МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ МІСЬКОГО ГОСПОДАРСТВА імені О. М. БЕКЕТОВА

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

для проведення практичних занять
із навчальної дисципліни

«ПРОМИСЛОВІ КОМП'ЮТЕРНІ МЕРЕЖІ»

(для студентів другого (магістерського) рівня вищої освіти за спеціальністю 151 – Автоматизація та комп'ютерно-інтегровані технології за освітньо-професійною програмою «Системна інженерія»)

Харків
ХНУМГ ім. О. М. Бекетова
2021

Методичні рекомендації для проведення практичних занять із навчальної дисципліни «Промислові комп'ютерні мережі» (для студентів другого (магістерського) рівня вищої освіти за спеціальністю 151 – Автоматизація та комп'ютерно-інтегровані технології за освітньо-професійною програмою «Системна інженерія») / Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова ; уклад. : І. В. Білецький, Н. В. Шульга, Ю. В. Пахомов, Л. В. Піддубна. – Харків : ХНУМГ ім. О. М. Бекетова, 2021. – 136 с.

Укладачі: канд. техн. наук, доц. І. В. Білецький,
д-р пед. наук, доц. Н. В. Шульга,
канд. техн. наук, доц. Ю. В. Пахомов,
канд. філос. наук, доц. Л. В. Піддубна

Рецензент

О. В. Прохоров, д-р техн. наук, проф., професор кафедри комп'ютерних наук та інформаційних технологій Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут»

Рекомендовано кафедрою автоматизації та комп'ютерно-інтегрованих технологій, протокол № 5 від 25.12.2020

ЗМІСТ

ВСТУП

Дисципліна «Промислові комп'ютерні мережі» належить до циклу фахової підготовки студентів другого (магістерського) рівня вищої освіти за спеціальністю 151 – Автоматизація та комп'ютерно-інтегровані технології та відповідає освітньо-професійній програмі «Системна інженерія».

Основна мета дисципліни – підготовка кваліфікованих фахівців для проєктування та монтажу систем контролю та автоматики технологічних процесів на базі сучасних засобів та надання спеціальних знань для самостійної роботи у різних сферах міського господарства. Підготовлений фахівець повинен вміти створювати проєкти промислових комп'ютерних мереж, а саме:

– створювати графічну частину проєкту за допомогою сучасного програмного забезпечення;

– налаштовувати промислові комп'ютерні мережі для їх використання в сфері автоматизації технологічних процесів;

– працювати на професійному рівні зі спеціалізованими промисловими комп'ютерними мережами;

– самостійно складати програми автоматизованого розрахунку та побудови промислових комп'ютерних мереж.

Вивчання курсу повинно супроводжуватися виконанням практичних робіт і самостійною роботою.

Дисципліна «Промислові комп'ютерні мережі» призначена для вивчення основних принципів, методів та засобів побудови комп'ютерних мереж, зокрема структурної організації локальних та глобальних мереж, мереж з асинхронним режимом передавання інформації, архітектури мережевих операційних систем та мережевих технологій.

Практична частина курсу складається з тринадцяти практичних робіт і призначена для отримання практичних навичок використання існуючих мережевих технологій для побудови локальних і глобальних комп'ютерних мереж. Усі практичні роботи виконуються у програмному середовищі Cisco

Packet Tracer, яке призначено для побудови та моделювання інформаційно-обчислювальних мереж та оцінки їх технічних параметрів. Роботи послідовно логічно впорядковані за складністю та охоплюють всі теми, що вивчаються в курсі.

Матеріал для кожної практичної роботи містить мету, основні теоретичні відомості, загальне завдання, варіанти індивідуальних завдань, список питань для самоперевірки, зміст звіту про виконання лабораторних робіт, а також список рекомендованих інформаційних джерел для підготовки та виконання практичних робіт.

ПРАКТИЧНЕ ЗАНЯТТЯ № 1 ВИВЧЕННЯ МЕРЕЖЕВИХ УТИЛІТ WINDOWS

1.1 Мета роботи

Отримання навичок використання мережевих утиліт Windows для діагностики та налаштування локальної мережі й доступу до інтернету.

1.2 Необхідний теоретичний матеріал

Операційна система Windows має безліч допоміжних інструментів для діагностики та налаштування комп'ютера для роботи в локальній мережі й доступу до інтернет-ресурсів. Більшість із них призначені переважно для системних адміністраторів. Але деякі можуть стати в пригоді й звичайним користувачам. Ці інструменти є утилітами, що запускаються на виконання з командного рядка. Принцип командного рядка полягає в тому, що вона дозволяє виконувати завдання без допомоги графічного інтерфейсу Windows. Для обслуговування Windows досить часто доводиться запускати системні утиліти з командного рядка, при цьому іноді потрібно виконання завдань з правами адміністратора.

Доступ до командного рядка можна отримати різними способами.

Спосіб 1. У вікні пошуку ввести *cmd*. На результатах пошуку натиснути правою кнопкою миші і вибрати в контекстному меню *«Запуск від імені адміністратора».*

Спосіб 2. Натиснути комбінацію клавіш *Win* + *R*. У вікні ввести *cmd* і потім натиснути *ENTER*. Але в такому випадку ми не зможемо запуститися з правами адміністратора.

Спосіб 3 (за допомогою ярлика):

1. На робочому столі викликаємо контекстне меню правою клавішею миші, вибираємо пункт *«Створити»* → *«Ярлик»;*

2. У рядку розташування файлу пишемо *«cmd.exe»* і натискаємо *«Далі»,* потім *«Готово»;*

3. Клацаємо на створеному ярлику правою клавішею миші й вибираємо пункт *«Властивості»*;

4. У вікні властивостей клацаємо кнопку *«Додатково»;*

5. У вікні додаткових властивостей ставимо галочку *«Запуск від імені адміністратора»*, потім натискаємо «*ОК»*.

Тепер при запуску ярлика буде запускатися командний рядок «*Windows 7 з правами адміністратора»*.

Спосіб 4 (З меню програм): *Пуск → Всі програми → Стандартні.* Далі в списку програм знайти *«Командний рядок»*, клацнути правою клавішею та в контекстному меню вибрати *«Запуск від імені адміністратора»*.

Примітка. У ОС Windows 10 з'явилася спеціальна вкладка в контекстному меню для запуску від імені адміністратора. Перейшовши в режим командного рядка можна запускати на виконання різні команди контролю та діагностики мережі. Виконання цих команд реалізуються відповідними однойменними утилітами. Перелік мережевих утиліт, які підлягають вивченню на цьому практичному занятті, наведено нижче:

hostname – визначення імені комп'ютера в локальній мережі;

ipconfig – інструмент для перегляду підключень до мережі;

ping – команда для відправлення мережевих тестових пакетів за вказаною адресою;

tracert – визначення маршруту проходження пакетів по мережі;

netstat – статистика підключень до мережі;

IP-адреса складається з двох частин: номера мережі й номера вузла в мережі.

Найпоширенішим є запис IP-адреси у вигляді чотирьох чисел, розділених крапками, кожне з яких представляє значення байта в десятковій формі, наприклад: 213.180.204.11. Запис адреси не передбачає спеціального

розмежувального знака між номером мережі та номером вузла. Для поділу цих частин зазвичай використовується два підходи:

– за допомогою маски (*RFC 950, RFC 1518*), що становить число в парі з IP-адресою. За допомогою операції «логічне І» над цими двома числами виділяється номер мережі;

– за допомогою класів адрес (*RFC 791*).

Уводиться п’ять класів адресів: *A, B, C, D, E. A, B*. Клас *C* використовується для адресації мереж, *D* і *E* мають спеціальне призначення. Ознакою, на підставі якої IP-адресу відносять до того чи іншого класу, є значення декількох перших бітів адреси. У таблиці 1.1 поданий розподіл адрес в IP мережах.

Таблиця 1.1 – Розподіл адрес в IP-мережах

Клас	Перші біти	Найменший номер мережі	Найбільший номер мережі	Максимальна кількість вузлів в мережі
A	0	1.0.0.0 (0 – не використовується)	126.0.0.0 (127 – зарезервований)	2^{24} (3 байти)
B	10	128.0.0.0	191.255.0.0	2^{16} (2 байти)
C	110	192.0.0.0	223.255.255.0	2^{8} (1 байт)
D	1110	224.0.0.0	239.255.255.255	групові адреси
E	11110	240.0.0.0	247.255.255.255	зарезервований

У межах IP-протоколу існують обмеження при призначенні IP-адрес, а саме:

– номери мереж і номери вузлів не можуть складатися з довічних нулів або одиниць;

– якщо IP-адреса складається тільки з двійкових нулів, то вона називається невизначеною адресою та позначає адресу того вузла, який згенерував цей пакет;

– якщо в поле номера мережі стоять тільки нулі, то за замовчуванням вважається, що вузол призначення належить тій самій мережі, що й вузол, який

відправив пакет; таку адресу можна використовувати тільки як адресу відправника;

– якщо всі двійкові розряди IP-адреси рівні 1, то пакет із такою адресою призначення повинен розсилатися всім вузлам, що знаходяться в тій самій мережі, що й джерело цього пакета; така адреса називається обмеженою широкомовною, оскільки пакет не зможе вийти за межі мережі;

– якщо в полі адреси призначення в розрядах, відповідних номеру вузла, стоять тільки одиниці, то пакет розсилається всім вузлам мережі, номер якої зазначений в адресі призначення; такий тип адреси називається широкомовним;

– якщо перший октет адреси дорівнює 127, то така адреса називається внутрішньою адресою стека протоколів; він використовується для тестування програм, організації клієнтської та серверної частин додатків, встановлених на одному комп'ютері;

– групові адреси, що належать до класу D, призначені для економічного поширення в інтернеті, великої корпоративної мережі аудіо- або відеопрограм.

Стандартним класам мереж можна поставити у відповідність такі значення маски:

клас A – 255.0.0.0;

клас B – 255.255.0.0;

клас C – 255.255.255.0.

Ipconfig – це утиліта командного рядка для виводу деталей поточного з'єднання та контролю над клієнтськими сервісами *DHCP* і *DNS*. Виводиться інформація про всі мережеві підключення, в яких містяться IP-адреса, маска підмережі й IP-адреса шлюзу.

У підключень по локальній мережі, які не використовуються для виходу в інтернет, адреса шлюзу може бути відсутньою. Якщо комп'ютер має пряме підключення до інтернету, то відображена адреса збігається з адресою комп'ютера в інтернеті. Якщо ж комп'ютер підключений через маршрутизатор, то відображається внутрішня адреса пристрою в локальній мережі.

Параметри утиліти *IPCONFIG* (довідково):

ipconfig [/all] [/renew [адаптер]] [/release [адаптер]] [/flushdns] [/displaydns] [/registerdns] [/showclassid адаптер] [/setclassid адаптер [код класу]], де */all* – виведення повної конфігурації *TCP/IP* для всіх адаптерів. Без цього параметра команда *ipconfig* виводить тільки IP-адреси, маски підмережі й основний шлюз для зазначеного в параметрах адаптера. Адаптери можуть являти собою фізичні інтерфейси, такі як встановлені мережеві адаптери, або логічні інтерфейси, такі як підключення віддаленого доступу;

/renew [адаптер] – оновлення конфігурації *DHCP* для всіх адаптерів (якщо адаптер не заданий) або для заданого адаптера. Ця опція доступна тільки на комп'ютерах з адаптерами, налаштованими для автоматичного отримання IP-адрес. Щоб вказати адаптер, введіть без параметрів ім’я, виведене командою ipconfig;

/release [адаптер] – відправлення повідомлення *DHCP RELEASE* сервера *DHCP* для звільнення поточної конфігурації *DHCP* і видалення конфігурації IP-адрес для всіх адаптерів (якщо адаптер не заданий) або для заданого адаптера. Цей адаптер відключає протокол *TCP/IP* для адаптерів, які налаштовані на автоматичне отримання IP-адрес. Щоб вказати адаптер, уведіть без параметрів ім’я, яке виведене командою *ipconfig*;

/flushdns – скидання та очищення вмісту кеша зіставлення імен DNS-клієнта. Під час усунення неполадок *DNS* цю процедуру використовують для видалення з кешу записів негативних спроб зіставлення та інших динамічно доданих записів;

/displaydns – відображення вмісту кеша зіставлення імен *DNS*-клієнта, що включає записи, попередньо завантажені з локального файлу *Hosts*, а також останні отримані записи ресурсів для запитів на зіставлення імен. Ця інформація використовується службою *DNS*-клієнта для швидкого зіставлення імен, що часто зустрічаються, без звернення до вказаних у конфігурації *DNS*-серверів;

/registerdns – динамічна реєстрація вручну імен *DNS* і IP-адрес, налаштованих на комп’ютері. Цей параметр корисний при усуненні неполадок у разі відмови в реєстрації імені *DNS* або при з’ясуванні причин неполадок

динамічного оновлення між клієнтом і *DNS*-сервером без перезавантаження клієнта. Імена, зареєстровані в *DNS*, визначаються параметрами *DNS* у додаткових властивостях протоколу *TCP/IP*;

/showclassid адаптер – відображення коду класу *DHCP* для зазначеного адаптера. Щоб переглянути код класу *DHCP* для всіх адаптерів, замість параметра адаптер вкажіть зірочку (*). Ця опція доступна тільки на комп'ютерах з адаптерами, налаштованими для автоматичного отримання IP-адрес;

/setclassid адаптер [код_класса] – задання коду класу *DHCP* для зазначеного адаптера. Щоб задати код класу *DHCP* для всіх адаптерів, замість параметра адаптер вкажіть зірочку (*). Ця опція доступна тільки на комп'ютерах з адаптерами, які налаштовані на автоматичне отримання IP-адрес. Якщо код класу *DHCP* не заданий, поточний код класу видаляється.

Утиліта *ipconfig* дозволяє також з'ясувати ініціалізацію конфігурації та дублювання IP-адрес:

– якщо конфігурація ініціалізована, то з'являється IP-адреса, маска, шлюз;

– якщо IP-адреса дублюється, то *маска мережі буде 0.0.0.0;*

– якщо при використанні динамічних IP-адрес комп'ютер не зміг отримати IP-адресу, то *вона буде 0.0.0.0.*

Команда *ping* призначена для перевірки з'єднань у мережах на основі протоколу *TCP/IP*. За цією командою відправляється ехо-запит за протоколом *ICMP* на ім'я або IP-адресу зазначеного хоста, і фіксує час отримання відповіді. За її допомогою можна визначити наявність певної адреси призначення, якість зв'язку з точки зору втрати переданої інформації та часу затримки.

Для використання команди введіть у командному рядку *ping* «ім'я хоста» і натиснути клавішу *Enter*, де замість «ім'я хоста» потрібно вказати доменне ім'я або IP-адресу комп'ютера (наприклад *ping yandex.ru*). Результат роботи команди буде містити інформацію про адресу комп'ютера, що пінгується, кількості

переданої інформації та часу відповіді, а також статистичну (сумарну) інформацію за всіма відправленими пакетами.

Протокол керувальних повідомлень *ICMP* (*Internet Control Message Protocol*) використовується для обміну службовою та діагностичною інформацією в мережі.

Команда *ping* дозволяє виконати відправлення керувального повідомлення типу *Echo Request* (тип дорівнює 8 і вказується в заголовку *ICMP*-повідомлення) вузлу й інтерпретувати отриману від нього відповідь у зручному для аналізу вигляді. У полі даних ICMP-пакету, що відправляється, зазвичай містяться символи англійського алфавіту. У відповідь на такий запит, опитуваний вузол повинен відправити ICMP-пакет із тими самими даними, які були прийняті, і типом повідомлення *Echo Reply* (код типу в *ICMP*-заголовку дорівнює *0*). Якщо при обміні ICMP-повідомленнями виникає якась проблема, то утиліта *ping* виведе інформацію для її діагностики.

Формат командного рядка:

ping [-t] [-a] [-n число] [-l розмір] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j список вузлів] | [-k список вузлів]] [-w таймаут] – ім’я отримувача, де *t* – безперервне відправлення пакетів. Для завершення й виведення статистики використовуються комбінації клавіш *Ctrl* + *Break* (вивід статистики та продовження), і *Ctrl* + *C* (вивід статистики і завершення);

a – визначення імені вузла за його адресою;

n (число) – число ехо-запитів, що відправляються;

l (розмір) – розмір поля даних у байтах запиту, що відправляється;

f – встановлення прапору, фрагментацію пакету, що забороняється;

TTL – встановлення терміну життя пакета (поле *«Time To Live»*);

R, (число) – запис маршруту для вказаного числа переходів;

j, (список вузлів) – вільний вибір маршруту по списку вузлів;

к, (список вузлів) – жорсткий вибір маршруту по списку вузлів;

w, таймаут – максимальний час очікування кожної відповіді в мілісекундах.

Приклади використання:

ping google.com – exo-запит до вузла з іменем *google.com i*з параметрами за замовчуванням, де кількість пакетів сиановить 4, довжина масива даних = 32 байта;

ping - a 192.168.1.50 – виконати пінг із визначенням імені кінцевого вузла на його адресу;

ping -w 5000 ya.ru – пінг с таймаутом очікування рівним 5 с (за замовчуванням – 4 с);

ping -n 5000 -l 1000 ab57.ru – опит вузла *ab57.ru 5000 раз*, пакетами с даними довжиною в 1000 байт. Допустима максимальна довжина даних – 65500;

ping -n 1 - l 3000 -f ya.ru – пінг с забороною фрагментації пакета;

ping -n 1 -r 3 ya.ru – відправити один ехо-запит на вузол *ya.ru* з відображенням перших трьох переходів по маршруту;

ping -i 5 ya.ru – пінг з указанням часу життя *TTL* = 5. Якщо для досягнення кінцевого вузла буде потрібно більша кількість переходів по маршруту, то маршрутизатор, який перервав доставку відповість повідомленням «*Перевищено термін життя (TTL), при передачі пакета»*.

За умовчуванням, за командою *ping* відправляється чотири невеликих пакети з довільними даними, в результаті роботи виводяться результати доставки кожного пакету та загальна статистика. Найперше *ping* виводить IP-адресу для запитуваного вузла. «*Затримка»* – час, за який пакет дійшов до вузла й повернувся назад. Необхідно пам’ятати, що «*Затримка»* включає не тільки час проходження запиту по мережі, але й час його обробки одержувачем. Тобто велике значення затримки може бути спричинено як завантаженістю мережі, так і завантаженістю вузла.

Ping також дозволяє перевірити за допомогою *TTL* кількість переходів (стрибків, хопів), які залишилися у пакета при поверненні. При проходженні кожного маршрутизатора *TTL* зменшується на 1. Знаючи його значення у відповідального вузла (зазвичай 32, 64, 128, 256), можна обчислити кількість пройдених маршрутизаторів.

Команда *tracert* призначена для визначення маршруту, по якому доставляється інформація за вказаною адресою. За її допомогою можна визначити, через які сегменти мережі передається інформація і, в разі відсутності зв'язку з зазначеним комп'ютером, визначити місце «розриву». Для трасування маршруту потрібно ввести в командному рядку *tracert «ім'я хосту»* і натиснути клавішу *Enter*, де замість *«ім'я хосту»* вказати доменне ім'я або IP-адресу комп'ютера (наприклад *tracert kharkov.ua*). У наслідок цього у командному рядку з'явиться список вузлів у вигляді часу відгуку (пінгу) і IP-адреси, через які проходять інтернет-пакети при доставці до місця призначення.

Команда *netstat* відображає інформацію про активні інтернет-підключення та відкриті порти на комп'ютері. Для перегляду інформації слід ввести у командному рядку *netstat -a* і натиснути клавішу *Enter*. Після виконання команди в командному рядку відобразиться інформація про активні підключених у вигляді використовуваного протоколу, локальної IP-адреси та порту, віддаленої IP-адреси й порту, а також стан підключення. Якщо на комп'ютері є відкриті порти, то команда виведе інформацію за ними.

Синтаксис (деякі параметри знехтувані):

netstat[-a] [-e] [-n] [-o] [-pProtocol] [-r] [-s] [Interval],

де *a* – відображення всіх активних з'єднань по протоколам *TCP* і *UDP*, а також списку портів, які очікують вхідні з'єднання (слухаючих портів);

b – відображення всіх активних з'єднань за протоколами *TCP* і *UDP*, а також списку портів, які очікують вхідні з'єднання (слухаючих портів) з інформацією про імена виконуваних файлів. Цей параметр застосуємо для операційних систем Windows XP і старше;

e – відображення статистики *Ethernet* у вигляді лічильників прийнятих і відправлених байт і пакетів;

n – відображення номерів портів у вигляді десяткових чисел;

o – відображення з'єднань, зокрема ідентифікатор процесу (*PID*) для кожного з'єднання;

r – відображення таблиці маршрутів. Еквівалент команди *route print*;

Interval – інтервал оновлення інформації, що відображається в секундах;

v – відображати детальну інформацію;

/? – відобразити довідку щодо використання *netstat*.

Приклади:

netstat -a | more – відобразити всі з'єднання в посторінковому режимі виведення на екран;

netstat -a > C:\netstatall.txt – відобразити всі з'єднання із записом результатів у файл *C: \ netstatall.txt*;

netstat -a | «find/I LISTENING» – відобразити всі з'єднання зі статусом *LISTENING*. *Ключ/I* у команді *find* вказує, що при пошуку тексту не потрібно враховувати регістр символів;

netstat -a | find/I «listening» > C:\listening.txt – відобразити всі з'єднання зі статусом *LISTENING* із записом результатів у файл *C:\listening.txt*.

1.3 Порядок виконання роботи

Завдання 1. Освоїти всі чотири способи виклику командного рядка.

Завдання 2. Використовуючи утиліту *hostname* – визначити ім'я вашого комп'ютера. Здається без параметрів.

Завдання 3. Вивчити утиліту *ipconfig* і продемонструвати її застосування без параметрів, із параметрами. Пояснити отримані результати.

Порядок дій:

– вивести основну конфігурацію протоколу TCP/IP для всіх адаптерів, уведіть: *ipconfig*;

– вивести повну конфігурацію TCP/IP для всіх адаптерів, уведіть: *ipconfig/all*;

– оновити конфігурацію IP-адреси, призначеної *DHCP*-сервером, тільки для адаптера *«Підключення по локальній мережі»,* введіть: *ipconfig/renew «Підключення по локальній мережі»*;

– скинути кеш зіставлення імен *DNS* за наявності несправностей у зіставленні імен, уведіть: *ipconfig/flushdns.*

Завдання 4. Освоїти роботу з командою *ping*. Придумати та реалізувати осмислене застосування команди *ping* із використанням перерахованих параметрів.

Завдання 5. Освоїти роботу з командою *tracert*. Визначити *«відстань»* до вибраних хостів мережі як усередині локальної мережі, так і за її межами.

Завдання 6. Освоїти роботу з командою *netstat*.

1.4 Звіт про виконання роботи

1. Сформувати запити з використанням описаних параметрів, отримати та прокоментувати результати.

2. Усі запити й результати повинні бути представлені на скріншотах із необхідними поясненнями.

3. Висновки за роботою.

1.5 Контрольні питання

1. Поясніть структуру IP-адреси на прикладі.

2. Яке призначення утиліти *ipconfig*?

3. Поясніть призначення команди *ping*.

4. Поясніть призначення команди *tracert*.

5. Поясніть призначення команди *netstat*.

ПРАКТИЧНЕ ЗАНЯТТЯ № 2 ЗНАЙОМСТВО З ПРОГРАМНИМ СЕРЕДОВИЩЕМ CISCO PACKET TRACER

2.1 Мета роботи

Вивчення інтерфейсу програми та отримання навичок роботи в програмному середовищі Cisco Packet Tracer.

2.2 Необхідний теоретичний матеріал

Комп'ютерна мережа (*computer network*) – становить єдину систему, в якій комп'ютери підключені для здійснення спільного обміну інформацією та ресурсами, за допомогою використання каналів зв'язку.

Канал зв'язку складається загалом із фізичного середовища, по якому передаються інформаційні сигнали, апаратури передачі даних і проміжної апаратури. Синонімом терміна *«канал зв'язку»* (*channel*) є термін *«лінія зв'язку» (line).*

Залежно від фізичного середовища передачі даних лінії зв'язку можна розділити так:

– провідні лінії зв'язку без ізолювальних і екранувальних обплетень;

– кабельні, де для передачі сигналів використовуються такі лінії зв'язку як кабелі «вита пара», коаксіальні або оптоволоконні кабелі;

– бездротові (радіоканали наземного та супутникового зв'язку), що використовують для передачі сигналів, електромагнітні хвилі, які розповсюджуються в просторі.

Cisco *Packet Tracer* – це емулятор мережі, створений компанією «*Cisco»*. Програма дає змогу будувати й аналізувати мережі на різноманітному обладнанні компанії «*Cisco»* в довільних топологіях із підтримкою різних протоколів.

Користувач отримує можливість вивчати роботу різних мережевих пристроїв: маршрутизаторів, комутаторів, точок бездротового доступу, персональних комп'ютерів, мережевих принтерів тощо.

Крім виконання завдань конфігурації мережі й емулювання налаштування мережевого обладнання, програма дозволяє промоделювати функціонування отриманої конфігурації мережі й перевірити певною мірою її працездатність.

Програма має безкоштовні версії, легко встановлюється та має простий і зручний інтерфейс. Недоліком можна вважати те, що вона містить у своєму арсеналі мережевого обладнання виключно вироби компанії «*Cisco*». Програма однак, є хорошим тренажером для отримання навичок роботи з мережевим обладнанням при налаштуванні мережі та дозволяє акцентувати увагу на безлічі важливих моментів, із якими можуть зіткнутися початківці-мережевики.

Будемо розглядати *Cisco Packet Tracer* версії 6.2, хоча вже доступна новіша версія 7.2. Після запуску відкривається головне вікно програми (рис. 2.1).

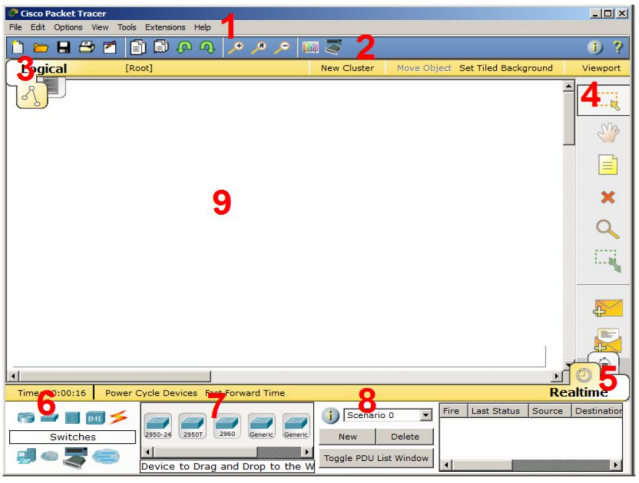

Рисунок 2.1 – Інтерфейс програми

Головне вікно умовно можна розподілити на такі зони:

1. Головне меню програми.
2. Панель інструментів – дублює деякі пункти меню.
3. Перемикач між логічною та фізичною організацією.

4. Ще одна панель інструментів, містить інструменти виділення, видалення, переміщення, масштабування об’єктів, а також саме формування довільних пакетів.

5. Перемикач між реальним режимом (*Real-Time*) і режимом симуляції.

6. Панель з групами кінцевих пристроїв і ліній зв’язку.

7. Самі кінцеві пристрої, тут містяться всілякі комутатори, вузли, точки доступу, провідники.

8. Панель створення призначених для користувача сценаріїв.

9. Робоча область.

У робочій області можна розміщувати різні мережеві пристрої, з’єднувати їх різними способами та внаслідок цього отримувати найрізноманітніші мережеві топології.

Зверху, над робочою областю, розташована головна панель програми та її меню. Меню дозволяє виконувати збереження, завантаження мережевих топологій, налаштування симуляції, а також багато інших цікавих функцій. Головна панель містить найчастіше використовувані функції меню (рис. 2.2).

Рисунок 2.2 – Головне меню *Packet Tracker*

Праворуч від робочої області розташована бічна панель, яка містить ряд кнопок, що відповідають за переміщення полотна робочої області, видалення об’єктів тощо. Знизу, під робочою областю, розташована панель обладнання (рис. 2.3).

Рисунок 2.3 – Панель обладнання

Маршрутизатори (роутери) використовуються для пошуку оптимального маршруту передачі даних на підставі алгоритмів маршрутизації.

Комутатори – пристрої, призначені для об'єднання декількох вузлів у межах одного або декількох сегментах мережі. Комутатор (*світч*) передає пакети інформації на підставі таблиці комутації, тому трафік йде тільки на ту *MAC*-адресу, якій він призначається, а не повторюється на всіх портах, як на концентраторі (хабі).

Бездротові пристрої в програмі представлені бездротовим маршрутизатором і трьома крапками доступу. Серед кінцевих пристроїв представлені *ПК*, ноутбук, сервер, принтер, телефони тощо. Інтернет у програмі представлений у вигляді хмар і модемів *DSL*.

Окремого розгляду заслуговують типи з'єднань (рис. 2.4).

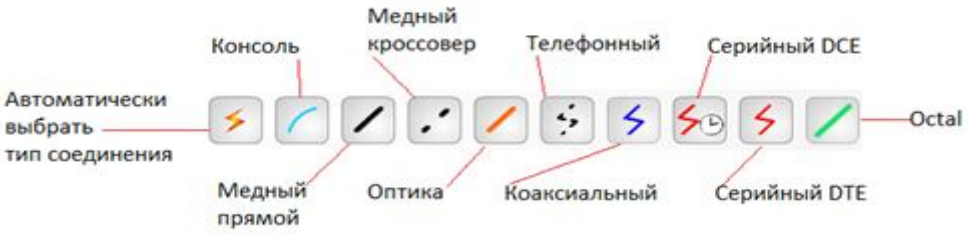

Рисунок 2.4 – Типи з'єднань

Можливий вибір таких з'єднань:

Автоматичний тип – при цьому типі з'єднання *Packet Tracer* автоматично вибирає найслушніший тип з'єднання для обраних пристроїв.

Консоль – консольні з'єднання. Консольне з'єднання може бути виконане між ПК і маршрутизаторами або комутаторами.

Мідь прямий – з'єднання мідним кабелем типу вита пара, обидва кінці кабелю обтиснуті в однаковій розкладці. Використовується для з'єднання різнорівневих пристроїв (*ПК*-концентратор (комутатор), комутатор-маршрутизатор).

Мідь перехресний (кросовер) – з'єднання мідним кабелем типу вита пара, кінці кабелю обтиснуті за перехресною схемою). Використовується для

з’єднання однорівневих пристроїв (ПК-ПК, концентратор-концентратор, маршрутизатор-маршрутизатор).

Оптика – з’єднання за допомогою оптичного кабелю, необхідно для з’єднання пристроїв, що мають оптичні інтерфейси.

Телефонний кабель – кабель для підключення телефонних апаратів. З’єднання через телефонну лінію може бути здійснено між пристроями, що мають модемні порти, наприклад, ПК мають можливість з’єднання з мережевою хмарою.

Коаксіальний кабель – з’єднання пристроїв за допомогою коаксіального кабелю. Використовується для з’єднання між кабельним модемом і хмарою.

Серійний DCE і серійний DTE – з’єднання через послідовні порти для зв’язку з інтернет-провайдером і виходу в інтернет або іншу *WAN*.

Елементи анімації та симуляції зображені на рисунку 2.5.

Рисунок 2.5 – Елементи анімації та симуляції

Інструменти *Add Simple PDU* (додати простий *PDU*, клавіша *P*) і *Add Complex PDU (*додати комплексний *PDU*, клавіша *C)* призначені для емуляції відправлення пакета з подальшим відстеженням його маршруту й даних усередині пакету.

Якщо клацнути на будь-якому вибраному елементі мережі, відкриється вікно, яке показує зовнішній вигляд пристрою, список модулів, які можна підключити до пристрою, закладка *Config* з описом поточної конфігурації,

закладка *Desktop* (для інших видів обладнання – *CLI (Command Line Interface))* для введення команд управління пристроєм.

Для зміни комплектації обладнання необхідно відключити його живлення, клікнувши мишкою на кнопці живлення й перетягнути мишею потрібний модуль у вільний слот, потім знову включити живлення (рис. 2.6).

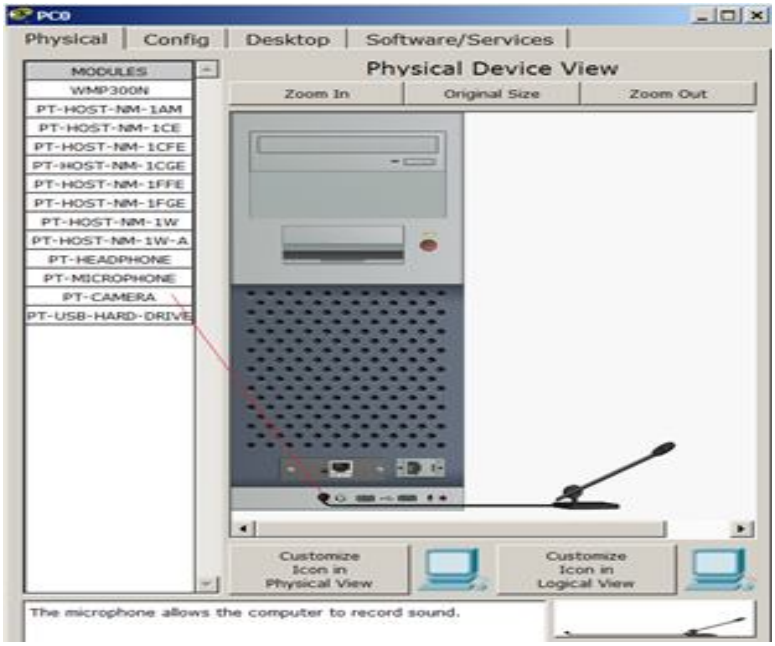

Рисунок 2.6 – Фізична конфігурація ПК

Як приклад, на малюнку доданий у фізичну конфігурацію ПК мікрофон *(PT-MICROPHONE)*, унаслідок чого ПК змінив свій значок у програмі (рис. 2.7).

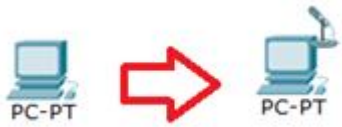

Рисунок 2.7 – Підключення мікрофона

Таким чином, у даному розділі були розглянуті теоретичні питання стосовно використання програмного середовища *Cisco Packet Tracer*. Програма дозволяє промоделювати функціонування отриманої конфігурації мережі й перевірити певною мірою її працездатність.

2.3 Приклади розв’зання задач

Приклад 1. Створення мережі з двох *ПК* у програмі *Cisco Parket Tracer.*

Як приклад, для початкового знайомства з програмою, побудуємо найпростішу мережу з двох *ПК*, з’єднаних крос-кабелем (рис. 2.8).

Рисунок 2.8 – Мережа з двох ПК

Для розв’язання цієї задачі на вкладці *END Devices* (Кінцеві пристрої) вибираємо тип комп’ютера та переносимо мишею в робочу область програми два примірника вибраного пристрою *(PC0 і PC1)* (рис. 2.9).

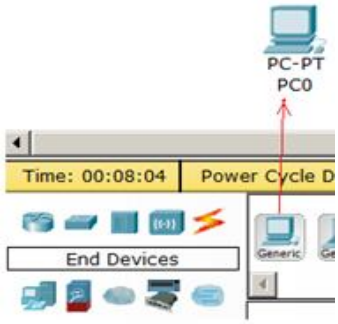

Рисунок 2.9 – Вибір типу комп’ютера

Комп’ютери з’єднуємо за допомогою *мідного кросовера*. Якщо при виборі кросовера зелені лампочки не засвітяться, то виберіть тип з’єднання автоматично.

Тепер розпочнемо налаштовувати лівий ПК: клацаємо на ньому мишею, переходимо на вкладку *IP Configuration* (Налаштування IP) (рис. 2.10).

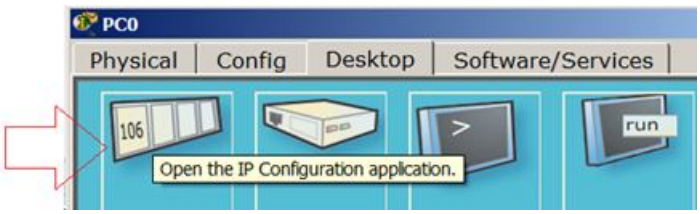

Рисунок 2.10 – Вкладка IP Configuration (Налаштування IP)

Для першого ПК вводимо *IP-адресу 192.168.1.1* і маску підмережі *255.255.255.0*, вікно закриваємо (рис. 2.11). Аналогічно налаштовуємо другий ПК на *адресу 192.168.1.2* і ту саму маску (рис. 2.11).

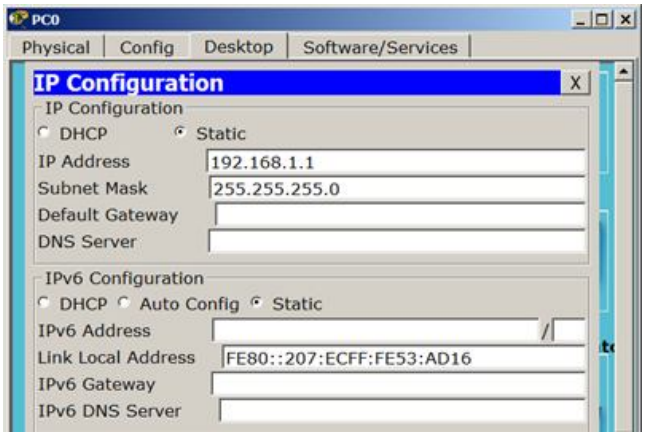

Рисунок 2.11 – Вікно настройки мережевих параметрів ПК

Далі перевіримо наявність зв'язку ПК і переконаємося, що ПК0 і ПК1 бачать один одного. Для цього на вкладці *Desktop* (Робочий стіл) перейдемо в поле *run* (Командний рядок) (рис. 2.12) і пропінгуємо сусідній ПК (рис. 2.13).

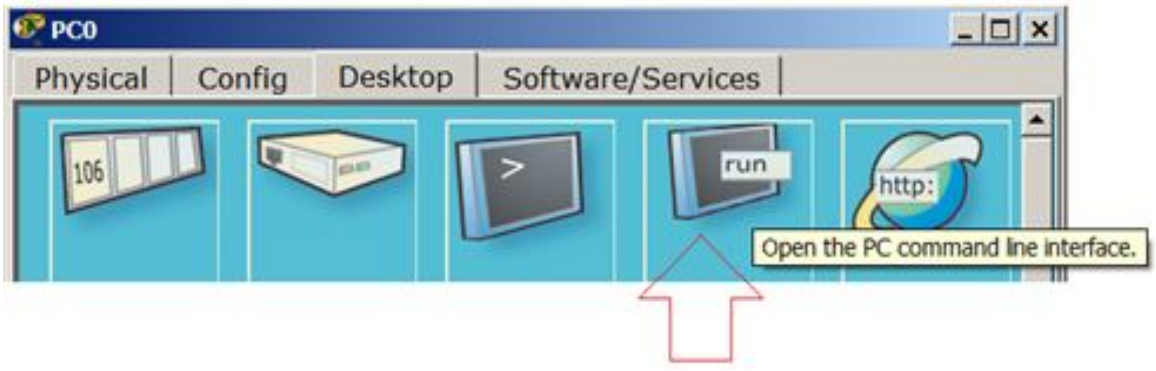

Рисунок 2.12 – Кнопка RUN

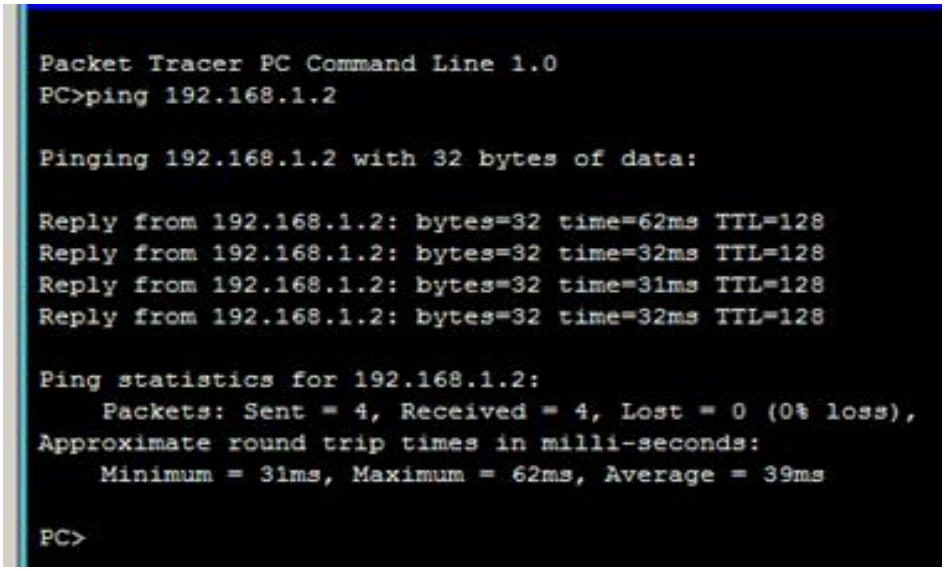

Рисунок 2.13 – *Ping* виконаний успішно

2.4 Звіт про виконання завдання

1. Звіт із практичного завдання повинен бути оформлений відповідно до загальноприйнятих правил оформлення практичних робіт і містити такі пункти:

– тема роботи;

– мета роботи;

– опис перебігу виконання роботи.

2. Вивчити теоретичний матеріал і інтерфейс програми.

3. Виконати наведені приклади з метою отримання навичок роботи з програмою.

4. Для кожного завдання описати процес його виконання з проміжними рисунками та скріншотами.

Контрольні питання

1. Поясніть структуру й елементи комп’ютерної мережі.

2. Поясніть призначення програми *Cisco Packet Tracer*.

3. Охарактеризуйте обладнання, яке доступно для проєктування комп’ютерних мереж за допомогою програми *Cisco Packet Tracer*.

4. Які типи з’єднань доступні у цій програмі?

5. Охарактеризуйте елементи анімації та симуляції.

ПРАКТИЧНЕ ЗАНЯТТЯ № 3 СТВОРЕННЯ ТА НАЛАШТУВАННЯ ЛОКАЛЬНИХ МЕРЕЖ

3.1 Мета роботи

Отримання навичок створення та налаштування різних конфігурацій локальної мережі з використанням програми *Cisco Packet Tracer*.

3.2 Необхідний теоретичний матеріал

Сегмент мережі – логічно або фізично відокремлена частина мережі. Характер і ступінь сегментації мережі залежить від природи мережі та пристроїв, що використовуються для з'єднання кінцевих станцій.

Розбиття мережі на сегменти переважно використовується з метою оптимізації мережевого потоку і/або збільшення рівня захищеності мережі загалом.

Зазвичай фізичний сегмент мережі обмежений мережевим пристроєм, що забезпечує з'єднання вузлів сегмента з іншою мережею. Для цього використовуються:

– мости або комутатори (2-й рівень в моделі *OSI*);

– маршрутизатори (3-й рівень в моделі *OSI*).

Фізичний сегмент мережі є доменом колізії. Пристрої, що працюють на першому рівні моделі *OSI* (повторювачі або концентратори) не дозволяють сегментувати мережу, оскільки вони не обмежують домен колізій. Широко практикується логічне сегментування, засноване на IP адресації.

Сегмент утворюється шляхом виділення діапазону адрес, який задається адресою мережі й мережевою маскою. У способі запису мережевої адреси виду xxx.xxx.xxx.xxx/yy число «yy» визначає кількість біт, які відводяться для позначення номера мережі. Відповідно, число 32-yy визначає кількість біт для адреси хоста в певній підмережі. Наприклад, у записах:

– 10.100.1.0/24, 10.100.2.0/24, 10.100.3.0/24 тощо – в кожному сегменті відведено 32 – 24 = 8 біт, тобто можна адресувати до 254 хостів + 1 адрес (255) резервується під широкомовний запит;

– 10.10.0.0/25, 10.10.10.0/26, 10.10.10.0/27 – аналогічно в сегментах до 126, 62, 30 вузлів відповідно.

Логічні підмережі з'єднуються за допомогою маршрутизаторів. Пристрої об'єднання мереж забезпечують зв'язок між сегментами локальних мереж, окремими локальними комп'ютерними мережами й підмережами будь-якого рівня. Існують такі класи пристроїв для об'єднання та сегментації мереж.

Концентратор (hub) працює на першому (фізичному) рівні моделі *OSI*. Об'єднує мережу в сегмент на фізичному рівні (домен колізії). Також концентратором називають мережевий пристрій першого рівня моделі *OSI*. Суть роботи концентратора проста: будь-який пакет приходить на довільний порт концентратора, передається на всі порти, крім порту, звідки пакет прийшов. Використання концентраторів у сучасних мережах небажано, оскільки пристрій забиває мережу зайвими широкомовними пакетами. Із цієї причини рекомендується використовувати комутатори.

Комутатор (switch) працює на другому (канальному) рівні моделі *OSI*. Поєднує кілька вузлів комп'ютерної мережі в межах одного або декількох фізичних сегментів мережі. Також комутатором називають мережевий пристрій другого рівня моделі *OSI*. Комутатор передає дані лише безпосередньо отримувачу, на відміну від концентратора. Це підвищує продуктивність (зменшує кількість широкомовних запитів) і безпеку мережі, позбавляючи інші сегменти мережі від необхідності (і можливості) обробляти дані, які їм не призначалися.

Маршрутизатор (router) працює на третьому (мережному) рівні моделі *OSI.* Пересилає пакети даних між різними сегментами мережі (фізичними або логічними). Також маршрутизатором називають мережевий пристрій третього рівня моделі *OSI*. Зазвичай маршрутизатор використовує адресу одержувача (IP-адресу), яка зазначена в пакетних даних, і визначає за таблицею маршрутизації

шлях, по якому потрібно передати дані. У такий спосіб забезпечується перенаправлення й оптимізація потоку даних. Якщо в таблиці маршрутизації для адреси немає описаного маршруту, то пакет відкидається. У ролі маршрутизатора може використовуватися як окремий мережевий пристрій, так і звичайний комп'ютер, у якого в наявності принаймі дві мережеві карти й він налаштований на виконання функцій маршрутизації.

3.3 Приклади розв'язання задач

Організація режиму симуляції роботи мережі.

Сформуйте в робочому просторі програми мережу з чотирьох ПК і двох хабів. Задайте для ПК IP-адреси та маску мережі *255.255.255.0* (рис. 3.1).

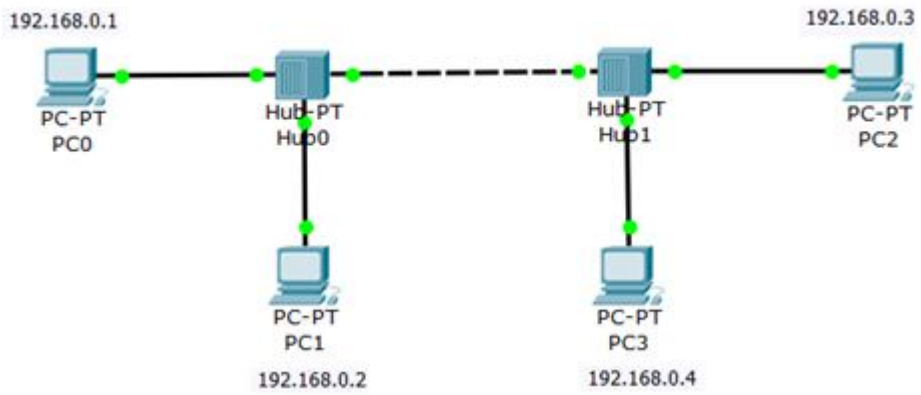

Рисунок 3.1 – Усі ПК розташовані в одній мережі

Тепер потрібно перейти в режим симуляції комбінацією клавіш *Shift + S*, або, натиснувши мишкою на іконку симуляції в правому нижньому куті робочого простору (рис. 3.2). *ICMP (Internet Control Message Protocol)* – мережевий протокол, що входить у стек протоколів *TCP/IP*. Зазвичай *ICMP* використовується для передачі повідомлень про помилки та інші виняткових ситуаціях, що виникли при передачі даних.

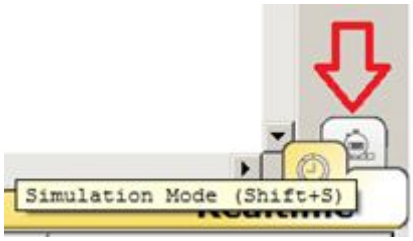

Рисунок 3.2 – Кнопка «Симуляція»

Натисніть на кнопку «Edit Filters» (Змінити фільтри) та вимкніть усі мережеві протоколи, крім *ICMP* (рис. 3.3).

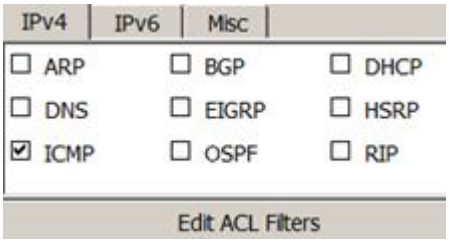

Рисунок 3.3 – Прапорець *ICMP* активний

З одного з вузлів спробуємо пропінгувати інший вузол. Для цього вибираємо далеко розташовані один від одного вузли, для того, щоб наочніше побачити, як будуть проходити пакети по мережі в режимі симуляції. Отже, з *PC1* пінгуємо *PC2* (рис. 3.4).

Ping – утиліта для перевірки з'єднань в мережах на основі *TCP/IP*. Утиліта відправляє запити (ICMP Echo-Request) протоколу ICMP зазначеному вузлу мережі й фіксує відповіді, що надходять *(ICMP Echo-Reply)*. Час між відправленням запиту й одержанням відповіді *(RTT)* дозволяє визначати двосторонні затримки *(RTT)* за маршрутом і частоту втрати пакетів, тобто побічно визначати завантаженість на каналах передачі даних і проміжних пристроях. Повна відсутність *ICMP*-відповідей може також означати, що віддалений вузол недоступний. У загальному випадку це також може означати що віддалений вузол або проміжний маршрутизатор налаштований так, що він блокує запит, що надходить, або ігнорує його та не відправляє відповідь *(ICMP Echo-Request).*

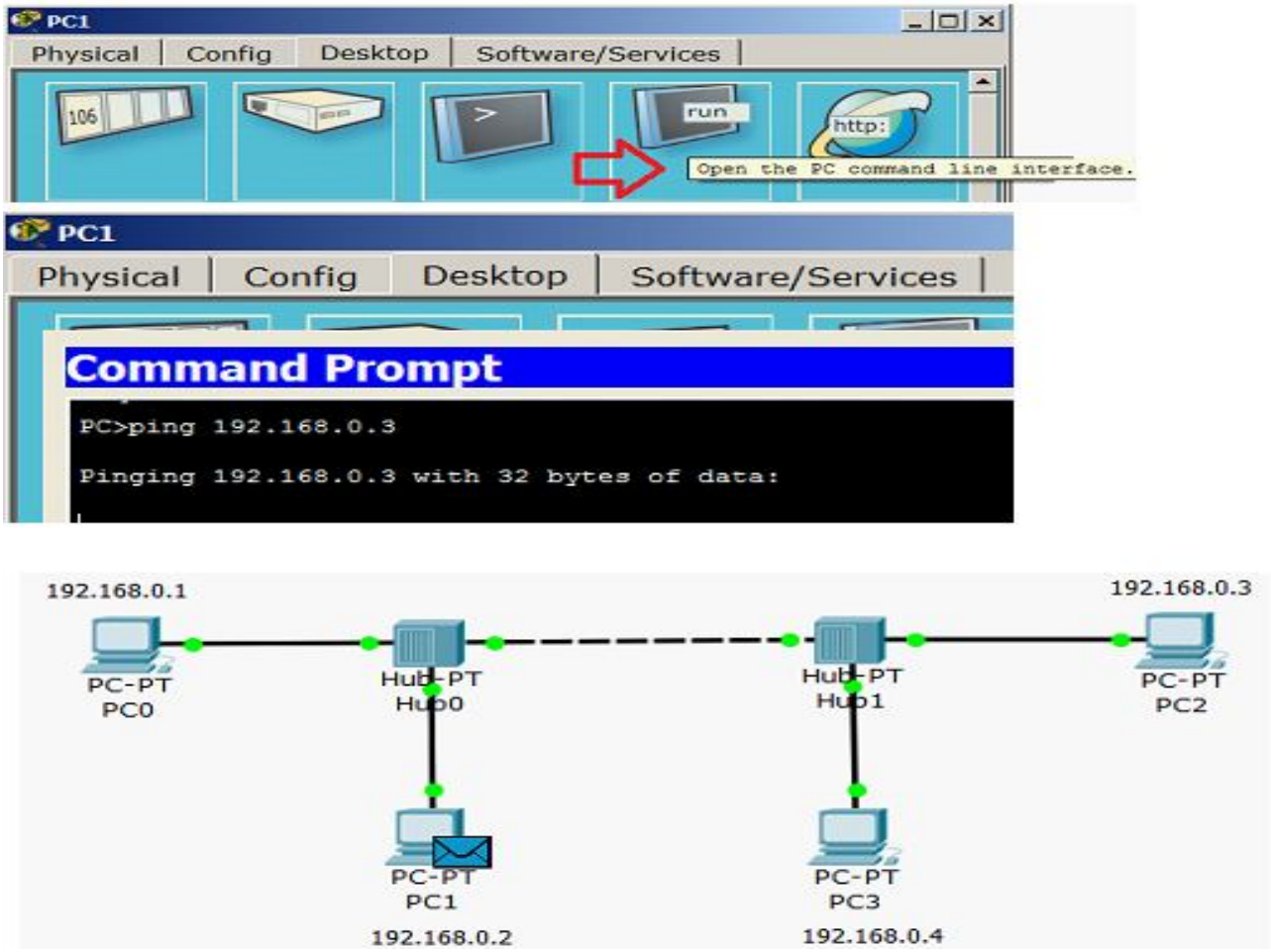

Рисунок 3.4 – *PC1* пінгує *PC2* (початок процесу)

На PC1 утворився пакет (конвертик), який чекає початку руху його по мережі. Запустити просування пакета в мережі покроково можна, якщо натиснути на кнопку *«Capture/Forward» («Уперед»)* у вікні симуляції. Якщо натиснути на кнопку *«Auto Capture/Play» («Відтворення»),* то ми побачимо увесь цикл проходження пакета по мережі. У *«Списку подій»* ми можемо бачити успішний результат «пінгу» (рис. 3.5).

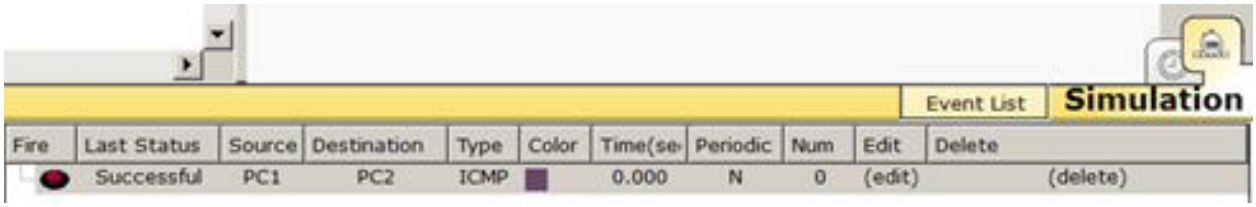

Рисунок 3.5 – Зв’язок PC1 та PC2

3.4 Висновки

У *Packet Tracer* передбачений режим моделювання (*Симуляції*), у якому показується, як працює утиліта *Ping*. Щоб перейти в цей режим, необхідно натиснути на значок *Simulation Mode* (*Симуляція*) в нижньому правому куті робочої області або комбінацію клавіш *Shift + S*. Відкриється *Simulation Panel* (*Панель симуляції*), в якій будуть відображатися всі події, пов'язані з виконання *ping-процесу*. Моделювання припиняється або при завершенні ping-процесу, або при закритті вікна симуляції. У режимі симуляції можна не тільки відслідковувати використовувані протоколи, а й бачити, на якому з семи рівнів моделі *OSI* конкретний протокол задіяний. У процесі перегляду анімації можна побачити принцип роботи хаба. Концентратор (хаб) передає прийнятий пакет в усі порти, крім порту, звідки надійшов цей пакет. Коли у відповідь пакет, згідно з протоколом, буде отримано відправником, то ми побачимо галочку «прийняття пакета». (рис. 3.6).

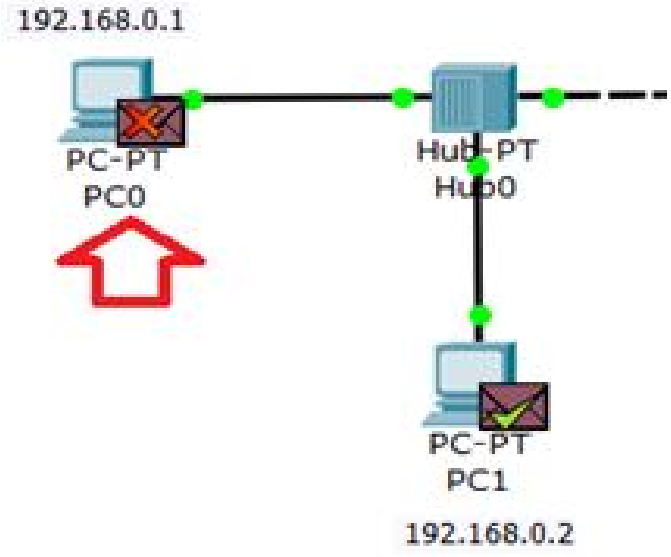

Рисунок 3.6 – Значки ігнорування пакетів та авторизація з'єднання

Якщо натиснути на кнопку *«Auto Capture/Play»* (*«Відтворення»*), то ми побачимо весь цикл проходження пакета по мережі (процес повториться чотири рази) (рис. 3.7).

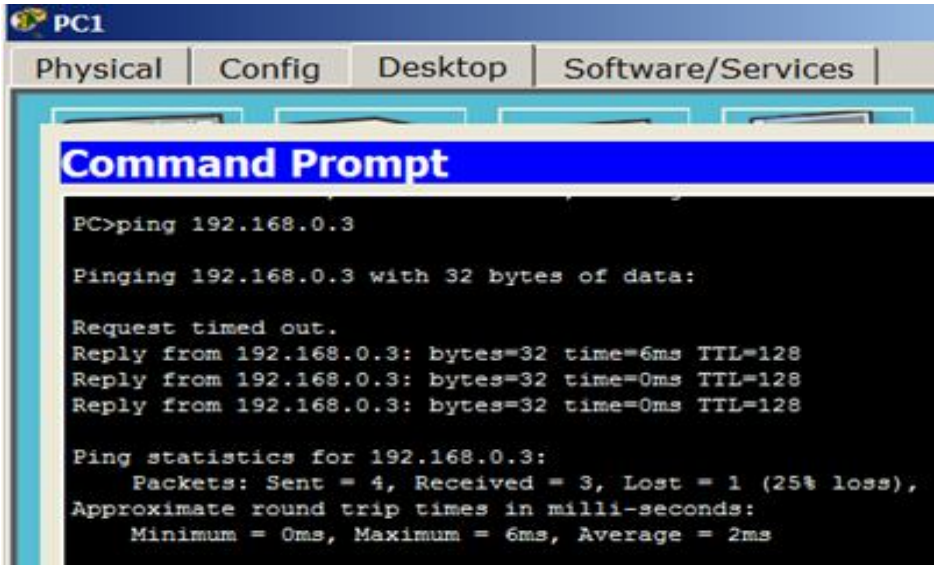

Рисунок 3.7 – Пінг від ПК1 до ПК2

Пояснення до рисунка:

TTL – час життя відправленого пакета (визначає максимальне число підмереж (маршрутизаторів), яке пакет може пройти під час його просування по мережі);

time – час, витрачений на відправлення запиту й отримання відповіді (сума часів на проходження пакета із запитом до проходження пакета з відповіддю);

min – мінімальний час відповіді;

max – максимальний час відповіді;

avg – середній час відповіді.

3.5 Завдання

Завдання 1. Побудова мережі з використанням концентратора.

1. Побудувати мережу з чотирьох ПК і сервера з використанням концентратора *(hub).* Сервер підключити до нульового порту концентратора.

2. Налаштувати статичні мережеві адреси на ПК мережі *(192.168.0.x, встановити маску 255.255.255.0)*.

3. Перевірити працездатність мережі, пропінгувавши з кожного комп’ютера сервер.

4. У режимі симулювання переглянути покроково просування по мережі тестового пакета, згенерованого командою *ping* із довільного ПК на сервер.

5. Привести скріншоти з результатами.

Завдання 2. Побудова мережі з використанням комутатора.

1. Побудувати мережу із чотирьох ПК і сервера з використанням комутатора *(switch).* Сервер підключити до нульового порту комутатора.

2. Налаштувати статичні мережеві адреси на ПК мережі *(192.168.0.x,* встановити маску *255.255.255.0).*

3. Перевірити працездатність мережі пропінгувати з кожного комп'ютера сервер.

4. Проаналізувати покроково поширення по мережі тестового пакета, згенерованого командою *ping*, у режимі *Simulation*.

5. Привести скріншоти з результатами.

3.6 Порядок виконання завдань

Для виконання *завдання 1* вибираємо тип обладнання *Hub's* (*Концентратори*). У меню *«список пристроїв даного типу обладнання»* обираємо конкретний концентратор – *Hub-PT* і перетягуємо його мишкою в робочу область програми. Далі обираємо тип пристрою *End Devices* (*Кінцеві пристрої)* і в додатковому *меню* обираємо настільний *комп'ютер PC-PT* і перетягуємо його мишею в робочу область програми. У такий спосіб встановлюємо ще три комп'ютери й один сервер.

Для підключення комп'ютерів і сервера до концентратора вибираємо новий тип пристроїв *Connections (З'єднання)*, далі обираємо «Copper Straiqht-Throuqh» («*Мідний прямий»*) тип кабелю. Щоб з'єднати мережеву карту комп'ютера з портом *Hub*-а, необхідно клацнути лівою клавішею миші на необхідному полі монітора. Відкриється графічне меню, у якому обрати *порт FastEthernet0* та протягнути *кабель* від ПК до концентратора, де в аналогічному *меню* вибрати будь-який вільний *порт Fast Ethernet* концентратора. При цьому

бажано завжди дотримуватися такого правила: для сервера обираємо 0-й *порт*, для PC1 – 1-й *порт*, для PC2 – 2-й *порт* і так далі.

Призначаємо вузлам мережі IP-адреса та маску. Для цього подвійним клацанням відкриваємо потрібний комп'ютер, далі *Config* (*Конфігурація*) – *Interface* (*Інтерфейс*) – *FastEthetnet0*. У групі параметрів IP *Configuration (Налаштування IP)* повинен бути активований *перемикач Static (Статичний)* у *поле IP Address* необхідно ввести *IP-адресу* комп'ютера, *маска* з'явиться автоматично. *Port status (Стан порту) – On (Вкл).*

Для перевірки працездатності мережі відправимо з комп'ютера на інший ПК тестовий сигнал *ping* та переключимось в режим *Simulation (Симуляція).* У вікні *Event list (Список подій),* за допомогою кнопки *Edit filters (Змінити фільтри),* спочатку очистимо *фільтри* від усіх типів сигналу, а потім встановимо тип протоколу тільки *ICMP*. Потім вікно *Event list (Список подій)* закриваємо.

У правій частині вікна, в графічному *меню* обираємо *Add Simple PDU (Простий PDU)* та клацанням миші встановлюємо його на ПК – обираємо джерело сигналу (довільний ПК), потім на вузлі призначення (*сервер*).

Натискаючи на кнопку «Capture/Forward» («Захват/Уперед»), спостерігаємо покрокове просування пакета *PDU* (рис. 3.8).

Fire	Last Status	Source	Destination	Type	Color	Time(se	Periodic	Num	Edit	Delete
	Successful	PC3	Server0	ICMP		0.000	N	0	(edit)	

Рисунок 3.8 – Успішне проходження пакетів по мережі

Для виконання *завдання 2* обираємо тип обладнання *Switches* (*Концентратори*). У *меню* «*Список пристроїв даного типу обладнання*» обираємо конкретний комутатор (наприклад 2950-24) і перетягуємо його мишею в робочу область програми. Потім усі дії аналогічні попередньому завданню.

Після виконання завдань зробити висновки про розбіжності, виявлені у функціонуванні концентратора та комутатора.

3.7 Вимоги до змісту звіту

1. Звіт із практичної роботи повинен бути оформлений відповідно до загальноприйнятих правил оформлення практичних робіт і містити такі пункти:

– тема роботи;

– мета роботи;

– опис перебігу виконання роботи.

2. Для кожного завдання описати процес його виконання з проміжними рисунками та скріншотами.

3.8 Контрольні питання

1. Поясніть, що таке сегмент мережі.

2. У чому полягають особливості фізичного сегментування?

3. На чому засноване логічне сегментування?

4. Які існують класи пристроїв для об’єднання та сегментації мереж?

5. Поясніть, що таке «режим симуляції» та яке його призначення.

6. Охарактеризуйте мережевий протокол *ICMP* (*Internet Control Message Protocol).*

7. Для чого необхідна утиліта *Ping*?

ПРАКТИЧНЕ ЗАНЯТТЯ № 4 ВИКОРИСТАННЯ ТЕХНОЛОГІЇ VIRTUAL LOCAL AREA NETWORK (VLAN)

4.1 Мета роботи

Отримання навичок створення та налаштування віртуальних локальних мереж на базі комутаторів.

4.2 Необхідний теоретичний матеріал

Приклади використання VLAN:

1. Об'єднання в єдину мережу комп'ютерів, підключених до різних комутаторів.

Припустимо, у вас є комп'ютери, які підключені до різних комутаторів, але їх потрібно об'єднати в одну мережу. Одну групу комп'ютерів ми об'єднаємо у віртуальну локальну мережу *VLAN 1*, а іншу – в мережу *VLAN 2* (рис. 4.1). Завдяки функції *VLAN* комп'ютери в кожній віртуальній мережі будуть працювати, немов підключені до одного комутатора. Комп'ютери з різних віртуальних мереж *VLAN 1* і *VLAN 2* будуть невидимі один для одного. Трафік кожної з віртуальних мереж буде ізольований, тобто пакети «чужої» мережі не будуть приходити на мережеві інтерфейси комп'ютерів «своєї» мережі і навпаки.

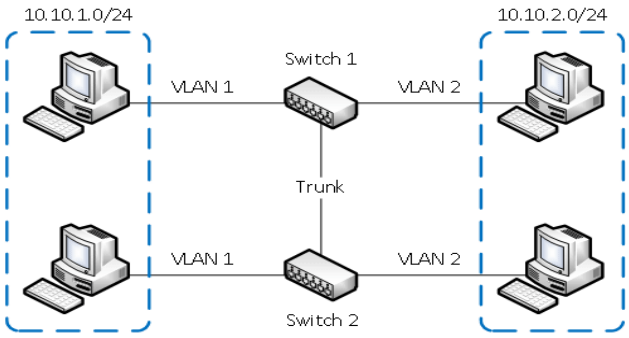

Рисунок 4.1 – Комп'ютери підключені до різних комутаторів, які об'єднані в одну віртуальну мережу

2. Поділ у різні підмережі комп’ютерів, підключених до одного комутатора.

На рисунку комп’ютери фізично підключені до одного комутатора, але розділені в різні віртуальні мережі *VLAN 1* і *VLAN 2*. Комп’ютери з різних віртуальних підмереж будуть невидимі один для одного (рис. 4.2).

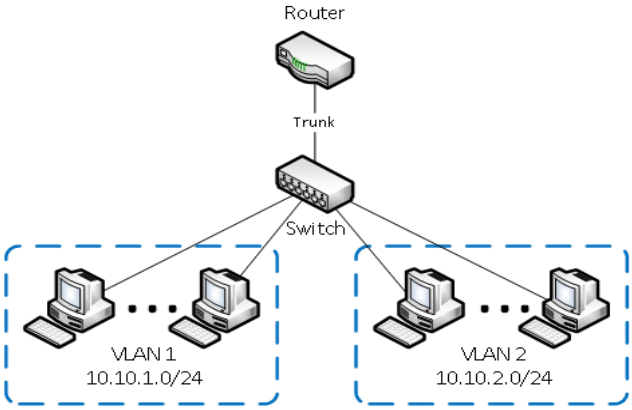

Рисунок 4.2 – Комп’ютери, підключені до одного комутатора та розділені на дві віртуальні мережі

3. Поділ гостьової Wi-Fi мережі та Wi-Fi мережі підприємства.

На рисунку 4.3 до роутера підключена фізично одна Wi-Fi точка доступу. На точці створені дві віртуальні Wi-Fi точки з назвами *HotSpot* і *Office*. До *HotSpot* будуть підключатися по Wi-Fi гостьові ноутбуки для доступу до інтернету, а до *Office* – ноутбуки підприємства. Із метою безпеки необхідно, щоб гостьові ноутбуки не мали доступ до мережі підприємства. Для цього комп’ютери підприємства й віртуальна Wi-Fi точка *Office* об’єднані у віртуальну локальну мережу *VLAN 1*, а гостьові ноутбуки будуть перебувати у віртуальній мережі *VLAN 2*. Гостьові ноутбуки з мережі *VLAN 2* цієї статті не будуть мати доступ до мережі підприємства *VLAN 1*.

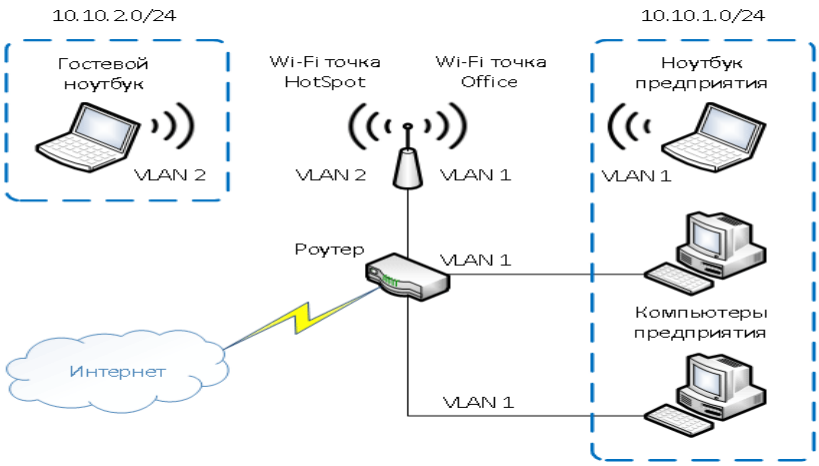

Рисунок 4.3 – Створення віртуальних точок доступу в мережі Wi-Fi

4.3 Приклад вирішення задач

Задача: є мережа, що складається з восьми ПК і двох комутаторів. До кожного комутатора підключені по чотири ПК. Комутатори з'єднані лінією зв'язку *GigabitEthernet*. Потрібно налаштувати дві віртуальні мережі, кожна з яких містить по чотири ПК попарно підключених до різних комутаторів.

Крок 1. На основі створеної в попередньому прикладі структури з чотирьох ПК, підключених до комутатора 2960, шляхом копіювання структури створимо дві однакових конфігурації мережі та з'єднаємо комутатори між собою кросовою лінією зв'язку (оскільки комутатори – пристрої одного рівня). Якщо попередня мережа не збережена, створимо нову мережу, що складається з двох комутаторів і підключених до кожного комутатора чотирьох ПК. З'єднаємо комутатори високошвидкісною лінією через порти *GigabitEthernet*. Це вихідна мережа, в якій ми маємо намір організувати дві віртуальні мережі, що містять ПК, підключені до різних комутаторів. Перевіримо також, щоб IP-адреси на всіх ПК ставилися до однієї підмережі (у разі необхідності відкоригуємо їх, наприклад, комп'ютером ПК1 – ПК8 дамо значення адрес: 192.168.1.1 – 102.168.1.8 відповідно).

Крок 2. Визначимо склад віртуальних мереж. Нехай до комутатора 1 підключені ПК1 – ПК4, а до комутатора 2 підключені ПК5 – ПК8. Ставимо

завдання: створити: vlan2 з ім'ям zona1 (ПК1, ПК2, ПК5, ПК6) і vlan3 з ім'ям «zona 2» (ПК3, ПК4, ПК7, ПК8). У прикладі 1 продемонстровано, що для створення віртуальних мереж на одному комутаторі досить конфігурувати їх порти, вказавши кожному порту до якої віртуальної мережі він належить. Проробимо цю операцію створення *Vlan2* і *Vlan3* для кожного комутатора окремо.

Крок 3. Налаштування *Vlan2* і *Vlan3* у комутаторі 1. Заходимо в настройки комутатора та входимо в консоль (закладка *CLI – Comand Line Interface*). Входимо в привілейований режим *«enable»* (у цьому режимі повинен з'явитися символ *«запрошення»* #), потім перейдемо в режим глобального конфігурування *«conf t».* Створимо нову віртуальну мережу. Уведемо: # *vlan 2*. Задамо ім'я мережі: # *name zona 1*. Вийти на попередній рівень # *exit*.

Крок 4. Налаштування портів кожного з'єднання. Алгоритм такий: дивимося, до яких портів комутатора підключаються ПК1 і ПК2. Для цього наводимо курсор на з'єднання й бачимо з боку комутатора номер порту підключення. Нехай для ПК1 і ПК2 це будуть порти *FastEthernet 0/1* і *0/2*. Визначимо ці порти, як порти доступу в складі *VLan2*. Для цього заходимо в налаштування інтерфейсу відповідного порту: # *interface fastEthernet 0/1*, задаємо режим функціонування порту (*accsess*): # *switchport mode access* та визначаємо *VLan,* до якої цей порт буде належати: # *switchport access vlan 2. # exit* – на цьому налаштування одного порту завершено.

Аналогічно налаштовуємо порт 0/2: # *interface fastEthernet 0/2,* # *switchport mode access,* # *switchport access vlan 2,* # *end* – налаштування другого порту завершено. Перевірити результат можна, використовуючи команду *show vlan*. У відповідь комутатор видасть таблицю, в якій показано, що до складу *Vlan1* входять усі порти (за замовчуванням) крім тих, які ми налаштували в складі *vlan* 2.

Аналогічно створимо *Vlan 3* з ім'ям *zona 2*, налаштувавши в її складі порти концентратора, до яких підключені ПК3 і ПК4. У такий спосіб ми перевели

порти, до яких підключені наші ПК, у віртуальні мережі *Vlan 2* і *Vlan 3* з іменами *zona 1* і *zona 2* відповідно.

Крок 5. Точно такі самі дії виконаємо з комутатором 2, створивши *Vlan 1* і *Vlan 2*, а потім закріпивши порти, до яких підключені ПК5, ПК6 за *Vlan 1*, а порти ПК7 ПК8 за *Vlan 2*. Якщо використовується кілька комутаторів, то необхідно між комутаторами налаштувати так званий *Trunk-port*. Технологія *Trunk* дозволяє організувати по одному фізичному з'єднанню кілька логічних потоків (або сегментів) трафіку. Кожен сегмент пов'язує комп'ютери, що належать до однієї *Vlan*-мережі, але підключені до різних комутаторів. Переходимо до налаштування *Trunk* - з'єднання.

Крок 6. Оскільки комутатори з'єднані лінією *Gigabit Ethernet*, заходимо в налаштування інтерфейсу порту *Gigabit Ethernet 1/1* на першому комутаторі: # *interface GigabitEthernet 1/1*, входимо в режим глобального конфігурування # *conf t*, потім у налаштування інтерфейсу # *int*, задаємо режим роботи порту # *switchport mode trunk*. Далі вказуємо, для яких *vlan* буде підтримуватися передача даних # *switchport trunk allowed vlan 1, 2*.

Крок 7. Те саме проробимо на другому комутаторі. Дві *Vlan*-мережі створені. *Vlan 1*: *zona1* (ПК1, ПК2, ПК5, ПК6), *Vlan 2*: *zona2* (ПК3, ПК4, ПК7, ПК8). Перевіримо їх взаємну ізольованість.

Крок 8. Перевірка доступності ПК, що належать до однієї і тієї самої *Vlan-мережі*. У мережі *zona 1* із ПК1 пропінгуємо ПК2 і ПК5. Успішний результат означає, що в підмережі *zona 1* ПК, які підключені до одного або різних комутаторів, «бачать» одне одного. У мережі *zona 2* із ПК3 пропінгуємо ПК4 і ПК8. Успішний результат означає, що в підмережі *zona 2* у ПК, які підключені до одного або різних комутаторів, «бачать» одне одного.

Крок 9. Перевірка ізольованості створених *Vlan*.

З ПК1 мережі *zona 1* пропінгуємо ПК3 і ПК7, що належать до мережі *zona 2*. Недоступність вузлів означає, що трафік із мережі *zona 1* ізольований від мережі *zona 2*. З ПК3 мережі *zona 2* пропінгуємо ПК2 і ПК6, що належать до

zona 1. Недоступність вузлів означає, що трафік із мережі *zona 2* ізольований від мережі *zona1*.

4.4 Завдання

У мережі з двома комутаторами виділити групу комп'ютерів, підключених до різних комутаторів, в ізольовану під-мережу.

Є мережа, що складається з бухгалтерії, відділу продажів і серверної. У відділі продажів є чотири ПК, а в бухгалтерії – п'ять ПК. Є також серверна, що містить два сервера: сервер відділу продажів і сервер бухгалтерії. Бухгалтерія знаходиться в будівлі 1, відділ продажів і серверна – в будівлі 2. У будівлі 1 усі комп'ютери підключені до комутатора 1, а в будівлі 2 – до комутатора 2.

Потрібно побудувати віртуальну мережу 1, у яку входить бухгалтерія та сервер 1 і віртуальну мережу 2 , у яку входить відділ продажів і сервер 2.

Завдання виконати по наступній схемі:

1. За допомогою програми *Cisco Packet Tracker* побудувати вихідну мережу, налаштувати фіксовані IP-адреси, перевірити працездатність мережі й доступність серверів.

2. Налаштувати необхідні *VLan-мережі*.

3. Перевірити працездатність кожної зі створених *VLan-мереж* і доступність свого сервера.

4. Перевірити ізольованість кожної зі створених *VLan-мереж* (переконатися, що широкомовні пакети не виходять за межі *VLan-мережі*.

5. Перевірити доступність довільного комп'ютера та сервера з іншої *VLan-мережі* шляхом перехресного пінгування (з однієї *VLan-мережі* спробувати пропінгувати будь-який комп'ютер іншої *VLan-мережі*).

4.5 Вимоги до змісту звіту

1. Звіт із лабораторної роботи повинен бути оформлений відповідно до загальноприйнятих правил оформлення лабораторних робіт і містити такі пункти:

– тема роботи;

– мета роботи;

– опис перебігу виконання роботи.

2. Для кожного завдання описати процес його виконання з проміжними рисунками та скріншотами.

4.6 Контрольні питання

1. Дайте визначення мережевої технології *VLAN*.

2. Охарактеризуйте комп’ютерну мережу, де комп’ютери підключені до різних комутаторів, які об’єднані в одну віртуальну мережу.

3. Охарактеризуйте комп’ютерну мережу, де комп’ютери підключені до одного комутатора та розділені на дві віртуальні мережі.

4. Охарактеризуйте комп’ютерну мережу, де був зроблений поділ гостьової Wi-Fi мережі та Wi-Fi мережі підприємства.

5. Опишіть алгоритм створення та налаштування мережі *VLAN* на базі двох комутаторів і восьми комп’ютерів.

ПРАКТИЧНЕ ЗАНЯТТЯ № 5 ОБ'ЄДНАННЯ ЛОКАЛЬНИХ МЕРЕЖ ЗА ДОПОМОГОЮ L2 І L3-КОМУТАТОРІВ

5.1 Мета роботи

Отримання навичок об'єднання декількох локальних мереж за допомогою L2 і L3-комутаторів. Вивчення функцій мережевих пристроїв з використанням програми *Cisco Packet Tracer*.

5.2 Необхідний теоретичний матеріал

Комутатори L2 і L3 комутують трафік на основі MAC-адрес. Маршрутизувати трафік «не вміють», оскільки не працюють на рівні пакетів і IP-адрес. Більшість з комутаторів підтримують технологію *Vlan* і тому здатні сегментувати трафік відповідно до утворення *Vlan* (трафік, що генерується *Vlan*, зокрема й широкомовний, переміщається виключно між портами своєї *Vlan*). Взаємодія кінцевих пристроїв, що належать до різних *Vlan-мереж,* неможлива без використання комутаторів L3 або маршрутизаторів.

Комутатори використовуються для підключення кінцевих пристроїв до мережі (утворюють мережі доступу). Комутатори:

– агрегують трафік від L2- комутаторів (підмереж);

– працюють з IP-пакетами;

– підтримують IP-маршрутизацію, тобто, кожен порт комутатора має IP-адресу та комутатор, який здатний відправляти пакети в суміжні підмережі.

Для виконання роботи будемо використовувати програмний продукт *Cisco Packet Tracker*, який дозволяє імітувати налаштування комутатора або маршрутизатора. Закладка *CLI* у програмі *Cisco Packet Tracer* імітує пряме кабельне (консольне) підключення до мережних пристроїв. Це один із найпоширеніших способів налаштування мережевого пристрою за допомогою командного рядка. Командний рядок являє собою місце, куди користувач

вводить символи, що формують управлінський вплив. Робота з командним рядком здійснюється в декількох режимах (табл. 5.1).

Таблиця 5.1 – Режими CLI

Режим	Перехід у режим	Вид командного рядка	Вихід із режиму
Призначений для користувача	Підключення	Router/Switch>	logout
Привілейований	enable	Router/Switch #	disable
Глобальна конфігурація	configure terminal (conf t)	Router/Switch (config)#	exit,end или Ctrl-Z
Налаштування інтерфейсів	Interface (int)	Router/Switch (config-if)	exit

Види командного рядка:

*Router/Switch***>** – призначений для користувача режим. У цьому режимі можна переглядати деяку статистику та проводити найпростіші операції на реалізацію пінгу. У цьому режимі доступні лише команди, які дозволяють виводити на екран інформацію без зміни установок мережевого пристрою.

Router/Switch – привілейований режим. Цей режим підтримує команди налаштування та тестування, детальну перевірку мережевого пристрою, маніпуляцію з файлами й доступ у режим конфігурації. Потрапити в нього можна, увівши команду enable.

*Router/Switch (config)***#** – режим глобального конфігурування. У цьому режимі доступні всі команди пристрою. Перехід у режим активується командою *#configure terminal* (або *#conf t*) (із привілейованого режиму).

Усі команди в консолі можна скорочувати, але важливо, щоб скорочення однозначно вказувало на команду. Використовуйте кнопку *Tab* і знак питання (?). При натисканні *Tab* скорочена команда дописується до повної, а знак питання (?), після команди, виводить список подальших можливостей і невелику довідку по ним. Можна перейти до наступної команді, збереженої в буфері. Для цього натисніть на стрілку вниз або Ctrl + N. Можна повернутися до командам, уведеним раніше. Натисніть на стрілку вгору або Ctrl + P.

Підмережі, побудовані на комутаторах L2, не здатні взаємодіяти між собою, оскільки «не вміють» працювати з IP-адресами. Для такої взаємодії використовуються L3- комутатори або маршрутизатори – пристрої, що працюють на мережному рівні моделі OSI.

5.3 Приклади розв'язання задач

Нехай є дві підмережі, зібрані на комутаторах L2 (рис. 5.1). Підмережа 1 зібрана на комутаторі *Switch 1* і підмережа 2 зібрана на комутаторі *Switch 2*. Потрібно об'єднати їх за допомогою комутатора L3 (*Multilayer Switch0*), як це показано на рисунку 5.1. Запускаємо *Cisco Packet Tracer* і створюємо спочатку мережі 1 і 2 з використанням комутаторів 2960-24TT, що мають 24 порти *Fast Ethernet* і два високошвидкісні порти *Gigabit Ethernet*.

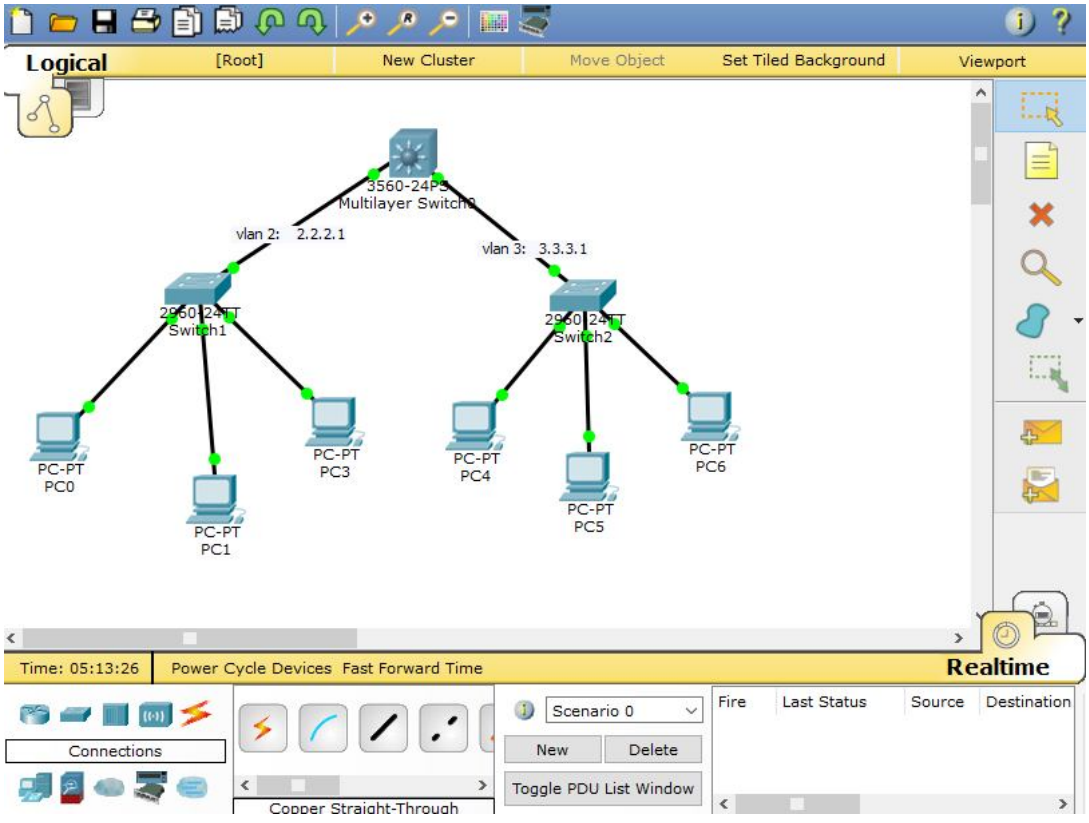

Рисунок 5.1 – Мережа 1 і мережа 2 на базі комутаторів L2

Потім розмістимо на схемі комутатор L3 (модель 3560-24PS), який також містить 24 порти *FastEthernet* і 2 високошвидкісних порти *GigabitEthernet*.

З'єднаємо в графічному інтерфейсі гігабітні порти комутатора L3 із гігабітними портами комутаторів L2 у такий спосіб:

Switch1 (*GigabitEthernet 0/1*) – *Switch0* (*GigabitEthernet 0/1*);

Switch2 (GigabitEthernet 0/2) – Switch0 (GigabitEthernet 0/2).

Фізична структура готова. Залишилося зробити правильні налаштування. Виходимо з того, що підмережі на кожному комутаторі повинні бути незалежні один від одного, тому для кожної з підмереж буде виділено свій адресний простір. Нехай це буде для *Switch1 – 192.168.2.0 255.255.255.0*, а для *Switch2 – 192.168.3.0 255.255.255.0.*

Для шлюзів призначимо такі адреси:

для Switch1: 192.168.2.1;

для Switch2: 191.168.3.1.

Тепер задаємо адреси для всіх ПК, підключених до мережі (табл. 5.2)

Таблиця 5.2 – Таблиця адрес для всіх ПК, підключених до мережі

Команда	Адреса	Маска	Шлюз
Switch1	Vlan 2		
PC0	192.168.2.2	255.255.255.0	192.168.2.1
PC1	192.168.2.3	255.255.255.0	192.168.2.1
PC2	192.168.2.4	255.255.255.0	192.168.2.1
Switch2	Vlan 3		
PC3	192.168.3.2	255.255.255.0	192.168.3.1
PC4	192.168.3.3	255.255.255.0	192.168.3.1
PC5	192.168.3.4	255.255.255.0	192.168.3.1

Для цього потрібно зайти на кожен ПК, вибрати закладку *Desktop/IP Configuration* і прописати адреси та маски. Далі налаштовуємо комутатори *Switch 1 і Switch 2*. На комутаторі *Switch 1 створюємо Vlan 2*. Клацаємо на

Switch 1 і переходимо в *CLI*, потім у режим глобального конфігурування (*enable → conf t*). Далі задаємо команду *vlan 2*, потім вводимо name V2 (V2 – це ім'я *vlan 2*). Потім переводимо порти, до яких підключені ПК, з *vlan 1* в *vlan 2*. Для цього заходимо в налаштування інтерфейсу відповідного порту комутатора:

 # Interface fastEthernet 0/1

задамо режим функціонування конкретного порту (*accsess*):

 # switchport mode access

і задамо *VLan* до якої цей порт буде належати:

 # switchport access vlan 2

 # exit – на цьому налаштування одного порту завершена.

Аналогічно встановлюємо на портах *fastEthernet0/2* і *fastEthernet 0/3* режим *access* і переводимо їх у *vlan 2*. Тепер наші ПК, підключення до цих портів належать до *vlan 2*. Такі самі дії виконаємо на *Switch 2*, створивши там *vlan 3* і перевівши в *vlan 3* усі підключені ПК.

Переходимо на *Switch0*. Створюємо *vlan 2* і *vlan 3* тими самими командами, що й у попередньому випадку. Потім налаштовуємо порти *gi0/1 gi0/2*, що зв'язують *Switch0* зі *Switch1* і *Switch2*, для цього заходимо в налаштування інтерфейсу відповідного порту комутатора, попередньо перейшовши в режим глобального конфігурування (*enable → confit*):

*interface gi 0/1*

задамо режим функціонування порту (*accsess*):

*switchport mode access*

та задамо *VLan* до якої цей порт буде належати:

 # switchport access vlan 2

 # exit – на цьому налаштування першого порту завершено.

Аналогічно для інтерфейсу *gi0/2*:

 # interface gi 0/2

задамо режим функціонування порту (*access*):

 # switchport mode access

і задамо *VLan,* до якої цей порт буде належати:

 # switchport access vlan 3

 # exit – на цьому налаштування другого порту завершена.

Тепер пропишемо адреси для цих інтерфейсів (*gi0/1 і gi0/2*):

gi0/1: 192.168.2.1 255.255.255.0

gi0/2: 192.168.3.1 255.255.255.0

Для цього переходимо в режим глобального конфігурування (*enable* → *conf t*) та задаємо команду *#int gi0/1*

#ip address 192.168.2.1 255.255.255.0

#no shutdown (увімкнути інтерфейс)

#exit

Такий самий блок команд виконуємо для інтерфейсу *gi0/2*. У результаті буде піднято два інтерфейси та дві *vlan* (*vlan 2* і *vlan 3*) на комутаторі L3. Переконатися в цьому можна, ввівши команду *Switch # show run*, або підвести мишу на графічному інтерфейсі до цікавого для нас пристрою та зафіксувавши положення курсору на об'єкті. І останнє. Щоб комутатор почав IP-маршрутизацію, потрібно ввести команду в режимі глобальної конфігурації: *Switch # ip routing*

Тепер можна перевірити пінгуванням доступність будь-яких ПК у мережі – всі ПК повинні бути доступні. Трафік між двома мережами маршрутизується через L3 комутатор, тобто на рівні IP-пакетів.

5.4 Завдання

1. Налаштувати мережу такої конфігурації:

– підмережа 1: три персональних комп'ютери підключені до комутатора 2960-24TT.

– підмережа 2: чотири персональні комп'ютери підключені до іншого комутатора 2960-24TT.

Обидві підмережі підключені гігабітними лінками до портів комутатора L3. Крім того, до комутатора L3 безпосередньо підключені два сервера (*Server1* і

Server2). Потрібно налаштувати мережу в такий спосіб, щоб *Server 1* був доступний для ПК тільки з підмережі 1, а *Server 2* – доступний для ПК тільки з підмережі 2.

2. Виконати налаштування в інтерфейсі програми *Cisco Packet Tracker*.

3. Привести покроковий опис і скріншоти виконуваних дій.

4. Перевірити отриманий результат шляхом пінгування.

5. Привести результати налаштування обладнання у вигляді скріншотів результатів виконання команди show run на кожному мережевому пристрої.

5.5 Вимоги до змісту звіту

1. Звіт з лабораторної роботи повинен бути оформлений відповідно до загальноприйнятих правил оформлення лабораторних робіт і містити такі пункти:

– тема роботи;

– мета роботи;

– опис перебігу виконання роботи.

2. Для кожного завдання описати процес його виконання з проміжними рисунками та скріншотами.

5.6 Контрольні питання

1. Дайте характеристику комутаторам 2-го рівня (L2 – комутаторам).

2. Яке призначення L3 – комутаторів.

3. Дайте характеристику режимів роботи з програмою *Cisco Packet Tracker* при використанні *CLI*.

4. Наведіть види командного рядка.

5. Опишіть алгоритм створення та налаштування мережі, у якій є дві підмережі, зібрані на комутаторах L2. Підмережа 1 зібрана на комутаторі *Switch 1* і підмережа 2 зібрана на комутаторі *Switch 2*. Потрібно об’єднати їх за допомогою комутатора L3 (*Multilayer Switch0*).

ПРАКТИЧНЕ ЗАНЯТТЯ № 6 НАЛАШТУВАННЯ МАРШРУТИЗАТОРА ДЛЯ ЗВ'ЯЗКУ ДВОХ МЕРЕЖ

6.1 Мета роботи

Отримання навичок об'єднання мереж за допомогою маршрутизатора з використанням програми *Cisco Packet Tracer*.

6.2 Необхідний теоретичний матеріал

Маршрутизатор призначений для об'єднання мереж і організації передачі даних від джерела до одержувача, використовуючи IP-адресацію.

Відомо, що IP-адреса складається з двох частин: адреси мережі й адресу свого пристрою в цій мережі. Усередині локальної мережі пристрої взаємодіють, використовуючи MAC-адресацію, а щоб вийти в іншу мережу, необхідно вказати адресу цієї мережі в переданому пакеті на мережевому рівні моделі OSI. Це можуть робити L3-комутатори й маршрутизатори. L3-комутатори переважно використовуються для маршрутизації трафіку в локальній мережі між створеними сегментами, хоча можуть використовуватися і для підключення до глобальної мережі. Маршрутизатор, на відміну від L3-комутаторів, мають розширений функціонал (NAT, VPN, функції брандмауера тощо), що дозволяє більш комфортно й безпечно налаштовувати взаємодію з зовнішнім світом. Функціонально, як маршрутизатор, так і L3-комутатор дозволяють вийти трафіку за межі мережі під зовнішній мережевий простір.

Для виконання практичної роботи будемо використовувати програмний продукт *Cisco Packet Tracker*, який дозволяє імітувати настройку комутатора або маршрутизатора. Закладка *CLI* в програмі *Cisco Packet Tracer* імітує пряме кабельне (консольне) підключення до мережних пристроїв. Це один із найпоширеніших способів налаштування мережевого пристрою за допомогою командного рядка. Командний рядок являє собою місце, куди користувач

вводить символи, що формують управлінський вплив. Робота з командним рядком здійснюється в декількох режимах (табл. 6.1).

Таблиця 6.1 – Режими CLI

Режим	Перехід у режим	Вид командного рядка	Вихід із режиму
Призначений для користувача	*Підключення*	*Router/Switch>*	*logout*
Привілейований	*enable*	*Router/Switch #*	*disable*
Глобальна конфігурація	*configure terminal (conf t)*	*Router/Switch (config)#*	*exit, end або Ctrl-Z*
Налаштування інтерфейсів	*Interface (int)*	*Router/Switch (config-if)*	*exit*

*Router/Switch***>** – призначений для користувача режим. У цьому режимі можна переглядати деяку статистику та проводити найпростіші операції з пінгуванням. У цьому режимі доступні лише команди, які дозволяють виводити на екран інформацію без зміни установок мережевого пристрою.

*Router/Switch***#** – привілейований режим. Цей режим підтримує команди налаштування й тестування, детальну перевірку мережевого пристрою, маніпуляцію з файлами та доступ у режим конфігурації. Потрапити в нього можна, увівши команду *enable*.

Router/Switch (config)# – режим глобального конфігурування. У цьому режимі доступні всі команди пристрою. Перехід у режим активується командою *#configure terminal* (або *#conf t)* (із привілейованого режиму).

Усі команди в консолі можна скорочувати, але важливо, щоб скорочення однозначно вказувало на команду. Використовуйте клавішу *Tab* і знак питання (?). При натисканні *Tab* скорочена команда дописується до повної, а знак питання (?), наступний за командою, виводить список подальших можливостей і невелику довідку по ним. Можна перейти до наступної команди, збереженої в буфері. Для цього натисніть на стрілку вниз або Ctrl + N. Можна

повернутися до команд, які були введені раніше. Натисніть на «стрілку вгору» або Ctrl + P.

6.3 Приклад використання маршрутизатора для зв'язку двох мереж

Потрібно побудувати мережу, зображену на рисунку 6.1, і налаштувати маршрутизатор для зв'язку мереж між собою.

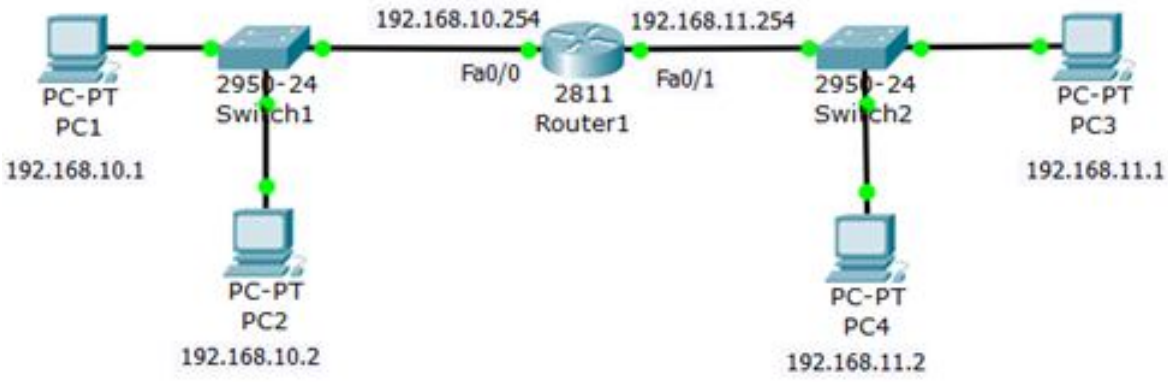

Рисунок 6.1 – Дві мережі, зв'язані через маршрутизатор

За допомогою *Cisco Packet Tracer* створюємо структуру необхідної мережі.

1. Створимо підмережу 1 із *PC1*, *PC2* та *Switch1* (2950): *192.168.10.0*, маска: *255.255.255.0*

2. Налаштуємо мережеві адреси вручну (*PC1: 192.168.10.1; PC2: 192.168.10.2*)

3. Вкажемо як адресу шлюзу: *192.168.10.254* (рис. 6.2)

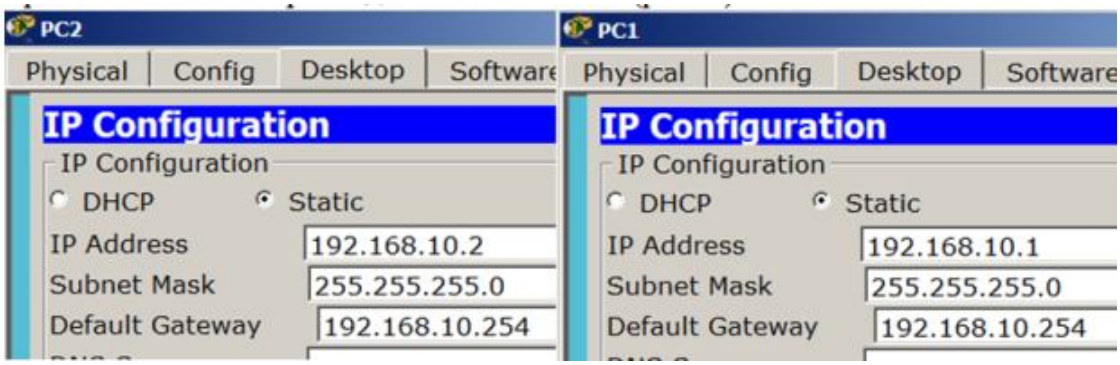

Рисунок 6.2 – Налаштування конфігурацій PC1 та PC2

1. Створимо підмережу 2 з *PC3*, *PC4* та *Switch2* (2950): *102.168.11.0*, маска: *255.255.255.0*

2. Налаштуємо мережеві адреси вручну (*PC3: 192.168.11.1; PC4: 192.168.11.2*).

3. Як шлюз вкажемо адресу: *192.168.11.254* (рис. 6.3)

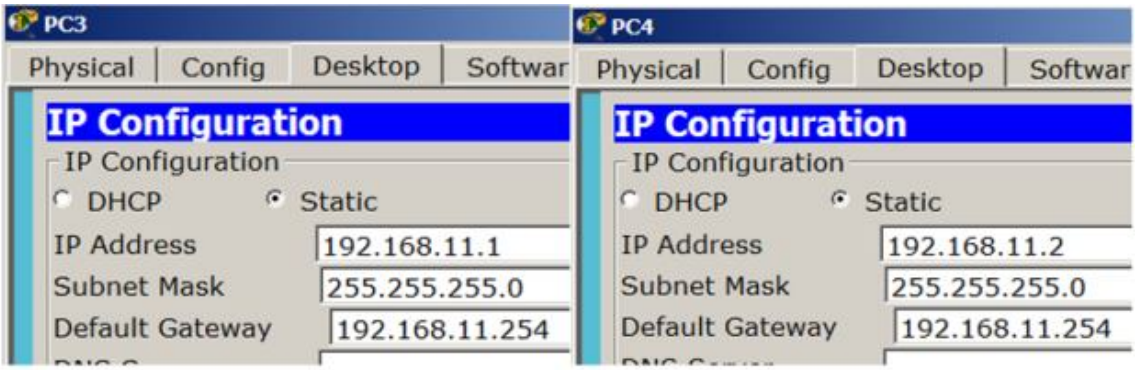

Рисунок 6.3 – Налаштування конфігурацій PC3 та PC4

Усі параметри маршрутизатора можна налаштувати з командного рядка на вкладці CLI. Налаштуємо порт маршрутизатора, до якого підключена мережа 1:

Enable – (умикаємо привілейований режим);

conf t (*config terminal* – входимо в режим глобальної конфігурації);

int fa0/1 (*interface fa0/1* – налаштовуємо інтерфейс *FastEthernet 0/1*);

ip address 192.168.10.254 255.255.255.0 (прописуємо IP адресу інтерфейсу та маску мережі маршрутизатора);

no sh (*no shutdown* – умикаємо інтерфейс, за умовчуванням усі інтерфейси вимкнені);

exit – (виходимо з режиму конфігурації інтерфейсу);

end – (закінчили редагування);

write – (зберегли конфігурацію).

Аналогічно налаштовуємо порт *fa0/1* роутера на роботу з мережею *192.168.11.0* (рис. 6.4). Для цього встановимо адресу цього мережевого інтерфейсу таку саму, як адреса шлюзу (за замовчуванням) у мережі 1: *192.168.11.254* і маску *255.255.255.0.* Ця сама адреса вказана в ПК як

шлюз. Тобто пакети в мережі 2, що не знайшли адреси в таблиці комутатора, будуть відправлені на цей інтерфейс (за замовчуванням).

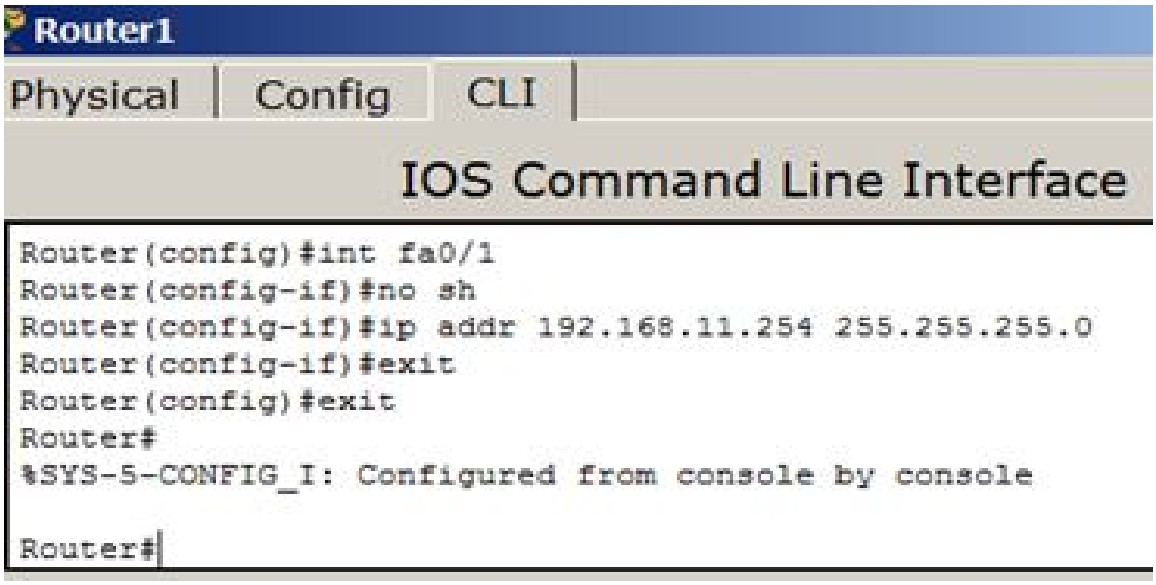

Рисунок 6.4 – Налаштування порту fa 0/1 роутера

У підсумку після налаштування маршрутизаторів на портах загоряються зелені маркери, тобто зв’язок між ними є.

Перевіряємо таблицю маршрутизації командою *show ip route* (рис. 6.5).

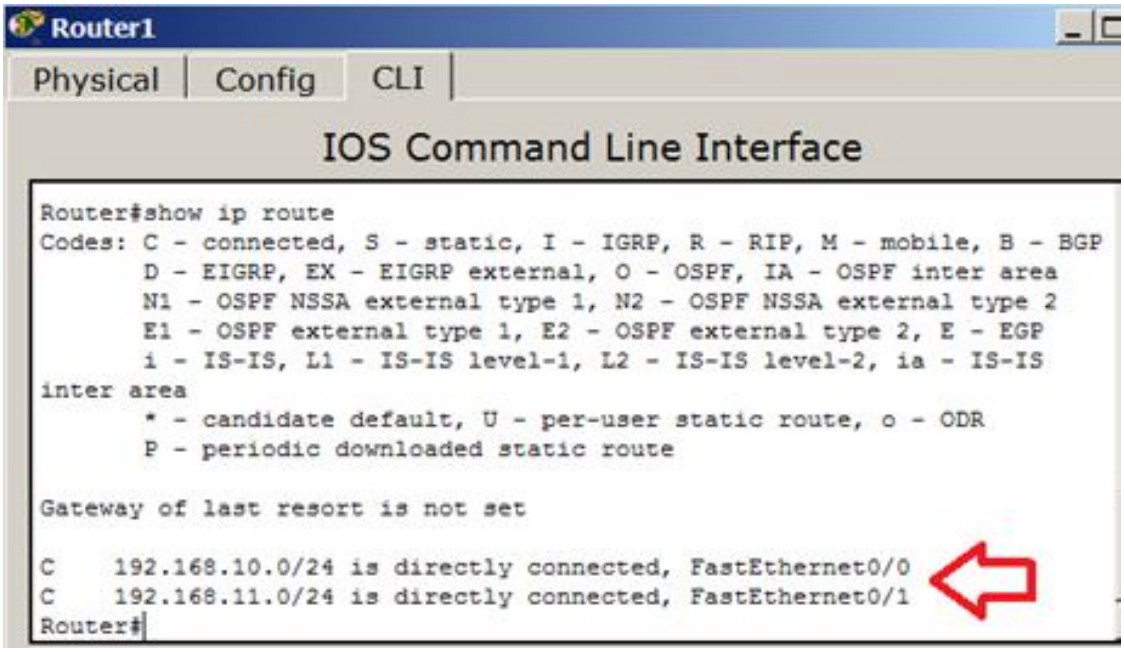

Рисунок 6.5 – Перевірка таблиці маршрутизації роутера

У нас роутер обслуговує дві мережі. Перевіряємо зв’язок роутера та ПК з кожної мережі командами *ping 192.168.10.0 і ping 192.168.11.0* (рис. 6.6).

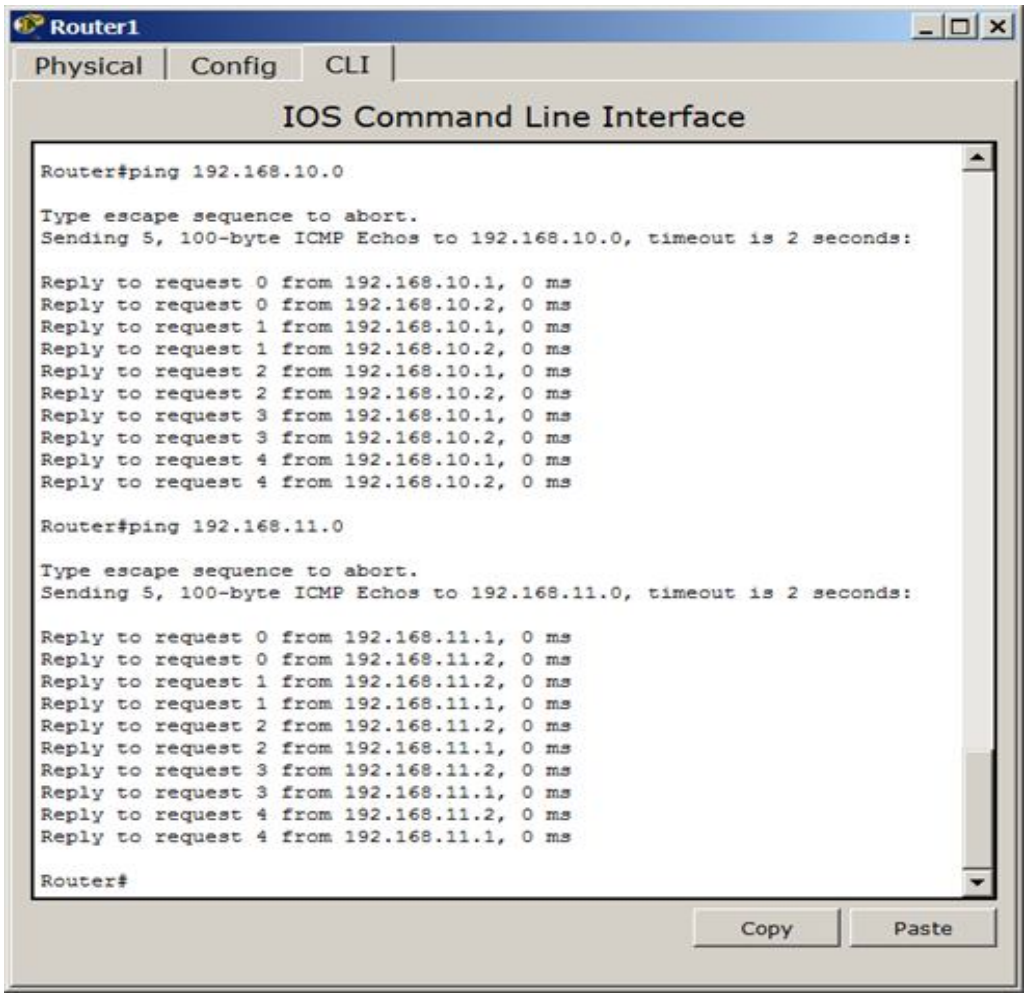

Рисунок 6.6 – Перевірка зв’язку роутера з ПК

І нарешті можна перевірити зв’язок ПК з різних мереж між собою (*ping*). З кожного ПК пропінгуємо інші. Пінги проходять – ПК взаємно доступні. Мережа налаштована.

6.4 Завдання

За допомогою програми *Cisco Packet Tracer* спроєктувати та побудувати таку мережу:

– сегмент 1 із чотирьох ПК на комутаторі 2960;

– сегмент 2 із п’яти ПК на комутаторі 2960;

– сегмент 3 із двох серверів на комутаторі 2960;

– маршрутизатор 2911 для об’єднання мереж;

– підмережі підключити до маршрутизатора гігабітними лінками;

– налаштувати IP-адреси підмереж і шлюзів;

– налаштувати мережу в такий спосіб, щоб сервери були доступні для всіх ПК.

6.5 Вимоги до змісту звіту

1. Звіт із практичної роботи повинен бути оформлений відповідно до загальноприйнятих правил оформлення практичних робіт і містити такі пункти:

– тема роботи;

– мета роботи;

– опис перебігу виконання роботи.

2. Для кожного завдання описати процес його виконання з проміжними рисунками та скріншотами.

6.6 Контрольні питання

1. Поясніть, для чого призначений маршрутизатор.

2. Перелічіть режими роботи з командним рядком.

3. Опишіть алгоритм створення й налаштування зв’язку двох мереж із використанням маршрутизатора.

4. Як налаштовується порт *fa0/1* роутера на роботу з мережею?

5. Як перевіряється таблиця маршрутизації роутера?

ПРАКТИЧНЕ ЗАНЯТТЯ № 7 НАЛАШТУВАННЯ МЕРЕЖІ З ДВОМА МАРШРУТИЗАТОРАМИ

7.1 Мета роботи

Ознайомлення з алгоритмами маршрутизації, а також вивчення статичних і динамічних принципів маршрутизації.

7.2 Необхідний теоретичний матеріал

Під маршрутизацією в мережах передачі даних розуміється процес визначення (вибору) шляху проходження інформації від джерела до адресата. Основною метою маршрутизації є забезпечення найкращого шляху проходження інформації з точки зору її мінімально можливої затримки та максимальної пропускної здатності мережі. Крім того, повинні забезпечуватися достатній захист і надійність передачі інформації.

Маршрутизація є однією з основних функцій мережевого рівня та в загальному випадку зводиться до вибору вузлом комутації шляху та подальшої передачі інформації, що надійшла на його вхід. При всій простоті постановки завдання, вибір оптимального маршруту є досить складним завданням, що не має однозначного вирішення для мереж із різною топологією, величиною та характером потоку даних. Складність вирішення цього завданні обумовлена низкою причин. По-перше, маршрутизація, як правило, вимагає координації роботи всіх вузлів мережі передачі даних. По-друге, система маршрутизації повинна справлятися з виходом із ладу окремих вузлів і ліній зв’язку. По-третє, система повинна враховувати перевантаження окремих областей мережі передачі даних і змінювати маршрути проходження повідомлень.

Варто зауважити, що основні принципи маршрутизації є загальними для різних видів комутації при цьому найбільшою різноманітністю способів

маршрутизації (рис. 7.1) характеризуються мережі комутації пакетів, щодо яких і будемо розглядати це питання.

Прийнято розрізняти централізовані й децентралізовані (розподілені) способи маршрутизації. У разі централізованого способу маршрутизація здійснюється одним центром управління (менеджером мережі), який визначає напрямок руху пакетів через мережу передачі даних. Вузли комутації цієї мережі приймають мінімальну участь в маршрутизації та мають порівняно просту структуру. Зі свого боку, при збільшенні кількості вузлів зростає складність організації централізованого управління мережею передавання даних. Істотним недоліком централізованого управлінні є безпосередня залежність надійності мережі від надійності її менеджера, яка зі збільшенням складності останнього має тенденцію до зниження. Крім того, менеджер мережі повинен мати оперативну інформацію про стан мережі, оскільки вихід із ладу вузла, або його перевантаженні може призвести до втрати працездатності всієї мережі.

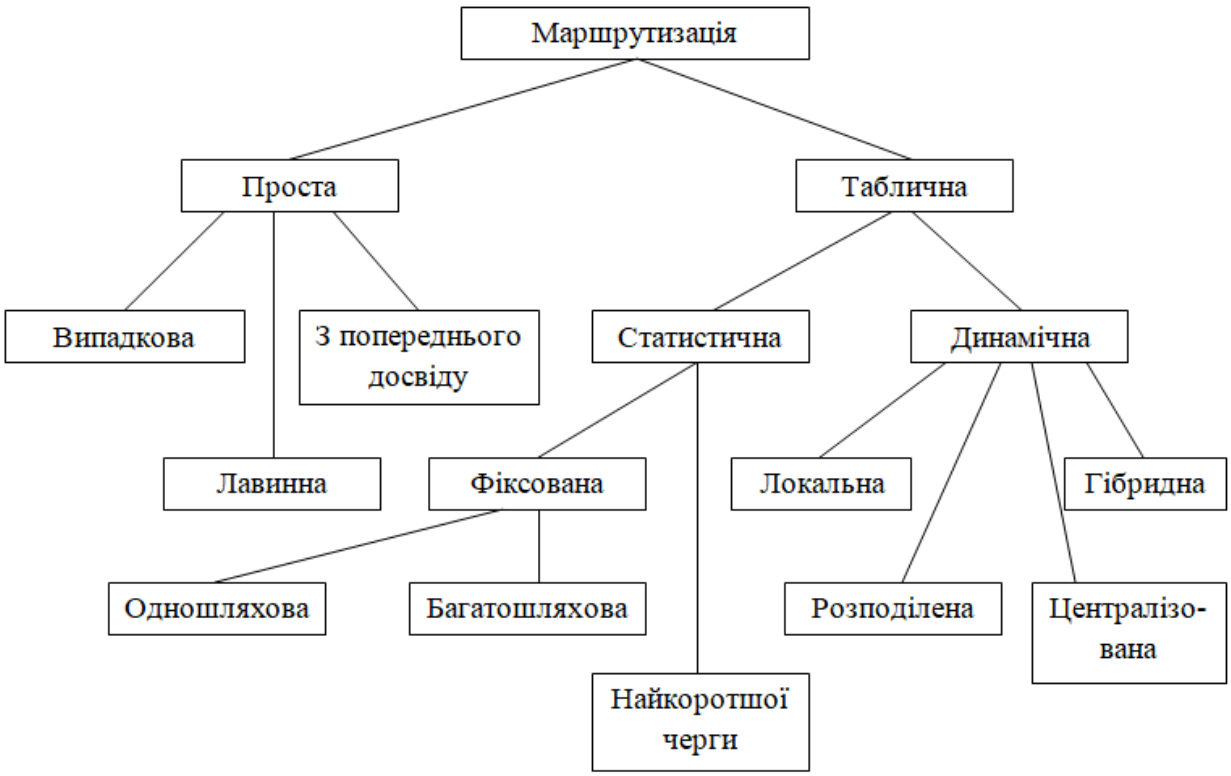

Рисунок 7.1 – Класифікація методів маршрутизації

При розподіленому управлінні кожен вузол самостійно, на основі інформації, що зберігається в ньому, визначає напрямок передачі пакетів. Це призводить до збільшення складності вузлів комутації. Однак система має більш високу живучість, оскільки вихід із ладу будь-якого вузла комутації не спричиняє втрату працездатності всієї мережі.

7.3 Порядок виконання роботи

Під час виконання роботи практично розглядаються основні команди операційної системи (далі – ОС) OSI (Internetwork Operating System), що використовуються для управління, налаштування та моніторингу пристроїв у мережі, з декількома маршрутизаторами: необхідно виконати конфігурацію двох маршрутизаторів на прикладі статичних маршрутів, привласнити імена вузлів мережі а також виконати перевірку конфігурації мережі та з'єднань.

Для виконання поставлених, завдань будуть потрібні наступні ресурси:

– два комутатора;

– два маршрутизатора;

– два ПК;

– кабелі Ethernet;

– ОС, що надає доступ до командного рядка.

Маршрутизатори мають інтерфейси *Fast Ethernet* і використовуються для з'єднання комутаторів. На ПК встановлюється програма емуляції терміналу. Схема ділянки досліджуваної мережі наведена на рисунку 7.2.

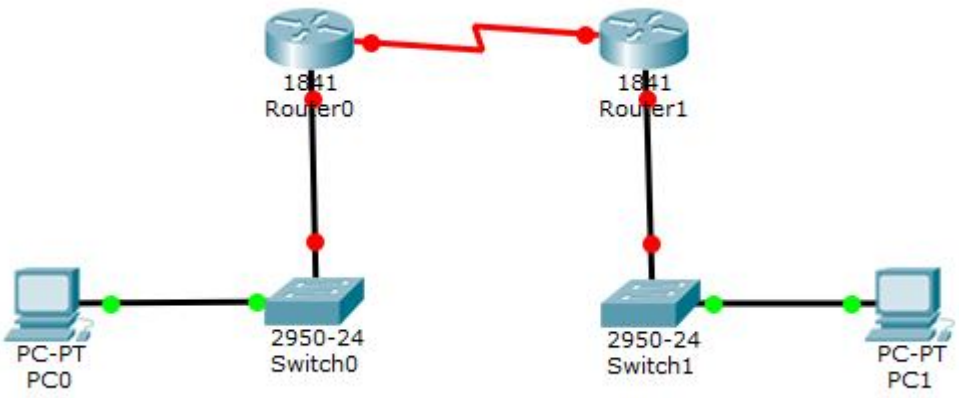

Рисунок 7.2 – Топологія модельованої мережі

Прикладним аспектом поставленого завдання є, наприклад, ситуація, при якій необхідно територіально розширити офіс компанії. Маршрутизатори необхідно налаштувати так, щоб організувати передачу трафіку між двома мережами.

Діяльність із реалізації завдання передбачає таке:

– створення топології мережі;

– установку модулів у маршрутизатори;

– підключення пристроїв мережі за допомогою кабелів;

– використання інтерфейсу командного рядка для базового налаштування маршрутизаторів;

– перевірку конфігурацій і можливостей підключення.

Розташування та конфігурація вузлів:

– перемістити два маршрутизатори (1841) з панелі інструментів на робоче поле;

– перемістити два комутатори (2950-24) із панелі інструментів на робоче поле;

– перемістити два комп’ютери (PC-PT) із панелі інструментів на робоче поле.

Для кожного з маршрутизаторів необхідно реалізувати таку послідовність дій:

– клацнути на іконці маршрутизатора *Router*. Відкриється вікно конфігурації маршрутизатора з вкладкою *Physical*;

– натиснути вимикач живлення для відключення маршрутизатора;

– перетягнута модуль *WIC-2T* на вільний слот праворуч;

– включити маршрутизатор і перейти на вкладку *CLI* дія перегляду завантаження процесу.

Далі потрібно присвоїти імена вузлам:

– клацнути на іконці маршрутизатора *Router 0*;

– вибрати опцію *Config*;

– встановити *Display Name в MainOffice*;

– клацнути на іконці маршрутизатора *Router 1*;

– вибрати опцію *Config*;

– встановити *Display Name в Rmt_Site1*.

Для підключення маршрутизатора за допомогою послідовного кабелю DCE (Data Communications Equipment), необхідно його вибрати на вкладці пристрою та з'єднати інтерфейс Serial0/1/0 маршрутизатора MainOffice з інтерфейсом Serial0/1/0 маршрутизатора Rmt_Site1. Отже, порядок вибору вузлів при підключенні кінців кабелю задає напрямок DCE-DTE. Згодом, для сторони DCE необхідно буде провести установку таймера (параметр *clock rate*).

Для з'єднання портів комутаторів і відповідних портів *FastEthernet0/0* маршрутизаторів, необхідно використовувати мідний кабель типу «*straight-through*». Також мідний кабель типу «*straight-through*» використовується для з'єднання інтерфейсів *FastEthernet* двох комп'ютерів із портом відповідного комутатора.

Для налаштування інтерфейсу *Fast Ethernet* вузла *PC0*, необхідно зайти у властивості вузла, і на вкладці «*Config*» вибрати пункт «*Interface – FastEthernet*». Потім необхідно встановити такі значення:

– IP address: 192.168.2.2;

– Subnet mask: 255.255.255.0;

– у пункті «*Global – Settings*»;

– *Gateway: 192.168.2.1.*

Для налаштування інтерфейсу вузла PC1 необхідно зайти у властивості вузла та на вкладці «*Config*» вибрати пункт «*Interface-FastEthernet*». Потім необхідно встановити такі значення:

– *IP address*: 172.16.255.253;

– *Subnet mask*: 255.255.0.0;

– у пункті «*Global-Settings*»;

– *Gateway*: 172.16.255.254.

Для призначення імені вузла маршрутизатора *MainOffice* необхідно:

– вибрати маршрутизатор *MainOffice* і в його властивостях – вкладку *CLI*;

– на питання «Continue with configuration dialog?» відповісти «*no*» і натиснути *ENTER*;

– перейти в режим глобального конфігурування (*Terminal Configuration Mode*), для чого послідовно ввести команди *Enable і configure terminal*. Якщо режим успішно активували, вид командного рядка зміниться *з* «*>*» на «#»;

– ввести команду *hostname MainOffice*;

– повернутися у вихідний режим (*Priveleged Exec mode*), натиснути сполучення клавіш *Ctrl і z*;

– зберегти конфігурацію, ввівши таку команду:

copy running – config startup – config.

Аналогічно необхідно призначити ім’я вузла *MainOffice* – другому маршрутизатору – *Rmt_Site1*.

Для налаштування послідовного інтерфейсу маршрутизатора *MainOffice*, необхідно:

– вибрати маршрутизатор *MainOffice*;

– перейти в режим глобального конфігурування (*Terminal Configuration Mode*);

– налаштувати послідовний інтерфейс *0/1/0*, для чого ввести команду *interface serial 0/1/0*;

– задати IP-адресу: *ip address 192.168.1.1 255.255.255.252;*

– задати тактову частоту: *clock rate 64000*;

– включити інтерфейс: *no shutdown*;

– повернутися у вихідний режим (*Priveleged Exec mode*).

Для налаштування інтерфейсу *Fast Ethernet* на маршрутизатор *MainOffice*, необхідно:

– вибрати маршрутизатор *MainOffice*;

– перейти в режим глобального конфігурування (*Terminal Configuration Mode)*;

– увести *interface fastethernet 0/0*;

– задати IP-адресу: *ip address 192.168.2.1 255.255.255.0;*

– включити інтерфейс: *no shutdown*;

– повернутися у вихідний: режим (*Priveleged Exec mode*);

– зберегти конфігурацію: *copy running-config startup-config*.

Потім аналогічно, за винятком завдання тактової частоти, необхідно налаштувати послідовний інтерфейс і інтерфейс *Fast Ethernet* на маршрутизаторі *Rmt_Site1*, використовуючи такі параметри:

– IP-адреса, для послідовного інтерфейсу: *192.168.1.2 255.255.255.252;*

– IP-адреса для інтерфейсу *Fast Ethernet: 172.16.255.254 255.255.0.0*

Вивчення динамічної маршрутизації. Для налаштування протоколу *RIP 2* на маршрутизаторі *MainOffice*, необхідно:

– вибрати маршрутизатор *MainOffice*;

– перейти в режим глобального конфігурування (*Terminal Configuration Mode)*;

– включити протокол *RIP* командою *router rip*;

– вказати версію протоколу (*RIP 2*): *version 2*;

– налаштувати мережі, що оголошуються:

MainOffice (config-router) #network 192.168.1.0

MainOffice (config-router) #network 192.168.2.0;

– повернутися у вихідний режим (*Priveleged Exec mode*);

– зберегти конфігурацію: *copy running-config startup-config*.

Аналогічно налаштувати протокол *RIP 2* на маршрутизаторі *Rmt_Sitel*, використовуючи такі параметри при налаштуванні мереж:

– Rmt_Site1 (config-router) #network 192.168.1.0;

– Rint_Site1 (config-router) #network 172.16.0.0.

Налаштування рівнів доступу проводиться з метою можливості активізації режиму *Priveleged Exec mode*. Для цієї мети переважно виконують доступ за паролем, для активації якого на обох маршрутизаторах необхідно увійти в режим глобального конфігурування (*Terminal Configuration Mode*) і ввести наступну команду, щоб задати пароль «*1ab34*»: *enable secret lab34*.

Щоб задати пароль для віддаленого доступу, необхідно увійти в режим глобального конфігурування (*Terminal Configuration Mode*) і ввести таку послідовність команд, щоб задати пароль. «*lab34_remote*»:

– для консольного режиму:

line console 0

password lab34_remote

login

exit

– для доступу через віртуальний термінал:

line vty 0 4

password lab34_remote

login

exit

Потім необхідно зберегти конфігурацію: *copy runnig-config startup-config*.

Для перевірки працездатності мережі необхідно виконати послідовність дій для кожного з маршрутизатора:

– увійти в режим *Priveleged Exec mode*;

– переглянути поточну, конфігурацію інтерфейсів за допомогою команди *show ip interface brief*;

– переглянути поточну таблицю конфігурації за допомогою команди *show ip route*;

– переглянути поточну конфігурацію маршрутизатора за допомогою *show running-config;*

– перевірити час передачі пакета між вузлами PC1 і PC0: PC > *ping 172.16.255.253*;

– виконати трасування маршруту між PC0 і PC1: PC > *tracert* 172.16.255.253.

7.4 Вимоги до змісту звіту

1. Звіт із практичної роботи повинен бути оформлений відповідно до загальноприйнятих правил оформлення практичних робіт і містити такі пункти:

– тема роботи;

– мета роботи;

– опис перебігу виконання роботи.

2. Для кожного завдання описати процес його виконання з проміжними рисунками та скріншотами.

7.5 Контрольні питання

1. Що розуміється під поняттям «маршрутизація»?

2. Які ви знаєте методи маршрутизації?

3. Охарактеризуйте поняття «централізовані та децентралізовані» (розподілені) способи маршрутизації.

4. Опишіть алгоритм налаштування конфігурації двох маршрутизаторів на прикладі статичних маршрутів.

5. Розкажіть, які ви виконували дії для реалізації завдання.

6. Як ви використовували інтерфейс командного рядка для базового налаштування маршрутизаторів?

7. Як ви виконували перевірку конфігурацій і можливостей підключення маршрутизаторів?

ПРАКТИЧНЕ ЗАНЯТТЯ № 8 НАЛАШТУВАННЯ DHCP-СЕРВЕРА НА РОУТЕРІ

8.1 Мета роботи

Отримання навичок налаштування *DHCP*-серверу на роутері з використанням програми *Cisco Packet Tracer*.

8.2 Необхідний теоретичний матеріал

Dynamic Host Configuration Protocol (DHCP) – це протокол управління мережею, який використовується в мережах TCP/IP, у якому DHCP-сервер динамічно привласнює кожному пристрою IP-адресу та інші параметри конфігурації мережі, щоб вони могли зв'язуватися з іншими IP-мережами.

Система доменних імен, більш відома як DNS, і протокол конфігурації динамічного хоста, також відомий як DHCP, становлять дві важливі області TCP/IP у мережі. DNS відповідає за перетворення імен хостів в IP-адреси, тоді як DHCP займається призначенням унікальних динамічних IP-адрес і відповідних масок підмережі та шлюзів за замовчуванням для запущених комп'ютерів у конкретній серверної мережі.

Завдяки динамічній адресації комп'ютер може мати іншу IP-адресу при кожному підключенні до мережі, до якої він належить, без втручання адміністратора. Завдяки цій функції DHCP кожному новому комп'ютеру, доданому в мережу, автоматично призначається унікальна IP-адреса. DHCP-сервери значно спрощують налаштування мереж і використовуються в більшості бездротових точок доступу та дротових Ethernet-маршрутизаторах.

8.3 Приклад налаштування DHCP-сервера на роутері Cisco-2950

Розглянемо мережу задану на рисунку 8.1 конфігурації. Тут усі пристрої містяться в одному сегменті 192.168.1.0/24, створюваному концентратором *Svitch0*. Шлюзом у мережі слугує роутер R1.

Потрібно конфігурувати маршрутизатор 2811, а саме налаштувати на ньому DHCP-сервер, який буде видавати по DHCP-адресі з пулу адрес мережі 192.168.1.0 для всіх ПК, підключених до комутатора. До того ж у налаштуваннях передбачена можливість задавати статичні адреси деяким обраним пристроям, наприклад серверу.

У наслідок цього PC1 і PC2 повинні отримувати налаштування динамічно, а сервер повинен мати попередньо встановлену статичну адресу.

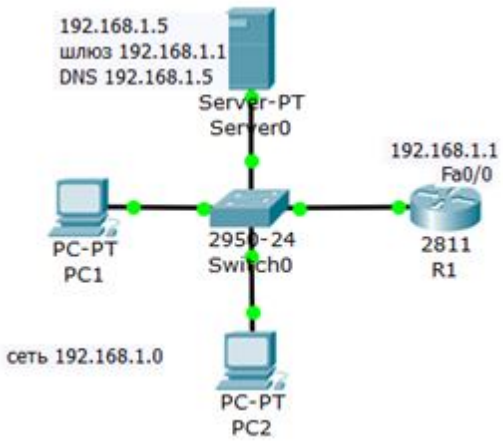

Рисунок 8.1 – Схема мережі

Розв'язання.

Попередньо за допомогою пакета *Cisco Packet Tracker* створимо й налаштуємо вихідну мережу (рис. 8.1). Перевіримо доступність сервера та маршрутизатора (шлюзу) з кожного ПК.

Якщо все доступно, заходимо на *роутер R1*, входимо в режим глобального конфігурування та виконуємо такі дії:

1. Резервуємо пул із 10 адрес:

R1 (config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10

Цією командою ми зобов'язали *роутер R1* не видавати адреси в діапазоні 192.168.1.1 – 192.168.1.10 при автоматичному призначення адрес у сегменті. Ми ці адреси резервуємо для своїх цілей, а саме:

– адресу 192.168.1.1 ми призначимо самому *роутеру*, як шлюз «за замовчуванням»;

– адресу 192.168.1.5 призначимо вручну для нашого сервера. На цьому самому сервері піднято DNS-сервіс і ми цю адресу зможемо використовувати як DNS-сервер;

– інші адреси зарезервуємо під майбутні хости цієї мережі.

Відповідно, першою DHCP-адресою, яку видасть *розтер,* повинна бути адреса 192.168.1.11.

2. Створюємо пул адрес, які будуть розподілятися між пристроями мережі:

R1 (config)#ip dhcp pool POOL1

R1 (dhcp-config)#network 192.168.1.0 255.255.255.0

R1 (dhcp-config)#default-router 192.168.1.1 – встановлюємо адресу шлюзу за умовчаннням

R1 (dhcp-config)#domain-name my-domain.com

R1 (dhcp-config)#dns-server 192.168.1.5 – встановлюємо адресу DNS сервера

3. Налаштовуємо (піднімаємо) *інтерфейс роутера:*

R1 (config)#interfacefa0/0

R1 (config-if)#ip address 192.168.1.1 255.255.255.0

R1 (config-if)#no shutdown

R1 (config-if)#exit

R1(config)#exit

R1#

Примітка. На всіх роутерах за замовчуванням усі інтерфейси знаходяться в пасивному стані (*down*). Команда *no shut* (скорочення від *no shutdown*)

використовується для того, щоб інтерфейс став активним. Зворотня команда – *shut*, вимкне інтерфейс.

Тепер потрібно зайти на PC1 PC2 і встановити в мережевих налаштуваннях отримання IP-адреси й адреси DNS-сервера в автоматичний режим.

Перевірка результату. Тепер обидва ПК отримали налаштування й командою *R1#show ip dhcp binding* на роутері можна подивитися на список виданих роутером адрес (рис. 8.2).

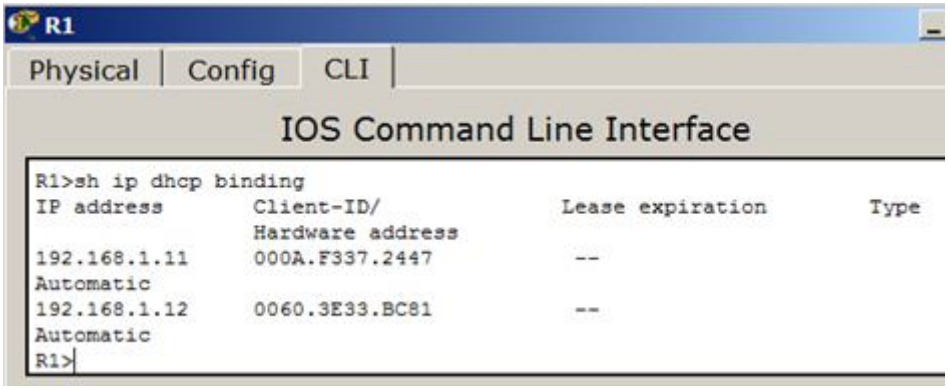

Рисунок 8.2 – Адреси видаються автоматично, починаючи з адреси 192.168.1.11

Отже, ми бачимо, що протокол DHCP дозволяє виробляти автоматичне налаштування мережі на всіх комп'ютерах (рис. 8.3).

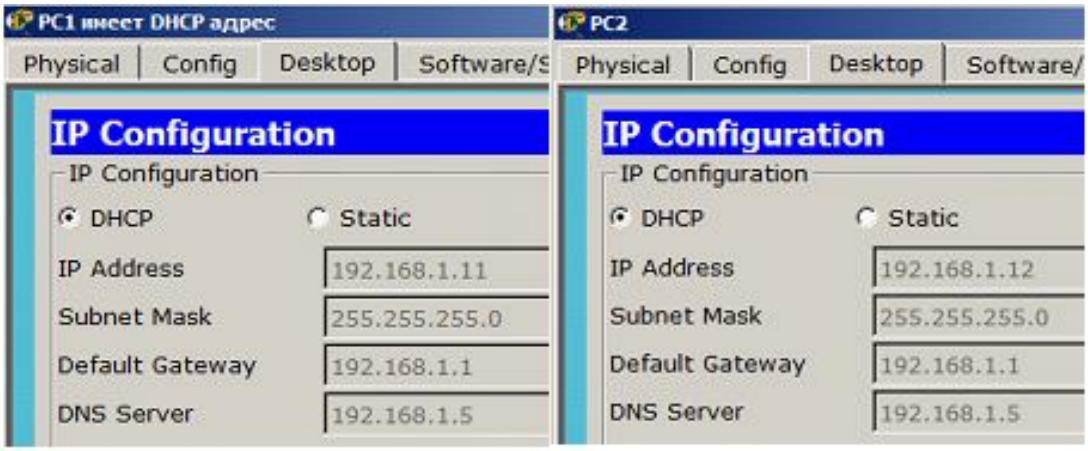

Рисунок 8.3 – PC1 і PC2 отримують IP-адреси від DHCP-сервера

8.4 Завдання

Додайте у вихідний сегмент два ПК і переконайтеся, що налаштування мережевих адрес, шлюзу та DNS відбудеться автоматично.

8.5 Вимоги до змісту звіту

1. Звіт із практичної роботи повинен бути оформлений відповідно до загальноприйнятих правил оформлення практичних робіт і містити такі пункти:

– тема роботи;

– мета роботи;

– опис перебігу виконання роботи.

2. Для кожного завдання описати процес його виконання з проміжними рисунками та скріншотами.

8.6 Контрольні питання

1. Дайте визначення протоколу Dynamic Host Configuration Protocol (DHCP).

2. Поясніть, що таке DHCP-сервер.

3. Розкажіть, які ви виконували дії для реалізації прикладу налаштування DHCP-сервера на роутері Cisco-2950.

4. Як ви виконували перевірку результату?

ПРАКТИЧНЕ ЗАНЯТТЯ № 9 КОНФІГУРАЦІЯ МЕРЕЖЕВИХ ЗАСОБІВ НА ОСНОВІ ПРОТОКОЛУ OSPF

9.1 Мета роботи

Отримати практичні навички конфігурації пристроїв «Cisco» використовуючи протокол маршрутизації OSPF.

9.2 Необхідний теоретичний матеріал

OSPF (Open Shortest Path First) – протокол динамічної маршрутизації, який:

– створено IETF у 1988 році (тобто є стандартним протоколом);

– OSPFv2 це поточна версія для IPv4 (описана в RFC 2328);

– IGP-протокол використовується для передачі інформації між маршрутизаторами в межах однієї автономної системи (AS);

– оснований на технології *link-state* (SPF).

Термінологія протоколу OSPF*:*

Канал/інтерфейс (link/interface) – з'єднання маршрутизатора з однією з підключених до нього мереж. Під час обговорення OSPF терміни інтерфейс і канал (*link*) часто вживаються як синоніми.

Метрика (metric) – умовний показник відстані до мережі призначення.

Вартість (cost) – умовний показник «вартості» пересилання даних по каналу. У OSPF залежить від пропускної здатності інтерфейсу (*bandwidth*).

Автономна система (autonomous system) – група маршрутизаторів, що обмінюється інформацією за допомогою одного протоколу маршрутизації (визначення відповідає тому, як цей термін використовується в протоколах IGP).

Ідентифікатор маршрутизатора (router ID, RID) – унікальне 32-бітове число, яке унікально ідентифікує маршрутизатор у межах однієї автономної системи.

Зона (area) – сукупність мереж і маршрутизаторів, що мають один і той самий ідентифікатор зони.

Оголошення про стан каналу (link-state advertisement, LSA) – одиниця даних, яка описує локальний стан маршрутизатора або мережі. Наприклад, для маршрутизатора LSA включає опис стану каналів і сусідство. Безліч усіх LSA, що описують маршрутизатори та мережі, утворюють базу даних стану каналів (LSDB).

База даних стану каналів (link state database, LSDB) – список усіх записів про стан каналів (LSA). Зустрічається також термін «*топологічна база даних (topological database)*», вживається як синонім бази даних стану каналів.

Сусіди (neighbours) – два маршрутизатори, інтерфейси яких знаходяться в одному широкомовному сегменті (і на яких включений OSPF на цих інтерфейсах).

Відносини сусідства (adjacency) – взаємозв'язок між сусідніми маршрутизаторами встановлено з метою синхронізації інформації.

База даних сусідів (neighbours database) – список усіх сусідів (також використовується термін «*neighbour table*»).

Пакети OSPF:

Hello – пакети, які використовуються для виявлення сусідів, установлення відносин сусідства та моніторингу їх доступності *(keep alive).*

DBD – пакети, які описують зміст *LSDB*.

LSR – пакети, за допомогою яких запитується повна інформація про *LSA*, якої бракує в *LSDB* локального маршрутизатора.

LSU – пакети, які передають повну інформацію, яка є в *LSA*.

LSAck – пакети, за допомогою яких підтверджується отримання інших пакетів.

9.3 Опис роботи протоколу

1. Включити *OSPF* на маршрутазаторі.

2. Маршрутизатор вибирає *Router ID* (унікальне ім’я маршрутизатора).

3. Включити *OSPF* на інтерфейсах (щоб протокол знав, про які інтерфейси можна повідомляти іншим маршрутизаторамh).

4. Виявлення сусідів за допомогою *hello-пакетів*:

а) маршрутизатори обмінюються *hello-пакетами* через усі інтерфейси на яких активований *OSPF*;

б) маршрутизатори, які знаходяться в одному широкомовному сегменті, стають сусідами, коли вони приходять до домовленості про визначені параметри, зазначені в їх *hello-пакетах*.

5. *Adjacency* (відносини сусідства, відносини суміжності) це тип сусідства між маршрутизаторами, за яким вони синхронізують *LSDB*. Установка цих відносин залежить від типу мережі:

а) якщо маршрутизатори перебувають у мережі з множинним доступом, вони вибирають *DR* і виконують синхронізацію *LSDB* з ним;

б) якщо маршрутизатори перебувають у мережі *point-to-point*, вони розпочинають синхронізацію *LSDB* один з одним.

6. Синхронізація *LSDB* відбувається в кілька етапів. За сформованими відносинами сусідства відбувається обмін такими пакетами:

а) *DBD* (короткий опис *LSA* в *LSDB*). За допомогою цих пакетів маршрутизатори повідомляють один одному про те, яку інформацію вони знають, у скороченому вигляді;

б) *LSR*. Після обміну *DBD-пакетами*, за допомогою *LSR* маршрутизатори запитують у сусіда інформацію, якої бракує;

в) *LSU* (містить повний опис *LSA*). У відповідь на *LSR*, який йому надіслав сусід, маршрутизатор відправляє *LSU*, з повним описом інформації, якої не вистачає у сусіда;

г) *LSAck*. Після отримання *LSU від сусіда*, маршрутизатор відправляє підтвердження, що він отримав інформацію;

д) якщо обидва маршрутизатори повинні запитати один в одного інформацію, то ця процедура повторюється й в іншу сторону;

е) після цього *LSDB* синхронізована, отже повністю однакова між сусідами.

7. Після синхронізації *LSDB*, маршрутизатор відправляє оновлення далі своїм сусідам в інших широкомовних сегментах.

8. Розсилаючи оголошення через зону, у всіх маршрутизаторів буде ідентичний *LSDB*.

9. Коли база даних побудована, кожен маршрутизатор використовує алгоритм *SPF (shortest path first)* для обчислення графа без петель, який буде описувати найкоротший шлях до кожного відомого пункту призначення з собою як кореня. Цей граф – дерево найкоротшого шляху.

10. Кожен маршрутизатор будує таблицю маршрутизації, ґрунтуючись на своєму дереві найкоротшого шляху.

Типи мереж, підтримувані протоколом *OSPF*:

– широкомовні мережі з множинним доступом *(broadcast*): Ethernet;

– точка-точка (*point-to-point*): тунелі, *T1, E1, PPP, HDLC, Frame-RelayP-to-P;*

– не широкомовні мережі з множинним доступом (*Non Broadcast Multiple Access, NBMA): Frame-Relay, ATM, X.25.*

У різних типах мереж робота *OSPF* відрізняється, зокрема відрізняється процес встановлення відносин сусідства та налаштування протоколу.

Виділений маршрутизатор (DR) і резервний виділений маршрутизатор (BDR).

У мережах із множинним доступом відносини сусідства повинні бути встановлені між усіма маршрутизаторами. Це призводить до того, що розсилається велика кількість копій LSA. Якщо, наприклад, кількість маршрутизаторів у мережі з множинним доступом один n, то буде встановлено n (n-1)/2 відносин сусідства. Кожен маршрутизатор буде розсилати n-1 LSA своїм сусідам, плюс одне LSA для мережі, в результаті мережа згенерує n^2 LSA.

Для запобігання проблеми розсилки копій LSA в мережах із множинним доступом вибираються DR і BDR.

Виділений маршрутизатор *(designated router, DR)* – управляє процесом розсилання LSA в мережі. Кожен маршрутизатор мережі встановлює відносини сусідства з DR. Інформація про зміни в мережі відправляється DR, маршрутизатором який виявив зміни, а DR відповідає за те, щоб ця інформація була відправлена іншим маршрутизаторам мережі. Недоліком у схемі роботи з DR маршрутизатором є те, що при виході його з ладу повинен бути обраний новий DK. Нові відносини сусідства повинні бути сформовані і, поки бази даних маршрутизаторів не синхронізуються з базою даних нового DR, мережа буде недоступна для пересилання пакетів. Для усунення цього недоліку вибирається BDR.

Резервний виділений маршрутизатор *(backup designated router, BDR).* Кожен маршрутизатор мережі встановлює відносини сусідства не тільки з DR, але й BDR. DR і BDR також встановлюють відносини сусідства та між собою. При виході з ладу DR, BDR стає DR і виконує всі його функції. Оскільки маршрутизатори мережі встановили відносини сусідства з BDR, то час недоступності мережі мінімізується.

Маршрутизатор, обраний DR або BDR в одній приєднаній до нього мережі з множинним доступом, може не бути DR (BDR) в іншій приєднаній мережі. Роль DR (BDR) є властивістю інтерфейсу.

9.4 Порядок виконання роботи

На рисунку 9.1 наведена топологія мережі та необхідне обладнання.

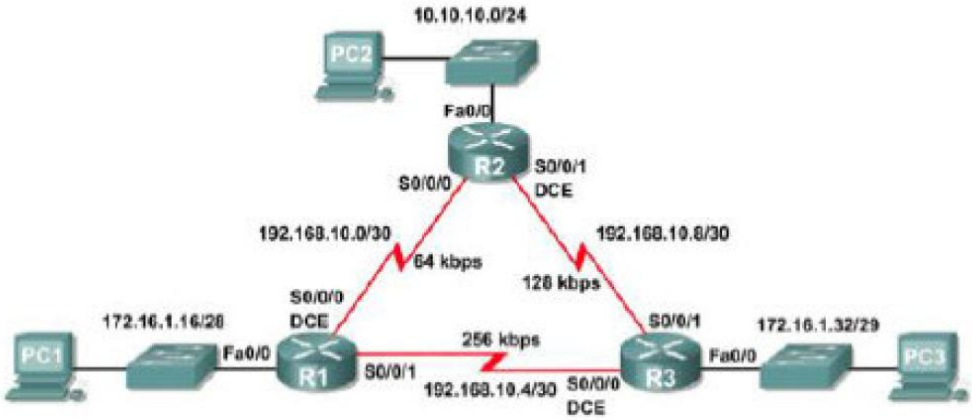

Рисунок 9.1 – Топологія мережі

Необхідні дані для проєктування наведені у таблиці 9.1

Таблиця 9.1 – Необхідні дані

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
R1	Fa0/0	172.16.1.17	255.255.255.240	N/A
	S0/0/0	192.168.10.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	Fa0/0	10.10.10.1	255.255.255.0	N/A
	S0/0/0	192.168.10.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	Fa0/0	172.16.1.33	255.255.255.248	N/A
	S0/0/0	19.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	N|C	172.16.1.20	255.255.255.240	172.16.1.17
PC2	N|C	10.10.10.10	255.255.255.0	10.10.10.1
PC3	N|C	172.16.1.35	255.255.255.248	172.16.1.33

1. Конфігурація.

Вибрати зі списку *Routers, Switches*, PC і розташувати на полі.

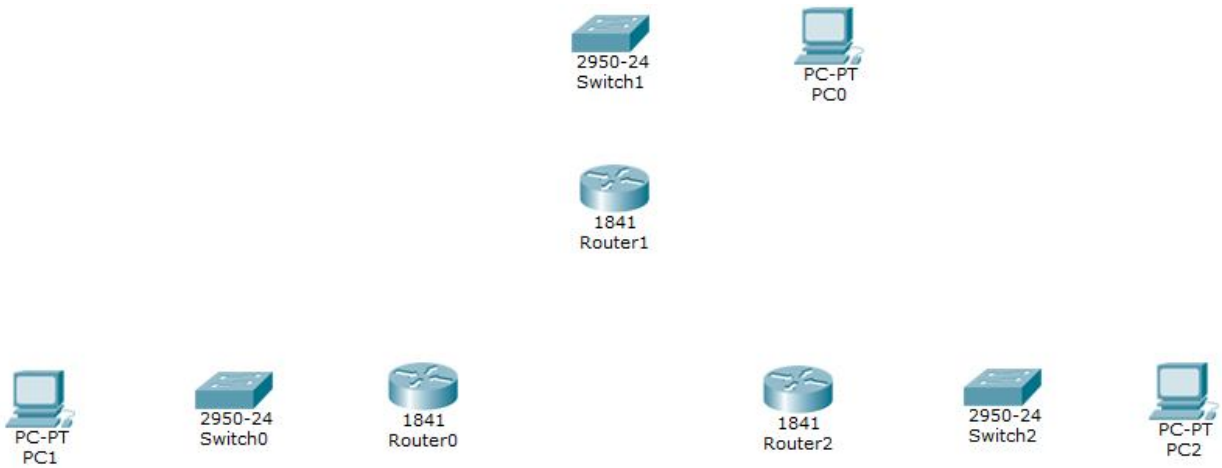

Рисунок 9.2 – Вибір обладнання

2. При натисканні на *Router* з’явиться вікно, в якому:

– виключити маршрутизатор;

– додати зі списку зліва модуль *WIC-2T*, перетягнувши його в одне з вільних місць;

– включити маршрутизатор.

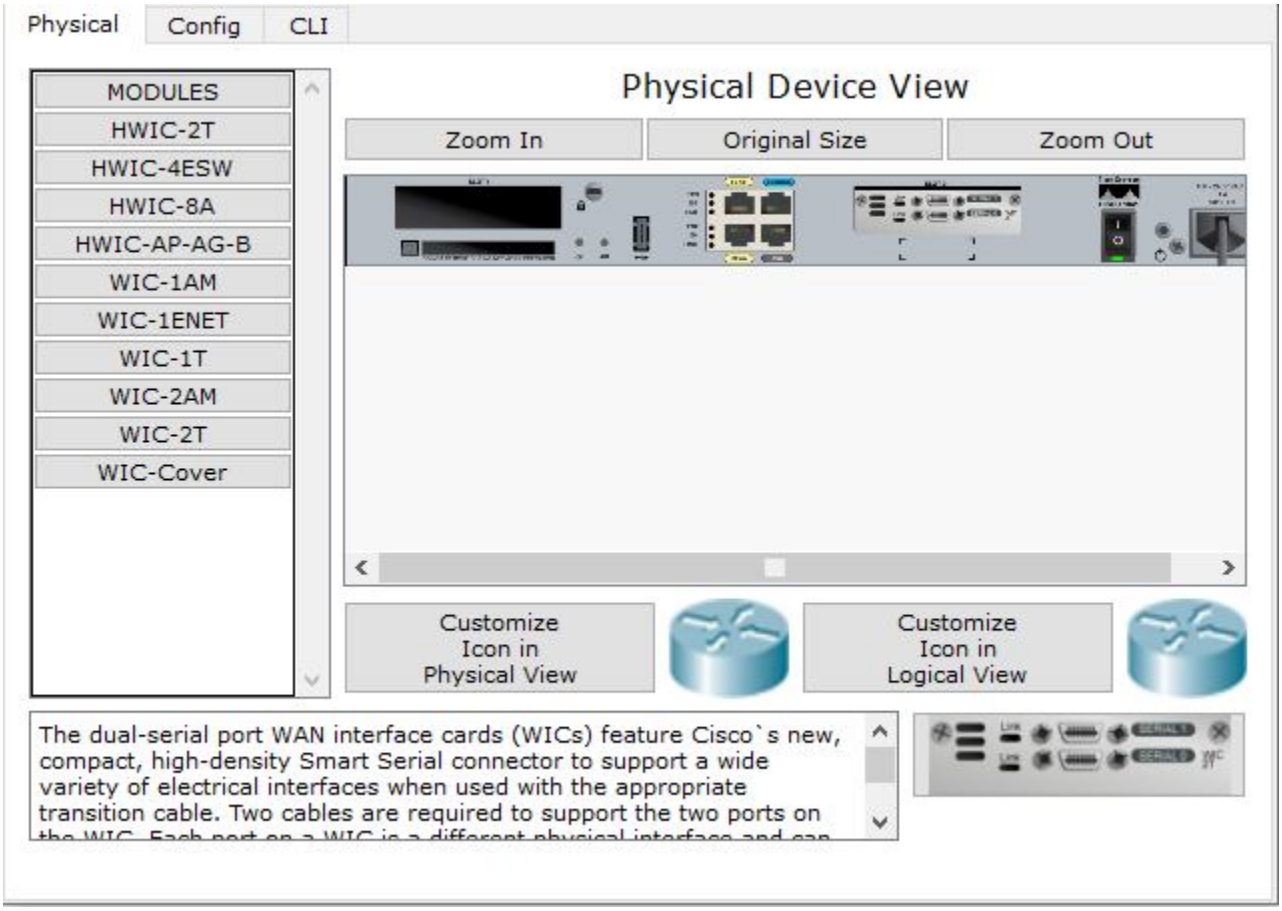

Рисунок 9.3 – Підключення маршрутизатора

3. З’єднати *Routers Serial* кабелем, а *Routers, Switches PC* – прямим кабелем.

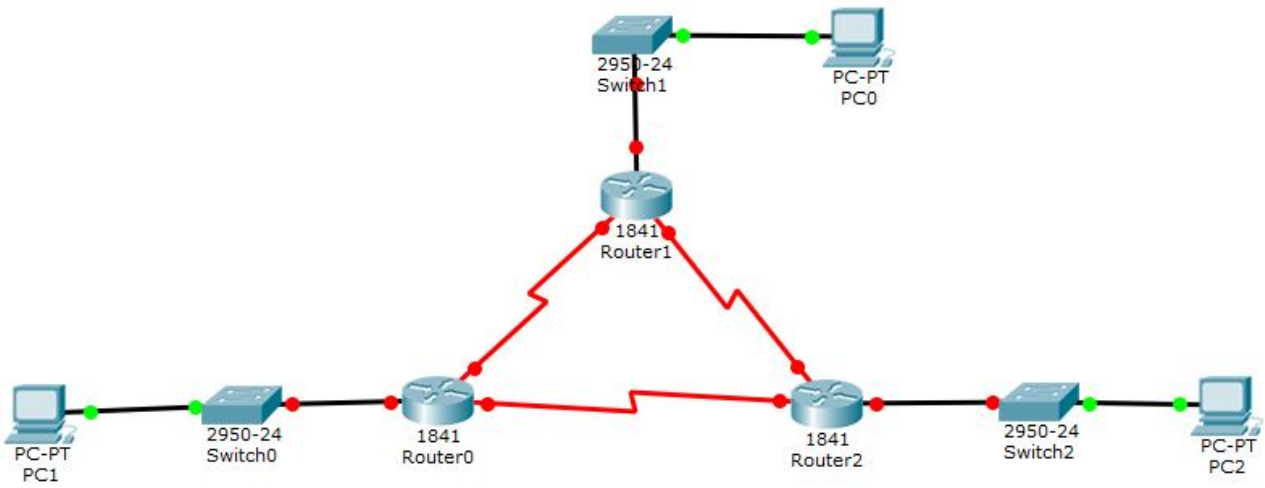

Рисунок 9.4 – З’єднання пристроїв

4. Натискаємо на *Router* і вибираємо панель *CLI* (рис. 9.5), набираємо команду *«no»*. Відповідно так робимо на всіх маршрутизаторах.

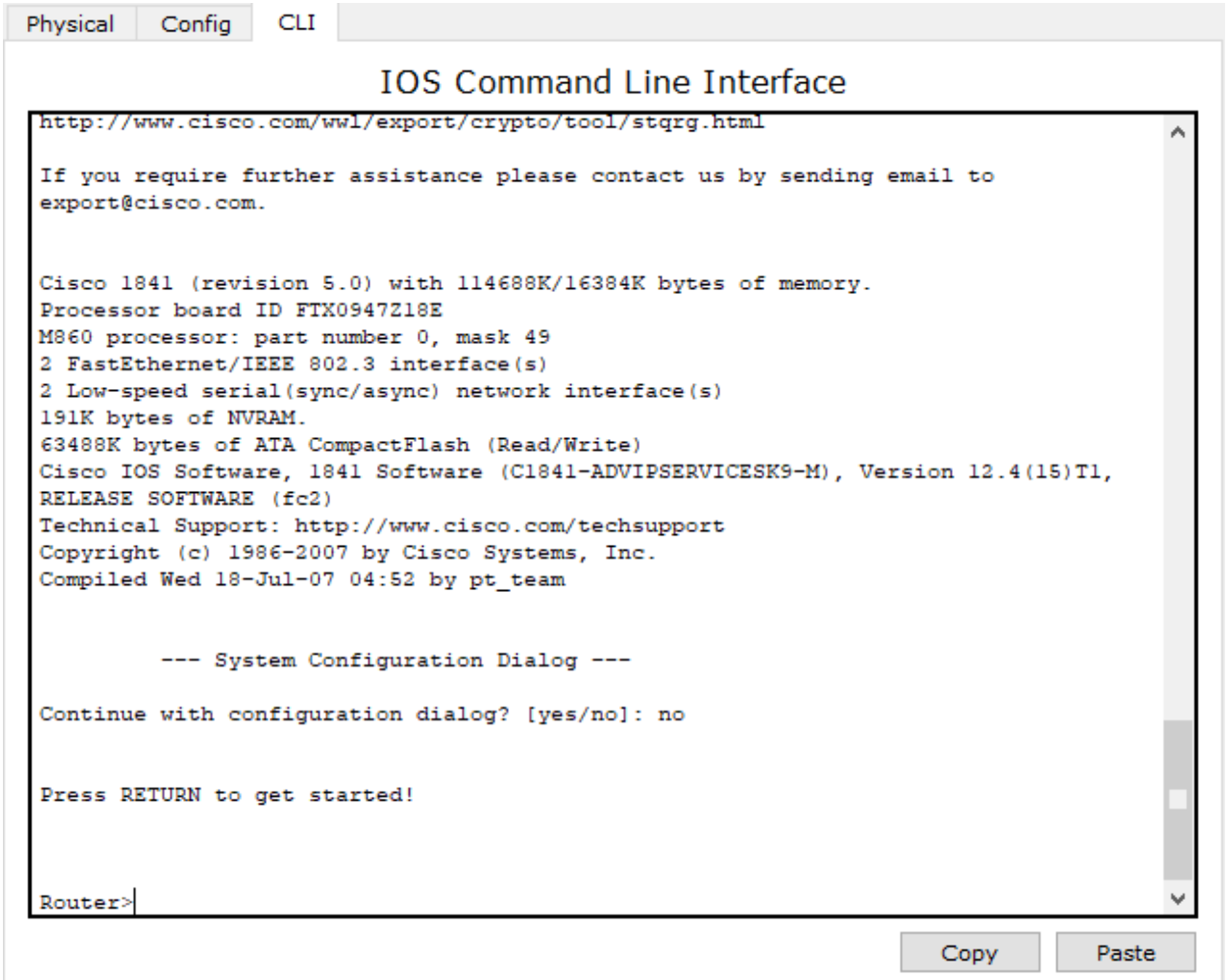

Рисунок 9.5 – Панель CLI

5. Входимо в привілейований режим *Router> enable*

6. Входимо в режим глобальної конфігурації *Router# configure terminal*

7. Змінюємо ім’я маршрутизатора *Router (config)#hostname R1*

R1 (config)#

8. Конфігуруємо інтерфейси на *Router1* і запускаємо:

R1 (config)#interface fastEthernet 0/0

R1 (config-if)#ip add 172.16.1.17 255.255.255.240

R1 (config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R1 (config-if)#exit

R1 (config)#interface Serial 0/0/0

R1 (config-if)#ip add 192.168.10.1 255.255.255.252

R1 (config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

R1 (config-if)#exit

R1 (config)#interface Serial 0/0/1

R1 (config-if)#ip add 192.168.10.5 255.255.255.252

R1 (config-if) #no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

R1 (config-if)#exit

Налаштовуємо *OSPF*, задаємо мережі для маршрутизатора:

– одиниця – це номер процесу на маршрутизаторі, на маршрутизаторах однієї області може відрізнятися;

– 0.0.0.3 – це wild card mask (перевернута маска), *area 0* – це номер області, на всіх маршрутизаторах однієї області він повинен бути однаковий.

R1 (config)#router ospf 1

R1 (config-router)#network 172.16.1.16 0.0.0.15 area 0

R1 (config-router)#network 192.168.10.0 0.0.0.3 area 0

03:00:43: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.9 on Serial0/0/0 from LOADING to FULL, Loading Done

R1 (config-router)#network 192.168.10.4 0.0.0.3 area 0

R1 (config-router) #end

03:24:26: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.10 on Serial0/0/1 from LOADING to FULL, Loading Done

9. Конфігуруємо інтерфейси на *Router2* і запускаємо:

R2 (config)# interface fastEthernet 0/0

R2 (config-if)#ip add 10.10.10.1 255.255.255.0

R2 (config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R2 (config-if)#exit

R2 (config)#interface Serial 0/0/0

R2 (config-if)#ip add 192.168.10.2 255.255.255.252

R2 (config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2 (config-if)#exit

R2 (config)# interface Serial 0/0/1

R2 (config-if)#ip add 192.168.10.9 255.255.255.252

R2 (config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

R2 (config-if) #exit

R2 (config)#router ospf 1

R2 (config-router)#network 10.10.10.0 0.0.0.255 area 0

R2 (config-router)#network 192.168.10.0 0.0.0.3 area 0

00:06:28: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0 from LOADING to FULL, Loading Done

R2 (config-router)#network 192.168.10.8 0.0.0.3 area 0

R2 (config-router) #end

00:30:05: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.10 on Serial0/0/1 from LOADING to FULL, Loading Done

10. Конфігуруємо інтерфейси на *Router3* і запускаємо:

R3 (config) #interface fastEthernet 0/0

R3 (config-if) #ip add 172.16.1.33 255.255.255.248

R3 (config-if) #no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R3 (config-if) #exit

R3 (config) #interface Serial 0/0/0

R3 (config-if) #ip add 192.168.10.6 255.255.255.252

R3 (config-if) #no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R3 (config-if) #exit

R3 (config) #interface Serial 0/0/1

R3 (config-if) #ip add 192.168.10.10 255.255.255.252

R3 (config-if) #no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

R3 (config-if) #exit

R3 (config) #router ospf 1

R3 (config-router)#network 172.16.1.32 0.0.0.7 area 0

R3 (config-router) #network 192.168.10.4 0.0.0.3 area 0

R3 (config-router) #

01:13:16: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0 from LOADING to FULL, Loading Done

R3 (config-router) #network 192.168.10.8 0.0.0.3 area 0

R3 (config-router) #end

01:13:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.9 on Serial0/0/1 from LOADING to FULL, Loading Done

У результаті ми отримуємо мережу, яка наведена на рисунку 9.6.

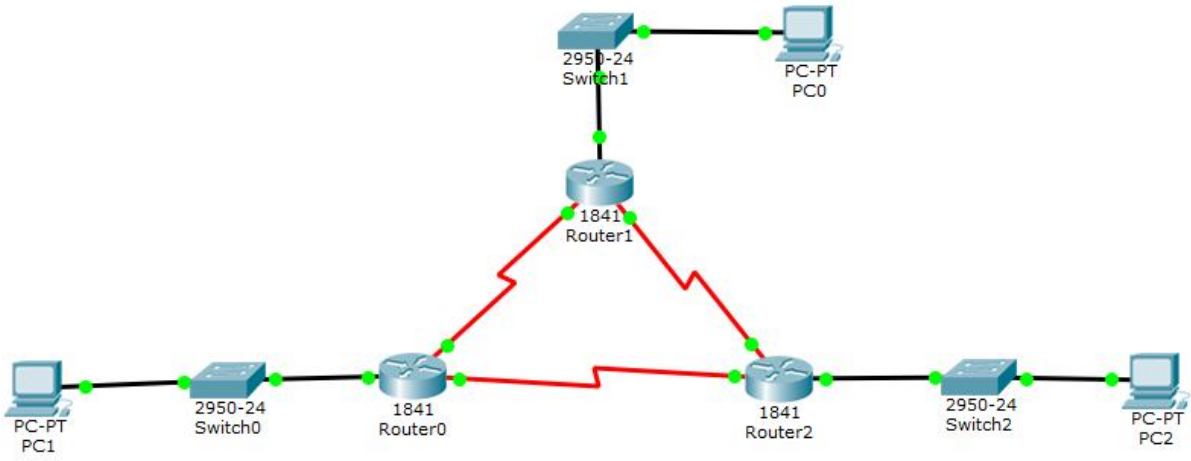

Рисунок 9.6 – Конфігурація пристроїв

11. Налаштовуємо PC і перевіряємо *ping* (рис. 9.7).

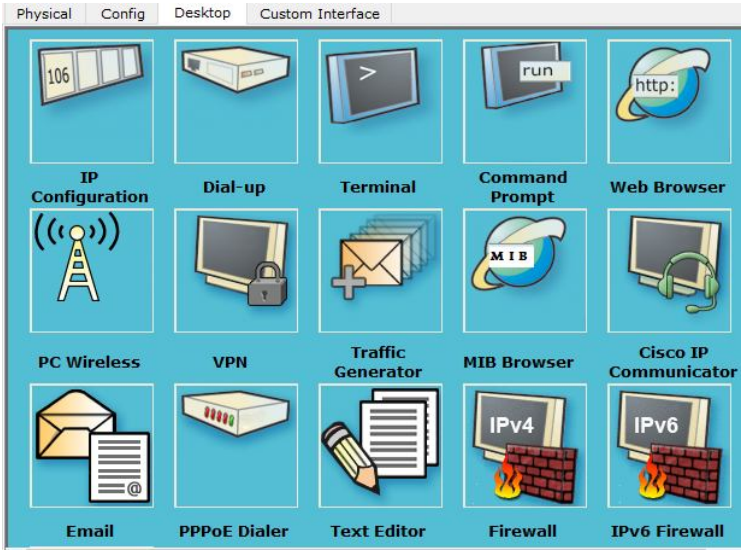

Рисунок 9.7 – Налаштування PC

Вибираємо IP *Configuration* і вносимо дані з таблиці адрес 9.1.

Заходимо в *Command Prompt* і пишемо адресу *ping,* адресу *хоста* іншої мережі (рис. 9.8).

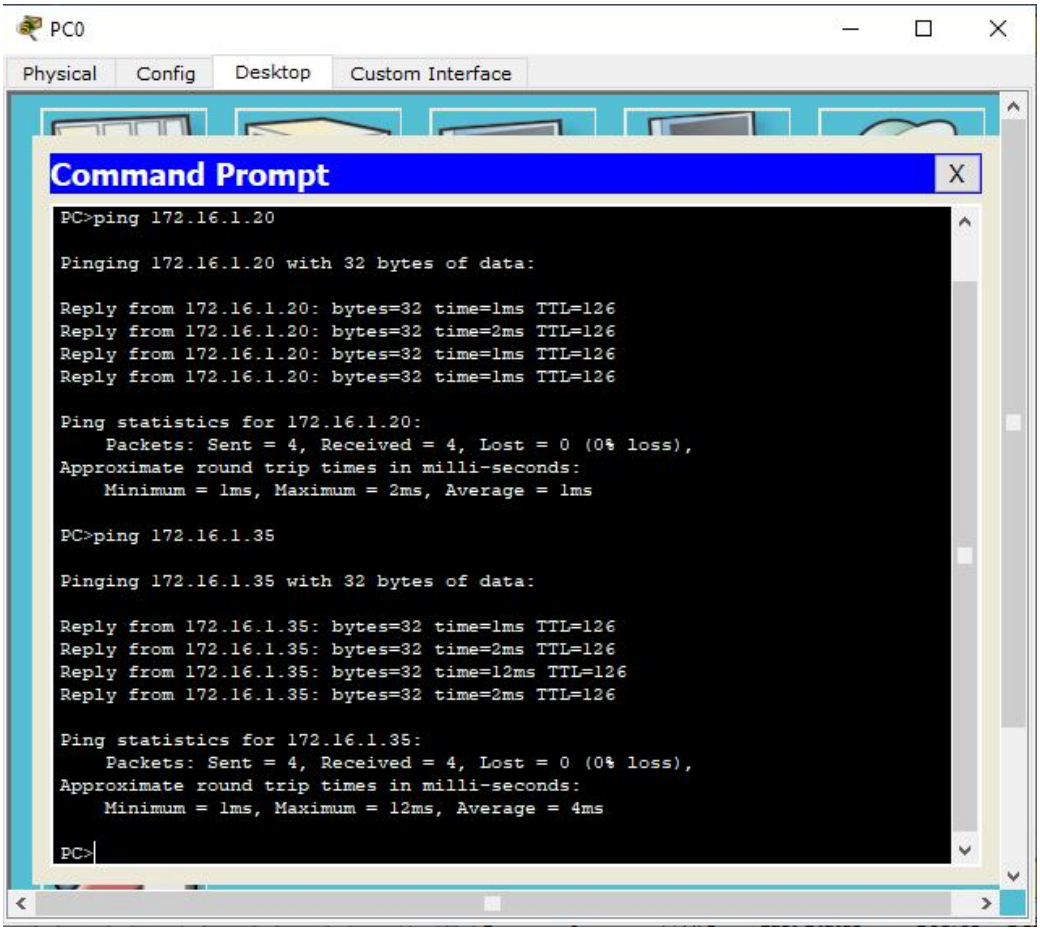

Рисунок 9.8 – Перевірка ping

Команди:

1) *R# show running-config*

Показує нам конфігураційний файл;

2) *R# show ip protocols*

Показуєм, які протоколи динамічної маршрутизації сконфігуровані та які параметри для них налаштовані;

3) *R# show ip route*

Показує таблицю маршрутизації, задіяні інтерфейси й метрики за конкретними маршрутами.

9.5 Вимоги до змісту звіту

1. Звіт із лабораторної роботи повинен бути оформлений відповідно до загальноприйнятих правил оформлення лабораторних робіт і містити такі пункти:

– тема роботи;

– мета роботи;

– опис перебігу виконання роботи.

2. Для кожного завдання описати процес його виконання з проміжними рисунками та скріншотами.

9.6 Контрольні питання

1. Дайте визначення протоколу OSPF (Open Shortest Path First).

2. Яке призначення протоколу OSPF?

3. Дайте визначення протоколу IGP.

4. Охарактеризуйте термінологію протоколу OSPF.

5. Перелічить і надайте характеристику пакетів OSPF.

6. Охарактеризуйте роботу протоколу.

7. Назвіть типи мереж, які підтримуються протоколом OSPF.

8. Для чого необхідний виділений маршрутизатор (DR) і резервний виділений маршрутизатор (BDR)?

ПРАКТИЧНЕ ЗАНЯТТЯ № 10 КОНФІГУРАЦІЯ МЕРЕЖЕВИХ ЗАСОБІВ НА ОСНОВІ ПРОТОКОЛУ RIPV2

10.1 Мета роботи

Отримати практичні навички конфігурації пристроїв «Cisco», використовуючи протокол маршрутизації RIPv2.

10.2 Необхідний теоретичний матеріал

Routing Information Protocol (RIP) використовує широкомовні *User Datagram Protocol (UDP)* пакети даних для обміну маршрутною інформацією. RIPv2 є безкласовим, дистанційно-векторним протоколом маршрутизації, який визначається в RFC 1723.

На рисунку.10.1 наведена класифікація протоколів маршрутизації.

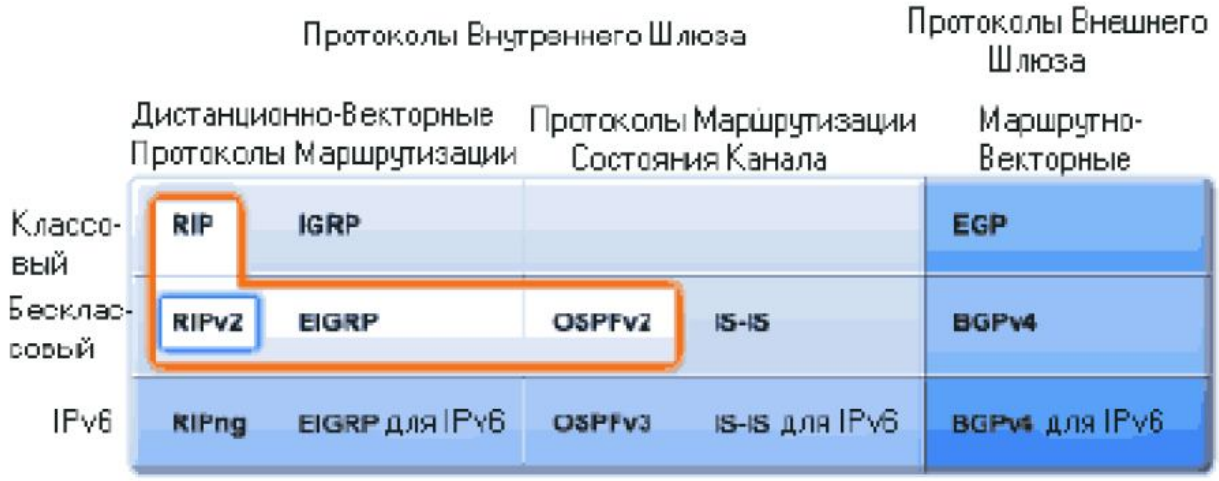

Рисунок 10.1 – Класифікація протоколів маршрутизації

До появи нових маршрутів, маршрутизатори RIP пристосовуються без труднощів. У черговому повідомленні своїм сусідам вони передають нову інформацію так, що та поступово стає відома всім маршрутизаторам мережі. А ось до негативних змін, пов’язаних із втратою будь-якого маршруту, їм

адаптуватися складніше. Справа в тому, що у форматі повідомлень протоколу RIP немає поля, де б містилася інформація про відсутність шляху до цієї мережі

Зрозуміти, що деякий маршрут більше недійсний, можна двома способами:

– на підставі закінчення часу життя маршруту;

– зазначенням спеціальної відстані до мережі, що стала недоступною, а саме нескінченності.

Для реалізації першого механізму кожен запис таблиці маршрутизації, отриманий по протоколу *RIP*, має час життя *(TTL).* При надходженні чергового повідомлення *RIP* із підтвердженням того, що запис дійсний, таймер TTL встановлюється в початковий стан, а потім із нього кожну секунду віднімається одиниця. Якщо за час тайм-ауту не прийде нове маршрутне повідомлення про цей маршрут, то він відзначається недіючим.

Час очікування пов’язаний з періодом розсилання векторів по мережі. Період розсилання в RIP дорівнює 30 с, а як тайм-аут прийнято шестиразове значення періоду розсилання 180 с. Шестиразовий запас часу потрібний для впевненості в тому, що проблеми полягають не у втратах повідомлень *RIP* (а це можливо, оскільки *RIP* використовує транспортний протокол *UDP*, що не гарантує доставку повідомлень), а в тому, що мережа дійсно стала недоступна. Якщо який-небудь маршрутизатор виходить з ладу, то через 180 с усі зроблені цим маршрутизатором записи стануть недійсними у його найближчих сусідів. Після цього процес повториться вже для сусідів найближчих сусідів – вони викреслять подібні записи через 360 с, оскільки перші 180 с найближчі сусіди ще передавали повідомлення про ці записи. Як бачимо, відомості про недоступні через відмову маршрутизатора мережі поширюються по мережі не дуже швидко, час поширення є кратним часу життя запису, а коефіцієнт кратності дорівнює кількості транзитних вузлів між самими далекими маршрутизаторами мережі. У цьому й полягає одна з причин вибору в якості періоду розсилки невеликої величини в 30 с.

Якщо збій відбувається лише на одному з інтерфейсів маршрутизатора або в мережі, через яку він пов’язаний з будь-яким сусідом, то ситуація зводиться до

щойно описаної – механізм тайм-ауту знову приводиться в дію, і недійсні маршрути поступово будуть викреслені з усіх маршрутизаторів мережі.

Тайм-аут працює в тих випадках, коли маршрутизатор не може послати сусідам повідомлення про недоступний маршрут завдяки своїй непрацездатності або непрацездатності лінії зв'язку, по якій можна було б передати повідомлення.

Якщо пересилання можливе, то маршрутизатори *RIP* не використовують спеціальні ознаки в повідомленні, а вказують нескінченну відстань до мережі, до того ж у протоколі *RIP* воно вибрано рівним 16 транзитним вузлам (при використанні іншої метрики маршрутизатора необхідно вказати її значення, яке вважається нескінченністю). При надходженні повідомлення, в якому відстань до деякої мережі дорівнює 16 (або 15, що приводить до того самого результату, оскільки отримане значення збільшується на 1), маршрутизатор повинен перевірити, чи виходить ця «негативна» інформація про мережу від того самого маршрутизатора, повідомлення якого послугувало свого часу підставою для запису про цю мережу в таблиці маршрутизації. Якщо це так, то інформація вважається достовірною, і маршрут відзначається як недоступний.

Значення «нескінченної» відстані задається настільки невеликим тому, що в деяких випадках перебої в лініях зв'язку викликають тривалі періоди некоректної роботи маршрутизатора *RIP*, що виражається в зацикленні пакетів у петлях мережі. І чим менше відстань, що використовується як «нескінченна», тим такі періоди стають коротшими.

Обмеження в 15 транзитних вузлів звужує сферу застосування *протоколу RIP* до мереж, у яких кількість проміжних маршрутизаторів не повинна перевищувати 15. Для масштабніших мереж потрібно використовувати інші протоколи маршрутизації, наприклад *OSPF*, або розбивати мережу на автономні області.

Методи боротьби з помилковими маршрутами в протоколі RIP.

Незважаючи на те, що протокол RIP не здатний повністю виключити перехідні стани в мережі, коли деякі маршрутизатори користуються застарілою

інформацією про неіснуючі вже маршрути, частково подібні проблеми вирішуються за допомогою спеціальних методів.

Так, труднощі, що виникають від появи петлі між сусідніми маршрутизаторами, запобігають за допомогою методу, який отримав назву «розщеплення горизонту» *(split horizon)*. Він полягає в тому, що маршрутна інформація про деяку мережу, що зберігається в таблиці маршрутизації, ніколи не передається маршрутизатору, від якого вона отримана (це той маршрутизатор, який є наступним у конкретному маршруті).

Однак розщеплення горизонту не допомагає в тих випадках, коли петлі утворюють не два, а декілька маршрутизаторів.

Для запобігання зациклення пакетів по складовим петлям при відмовах зв'язків застосовуються два інших прийоми, які звуться «примусові поновлення» (triggered update) і «заморожування змін» (hold down).

Спосіб примусових оновлень полягає в тому, що, отримавши дані про зміну метрики до будь-якої мережі, маршрутизатор не чекає закінчення періоду передачі таблиці маршрутизації, а передає дані про маршрут, котрий змінився негайно. Цей прийом допомагає запобігати передачі застарілих відомостей про маршрут, що відмовив, але він перевантажує мережу сервісними повідомленнями, тому примусові оголошення також робляться з деякою затримкою.

У зв'язку з цим не виключено, що регулярне оновлення на будь-якому маршрутизаторі випередить надходження примусового поновлення від попереднього маршрутизатора в ланцюжку, і цей маршрутизатор встигне передати по мережі застарілу інформацію про неіснуючий маршрут.

Другий прийом дозволяє виключити подібні ситуації. Він пов'язаний з введенням тайм-ауту на прийняття нових даних про мережу, яка щойно стала недоступною та запобігає прийняття застарілих відомостей про конкретний маршрут від тих маршрутизаторів, що знаходиться на деякій відстані. Передбачається, що протягом тайм-ауту заморожування змін дозволить цим маршрутизаторам викреслити цей маршрут зі своїх таблиць, оскільки вони не

отримають про нього нових записів і не будуть поширювати застарілу інформацію.

10.3 Порядок виконання роботи

На рисунку 10.2 наведена топологія мережі й необхідне обладнання для проєктування мережі.

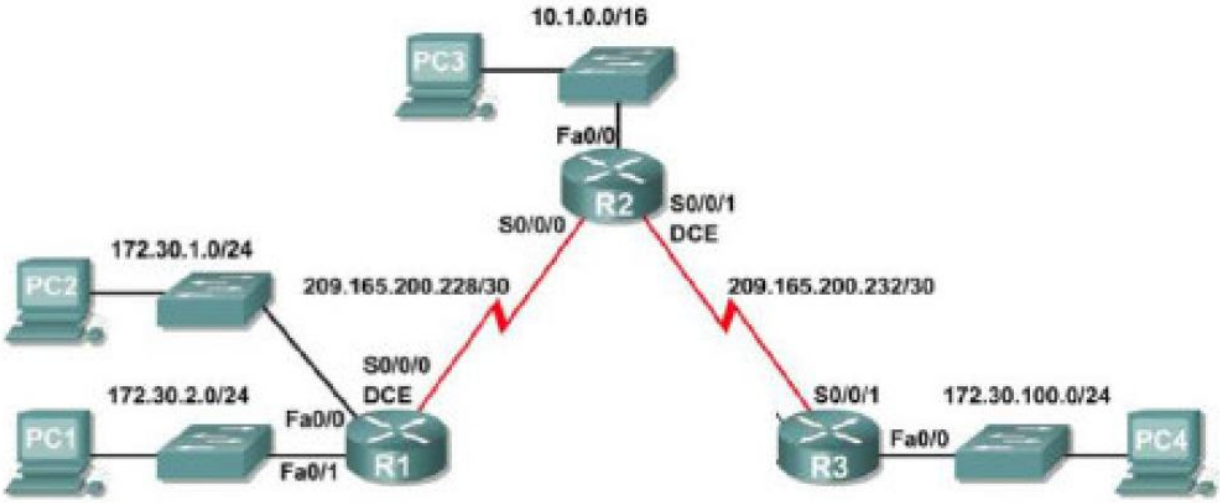

Рисунок 10.2 – Топологія мережі

Необхідні дані для проєктування у наведені таблиці 10.1.

Таблиця 10.1 – Таблиця адрес

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчув.
1	2	3	4	5
R1	Fa0/0	172.30.1.1	255.255.255.0	N/A
	Fa0/1	172.30.2.1	255.255.255.0	N/A
	S0/0/0	209.165.200.230	255.255.255.252	N/A
R2	Fa0/0	10.1.0.1	255.255.0.0	N/A
	S0/0/0	209.165.200.229	255.255.255.252	N/A
	S0/0/1	209.165.200.233	255.255.255.252	N/A

Продовження таблиці 10.1

1	2	3	4	5
R3	Fa0/0	172.30.100.1	255.255.255.0	N/A
	S0/0/1	209.165.200.234	255.255.255.252	N/A
PC1	N|C	172.30.1.10	255.255.255.0	172.30.2.1
PC2	N|C	172.30.2.10	255.255.255.0	172.30.1.1
PC3	N|C	10.1.0.10	255.255.0.0	10.1.0.1
PC4	N|C	172.30.100.10	255.255.255.0	172.30.100.1

1. Конфігурація.

Вибрати зі списку *Routers. Switches PC* і розташувати на полі (рис. 10.3).

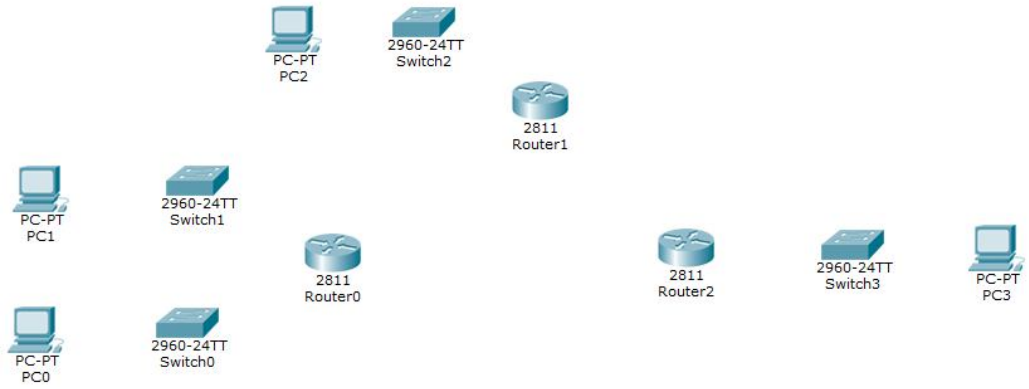

Рисунок 10.3 – Розміщення обладнання

2. Натискаючи на *Router* побачите вікно, в якому:

– виключити маршрутизатор;

– додати зі списку зліва модуль *WIC-1T*, перетягнувши його в одне з вільних місць;

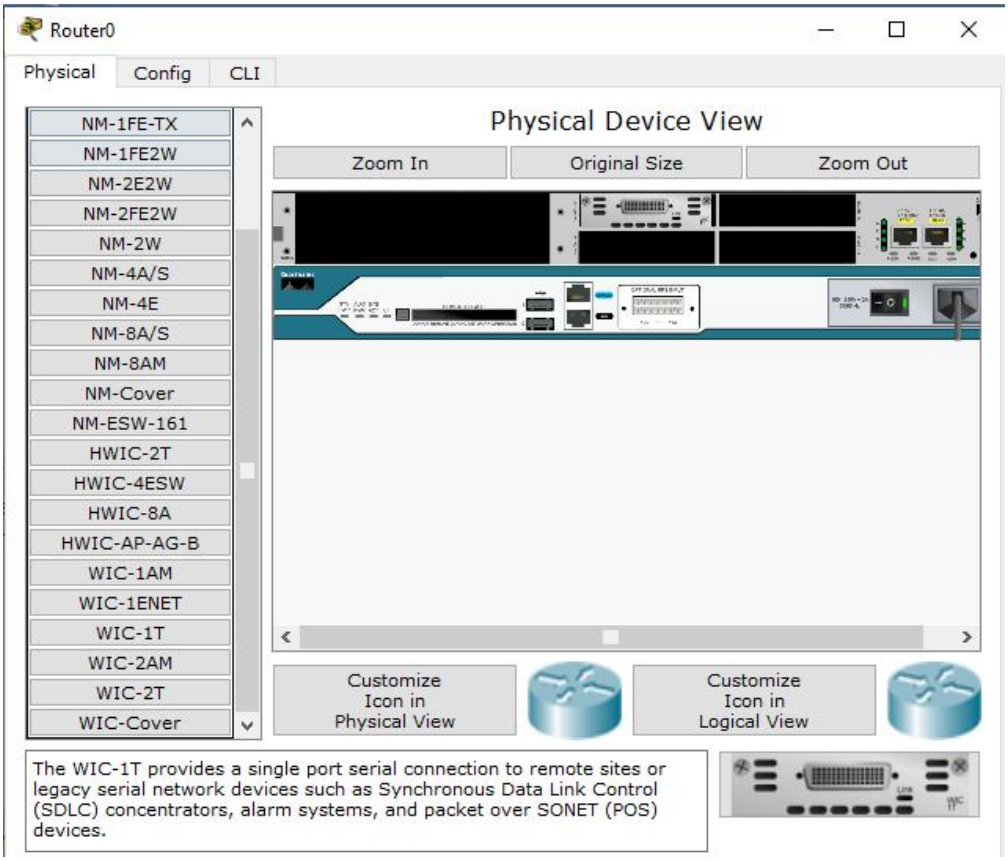

Рисунок 10.4 – Підключення маршрутизатора

– включити маршрутизатор.

На Router 1 (центральний маршрутизатор) вибрати модуль WIC-2T.

3. З’єднати *Routers Serial* кабелем, а *Routers, Switches PC* – прямим кабелем.

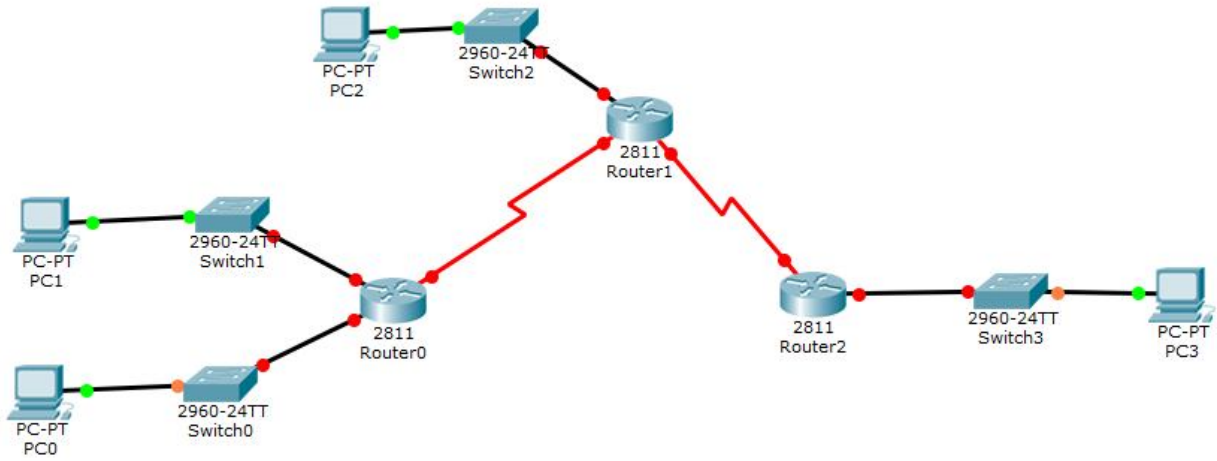

Рисунок 10.5 – З’єднання пристроїв

4. Натискаємо на *Router* і вибираємо панель *CLI* (рис. 10.6), набираємо команду *«no».* Відповідно так робимо на всіх маршрутизаторах.

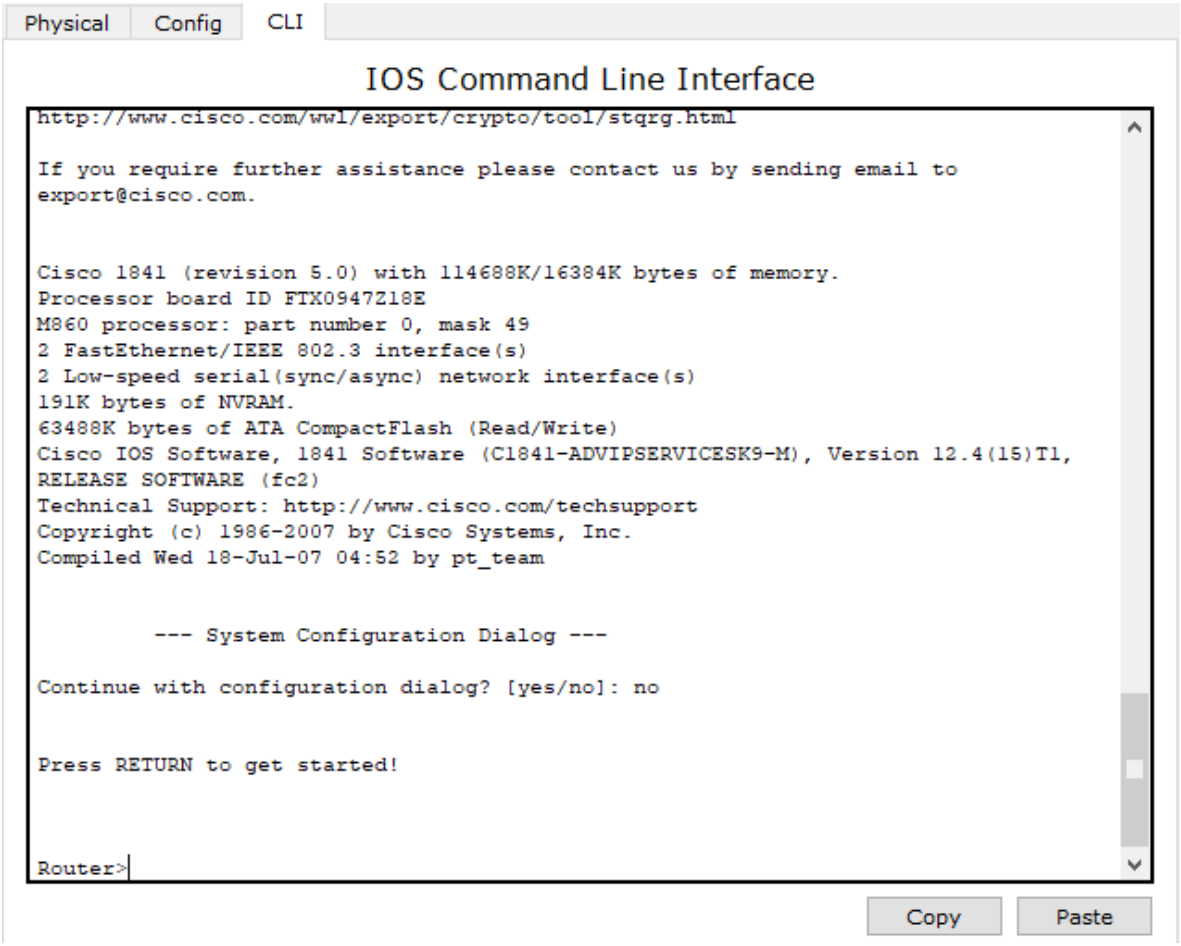

Рисунок 10.6 – Панель CLI

5. Входимо в привілейований режим *Router> enable*

6. Входимо в режим глобальної конфігурації *Router# configure terminal*

7. Змінюємо ім’я маршрутизатора *Router (config)#hostname R1 R1 (config)#*

8. Конфігуруємо інтерфейси на *Router1* і запускаємо:

R1 (config)#interface fastEthernet 0/0

R1 (config-if)#ip add 172.30.1.1 255.255.255.0

R1 (config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up:

R1 (config-if)#exit

R1 (config)#interface fastEthernet 0/1

R1 (config-if)#ip add 172.30.2.1 255.255.255.0

R1 (config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

R1 (config-if)#exit

R1 (config)#interface Serial 0/3/0

R1 (config-if)#ip add 209.165.200.230 255.255.255.252

R1 (config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to down

R1 (config-if)#exit

Примітка. Serial інтерфейс стане активний, коли на іншому кінці кабелю будуть виконані налаштування порту.

Налаштовуємо *RIP:*

– команда *router rip* надає можливість конфігурувати протокол *RIP* на *Cisco routers;*

– команда *network* активізує інтерфейс для роботи з цим протоколом, а також дозволяє оголосити мережі, безпосередньо підключені до маршрутизатора;

– далі необхідно відключити автопідсумовування: це потрібно для того, щоб маршрутизатор прийняв інформацію про підмережі.

R1 (config) #router rip

R1 (config-router) #version 2

R1 (config-router) #network 172.30.0.0

R1 (config-router) #network 209.165.200.0

R1 (config-router) #no auto-summary

R1 (config-router) #exit

9. Конфігуруємо інтерфейси на *Router2* і запускаємо:

Router (config)#hostname R2

R2 (config)# interface fastEthernet 0/0

R2 (config-if)#ip add 10.1.0.1 255.255.0.0

R2 (config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R2 (config-if)#exit

R2 (config)#interface Serial 0/3/0

R2 (config-if)#ip add 209.165.200.229 255.255.255.252

R2 (config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

R2 (config-if)#exit

R2 (config)# interface Serial 0/3/1

R2 (config-if)#ip add 209.165.200.233 255.255.255.252

R2 (config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/3/1, changed state to down

R2 (config-if) #exit

R2 (config) #router rip

R2 (config-router) #version 2

R2 (config-router) #network 10.0.0.0

R2 (config-router) #network 209.165.200.0

R2 (config-router) #no auto-summary

R2 (config-router) #exit

10. Конфігуруємо інтерфейси на Router3 і запускаємо:

Router (config)#hostname R3

R3 (config) #interface fastEthernet 0/0

R3 (config-if) #ip add 172.30.100.1 255.255.255.0

R3 (config-if) #no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R3 (config-if) #exit

R3 (config) #interface Serial 0/3/0

R3 (config-if) #ip add 209.165.200.234 255.255.255.252

R3 (config-if) #no shutdown

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

R3 (config-if) #exit

R3 (config) #router rip

R3 (config-router) #version 2

R3 (config-router) #network 172.30.0.0

R3 (config-router) #network 209.165.200.0

R3 (config-router) #no auto-summary

R3 (config-router) #exit

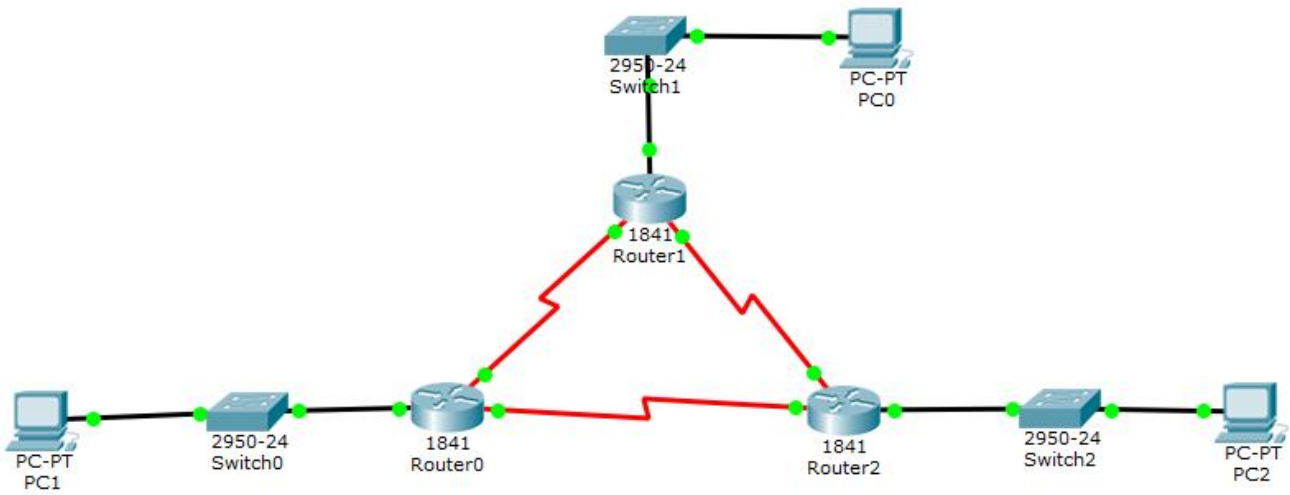

Рисунок 10.7 – З’єднання пристроїв

11. Налаштовуємо *PC* і перевіряємо *ping*.

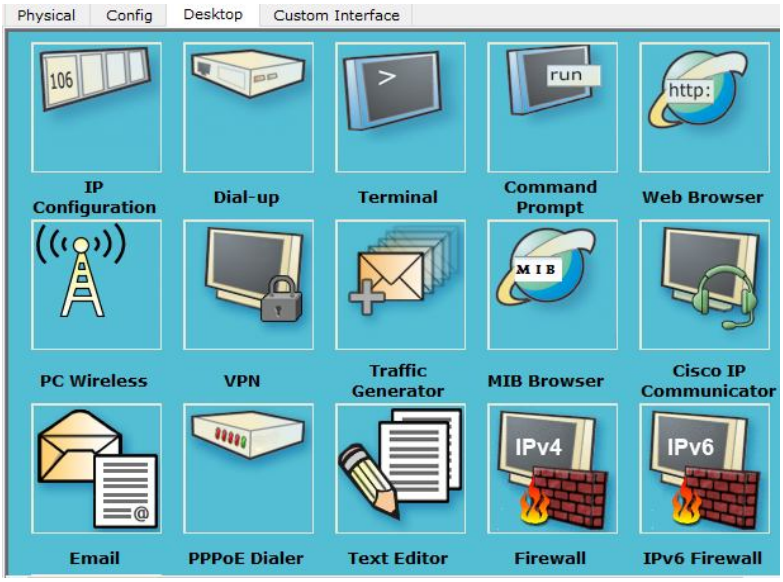

Рисунок 10.8 – Вікно «*Desktop*»

Вибираємо *IP Configuration* і вносимо дані з таблиці адрес 10.1.

Заходимо в *Command Prompt* і пишемо адресу *ping,* адресу *хоста* іншої мережі.

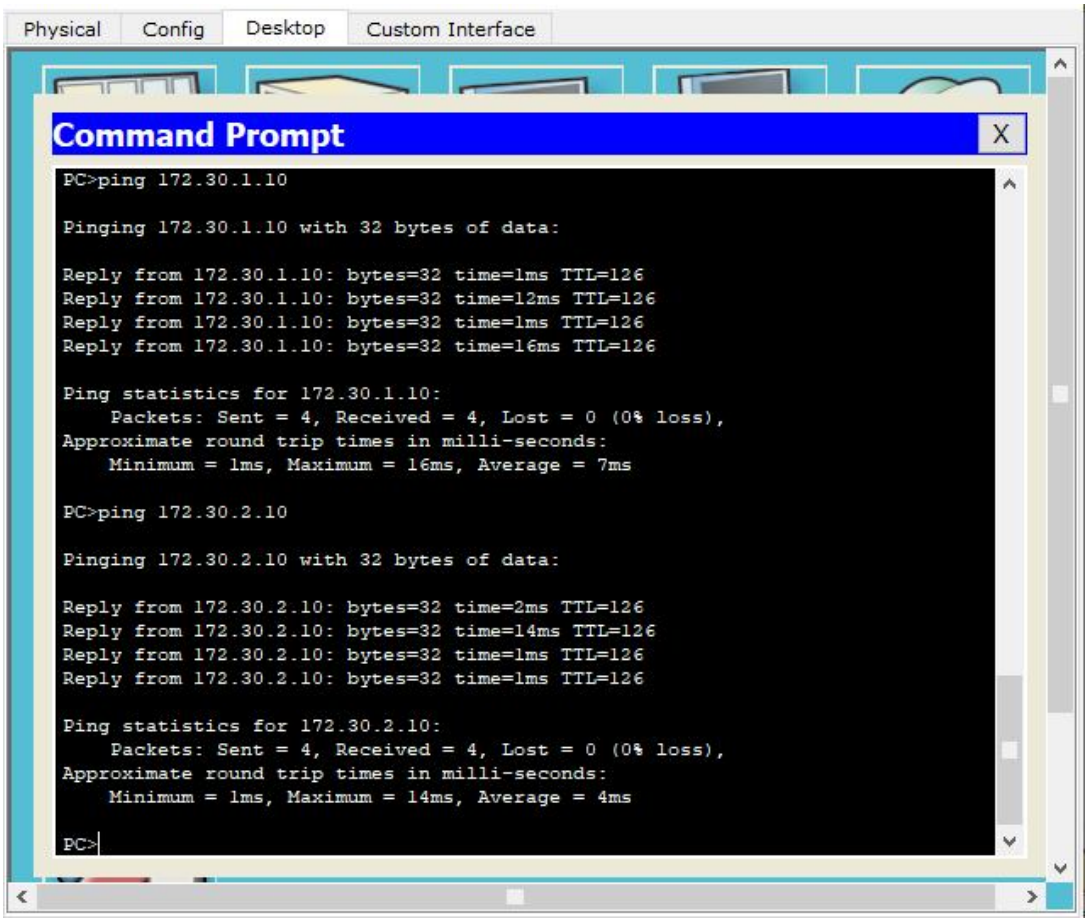

Рисунок 10.9 – Перевірка ping

10.4 Вимоги до змісту звіту

1. Звіт із практичної роботи повинен бути оформлений відповідно до загальноприйнятих правил оформлення практичних робіт і містити такі пункти:

– тема роботи;

– мета роботи;

– опис перебігу виконання роботи.

2. Для кожного завдання описати процес його виконання з проміжними рисунками та скріншотами.

10.5 Контрольні питання

1. Дайте визначення протоколу Routing Information Protocol (RIP).

2. Як відбувається обмін маршрутною інформацією у протоколі RIP?

3. Охарактеризуйте методи боротьби з помилковими маршрутами в протоколі RIP.

4. Охарактеризуйте поняття «примусові поновлення» (triggered update) і «заморожування змін» (hold down).

5. Розкажіть, які ви виконували дії для реалізації прикладу «Конфігурація мережевих засобів на основі протоколу RIPv2».

ПРАКТИЧНЕ ЗАНЯТТЯ № 11 КОНФІГУРАЦІЯ МЕРЕЖЕВИХ ЗАСОБІВ НА ОСНОВІ ПРОТОКОЛУ EIGRP

11.1 Мета роботи

Отримати практичні навички конфігурації пристроїв «Cisco» використовуючи протокол маршрутизації *EIGRP*.

11.2 Необхідний теоретичний матеріал

Протокол EIGRP – це внутрішній протокол маршрутизації шлюзу, розроблений фірмою «Cisco» для роботи з протоколами *TCP/IP і OSI.* (Комплект протоколів взаємозв'язку відкритих систем в internet-мережах. Група локальних обчислювальних мереж, об'єднаних загальним протоколом зв'язку).

EIGRP – це поліпшена версія I*GRP*. У цьому протоколі так само, як і в *IGRP* використовується технологія дистанційних векторів, і основна дистанційна інформація залишається колишньою. Але властивості конвергенції та ефективність роботи цього протоколу значно покращені. Протокол *EIGRP* передбачає модернізацію архітектури мережі зі збереженням коштів, що вкладені в розробку мережі на базі протоколу *IGRP*.

Протокол *EIGRP* складається з чотирьох основних компонентів:

– виявлення/відновлення сусіда *(Neighbor Discovery/Recovery);*

– надійний транспортний протокол (*Reliable Transport Protocol*);

– блок кінцевих станів алгоритму *DUAL (DUAL Finite State Machine*);

– модулі, залежні від протоколів (*Protocol Dependent Modules*).

Виявлення/відновлення сусіда – це процес, який використовується маршрутизатором для динамічного розпізнавання інших маршрутизаторів у мережах, до яких вони безпосередньо підключені. Маршрутизатори повинні також розпізнавати відсутність доступу до сусіда або припинення його роботи. Цей процес забезпечується за допомогою посилки маленьких пакетів вітань

(*Hello*), при цьому непродуктивні витрати досить незначні. Поки маршрутизатор отримує пакети *Hello*, він може визначати, що його сусід функціонує нормально. Як тільки це визначено, сусід може здійснювати обмін маршрутною інформацією.

Надійний транспортний протокол відповідає за гарантовану, упорядковану доставку пакетів *EIGRP* усім сусідам. Він підтримує різнотипну передачу пакетів як у режимі мультивідправлення, так і одиночного відправлення. Одні пакети *EIGRP* повинні передаватися з великим ступенем надійності, а для інших це зовсім необов'язково. Для підвищення ефективності надійність надається тільки в разі потреби. Наприклад, у мережі з мультидоступом і можливостями мультивідправлення, такій як Ethernet, немає потреби посилати пакети *Hello* всім сусідам індивідуально. Тому *EIGRP* посилає в режимі мультивідправлення один пакет *Hello* із зазначенням (записаним у пакеті), інформує одержувачів, що прийом цього пакета не потрібно підтверджувати. Інші типи пакетів, наприклад Update (оновлення), вимагають підтвердження отримання, що і вказується в пакеті. Надійний транспортний протокол забезпечений засобами швидкої передачі пакетів у режимі мультивідправлення в тому разі, якщо непідтверджені пакети очікують відправлення. Такі засоби допомагають не збільшувати час конвергенції за наявності каналів зв'язку, які працюють з різною швидкістю.

Блок кінцевих станів алгоритму *DUAL* реалізує процес прийняття рішень для розрахунків усіх маршрутів. Блок відстежує всі маршрути, оголошені усіма сусідами. Дистанційна інформація – це показник, який використовується алгоритмом *DUAL* для вибору ефективних шляхів, що не містять циклів. Алгоритм *DUAL* вибирає маршрути, які включаються в таблицю маршрутизації, засновану на принципі ймовірних подальших елементів. Наступний елемент – це сусідній маршрутизатор, який використовується для передачі пакетів і має найдешевший шлях до пункту призначення, при гарантії що такий шлях не є частиною циклу маршрутизації. Коли немає ймовірних подальших елементів, але є сусіди, що оголошували пункт призначення, необхідно робити перерахунок. При цьому визначається новий наступний елемент. Час

перерахунку впливає на загальний час конвергенції. І хоча перерахунок не вимагає інтенсивного використання процесора, намагайтеся уникати їх без необхідності. У разі зміни топології алгоритм *DUAL* перевіряє наявність ймовірних подальших елементів. Якщо вони присутні, алгоритм використовує всі, що знаходить, щоб запобігти зайвих перерахунків.

Таблиця сусідів *(Neighbor Table*). Кожен маршрутизатор зберігає відомості про суміжних сусідів. У разі виявлення нового сусіда записується його адресу й інтерфейс. Ця інформація зберігається в структурі даних цього сусіда. Таблиця сусідів містить елементи цієї структури. Для кожного модуля, залежного від протоколу, ведеться одна таблиця сусідів. Коли маршрутизатор посилає пакет *Hello*, він оголошує Hold Time – час, протягом якого маршрутизатор чекає відгуку сусіда. Якщо пакет *Hello* не приймається протягом відведеного часу, то це свідчить про те, що сусід або недосяжний, або не працює. Закінчення часу Hold Time є ознакою, за якою алгоритм *DUAL* визначає зміни топології мережі.

Елемент таблиці сусідів також включає в себе інформацію, необхідну для механізму роботи надійного транспортного протоколу. Для узгодження підтвердження прийому пакетів даних використовуються послідовні номери. Записується останній послідовний номер, отриманий від сусіда, завдяки чому можна виявити неузгоджені пакети. Для постанови пакетів у чергу в разі повторної передачі застосовується список передачі (transmission list), який складається для кожного сусіда. Для оцінки оптимальних інтервалів повторної передачі в структурі даних сусіда зберігаються таймери повного обходу маршруту.

Таблиця топології поповнюється модулями, залежними від протоколів, а працює з нею блок кінцевих станів алгоритму *DUAL*. Таблиця містить усі пункти призначення, оголошені сусідніми маршрутизаторами. До кожного елементу прив’язано адресу пункту призначення та список сусідів, які оголосили цей пункт призначення. Для кожного сусіда записується оголошений показник, який сусід зберігає в таблиці маршрутизації. Якщо сусід оголошує цей пункт призначення, то для передачі пакета повинен використовуватися маршрут, який

відповідає цьому показнику. Це важливе правило, якого повинні дотримуватися дистанційні векторні протоколи.

Також до кожного пункту прив’язаний показник, який маршрутизатор використовує для передачі до пункту призначення. Цей показник становить суму кращих оголошених показників усіх сусідів і вартість зв’язку до кращого сусіда. Цей сумарний показник маршрутизатор використовує в таблиці маршрутизації та для оголошення інших маршрутизаторів.

Елемент таблиці топології для пункту призначення може перебувати в одному з двох станів. Вважається, що маршрут знаходиться в пасивному стані (*Passive state*), коли в цей момент маршрутизатор не виробляє перерахунок маршруту. Маршрут знаходиться в активному стані (*Active state*), коли в цей момент маршрутизатор виробляє перерахунок маршруту. Якщо завжди є ймовірні подальші елементи, маршрут ніколи не переходить в активний стан, тому немає необхідності перераховувати маршрут.

Коли ж ймовірних подальших елементів немає, маршрут переходить в активний стан, і відбувається перерахунок маршруту. Перерахунок маршруту починається з посилки маршрутизатором пакета запитів (*Query*) усім сусідам. Сусідні маршрутизатори можуть або відгукнутися (*Reply*), якщо вони мають у своєму розпорядженні ймовірні наступні елементи для пункту призначення, або повернути запит, тим самим повідомляючи, що вони виробляють перерахунок маршруту (цей варіант факультативний). В активному стані маршрутизатор не може змінити найближчого транзитного сусіда, використовуваного для подальшого пересилання пакетів. Коли на запит отримано всі відгуки, маршрут переходить у пасивний стан і можна вибирати новий наступний елемент.

Коли зв’язок із сусідом, який являє собою тільки ймовірний наступний елемент, переривається, всі маршрутизатори які пов’язані з ним, починають перерахунок маршруту й він переходить в активний стан.

11.3 Порядок виконання роботи

На рисунку 11.1 наведена топологія мережі та необхідне обладнання для проєктування мережі.

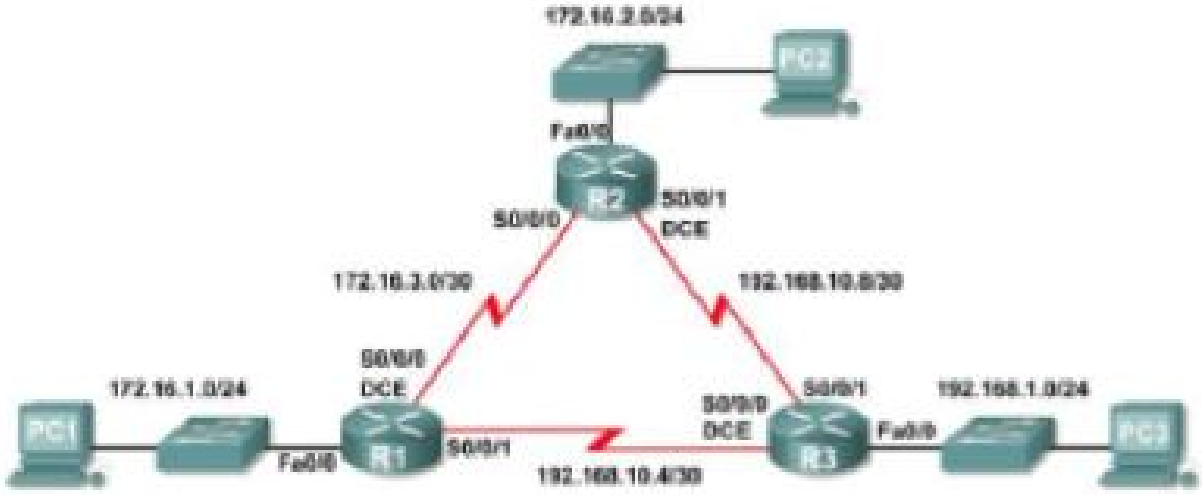

Рисунок 11.1 – Топологія мережі

Необхідні дані для проєктування наведені у таблиці 11.1.

Таблиця 11.1 – Таблиця адрес

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
1	2	3	4	5
R1	Fa0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	Fa0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A

Продовження таблиці 11.1

1	2	3	4	5
PC1	N|C	172.16.1.10	255.255.255.0	172.16.1.1
PC2	N|C	172.16.2.10	255.255.255.0	172.16.2.1
PC3	N|C	192.168.1.10	255.255.255.0	192.168.1.1

На рисунку 11.2 наведена конфігурація розташування обладнання.

1. Вибрати зі списку *Routers. Switches. PC* і розташувати на полі.

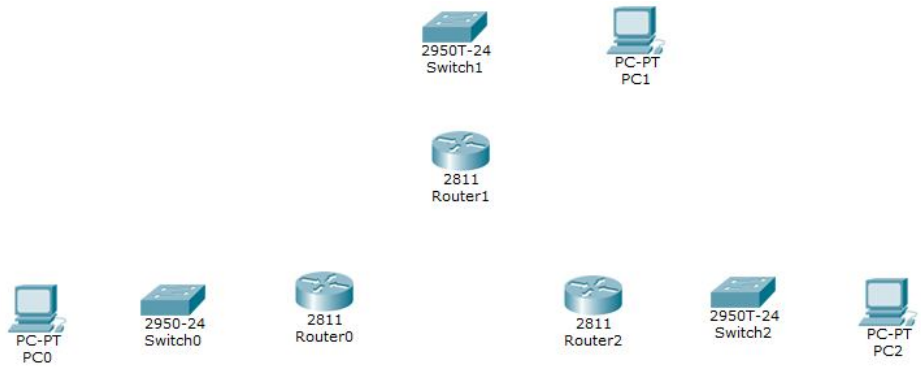

Рисунок 11.2 – Розташування обладнання

2. Натиснути на *Router*, з’явиться вікно, в якому потрібно виконати таке:

– вимкнути маршрутизатор, додати зі списку зліва модуль WIC-1T, перетягнувши його в одне з вільних місць (див. рис.11.3);

– увімкнути маршрутизатор.

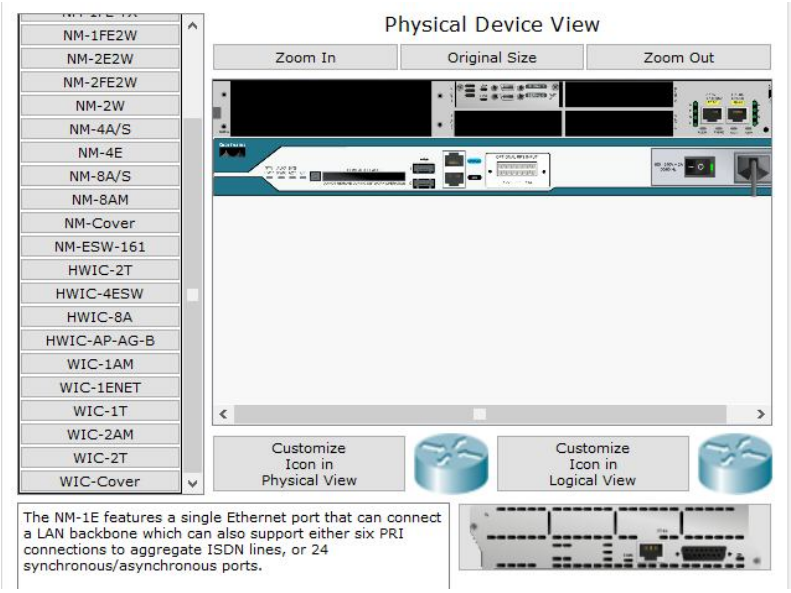

Рисунок 11.3 – Підключення маршрутизатора

3. З’єднайте *Routers Serial* кабелем, а *Routers Switches PC* – прямим кабелем (рис. 11.4).

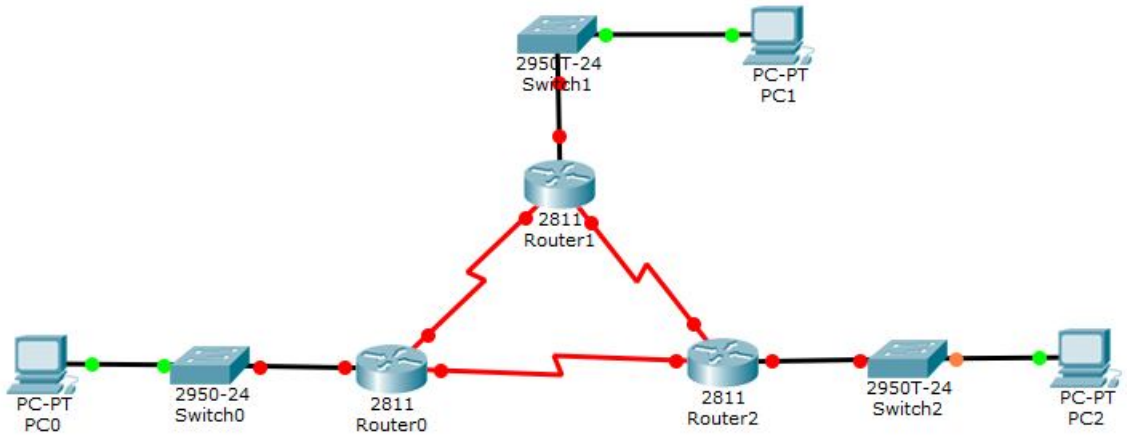

Рисунок 11.4 – З’єднання пристроїв

4. Натискаємо на *Router* і вибираємо панель *CLI,* набираємо команду «*no*» (рис 11.5). Відповідно так робимо на всіх маршрутизаторах.

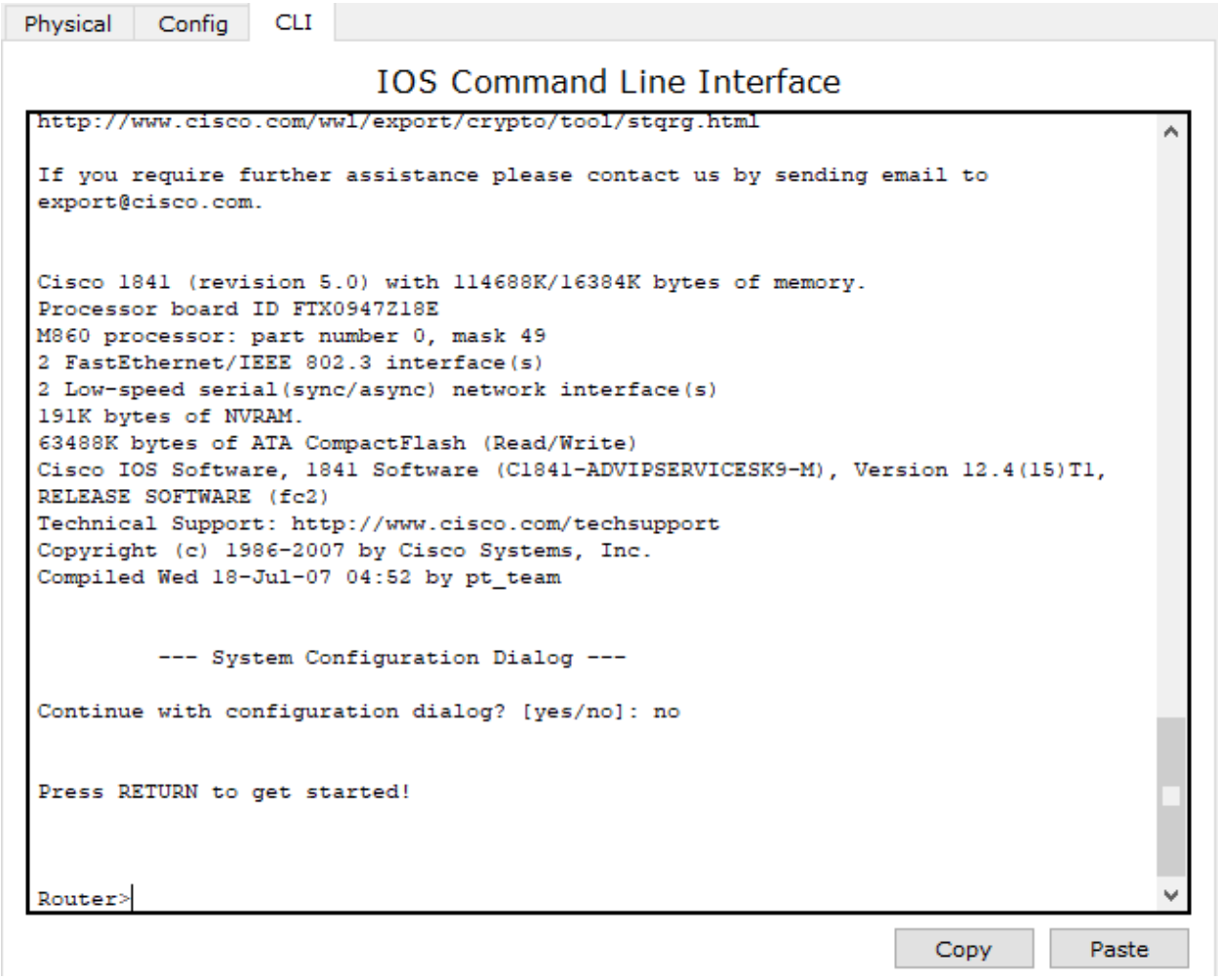

Рисунок 11.5 – Панель CLI

5. Входимо в привілейований режим *Router> enable*

6. Входимо в режим глобальної конфігурації *Router# configure terminal*

7. Змінюємо ім’я маршрутизатора *Router (config)#hostname R1 R1 (config)#*

8. Конфігуруємо інтерфейси на *Router1* і запускаємо:

R1 (config)#interface fastEthernet 0/0

R1 (config-if)#ip add 172.16.1.1 255.255.255.0

R1 (config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R1 (config-if)#exit

R1 (config)#interface Serial 0/3/0

R1 (config-if)#ip add 172.16.3.1 255.255.255.252

R1 (config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to down

R1 (config-if)#exit

R1 (config)#interface Serial 0/3/1

R1 (config-if)#ip add 192.168.10.5 255.255.255.252

R1 (config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/3/1, changed state to down

R1 (config-if)#exit

Налаштовуємо *EIGRP*:

– «1» – це номер автономної системи, на всіх маршрутизаторах однієї автономної системи він повинен бути однаковий;

– після адреси мережі можна додати *wild card mask*, але це не обов’язково тому, що маску мережі протокол візьме з інтерфейсу в цій мережі;

– далі необхідно відключити автопідсумовування: це потрібно для того, щоб маршрутизатор прийняв інформацію про підмережу;

– призначення *clock rate* на маршрутизаторі означає, що ми задаємо реальну швидкість каналу в бітах, *clock rate* призначається тільки з одного боку глобальної лінії зв'язку.

R1 (config) #router eigrp 1

R1 (config-router) #network 172.16.0.0

R1 (config-router) #network 192.168.10.4 0.0.0.3

R1 (config-router) #no auto-summary

R1 (config-router) #exit

9. Конфігуруємо інтерфейси на *Router2* і запускаємо.

Router (config)#hostname R2

R2 (config)# interface fastEthernet 0/0

R2 (config-if)#ip add 172.16.2.1 255.255.255.0

R2 (config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R2 (config-if)#exit

R2 (config)#interface Serial 0/3/0

R2 (config-if)#ip add 172.16.3.2 255.255.255.252

R2 (config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

R2 (config-if)#exit

R2 (config)# interface Serial 0/3/1

R2 (config-if)#ip add 192.168.10.9 255.255.255.252

R2 (config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/3/1, changed state to down

R2 (config-if) #exit

R2 (config) #router eigrp 1

R2 (config-router) #network 172.16.0.0

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/3/0) is up: new adjacency

R2 (config-router) #network 192.168.10.8 0.0.0.3

R2 (config-router) #no auto-summary

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/3/0) resync: summary configured

R2 (config-router) #exit

10. Конфігуруємо інтерфейси на *Router3* і запускаємо:

Router (config)#hostname R3

R3 (config) #interface fastEthernet 0/0

R3 (config-if) #ip add 192.168.1.1 255.255.255.0

R3 (config-if) #no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R3 (config-if) #exit

R3 (config) #interface Serial 0/3/0

R3 (config-if) #ip add 192.168.10.6 255.255.255.252

R3 (config-if) #no shutdown

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

R3 (config-if) #exit

R3 (config) #interface Serial 0/3/1

R3 (config-if) #ip add 192.168.10.10 255.255.255.252

R3 (config-if) #no shutdown

%LINK-5-CHANGED: Interface Serial0/3/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/1, changed state to up

R3 (config-if) #exit

R3 (config) #router eigrp 1

R3 (config-router) #network 192.168.1.0

R3 (config-router) #network 192.168.10.4 0.0.0.3

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.5 (Serial0/3/0) is up: new adjacency

R3 (config-router) #network 192.168.10.8 0.0.0.3

% DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.9 (Serial0/3/1) is up: new adjacency

R3 (config-router) #no auto-summary

% DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.5 (Serial0/3/0) resync: summary configured

% DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.9 (Serial0/3/1) resync: summary configured

R3 (config-router) #exit

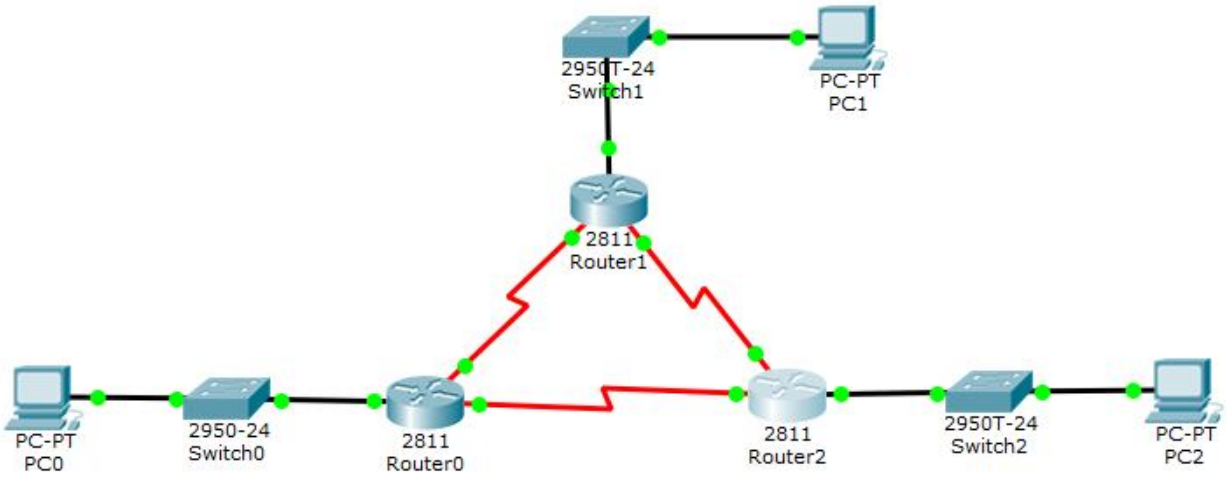

Рисунок 11.6 – З’єднання пристроїв

11. Налаштовуємо *PC* і перевіряємо *ping* (рис. 11.7, 11.8).

12. Вибираємо *IP Configuration* і вносимо дані з таблиці адрес 11.1.

Заходимо в *Command Prompt* і пишемо адресу *ping,* адресу *хоста* іншої мережі.

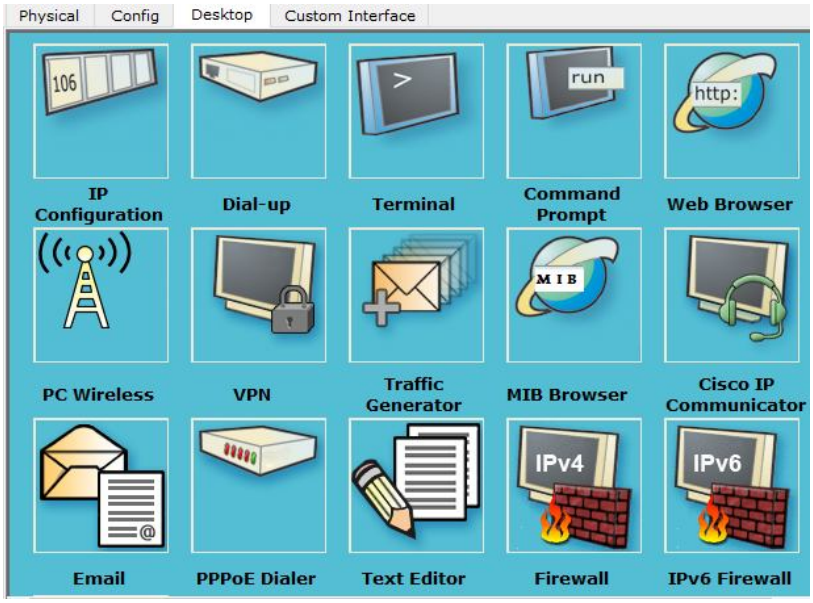

Рисунок 11.7 – Вікно Desktop

Команди:

1) *R# show running-config.* показує нам конфігураційний файл;

2) *R# show ip protocols.* Показує, які протоколи динамічної маршрутизації сконфігуровані та які параметри налаштовані для них;

3) *R# show ip route.* показує таблицю маршрутизації, задіяні інтерфейси й метрики за конкретними маршрутами.

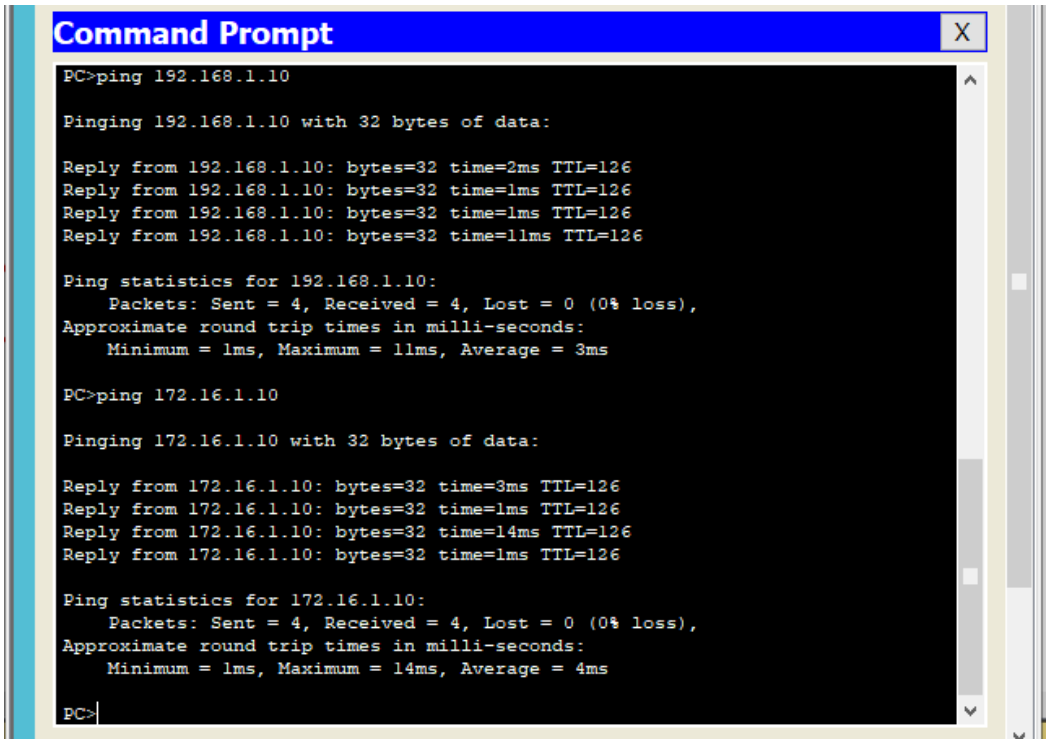

Рисунок 11.8 – Перевірка ping

11.4 Вимоги до змісту звіту

1. Звіт із практичної роботи повинен бути оформлений відповідно до загальноприйнятих правил оформлення практичних робіт і містити наступні пункти:

– тема роботи;

– мета роботи;

– опис перебігу виконання роботи.

2. Для кожного завдання описати процес його виконання з проміжними рисункам та скріншотами.

11.5 Контрольні питання

1. Дайте визначення протоколу EIGRP.

2. Із яких компонентів складається протокол EIGRP?

3. Поясніть значення компонента «Виявлення/Відновлення сусіда» (Neighbor Discovery/Recovery).

4. За що відповідає транспортний протокол (Reliable Transport Protocol)?

5. Охарактеризуйте компонент «Блок кінцевих станів алгоритму DUAL (DUAL Finite State Machine)».

6. Охарактеризуйте поняття «Таблиця сусідів (Neighbor Table)»; «Таблиця топології»; «Стан маршруту».

7. Розкажіть, які ви виконували дії для реалізації прикладу «Конфігурація мережевих засобів на основі протоколу EIGRP».

ПРАКТИЧНЕ ЗАНЯТТЯ № 12 СПИСКИ ДОСТУПУ ACCESS LIST (ACL)

12.1 Мета роботи

Отримання навичок налаштування списків доступу Access list (ACL) з використанням програми Cisco Packet Tracer.

12.2 Необхідний теоретичний матеріал

Списки доступу використовуються в низці випадків і є механізмом завдання умов, які маршрутизатор перевіряє перед виконанням будь-яких дій. Маршрутизатор перевіряє кожен пакет і на підставі перелічених вище критеріїв, зазначених в ACL, визначає, що потрібно зробити з пакетом, пропустити або відкинути. Типовими критеріями є адреси відправника й одержувача пакету, тип протоколу. Кожен критерій у списку доступу записується окремим рядком. ACL загалом являє собою набір рядків із критеріями, що мають один і той самий номер (або ім'я). Порядок завдання критеріїв у списку істотний. Перевірка пакету на відповідність списку проводиться послідовним застосуванням критеріїв із цього списку (в тому порядку, в якому вони були введені). Пакет, який не відповідає жодному з введених критеріїв, буде відкинутий. Для кожного протоколу на інтерфейс може бути призначений тільки один список доступу.

При складанні ACL використовується лише два види впливу: «*Дозволити»* або *«Заборонити*».

Дозволити (permit) – при додаванні одного або декількох діапазонів «дозволу» всі інші діапазони за замовчуванням забороняються. Тільки пакети з дозволеного діапазону IP-адрес зможуть пройти далі через інтерфейс.

Заборонити (deny) – при додаванні одного або декількох діапазонів «заборонити» всі інші діапазони трафіку за замовчуванням дозволяються.

Поєднання дозволу та заборони – можна використовувати поєднання правил «*дозволити*» і «*заборонити*», щоб вказати вкладений дозволений або заборонений діапазон IP-адрес.

Розглянемо два простих прикладу стандартних списків:

 # Access-list 1 permit host 10.0.0.10 – дозволяємо проходження трафіку від вузла *10.0.0.10*.

 # Access-list 2 deny 10.0.1.0 0.0.0.255 – забороняємо проходження пакетів із підмережі *10.0.1.0/24*.

Списки доступу бувають декількох видів: стандартні, розширені, динамічні та інші. У стандартних ACL є можливість задати лише IP-адреси джерел пакетів для їх заборон або дозволів.

Розширений список дозволяє виділяти трафік за багатьма параметрами:

– IP-адреса джерела;

– порт джерела;

– протокол;

– IP-адреса одержувача;

– порт одержувача.

Фільтрувати трафік можна в різних напрямах: – вхідному або вихідному. Для кожного напряму створюється окремий лист доступу. Листи доступу створюються лише на L3-обладнанні (комутатори, маршрутизатори), до того ж не всі моделі підтримують цей сервіс.

Кожен інтерфейс у конкретний момент часу може бути налаштований тільки на один ACL. Мається на увазі, що інтерфейс при аналізі пакета може використовувати тільки один ACL. ACL «*за замовчуванням*» не має записів, а це означає, що немає заборон – «*усе дозволено*».

12.3 Приклади створення стандартних списків доступу

Створимо структуру, що складається з двох підмереж: 192.168.0.0 і 10.0.0.0. (рис.12.1).

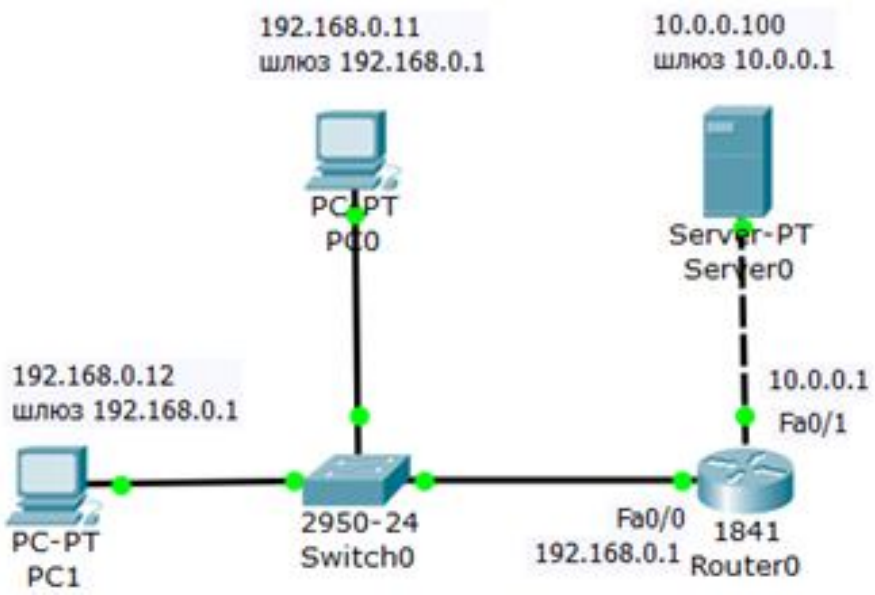

Рисунок 12.1 – Схема мережі

Необхідно дозволити доступ на сервер пристрою PC1 з адресою 192.168.0.12, а PC0 з адресою 192.168.0.11 – заборонити (рис.12.2).

Рисунок 12.2 – Постановка задачі

Запускаємо *Cisco Packet Tracker*, створюємо задану конфігурацію та прописуємо адреси на кожному PC. Потім заходимо на «*роутер*» і налаштовуємо його.

Інтерфейс 0/0 маршрутизатора 1841 налаштуємо на адресу 192.168.0.1 і включимо такими командами:

Router>en

Router#conf t

Router (config)#int fa0/0

Router (config-if)#ip addr 192.168.0.1 255.255.255.0

Router (config-if)#no shut

Router (config-if)#exit

Другий інтерфейс маршрутизатора (порт 0/1) налаштуємо на адресу 10.0.0.1 і так само включимо:

Router (config)#intfa0/1

Router (config-if)#ip addr 10.0.0.1 255.255.255.0

Router (config-if)#no shut

Конфігуруємо сервер (рис. 12.3).

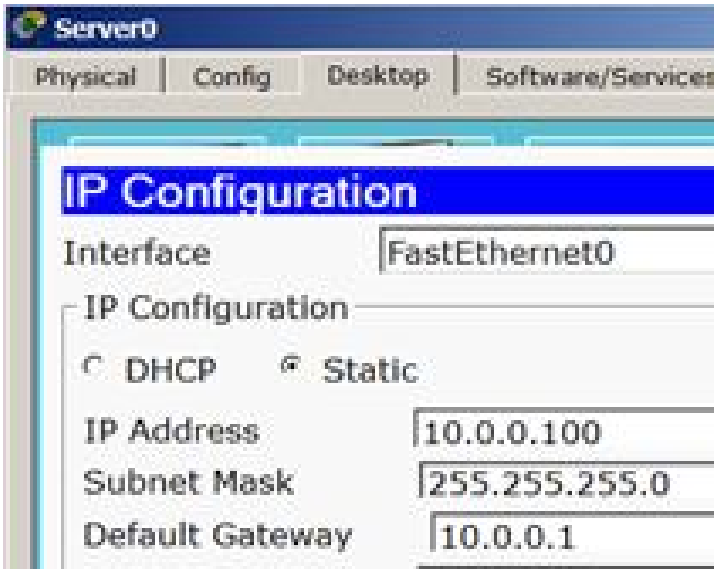

Рисунок 12.3 – Конфігурування сервера

Перевіряємо доступність сервера з різних ПК *(ping)*. Сервер повинен бути доступним.

Поки не заданий список доступу на інтерфейсі, все дозволено *(permit).* Але варто створити список, відразу діє механізм: «Усе, що не дозволено, то заборонено». Тому немає необхідності щось забороняти *(deny)* – вказуємо що дозволено, а *«іншим – заборонити»* мається на увазі «*автоматично»*. За умовами завдання нам потрібно на *Router0* пропустити пакети з вузла 192.168.0.12 на сервер.

Відповідний ACL створюється такими командами (рис. 12.4).

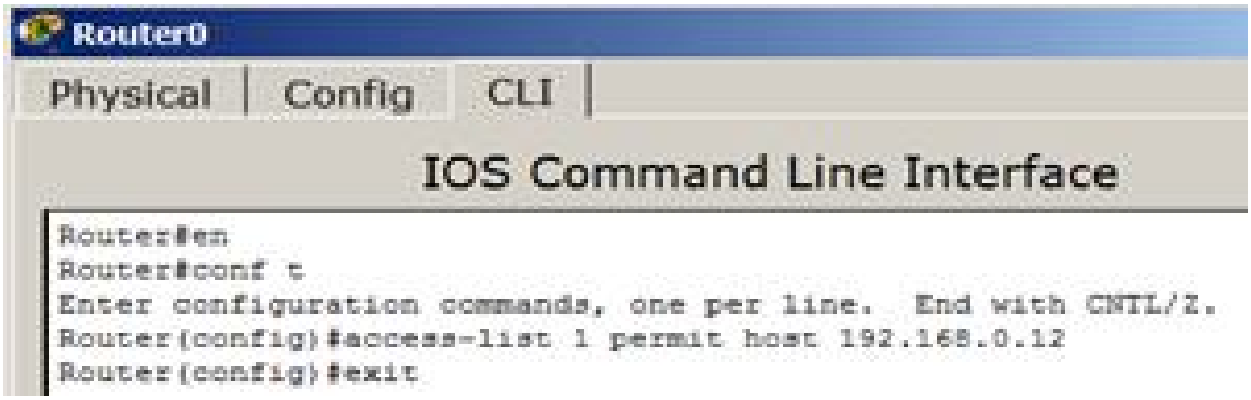

Рисунок 12.4 – Створення *ACL* на *Router0*

Спочатку створюється просто дозвіл на пропуск трафіку, що надходить від джерела PC1.

Застосовується це правило на інтерфейсі залежно від напрямку (PC1 розташований з боку порту Fa0/0). Тобто список доступу (правило з номером 1) повинен діяти на інтерфейсі fa0/0 на вхідному (in) від PC1 напрямку. Ця умова задається такою командою (рис. 12.5)

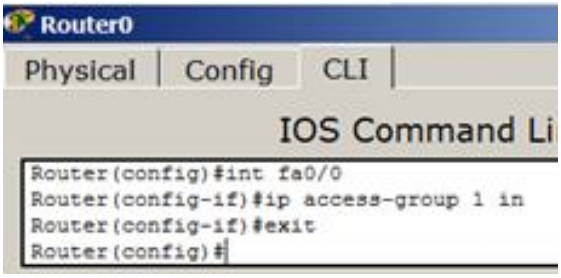

Рисунок 12.5 – Застосовуємо правило до порту Fa0/0

Вхідний трафік (*in*) – це той, який приходить на інтерфейс іззовні. Вихідний (*out*) – той, який відправляється з інтерфейсу зовні. Список доступу ви можете застосувати або на вхідний трафік, тоді невідповідні пакети не будуть навіть потрапляти на маршрутизатор і, відповідно, далі в мережу, або на вихідний, тоді пакети приходять на маршрутизатор, обробляються їм, доходять до цільового інтерфейсу й тільки на ньому обробляються. Зазвичай, списки застосовують на вхідний трафік (*in*).

Тепер перевіримо зв'язок наших PC із сервером (*ping*). Ми бачимо, що для PC0 сервер став недоступним, а для PC1 – доступним. Завдання виконано. Давайте подивимося ACL (рис. 12.6).

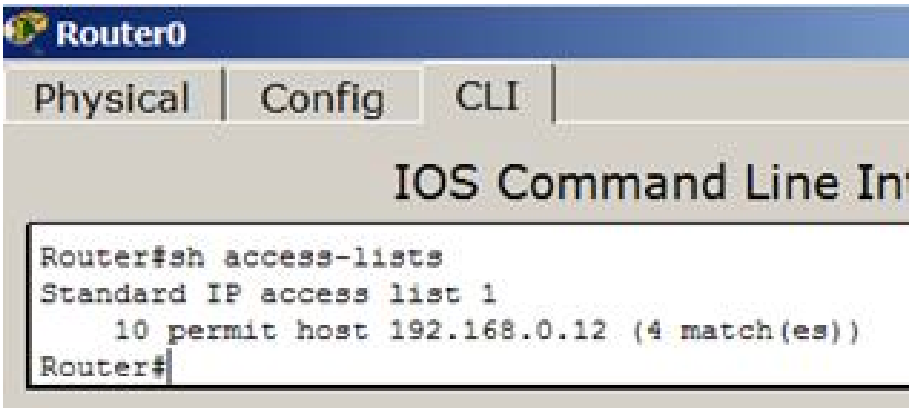

Рисунок 12.6 – Вузол 192.168.0.12 дозволений

Такий запис потрібно читати так: «*Через цей інтерфейс дозволена передача пакетів, що надійшли тільки від 192.168.0.12 (таких передач було 4)*».

Для скасування будь-якого правила вводимо його повторно з префіксом «no». Тоді це правило виключається з конфігурації. Наприклад, якщо виконати команду *Router (config-if) #no ip access-group 1 in*, то ACL буде скасований і знову всі ПК зможуть пінгувати сервер.

Завдання 1. Додайте в структуру мережі ще один PC та організуйте йому доступ до сервера. Перевірте правильність налаштування. Скасуйте діючий список доступу. Переконайтеся, що тепер всі три ПК отримали доступ до сервера.

12.4 Розширені списки доступу ACL

На відміну від стандартних списків, розширені списки фільтрують трафік більш «тонко». Під час створення розширених списків у правилах доступу можна включати фільтрацію трафіку по протоколам і портам.

Для вказівки портів у правилі доступу використовуються позначення, які наведені у таблиці 12.1.

Таблиця 12.1 – Позначення для портів

Позначення	Дія
lt n	Усі номери портів, менші n
gt n	Усі номери портів, більші n
eq n	Порт n
neq n	Усі порти, за виключенням n
range n m	Усі порти від n до m включно

На практиці все відбувається приблизно так: нехай є мережа (рис. 12.7), створимо її за допомогою *Cisco Packet Trasker.*

Тут ми бачимо дві підмережі (10.0.1.0/24 і 192.168.1.0/24).

Завдання 1. Дозволити доступ до FTP-сервера 10.0.1.3 для вузла 192.168.1.2 і заборонити для вузла 192.168.1.3.

Зверніть увагу! Не заборонити доступ до комп'ютера з ім'ям *Server0*, як такого, а заборонити доступ до одного з встановлених там сервісів (*FTP-Server*).

Створюємо розширені списки доступу й забороняємо *FTP-трафік*.

При виборі сервера в *Cisco Packet Tracker*, на сервері 10.0.1.3 за замовчуванням піднято *FTP-сервіс* зі значеннями ім'я користувача *Cisco*, пароль *Cisco*.

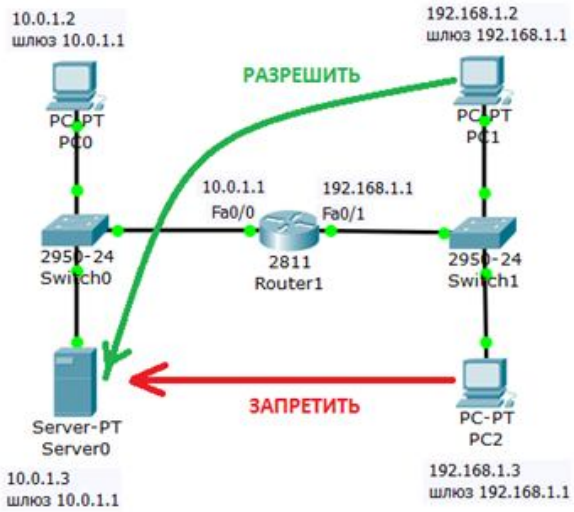

Рисунок 12.7 – Схема мережі (стрілками позначено завдання)

Переконаємося, що вузол *Server0* доступний і *FTP* працює, для цього заходимо на PC1 і зв'язуємося з сервером за допомогою командного рядка (*Command Promt*) (рис. 12.8). Виконуємо будь-які команди, наприклад, DIR – читання директорії 10.0.1.3.

```
Packet Tracer PC Command Line 1.0
PC>ftp 10.0.1.3
Trying to connect...10.0.1.3
Connected to 10.0.1.3
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 10.0.1.3:
0    : asa842-k8.bin                                5571584
1    : c1841-advipservicesk9-mz.124-15.T1.bin       33591768
2    : c1841-ipbase-mz.123-14.T7.bin                13832032
3    : c1841-ipbasek9-mz.124-12.bin                 16599160
4    : c2600-advipservicesk9-mz.124-15.T1.bin       33591768
5    : c2600-i-mz.122-28.bin                        5571584
6    : c2600-ipbasek9-mz.124-8.bin                  13169700
7    : c2800nm-advipservicesk9-mz.124-15.T1.bin     50938004
8    : c2800nm-advipservicesk9-mz.151-4.M4.bin      33591768
9    : c2800nm-ipbase-mz.123-14.T7.bin              5571584
10   : c2800nm-ipbasek9-mz.124-8.bin                15522644
11   : c2950-i6q412-mz.121-22.EA4.bin               3058048
12   : c2950-i6q412-mz.121-22.EA8.bin               3117390
13   : c2960-lanbase-mz.122-25.FX.bin               4414921
14   : c2960-lanbase-mz.122-25.SEE1.bin             4670455
15   : c2960-lanbasek9-mz.150-2.SE4.bin             4670455
16   : c3560-advipservicesk9-mz.122-37.SE1.bin      8662192
17   : pt1000-i-mz.122-28.bin                       5571584
18   : pt3000-i6q412-mz.121-22.EA4.bin              3117390
ftp>quit

Packet Tracer PC Command Line 1.0
PC>221- Service closing control connection.
PC>
```

Рисунок 12.8 – FTP-сервер доступний

Примітка. При наборі пароля на екрані нічого не відображається. Отже, переконалися, що сервіс доступний, тепер поставимо список правил, що регулює доступ до нього. Попередньо потрібно знати, які порти використовує сервер. Будь-який FTP-сервер задіє порти 20 і 21 (ці порти служать для FTP – передачі команд і даних).

Створимо розширений ACL (*access-list extended 101*). 101 – це номер ACL. Розберемо послідовність наведених на рисунку 12.9 команд, які прямують після рядка: *#ip access-list extended 101*

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended 101
Router(config-ext-nacl)#permit tcp 192.168.1.2 0.0.0.0 10.0.1.3 0.0.0.0 eq 21
Router(config-ext-nacl)#permit tcp 192.168.1.2 0.0.0.0 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 21
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0. 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#
```

Рисунок 12.9 – Розширений ACL

Два перші рядки (*permit*) дозволяють проходження *TCP-трафіку*, що надходить із портів 20 і 21 вузла (точніше сказати – *хоста*) 192.168.1.2 у напрямку *хоста* 10.0.1.3 на порти 20 і 21.

Два наступні рядки (*deny*) повинні б заборонити надходження точно такого самого трафіку від *хоста* 192.168.1.3. але в рядку з портом 20 допущена помилка – знайдіть її, тому з'явився п'ятий рядок, який вже виправлений.

Порада. Як ви вже зрозуміли, набирати команди потрібно уважно, навіть один зайвий пробіл може призвести до помилки під час виконання команди.

Отже, ACL із номером 101 створений і застосуємо його на вхід (*in*) Fa0/1 тому, що трафік входить на цей порт *роутера* з боку мережі 192.168.1.0 (рис. 12.7).

Команда застосування ACL виглядає так (рис. 12.10).

```
Router(config-ext-nacl)#int fa0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
Building configuration...
[OK]
Router#
```

Рисунок 12.10 – Застосування правила з номером 101 до порту 0/1 роутера

Тепер переконаємося, що рішення досягнуто. Перевіряємо доступність *FTP-сервера* з PC2 (рис. 12.11).

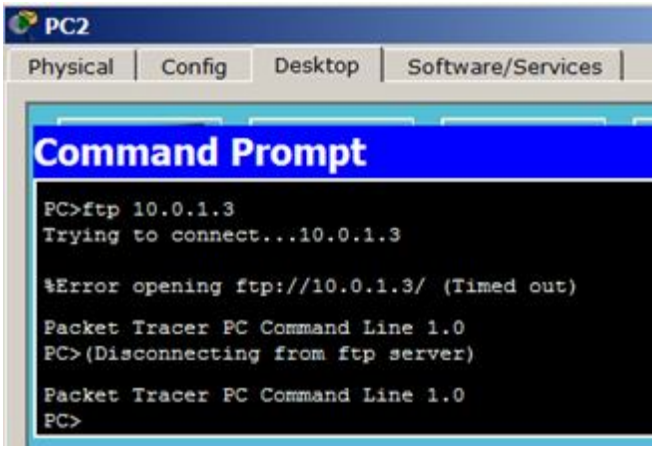

Рисунок 12.11 – Для PC2 FTP-сервер не доступний

Перевіряємо доступність *FTP-сервера* з PC 1 (рис. 12.12).

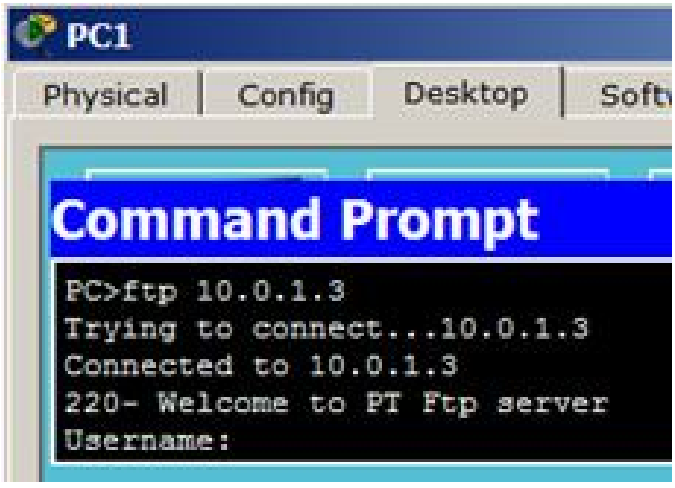

Рисунок 12.12 – Для PC1 FTP-сервер доступний

Завдання 2. Додайте в сегмент 192.168.1.0 ще один PC і організуйте йому доступ до *FTP-сервера*. Перевірте, чи правильно встановлені PC. Скасуйте діючий список доступу. Переконайтеся, що тепер усі три PC отримали доступ до сервера.

12.5 Вимоги до оформлення звіту

1. Звіт із цієї роботи повинен бути оформлений відповідно до загальноприйнятих правил оформлення практичних занять і містити такі пункти:

– тема роботи;

– мета роботи;

– вихідні дані;

– завдання.

2. Опис перебігу виконання робіт (із проміжними рисунками та скріншотами.

12.6 Контрольні питання

1. Для чого використовуються списки доступу?
2. Які існують типові критерії для перевірки пакетів?
3. Які види впливу використовуються при складанні ACL?
4. Які бувають списки доступу?
5. Наведіть приклади створення стандартних списків доступу.
6. Опишіть налаштування *Router0*.
7. Опишіть налаштування серверу.
8. Охарактеризуйте скасування діючого ACL.

ПРАКТИЧНЕ ЗАНЯТТЯ № 13 НАЛАШТУВАННЯ ОСНОВНИХ ПАРАМЕТРІВ БЕЗПРОВІДНОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ CISCO PACKET TRACER

13.1 Мета роботи

Отримання практичних навичок у використанні інструментів програмного середовища *Cisco Packet Tracer* для налаштування базової бездротової мережі.

13.2 Необхідний теоретичний матеріал

Роутер Cisco Linksys використовується для організації бездротового з'єднання. Ці висококласні пристрої стануть раціональним придбанням для користувачів, яким необхідний високошвидкісний вихід в інтернет незалежно від їх місця розташування в приміщенні. Залежно від моделі, *роутери Cisco Linksys* підтримують мережеві стандарти Wi-Fi 802.11 a / b / g / n / ac, надаючи швидкість з'єднання від 54 Мбіт/с до 1300 Мбіт/с. Крім того, деякі зі стандартів передбачають функціонування пристроїв, що підключаються на діапазоні радіочастот у 5 ГГц.

Широкосмугове підключення до Інтернету відзначається високою швидкістю передавання даних. Найпоширеніші два варіанти широкосмугового підключення:

– за допомогою цифрової абонентської лінії (DSL);

– за допомогою кабелю.

Зазвичай підключення DSL надають телефонні компанії, а підключення за допомогою кабелю – компанії кабельного телебачення. Інтернет-провайдери часто пропонують широкосмугові модеми, а деякі з них також поєднання модемів та безпровідних маршрутизаторів. Безпровідний маршрутизатор передає дані між абонентською мережею та інтернетом. Безпровідний маршрутизатор дає змогу підключити комп'ютер до мережі за допомогою

радіосигналів, а не кабелів. Безпровідні маршрутизатори підтримують мережеві стандарти Wi-Fi 802.11, за які було сказано раніше.

Адаптер безпровідної мережі – це пристрій, який підключає ПК до безпровідної мережі. Щоб підключити портативний пристрій або настільний комп'ютер до безпровідної мережі, вони мають бути обладнані адаптером безпровідної мережі. Більшість ноутбуків і планшетів, а також деякі настільні комп'ютери постачаються з попередньо встановленим адаптером безпровідної мережі.

13.3 Порядок виконання роботи

Створіть топологію, зображену на рисунку 13.1 у Cisco Packet Tracer.

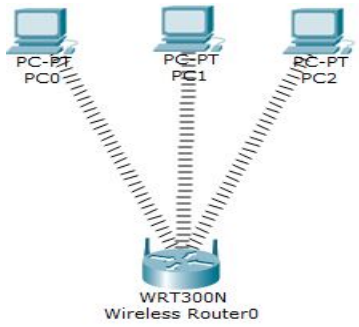

Рисунок 13.1 – Бездротова топологія

У цій топології є три комп'ютери, підключених за допомогою *Linksys* і бездротового маршрутизатора:

– *DHCP* налаштований і включений на бездротовому маршрутизаторі;

– *IP-пул для DHCP* знаходиться від 192.168.0.100 до 192.168.0.150;

– *ПК* налаштовані на отримання *IP* від сервера *DHCP*;

– безпека не налаштована;

– за замовчуванням *SSID* налаштований на «*Default*»;

– *топологія* працює в режимі «*infrastructure*»;

– *ім'я користувача* й пароль за умовчуванням «*admin*»;

– *IP бездротового пристрою* встановлений в 192.168.0.1.

Необхідно виконати наступні дії:

– налаштувати статичну *IP-адресу* для *ПК* і для бездротового маршрутизатора;

– змінити ідентифікатор *SSID* на «*Mother Network*»;

– змінити *IP-адресу* маршрутизатора на 10.0.0.1, PC0 на 10.0.0.2, 10.0.0.3 на PC1, PC2 на 10.0.0.4;

– забезпечити безпеку мережі за допомогою установки ключа *WEP* на маршрутизаторі;

– підключитися до персонального комп'ютера за допомогою ключа *WEP*.

Мережа має 192.168.0.0 адресу й усі *DHCP*-клієнти функціонують у належний спосіб. Отже, необхідно спочатку підключитися до бездротового маршрутизатора, щоб включити *DHCP*.

Двічі клацніть на *ПК* і виберіть *веббраузер*. Як відомо, *IP-адреса* бездротового маршрутизатора: – 192.168.0.1, введіть її в *веббраузері* і натисніть «*Enter*», тепер він буде запитувати ім'я користувача, яким є «*admin*» і пароль «*admin*» (рис. 13.2).

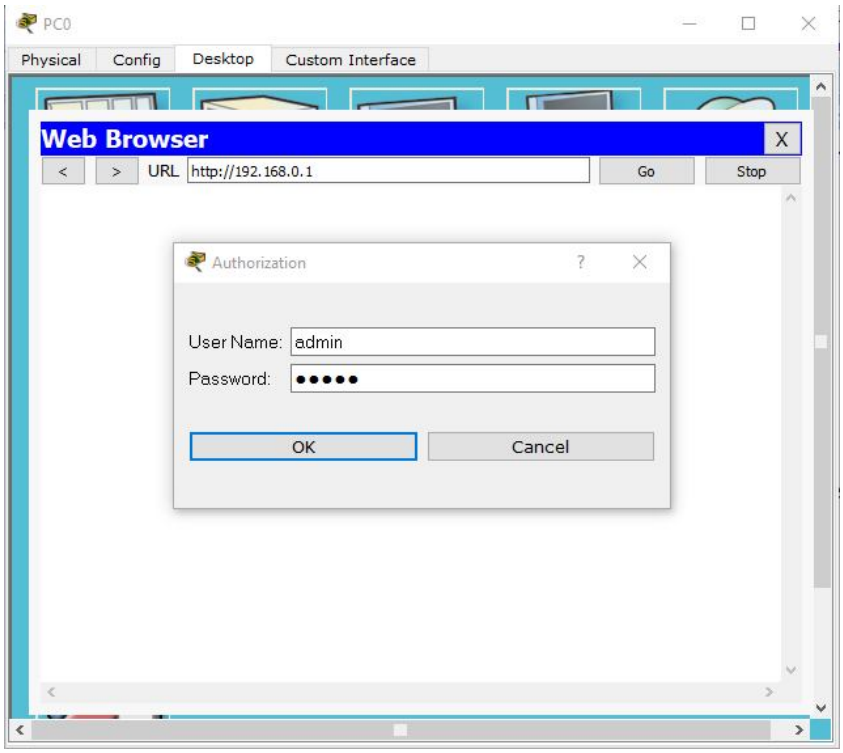

Рисунок 13.2 – Вікно авторизації

Прокрутіть до низу екран «*Network Setup*» і виберіть «*Відключити DHCP*» (рис. 13.3).

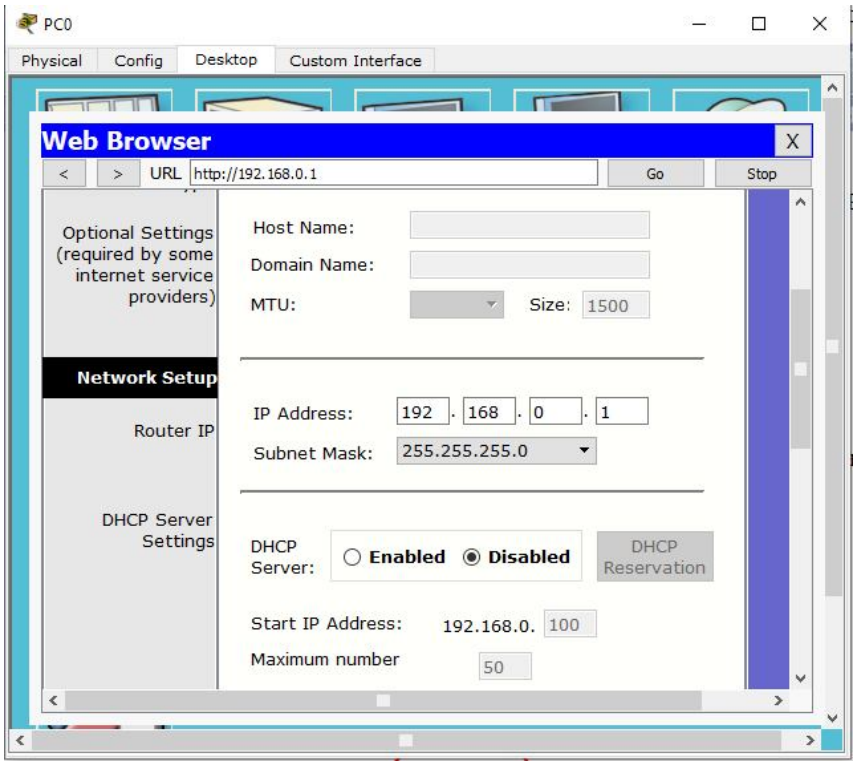

Рисунок 13.3 – Відключення DHCP

Перейдіть до кінця сторінки й натисніть на кнопку «*Save Settings*», це дозволить зберегти налаштування, натисніть на кнопку «*Продовжити*» для подальшого налаштування (рис. 13.4).

Рисунок 13.4 – Збереження налаштувань

Тепер виберіть «*Administration*» із меню верхнього рівня та змініть пароль для тестування, а також перейдіть у кінець сторінки і натисніть на кнопку «*Save Settings*» (рис. 13.5).

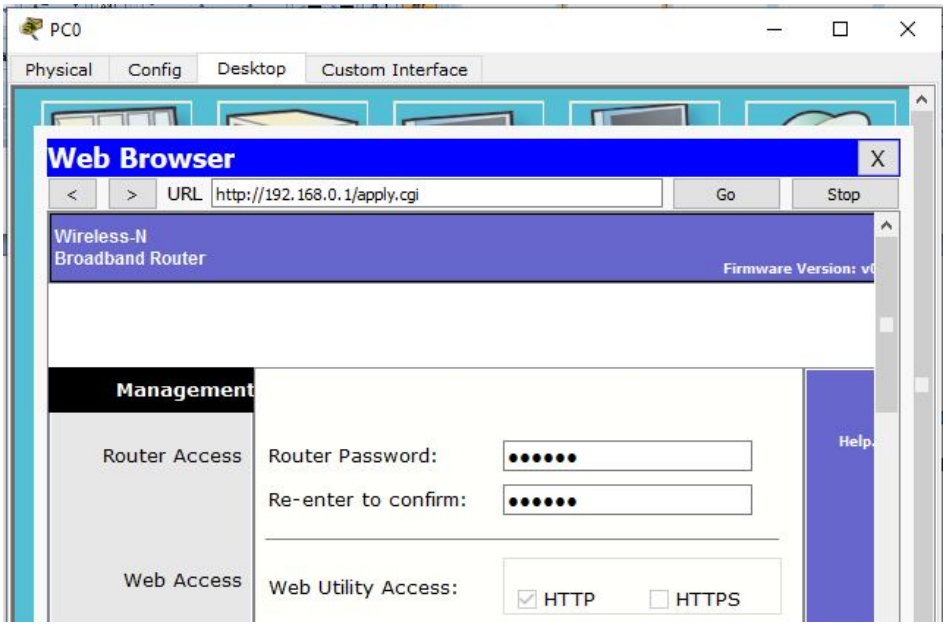

Рисунок 13.5 – Зміна паролю

Натисніть на кнопку «*Продовжити*» для подальшого налаштування. На цей раз буде запит на переавторизацію (рис. 13.6).

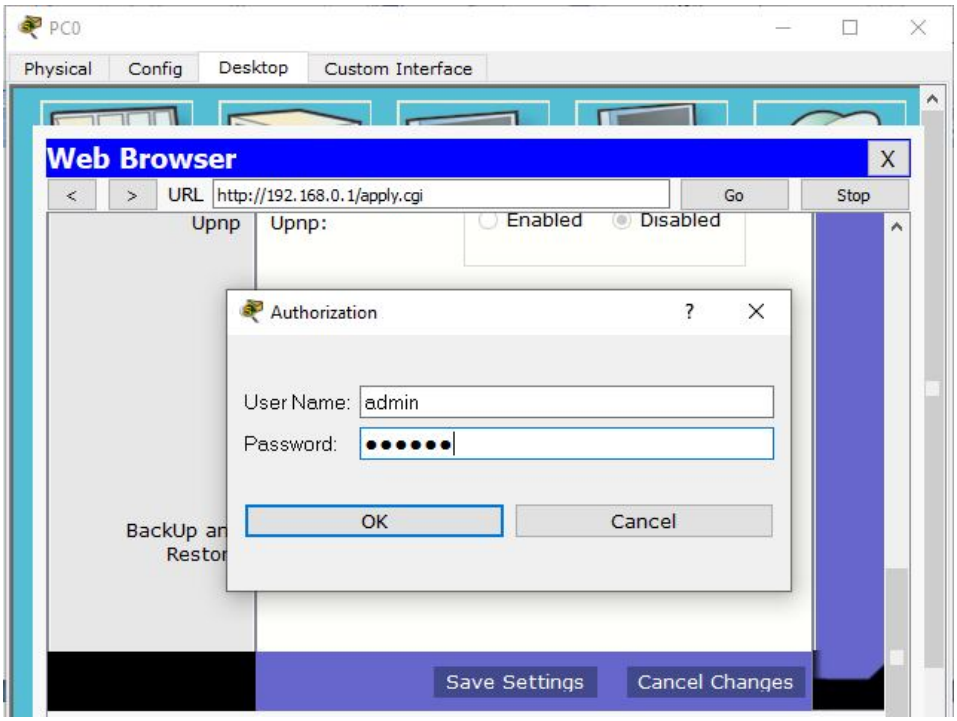

Рисунок 13.6 – Вікно переавторизації

Тепер натисніть на вкладці «*Wireless*» і встановіть за замовчуванням *SSID* як «*MotherNetwork*» (рис. 13.7).

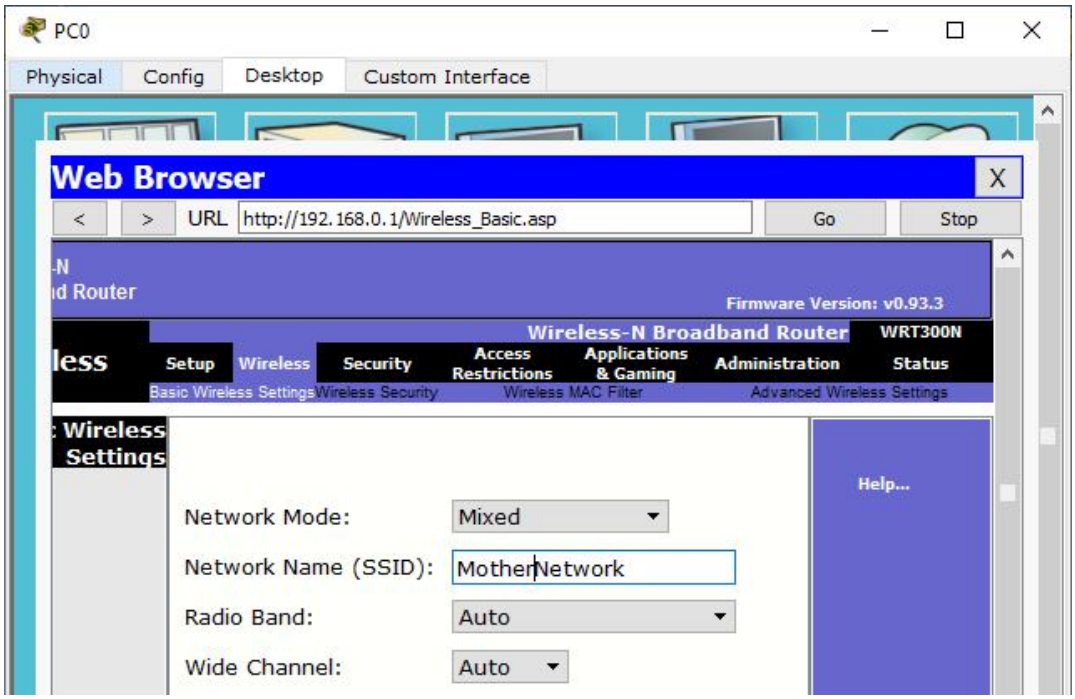

Рисунок 13.7 – Установка *SSID*

Тепер виберіть «*Wireless Security*» і змініть режим безпеки на «*WEP*» (рис. 13.8).

Рисунок 13.8 – Зміна режиму безпеки

Встановіть «*Key1*» у «0123456789» (рис. 13.9).

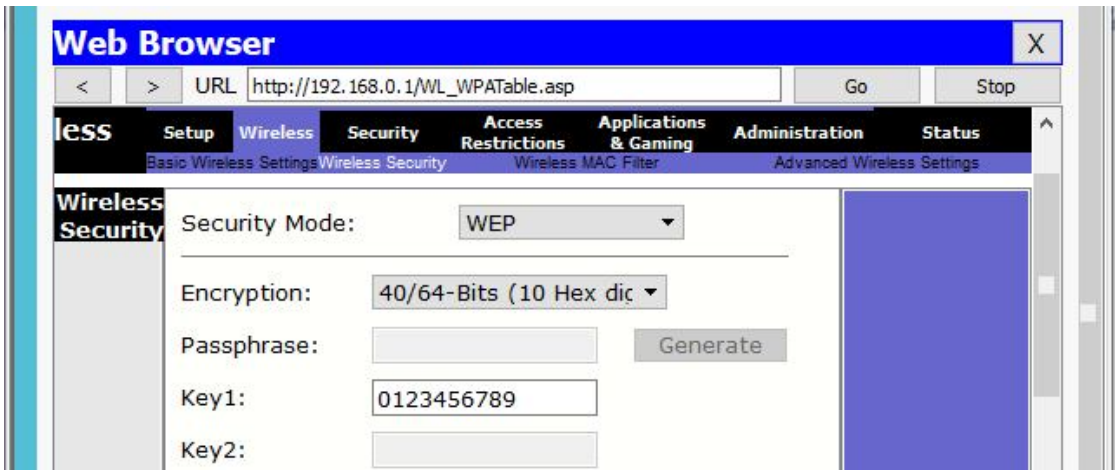

Рисунок 13.9 – Значення параметра «*Key1*»

Перейдіть у кінець сторінки й натисніть на кнопку «*Save Settings*».

Тепер необхідно налаштувати статичний IP на всіх трьох ПК. Після клацання на ПК виберіть вкладку «*Desktop»* та натисніть на конфігурації IP, виберіть «*Static IP»* і встановіть *IP*, як зазначено нижче в таблиці 13.1.

Таблиця 13.1 – Конфігурації IP адреси

PC	IP	Subnet Mask	Default Gateway
PC0	192.168 0.2	255.255.255.0	192.168.0.1
PC1	192.168.0.3	255.255.255.0	192.168.0.1
PC2	192.168.0.4	255.255.255.0	192.168.0.1

Тепер настав час для підключення ПК від бездротового маршрутизатора. Щоб зробити це, натисніть на ПК і виберіть «*Робочий стіл*», а потім натисніть на кнопку *«PC Wireless»* (мал. 13.10).

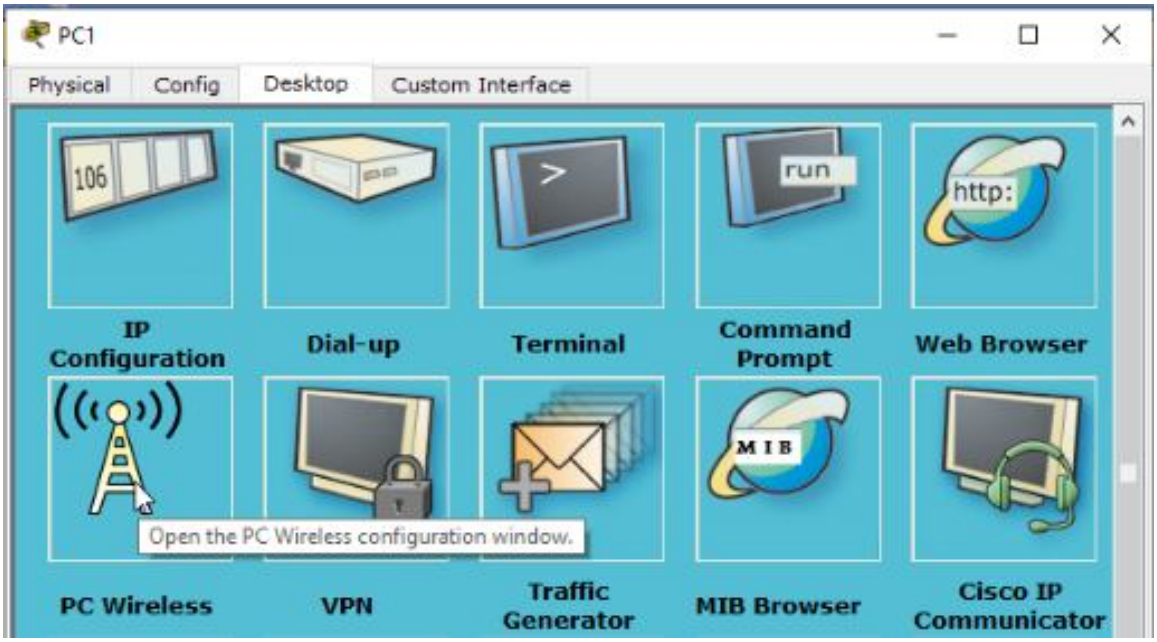

Рисунок 13.10 – Підключення ПК до бездротового маршрутизатора

Натисніть на вкладці «*Connect*» і натисніть на кнопку «*Оновити*» (рис. 13.11).

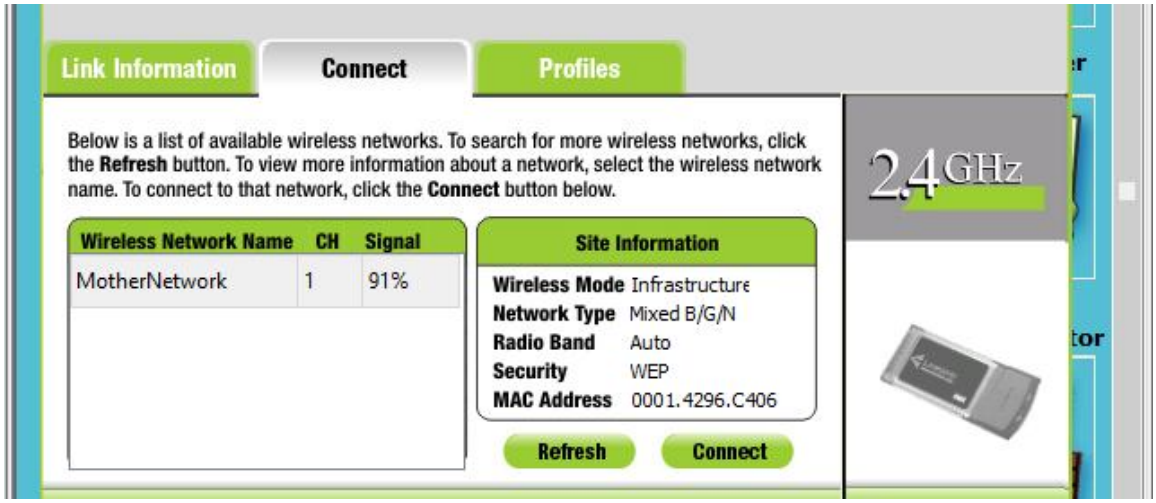

Рисунок 13.11 – Вкладка «*Connect*»

Як можна побачити на рисунку 13.11, у бездротового пристрою доступу *MotherNetwork* потужність сигналу становить 91%. Натисніть на кнопку «*Connect*» для підключення *MotherNetwork*.

Потім відбудеться запит ключа *WEP*. Уведіть «0123456789» і натисніть кнопку «*Connect*» (рис. 13.12).

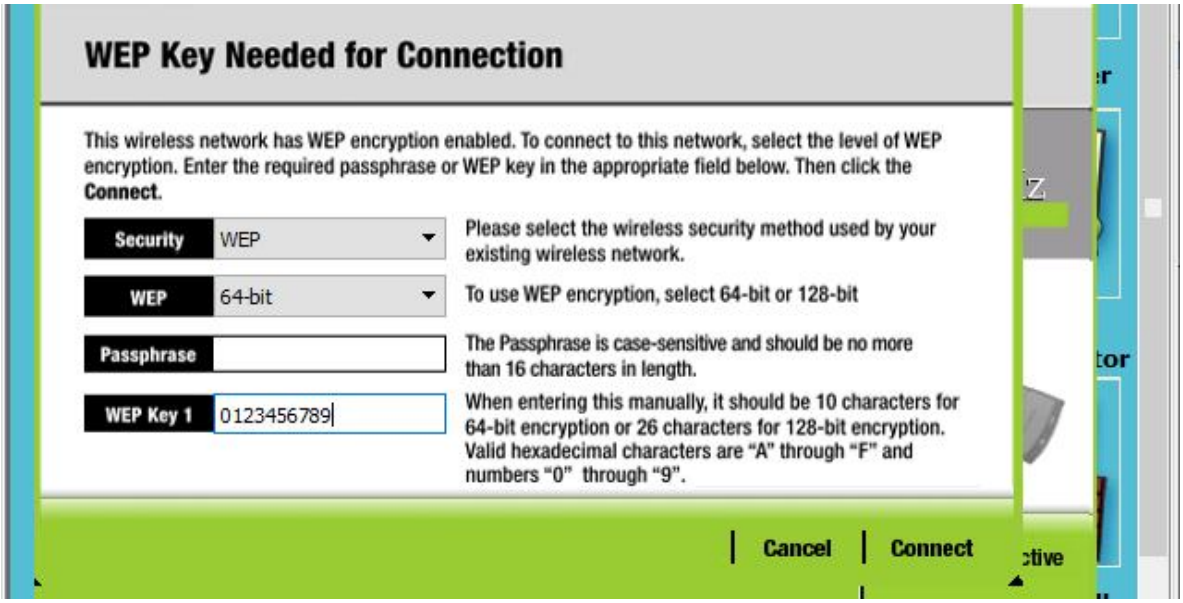

Рисунок 13.12 – Уведення ключа *WEP*

Можна побачити на рисунку 13.13, що система підключена та PC1 карта активна.

Рисунок 13.13 – Система підключена

Повторіть дії для PC0 і PC2.

13.4 Вимоги до оформлення звіту

1. Звіт із практичної роботи повинен бути оформлений відповідно до загальноприйнятих правил оформлення практичних робіт і містити такі пункти:

– тема роботи;

– мета роботи;

– опис перебігу виконання роботи.

2. Для кожного завдання описати процес його виконання з проміжними рисунками та скріншотами.

13.5 Контрольні питання

1. Назвіть обладнання, яке використовується для організації бездротового з’єднання.

2. Які ви виконували дії для реалізації прикладу «*Налаштування основних параметрів безпровідної мережі за допомогою Cisco Packet Tracer»*?

3. Який порядок підключення до бездротового маршрутизатора, щоб потім включити DHCP?

4. Який порядок налаштування статичної IP-адреси на всіх трьох ПК?

5. Поясніть, у який спосіб відбувалося підключення ПК від бездротового маршрутизатора.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Промислові мережі та інтеграційні технології в автоматизованих системах : навч. посібник / О. М. Пупена, І. В. Ельперін, Н. М. Луцька, А. П. Ладанюк. – Київ : Вид-во «Ліра-К», 2011. – 552 с.

2. Олифер В. Г. Новые технологии и оборудование IP-сетей / В. Г. Олифер, Н. А. Олифер. – СПб. : «БХВ-Санкт-Петербург», 2000. – 512 с.

3. Ретано А. Принципы проектирования корпоративных IP-сетей: [пер. с англ.] / А. Ретано. – М. : «Вильямс», 2002. – 368 с.

4. Таненбаум Э. Компьютерные сети : монографія : [пер. с англ.] / Э. Таненбаум. – 4-е изд. – СПб. : «Питер», 2003. – 992 с.

5. Баженов В. А. Комп'ютерні технології : підручник для студентів вузів / В. А. Баженов, П. С. Венгерський, В. М. Горлач. – Київ : Вид-во «Каравелла», 2004. – 463 с.

6. Мультисервисные сети / В. В. Величко,. Е. А. Субботин, В. П. Шувалов, А. Ф. Ярославцев. – М.: Горячая линия. Телеком, 2005. –592 с.

7. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : монография / В. Г. Олифер, Н. А. Олифер – СПб. : «Питер», 2001. – 672 с.

8. Стивенс У. Р. Протоколы TCP/IP : практ. рук.: [пер. с англ.] / У. Р. Стивенс. – СПб. : Невский диалект ; БХВ- Санкт-Петербург, 2003. – 672 с.

9. Гаскин Д. Администрирование Novell NetWare 6.0/6.5 : монография: [пер. с англ.] / Д. Гаскин;– СПб. : БХВ- Санкт-Петербург, 2003. – 1056 с.

10. Хант К. TCP/IP. Сетевое администрирование : монография: [пер. с англ.] / К. Хант. – СПб. : «Символ-Плюс», 2004. – 816 с.

11. Сліпченко В.Г. Локальні комп'ютерні мережі. Проектування, використання та програмування : навч. посіб. / В. Г. Сліпченко, В. І. Гайдаржи, В. А. Лабжинський. – Київ : ІВЦ «Політехніка», 2002. – 184 с.

12. Net Cracker 4.1. User Manual. Нормативные материалы [Электронный ресурс]. – Режим доступа : http://soft-landia.ru/netcracker.html

13. Практичне руководство «Internetworking Guide» [Электронный ресурс]. – Режим доступа: http://www.cisco.com

14. Автоматизация технологических процессов. [Электронный ресурс]. – Режим доступа http://microl.ua/index.php?page=shop.product_details&flypage=garden_flypage.tpl&product_id=157&category_id=68&option=com_virtuemart&Itemid=71

15. Нові продукти АСУ ТП і КВП. [Електронний ресурс]. – Режим доступу : http://ua.automation.com/produkty-dlya-avtomatizatsii

16. Модуль USART [Электронный ресурс]. – Режим доступа: http://www.gaw.ru/html.cgi/txt/doc/micros/avr/arh_xmega_a/21.htm

Виробничо-практичне видання

Методичні рекомендації
для проведення практичних занять
із навчальної дисципліни

«ПРОМИСЛОВІ КОМП'ЮТЕРНІ МЕРЕЖІ»

(для студентів другого (магістерського) рівня вищої освіти за спеціальністю 151 – Автоматизація та комп'ютерно-інтегровані технології за освітньо-професійною програмою «Системна інженерія»)

Укладачі: **БІЛЕЦЬКИЙ** Ігор Васильович,
ШУЛЬГА Наталія Вікторівна,
ПАХОМОВ Юрій Васильович,
ПІДДУБНА Лідія Валеріївна

Редактор *В. І Шалда*
Компютерний набір і верстання *Ю. В. Пахомов*

План 2021, поз. 300М

Підп. до друку 14.06.2021. Формат 60 × 84/16.
Друк на ризографі. Ум. друк. арк. 7,9.
Тираж 50 пр. Зам. №

Видавець і виготовлювач:
Харківський національний університет
міського господарства імені О. М. Бекетова,
вул. Маршала Бажанова, 17, Харків, 61002.
Електронна адреса: office@kname.edu.ua
Свідоцтво суб'єкта видавничої справи:
ДК № 5328 від 11.04.2017.