

Затверджено науково-методичною
радою ЖДТУ
протокол від «__» _____ 20__ р.
№ __

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
для проведення лабораторних робіт
з навчальної дисципліни
**«КОМП'ЮТЕРНІ РАДІОМЕРЕЖІ ТА ІНФОРМАЦІЙНІ
ТЕХНОЛОГІЇ»**

для студентів освітнього рівня «МАГІСТР»
спеціальності 163 «Біомедична інженерія»
освітньо-професійна програма «Біомедична інженерія»
факультет інформаційно-комп'ютерних технологій
кафедра біоінженерії та телекомунікацій

Розглянуто і рекомендовано
на засіданні кафедри
біоінженерії та телекомунікацій
протокол від «__» _____ 201__ р.
№ _____

Розробник: к.т.н., ст. викл. кафедри біоінженерії та
телекомунікацій Коломієць Р. О.

Житомир
2017 – 2018 н.р.

ЗМІСТ

Лабораторна робота №1. ЗНАЙОМСТВО З СЕРЕДОВИЩЕМ ДЛЯ МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ CISCO PACKET TRACER	4
1.1. Короткі теоретичні відомості	4
1.2. Порядок виконання роботи	10
1.3. Рекомендований зміст звіту	13
1.4. Контрольні запитання	14
Лабораторна робота №2. ПОБУДОВА СКЛАДЕНОЇ МЕРЕЖІ З БЕЗКЛАСОВОЮ АДРЕСАЦІЄЮ	15
2.1. Короткі теоретичні відомості	15
2.2. Порядок виконання роботи	20
2.3. Рекомендований зміст звіту	21
2.4. Контрольні запитання	22
Лабораторна робота №3. СТАТИЧНА МАРШРУТИЗАЦІЯ	23
3.1. Короткі теоретичні відомості	23
3.2. Порядок виконання роботи	24
3.3. Рекомендований зміст звіту	25
3.4. Контрольні запитання	25
Лабораторна робота №4. ДИНАМІЧНА МАРШРУТИЗАЦІЯ	26
4.1. Короткі теоретичні відомості	26
4.2. Порядок виконання роботи	31
4.3. Рекомендований зміст звіту	32
4.4. Контрольні запитання	32
Література	33

Лабораторна робота №1

ЗНАЙОМСТВО З СЕРЕДОВИЩЕМ ДЛЯ МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ CISCO PACKET TRACER

Мета роботи: ознайомитися з середовищем для моделювання та оптимізації комп'ютерних мереж Cisco Packet Tracer. Навчитися складати моделі комп'ютерних мереж та конфігурувати віртуальне обладнання.

1.1 Короткі теоретичні відомості

Програмні продукти Packet Tracer дають можливість створювати мережеві топології з широкого спектру маршрутизаторів і комутаторів компанії Cisco, робочих станцій і мережевих з'єднань типу Ethernet, Serial, ISDN, Frame Relay. Ця функція може бути виконана як для навчання, так і для роботи. Наприклад, щоб зробити настройку мережі ще на етапі планування або щоб створити копію робочої мережі з метою усунення несправності.

Для запуску Cisco Packet Tracer необхідно запустити виконуваний файл *PacketTracer5.exe*. Загальний вид програми можна побачити на рис. 1.1.

Робоча область вікна програми складається з наступних елементів:

1. *Menu Bar* - панель, яка містить меню *File, Edit, Options, View Tools, Extensions, Help*.

2. *Main Tool Bar* - містить графічні зображення ярликів для доступу до команд меню *File, Edit, View* і *Tools*, а також кнопку *Network Information*.

3. *Common Tools Bar* - панель, яка забезпечує доступ до найбільш використовуваним інструментам програми: *Select*, *Move Layout*, *Place Note*, *Delete*, *Inspect*, *Add Simple PDU* і *Add Complex PDU*.

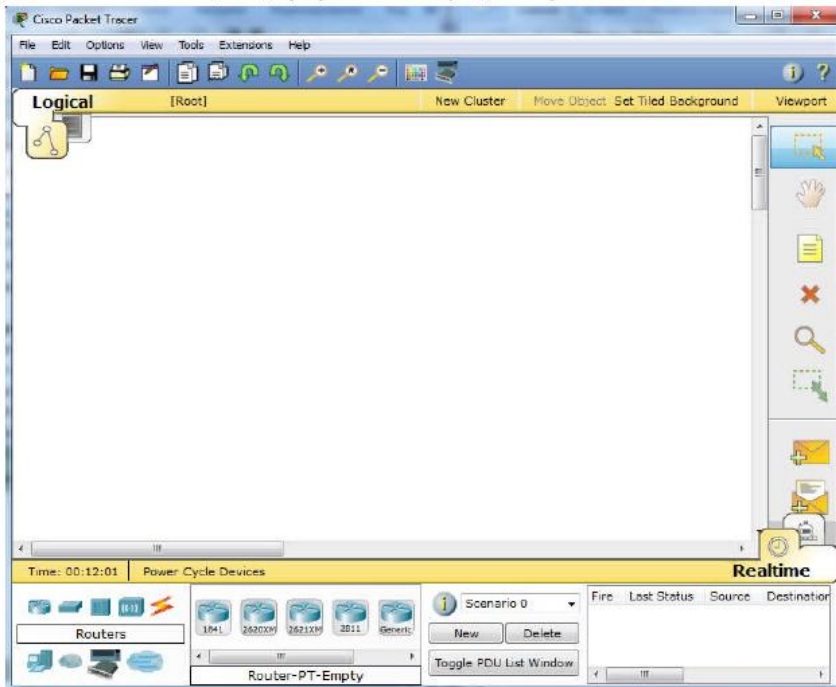


Рис. 1.1 – Головне вікно програми Cisco Packet Tracer 5

4. *Logical/Physical Workspace and Navigation Bar* – панель, яка дає можливість перемикати робочу область: фізичну або логічну, а також дозволяє переміщатися між рівнями кластера.

5. *Workspace* - область, в якій відбувається створення мережі, проводяться спостереження за симуляцією і є видимою різною інформацією та статистикою.

6. *Realtime/Simulation Bar* - за допомогою закладок цієї панелі можна перемикатися між режимом *Realtime* і режимом *Simulation*. Вона також містить кнопки, що відносяться до *Power Cycle Devices*, кнопки *Play Control* і перемикач *Event List* в режимі *Simulation*.

7. *Network Component Box* - це область, в якій вибираються пристрої та зв'язки для розміщення їх на робочому просторі. Вона містить область *Device-type Selection* і область *Device-specific Selection*.

8. *Device-type Selection Box* - ця область містить доступні типи пристроїв і зв'язків в *Packet Tracer*. Область *Device-specific Selection* змінюється залежно від вибраного пристрою.

9. *Device-specific Selection Box* - ця область використовується для вибору конкретних пристроїв і з'єднань, необхідних для створення в робочому просторі моделі мережі.

10. *User Created Packet Window* - це вікно керує пакетами, які були створені в мережі під час симуляції сценарію.

Для створення топології необхідно вибрати пристрій з панелі *Network Component*, а потім з панелі *Device-type Selection* вибрати тип вибраного пристрою. Після цього потрібно натиснути ліву кнопку миші в полі робочої області програми (*Workspace*). Також можна перемістити пристрій прямо з області *Device-type Selection*, але при цьому буде вибрана модель пристрою за умовчанням.

Для швидкого створення декількох екземплярів одного і того ж пристрою потрібно, утримуючи кнопку `Ctrl`, натиснути на пристрій в області *Device-specific Selection* і відпустити кнопку `Ctrl`. Після цього можна кілька разів натиснути на робочій області для добавлення копій пристроїв.

У *Packet Tracer* представлені наступні типи пристроїв:

- маршрутизатори;
- комутатори (у тому числі і мости);
- хаби та повторювачі;
- кінцеві пристрої - ПК, сервери, принтери, IP-телефони;
- бездротові пристрою: точки доступу та бездротові маршрутизатори;
- решта пристроїв - хмара, DSL-модем і кабельний модем.

Додамо необхідні елементи в робочу область програми так, як показано на рис. 1.2.

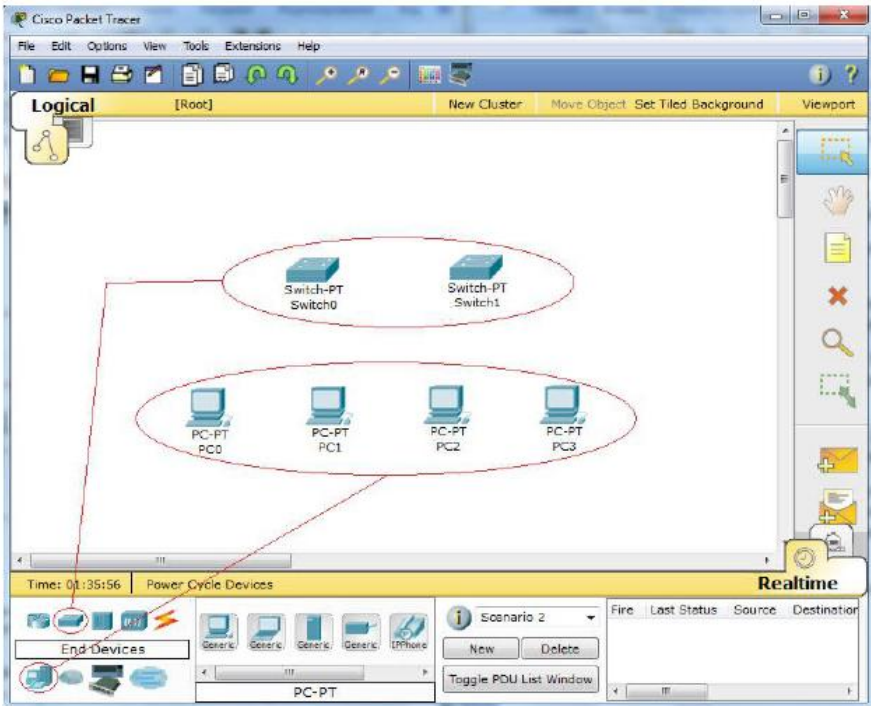


Рис. 1.2 – Додавання пристроїв у мережу

При додаванні кожного елемента користувач має можливість дати йому ім'я і встановити необхідні параметри. Для цього необхідно натиснути на потрібний елемент лівою кнопкою миші (ЛКМ) і в діалоговому вікні пристрою перейти до вкладки *Config*. Діалогове вікно властивостей кожного елемента має дві вкладки:

- *Physical* - містить графічний інтерфейс пристрою і дозволяє симулювати роботу з ним на фізичному рівні;
- *Config* - містить всі необхідні параметри для настройки пристрою і має зручний для цього інтерфейс.

Також залежно від пристрою, властивості можуть мати додаткову вкладку для управління роботою вибраного елемента: *Desktop* (якщо вибрано кінцевий пристрій) або *CLI* (якщо вибраний маршрутизатор) і т.д.

Для видалення непотрібних пристроїв з робочої області програми використовується кнопка *Delete* (Del).


Додані елементи зв'язуються за допомогою сполучних зв'язків. Для цього необхідно вибрати вкладку *Connections* з панелі *Network Component Box*. Там знаходяться всі можливі типи з'єднань між пристроями. Виберемо відповідний тип кабелю. Вказівник миші зміниться на курсор “*connection*” (має вигляд роз'єму). Потрібно натиснути на першому пристрої і вибрати відповідний інтерфейс, до якого потрібно виконати з'єднання, а потім натиснути на другий пристрій, виконавши ту ж операцію. Можна також з'єднати за допомогою *Automatically Choose Connection Type* (автоматично сполучає елементи в мережі). Між пристроями з'явиться кабельне з'єднання, а індикатори на кожному кінці покажуть статус з'єднання (для інтерфейсів які мають індикатор).







Packet Tracer підтримує широкий діапазон мережевих з'єднань (див. табл. 1.1). Кожен тип кабелю може бути сполучений лише з певними типами інтерфейсів.



Рис.1.3 – Підтримувані в Packet Tracer типи кабелів

Таблиця 1.1.

Тип кабелю	Описання
 Console	Консольне з'єднання може бути виконане між ПК і маршрутизаторами або комутаторами. Повинні бути виконані деякі вимоги для роботи консольного сеансу з ПК: швидкість з'єднання з обох боків повинна бути однаковою, повинно бути 7 біт даних (або 8 біт) для обох сторін, контроль парності повинен бути однаковий, повинно бути 1 або 2 стопових біти (але вони не обов'язково повинні бути однаковими), а потік даних може бути чим завгодно для обох сторін.

 <p>Copper Straight- through</p>	<p>Цей тип кабелю є стандартним середовищем передачі Ethernet для з'єднання пристроїв, які функціонують на різних рівнях моделі OSI. Він повинен бути сполучений з наступними типами портів: мідний 10 Мбіт/с (Ethernet), мідний 100 Мбіт/с (Fast Ethernet) і мідний 1000 Мбіт/с (Gigabit Ethernet).</p>
 <p>Copper Cross-over</p>	<p>Цей тип кабелю є середовищем передачі Ethernet для з'єднання пристроїв, які функціонують на однакових рівнях моделі OSI. Він може бути сполучений з наступними типами портів: мідний 10 Мбіт/с (Ethernet), мідний 100 Мбіт/с (Fast Ethernet) і мідний 1000 Мбіт/с (Gigabit Ethernet).</p>
 <p>Fiber</p>	<p>Оптоволоконне середовище використовується для з'єднання між оптичними портами (100 Мбіт/с або 1000 Мбіт/с).</p>
 <p>Phone</p>	<p>З'єднання через телефонну лінію може бути здійснено тільки між пристроями, що мають модемні порти. Стандартне представлення модемного з'єднання - це кінцевий пристрій (наприклад, ПК) що додзвонюється в мережеву хмару.</p>
 <p>Coaxial</p>	<p>Коаксіальне середовище використовується для з'єднання між коаксіальними портами, такі як кабельний модем? сполучений з хмарою Packet Tracer.</p>
 <p>Serial DCE and DTE</p>	<p>З'єднання через послідовні порти, часто використовуються для зв'язків WAN. Для налаштування таких з'єднань необхідно встановити синхронізацію на стороні DCE-пристрою. Синхронізація DTE виконується по вибору. Сторону DCE можна визначити по маленькій піктограмі "годинника" поряд з портом. При виборі типу з'єднання <i>Serial DCE</i> перший пристрій, до якого застосовується з'єднання, автоматично стає DCE-пристроєм, а другий - автоматично стане стороною DTE. Можливо і зворотне розташування сторін, якщо вибраний тип з'єднання <i>Serial DTE</i>.</p>

Після створення мережі її потрібно зберегти, вибравши пункт меню *File* → *Save* або піктограму *Save* на панелі *Main Tool Bar*. Файл збереженої топології має розширення *.pkt . Packet Tracer

дає можливість симулювати роботу з інтерфейсом командного рядка (ІКР) операційної системи Cisco IOS, встановленої на всіх комутаторах і маршрутизаторах компанії Cisco.

Підключившись до пристрою, ми можемо працювати з ним так, як за консоллю реального пристрою. Симулятор забезпечує підтримку практично всіх команд доступних на реальних пристроях.

Підключення до ІКР комутаторів або маршрутизаторів можна провести, натиснувши на необхідний пристрій і перейшовши у вікно властивостей до вкладки CLI. Для симуляції роботи командного рядка на кінцевому пристрої (комп'ютері) необхідно у властивостях вибрати вкладку *Desktop*, а потім натиснути на ярлик *Command Prompt*.

1.2 Порядок виконання роботи

1. Додати на робочу область програми 2 комутатора SWITCH-PT. За замовчуванням вони мають імена - Switch0 та Switch1.
2. Додати на робоче поле чотири комп'ютера з іменами за замовчуванням PC0, PC1, PC2, PC3.
3. З'єднати пристрої в мережу Ethernet, як показано на рис. 1.4.
4. Зберегти створену топологію, натиснувши кнопку *Save* (у меню *File* → *Save*).
5. Відкрити властивості пристрою PC0, натиснувши на його зображення. Перейти до вкладки *Desktop* і симулювати роботу (*Run*), натиснувши *Command Prompt*.
6. Отримати список команд, ввівши «?» і натиснувши *Enter*. Для конфігурації комп'ютера скористатися командою *ipconfig* з командного рядка, наприклад:

```
ipconfig 192.168.1.2 255.255.255.0
```

IP-адресу і маску мережі також можна вводити в зручному графічному інтерфейсі пристрою (див. рис. 1.5). Поле *DEFAULT GATEWAY* - адреса шлюзу не важлива, оскільки створювана мережа не потребує маршрутизації.

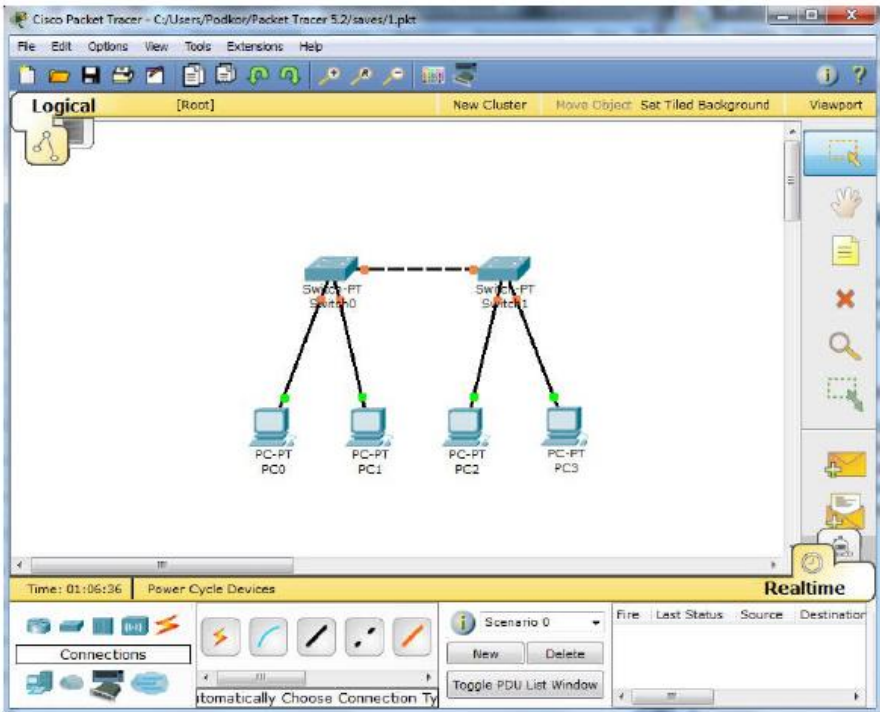


Рис. 1.4 – Приклад з'єднання пристроїв у мережу Ethernet

Таким же шляхом налаштувати кожен комп'ютер. IP-адреси та маски підмереж всіх комп'ютерів представлені в таблиці 1.2.

Таблиця 1.2.

Пристрій	IP-adress	Subnet Mask
PC0	192.168.1.2	255.255.255.0
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.4	255.255.255.0
PC3	192.168.1.5	255.255.255.0

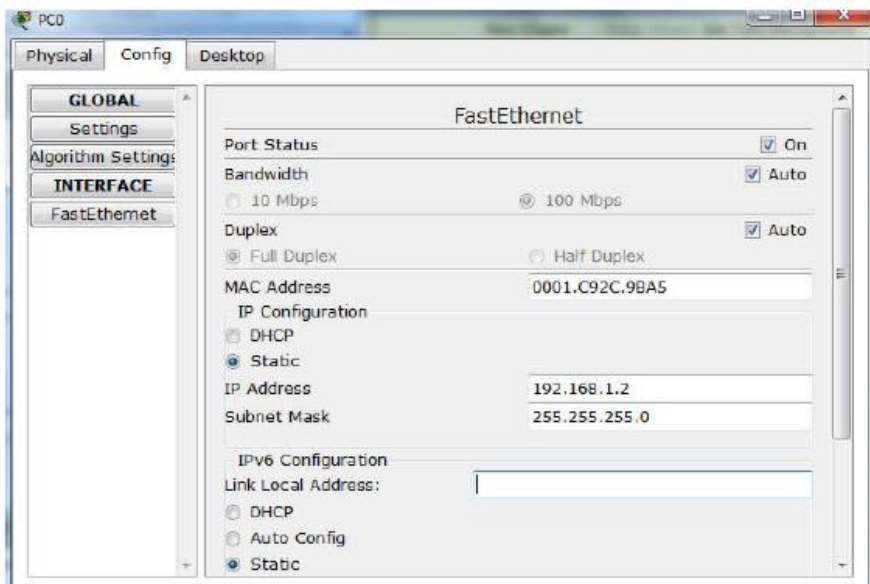


Рис. 1.5 – Вікно налаштування властивостей елемента мережі

7. На кожному комп'ютері подивитися призначену командою *ipconfig* адресу без параметрів.
8. Якщо все зроблено правильно, можливо пропінгувати будь-який комп'ютер з будь-якого іншого. Наприклад, зайти на комп'ютер PC3 і пропінгувати комп'ютер PC0. Ми повинні побачити звіт про пінг подібний до рис. 1.6.
9. Отримати у викладача варіант для індивідуальної роботи (див. Додаток А).
10. За отриманим варіантом скласти модель мережі (свічі розставляються самостійно).
11. З'ясувати, який вигляд матиме таблиця маршрутизації для довільних п'яти комп'ютерів.
12. Пропінгувати обрані п'ять комп'ютерів із п'ятьма іншими (також обираються довільно).
13. По пп.. 10-12 зробити скріншоти для звіту.

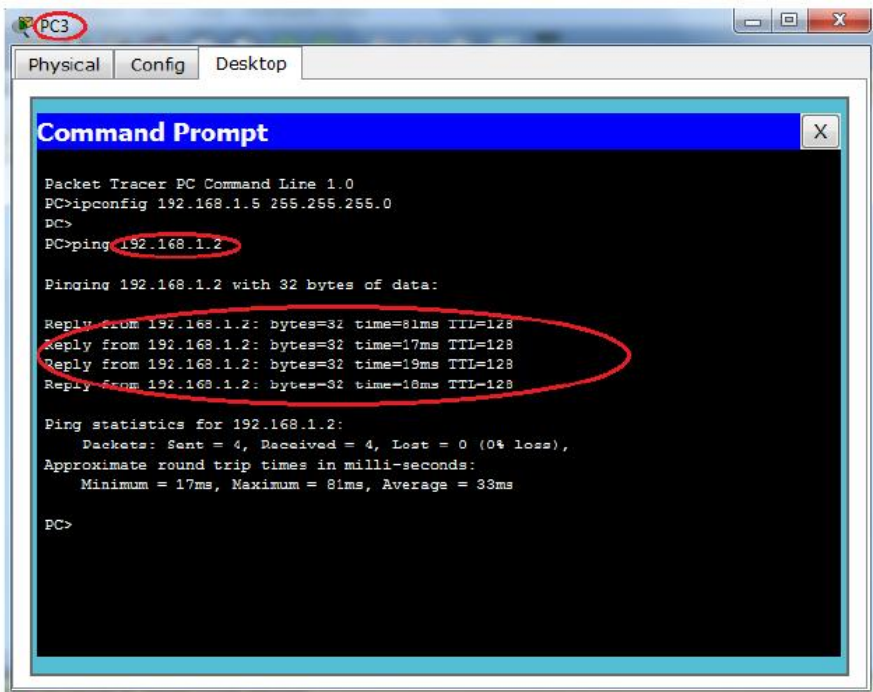


Рис. 1.6 – Результат пінгування двох комп'ютерів у мережі

1.3 Рекомендований зміст звіту

1. Назва роботи, мета, версія програмного забезпечення.
2. Варіант для виконання та логічна топологія мережі.
3. Модель мережі у Packet Tracer.
4. Таблиці маршрутизації для довільних п'яти комп'ютерів.
5. Результат виконання команди ping.
6. Висновки.

1.4 Контрольні запитання

1. Які переваги дає використання керованого мережевого устаткування?
2. Навіщо в комутаторах використовується таблиця комутації?
3. Для чого кожен запис в таблиці комутації має обмежений час життя і віддаляється, якщо пристрій з даною мас-адресою перестає відправляти пакети?
4. У класичному варіанті технології Ethernet (із загальним середовищем передачі, що розділяється) основним чинником, що обмежує максимальну кількість пристроїв в мережі, було зростання вірогідності виникнення колізії. При використанні комутаторів колізії відсутні. Чим тоді, на ваш погляд обмежується максимальна кількість пристроїв в такій мережі?
5. Як може змінитися доступність вузлів мережі після додавання віртуальних мереж?
6. Як може змінитися таблиця комутації після додавання віртуальних мереж?
7. Чим відрізняється виведення команд `show vlan`, `show vlan brief`, `show interface trunk`?
8. Які переваги дає використання віртуальних мереж (VLAN)?
9. Чому VLAN 10 в роботі можна назвати службовим?

Лабораторна робота №2

ПОБУДОВА СКЛАДЕНОЇ МЕРЕЖІ З БЕЗКЛАСОВОЮ АДРЕСАЦІЄЮ

Мета роботи: навчитися складати моделі складених мереж у Cisco Packet Tracer; вивчити основи безкласової адресації в IP-мережах.

2.1 Короткі теоретичні відомості

Для організації локальної комп'ютерної мережі Інтернет-провайдер надає в розпорядження користувача деяку, як правило, безперервну область адрес. Область виділених адрес або відповідає одному із стандартних класів IP-адресов, або задається певною адресною маскою. У будь-якому випадку всі адреси виділеної області мають однаковий префікс, тобто однакову цифрову послідовність в старших розрядах. Мережевий адміністратор може управляти наданим йому адресним простором, забезпечуючи гнучку логічну структурування новостворюваної мережі. Гнучка структурація мережі використовує безкласову адресацію, засновану на змінній довжині маски підмережі (англ. VLSM - Variable Length Subnet Mask). Маска вказується в настройках кожного мережевого пристрою спільно з IP-адресом і визначає межу між номером мережі і номером вузла. Двійковий запис маски має одиниці в розрядах, що визначають номер мережі, і нулі в розрядах, відповідних номеру вузла. Структурація дозволяє формувати призначені для користувача сегменти (підмережі) в цілях:

- розбиття власної мережі на декілька підмереж (subnetting) для локалізації трафіку і підвищення надійності без отримання від постачальника послуг додаткових номерів мереж;

- об'єднання адресних просторів що є у нього декількох мереж (supernetting) з метою спрощення внутрішньо-мережевого обміну, зменшення об'єму таблиць маршрутизації і підвищення продуктивності мереж.

Кількість адрес в підмережі не рівна кількості можливих вузлів. Нульова адреса IP резервується для ідентифікації підмережі, останній - як ширококомовна адреса. Тому в мережах максимальна кількість адрес вузлів в мережі на два менше, ніж загальна кількість адрес.

Розглянемо деякі випадки розділення адресного простору на окремі підмережі.

Приклад 1

Мережевому користувачеві виділений адресний простір 226.205.50.0/24. Потрібно організувати 4 підмережі, найбільша з яких налічує 40 вузлів. Слід врахувати можливе зростання числа вузлів на 20%.

Для організації 4 підмереж збільшимо довжину префікса на два розряди. При цьому розширений мережевий префікс (постійна частина адреси) міститиме $2^4 + 2 = 26$ розрядів. Змінна частина адрес в кожній підмережі забезпечується 6 бітами, що залишилися, що з урахуванням адреси мережі і ширококомовної адреси дозволяє створити підмережу з $2^6 - 2 = 62$ вузлами; такий адресний простір достатній для роботи найбільшої підмережі.

Для кожної підмережі нижня межа адресного простору зміщується на суму чисельних значень кодових символів, що входять в префікс цієї підмережі. При заданому адресному просторі префікси підмереж розміщуються в двох старших розрядах 4-го байта.

Встановимо для підмережі «0» префікс 00, для підмережі «1» - префікс 01, для підмережі «2» - префікс 10 і для підмережі «3» - префікс 11. Тоді адресний простір для вузлів підмережі «0» почнеться із значення 226.205.50.1, адресний простір для вузлів підмережі «1» - із значення 226.205.50.65, для підмережі «2» - із значення 226.205.50.129 і для підмережі «3» - із значення 226.205.50.193

Результати розрахунку адрес підмереж зведені в таблицю 2.1.

Таблиця 2.1

Название сети	IP-адрес сети	Сетевой префикс	Префикс	Диапазон адресов узлов подсети	Широковещательный адрес
Основная сеть	226.205.50.0/24	11100010.11001101.00110010	-	-	-
Подсеть 0	226.205.50.0/26	11100010.11001101.00110010.00	00	226.205.50.1 - 226.205.50.62	226.205.50.63
Подсеть 1	226.205.50.64/26	11100010.11001101.00110010.01	01	226.205.50.65 - 226.205.50.126	226.205.50.127
Подсеть 2	226.205.50.128/26	11100010.11001101.00110010.10	10	226.205.50.129 - 226.205.50.190	226.205.50.191
Подсеть 3	226.205.50.192/26	11100010.11001101.00110010.11	11	226.205.50.193 - 226.205.50.254	226.205.50.255

У даному прикладі було розглянуто формування підмереж рівного розміру.

На практиці часто потрібно організувати підмережі нерівного розміру. Наприклад, окрім основних підмереж, для зв'язку маршрутизаторів необхідні сполучні підмережі з невеликого числа адрес.

Приклад 2

Користувачеві виділений блок адрес 192.144.128.0/22. Потрібно організувати три підмережі по 50 вузлів, виділити адреси для двох пар маршрутизаторів і залишити деякий резерв.

Розділимо адресний простір на 4 однакових підмережі, виділивши 2 бита для нумерації цих підмереж: підмережа S0(00), підмережа S1(01), підмережа S2(10) і підмережа S3(11). Кожній підмережі відповідає 256 адрес. У просторі підмережі S3 додатково організовуємо дві підмережі S3-1 і S3-2, кожна на 4 адреси для підключення маршрутизаторів.

Результати формування адресного простору приведені в таблиці 2.2.

Таблиця 2.2

Адресный пул поставщика	Префикс поставщика (22 разряда)	Наименование подсети	Основной префикс пользователя (2 разряда)	Дополнительный префикс пользователя (6 разрядов)	Количество адресов подсети
2 ¹⁰ = 1024 адреса	11000000.10010000.100000	S0	00	-	256
	11000000.10010000.100000	S1	01	-	256
	11000000.10010000.100000	S2	10	-	256
	11000000.10010000.100000	S3, включая	11	-	256, в том числе
S3-1		11	000000	S3-1 – 4 адреса;	
	S3-2	11	000001	S3-2 – 4 адреса;	
					резерв – 248 адресов

Використання масок змінної довжини дозволило сформувати підмережі з адресними просторами, що перекриваються. Так, адресні простори підмереж S3-1 і S3-2 розмістилися усередині адресного простору підмережі S3.

Підключення мережі користувача до глобальної мережі здійснюється мережевим провайдером (Internet Service Provider), як правило, через окремий маршрутизатор (роутер), що позначається як RISP.

Можлива структура мережі користувача, відповідна умовам даного прикладу і проведеному розділенню адресного простору, показана на рис. 2.1.

Використання безкласової технології дозволяє гнучко формувати в мережі Інтернет окремі адресні простори (домени); при цьому інформація про внутрішні підмережі використовується тільки в межах цього адресного простору. Поза таким простором всім внутрішнім підмережам, що мають загальний префікс, відповідає один запис адреси призначення в таблицях маршрутизації.

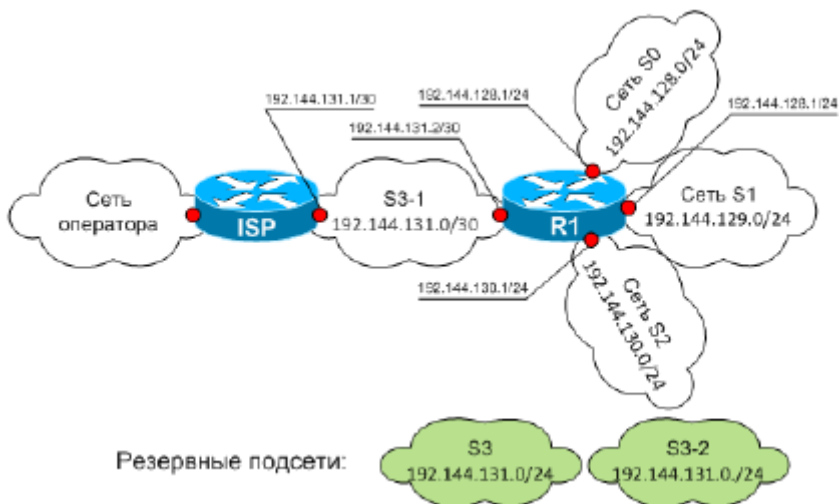


Рис. 2.1 - Сконфігурована мережа користувача

При передачі інформації від зовнішнього джерела до даного домена всі підмережі цього адресного простору фактично об'єднуються (агрегатуються) в одну загальну мережу, що істотно скорочує час обробки передаваних повідомлень, особливо в магістральних маршрутизаторах.

Агрегування підмереж може застосовуватися і при передачі інформації усередині домена. Використовуючи однакові символи в старших розрядах префікса, можна проводити об'єднання декількох підмереж для підвищення продуктивності маршрутизаторів усередині домена.

2.2 Порядок виконання роботи

1. Розділити адресний простір початкової мережі між декількома підмережами.
2. Привласнити адреси мережевим інтерфейсам комп'ютерів і маршрутизаторів.
3. Зібрати мережу із заданою топологією.
4. Провести настройку використовуваних мережеских пристроїв.
5. Перевірити роботу складеної мережі.
6. Виконати індивідуальне завдання.

2.4 Контрольні запитання

1. У чому полягає основна відмінність між комутатором і маршрутизатором?
2. Перерахуйте переваги технології VLSM перед класовою адресацією?
3. Що зберігається в agr-таблиці?
4. Для чого використовуються agr-таблиці?

Лабораторна робота №3

СТАТИЧНА МАРШРУТИЗАЦІЯ

Мета роботи: вивчити основи статичної маршрутизації в IP-мережах. Навчитися складати модель мережі зі статичною маршрутизацією у середовищі Cisco Packet Tracer.

3.1 Короткі теоретичні відомості

Статична маршрутизація - вид маршрутизації, при якому інформація про маршрути заноситься в таблиці маршрутизації кожного маршрутизатора уручну адміністратором мережі. Як можна зрозуміти - з принципу організації даного вигляду відразу ж витікає ряд недоліків. Перш за все, це дуже погана масштабованість, оскільки при додаванні нової підмережі у велику мережу, де вже є N підмереж, потрібно буде зробити $2(N+1)$ записів про маршрути, причому при достатньо великій сегментації мережі (кількість підмереж понад 4...6) таблиця маршрутизації на кожному з маршрутизаторів сильно відрізнятиметься від таблиць на інших пристроях. Іншим недоліком є неможливість відстежити проблеми, що виникають внаслідок помилок на устаткуванні каналного рівня, коли передача даних неможлива, а порт маршрутизатора як і раніше знаходиться в активному стані (стан up).

Необхідність уручну задавати маршрути також спричиняє за собою необхідність документування цих маршрутів. Всі ці проблеми вирішуються у протоколах динамічної маршрутизації за допомогою передачі службової ширококомовної інформації в мережу.

Проте статична маршрутизація продовжує успішно використовуватися при організації роботи комп'ютерних мереж невеликого розміру (1-2 маршрутизатора), через легкість

конфігурації та відсутності додаткового навантаження на мережу у вигляді широкомовного службового трафіку, характерного для динамічних протоколів маршрутизації. Також статична маршрутизація використовується на комп'ютерах усередині мережі. У такому разі зазвичай задається маршрут шлюзу за замовчуванням. При використанні статичних записів процесору маршрутизатора не потрібно проводити ніяких розрахунків, пов'язаних з визначенням маршрутів.

Статична маршрутизація в ОС Linux налаштовується за допомогою консольних утиліт `route` та `ip route`. Дані команди дозволяють переглядати таблицю маршрутизації хоста, а так само видаляти і додавати записи в неї.

Оскільки Cisco Packet Tracer емулює роботу реальних пристроїв Cisco, то і конфігурація статичної маршрутизації мережі в цій конфігурації реального мережевого устаткування Cisco. Нижче приведений приклад конфігурації мережевих інтерфейсів маршрутизатора і статичної маршрутизації для консолі Cisco IOS.

```
Router>enable (вход в привилегированный режим)
Router#configure terminal (вход в консоль настройки)
Router(config)#interface fa0/0 (выбор интерфейса маршрутизатора для настройки)
Router(config-if)#ip address 192.168.1.1 255.255.255.0 (конфигурация параметров IP
интерфейса)
Router(config-if)#no shutdown (запуск интерфейса)
Router(config-if)#interface fa1/0
Router(config-if)#ip address 172.16.10.20 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit (выход из режима конфигурирования интерфейсов маршрутизатора)
Router(config)#ip route 192.168.2.0 255.255.255.0 172.16.10.30 (конфигурация маршрута
в другую сеть, где 172.16.10.30 – IP маршрутизатора, соединенного с указанной сетью;
так же можно вместо IP адреса указать интерфейс маршрутизатора)
Router(config)#exit (выход из консоли настройки)
Router#write mem (сохранение конфигурации)
```

3.2 Порядок виконання роботи

1. Створити в середовищі Cisco Packet Tracer модель мережі, представленій на рис. 3.1.

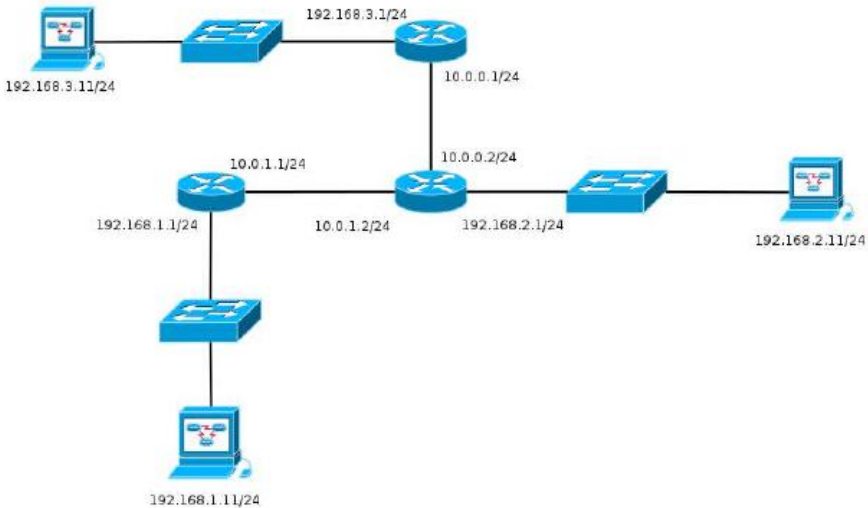


Рис. 3.1 – Модель мережі для налаштування статичної маршрутизації

2. Налаштувати для кожного з роутерів статичну маршрутизацію (зауваження: IP-адреси комп'ютерам назначати згідно схеми v.1.1.n, де v – номер варіанту, n – номер комп'ютера).
3. Вивести таблицю маршрутизації для кожного роутера (команда `show ip route`).
4. Перевірити правильність налаштування за допомогою команд `ping` і `tracert` в консолі кожного комп'ютера.
5. По пп. 1, 3, 4 зробити скріншоти для звіту.

3.3 Рекомендований зміст звіту

1. Назва роботи, мета, версія програмного забезпечення.
2. Модель мережі для налаштування статичної маршрутизації з призначеними всім елементам мережі відповідних IP-адрес.
3. Таблиці маршрутизації для кожного роутера.
4. Результати команд ping і tracert для всіх пар комп'ютерів.
5. Висновки.

3.4 Контрольні запитання

1. Який, на ваш погляд, головний недолік статичної маршрутизації?
2. Запропонуйте декілька ситуацій, в яких зручно використовувати маршрут «за умовчанням».
3. У яких випадках використовувати маршрут «за умовчанням» небажано?

Лабораторна робота №4

ДИНАМІЧНА МАРШРУТИЗАЦІЯ

Мета роботи: вивчити основи динамічної маршрутизації в IP-мережах. Навчитися складати модель мережі зі статичною маршрутизацією у середовищі Cisco Packet Tracer.

4.1 Короткі теоретичні відомості

Динамічна маршрутизація - вид маршрутизації, при якому таблиця маршрутизації заповнюється і оновлюється автоматично за допомогою одного або декількох протоколів маршрутизації (RIP, OSPF, EIGRP, BGP). Маршрут до мереж призначення будується на основі таких критеріїв як

- кількість ретрансляційних переходів;
- пропускна спроможність каналу зв'язку;
- затримки передачі даних.

Оптимальні шляхи обчислюються по різних алгоритмах за допомогою теорії графів.

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

Протоколи маршрутизації діляться на три типи:

1. Дистанційно векторні протоколи (RIP);
2. Протоколи з відстежуванням стану каналів (OSPF);
3. Змішані протоколи (EIGRP).

4.1.1. Протокол RIP2

RIP (Routing Information Protocol) - протокол дистанційно-векторної маршрутизації, що використовує для знаходження оптимального шляху алгоритм Беллмана-Форда. Цей протокол найбільш поширений в невеликих комп'ютерних мережах.

Алгоритм маршрутизації був вперше запропонований у 1969 р. для ARPANET. Друга версія протоколу - протокол RIP2 була розроблена в 1994 р. і є покращеною версією першого. У цьому протоколі була підвищена безпека за рахунок введення додаткової маршрутної інформації, і замість broadcast використовується multicast. У якості метрики маршрутизації протокол оперує так званими хопами (ретрансляційними стрибками). Максимальне число стрибків в RIP першої версії обмежене 15. У RIP2 обмеження розширене до 25 хопів.

Принцип роботи дистанційно-векторного протоколу полягає у наступному:

1. Кожен маршрутизатор, що використовує протокол RIP періодично ширококомовно розсилає своїм сусідам спеціальний пакет-вектор, що містить відстані (вимірюються в метриці) від даного маршрутизатора до всіх відомих йому мереж.

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

3. Маршрутизатор вибирає з декількох альтернативних маршрутів маршрут з найменшим значенням метрики, а маршрутизатор, що передав інформацію про такий маршрут позначається як наступний (next hop).

Алгоритм RIP допускає виникнення петель маршрутизації, які можуть бути викликані неузгодженістю синхронізації таблиць на роутерах, помилках в каналі або негативними вершинами графа при розрахунку оптимального шляху (наслідок алгоритму

Беллмана-Форда). У разі виникнення петлі маршрутизації метрика буде рівна 16 (нескінченно велика) і даний маршрут перестане розглядатися (метод *poison reverse*). У RIP існує спеціальний механізм боротьби з петлями маршрутизації, званий «метод розщеплювання горизонту» (*split horizon*), який можна описати як «не говори мені те, що я тобі сказав». Таким чином маршрутизатор не передаватиме своєму сусідові отриману від цього сусіда ж інформацію. Крім боротьби з петлями, даний метод зменшує об'єм передаваної по мережі службової маршрутної інформації.

Протокол RIP непридатний для роботи у великих мережах, оскільки засмічує мережу інтенсивним трафіком, а вузли мережі оперують тільки векторами-відстанями, не маючи точної інформації про стан каналів і топології мережі. Сьогодні навіть у невеликих мережах протокол витісняється протоколами EIGRP (протокол Cisco) і OSPF, які перевершують його по можливостям.

4.1.2. Протокол OSPF

OSPF (Open Shortest Path First) - протокол динамічної маршрутизації, що заснований на технології відстежування стану каналу (*link-state*). Був розроблений IETF в 1988 р. та ґрунтується на алгоритмі Дейкстри для пошуку найкоротшого шляху. В якості метрики OSPF використовує коефіцієнт якості обслуговування (так звана вартість каналу або *cost*). Відстежування стану каналу вимагає відправки оголошень про стан каналу (*link-state advertisement, LSA*) на активні інтерфейси всіх доступних маршрутизаторів зони. У цих оголошеннях міститься опис всіх каналів маршрутизатора, відносини сусідства і вартість кожного каналу. Для обчислення вартості каналу використовується відношення $10^8 / \text{ширина_канала}$. Для відправки оголошень OSPF використовує *multicast* повідомлення (на відміну від RIP). LSA повідомлення відправляються тільки якщо відбулися які-небудь зміни в мережі, але раз в 30 хвилин LSA повідомлення відправляються в примусовому порядку.

Протокол реалізує ділення автономної системи на зони (*areas*). Маршрутизатором, що належить одній зоні не відома детальна топологія інших зон. Використання зон дозволяє

понижити навантаження на мережу і процесори маршрутизаторів (зменшення об'єму розрахунків по SPF) зменшити розмір таблиць маршрутизації.

Розрізняють наступні типи зон:

- магістральна (backbone) - формує ядро мережі OSPF;
- стандартна (standart) - зона, яка створюється за замовчуванням і яка приймає оновлення каналів, сумарні та зовнішні маршрути;
- тупикова (stub) - не приймає інформацію про зовнішні маршрути для автономної системи, але приймає маршрути інших зон; для передачі інформації за межі автономної зони використовує маршрут за замовчуванням;
- повністю тупикова (totlly stubby) - не приймає інформацію як про зовнішніх маршрутах автономної системи, так і маршрути інших зон; використовує шлюз за замовчуванням.

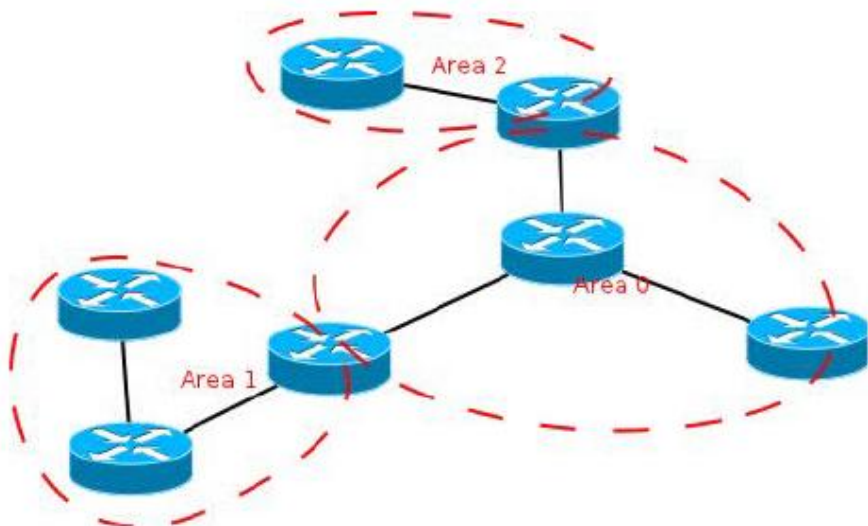


Рис. 4.1 – Розділення мережі на зони маршрутизації

Маршрутизатори усередині зон також діляться на типи:

- внутрішній (internal) - маршрутизатор, всі інтерфейси якого належать одній зоні.

- прикордонний (area border, ABR) - сполучає одну або більше зон з магістральною.

- магістральний (backbone) - хоча б один інтерфейс маршрутизатора даного типу належить до магістральної зони;

- прикордонний маршрутизатор автономної системи (AS boundary, ASBR) - обмінюється інформацією з маршрутизаторами в інших автономних системах. Може бути як внутрішнім, прикордонним, так і магістральним.

Поетапний опис роботи протоколу:

1. Всі маршрутизатори обмінюються спеціальними hello-пакетами через всі інтерфейси, на яких активований протокол OSPF. Таким чином визначаються маршрутизатори-сусіди, що розділяють загальний канал передачі даних. Надалі hello-пакети посилаються з інтервалом раз в 30 секунд.

2. Маршрутизатори намагаються перейти в стан сусідства зі своїми сусідами. Перехід в даний стан визначається типом маршрутизаторів і типом мережі, по якій відбувається обмін hello-пакетами, за зонною ознакою. Пара маршрутизаторів в стані сусідства синхронізує між собою базу даних стану каналів.

3. Кожен маршрутизатор посилає оголошення про стан каналу своїм сусідам, а що кожен отримав таке оголошення записує інформацію в базу даних стану каналів і розсилає копію оголошення іншим своїм сусідам.

4. При розсилці оголошень по зоні, всі маршрутизатори будують ідентичну базу даних стану каналів.

5. Кожен маршрутизатор використовує алгоритм SPF для обчислення графа (дерева найкоротшого шляху) без петель, який описуватиме найкоротший шлях до кожного відомого призначення з собою в якості кореня.

6. Кожен маршрутизатор буде власну маршрутизацію ґрунтуючись на побудованому дереві найкоротшого шляху.

4.2 Порядок виконання роботи

1. Створити в середовищі Cisco Packet Tracer модель мережі, представленій на рис. 4.2.

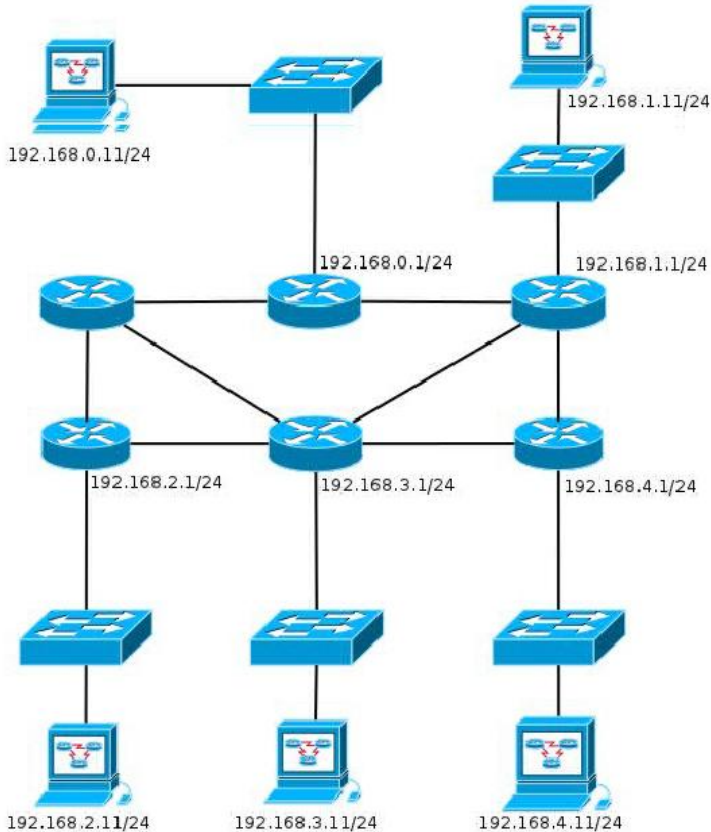


Рис. 4.2 – Модель мережі для налаштування динамічної маршрутизації

2. Налаштувати для кожного з роутерів динамічну маршрутизацію згідно протоколу RIP2 (зауваження: при цьому потрібно брати до уваги періоди розсилання таблиць маршрутизації).

3. Перевірити правильність налаштування за допомогою команд `ping` і `tracert` в консолі для кожного комп'ютера.

4. В цій же моделі мережі з уже налаштованим протоколом RIP2 налаштувати маршрутизацію за протоколом OSPF.
5. Вивести таблицю маршрутизації на кожному роутері. Пояснити заміщення записів протоколу RIP2.
6. Вивести таблиці сусідів для кожного маршрутизатора (`show ip ospf neighbor`).
7. Порівняти маршрути, отримані за допомогою протоколу RIP2 з маршрутами, отриманими за допомогою протоколу OSPF. Прийміть до уваги адміністративну відстань та метрику.
8. По пп. 1, 3, 5, 6 зробити скріншоти для звіту. На основі п. 7 зробити відповідні висновки.

4.3 Рекомендований зміст звіту

1. Назва роботи, мета, версія програмного забезпечення.
2. Модель мережі для налаштування статичної маршрутизації з призначеними всім елементам мережі відповідних IP-адрес.
3. Таблиці маршрутизації для кожного роутера при використанні протоколу RIP2.
4. Результати команд `ping` і `tracert` для всіх пар комп'ютерів (при використанні протоколу RIP2).
5. Таблиці маршрутизації для кожного роутера при використанні протоколу OSPF.
6. Результати команд `ping` і `tracert` для всіх пар комп'ютерів (при використанні протоколу OSPF).
7. Висновки. Порівняння маршрутів при використанні різних протоколів.

4.4 Контрольні запитання

1. Поясніть, чому видалення однієї будь-якої лінії зв'язку в схемі на рис. 4.2 не приводить до втрати повнозв'язності мережі?
2. Вкажіть, які недоліки має динамічна маршрутизація в порівнянні із статичною.

Література

1. Б. Хилл – Полный справочник по Cisco – М. –СПб. –К.: Изд. дом «Вильямс», 2004. – 722 с.
2. А. Леинванд, Б. Писки – Конфигурирование маршрутизаторов Cisco / 2-е изд. – М.: Изд. дом «Вильямс», 2001. – 368 с.

Интернет посилання:

- 1 Детальна інформація по маршрутизації в Cisco з прикладами команд http://xgu.ru/wiki/Cisco_Routing
2. Класифікація алгоритмів маршрутизації:
https://secure.wikimedia.org/wikipedia/ru/wiki/Алгоритмы_маршрутизации
3. Детальна інформація по протоколу OSPF: <http://xgu.ru/wiki/OSPF> , <http://book.itep.ru/4/44/osp44112.htm>
4. Детальна інформація по протоколу RIP/RIP2:
<http://xgu.ru/wiki/RIP> , <http://book.itep.ru/4/44/rip44111.htm>

