Міністерство освіти і науки України
Центральноукраїнський національний технічний університет
Факультет будівництва, транспорту та енергетики
Кафедра автоматизації виробничих процесів

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

до виконання практичних робіт з навчальної дисципліни

«ПРОЄКТУВАННЯ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ»

для здобувачів першого (бакалаврського) рівня вищої освіти
спеціальності G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка»
освітньої програми «Інтернет речей та електронні комунікації»
денної та заочної форм навчання

ЗАТВЕРДЖЕНО
на засіданні кафедри автоматизації виробничих процесів
Протокол № 1 від 28.08.2026 року

Кропивницький – 2026

ВІДОМОСТІ ПРО ВИДАННЯ

Проєктування інфокомунікаційних мереж : методичні рекомендації до виконання практичних робіт для здобувачів денної та заочної форм навчання спеціальності G5 / Центральноукраїнський національний технічний університет ; уклад. О. А. Смірнов, Ю. М. Пархоменко. – Кропивницький : ЦНТУ, 2026.

Розробники:

Смірнов О.А., д-р техн. наук, професор кафедри КбПЗ;
Пархоменко Ю.М., канд. техн. наук, доцент кафедри АВП.

© Центральноукраїнський національний технічний університет, 2026

ЗМІСТ

ВСТУП

Практична робота № 1. Середовище моделювання Cisco Packet Tracer

Практична робота № 2. Статична маршрутизація

Практична робота № 3. Протокол DHCP

Практична робота № 4. Налаштування технології NAT/PAT

Практична робота № 5. Динамічна маршрутизація. Протокол RIPv2

Практична робота № 6. Динамічна маршрутизація. Протокол OSPF

Практична робота № 7. Маршрутизація з використанням протоколу EIGRP

Практична робота № 8. Віртуальні локальні мережі (VLAN)

ПОРЯДОК ОЦІНЮВАННЯ ТА ВИМОГИ ДО ЗВІТІВ

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

ОФІЦІЙНІ ІНФОРМАЦІЙНІ РЕСУРСИ

ВСТУП

Дисципліна «Проєктування інфокомунікаційних мереж» спрямована на формування практичних умінь аналізувати мережеві вимоги, створювати топології, визначати адресні плани, налаштовувати комутацію, маршрутизацію й мережеві сервіси та перевіряти працездатність прийнятих рішень.

Методичні рекомендації містять вісім практичних робіт, що охоплюють Cisco Packet Tracer, статичну маршрутизацію, DHCP, NAT/PAT, протоколи RIPv2, OSPF, EIGRP та VLAN. Роботи виконуються у симуляторі Cisco Packet Tracer відповідно до наведених схем, інструкцій і контрольних питань.

ОРГАНІЗАЦІЯ ПРАКТИЧНИХ ЗАНЯТЬ

Порядок виконання: опрацювати теорію; створити топологію за схемою; задати IP-параметри та конфігурації; перевірити зв’язність і маршрутні таблиці; зберегти файл .pkt та підтверджувальні скриншоти; оформити й захистити звіт.

Завдання виконуються лише в навчальному або авторизованому середовищі моделювання. Приклади команд Cisco IOS у вихідних матеріалах подано для відповідних моделей пристроїв; на інших версіях обладнання синтаксис і назви інтерфейсів можуть відрізнятися.

ПРАКТИЧНА РОБОТА № 1
Середовище моделювання Cisco Packet Tracer

Мета роботи

Ознайомитися з інтерфейсом і основними можливостями Cisco Packet Tracer; навчитися додавати мережеві пристрої, з'єднувати їх, задавати базові IP-параметри та перевіряти зв'язок між вузлами.

Програмне та апаратне забезпечення

Cisco Packet Tracer 8.x або новіша доступна версія; віртуальні маршрутизатори Cisco ISR, комутатори Cisco Catalyst, ПК/Server-PT. За наявності — ПК з Windows/Linux для додаткової перевірки команд ping/tracert.

Очікувані результати

– орієнтуватися в основних панелях Cisco Packet Tracer
– додавати маршрутизатори, комутатори та кінцеві пристрої
– вибирати тип з'єднання та підключати пристрої
– налаштовувати IPv4-адреси кінцевих вузлів і перевіряти зв'язок командою ping

Короткі теоретичні відомості

Cisco Packet Tracer — навчальний симулятор мереж, у якому можна будувати логічні топології, конфігурувати Cisco IOS, перевіряти IP-зв'язність і спостерігати проходження пакетів. Для базової роботи достатньо режиму Realtime, панелі вибору пристроїв, Connections та вкладок Config/CLI/Desktop.

Матеріали до виконання практичної роботи

У практичній роботі потрібно відтворити навчальну мережу, наведену на рисунку 1, додати мережеві пристрої, з'єднати їх, налаштувати IPv4-параметри двох ПК і перевірити зв'язок між ними.

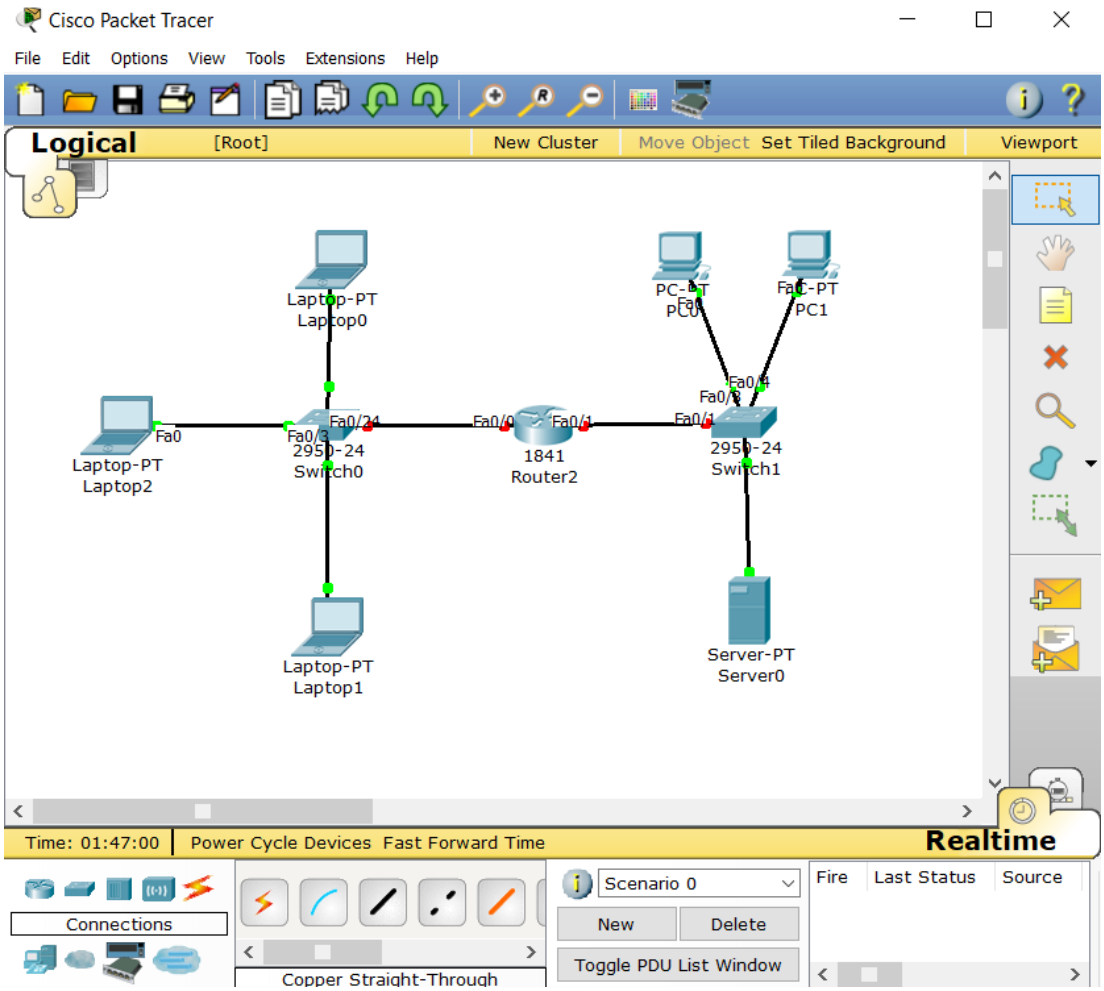


Рисунок 1. – Вихідна топологія мережі

Порядок виконання

1. Створіть новий проєкт і відтворіть топологію, показану на рисунку 1.
2. Додайте маршрутизатор, як показано на рисунку 2; потім додайте комутатори та кінцеві пристрої.

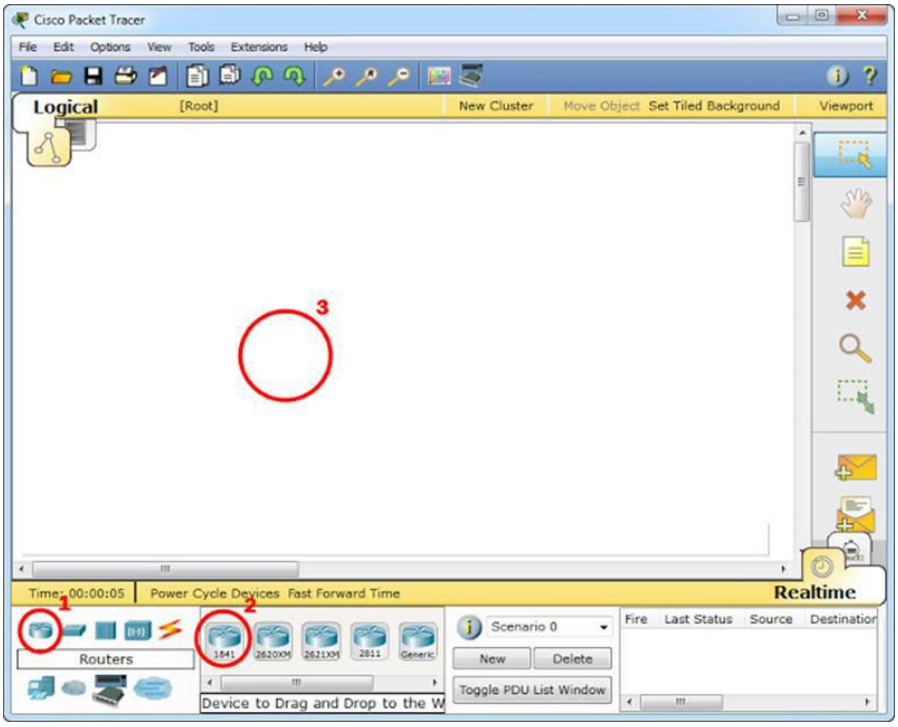


Рисунок 2. – Додавання маршрутизатора в робоче поле Cisco Packet Tracer

3. З’єднайте пристрої. Для вибору кабелю використовуйте меню Connections; приклад наведено на рисунку 3.

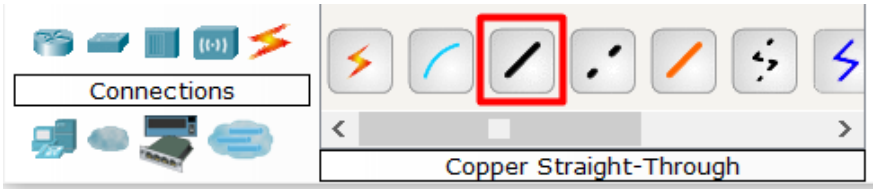


Рисунок 3. – Вибір типу мережевого з’єднання

4. Для кожного ПК відкрийте Desktop → IP Configuration (рисунок 4).

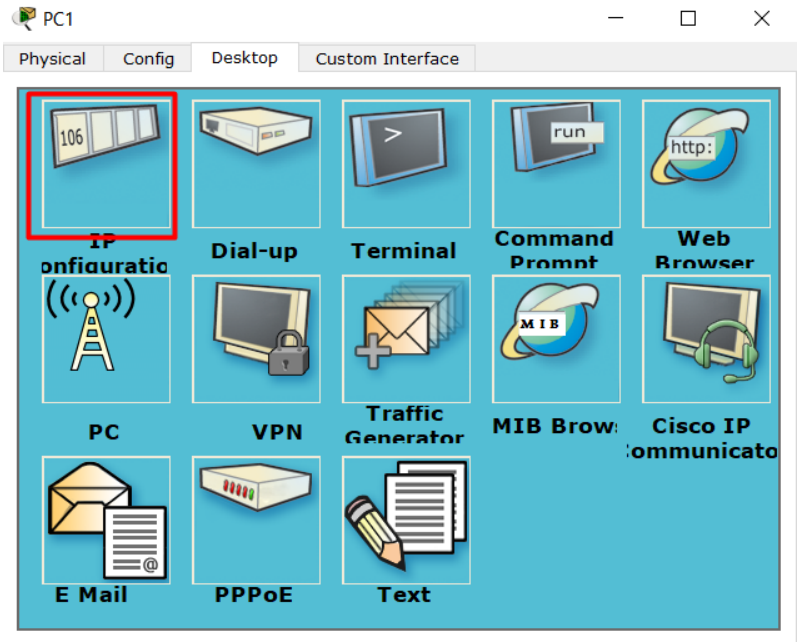


Рисунок 4. – Перехід до налаштування IP Configuration

5. Призначте PC1 адресу 192.168.1.2/24 (рисунок 5), а PC0 – 192.168.1.1/24 (рисунок 6).

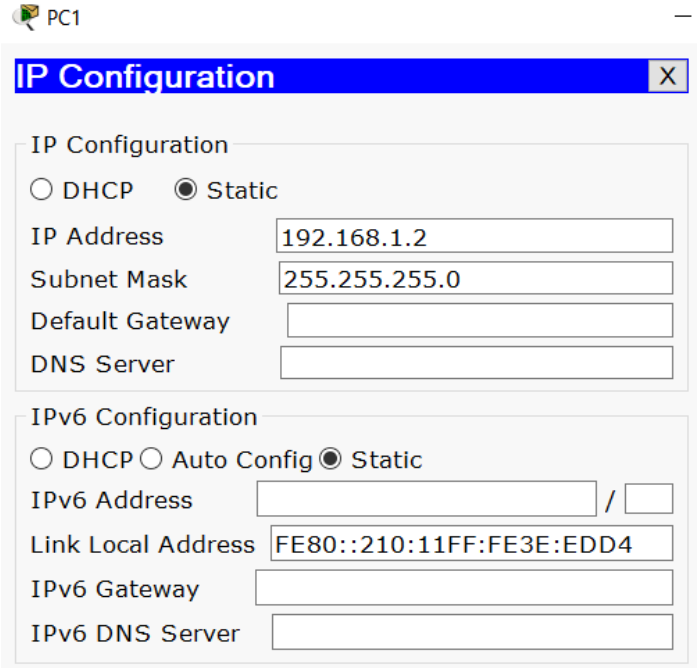


Рисунок 5. – Приклад налаштування PC1

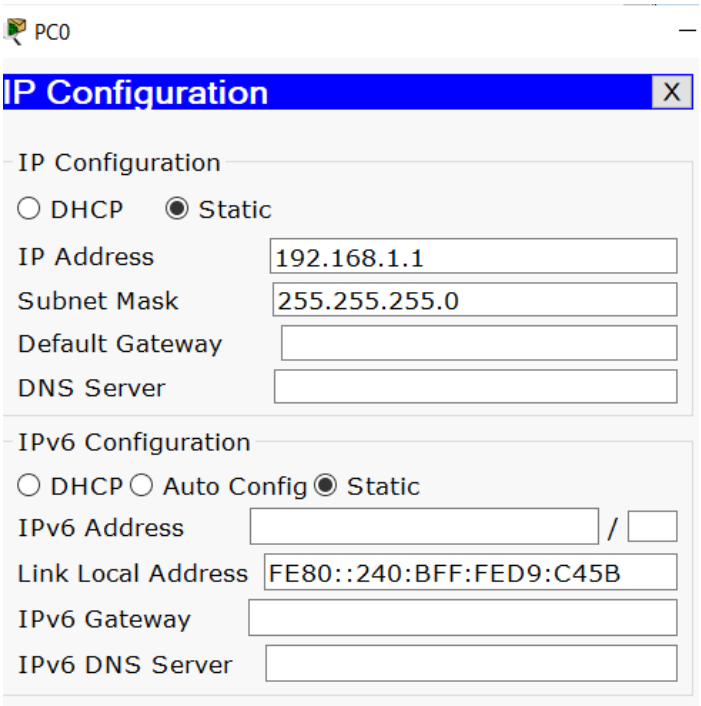


Рисунок 6. – Приклад налаштування PC0

6. На одному з ПК відкрийте Command Prompt (рисунок 7) і виконайте ping адреси іншого ПК.

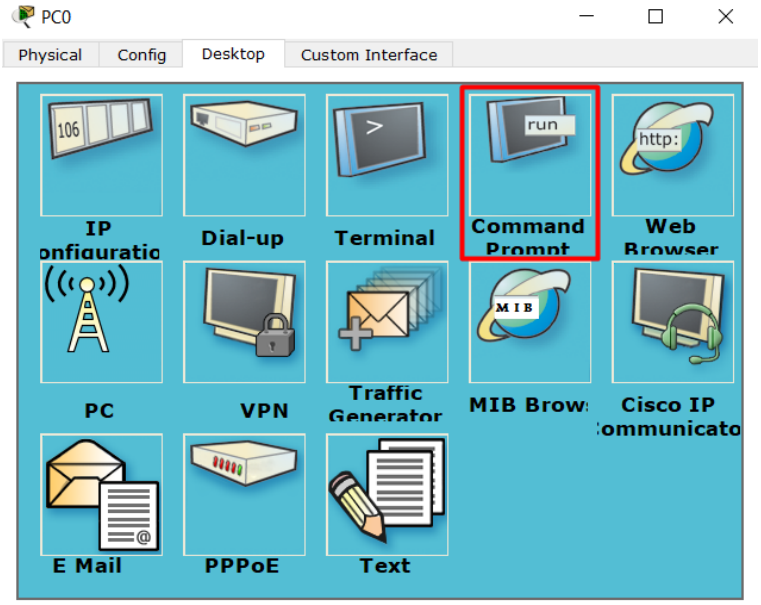


Рисунок 7. – Відкриття Command Prompt на ПК

7. Переконайтеся, що пакети успішно передаються; приклад результату наведено на рисунку 8.

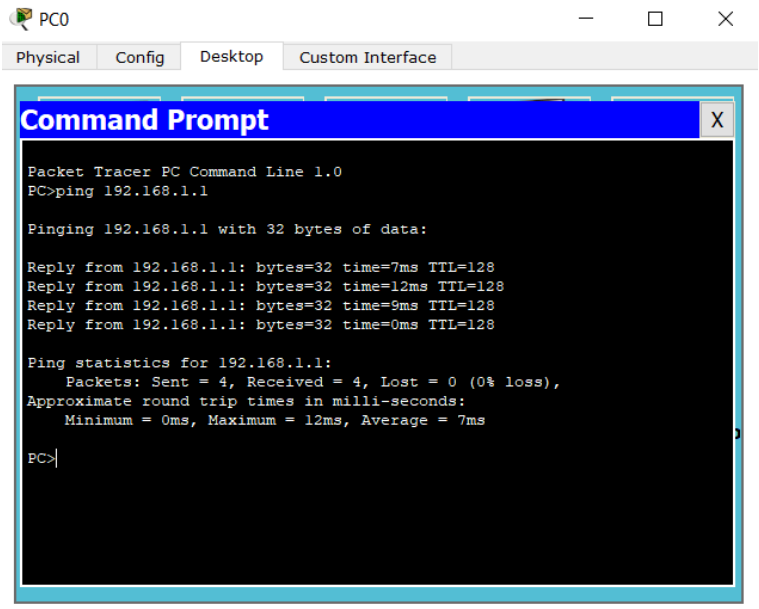


Рисунок 8. – Перевірка зв’язку командою ping

Контрольні питання

1. Яке призначення Cisco Packet Tracer?
2. Які типи мережевих з’єднань доступні в Packet Tracer?
3. Для чого використовується IP Configuration?
4. Яке призначення команди ping?
5. На якому рівні моделі OSI працює комутатор?
6. Які основні режими роботи має Cisco Packet Tracer?

Вимоги до звіту

– титульний аркуш із номером і темою роботи
– схема мережі та, за потреби, таблиця адресації
– основні команди або параметри налаштування
– результати перевірки (ping та відповідні show-команди)
– 2–3 скриншоти ключових етапів
– короткий висновок про отримані результати

ПРАКТИЧНА РОБОТА № 2
Статична маршрутизація

Мета роботи

Набути практичних навичок побудови IP-мережі з кількома маршрутизаторами, налаштування інтерфейсів і статичних маршрутів та перевірки наскрізної досяжності вузлів.

Програмне та апаратне забезпечення

Cisco Packet Tracer 8.x або новіша доступна версія; віртуальні маршрутизатори Cisco ISR, комутатори Cisco Catalyst, ПК/Server-PT. За наявності — ПК з Windows/Linux для додаткової перевірки команд ping/tracert.

Очікувані результати

– складати простий адресний план
– налаштовувати IP-адреси інтерфейсів Cisco IOS
– створювати статичні маршрути
– перевіряти таблицю маршрутизації й досяжність вузлів

Короткі 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.

Статична маршрутизація - вид маршрутизації, при якому маршрути вказуються в явному вигляді при конфігурації маршрутизатора. Вся маршрутизація при цьому відбувається без участі будь-яких протоколів маршрутизації.

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.

Статичний маршрут задається адміністратором вручну. У Cisco IOS використовують команду ip route <мережа> <маска> <next-hop або інтерфейс>. Такий підхід доцільний для невеликих мереж і добре підходить для відпрацювання логіки маршрутизації.

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 адміністрування 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.

Приклад налаштування статичної маршрутизації

На рисунку 9. 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.

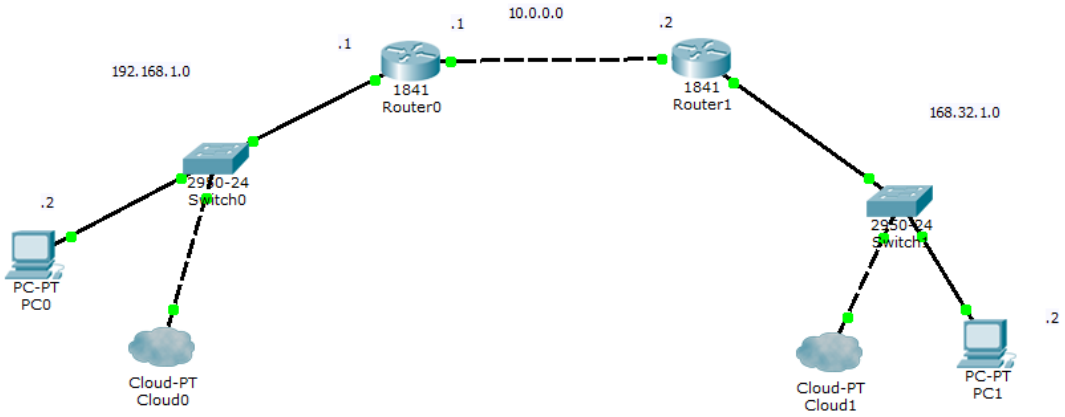


Рисунок 9. – Топологія з трьома під мережами

Матеріали до виконання практичної роботи

Вихідна мережа складається з чотирьох підмереж: 192.168.10.0/24, 192.168.20.0/24, 10.10.10.0/30 та 168.75.89.0/29. Топологію наведено на рисунку 10. Необхідно забезпечити наскрізний зв’язок за допомогою статичних маршрутів.

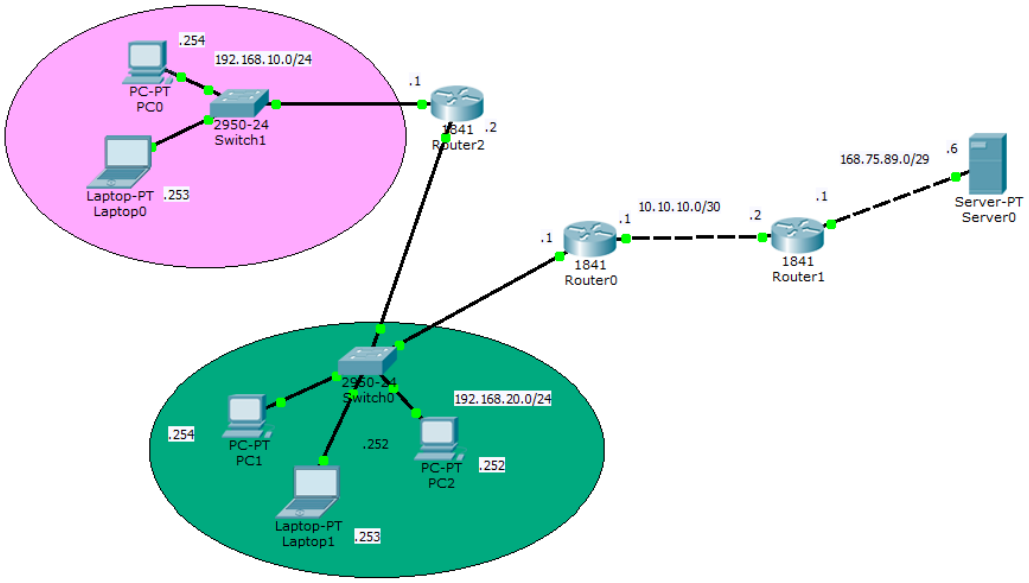


Рисунок 10. – Топологія мережі для налаштування статичної маршрутизації

Порядок виконання

1. Налаштуйте IP-адреси та маски всіх інтерфейсів маршрутизаторів відповідно до рисунка 9.
2. Для кінцевих вузлів задайте IP-адреси, маски, шлюзи та, за потреби, DNS-сервер.

3. На маршрутизаторах додайте статичні маршрути до мереж, які не є безпосередньо підключеними.
4. Перевірте таблицю маршрутизації командою show ip route.
5. Перевірте наскрізну досяжність командою ping.

Основні команди

```
ip route <мережа призначення> <маска> <IP next-hop>
show ip route
ping <IP-адреса>
```

Контрольні питання

1. Що таке маршрутизація?
2. Що називають статичною маршрутизацією?
3. Які переваги та недоліки статичної маршрутизації?
4. Які параметри містить команда ip route?
5. Для чого використовується шлюз за замовчуванням?
6. Як перевірити таблицю маршрутизації?

Вимоги до звіту

– титульний аркуш із номером і темою роботи
– схема мережі та, за потреби, таблиця адресації
– основні команди або параметри налаштування
– результати перевірки (ping та відповідні show-команди)
– 2–3 скриншоти ключових етапів
– короткий висновок про отримані результати

ПРАКТИЧНА РОБОТА № 3
Протокол DHCP

Мета роботи

Навчитися проєктувати параметри DHCP-пулу та налаштовувати автоматичне надання IPv4-параметрів клієнтам у Cisco Packet Tracer.

Програмне та апаратне забезпечення

Cisco Packet Tracer 8.x або новіша доступна версія; віртуальні маршрутизатори Cisco ISR, комутатори Cisco Catalyst, ПК/Server-PT. За наявності — ПК з Windows/Linux для додаткової перевірки команд ping/tracert.

Очікувані результати

– визначати параметри DHCP-пулу
– налаштовувати DHCP на сервері або маршрутизаторі
– отримувати адресу клієнтом у режимі DHCP
– перевіряти видані адреси й усувати прості помилки

Короткі 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 рисунку 11. 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.

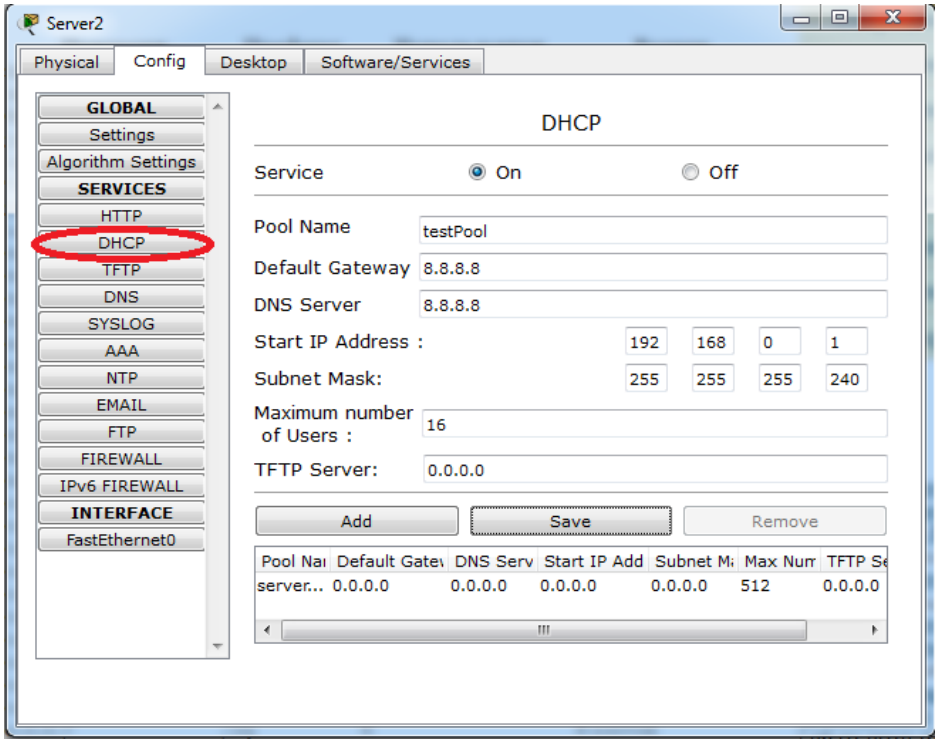


Рисунок 11. – Приклад налаштування DHCP пулу

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

Матеріали до виконання практичної роботи

У схемі на рисунку 12 використано дві мережі: 192.168.10.0/24 та 192.168.15.0/24. Клієнти першої мережі отримують параметри від Server0, а клієнти другої – від маршрутизатора. Така побудова дозволяє порівняти два варіанти організації DHCP.

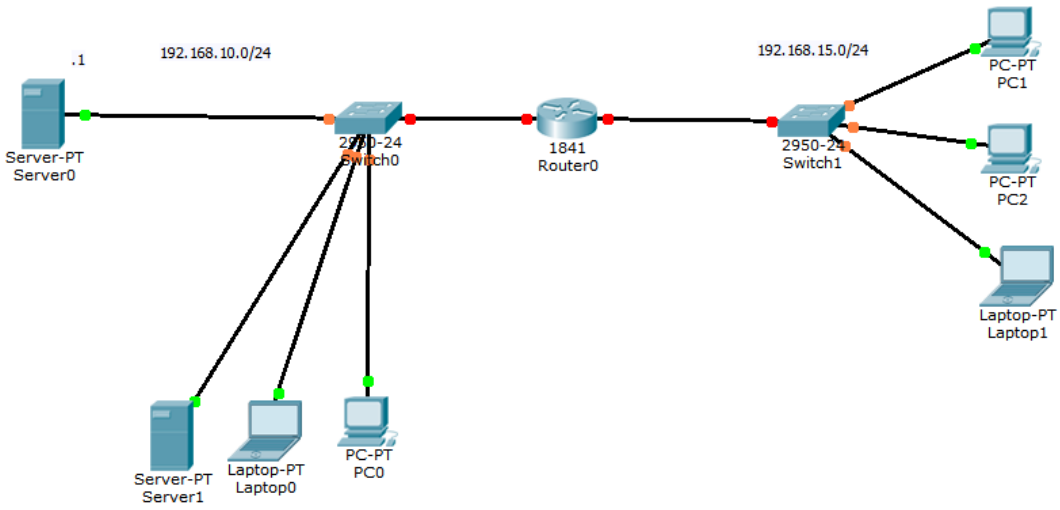


Рисунок 12. – Схема мережі для дослідження DHCP

Порядок виконання

1. Активуйте DHCP на Server0 та створіть пул для мережі 192.168.10.0/24.
2. Налаштуйте інтерфейс маршрутизатора в цій мережі на отримання параметрів через DHCP, якщо цього вимагає схема.
3. На другому інтерфейсі маршрутизатора задайте статичну адресу для мережі 192.168.15.0/24.
4. Створіть на маршрутизаторі DHCP-пул для другої мережі.
5. Виключіть із пулу адресу інтерфейсу маршрутизатора та інші статичні адреси.
6. На клієнтах увімкніть отримання адреси через DHCP.
7. Перевірте отримані параметри й зв’язок із шлюзом.

Основні команди

```
ip dhcp excluded-address <початкова> <кінцева>
ip dhcp pool <ім'я>
network <мережа> <маска>
default-router <IP шлюзу>
dns-server <IP DNS>
show ip dhcp binding
```

Контрольні питання

1. Для чого призначений DHCP?
2. Що таке DHCP-пул?
3. Які параметри може отримати клієнт через DHCP?
4. Навіщо виключати окремі адреси з пулу?
5. Які повідомлення утворюють послідовність DORA?
6. Як перевірити видані DHCP-адреси на маршрутизаторі?

Вимоги до звіту

– титульний аркуш із номером і темою роботи
– схема мережі та, за потреби, таблиця адресації
– основні команди або параметри налаштування
– результати перевірки (ping та відповідні show-команди)
– 2–3 скриншоти ключових етапів
– короткий висновок про отримані результати

ПРАКТИЧНА РОБОТА № 4
Налаштування технології NAT/PAT

Мета роботи

Набути практичних навичок налаштування NAT/PAT для доступу вузлів приватної IPv4-мережі до зовнішньої мережі.

Програмне та апаратне забезпечення

Cisco Packet Tracer 8.x або новіша доступна версія; віртуальні маршрутизатори Cisco ISR, комутатори Cisco Catalyst, ПК/Server-PT. За наявності — ПК з Windows/Linux для додаткової перевірки команд ping/tracert.

Очікувані результати

– розрізняти inside та outside інтерфейси
– створювати ACL для внутрішньої мережі
– налаштовувати PAT (NAT overload)
– перевіряти таблицю трансляцій NAT

Короткі 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).

Матеріали до виконання практичної роботи

Схему для дослідження NAT/PAT наведено на рисунку 13. у варіанті цієї роботи основну увагу приділено PAT (NAT overload).

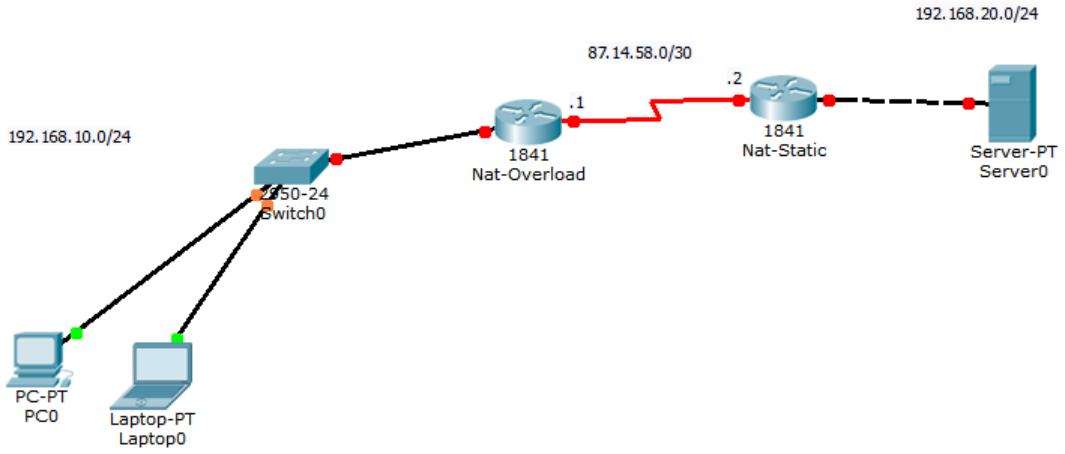


Рисунок 13. – Схема мережі для дослідження NAT/PAT

Порядок виконання

1. Налаштуйте адресацію кінцевих пристроїв та інтерфейсів маршрутизаторів відповідно до рисунка 13.
2. На граничному маршрутизаторі визначте внутрішній і зовнішній інтерфейси.

3. Створіть стандартний ACL для внутрішньої приватної мережі.
4. Налаштуйте PAT через зовнішній інтерфейс.
5. Створіть трафік із внутрішньої мережі до зовнішнього вузла.
6. Перевірте таблицю трансляцій NAT.

Основні команди

```
ip nat inside
ip nat outside
access-list 1 permit <мережа> <wildcard>
ip nat inside source list 1 interface <outside-interface> overload
show ip nat translations
show ip nat statistics
```

Контрольні питання

1. Для чого застосовується NAT?
2. Чим PAT відрізняється від статичного NAT?
3. Що означають ip nat inside та ip nat outside?
4. Навіщо під час PAT використовується ACL?
5. Якою командою переглянути активні трансляції NAT?

Вимоги до звіту

– титульний аркуш із номером і темою роботи
– схема мережі та, за потреби, таблиця адресації
– основні команди або параметри налаштування
– результати перевірки (ping та відповідні show-команди)
– 2–3 скриншоти ключових етапів
– короткий висновок про отримані результати

ПРАКТИЧНА РОБОТА № 5
Динамічна маршрутизація. Протокол RIPv2

Мета роботи

Дослідити принципи дистанційно-векторної маршрутизації та навчитися налаштовувати RIPv2 у мережі з кількома маршрутизаторами.

Програмне та апаратне забезпечення

Cisco Packet Tracer 8.x або новіша доступна версія; віртуальні маршрутизатори Cisco ISR, комутатори Cisco Catalyst, ПК/Server-PT. За наявності — ПК з Windows/Linux для додаткової перевірки команд ping/tracert.

Очікувані результати

– вмикати RIPv2 та оголошувати мережі
– використовувати no auto-summary
– аналізувати RIP-маршрути
– перевіряти наскрізну досяжність

Короткі теоретичні відомості

RIP — дистанційно-векторний протокол маршрутизації. Його метрика — кількість переходів; 15 — максимально допустиме значення, а 16 означає недосяжність. RIPv2 підтримує маски підмереж і передає оновлення через multicast.

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 рисунку 14.

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 42

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

Матеріали до виконання практичної роботи

У схемі використовуються мережі 192.168.10.0/24, 192.168.20.0/24 та транзитна мережа 8.8.8.0/30. Топологію наведено на рисунку 14. Для цієї практичної використовується RIPv2.

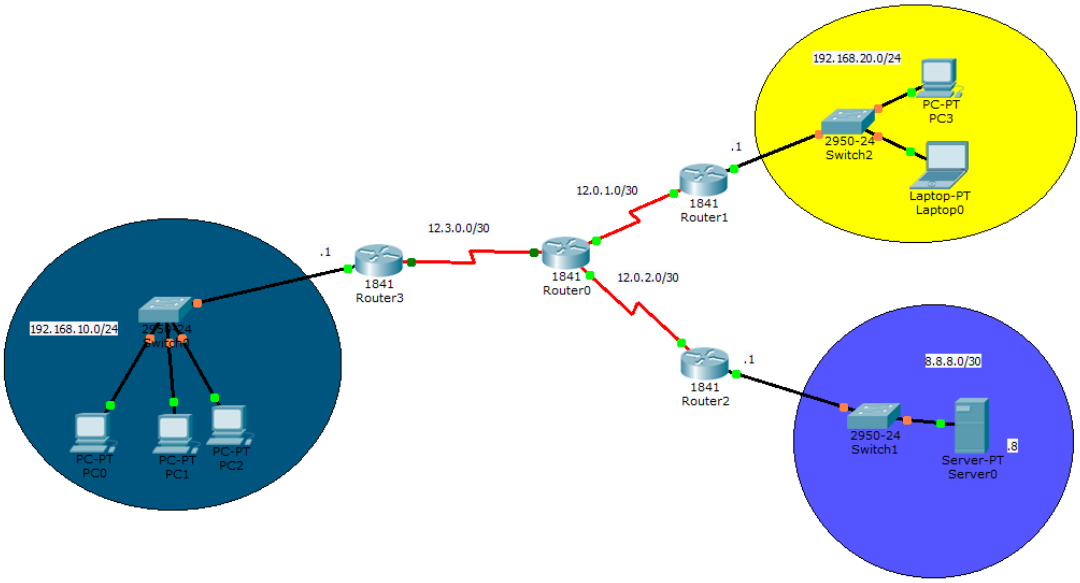


Рисунок 14. – Топологія мережі для налаштування RIPv2

Порядок виконання

1. Налаштуйте IP-адреси всіх LAN- і транзитних інтерфейсів відповідно до рисунка 14.
2. Перевірте зв’язок між безпосередньо підключеними вузлами.
3. На кожному маршрутизаторі увімкніть RIP версії 2.
4. Оголосіть безпосередньо підключені мережі та вимкніть автоматичне сумаризування.
5. Перевірте появу RIP-маршрутів у таблиці маршрутизації.
6. Виконайте ping між крайніми мережами.

Основні команди

```
router rip
version 2
no auto-summary
network <мережа>
show ip route rip
show ip protocols
```

Контрольні питання

1. Що таке динамічна маршрутизація?
2. Яка метрика використовується RIP?
3. Чим RIPv2 відрізняється від RIPv1?
4. Що означає метрика 16 у RIP?

5. Для чого застосовують no auto-summary?
6. Як у таблиці маршрутизації позначаються RIP-маршрути?

Вимоги до звіту

– титульний аркуш із номером і темою роботи
– схема мережі та, за потреби, таблиця адресації
– основні команди або параметри налаштування
– результати перевірки (ping та відповідні show-команди)
– 2–3 скриншоти ключових етапів
– короткий висновок про отримані результати

ПРАКТИЧНА РОБОТА № 6
Динамічна маршрутизація. Протокол OSPF

Мета роботи

Навчитися налаштовувати однозонний OSPF у Cisco IOS і перевіряти сусідство та маршрути.

Програмне та апаратне забезпечення

Cisco Packet Tracer 8.x або новіша доступна версія; віртуальні маршрутизатори Cisco ISR, комутатори Cisco Catalyst, ПК/Server-PT. За наявності — ПК з Windows/Linux для додаткової перевірки команд ping/tracert.

Очікувані результати

– вмикати OSPF з process ID
– оголошувати мережі через wildcard mask
– перевіряти OSPF neighbors
– аналізувати OSPF-маршрути та зв’язність

Короткі 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*). Мережі оголошують командою network із wildcard mask.

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 процесу]* – перейти в режим конфігурування протоколу OSPF;

- *network [IP-адреса зовнішньої мережі] [маска мережі] area [індекс мережі]* – додати мережу для обробки протоколом OSPF.

Router0:

Router>enable

Router#configure terminal

Router(config)#interface fastEthernet 0/0 48

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 49

Матеріали до виконання практичної роботи

Мережа містить кілька локальних сегментів і серверний сегмент; її топологію наведено на рисунку 15. 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.. У базовому варіанті використовується одна область – area 0.

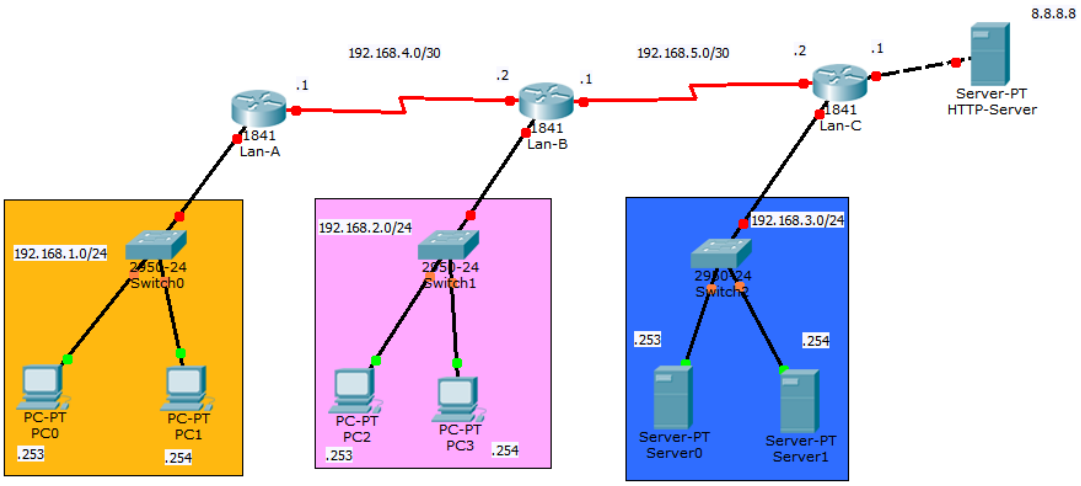


Рисунок 15. – Топологія мережі для налаштування OSPF

Порядок виконання

1. Налаштуйте IP-адреси та маски всіх інтерфейсів маршрутизаторів відповідно до рисунка 15.
2. Налаштуйте адреси, маски й шлюзи кінцевих вузлів.
3. На маршрутизаторах увімкніть процес OSPF.
4. Оголосіть потрібні мережі в area 0 за допомогою wildcard mask.
5. Перевірте формування сусідства OSPF.
6. Перевірте OSPF-маршрути та наскрізну досяжність.

Основні команди

```
router ospf 1
network <мережа> <wildcard> area 0
show ip ospf neighbor
show ip route ospf
show ip protocols
```

Контрольні питання

1. Чим протокол стану каналів відрізняється від дистанційно-векторного?
2. Яка метрика використовується OSPF?
3. Для чого потрібні hello-пакети?
4. Що таке area 0?
5. Як перевірити OSPF-сусідів?

6. Як у таблиці маршрутизації позначаються OSPF-маршрути?

Вимоги до звіту

– титульний аркуш із номером і темою роботи
– схема мережі та, за потреби, таблиця адресації
– основні команди або параметри налаштування
– результати перевірки (ping та відповідні show-команди)
– 2–3 скриншоти ключових етапів
– короткий висновок про отримані результати

ПРАКТИЧНА РОБОТА № 7
Маршрутизація з використанням протоколу EIGRP

Мета роботи

Набути практичних навичок налаштування EIGRP у Cisco IOS та перевірки сусідства і маршрутів.

Програмне та апаратне забезпечення

Cisco Packet Tracer 8.x або новіша доступна версія; віртуальні маршрутизатори Cisco ISR, комутатори Cisco Catalyst, ПК/Server-PT. За наявності — ПК з Windows/Linux для додаткової перевірки команд ping/tracert.

Очікувані результати

– налаштовувати EIGRP з однаковим номером AS
– оголошувати мережі
– перевіряти EIGRP neighbors
– аналізувати маршрути, позначені літерою D

Короткі 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, 53

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) (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 K 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).

```
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
```

Матеріали до виконання практичної роботи

Топологію мережі наведено на рисунку 16. Необхідно налаштувати EIGRP на маршрутизаторах з однаковим номером автономної системи, перевірити сформовані маршрути та, за можливості, дослідити роботу резервного шляху.

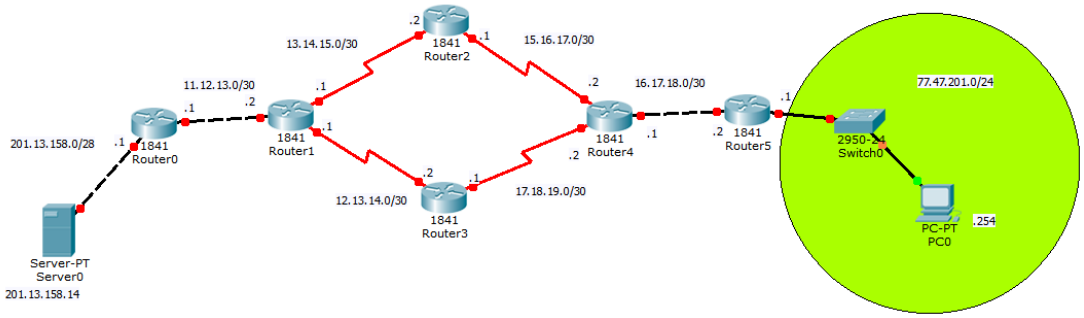


Рисунок 16. – Топологія мережі для налаштування EIGRP

Порядок виконання

1. Налаштуйте IP-адреси всіх інтерфейсів і кінцевих вузлів відповідно до рисунка 16.
2. На всіх маршрутизаторах увімкніть EIGRP з однаковим номером AS.
3. Оголосіть безпосередньо підключені мережі.
4. Вимкніть автоматичне сумаризування, якщо це потрібно для використовуваної версії IOS.
5. Перевірте таблицю сусідів EIGRP і таблицю маршрутизації.
6. Перевірте ping між крайніми мережами.
7. Додатково: відключіть активний шлях і перевірте, чи використовується резервний маршрут.

Основні команди

```
router eigrp <AS>
network <мережа> <wildcard>
no auto-summary
show ip eigrp neighbors
show ip eigrp topology
show ip route eigrp
```

Контрольні питання

1. Які особливості EIGRP?
2. Що таке номер автономної системи в EIGRP?
3. Який алгоритм використовує EIGRP?
4. Які параметри враховує метрика EIGRP?
5. Як перевірити EIGRP-сусідів?
6. Як у таблиці маршрутизації позначаються EIGRP-маршрути?

Вимоги до звіту

– титульний аркуш із номером і темою роботи
– схема мережі та, за потреби, таблиця адресації
– основні команди або параметри налаштування
– результати перевірки (ping та відповідні show-команди)
– 2–3 скриншоти ключових етапів
– короткий висновок про отримані результати

ПРАКТИЧНА РОБОТА № 8
Віртуальні локальні мережі (VLAN)

Мета роботи

Навчитися створювати VLAN, призначати access-порти, налаштовувати trunk і перевіряти логічну сегментацію мережі.

Програмне та апаратне забезпечення

Cisco Packet Tracer 8.x або новіша доступна версія; віртуальні маршрутизатори Cisco ISR, комутатори Cisco Catalyst, ПК/Server-PT. За наявності — ПК з Windows/Linux для додаткової перевірки команд ping/tracert.

Очікувані результати

– створювати VLAN і давати їм імена
– призначати access-порти
– налаштовувати 802.1Q trunk
– перевіряти членство портів і зв’язність усередині VLAN

Короткі 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 рисунку 17 показано приклад мережі із використанням технології VLAN.

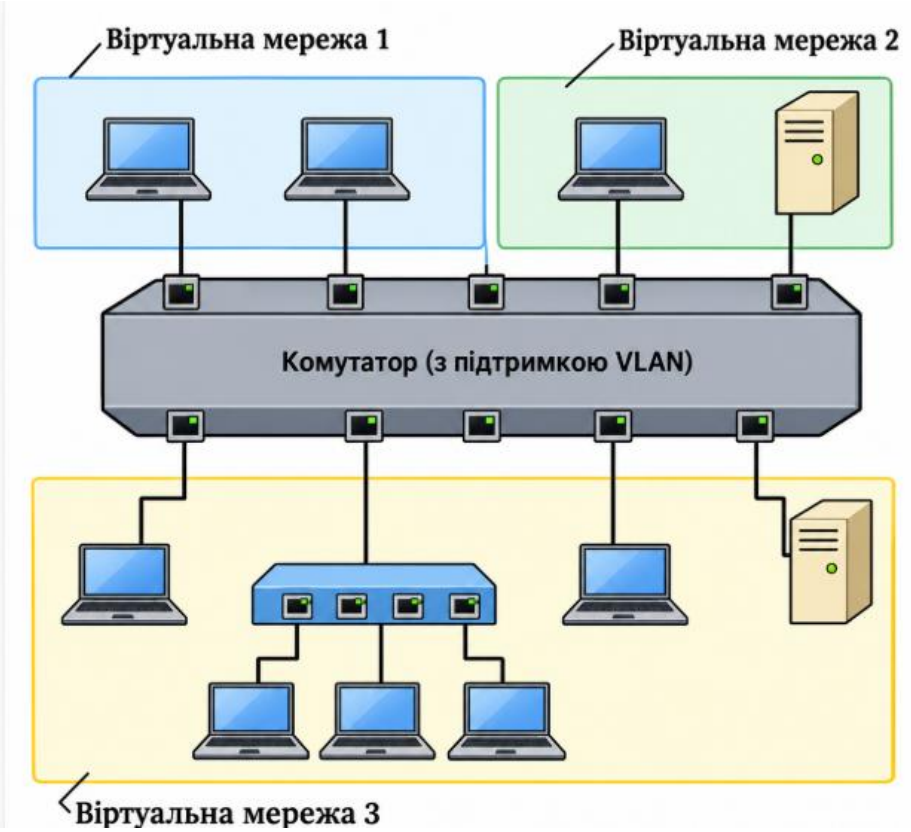


Рисунок 17. – Приклад реалізації мережі за технологією VLAN

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).

Матеріали до виконання практичної роботи

Вихідна схема на рисунку 18 містить кілька VLAN і маршрутизацію між ними. Для базового виконання достатньо налаштувати дві VLAN; третю VLAN зі схеми можна використати як додаткове завдання.

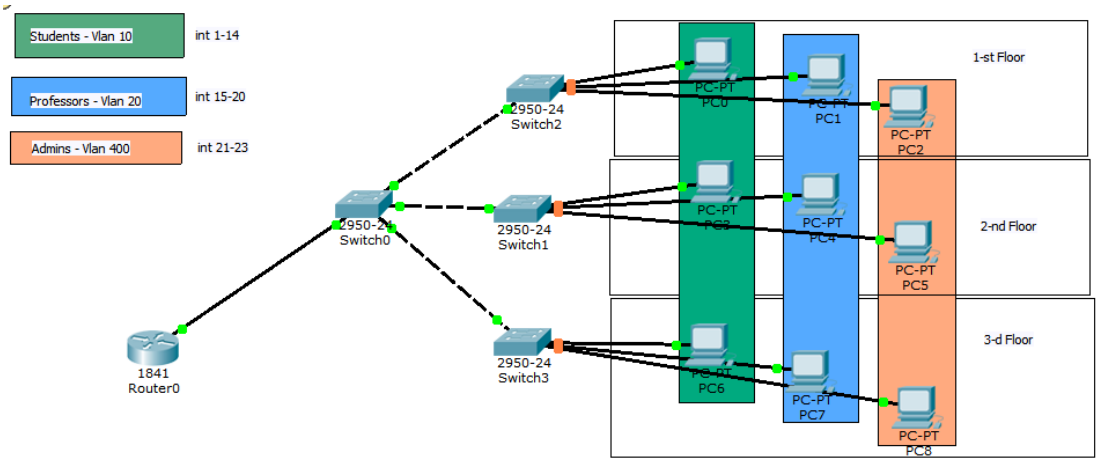


Рисунок 18. – Схема мережі з VLAN та міжвлановою взаємодією

Порядок виконання

1. Створіть на комутаторах VLAN 10 і VLAN 20. За бажанням додайте VLAN 400, яка присутня на рисунку 17.
2. Призначте порти кінцевих вузлів у відповідні VLAN як access-порти.
3. Між комутаторами налаштуйте trunk-порти.

4. Якщо потрібна міжвланова взаємодія, налаштуйте на маршрутизаторі підінтерфейси з encapsulation dot1Q.
5. Налаштуйте IP-адресацію кінцевих пристроїв.
6. Перевірте show vlan brief, show interfaces trunk та ping.

Основні команди

```
vlan 10
name VLAN10
interface <порт>
switchport mode access
switchport access vlan 10
switchport mode trunk
interface <інтерфейс>.<vlan>
encapsulation dot1Q <vlan>
```

Контрольні питання

1. Що таке VLAN?
2. Чим access-порт відрізняється від trunk-порту?
3. Для чого використовується IEEE 802.1Q?
4. Як створити VLAN на комутаторі Cisco?
5. Для чого потрібен пристрій третього рівня при обміні між VLAN?
6. Якою командою переглянути створені VLAN?

Вимоги до звіту

– титульний аркуш із номером і темою роботи
– схема мережі та, за потреби, таблиця адресації
– основні команди або параметри налаштування
– результати перевірки (ping та відповідні show-команди)
– 2–3 скриншоти ключових етапів
– короткий висновок про отримані результати

ВИМОГИ ДО ЗВІТІВ

Звіт про кожну практичну роботу включає тему, мету, завдання, схему топології й таблицю адресації (за потреби), фрагменти команд або налаштувань, результати перевірок (ping, tracert, show-команди), 2–3 показові скриншоти та короткий висновок. Файл проєкту Cisco Packet Tracer передається викладачеві у форматі .pkt.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Євсеєв С. П., Дженюк Н. В., Толкачов М. Ю., Король О. Г., Воропай Н. І. Комп'ютерні мережі. Книга 1. Технології комп'ютерних мереж : навч. посіб. Харків – Львів : Новий Світ – 2000, 2023. 471 с.

2. Мартинова О. П., Крайносвіт А. А., Романкевич О. М. Мережеві інформаційні технології : навчальний посібник для виконання лабораторних робіт. Київ : КПІ ім. Ігоря Сікорського, 2024. 128 с.

3. Данілова В. А., Шликов В. В. Телемедицина та комп'ютерні мережі : лабораторний практикум у Cisco Packet Tracer. Київ : КПІ ім. Ігоря Сікорського, 2021. 73 с.

4. Ролік О. І., Бойко О. В. Комп'ютерні мережі. Комп'ютерний практикум. Київ : КПІ ім. Ігоря Сікорського, 2025. 176 с.

5. Коваленко О. В., Коваленко А. С., Авраменко К. Д., Черкашин М. Ю. Комп'ютерні мережі. Лабораторні роботи. Кропивницький : ЦНТУ, 2025. 86 с.

6. Тарбаєв С. І., Домрачева К. О., Заїка В. Ф., Трембовецький М. П. Проектування інфокомунікаційних мереж : навч. посіб. Київ : ДУІКТ, 2019. 186 с.

7. Odom W. CCNA 200-301 Official Cert Guide. Volume 1. 2nd ed. Cisco Press, 2024. 944 p.

8. Odom W., Gooley J., Hucaby D. CCNA 200-301 Official Cert Guide. Volume 2. 2nd ed. Cisco Press, 2024. 752 p.

ОФІЦІЙНІ ІНФОРМАЦІЙНІ РЕСУРСИ

Cisco Networking Academy: https://www.netacad.com/

Cisco Packet Tracer: https://www.netacad.com/resources/lab-downloads?courseLang=en-US

Cisco Technical Documentation: https://www.cisco.com/c/en/us/support/index.html

IETF RFC Editor: https://www.rfc-editor.org/

DHCP (RFC 2131): https://www.rfc-editor.org/rfc/rfc2131

Traditional NAT (RFC 3022): https://www.rfc-editor.org/rfc/rfc3022

Wireshark User's Guide: https://www.wireshark.org/docs/wsug_html_chunked/