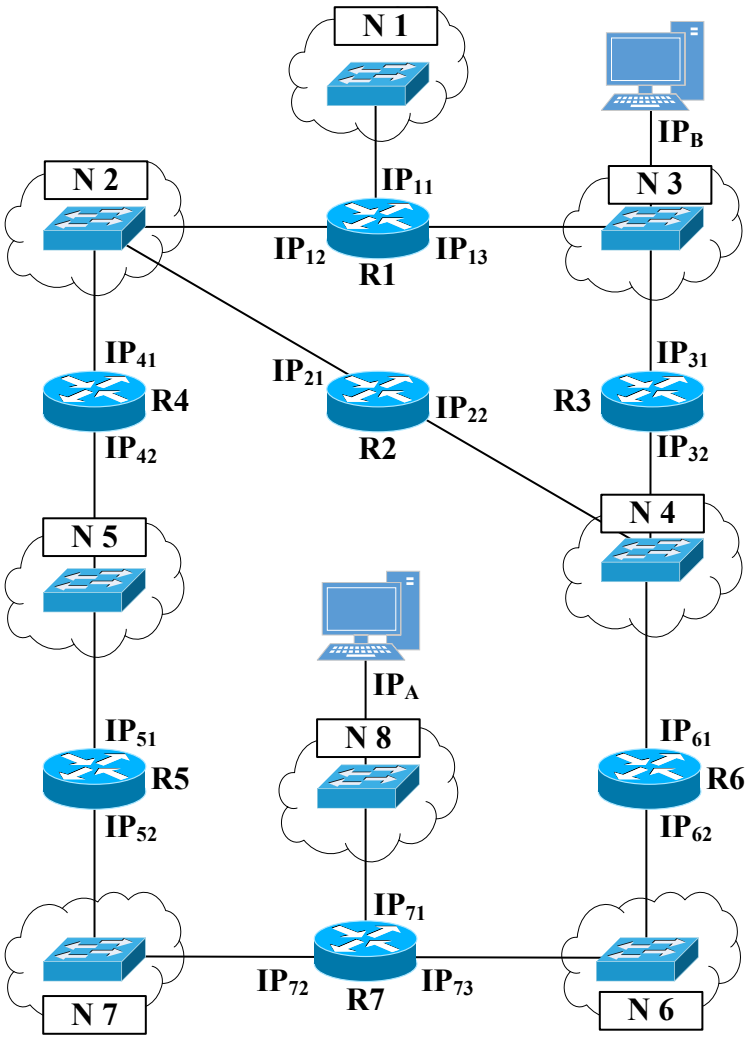


Рис. 2.1. Приклад схеми маршрутизації

Маршрутизатори мають по кілька портів (інтерфейсів), які приєднані до відповідних IP-мереж. Кожний порт маршрутизатора має свою власну IP-адресу в тій IP-мережі, яка до нього підключена. Наприклад, маршрутизатор 1 має три порти, приєднані до мереж N1, N2 і N3. IP-адреса порту 1 маршрутизатора 1 − IP_{11} – належить мережі N1, IP-адреса порту 2 маршрутизатора 1 − IP_{12} – належить мережі N2, а IP-адреса порту 3 маршрутизатора 1 − IP_{13} – належить мережі N3.

Зазначимо, що в розглянутій мережі існують кілька альтернативних маршрутів передачі IP-пакетів між двома кінцевими вузлами. Так, IP-пакет, відправлений з вузла A у вузол B, може пройти через маршрутизатори 7, 5, 4, 1 або маршрутизатори 7, 6, 3. Існують і інші маршрути між вузлами A і B. Вибір маршруту з декількох можливих вирішують маршрутизатори, а також кінцеві вузли на підставі відповідних записів у таблиці маршрутизації.

Використовуючи умовні позначки для IP-адрес портів маршрутизаторів і номерів IP-мереж у тому вигляді, як вони наведені на рис. 2.1, розглянемо приклад таблиці маршрутизації маршрутизатора 4 (рис. 2.2).

Адреса призначення	Маска	IP-адреса наступного маршрутизатора	IP-адреса вихідного порту	Метрика маршруту
N1	маска для N1	IP_{12} (R1)	IP_{41}	1
N2	маска для N2	–	IP_{41}	0 (під'єднана)
N3	маска для N3	IP_{12} (R1)	IP_{41}	1
N4	маска для N4	IP_{21} (R2)	IP_{41}	1
N5	маска для N5	–	IP_{42}	0 (під'єднана)
N6	маска для N6	IP_{21} (R2)	IP_{41}	2
IP_B	255.255.255.255	IP_{21} (R2)	IP_{41}	2
0.0.0.0 (маршрут за замовчуванням)	0.0.0.0	IP_{51} (R5)	IP_{42}	–

Рис. 2.2. Таблиця маршрутизації маршрутизатора 4

Перший стовпець таблиці маршрутизації містить адреси призначення (номери мереж або вузлів). У кожному рядку таблиці після адреси призначення вказується IP-адреса відповідного порту наступного (суміжного) маршрутизатора, на який необхідно направити IP-пакет, щоб той пересувався в напрямку до заданої адреси призначення по маршруту, відповідному певному рядку таблиці маршрутизації.

Перед тим як передати IP-пакет наступному маршрутизатору, маршрутизатор 4 повинен визначити, на який із власних портів (IP_{41} або IP_{42}) він повинен направити даний IP-пакет. Для цього служить третій стовпець таблиці маршрутизації, що містить IP-адреси (або умовні номери) портів маршрутизатора 4.

У загальному випадку в таблиці маршрутизації можлива наявність відразу декількох рядків, що відповідають тій самій адресі призначення. У цьому випадку при виборі маршруту береться до уваги стовпець, що містить значення метрики маршруту. При цьому буде обраний маршрут з мінімальною метрикою. У прикладі таблиці маршрутизації, показаної на рис. 2.1, метрика відповідає кількості маршрутизаторів між IP-мережею, приєднаною до певного порту маршрутизатора 4, з якого буде відправлений IP-пакет, і мережею призначення, у яку повинен бути доставлений IP-пакет. Значення метрики для мереж, безпосередньо підключених до портів маршрутизатора 4, у розглянутому прикладі прийняте рівним 0, однак у загальному випадку не виключена можливість задавання метрики безпосередньо підключеної мережі значенням, що дорівнює 1.

Маршрутизатор після вилучення з IP-пакета IP-адреси призначення послідовно порівнює його з адресами призначення з кожного рядка таблиці маршрутизації. Рядок, у якому такий збіг відбувся, вказує на IP-адресу порту суміжного маршрутизатора (часто називаний шлюзом), на який слід направити IP-пакет. Наприклад, якщо на який-небудь порт маршрутизатора 4 надходить IP-пакет, адресований у мережу N6, то з таблиці маршрутизації випливає, що IP-адреса наступного маршрутизатора (шлюз) − IP_{21}. Таким чином, маршрутизатор 4 повинен направити IP-пакет через власний порт із IP-адресою IP_{41} на порт 1 суміжного маршрутизатора 2, що має IP-адресу IP_{21}.

Найчастіше в якості адреси призначення в таблиці маршрутизації вказується не вся IP-адреса (адреса вузла призначення), а тільки номер мережі призначення. Таким чином, для всіх IP-пакетів, що направляються в ту саму мережу, маршрутизатор буде вибирати той самий маршрут (без урахування можливих змін у стані мережі, наприклад відмов маршрутизаторів). Однак у деяких випадках виникає необхідність для одного з вузлів мережі визначити маршрут, що відрізняється від маршруту, заданого для всіх інших вузлів мережі (специфічний маршрут). Для цього в таблицю маршрутизації для даного вузла поміщають окремий рядок, що містить його повну IP-адресу й відповідну маршрутну інформацію. Такого роду запис є в таблиці маршрутизації маршрутизатора 4 для кінцевого вузла B (рис. 2.2), що дозволяє направити IP-пакет, адресований кінцевому вузлу B, на маршрутизатор 2 (порт IP_{21}) через свій власний порт 2 (порт IP_{42}), а не на маршрутизатор 1 (порт IP_{12}) через свій власний порт 1 (порт IP_{41}), як усі інші IP-пакети, адресовані всім іншим вузлам мережі N3. Якщо в таблиці маршрутизації є записи про маршрути як до IP-мережі в цілому, так і до її окремого вузла, то при надходженні IP-пакета, адресованого даному вузлу, маршрутизатор віддасть перевагу маршруту, зазначеному в таблиці маршрутизації для даного вузла (специфічному маршруту).

З рис. 2.2 видно, що таблиця маршрутизації маршрутизатора 4 містить у явному вигляді тільки інформацію про маршрути до мереж призначення N1 – N6. Для відправлення IP-пакета в інші мережі призначення використовується єдиний маршрут за замовчуванням. Такий підхід дозволяє значно скоротити обсяг таблиці маршрутизації і тим самим зменшити час її перегляду. У розглянутому прикладі маршрутизатор 4 буде відправляти IP-пакети, адресовані в усі мережі, за винятком мереж N1 – N6, використовуючи маршрут за замовчуванням − через власний порт IP_{42} на порт маршрутизатора 5 IP_{51}.

Завдання маршрутизації вирішують не тільки маршрутизатори, але й кінцеві вузли − комп'ютери. Вирішення цього завдання починається з того, що кінцевий вузол визначає, чи направляється пакет в іншу мережу або адресований певному вузлу даної мережі. Якщо номер мережі призначення збігається з номером даної мережі, це означає, що пакет маршрутизувати не потрібно. А якщо ні, то маршрутизація потрібна.

Таблиця маршрутизації кінцевого вузла B, що належить мережі N3, може виглядати так, як показано на рис. 2.3. Тут IP_B − мережева адреса кінцевого вузла B. На підставі цієї таблиці маршрутизації кінцевий вузол B вибирає, на який із двох наявних у мережі N3 маршрутизаторів (R1 або R3) слід направляти IP-пакет.

Зазначимо, що кінцеві вузли для маршрутизації часто використовують тільки єдиний маршрут − маршрут за замовчуванням. За наявності одного маршрутизатора в мережі цей варіант − єдиний можливий для всіх кінцевих вузлів. Але навіть за наявності декількох маршрутизаторів у мережі, коли перед кінцевим вузлом стоїть проблема їх вибору, як правило, обирають задавання маршруту за замовчуванням.

Адреса призначення	Маска	IP-адреса наступного маршрутизатора	IP-адреса вихідного порту	Метрика маршруту
N1	маска для N1	IP_{13} (R1)	IP_B	1
N2	маска для N2	IP_{13} (R1)	IP_B	1
N3	маска для N3	–	IP_B	0 (під'єднана)
N4	маска для N4	IP_{31} (R3)	IP_B	1
N5	маска для N5	IP_{13} (R1)	IP_B	4
N6	маска для N6	IP_{31} (R3)	IP_B	2
0.0.0.0 (маршрут за замовчуванням)	0.0.0.0	IP_{31} (R3)	IP_B	–

Рис. 2.3. Таблиця маршрутизації кінцевого вузла B

Розглянемо таблицю маршрутизації іншого кінцевого вузла − вузла A (рис. 2.4). Компактний вигляд таблиці маршрутизації вузла A відображує той факт, що всі IP-пакети, що

направляються з вузла А, або не виходять за межі мережі N8, або проходять через порт 1 маршрутизатора 7. Цей маршрутизатор і визначений у таблиці маршрутизації як маршрутизатор за замовчуванням.

Адреса призначення	Маска	IP-адреса наступного маршрутизатора	IP-адреса вихідного порту	Метрика маршруту
N8	маска для N3	–	IP_A	0 (під'єднана)
0.0.0.0 (маршрут за замовчуванням)	0.0.0.0	IP_{71} (R7)	IP_A	–

Рис. 2.4. Таблиця маршрутизації кінцевого вузла А

2.3 Процедура пошуку маршруту в таблиці маршрутизації

Розглянемо процедуру пошуку маршруту в таблиці маршрутизації з урахуванням масок. Дана процедура в загальному випадку складається з трьох етапів і починається після того, як маршрутизатор вилучив із IP-пакета IP-адресу одержувача.

Етап 1. Після вилучення IP-адреси одержувача маршрутизатор у першу чергу здійснює пошук у таблиці маршрутизації маршруту до вузла призначення (одержувача IP-пакета з певною IP-адресою – наприклад комп'ютер). Для цього з кожного запису (рядка) таблиці маршрутизації, у якому маска має значення 255.255.255.255, маршрутизатор витягає адресу призначення (це й буде IP-адреса конкретного одержувача, оскільки для нього маска у двійковому вигляді складається з усіх одиниць) і порівнює його з адресою, вилученою з IP-пакета. Якщо в якому-небудь рядку таблиці маршрутизації збіг відбувся, то з відповідного рядка вилучається IP-адреса наступного маршрутизатора й ідентифікатор (номер або IP-адреса) вихідного порту маршрутизатора, на який згодом буде направлений розглядуваний IP-пакет.

Етап 2. Якщо ж збіг не відбувся, то далі маршрутизатор здійснює пошук у таблиці маршрутизації маршруту до мережі призначення (групи вузлів). Для цього маршрутизатор знову переглядає таблицю маршрутизації, причому з кожним її записом робить такі дії:

− порозрядно застосовується операція логічного «І» до однойменних розрядів маски, що міститься в даному записі, і IP-адреси одержувача, вилученої з IP-пакета, що дозволяє у результаті виділити з IP-адреси одержувача значення номера IP-мережі призначення;

− отримане значення номера IP-мережі призначення (результат порозрядного застосування операції логічного «І» на попередньому кроці) порівнюється зі значенням, яке поміщено в полі адреси призначення того самого запису таблиці маршрутизації;

− якщо збіг відбувся, то маршрутизатор відповідно відзначає (запам'ятовує) цей рядок (запис) таблиці маршрутизації;

− якщо переглянуто не всі рядки, то маршрутизатор аналогічно переглядає наступний рядок, після чого відбувається перехід до наступного кроку.

Етап 3. Маршрутизатор після перегляду всіх рядків таблиці маршрутизації (включаючи рядок про маршрут за замовчуванням) виконує одне з таких дій:

− якщо не відбулося жодного збігу й маршрут за замовчуванням відсутній, то IP-пакет відкидається;

− якщо відбувся один збіг, то IP-пакет відправляється по маршруту, зазначеному в рядку з адресою призначення, що збіглася (надходить на відповідний порт маршрутизатора);

− якщо відбулося кілька збігів, то всі позначені рядки порівнюються й вибирається маршрут з того рядка, у якому кількість двійкових розрядів мережевої частини адреси призначення, відповідна одиницям у масці, найбільша (інакше кажучи, у ситуації, коли IP-адреса одержувача, витягнута з IP-пакета, належить відразу декільком підмережам, маршрутизатор використає маршрут до найменшої з підмереж, тобто до підмережі з найменшою кількістю вузлів). За наявності в таблиці маршрутизації декількох маршрутів до однієї і тієї самої

мережі призначення (у випадку рівної кількості двійкових розрядів мережевої частини адреси призначення в декількох рядках таблиці маршрутизації) буде обрано маршрут з найменшим значенням метрики, а при рівних значеннях метрик можливе (для деяких маршрутизаторів) відправлення IP-пакетів по декількох маршрутах, забезпечуючи тим самим роботу в режимі розподілу (балансування) навантаження.

Зазначимо, що в таблиці маршрутизації запис із адресою призначення 0.0.0.0 і маскою 0.0.0.0 відповідає маршруту за замовчуванням. Дійсно, після порозрядного застосування операції логічного «І» до однойменних розрядів маски, що має значення 0.0.0.0 і будь-яку IP-адресу одержувача, витягнуту з IP-пакета, результат буде мати вигляд 0.0.0.0, який збігається з адресою призначення, зазначеною в такому записі. Маршрут за замовчуванням буде обраний маршрутизатором в останню чергу тільки за відсутності збігів з іншими записами таблиці маршрутизації оскільки маска 0.0.0.0 не містить жодної одиниці (фактично маска вигляду 0.0.0.0 має на увазі відсутність мережевої частини в IP-адресі, що й призведе до вибору такого маршруту в останню чергу на останньому кроці етапу 3).

2.4. Особливості таблиць маршрутизації маршрутизаторів Cisco

До таблиці маршрутизації маршрутизаторів Cisco входять:

− IP-адреси й маски безпосередньо підключених мереж (маршрути до безпосередньо підключених мереж) − мереж, у яких знаходяться інтерфейси маршрутизатора. Дані маршрути вносяться в таблицю маршрутизації в процесі конфігурування маршрутизатора. У таблиці маршрутизації вони позначаються буквою C (Connected);

− IP-адреси й маски інтерфейсів маршрутизатора, які вводяться при конфігуруванні відповідних інтерфейсів (маршрути до власних інтерфейсів маршрутизатора). У таблиці маршрутизації вони позначаються буквою L (Local);

− статичні маршрути, які позначаються буквою S (Static);

− динамічні маршрути (позначення залежить від назви протоколу маршрутизації).

У маршрутизаторах компанії Cisco використовується додаткова ознака, за якою проводиться вибір маршруту, − адміністративна відстань. Адміністративна відстань необхідна маршрутизатору для ухвалення рішення про те, який з маршрутів помістити в таблицю маршрутизації у випадку, якщо інформація про мережу або вузол призначення може бути отримана від різних джерел (введена вручну чи отримана від протоколів маршрутизації).

Більший пріоритет має той маршрут, який має меншу адміністративну відстань. Зазначимо, що за замовчуванням для безпосередньо підключеної мережі значення адміністративної відстані дорівнює 0, для статичного маршруту до наступного маршрутизатора – 1, для протоколів динамічної маршрутизації RIP – 120, OSPF – 110. Маршрут з адміністративною відстанню 255 уважається недоступним. Зазначимо, що значення адміністративної відстані можна змінювати за допомогою відповідних команд.

У випадку двох однакових маршрутів з однаковим значенням адміністративної відстані вибір маршруту проводиться на основі значення метрики маршруту. У такий спосіб метрики маршрутів при виборі одного маршруту з декількох ураховуються в другу чергу після адміністративної відстані. Використання адміністративної відстані, як додаткової ознаки для вибору маршруту, дозволяє задавати резервні маршрути. Однак, на відміну від метрики маршруту, значення адміністративної відстані використовуються тільки локально (розсилання адміністративної відстані протоколами маршрутизації не проводиться).

Зазначимо, що в таблицю маршрутизації записуються не всі можливі маршрути, а тільки маршрути, які мають найменше значення адміністративної відстані або метрики при рівності адміністративних відстаней (якщо ввімкнена функція балансування навантаження, то до таблиці маршрутизації записуються й маршрути з однаковими адміністративними відстанями та метриками).

Контрольні питання

1. Яка максимально можлива загальна довжина IP-пакета?
2. Для чого призначено поле ідентифікатора IP-пакета?
3. Як змінюється значення поля часу життя при проходженні IP-пакета через маршрутизатор?
4. Яке поле IP-пакета дозволяє забезпечити якість обслуговування?
5. Яка максимальна кількість приорітетів обслуговування може бути задана у відповідному службовому полі IP-пакета?
6. Що таке маршрутизація IP-пакетів?
7. На якому рівні семирівневої моделі виконується маршрутизація?
8. Які існують джерела записів в таблиці маршрутизації?
9. Чим відрізняється однокрокова маршрутизація від багатокрокової (маршрутизації від джерела)?
10. Що таке статична маршрутизація?
11. Які є недоліки у статичній маршрутизації?

3. РОЗРОБЛЕННЯ ПЛАНУ РОЗПОДІЛУ ІНФОРМАЦІЇ ДЛЯ СТАТИЧНОЇ МАРШРУТИЗАЦІЇ В МЕРЕЖІ НА ОСНОВІ ПРОТОКОЛУ IP

3.1. Основні кроки розроблення плану розподілу інформації

Для вирішення завдання розроблення плану розподілу інформації для статичної маршрутизації в мережі на основі протоколу IP треба виконати такі кроки:

1. Виконати розбиття загального адресного простору IP-мережі на підмережі.
2. Виконати розподіл IP-адрес у підмережах. Визначити мережеві параметри обладнання.
3. Визначити метрики трактів між суміжними маршрутизаторами мережі відповідно до швидкості передачі тракту.
4. Утворити відповідний розглядуваній схемі IP-мережі зважений граф, на якому номери вершин будуть відповідати номерам маршрутизаторам, а ваги ребер – метрикам трактів.
5. Визначити основні маршрути (маршрути першого вибору) за допомогою алгоритму Дейкстри.
6. Розробити таблицю маршрутизації для кожного маршрутизатора мережі, сформувавши тим самим план розподілу інформації.
7. Перевірити правильність розроблення плану розподілу інформації (досяжність один одному всіх підмереж складної IP-мережі) шляхом імітаційного моделювання в програмному середовищі Cisco Packet Tracer.
8. Додаткове завдання, яке виконується за вказівкою викладача після перевірки правильності розроблення плану розподілу інформації (досяжності одна одній всіх мереж): самостійно визначити для одного з основних маршрутів (маршрутів першого вибору) один резервний маршрут (маршрут другого вибору), який не містить спільних маршрутизаторів з основним маршрутом. Резервний маршрут (маршрут другого вибору) повинен містити не менше трьох маршрутизаторів (для подальшого проведення дослідження, у ході якого будуть

виявлені певні недоліки при застосуванні таких маршрутів), якщо інше не передбачено завданням або викладачем. В існуючі таблиці маршрутизації маршрутизаторів, які входять до складу вибраного резервного маршруту, додати резервні статичні маршрути з адміністративною відстанню більшою, ніж основні маршрути, за допомогою відповідних команд у командному рядку маршрутизаторів. Зазначимо, що резервні (як і основні) статичні маршрути повинні бути визначені для двох напрямків. Це необхідно для того, щоб IP-пакети змогли досягнути вузла призначення, а IP-пакети, спрямовані від вузла призначення, − досягнути вузла-відправника.

3.2. Вихідні дані для розроблення плану розподілу інформації

Для виконання завдання розроблення плану розподілу інформації для статичної маршрутизації в мережі на основі протоколу IP необхідні такі вихідні дані:

− схема IP-мережі;

− загальний адресний простір IP-мережі (при виконанні завдання розбиття загального адресного простору на відповідні підмережі здійснюється самостійно, але з урахуванням того, що маска підмереж для з'єднання суміжних маршрутизаторів повинна мати вигляд 255.255.255.252 («/30»);

− критерій вибору маршруту та повязані з ним дані для визначення метрик трактів (при виконанні завдання, якщо інше не вказано у вихідних даних, критерієм вибору маршруту вважається пропускна здатність, а метрика тракту зворотно пропорційна максимальній швидкості передачі тракту).

Приклад схеми IP-мережі з відповідними вихідними даними показаний на рис. 3.1.

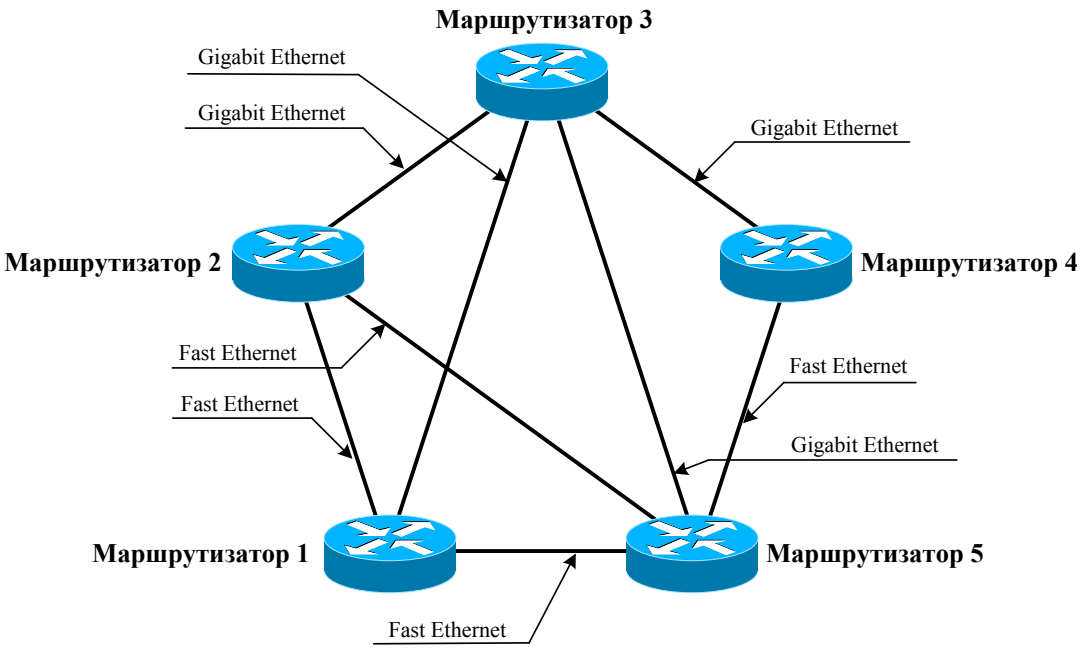


Рис. 3.1. Схема IP-мережі

3.3. Розбиття загального адресного простору IP-мережі на підмережі

Виконаємо розбиття загального адресного простору IP-мережі 10.0.0.0/16 (маска 255.255.0.0) на відповідні підмережі. При виконанні завдання розбиття загального адресного простору на підмережі треба врахувати, що для кожного з маршрутизаторів необхідно виділити по одній підмережі для підключення обладнання користувачів (розміри цих підмереж при виконанні завдання доцільно вибрати однаковими) і, крім того, треба виділити по одній підмережі, які мають по дві індивідуальні IP-адреси, для з'єднання портів суміжних маршрутизаторів. Зазначимо, що для виконання останньої умови треба, щоб маска підмереж для з'єднання маршрутизаторів мала вигляд 255.255.255.252 («/30»).

З метою зниження громіздкості обчислень розподіл IP-адрес зручніше проводити за допомогою програмного забезпечення. Однією з найбільш придатних для цього програм є Free Advanced Subnet Calculator.

Для розбиття IP-мереж будемо використовувати тільки закладку «CIDR Calculator». Вихідна IP-адреса та розширений префікс (чи кількість одиниць у масці) вводяться у вікна «Address

Block» та «CIDR Mask» відповідно. Розбиття загального адресного простору (мережі) на підмережі можна провести, якщо відомий один з параметрів: кількість одиниць у масці − «Mask Bits», кількість розрядів для позначення номера вузла в масці - «Hosts Bits», необхідна кількість підмереж − «Number of Subnets», необхідна кількість вузлів у підмережі - «Hosts per Subnet». Для отримання результатів необхідно натиснути на кнопку «Generate Subnets».

Спочатку розіб'ємо загальний адресний простір (мережу) 10.10.0.0/16 на підмережі рівного розміру. Для виконання завдання нам треба 6 підмереж рівного розміру: 5 − для підключення обладнання користувачів (за кількістю маршрутизаторів) і ще 1 підмережа, яку в подальшому розіб'ємо на підмережі для з'єднання портів суміжних маршрутизаторів (підмережі з двома індивідуальними IP-адресами). Зазначимо, що при розбитті мережі на підмережі рівного розміру кількість цих підмереж буде завжди дорівнювати степеню числа два, тому вибираємо кількість підмереж такою, що дорівнює найближчому більшому числу, яке дорівнює степеню числа два, тобто 8 ($2^3 = 8$).

Далі вводимо до програми такі дані: у вікно «Address Block» - 10.0.0.0, у вікно «CIDR Mask» − 16 бітів. Для розбиття мережі на підмережі вводимо до вікна «Nunber of Subnet» значення 8 і натискаємо на кнопку «Generate Subnets». Результат розбиття зображено на рис. 3.2 та зведено в табл. 3.1.

Таблиця 3.1

Результати розбиття мережі 10.0.0.0/16 на підмережі рівного розміру

Номер з/п	Підмережа	Маска	Кількість вузлів	Діапазон адрес	Широкомовна адреса
1	10.0.0.0/19	255.255.224.0	8190	10.0.0.1 − 10.0.31.254	10.0.31.255
2	10.0.32.0/19	255.255.224.0	8190	10.0.32.1 − 10.0.63.254	10.0.63.255
3	10.0.64.0/19	255.255.224.0	8190	10.0.64.1 − 10.0.95.254	10.0.95.255
4	10.0.96.0/19	255.255.224.0	8190	10.0.96.1 − 10.0.127.254	10.0.127.255
5	10.0.128.0/19	255.255.224.0	8190	10.0.128.1 − 10.0.159.254	10.0.159.255
6	10.0.160.0/19	255.255.224.0	8190	10.0.160.1 − 10.0.191.254	10.0.191.255

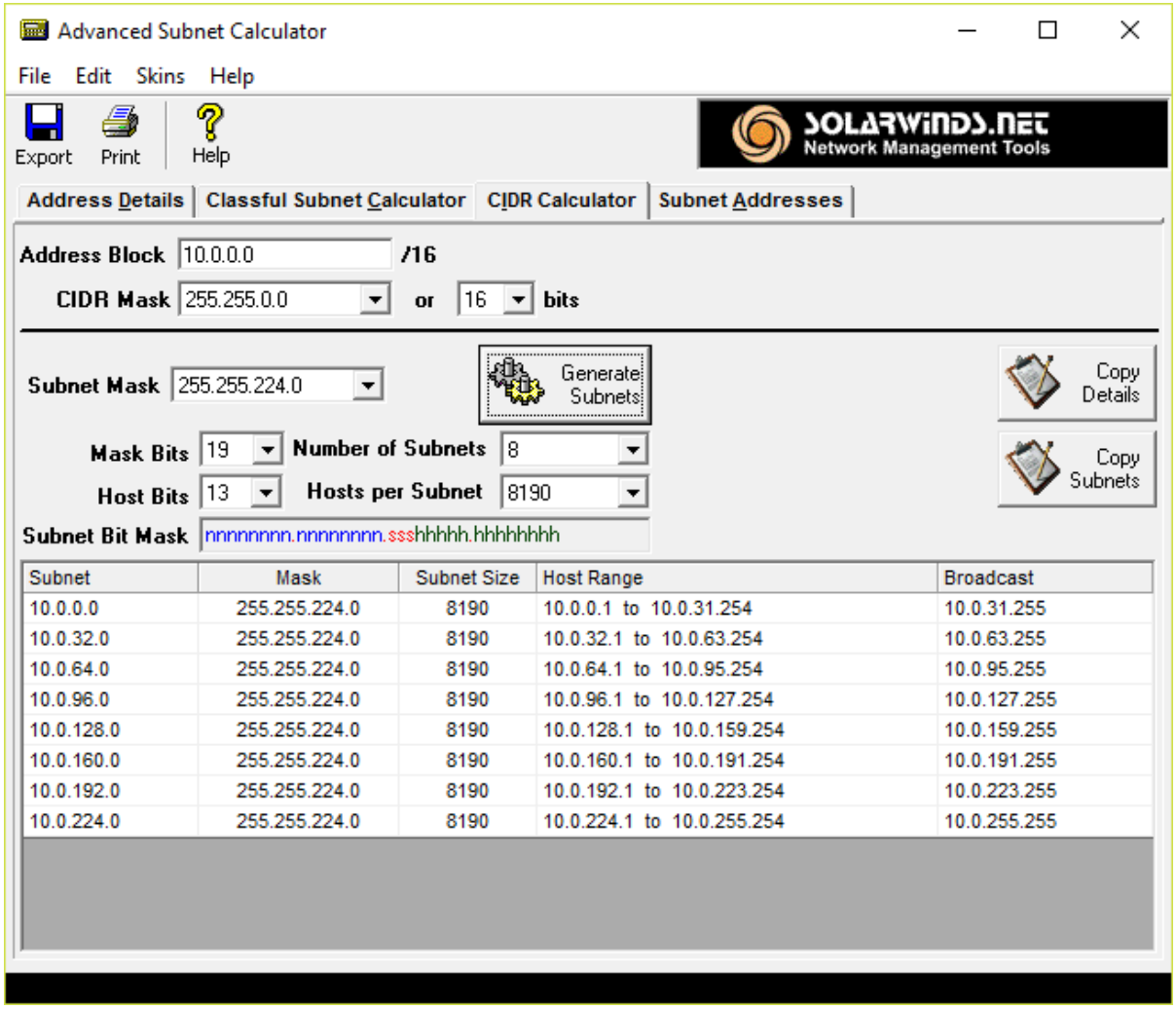


Рис. 3.2. Розбиття мережі 10.0.0.0/16 на 8 підмереж рівного розміру

Тепер з табл. 3.1 виберемо одну з мереж, нехай це буде мережа 10.0.160.0/19, і розіб'ємо її на підмережі з двома індивідуальними IP-адресами, необхідними для з'єднання портів суміжних маршрутизаторів.

Для розбиття мережі 10.0.160.0/19 на підмережі з двома індивідуальними IP-адресами вводимо до вікна «Host per Subnet» значення 2 та натискаємо на кнопку «Generate Subnets». Результат розбиття зображено на рис. 3.3 та зведено в табл. 3.2.

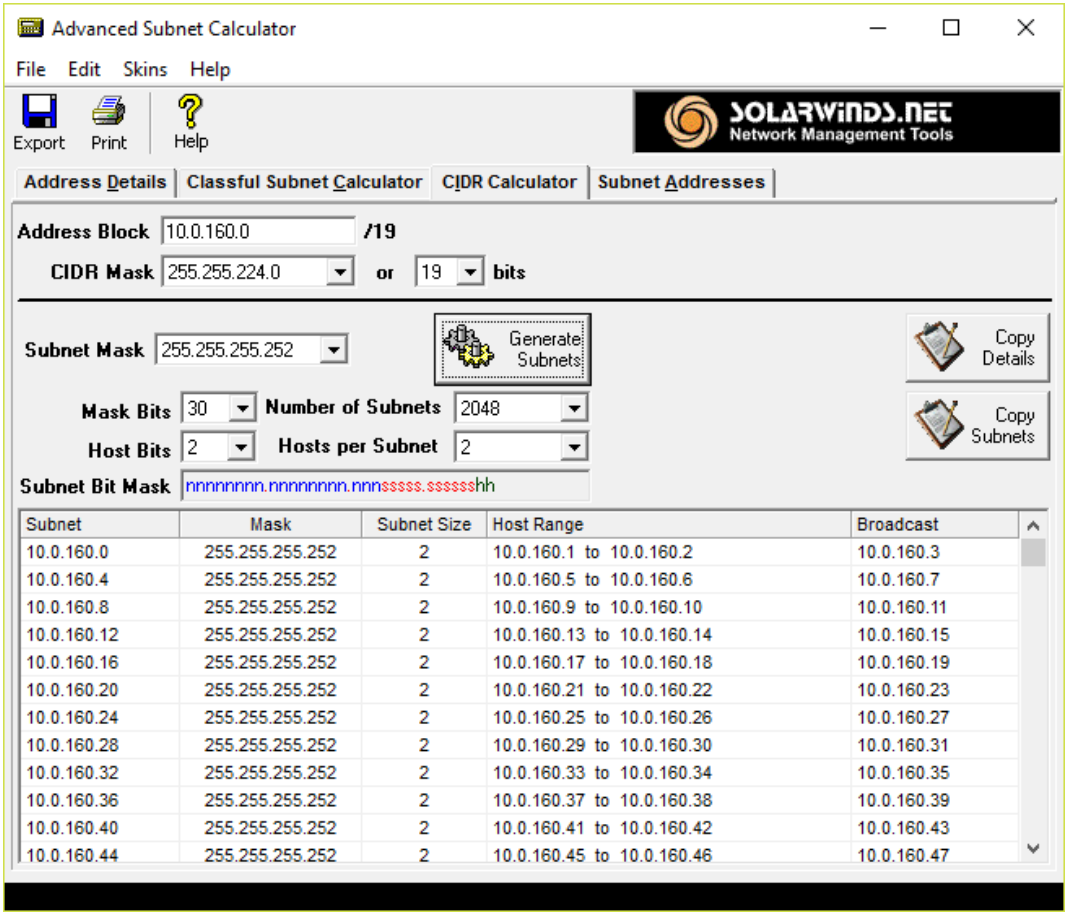


Рис. 3.3. Розбиття мережі 10.0.160.0/19 на підмережі з двома індивідуальними IP-адресами

Таблиця 3.2

Результати розбиття мережі 10.0.160.0/19 на підмережі з 2 вузлами

Номер з/п	Підмережа	Маска	Кількість вузлів	Діапазон адрес	Широкомовна адреса
1	10.0.160.0/30	255.255.255.252	2	10.0.160.1 – 10.0.160.2	10.0.160.3
2	10.0.160.4/30	255.255.255.252	2	10.0.160.5 – 10.0.160.6	10.0.160.7
3	10.0.160.8/30	255.255.255.252	2	10.0.160.9 – 10.0.160.10	10.0.160.11
4	10.0.160.12/30	255.255.255.252	2	10.0.160.13 – 10.0.160.14	10.0.160.15
5	10.0.160.16/30	255.255.255.252	2	10.0.160.17 – 10.0.160.18	10.0.160.19
6	10.0.160.20/30	255.255.255.252	2	10.0.160.21 – 10.0.160.22	10.0.160.23
7	10.0.160.24/30	255.255.255.252	2	10.0.160.25 – 10.0.160.26	10.0.160.27
8	10.0.160.28/30	255.255.255.252	2	10.0.160.29 – 10.0.160.30	10.0.160.31

На рис. 3.4 показана схема IP-мережі з результатами розбиття загального адресного простору 10.10.0.0/16 на відповідні підмережі.

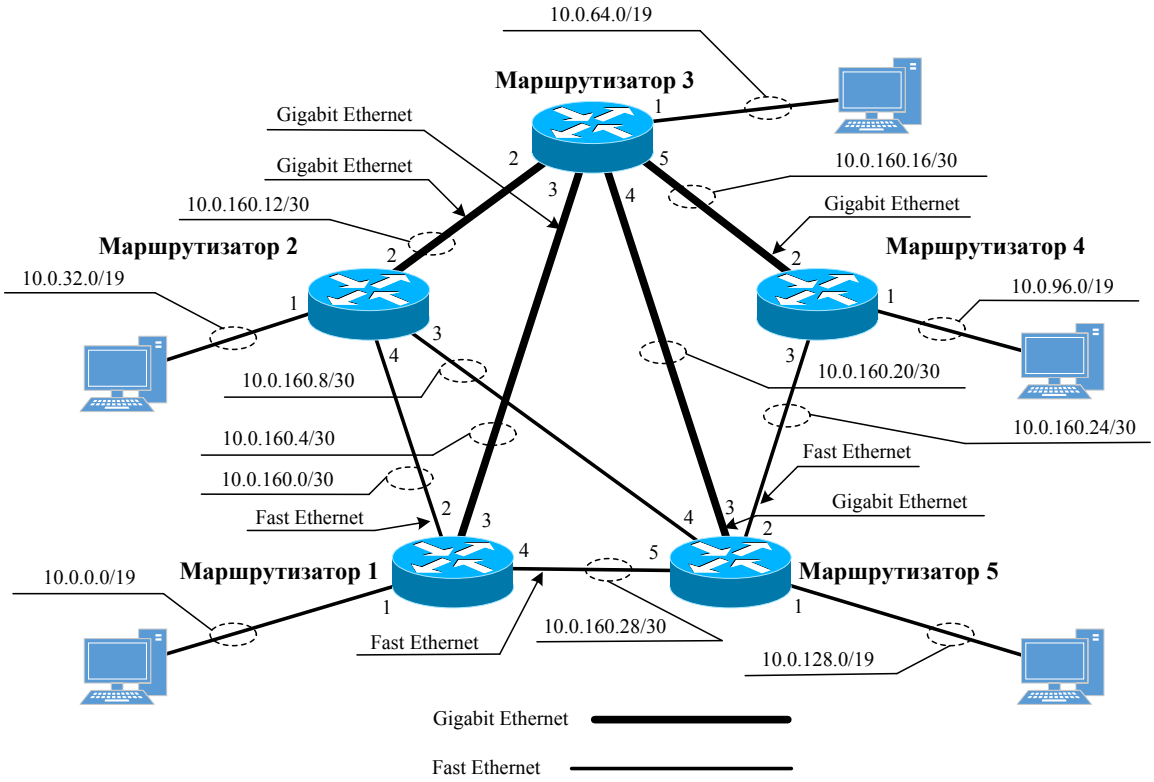


Рис. 3.4. Схема IP-мережі з результатами розбиття загального адресного простору 10.10.0.0/16 на відповідні підмережі

3.4. Розподіл IP-адрес. Визначення мережевих параметрів обладнання

Результом розбиття загального адресного простору є підмережі для підключення обладнання користувачів, а також підмережі для з'єднання між собою маршрутизаторів. Виконаємо розподіл IP-адрес в утворених підмережах і визначимо мережеві параметри для кожного з портів кожного маршрутизатора та для кожного персонального комп'ютера.

Результати розподілу IP-адрес і визначення мережевих параметрів наведені в табл. 3.3, 3.4. Схема IP-мережі з результатами визначення мережевих параметрів обладнання показана на рис. 3.5.

Таблиця 3.3

Мережеві параметри портів маршрутизаторів

Пристрій	Мережевий параметр порту			IP-адреса порту суміжного маршрутизатора (шлюзу)
	Інтерфейс/ номер порту	IP-адреса	Маска	
Маршрутизатор 1	Fa 1/0	10.0.0.1	255.255.224.0	–
	Fa 2/0	10.0.160.2	255.255.255.252	10.0.160.1
	Gig 3/0	10.0.160.5	255.255.255.252	10.0.160.6
	Fa 4/0	10.0.160.29	255.255.255.252	10.0.160.30
Маршрутизатор 2	Fa 1/0	10.0.32.1	255.255.224.0	–
	Gig 2/0	10.0.160.14	255.255.255.252	10.0.160.13
	Fa 3/0	10.0.160.9	255.255.255.252	10.0.160.10
	Fa 4/0	10.0.160.1	255.255.255.252	10.0.160.2
Маршрутизатор 3	Fa 1/0	10.0.64.1	255.255.224.0	–
	Gig 2/0	10.0.160.13	255.255.255.252	10.0.160.14
	Gig 3/0	10.0.160.6	255.255.255.252	10.0.160.5
	Gig 4/0	10.0.160.21	255.255.255.252	10.0.160.22
	Gig 5/0	10.0.160.17	255.255.255.252	10.0.160.18
Маршрутизатор 4	Fa 1/0	10.0.96.1	255.255.224.0	–
	Gig 2/0	10.0.160.18	255.255.255.252	10.0.160.17
	Fa 3/0	10.0.160.26	255.255.255.252	10.0.160.25
Маршрутизатор 5	Fa 1/0	10.0.128.1	255.255.224.0	–
	Fa 2/0	10.0.160.25	255.255.255.252	10.0.160.26
	Gig 3/0	10.0.160.22	255.255.255.252	10.0.160.21
	Fa 4/0	10.0.160.10	255.255.255.252	10.0.160.9
	Fa 5/0	10.0.160.30	255.255.255.252	10.0.160.29

Таблиця 3.4

Мережеві параметри персональних комп’ютерів

Пристрій	Мережевий параметр			IP-адреса порту суміжного маршрутизатора (шлюзу)
	Інтерфейс/ номер порту	IP-адреса	Маска	
PC1	Fa 0	10.0.0.2	255.255.224.0	10.0.0.1
PC2	Fa 0	10.0.32.2	255.255.224.0	10.0.32.1
PC3	Fa 0	10.0.64.2	255.255.224.0	10.0.64.1
PC4	Fa 0	10.0.96.2	255.255.224.0	10.0.96.1
PC5	Fa 0	10.0.128.2	255.255.224.0	10.0.128.1

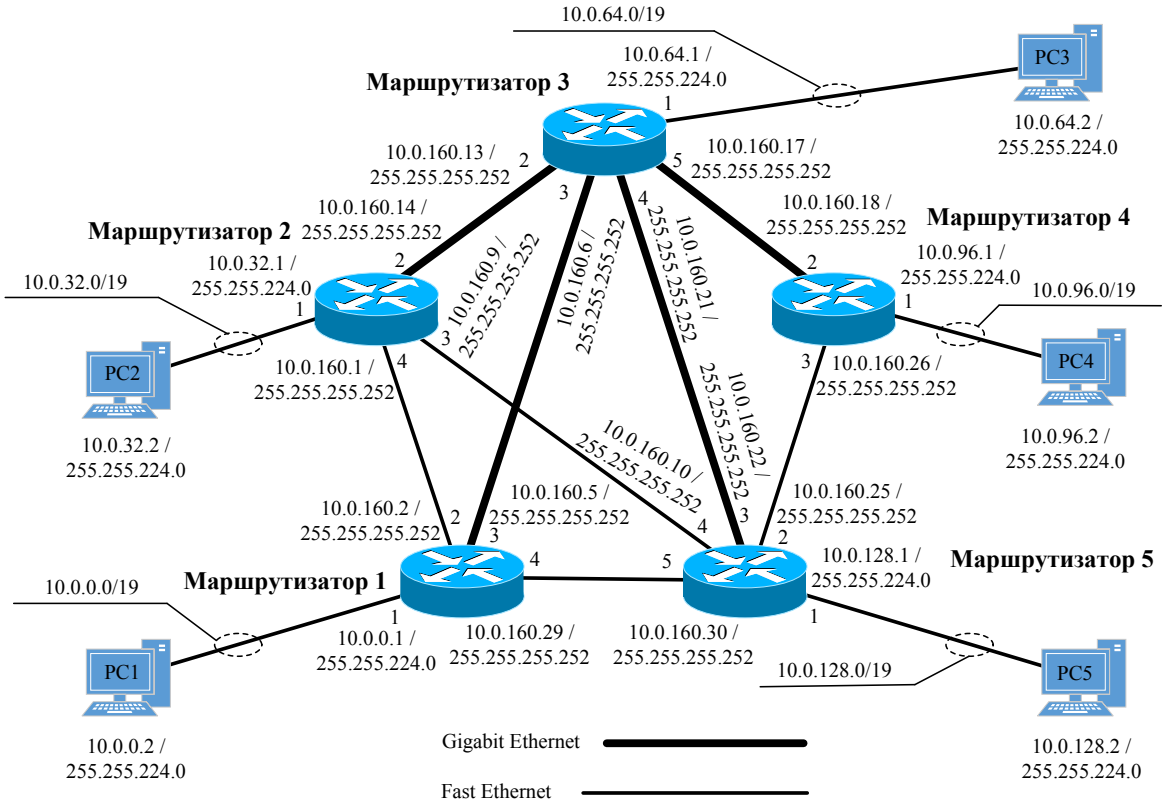


Рис. 3.5. Схема IP-мережі з результатами визначення мережевих параметрів обладнання

3.5. Визначення метрик трактів

Відповідно до розглядуваного завдання критерієм вибору маршруту є пропускна здатність, а метрика тракту зворотно пропорційна пропускній здатності тракту (максимальній швидкості передачі тракту (Мбіт/с). Таким чином, метрики трактів можна розрахувати за формулою

Метрика тракту = 1000 / Максимальна швидкість передачі тракту,

де 1000 – це пропускна здатність, Мбіт/с, відносно якої визначається метрика тракту (може бути вибрано довільне значення, але таке, щоб значення метрик знаходилося в діапазоні 1 ÷ 65535).

Таким чином, відстань (метрика) шляху безпосередньо залежить від швидкості передачі. Маршрутизатори повинні використовувати шлях з найменшою відстанню (найменшою метрикою) як основний шлях. Якщо існує ще один шлях (альтернативний) з більшою відстанню (більшою метрикою), то він не буде використовуватися доти, поки шлях з меншою відстанню (метрикою) залишається доступним.

Проведемо розрахунок:

Метрика тракту Fast Ethernet = 1000 / 100 = 10,

Метрика тракту Gigabit Ethernet = 1000 / 1000 = 1.

3.6. Утворення зваженого графа, відповідного IP-мережі

Утворимо відповідний розглядуваній схемі IP-мережі зважений граф (рис. 3.6), на якому номери вершин будуть відповідати номерам маршрутизаторів, а ваги ребер – метрикам трактів.

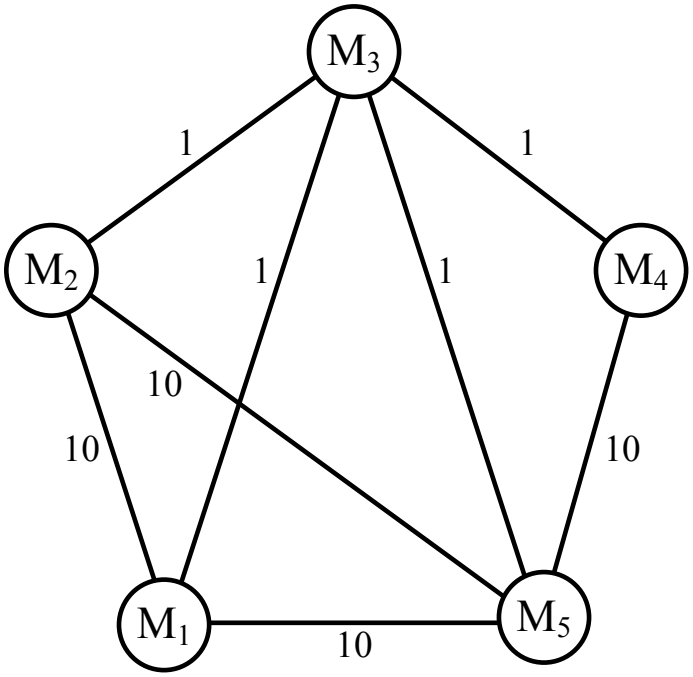


Рис. 3.6. Зважений граф, відповідний схемі IP-мережі

Далі сформуємо матрицю суміжності графа:

$$\begin{pmatrix} 0 & 10 & 1 & \infty & 10 \\ 10 & 0 & 1 & \infty & 10 \\ 1 & 1 & 0 & 1 & 1 \\ \infty & \infty & 1 & 0 & 10 \\ 10 & 10 & 1 & 10 & 0 \end{pmatrix}.$$

3.7. Визначення основних маршрутів

Знайдемо множину найкоротших шляхів в утвореному графі (рис. 3.2) від кожної вершини графа до всіх інших його вершин. Пошук найкоротших шляхів будемо здійснювати з використанням алгоритму Дейкстри. Знайдені найкоротші шляхи будемо вважати основними маршрутами (маршрутами 1-го вибору).

Процедуру пошуку наукоротших шляхів у графі з відображенням всіх його кроків, загальна кількість яких дорівнює кількості вершин графа (кроки мають номери від нуля до числа на одиницю менше, ніж кількість вершин графа), наведено в табл. 3.5 – 3.9, кожна з яких відповідає тільки одному кроку алгоритму Дейкстри. При практичному застосуванні розглядуваної процедури всі кроки алгоритму можуть бути поміщені в одну таблицю і, таким чином, для пошуку найкоротших шляхів від кожної вершини кількість таблиць повинна дорівнювати кількості вершин графа. Зазначимо, що при виконанні завдання покрокове представлення процедури пошуку найкоротших шляхів виконується тільки для однієї довільно вибраної вершини графа, кроки пошуку найкоротших шляхів від інших вершин графа повинні бути представлені в одній таблиці.

Розглянемо покроково процедуру пошуку найкоротших шляхів від вершини M_1 до всіх інших вершин за допомогою алгоритму Дейкстри, користуючись для зручності матрицею суміжності графа, сформованою вище.

Крок 0 (табл. 3.5). Утворюємо таблицю з кількістю рядків, що дорівнює кількості вершин графа, і заносимо до першого рядка (інші рядки залишаються порожніми), що відповідає кроку 0:

– початкову вершину M_1 до стовпця «Множина вершин», який містить множину фіксованих вершин графа на певному кроці;

– метрики ребер графа, що сполучають початкову вершину M_1 з суміжними вершинами (для зручності користуючись заздалегідь сформованою матрицею суміжності графа). Якщо ребро відсутнє, вважаємо що метрика відсутнього ребра має нескінченно велике значення (за бажанням замість знака нескінченності можна поставити прочерк).

Таблиця 3.5

Результати пошуку найкоротших шляхів від вершини M_1 до інших вершин графа (крок 0)

Номер кроку	Множина вершин	Метрика шляху від початкової вершини M_1 до кінцевої вершини шляху на певному кроці			
		M_2	M_3	M_4	M_5
0	$\{M_1\}$	10	1	∞	10
1					
2					
3					
4					

Крок 1 (табл. 3.6). Вибираємо одну з суміжних вершин (M_2, M_3, M_4, M_5) з вершиною на попередньому кроці (M_1 – на кроці 0) за найменшою метрикою шляху від початкової вершини M_1 до суміжних вершин (M_2, M_3, M_4, M_5). Зазначимо, що на кроці 1 метрики шляхів від початкової вершини до інших суміжних з нею вершин будуть визначатися метриками відповідних ребер, оскільки на кроці 1 до кожного зі шляхів входить тільки одне

ребро. Таким чином, вибраною вершиною є вершина M_3, оскільки метрика шляху від початкової вершини M_1 до вершини M_3 є найменшою (значення цієї метрики дорівнює 1). Вибрана таким способом вершина M_3 стає «фіксованою» на кроці 1 (фіксується метрика найкоротшого шляху до неї від початкової вершини). На наступних кроках статус вершини M_3 не зміниться, вона до останнього кроку буде мати статус фіксованої. Таким чином, для позначення того, що вершина M_3 отримала статус фіксованої на кроці 1, занесемо у другий рядок таблиці та стовпець, що відповідає вершині M_3, значення метрики цієї вершини, записаної в дужках; також занесемо цю метрику до всіх інших рядків, що відповідають наступним крокам, після чого заштрихуємо чарунки рядка, відповідного вершині M_3, починаючи з чарунки, до якої була занесена метрика фіксованої вершини M_3 (1 в дужках на кроці 1), до чарунки, що відповідає останньому кроку 4, а також включаємо до множини шляхів фіксовану вершину M_3 (табл. 3.6). Зазначимо, що заштриховані чарунки на наступних кроках не використовуються.

Далі визначаємо метрики шляхів від початкової вершини M_1 до вершин графа на кроці 1 – M_2, M_4, M_5 - шляхом вибору найменшого з двох значень:

– значення метрики на попередньому кроці (кроці 0);

– значення метрики, отриманого шляхом додавання метрики фіксованої вершини на цьому кроці (вершини M_3), що дорівнює 1 (записана в дужках), до метрик ребер між вершиною M_3 та вершинами M_2, M_4, M_5.

Визначені вищевказаним способом метрики шляхів від початкової вершини M_1 до вершин графа на кроці 1 – M_2, M_4, M_5 - записуються у відповідні цим вершинам чарунки в рядку таблиці, який відповідає кроку 1.

Таблиця 3.6

Результати пошуку найкоротших шляхів від вершини M_1 до інших вершин графа (крок 1)

Номер кроку	Множина вершин	Метрика шляху від початкової вершини M_1 до кінцевої вершини шляху на певному кроці			
		M_2	M_3	M_4	M_5
0	$\{M_1\}$	10	1	∞	10
1	$\{M_1, M_3\}$	2	(1)	2	2
2			1		
3			1		
4			1		

Крок 2 (табл. 3.7). Вибираємо одну з вершин (M_2, M_4, M_5) за найменшою метрикою шляху від початкової вершини M_1 до суміжних вершин (M_2, M_4, M_5), а заштриховані чарунки ігноруємо. Зазначимо, що в даному прикладі метрики трьох можливих шляхів є однаковими (всі метрики мають значення 2), що свідчить про існування трьох найкоротших шляхів на цьому кроці. У цьому випадку довільно вибираємо одну з вершин, оскільки метрики всіх вершин однакові (з метою забезпечення однозначності рекомендується завжди вибирати вершину з найменшим номером серед вершин з однаковими метриками). Нехай вибраною вершиною буде вершина M_2, яка стає «фіксованою» на кроці 2. Для позначення того, що вершина M_2 отримала статус фіксованої на кроці 2, занесемо у третій рядок таблиці та стовпець, що відповідає вершині M_2, значення метрики цієї вершини, записаної в дужках; також занесемо цю метрику до всіх інших рядків, що відповідають наступним крокам, після чого заштрихуємо чарунки рядка, відповідного вершині M_2, починаючи з чарунки, до якої була занесена метрика фіксованої вершини M_2 (2 в дужках на кроці 2), до чарунки, що відповідає

останньому кроку 4, а також включаємо до множини шляхів фіксовану вершину M_2 (табл. 3.7). Зазначимо, що заштриховані чарунки на наступних кроках не використовуються.

Далі визначаємо метрики шляхів від початкової вершини M_1 до вершин графа на кроці 2 – M_4, M_5, – шляхом вибору найменшого з двох значень:

– значення метрики на попередньому кроці (кроці 1);

– значення метрики, отриманого шляхом додавання метрики фіксованої вершини на цьому кроці (вершини M_2), що дорівнює 2 (записана в дужках), до метрик ребер між вершиною M_2 та вершинами M_4, M_5.

Визначені вищевказаним способом метрики шляхів від початкової вершини M_1 до вершин графа на кроці 1 – M_4, M_5 – записуються у відповідні цим вершинам чарунки в рядку таблиці, який відповідає кроку 2.

Таблиця 3.7

Результати пошуку найкоротших шляхів від вершини M_1 до інших вершин графа (крок 2)

Номер кроку	Множина вершин	Метрика шляху від початкової вершини M_1 до кінцевої вершини шляху на певному кроці			
		M_2	M_3	M_4	M_5
0	$\{M_1\}$	10	1	∞	10
1	$\{M_1, M_3\}$	2	(1)	2	2
2	$\{M_1, M_3, M_2\}$	(2)	1	2	2
3		2	1		
4		2	1		

Крок 3 (табл. 3.8). Вибираємо одну з вершин (M_4, M_5) за найменшою метрикою шляху від початкової вершини M_1 до

вершин (M_4, M_5), а заштриховані чарунки ігноруємо. Зазначимо, що в даному прикладі метрики двох можливих шляхів є однаковими (всі метрики мають значення 2), що свідчить про існування трьох найкоротших шляхів на цьому кроці. У цьому випадку довільно вибираємо одну з вершин, оскільки метрики всіх вершин однакові (з метою забезпечення однозначності рекомендується завжди вибирати вершину з найменшим номером серед вершин з однаковими метриками). Нехай вибраною вершиною буде вершина M_4, яка стає «фіксованою» на кроці 3. Для позначення того, що вершина M_4 отримала статус фіксованої, на кроці 3 занесемо у четвертий рядок таблиці та стовпець, що відповідає вершині M_4, значення метрики цієї вершини, записаної в дужках; також занесемо цю метрику до всіх інших рядків, що відповідають наступним крокам, після чого заштрихуємо чарунки рядка, відповідного вершині M_4, починаючи з чарунки, до якої була занесена метрика фіксованої вершини M_4 (2 в дужках на кроці 3), до чарунки, що відповідає останньому кроку 4, а також включаємо до множини вершин фіксовану вершину M_4 (табл. 3.8). Зазначимо, що заштриховані чарунки на наступному кроці не використовуються.

Далі розраховуємо метрику шляху від початкової вершини M_1 до вершини графа на кроці 3 − M_5 − шляхом вибору найменшого з двох значень:

− значення метрики на попередньому кроці (кроці 2);

− значення метрики, отриманого шляхом додавання метрики фіксованої вершини на цьому кроці (вершини M_4), що дорівнює 2 (записана в дужках), до метрики ребра між вершиною M_4 та вершиною M_5.

Визначена вищевказаним способом метрика шляху від початкової вершини M_1 до вершини графа на кроці 3 − M_5 − записується у відповідну цій вершині чарунку в рядку таблиці, який відповідає кроку 3 (на кроці 3 це єдний шлях, що відповідає єдиній незаштрихованій чарунці).

Таблиця 3.8

Результати пошуку найкоротших шляхів від вершини M_1 до інших вершин графа (крок 3)

Номер кроку	Множина вершин	Метрика шляху від початкової вершини M_1 до кінцевої вершини шляху на певному кроці			
		M_2	M_3	M_4	M_5
0	$\{M_1\}$	10	1	∞	10
1	$\{M_1, M_3\}$	2	(1)	2	2
2	$\{M_1, M_3, M_2\}$	(2)	1	2	2
3	$\{M_1, M_3, M_2, M_4\}$	2	1	(2)	2
4		2	1	2	

Крок 4 (табл. 3.9). На попередньому кроці 3 залишилася тільки одна незаштрихована чарунка, яка відповідає вершині M_5. Таким чином, вершина 5 стає «фіксованою» на кроці 4. Для позначення того, що вершина M_5 отримала статус фіксованої на кроці 4, занесемо у п’ятий рядок таблиці та стовпець, що відповідає вершині M_5 значення метрики цієї вершини, записаної в дужках, а також заштрихуємо відповідну чарунку. Крім того, вершину M_5 треба включити до стовпця «Множина вершин» рядка таблиці, що відповідає кроку 4.

Таким чином, на кроці 4 була отримана табл. 3.9 з довжинами найкоротших шляхів від початкової вершини M_1 до всіх інших вершин графа. За допомогою цієї таблиці знайдемо найкоротші шляхи, причому пошук будемо проводити у зворотному напрямку, тобто від кінцевої вершини шляху до початкової вершини M_1.

Таблиця 3.9

Результати пошуку найкоротших шляхів від вершини M_1 до інших вершин графа (крок 4)

Номер кроку	Множина вершин	Метрика шляху від початкової вершини M_1 до кінцевої вершини шляху на певному кроці			
		M_2	M_3	M_4	M_5
0	$\{M_1\}$	10	1	∞	10
1	$\{M_1, M_3\}$	2	(1)	2	2
2	$\{M_1, M_3, M_2\}$	(2)	1	2	2
3	$\{M_1, M_3, M_2, M_4\}$	2	1	(2)	2
4	$\{M_1, M_3, M_2, M_4, M_5\}$	2	1	2	(2)

Приклад пошуку найкоротшого шляху від вершини M_1 до вершини M_5 показано в табл. 3.10. Пошук починається з кінцевої вершини M_5. Знайдений найкоротший шлях – $M_5 \rightarrow M_3 \rightarrow M_1$.

Знайдені найкоротші шляхи від вершини M_1 до всіх інших вершин графа за допомогою табл. 3.9:

$M_1 \rightarrow M_3 \rightarrow M_2$ (метрика 2),

$M_1 \rightarrow M_3$ (метрика 1),

$M_1 \rightarrow M_3 \rightarrow M_4$ (метрика 2),

$M_1 \rightarrow M_3 \rightarrow M_5$ (метрика 2).

Таблиця 3.10

Приклад пошуку найкоротшого шляху від вершини M_1 до вершини M_5 (пошук починається з кінцевої вершини M_5, найкоротший шлях – $M_5 \rightarrow M_3 \rightarrow M_1$)

Номер кроку	Множина вершин	Метрика шляху від початкової вершини M_1 до кінцевої вершини шляху на певному кроці			
		M_2	M_3	M_4	M_5
0	$\{M_1\}$	10	1	∞	10
1	$\{M_1, M_3\}$	2	(1)	2	2
2	$\{M_1, M_3, M_2\}$	(2)	1	2	2
3	$\{M_1, M_3, M_2, M_4\}$	2	1	(2)	2
4	$\{M_1, M_3, M_2, M_4, M_5\}$	2	1	2	(2)

Дерево найкоротших шляхів графа від вершини M_1 показано на рис. 3.7.

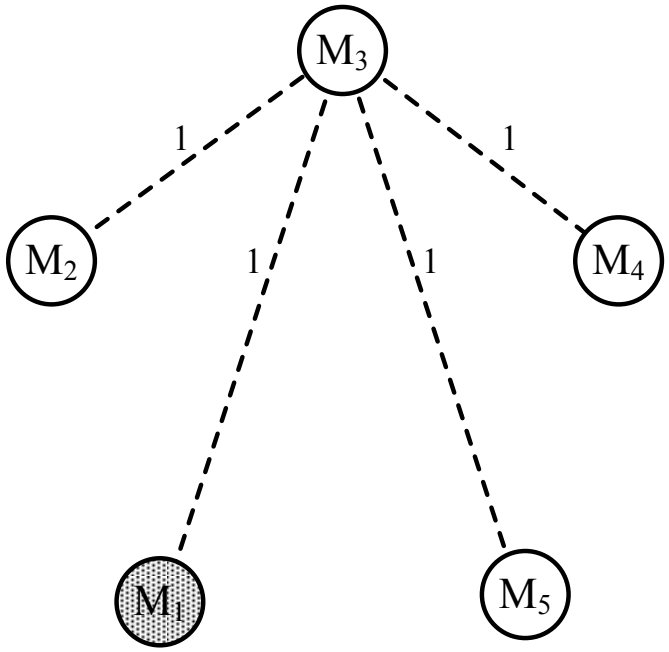


Рис. 3.7. Дерево найкоротших шляхів графа від вершини M_1

Результати пошуку найкоротших шляхів від вершин M_2, M_3, M_4, M_5 до інших вершин графа наведені в табл. 3.11 – 3.14.

Таблиця 3.11

Результати пошуку найкоротших шляхів від вершини M_2 до інших вершин графа

Номер кроку	Множина шляхів	Метрика шляху від початкової вершини M_2 до кінцевої вершини шляху на певному кроці			
		M_1	M_3	M_4	M_5
0	$\{M_2\}$				
1					
2					
3					
4					

Знайдені найкоротші шляхи від вершини M_2 до всіх інших вершин графа:

$M_2 \rightarrow M_3 \rightarrow M_1$ (метрика 2),

$M_2 \rightarrow M_3$ (метрика 1),

$M_2 \rightarrow M_3 \rightarrow M_4$ (метрика 2),

$M_2 \rightarrow M_3 \rightarrow M_5$ (метрика 2).

Таблиця 3.12

Результати пошуку найкоротших шляхів від вершини M_3 до інших вершин графа

Номер кроку	Множина шляхів	Метрика шляху від початкової вершини M_3 до кінцевої вершини шляху на певному кроці			
		M_1	M_2	M_4	M_5
0	$\{M_3\}$				
1					
2					
3					
4					

Знайдені найкоротші шляхи від вершини M_3 до всіх інших вершин графа:

$M_3 \to M_2$ (метрика 1),

$M_3 \to M_1$ (метрика 1),

$M_3 \to M_4$ (метрика 1),

$M_3 \to M_5$ (метрика 1).

Таблиця 3.13

Результати пошуку найкоротших шляхів від вершини M_4 до інших вершин графа

Номер кроку	Множина шляхів	Метрика шляху від початкової вершини M_4 до кінцевої вершини шляху на певному кроці			
		M_1	M_2	M_3	M_5
0	$\{M_4\}$				
1					
2					
3					
4					

Знайдені найкоротші шляхи від вершини M_4 до всіх інших вершин графа:

$M_4 \to M_3 \to M_2$ (метрика 2),

$M_4 \to M_3$ (метрика 1),

$M_4 \to M_3 \to M_1$ (метрика 2),

$M_4 \to M_3 \to M_5$ (метрика 2).

Таблиця 3.14

Результати пошуку найкоротших шляхів від вершини M_5 до інших вершин графа

Номер кроку	Множина шляхів	Метрика шляху від початкової вершини M_5 до кінцевої вершини шляху на певному кроці			
		M_1	M_2	M_3	M_4
0	$\{M_5\}$				
1					
2					
3					
4					

Знайдені найкоротші шляхи від вершини M_5 до всіх інших вершин графа:

$M_5 \to M_3 \to M_2$ (метрика 2),

$M_5 \to M_3$ (метрика 1),

$M_5 \to M_3 \to M_4$ (метрика 2),

$M_5 \to M_3 \to M_1$ (метрика 2).

Дерева найкоротших шляхів графа від вершин M_2, M_3, M_4, M_5 до інших вершин графа показані відповідно на рис. 3.8 – 3.11.

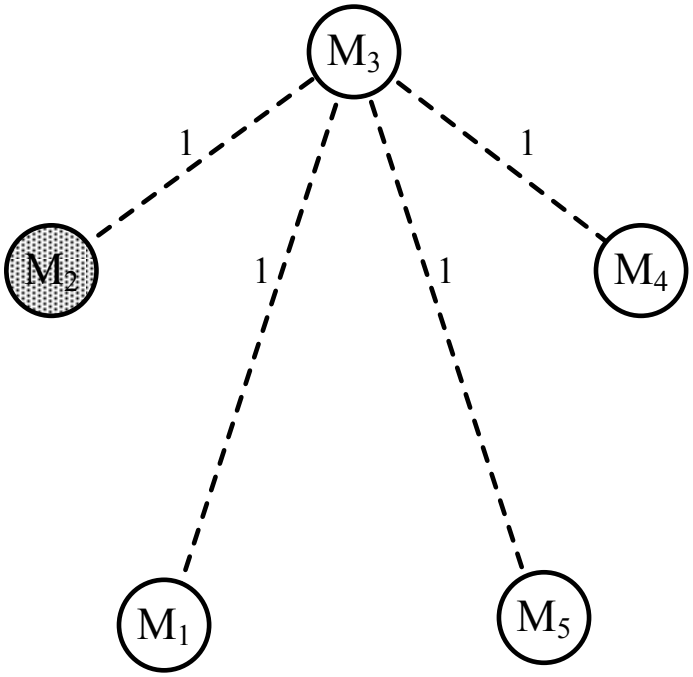


Рис. 3.8. Дерево найкоротших шляхів графа від вершини M_2

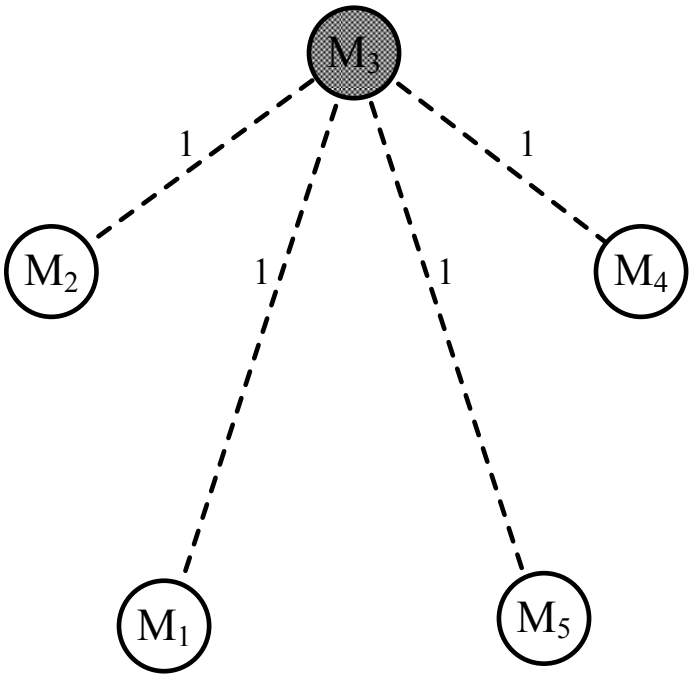


Рис. 3.9. Дерево найкоротших шляхів графа від вершини M_3

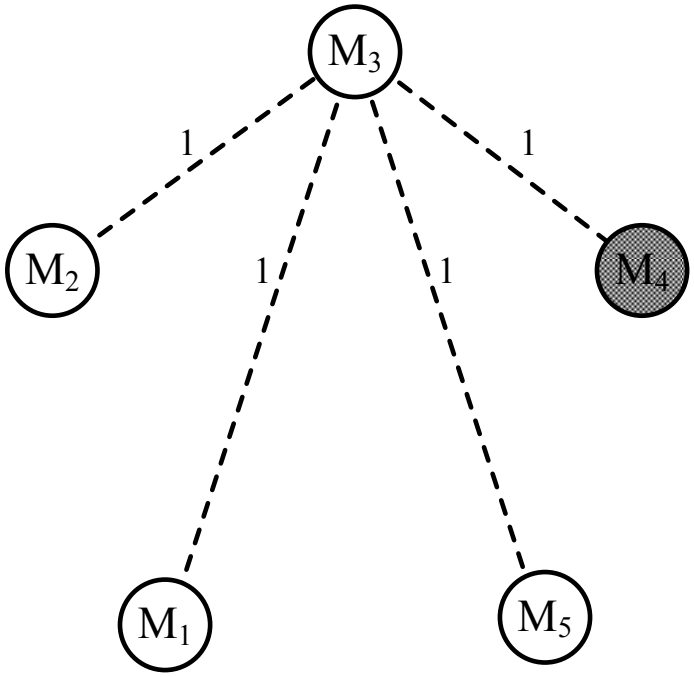


Рисунок 3.10. Дерево найкоротших шляхів графа від вершини M_4

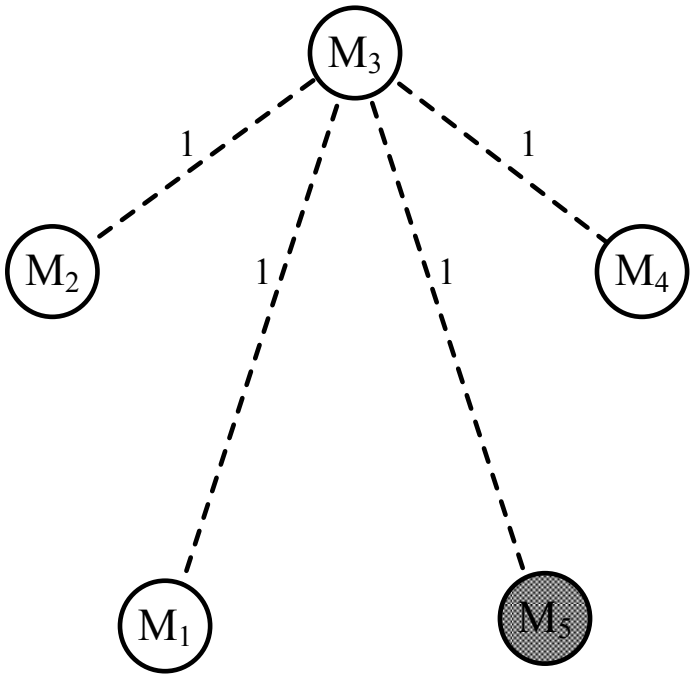


Рис. 3.11. Дерево найкоротших шляхів графа від вершини M_5

3.8. Розроблення таблиць маршрутизації

Розробимо по одній таблиці маршрутизації для кожного маршрутизатора, сформувавши тим самим план розподілу інформації, враховуючи, що в розглядуваній мережі застосована однокрокова маршрутизація, при якій кожний маршрутизатор відповідає тільки за вибір одного кроку маршруту, а повний маршрут забезпечується в результаті сумісної роботи всіх маршрутизаторів, через які проходить IP-пакет. Таким чином, таблиця маршрутизації кожного маршрутизатора буде містити дані тільки про суміжний (наступний, найближчий) маршрутизатор, а не про всі маршрутизатори задаваного маршруту.

Для забезпечення досяжності між підмережами користувачів необхідно до таблиць маршрутизації маршрутизаторів записати відповідні статичні маршрути. Використовучи дерева найкоротших шляхів графа (рис. 3.7 – 3.11), визначаємо для кожного з маршрутизаторів один крок маршруту, тобто суміжний маршрутизатор, який буде наступним при відправленні IP-пакета у відповідну мережу користувачів. Розроблені таблиці маршрутизації, що містять статичні маршрути, наведені в табл. 3.15 – 3.19.

Таблиця 3.15

Таблиця маршрутизації для маршрутизатора 1

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
10.0.32.0	255.255.224.0	10.0.160.6	1
10.0.64.0	255.255.224.0	10.0.160.6	1
10.0.96.0	255.255.224.0	10.0.160.6	1
10.0.128.0	255.255.224.0	10.0.160.6	1

Таблиця 3.16

Таблиця маршрутизації для маршрутизатора 2

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
10.0.0.0	255.255.224.0	10.0.160.13	1
10.0.64.0	255.255.224.0	10.0.160.13	1
10.0.96.0	255.255.224.0	10.0.160.13	1
10.0.128.0	255.255.224.0	10.0.160.13	1

Таблиця 3.17

Таблиця маршрутизації для маршрутизатора 3

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
10.0.0.0	255.255.224.0	10.0.160.5	1
10.0.32.0	255.255.224.0	10.0.160.14	1
10.0.96.0	255.255.224.0	10.0.160.18	1
10.0.128.0	255.255.224.0	10.0.160.22	1

Таблиця 3.18

Таблиця маршрутизації для маршрутизатора 4

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
10.0.0.0	255.255.224.0	10.0.160.17	1
10.0.32.0	255.255.224.0	10.0.160.17	1
10.0.64.0	255.255.224.0	10.0.160.17	1
10.0.128.0	255.255.224.0	10.0.160.17	1

Таблиця 3.19

Таблиця маршрутизації для маршрутизатора 5

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
10.0.0.0	255.255.224.0	10.0.160.21	1
10.0.32.0	255.255.224.0	10.0.160.21	1
10.0.64.0	255.255.224.0	10.0.160.21	1
10.0.96.0	255.255.224.0	10.0.160.21	1

3.9. Перевірка правильності розроблення плану розподілу інформації шляхом імітаційного моделювання в програмному середовищі Cisco Packet Tracer

Перевіримо правильність розроблення плану розподілу інформації (досяжність одна одній всіх підмереж складеної IP-мережі) шляхом імітаційного моделювання в програмному середовищі Cisco Packet Tracer.

Створена в програмному середовищі Cisco Packet Tracer імітаційна модель IP-мережі показана на рис. 3.12.

При створенні імітаційної моделі були використані моделі маршрутизаторів типу Generic (з порожніми слотами), у які було встановлено необхідні типи та кількість знімних модулів з електричними портами Fast Ethernet та Gigabit Ethernet. Зазначимо, що нумерація слотів йде справа наліво, а номер першого слоту дорівнює нулю (при створенні імітаційної моделі перший слот не використовувався та залишився порожнім).

Перевірку вмісту таблиць маршрутизації можна виконати за допомогою команди show ip route, яку необхідно вводити в привілейованому режимі. Результати виконання команди show ip route показані на рис. 3.13 – 3.17.

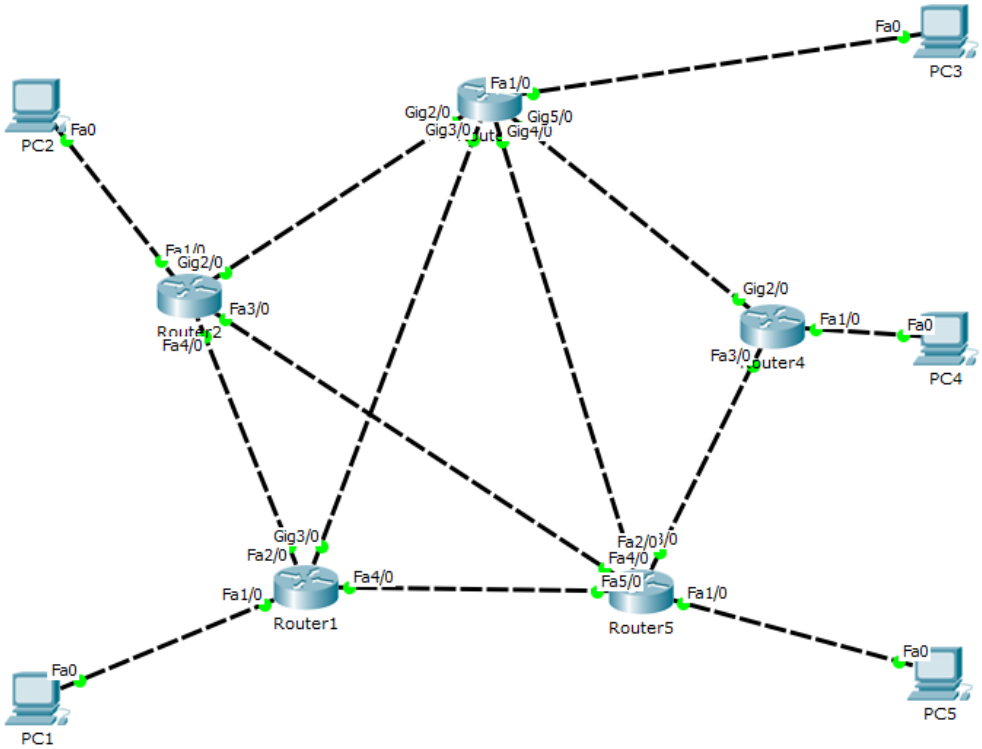


Рис. 3.12. Імітаційна модель IP-мережі, створена в програмному середовищі Cisco Packet Tracer

```
Router1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.0.0.0/19 is directly connected, FastEthernet1/0
S       10.0.32.0/19 [1/0] via 10.0.160.6
S       10.0.64.0/19 [1/0] via 10.0.160.6
S       10.0.96.0/19 [1/0] via 10.0.160.6
S       10.0.128.0/19 [1/0] via 10.0.160.6
C       10.0.160.0/30 is directly connected, FastEthernet2/0
C       10.0.160.4/30 is directly connected, GigabitEthernet3/0
C       10.0.160.28/30 is directly connected, FastEthernet4/0
```

Рис. 3.13. Таблиця маршрутизації маршрутизатора 1

```
Router2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
S       10.0.0.0/19 [1/0] via 10.0.160.13
C       10.0.32.0/19 is directly connected, FastEthernet1/0
S       10.0.64.0/19 [1/0] via 10.0.160.13
S       10.0.96.0/19 [1/0] via 10.0.160.13
S       10.0.128.0/19 [1/0] via 10.0.160.13
C       10.0.160.0/30 is directly connected, FastEthernet4/0
C       10.0.160.8/30 is directly connected, FastEthernet3/0
C       10.0.160.12/30 is directly connected, GigabitEthernet2/0
```

Рис. 3.14. Таблиця маршрутизації маршрутизатора 2

```
Router3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
S       10.0.0.0/19 [1/0] via 10.0.160.5
S       10.0.32.0/19 [1/0] via 10.0.160.14
C       10.0.64.0/19 is directly connected, FastEthernet1/0
S       10.0.96.0/19 [1/0] via 10.0.160.18
S       10.0.128.0/19 [1/0] via 10.0.160.22
C       10.0.160.4/30 is directly connected, GigabitEthernet3/0
C       10.0.160.12/30 is directly connected, GigabitEthernet2/0
C       10.0.160.16/30 is directly connected, GigabitEthernet5/0
C       10.0.160.20/30 is directly connected, GigabitEthernet4/0
```

Рис. 3.15. Таблиця маршрутизації маршрутизатора 3

```
Router4#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
S       10.0.0.0/19 [1/0] via 10.0.160.17
S       10.0.32.0/19 [1/0] via 10.0.160.17
S       10.0.64.0/19 [1/0] via 10.0.160.17
C       10.0.96.0/19 is directly connected, FastEthernet1/0
S       10.0.128.0/19 [1/0] via 10.0.160.17
C       10.0.160.16/30 is directly connected, GigabitEthernet2/0
C       10.0.160.24/30 is directly connected, FastEthernet3/0
```

Рис. 3.16. Таблиця маршрутизації маршрутизатора 4

```
Router5#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
S       10.0.0.0/19 [1/0] via 10.0.160.21
S       10.0.32.0/19 [1/0] via 10.0.160.21
S       10.0.64.0/19 [1/0] via 10.0.160.21
S       10.0.96.0/19 [1/0] via 10.0.160.21
C       10.0.128.0/19 is directly connected, FastEthernet1/0
C       10.0.160.8/30 is directly connected, FastEthernet4/0
C       10.0.160.20/30 is directly connected, GigabitEthernet3/0
C       10.0.160.24/30 is directly connected, FastEthernet2/0
C       10.0.160.28/30 is directly connected, FastEthernet5/0
```

Рис. 3.17. Таблиця маршрутизації маршрутизатора 5

Також перевірку вмісту таблиць маршрутизації можна виконати за допомогою інструменту перевірки окремих властивостей обладнання (рис. 3.18).

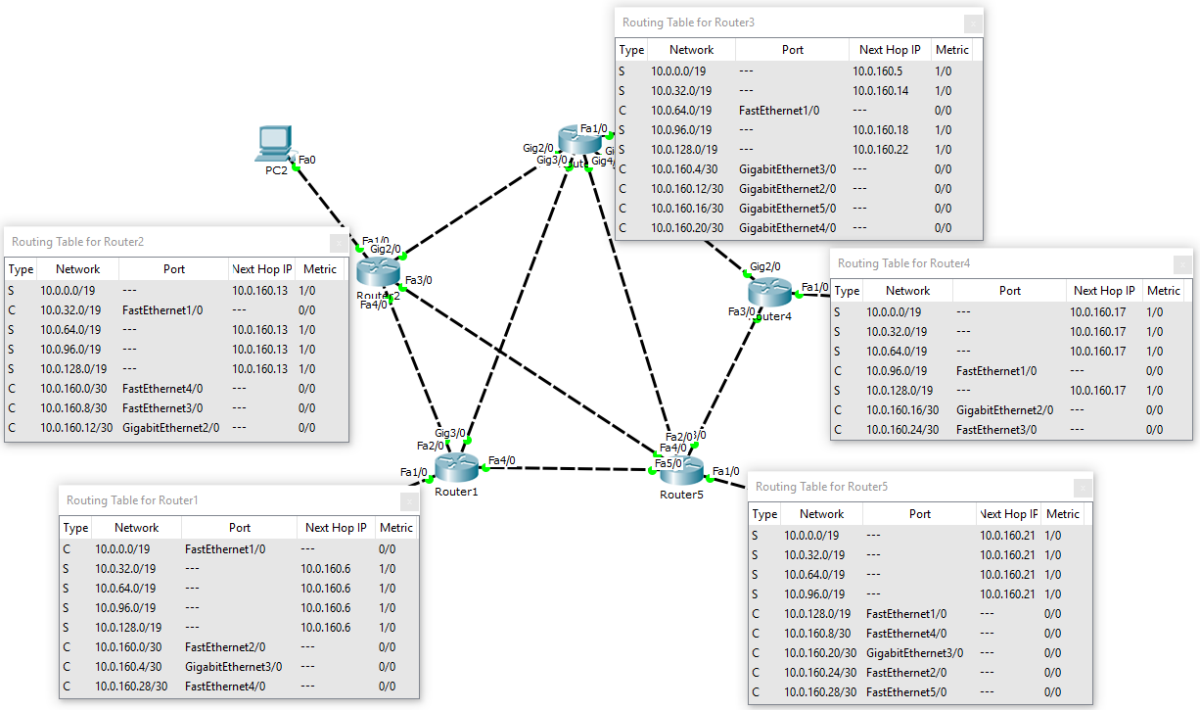


Рис. 3.18. Таблиці маршрутизації маршрутизаторів

З рис. 3.13 – 3.18 видно, що вміст таблиць маршрутизації відповідає розробленому плану розподілу інформації (табл. 3.15 – 3.19). Тепер, використовуючи команду ping або інструмент формування exo-запиту протоколу ICMP, треба впевнитися в тому, що комп'ютери різних сегментів досяжні один одному.

Далі перевіримо маршути передачі exo-запитів протоколу ICMP за допомогою команди tracert {IP-адрес}, яку необхідно вводити до командного рядка відповідного комп'ютера. Результати визначення маршрутів передачі IP-пакетів показані на рис. 3.19 – 3.22.

```
PC>tracert 10.0.32.2

Tracing route to 10.0.32.2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.0.0.1
  2    0 ms      0 ms      0 ms      10.0.160.6
  3    0 ms      0 ms      0 ms      10.0.160.14
  4    0 ms      0 ms      0 ms      10.0.32.2
```

Рис. 3.19. Результати визначення маршруту передачі IP-пакетів від комп'ютера PC1-10.0.0.2 до комп'ютера PC2-10.0.64.2

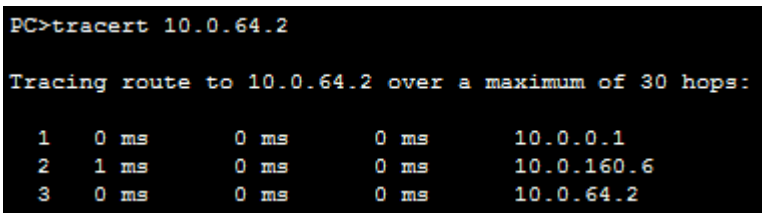


Рис. 3.20. Результати визначення маршруту передачі IP-пакетів від комп'ютера PC1-10.0.0.2 до комп'ютера PC3-10.0.64.2

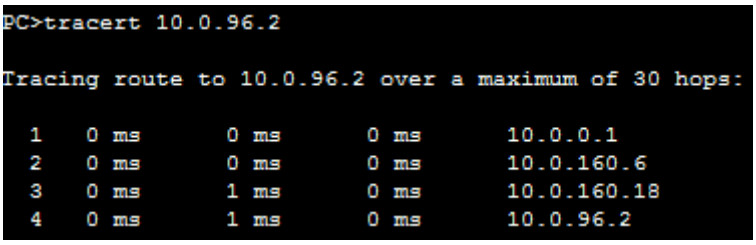


Рис. 3.21. Результати визначення маршруту передачі IP-пакетів від комп'ютера PC1-10.0.0.2 до комп'ютера PC4-10.0.96.2

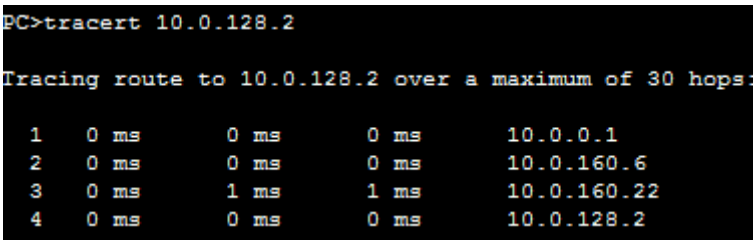


Рис. 3.22. Результати визначення маршруту передачі IP-пакетів від комп'ютера PC1-10.0.0.2 до комп'ютера PC2-10.0.128.2

За результатами визначення маршрутів передачі IP-пакетів (рис. 3.19 – 3.22) на основі рис. 3.9 побудуємо відповідні дерева шляхів і перевіримо їх на відповідність визначеним раніше маршрутам і деревам шляхів, отриманим за допомогою алгоритму Дейкстри (рис. 3.7 – 3.11). Приклад побудови дерева шляхів, коренем якого є маршрутизатор 1, показано на рис. 3.23 (інші дерева шляхів створюються самостійно).

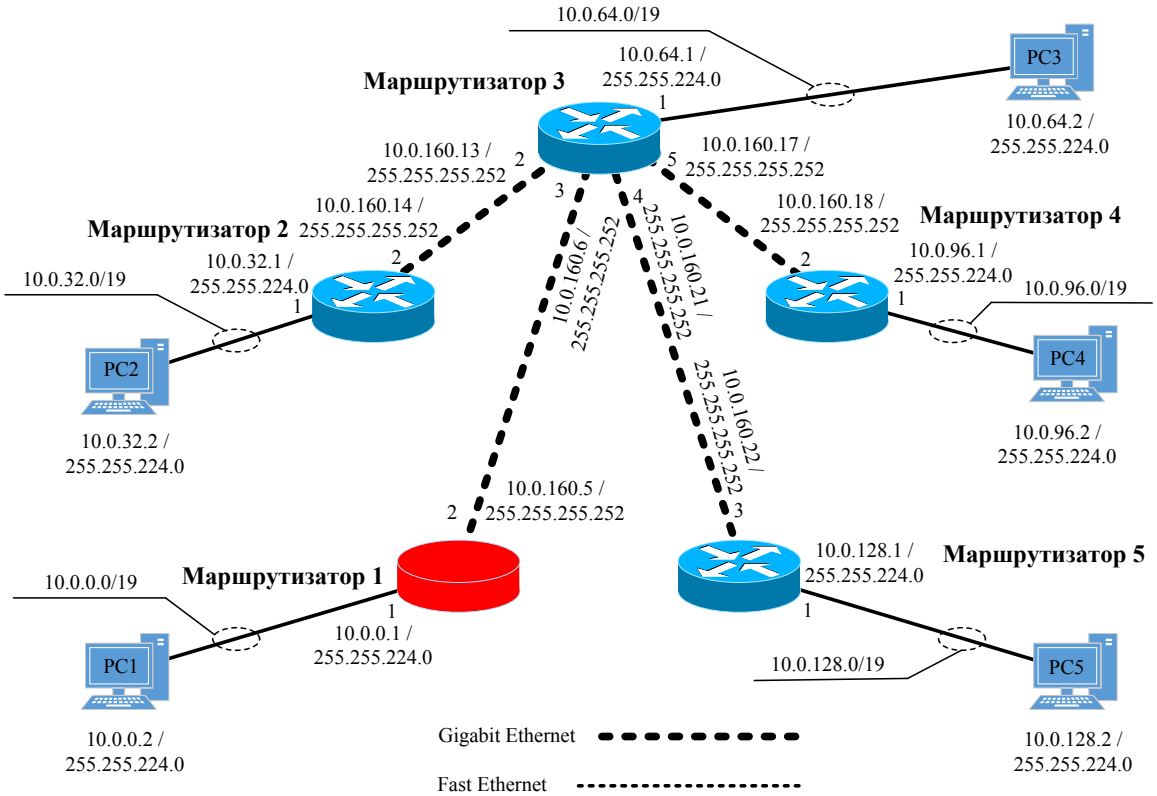


Рис. 3.23. Дерево найкоротших шляхів від маршрутизатора 1 до інших маршрутизаторів IP-мережі

З рис. 3.23 можна зробити висновок про відповідність дерев шляхів, отриманих на основі алгоритму Дейкстри та шляхом імітаційного моделювання, що свідчить про правильність розробленого плану розподілу інформації та коректність конфігурування мережевого обладнання.

4. ОСНОВНІ КОМАНДИ КОМАНДНОГО РЯДКА ОПЕРАЦІЙНОЇ СИСТЕМИ CISCO IOS ДЛЯ КОНФІГУРУВАННЯ СТАТИЧНОЇ МАРШРУТИЗАЦІЇ

Розглянемо основні команди командного рядка операційної системи Cisco IOS для конфігурування статичної маршрутизації.

1. Відображення вмісту таблиці маршрутизації виконується за допомогою команди show ip route, яку необхідно вводити в привілейованому режимі.

Зазначимо, що в таблиці маршрутизації будуть показані тільки маршрути, які використовуються на даний момент (маршрути другого вибору, тобто резервні маршрути будуть відсутні). Усі введені статичні маршрути зберігаються в конфігуруванні маршрутизатора (активному або після збереження активного конфігурування командою copy running-config startup-config – у стартовій), які можна переглянути командою show running-config (show startup-config – для стартового конфігурування) у привілейованому режимі.

2. Конфігурування IP-адреси та маски порту маршрутизатора здійснюється командою ip address {IP-адреса} {маска мережі}, яку необхідно вводити в режимі детального конфігурування відповідного інтерфейсу.

3. Введення статичних маршрутів здійснюється командою ip route {IP-адреса} {маска} {IP-адреса суміжного маршрутизатора або його ім’я} {адміністративна відстань (необов’язково)}, яку необхідно вводити в режимі глобального конфігурування.

Видалення статичних маршрутів здійснюється командою no ip route з тими самими параметрами, які використовувалися при створенні статичного маршруту.

Введення статичного маршруту за замовчуванням здійснюється командою ip route 0.0.0.0 0.0.0.0 {IP-адреса суміжного маршрутизатора або ім’я вихідного інтерфейсу маршрутизатора} {адміністративна відстань (необов’язково)}.

У дод. 1 наведено основні режими конфігурування пристроїв з операційною системою Cisco IOS, а в дод. 2 – контекстну довіру в командному рядку операційної системи Cisco IOS.

5. ОСНОВИ ПРОВЕДЕННЯ ДОСЛІДЖЕННЯ СТАТИЧНОЇ МАРШРУТИЗАЦІЇ В IP-МЕРЕЖІ У ПРОГРАМНОМУ СЕРЕДОВИЩІ CISCO PACKET TRACER

5.1. Створення імітаційної моделі IP-мережі та перевірка її роботи

Рекомендації щодо створення імітаційної моделі схеми IP-мережі в програмному середовищі Cisco Packet Tracer та проведення в ньому дослідження принципів статичної маршрутизації викладемо з використанням у якості прикладу схеми, що показана на рис. 5.1.

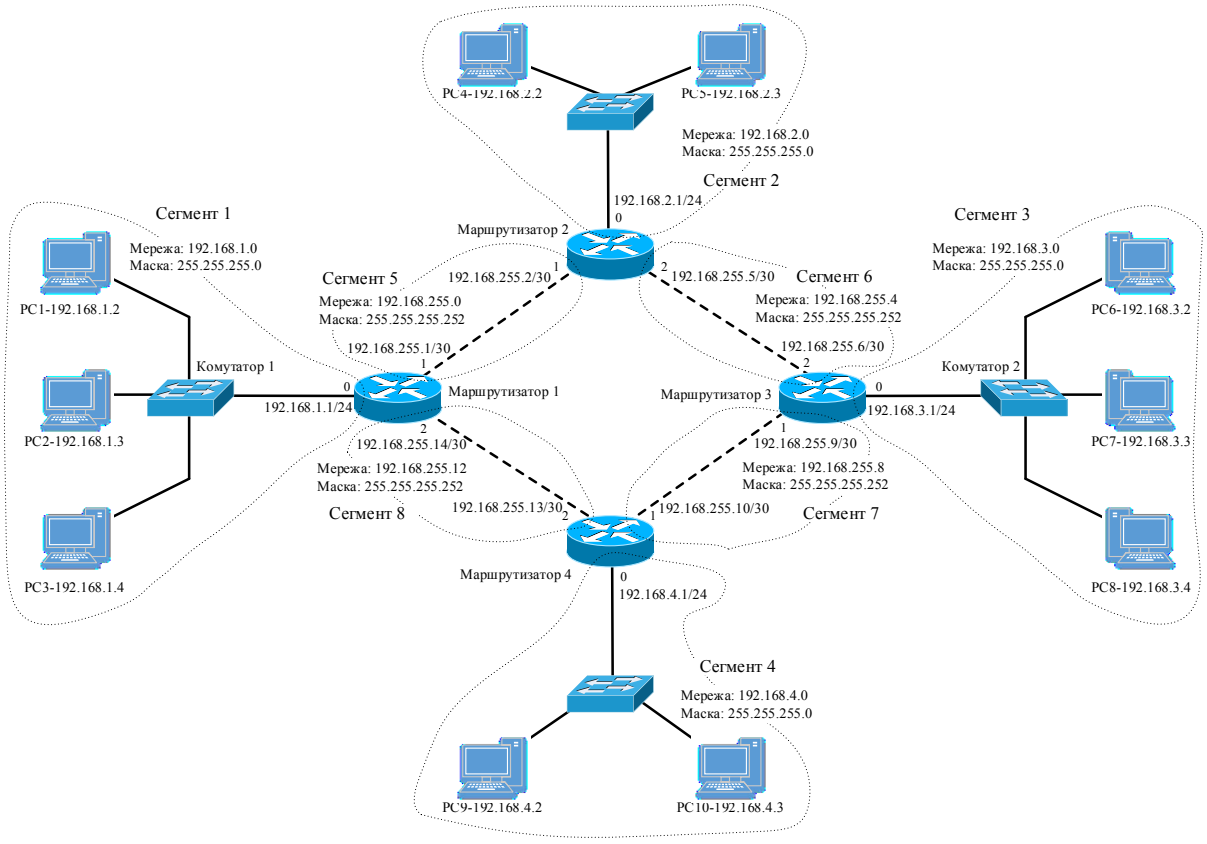


Рис. 5.1. Схема IP-мережі

З рис. 5.1 видно, що імя кожного з комп'ютерів містить його IP-адресу, а до складу мережі входять чотири IP-мережі класу C, адресний простір яких використовується відповідними комп'ютерами (табл. 5.1).

Таблиця 5.1

IP-мережі, адресний простір яких використовується відповідними комп'ютерами

Номер сегмента	Підмережа	Маска	Кількість вузлів	Діапазон адрес	Широкомовна адреса
1	192.168.1.0/24	255.255.255.0	254	192.168.1.1 – 192.168.1.254	192.168.1.255
2	192.168.2.0/24	255.255.255.0	254	192.168.2.1 – 192.168.2.254	192.168.2.255
3	192.168.3.0/24	255.255.255.0	254	192.168.3.1 – 192.168.3.254	192.168.3.255
4	192.168.4.0/24	255.255.255.0	254	192.168.4.1 – 192.168.4.254	192.168.4.255

Для забезпечення з'єднання маршрутизаторів між собою (оскільки кожний з портів маршрутизатора повинен належати окремій IP-мережі) IP-мережа класу C 192.168.255.0/24 була розбита на підмережі з двома вузлами (маска 255.255.255.252 або /30). Вибрані підмережі для з'єднання маршрутизаторів наведені в табл. 5.2.

Таблиця 5.2

Підмережі для з'єднання маршрутизаторів між собою

Номер сегмента	Підмережа	Маска	Кількість вузлів	Діапазон адрес	Широкомовна адреса
5	192.168.255.0	255.255.255.252	2	192.168.255.1 – 192.168.255.2	192.168.255.3
6	192.168.255.4	255.255.255.252	2	192.168.255.5 – 192.168.255.6	192.168.255.7
7	192.168.255.8	255.255.255.252	2	192.168.255.9 – 192.168.255.10	192.168.255.11
8	192.168.255.12	255.255.255.252	2	192.168.255.13 – 192.168.255.14	192.168.255.15

У табл. 5.3 наведено розподіл IP-адрес у розглядуваній IP-мережі.

Таблиця 5.3

Розподіл IP-адрес у розглядуваній IP-мережі

Пристрій	Номер інтерфейсу	Номер сегмента	IP-адреса	Маска	IP-адреса суміжного маршрутизатора (шлюзу)
Маршрутизатор 1	0	1	192.168.1.1/24	255.255.255.0	–
	1	5	192.168.255.1/30	255.255.255.252	192.168.255.2/30
	2	8	192.168.255.14/30	255.255.255.252	192.168.255.13/30
Маршрутизатор 2	0	2	192.168.2.1/24	255.255.255.0	–
	1	5	192.168.255.2/30	255.255.255.252	192.168.255.1/30
	2	6	192.168.255.5/30	255.255.255.252	192.168.255.6/30
Маршрутизатор 3	0	3	192.168.3.1/24	255.255.255.0	–
	1	7	192.168.255.9/30	255.255.255.252	192.168.255.5/30
	2	6	192.168.255.6/30	255.255.255.252	192.168.255.10/30
Маршрутизатор 4	0	4	192.168.4.1/24	255.255.255.0	–
	1	7	192.168.255.10/30	255.255.255.252	192.168.255.9/30
	2	8	192.168.255.13/30	255.255.255.252	192.168.255.14/30
PC1-192.168.1.2	0	1	192.168.1.2/24	255.255.255.0	192.168.1.1/24
PC2-192.168.1.3	0	1	192.168.1.3/24	255.255.255.0	192.168.1.1/24
PC3-192.168.1.4	0	1	192.168.1.4/24	255.255.255.0	192.168.1.1/24
PC4-192.168.2.2	0	2	192.168.2.2/24	255.255.255.0	192.168.2.1/24
PC5-192.168.2.3	0	2	192.168.2.3/24	255.255.255.0	192.168.2.1/24
PC6-192.168.3.2	0	3	192.168.3.2/24	255.255.255.0	192.168.3.1/24
PC7-192.168.3.3	0	3	192.168.3.3/24	255.255.255.0	192.168.3.1/24
PC8-192.168.3.4	0	3	192.168.3.4/24	255.255.255.0	192.168.3.1/24
PC9-192.168.4.2	0	4	192.168.4.2/24	255.255.255.0	192.168.4.1/24
PC10-192.168.4.3	0	4	192.168.4.3/24	255.255.255.0	192.168.4.1/24

Далі, використовуючи дані табл. 5.3, виконаємо введення відповідних масок та IP-адрес до комп’ютерів і маршрутизаторів.

Для введення IP-адреси комп’ютера, маски та IP-адреси шлюзу необхідно в діалоговому вікні властивостей перейти до вкладки Desktop і натиснути на значок IP Configuration. Після цього в поле IP Address треба ввести IP-адресу, в поле Subnet Mask − маску, а в поле Default Gateway − IP-адресу шлюзу (рис. 5.2).

Для конфігурування маршрутизаторів за допомогою графічного інтерфейсу симулятора на кожному з маршрутизаторів необхідно в діалоговому вікні властивостей пристрою вибрати вкладку Config і в меню ліворуч натиснути на кнопку, відповідну необхідному фізичному інтерфейсу маршрутизатора. У поля, що з’являться праворуч, IP Address та Subnet Mask, треба ввести відповідно IP-адресу інтерфейсу маршрутизатора та маску. Після цього треба встановити прапорець у полі On, що призведе до ввімкнення інтерфейсу

маршрутизатора. Приклад конфігурування порту маршрутизатора за допомогою графічного інтерфейсу симулятора показано на рис. 5.3.

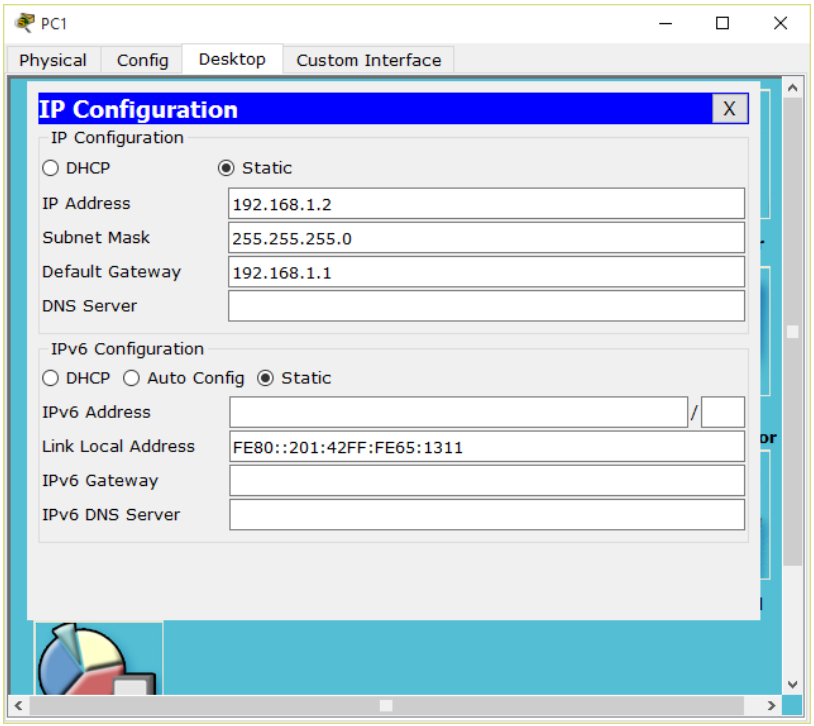


Рис. 5.2. Введення IP-адреси комп’ютера, маски та IP-адреси шлюзу до PC1-192.168.1.2

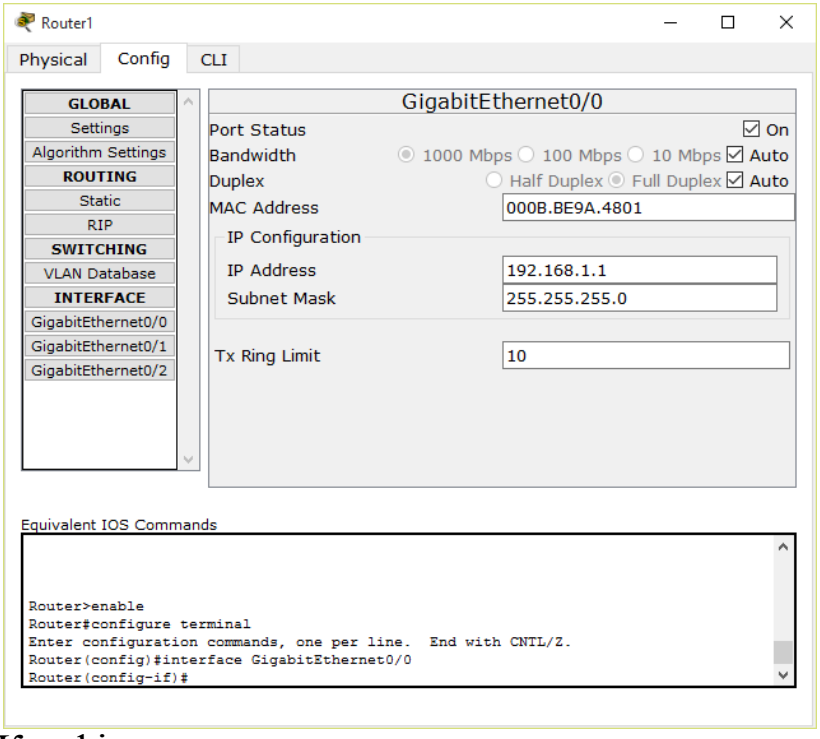


Рис. 5.3. Конфігурування порту маршрутизатора за допомогою графічного інтерфейсу

Також треба установити ім’я маршрутизатора. Для цього в діалоговому вікні властивостей маршрутизатора треба вибрати вкладку Config і в меню ліворуч натиснути на кнопку GLOBAL. Після цього ввести у вікна Display Name та Hostname відповідне ім’я. Приклад встановлення імені маршрутизатора за допомогою графічного інтерфейсу симулятора показано на рис. 5.4.

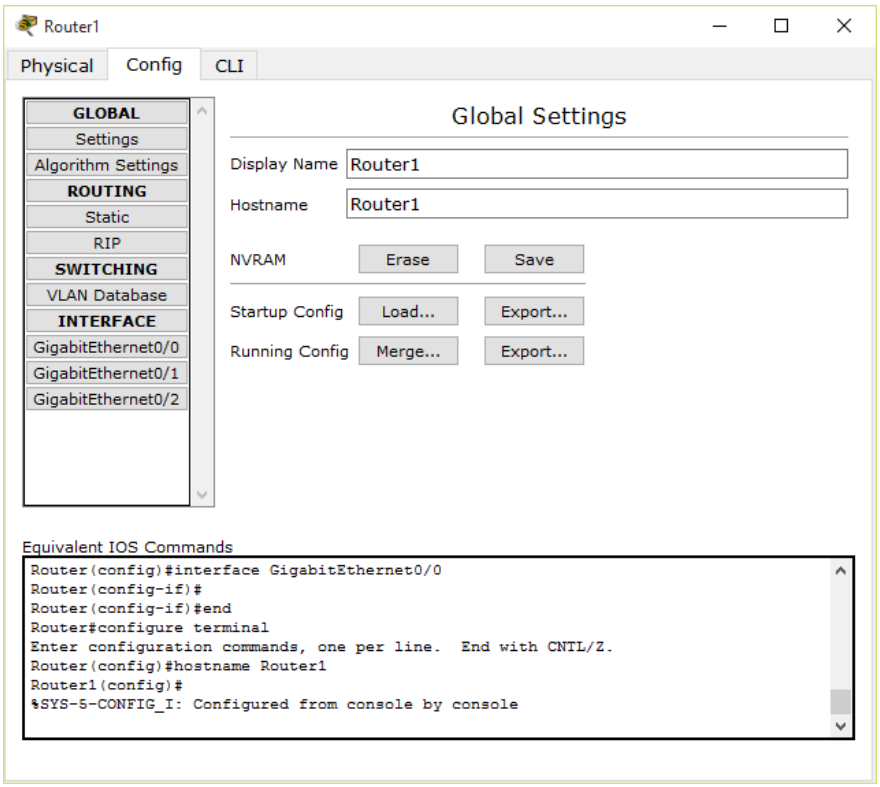


Рис. 5.4. Встановлення імені маршрутизатора за допомогою графічного інтерфейсу

Далі розглянемо варіант конфігурування інтерфейсів маршрутизаторів за допомогою командного рядка операційної системи Cisco IOS на прикладі маршрутизатора 1.

Установлення імені маршрутизатора здійснюється командою hostname{ім’я маршрутизатора}, яку необхідно вводити в привілейованому режимі:

```
Router>enable
Router#configure terminal
Router(config)#hostname Router1.
```

Конфігурування IP-адреси та маски інтерфейсу маршрутизатора здійснюється командою ip address {IP-адреса} {маска мережі}, яку необхідно вводити в режимі детального конфігурування відповідного інтерфейсу.

Розглянемо приклад конфігурування IP-адреси та маски інтерфейсу GigabitEthernet0/0 маршрутизатора 1:

```
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#ip address 192.168.1.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit.
```

Після конфігурування всього обладнання здійснимо перевірку вмісту таблиць маршрутизації маршрутизаторів за допомогою команди show ip route, яку необхідно вводити в привілейованому режимі:

```
Router1#show ip route

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

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
192.168.255.0/24 is variably subnetted, 4 subnets, 2 masks
C 192.168.255.0/30 is directly connected, GigabitEthernet0/1
L 192.168.255.1/32 is directly connected, GigabitEthernet0/1
C 192.168.255.12/30 is directly connected, GigabitEthernet0/2
L 192.168.255.14/32 is directly connected, GigabitEthernet0/2.
```

Також перевірку вмісту таблиць маршрутизації можна виконати за допомогою інструменту перевірки окремих властивостей обладнання (рис. 5.5).

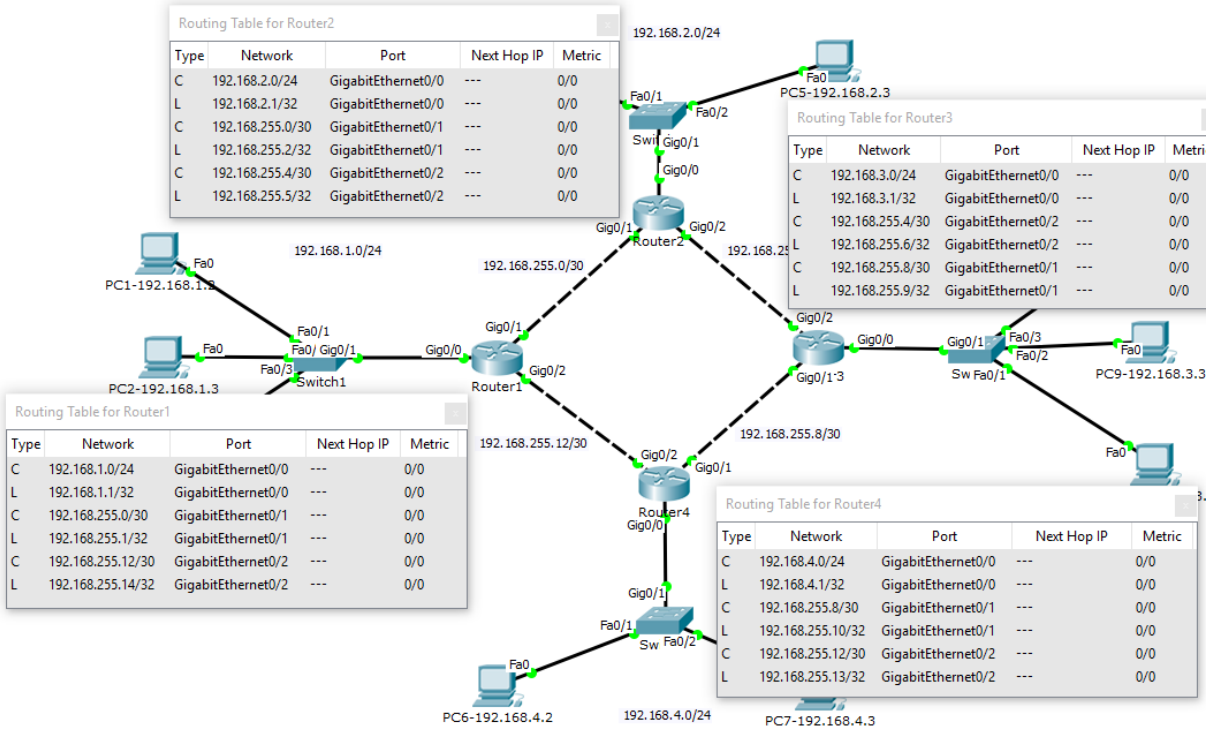


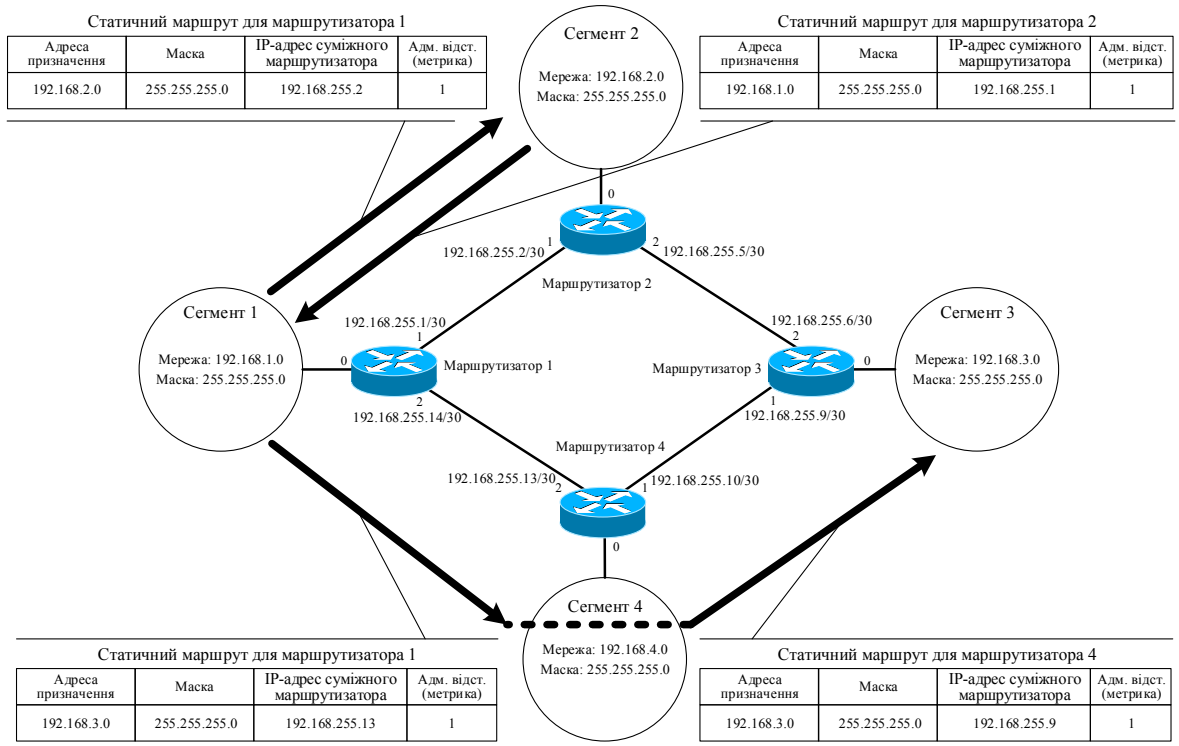
Рис. 5.5. Таблиці маршрутизації до введення статичних маршрутів

Зазначимо, що зараз статичні маршрути ще не введені до таблиць маршрутизації, тому в таблицях маршрутизації будуть міститися тільки дані, які маршрутизатор отримав після введення IP-адрес і масок інтерфейсів.

Далі, використовуючи команду ping або інструмент формування exo-запиту протоколу ICMP, треба впевнитися в тому, що між комп'ютерами різних сегментів зв'язок відсутній. Це відбувається через відсутність відповідних маршрутів у таблицях маршрутизації маршрутизаторів.

Для забезпечення досяжності між різними IP-мережами (різними сегментами розглядуваної мережі) необхідно до таблиць маршрутизації маршрутизаторів записати відповідні статичні маршрути. Зазначимо, що статичні маршрути повинні бути прописані для двох напрямків. Це необхідно для того, щоб IP-пакети змогли досягнути вузла призначення, а IP-пакети, спрямовані від вузла призначення, – досягнути вузла-відправника.

Приклади формування статичних маршрутів показані на рис. 5.6. Зазначимо, що при конфігуруванні маршрутизаторів за допомогою графічного інтерфейсу симулятора введення значень адміністративної відстані маршрутів не передбачено (значення адміністративної відстані всіх маршрутів будуть дорівнювати значенню за замовчуванням − 1, поля для введення значення адміністративної відстані в графічному інтерфейсі не існує).



Шлях проходження IP-пакетів від сегмента 1 до сегмента 3 визначається вмістом таблиць маршрутизації маршрутизаторів 1 та 4

Рис. 5.6. Приклади формування статичних маршрутів

Результати формування необхідних статичних маршрутів для забезпечення повнозв'язності мережі наведено в табл. 5.4 – 5.7.

Таблиця 5.4

Статичні маршрути для маршрутизатора 1

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.2.0	255.255.255.0	192.168.255.2	1
192.168.3.0	255.255.255.0	192.168.255.2	1
192.168.3.0	255.255.255.0	192.168.255.13	1
192.168.4.0	255.255.255.0	192.168.255.13	1

Таблиця 5.5

Статичні маршрути для маршрутизатора 2

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.1	1
192.168.3.0	255.255.255.0	192.168.255.6	1
192.168.4.0	255.255.255.0	192.168.255.6	1
192.168.4.0	255.255.255.0	192.168.255.1	1

Таблиця 5.6

Статичні маршрути для маршрутизатора 3

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.5	1
192.168.1.0	255.255.255.0	192.168.255.10	1
192.168.2.0	255.255.255.0	192.168.255.5	1
192.168.4.0	255.255.255.0	192.168.255.10	1

Таблиця 5.7

Статичні маршрути для маршрутизатора 4

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.14	1
192.168.2.0	255.255.255.0	192.168.255.9	1
192.168.2.0	255.255.255.0	192.168.255.14	1
192.168.3.0	255.255.255.0	192.168.255.9	1

Для введення статичних маршрутів за допомогою графічного інтерфейсу симулятора на кожному з маршрутизаторів необхідно в діалоговому вікні властивостей пристрою вибрати вкладку Config і в меню ліворуч натиснути на кнопку Static. У поля, що з’являться праворуч, Network, Mask та Next Hop, треба ввести відповідно адресу призначення (IP-адресу

мережі або вузла), маску (якщо адреса призначення – це IP-адреса вузла, то треба вводити 255.255.255.255) та IP-адресу суміжного маршрутизатора, а потім натиснути кнопку Add. Приклад введення статичних маршрутів за допомогою графічного інтерфейсу симулятора показано на рис. 5.7.

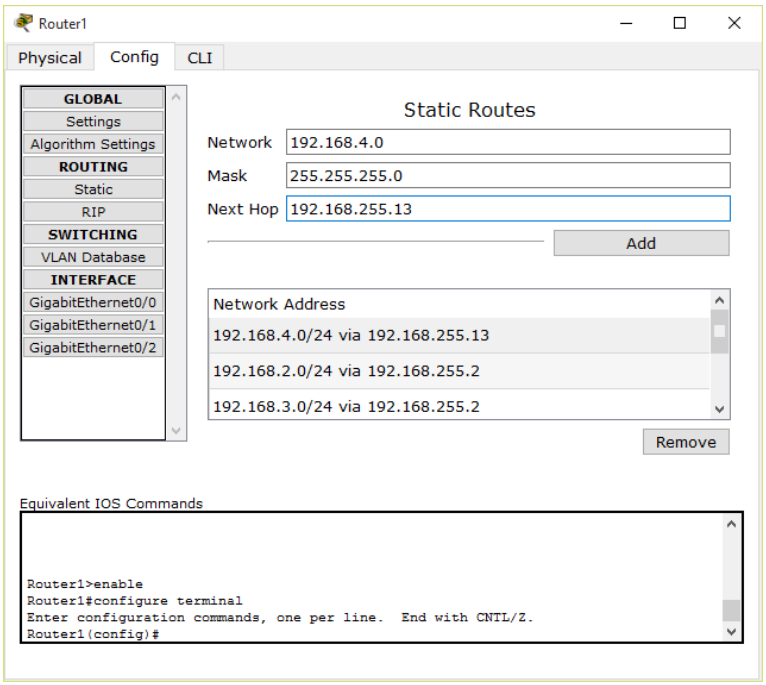


Рис. 5.7. Приклад введення статичних маршрутів за допомогою графічного інтерфейсу симулятора

Далі розглянемо варіант введення статичних маршрутів за допомогою командного рядка операційної системи Cisco IOS.

Введення статичних маршрутів здійснюється командою ip route, яку необхідно вводити в режимі глобального конфігурування:

ip route {IP-адреса} {маска} {IP-адреса суміжного маршрутизатора або його ім’я} {адміністративна відстань (необов’язково)}.

Видалення статичних маршрутів здійснюється командою no ip route з тими самими параметрами, які використовувалися при створенні статичного маршруту.

Розглянемо введення статичних маршрутів за допомогою командного рядка операційної системи Cisco IOS на прикладі маршрутизатора 1 (адміністративну відстань вводити не будемо – використовується її значення за замовчуванням – 1):

```
Router1>enable
Router1#configure terminal
Router1(config)#ip route 192.168.2.0 255.255.255.0 192.168.255.2
Router1(config)#ip route 192.168.3.0 255.255.255.0 192.168.255.2
Router1(config)#ip route 192.168.3.0 255.255.255.0 192.168.255.13
Router1(config)#ip route 192.168.4.0 255.255.255.0 192.168.255.13
Router1(config)#exit
Router1#copy running-config startup-config.
```

Після введення статичних маршрутів перевіримо вміст таблиць маршрутизації за допомогою команди show ip route, яку необхідно вводити в привілейованому режимі:

```
Router1#show ip route

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

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
S 192.168.2.0/24 [1/0] via 192.168.255.2
S 192.168.3.0/24 [1/0] via 192.168.255.2
                 [1/0] via 192.168.255.13
S 192.168.4.0/24 [1/0] via 192.168.255.13
```

192.168.255.0/24 is variably subnetted, 4 subnets, 2 masks
C 192.168.255.0/30 is directly connected, GigabitEthernet0/1
L 192.168.255.1/32 is directly connected, GigabitEthernet0/1
C 192.168.255.12/30 is directly connected, GigabitEthernet0/2
L 192.168.255.14/32 is directly connected, GigabitEthernet0/2.

Також перевірку вмісту таблиць маршрутизації можна виконати за допомогою інструменту перевірки окремих властивостей обладнання (рис. 5.8).

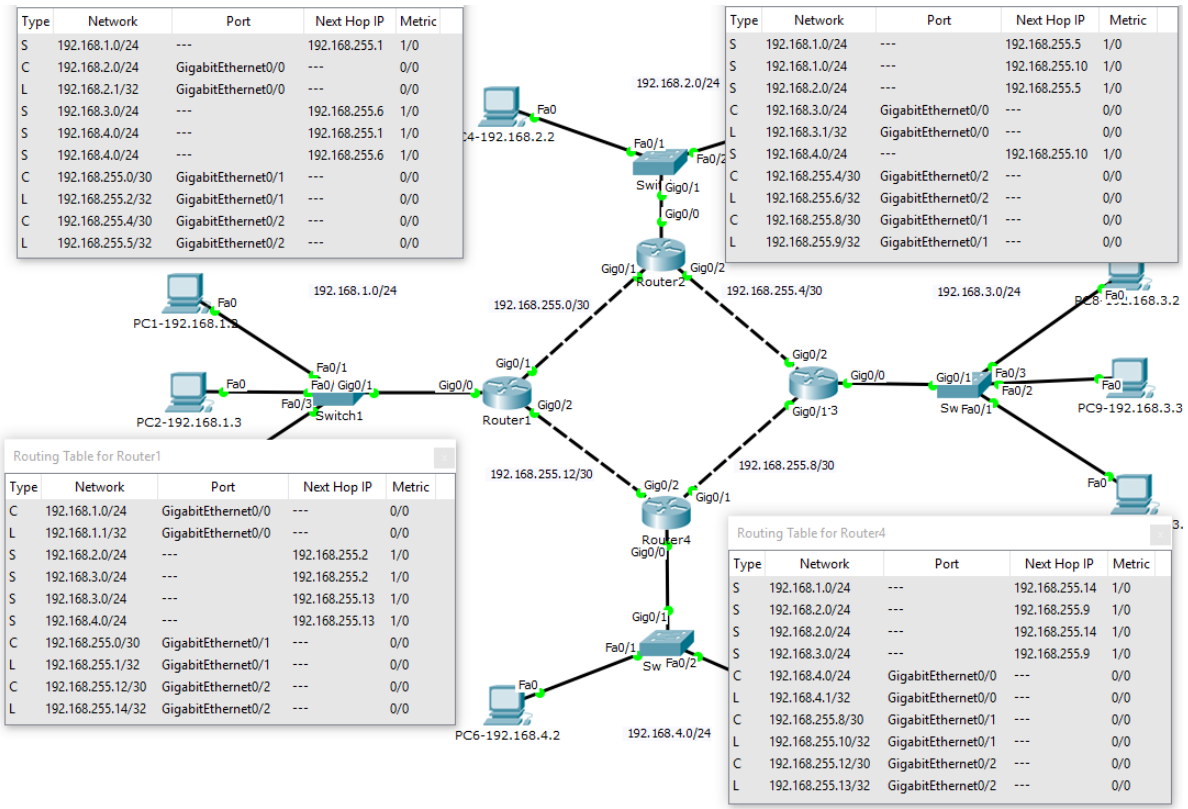


Рис. 5.8. Таблиці маршрутизації після введення статичних маршрутів

Далі, використовуючи команду ping або інструмент формування exo-запиту протоколу ICMP, треба впевнитися в тому, що комп’ютери різних сегментів досяжні один одному.

5.2. Дослідження імітаційної моделі IP-мережі в режимі візуального моделювання взаємодії мережевих компонентів та аналіз результатів моделювання

5.2.1. Дослідження процесів передачі IP-пакета до порту маршрутизатора за участю протоколу ARP

Проведемо дослідження принципів передачі IP-пакета до порту маршрутизатора за участю протоколу ARP. Дослідження будемо проводити в режимі візуального моделювання взаємодії мережевих компонентів.

Для підготовки до візуального моделювання необхідно виконати таке:

− натиснути на кнопку режиму візуального моделювання взаємодії мережевих компонентів перемикача режимів для переходу в цей режим;

− налаштувати фільтр протоколів таким чином, щоб візуально відображувалися тільки пакети протоколів ARP та ICMP;

− переконатися, що ARP-таблиця вибраного комп'ютера є порожньою, використовуючи інструмент виклику меню перевірки окремих властивостей обладнання (збільшуване скло) або команду arp-a, і за необхідності видалити її вміст командою arp-d;

− переконатися, що MAC-таблиця комутатора є порожньою, використовуючи інструмент виклику меню перевірки окремих властивостей обладнання (збільшуване скло) або команду show mac-address-table операційної системи Cisco IOS, яку необхідно вводити в командний рядок в привілейованому режимі:

```
Switch>enable
Switch#show mac-address-table.
```

Якщо MAC-таблиця не є порожньою, треба видалити її вміст командою clear mac-address-table, яку необхідно ввести в командний рядок операційної системи Cisco IOS у привілейованому режимі:

Switch>enable
Switch#clear mac-address-table;

− натиснути на значок інструменту формування ехо-запиту протоколу ICMP, а потім спочатку натиснути на значок PC1-192.168.1.2 (це – передавач ехо-запиту), після чого натиснути на значок PC7-192.168.4.3 (це − отримувач ехо-запиту та передавач ехо-відповіді).

Далі запустимо процес моделювання в покроковому режимі, натиснувши необхідну кількість разів на кнопку Capture/Forward.

Результати моделювання для кожного кроку показано на рис. 5.19 – 5.31.

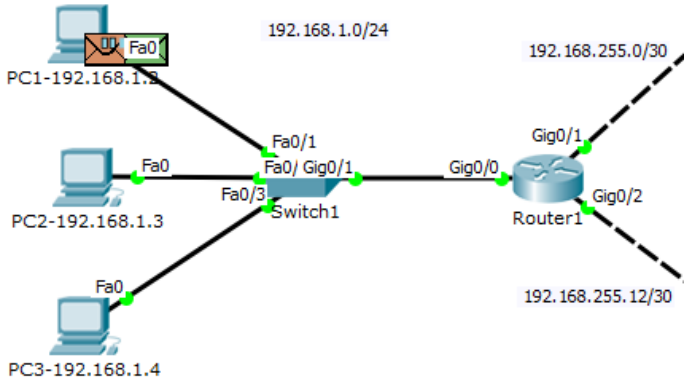


Рис. 5.19. Результати моделювання (крок 1, формування ехо-запиту і широкомовного запиту протоколу ARP)

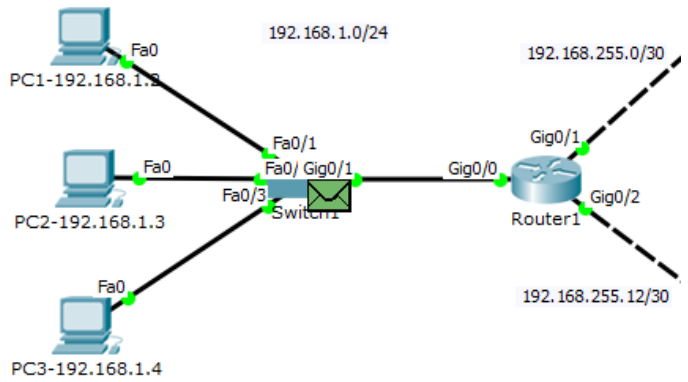


Рис. 5.10. Результати моделювання (крок 2, передача широкомовного запиту протоколу ARP до комутатора)

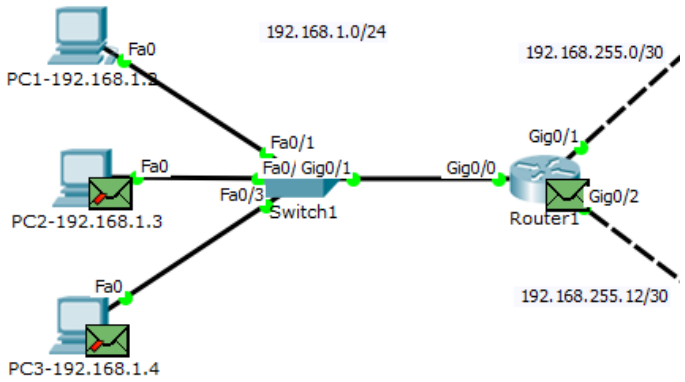


Рис. 5.11. Результати моделювання (крок 3, широкомовне розсилання запиту протоколу ARP комутатором, формування протоколу ARP-відповіді маршрутизатором)

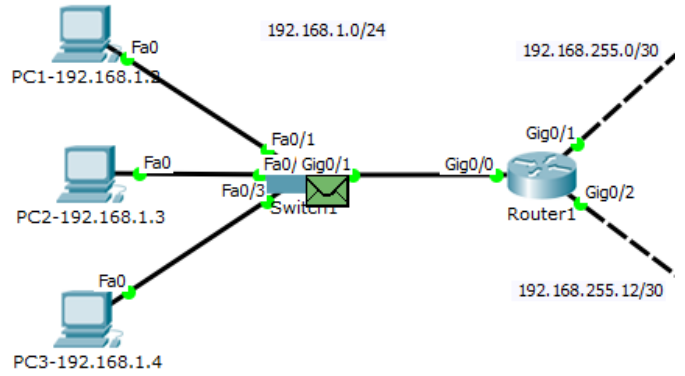


Рис. 5.12. Результати моделювання (крок 4, передача ARP-відповіді)

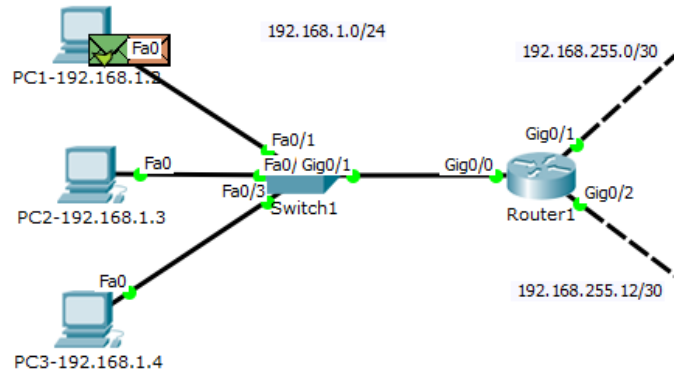


Рис. 5.13. Результати моделювання (крок 5, приймання ARP-відповіді комп’ютером PC1-192.168.1.2)

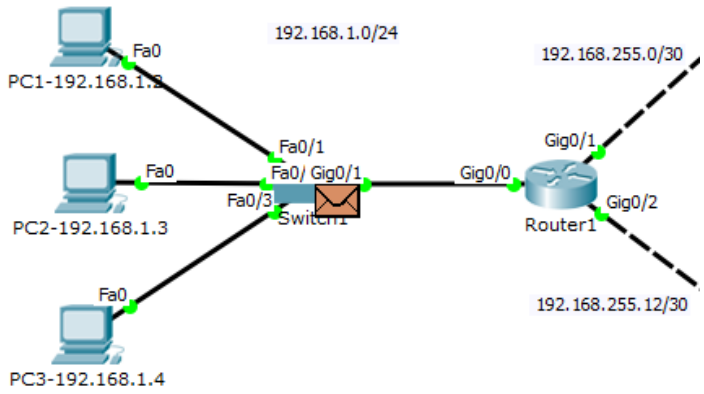


Рис. 5.14. Результати моделювання (крок 6, передача ехо-запиту протоколу ICMP)

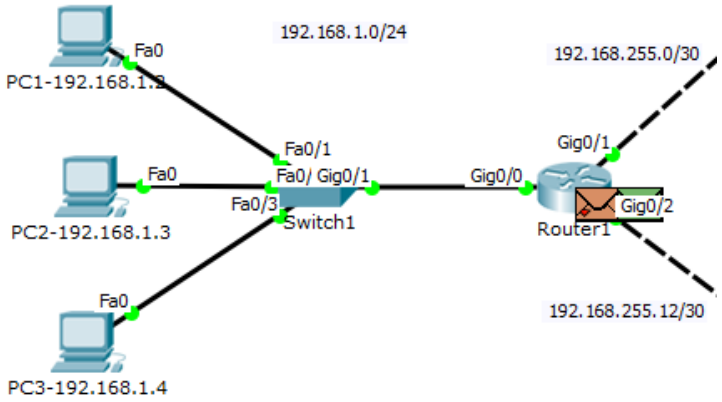


Рис. 5.15. Результати моделювання (крок 7, формування широкомовного запиту протоколу ARP маршрутизатором 1)

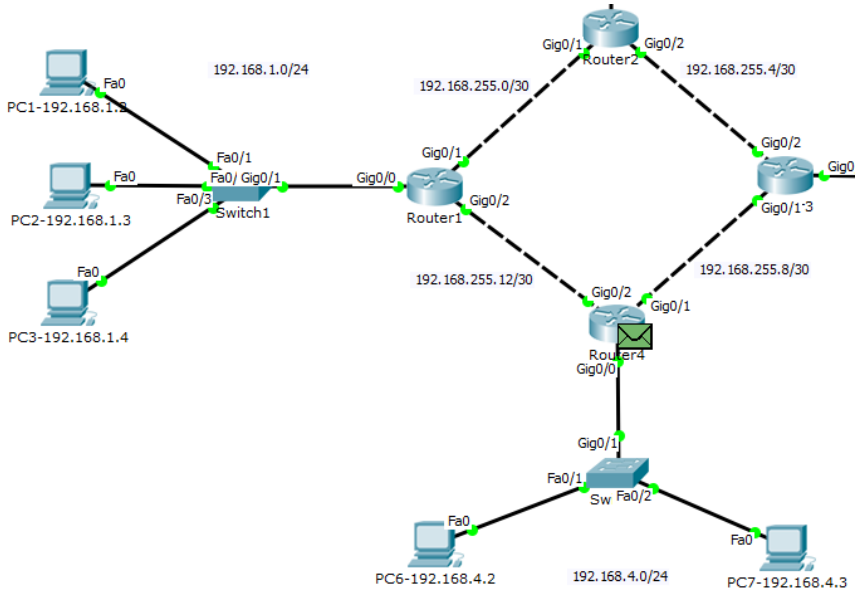


Рис. 5.16. Результати моделювання (крок 8, формування ARP-відповіді маршрутизатором 4)

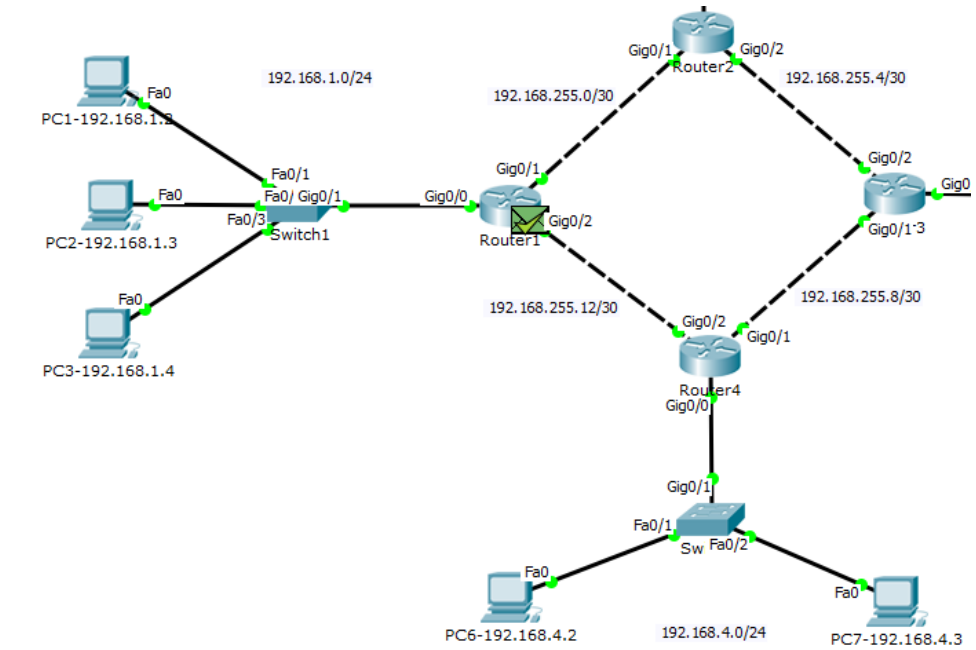


Рис. 5.17. Результати моделювання (крок 9, приймання ARP-відповіді маршрутизатором 1)

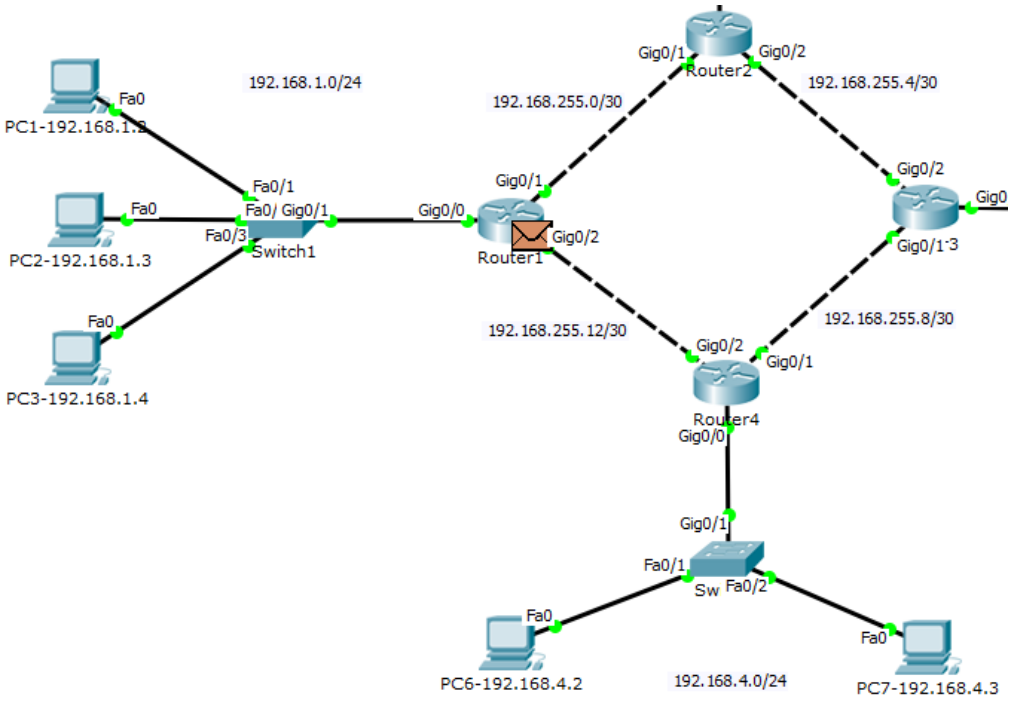


Рис. 5.18. Результати моделювання (крок 10, передача ехо-запиту протоколу ICMP)

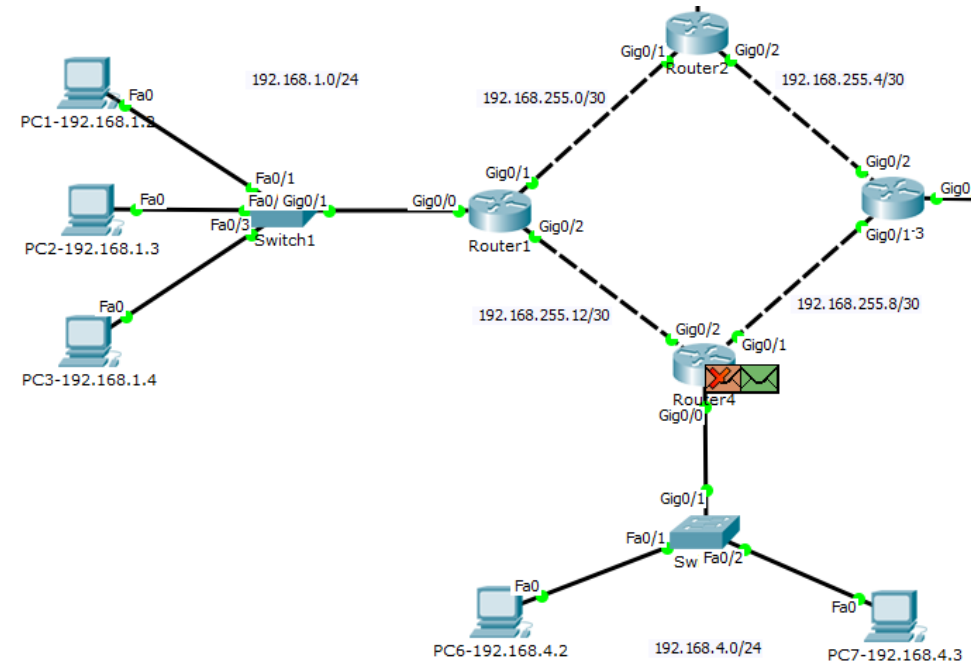


Рис. 5.19. Результати моделювання (крок 11, формування широкомовного запиту протоколу ARP маршрутизатором 4)

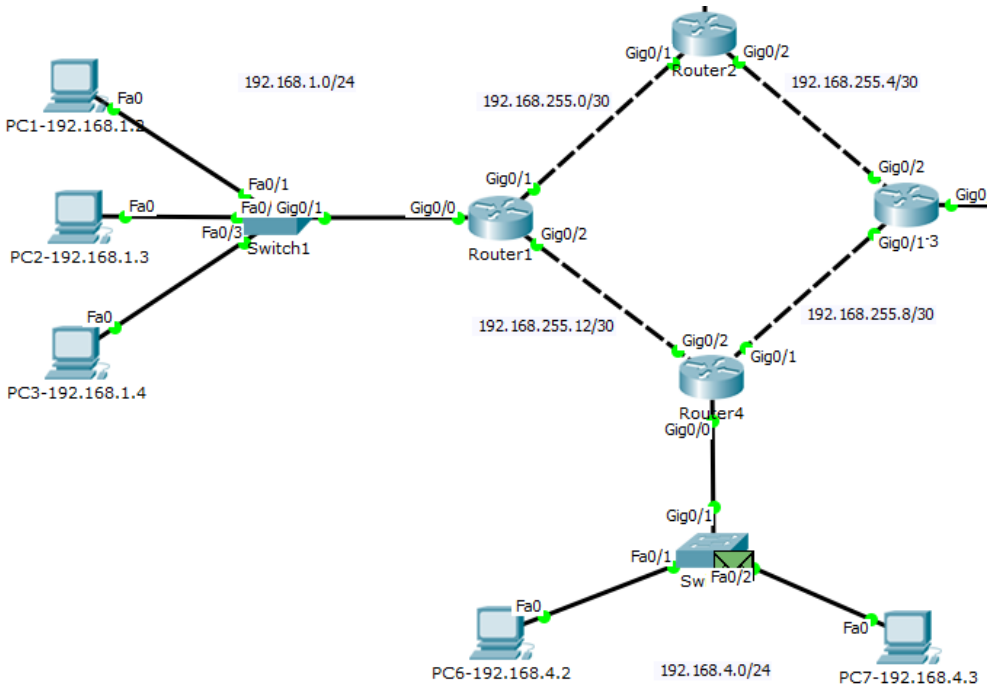


Рис. 5.20. Результати моделювання (крок 12, передача широкомовного запиту протоколу ARP до комутатора)

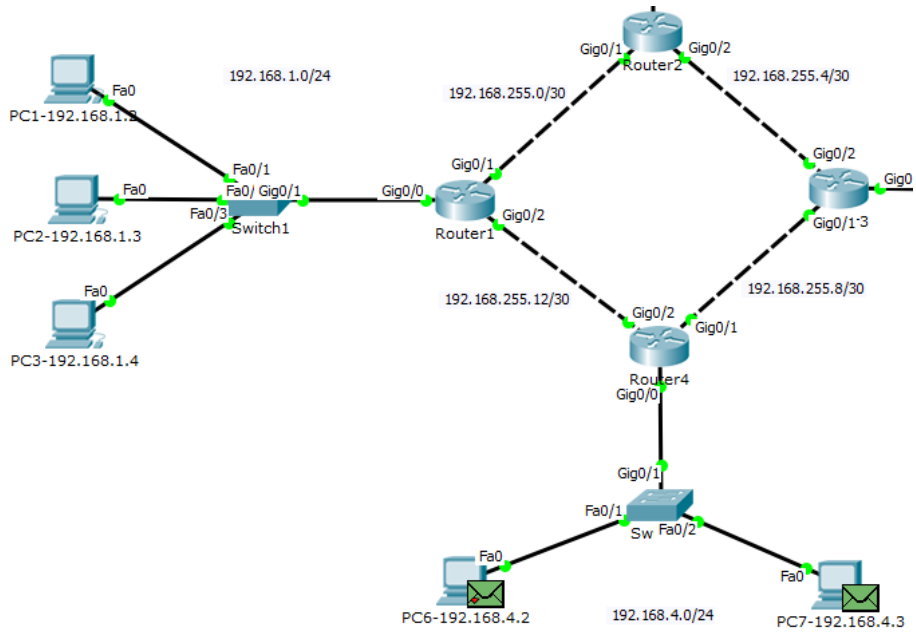


Рис. 5.21. Результати моделювання (крок 13, широкомовне розсилання запиту протоколу ARP комутатором, формування протоколу ARP-відповіді комп’ютером PC7-192.168.4.3)

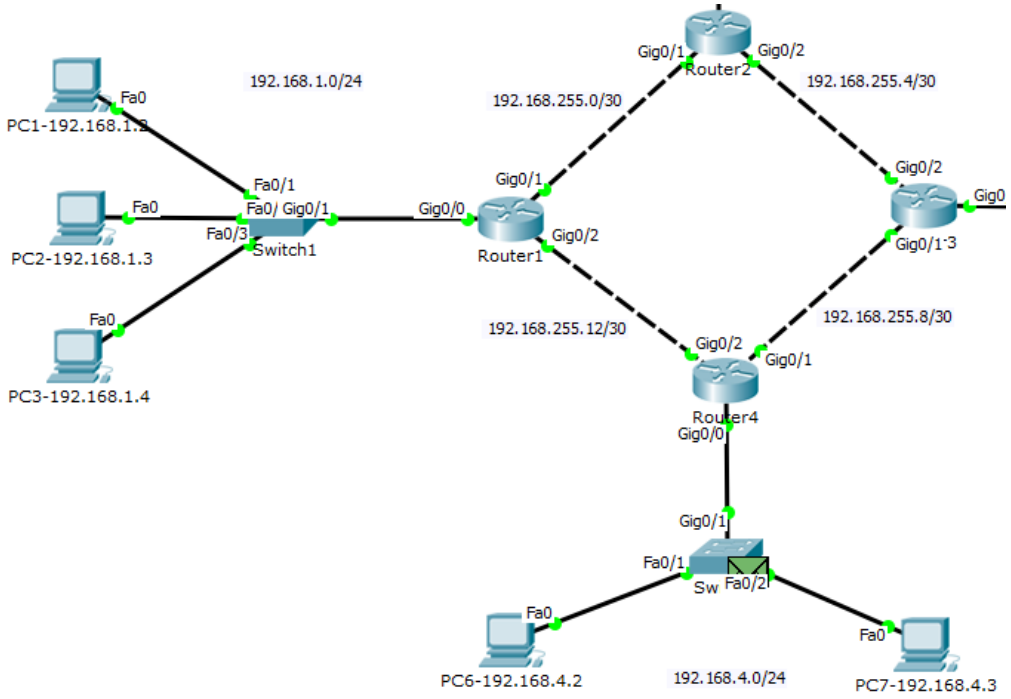


Рис. 5.22. Результати моделювання (крок 14, передача ARP-відповіді комутатором)

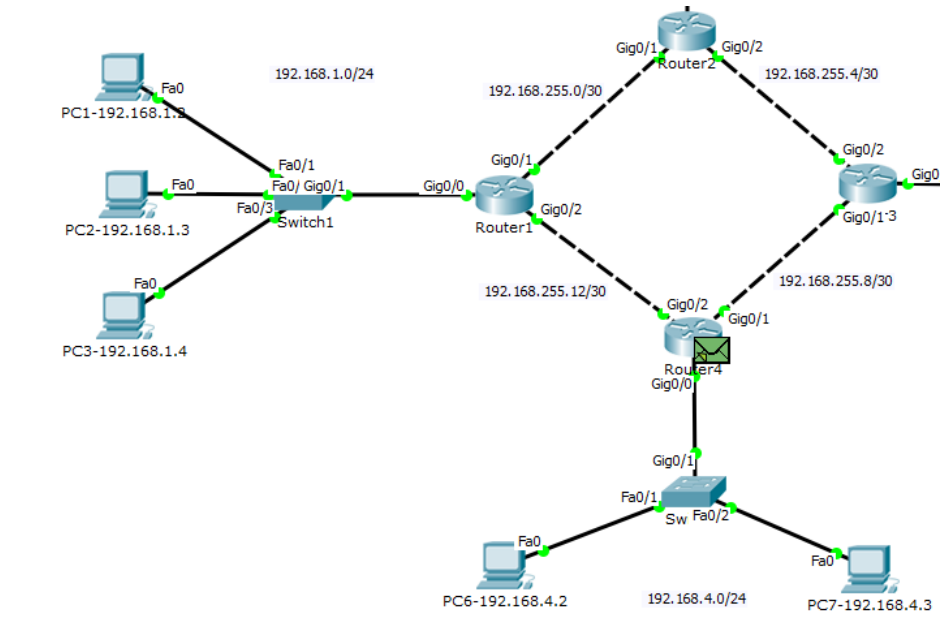


Рис. 5.23. Результати моделювання (крок 15, приймання ARP-відповіді маршрутизатором 4)

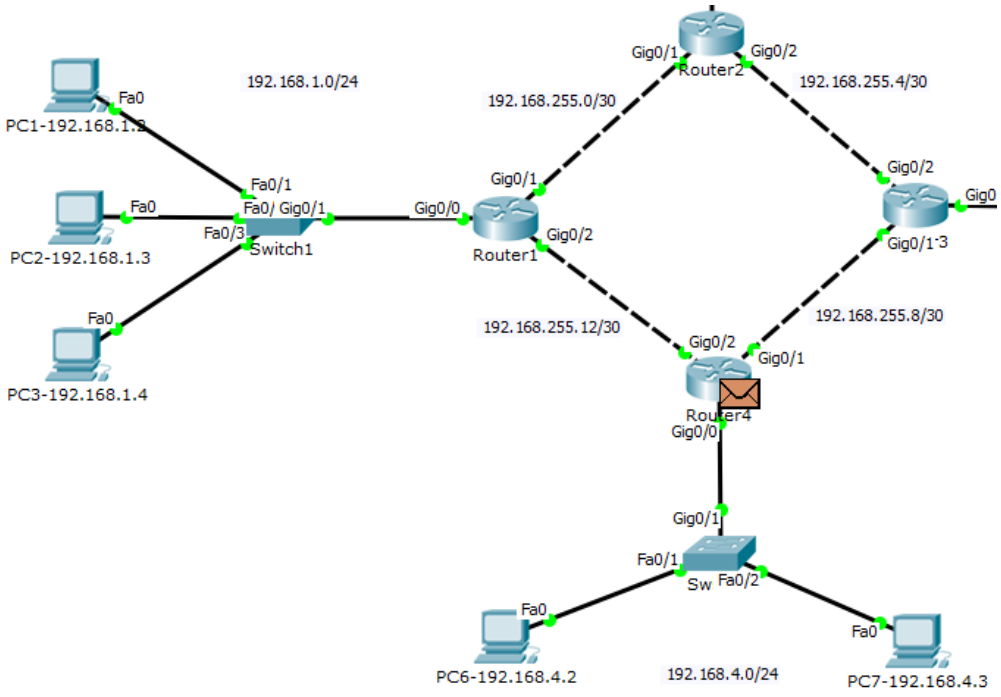


Рис. 5.24. Результати моделювання (крок 16, передача ехо-запиту протоколу ICMP)

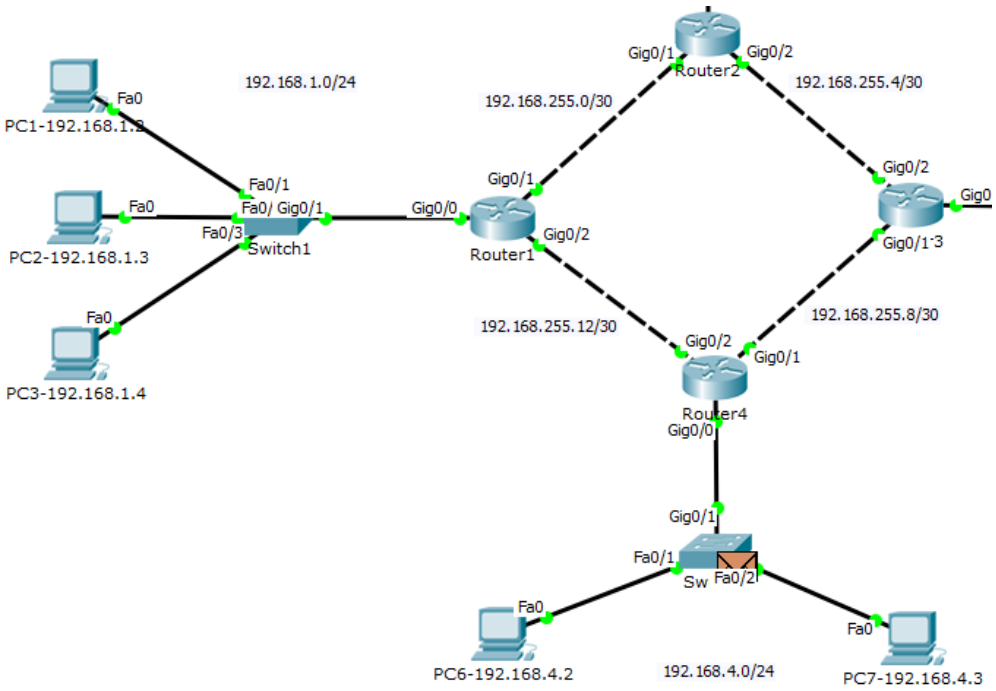


Рис. 5.25. Результати моделювання (крок 17, передача ехо-запиту протоколу ICMP)

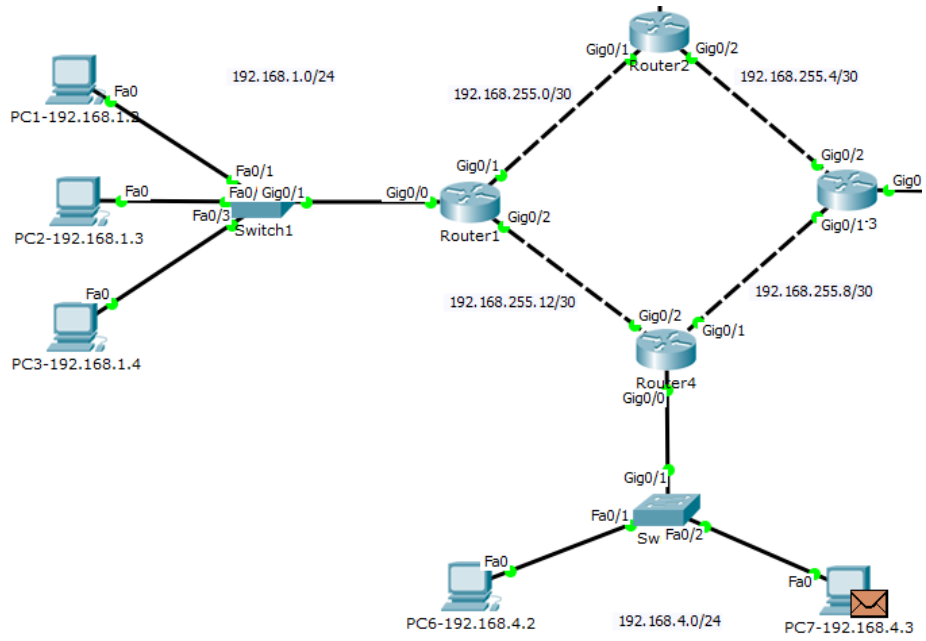


Рис. 5.26. Результати моделювання (крок 18, приймання ехо-запиту протоколу ICMP комп’ютером PC7-192.168.4.3, формування ехо-відповіді протоколу ICMP)

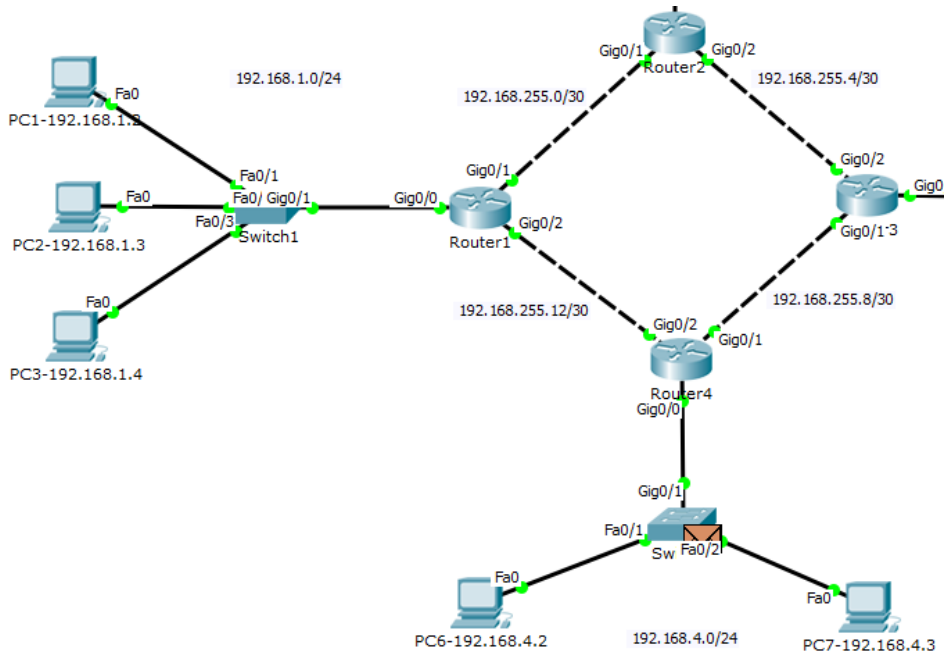


Рис. 5.27. Результати моделювання (крок 19, передача ехо-відповіді протоколу ICMP)

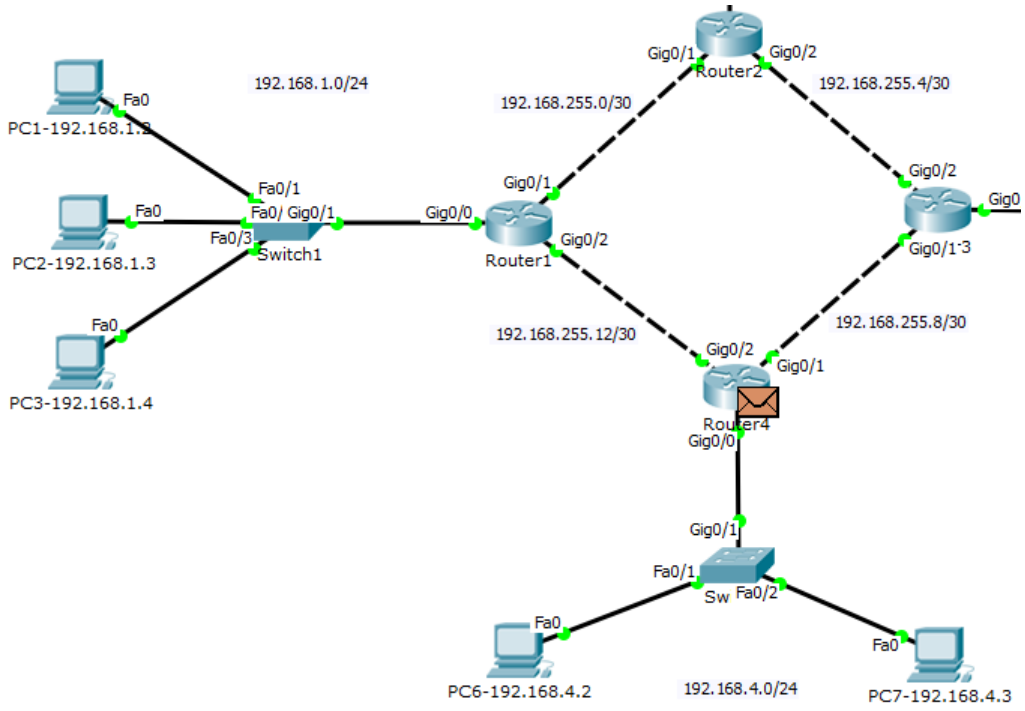


Рис. 5.28. Результати моделювання (крок 20, передача ехо-відповіді протоколу ICMP)

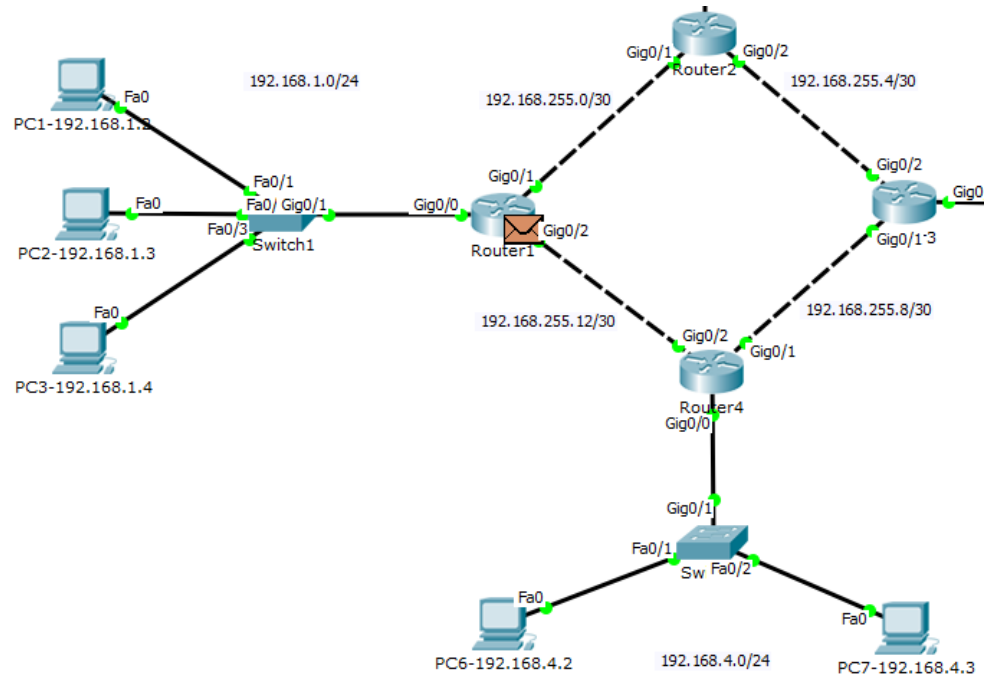


Рис. 5.29. Результати моделювання (крок 21, передача ехо-відповіді протоколу ICMP)

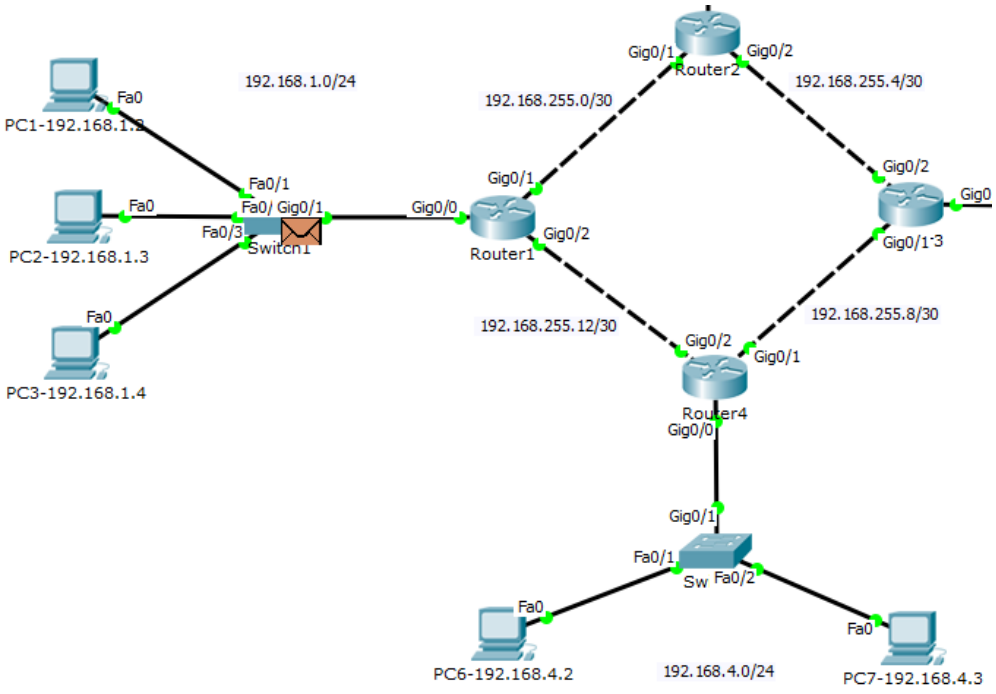


Рис. 5.30. Результати моделювання (крок 22, передача ехо-відповіді протоколу ICMP)

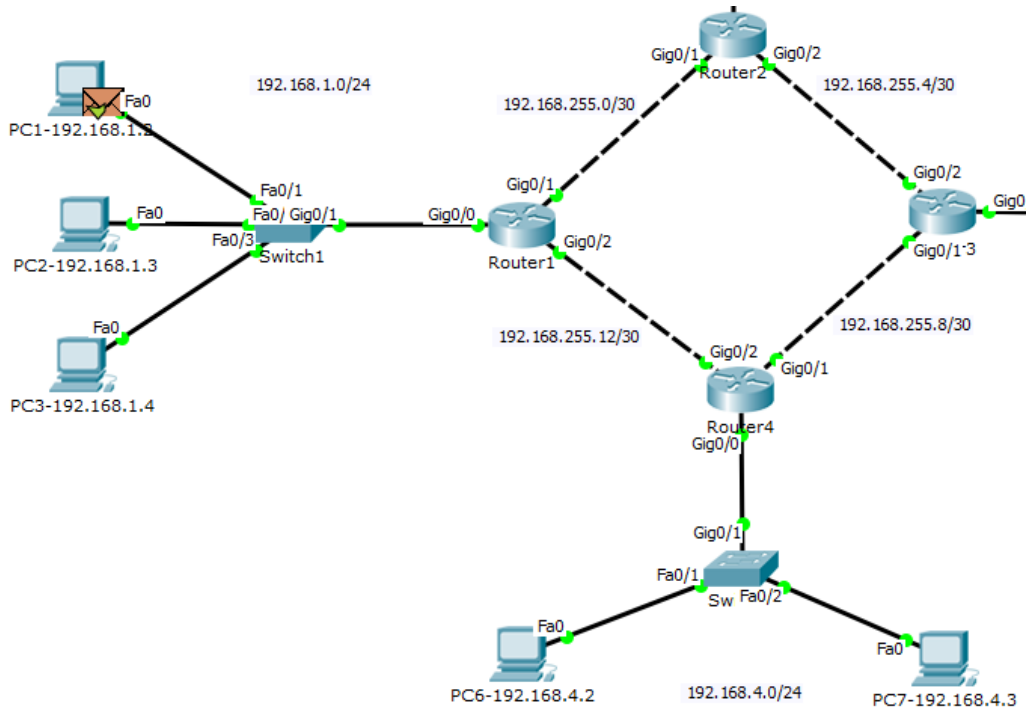


Рисунок 5.31. Результати моделювання (крок 23, успішне приймання ехо-відповіді протоколу ICMP комп'ютером PC1-192.168.1.2)

З результатів моделювання видно, що перед передачею ехо-запиту протоколу ICMP, спрямованого в іншу мережу, здійснюється визначення MAC-адреси шлюзу (інтерфейсу 0 маршрутизатора 1, IP-адреса 192.168.1.1) за допомогою передачі комутатором на всі свої порти (розсилання) кадру Ethernet з широкомовною MAC-адресою, яка містить у своєму полі даних запит протоколу ARP, оскільки ARP-таблиця комп'ютера – відправника ехо-запиту – була порожня. Також протокол ARP використовується:

– інтерфейсом 2 маршрутизатора 1 для визначення MAC-адреси інтерфейсу суміжного маршрутизатора (інтерфейсу 2 маршрутизатора 4, IP-адреса 192.168.255.13);

– інтерфейсом 0 маршрутизатора 4 для визначення MAC-адреси отримувача ехо-запиту (PC7-192.168.4.3).

Після визначення відповідних MAC-адрес здійснюється передача ехо-запиту протоколу ICMP.

5.2.2. Дослідження маршутів передачі IP-пакетів

Проведемо дослідження маршутів передачі IP-пакетів шляхом застосування команди tracert {IP-адреса}, яку необхідно вводити до командного рядка відповідного комп'ютера. Принципи визначення маршруту IP-пакета до вузла призначення за допомогою команди tracert в операційній системі Windows наведені в дод. 3.

Для перевірки маршруту передачі IP-пакетів від комп'ютера PC2-192.168.1.3 до комп'ютера PC7-192.168.4.3 треба до командного рядка комп'ютера PC2-192.168.1.3 ввести команду

tracert 192.168.4.3.

Результати визначення маршруту передачі IP-пакетів від комп'ютера PC2-192.168.1.3 до комп'ютера PC7-192.168.4.3 показано на рис. 5.32. З рис. 5.32 видно, що маршрут IP-пакета проходить через вузли з IP-адресами 192.168.1.1 (це IP-адреса інтерфейсу 0 маршрутизатора 1) і 192.168.255.13 (це IP-адреса інтерфейсу 2 маршрутизатора 4). Останній рядок результатів роботи команди tracert відповідає IP-адресі отримувача − IP-адресі комп'ютера PC7-192.168.4.3.

```
PC>tracert 192.168.4.3

Tracing route to 192.168.4.3 over a maximum of 30 hops:

  1    4 ms      4 ms      4 ms      192.168.1.1
  2    7 ms      6 ms      6 ms      192.168.255.13
  3    10 ms     10 ms     10 ms     192.168.4.3

Trace complete.
```

Рис. 5.32. Результати визначення маршруту передачі IP-пакетів від комп'ютера PC2-192.168.1.3 до комп'ютера PC7-192.168.4.3 за допомогою команди tracert

Команда tracert дозволяє визначити маршрут проходження IP-пакета до вузла призначення за допомогою посилання до вузла призначення серії exo-запитів протоколу ICMP з різними значеннями параметра TTL (строку життя IP-пакета) в IP-пакетах. За замовчуванням кожна серія містить 3 IP-пакети з однаковим значенням TTL.

Далі дослідимо принцип визначення маршруту передачі IP-пакета командою tracert у режимі візуального моделювання взаємодії мережевих компонентів, для чого перейдемо в цей режим і налаштуємо фільтр протоколів таким чином, щоб візуально відображувалися тільки пакети протоколу ICMP. Далі введемо до командного рядка комп'ютера PC2-192.168.1.3 команду tracert 192.168.4.3 та, послідовно натискуючи на кнопку Capture / Forward, дослідимо вміст поля TTL IP-пакетів (рис. 5.33 – 5.37).

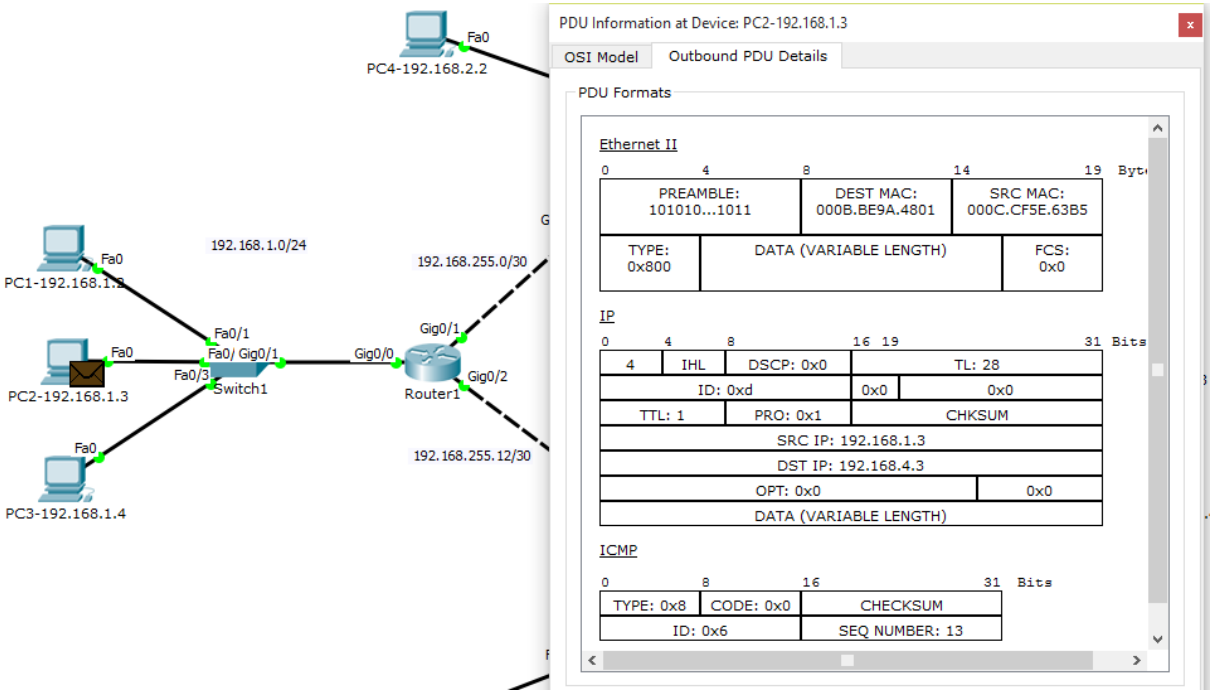


Рис. 5.33. Формування exo-запиту протоколу ICMP, який поміщається в IP-пакет з параметром TTL = 1

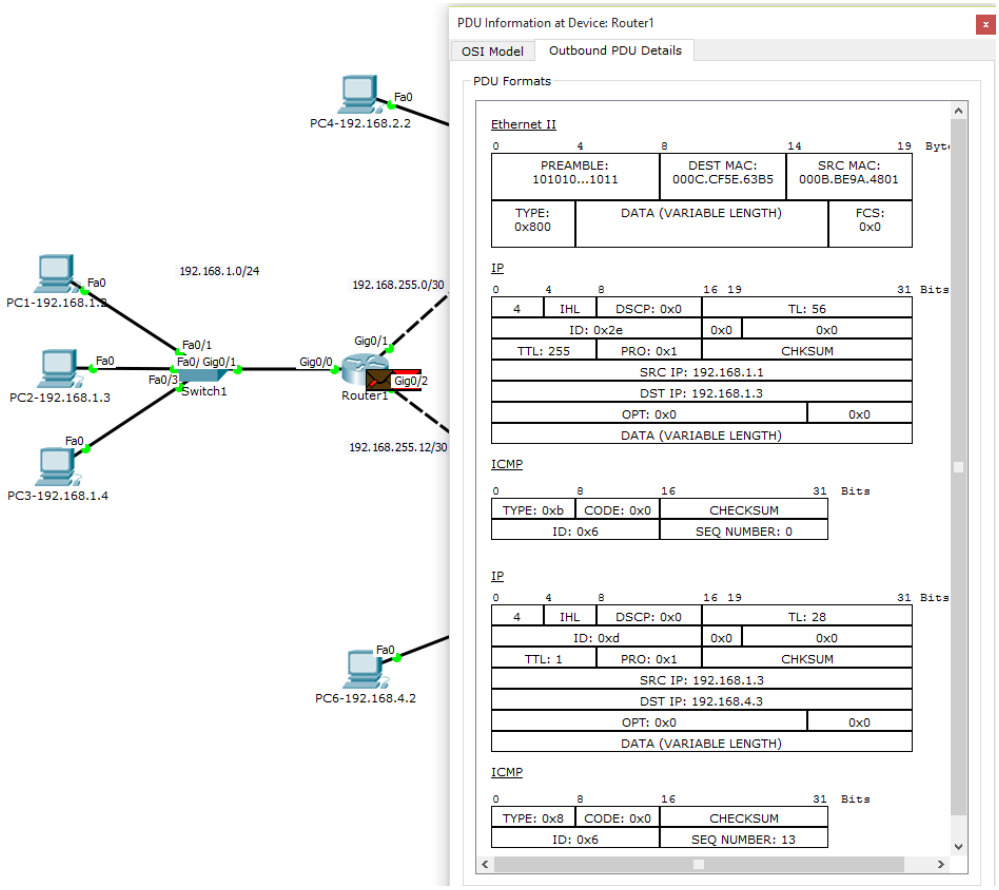


Рис. 5.34. Видалення маршрутизатором 1 IP-пакета з параметром TTL = 1 і надсилання повідомлення про видалення IP-пакета (закінчення часу життя IP-пакета), яке містить видалений IP-пакет і ехо-запит протоколу ICMP

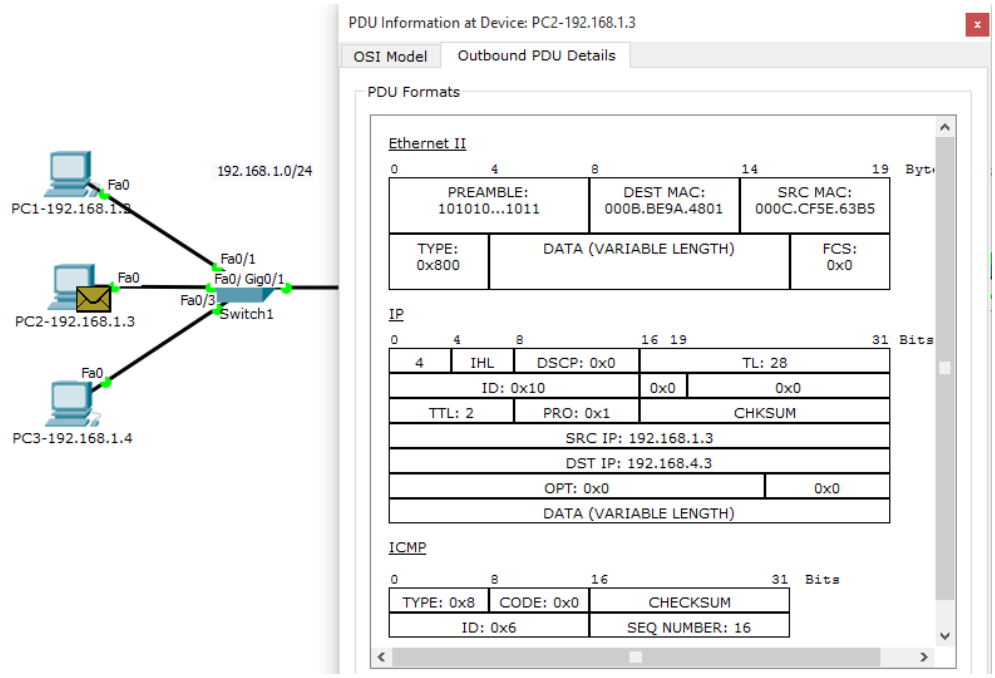


Рис. 5.35. Формування ехо-запиту протоколу ICMP, який поміщається в IP-пакет з параметром TTL = 2

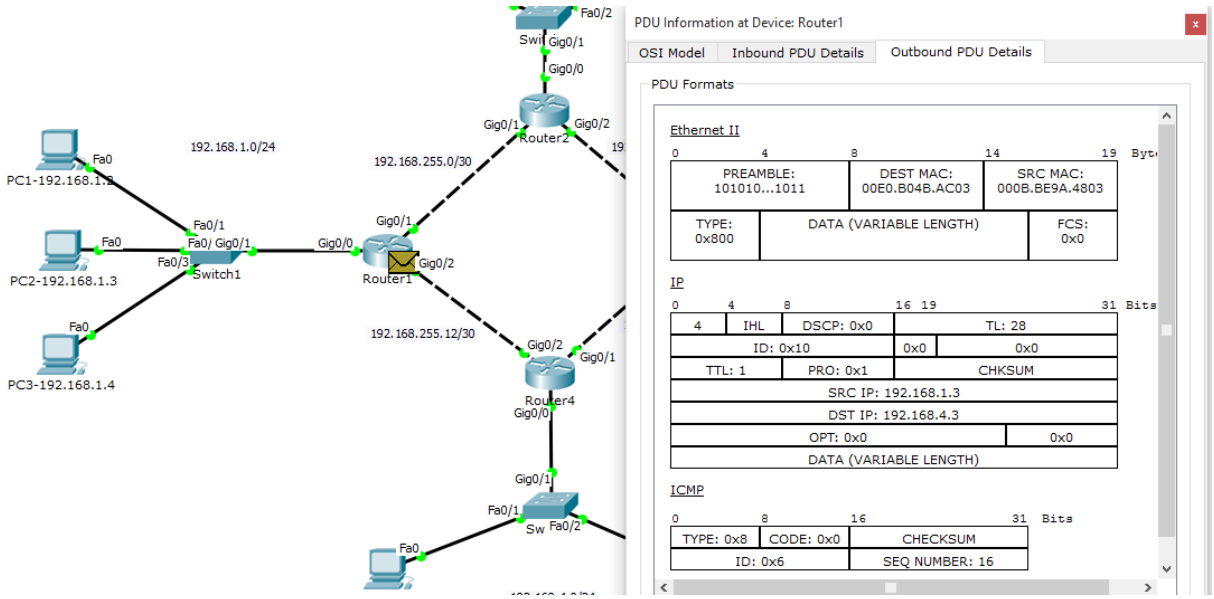


Рис. 5.36. Зменшення на 1 параметра TTL при проходженні IP-пакета через маршрутизатор 1 (TTL = 2 – 1 = 1)

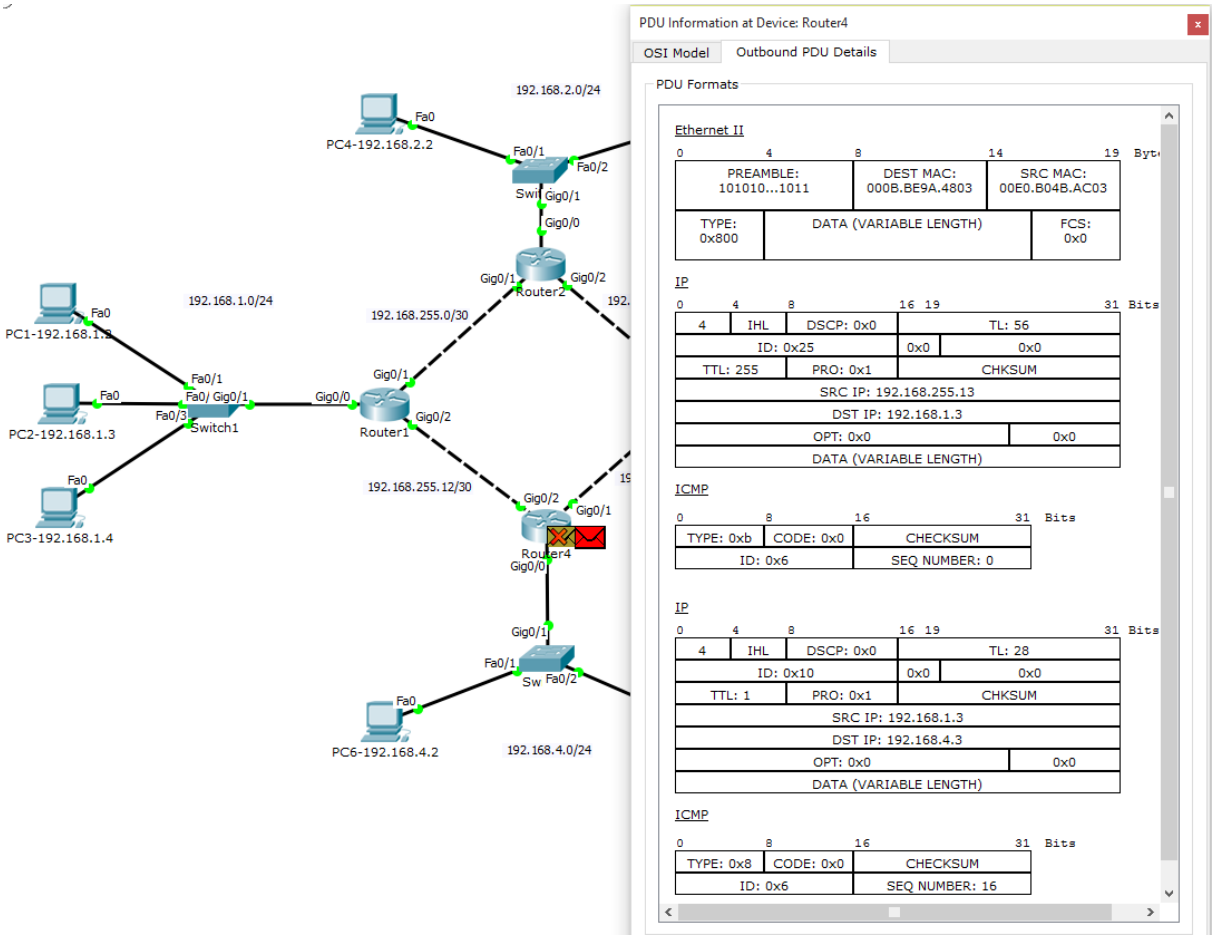


Рис. 5.37. Видалення маршрутизатором 2 IP-пакета з параметром TTL = 1 і надсилання повідомлення про видалення IP-пакета (закінчення часу життя IP-пакета), яке містить видалений IP-пакет і ехо-запит протоколу ICMP

Далі перевіримо маршрут передачі IP-пакетів від комп'ютера PC1-192.168.1.2 до комп'ютера PC10-192.168.3.4 в режимі моделювання в реальному часі. Для цього перейдемо в цей режим і до командного рядка комп'ютера PC1-192.168.1.2 введемо команду

tracert 192.168.3.4.

Потім повторимо команду tracert 192.168.3.4 декілька разів.

Результати визначення маршруту передачі IP-пакетів від комп'ютера PC1-192.168.1.2 до комп'ютера PC10-192.168.3.4 показані на рис. 5.38.

```
PC>tracert 192.168.3.4

Tracing route to 192.168.3.4 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      192.168.1.1
  2    0 ms      0 ms      0 ms      192.168.255.13
  3    0 ms      0 ms      0 ms      192.168.255.9
  4    11 ms     0 ms      0 ms      192.168.3.4

Trace complete.
```

а)

```
PC>tracert 192.168.3.4

Tracing route to 192.168.3.4 over a maximum of 30 hops:

  1    0 ms      1 ms      0 ms      192.168.1.1
  2    0 ms      0 ms      0 ms      192.168.255.2
  3    0 ms      0 ms      0 ms      192.168.255.9
  4    0 ms      0 ms      0 ms      192.168.3.4

Trace complete.
```

б)

Рис. 5.38. Результати визначення маршруту передачі IP-пакетів від комп'ютера PC1-192.168.1.2 до комп'ютера PC10-192.168.3.4 за допомогою команди tracert: а – непарний номер IP-пакета; б – парний номер IP-пакета

З аналізу результатів, отриманих за допомогою команди tracert (рис. 5.38), видно, що у випадку наявності в таблиці маршрутизації маршрутизатора Cisco 2911 двох статичних маршрутів з однаковими значеннями адміністративної відстані обидва маршрути використовуються для передачі IP-пакетів і працюють у режимі розподілу навантаження.

5.2.3. Дослідження альтернативних (резервних) маршутів передачі IP-пакетів

Одним із засобів підвищення відмовостійкості мережі є використання альтернативних (резервних) маршрутів. Альтернативні маршрути можна задавати за допомогою команди ip route з додатковим параметром адміністративної відстані. Приклад формування основних та альтернативних маршрутів показано на рис. 5.39.

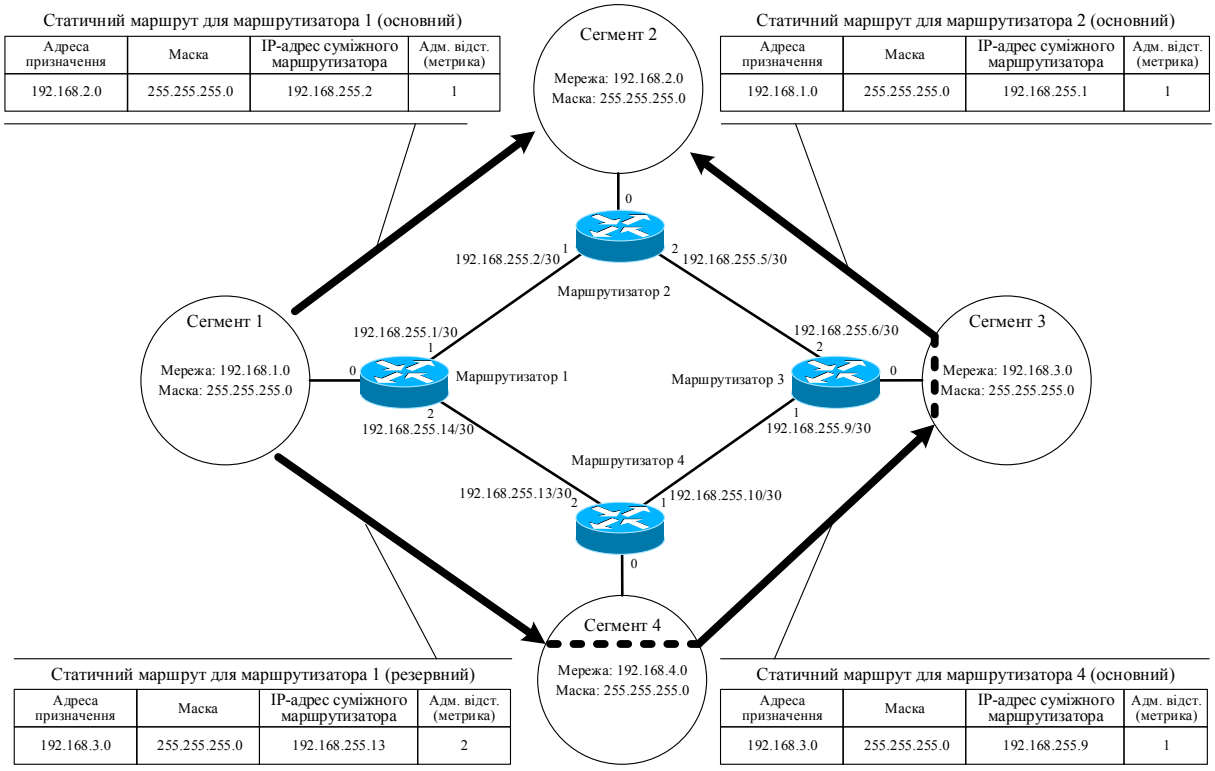


Рис. 5.39. Приклад формування основного та резервного статичних маршрутів

Результати формування необхідних основних і резервних статичних маршрутів мережі наведено в табл. 5.8 – 5.11.

Таблиця 5.8

Статичні маршрути для маршрутизатора 1

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.2.0	255.255.255.0	192.168.255.2	1
192.168.2.0	255.255.255.0	192.168.255.13	2
192.168.3.0	255.255.255.0	192.168.255.2	1
192.168.3.0	255.255.255.0	192.168.255.13	2
192.168.4.0	255.255.255.0	192.168.255.13	1
192.168.4.0	255.255.255.0	192.168.255.2	2

Таблиця 5.9

Статичні маршрути для маршрутизатора 2

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.1	1
192.168.1.0	255.255.255.0	192.168.255.6	2
192.168.3.0	255.255.255.0	192.168.255.6	1
192.168.3.0	255.255.255.0	192.168.255.1	2
192.168.4.0	255.255.255.0	192.168.255.6	1
192.168.4.0	255.255.255.0	192.168.255.1	2

Таблиця 5.10

Статичні маршрути для маршрутизатора 3

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.5	1
192.168.1.0	255.255.255.0	192.168.255.10	2
192.168.2.0	255.255.255.0	192.168.255.5	1
192.168.2.0	255.255.255.0	192.168.255.10	2
192.168.4.0	255.255.255.0	192.168.255.10	1
192.168.4.0	255.255.255.0	192.168.255.5	2

Таблиця 5.11

Статичні маршрути для маршрутизатора 4

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.14	1
192.168.1.0	255.255.255.0	192.168.255.9	2
192.168.2.0	255.255.255.0	192.168.255.9	1
192.168.2.0	255.255.255.0	192.168.255.14	2
192.168.3.0	255.255.255.0	192.168.255.9	1
192.168.3.0	255.255.255.0	192.168.255.14	2

Введемо до таблиць маршрутизації всіх маршрутизаторів необхідні маршрути:

```
Router1>enable
Router1#configure terminal
Router1(config)#ip route 192.168.2.0 255.255.255.0 192.168.255.2 1
Router1(config)#ip route 192.168.2.0 255.255.255.0 192.168.255.13 2
Router1(config)#ip route 192.168.3.0 255.255.255.0 192.168.255.2 1
Router1(config)#ip route 192.168.3.0 255.255.255.0 192.168.255.13 2
Router1(config)#ip route 192.168.4.0 255.255.255.0 192.168.255.13 1
Router1(config)#ip route 192.168.4.0 255.255.255.0 192.168.255.2 2
Router1(config)#exit
Router1#copy running-config startup-config;


Router2>enable
Router2#configure terminal
Router2(config)#ip route 192.168.1.0 255.255.255.0 192.168.255.1 1
Router2(config)#ip route 192.168.1.0 255.255.255.0 192.168.255.6 2
Router2(config)#ip route 192.168.3.0 255.255.255.0 192.168.255.6 1
Router2(config)#ip route 192.168.3.0 255.255.255.0 192.168.255.1 2
Router2(config)#ip route 192.168.4.0 255.255.255.0 192.168.255.6 1
Router2(config)#ip route 192.168.4.0 255.255.255.0 192.168.255.1 2
Router2(config)#exit
Router2#copy running-config startup-config;

Router3>enable
Router3#configure terminal
Router3(config)#ip route 192.168.1.0 255.255.255.0 192.168.255.5 1
```

```
Router3(config)#ip route 192.168.1.0 255.255.255.0 192.168.255.10 2
Router3(config)#ip route 192.168.2.0 255.255.255.0 192.168.255.5 1
Router3(config)#ip route 192.168.2.0 255.255.255.0 192.168.255.10 2
Router3(config)#ip route 192.168.4.0 255.255.255.0 192.168.255.10 1
Router3(config)#ip route 192.168.4.0 255.255.255.0 192.168.255.5 2
Router3(config)#exit
Router3#copy running-config startup-config;

Router4>enable
Router4#configure terminal
Router4(config)#ip route 192.168.1.0 255.255.255.0 192.168.255.14 1
Router4(config)#ip route 192.168.1.0 255.255.255.0 192.168.255.9 2
Router4(config)#ip route 192.168.2.0 255.255.255.0 192.168.255.9 1
Router4(config)#ip route 192.168.2.0 255.255.255.0 192.168.255.14 2
Router4(config)#ip route 192.168.3.0 255.255.255.0 192.168.255.9 1
Router4(config)#ip route 192.168.3.0 255.255.255.0 192.168.255.14 2
Router4(config)#exit
Router4#copy running-config startup-config.
```

Після введення статичних маршрутів перевіримо вміст таблиць маршрутизації за допомогою команди show ip route, яку необхідно вводити в привілейованому режимі:

```
Router1#show ip route

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
S 192.168.2.0/24 [1/0] via 192.168.255.2
S 192.168.3.0/24 [1/0] via 192.168.255.2
S 192.168.4.0/24 [1/0] via 192.168.255.13
192.168.255.0/24 is variably subnetted, 4 subnets, 2 masks
C 192.168.255.0/30 is directly connected, GigabitEthernet0/1
L 192.168.255.1/32 is directly connected, GigabitEthernet0/1
C 192.168.255.12/30 is directly connected, GigabitEthernet0/2
L 192.168.255.14/32 is directly connected, GigabitEthernet0/2.
```

Також перевірку вмісту таблиць маршрутизації можна виконати за допомогою інструменту перевірки окремих властивостей обладнання (рис. 5.40).

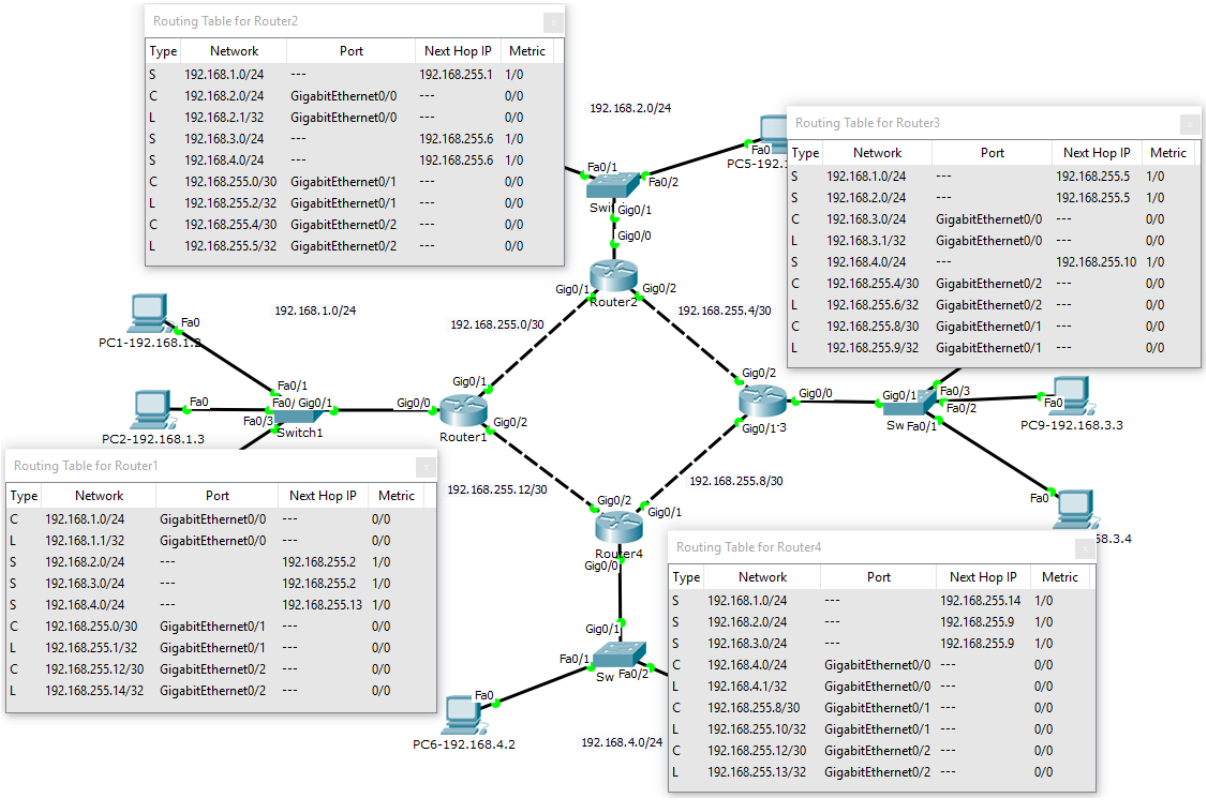


Рис. 5.40. Результат перевірки вмісту таблиць маршрутизації за допомогою інструменту перевірки окремих властивостей обладнання

Зазначимо, що в таблиці маршрутизації резервні маршрути відсутні, оскільки їхня адміністративна відстань менша, ніж основних маршрутів. Усі введені статичні маршрути зберігаються в конфігуруванні маршрутизатора (активному або після збереження активного командою copy running-config startup-config – у стартовому), які можна переглянути командою show в привілейованому режимі:

Router1#show running-config
Router1#show startup-config.

Однак якщо вимкнути один з інтерфейсів, то маршрутизатор виявить недоступний маршрут, що призведе до виключення з таблиці маршрутизації недоступного маршрутуту, а замість нього, за наявності, в таблицю маршрутизації буде поміщено альтернативний маршрут. Для прикладу на маршрутизаторі 1 вимкнемо інтерфейс 1:

Router1#show ip route

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
S 192.168.2.0/24 [2/0] via 192.168.255.13
S 192.168.3.0/24 [2/0] via 192.168.255.13
S 192.168.4.0/24 [1/0] via 192.168.255.13
192.168.255.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.255.12/30 is directly connected, GigabitEthernet0/2
L 192.168.255.14/32 is directly connected, GigabitEthernet0/2.

Далі перевіримо роботу мережі в режимі візуального моделювання взаємодії мережевих компонентів за допомогою інструменту формування exo-запитів протоколу ICMP, а також з застосуванням команди tracert у режимі моделювання в реальному часі.

Спочатку проведемо перевірку для випадку, коли всі інтерфейси маршрутизаторів ввімкнені (на рис. 5.41 показано результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2).

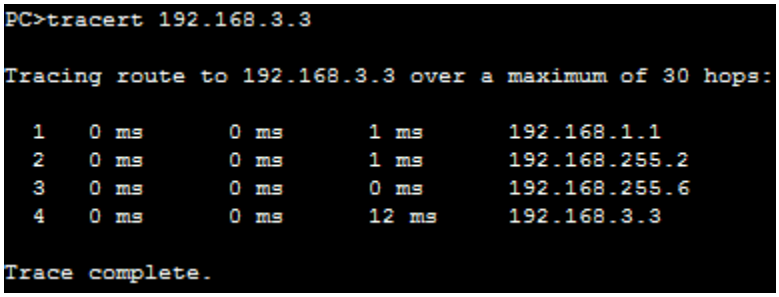


Рис. 5.41. Результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2

З рис. 5.41 видно маршрут проходження IP-пакетів.

Потім вимкнемо інтерфейс 1 маршрутизатора 1 і повторимо перевірку за допомогою команди tracert (на рис. 5.42 показано результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2 для випадку вимкненого інтерфейсу 1 маршрутизатора 1).

```
PC>tracert 192.168.3.3

Tracing route to 192.168.3.3 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.1
  2    0 ms      0 ms      0 ms      192.168.255.13
  3    *         *         *         Request timed out.
  4    *         *         *         Request timed out.
  5    *         *         *         Request timed out.
  6
```

Рис. 5.42. Результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2

З рис. 5.42 видно, що була отримана відповідь тільки від вузла з IP-адресою 192.168.255.13 (це інтерфейс 2 маршрутизатора 4), а відповідей від інших вузлів нема. Таким чином, можна зробити висновок, що маршрут є недосяжним (причини недосяжності маршруту в даному випадку тут не видно).

Для з'ясування причини недосяжності маршруту від комп'ютера PC1-192.168.1.2 до комп'ютера PC9-192.168.3.3 перейдемо в режим візуального моделювання взаємодії мережевих компонентів і скористаємось інструментом формування exo-запитів протоколу ICMP (рис. 5.43 – 5.51).

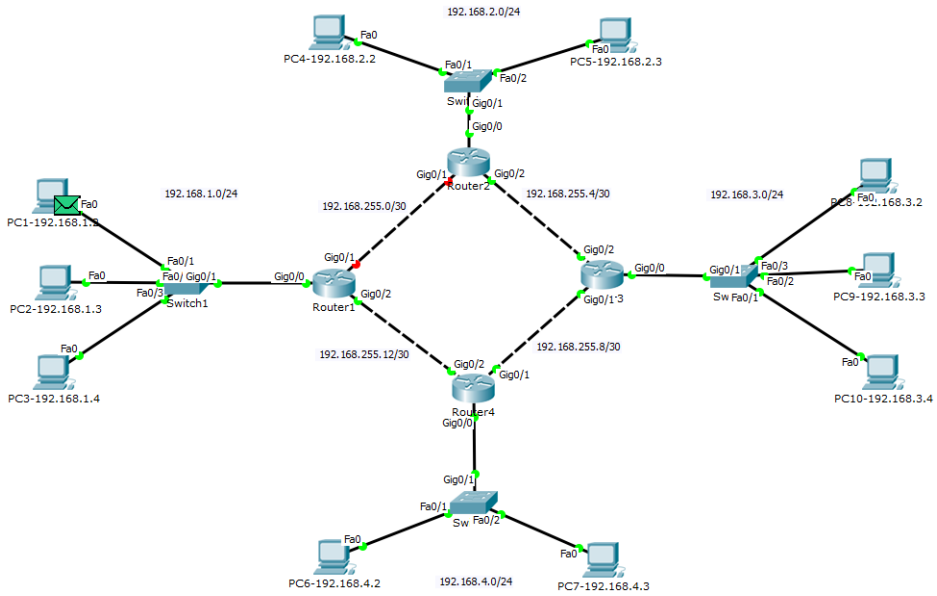


Рис. 5.43. Результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2 (крок 1)

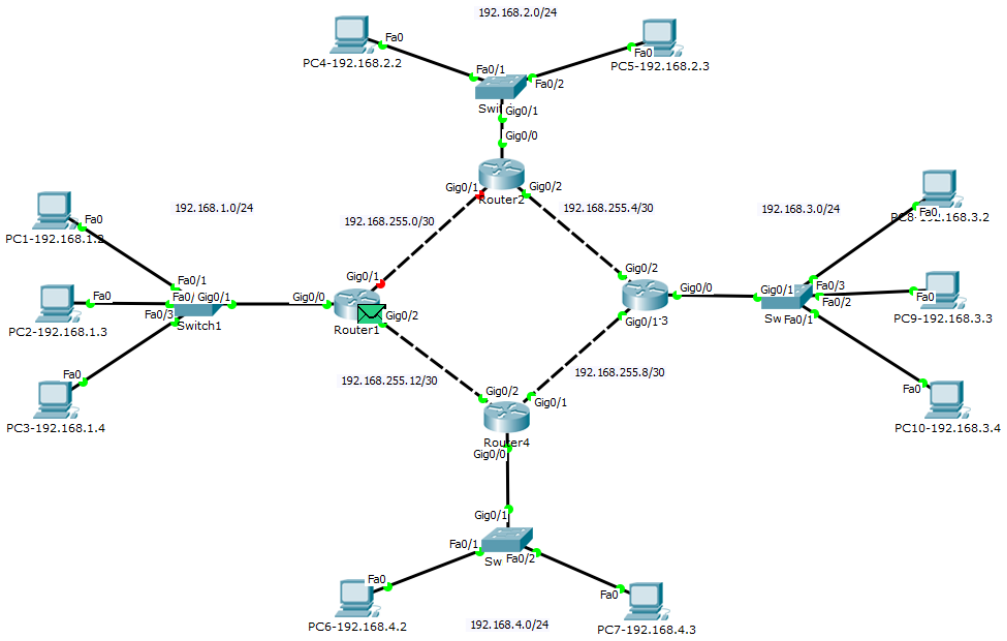


Рис. 5.44. Результат застосування команди tracert 192.168.3.3 з комп’ютера PC1-192.168.1.2 (крок 3)

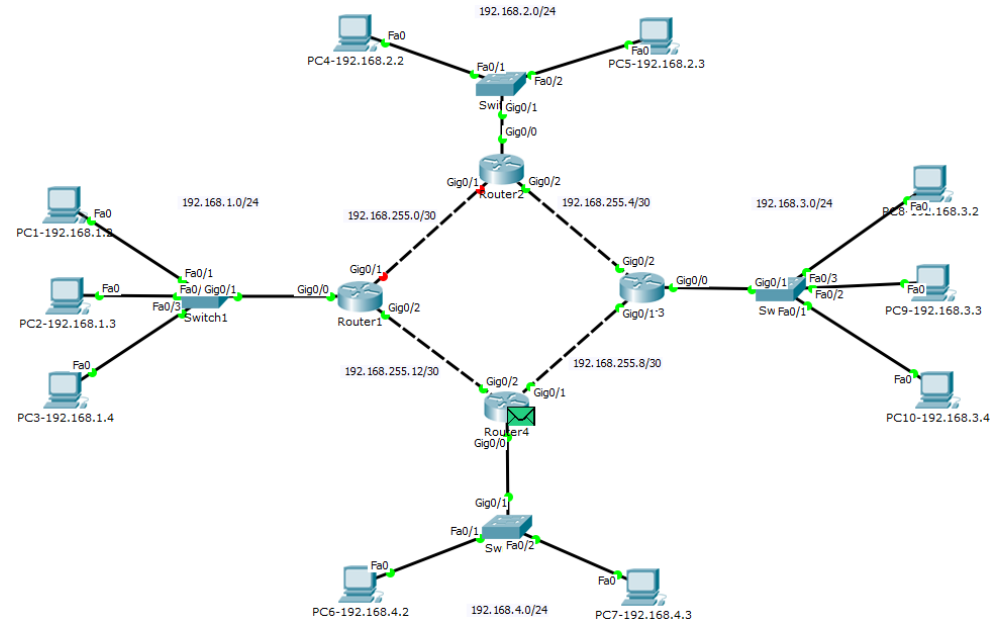


Рис. 5.45. Результат застосування команди tracert 192.168.3.3 з комп’ютера PC1-192.168.1.2 (крок 4)

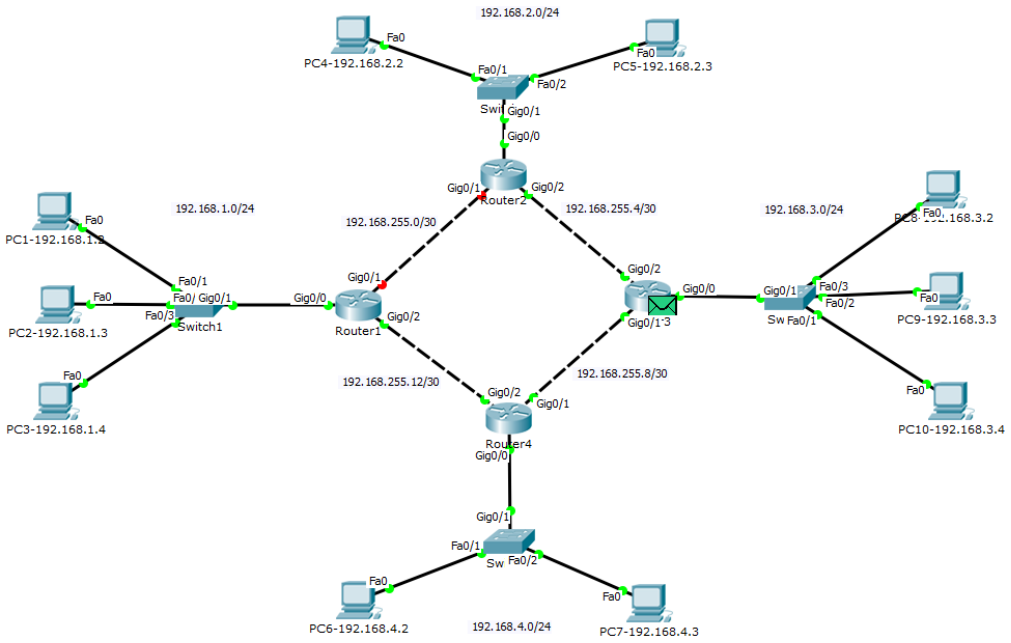


Рис. 5.46. Результат застосування команди tracert 192.168.3.3 з комп’ютера PC1-192.168.1.2 (крок 5)

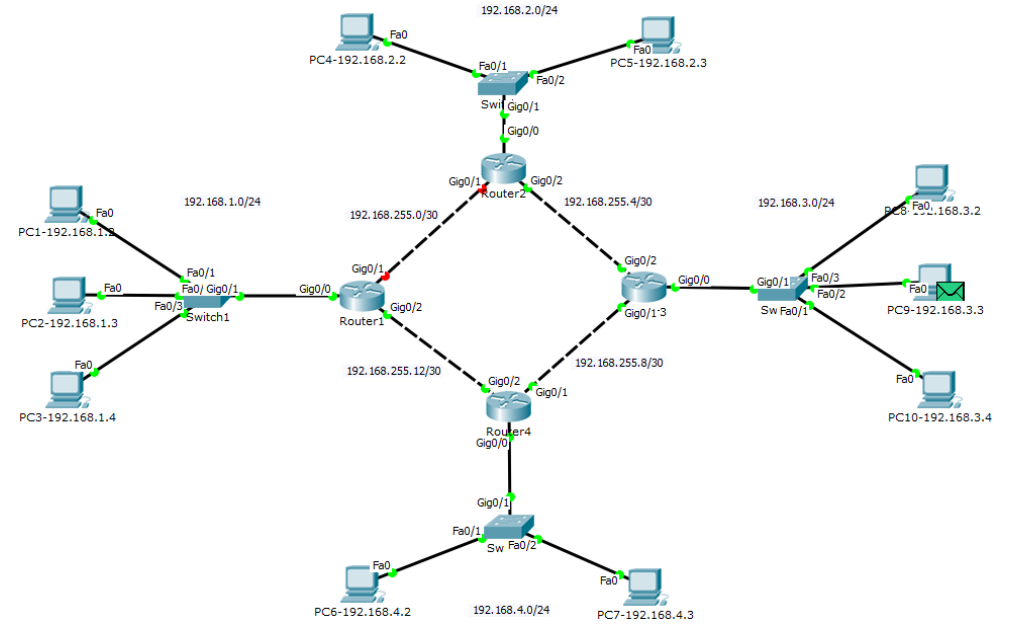


Рис. 5.47. Результат застосування команди tracert 192.168.3.3 з комп’ютера PC1-192.168.1.2 (крок 7)

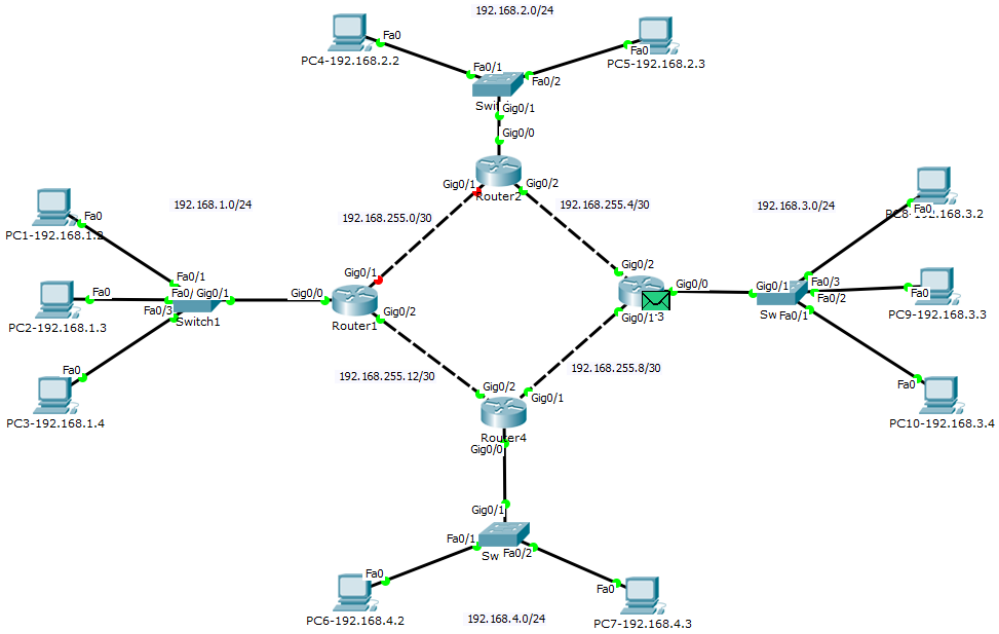


Рис. 5.48. Результат застосування команди tracert 192.168.3.3 з комп’ютера PC1-192.168.1.2 (крок 9)

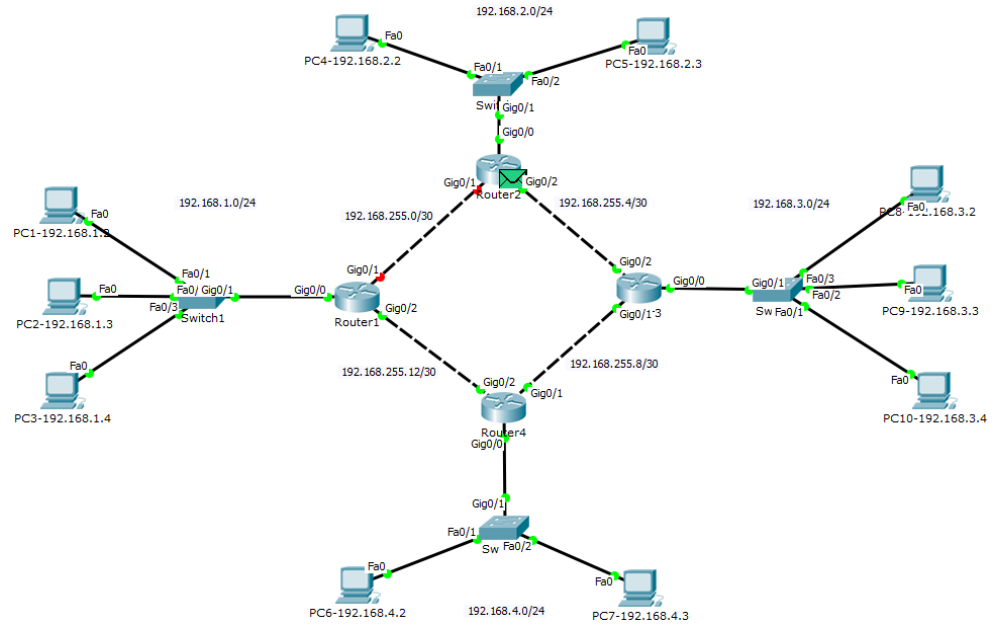


Рис. 5.49. Результат застосування команди tracert 192.168.3.3 з комп’ютера PC1-192.168.1.2 (крок 10)

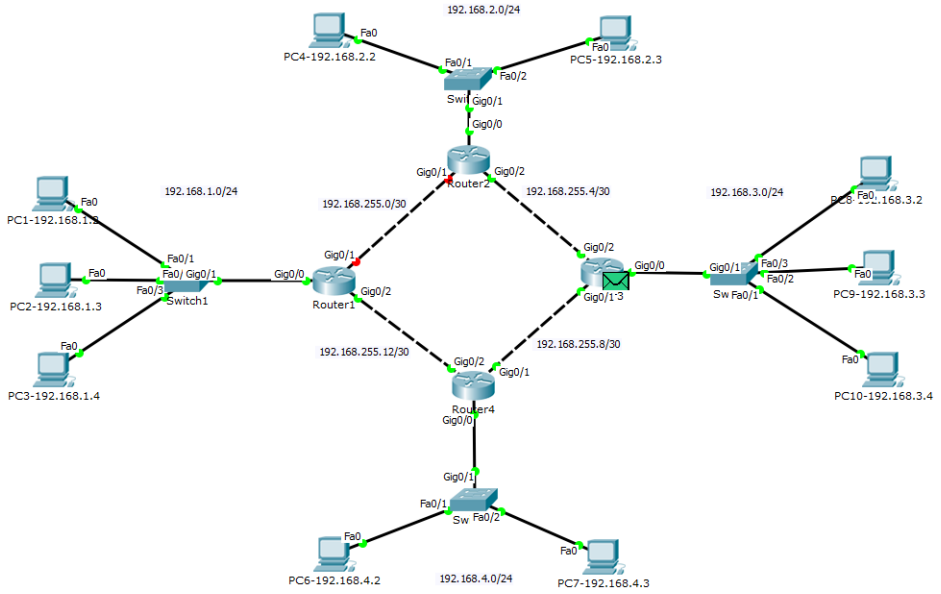


Рис. 5.50. Результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2 (крок 11, зациклення пакета)

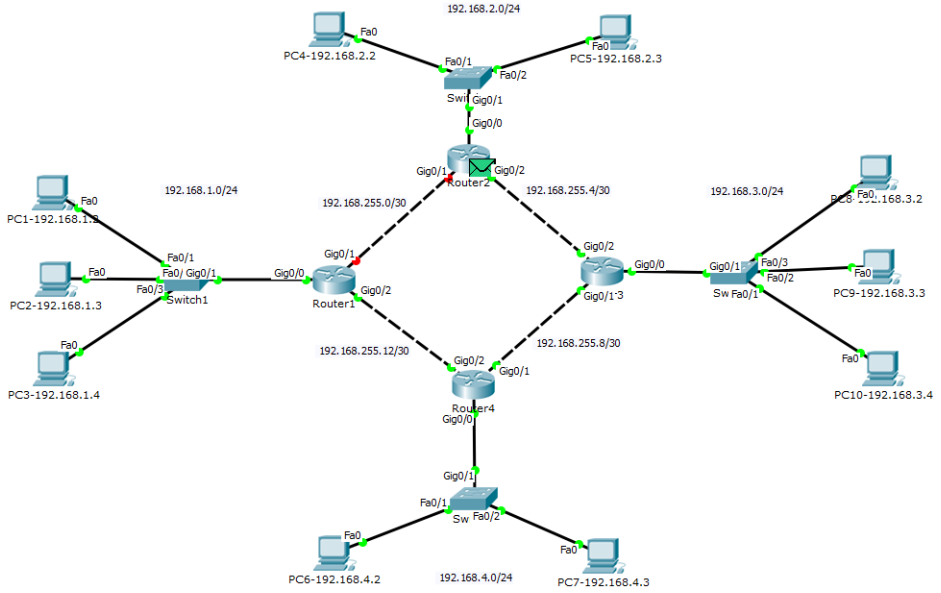


Рис. 5.51. Результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2 (крок 12, зациклення пакета)

З рис. 5.43 – 5.51 видно, що ехо-запит протоколу ICMP досягнув вузла призначення – комп'ютера PC9-192.168.3.3, але ехо-відповідь була направлена на маршрутизатор 2, оскільки для маршрутизатора 3 наявний у таблиці маршрутизації маршрут до мережі призначення 192.168.1.0 проходить через інтерфейс з IP-адресою 192.168.255.5 маршрутизатора 2. З аналізу таблиці

маршрутизації маршрутизатора 2 видно, що наявний у таблиці маршрутизації маршрут до мережі призначення 192.168.1.0 проходить через інтерфейс з IP-адресою 192.168.255.6 маршрутизатора 3. Таким чином, записи в таблиці маршрутизації маршрутизаторів 3 і 2 призводять до зациклення IP-пакета між інтерфейсами цих маршрутизаторів, а саме між інтерфейсом 2 з IP-адресою 192.168.255.5 маршрутизатора 2 та інтерфейсом 2 з IP-адресою 192.168.255.6 маршрутизатора 3 (рис. 5.52). Таке зациклення буде відбуватися доти, поки параметр TTL в IP-пакеті не бере нульового значення.

Таким чином, з отриманих результатів можна зробити висновок, що використання альтернативних маршрутів при статичній маршрутизації в загальному випадку може призвести до зациклення пакетів в IP-мережі, оскільки при статичній маршрутизації маршрутизатори не мають мажливості виявити недосяжність маршруту для випадку, коли ця недосяжність викликана несправністю або вимкненням інтерфейсу несуміжного маршрутизатора.

Статичний маршрут для маршрутизатора 3

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.5	1

Статичний маршрут для маршрутизатора 2

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.6	2

Рис. 5.52. Записи в таблицях маршрутизації маршрутизаторів 3 і 2, що призводять до зациклення IP-пакета, спрямованого до мережі 192.168.1.0, між інтерфейсом 2 з IP-адресою 192.168.255.5 маршрутизатора 2 та інтерфейсом 2 з IP-адресою 192.168.255.6 маршрутизатора 3

Результат перевірки вмісту таблиць маршрутизації за допомогою інструменту перевірки окремих властивостей обладнання для випадку вимкненого інтерфейсу 1 маршрутизатора 1 показано на рис. 5.53.

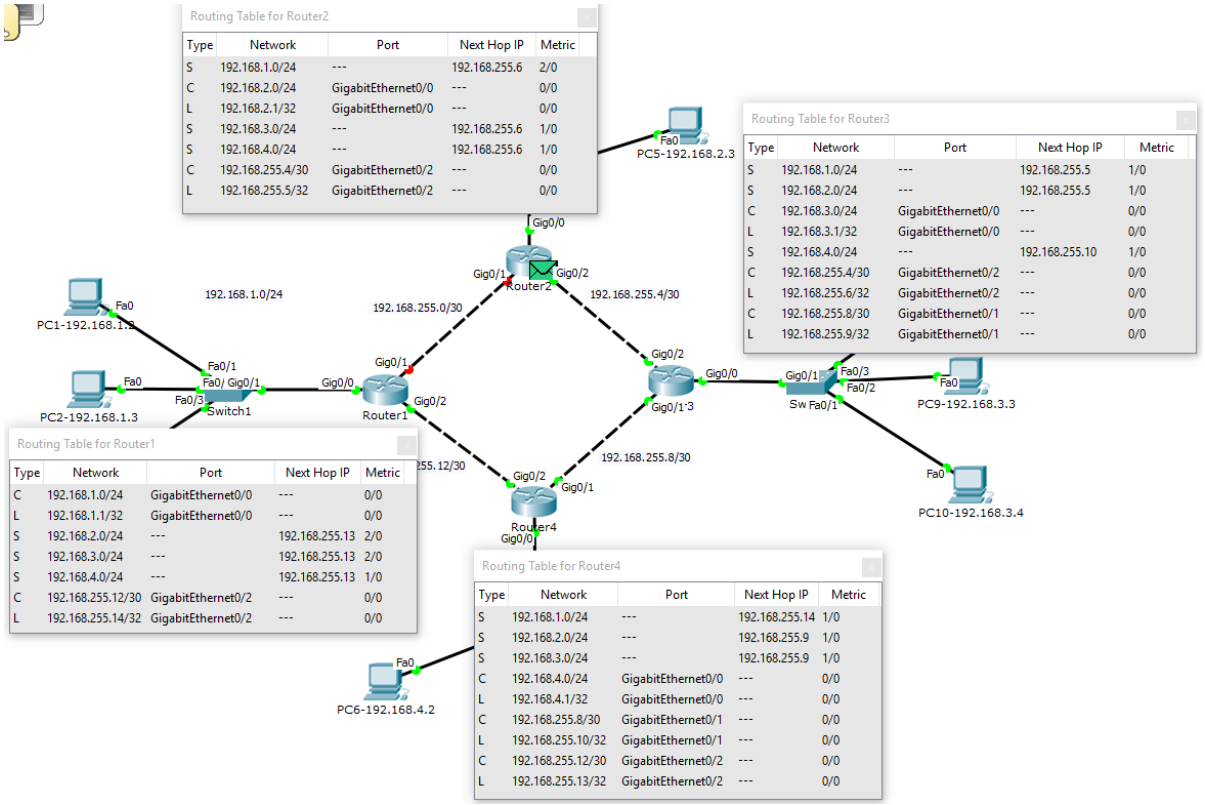


Рис. 5.53. Результат перевірки вмісту таблиць маршрутизації за допомогою інструменту перевірки окремих властивостей обладнання для випадку вимкненого інтерфейсу 1 маршрутизатора 1

Але слід зазначити, що якщо основний статичний маршрут буде визначатися безпосереднім з’єднанням маршрутизаторів, а альтернативний статичний маршрут буде проходити тільки через один маршрутизатор, то зациклення IP-пакетів відбуватися не буде, оскільки в цьому випадку безпосередньо з’єднані маршрутизатори будуть мати можливість виявлення недосяжності маршрутів, і єдиним варіантом для них буде спрямування пакетів через альтернативний маршрут, який проходить тільки через один маршрутизатор (вважається, що може мати місце тільки одна відмова в мережі, тому якщо основний маршрут недосяжний, то альтернативний маршрут буде

досяжним). Таким чином, в IP-мережі з трьома маршрутизаторами (повнозв'язній або кільцевій, що те саме для трьох вузлів) застосування альтернативних маршрутів не призведе до зациклення IP-пакетів. З вищевказаного можна зробити висновок, що застосування статичних альтернативних маршрутів має певні обмеження та може бути здійснено тільки після перевірки на відсутність можливості зациклення IP-пакетів. Дослідження роботи IP-мережі з трьома маршрутизаторами та альтернативними маршрутами виконується в години самостійної роботи.

Також слід зазначити, що в маршрутизаторах Cisco існує можливість відслідкування доступності маршруту шляхом застосування функції Cisco Enhanced Object Tracking, яка є пропрієтарною (нестандартною).

5.2.4. Дослідження маршутів передачі IP-пакетів за замовчуванням

Якщо в таблиці маршрутизації буде відсутній запис про IP-адресу мережі або вузла призначення, IP-пакет, адресований до невідомої маршрутизатору адреси призначення, буде видалено. Для надання можливості передачі такого пакета використовується маршрут за замовчуванням, для якого адресою призначення та маскою є 0.0.0.0. Таким чином, IP-пакет, адресований до невідомої маршрутизатору адреси призначення, буде передано по маршруту за замовчуванням. Як правило, маршрут за замовчуванням використовується для виходу в загальну мережу, наприклад мережу Інтернет.

Введення статичного маршруту за замовчуванням здійснюється командою ip route, яку необхідно вводити в режимі глобального конфігурування:

ip route 0.0.0.0 0.0.0.0 {IP-адреса суміжного маршрутизатора або ім'я вихідного інтерфейсу маршрутизатора} {адміністративна відстань (необов'язково)}.

У випадку наявності декількох статичних маршрутів до адреси призначення вибирається більш специфічний, тобто той, у якому зазначена більш точно мережа призначення. А отже, маршрут за замовчуванням має найнижчий пріоритет. Це зручно, тому що дозволяє значно скоротити кількість записів у таблиці маршрутизації, що дозволяє створювати тільки ті маршрути, у яких IP-адреса суміжного маршрутизатора або ім'я вихідного інтерфейсу маршрутизатора відрізняються від маршруту за замовчуванням.

Проведемо дослідження принципів роботи маршрутизаторів зі статичними маршрутами за замовчуванням. Для цього видалимо всі статичні маршрути з таблиць маршрутизації всіх маршрутизаторів командою no ip route з відповідними параметрами або за допомогою графічного інтерфейсу симулятора. А потім до кожного з маршрутизаторів введемо по одному маршруту за замовчуванням. Причому маршрути за замовчуванням будемо вибирати таким чином, щоб IP-пакети від одного з маршрутизаторів передавалися до іншого і так далі по кільцю (IP-пакети не повинні повертатися до маршрутизатора, який їх передав, з метою уникнення їх зациклення).

Результати формування статичних маршрутів за замовчуванням для забезпечення повнозв'язності мережі наведені в табл. 5.12 – 5.15.

Таблиця 5.12

Статичний маршрут за замовчуванням для маршрутизатора 1

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
0.0.0.0	0.0.0.0	192.168.255.2	1

Таблиця 5.13

Статичний маршрут за замовчуванням для маршрутизатора 2

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
0.0.0.0	0.0.0.0	192.168.255.6	1

Таблиця 5.14

Статичний маршрут за замовчуванням для маршрутизатора 3

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
0.0.0.0	0.0.0.0	192.168.255.10	1

Таблиця 5.15

Статичний маршрут за замовчуванням для маршрутизатора 4

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
0.0.0.0	0.0.0.0	192.168.255.14	1

Після введення маршрутів за замовчуванням перевірка роботи IP-мережі здійснюється в режимі візуального моделювання взаємодії мережевих компонентів та інструменту формування ехо-запитів протоколу ICMP, а також за допомогою команди tracert у режимі моделювання в реальному часі. Ґрунтовний аналіз результатів моделювання виконується самостійно.

З результатів моделювання можна зробити висновок, що за допомогою одного статичного маршруту за замовчуванням вдалося забезпечити доступність усіх сегментів IP-мережі, але при цьому напрями передачі та приймання IP-пакетів різні (IP-пакети передаються по кільцевому сегменту тільки за годинниковою стрілкою), що є недоліком такого способу задавання статичних маршрутів.

6. ВАРІАНТИ ЗАВДАНЬ ДЛЯ РОЗРОБЛЕННЯ ПЛАНУ РОЗПОДІЛУ ІНФОРМАЦІЇ ДЛЯ СТАТИЧНОЇ МАРШРУТИЗАЦІЇ В МЕРЕЖІ НА ОСНОВІ ПРОТОКОЛУ IP

На рис. 6.1 – 6.21 показано варіанти завдань для розроблення плану розподілу інформації для статичної маршрутизації в IP-мережі та дослідження її роботи у програмному середовищі імітаційного моделювання.

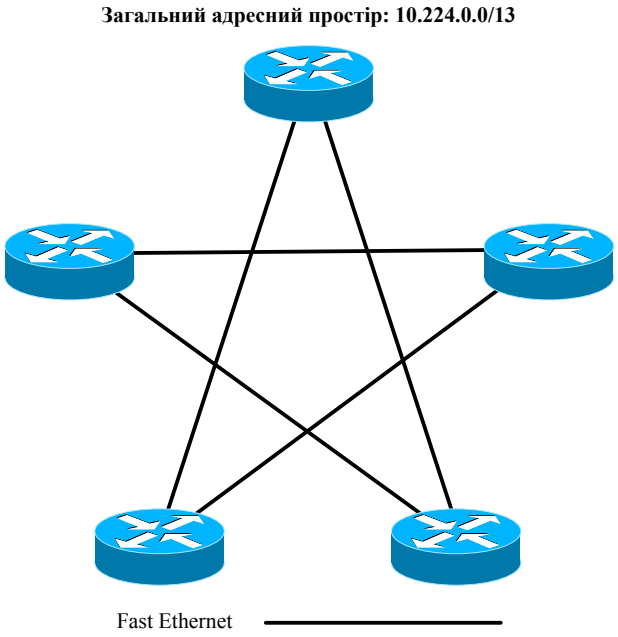


Рис. 6.1. Варіант 1

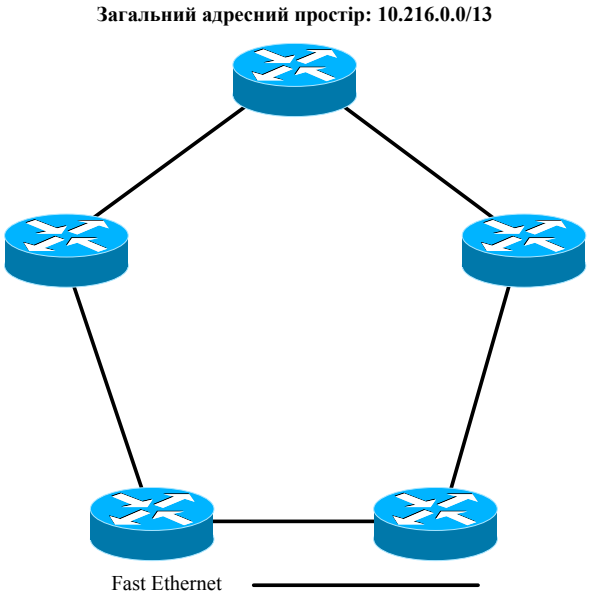


Рис. 6.2. Варіант 2

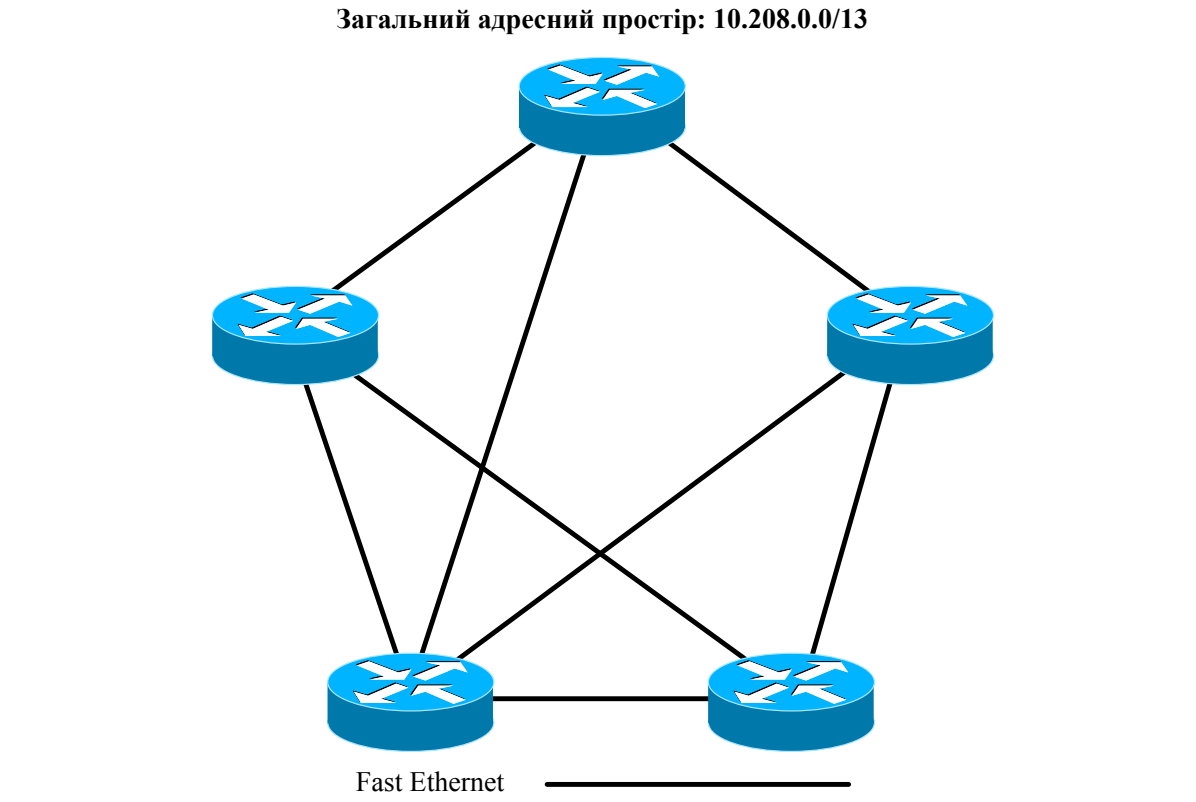


Рис. 6.3. Варіант 3

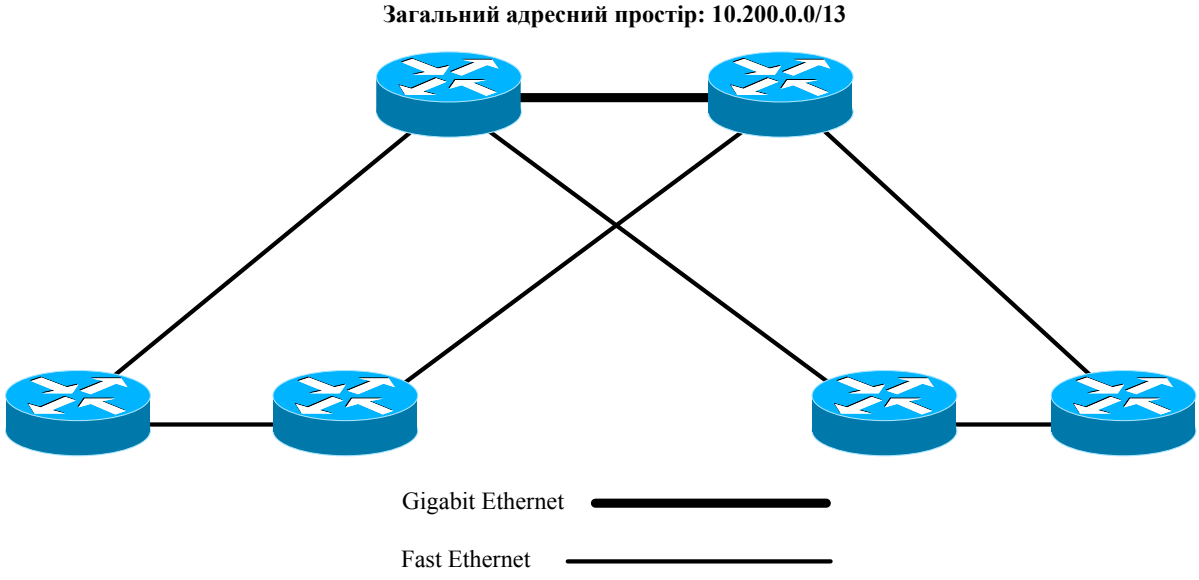


Рис. 6.4. Варіант 4

Загальний адресний простір: 10.64.0.0/13

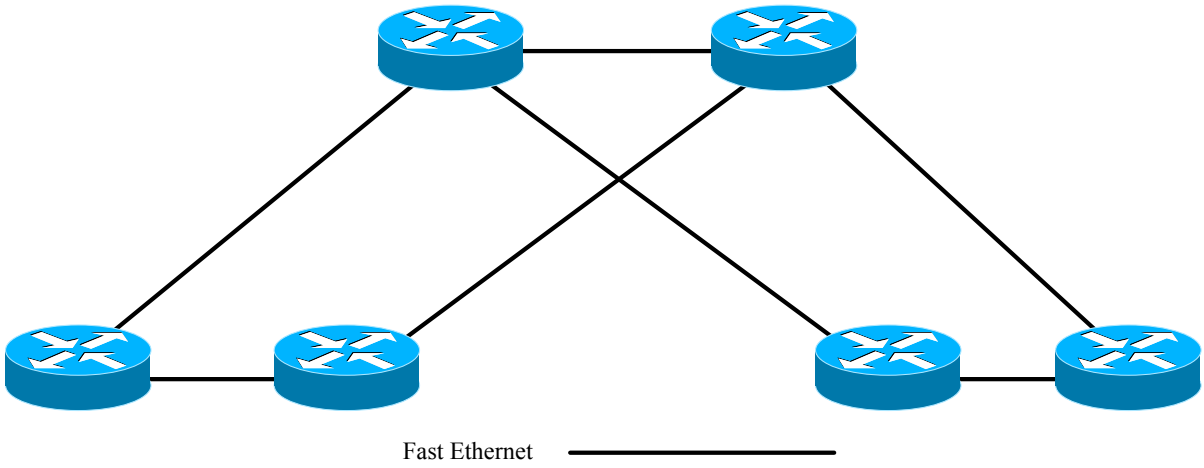


Рис. 6.5. Варіант 5

Загальний адресний простір: 10.0.0.0/11

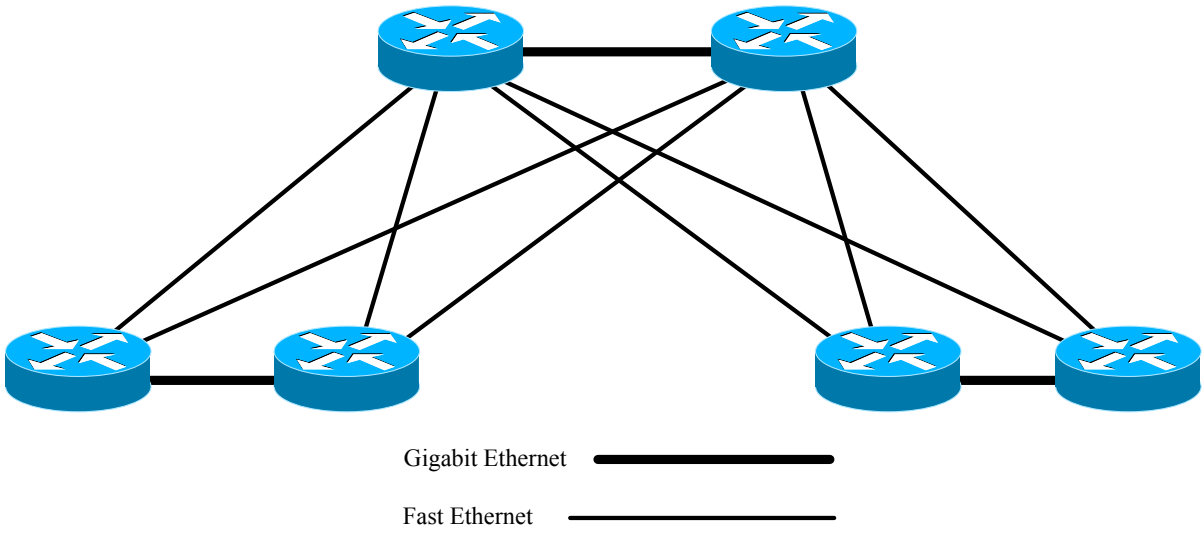


Рис. 6.6. Варіант 6

Загальний адресний простір: 10.0.0.0/12

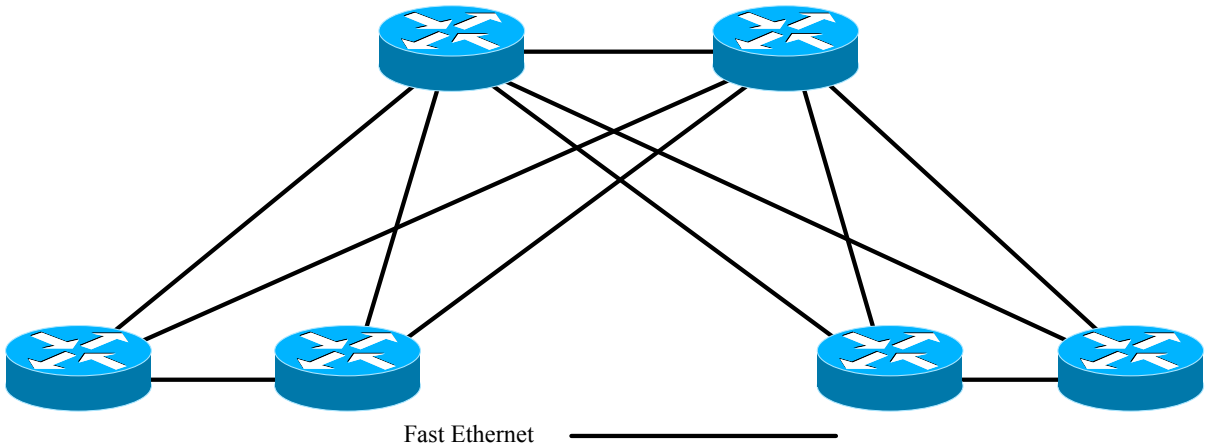


Рис. 6.7. Варіант 7

Загальний адресний простір: 10.0.0.0/13

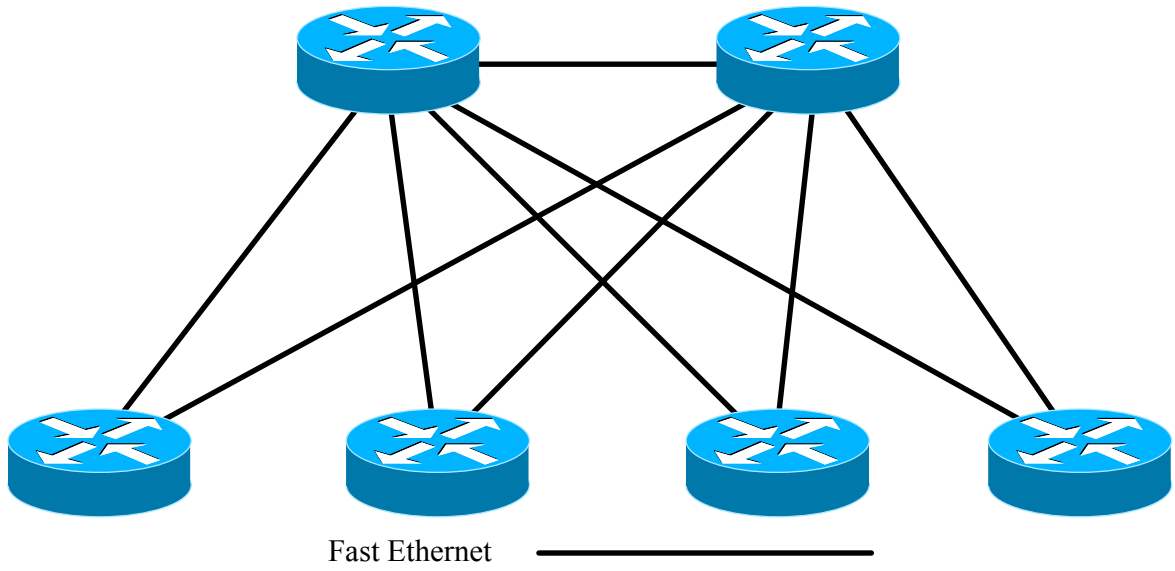


Рис. 6.8. Варіант 8

Загальний адресний простір: 10.0.0.0/14

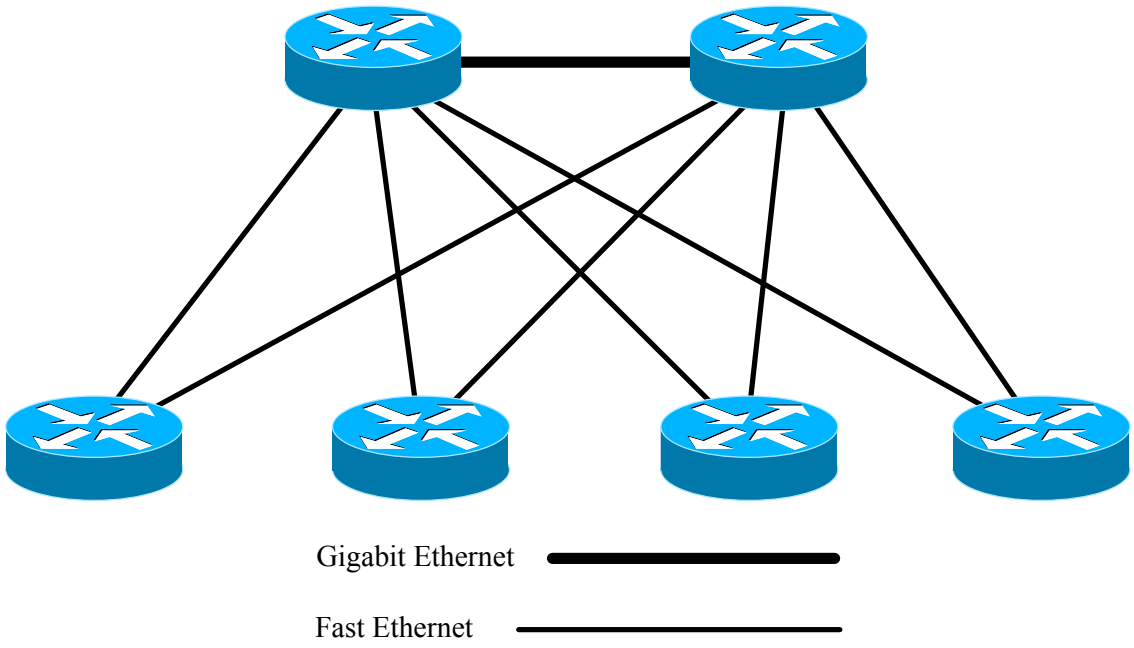


Рис. 6.9. Варіант 9

Загальний адресний простір: 10.0.0.0/15

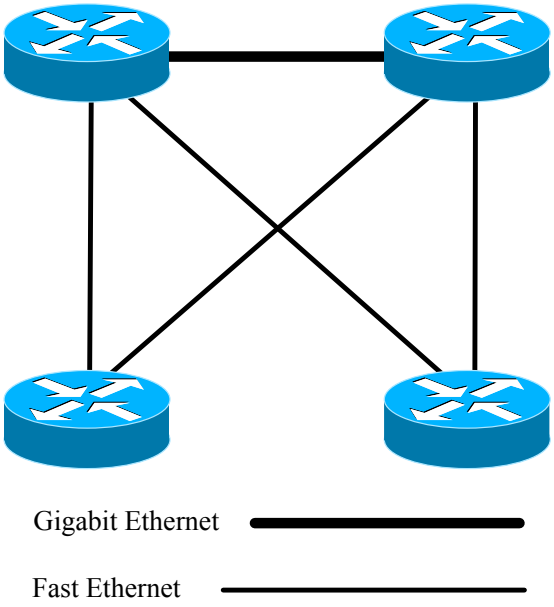


Рис. 6.10. Варіант 10

Загальний адресний простір: 10.0.0.0/20

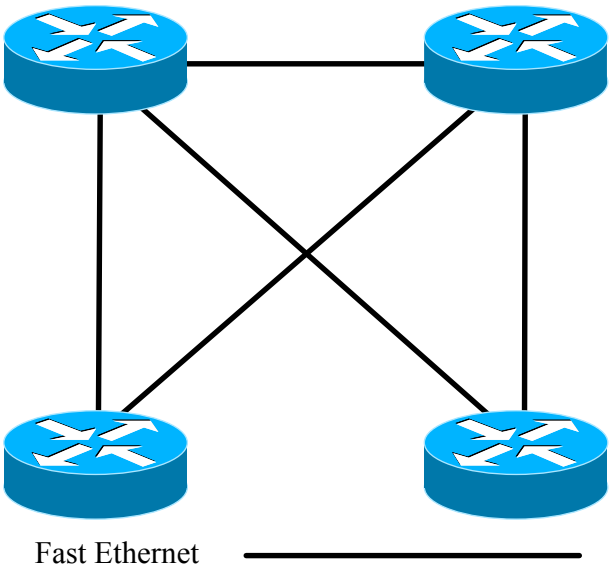


Рис. 6.11. Варіант 11

Загальний адресний простір: 10.0.0.0/19

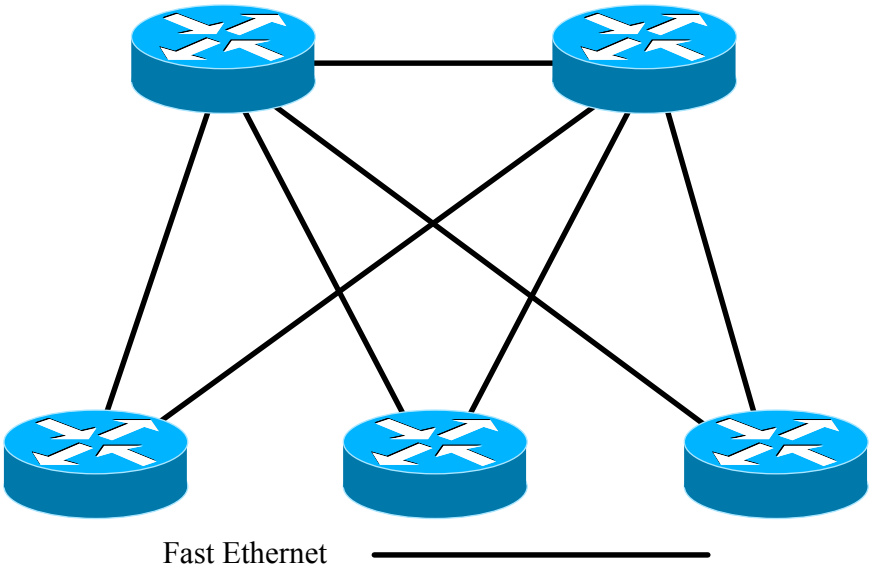


Рис. 6.12. Варіант 12

Загальний адресний простір: 10.0.0.0/18

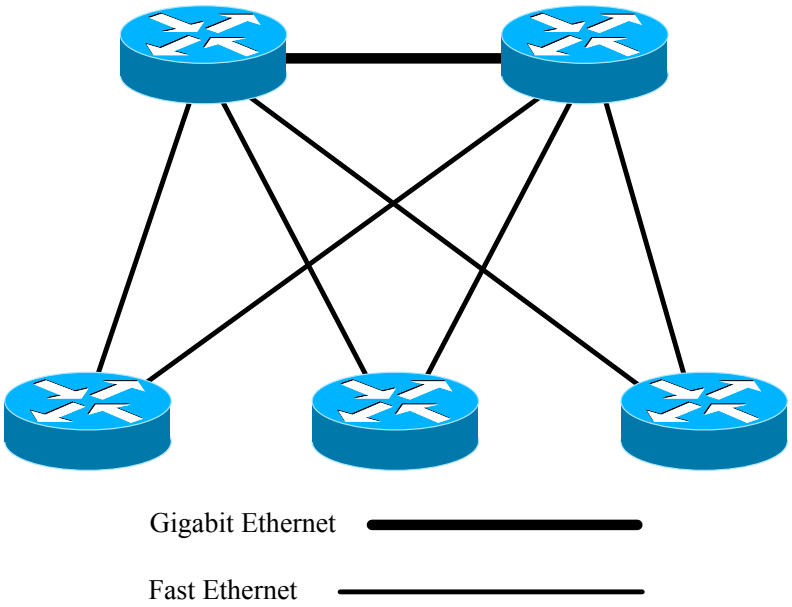


Рис. 6.13. Варіант 13

Загальний адресний простір: 10.0.0.0/17

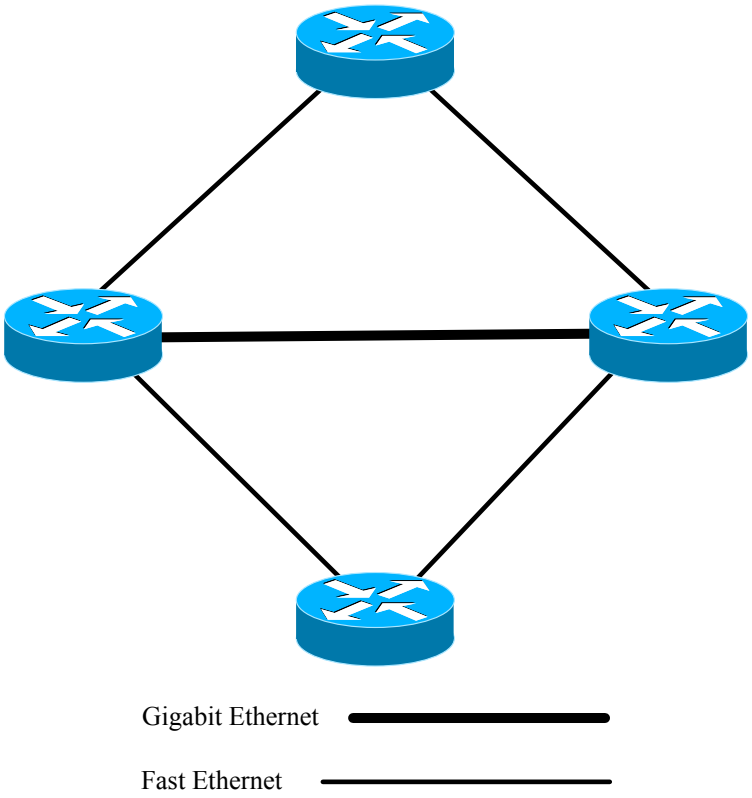


Рис. 6.14. Варіант 14

Загальний адресний простір: 10.56.0.0/13

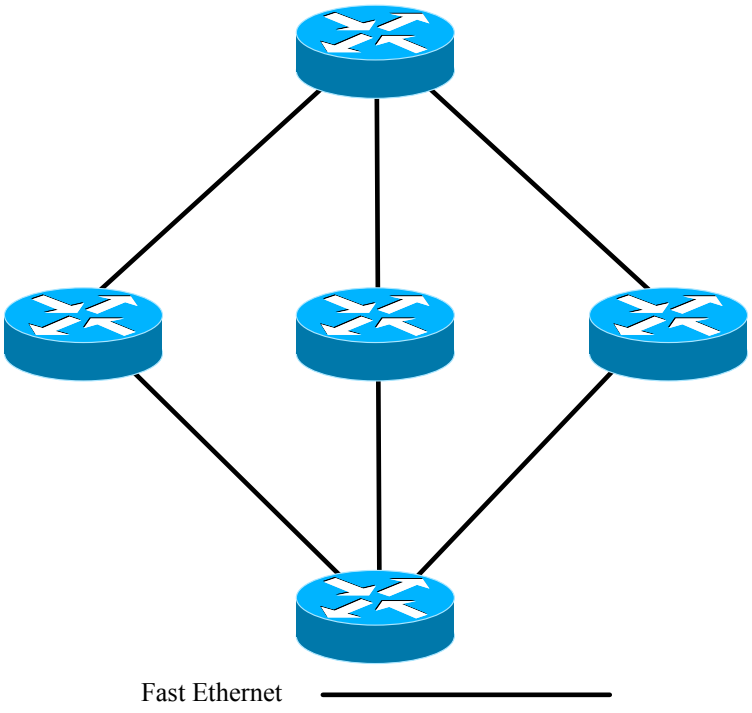


Рис. 6.15. Варіант 15

Загальний адресний простір: 10.48.0.0/13

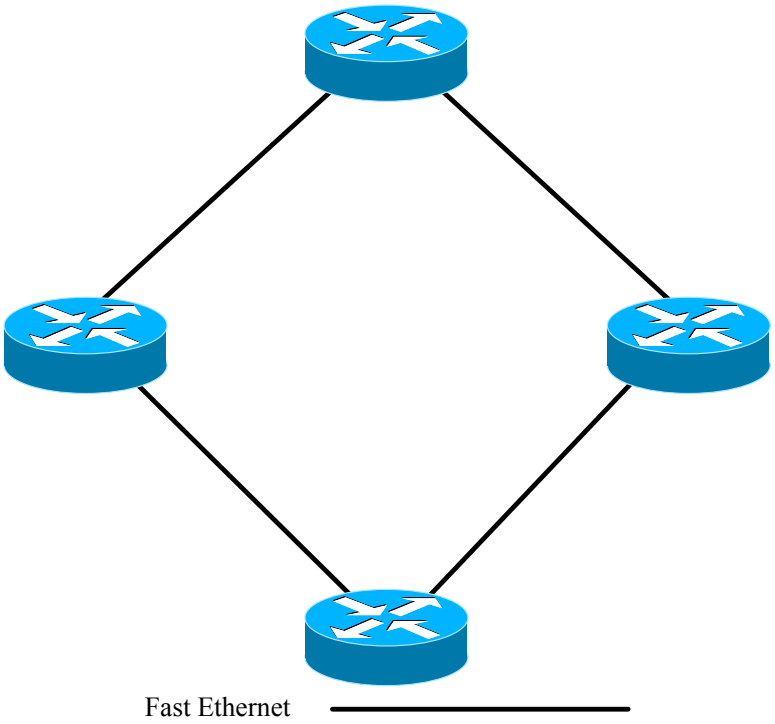


Рис. 6.16. Варіант 16

Загальний адресний простір: 10.40.0.0/13

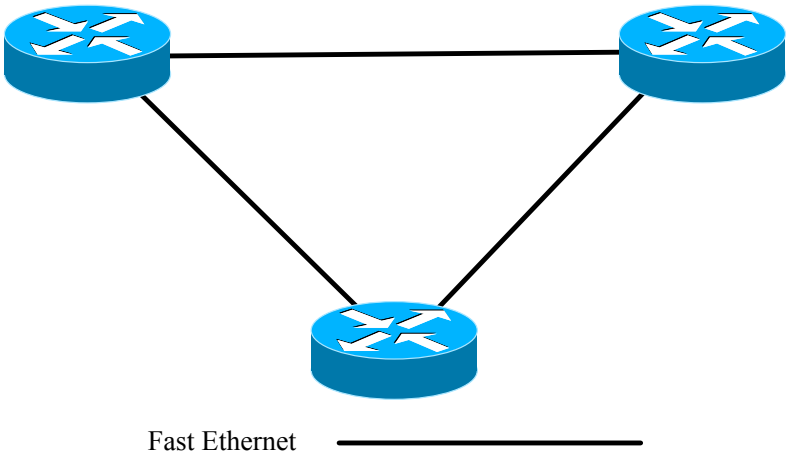


Рис. 6.17. Варіант 17

Загальний адресний простір: 10.32.0.0/13

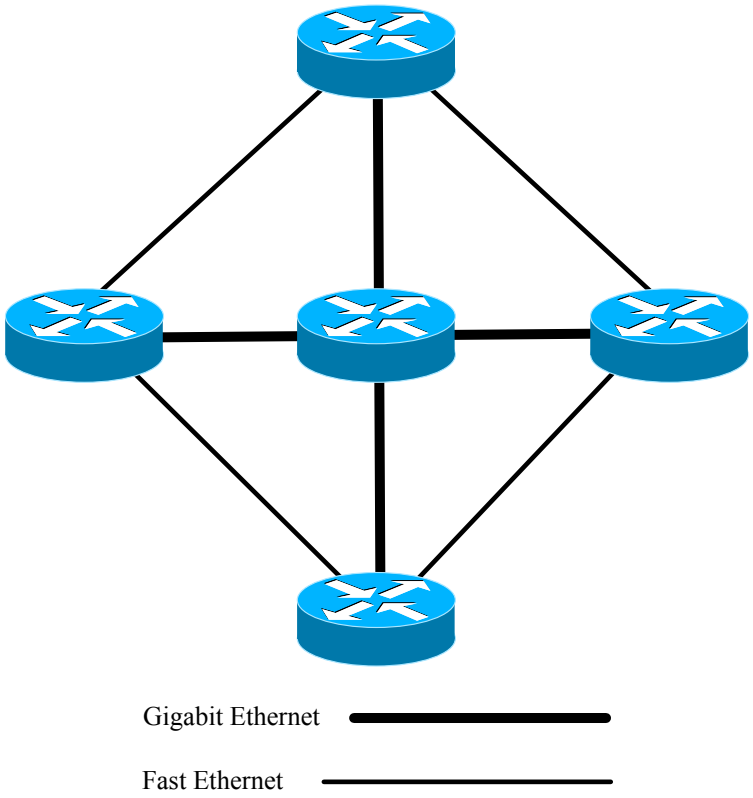


Рис. 6.18. Варіант 18

Загальний адресний простір: 10.24.0.0/13

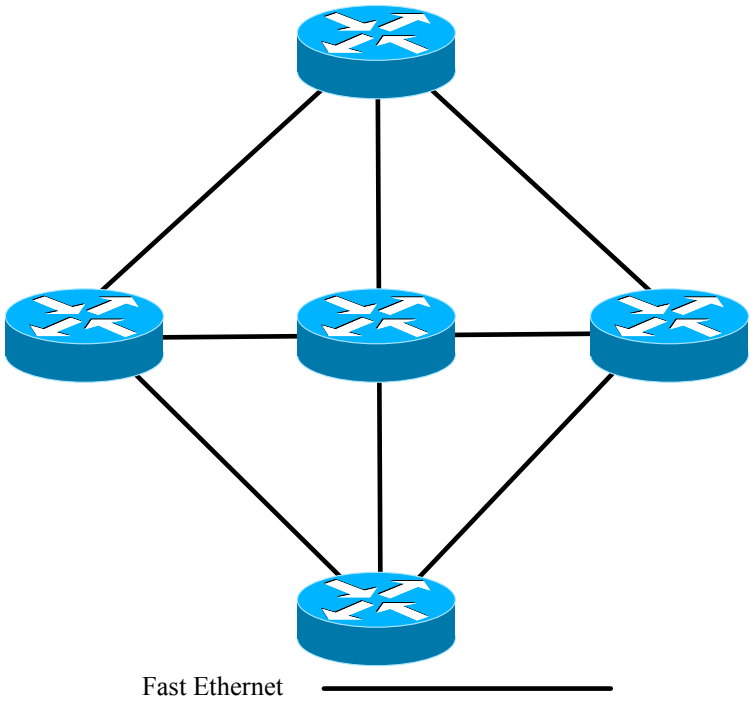


Рис. 6.19. Варіант 19

Загальний адресний простір: 10.16.0.0/13

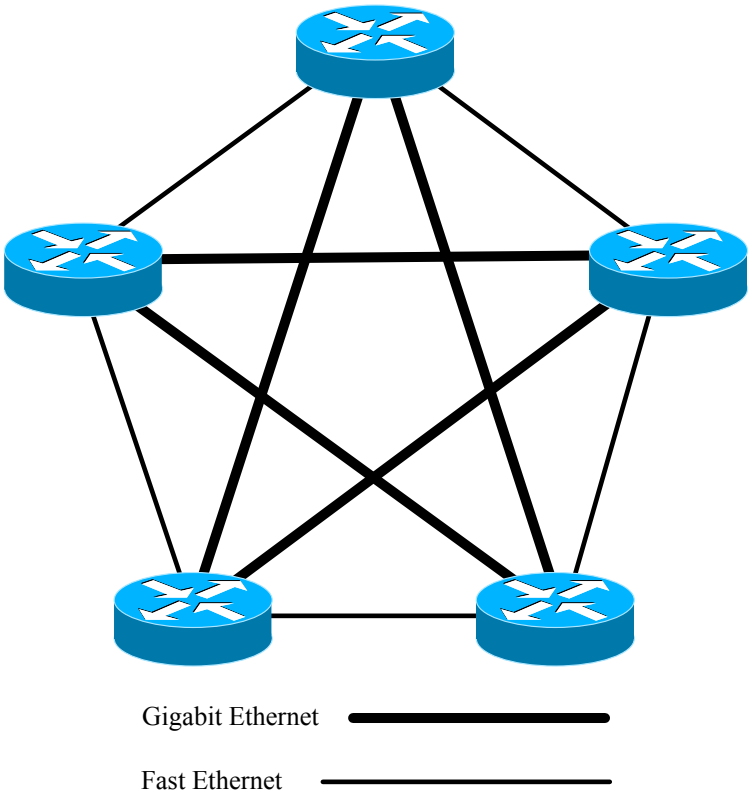


Рис. 6.20. Варіант 20

Загальний адресний простір: 10.8.0.0/13

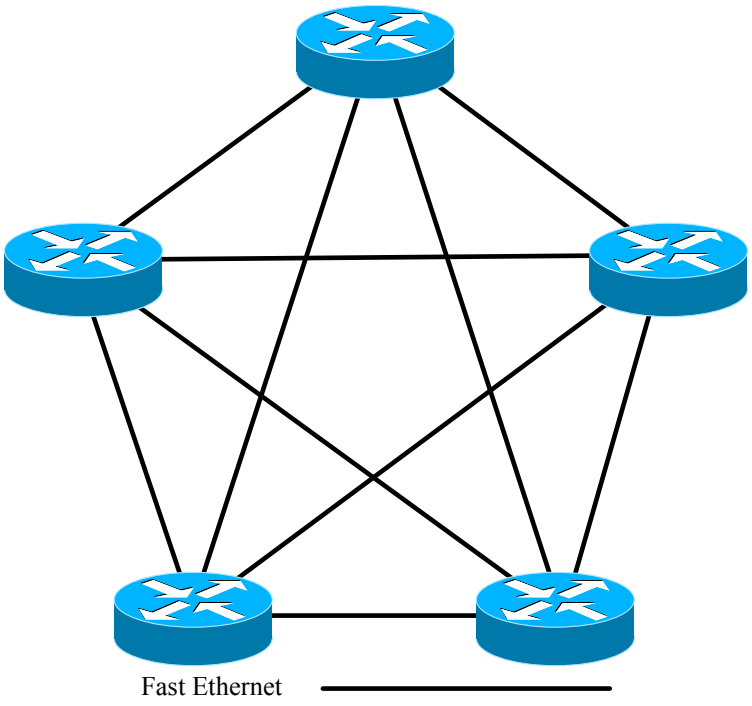
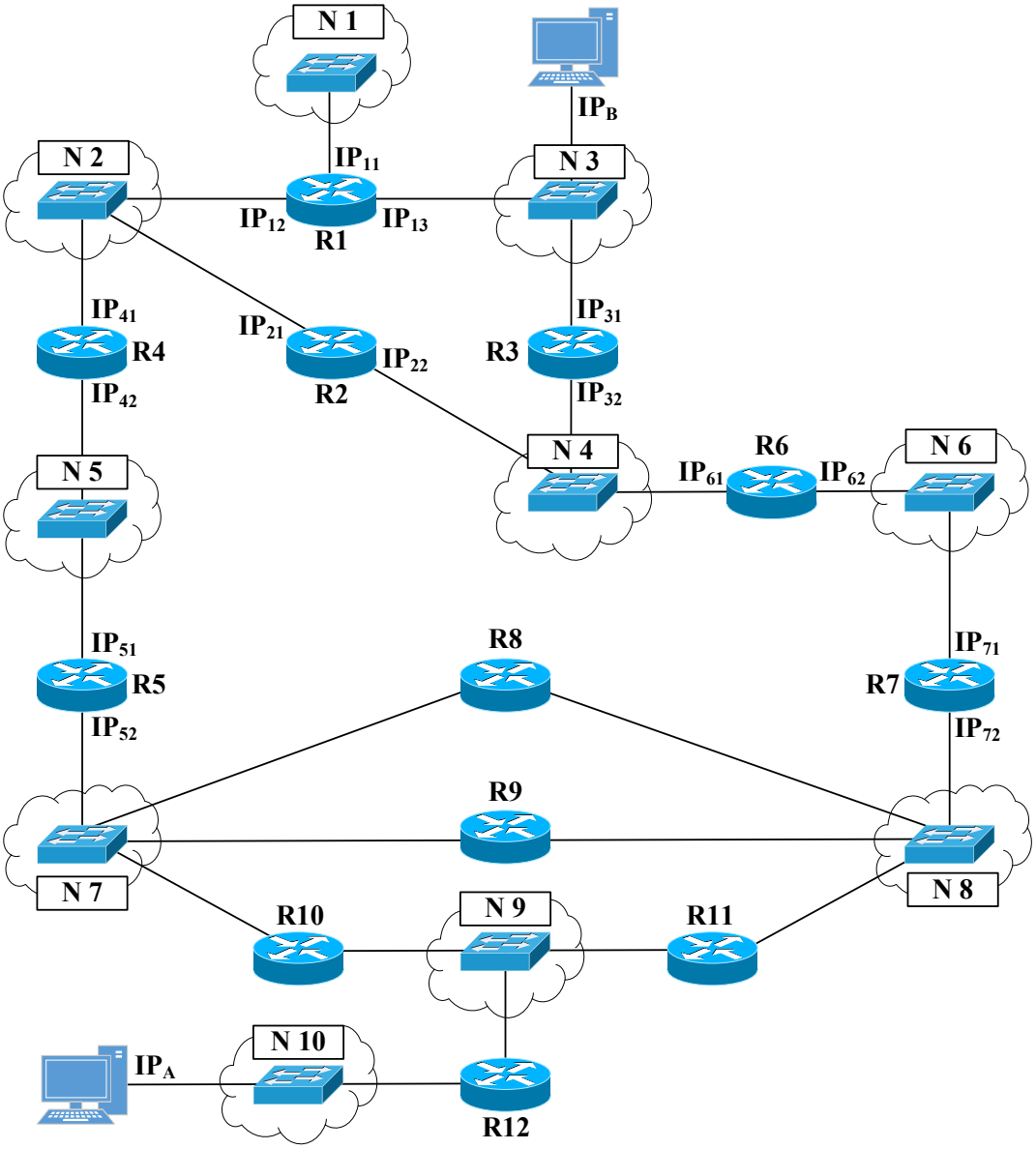


Рис. 6.21. Варіант 21

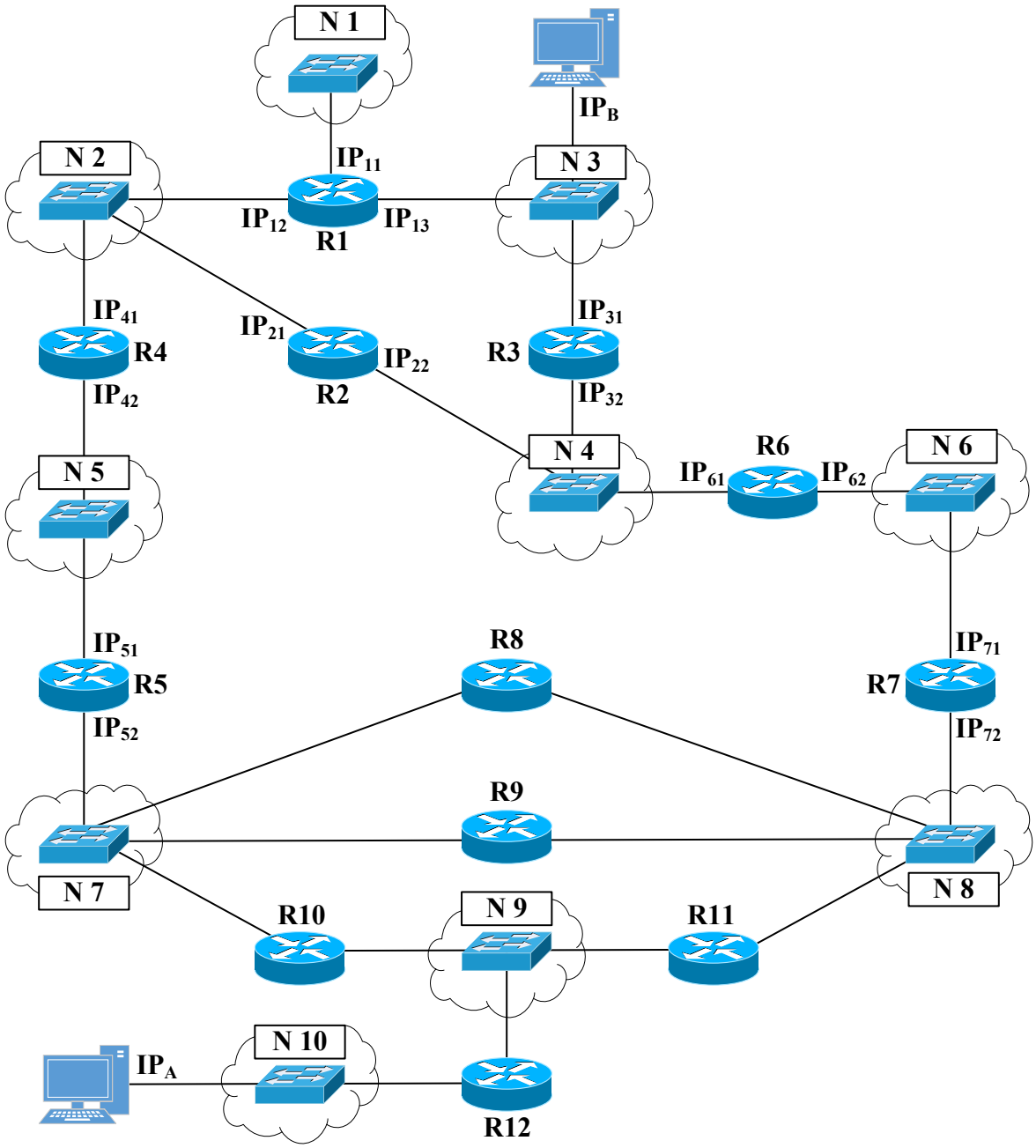
7. ТИПОВІ ЗАВДАННЯ ДЛЯ ПРОВЕДЕННЯ ТЕСТОВОГО КОНТРОЛЮ ЗНАНЬ

Q1. **Увага! Питання з декількома правильними відповідями.** Для задавання маршруту від маршрутизатора 4 до мережі призначення N1 таблиця маршрутизації маршрутизатора 4 може містити такі дані (рядки):



V1) адреса – N1, шлюз – IP_{12}, порт – IP_{41}, метрика – 1;
V2) адреса – N1, шлюз – IP_{51}, порт – IP_{42}, метрика – 6;
V3) адреса – N5, шлюз – IP_{51}, порт – IP_{42}, метрика – 6;
V4) адреса – N2, шлюз – IP_{12}, порт – IP_{41}, метрика – 1;
V5) адреса – N1, шлюз – IP_{21}, порт – IP_{41}, метрика – 3;
V6) адреса – N2, шлюз – IP_{21}, порт – IP_{41}, метрика – 3.

Q2. **Увага! Питання з декількома правильними відповідями.** Для задавання маршруту від маршрутизатора 4 до вузла призначення IP_B таблиця маршрутизації маршрутизатора 4 може містити такі дані (рядки):



V1) адреса − IP_B, шлюз – IP_{12}, порт − IP_{41}, метрика – 1;
V2) адреса − IP_B, шлюз – IP_{51}, порт − IP_{42}, метрика – 5;
V3) адреса – N3, шлюз – IP_{12}, порт − IP_{41}, метрика – 1;
V4) адреса – N5, шлюз – IP_{51}, порт − IP_{42}, метрика – 5;
V5) адреса – N2, шлюз – IP_{12}, порт − IP_{41}, метрика – 1.

Q3. Пошук маршруту до вузла призначення здійснюється маршрутизатором:

V1) завжди в першу чергу;

V2) коли специфічний маршрут не знайдено;

V3) коли неспецифічний маршрут не знайдено;

V4) коли знайдено статичний маршрут;

V5) коли маршрут до мережі призначення не знайдено.

Q4. **Увага! Питання з декількома правильними відповідями.** Пошук маршруту до мережі призначення здійснюється маршрутизатором тільки у випадку, коли:

V1) специфічний маршрут не знайдено;

V2) маршрут до вузла призначення не знайдено;

V3) неспецифічний маршрут не знайдено;

V4) знайдено статичний маршрут;

V5) знайдено динамічний маршрут.

Q5. **Увага! Питання з декількома правильними відповідями.** Маршрутизатор у першу чергу шукає специфічний маршрут:

V1) який є маршрутом до вузла призначення;

V2) який є маршрутом до мережі призначення;

V3) ознакою якого є маска, що містить 32 одиниці (у двійковому вигляді);

V4) ознакою якого є маска вигляду 255.255.255.255;

V5) ознакою якого є маска вигляду 0.0.0.0;

V6) ознакою якого є маска, що містить 32 нулі (у двійковому вигляді).

Q6. **Увага! Питання з декількома правильними відповідями.** Маршрутизатор у першу чергу шукає специфічний маршрут, для чого:

V1) адреса призначення, яка відповідає запису (рядку) таблиці маршрутизації, що містить маску 255.255.255.255, порівнюється з IP-адресою, вилученою з IP-пакета;

V2) адреса призначення, яка відповідає запису (рядку) таблиці маршрутизації, що містить маску з 32 одиниць (у двійковому вигляді), порівнюється з IP-адресою, вилученню з IP-пакета;

V3) адреса призначення, яка відповідає запису (рядку) таблиці маршрутизації, що містить маску з 32 нулями (у двійковому вигляді), порівнюється з IP-адресою, вилученою з IP-пакета;

V4) адреса призначення, яка відповідає запису (рядку) таблиці маршрутизації, що містить маску 0.0.0.0, порівнюється з IP-адресою, вилученою з IP-пакета;

V5) адреса призначення, яка відповідає запису (рядку) таблиці маршрутизації, що містить маску 127.0.0.0, порівнюється з IP-адресою, вилученою з IP-пакета.

Q7. При пошуку маршруту до мережі призначення маршрутизатором:

V1) для кожного запису (рядка) таблиці маршрутизації виконується побітно операція логічного добутку маски мережі, відповідної запису (рядку) таблиці маршрутизації, та IP-адреси, вилученої з IP-пакета;

V2) для кожного запису (рядка) таблиці маршрутизації виконується побітно операція логічної суми маски мережі, відповідної запису (рядку) таблиці маршрутизації, та IP-адреси, вилученої з IP-пакета;

V3) для кожного запису (рядка) таблиці маршрутизації виконується побітно операція логічного добутку шлюзу призначення, відповідного запису (рядку) таблиці маршрутизації, та IP-адреси, вилученої з IP-пакета;

V4) результат побітної логічної суми маски мережі та IP-адреси, вилученої з IP-пакета, порівнюється з адресою призначення, яка міститься в тому самому записі (рядку) таблиці маршрутизації, що і вищевказана маска;

V5) маршрутизатор відмічає запис (рядок) таблиці маршрутизації, якщо було виявлено співпадання результату побітної логічної суми маски мережі, що міститься в цьому запису (рядку), та IP-адреси, вилученої з IP-пакета, з адресою призначення, відповідної вищевказаному запису (рядку) таблиці маршрутизації.

Q8. При пошуку маршруту до мережі призначення маршрутизатором:

V1) результат побітного логічного добутку маски мережі та IP-адреси, вилученої з IP-пакета, порівнюється з адресою призначення, яка міститься в тому самому записі (рядку) таблиці маршрутизації, що і вищевказана маска;

V2) для кожного запису (рядка) таблиці маршрутизації виконується побітно операція логічної суми маски мережі, відповідної запису (рядку) таблиці маршрутизації, та IP-адреси, вилученої з IP-пакета;

V3) для кожного запису (рядка) таблиці маршрутизації виконується побітно операція логічного добутку шлюзу призначення, відповідного запису (рядку) таблиці маршрутизації, та IP-адреси, вилученої з IP-пакета;

V4) результат побітної логічної суми маски мережі та IP-адреси, вилученої з IP-пакета, порівнюється з адресою призначення, яка міститься в тому самому записі (рядку) таблиці маршрутизації, що і вищевказана маска;

V5) маршрутизатор відмічає запис (рядок) таблиці маршрутизації, якщо було виявлено співпадання результату побітної логічної суми маски мережі, що міститься в цьому запису (рядку), та IP-адреси, вилученої з IP-пакета, з адресою призначення, відповідної вищевказаному запису (рядку) таблиці маршрутизації.

Q9. При пошуку маршруту до мережі призначення маршрутизатором:

V1) маршрутизатор відмічає запис (рядок) таблиці маршрутизації, якщо було виявлено співпадання результату побітного логічного добутку маски мережі, що міститься в цьому запису (рядку), та IP-адреси, вилученої з IP-пакета, з адресою призначення, відповідної вищевказаному запису (рядку) таблиці маршрутизації;

V2) для кожного запису (рядка) таблиці маршрутизації виконується побітно операція логічної суми маски мережі, відповідної запису (рядку) таблиці маршрутизації, та IP-адреси, вилученої з IP-пакета;

V3) для кожного запису (рядка) таблиці маршрутизації виконується побітно операція логічного добутку шлюзу призначення, відповідного запису (рядку) таблиці маршрутизації, та IP-адреси, вилученої з IP-пакета;

V4) результат побітної логічної суми маски мережі та IP-адреси, вилученої з IP-пакета, порівнюється з адресою призначення, яка міститься в тому самому записі (рядку) таблиці маршрутизації, що і вищевказана маска;

V5) маршрутизатор відмічає запис (рядок) таблиці маршрутизації, якщо було виявлено співпадання результату побітної логічної суми маски мережі, що міститься в цьому запису (рядку), та IP-адреси, вилученої з IP-пакета, з адресою призначення, відповідної вищевказаному запису (рядку) таблиці маршрутизації.

Q10. У ході пошуку маршруту до мережі призначення маршрутизатор знищує (відкидає) IP-пакет, якщо:

V1) не було виявлено жодного співпадання результату побітного логічного добутку маски мережі та IP-адреси, вилученої з IP-пакета, з адресою призначення, відповідної запису (рядку) таблиці маршрутизації;

V2) не було виявлено жодного співпадання результату побітного логічного добутку адреси призначення з таблиці маршрутизації та IP-адреси, вилученої з IP-пакета, з адресою призначення, відповідної запису (рядку) таблиці маршрутизації;

V3) не було виявлено жодного співпадання результату побітного логічного добутку адреси шлюзу з таблиці маршрутизації та маски мережі, вилученої з IP-пакета, з адресою призначення, відповідної запису (рядку) таблиці маршрутизації;

V4) не було виявлено жодного співпадання результату побітної логічної суми маски мережі та IP-адреси, вилученої з IP-пакета, з адресою призначення, відповідної запису (рядку) таблиці маршрутизації;

V5) не було виявлено жодного співпадання результату побітної логічної суми адреси призначення з таблиці маршрутизації та IP-адреси, вилученої з IP-пакета, з адресою призначення, відповідної запису (рядку) таблиці маршрутизації.

Q11. **Увага! Питання з декількома правильними відповідями.** Запис (рядок) у таблиці маршрутизації, який містить адресу призначення 0.0.0.0 та маску 0.0.0.0, задає:

V1) маршрут за замовчуванням;

V2) маршрут, який буде вибраний тільки за відсутності інших маршрутів до адреси призначення;

V3) маршрут, який буде обраний у першу чергу;

V4) маршрут, який має пріоритет перед іншими маршрутами;

V5) правильних відповідей нема.

Q12. **Увага! Питання з декількома правильними відповідями.** Для того щоб маршрутизатору задати маршрут за замовчуванням, необхідно, щоб запис (рядок) таблиці маршрутизації містив:

V1) адресу призначення 00000000.00000000.00000000.00000000 та маску 00000000.00000000.00000000.00000000;

V2) адресу призначення 0.0.0.0 та маску 0.0.0.0;

V3) адресу призначення 255.255.255.255 та маску 255.255.255.255;

V4) адресу призначення 0.0.0.0 та маску 255.255.255.255;

V5) адресу призначення 11111111.11111111.11111111.11111111 та маску 11111111.11111111.11111111.11111111.

Q13. **Увага! Питання з декількома правильними відповідями.** Запис (рядок) у таблиці маршрутизації, який містить маску 255.255.255.255, задає:

V1) маршрут за замовчуванням;

V2) маршрут, який буде вибраний тільки за відсутності інших маршрутів до адреси призначення;

V3) специфічний маршрут;

V4) неспецифічний маршрут;

V5) маршрут до вузла призначення.

Q14. **Увага! Питання з декількома правильними відповідями.** Для того щоб маршрутизатор не знищував (не відкидав) IP-пакет у випадку відсутності явно заданих маршрутів, необхідно задати маршрут, який містить:

V1) адресу призначення 00000000.00000000.00000000.00000000 та маску 00000000.00000000.00000000.00000000;

V2) адресу призначення 0.0.0.0 та маску 0.0.0.0;

V3) адресу призначення 255.255.255.255 та маску 255.255.255.255;

V4) адресу призначення 0.0.0.0 та маску 255.255.255.255;

V5) адресу призначення 11111111.11111111.11111111.11111111 та маску 11111111.11111111.11111111.11111111.

Перевірити правильні відповіді на тестові питання можна в дод. 4.

Бібліографічний список

1. Олифер, В. Г., Компьютерные сети. Принципы, технологии, протоколы [Текст]: учеб. для вузов / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – СПб.: Питер, 2010. – 944 с.
2. Песин, И. Повесть об IP-адресации [Электронный ресурс] / И. Песин. – Режим доступа: http://ivanpesin.info/articles/povest_ob_ip.html.
3. Фильчагин, А. Ю. IP-маршрутизация в операционной системе Windows [Электронный ресурс]: учеб. пособие / А. Ю. Фильчагин http://opds.sut.ru/old/electronic_manuals/ip_rout/up.doc.
4. Методичні вказівки до практичних занять з дисциплін «Телекомунікаційні та інформаційні мережі», «Інтегральні цифрові мережі зв'язку» (розподіл IP-адрес) [Текст] / С. І. Приходько, О. С. Жученко, К. А. Трубчанінова, С. С. Єременко. − Харків: УкрДАЗТ, 2012. – 42 с.
5. TCP/IP. Для профессионалов [Текст] / Т. Паркер, К. Сиян. – 3-е изд. – СПб.: Питер, 2004. – 859 с.
6. QoS (ToS) part 1 [Електронний ресурс]. – Режим доступу: http://bos-info.com/cisco/qos-tos-part-1.html.
7. Семёнов, Ю. А. Телекоммуникационные технологии [Электронный ресурс] / Ю. А. Семёнов. – Режим доступа: http://book.itep.ru/1/intro1.htm.

Додаток 1

Основні режими конфігурування пристроїв з операційною системою Cisco IOS

Таблиця Д.1.1

Основні режими конфігурування пристроїв з операційною системою Cisco IOS

Режим	Символи запрошення в командному рядку	Команда входу в режим	Команда виходу з режиму
Користувацький	Router>	Установлюється при вході в пристрій після натискання клавіші Enter	exit (ex)
Привілейований	Router#	enable (en)	disable (disab)
Глобального конфігурування	Router(config)#	configure terminal (conf)	exit (ex)
Детального конфігурування	Router(config-mode) #, де *mode* – назва об'єкта, що підлягає конфігуруванню, наприклад: Router(config-if) # – конфігурування інтерфейсу; Router(config-line) # – конфігурування термінальної лінії; Router(config-router) # – конфігурування динамічної маршрутизації; Router(config-vlan) # – конфігурування віртуальної локальної мережі VLAN	Команди, відповідні до об'єкта конфігурування	exit (ex)

Додаток 2

Контекстна довідка в командному рядку операційної системи Cisco IOS

Для виведення на екран списку всіх доступних команд операційної системи Cisco IOS необхідно використовувати команду «help» або «?» контекстної довідки, яка вводиться в привілейованому режимі:

Switch1>enable
Switch1#?
Switch1#help.

Якщо ввести відому частину команди, а після неї без пробілу поставити знак питання «?», то операційна система Cisco IOS виведе на екран список усіх можливих команд, що починаються з уведеної частини команди, наприклад

Switch1#di? (перед знаком питання нема пробілу!)
dir disable disconnect.

Крім того, можна одержати список можливих підкоманд для команди. Для цього необхідно ввести частину цієї команди, потім пробіл, а після нього знак питання «?». При цьому буде виведено на екран список можливих варіантів продовження цієї команди, наприклад

Switch1#show vlan ? (перед знаком питання є пробіл!)

```
Switch1#show vlan ?
  brief  VTP all VLAN status in brief
  id     VTP VLAN status by VLAN id
  name   VTP VLAN status by VLAN name
  <cr>
```

Також символ знака питання «?» (з пробілом перед ним!) можна використовувати для одержання списку доступних параметрів команди, наприклад

Switch1#show vlan id ? (перед знаком питання є пробіл!)

```
Switch1#show vlan id ?
  <1-1005>  ISL VLAN IDs 1-1005
```

Додаток 3

Принципи визначення маршруту IP-пакета (команда tracert)

Утиліта трасування маршруту до заданого вузла tracert.exe в операційній системі Windows є одним з найчастіше використовуваних інструментів мережевої діагностики. Основне її призначення − одержати ланцюжок вузлів, через які проходить IP-пакет, адресований кінцевому вузлу.

Застосування утиліти tracert.exe здійснюється шляхом введення до командного рядка операційної системи Windows команди tracert з відповідними параметрами.

Команда tracert дозволяє визначити маршрут проходження IP-пакета до вузла призначення за допомогою посилання до вузла призначення серії ехо-запитів протоколу ICMP з різними значеннями параметра TTL (строку життя IP-пакета) в IP-пакетах. За замовчуванням кожна серія містить 3 IP-пакети з однаковим значенням TTL.

Кожен маршрутизатор, через який проходить IP-пакет, зобов'язаний перед подальшим пересиланням пакета зменшити значення його поля TTL на 1. Фактично TTL служить лічильником вузлів. Передбачається, що коли параметр TTL стає рівним 0, маршрутизатор посилає вузлу відправнику IP-пакета повідомлення ICMP про видалення IP-пакета (про закінчення часу життя IP-пакета).

Команда tracert визначає маршрут, посилаючи першу серію ехо-запитів зі значенням TTL, що дорівнює 1, і збільшуючи значення цього параметра на одиницю для кожної наступної серії ехо-запитів, що відправляються доти, поки кінцевий вузол не відповість або поки не буде досягнуто максимальне значення кількості переходів.

Для ехо-запитів першої серії параметр TTL становить 1, тому перший же маршрутизатор повертає назад повідомлення, що вказує про видалення IP-пакета (про закінчення часу життя IP-пакета), у якому міститься копія IP-пакета й копія ехо-запиту. Далі tracert фіксує IP-адресу маршрутизатора, яка відправила повідомлення про видалення IP-пакета (про закінчення часу життя IP-пакета), а також час між відправленням IP-пакета й одержанням відповіді (ці відомості виводяться в командному рядку як результат роботи команди tracert).

Потім tracert повторює відправлення серії IP-пакетів, але вже з параметром TTL, що дорівнює 2, що змушує перший маршрутизатор зменшити параметр TTL на одиницю й направити IP-пакети до наступного маршрутизатора, який у свою чергу, одержавши IP-пакети з параметром TTL, що дорівнює 1, так само повертає назад повідомлення, що вказує про видалення IP-пакета (про закінчення часу життя IP-пакета).

Цей процес повторюється доти, поки пакет не досягне вузла призначення або поки не буде досягнуто максимальне значення кількості переходів (за замовчуванням − 30). На вузлі призначення IP-пакет з параметром TTL, що дорівнює 1, не відкидається. При одержанні відповіді від цього вузла процес визначення маршруту вважається завершеним.

Зазначимо, що деякі маршрутизатори можуть не посилати повідомлення про закінчення часу життя для IP-пакетів з нульовими значеннями TTL, і їх не бачить команда tracert. У цьому випадку перехід позначається рядком зірочок (*).

Синтаксис команди tracert (параметри наведені в табл. Д.3.1):

tracert <ім’я призначення або IP-адреса> [-d]

[-h <максимальна кількість переходів>] [-j <список вузлів>] [-w <таймаут>].

Таблиця Д.3.1

Параметри команди tracert

Параметр	Призначення
<ім’я призначення або _IP-адрес>	Доменне ім’я вузла призначення або IP-адреса
-d	Не використовувати перетворення в імена вузлів. Прискорює виконання команди tracert за рахунок відмови від перетворення IP-адрес маршрутизаторів у доменні імена
-h	Максимальна кількість переходів по шляху до вузла призначення. За замовчуванням використовується значення 30
-j	Дозволяє вказати проміжні вузли призначення у вигляді списку IP-адрес, розділених пробілами (маршрутизатори повинні підтримувати режим маршрутизації від джерела). Можна вказати до дев'яти проміжних вузлів
-w	Час очікування відповіді ICMP Time Exceeded або відповіді Echo Reply на тестовий запит (мілісекунди). Якщо відповідь не була отримана за зазначений час, відображується символ (*). За замовчуванням використовується значення 4000 (4 с)

Додаток 4

Відповіді на тестові питання з розд. 7

Тестове питання	Правильна відповідь
Q1	V1, V2, V5
Q2	V1, V2
Q3	V1
Q4	V1, V2
Q5	V1, V3, V4
Q6	V1, V2
Q7	V1
Q8	V1
Q9	V1
Q10	V1
Q11	V1, V2
Q12	V1, V2
Q13	V3, V5
Q14	V1, V2