Міністерство освіти і науки
Національний технічний університет України
«Київський політехнічний інститут»

В.В. Шликов, О.Г. Кисельова, І.Ю. Свергун

Методичні вказівки до виконання лабораторних робіт з кредитного модуля «Телемедицина та комп'ютерні мережі» з дисципліни «Біокібернетика та робототехніка» за спеціальністю 163 «Біомедична інженерія»

Затверджено Вченою Радою ФБМІ

Київ
НТУУ «КПІ»
2016

Гриф надано Вченою радою
факультету біомедичної інженерії
(Протокол № 8 від 24квітня 2016 р.)

Затверджено на засіданні
кафедри біомедичної інженерії
(протокол №7 від 24 лютого 2016 р.)

Методичні вказівки до виконання лабораторних робіт з кредитного модуля «Телемедицина та комп'ютерні мережі»з дисципліни «Біокібернетика та робототехніка» за спеціальністю 163 «Біомедична інженерія».

Рецензент:

О.Д. Фіногенов, к.техн., доц.
Національний технічний університет України
«Київський політехнічний інститут»

Відповідальний редактор:
В.І. Зубчук, к.техн.н.,
Національний технічний університет України
«Київський політехнічний інститут»

Шликов В.В., Кисельова О.Г., Свергун І.Ю.
Методичні вказівки до виконання лабораторних робіт з кредитного модуля «Телемедицина та комп'ютерні мережі» з дисципліни «Біокібернетика та робототехніка» за спеціальністю 163 «Біомедична інженерія»
/ Укл. В.В. Шликов, О.Г. Кисельова, І.Ю. Свергун. – К.: НТУУ «КПІ», 2016. – 57 с.

ЗМІСТ

ЛАБОРАТОРНА РОБОТА №1.

Тема: Статична маршрутизація

Мета роботи: ознайомитись з основними можливостями середовища Cisco Packet Tracer; набути навичок налаштування маршрутизації пакетів за допомогою статичних маршрутів.

Теоретичні відомості

Маршрутизація (англ. *Routing*) — процес визначення маршруту прямування інформації між мережами. Маршрутизатор (або роутер від англ. слова *router*) приймає рішення, що базується на IP-адресі отримувача пакету. Для того, щоб переслати пакет далі, всі пристрої на шляху слідування використовують IP-адресу отримувача. Для прийняття правильного рішення маршрутизатор має знати напрямки і маршрути до віддалених мереж.

При використанні статичної маршрутизації маршрути задаються вручну адміністратором.

Оскільки статичні маршрути конфігуруються вручну, будь-які зміни мережної топології вимагають участі адміністратора для додавання і видалення статичних маршрутів відповідно до змін. У великих мережах підтримка таблиць маршрутизації вручну може вимагати величезних витрат часу адміністратора. У невеликих мережах це робити легше. Статична маршрутизація не має можливості масштабування, яку має динамічна маршрутизація через додаткові вимоги до налаштування і втручання адміністратора. Але і у великих мережах часто конфігуруються статичні маршрути для спеціальних цілей у комбінації з протоколами динамічної маршрутизації, оскільки статична маршрутизація є стабільнішою і вимагає мінімум апаратних ресурсів маршрутизатора для обслуговування таблиці.

Статична маршрутизація має наступні **особливості:**

1. Забезпечує підтримку маршрутизації для невеликих мереж, які не передбачено суттєво розширювати;
2. Забезпечує маршрутизацію для кінцевої (тупикової) мережі;
3. Задає єдиний маршрут за замовчуванням до будь-якої мережі, якщо мережа не містить більш специфічного шляху.

Переваги статичної маршрутизації:

1. Мінімальне використання процесора;
2. Легша для розуміння адміністратора;
3. Легша для конфігурування в малих мережах;
4. Передбачуваність в будь-який момент часу.

Недоліки статичної маршрутизації:

1. Конфігурування та обслуговування потребує багато часу;
2. Під час конфігурування можливі помилки (особливо у великих мережах); для підтримки заміни маршрутної інформації потрібне втручання адміністратора;
3. Зі зростанням мережі погано масштабується; для належного виконання потребує повного знання усієї мережі.

Приклад налаштування статичної маршрутизації

На рис. 1.1 зображено топологію з трьома підмережами. Для налаштування статичної маршрутизації в такому випадку необхідно виконати наступні дії:

1. Налаштувати на кожному кінцевому пристрої (комп’ютери, ноутбуки, сервери) IP-адресу, маску підмережі, IP-адресу шлюзу та IP-адресу DNS-сервера;
2. Налаштувати аналогічно до кінцевих пристроїв кожен з інтерфейсів роутера;
3. Налаштувати статичні маршрути для кожної з під мереж на роутері.

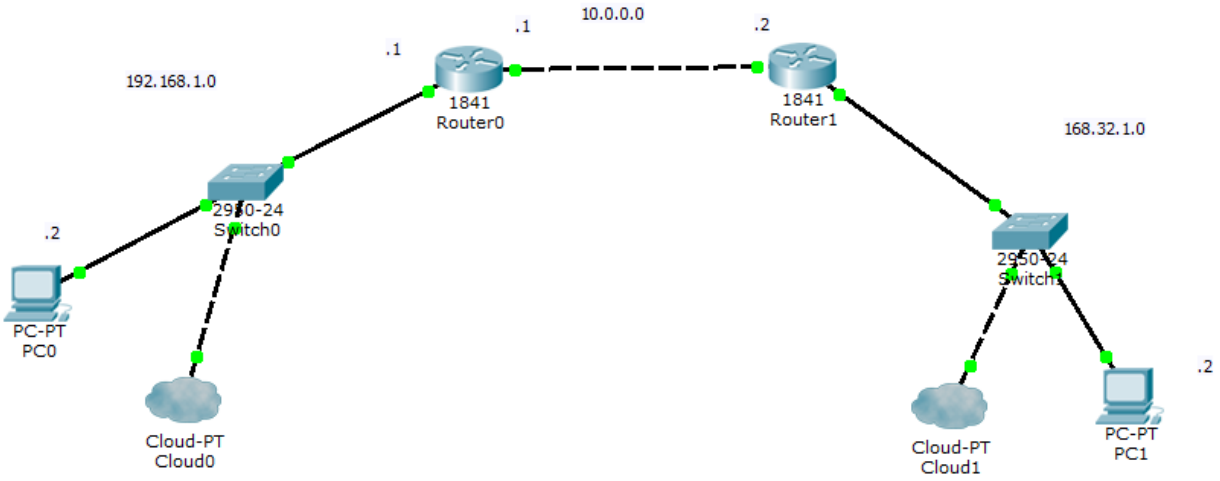

Рис. 1.1 — Топологія з трьома під мережами

Розглянемо приклад налаштування кінцевого пристрою на прикладі комп’ютера PC0 (рис. 1.2).

На рис. 1.2 зображена вкладка Desktop меню налаштування PC0. Для того щоб встановити для нього потрібні налаштування необхідно перейти до меню IP Configuration. В цьому випадку відкриється вікно, зображене на рис. 1.3.

Тобто, для кожного з пристроїв потрібно встановити налаштування аналогічні до зображених на рис. 1.3.

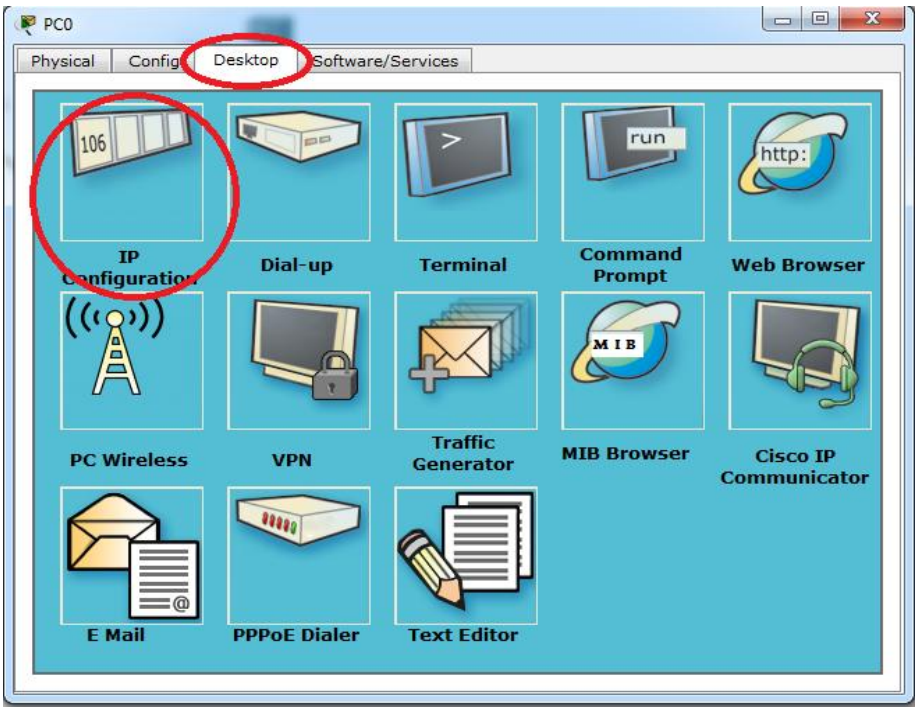

Рис. 1.2 — Розташування меню налаштування комп'ютера

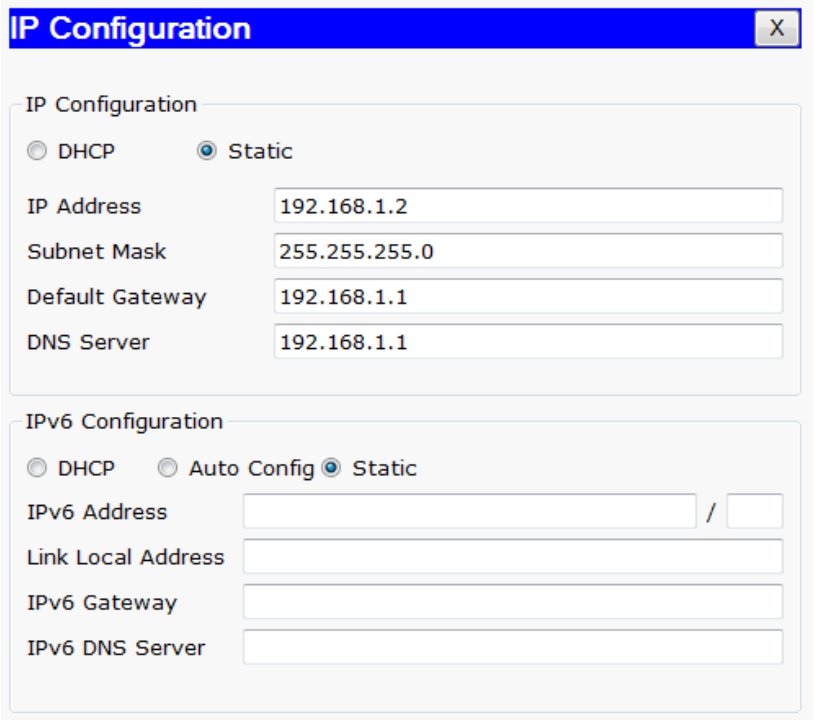

Рис. 1.3 – Налаштування комп’ютера PC0

Налаштування роутера відбувається наступним чином:

```
Router>enable
Router#conf igure terminal
Router(config)#interface fa0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#int fa0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 10.0.0.1 255.255.255.252
Router(config-if)#exit
Router(config)#ip route 168.32.1.0 255.255.255.0 10.0.0.2
```

Розглянемо команди, які застосовувались для налаштування роутера:

- *enable* – використовується для доступу до режиму конфігурування роутера (аналогічно до команди sudo для отримання прав адміністратора в ОС Linux)
- *configure terminal* – перехід в режим конфігурування роутера;
- *interface fa0/0* – перехід в режим конфігурування інтерфейсу fa0/0;
- *no shutdown* – увімкнути інтерфейс (подати на нього живлення);
- *ip address <IP-адреса> <маска підмережі>* – становити інтерфейсу роутера IP-адресу та маску під мережі;
- *exit* – повернутись на один рівень конфігурування назад;
- *ip route <IP-адреса мережі, до якої потрібно отримати доступ> <маска мережі, до якої потрібно отримати доступ> <IP-адреса інтерфейсу роутера, через який отримується доступ в потрібну мережу>* - команда для налаштування статичного маршруту.

Налаштування Router1 відбувається аналогічно.

Опис лабораторної роботи

Комп’ютерна мережа має структуру, що представлена на рис. 1.4:

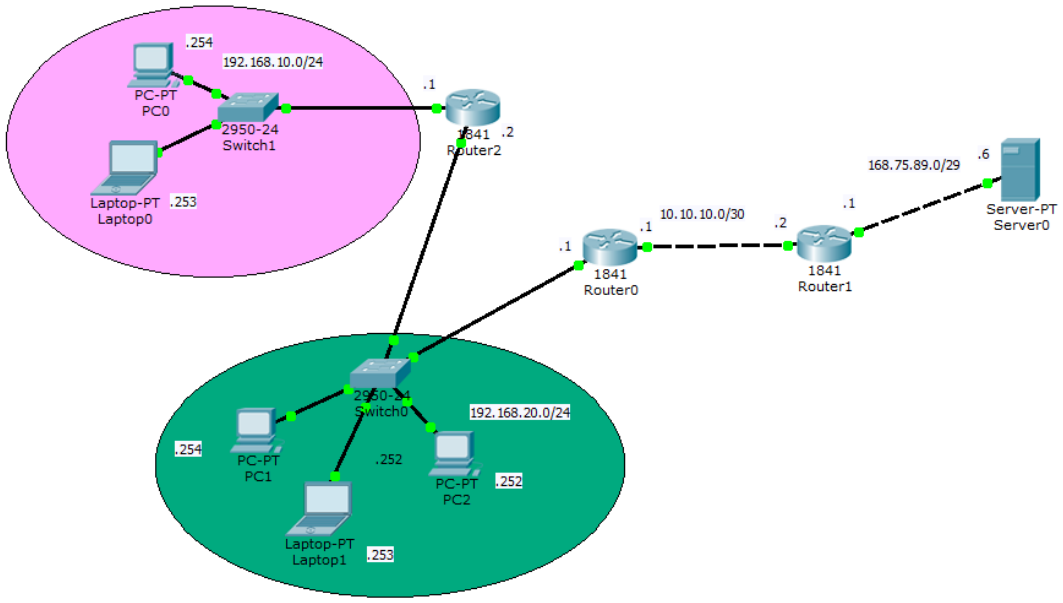

Рис. 1.4 — Топологія завдання до лабораторної роботи №1

Є чотири мережі: 192.168.10.0/24, 192.168.20.0/24, 10.10.10.0/30 та 168.75.89.0/29. Для забезпечення зв'язку між мережами потрібно налаштувати статичні маршрути на кожному з роутерів, що не є безпосередньо приєднаними до мереж. Необхідно налаштувати статичну маршрутизацію між всіма мережами.

Хід роботи:

1. Для всіх роутерів в топології необхідно встановити IP-адреси та маски підмереж для кожного з інтерфейсів.

2. Для кожного з кінцевих пристроїв (ноутбуків, комп'ютерів та сервера) необхідно встановити IP-адресу для даного пристрою, маску підмережі, IP-адресу шлюзу (gateway) та IP-адресу DNS-сервера. Потрібні IP-адреси вказані біля кожного з пристроїв.
3. Налаштувати статичні маршрути на кожному з роутерів, що не безпосередньо приєднані до мереж. Для прокладання статичних маршрутів необхідно використовувати наступну команду:

   ip route [IP-адреса мережі до якої прокладаємо маршрут] [маска підмережі] [IP-адреса інтерфейсу через який отримуємо доступ]
4. Перевірити функціонування маршрутизації за допомогою команди ping.

Контрольні питання

1. Що таке маршрутизація?
2. Дайте визначення поняттю статичної маршрутизації.
3. Вкажіть особливості статичної маршрутизації.
4. Наведіть переваги статичної маршрутизації.
5. Які недоліки статичної маршрутизації?
6. Вкажіть алгоритм налаштування статичної маршрутизації в мережі.
7. Які команди необхідні для налаштування статичної маршрутизації?
8. Назвіть призначення IP-адреси та маски підмережі.
9. Що таке DNS-сервер?

ЛАБОРАТОРНА РОБОТА №2

Тема: Протокол DHCP

Мета роботи: ознайомитись з протоколом DHCP, набути практичних навичок з налаштування DHCP-серверів.

Теоретичні відомості

Протокол динамічної конфігурації вузла (*Dynamic Host Configuration Protocol, DHCP*) – це протокол прикладного рівня, що дозволяє комп'ютерам автоматично одержувати IP-адресу й інші параметри, необхідні для роботи в мережі TCP/IP. Даний протокол працює за моделлю “клієнт-сервер”, тобто на запити клієнтів відповідає спеціальний DHCP-сервер. В ролі такого сервера може виступати як сервер (будь-який комп'ютер з налаштованим відповідним програмним забезпеченням), так і маршрутизатор (роутер, *router*). Діапазон адрес, які розподіляються DHCP-сервером, як правило, задаються адміністратором мережі. Цей діапазон прийнято називати пулом (*pool*) адрес протоколу DHCP. Протокол DHCP використовується в більшості великих мереж TCP/IP. Крім IP-адреси, DHCP також може повідомляти клієнтові додаткові параметри, необхідні для нормальної роботи в мережі. Ці параметри називаються опціями DHCP, з них, найбільш часто використовуванними є: IP-адреса маршрутизатора за замовчуванням (*default gateway*), адреса сервера служби DNS, домен DNS-сервера.

Виділяють наступні **види розподілення IP-адрес** протоколом DHCP:

1. Ручний розподіл — адміністратор мережі вручну визначає IP-адресу для кожної MAC-адреси;
2. Автоматичний розподіл — клієнту видається будь-яка доступна IP-адреса

для постійного користування;

3. Динамічний розподіл — аналогічно попередньому випадку, клієнту видається будь-яка вільна IP-адреса, але не для постійного користування, а на визначений термін, після закінчення якого IP-адреса знову вважається вільною.

Зрозуміло, що останній тип розподілу є найбільш гнучким і потребує мінімум уваги адміністратора мережі. Саме тому, він і є найбільш розповсюдженим.

Також, варто зазначити, що при динамічному розподілі, якщо кінцевий пристрій отримав IP-адресу та активно її використовує, то при закінченні терміну її «оренди» йому буде продовжено термін користування нею. Але, якщо комп'ютер припинить надсилати пакети помічені цією адресою (його вимкнули чи відключили від мережі), то після того як збіжить на володіння IP-адресою, то вона повернеться назад у пул доступних адрес, і може бути надана вже іншому пристрою.

Протокол DHCP є клієнт-серверним, тобто в його роботі беруть участь клієнт DHCP та сервер DHCP. Передача даних базується на протоколі UDP. Сервер приймає запити на 67 порт, а клієнти приймають повідомлення на 68 порт.

Для виконання своїх функцій протокол DHCP використовує такі **повідомлення:**

1. Знаходження DHCP (DHCPDISCOVER) — бродкаст запит (власна IP-адреса = 0.0.0.0, IP-адреса призначення = 255.255.255.255), клієнта для пошуку доступного DHCP-сервера;
2. Пропозиція DHCP (DHCPOFFER) — після того, як сервер отримав запит, він відправляє пакет із запропонованою конфігурацією;
3. Запит DHCP (DHCPREQUEST) — вибравши одну із конфігурацій, яка

була запропонована DHCP серверами, клієнт відправляє запит до сервера, який містить вибрану клієнтом адресу;

4. Підтвердження DHCP (DHCPACK) — сервер підтверджує запит клієнта, після чого клієнт може налаштувати свій інтерфейс відповідно до вибраної конфігурацій.

Також, протокол DHCP має декілька **інших повідомлень** для відмови, відміни, звільнення від запропонованої конфігурації та запит для отримання додаткових параметрів:

1. Відмова DHCP (DHCPDECLINE) — якщо при триманні пакету типу DHCPPACK клієнт знаходить в мережі пристрій з аналогічною адресою, то він відсилає повідомлення даного типу, після чого процедура запиту адреси повторюється.
2. Відміна DHCP (DHCPNACK) — сервер не може надати клієнту IP-адресу, яку той попросив у запиті.
3. Звільнення DHCP (DHCPRELEASE) — клієнт припиняє оренду IP-адреси.
4. Інформація DHCP (DHCPINFORM) — тип повідомлення, призначений для тримання додаткових параметрів мережі (адреси сервера DNS, шлюзу за умовчанням та ін.

Протокол DHCP широко використовується в сучасних комп'ютерних мережах через свої переваги, але є і певні недоліки.

Перевагами використання протоколу DHCP є:

1. Надійність налаштування — як правило, автоматичне налаштування більш надійне, оскільки відсутній людський фактор;
2. Знижені затрати часу на конфігурування мережі.

Недоліки протоколу DHCP:

1. Низький рівень безпеки, який обумовлений використанням протоколів

UDP та IP;

2. Мережі не захищені від появи в мережі несанкційованих DHCP-серверів;
3. Відносно часті відмови протоколу.

Приклад протоколу DHCP:

IP-адреси, які буде роздавати DHCP-сервер, зберігаються в DHCP пулі. Приклад налаштування такого пулу адрес показаний на рис. 2.1. Потрібно вказати назву пулу (Pool Name), порт за умовчанням (Default Gateway), IP-адресу DNS-сервера, початкову адресу пулу, маску підмережі та максимальну кількість адрес, які можна роздати.

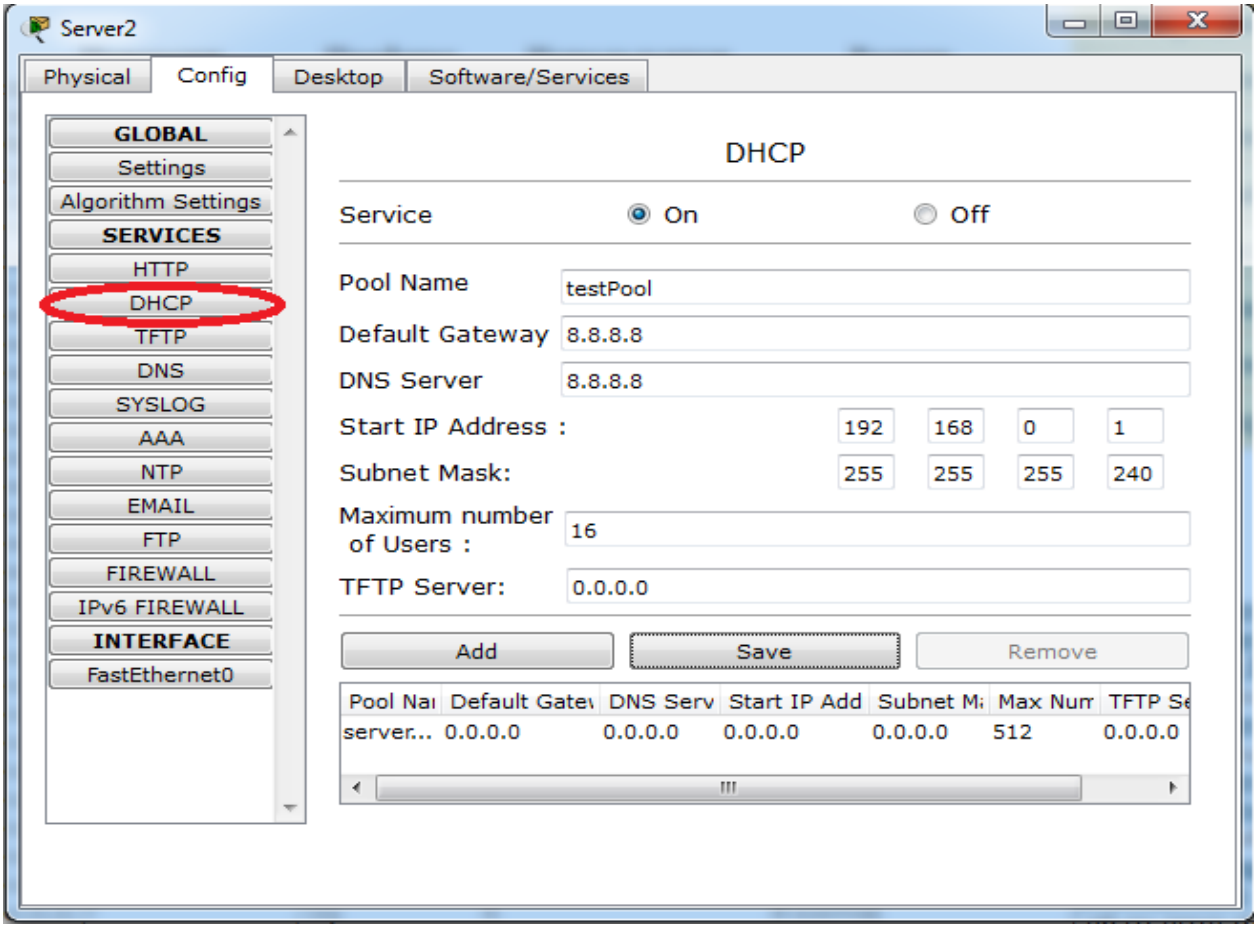

Рис. 2.1 – Приклад налаштування DHCP пулу

Роутер також може виконувати роль DHCP-сервера. Налаштування протоколу DHCP на роутері виконується за допомогою наступних **команд:**

- *int [ім'я інтерфейсу роутера]* – перехід у режим конфігурування інтерфейсу;
- *ip add dhcp* – налаштування інтерфейсу за DHCP;
- *ip dhcp pool [ім'я пулу]* – створення пулу з вказаним ім'ям;
- *network [маска підмережі] [IP-адреса підмережі]* – використати IP-адреси мережі з вказаними параметрами для розповсюдження;
- *default-router [IP-адреса інтерфейсу роутера в підмережі]* – встановити порт за умовчанням для даного пулу;
- *dns-server [IP-адреса DNS-сервера]* – встановити адресу DNS-сервера для даного пулу.

Приклад:

```
Router(config)#ip dhcp pool routerPool
Router(dhcp-config)#network 192.168.0.0 255.255.255.240
Router(dhcp-config)#default-router 8.8.8.8
Router(dhcp-config)#dns-server 8.8.8.8
```

Часто необхідно видалити з пулу адреси які вже закріплені за інтерфейсами роутера чи кінцевого пристрою. Для цього використовується наступна **команда:**

- *ip dhcp excluded-address [IP-адреса, яку потрібно виключити з пулу]* – виключення IP-адреси з пулу.

Приклад:

```
Router(config)#ip dhcp excluded-address 8.8.8.1
```

Опис лабораторної роботи

Комп’ютерна мережа має структуру, що представлено на рисунку 2.2.

Є дві мережі: 192.168.10.0/24 та 192.168.15.0/24. Завдання лабораторної роботи полягає у тому, що кінцеві пристрої в мережі 192.168.10.0 повинні отримати налаштування за допомогою протоколу DHCP, який налаштовано та активовано на Server0. Комп’ютери в мережі 192.168.15.0 отримують налаштування від Roter0.

Зверніть увагу, що інтерфейс маршрутизатора, який знаходиться у мережі 192.168.10.0 також отримує налаштування від сервера за допомогою протоколу DHCP.

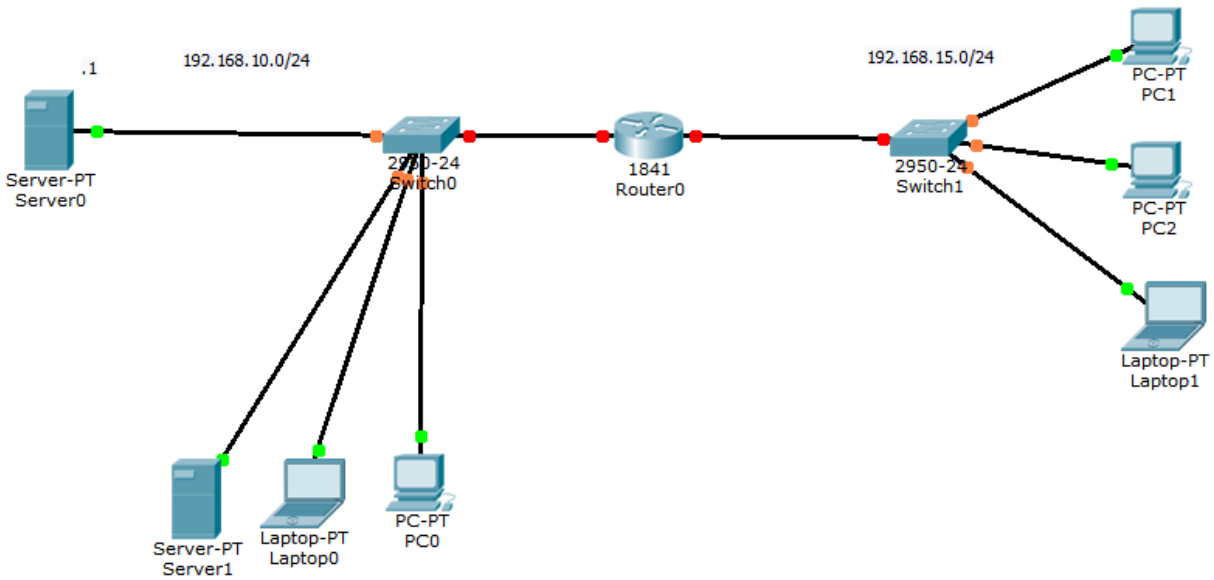

Рис. 2.2 – Структура комп’ютерної мережі

Хід роботи:

1. Активувати на сервері протокол DHCP та налаштувати пул так як вказано у завданні.
2. Налаштувати роутер.

3. Інтерфейс роутера, який підключено до підмережі з DHCP-сервером має отримувати IP-адресу за допомогою DHCP.
4. Для іншого інтерфейсу налаштувати IP-адресу вручну, таку як вказано у завданні.
5. Створити DHCP пул на роутері (необхідні параметри вказані у завданні).
6. Виключити з пулу адресу зайняту інтерфейсом роутера.
7. Всі кінцеві станції мають отримувати налаштування за допомогою DHCP.

Контрольні питання

2. Навіщо призначений протокол DHCP?
3. Вкажіть особливості протоколу DHCP.
4. Що таке DHCP пул?
5. Які параметри вказуються при налаштуванні протоколу DHCP?
6. Які команди використовуються для налаштування протоколу DHCP на роутері?
7. Яка команда використовується для виключення IP-адреси з DHCP пулу?
8. Вкажіть переваги застосування протоколу DHCP.
9. Наведіть недоліки застосування протоколу DHCP.
10. Чи застосовується протокол DHCP в сучасних комп’ютерних мережах?

ЛАБОРАТОРНА РОБОТА №3

Тема: Налаштування технології NAT

Мета роботи: ознайомитись з технологією трансляції мережевих адрес NAT та отримати практичні навички з її налаштування за допомогою програмного середовища Cisco Packet Tracer.

Теоретичні відомості

NAT (англ. *Network Address Translation* - перетворення адрес в мережі) - це механізм, який використовується в мережах TCP/IP для перетворення IP-адрес пакетів, які проходять через дану мережу.

Існує **три режими** роботи технології NAT:

1. Статичний NAT — одна IP-адреса замінюється іншою IP-адресою (один до одного);
2. Динамічний NAT — заміна незареєстрованої адреси на одну із адрес групи зарезервованих (багато до багатьох);
3. Перевантажений NAT — вид динамічного NAT, коли декілька незареєстрованих адрес використовують одну й ту ж IP-адресу, користуючись різними портами (багато до одного).

NAT призначений для виконання **наступних функцій:**

1. Економія IP-адрес — адреси всередині мережі можна замінити на одну зовнішню публічну адресу;
2. Обмеження надходження пакетів всередину мережі;
3. Фільтрування вихідних пакетів;
4. Забезпечення можливості обмежити доступ до певних серверів всередині мережі.

Але дана технологія також має і певні **недоліки**, такі як проблеми з ідентифікацією користувачів, та несумісність із старими протоколами.

Налаштування технології NAT

Для налаштування NAT на роутері використовуються наступні **команди**:

- *ip nat inside source static [IP-адреса інтерфейсу через який отримуємо доступ] [IP-адрес в мережі до якого транслюється мережевих адрес]* – активація NAT в статичному режимі;
- *ip nat inside source list [номер списку] [IP-адреси списку] overload* – активація NAT в режимі перевантаження;
- *ip nat inside* – вказати інтерфейс направлений «в середину» мережі, IP-адреси якої потрібно змінювати (використовується в режимі конфігурації інтерфейсу);
- *ip nat outside* – вказати інтерфейс, який направлений «назовні» (використовується в режимі конфігурації інтерфейсу).

Опис лабораторної роботи

Є дві мережі: внутрішня 192.168.10.0/24 і зовнішня 192.168.20.0/24. Маршрутизація між мережами забезпечується роутерами Cisco 1841, що утворюють підмережу 87.14.58.0/30. Для забезпечення доступу клієнтів із внутрішньої мережі до ресурсів зовнішньої мережі на роутерах потрібно налаштувати трансляцію мережевих адрес за технологією NAT. Структура комп'ютерної мережі зображена на рис. 3.1.

В результаті, пакети після проходження роутера мають змінювати IP-адресу призначення, на відповідну адресу інтерфейсу ротера. Пакет відповіді також має змінити IP-адресу призначення після проходження роутера.

Хід роботи:

1. Для кожного з кінцевих пристроїв (ноутбуків, комп'ютерів та сервера) потрібно встановити IP-адресу даного пристрою в мережі, маску мережі, IP-адресу шлюзу (gateway) та IP-адресу DNS-сервера. Потрібні IP-адреси вказані біля кожного з пристроїв.
2. Налаштувати інтерфейси роутерів (увімкнути їх та присвоїти IP-адреси та маски під мереж).
3. Налаштувати NAT в статичному режимі на роутері Nat-Static.
4. Налаштувати NAT в режимі перевантаження на роутері Nat-Overload.
5. Впевнитись, що виконується заміна IP-адрес в обох підмережах.

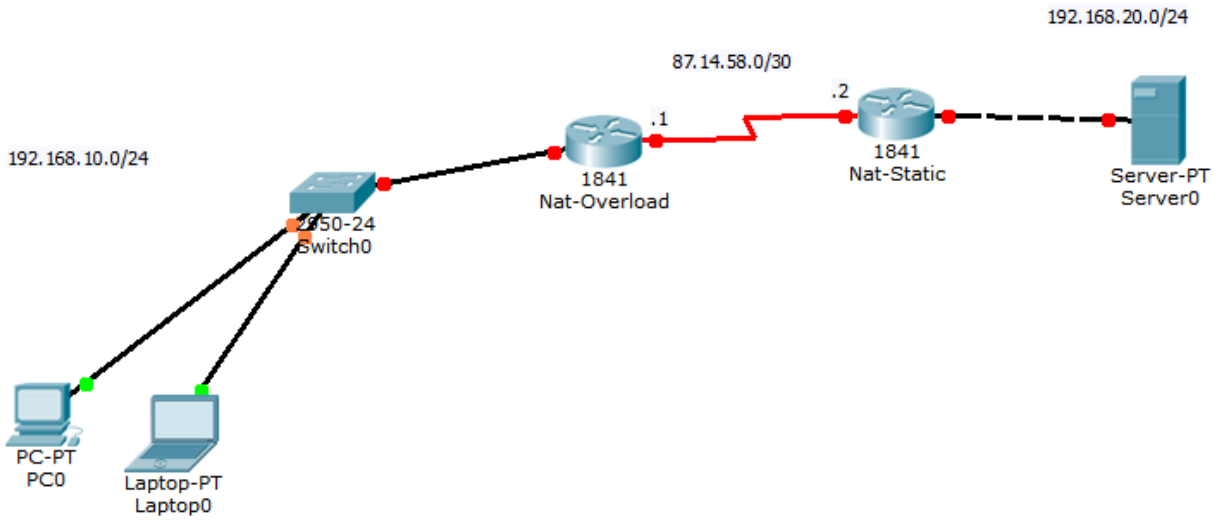

Рис. 3.1 – Структура комп’ютерної мережі

Контрольні питання

1. Вкажіть призначення технології NAT.
2. Які режими роботи NAT існують?
3. Наведіть команди, які необхідно використовувати при налаштуванні NAT в статичному режимі.
4. Вкажіть команди, які необхідно використовувати при налаштуванні NAT в режимі перевантаження.
5. Наведіть переваги технології NAT.
6. Чи використовується технологія NAT в сучасних комп’ютерних мережах?

ЛАБОРАТОРНА РОБОТА № 4

Тема: Динамічна маршрутизація. Протокол динамічної маршрутизації RIP

Мета роботи: ознайомитись з основними поняттями динамічної маршрутизації; отримати навички налаштування динамічної маршрутизації за допомогою протоколу RIP.

Теоретичні відомості

Динамічна маршрутизація — це такий тип маршрутизації, в якому маршрути обчислюються автоматично за допомогою протоколів динамічної маршрутизації чи демонами маршрутизації. Демоном динамічної маршрутизації називається спеціальна програма для обчислення маршрутів, як правило вона вміє використовувати декілька різних протоколів маршрутизації. Розповсюдженими є такі демони як *Quagga, GNU Zebra, XORP, Bird.* Розповсюдженими протоколами динамічної маршрутизації є *RIP, OSPF, EIGRP, IS-IS, BGP, HSRP* та ін. Дані протоколи отримують інформацію про топологію і стан каналів зв'язку від інших маршрутизаторів у мережі.

Протоколи динамічної маршрутизації поділяють на дві великі групи:

1. Дистанційно-векторні протоколи динамічної маршрутизації (*Disance-vector Routing Protocols*);
2. Протоколи стану каналів зв'язку(*Link-sate Routing Protocols*).

Основна різниця між цими протоколами полягає в тому, що дистанційно-векторні протоколи будують в пам'яті повний граф комп'ютерної мережі, в той час коли протоколи стану каналів зв'язку визначають та використовують лише найкращі маршрути.

Дистанційно-векторний протокол маршрутизації RIP (*Routing Information Protocol*) — це один із протоколів маршрутизації в невеликих комп'ютерних мережах, який дозволяє маршрутизаторам динамічно оновлювати маршрутну інформацію (напрямок і дальність в хопах, *hop*), отримуючи її від сусідніх маршрутизаторів.

Хопом називається процес передачі пакету між вузлами мережі, на кожному хопі параметр пакету TTL зменшується на одиницю. Чим більше хопів — тим довший і складніший маршрут.

У цьому протоколі всі мережі мають номери (спосіб утворення номера залежить від використовуваного в мережі протоколу мережевого рівня), а всі маршрутизатори мають ідентифікатори. Протокол RIP широко використовує поняття «вектор відстаней». Вектор відстаней являє собою набір пар чисел, що є номерами мереж і відстанями до них в хопах.

Вектора відстаней ітераційно поширюються маршрутизаторами по мережі, і через кілька кроків кожен маршрутизатор має дані про досяжних для нього мережах і про відстані до них. Якщо зв'язок з будь мережею обривається, то маршрутизатор відзначає цей факт тим, що привласнює елементу вектора, відповідної відстані до цієї мережі, максимально можливе значення, яке має спеціальний зміст – "зв'язку немає". Таким значенням в протоколі RIP є метрика число 16. Максимальна кількість хопів, дозволений RIP – 15 (метрика 16 означає «нескінченно велику метрику», тобто недосяжний сегмент мережі). Кожен RIP-маршрутизатор за замовчуванням сповіщає в мережу свою повну таблицю маршрутизації раз на 30 секунд, генеруючи досить багато трафіку на низькошвидкісних лініях зв'язку.

Формат RIP пакету включає записи з маршрутною інформацією: *command* – команда, що визначає призначення (1 – Request; 2 – Response), *version* – номер версії протоколу (залежно від версії, визначається формат пакета), *must*

be zero – значення повинно бути нулем, *RIP Entry (RTE)* – запис маршрутної інформації RIP. Протокол RIP працює на прикладному рівні стека TCP/IP, використовуючи протокол UDP та порт 520.

Також, протокол RIP має опцію аутентифікації. Якщо вона увімкнена, то оброблюються лише ті пакети, які містять правильний аутентифікаційний код. Шифрування цього коду відбувається за допомогою алгоритму MD5.

При використанні протоколу RIP працює евристичний алгоритм динамічного програмування Беллмана-Форда (*Bellman–Ford algorithm*), і рішення, знайдене з його допомогою є не оптимальним, а близьким до оптимального. Перевагою протоколу RIP є його обчислювальна простота, а недоліками – збільшення трафіку при періодичній розсилці широкомовних пакетів і неоптимальність знайденого маршруту.

Налаштування протоколу маршрутизації RIP

Для налаштування дистанційно-векторного проколу маршрутизації RIP використовуються наступні **команди:**

- *router rip* – перейти в режим конфігурування протоколу RIP;
- *network [IP-адреса зовнішньої мережі]* – додати мережу, яка не є безпосередньо приєднаною до роутера, для обробки протоколом RIP.

Розглянемо налаштування протоколу динамічної маршрутизації RIP в простій топології, що зображено на рис. 4.1.

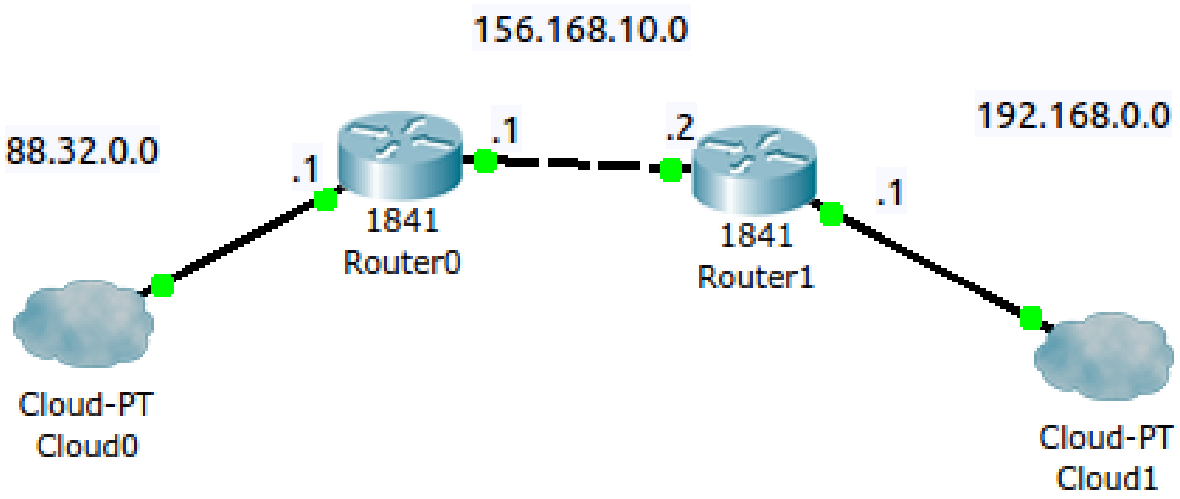

Рис. 4.1 — Проста топологія для налаштування динамічної маршрутизації

Router0:

```
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 88.32.0.1 255.255.255.0
Router(config)#interface fastEthernet 0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 156.168.10.1 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 88.32.0.0
Router(config-router)#network 156.168.10.0
```

Router1:

```
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 156.168.10.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-router)#network 156.168.10.0
Router(config-router)#exit
```

Опис лабораторної роботи

Є три мережі: 192.168.10.0/24, 192.168.20.0/24, 8.8.8.0/30. Для забезпечення зв'язку між мережами потрібно налаштувати статичні маршрути на кожному з роутерів із використанням дистанційно-векторного протоколу маршрутизації RIP. Структура мережі зображена на рис. 4.2.

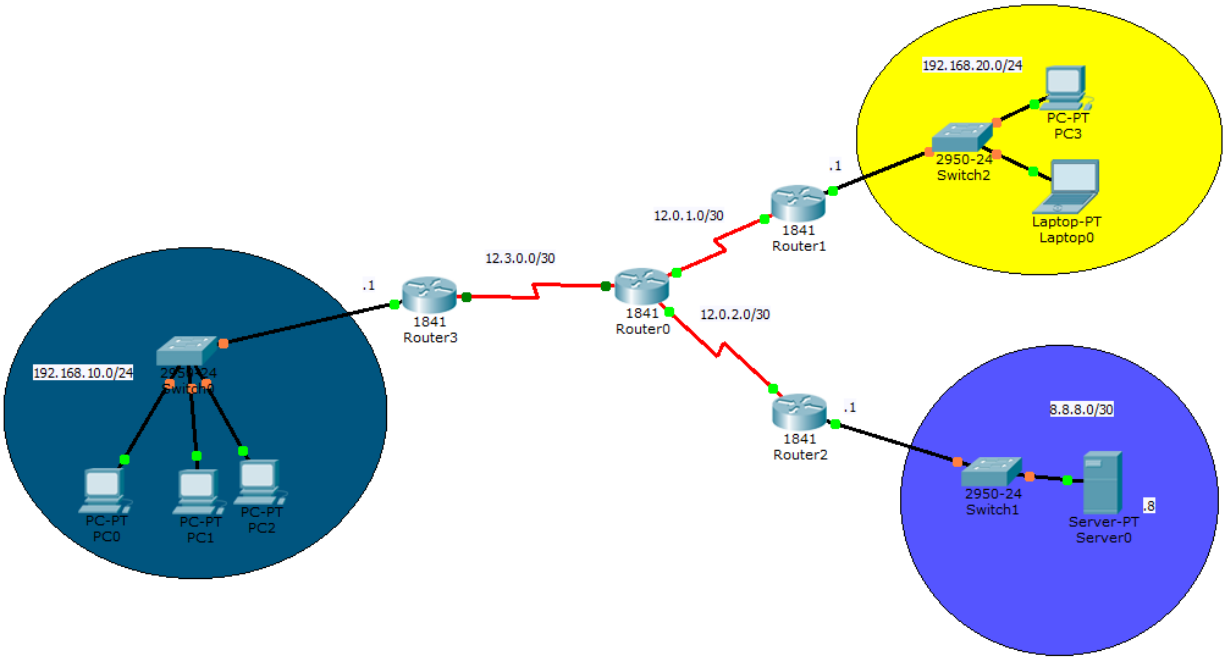

Рис. 4.2 – Структура мережі лабораторної роботи

Хід роботи:

1. Для кожного з кінцевих пристроїв (ноутбуків, комп'ютерів та сервера) потрібно встановити IP-адресу для даного пристрою, маску мережі, IP-адресу шлюзу (gateway) та IP-адресу DNS-сервера. Потрібні IP-адреси вказані біля кожного з пристроїв.
2. Для всіх роутерів в топології потрібно встановити IP-адреси та маски на домені RIP для кожного з інтерфейсів.
3. Налаштувати маршрутизацію між усіма підмережами за допомогою протоколу динамічної маршрутизації RIP.

Контрольні питання

1. Що таке динамічна маршрутизація?
2. Чим динамічна маршрутизація відрізняється від статичної маршрутизації?
3. Які переваги динамічної маршрутизації над статичною?
4. Чи є у динамічної маршрутизації недоліки, порівняно зі статичною маршрутизацією?
5. Чим відрізняються дистанційно-векторні протоколи від протоколів стану?
6. Назвіть особливості протоколу RIP.
7. Назвіть недоліки та переваги протоколу RIP.
8. Назвіть команди, які використовуються при налаштуванні протоколу RIP.

ЛАБОРАТОРНА РОБОТА № 5

Тема: Динамічна маршрутизація. Протокол динамічної маршрутизації OSPF

Мета роботи: ознайомитись з особливостями протоколу OSPF, отримати навички з налаштування динамічної маршрутизації за допомогою протоколу OSPF.

Теоретичні відомості

Протокол динамічної маршрутизації OSPF (*Open Shortest Path First*) заснований на технології відстеження стану каналу (*link-state technology*), що використовує для знаходження найкоротшого шляху алгоритм Дейкстри (*Dijkstra's algorithm*).

Алгоритм роботи протоколу:

1. Маршрутизатори обмінюються hello-пакетами через всі інтерфейси, на яких активований OSPF; якщо маршрутизатори мають спільний канал, то вони стають сусідами;
2. Маршрутизатори, які стали сусідами, обмінюються між собою таблицями маршрутизації;
3. Маршрутизатори постійно повідомляють сусіднім маршрутизаторам стан своїх каналів;
4. Кожен маршрутизатор відправляє отримані дані про стан каналів інших маршрутизаторів своїм сусідам;
5. В кінці такого обміну пакетами всі маршрутизатори мережі мають однакову базу даних станів каналів мережі;
6. Використовуючи алгоритм Дейкстри, кожен маршрутизатор,

використовуючи базу стану каналів, обраховується граф, який буде описувати найкоротший шлях до кожного вузла мережі із собою в якості кореня;

7. На основі знайденого графу будується таблиця маршрутизації роутера.

В протоколі динамічної маршрутизації OSPF використовуються наступні **типи пакетів:**

1. hello-пакет — призначений для встановлення та підтримання зв'язку із сусідами;
2. Database Description — містить у собі вміст бази даних станів каналу роутера;
3. Link State Request — використовується для запиту частини бази даних сусіднього маршрутизатора;
4. Link State Update — призначений для повідомлення інших маршрутизаторів про зміну стану канала;
5. Link State Acknowledgment — призначений для підтвердження отримання пакету Link State Update.

Протокол OSPF обчислює маршрути в IP-мережах, зберігаючи при цьому інші протоколи обміну маршрутною інформацією. Кожен маршрутизатор зберігає інформацію про те, в якому стані на його думку знаходиться сусід. Маршрутизатор покладається на сусідні маршрутизатори і передає їм пакети даних тільки в тому випадку, якщо він впевнений, що вони повністю працездатні. Крім інформації про сусідів, маршрутизатор в своєму оголошенні перераховує IP-підмережі, з якими він пов'язаний безпосередньо. За алгоритмом Дейкстри маршрутизатор обчислює шлях не до конкретної мережі, а до маршрутизатора, що підключений до цієї мережі. Кожен маршрутизатор

має унікальний ідентифікатор, який передається в оголошенні про стани зв'язків. Такий підхід дає можливість не витрачати IP-адреси на зв'язки типу «точка-точка» між маршрутизаторами, до яких не підключені робочі станції.

Налаштування протоколу маршрутизації OSPF

Для налаштування протоколу OSPF використовуються наступні **команди:**

- *router ospf [індекс мережі]* – перейти в режим конфігурування протоколу OSPF;
- *network [IP-адреса зовнішньої мережі] [маска мережі] area [індекс мережі]* – додати мережу для обробки протоколом OSPF.

Розглянемо налаштування протоколу OSPF в мережі зображеній на рис. 5.1.

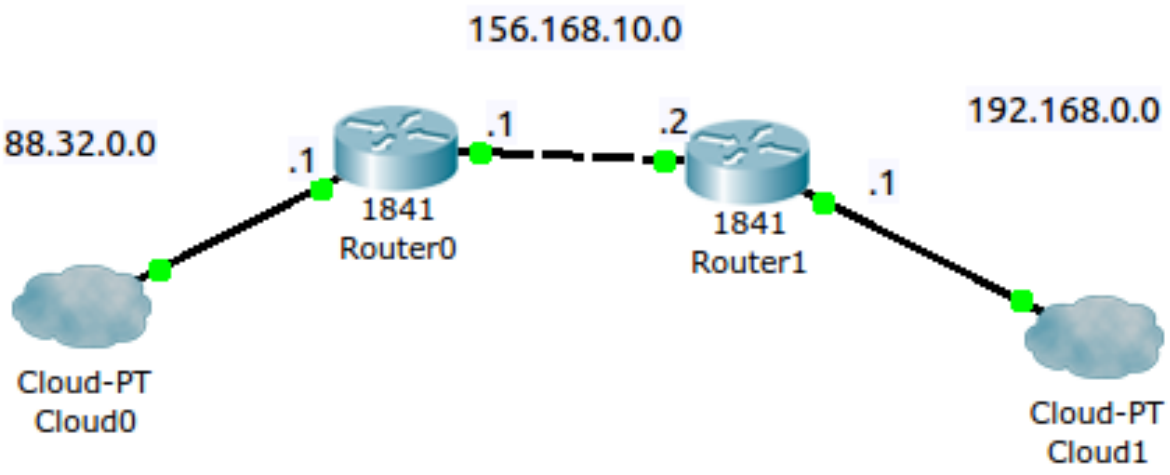

Рис. 5.1 — Проста топологія з трьома під мережами

Router0:

```
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
```

Router(config-if)#no shutdown

Router(config-if)#ip address 88.32.0.1 255.255.255.0

Router(config)#interface fastEthernet 0/1

Router(config-if)#no shutdown

Router(config-if)#ip address 156.168.10.1 255.255.255.0

Router(config-if)#exit

Router(config)#router ospf 10

Router(config-router)#network 88.32.0.0 0.0.0.255 area 5

Router(config-router)#network 156.168.10.0 0.0.0.255 area 5

Router1:

Router>enable

Router#configure terminal

Router(config)#interface fastEthernet 0/0

Router(config-if)#no shutdown

Router(config-if)#ip address 156.168.10.2 255.255.255.0

Router(config-if)#exit

Router(config)#interface fastEthernet 0/1

Router(config-if)#ip address 192.168.0.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#router ospf 10

Router(config-router)#network 192.168.0.0 0.0.0.255 area 5

Router(config-router)#network 156.168.10.0 0.0.0.255 area 5

Опис лабораторної роботи

Є три мережі: 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 і сервер в мережі 8.8.8.0/30. Для забезпечення зв'язку між мережами потрібно налаштувати маршрути на кожному з роутерів із використанням протоколу динамічної маршрутизації OSPF. Структура комп'ютерної мережі зображена на рис. 5.2.

Хід роботи:

1. Для всіх роутерів в топології потрібно встановити IP-адреси та маски на домені OSPF для кожного з інтерфейсів.
2. Для кожного з кінцевих пристроїв (ноутбуків, комп'ютерів та сервера) потрібно встановити IP-адресу для даного пристрою, маску мережі, IP-адресу шлюзу (gateway) та IP-адресу DNS-сервера. Потрібні IP-адреси вказані біля кожного з пристроїв.
3. Налаштувати маршрутизацію між мережами за допомогою OSPF.

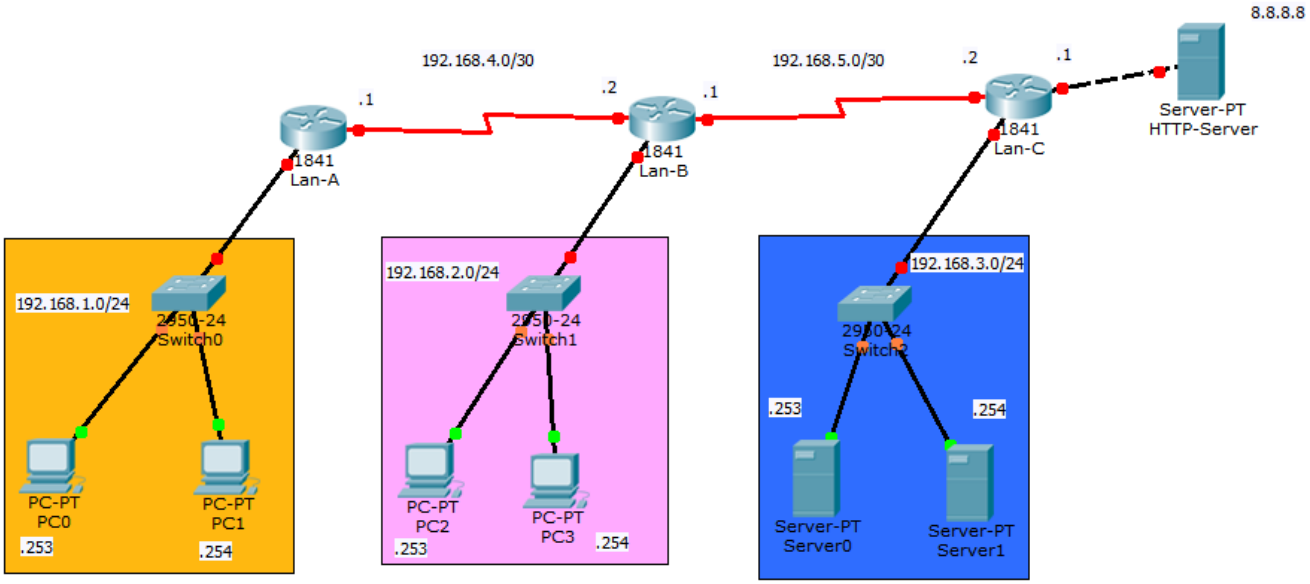

Рис. 5.2 — Структура комп’ютерної мережі лабораторної

Контрольні питання

1. Що таке динамічна маршрутизація?
2. Чим динамічна маршрутизація відрізняється від статичної маршрутизації?
3. Чим протоколи стану каналу відрізняються від дистанційно-векторних протоколів?
4. Які переваги динамічної маршрутизації над статичною?
5. Вкажіть особливості протоколу OSPF.
6. Наведіть алгоритм роботи протоколу OSPF.
7. Що таке hello-пакети? Вкажіть їх призначення.
8. Порівняйте протоколи RIP та OSPF, які в кожного з них є недоліки та переваги?
9. Вкажіть команди, які використовуються для налаштування протоколу динамічної маршрутизації OSPF.

ЛАБОРАТОРНА РОБОТА № 6

Тема: Маршрутизація із використанням протоколу EIGRP

Мета роботи: ознайомитись з особливостями протоколу EIGRP, отримати навички з налаштування динамічної маршрутизації за допомогою протоколу EIGRP.

Теоретичні відомості

Протокол EIGRP (*Enhanced Interior Gateway Routing Protocol*) – дистанційно-векторний протокол динамічної маршрутизації, розроблений компанією Cisco. Іноді цей протокол називають гібридним протоколом, оскільки він має риси як дистанційно-векторних протоколів, так і протоколів стану каналу.

Для реалізації маршрутизації в мережі протокол EIGRP використовує наступні типи **повідомлень**:

1. *hello* — використовуються для знаходження сусідів;
2. *udate* — містять інформацію про зміни в маршрутах, можуть відправлятися якомусь конкретному маршрутизатору, або групі маршрутизаторів;
3. *query* — пакети запиту, використовуються у випадку коли роутер перераховує маршрут в певну мережу і не знаходить резервного маршруту в цю мережу;
4. *reply* — відповідь на отриманий query-пакет;
5. *acknowledgment* — пакет підтвердження отримання пакетів типу update, query чи reply.

Для протоколу EIGRP важливим є підтвердження доставки пакету, тому для передачі пакетів використовується протокол RTP (*Real-time Transport Protocol*).

Обчислення нових маршрутів виконується за допомогою алгоритму DUAL (*Diffusing Update Algorithm*). Основним етапом в цьому алгоритмі є обчислення метрик для кожного маршруту. Метрика — це коефіцієнт, який кількісно характеризує якість маршруту. Для обчислення метрики маршруту використовуються такі **величини**:

1. bandwidth — швидкість передачі даних по маршруту (kbit/s);
2. delay — затримка пакету на всіх інтерфесах роутерів, які він проходить;
3. reliability — використовується найгірший показник надійості на всьому маршруті, який визначаться за допомогою keep-alive з'єднань;
4. loading — найгірший показник завантаження лінку на всьому шляху, обчислюється за допомогою packet rate (кількісь пакетів, які проходять по лінку за секунду), та bandwidth інтерфейсу;
5. MTU — використовується мінімальний MTU (maximum transmission unit — максмальний розмір корисного блока даних одного пакету) всього маршруту.

За умовчанням, використовуються лише перші два компоненти. Використовувати інші компоненти не рекомендується, оскільки це може привести до частого перерахунку маршрутів.

Обчислення метрики маршруту відбувається за наступним **алгоритмом**:

1. За умовчанням, величини коефіцієнтів: K1 = K3 = 1, K2 = K4 = K5 = 0.
2. Обчислюється значення *bandwidth*:

$$bandwidth = (10000000/bandwidth(i)) * 256,$$

де bandwidth(i) — найменша пропускна здатність з усіх інтерфейсів, які є на маршруті.

3. Обчислюється значення параметру *delay*:

$$delay = delay(i) * 256,$$

де delay(i) — сума всіх затримок інтерфейсів маршруту в десятках мікросекунд.

4. При використанні значення параметру K5 = 0 (значення за умовчанням), використовується формула (1):

$$Metric = (K1 * bandwidth) + [(K2 * bandwidth) / (256 - load)] + (K3 * delay) \quad (1)$$

5. Якщо значення коефіцієнтів K1, K2, K3 рівні значенням за умовчанням, то формула (1) спрощується:

$$Metric = bandwidth + delay.$$

6. Якщо K5 не дорівнює 0, то формула (1) має вигляд:

$$Metric = metric * [K5 / (reliability + K4)].$$

Значння коефіцієнтів К передаються роутерами в hello-пакетах.

Налаштування протоколу маршрутизації EIGRP

Для налаштування протоколу EIGRP використовуються наступні **команди**:

- *router eigrp [індекс мережі]* — перейти в режим онфігурування протоколу EIGRP;
- *network [IP-адреса зовнішньої мережі] [маска мережі]* — додати мережу для обробки протоколом EIGRP;
- *no auto-summary* — вимкнути автоматичну сумаризацію маршрутів (використовується для сумісності із старими пристроями).

Розглянемо налаштування протоколу OSPF в мережі зображеній на рис. 6.1.

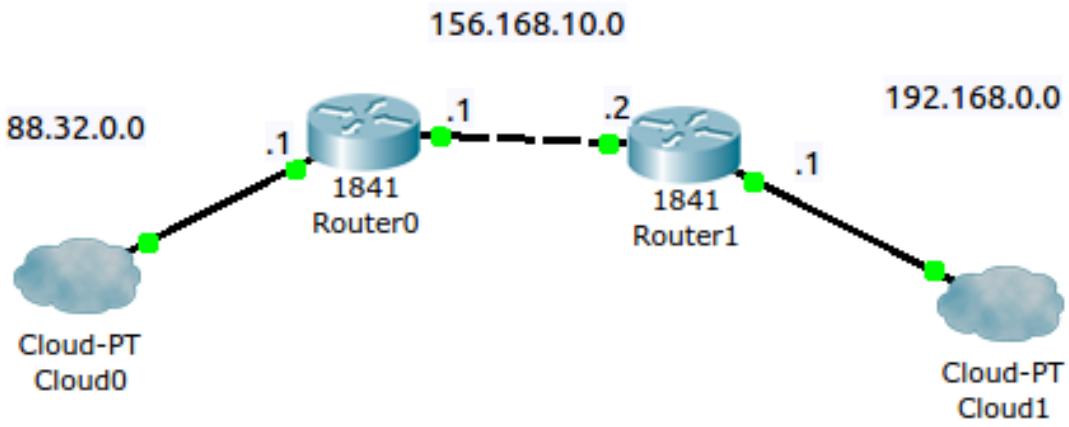

Рис. 6.1 — Проста топологія з трьома під мережами

Router0:

```
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 88.32.0.1 255.255.255.0
Router(config)#interface fastEthernet 0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 156.168.10.1 255.255.255.0
Router(config-if)#exit
Router(config)#router eigrp 20
Router(config-router)#network 88.32.0.0 255.255.255.0
Router(config-router)#network 156.168.10.0 255.255.255.0
Router(config-router)#no auto-summary
```

Router1:

```
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 156.168.10.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#router eigrp 20
Router(config-router)#network 192.168.0.0 255.255.255.0
Router(config-router)#network 156.168.10.0 255.255.255.0
Router(config-router)#no auto-summary
```

Опис лабораторної роботи

Топологія мережі зображена на рис. 6.2.

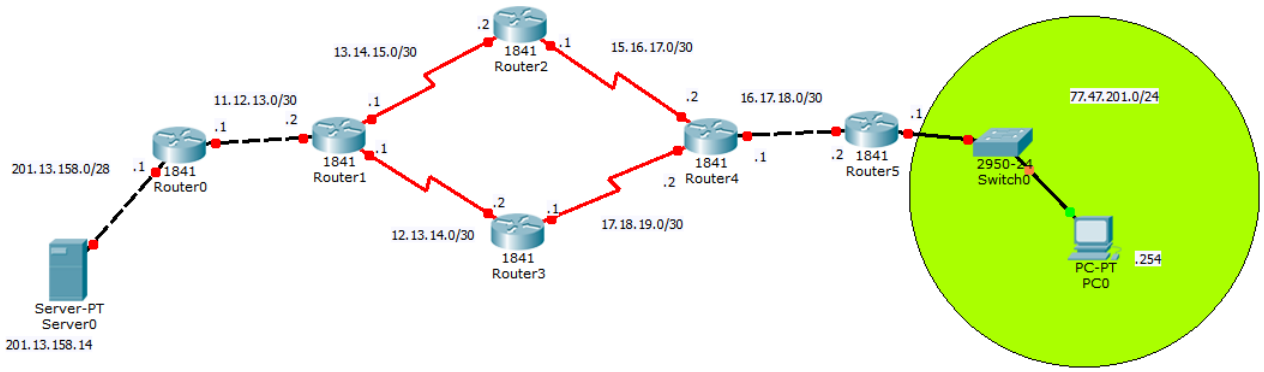

Рис. 6.2 — Структура комп’ютерної мережі.

Необхідно налаштувати маршрути на кожному з роутерів на домені EIGRP для кожного з інтерфейсів.

Хід роботи:

1. Для кожного з кінцевих пристроїв (ноутбуків, комп'ютерів та сервера) потрібно встановити IP-адресу для даного пристрою, маску мережі, IP-адресу шлюзу (gateway) та IP-адресу DNS-сервера. Потрібні IP-адреси вказані біля кожного з пристроїв.
2. Для всіх роутерів в топології потрібно встановити IP-адреси та маски для кожного з інтерфейсів.
3. Налаштувати маршрутизацію між мережами за допомогою протоколу EIGRP.
4. Перевірити, через який із маршрутизаторів проходять пакети — Router2 чи Router3.
5. Вимкнути маршрутизатор, через який проходять пакети і перевірити, що пакети передаються за допомогою іншого маршрутизатора.

Контрольні питання

1. Що таке динамічна маршрутизація?
2. Чим динамічна маршрутизація відрізняється від статичної маршрутизації?
3. Чим протоколи стану каналу відрізняються від дистанційно-векторних протоколів?
4. Які переваги динамічної маршрутизації над статичною?
5. Вкажіть особливості протоколу EIGRP.
6. Яким чином обчислюється метрика маршруту?
7. Наведіть алгоритм роботи протоколу EIGRP.
8. Що таке hello-пакети? Вкажіть їх призначення.
9. Порівняйте протоколи EIGRP та OSPF, які в кожного з них є недоліки та переваги?
10. Вкажіть команди, які використовуються для налаштування протоколу динамічної маршрутизації EIGRP.

ЛАБОРАТОРНА РОБОТА № 7

Тема: Віртуальні локальні комп’ютерні мережі (VLAN)

Мета роботи: ознайомитись з технологією VLAN, отримати навички з її налаштування середовищі Cisco Packet Tracer.

Теоретичні відомості

Логічна («віртуальна») локальна комп'ютерна мережа VLAN (*Virtual Local Area Network*), являє собою групу хостів (*host*) із загальним набором вимог, які взаємодіють так, ніби вони підключені до мережевого домену, незалежно від їх фізичного місцезнаходження. VLAN має ті ж властивості, що й фізична локальна мережа, але дозволяє кінцевим станціям групуватися разом, навіть якщо вони не знаходяться в одній фізичній мережі. За допомогою віртуальних локальних мереж можна легко розділити мережу так, щоб вузли мережі не використовували єдиний сервер DHCP і отримували локальні адреси, або отримували адресу з іншого серверу DHCP.

Віртуальні мережі VLAN можуть бути побудовані на базі портів комутаторів. VLAN, побудовані на базі портів, мають деякі обмеження. Вони дуже прості в установці, але дозволяють підтримувати для кожного порту тільки одну VLAN. Це стосується мереж, що використовують концентратори або мереж з потужними серверами, до яких звертається багато користувачів (сервер не вдасться включити в різні VLAN). Крім того, вносити зміни в VLAN на основі портів досить складно, оскільки при кожній зміні потребується фізичне перемикання пристроїв. У випадку коли одному порту комутатора можуть відповідати декілька мереж VLAN (наприклад, якщо з'єднання VLAN проходить через кілька світчів, switch) цей порт повинен бути членом транка

(*trunk*). На рис. 7.1 показано приклад мережі із використанням технології VLAN.

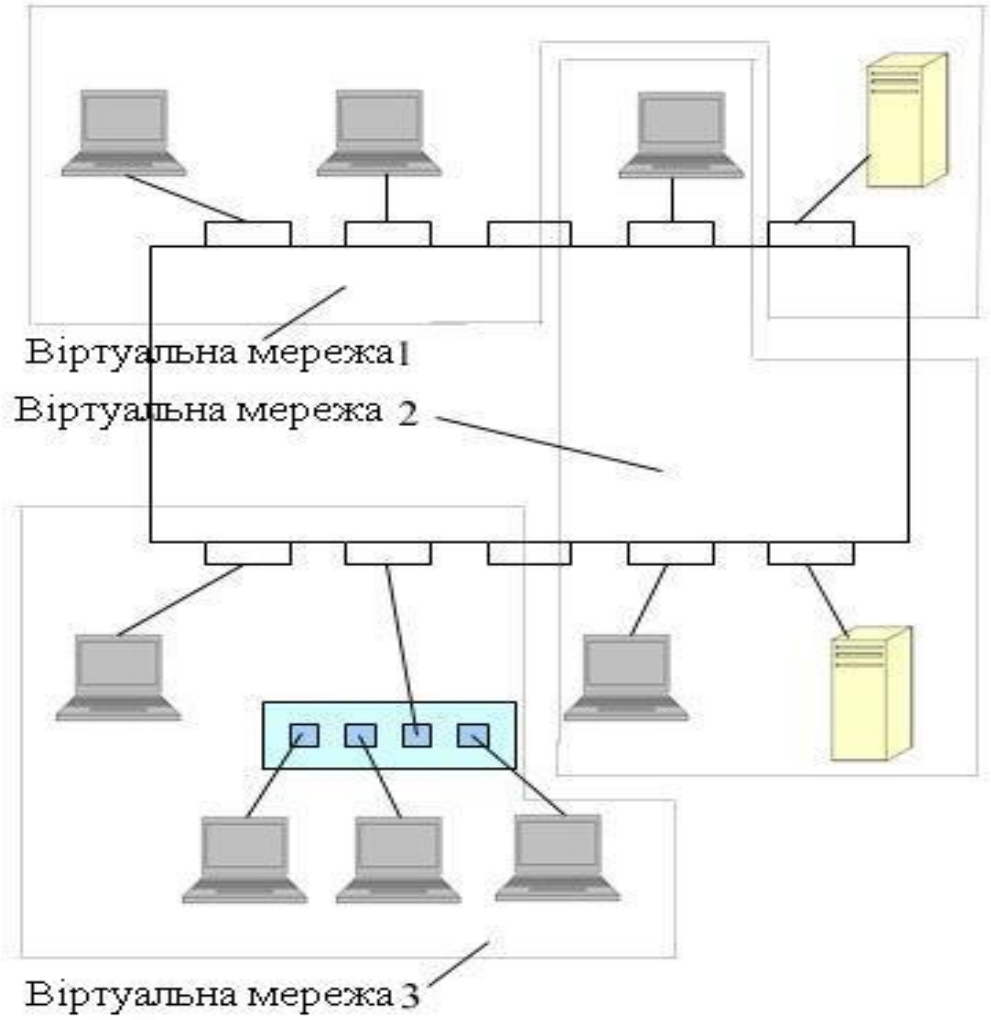

Рис. 7.1 – Приклад реалізації мережі за технологією VLAN

Групування MAC-адрес у віртуальну мережу на кожному комутаторі позбавляє від необхідності зв'язку комутаторів з декількома портами, тому що в цьому випадку MAC-адреса є включеною до віртуальної мережі. Однак цей спосіб вимагає виконання великої кількості ручних операцій по маркуванню MAC-адрес на кожному комутаторі мережі. У випадку коли віртуальні мережі VLAN створюються на основі мережевих адрес, наприклад за IP-адресою,

комутатори мають підтримувати не тільки протоколи канального рівня, але й протоколи мережевого рівня, тобто є комбінованими комутаторами-маршрутизаторами.

Технологія віртуальних мереж створює гнучку основу для побудови великої мережі, з'єднаної маршрутизаторами, тому що комутатори дозволяють створювати повністю ізольовані сегменти програмним шляхом, не прибігаючи до фізичної комутації. При з'єднанні віртуальних мереж через маршрутизатор для кожної віртуальної мережі виділяється в цьому випадку окремий кабель й окремий порт маршрутизатора.

Команди для налаштування віртуальних локальних мереж

- *switchport mode access* – встановити тип лінку access (не передавати інформацію про віртуальні мережі);
- *switchport mode trunk* – встановити тип лінку trunk (передавати інформацію про віртуальні мережі);
- *switchport access vlan [номер віртуальної мережі]* – дати віртуальній мережі із заданим номером доступ через інтерфейс;
- *switchport trunk allowed vlan all* – дозволити проходити через інтерейси пакетам всіх віртуальних мереж;
- *encapsulation dot1Q [номер віртуальної мережі]* – пропускати пакети вітуально мережі із заданим номером через інтерфейс (для роутера).

Опис лабораторної роботи

Задання лабораторної роботи полягає в тому, щоб розділити кінцеві пристрої на три віртуальні підмережі за допомогою технології VLAN. Надавати кінцевим пристроям налаштування має роутер, який також займається

маршрутизацією пакетів між всіма підмережами. Схему комп'ютерної мережі зображено на рис. 7.2.

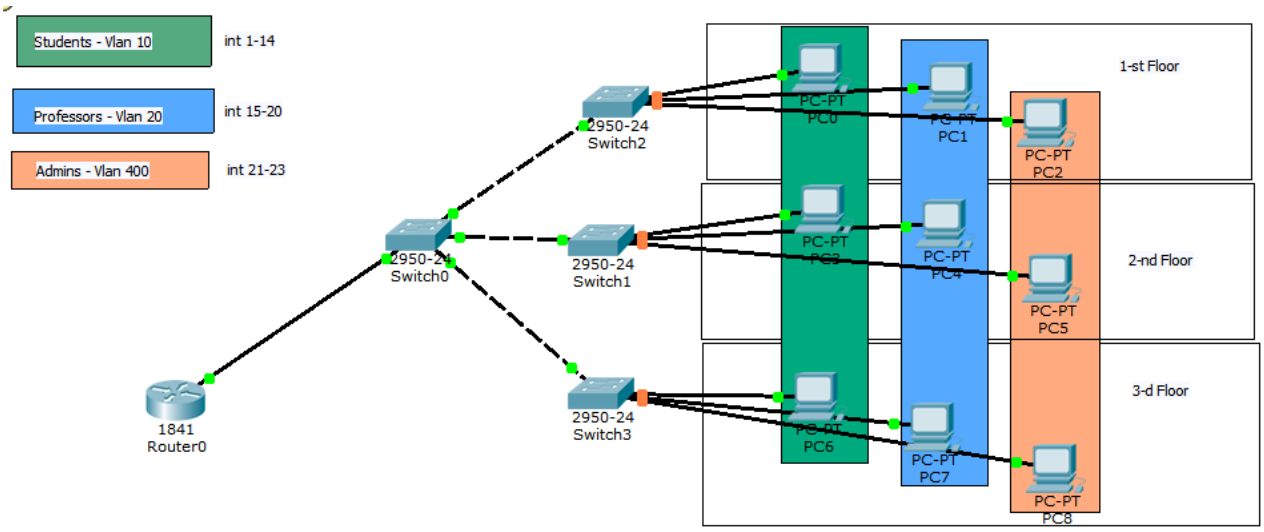

Рис. 7.2 – Схема комп’ютерної мережі лабораторної №7

Хід роботи:

1. На кожному зі свічів створити віртуальні мережі (vlan) з номерами 10, 20 та 400.
2. Для кожного з інтерфейсів свічів встановити потрібний тип передачі даних (access або trunk). Назви vlan-ів та порти через які вони передають дані вказані на схемі комп'ютерної мережі.
3. Створити три саб-інтерфейси на роутері, кожен повинен відповідати за свою віртуальну підмережу і належати до відповідного vlan-у. Налатувати на кожному із них IP-адреси.
4. Створити три пули адрес. Виключити з пулу адреси, зайняті саб-інтерфейсами роутера.

Контрольні питання

1. Що таке віртуальна комп’ютерна мережа?
2. Вкажіть переваги застосування локальних вітуальних комп’ютерних мереж.
3. Пристрої якого типу виконують більшу частину роботи при використанні технології VLAN?
4. Наведіть команди, необхідні для створення віртуальної комп'ютерної мережі.
5. Вкажіть, а якими параметрами можна групувати кінцеві пристрої в логічні комп’терні мережі?
6. Навіщо застосовуються access та trunk лінки? В чому різниця між ними?

ЛАБОРАТОРНА РОБОТА № 8

Тема: Протокол зв'язного дерева STP

Мета роботи: ознайомитись з особливостями протоколів зв'язаних дерев, отримати навички з її налаштування протоколу STP в середовищі Cisco Packet Tracer.

Теоретичні відомості

Основною задачею протоколів зв'язного дерева є попередження утворення «петель» в мережах. Іноді трапляється так, що свічі випадково з'єднуються в кільце. Така ситуація небезпечна тим, що деякі пакети, які з якихось причин не вдалося змаршрутизувати, починають постійно рухатись по цьому колу, збільшуючи навантаження на мережу. Аналогічно поводять себе і пакети з бродкаст (*Broadcast*) адресами (ті що розсилаються свічем на всі порти). Для вирішення таких ситуацій використовуються протоколи зв'язного дерева, які вимикають живлення на якомусь з лінків (*link*), для того, щоб розімкнути кільце.

Протокол STP (*Spanning Tree Protocol*) не є єдиним протоколом, який вирішує дану проблему. Крім STP розповсюдженими протоколам зв'язного дерева є RSTP (*Rapid Spanning Tree Protocol*), MSTP (*Multiple Spanning Tree Protocol*), PVSTP (*Per-VLAN Spanning Tree Protocol*) та SPB (*Shortest Path Bridging*).

Робота протоколу STP описується наступним **алгоритмом**:

1. Після ввімкнення свічів, кожен з них вважає себе кореневим (так званим *root*-ом).
2. Кожен комутатор має власний ідентифікатор (*Bridge ID*), який обчислюється за допомогою декількох параметрів (номера віртуальної

мережі, MAC-адреси свіча та ін.). Ці ідентифікатори розстилаються на всі порти в складі hello-пакетів (відправляються раз в 2 секунди).

3. Якщо комутатор отримує hello-пакет з ідентифікатором меншим за свій власний, то він перестає посилати пакети з власним ідентифікатором, а пересилає отриманий.

4. Залишається тільки один свіч, який продовжує генерувати і пересилати власний ідентифікатор — тепер він стає кореневим мостом (*root bridge*).

5. Для кожної підмережі, до якої приєднано два і більше мости, визначається designated port — порт, через який пакети з кореневого мосту потрапляють в цю підмережу.

6. Всі порти в сегменті мережі, до яких приєднано два і більше портів мосту, блокуються, за виключенням *root port* та *designated port*.

Команди для налаштування віртуальних локальних мереж

- *spanning-tree vlan [номер віртуальної мережі] root primary* – зробити комутатор кореневим у віртуальній мережі з вказаним номером;
- *spanning-tree vlan [номер віртуальної мережі] port-priority [0-240]* – встановити пріоритет для лінку комутатора у віртуальній мережі з вказаним номером.

Опис лабораторної роботи

Схему комп'ютерної мережі зображено на рис. 8.1. Потрібно зробити так, щоб кожен комутатор був кореневим для своєї віртуальної мережі. Для комутаторів, які з'єднуються між собою двома лінками, потрібно неактивний лінк зробити активним і навпаки.

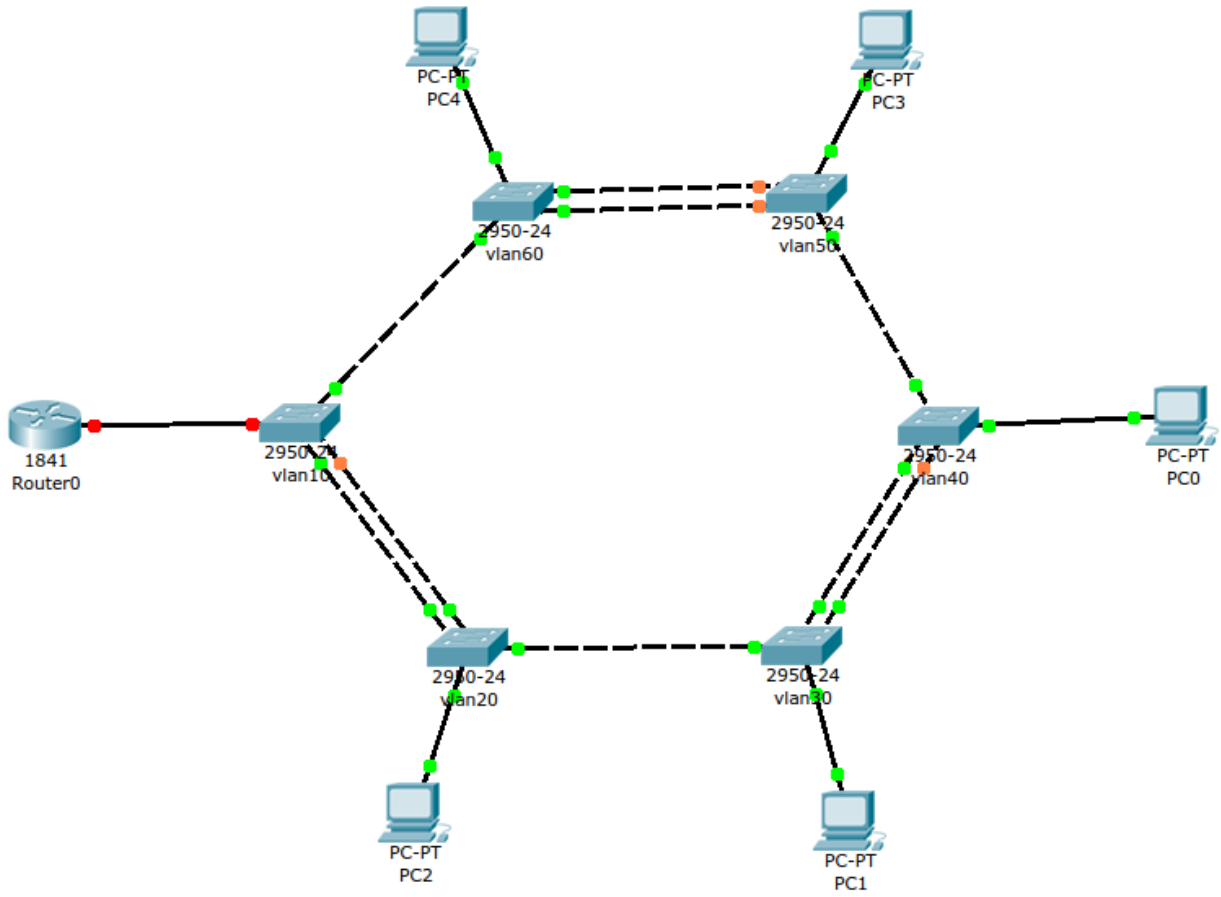

Рис. 8.1 – Схема комп’ютерної мережі лабораторної №8

Хід роботи:

1. Сконфігурувати віртуальні мережі з вказаними номерами.
2. Зробити кожен з комутаторів кореневим у своїй віртуальній мережі.
3. Змінити приорітети лінків (для комутаторів, які з'єднані між собою двома лінками)
4. Перевірити правильність роботи в мережі за допомогою вкладки “Simulation”.

Контрольні питання

1. Що таке віртуальна комп’ютерна мережа?
2. Вкажіть переваги застосування локальних вітуальних комп’ютерних мереж.
3. Навіщо використовуються протоколи зв'язних дерев?
4. Наведіть приклади розповсюджених протоколів, які працюють за алгоритмом зв'язного дерева.
5. Опишіть алгоритм роботи протоколу STP.
6. Який комутатор називається кореневим? Які особливості роботи кореневого комутатора?
7. Чим небезпечне утворення “петель” в топологіях?
8. Наведіть команди, які використовуються для конфігурування протоколу зв'язного дерева.

СПИСОК КОМАНД,

ЩО ВИКОРИСТОВУЮТЬСЯ В ЛАБОРАТОРНИХ РОБОТАХ

Команда	Призначення команди
Router>enable	отримати доступ до конфігурування пристрою
Router#configure terminal	перехід в режим конфігурування пристрою
Router(config)#interface [ім'я інтерфейсу]	перехід в режим конфігурування інтерфейсу
Router(config-if)#shutdown	управління подачею напруги на інтерфейс (вімкнення, вимкнення)
Router(config-if)#no [команда]	відмінити команду
Router(config-if)#ip address [IP-адреса] [маска підмережі]	встановити IP-адресу та маску підмережі для інтерфейсу
Router(config-if)#exit	повернутись на один рівень конфігурування назад
Router(config-if)#end	перейти до початкового режиму конфігурації (Router#)
Router(config)#ip route [IP-адреса мережі] [маска підмережі] [IP-адреса інтерфейсу]	додати статичний маршрут

Команда	Призначення команди
Router(config-if)#ip address dhcp	отримати налаштування інтерфейсу за допомогою DHCP
Router(config)#ip dhcp pool [назва пулу]	створити DHCP пул IP-адрес
Router(dhcp-config)#network [IP-адреса мережі] [маска підмережі]	додати всі IP-адреси мережі в DHCP пул
Router(dhcp-config)#default-router [IP-адреса]	встановити IP-адресу шлюзу за умовчанням для розповсюдження протоколом DHCP
Router(dhcp-config)#dns-server [IP-адреса]	встановити IP-адресу DNS-сервера за умовчанням для розповсюдження протоколом DHCP
Router(config)#ip dhcp excluded-address [IP-адреса]	виключення IP-адреси з пулу
Router(config)#ip nat inside source static [IP-адреса] [IP-адреса]	активація NAT в статичному режимі (замінювати одну IP-адресу на іншу)
Router(config-if)#ip nat inside	вказати інтерфейс направлений «в середину» мережі, IP-адреси якої потрібно змінювати
Router(config-if)#ip nat outside	вказати інтерфейс, який направлений «назовні»
Router(config)#ip nat inside source list [номер списку] interface [назва інтерфейсу] overload	активація NAT в режимі перевантаження

Команда	Призначення команди
Router(config-if)#clock rate [величина]	встановлення швидкості передачі даних serial-лінку
Router(config)#router rip	перейти в режим конфігурування протоколу RIP
Router(config-router)#network [IP-адреса мережі]	додати мережу, яка не є безпосередньо приєднаною до роутера, для обробки протоколом RIP
Router(config)#router ospf [номер мережі]	перейти в режим конфігурування протоколу OSPF
Router(config-router)#network [IP-адреса мережі] [маска підмережі] area [номер зони OSPF]	додати мережу для обробки протоколом OSPF
Router(config)#router eigrp [номер мережі]	перейти в режим онфігурування протоколу EIGRP
Router(config-router)#network [IP-адреса мережі] [маска підмережі]	додати мережу для обробки протоколом EIGRP
Router(config-router)#no auto-summary	вимкнути автоматичну сумаризацію маршрутів (використовується для сумісності із старими пристроями)
Switch(config)#vlan [номер віртуальної мережі]	створити віртуальну мережу
Switch(config-vlan)#name [назва віртуальної мережі]	змінити назву віртуальної мережі

Команда	Призначення команди
Switch(config)#interface range [діапазон інтерфейсів]	перейти в режим конфігурації діапазону інтерфейсів
Switch(config-if)#switchport mode access	встановити тип лінку access
Switch(config-if-range)#switchport access vlan [номер віртуальної мережі]	дати віртуальній мережі із заданим номером доступ через інтерфейс (в режимі access)
Switch(config-if-range)#switchport access vlan all	дати всім віртуальним мережам доступ через інтерфейс (в режимі access)
Switch(config-if)#switchport mode trunk	встановити тип лінку trunk
Switch(config-if)#switchport trunk allowed vlan [номер віртуальної мережі]	дати віртуальній мережі із заданим номером доступ через інтерфейс (в режимі trunk)
Switch(config-if-range)#switchport trunk allowed vlan all	дати всім віртуальним мережам доступ через інтерфейс (в режимі trunk)
Router(config)#interface [назва інтерфейсу].[номер саб-інтерфейсу]	створити саб-інтерфейс
Router(config-subif)#encapsulation dot1Q [номер віртуальної мережі]	пропускати пакети вітуально мережі із заданим номером через інтерфейс (для роутера)
Switch(config-if)#spanning-tree vlan [номер віртуальної мережі] root primary	зробити комутатор кореневим у віртуальній мережі з вказаним номером

Команда	Призначення команди
Switch(config-if)#spanning-tree vlan [номер віртуальної мережі] port-priority [0-240]	встановити пріоритет для лінку комутатора у віртуальній мережі з вказаним номером

РЕКОМЕНДОВАНИЙ ПЕРЕЛІК ЕЛЕКТРОННИХ ДЖЕРЕЛ ІНФОРМАЦІЇ

Адреса джерела інформації	Опис джерела інформації
http://dflt.ru/articles/networks/tablica-masok-podseti	Таблиця масок підмереж
http://ip-calculator.ru/	Калькулятор IP-адрес
http://xgu.ru/	База даних знань системного адміністратора – містить велику кількість як теоретичного матеріалу, так і практичні керівництва для налаштування телекомунікаційних пристроїв
http://www.cisco.com/cisco/web/support/index.html	Офіційна документіція від компанії Cisco

ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ТА ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013. ISBN 978-617-574-087-3
2. Буров Є. В. Комп'ютерні мережі: підручник / Євген Вікторович Буров. — Львів: «Магнолія 2006», 2010. ISBN 966-8340-69-8.
3. Одом У. Офіційне керівництво Cisco з підготовки до сертифікаційних іспитів CCENT / CCNA ICND1 640-822. ISBN 978-5-8459-1807-9, 978-1-58-720-425-8; 2012 г.
4. Алан Леінванд, Брюс Пінскі. Конфігурування маршрутизаторів Cisco — Cisco Router Configuration. — 2-ге вид. — М.: «Вільямс», 2001. — ISBN 1-57870-241-0.
5. Cisco Systems Керівництво Cisco з міждоменної багатоадресової маршрутизації — Interdomain Multicast Solutions Guide. — М.: «Вильямс», 2004. — ISBN 5-8459-0605-9.
6. Том М. Томас II. Структура та реалізація мереж на основі протоколу OSPF. Керівництво Cisco — OSPF Network Design Solutions. — 2-ге вид. — М.: «Вільямс», 2004. —ISBN 1-58705-032-3.