МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Б.Ю. Жураковський, І.О.Зенів

КОМП'ЮТЕРНІ МЕРЕЖІ

НАВЧАЛЬНИЙПОСІБНИК ДЛЯ ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

*Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для студентів,
які навчаються за спеціальністю 126 «Інформаційні системи та технології»,
спеціалізацією «Інформаційне забезпечення робототехнічних систем»*

Київ
КПІ ім. Ігоря Сікорського
2020

УДК 004.7(075.8)

Рицинзенти: *Ткаченко О.М.,* д.т.н., доцент, завідувач кафедри комп'ютерної інженерії Державного університету телекомунікацій

Коршун Н.В., д.т.н., доцент, професор кафедри інформаційної та технічної безпеки Київського університету ім. Б.Гринченка

Відповідальний редактор *Батрак Є.В.,* канд. техн. наук, доц.

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол №8 від 09.04.2020 р.) за поданням Вченої ради Факультету інформатики та обчислювальної техніки (протокол №7 від 17.02.2020 р.)

Електронне мережне навчальне видання

Жураковський Богдан Юрійович, доктор техн. наук, проф.
Зенів Ірина Онуфріївна, канд. техн. наук, доц.

КОМП'ЮТЕРНІ МЕРЕЖІ
НАВЧАЛЬНИЙ ПОСІБНИК ДЛЯ ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

КОМП'ЮТЕРНІ МЕРЕЖІ НАВЧАЛЬНИЙ ПОСІБНИК ДЛЯ ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ [Електронний ресурс]: навч. посіб. для студ. спеціальності 126«Інформаційні системи та технології»/ спеціалізації «Інформаційне забезпечення робототехнічних систем» / Б.Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 10,08 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. –213 с.

Посібник призначений для опанування практичних навичок, що необхідні майбутнім фахівцям для вивчення дисципліни «Комп'ютерні мережі». Обсяг та переліктем запропонованого посібника повністю покриває потреби 126 спеціальності. Для кожної теми наведено перелік питань для самоконтролю, задачі для роботи в аудиторії різногорівня складності та вказано питання, що будуть включені в модульну контрольну роботу. Посібник призначений для студентів спеціальності 126 «Інформаційні системи та технології» всіх форм навчання.

©Б. Ю. Жураковський, І. О. Зенів, 2020
© КПІ ім. Ігоря Сікорського, 2020

ЗМІСТ

ВСТУП.	3
Лабораторна робота №1**«***Введення в програму Cisco Packet Tracer, режим симуляції*»	7
Лабораторна робота №2 «*Моделювання мережі з топологією зірка на базі концентратора і комутатора*»	26
Лабораторна робота №3 «*Основи роботи з мережною операційною системою Cisco IOS*»	45
Лабораторна робота №4 «*Побудова віртуальних локальних мереж(VLAN)*»	62
Лабораторна робота №5 «*Налагодження та дослідження роботи протоколу динамічного конфігурування вузлів DHCP*»	88
Лабораторна робота №6 «*Вивчення динамічної маршрутизації на протоколах RIP, EIGRP і OSPF*»	117
Лабораторна робота №7 «*Створення списків доступу ACL*»	143
Лабораторна робота №8 «*Налаштування статичних та динамічних трансляцій мережних адрес*»	162
Лабораторна робота№9 «*Створення та налаштування безпроводової мережі*»	186
Література	213

ВСТУП. ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТІВ З ЛАБОРАТОРНИХ РОБІТ

Навчальний посібник розроблений для студентів, які навчаються за напрямком підготовки 126 «Інформаційні системи та технології» з навчальної дисципліни «Комп'ютерні мережі». Зазначена дисципліна згідно з освітньо-професійною програмою та навчальними планами підготовки бакалаврів належить до нормативної частини циклу дисциплін професійної і практичної підготовки.

Основним призначенням даного посібника є: поглиблення теоретичних знань, отриманих студентами під час вивчення змістового модуля; набуття практичних навичок із налагодження та діагностики роботи мережних пристроїв; набуття навичок дослідження процесів передачі даних у незахищених та захищених локальних мережах при використанні різних мережевих технологій та протоколів, а також набуття навичок усунення вразливостей та протидії мережним атакам на кінцеві вузли та комунікаційні пристрої мереж.

Для проведення лабораторних робіт передбачається використання спеціалізованих програмних комплексів із комп'ютерної симуляції/емуляції роботи мережних пристроїв і вузлів та мереж у цілому. Такий підхід забезпечує набуття студентами комплексних знань та практичних навичок у сфері професійної діяльності.

Перевагою даних методичних рекомендацій є подача перед кожним із завдань на лабораторну роботунеобхідних теоретичних відомостей, пов'язаних із вивченням досліджуваної технології чи протоколу захисту інформації. Методичні рекомендації містять достатньо деталізовану довідникову інформацію з питань налагодження та діагностики роботи засобів захисту мережних пристроїв, а також ознайомлюють студентів із

готовими прикладами налагоджень пристроїв. Слід зазначити, що роботи виконуються індивідуально за варіантами. Вибір номера варіанта проводиться засписком групи. Під час іменування комунікаційних пристроїв, кінцевих вузлів, розрахунку параметрів та розподілу IP-адрес також застосовується індивідуалізований підхід. Він полягає у тому, що у назвах пристроїв, IP-адресах мереж використовуються дві останні цифри номера групи (G) та дві цифри номера варіанта (N). Наприклад, IP-адреса мережі 192.G.N.0/24 для 312-ї групи та 25-го номера варіанта виглядатиме як 192.12.25.0/24. Додаткові параметри налагоджень також обираються відповідно доваріанта.

Повне виконання лабораторної роботипередбачає виконання таких етапів: ознайомлення з теоретичними відомостями; аналіз модельного прикладу (сценарію) розрахунків та налагоджень; аналіз індивідуального варіанта завдання; підготовка інформації для налагодження пристроїв та з’єднань; виконання, за потреби, теоретичних розрахунків; проведення налагоджень мережних пристроїв та кінцевих вузлів; діагностика роботи побудованої мережі; визначення проблем при взаємодії вузлів та їх усунення; дослідження процесів передачі даних у побудованій мережі; формулювання висновків за результатами роботи; оформлення та захист звіту; підготовка до подальших контрольнихзаходів.

Звіт із лабораторної роботи оформлюється згідно з вимогами Державного стандарту України ДСТУ 3008-95 *Документація. Звіти у сфері науки і техніки. Структура і правила оформлення,* міжнародних стандартів ISO 5966:1982 і повинен містити такі складові: номер роботи; тема роботи; мета роботи; розділ, у якому описано хід виконання роботи відповідно до пунктів завдання; висновки; додаток із лістингами налагоджень усіх комунікаційних пристроїв, рукописні відповіді на контрольні питання (додаються за вказівкою викладача). Звіт виконується в електронному вигляді, роздруковується, доповнюється відповідями на контрольні питання і

здається на кафедру для перевірки та захисту.

Під час оформлення звіту необхідно дотримуватися такихвимог: звіт оформлюється на аркушах формату А4. Нумерація сторінок наскрізна в межахроботи.

Лабораторна робота№ 1

Тема:ВВЕДЕННЯ В ПРОГРАМУ CISCO PACKET TRACER, РЕЖИМ СИМУЛЯЦІЇ.

***Мета заняття*:**вивчити інтерфейс програми Cisco Packet Tracer,головне меню,панель інструментів, устаткування, лінії зв'язку, графічне меню, елементи анімації і симуляції, застосувати отримані знання при виконанні практичних завдань.

Теоретичні відомості

Введення в програму Cisco Packet Tracer (CPT)

Cisco є всесвітньо відомим розробником і виробником мережевого устаткування. Ця американська компанія прагне представити повний спектр мережевого обладнання, і таким чином надати можливість клієнту закупити абсолютно все необхідне мережеве обладнання виключно у **Cisco Systems**.

Cisco Packet Tracer - це емулятор мережі, створений компанією **Cisco**. Програма дозволяє будувати і аналізувати мережі на різноманітному обладнанні в довільних топологіях з підтримкою різних протоколів. У ній ви отримуєте можливість вивчати роботу різних мережевих пристроїв: маршрутизаторів, комутаторів, точок бездротового доступу, персональних комп'ютерів, мережевих принтерів і т.д. Цей додаток є найбільш простим і ефективним серед своїх конкурентів. **Cisco Packet Tracer** це те, з чого варто починати вивчати обладнання **Cisco**. (Рис. 1.1).

Рис. 1.1. Логотип програми CPT

Інтерфейс програми Cisco Packet Tracer

На рис. 1.2 представлений ***інтерфейс*** (головне вікно) програми Cisco Packet Tracer.

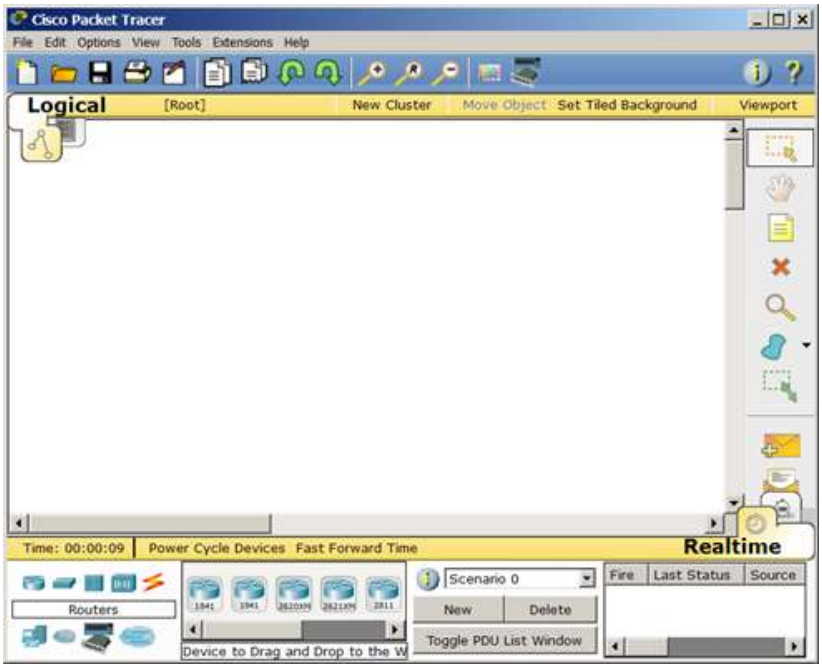


Рис. 1.2. Інтерфейс програми Cisco Packet Tracer (CPT)

Головне меню

Головне меню показано на рис. 1.3

Рис. 1.3. Головне меню

File (Файл) - містить операції відкриття / збереження документів.

Edit (Правка) - містить стандартні операції "копіювати / вирізати, скасувати / повторити";

Options (Налаштування) - містить налаштування програми. Зокрема, тут розташована кнопка **ChangeLanguage**, що дозволяє виробляти локалізацію програми на інші мови.

View (Вид) - містить інструменти зміни масштабу робочої області і панелі інструментів;

Tools (Інструменти) - містить кольорову палітру і вікно для користувача пристроїв;

Exensions (Розширення) - містить майстер проектів і ряд інших інструментів;

Help (Допомога)-містить допомогу по програмі.

Панель інструментів

Панель інструментів наведена на рис. 1.4.

Рис. 1.4. Панель інструментів

Панель інструментів за допомогою піктограм дублює основні пункти

головного меню програми.

Устаткування

Знизу, під робочою областю, розташована панель обладнання. Дана панель містить в своїй лівій частині типи (класи) пристроїв, а в правій частині - їх найменування (моделі). При наведенні на кожне з пристроїв, в прямокутнику, що знаходиться в центрі між ними буде відображатися його тип. Типи обладнання представлені на рис. 1.5.

Рис. 1.5.Панель обладнання Packet Tracer (Основні типи обладнання)

Маршрутизатори (**роутери**) використовується для пошуку оптимального маршруту передачі даних на підставі алгоритмів маршрутизації. **Комутатори** - пристрої, призначені для об'єднання декількох вузлів в межах одного або декількох сегментах мережі. **Комутатор** (**світч**) передає пакети інформації на підставі таблиці комутації, тому трафік йде тільки на той MAC-*адрес*, 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** ви побачите ПК, ноутбук, *сервер*, принтер, телефони і так далі. **Інтернет** в програмі представлений у вигляді хмар і модемів DSL. Призначені для користувача пристрої та хмара для

багатокористувацької роботи показані на рис. 1.6.

Рис. 1.6. Призначені для користувача пристрої та хмара для багатокористувацької роботи

Лінії зв'язку

За допомогою ліній зв'язку створюються з'єднання вузлів мережі в єдину топологію і при цьому кожен тип кабелю може бути з'єднаний лише з певними типами інтерфейсів пристроїв (рис. 1.7).

Рис. 1.7. Типи ліній зв'язку

Автоматичний тип - при даному типі з'єднання Packet Tracer автоматично вибирає найбільш кращі тип з'єднання для обраних пристроїв.

Консоль - консольні з'єднання. Консольне з'єднання може бути виконано між ПК і маршрутизаторами або комутаторами.

Мідь прямий - з'єднання мідним кабелем типу вита пара, обидва кінці кабелю обтиснуті в однаковій розкладці.

Мідь кросовер - з'єднання мідним кабелем типу вита пара, кінці

кабелю обтиснуті як кросовер.

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. Приклад - ПК, додзвонюється в мережеве хмара.

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'язків *Інтернет*. Для настройки таких з'єднань необхідно встановити синхронізацію на стороні *DCE-пристрої*. Сторону *DCE* можна визначити по малесенькій іконці "годин" поруч з портом.

Графічне меню

На рис. 1.8 показано графічне меню програми.

Рис. 1.8.Графічне меню (повернуто)

На цьому рисунку зліва направо:

Інструмент **Select** (Вибрати) можна активувати клавішею **Esc**. Він використовується для виділення одного або більше об'єктів для подальшого їх переміщення, копіювання або видалення.

Інструмент **Move Layout** (Перемістити шар, гаряча клавіша **M**) використовується для прокрутки великих проектів мереж.

Інструмент **Place Note** (Зробити позначку, клавіша **N**) додає текст в

робочій області проекту.

Інструмент **Delete** (Видалити, клавіша **Del**) видаляє виділений об'єкт або групу об'єктів.

Інструмент **Inspect** (Перевірка, клавіша **I**) дозволяє, в залежності від типу пристрою, переглядати вміст таблиць (*ARP*, *NAT*, таблиці маршрутизації ін.).

Інструмент **Drawapolygon** (Нарисувати багатокутник) дозволяє рисувати прямокутники, еліпси, лінії і зафарбовувати їх кольором.

Інструмент **Resize Shape** (Змінити розмір форми, комбінація клавіш **Alt + R**) призначений для зміни розмірів нарисованих об'єктів (чотирикутників і кіл).

Елементи анімації і симуляції

Ці елементи інтерфейсу показані на рис. 1.9.

Рис. 1.9. Елементи анімації і симуляції

Інструменти **Add Simple PDU** (Додати простий *PDU*, клавіша **P**) і **Add Complex PDU** (Додати комплексний *PDU*, клавіша **C**) призначені для емуляції відправки пакета з подальшим відстеженням його маршруту і даних всередині пакету.

Фізичне представлення обладнання

У програмі можливо фізичне уявлення обладнання в вигляді його фізичної конфігурації (рис. 1.10).

Рис. 1.10. Фізична конфігурація ПК

Для зміни комплектації обладнання необхідно відключити його харчування, кликнувши мишкою на кнопці харчування і перетягнути мишею потрібний модуль у вільний ***слот***, потім включити харчування. Як приклад я додав в фізичну конфігурацію ПК мікрофон (PT-MICROPHONE), в результаті чого ПК змінив свій значок в програмі (рис. 1.11).

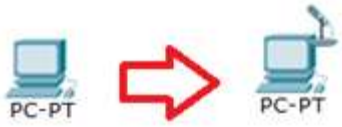


Рис. 1.11. Зміна піктограми ПК після підключення до нього мікрофона

Решта модулі додаються в пристрої аналогічно. Так, на комп'ютер є можливість додати не тільки мікрофон, але і, наприклад, навушники або жорсткий диск для зберігання даних.

Завдання на лабораторну роботу

Завдання 1.1. Створення мережі з 2х ПК і налаштування її роботи.

Завдання 1.2. Вивчення режиму симуляції в Cisco Packet Tracer.

Завдання 1.3. Налаштування мережевих параметрів ПК в його графічному інтерфейсі.

Завдання 1.1. Створення мережі з двох ПК в програмі Cisco Parket Tracer

Як приклад для початкового знайомства з програмою побудуємо найпростішу мережу з двох ПК, з'єднаних кросовим кабелем (рис. 1.12).

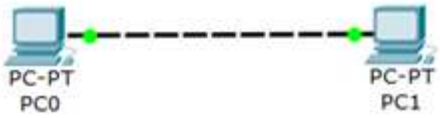


Рис. 1.12. Мережа з двох ПК

Для вирішення нашої задачі на вкладці **EndDevicesCtrl+Alt+V** (Кінцеві пристрої) вибираємо тип комп'ютера і переносимо його мишею в робочу область програми (рис. 1.13).

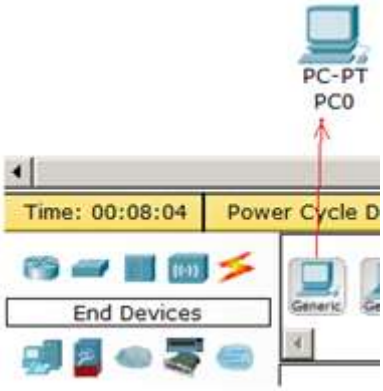


Рис. 1.13. Встановлюємо в робочу область програми перший ПК

Комп'ютери з'єднуємо за допомогою мідного кросовера **CopperCross-**

Over (Перехресний кабель).

Порада

Якщо при виборі кросовера зелені лампочки не засвітяться, то виберіть тип з'єднання Автоматично.

Тепер приступимо до налаштування лівого ПК: клацаємо на ньому мишею, переходимо на вкладку **Ip Configuration** (Налаштування *IP*) - рис. 1.14.

Рис.1.14. Стрілка показує на кнопку відкриття вікна IP Configuration

Для першого ПК вводимо ***IP адреса*** 192.168.1.1 і маску підмережі 255.255.255.0, вікно закриваємо (рис. 1.15). Аналогічно налаштовуємо другий ПК на адресу 192.168.1.2 і ту ж маску.

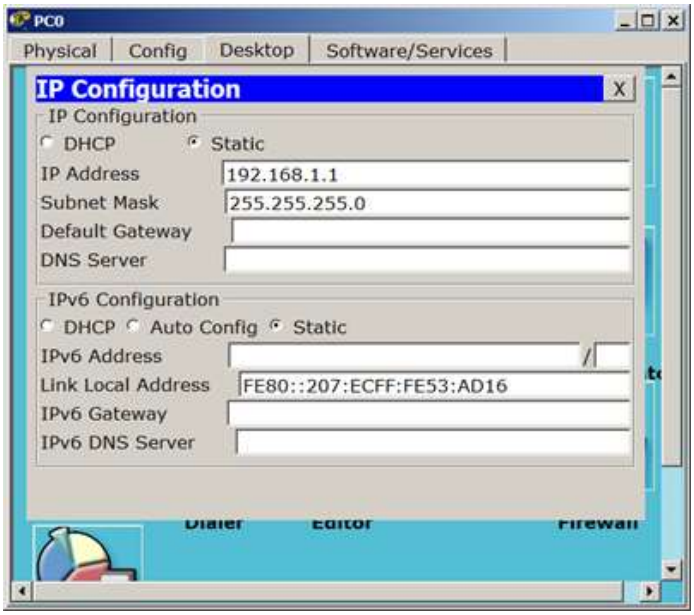


Рис. 1.15. Вікно налаштування PC0

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) і пропінгуємо сусідній ПК (рис. 1.16).

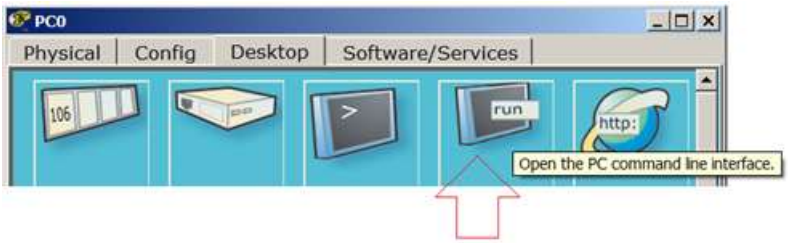


Рис. 1.16.Кнопка run

Як видно з рис. 1.17. зв'язок між ПК присутній (налаштована).

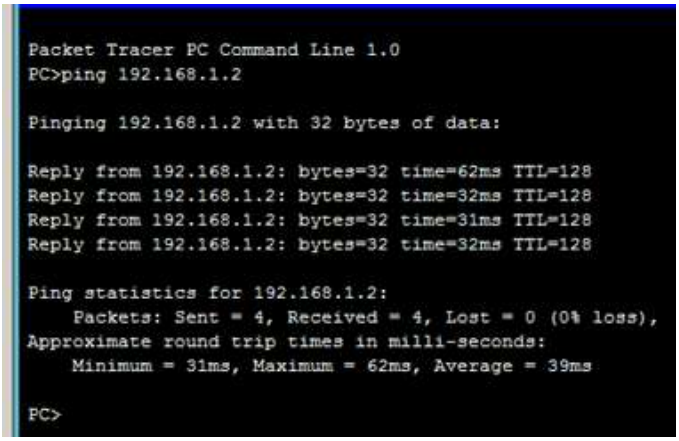


Рис. 1.17. Пінг пройшов успішно

Завдання 1.2.Організація режиму симуляції роботи мережі

Сформуйте в робочому просторі програми мережу з 4х ПК і 2х хабів. Задайте для ПК IP адреси і маску мережі 255.255.255.0 (рис. 1.18).

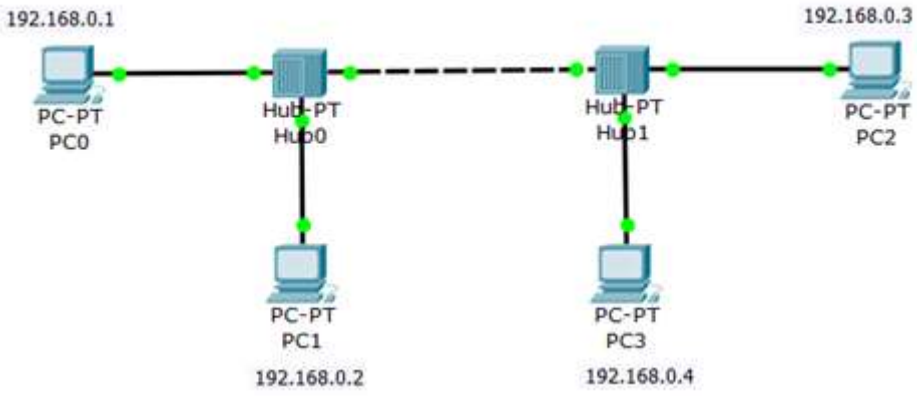


Рис. 1.18. Всі ПК розташовані в одній мережі

Порада

*Схему можна зберегти як картинки з розширенням * PNG командою* ***File-Print-Print to file****.*

Тепер потрібно перейти в режим симуляції комбінацією клавіш **Shift + S,** або, клацнувши мишею на іконку симуляції в правому нижньому кутку робочого простору (рис. 1.19).

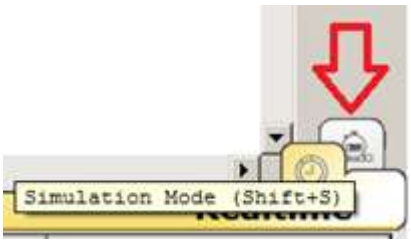


Рис. 1.19.Кнопка Симуляція

Натисніть на кнопку**EditFilters** (Змінити фільтри) і виключіть всі мережеві протоколи, крім *ICMP* (рис. 1.20).

Рис. 1.20. Прапорець ICMP активний

ICMP(Internet Control Message Protocol) - мережевий протокол, що входить в стек протоколів TCP / IP. В основному *ICMP* використовується для передачі повідомлень про помилки та інші виняткових ситуаціях, що виникли при передачі даних.

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. 1.21).

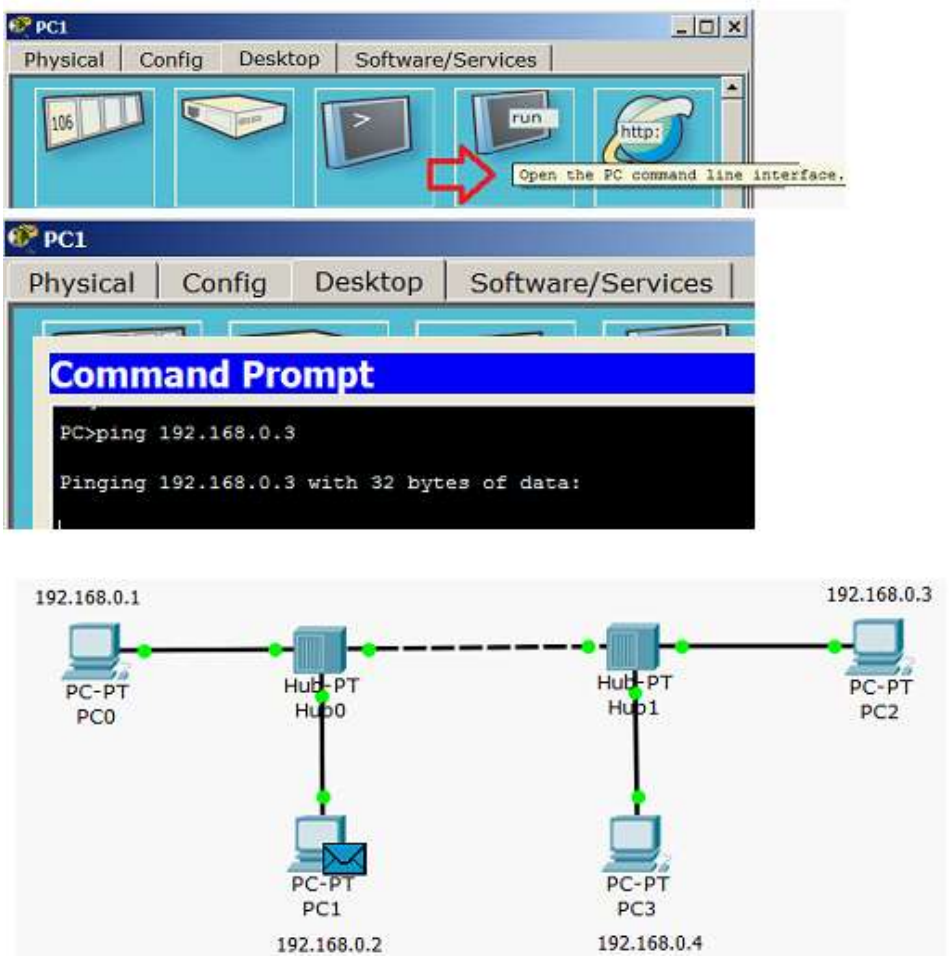


Рис. 1.21. PC1 пінг PC2 (початок процесу)

Ping - утиліта для перевірки з'єднань в мережах на основі TCP / IP.Утіліта 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 (або будь-якої з проміжних маршрутизаторів) блокує ***ICMP Echo-Reply*** або ігнорує ***ICMP Echo-Request***.

На *PC1* утворився пакет (конвертик), який чекає початку руху його по мережі. Запустити просування пакет в мережу покроково можна, натиснувши на кнопку **Capture/Forward** (**Вперед**) у вікні симуляції. Якщо натиснути на кнопку **AutoCapture/Play**(**відтворення**), то побачимо весь цикл проходження пакета по мережі. В (Список подій) можемо бачити успішний результат пінга (рис. 1.22).

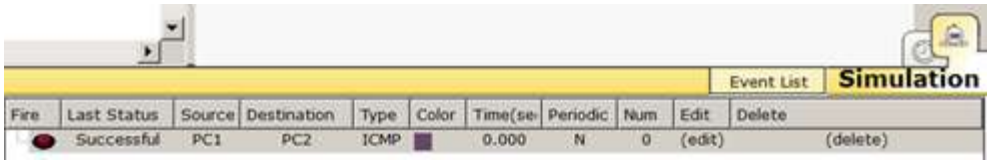


Рис. 1.22. Зв'язок PC1 і PC2 є

Модель OSI в Cisco Packet Tracer

Клацання мишею на конверті покаже додаткову інформацію про рух пакета по мережі. При цьому на першій вкладці побачимо **модель OSI** (рис. 1.23). На вкладці *OSI Model* (Модель OSI) представлена інформація про рівні *OSI*, на яких працює дане мережеве пристрій.

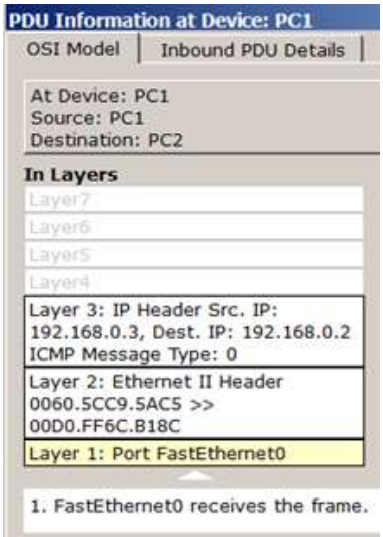


Рис. 1.23. Моніторинг руху пакета на моделі OSI

На іншій вкладці можна подивитися структуру пакета (рис. 1.24).

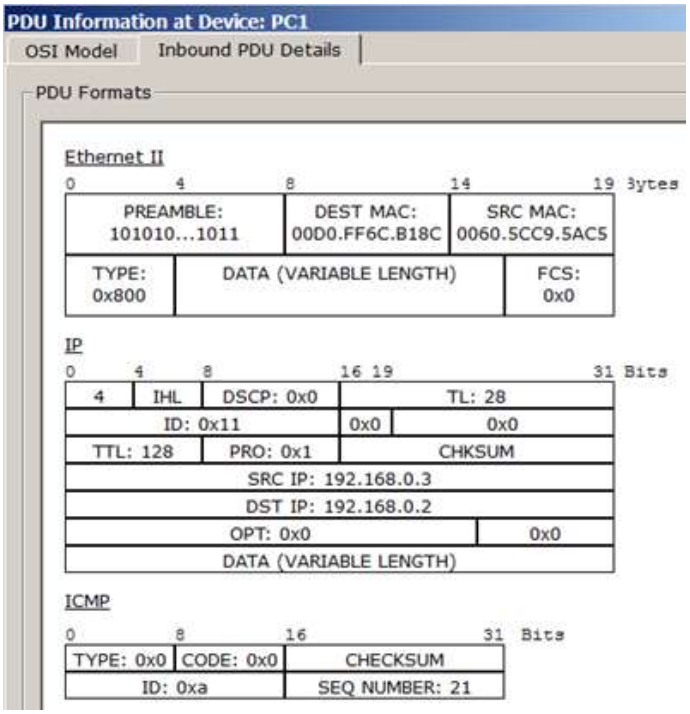


Рис. 1.24.Структура пакета

Підіб'ємо якийсь проміжний підсумок нашої роботи.

У **Packet Tracer** передбачений режим **моделювання (Симуляції),** в якому показується, як працює ***утиліта Ping***. Щоб перейти в даний 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* даний протокол задіяний. У процесі перегляду анімації ми побачили принцип роботи хаба. Концентратор (***хаб***) повторює пакет на всіх портах в надії, що на одному з них є одержувач інформації. Якщо пакети якимось вузлів які не призначені, ці вузли ігнорують пакети. А коли пакет повернеться відправнику, то побачимо галочку "прийняття пакету" (Рис. 1.25).

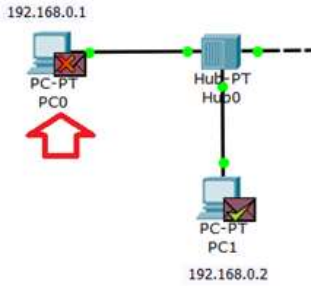


Рис. 1.25. Значки ігнорування пакетів та авторизація з'єднання

Командний рядок

Якщо натиснути на кнопку**Auto Capture/Play**(Відтворення), то побачимо весь цикл проходження пакета по мережі (процес повториться 4 рази) - рис. 1.26.

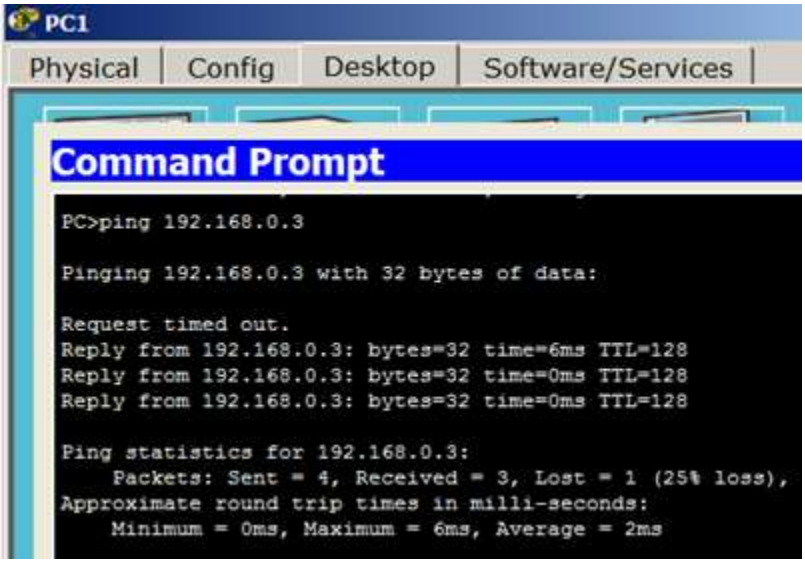


Рис. 1.26. Пінг від ПК1 до ПК2

тут:

TTL- час життя відправленого пакета (визначає максимальне число маршрутизаторів, яке пакет може пройти при його просуванні по мережі),

time - час, витрачений на відправку запиту і отримання відповіді,

min - мінімальний час відповіді,

max - максимальний час відповіді,

avg - середній час відповіді.

Завдання 1.3.Налаштування мережевих параметрів ПК в його графічному інтерфейсі

Додаємо в нашу мережу ще один ПК - PC4. Відкриємо властивості пристрою PC4, натиснувши на його зображення. Для конфігурації комп'ютера скористаємося командою **ipconfig** з командного рядка (рис. 1.27).

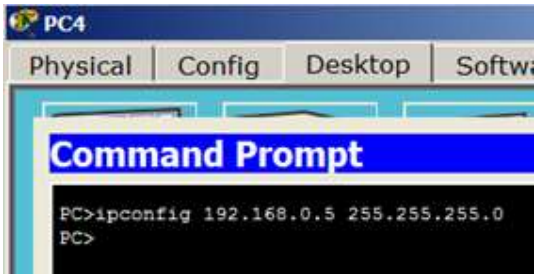


Рис. 1.27. Призначаємо для ПК ***IP*** адресу і маску мережі

Як варіант, *IP адреса* і *маску* мережі можна вводити в графічному інтерфейсі пристрою (рис. 1.28).

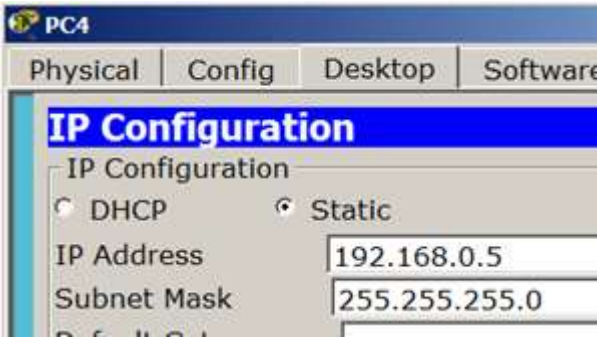


Рис. 1.28. Другий спосіб конфігурації комп'ютера (налаштування вузла мережі)

На кожному комп'ютері перевіримо призначені нами параметри командою **ipconfig** (рис. 1.29).

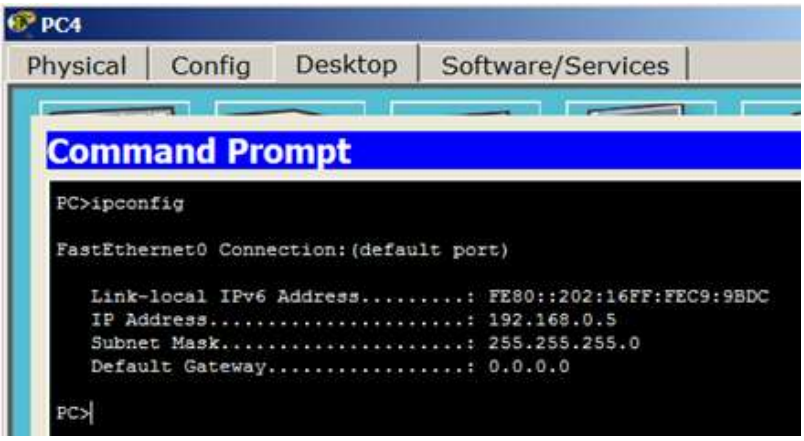


Рис. 1.29. Перевірка конфігурації ПК3

Склад звіту лабораторної роботи

В звіті повинно бути відображено:

1. Тема роботи.
2. Мета роботи.
3. Постановка задачі.
4. Виконання завдання 1.1 з відповідними скріншотами.
5. Виконання завдання 1.2 з відповідними скріншотами.
6. Виконання завдання 1.3 з відповідними скріншотами.
7. Висновок

Контрольні питання

1. Яке устаткування використовується в програмі Cisco Packet Tracer.
2. Які лінії зв'язку використовується в програмі Cisco Packet Tracer.
3. Що собою представляє графічне менюCisco Packet Tracer.
4. Які елементи анімації і симуляції використовуються в програмі Cisco Packet Tracer.
5. Яким чином забезпечується фізичне представлення обладнання.
6. Для чого викоистовується *ICMP (Internet Control Message Protocol)*.
7. Для чого використовується утиліта Ping.
8. Модель OSI в Cisco Packet Tracer.
9. Для чого уPacket Tracer передбачений режим моделювання (Симуляції)?

Лабораторна робота№ 2

Тема: МОДЕЛЮВАННЯ МЕРЕЖІ З ТОПОЛОГІЄЮ ЗІРКА НА БАЗІ КОНЦЕНТРАТОРА І КОМУТАТОРА

Мета заняття: вивчити моделювання мережі з топологією зірка на базі концентратора і комутатора, застосувати отримані знання при виконанні практичних завдань.

Теоретичні відомості

Зірка - базова топологія комп'ютерної мережі, в якій всі комп'ютери мережі приєднані до центрального вузла, утворюючи фізичний сегмент мережі. Центральним вузлом виступає концентратор, комутатор або ПК.

Робоча станція, з якої необхідно передати дані, відсилає їх на концентратор. У певний момент часу тільки одна машина в мережі може пересилати дані, якщо на концентратор одночасно приходять два пакети, обидві посилки виявляються не прийнятими і відправникам потрібно буде почекати випадковий проміжок часу, щоб відновити передачу даних. Цей недолік відсутній на мережевому пристрої більш високого рівня - комутаторі, який, на відміну від концентратора, що подає пакет на всі порти, подає лише на певний ***порт*** - одержувачу. Одночасно може бути передано кілька пакетів. Скільки - залежить від комутатора.

Переваги топології зірка:

- вихід з ладу однієї робочої станції не відбивається на роботі всієї мережі в цілому;

- легкий пошук несправностей і обривів в мережі; висока продуктивність мережі (за умови правильного проектування);
- гнучкі можливості адміністрування; гарна масштабованість. Для того щоб підключити нову робочу станцію, потрібно просто прокласти окремий кабель від комутатора;
- в мережу без проблем і додаткових зусиль можна вбудувати додаткові пристрої;
- висока продуктивність, особливо якщо порівнювати з аналогічними варіантами топології.

Недоліки топології зірка:

- вихід з ладу центрального концентратора обернеться непрацездатністю мережі (або сегмента мережі) в цілому;
- для прокладки мережі найчастіше потрібна більше кабелі, ніж для більшості інших топологій;
- число робочих станцій в мережі (або сегменті мережі) обмежена кількістю портів в центральному концентраторі;
- вартість реалізації, в якій має бути центральний вузол більша ніж у шинній топології кількість кабелю;
- щоб використовувати мережеве обладнання, потрібно виділити також додаткові витрати, так як потрібно придбання окремого пристрою, до якого будуть підключатися всі комп'ютери, підключені до мережі.

Відмінності у мережевому обладнанні для організації мережевих технологій

Залежно від властивостей та функцій мережевого обладнання одна й та ж сама фізична топологія може ставати зовсім іншою логічною топологією.

Комутатор (світч)– пристрій, призначений для з’єднання вузлів мережі у межах одного або декількох сегментів. Світч використовує другий рівень моделі OSI. Вхідний пакет, що надходить до комутатора, буде переданим

тільки одержувачу, що підвищує безпеку, а також продуктивність на відміну від концентратора. Принцип роботи полягає в зберіганні таблиці комутації, в якій міститься список відповідностей MAC-адрес вузлів до портів комутатора. Комутатор реалізує топологію логіної зірки.

Маршрутизатор (роутер) – пристрій, що служить для зв'язку різних мереж. Роутер працює на третьому рівні мережевої моделі OSI і для доставки пакетів використовує типологію мережі і правила задані адміністратором. Маршрутизатор може виконувати трансляцію адрес одержувача і відправника. Також може здійснювати фільтрацію потоку пакетів для обмеження або шифрування чи дешифрування даних. Важливою відмінністю між мережами, що використовують комутатори і маршрутизатори, є те, що мережі з комутаторами не блокують радіопередачі. В результаті комутатори можуть бути зіпсовані потоками пакетів радіопередач. Маршрутизатори блокують радіопередачі по локальній мережі, таким чином, потік радіопередач зачіпає тільки той домен, з якого він виходить.

Концентратор (хаб) – пристрій, призначений для побудови комп’ютерної мережі. Хаб використовує перший рівень мережевої моделі OSI і є ретранслятором в режимі напівдуплекса. Тобто вхідний пакет даних з поширюється концентратором на всі інші порти мережі; при виникненні колізії пристрій не встановлюватиме трансляцію і відновлює її через деякий проміжок часу. Концентратор реалізує топологію логічної шини.

Шлюзи – програмно-апаратні комплекси, що з'єднують різні мережі або мережеві пристрої. Шлюзи дозволяють вирішувати проблеми відмінності протоколів або систем адресації.

Повторювачі – пристрої мережі, що підсилюють і заново формують вхідний сигнал мережі на відстань іншого сегмента.

Мости – пристрої мережі, які з'єднують два окремих сегмента, обмежених своєю фізичною довжиною, і передають трафік між ними. Мости також можуть підсилювати і конвертувати сигнали.

Завдання на лабораторну роботу

Завдання 2.1. Моделювання мережі з топологією зірка на базі концентратора.

Завдання 2.2. Моделювання мережі з топологією зірка на базі комутатора.

Завдання 2.3. Проектування локальної мережі з хаба, комутатора і 4х ПК.

Завдання 2.4. Дослідження якості передачі трафіку по мережі.

Завдання 2.5. Проектування локальної мережі з заміною хабів комутаторами.

Завдання 2.1. Моделювання мережі з топологією зірка на базі концентратора

В даному прикладі за допомогою програмного симулятора ***Packet Tracer*** збудуємо***мережу*** з топологією ***Зірка*** на базі концентратора (рис. 2.1) і вивчимо ряд нових прийомів роботи в цій програмі.

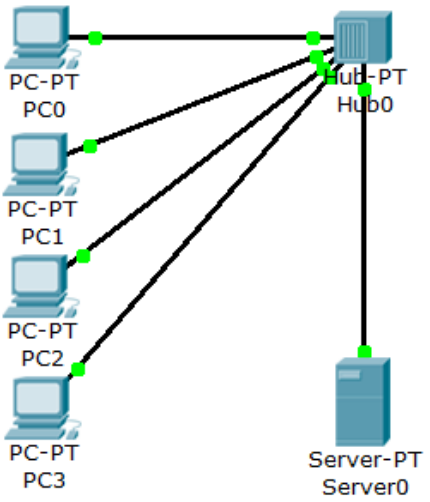


Рис. 2.1. Моделювання мережі з топологією зірка на базі концентратора

Компонування вузлів мережі вробочій області

Вибираємо ***типобладнання*** **Hub's** (Концентратори). В ***меню "список пристроїв даного типу обладнання"*** вибираємо конкретний концентратор - ***Hub***-PT і перетягуємо його мишею в робочу область програми. Далі вибираємо тип пристрою **End Devices** (Кінцеві пристрої) і в додатковому ***меню*** вибираємо настільний ***комп'ютер PC-PT*** і перетягуємо його мишею в робочу область програми. Таким чином, встановлюємо ще три комп'ютери і один ***сервер***. Для підключення комп'ютерів і сервера до концентратора вибираємо новий тип пристроїв **Connections** (З'єднання), далі вибираємо **CopperStraight-Through** (Мідний прямий) тип кабелю. Щоб з'єднати мережеву карту комп'ютера з портом ***Hub-а***, необхідно клацнути лівою клавішею миші по потрібному комп'ютера. В відкрилися графічному ***меню*** вибрати ***порт*** **FastEthernet0** і протягнути ***кабель*** від ПК до концентратора, де в аналогічному ***меню*** вибрати будь-який вільний ***порт*** **Fast Ethernet** концентратора. При цьому бажано завжди дотримуватися наступного правила: для сервера вибираємо 0-й ***порт***, для PC1 - 1й ***порт***, для PC2 - 2й ***порт*** і так далі. Призначаємо вузлів мережі ***IP***-адреса і маску. Для цього подвійним клацанням відкриваємо потрібний комп'ютер, далі **Config** (Конфігурація) - **Interface** (Інтерфейс) –**FastEthetnet 0**. У групі параметрів **IP Configuration** (Налаштування IP) повинен бути активований ***перемикач*** **Static** (Статичний) в ***поле*****IP Address** необхідно ввести IP-***адресу*** комп'ютера, ***маска*** з'явиться автоматично. **Port status** (Стан порту) - **On** (Увімкнути).

Інструмент створення заміток Place Note

Використовуючи інструмент створення заміток **Place Note** (клавіша **N**), підписуємо всі IP пристрої, а вгорі робочої області створюємо заголовок нашого проекту **"Вивчення топології зірка"** - рис. 2.2.

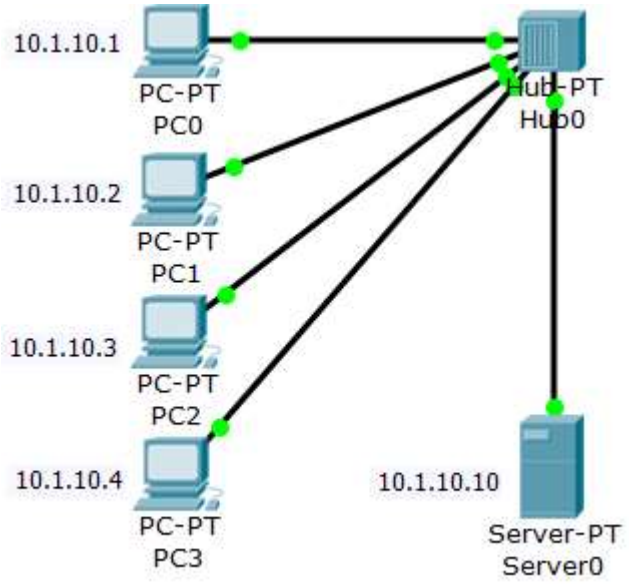


Рис. 2.2. Використовуємо інструмент Place Note (Замітка)

Порада

IP адреси слід скопіювати з вікна ***Config*** *(Конфігурація). При цьому активуйте інструмент* ***Place Note*** *(Замітка).*

З метою виключення нагромадження робочої області написами, приберемо написи (**мітки**) типів пристроїв: відкриємо ***меню*****Options** (Опції) у верхній частині вікна ***Packet Tracer***, потім в випадаючому списку виберемо ***пункт*****Preferens** (Налаштування), а в діалоговому вікні знімемо прапорець **Show device model labels** (Показати моделі пристроїв) - рис. 2.3.

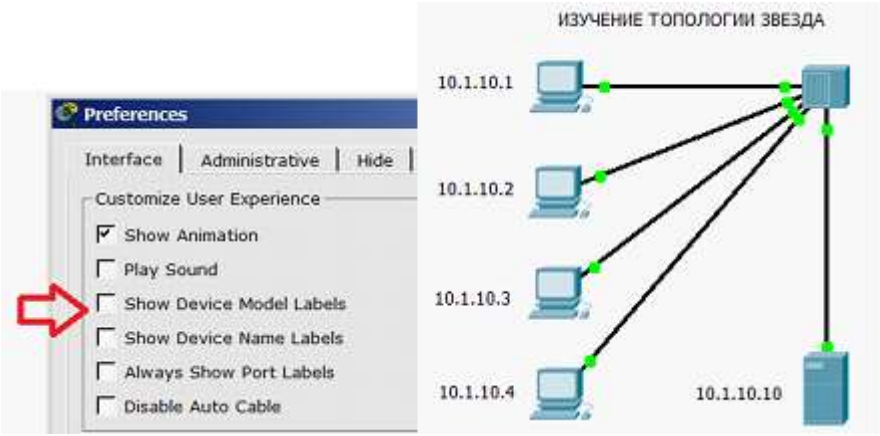
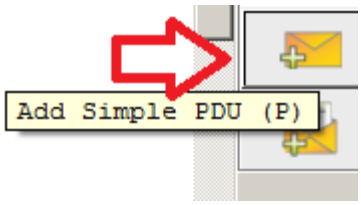


Рис. 2.3. Дезактивуємо прапорець Show device model labels

Для перевірки працездатності мережі відправимо з комп'ютера на інший ПК тестовий сигнал ***ping*** і перемкнемося в режим **Simulation** (Симуляція). У вікні **Event list** (Список подій), за допомогою кнопки **Edit filters** (Змінити фільтри), спочатку очистіть фільтри від всіх типів сигналу, а потім встановимо тип контролю сигналу: тільки *ICMP*.

Далі вікно **Event list** (Список подій) закриваємо (рис. 2.4).

Рис. 2.4. Кнопка Event list (Список подій)



У правій частині вікна, в графічному ***меню*** вибираємо (Простий *PDU*) і клацанням миші, встановлюємо його на ПК - вибираємо джерело сигналу (наприклад, PC3) і, потім, на вузлі призначення (нехай це буде ***сервер***). Натискаючи на кнопку **Capture/Forward** (Захоплення / Уперед) спостерігаємо покрокове просування пакета *PDU* - рис. 2.5.

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

Рис. 2.5. Успішне проходження пакетів по мережі

PDU

PDU - узагальнена назва фрагмента даних на різних рівнях Моделі **OSI**: кадр Ethernet, IP-пакет, UDP-датаграмма, TCP-сегмент і т. д.

Корисні прийоми роботи в CPT

Припустимо, що вам потрібно спроектувати і налаштувати наступну ***мережу*** (рис. 2.6). Розглянемо, як можна прискорити і спростити цей процес.

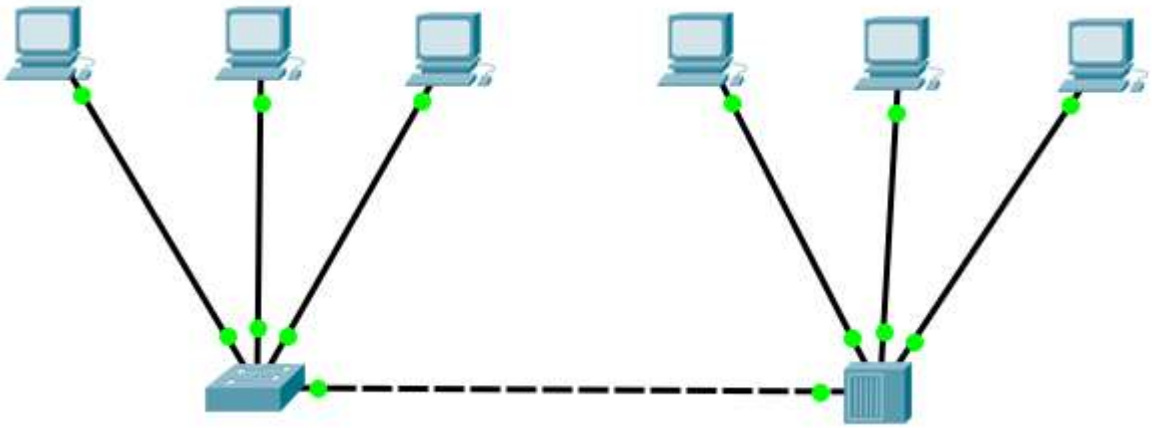


Рис. 2.6. Постановка задачі

Помістіть в робочу область перший ПК (це буде PC) і налаштуйте його (рис. 2.7).

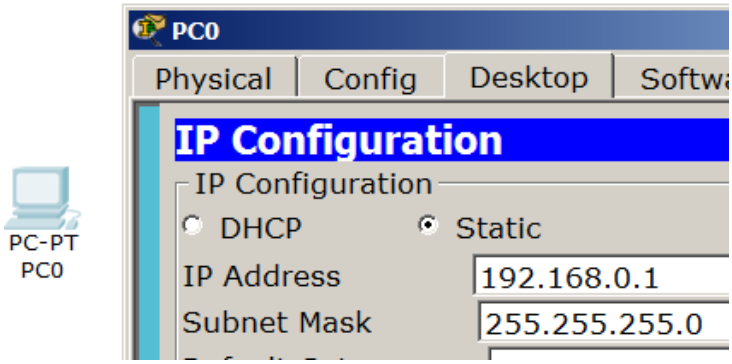


Рис. 2.7. Налаштовуємо PC0

Утримуючи клавішу **Ctrl** скопіюйте цей ПК кілька разів і налаштуйте інші адреси ПК, змінюючи тільки останню цифру IP адреси (рис. 2.8).

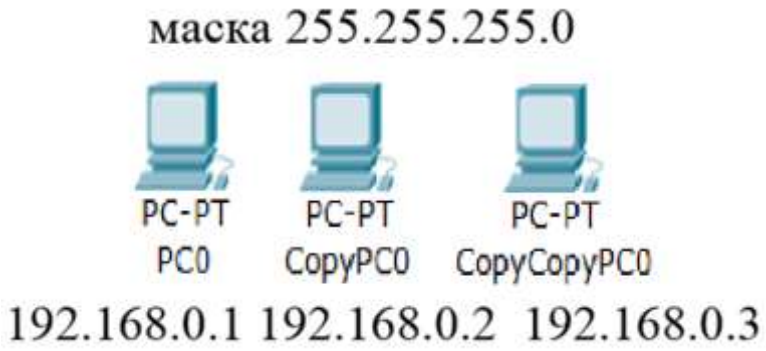


Рис. 2.8. Швидке створення і настройка трьох ПК

Далі скопіюйте, утримуючи **Ctrl** відразу три ПК і налаштуйте їх також, змінюючи тільки останню цифру IP адреси (рис. 2.9).

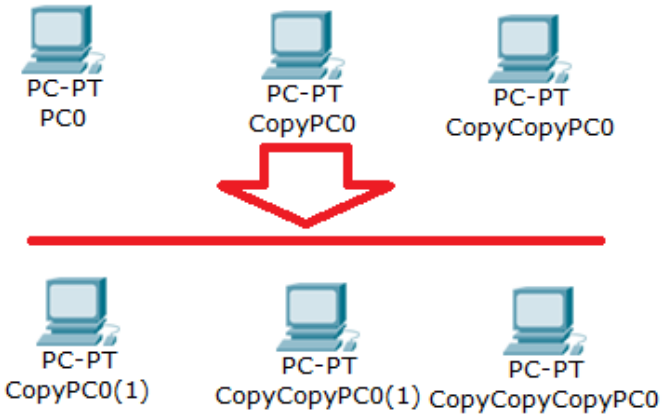


Рис. 2.9. Копіюємо все три ПК відразу

Додавання світча і ***хаба*** робимо традиційно, а підключення кабелю - автоматичне.

Hub працює на 1м рівні моделі *OSI* і відправляє інформацію в усі порти, крім порту - источніка. ***Switch*** працює на 2м рівні *OSI* і відправляє інформацію тільки в порт призначення за рахунок використання *таблиці MAC* адрес хостів. У мережах *IP* існує 3 основних способи передачі даних*:* ***Unicast, Broadcast, Multicast.***

• ***Unicast***(юнікаст) - процес відправки пакета від одного хоста до іншого хосту.

• ***Multicast***(мультикаст) - процес відправки пакета від одного хоста до деякої обмеженої групи хостів.

• ***Broadcast***(бродкаст) - процес відправки пакета від одного хоста до всіх хостам в мережі.

У деяких випадках ***switch*** *може відправляти фрейми як* ***hub****, наприклад, якщо* ***фрейм*** *бродкастовий (****broadcast*** *- широкомовлення) або* ***unknown unicast*** *(невідомому єдиному адресату).*

Завдання 2.2.Моделювання мережіз топологією зірка на базі комутатора

Роботу мережі з топологією ***зірка*** на базі концентратора вже вивчили. Тепер розглянемо аналогічну мережу на базі комутатора (рис. 2.10).

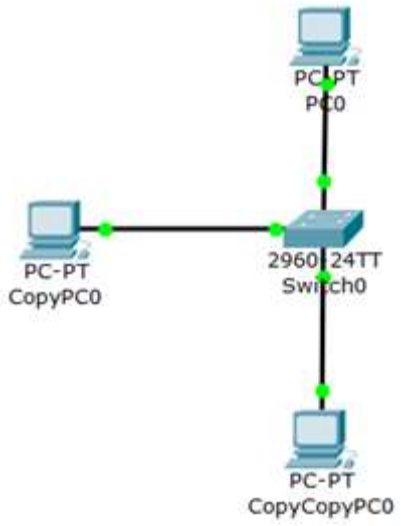


Рис. 2.10. Зірка на базі комутатора моделі 2960

На вкладці ***Physical*** ви можете подивитися вид комутатора, що має 24 порти ***Fast Ethernet*** і 2 порти ***Gigabit Ethernet*** (рис. 2.11).

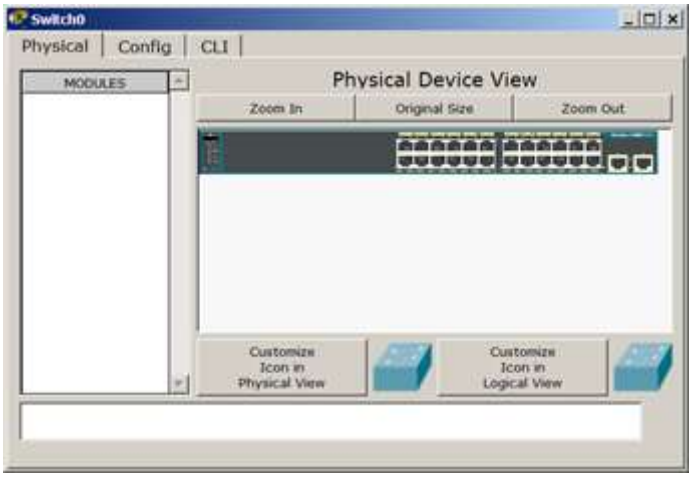


Рис. 2.11. Фізичний зовнішній вигляд комутатора моделі 2960

У режимі **Simulation** налаштуємо фільтри

і за допомогою функції переглянемо проходження пакета між двома ПК через ***комутатор***. Як бачимо, маршрути пакетав концентраторі і комутаторі будуть різними: як в прямому, так і в зворотному напрямку хаб відправляє всім, а ***комутатор*** - тільки одному.

Завдання 2.3.Проектування локальної мережі з хаба, комутатора і 4х ПК

Проведіть проектування локальної мережі з хаба, комутатора і 4х ПК. ***Мережа***, яку необхідно спроектувати представлена на рис. 2.12.

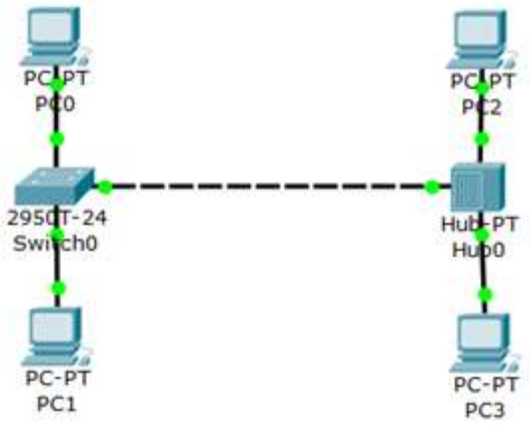


Рис. 2.12. Проектована мережа

Проведіть настройку і діагностику цієї мережі двома способами (утилітою **ping** і у вікні списку *PDU*. Переконайтеся в успішності роботи мережі в режимі симуляції.

Перед виконанням симуляції необхідно задати фільтрацію пакетів. Для цього потрібно натиснути на кнопку "Змінити фільтри", відкриється вікно, в якому потрібно залишити тільки протоколи "ICMP" і "ARP". Кнопка "Авто захоплення / Відтворення" має на увазі моделювання всього ping-процесу в єдиному процесі, тоді як "Захоплення / Вперед" дозволяє відображати його покроково.

Завдання 2.4.Дослідження якості передачі трафіку по мережі

При дослідженні пропускної здатності *ЛВС* (якості передачі трафіку по мережі) бажано збільшити розмір пакета і відправляти запити з коротким інтервалом часу, не чекаючи відповіді від віддаленого вузла, для того, щоб створити серйозну навантаження на ***мережу***. Однак, ***утиліта ping*** не дозволяє відправляти ***ехо-запит*** без отримання ехо-відповіді на попередній ***запит*** і до закінчення часу очікування. Тому для організації істотного трафіку скористаємося програмою **Traffic Generator**. Для роботи створіть і

налаштуйте наступну мережу (рис. 2.13).

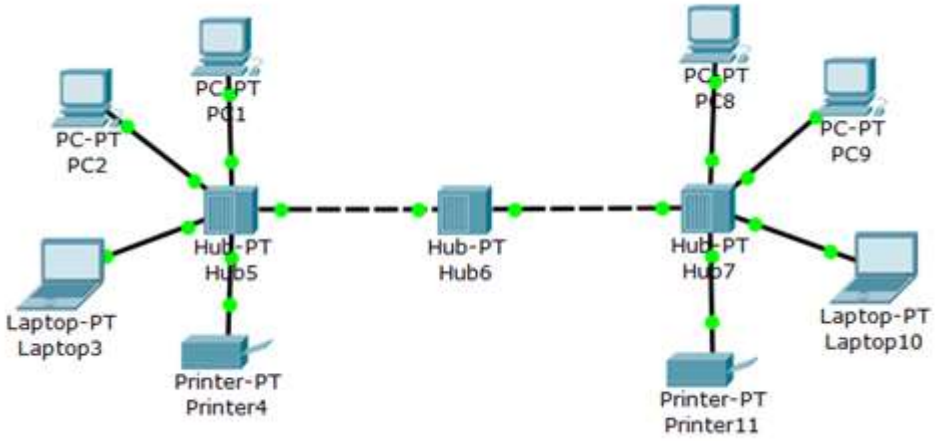


Рис. 2.13 Топология сети для нашей работы

Знайомство з Traffic Generator

У вікні управління PC1 у вкладці **Desktop** виберіть ***додаток Traffic Generator*** і визначте установки, як на рис. 2.14 для передачі трафіку від PC1 на PC8.

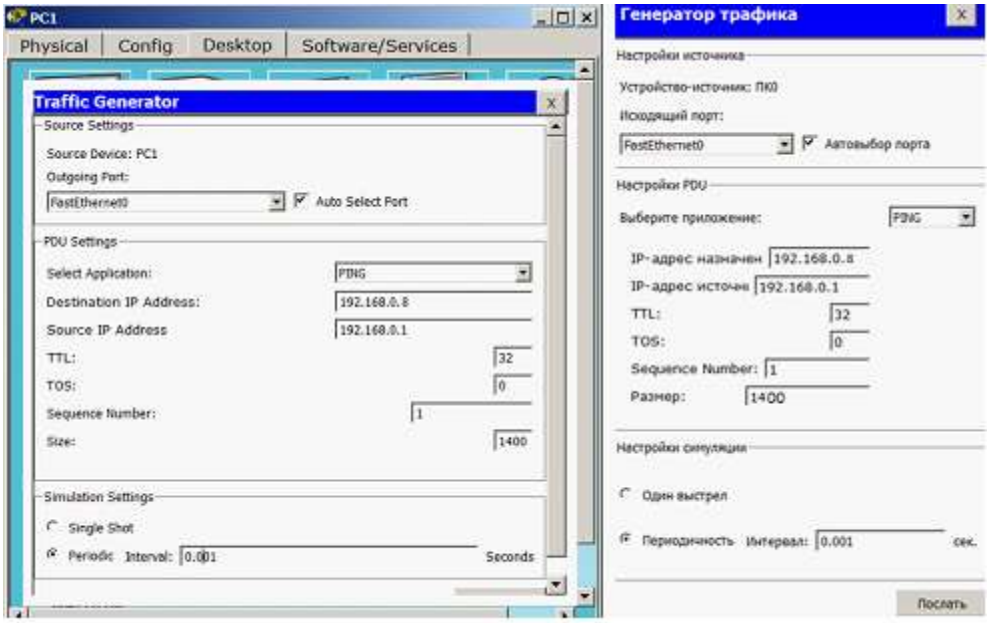


Рис. 2.14. Налаштування генератора трафіку (Варіант трафіку від PC1 до PC8)

Отже, за допомогою протоколу *ICMP*був сформований трафік між комп'ютерами PC1 з адресою 192.168.0.1 і PC8 з адресою 192.168.0.8. При цьому в розділі **Source Settings** (Настройки джерела) необхідно встановити прапорець **Auto Select Port** (Автоматичний вибір порту), а в **розділі PDU Settings** (налаштування IP-пакета) задати наступні значення параметрів цього поля:

Select application: *PING*
Destination: IPAddress: 192.168.0.8 (адресполучателя);
Source IP Address: 192.168.0.1 (адреса відправника);
TTL: 32 (час життя пакета);
TOS: 0 (тип обслуговування, "0" - звичайний, без пріоритету);
Sequence Number: 1 (початкове значення лічильника пакетів);
Size: 1400 (розмір поля даних пакета в байтах);
Simulations Settings - тут необхідно активувати перемикач;
Periodic Interval: 0.3 Seconds (період повторення пакетів).

Не обов'язково використовувати ті настройки, які поставив автор. Можете вказати свої, наприклад, Size: 1500, PeriodicInterval: 0.5 Seconds. Однак, якщо невірно вкажете IP джерела, то генератор працювати не буде.

Після натискання на кнопку **Send** (Послати) між PC1 і PC8 почнеться *активний обмін даними.* Не закривайте вікно генератора трафіку настройки, щоб не перервати ***потік*** трафіку - лампочки повинні постійно блимати!

TTL

TTL - час життя пакета. Наявність цього параметра не дозволяє пакету нескінченно ходити по мережі. TTL зменшується на одиницю на кожному вузлі (хопі), через який проходить пакет.

Дослідження якості роботи мережі

Для оцінки якості роботи мережі передамо потік пакетів між PC1 і PC8 за допомогою команди ping -n 200 192.168.0.8і будемо оцінювати якість роботи мережі по числу втрачених пакетів. ***Параметр*** "-n" дозволяє задати кількість переданих ехо-запитів (у нас їх 200) - рис. 2.15.

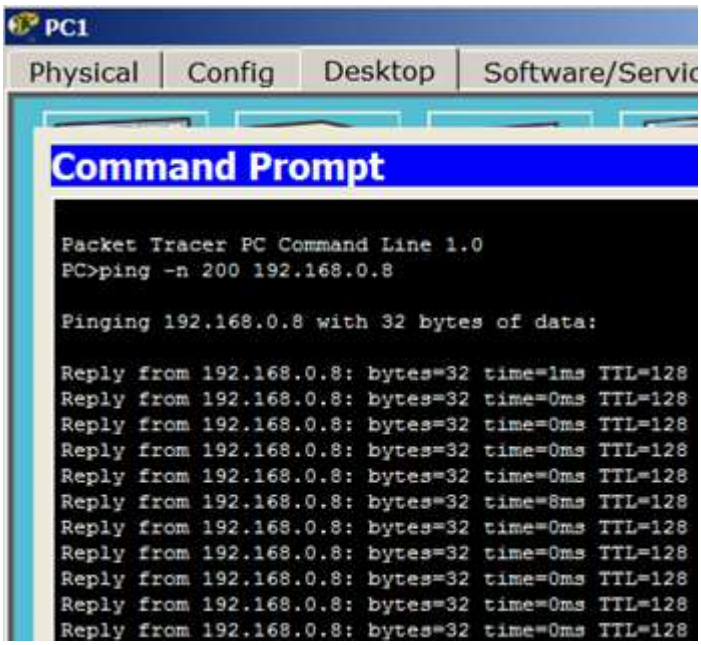


Рис. 2.15. Відправляємо 200 пакетів на PC8

Одночасно з пінгом, навантажте мережу, включивши генератор трафіку на комп'ютері PC2 (вузол призначення - PC8, розмір поля даних-2500 байт, період повторення передачі - 0,1 сек.– рис. 2.16.

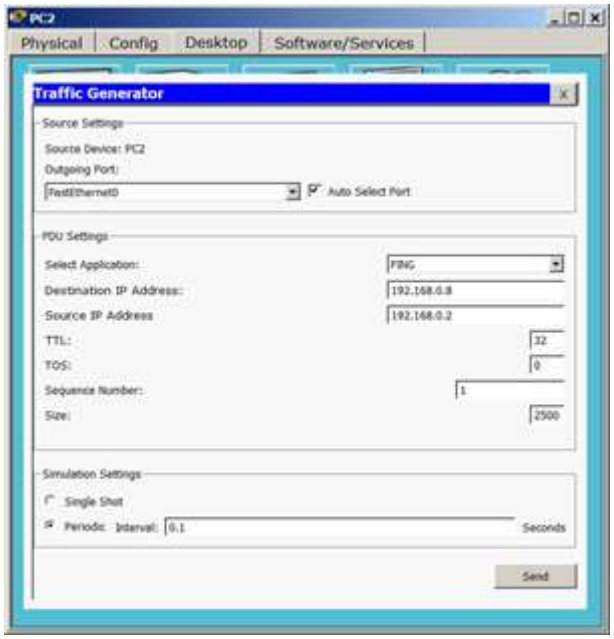


Рис. 2.16. Збільшуємо навантаження на мережу

Для оцінки якості роботи мережі - зафіксуйте число втрачених пакетів (рис. 2.17).

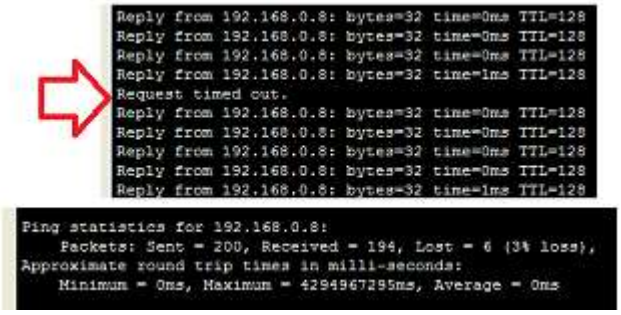


Рис. 2.17**.** Загублено 6 пакетів

Примітка

Як варіант можна було б завантажити мережу шляхом організації ще одного потоку трафіку між будь-якими вузлами мережі, наприклад, включивши генератор трафіку ще на ноутбуці PC3.

На закінчення цієї частини нашої роботи зупиніть ***Traffic Generator*** *на всіх вузлах, натиснувши кнопку* ***Stop****.*

Підвищення пропускної здатності локальної обчислювальної мережі

Перевіримо той факт, що установка комутаторів замість хабів усуває можливість виникнення колізій між пакетами користувачів мережі. Замініть центральний концентратор на ***комутатор*** (рис. 2.18). Трохи почекайте і переконайтеся, що ***мережа*** знаходиться в робочому стані - все маркери порту не червоні, а зелені.

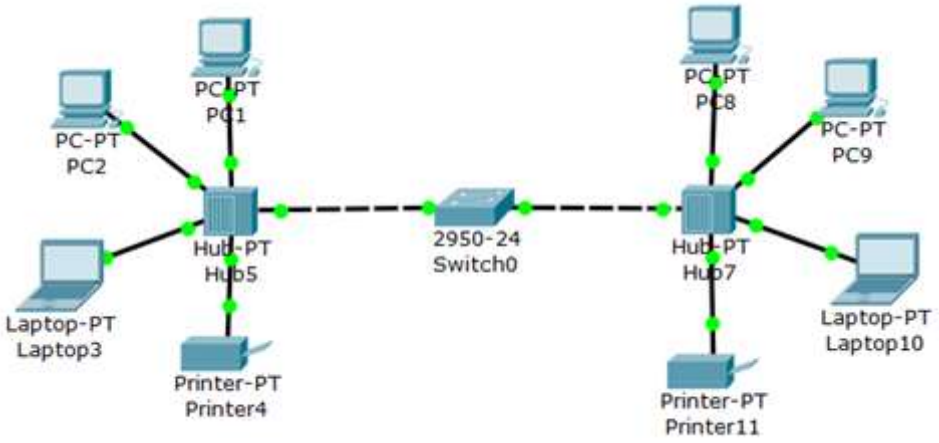


Рис. 2.18**.** Топологія мережі при заміні центрального концентратора на комутатор

Знову поставте потік пакетів між PC1 і PC8 за допомогою команди ***ping*** -n 200 192.168.0.8і включите ***Traffic Generator*** на PC2. Простежте роботу нового варіанту мережі. Переконайтеся, що за рахунок зниження паразитного трафіку якість роботи мережі стало вище (рис 2.19)

```
Ping statistics for 192.168.0.8:
    Packets: Sent = 200, Received = 199, Lost = 1 (1% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4294967295ms, Average = 0ms
```

```
Ping statistics for 192.168.0.8:
    Packets: Sent = 200, Received = 199, Lost = 1 (1% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4294967295ms, Average = 0ms
```

Рис. 2.19. Втрачено 1 пакет

Завдання 2.5. Проектування локальної мережі з заміною хабів комутаторами.

Перевірте самостійно, що заміна не одного, а всіх хабів комутаторами істотно поліпшить якість передачі трафіку в мережі.

Склад звіту лабораторної роботи

В звіті повинно бути відображено:

1. Тема роботи.
2. Мета роботи.
3. Виконання завдання 2.1 з відповідними скріншотами.
4. Виконання завдання 2.2 та 2.3 з відповідними скріншотами.
5. Виконання завдання 2.4 з відповідними скріншотами.
6. Виконання завдання 2.5 з відповідними скріншотами.
7. Висновки

Контрольні питання

1. Наведіть різновиди топологій комп'ютерних мереж.
2. Що собою представляє зіркова топологія.
3. Переваги зіркової топології.
4. Недоліки зіркової топології.
5. Дайте визначення такому пристрою для організації мережевих технологій, як комутатор (світч).
6. Дайте визначення такому пристрою для організації мережевих технологій, як маршрутизатор (роутер).
7. Дайте визначення такому пристрою для організації мережевих технологій, якконцентратор (хаб)

8. Дайте визначення таким пристроямдля організації мережевих технологій, якшлюзи.
9. Дайте визначення таким пристроямдля організації мережевих технологій, якповторювачі (репітери).
10. Дайте визначення таким пристроямдля організації мережевих технологій, якмости.

Лабораторна робота№ 3

Тема: ОСНОВИ РОБОТИ З МЕРЕЖНОЮ ОПЕРАЦІЙНОЮ СИСТЕМОЮ CISCO IOS. КОМАНДНИЙ РЯДОК УПРАВЛІННЯ ПРИСТРОЯМИ CLI.

Мета заняття: дослідити можливості Cisco IOS з налагодження та діагностування основних параметрів функціонування керованих комутаторів Cisco,вивчити командний рядок управління пристроями через пряме кабельне (консольне) підключення,застосувати отримані знання при виконанні практичних завдань.

Теоретичні відомості

Мережна операційна система Cisco IOS

Для забезпечення функціонування мережних пристроїв фірмою Cisco розробляються як різні варіанти FirmWare, так і спеціалізовані мережні ОС. Використання Cisco FirmWare характерне для більшості моделей точок доступу та безпровідних маршрутизаторів, деяких моделей комутаторів. Більшість моделей комутаторів та маршрутизаторів Cisco використовують спеціалізовані мережні ОС.

Основними мережними ОС Cisco є:

– Cisco IOS (Cisco Internetwork OperatingSystem);

– Cisco NX-OS (NexusOS);

– Cisco IOSXR;

– Cisco IOSXE.

У сучасних комутаторах та маршрутизаторах Cisco найчастіше використовується спеціалізована мережна ОС Cisco IOS. У старих моделях

комутаторів використовувалася CatOS (Catalyst Operating System), але її рекомендується замінювати на більш сучасну IOS. Для спеціалізованих комутаторів серій Nexus (технології Ethernet) та MDS (технології Fibre Channel), які використовуються в центрах обробки та збереження даних, Cisco розроблено мережну ОС Cisco NX-OS. Для сучасних високопродуктивних маршрутизаторів розроблено ОС, відому як Cisco IOS XR. Також розроблена і широко впроваджується для використання в комутаторах, маршрутизаторах та інших пристроях ОС наступного покоління Cisco IOSXE.

Cisco IOS є багатозадачною ОС, яка виконує функції мережної організації, комутації, маршрутизації та передачі даних. Ядро цієї ОС є монолітним, це означає, що всі елементи системи розміщені в одному образі і всі процеси запускаються в одному адресному просторі. У Cisco IOS немає міжпроцесного захисту пам'яті, це означає, що крах одного процесу може викликати крах або перезавантаження всієї системи.

Cisco IOS поставляється у вигляді монолітного образу, який орієнтований на конкретну модель пристрою. Образи можуть мати певні набори властивостей та версії. Конкретний образ IOS ідентифікується трьома параметрами:

- апаратна платформа (серія) пристрою, для якої вінпризначений;
- набір можливостей (Feature Set, Packages),
- версіяОС.

Команди базового налагодження керованого комутатора Cisco

Конфігурування керованого комутатора Cisco передбачає налагодження: параметрів іменування, системного годинника, параметрів консольного підключення, параметрів термінального вікна, часових періодів (тайм-аутів) сеансу, системних повідомлень, безпечного доступу до пристрою, параметрів IP-адресації та багато ін.

Іменування пристроїв у Cisco IOS використовується:

- для ідентифікації пристрою під час підключення (як за консольного підключення, так і в разі мережних термінальних підключень за допомогою протоколів віддаленого доступу Telnet чи SSH);

- під час розсилки інформації про пристрій іншим пристроям (наприклад, за допомогою протоколів виявлення пристроїв LLDP чи CDP);

- для генерації ключів у разі використання криптографічних засобів (наприклад, у протоколі SSH).

Для зміни імені пристрою призначена команда **hostname**. Повернення імені пристрою за замовчуванням – **no hostname**. За замовчуванням заводське ім'я комутатора **Switch**.

Операційна система Cisco IOS на пристроях Cisco забезпечує функціонування системного (програмного) годинника/календаря. У деяких моделях пристроїв також наявний і апаратний годинник/календар. Відповідно існують механізми обміну даними між ними. Параметри системних часу (та дати) пристрою можуть встановлюватися як за допомогою команд локального застосування, так і з використанням мережного джерела часу. У першому випадку за умови відсутності апаратного годинника параметри системного часу не зберігаються у конфігураційному файлі і є актуальними лише на період роботи пристрою. Після перезавантаження їх необхідно встановлювати заново. У другому випадку системний час після завантаження пристрою синхронізуються з часом сервера часу за протоколом NTP. Надалі операція синхронізації виконується періодично. Звичайно, що це потребує певних специфічнихналагоджень.

Встановлення системного часу здійснюється за допомогою команди **clock set**, встановлення часового поясу – за допомогою команди **clock timezone**. Для активації переходу на літній час застосовується команда **clock summertime**. Для виведення параметрів часу та дати апаратного годинника пристрою у ручному

режимі застосовується команда **clock read-calendar**. Для налагодження використання апаратного годинника пристрою як авторитетного джерела мережного часу застосо вується команда **clock calendar-valid**. Для одноразової ручної синхронізації параметрів часу апаратного годинника з параметрами часу програмного годинника пристрою застосовується команда **clock update-calendar**. Синтаксис розглянутих команд наведено нижче.

Синтаксис команди **hostname** (режим глобального конфігурування):

hostname *device-name*,

де ***device-name*** – текстове ім'я пристрою; теоретично може містити до 63 символів (літер, цифр, спец. символів), рекомендується задавати ім'я довжиною до 10 символів, оскільки в більшості систем існує обмеження на довжину службової частини командного рядка.

Синтаксис команди **clock set** (привілейований режим):

clock set *hh*:*mm*:*ss dd month yyyy*,

де ***hh*:*mm*:*ss*** – години (у 24-годинному форматі), хвилини, секунди;

dd – день, значення у діапазоні від 1 до 31;

month – місяць, назва місяця англійською мовою;

yyyy – рік, чотирицифрове значення в діапазоні від 1993 до 2035.

Синтаксис команди **clock timezone** (режим глобального конфігурування):

clock timezone *time-zone hh*[*mm*],

де ***time-zone*** – часовий пояс (текстове значення вигляду WET – Western European Time, CET –Central European Time, EET – Eastern European Time, EEST – Eastern European Summer Time і т.д.), за замовчуванням установлено універсальний глобальний час (UTC, Coordinated Universal Time);

hh – години, зсув від UTC, ціле число в діапазоні від – 23 до 23; ***mm*** – хвилини, зсув від UTC, ціле число в діапазоні від – 59 до 59.

Синтаксис команди **clock summertime** (режим глобального конфігурування):

clock summertime *time-zone* date [***b_day, b_month, b_year, b_hh:mm***

e_day, e_month, e_year, e_hh:mm [***shift***]

clock summertime ***time-zone*** **reccuring** [***b_week, b_day, b_month, b_hh:mm e_week, e_day, e_month, e_hh:mm***] [***shift***],

де ***time-zone*** – часовий пояс;

date – службова конструкція, за допомогою якої зазначається початкова і кінцева дати літнього часу;

reccuring – службова конструкція, яка зазначає, що перехід на літній час повинен здійснюватися щороку;

b_day, e_day – день початку і закінчення дії літнього часу, решта параметрів трактуються подібним чином;

shift – кількість хвилин, які необхідно додати у момент переходу на літній час, за замовчуванням – 60 хв.

Основні команди налагодження консольного підключення до пристроїв Cisco

Для консольного підключення (а також і для підключень по інших термінальних лініях) використовуються спеціальні програми-емулятори терміналу, які мають можливість працювати з послідовними портами комп’ютера. Це можуть бути як вбудовані в систему програмні продукти, так і розробки сторонніх виробників. Як приклади можна навести вбудовану в ОС Windows програму HyperTerminal та широковживані відкриті кросплатформені розробки PuTTY, SecureCRT.

Для термінальної програми, за допомогою якої здійснюється консольне підключення до пристрою (комутатора чи маршрутизатора), можна налагодити такі параметри взаємодії, як:

– швидкість (приймання і передавання даних для лінії, біт/с);

– біти даних (кількість бітів даних на символ, яку розуміє і генерує

апаратне забезпечення);

– парність (біт парності для асинхронної послідовної лінії зв'язку, фактично це сума бітів даних, яка показує, що дані містять або не містять парну чи непарну кількість одиничних бітів);

– стопові біти (стопові розряди, які передаються для кожного байта);

– керування потоком (керування потоком даних між пристроями, які підключені через послідовну лінію зв'язку).

Вибір лінії консольного підключення для налагодження здійснюється командою **line console 0** (режим глобального конфігурування). Для налагодження параметрів лінії на стороні комутатора (чи іншого пристрою Cisco) використовуються команди **speed, databits, parity, stopbits, flowcontrol** відповідно. Повернення до стандартних значень параметрів здійснюється з використанням службового слова **no** з відповідною командою (наприклад, **no speed).** Також можна використати команду **default** (наприклад, **default speed).** Синтаксис указаних команд наведено нижче.

Синтаксис команди **speed** (режим конфігурування лінії):

speed *value*,

де ***value*** – значення швидкості у біт/с, число з діапазону 0…4294967295. Як правило, задається з набору стандартних значень 110, 300, 1200, 2400, 4800, 9600, 19200 і т.д. Верхня межа за лежить від мікросхеми UART, на якій реалізовано послідовний порт консолі. За замовчуванням встановлюється швидкість 9600 біт/с.

Синтаксис команди **databits** (режим конфігурування лінії):

databits *value*,

де ***value*** – кількість бітів даних на символ, набуває значень 5, 6, 7.

За замовчуванням становить 8бітів.

Синтаксис команди **parity** (режим конфігурування лінії):

parity *value*,

де ***value*** – параметр, який може набувати значень **even**, **mark**, **none**, **odd**,

space; за замовчуванням значення не визначене;

none – біт парності відсутній і не передається;

even – біт парності дорівнює 0, якщо у переданому символі парна кількість одиничних бітів;

mark – біт парності завжди дорівнює 1;

odd – біт парності дорівнює 0, якщо у переданому символі непарна кількість одиничних бітів;

space – біт парності завжди дорівнює 0;

Синтаксис команди **stopbits** (режим конфігурування лінії):

stopbits *value*,

де ***value*** – параметр, який може набувати значень 1; 1.5; 2. За замовчуванням – 2.

Синтаксис команди **flowcontrol** (режим конфігурування лінії):

flowcontrol *value* [lock] [in | out],

де ***value*** – параметр, який може набувати значень **none**, **hardware**, **software**, за замовчуванням керування потоком даних відсутнє;

none – параметр вимикання режиму керування потоком даних;

hardware – параметр вмикання режиму апаратного керування потокомданих;

software – параметр вмикання режиму програмного керування потокомданих;

lock – службова конструкція, яка забороняє вимикання режиму керування потоком даних, застосовується лише для параметра **software**;

in–параметр,якийвказуєнавстановленняконтролюпотокунавхідлінії;

out – параметр, який вказує на встановлення контролю потоку на вихід лінії;

Якщо не вказаний жоден із параметрів **in** або **out**, то вважається, що контроль потоку здійснюється в обох напрямках.

Синтаксис команди **default** (режим конфігурування лінії):

default *value*,

де ***value*** – параметр, який може набувати значень **speed, databits, parity, stopbits, flowcontrol, history size**

Для інших ліній можуть здійснюватися налагодження, подібні до тих, що здійснюються для консольноїлінії.

Для зручності відображення інформації під час налагодження пристрою доцільно встановити параметри термінального вікна, в якому вводяться команди та виводяться їх результати. Правильний підбір параметрів допомагає розв'язати проблему занадто довгих рядків або їх великої кількості. Для налагодження ширини та висоти використовуються команди **width** та **length**. Повернення до стандартних розмірів здійснюється командами **no width** та **no length** відповідно.

Синтаксис команди **width** (режим конфігурування лінії):

width ***columns***,

де ***columns*** – кількість стовпчиків вікна термінальної програми, за замовчуванням – 80.

Синтаксис команди **length** (режим конфігурування лінії):

length ***lines***,

де ***lines*** – кількість рядків термінальної програми (може змінюватися в діапазоні від 0 до 512), за замовчуванням – 24.

Консоль

Більшість мережевих пристроїв компанії CISCO допускають ***конфігурацію***. Для цього ***адміністратор*** мережі повинен підключитися до пристрою через пряме кабельне (консольне) підключення (рис. 3.1).

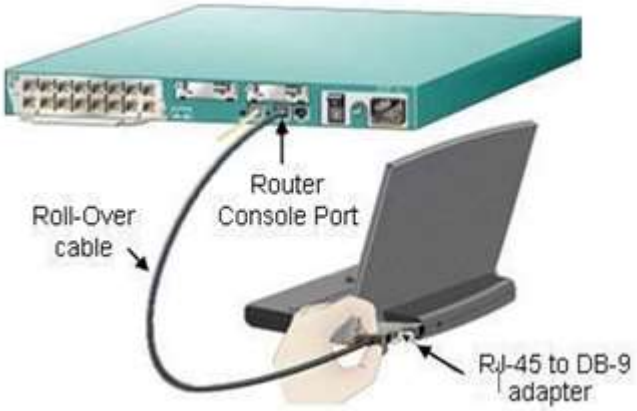


Рис. 3.1. Консольне підключення до мережевого пристрою

Отже, ***програмування*** пристроїв CISCO найчастіше роблять через консольний ***порт*** RJ-45. На рис. 3.2 і рис. 3.3 наведені фотографії консольних роз'ємів на маршрутизаторі і 2 варіанти консольного кабелю.

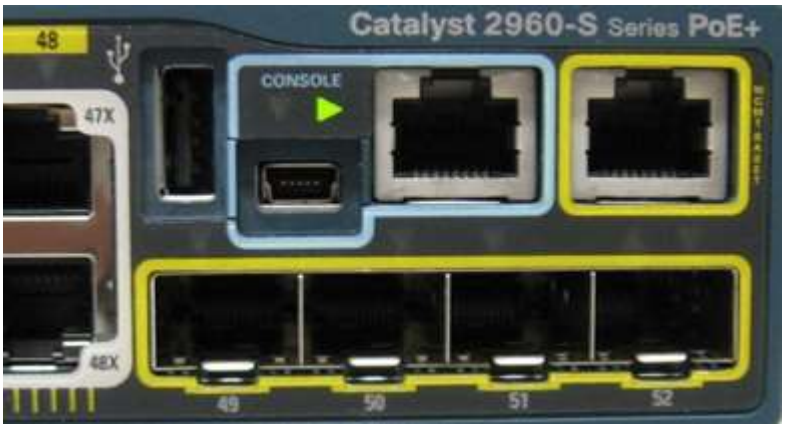


Рис. 3.2. Синім кольором показані роз'єми під керуючий (консольний) кабель

Рис. 3.3. Варіанти консольних кабелів

Примітка
Класичний консольний кабель має роз'єм DB9 для підключення до COM-порту комп'ютера і роз'єм RG-45 для підключення до консольного порту маршрутизатора. Зараз Cisco активно просуває нові маршрутизатори серій 28xx, 38xx і т.д. У них передбачена можливість конфігурації через USB-інтерфейс (використовуються звичайні USB-кабелі).

Підключивши **консоль** і отримавши **доступ** до пристрою через командний рядок, користувач (**адміністратор** мережі або мережевий інженер) може задавати різні команди і, тим самим, визначати параметри **конфігурації**обладнання.

Режими роботи з пристроєм при використанні CLI

Командний рядок являє собою місце, куди користувач вводить символи, що формують управлінський вплив. Робота з командним рядком здійснюється в декількох режимах (таблиця 3.1).

Таблиця 3.1. Режими командного інтерфейса

Режим	**Перехід в режим**	**Вид командного рядка**	**Вихід з режиму**
Користувацький	Підключення	Router>	logout
Привілейований	Enable.	Router#	disable
Глобальна конфігурація	Configure terminal	Router(config)#	exit,end или Ctrl-Z
Налаштування інтерфейсів	Interface	Router(config-if)	exit

Вид командного рядка:

Router> Запрошення, яке характеризує призначений для користувача режим, в якому можна переглядати деяку статистику і проводити найпростіші операції на кшталт пінга. Це режим для мережевого оператора,

інженера першої лінії техпідтримки, щоб він нічого не пошкодив і зайвого не дізнався. Іншими словами, команди в цьому режимі дозволяють виводити на екран інформацію без зміни установок мережевого пристрою.

Router# Запрошення в привілейованому режимі. Привілейований режим підтримує команди настройки і тестування, детальну перевірку мережевого пристрою, маніпуляцію з файлами і доступ в режим конфігурації. Потрапити в нього можна, ввівши команду enable.

Router(config)#Запрошення в режимі глобальної конфігурації. Він дозволяє нам вносити зміни в налаштування пристрою. Команди режиму глобального конфігурування визначають поведінку системи в цілому. Активується командою #configure terminal з привілейованого режиму.

Завдання на лабораторну роботу

Завдання 3.1.Знайомство з командами Cisco IOS.

Завдання 3.2. Парольний доступ до привілейованого режиму на комутаторах.

Завдання3.1.Знайомство з командами Cisco IOS

В ***CiscoPacket Tracer*** інтерфейс командного рядка для пристроїв доступний у вікні налаштувань параметрів мережевого пристрою на вкладці "***CLI***". Це вікно імітує пряме кабельне (консольне) підключення до мережних пристроїв. Робота з командним рядком (***CLI***) для настройки (програмування) мережевого проводиться за допомогою команд операційної системи Cisco IOS (рис. 3.4).

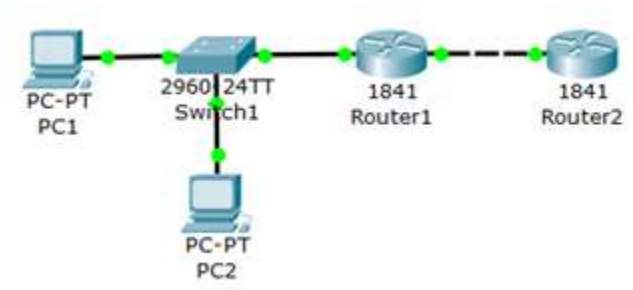


Рис. 3.4. Мережа для виконання команд ОС CiscoIOS

Вище ми говорили про режими командного інтерфейсу - *призначеному для користувача, привілейованому і глобальної конфігурації.* Виконайте усі команди входу і виходу в ці режими для Router1. При вході в мережевий пристрій Router1 і натисканні на клавішу ***Enter*** *командний рядок* має вигляд як на рис. 3.5. Вихід з призначеного для користувача режиму - ***logout.***

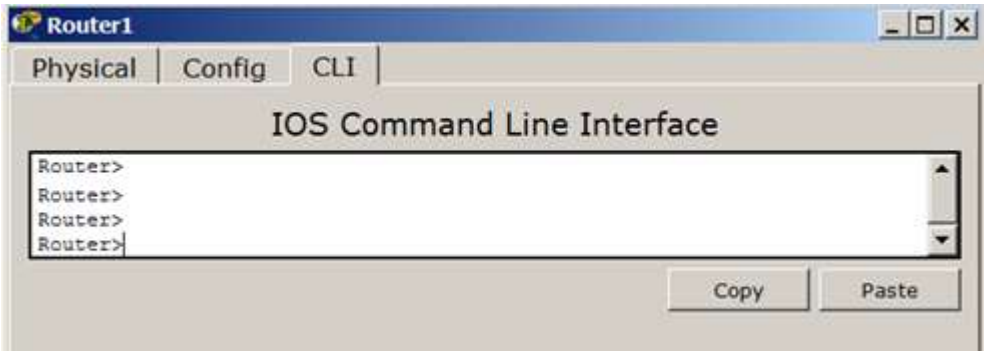


Рис. 3.5. Вид командного рядка в користувацькому режимі

Щоб отримати доступ до повного набору команд, необхідно спочатку активізувати привілейований режим командою ***enable***. Про перехід в привілейований режим буде свідчити поява в командному рядку запрошення у вигляді знака #. Вихід з привілейованого режиму проводиться командою ***disable***.

Примітка

Замість ***enable*** *можна було набрати* ***en.*** *Команди в будь-якому режимі IOS розпізнає по першим унікальним символам.Режим глобального*

конфігурування - реалізує потужні однорядкові команди, які вирішують завдання конфігурації. Для входу в режим глобального конфігурування використовується ***команда*** *привілейованого режиму* ***configure terminal****. Вихід командою* ***exit*** *або* ***end****.*

Встановлення пароля на вхід в привілейований режим

Пароль доступу дозволяє вам контролювати ***доступ*** в привілейований режим від недосвідчених користувачів і зловмисників. Нагадаємо, що тільки в привілейованому режимі можна вносити конфігураційні зміни. На Router1 встановіть ***пароль*** доступу в цей режим як "parol" командою **Router1 (config) #enable password parol**, потім вийдіть з привілейованого режиму мережевого пристрою, тобто перейдіть в призначений для користувача режим. Спробуйте знову зайти в привілейований режим. Як бачите, без введення пароля це тепер неможливо (рис. 3.6).

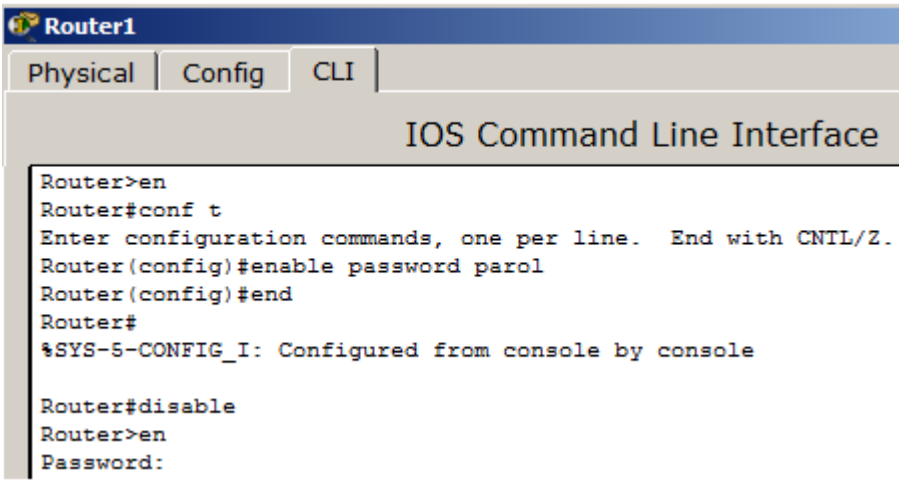


Рис. 3.6. Встановленняпароля на вхід в привілейований режим

Для зміни пароля введемо новий ***пароль*** привілейованого режиму (рис. 3.7).

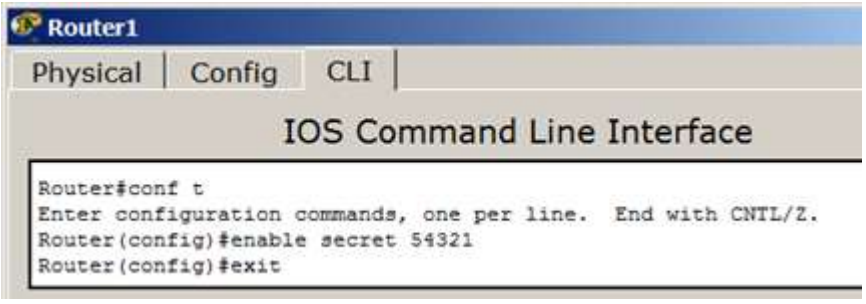


Рис. 3.7**.** Був пароль 12345, став пароль 54321

Для скидання пароля можна зробити перезавантаження роутера (рис. 3.8).

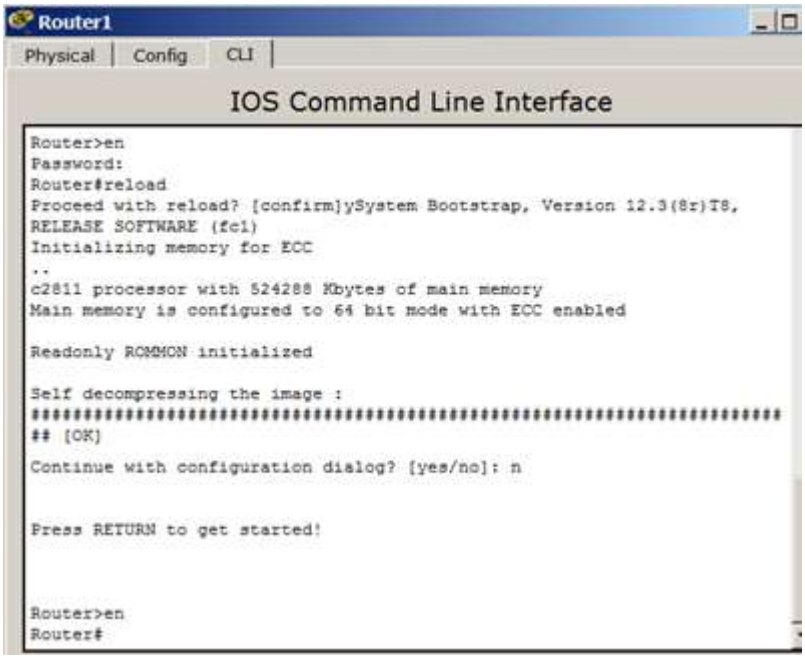


Рис. 3.8. Перезавантаження R1 командою reload

Поради при роботі з CLI

Всі 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 (?), 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, введеним раніше. Натисніть на Стрілку вгору або **Ctrl + P** (рис. 3.9).

Рис. 3.9. Стрілки Вгору або Вниз на клавіатурі дозволяють перегортати команди, які раніше використовувалася вами

Активна ***конфігурація*** автоматично не зберігається і буде втрачена в разі збою електроживлення. Щоб зберегти настройки роутера використовуйте команду **write memory** (рис. 3.10).

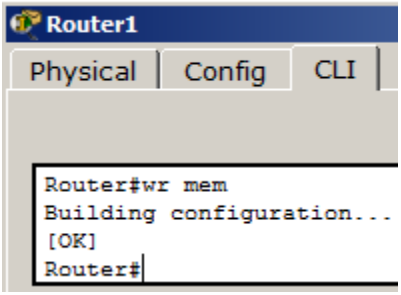


Рис. 3.10. Збереження поточної конфігурації R1

Завдання 3.2. Парольний доступ до привілейованого режиму на комутаторах

Схема мережі показана на рис. 3.11.

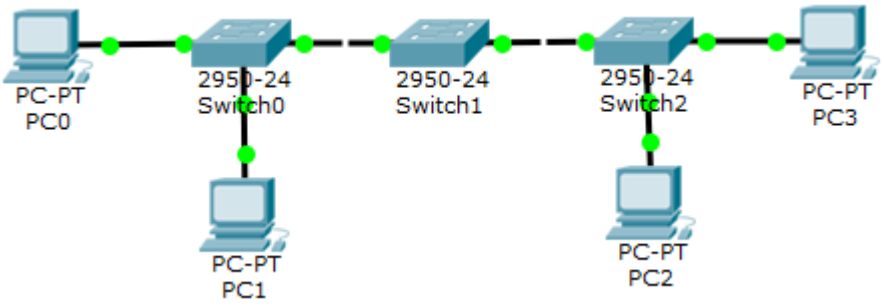


Рис. 3.11. Схема мережі

Потрібно:

1. Побудувати мережу, вказану на рис. 3.11;

2. Змінити ім'я комутаторів Cisco;

3.Забезпечити парольний доступ до привілейованого режиму на комутаторах;

4. Задати ip-адреси і маски комутаторів (172.16.1.11/24, 172.16.1.12/24, 172.16.1.13/24);

5. Задати ip-адреси і маски мереж персональних комп'ютерів. (172.16.1.1/24, 172.16.1.2/24, 172.16.1.3/24, 172.16.1.4/24);

6. Переконатися в досяжності всіх об'єктів мережі по протоколу IP;

7. Переключившись в "Режим симуляції" і розглянути і пояснити процес обміну даними по протоколу ICMP між пристроями (виконавши команду Ping з одного комп'ютера на інший).

Склад звіту лабораторна робота

В звіті повинно бути відображено:

1. Тема роботи.
2. Мета роботи.
3. Виконання завдання 3.1 з відповідними скріншотами.
4. Виконання завдання 3.2 з відповідними скріншотами.
5. Висновки

Контрольні питання

1. Загальна характеристика Cisco IOS. Платформи, набори можливостей та версії Cisco IOS, які використовуються для комутаторівCisco.
2. Командні режими Cisco IOS для комутаторів Cisco. Команди переходів між командними режимами Cisco IOS длякомутаторів.
3. Особливості отримання довідкової інформації у командному рядку CiscoIOS.
4. Наведіть перелік та поясніть призначення основних команд налагодження системного часу в комутаторахCisco.
5. Наведіть перелік та поясніть призначення команд іменування пристроїв та створення системних повідомлень для пристроївCisco.
6. Наведіть перелік та поясніть призначення основних команд налагодження консольного підключення для пристроївCisco.
7. Наведіть перелік та поясніть призначення основних команд налагодження часових тайм-аутів та команд термінального виведення для пристроївCisco.
8. Режими роботи з пристроєм при використанні CLI.
9. Парольний доступ до пристроївCisco.

Лабораторна робота№ 4

Тема: ПОБУДОВА ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ (VLAN)

Мета заняття:навчитися будувати віртуальні локальні мережі,застосувати отримані знання при виконанні практичних завдань.

Теоретичні відомості

Віртуальні локальні мережі

Віртуальною локальною мережею (VLAN)називається логічна *група* вузлів мережі, трафік якої, в тому числі і широкомовний, на канальному рівні повністю ізольований від інших вузлів мережі. Це означає, що передача кадрів між різними віртуальними мережами на підставі MAC-адреси неможлива незалежно від типу адреси - унікального, групового або широкомовного. У той же час всередині віртуальної мережі кадри передаються по технології комутації, тобто лише на той *порт*, який пов'язаний з адресою призначення кадру. Таким чином за допомогою віртуальних мереж вирішується проблема поширення широкомовних кадрів і спричинених ними наслідків, які можуть розвинутися в широкомовні шторми і істотно знизити *продуктивність* мережі.

VLAN мають такі переваги:

- Гнучкість впровадження.*VLAN*є ефективним способом угруповання мережевих користувачів в віртуальні робочі групи, незважаючи на їх фізичне розміщення в мережі;

-*VLAN* забезпечують можливість контролю широкомовних повідомлень, що збільшує смугу пропускання, доступну для користувача;

-*VLAN* дозволяють підвищити безпеку мережі, визначивши за допомогою фільтрів, налаштованих на комутаторі або маршрутизаторі, політику взаємодії користувачів з різних віртуальних мереж.

При використанні*віртуальних локальних мереж*вже не потрібно підключати користувачів одного відділу до окремого комутатора, що дозволяє скоротити кількість використовуваних пристроїв і*магістраль*них кабелів, *комутатор, програмне забезпечення* якого підтримує функцію *віртуальних локальних мереж,* дозволяє виконувати логічну сегментацію мережі шляхом відповідної програмної настройки. Це дає можливість підключати користувачів, що знаходяться в різних сегментах, до одного комутатора, а також скорочує кількість необхідних фізичних інтерфейсів на маршрутизаторі.

Типи VLAN

У комутаторах можуть бути реалізовані наступні типи*VLAN*:

- На основі портів;
- На основі стандарту*IEEE 802.1Q*;
- На основі стандарту IEEE 802.1ad (Q-in-Q *VLAN*);
- На основі портів і протоколів IEEE 802.1v;
- На основі MAC-адрес;
- Асиметричні.

також для *сегментування* мережі на канальному рівні моделі *OSI* в комутаторах можуть використовуватися інші функції, наприклад *функція Traffic Segmentation*.

При правильному налаштуванні віртуальні локальні мережі покращують продуктивність зайнятих мереж. VLAN групи групують клієнтські пристрої, які часто спілкуються між собою. Трафік між пристроями, розділеними на дві або більше фізичних мереж, зазвичай обробляють основні маршрутизатори мережі. За допомогою VLAN цей трафік обробляється більш ефективно

мережевими комутаторами.

VLAN також приносять переваги безпеці у великих мережах, дозволяючи краще контролювати, які пристрої мають локальний доступ один до одного. Гостьові мережі Wi-Fi часто реалізуються за допомогою бездротових точок доступу, що підтримують VLAN.

Статичні та динамічні VLAN

Мережеві адміністратори часто посилаються на статичні VLAN як VLAN на портах. У статичній VLAN адміністратор призначає окремі порти мережі перемикатися у віртуальну мережу. Незалежно від того, який пристрій підключається до цього порту, він стає членом цієї попередньо призначеної віртуальної мережі.

У динамічній конфігурації VLAN адміністратор визначає приналежність до мережі відповідно до характеристик пристроїв, а не розташування порту комутатора. Наприклад, динамічну VLAN можна визначити зі списком фізичних адрес (MAC-адреси) або іменами мережевих облікових записів.

Стандарти VLAN та стандартні VLAN

Стандарти VLAN для мереж Ethernet відповідають галузевому стандарту IEEE 802.1Q. Стандарт 802.1Q складається з 32 бітів (4 байти) даних, вставлених у заголовок кадру Ethernet. Перші 16 біт цього поля містять жорстко закодований номер 0x8100, який запускає пристрої Ethernet розпізнавати кадр як належний 802.1Q VLAN. Останні 12 біт цього поля містять номер VLAN, число від 1 до 4094.

Найкращі практики адміністрування VLAN визначають кілька стандартних типів віртуальних мереж:

- **Рідна локальна мережа**: пристрої Ethernet VLAN розглядають всі нетегіровані кадри як належність до рідної локальної мережі за

замовчуванням. Власною локальною мережею є VLAN 1, хоча адміністратори можуть змінити цей номер за замовчуванням.

- **Управління VLAN**: Підтримує віддалені з'єднання від мережевих адміністраторів. Деякі мережі використовують VLAN 1 як VLAN управління, а інші встановлюють для цього спеціальний номер (щоб уникнути конфлікту з іншим мережевим трафіком).

Завдання на лабораторну роботу

Завдання 4.1.Налаштування VLAN з одним комутатором.

Завдання 4.2.Налаштування віртуальної мережі на комутаторі 2960.

Завдання4.3.VLAN з двома комутаторами. Розділяється загальний канал (транк).

Завдання 4.4.Налаштування віртуальної мережі з двох світчей і чотирьох ПК.

Віртуальні локальні мережі VLAN

VLAN* (*Virtul Local Area Network*)** — віртуальна локальна ***комп'ютерна мережа з групи хостів із загальним набором вимог. *VLAN* дозволяють хостам групуватися або дистанціюватися між собою. Пристрої, в межах однієї *VLAN* можуть спілкуватися, а вузли, що знаходяться в різних *VLAN'ax*, невидимі один для одного.

Завдання 4.1. НалаштуванняVLAN з одним комутатором

Для малювання ПК вибираємо в кінцевих пристрої настільний комп'ютер і, утримуючи **Ctrl**, (так швидше) натисніть 1 раз на ПК а потім малюйте потрібну кількість ПК, клацаючи мишкою (рис. 4.1). Цим прийомом ви зможете за один раз намалювати відразу 4 ПК.

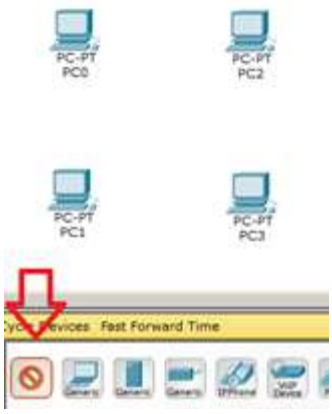


Рис. 4.1. Вибір пристрою, утримуючи Ctrl

Встановлюємо комутатор і, утримуючи **Ctrl**, створюємо підключення прямим кабелем, вибираючи порти комутатора. Після ініціалізації портів всі лампи загоряться зеленим. На схему буде дві підмережі (рис. 4.2).

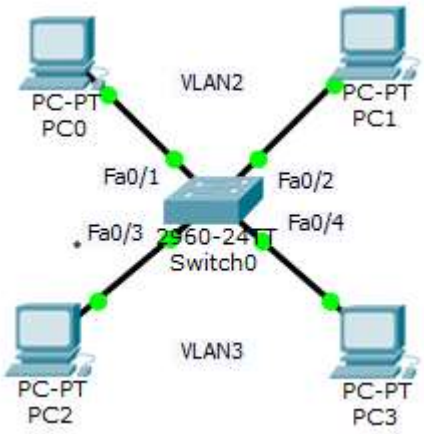


Рис. 4.2. Дві підмережі: VLAN2 і VLAN3

Примітка

Ім'я VLAN1 використовується за умовчанням, його краще в нашому прикладі не використовувати.

На комутаторі набираємо команду ***en*** і входимо в привілейований режим. Потім набираємо команду ***conf t*** для входу в режим глобального конфігурування. Якщо підвести курсор миші до портів комутатора, то ви побачите які порти в якому сегменті задіяні. Для VLAN3 - це ***Fa0 / 3*** і ***Fa0 / 4***

(припустимо, що це буде бухгалтерія - ***buh***) і для VLAN2 - це **Fa0 / 1** і **Fa0 / 2** (припустимо, що це буде склад - ***sklad***). Спочатку будемо конфігурувати другий сегмент мережі VLAN2 (sklad) - рис. 4.3.

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name sklad
```

Рис. 4.3.VLAN2 отримує ім'я sklad

У віртуальній мережі VLAN2 налаштовуємо порти комутатора Fa0 / 1 і Fa0 / 2 як ***access*** порти, тобто порти для підключення користувачів (рис. 4.4).

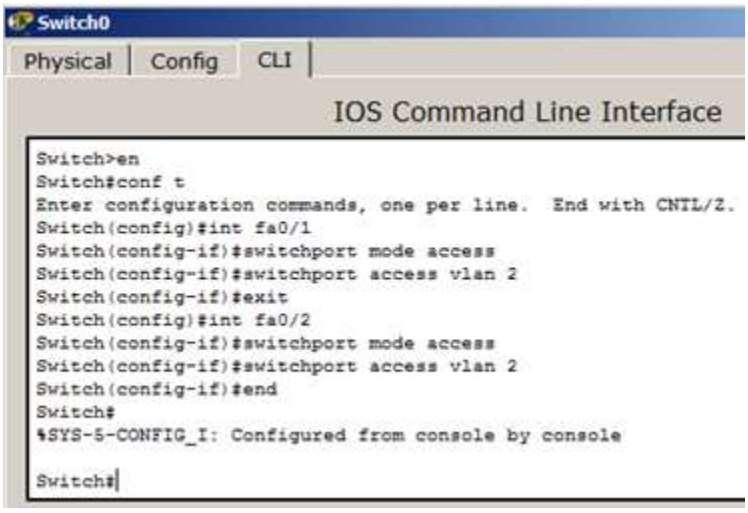


Рис. 4.4.Вказуємо порти комутатора для підключення користувачів

Тепер командою ***show vlan*** можна перевірити результат (рис. 4.5).

```
Switch0
Physical | Config | CLI
IOS Command Line Interface
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
2    sklad                            active    Fa0/1, Fa0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Рис. 4.5.Підмережа VLAN2 склад налаштована

Далі працюємо з VLAN3 (рис. 4.6).

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config-vlan)#vlan 3
Switch(config-vlan)#name buh
Switch(config-vlan)#exit
Switch(config)#
```

Рис. 4.6.VLAN3 отримує ім'я buh

У віртуальній мережі VLAN3 налаштовуємо порти комутатора Fa0 / 3 і Fa0 / 4 як ***access*** порти, тобто порти для підключення користувачів, потім командою show vlan можна перевірити і переконатися, що ми створили в мережі 2 сегмента на різні порти комутатора (рис. 4.7).

```
Switch0
Physical | Config | CLI
IOS Command Line Interface

Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#int fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
2    sklad                            active    Fa0/1, Fa0/2
3    buh                              active    Fa0/3, Fa0/4
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Рис. 4.7.Ми налаштували VLAN2 і VLAN3

Налаштовуємо IP адреса комп'ютерів – для VLAN2 з мережі 192.168.2.0, а для VLAN3 з мережі 192.168.3.0 (рис. 4.8).

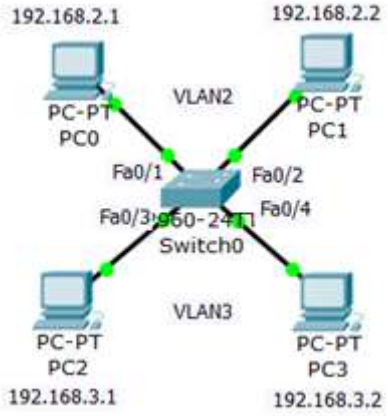


Рис. 4.8.Налаштовуємо IP адреса комп'ютерів

Перевіряємо зв'язок ПК в межах VLAN і відсутність зв'язку між VLAN2 і VLAN3 (рис. 4.9).

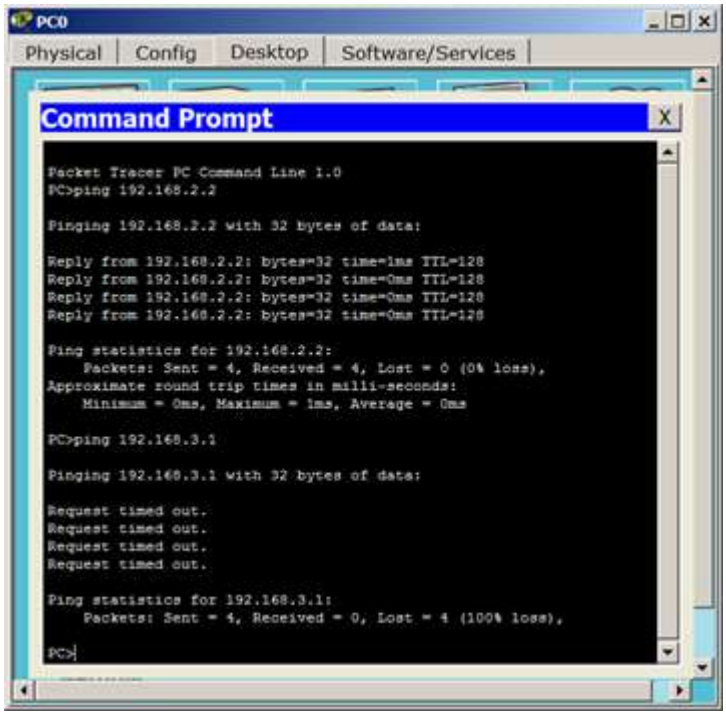


Рис. 4.9.Все працює так, як було задумано

Отже, на комп'ютері ПК0 переконалися, що комп'ютер в своєму сегменті бачить ПК, а в іншому сегменті - ні.

Завдання4.2.Налаштування віртуальної мережі на комутаторі 2960

У даній роботі розглядається налаштування VLAN на комутаторі фірми Cisco в програмі **CPT**.

Створіть ***мережу, топологія*** якої представлена на рис. 4.10.

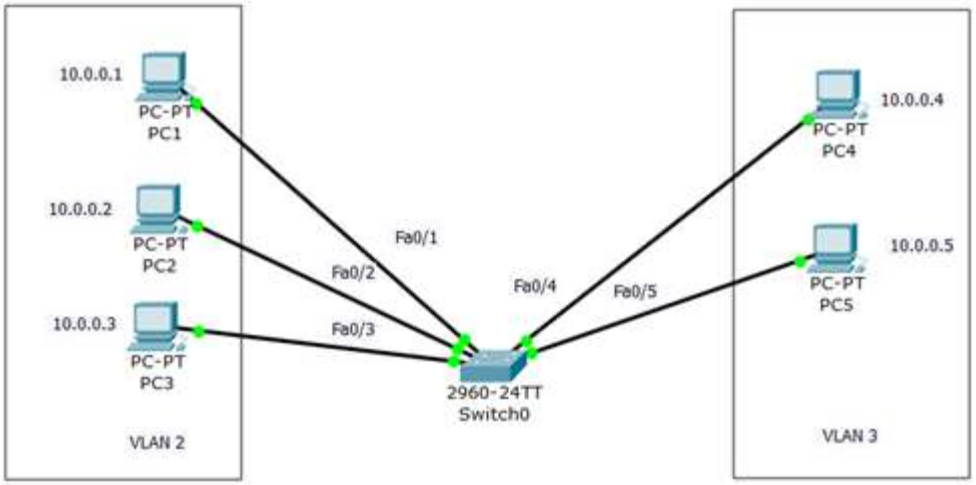


Рис. 4.10.Схема мережі з одним комутатором

Завданням даної роботи є створення 2х незалежних груп комп'ютерів: ПК1-ПК3 повинні бути доступні тільки один для одного, а друга незалежна група - комп'ютери ПК4 і ПК5.

Налаштування комутатора

Спочатку сформуємо ***VLAN2***. Двічі клацніть лівою кнопкою миші по комутатору. У вікні, перейдіть на вкладку ***CLI***. Ви побачите вікно консолі. Натисніть на клавішу ***Enter*** для того, щоб приступити до введення команд. Перейдемо в привілейований режим, виконавши команду ***enable***:

Switch> en

За замовчуванням всі ПК об'єднані в ***VLAN1***. Для реалізації мережі, яку ми запланували, створимо на комутаторі ще два ***VLAN*** (2 і 3). Для цього в привілейованому режимі виконайте наступну команду для переходу в режим конфігурації:

Switch # conf t

Тепер вводимо команду ***VLAN 2***. Даною командою ви створите на комутаторі ***VLANc*** номером 2. Покажчик введення ***Switch (config)*** #

зміниться на ***Switch (config-vlan)*** # це свідчить про те, що ви конфігуріруете вже не весь комутатор в цілому, а тільки окремий VLAN, в даному випадку ***VLAN*** номер 2 (рис. 4.11).

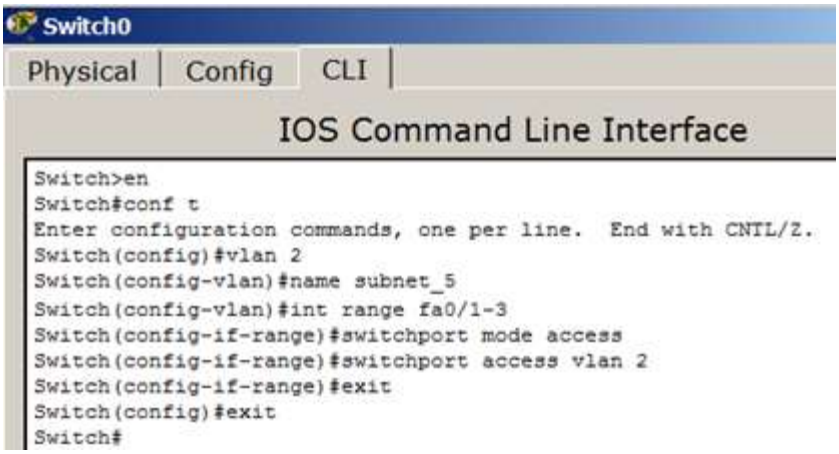


Рис. 4.11.Лістинг команд для формування VLAN2

Примітка

Командою VLAN2, ми створюємо на комутаторі новий VLAN з номером 2. Команда ***name subnet_5*** *привласнює ім'я subnet_5 віртуальної мережі номер 2. Виконуючи команду* ***interface range fast Ethernet 0 / 1-3*** *ми переходимо до конфігурації* ***інтерфейсів fast Ethernet 0/1, fast Ethernet 0/2 і fast Ethernet 0/3*** *комутатора. Слово* ***range*** *в даній команді, вказує на те, що ми будемо конфігурувати не один порт, а діапазон портів. Команда* ***switch port mode access*** *конфигурирует обраний порт комутатора, як порт доступу (access порт). Команда* ***switch port access vlan 2*** *вказує, що даний порт є портом доступу для VLAN номер 2.*

Вийдіть з режиму конфігурації, двічі набравши команду **exit** і перегляньте результат конфігурації (рис. 4.12), виконавши команду **shvlbr**. Як бачимо, на комутаторі з'явився VLAN з номером 2 і ім'ям subnet_5, портами доступу якого є fast Ethernet 0/1, fast Ethernet 0/2 і fast Ethernet 0/3.

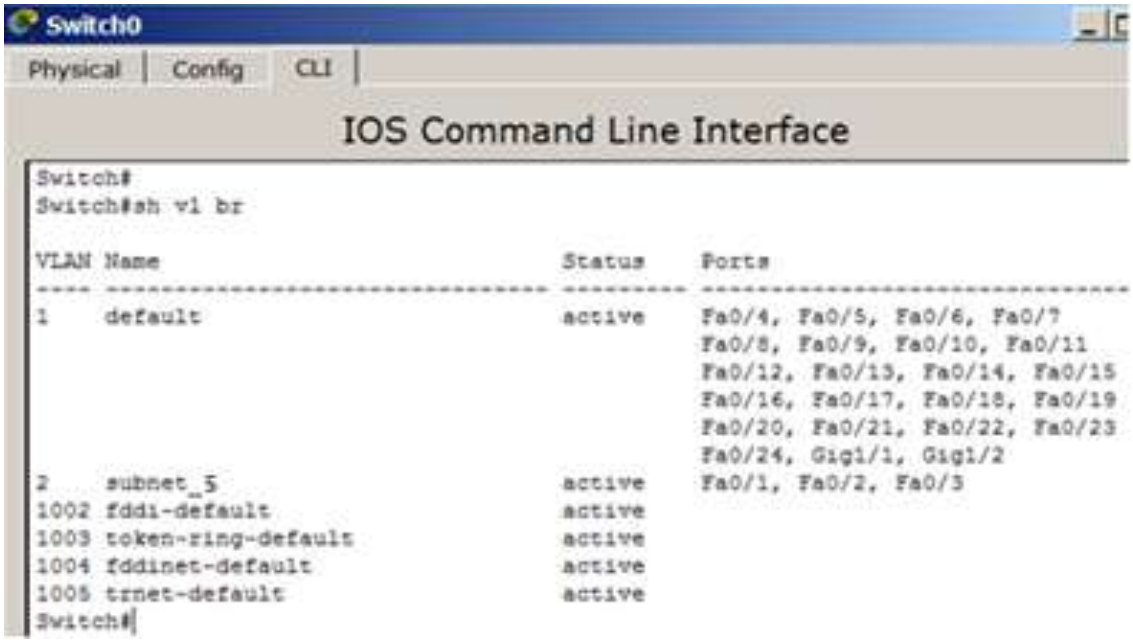


Рис. 4.12.Перегляд інформації про VLAN на комутаторі

Примітка

Команда **shvlbr** *виводить інформацію про існуючі на комутаторі VLAN-ах. В результаті виконання команди на екрані з'явиться:* ***номера VLAN*** *(перший стовпець),* ***назва VLAN*** *(другий стовпець),* ***стан VLAN*** *(працює він чи ні) - третій стовпець,* ***порти****, що належать до даного VLAN (четвертий стовпець).*

Далі аналогічним чином створимо **VLAN 3** з ім'ям **subnet_6** і зробимо його портами доступу інтерфейси fastEthernet 0/4 і fastEthernet 0/5. Результат показаний на рис. 4.13.

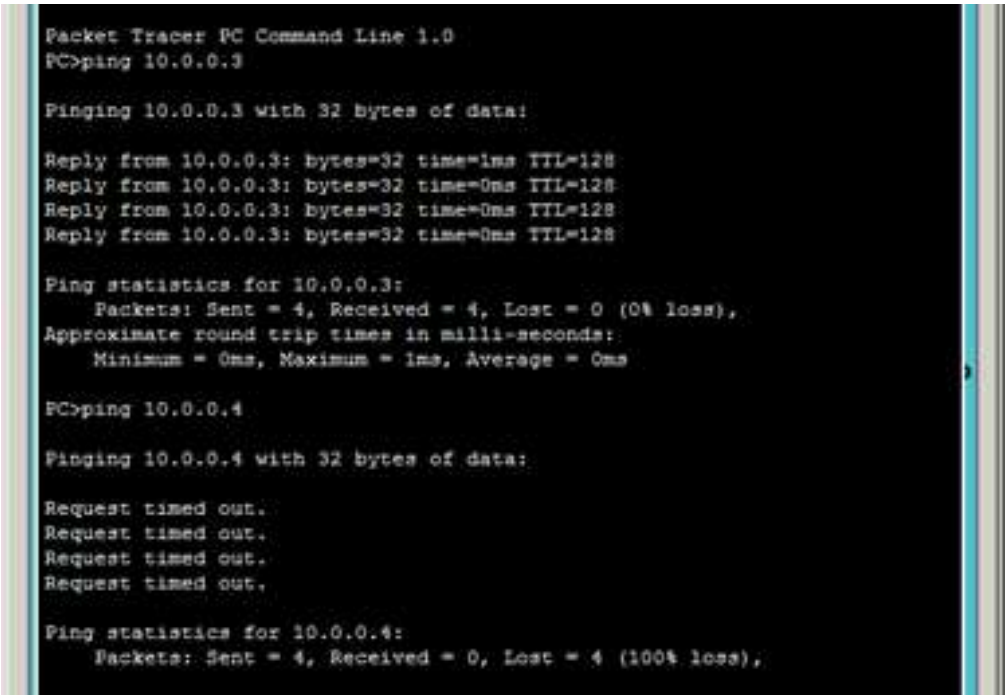
```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 3
Switch(config-vlan)#name subnet_6
Switch(config-vlan)#int range fa0/4-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 3
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vl br
VLAN Name                             Status    Ports
---- -------------------------------- ---------
------------------------------
1    default                          active    Fa0/6, Fa0/7, Fa0/8,
Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12,
Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16,
Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20,
Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24,
Gig0/1
                                                Gig0/2
2    subnet_5                         active    Fa0/1, Fa0/2, Fa0/3
3    subnet_6                         active    Fa0/4, Fa0/5
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Рис. 4.13.Результат - налаштування на коммутаторі VLAN2 і VLAN3

Перевірка результатів роботи

Мережа налаштована і потрібно її протестувати. Результат позитивний, якщо в межах своєї VLAN комп'ютери доступні, а комп'ютери з різних VLAN не доступні (рис. 4.14). Усі п'ять комп'ютерів знаходяться в одній мережі 10.0.0.0/8, але вони знаходяться в різних віртуальних локальних мережах.



```
Packet Tracer PC Command Line 1.0
PC>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time=1ms TTL=128
Reply from 10.0.0.3: bytes=32 time=0ms TTL=128
Reply from 10.0.0.3: bytes=32 time=0ms TTL=128
Reply from 10.0.0.3: bytes=32 time=0ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рис. 4.14.Пінг з PC1 на PC3 і PC4

Завдання4.3.VLAN з двома комутаторами. Розділяється загальний канал (транк)

На практиці часто виникає завдання поділу пристроїв, підключених до одного або декількох комутаторів на кілька непересічних локальних мереж. У разі, якщо використовується тільки один ***комутатор***, то це завдання вирішується шляхом конфігурації портів комутатора, вказавши кожному порту до якої локальної мережі він належить. Якщо ж використовується кілька комутаторів (рис. 4.15), то необхідно між комутаторами крім даних передавати інформацію до якої локальної мережі відноситься ***кадр***. Для цього був розроблений стандарт 802.1Q.

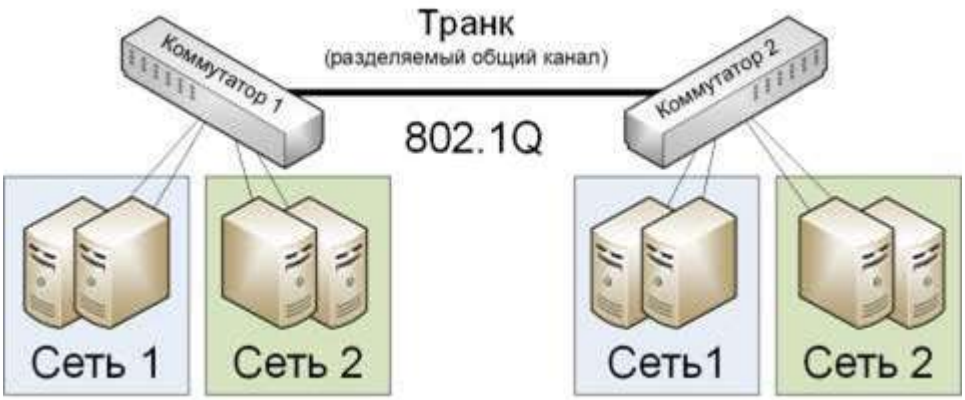


Рис. 4.15.Віртуальні локальні мережі (VLAN) з використанням двох комутаторів

Від теорії перейдемо до практики і зробимо дублювання нашої мережі (тій, яка була показана раніше на рис. 4.10). Для цього виділимо всю ***мережу*** інструментом **Select** (Виділити), і, утримуючи клавішу **Ctrl**, перетягнемо на нове ***місце*** в робочій області програми. Так ми зробимо ***копіювання*** (рис. 4.16).

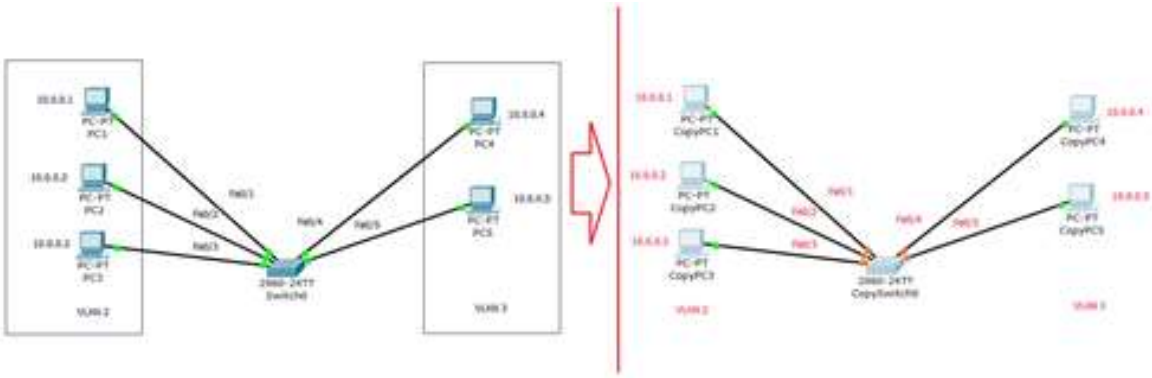


Рис. 4.16. Дублюємо мережу з одним комутатором

З'єднаємо комутатори перехресним кабелем (кросом) через найпродуктивніші порти –*GigabitEthernet*(рис. 4.17).

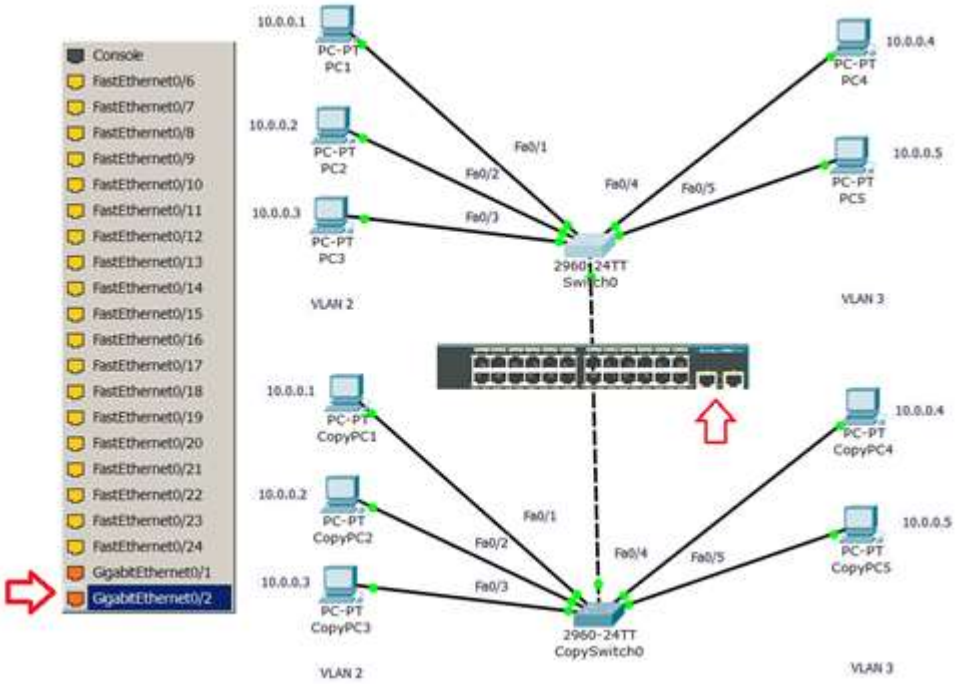


Рис. 4.17.З'єднуємо комутатори через Gigabit Ethernet порти

Тепер поправимо настройки на дублікаті вихідної мережі (рис. 4.18).

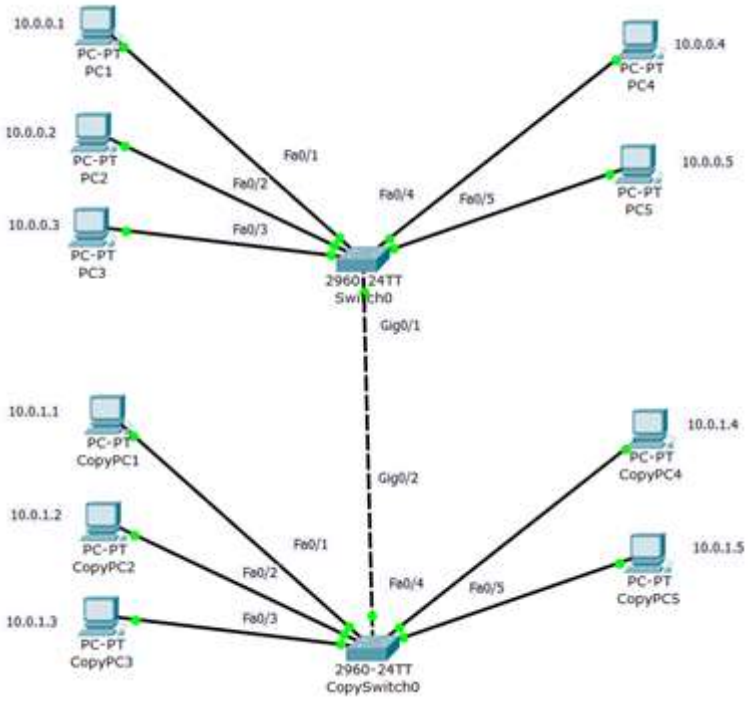


Рис. 4.18.Налаштовуємо мережу-дублікат

Зазначимо новий варіант підмереж VLAN2 і VLAN3, а також виділимо **trunk**

(транк) ***зв'язок*** комутаторів (рис. 4.19).

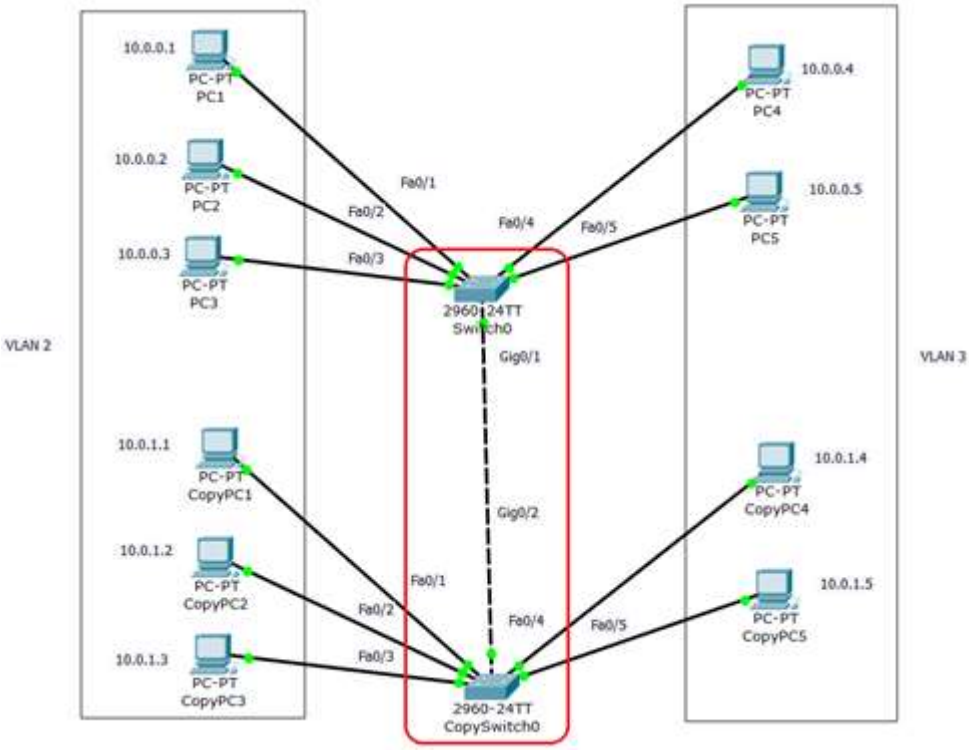


Рис. 4.19. В мережі позначаємо підмережі VLAN2 і VLAN3

Налаштовуємо транк порт Gig0/1

При налаштуванні ***Gig0 / 1*** на комутаторі ***Switch0*** міняємо стан порту і вказуємо ***vlan*** 2 і 3 для роботи з ним (рис. 4.20).

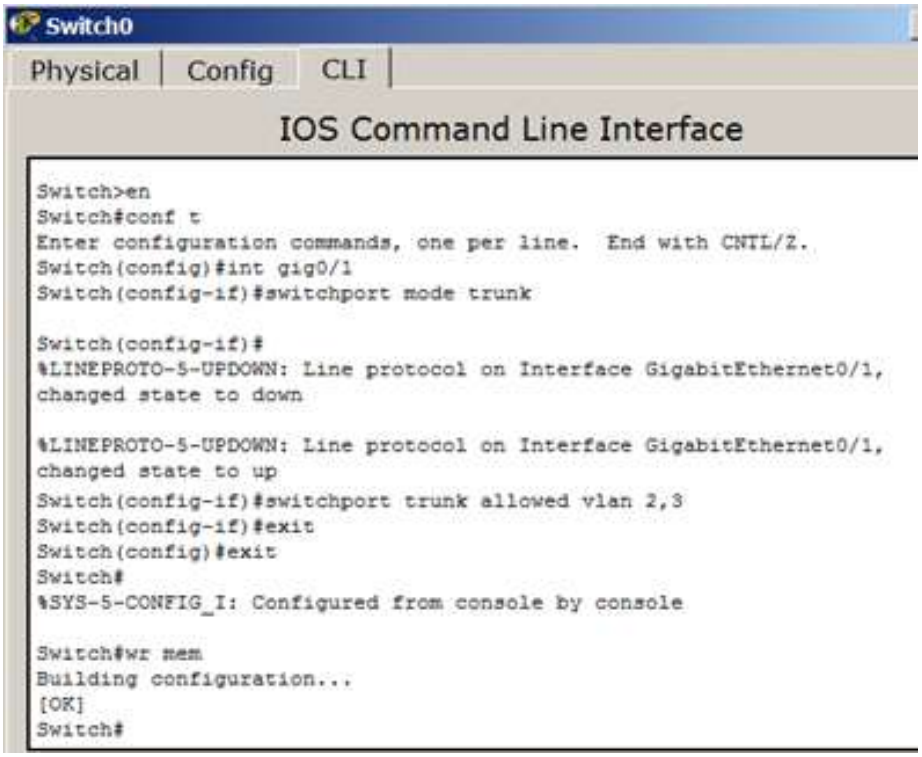


Рис. 4.20.Налаштовуємо транк порт Gig0/1 на коммутаторі Switch0

Налаштовуємо транк порт Gig0/2

Транк порт ***Gig0/2*** на комутаторе ***CopySwitch0*** налаштовуємо аналогічно (рис. 4.21).

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int gi0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allow vlan 2,3
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#end
```

Рис. 4.21.Налаштовуємо trunk порт Gig0/2 на комутаторі CopySwitch0

Діагностика результатів роботи

Перевіряємо пінг з PC1 в різні vlan (рис. 4.22) .Все відмінно: в межах своєї vlan ПК доступні, а між ПК різних vlan зв'язку немає.

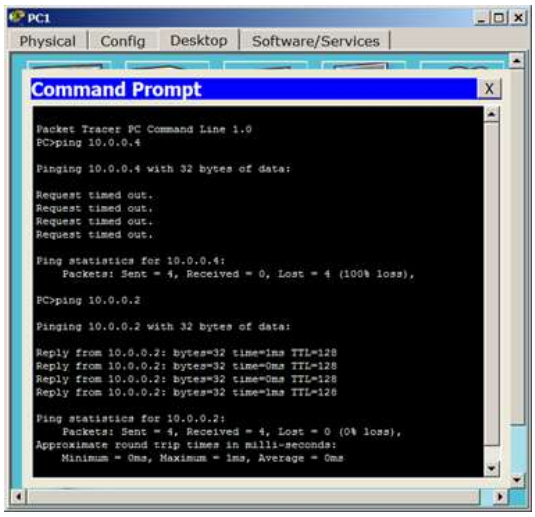


Рис. 4.22.Пінг з PC1 в різні vlan

Завдання 4.4.Налаштування віртуальної мережі з двох світчей і чотирьох ПК

Далі розглянемо як налаштувати VLAN з двох світчей і чотирьох ПК.

Створіть мережу, топологія якої представлена на рис. 4.23. Поки в мережі 10.0.0.0 немає поділу на VLAN - все комп'ютери доступні між собою.

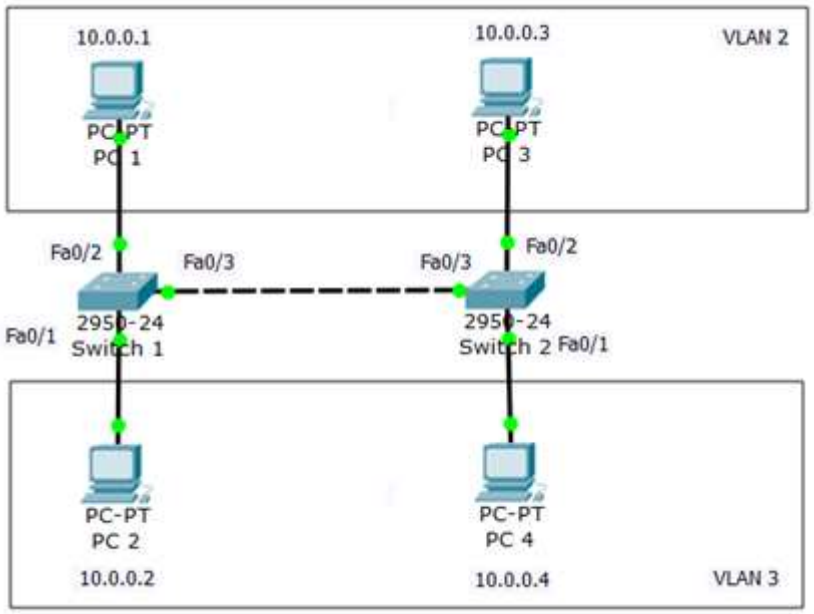


Рис. 4.23. Схема мережі

Отже, підмережі Vlan 2 належать порти комутаторів Fa0 / 2, а Vlan 3 належать порти комутаторів Fa0 / 1.

Налаштування VLAN 2 і VLAN3

Перейдіть до налаштування комутатора ***Switch1.*** Відкрийте його консоль. У вікні, перейдіть на вкладку *CLI*, увійдіть в привілейований режим і налаштуйте *VLAN 2 і VLAN3*. Потім перегляньте інформацію про існуючі на комутаторі VLAN-ах командою: Switch1 # sh vl br (рис. 4.24).

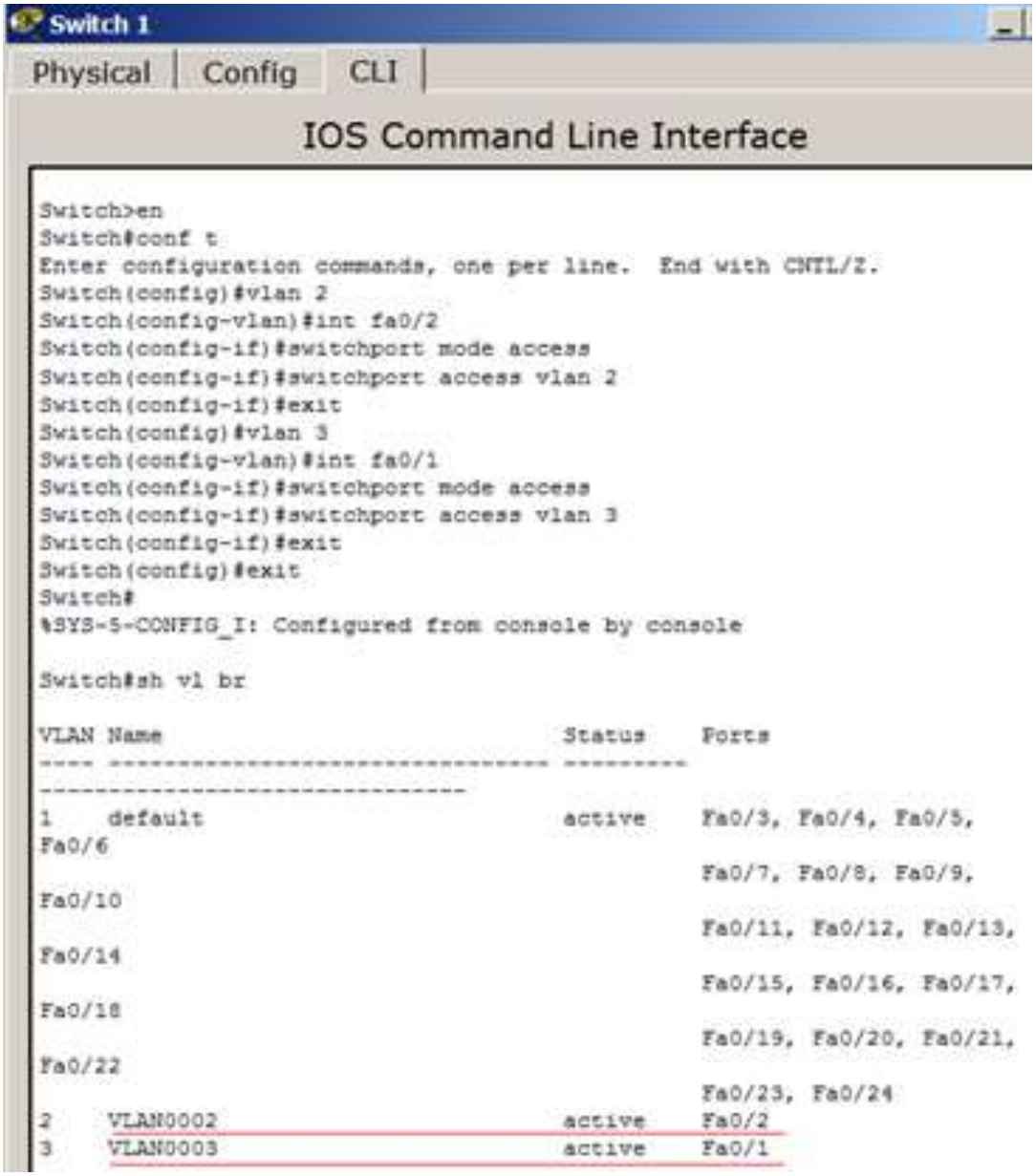


Рис. 4.24. Конфігурацфія Switch1

Аналогічним чином настройте Switch2, виходячи з того, що за умовами завдання у нас Fa0/2 розташований в Vlan2, а Fa0 / 1 знаходиться в Vlan 3 (це не завжди так). Результат конфігурації S2 показаний на рис. 4.25.

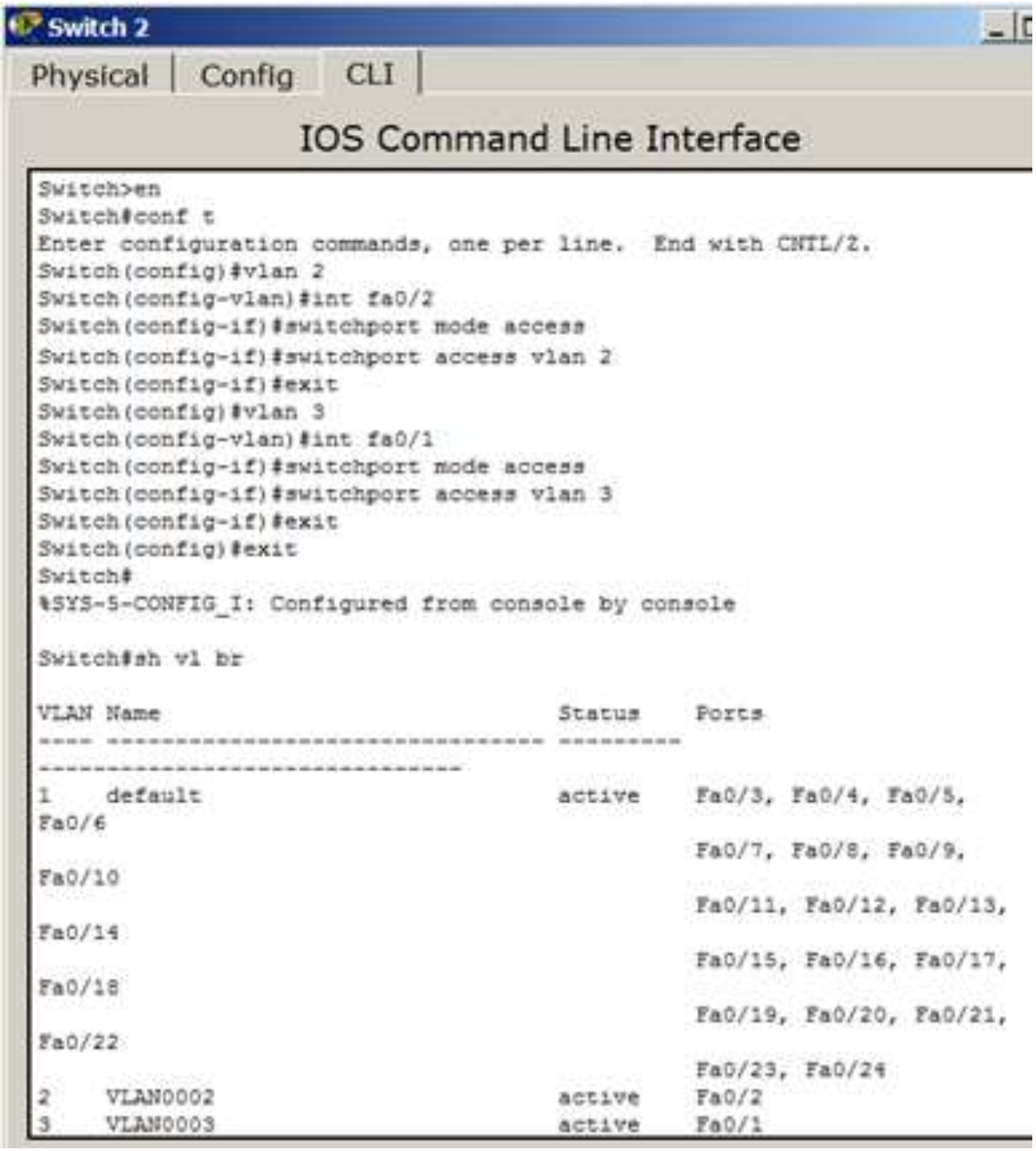


Рис. 4.25. Конфігурація Switch2

Отже, підмережі Vlan 2 належать порти комутаторів Fa0 / 2, а Vlan 3 належать порти комутаторів Fa0 / 1. Оскільки в даний момент немає обміну інформації про Vlan, то всі комп'ютери роз'єднані (рис. 4.26).

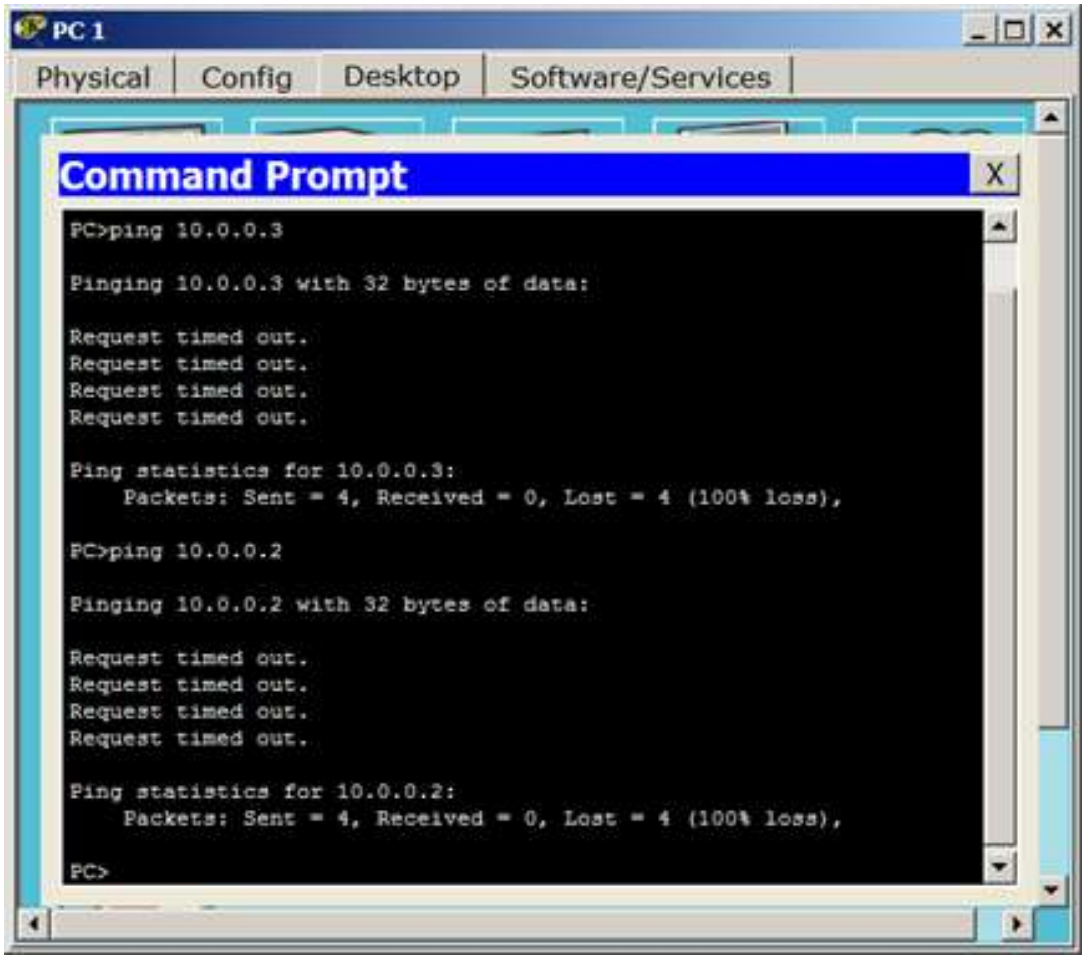


Рис. 4.26.Зв'язків між ПК немає

Налаштування зв'язку комутаторів через транковий порт

Тепер організуємо магістраль обміну між комутаторами. Для цього налаштуємо третій порт **Fa0 / 3** на кожному комутаторі як транковий. Увійдіть в консоль комутатора **Switch1** і задайте транковий порт (рис. 4.27).

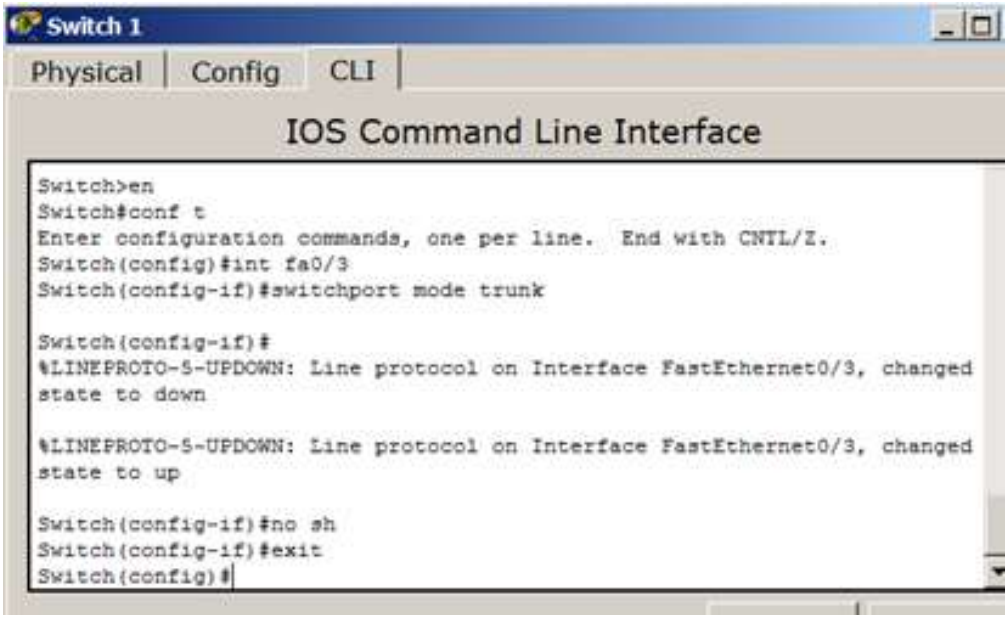


Рис. 4.27.Налаштовуємо транковий порт на S1

Відкрийте конфігурацію коммутатораS1 на інтерфейсі **Fast Ethernet 0/3** і переконайтеся, що порт транковий (рис. 4.28).

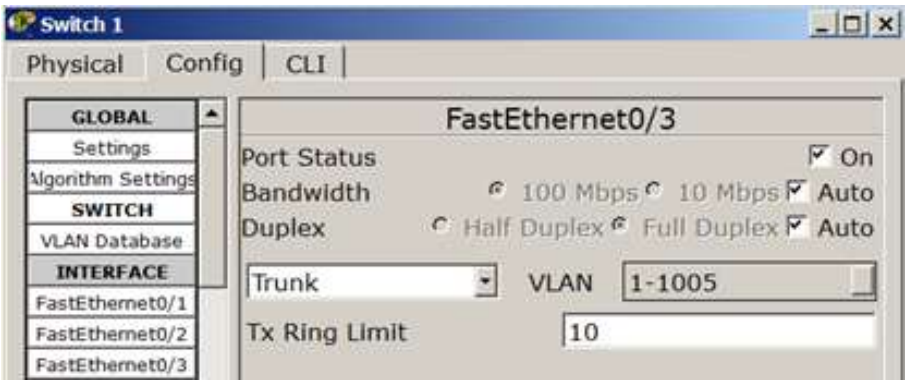


Рис. 4.28.Конфігурація інтерфейсу FastEthernet0 / 3 на Switch1

На комутаторі **Switch2** інтерфейс **FastEthernet 0/3** автоматично налаштується як транковий (рис. 4.29).

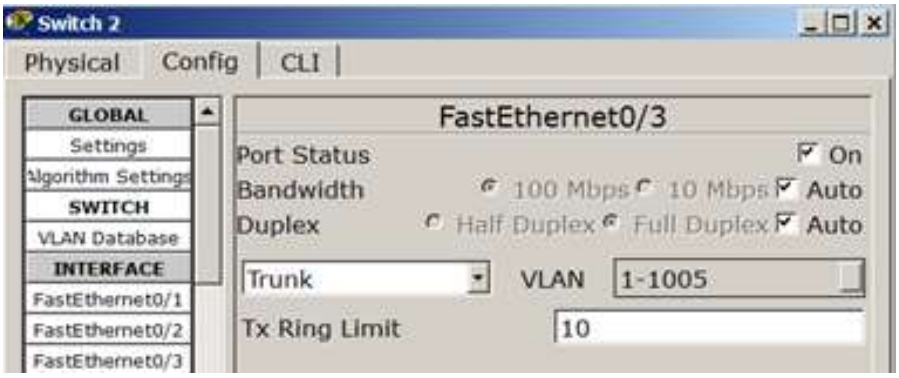


Рис. 4.29.Конфігурація інтерфейсу FastEthernet0 / 3 на Switch2

Тепер комп'ютери, що входять в один *Vlan* повинні пінгувати, а комп'ютери в різних віллах будуть взаємно недоступні (рис. 4.30).

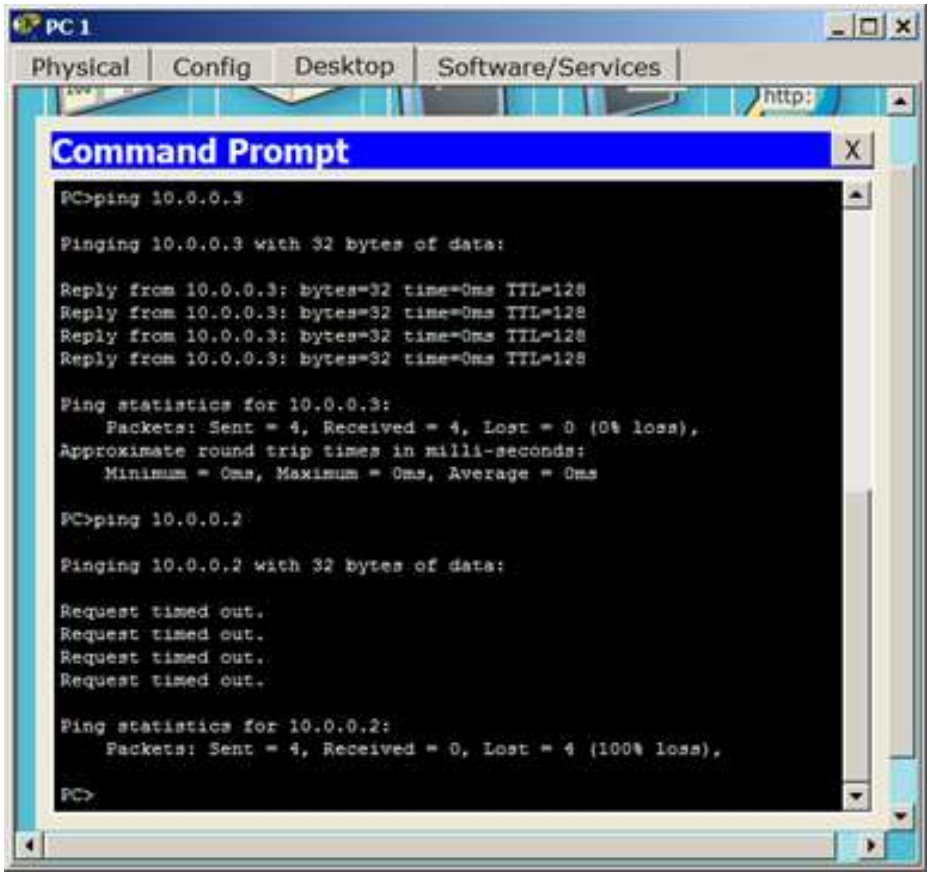


Рис. 4.30.Перевірка зв'язку PC1 з ПК в VLAN 2 і VLAN 3

Склад звіту лабораторної роботи

В звіті повинно бути відображено:

1. Тема роботи.
2. Мета роботи.
3. Виконання завдання 4.1 з відповідними скріншотами.
4. Виконання завдання 4.2 з відповідними скріншотами.
5. Виконання завдання 4.3 з відповідними скріншотами.
6. Виконання завдання 4.4 з відповідними скріншотами.
7. Висновки

Контрольні питання

1. Поняття віртуальної мережі.
2. Переваги віртуальних мереж.
3. Типи віртуальних мереж.
4. Статичні та динамічні VLAN.
5. Стандарти VLAN.

Лабораторна робота№ 5

Тема: НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУДИНАМІЧНОГО КОНФІГУРУВАННЯ ВУЗЛІВ DHCP У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження роботи протоколу динамічного конфігурування вузлів DHCP на обладнанні Cisco; отримати практичні навички налагодження, моніторингу та діагностування роботи DHCP-сервера на базі маршрутизатора Cisco; дослідити процес роботи протоколу DHCP та процеси передачі даних у побудованій мережі.

Теоретичні відомості

Загальні відомості про технології та протоколи логічної адресації в IP-мережах

Для забезпечення ефективного функціонування будь-якоговузла в IP-мережі його мережному адаптеру/інтерфейсу необхідно при- значити такі параметри логічноїадресації:

- IP-адресаадаптера/інтерфейсу;
- маска/префікс мережі(підмережі);
-IP-адреса шлюзу зазамовчуванням;
- IP-адресаDNS-сервера;
- IP-адресаWINS-сервера.

Для функціонування вузла у локальній мережі, яка не має під- ключення

до іншої мережі, достатньо призначати лише перші два параметри. Коли ж виникає потреба забезпечити міжмережний обмін між локальними мережами або підключення до глобальної мережі, необхідно встановлювати IP-адресу шлюзу за замовчуванням. У деяких випадках таких адрес може бути кілька. Для забезпечення доступу до ресурсів серверів з використанням символьних домен- них імен вузлів необхідно встановлювати IP-адресу DNS-сервера. У більшості ОС передбачена можливість використання кількох IP-адрес DNS-серверів. IP-адреса WINS-сервера необхідна в ОС WIndows для зіставлення NetBIOS-імен комп'ютерів з IP-адресами. Нині служба WINS використовується досить рідко.

Призначення параметрів IP-адресації може здійснюватися як статично адміністратором, так динамічно з використанням спеціальних технологій та протоколів. Статично параметри призначаються вузлам, які постійно знаходяться у мережі. Це можуть бути як кінцеві вузли (сервери, стаціонарні робочі станції, мережні принтери тощо), так і комунікаційні пристрої (комутатори, маршрутизатори, точки доступу, міжмережні екрани тощо). Динамічно параметри призначаються вузлам, які мігрують між мережами. Це можуть бути переносні робочі станції, планшети тощо.

Для статичного призначення параметрів IP-адресації використовуються як графічні засоби ОС, так і відповідні команди, що виконуються у командному рядку. Наприклад, в ОС Unix/Linux застосовується команда **ifconfig**. Серед засобів динамічного призначення у першу чергу необхідно згадати такі технології та протоколи:

- технологія автоматичного самопризначення адрес APIPA (Automatic Private IP Addressing) відома також як IPAC (Internet Protocol Automatic Configuration) для вузлів ОС Windows або Zeroconf (Zero Configuration Networking) для вузлів ОС Linux;
- протокол динамічного конфігурування вузлів DHCP (Dynamic Host Control Protocol);

- протокол віддаленого завантаження BOOTP (Bootstrap Protocol).

Технологія APIPA реалізована як для IP версії 4, так і для IP версії 6. У першому випадку передбачається самопризначення IP- адрес з адресного діапазону мережі 169.254.0.0/16, у другому – з адресного діапазону мережі FE80::/64. Програмно технологія APIPA реалізована як складова DHCP-клієнта.

Протокол DHCP реалізовано за клієнт-серверною схемою. DHCP-клієнт звертається з запитами про надання адресної інформації до DHCP-сервера. DHCP-сервер обслуговує запити клієнтів, відстежує актуальність бази даних виданих і вільних адрес, контролює активність вузлів та виконує інші сервісні операції. Окрім сервера та клієнта в протоколі DHCP реалізується ще один вид вузла – зв'язний агент, який використовується для пересилки запитів між клієнтами і серверами, що розташовані у різних IP-мережах.

Призначення параметрів IP-адресації за допомогою засобів про- токолу DHCP (надалі призначення IP-адрес) може бути виконано одним з трьох способів:

- динамічне призначення IP-адрес;
- автоматичне призначення IP-адрес;
- ручне призначення IP-адреси.

При динамічному призначенні IP-адрес DHCP-сервер видає DHCP-клієнту будь-яку вільну IP-адресу на обмежений час. При автоматичному призначенні IP-адрес DHCP-сервер спочатку видаєDHCP-клієнту будь-яку вільну IP-адресу, запам'ятовує параметри клієнта (фізичну, MAC-адресу) і при наступних спробах отримання адреси цим клієнтом видає лише її. При ручному призначенні IP-адреса призначається адміністратором DHCP-клієнту по його MAC-адресі, відповідність IP-адреса-MAC-адреса зберігається у відповідній базі даних чи файлі, а DHCP-сервер використовується лише для передачі IP-адреси. Якщо MAC-адреса вузла відсутня, то IP-адреса на видається.

Кожен із способів має свої переваги і недоліки. Динамічне при- значення IP-адрес з одного боку забезпечує можливість швидкого призначення параметрів IP-адресації великій кількості клієнтів, а з іншого – дає можливість вузлу зловмисника безпроблемноотримати IP-адресу, визначити всі параметри адресації мережі і на основі отриманої інформації надалі виконувати атаки на певні вузли чи групи вузлів мережі. Ручне призначення IP-адрес з одного боку ви- магає володіння повною інформацією про фізичні та логічні адреси вузлів та вимагає набагато більше часу на налагодження DHCP- сервера, з іншого – забезпечує вищий рівень захисту, тобто ускладнює завданнязловмисникові.

Більшість сучасних виробників маршрутизаторів (зокрема Cisco, Huawei, Juniper) реалізовуються підтримку функціонування як DHCP-серверів, так і DHCP-клієнтів та зв'язних агентів на своїх пристроях.

Порядок налагодження DHCP-сервера на базі маршрутизатора Cisco

У практиці побудови мереж маршрутизатор Cisco у більшості випадків налагоджується як DHCP-сервер, у деяких випадках – як зв'язний агент DHCP і досить рідко – як DHCP-клієнт. Налагодження функціонування DHCP-сервера на базі маршрутизатора Cisco згідно з рекомендаціями виробника складається із певних обов'язкових та необов'язкових етапів. Порядок виконання згаданих етапів є таким:

1. Включити функціонування DHCP-сервера на маршрутизаторі (залежно від ситуації, за замовчуванням запускаєтьсяавтоматично).
2. Налагодити DHCP Database Agent або відключити DHCP Conflict Logging(обов'язково).
3. Виключити IP-адреси, які не будуть призначатися DHCP-клієнтам(обов'язково).

4. Створити та налагодити набір (набори) IP-адрес, які будуть призначатися DHCP-клієнтам(обов'язково).
5. Налагодити ручне призначення IP-адрес(необов'язково).
6. Налагодити параметри завантажувального файла для даного DHCP-сервера(необов'язково).
7. Зазначити кількість перевірочних запитів протоколу ICMP (необов'язково).
8. Встановити значення тайм-ауту для перевірочних запитів протоколу ICMP(необов'язково).
9. При налагодженні зв'язного агента DHCP для даного порядку додаються наступні етапи :
10. Активувати Cisco IOS DHCP-клієнта на інтерфейсах Ethernet/Fast Ethernet (необов'язково).
11. Налагодити параметри імпорту опцій DHCP-сервера та автоконфігурування (необов'язково).
12. Налагодити параметри опцій зв'язного агента DHCP в повідомленнях BOOTREPLY(необов'язково)
13. Налагодити параметри політики передачі для зв'язного агента DHCP(необов'язково).
14. Активувати додаткові можливості зв'язного агента DHCP (необов'язково).
15. На практиці можливе застосування іншого порядку.

Команди налагодження DHCP-сервера на базі маршрутизатора Cisco

Включення функціонування DHCP-сервера на маршрутизаторі Cisco виконується командою ***service dhcp***. Виключення — командою ***no service***

dhcp. За замовчуванням на маршрутизаторі Cisco DHCP-сервер є включеним. Якщо використання DHCP-сервера не планується, то з метою підвищення рівня захисту пристрою рекомендується даний функціонал відключати.

Основною командою, від якої походить більшість команд для налагодження засобів протоколу DHCP у Cisco IOS є команда ***ip dhcp***. Перелік та призначення похідних команд можна отримати за допомогою інтерактивної довідки командного рядка. Слід зауважити, що для різних моделей маршрутизаторів, версій IOS та наборів властивостей, переліки можуть відрізнятися. У більшості випадків у режимі конфігурування протоколу маршрутизації доступними є такі команди ***ip dhcp aaa***, ***ip dhcp binding***, ***ip dhcp bootp***, ***ip dhcp class***, ***ip dhcp compatibility***, ***ip dhcp conflict***, ***ip dhcp database***, ***ip dhcp excluded-address***, ***ip dhcp limit***, ***ip dhcp limited-broadcast-address***, ***ip dhcp ping***, ***ip dhcp pool***, ***ip dhcp relay***, ***ip dhcp smart-relay***, ***ip dhcp update***, ***ip dhcp use***. У деяких випадках використовуються і інші команди. Призначення та синтаксис основних команд наведено нижче.

Створення або редагування набору (пулу) адрес, які будуть видаватися DHCP-клієнтами, виконується командою ***ip dhcp pool***. Після виконання даної команди здійснюється перехід до режиму налагодження протоколу DHCP. У цьому режимі наявно більше ніж 25 команд, які стосуються різних аспектів налагодження пулу адрес протоколу DHCP.

Після переходу до режиму налагодження протоколу DHCP на ступним кроком є зазначення IP-адреси та маски (префікса) мережі адреси якої будуть призначатися DHCP-клієнтам. Для цього використовується команда ***network***. Ще одним важливим кроком є зазначення IP-адреси шлюзу за замовчуванням для даної мережі. Для цього використовується команда ***default-router***. Можливе використання до 8 шлюзів. На практиці достатньо одного. Наступними (необов’язковими) кроками є зазначення сервера (серверів) служб DNS, WINS, а також типу вузлів NetBIOS для WINS. Для цього виконуються відповідно команди ***dns-server***, ***netbios-name-server***, ***netbios-node-***

type. IP-адреси, що вказуються як параметри цих команд, можуть належати іншим мережам. DHCP-сервер може також видавати назву домену. Для цього використовується команда ***domain-name***. Важливим параметром налагодження DHCP- маршрутизатора є час, на який виділяється IP-адреса, відомий також як час оренди адреси. Для його налагодження використовується команда***lease***.

Для вилучення з пулу IP-адрес, які не будуть призначатися, використовується команда ***ip dhcp excluded-address***. Цією командою можна вилучити як одну адресу, так і певний діапазон адрес. З метою усунення конфліктів вилучення IP-адрес рекомендується виконувати перед створенням пулу.

Перед виділенням IP-адреси з пулу алгоритмом роботи DHCP-сервера передбачена попередня перевірка, чи дійсно дана адреса є вільною. Для цього DHCP-сервер двічі посилає ICMP-запит за даною адресою. Якщо відповіді на запит немає, то DHCP-сервер вважає, що адреса є вільною і надає її клієнтові. Параметри даної перевірки (кількість запитів, інтервал між ними) можна змінити. Для цього використовуються команди ***ip dhcp ping packets*** *та* ***ip dhcp ping timeout***. Для активації/деактивації журналювання конфліктів адрес використовується команда ***ip dhcp conflict logging***.

Одним з режимів роботи DHCP є ручне призначення IP-адрес. У цьому випадку для кожного клієнта формується окремий пул і в цьому пулі за допомогою спеціалізованих команд проводиться налагодження призначення адреси. Для налагодження ручного призначення IP-адрес використовуються спеціальні команди **host**, **client-identifier**, **client-name**. Для зазначення IP-адреси шлюзу за замовчуванням, IP-адрес DNS-сервера та WINS-сервера використовуються вищезгадані команди ***default-router***, ***dns-server***, ***netbios-name-server***та деякі інші.

Завантаження конфігурації для DHCP-сервера можливе з внут- рішнього (Flash-пам’ять) або зовнішнього джерела (TFP, TFTP, RCP-сервери). Для

цього використовуються команди ***bootfile*** та ***ip dhcp database***.

Типи серверів. CiscoServer.

Як правило, ***сервер*** віддає в ***мережу*** свої ресурси, а клієнт ці ресурси використовує. Також, на серверах встановлюються спеціалізоване програмне і ***апаратне забезпечення***. На одному комп'ютері може працювати одночасно кілька програм-серверів. Сервіси серверів часто визначають їх назву:

Cisco HTTP (WEB) сервер - дозволяє створювати найпростіші веб-сторінки і перевіряти проходження пакетів на 80-й ***порт*** сервера. Ці сервери надають ***доступ*** до веб-сторінок і супутнім ресурсів, наприклад, картинкам.

DHCP сервер - дозволяє організовувати пули мережевих налаштувань для автоматичної конфігурації мережевих інтерфейсів. ***Dynamic Host Configuration Protocol*** забезпечує автоматичний розподіл ***IP***-адрес між комп'ютерами в мережі. Така технологія широко застосовується в локальних мережах з загальним виходом в ***Інтернет***.

DNS сервер - дозволяє організувати службу розв'язання доменних імен. ***Функція DNS***-сервера полягає в перетворенні доменних імен серверів в ***IP***-адреси.

Cisco EMAIL - ***поштовий сервер***, для перевірки поштових правил. Електронний ***лист*** можна надіслати безпосередньо одержувачу - спочатку воно потрапляє ***на сервер***, на якому зареєстрована обліковий ***запис***відправника. Той, в свою ***чергу***, відправляє "посилку" сервера одержувача, з якого останній і забирає повідомлення.

FTP - файловий ***сервер***. У його завдання входить зберігання файлів і забезпечення доступу до них клієнтських ПК, наприклад, за протоколом FTP. Ресурси ***файл***-сервера можуть бути або відкриті для всіх комп'ютерів в мережі, або захищені системою ідентифікації та правами доступу.

Отже, емулятор мережевий середовища Cisco Packet Tracer дозволяє проводити настройку таких мережевих сервісів, як: ***HTTP, DHCP, DNS, EMAIL, FTP*** і ряду інших в складі сервера мережі. Розглянемо настойку деяких з них.

Завдання на лабораторну роботу

Завдання 5.1. Налаштування WEB сервера.

Завдання 5.2. Налаштування мережевих сервісів DNS, DHCP і Web.

Завдання 5.3. Конфігурування DHCP сервера на маршрутизаторі.

Завдання 5.4. Приклад налаштування інтерфейсу маршрутизатора в якості DHCP клієнта.

Завдання 5.5. DHCP сервіс на маршрутизаторі 2811.

Завдання 5.1. Налаштування WEB сервера

Топологія для наших досліджень приведена на рис. 5.1.

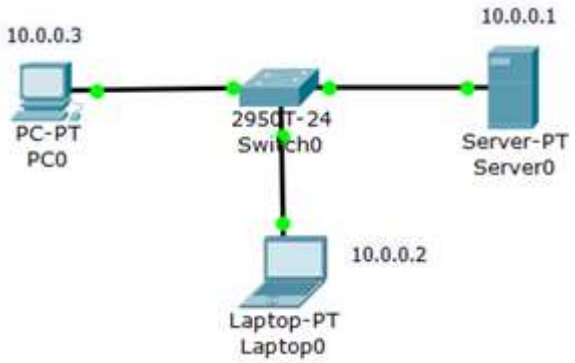


Рис. 5.1.Схема мережі

Створюємо WEB-документ на сервері

Для створення HTTP-сервера відкриваємо на сервері вкладку HTTP і редагуємо першу сторінку сайту з назвою **index.html.** Включаємо службу

HTTP перемикачем On (рис. 5.2).

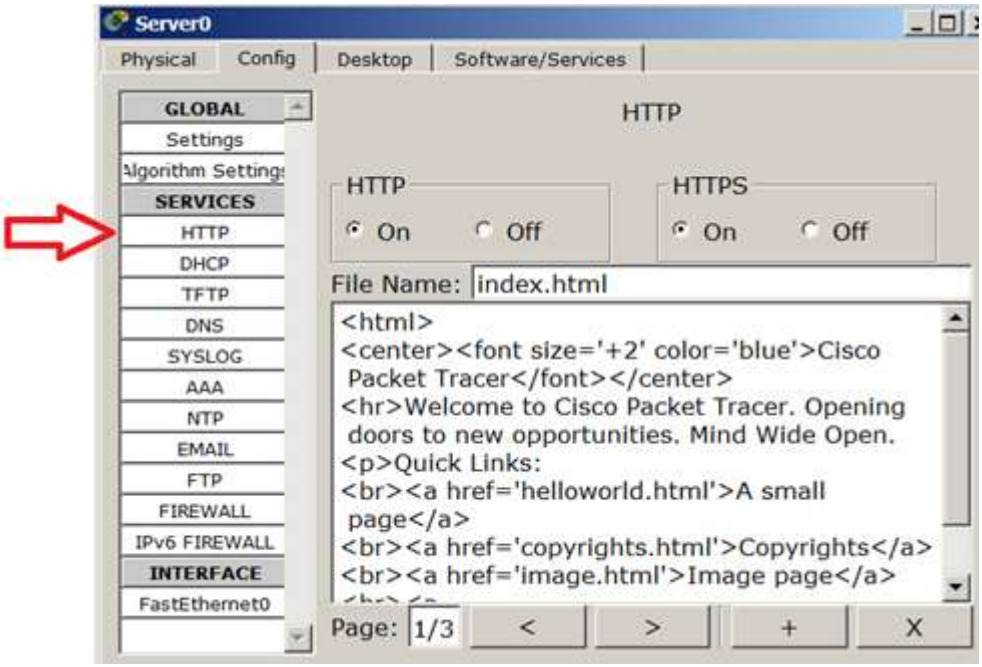


Рис. 5.2.Вкладка Config, служба сервера HTTP

В цьому вікні можна добавити нову сторінку кнопкою + або видалити ***поточну*** кнопкою X. Перемикання між кількома сторінками здійснюється кнопками < | >.

У вікні **html** коду створюємо текст першої сторінки сайту**index.html**. Варіант 1 (рис. 5.3).

```
<html>
<body>
<h1>Welcome to WEB-Server CISCO!</h1>
<p>Server working: <font color="red"><b>OK!</b></font></p>
</body>
</html>
```

Рис. 5.3.Текст web-сторінки, варіант 1

Або варіант 2 (рис. 5.4).

```
<html>
<center><font size='+2' color='blue'>Welcome to Cisco Packet Tracer HTML Server! </font></center>
<body>
Hello!<br/>I am OK!
</body>
</html>
```

Рис. 5.4.Текст web-сторінки, варіант 2

Текст можна переносити в це вікно через буфер обміну. Він може бути тільки на англійській мові.

Для того, щоб перевірити працездатність нашого сервера, відкриваємо

клієнтську машину (10.0.0.2 або 10.0.0.3) і на вкладці **Desktop** (Робочий стіл) запускаємо додаток **Web Browser**. Після чого набираємо адресу нашого **WEB**-сервера 10.0.0.1 і натискаємо на кнопку **GO**. Переконуємося, що наш веб-сервер працює.

Завдання 5.2. Налаштування мережевих сервісів DNS, DHCP і Web

Створіть схему мережі, представлених нарис. 5.5.

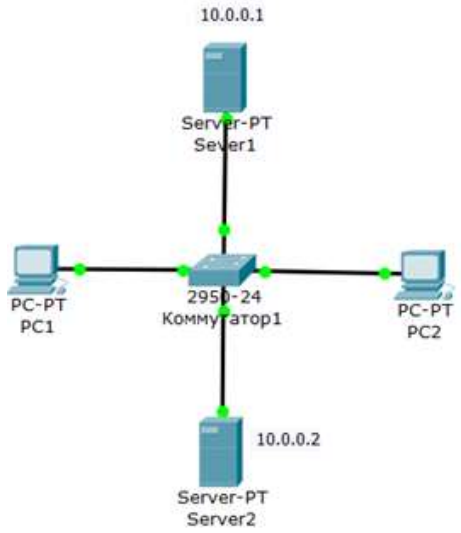


Рис. 5.5.Схема мережі

Наше завдання полягає в тому, щоб налаштувати Server1 як ***DNS*** і ***Web-сервер,*** а Server2 як ***DHCP сервер***. Нагадаю, що робота ***DNS***-сервера полягає в перетворенні доменних імен серверовв ***IP***-адреси. ***DHCP сервер*** дозволяє організовувати пули для автоматичної конфігурації мережевих інтерфейсів, тобто, забезпечує автоматичний розподіл ***IP***-адрес між комп'ютерами в мережі. Інакше кажучи, в нашому випадку комп'ютери отримують ***IP***-адреси завдяки сервісу ***DHCP*** Server2 і відкривають, наприклад, ***сайт*** на Server1.

Налаштовуємо IP адреси серверів і DHCP на ПК

Увійдіть в конфігурацію PC1 і PC2 і встановіть налаштування IP через

DHCP сервер рис. 5.6.

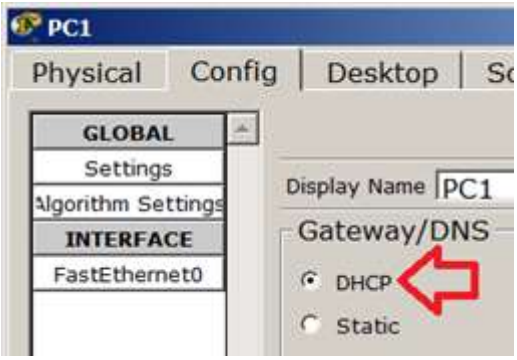


Рис. 5.6. Налаштування IP на PC1

Задайте в конфігурації серверів настройки IP: Server1 – 10.0.0.1 (рис. 5.7), Server2 – 10.0.0.2 (рис. 5.8). Маска підмережі встановиться автоматично як 255.0.0.0.

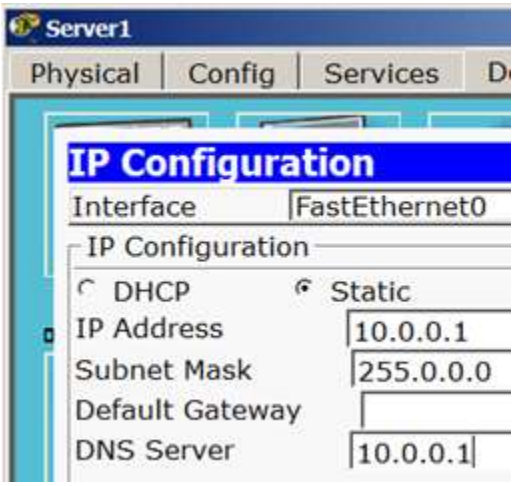


Рис. 5.7. Конфігурації серверів настройки IP Server1 – 10.0.0.1

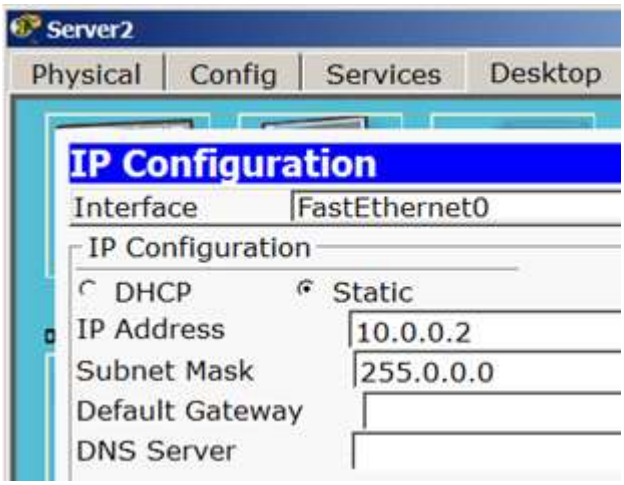


Рис. 5.8.Конфігурації серверів настройки IP Server2 – 10.0.0.2

Налаштування служб DNS і HTTP на Server1

У конфігурації Server1 увійдіть вкладку DNS і задайте дві ресурсні записи (Resource Records) в прямій зоні DNS.

Зона DNS - частина дерева доменних імен (включаючи ресурсні записи), що розміщується як єдине ціле на сервері доменних імен (DNS-сервері). У зоні прямого перегляду на запит доменного імені йде відповідь у вигляді IP адреси. У зоні зворотного перегляду по IP ми дізнаємося доменне ім'я ПК.

Спочатку в ресурсної записи типу **A Record** зв'яжіть доменне ім'я комп'ютера **server1.yandex.ru** з його **IP адресою 10.0.0.1** і натисніть на кнопку **Add** (додати) і активуйте перемикач **On** – рис. 5.9.

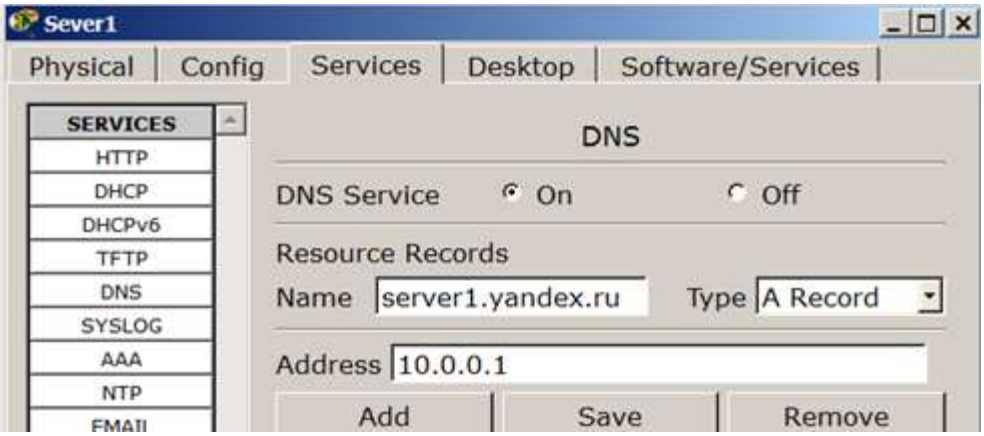


Рис. 5.9. Введення ресурсного запису типу A Record

Далі в ресурсної записи типу **CNAME** зв'яжіть назву сайту з сервером і натисніть на кнопку **Add** (додати) –рис.5.10.

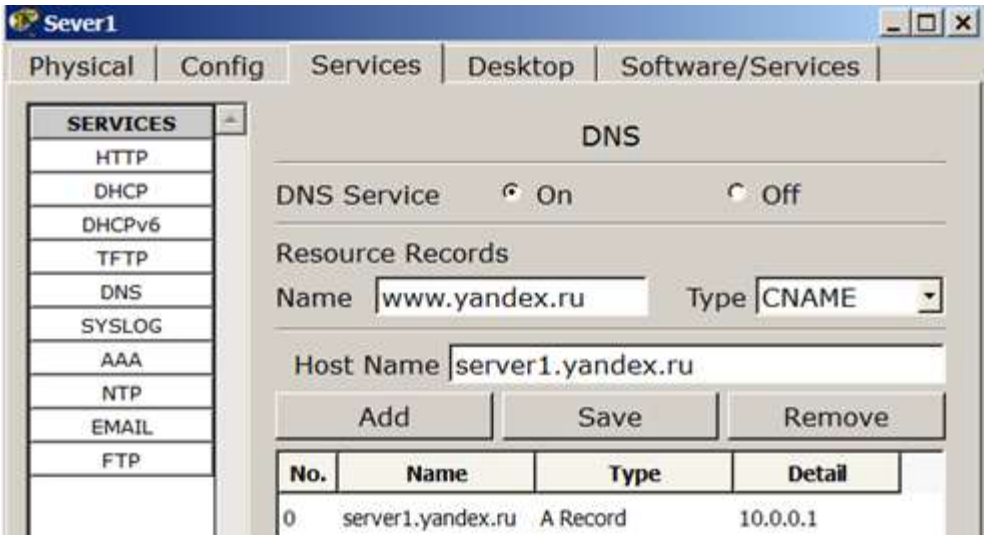


Рис. 5.10.Введення ресурсної записи типу CNAME

В результаті має вийти наступне (рис. 5.11).

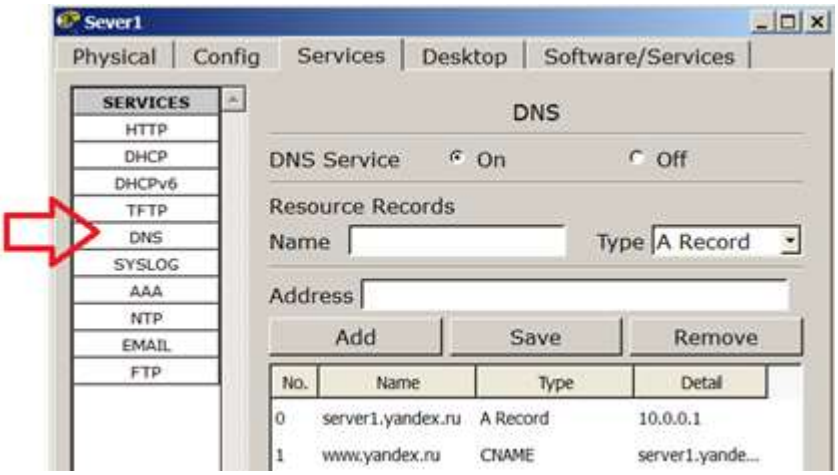


Рис. 5.11.Служба DNS в прямій зоні

Тепер налаштуємо службу HTTP. У конфігурації Server1 увійдіть вкладку HTTP і створіть стартову сторінку сайту (рис. 5.12).

```
<html>
<center><font size='+2' color='green'>Web Server</font></center>
www.yandex.ru
<p>
Hello!<br/>I am Server1
</html>
```

Рис. 5.12**.** Стартова сторінка сайту

Увімкніть командний рядок на Server1 і перевірте роботу служби DNS. Для перевірки правильності роботи прямої зони DNS сервера введіть команду ***SERVER> nslookup***. Якщо все правильно налаштовано, то отримаєте відгук на запит із зазначенням доменного імені DNS сервера в мережі і його IP адреси (рис. 5.13).

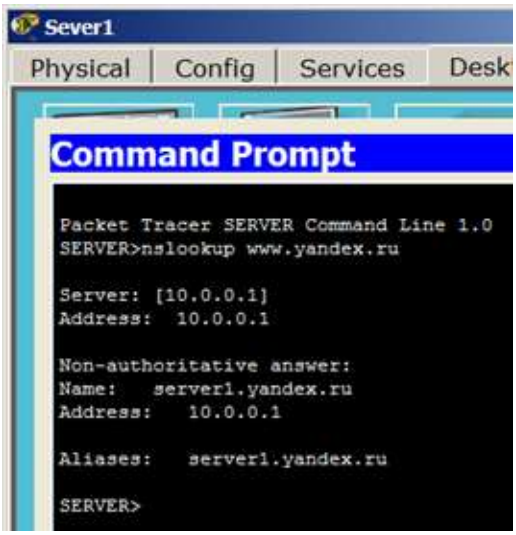


Рис. 5.13.Служба DNS в прямий зоні DNSна Server1 налаштована правильно

Команда **nslookup** служить для визначення ip-адреса по доменному імені (і навпаки).

Налаштування служби DHCP на Server2

Увійдіть в конфігурацію Server2 і на вкладці DHCP налаштуйте службу DHCP. Для цього наберіть нові значення пулу, встановіть перемикач **On** і натисніть на кнопку **Save** (Зберегти) -рис. 5.14.

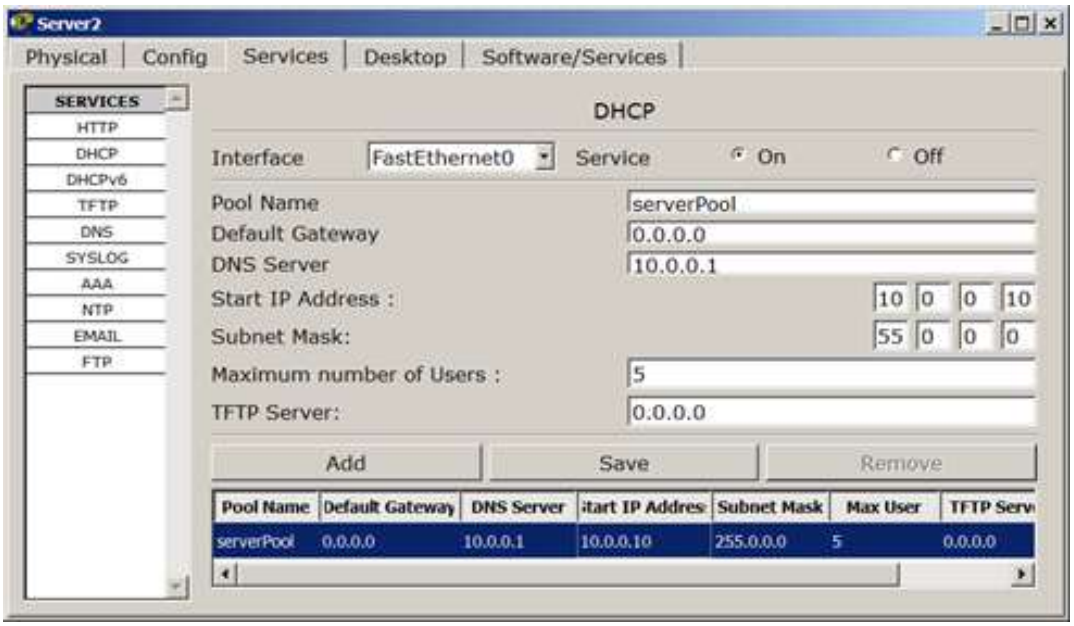


Рис. 5.14.Налаштування DHCP сервера.

Перевірка роботи клієнтів

Увійдіть в конфігурації хоста PC1і PC2 і в командному рядку налаштуйте протокол TCP / IP. Для цього командою PC> ipconfig / release скиньте (очистіть) старі параметри IP адреси(рис.5.15).

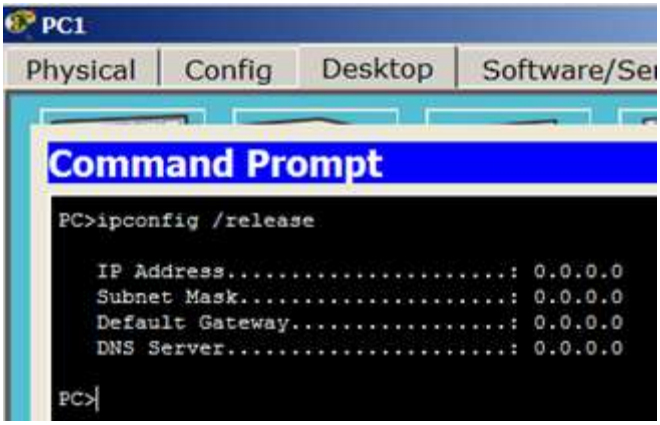


Рис. 5.15.Видалення конфігурації IP-адрес для всіх адаптерів

Команда ***ipconfig / release*** відправляє повідомлення **DHCP RELEASE** сервера DHCP для звільнення поточної конфігурації DHCP і видалення конфігурації IP-адрес для всіх адаптерів (якщо адаптер не заданий). Цей ключ відключає протокол TCP / IP для адаптерів, настроєних для автоматичного отримання IP-адрес.

Тепер командою ***PC> ipconfig / renew*** отримаєте нові параметри від DHCP сервера (рис. 5.16).

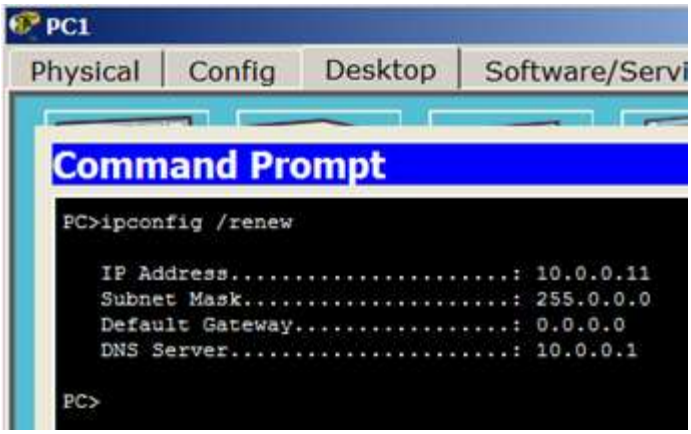


Рис. 5.16.Конфігурація протокол TCP/IP клієнта від DHCP сервера

Аналогічно зробіть для PC2 (рис. 5.17).

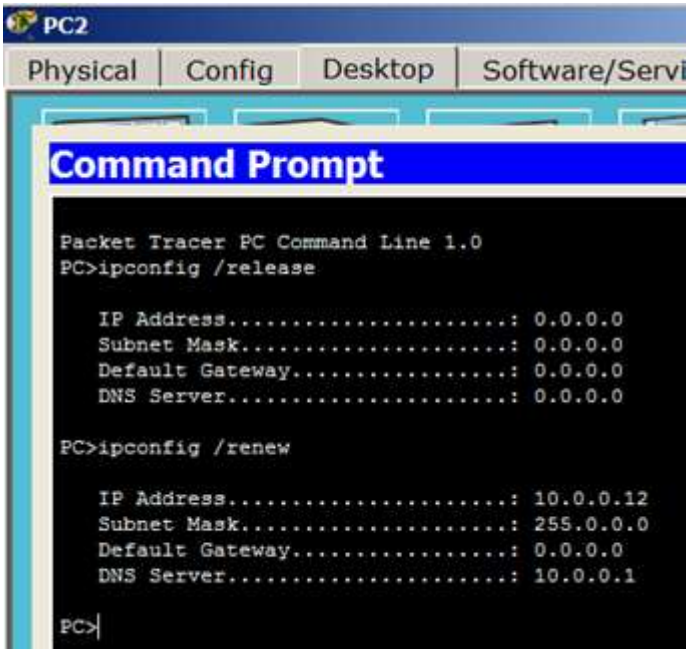


Рис.5.17.PC2 отримав IP адрес від DHCP сервера Server2

Залишилося перевірити роботу WEB сервера Server1 і відкрити сайт в браузері на PC1 або PC2 (рис. 5.18).

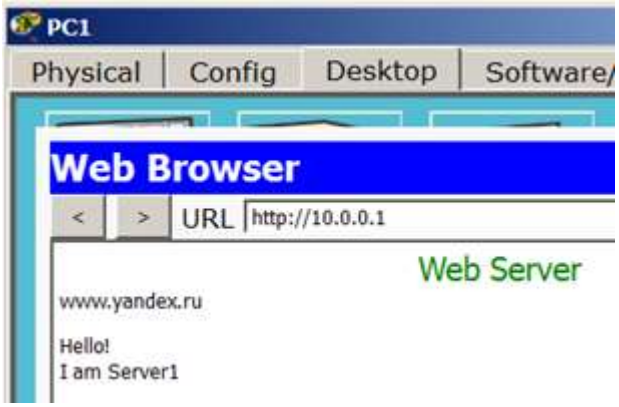


Рис. 5.18. Перевірка роботи служби HTTP на Server1

Приклади роботи маршрутизатора в ролі DHCP сервера

Маршрутизація (routing) - процес визначення маршруту проходження інформації в мережах зв'язку. Завдання маршрутизації полягає у визначенні послідовності транзитних вузлів для передачі пакета від джерела до адресата. ***Визначення*** маршруту слідування і просування ***IP-***пакетів виконують спеціалізовані мережеві пристрої - маршрутизатори. Кожен ***маршрутизатор*** має від двох і більше мережевих інтерфейсів, до яких підключені: *локальні мережі* або *маршрутизатори сусідніх мереж*.

Маршрутизатор (router, роутер) - мережевий пристрій третього рівня моделі OSI, що володіє як мінімум двома мережевими інтерфейсами, які знаходяться в різних мережах. Маршрутизатор може мати інтерфейси: для роботи по мідному кабелю, оптичному кабелю, так і по бездротових "лініях" зв'язку.

Вибір маршруту ***маршрутизатор*** здійснює на основі таблиці маршрутизації. Таблиці маршрутизації містять інформацію про мережі, і інтерфейсів, через які здійснюється підключення безпосередньо, а також містяться відомості про маршрутах або шляхах, за якими ***маршрутизатор*** зв'язується з віддаленими мережами, які не підключеними до нього

безпосередньо. Ці маршрути можуть призначатися адміністратором статично або визначатися динамічно за допомогою програмного протоколу маршрутизації. ***Таблиця*** маршрутизації містить набір правил - записів, що складаються з певних полів. Кожне правило містить наступні основні поля-компоненти:

- адрес IP-мережі отримувача,
- маску,
- адреса наступного вузла, якому слід передавати пакети,
- адміністративне відстань - ступінь довіри до джерела маршруту,
- метрику - деяку вагу - вартість маршруту,
- інтерфейс, через який будуть просуватися дані.

Приклад таблиці маршрутизації:

```
192.168.64.0/16 [110/49] via 192.168.1.2, 00:34:34, FastEthernet0/0.1

где 192.168.64.0/16 – сеть назначения,
    110/- административное расстояние
    /49 – метрика маршрута,
    192.168.1.2 – адрес следующего маршрутизатора, которому следует
                  передавать пакеты для сети 192.168.64.0/16,
    00:34:34 – время, в течение которого был известен этот маршрут,
    FastEthernet0/0.1 – интерфейс маршрутизатора, через который можно
                  достичь «соседа» 192.168.1.2.
```

Протокол ***DHCP*** є ***стандартний протокол***, який дозволяє серверу динамічно привласнювати клієнтам IP-адреси і відомості про конфігурацію. Ідея роботи ***DHCP*** сервісу така: на ПК задані настройки отримання ***ip адреси*** автоматично. Після включення і завантаження кожен ПК відправляє широкомовний ***запит*** в своїй мережі з питанням "Є тут ***DHCP сервер*** - мені потрібен ***ip адрес***?". Даний ***запит*** отримують всі комп'ютері в підмережі, але відповість на цей ***запит*** лише ***DHCP сервер***, який відправить комп'ютера вільний ***ip адрес*** з пулу, а також маску і ***адрес*** шлюзу. ***Комп'ютер*** отримує

параметри від ***DHCP*** сервера і застосовує їх. Після перезавантаження ПК знову відправляє широкомовний ***запит*** і може отримати інший ***ip адрес*** (перший вільний який знайдеться в пулі адрес на ***DHCP*** сервері).

Маршрутизатор можна конфігурувати як ***DHCP сервер***. Інакше кажучи, ви можете програмувати ***інтерфейс*** маршрутизатора на роздачу налаштувань для хостів. Системний адміністратор налаштовує на сервері ***DHCP*** параметри, які передаються клієнтові. Як правило, ***серверDHCP*** надає клієнтам щонайменше: ***IP-адрес***, маску підмережі і основний ***шлюз***. Однак надаються і додаткові відомості, такі, наприклад, як ***адрес*** сервера ***DNS***.

Завдання5.3.Конфігурування DHCP сервера на маршрутизаторі

Схема мережі приведена на рис. 5.19. За допомогою налаштувань ПК, представлених на малюнку, вказуємо хосту, що він повинен отримувати ***IP адрес, адреса*** основного шлюзу і ***адреса DNS*** сервера від ***DHCP*** сервера.

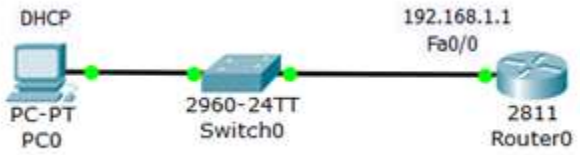


Рис. 5.19.Схема мережі

Зробимо налаштування R0:

Router (config)#ip dhcp pool TST створюємо*пулIP*адрес для*DHCP*сервера з іменем*TST*

Router (dhcp-config)#network 192.168.1.0 255.255.255.0 вказуємо з якої мережі ми будемо роздавати *IP* адреси (перший *параметр–адреса* данної мережі, а другий *параметр* – її *маска*)

Router (dhcp-config)#default-router 192.168.1.1вказуємо *адресу* основного

шлюзу, котрий буде розсилатись в повідомленнях *DHCP*

Router (dhcp-config)#dns-server 5.5.5.5 вказуємо *адресу DNS* сервера, котрий також буде розсилатись хостам в повідомленнях*DHCP*

Router (dhcp-config)#exit

Router (config)#ip dhcp excluded-address 192.168.1.1цей *хост* виключений з пула, тобто, ні один з хостів мережі не отримає від *DHCP* сервера цю *адресу*.

Повний лістинг цих команд наведено нарис. 5.20.

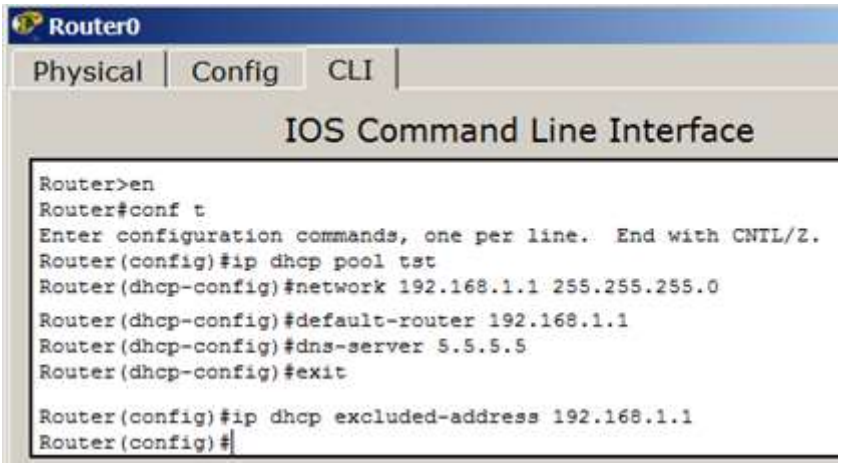


Рис. 5.20.Команди для конфігурування R0

Перевіримо результат отримання динамічних параметрів для PC0 (рис. 5.21).

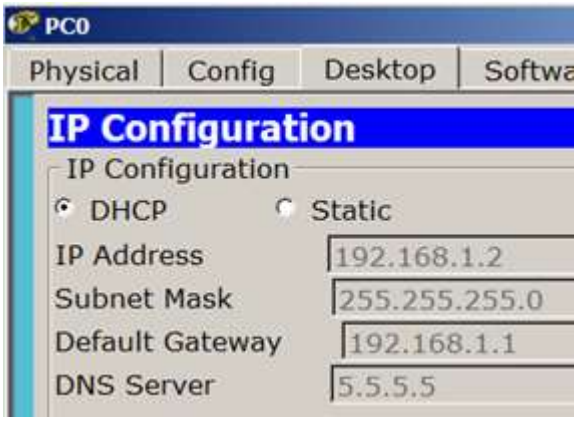


Рис.5.21.DHCP працює

Перевіримо працездатність DHCP сервера на хості PC0 командою **ip config/all** (рис. 5.22).

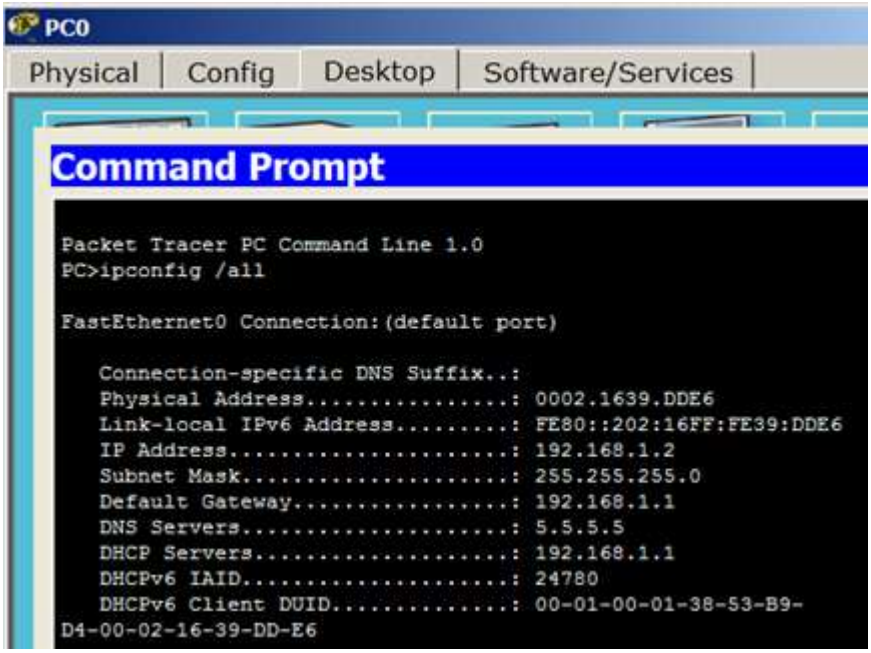


Рис. 5.22. Хост отримав налаштування від DHCP сервера

Хост успішно отримав *IP адресу*, *адреса* шлюза і *адреса DNS* сервера від *DHCP* сервера R0.

Завдання 5.4.Налаштування інтерфейсу маршрутизатора в якості DHCP клієнта

Схема мережі показана нарис. 5.23.

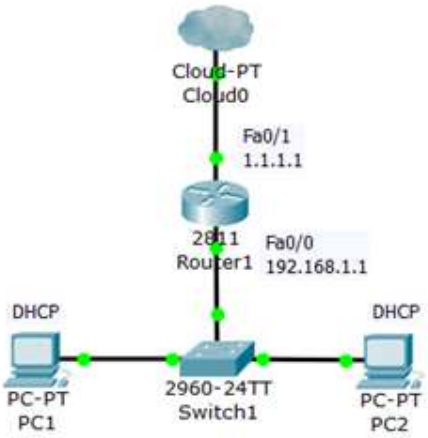


Рис. 5.23.Схема мережі

Конфігуруємо ***інтерфейс*** Fa0/0 для R1 (рис. 5.24).

Рис. 5.24. Конфігуруємо інтерфейс маршрутизатора

Спостерігаємо результат (рис. 5.25).

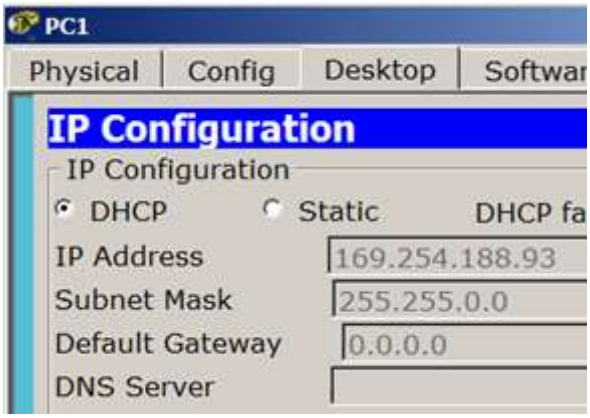


Рис. 5.25.DHCP не працює

Після налаштування інтерфейсу роутера на отримання налаштувань (настройок) по ***DHCP, DHCP*** клієнт на PC1 перестав отримувати ***IP-адресу*** - IP з діапазону 169.254.x.x / 16 призначається автоматично самим ПК при проблемах з отриманням адреси по ***DHCP***. ***Інтерфейс*** роутера ***IP-адреса*** так само не отримає тому, що в даній підмережі немає ***DHCP*** серверів.

Завдання 5.5. DHCP сервіс на маршрутизаторі 2811

У цьому завданні будемо конфігурувати ***маршрутизатор*** 2811, а саме, налаштовувати на ньому ***DHCP сервер***, який буде видавати по *DHCP* адреси з мережі 192.168.1.0 (рис. 5.26). PC1 і PC2 буду отримувати налаштування динамічно, а для сервера бажано мати постійну адресу, тобто, коли вона задана статично.

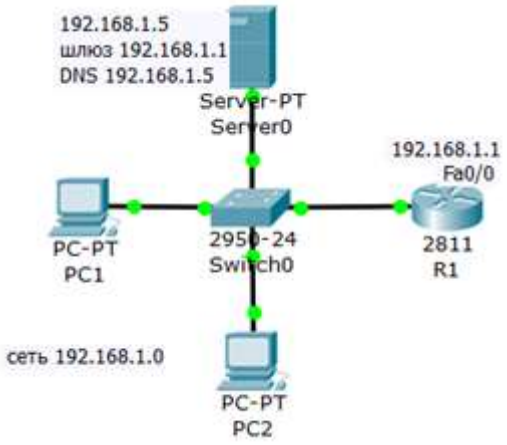


Рис. 5.26.Схема мережі

Примітка

Як пристрій з постійною адресою тут можна включити ще й принтер.

Резервуємо 10 адрес

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

Примітка

Цією командою зобов'язуємо маршрутизатор R1 не видавати адреси з 192.168.1.1 по 192.168.1.10 тому, що адреса 192.168.1.1 буде використовуватися самим маршрутизатором як шлюз, а решта адрес ми зарезервуємо під різні хости цієї мережі.

Таким чином, перша *DHCP адреса*, яка видасть R1 дорівнює **192.168.1.11**.

Створюємо пул адрес, які будуть видаватися з мережі 192.168.1.0

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

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

R1 (dhcp-config)#dns-server 192.168.1.5

Примітка

Згідно з цими налаштуваннями видавати адреси з мережі 192.168.1.0 (крім тих, що ми виключили) буде маршрутизатор R1 через шлюз 192.168.1.1.

Налаштовуємо інтерфейс маршрутизатора

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

Команда ***no shut*** *(скорочення від* ***no shutdown****) використовується для того, щоб б інтерфейс був активним. Зворотній команда* **- shut***, вимкне інтерфейс.*

Перевірка результату

Тепер обидва ПК отримали налаштування і командою R1#show ip dhcp binding можна подивитися на ***список*** виданих роутером адрес (рис. 5.27).

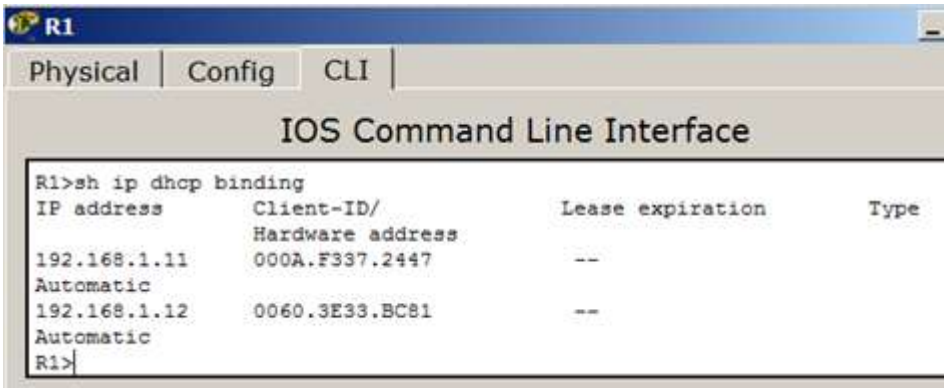


Рис. 5.27. Адреси видаються автоматично, починаючи з адресу 192.168.1.11

Бачимо, що протокол DHCP дозволяє виробляти автоматичну налаштування мережі на всіх комп'ютерах (рис. 5.28).

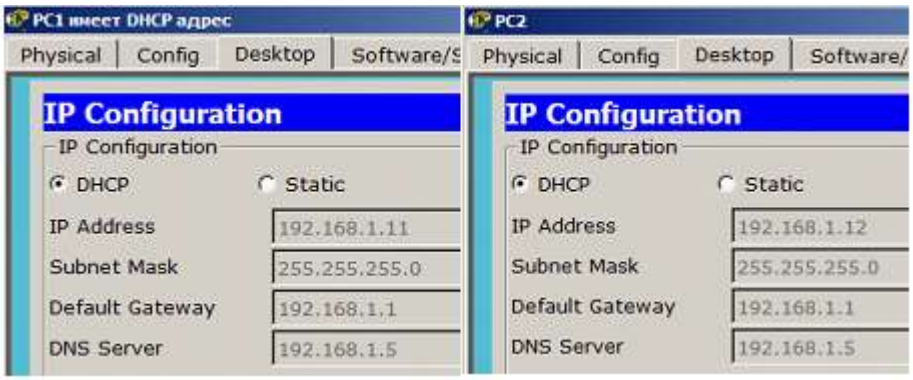


Рис. 5.28. PC1 и PC2 отримують IP адреси від DHCP сервера

Склад звіту лабораторної роботи

В звіті повинно бути відображено:

1. Тема роботи.
2. Мета роботи.
3. Виконання завдання 5.1 з відповідними скріншотами.
4. Виконання завдання 5.2 з відповідними скріншотами.
5. Виконання завдання 5.3 з відповідними скріншотами.

6. Виконання завдання 5.4 з відповідними скріншотами.
7. Виконання завдання 5.5 з відповідними скріншотами.
8. Висновки

Контрольні питання

1. Наведіть перелік параметрів IP-адресаціївузла.
2. Технології та протоколи динамічного призначення параметрів IP-адресації.
3. Технологія APIPA.
4. Загальна характеристика протоколу DHCP.
5. Ролі пристроїв у протоколіDHCP.
6. Наведіть характеристики протоколу DHCP стосовно моделі OSI та стеку TCP/IP.
7. Наведіть основні параметри адресації, які надаються мережному вузлу за протоколом DHCP.
8. Наведіть перелік та призначення способів призначення параметрів IP-адресації у протоколі DHCP.
9. Наведіть перелік та призначення основних повідомлень протоколу DHCP.
10. Які механізми (елементи) захисту мережі може надати протокол DHCP?
11. Наведіть перелік та призначення основних команд для налагодження DHCP-сервера на маршрутизаторі Cisco при умові динамічного призначення адрес.
12. Наведіть перелік та призначення основних команд для налагодження DHCP-сервера на маршрутизаторі Cisco при умові статичного призначенняадрес.

Лабораторна робота№ 6

Тема: ВИВЧЕННЯ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ НА ПРОТОКОЛАХ RIP, EIGRP І OSPF

***Мета заняття*:**вивчити принципи динамічної маршрутизації на протоколах RIP, EIGRP і OSPF,застосувати отримані знання при виконанні практичних завдань.

Теоретичні відомості

Маршрутизація - процес визначення в мережі найкращого шляху, по якому пакет може досягти адресата. ***Динамічна маршрутизація*** може бути здійснена з використанням одного і більше протоколів (*RIP v2, OSPF* і ін.).

Протокол маршрутизації – засіб комунікації між маршрутизаторами, який дозволяє пристроям сумісно використовувати інформацію про мережі та визначати відстань до різних вузлів та мереж. Інформація, яку один маршрутизатор отримує від другого (шляхом протоколу маршрутизації), використовується для побудови та підтримки в актуальному стані *таблиці маршрутизації*.

Динамічна маршрутизація

Динамічна маршрутизація— вид маршрутизації, при якому таблиця маршрутизації заповнюється і оновлюється автоматично за допомогою одного або декількох протоколів маршрутизації (RIP, OSPF, EIGRP, BGP).

Кожний*протокол маршрутизації* використовує свою систему оцінки маршрутів (метрику). Маршрут до мереж призначення будується на основі таких критеріїв як:

- кількість ретрансляційних переходів;
- пропускна здатність каналу зв'язку;
- затримки передачі даних;
- та ін.

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

Більшість алгоритмів маршрутизації може бути віднесено до однієї із двох категорій:

• ***дистанційно-векторний протокол (ДВП);***

• ***протокол з врахуванням стану каналу (ПСК).***

Дистанційно-векторний протокол визначає напрям або вектор та відстань до потрібного вузла об’єднаної мережі.

Прикладами таких протоколів є *RIP, IGRP, EIGRP, BGP*.

Деякий час протокол *EIGRP* вважався гібридним протоколом, оскільки поєднує у собі особливості обох алгоритмів: дистанційно-векторного та з врахуванням стану каналу, але на сьогоднішній день фірма *Cisco* відносить його до *ДВП.* Він має набагато кращі характеристики, ніж класичні *ДВП*.

Протокол з врахуванням стану каналу, який також ще називають алгоритмом вибору найкоротшого шляху (*shortest path first – SPF*), відтворює топологію усієї мережі. Приклади: *OSPF, IS-IS, NLSP*.

Концепція дистанційно-векторної маршрутизації

При використанні дистанційно-векторних алгоритмів між маршрутизаторами періодично пересилаються копії таблиць маршрутизації (ТМ). В таких регулярних оновленнях маршрутизатори повідомляють один

одного про зміни у топології мережі. Дистанційно-векторні алгоритми маршрутизації також називаються ще алгоритмами *Беллмана-Форда* (кожен маршрутизатор отримує *ТМ* від сусідніх маршрутизаторів).

В дистанційно-векторному алгоритмі накопичуються відстані в мережі, що дозволяє підтримувати базу даних *(БД),* яка містить інформацію про топологію мережі.

Однак дистанційно-векторні алгоритми не надають маршрутизаторам точну топологію всієї мережі, оскільки кожному маршрутизатору відомі лише сусідні (прилеглі) маршрутизатори.

Кожен маршрутизатор, що використовує дистанційно-векторну маршрутизацію, починає свою роботу з визначення сусідніх маршрутизаторів. Для кожного інтерфейсу безпосередньо під'єднаної мережі, вектор відстані встановлюється нульовим. В процесі розрахунку вектора відстані, маршрутизатори знаходять найкращий маршрут до сусідів-отримувачів на основі інформації, отриманої від сусідів.

Оновлення ТМ відбувається при зміні топології мережі. В міру формування векторів відстані зміни топології заносяться в ТМ наступних маршрутизаторів. Дистанційно-векторні алгоритми потребують, щоб кожен маршрутизатор пересилав всю ТМ кожному із своїх сусідів.

Протокол RIP

RIP — протокол дистанційно-векторної маршрутизації, який використовує для знаходження оптимального шляху ***алгоритм*** Беллмана-Форда. ***Алгоритм*** маршрутизації *RIP* - один з найпростіших протоколів маршрутизації. Кожні 30 секунд він передає в мережу свою таблицю маршрутизації. Основна відмінність протоколів в тому, що *RIPv2* (на відміну від *RIPv1*) може працювати по мультикаст, тобто, розсилаючи на мультикаст ***адресу***. Максимальна кількість "хопів" (кроків до місця призначення),

дозволене в *RIP1*, дорівнює 15 (***метрика*** 15). Обмеження в 15 хопів не дає застосовувати *RIP* в великих мережах, тому протокол найбільш поширений в невеликих комп'ютерних мережах. Друга версія протоколу - протокол *RIP2* була розроблена в 1994 році і є покращеною версією першого. У цьому протоколі підвищено безпеку за рахунок введення додаткової ***маршрутної*** інформації. Принцип дистанційно-векторного протоколу: кожен ***маршрутизатор***, який використовує протокол *RIP* періодично широкомовно розсилає своїм сусідам спеціальний *пакет-вектор*, що містить відстані (вимірюються в метриці) від даного ***маршрутизатора*** до всіх відомих йому мереж. ***Маршрутизатор*** отримав такий вектор, нарощує компоненти ***вектора*** на величину відстані від себе до даного сусіда і доповнює ***вектор*** інформацією про відомих безпосередньо йому самому мережах або мережах, про які йому повідомили інші маршрутизатори. Доповнений вектор ***маршрутизатор*** розсилає всім своїм сусідам. ***Маршрутизатор*** вибирає з кількох альтернативних маршрутів ***маршрут*** з найменшим значенням метрики, а ***маршрутизатор***, який передав інформацію про такий маршрут позначається як наступний (***next hop***). Протокол непридатний для роботи у великих мережах, так як засмічує мережу інтенсивним трафіком, а вузли мережі оперують тільки ***векторами***-відстаней, не маючи точної інформації про стан каналів і топології мережі. Сьогодні навіть в невеликих мережах ***протокол*** витісняється переважаючими його за можливостями протоколами *EIGRP і OSPF*.

Протокол EIGRP

Дистанційно-векторний протокол маршрутизації ***EIGRP (Enhanced Interior Gateway Routing Protocol)***був розроблений та реалізований фірмою Cisco у 1992 р.

Він є суттєвим вдосконаленням свого попередника - протоколу маршрутизації *IGRP*.

Переваги використання протоколу EIGRP:

- *швидка конвергенція.* На маршрутизаторах протоколу *EIGRP* конвергенція відбувається значно швидше, оскільки вона базується на сучасному алгоритмі дифузії поновлень маршрутизації *DUAL* (*Diffusing Update Algorithm*).

Цей алгоритм гарантує відсутність петель у кожний момент часу на всьому маршруті та дозволяє усім маршрутизаторам, що належать до даної топології, виконати одночасну синхронізацію. Крім того, якщо у традиційних дистанційно-векторних протоколів певний маршрут став недоступним, маршрутизатори повинні чекати чергового періодичного поновлення, а протокол *EIGRP* буде при цьому використовувати резервний шлях (якщо такий існує);

- *ефективне використання смуги пропускання*.

По-перше, протокол *EIGRP* використовує розсилання часткових, обмежених за обсягом поновлень (*Partial, bounded updates*) маршрутизації, і як наслідок цього забезпечується мінімальне використання такими поновленнями смуги пропускання в умовах стабільної роботи мережі. Маршрутизатори *EIGRP*, як правило, розсилають часткові, поетапні поновлення маршрутизації, а не повні таблиці маршрутизації. Цей процес аналогічний роботі протоколу *OSPF*, однак на відміну від нього, маршрутизатори протоколу *EIGRP* розсилають ці часткові поновлення не всім маршрутизаторам даної області, лише тим, яким вони дійсно потрібні. Саме тому такі поновлення називаються обмеженими. По-друге, у протоколі *EIGRP* замість регулярного розсилання поновлень маршрутизації маршрутизатори підтримують постійний контакт один з одним шляхом розсилання невеликих пакетів вітання. Хоча пакети вітання розсилаються регулярно, внаслідок невеликого розміру вони досить незначно використовують смугу пропускання (на відміну від протоколів *RIP* та *IGRP*, які розсилають сусіднім пристроям свою повну таблицю маршрутизації

кожні 30 або 90 секунд, відповідно);

- *підтримка масок підмереж змінної довжини VLSM* (*Variable-Length Subnet Mask*) і безкласової міждоменної маршрутизації CIDR (*Classless Interdomain Routing*). На відміну від протоколу IGRP, EIGRP забезпечує повну підтримку безкласового IP шляхом обміну масками підмереж у повідомленнях поновлення маршрутів. Це дозволяє мережевим проектувальникам максимально використовувати адресний простір;

- *підтримка декількох протоколів мережевого рівня.* Протокол *EIGRP* підтримує протоколи *IP, IPX* та *AppleTalk* шляхом використання залежних від протоколу модулів (protocol-dependent module, *PDM*);

- *використання складної та гнучкої метрики маршрутів.* Метрика протоколу *EIGRP*, на відміну від багатьох інших протоколів маршрутизації (крім протоколу *IGRP*), може враховувати одразу чотири показники (пропускна спроможність, час затримки, завантаженість та надійність каналу). При цьому адміністратор може задавати значимість кожного з цих показників.

Протокол EIGRP у своїй роботі використовує дані трьох таблиць: *маршрутизації, сусідніх пристроїв та топології*. Ці таблиці ще називають базами даних протоколу.

Таблиця сусідніх пристроїв.Кожний маршрутизатор *EIGRP* підтримує таблицю сусідніх пристроїв (*neighbor table*), в якій перераховані суміжні маршрутизатори. Для кожного протоколу (наприклад, *IP, IPX*), що підтримується протоколом *EIGRP*, є своя *таблиця сусідніх пристроїв* (*ТСП*). При виявленні нових сусідніх пристроїв їх адреси та інтерфейси заносяться у ці таблиці. Проглянути зміст ТСП можна за командою *show ip eigrp neighbors).*

При відправленні пакета привітання сусідній пристрій повідомляє час утримання, що вказує, як довго маршрутизатор розглядає свій сусідній пристрій як досяжний та працездатний. Якщо за період утримання від

маршрутизатора не надійшов пакет привітання, то вважається, що час утримання вичерпано. В такому випадку алгоритм *DUAL* інформується про зміну топології і повинен знову обчислити параметри нової топології.

Топологічна таблиця

Топологічна таблиця (topology table) містить всі *ТМ* протоколу *EIGRP*, наявні на пристроях даної автономної системи (проглянути зміст топологічної таблиці можна за командою *show ip eigrp topology*).

Алгоритм *DUAL* отримує інформацію з *ТСП* і топологічної таблиці (*ТТ*) та обчислює маршрути з найменшою оцінкою до кожного пункту призначення. Завдяки цьому маршрутизатори протоколу *EIGRP* можуть швидко визначити альтернативні маршрути та використати їх у разі потреби.

Первинний маршрут (*successor*) записується у *ТМ*, а його копія – у *ТТ*. Усі маршрутизатори *EIGRP* підтримують *ТТ* для кожного зконфігурованого мережевого протоколу. У цій таблиці містяться маршрути до усіх пунктів призначення, які стали відомі маршрутизатору.

Завдання на лабораторну роботу

Завдання 6.1. Налаштування протоколу RIP версії 2 для мережі з шести пристроїв.

Завдання 6.2. Провести конфігурування протоколу RIP версії 2 для мережі з чотирьох пристроїв.

Завдання 6.3. Конфігурування протоколу EIGRP.

Завдання 6.4. Конфігурування протоколу OSPF для 4-х пристроїв.

Завдання 6.5. Налаштування маршрутизації по протоколу OSPF для 6 пристроїв.

Завдання 6.1. Налаштування протоколу RIP версії 2 для мережі з шести пристроїв

Завдання - налаштувати маршрутизацію на схемі, представлену на рис. 6.1.

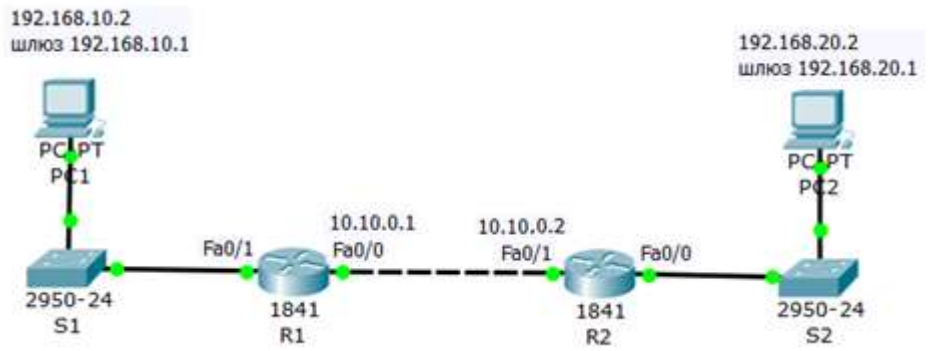


Рис. 6.1. Схема мережі

Примітка

Під час налаштування мережі не забувайте включати порти.

Налаштування протоколу RIP на маршрутизаторі R1

Увійдіть в конфігурації в консоль роутера і виконайте наступні налаштування (рис. 6.2).

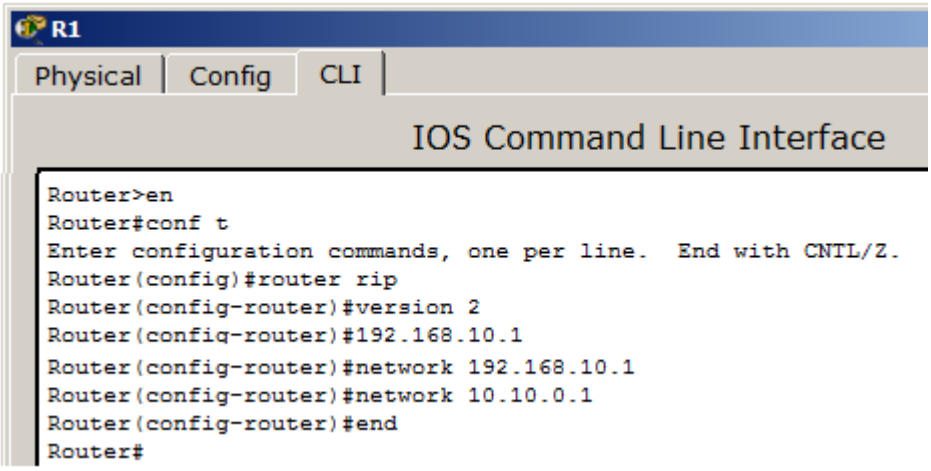


Рис. 6.2. Налаштування протокола RIPv2 на маршрутизаторі Router1

Примітка

Router (config)#router rip*(Вхід в режим конфігурування протоколу RIP).*

Router (config-router)#network 192.168.10.1 *(Підключення клієнтської мережі до роутера з боку комутатора S1).*

Router (config-router)#network 192.168.20.1*(Підключення другої мережі, тобто мережі між роутерами).*

Router (config-router)#version 2 *(Завдання використання другої версії протокол RIP).*

Налаштування протоколу RIP на маршрутизаторі R2

Увійдіть в конфігурації роутера 2 і виконайте наступні налаштування (рис. 6.3).

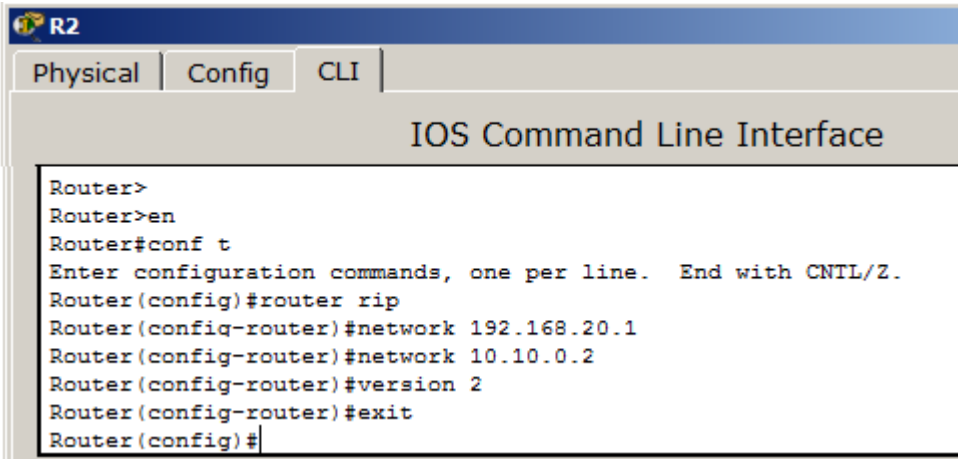


Рис. 6.3. Налаштування протокола RIPv2 на маршрутизаторі R2

Перевіряємо налаштування комутаторів і протоколу RIP

Подивимося налаштування протоколу RIPv2 на маршрутизаторах R1 і R2 (рис. 6.4).

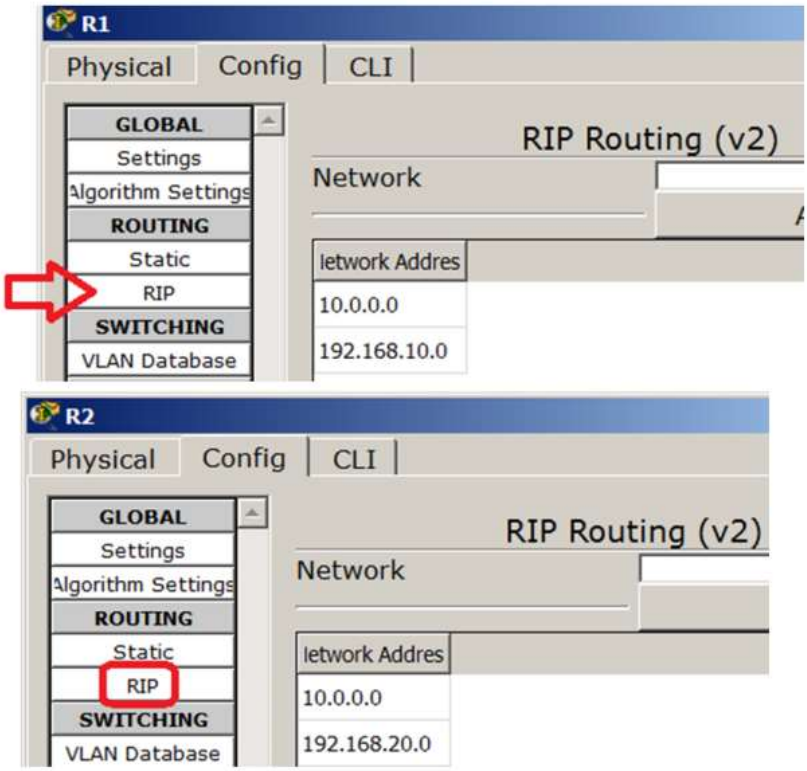


Рис. 6.4. Налаштування маршрутизаторів R1 і R2

Щоб переконатися в тому, що маршрутизатори дійсно правильно сконфігуровані і працюють коректно, перегляньте таблицю RIP роутерів, використовуючи команду: **Router # show ip route rip** (рис. 6.5 і рис. 6.6).

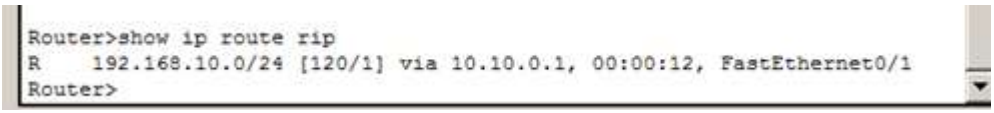


Рис. 6.5. Таблиця маршрутизації R1

Дана таблиця показує, що до мережі 192.168.10.0 є тільки один маршрут: через R1(мережа 10.10.0.1).

Рис. 6.6.Таблиця маршрутизації R2

Дана таблиця показує, що до мережі 192.168.20.0 є тільки один маршрут: через R2 (мережа 10.10.0.2).

Перевірка зв'язку між PC1 і PC2

Перевіримо, що маршрутизація проводиться вірно (рис. 6.7).

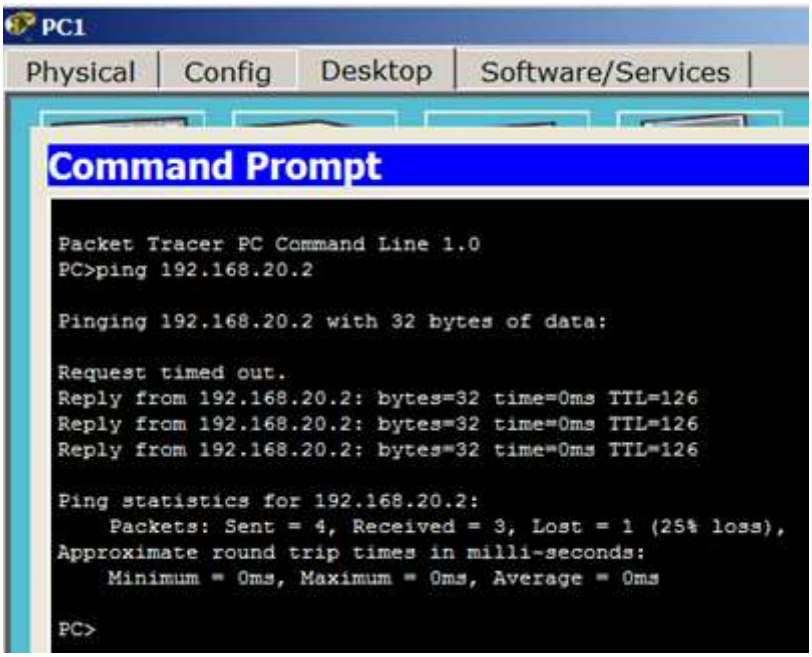


Рис. 6.7.Пінг з PC1 на PC2

Завдання 6.2. Провести конфігурування протоколу RIP версії 2 для мережі з чотирьох пристроїв (схема на рис.6.8)

Завдання 6.3. Конфігурування протоколу EIGRP

Схема мережі зображена на рис. 6.8.

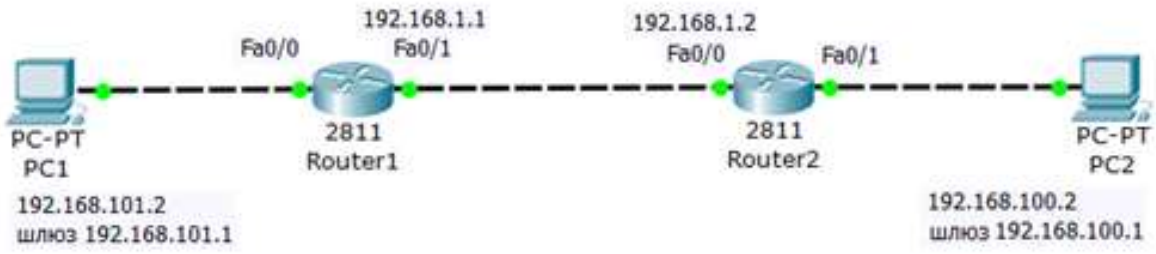


Рис. 6.8. Схема для конфігурації протоколу EIGRP

Налаштування протоколу *EIGRP* дуже схоже на налаштування протоколу *RIP*.

Програмування R1

Конфігуруємо R1 (рис.6.9).

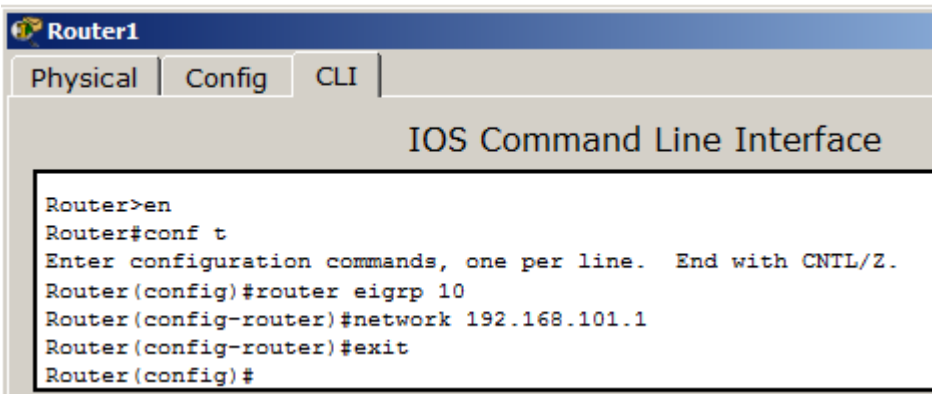


Рис. 6.9. Конфігурування R1

Програмування R2

Конфігуруємо R2 (рис. 6.10).

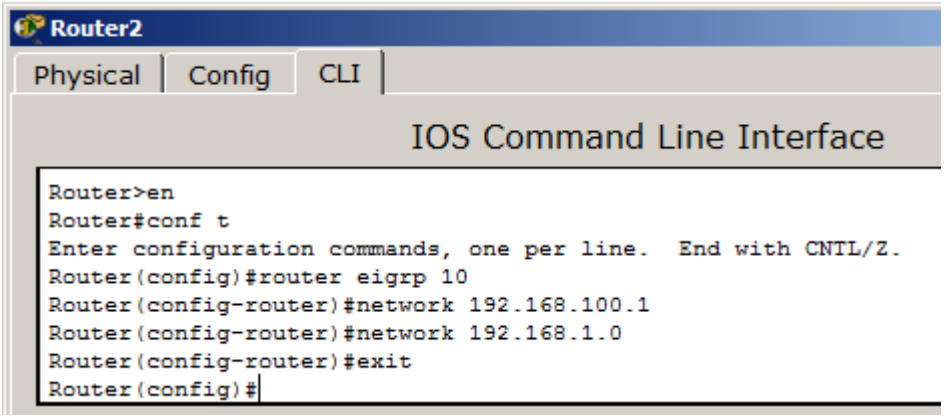


Рис. 6.10. Конфігурування R2

Перевірка роботи мережі

Перевіряємо роботу маршрутизаторів (рис. 6.11).

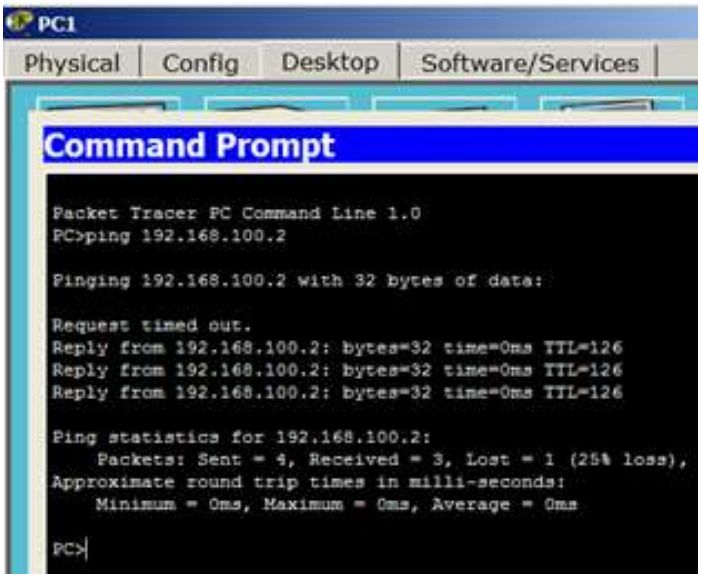


Рис. 6.11. Результат перевірки роботоспроможностімережі

Алгоритм вибору маршруту за станом каналу

Другим базовим алгоритмом маршрутизації є алгоритм вибору маршруту за станом каналу. Такі алгоритми відомі, як алгоритми **Дейкстри** або ***алгоритми вибору найкоротшого шляху (Shortest Path First).*** Вони підтримують складну базу топологічної інформації. Тоді як дистанційно-векторні алгоритми не містять певної інформації про віддалені мережі та

маршрутизатори, алгоритми з використанням стану каналу підтримують повну інформацію про віддалені маршрутизатори та їх з’єднання. Під час маршрутизації за станом каналу використовуються:

- анонси стану каналу – *(Link-State Advertisement LSA).* Це невеликі пакети, що містять інформацію про маршрути, що розсилаються між маршрутизаторами;

- топологічна база даних *(Topological Database).* Ця база містить інформацію, отриману в повідомленнях LSA;

- алгоритм вибору найкоротшого шляху *(Shortest Path First).* Відповідний алгоритм здійснює обчислення над базою даних, результатом якого є побудова зв’язного дерева протоколу SPF;

- таблиця маршрутизації *(Routing Table).* Ця таблиця містить відомі маршрути та відповідні їм інтерфейси.

Маршрутизатори обмінюються повідомленнями *LSA*, починаючи з безпосередньо під’єднаних мереж. Кожен маршрутизатор паралельно з іншими створює топологічну *БД,* яка складається з інформації, що отримана з цих повідомлень. Якщо маршрутизатор взнає про зміну стану каналу, він розсилає цю інформацію всім іншим маршрутизаторам об’єднаної мережі, щоб вони могли її використовувати для маршрутизації.

Протокол OSPF

Алгоритм роботи протоколу динамічної маршрутизації *OSPF* заснований на використанні усіма маршрутизаторами єдиної ***базиданих***, яка описує, з якими мережами пов'язаний кожен ***маршрутизатор***. Описуючи кожну ***зв'язок***, маршрутизатори пов'язують з нею метрику - ***значення***, що характеризує "якість" каналу зв'язку. Це дозволяє маршрутизаторів *OSPF* (на відміну від *RIP*, де всі канали рівнозначні) враховувати реальну пропускну

здатність каналу і виявляти найкращі маршрути.

OSPF (Open Shortest Path First) - протокол динамічної маршрутизації, заснований на технології відстеження стану каналу link-state (*LSA*). Заснований на алгоритмі для пошуку найкоротшого шляху. Відстеження стану каналу вимагає відправки оголошень про стан каналу (*LSA*) на активні інтерфейси всіх доступних маршрутизаторів зони. У цих оголошеннях міститься опис усіх каналів маршрутизатора і ***вартість*** кожного каналу. *LSA* повідомлення відправляються, тільки якщо відбулися які-небудь зміни в мережі, але раз в 30 хвилин LSA повідомлення відправляються в примусовому порядку. Протокол реалізує ***поділ*** автономної системи на зони (*areas*). Використання зон дозволяє знизити навантаження на ***мережу*** і процесори маршрутизаторів і зменшити розмір таблиць маршрутизації.

Опис роботи протокола

Всі маршрутизатори обмінюються спеціальними *Hello-пакетами* через всі інтерфейси, на яких активований протокол *OSPF*. Таким чином, визначаються маршрутизатори-сусіди, що розділяють загальний ***канал передачі даних***. Надалі *hello*-пакети надсилаються з інтервалом раз в 30 секунд. Маршрутизатори намагаються перейти в стан сусідства зі своїми сусідами. Перехід в даний стан визначається типом маршрутизаторів і типом мережі, по якій відбувається обмін hello-пакетами, за зонною ознакою. Пара маршрутизаторів в стані сусідства синхронізує між собою базу даних стану каналів. Кожен ***маршрутизатор*** посилає оголошення про стан каналу своїм сусідам, а кожен отримуючий таке оголошення записує інформацію в базу даних стану каналів і розсилає копію оголошення іншим своїм сусідам. При розсилці оголошень по зоні, всі маршрутизатори будують ідентичну базу даних стану каналів. Кожен ***маршрутизатор*** використовує ***алгоритмSPF*** для обчислення графа (дерева найкоротшого шляху) без петель. Кожен

маршрутизатор будує власну маршрутизацію, грунтуючись на побудованому дереві найкоротшого шляху.

Пряма ізворотня маска

В обладнанні **Cisco** іноді доводиться використовувати зворотну маску, тобто не звичну нам **255.255.255.0** (***Subnet mask*** - пряма маска), а **0.0.0.255** (***Wildcard mask*** - зворотна маска). Зворотна***маска*** використовується в листах допуску (***access list***) і при описі мереж в протоколі **OSPF**. Пряма ***маска*** використовується у всіх інших випадках. Відмінність масок полягає також в тому, що пряма ***маска*** оперує мережами, а зворотна - хостами. За допомогою зворотної маски ви можете, наприклад, виділити в усіх підмережах хости з конкретною адресою і дозволити їм ***доступ в Інтернет***. Так, як найчастіше за все в локальних мережах використовують адреси типу 192.168.1.0 з маскою 255.255.255.0, то найпоширеніша Wildcard mask (шаблонна ***маска*** або зворотна ***маска***, або інверсна ***маска***) – маска 0.0.0.255

Шаблонна маска (***wildcard mask***) - маска, яка вказує на кількість хостів мережі. Є доповненням для маски підмережі. Обчислюється за формулою для кожного з октетів маски підмережі як 255-маска підмережі. Наприклад, для мережі 192.168.1.0 і маскою підмережі 255.255.255.242 шаблонна маска буде виглядати як 0.0.0.13. Шаблонна маска використовується в налаштуванні деяких протоколів маршрутизації, а також є зручним параметром обмежень в списках доступу.

Розрахунок Wildcard mask

Існує ***зв'язок***, між зворотною та ***прямою*** маскою: в сумі ці маски по кожному розряду ***повинні*** складати 255. Нехай наша ***мережа*** 192.168.32.0 / 28. Розрахує *wildcard mask*: ***префікс*** / 28 це 255.255.255.240 або 11111111.11111111.11111111.11110000. Для w*ildcard mask* нам потрібні тільки нулі, тобто, 11110000 переводимо в десяткове число і вважаємо:

128/64/32/16/8/4/2/1 це буде 8 + 4 + 2 + 1 = 15, тобто наша *wildcard mask* буде дорівнює 0.0.0.15.

Самостійно

Дана пряма *маска* **255.255.255.248**. Виконайте розрахунок і доведіть, що зворотна дорівнює **0.0.0.7**.

Завдання 6.4. Конфігурування протоколу OSPF для 4-х пристроїв

Зберіть схему, зображену на рис. 6.12.

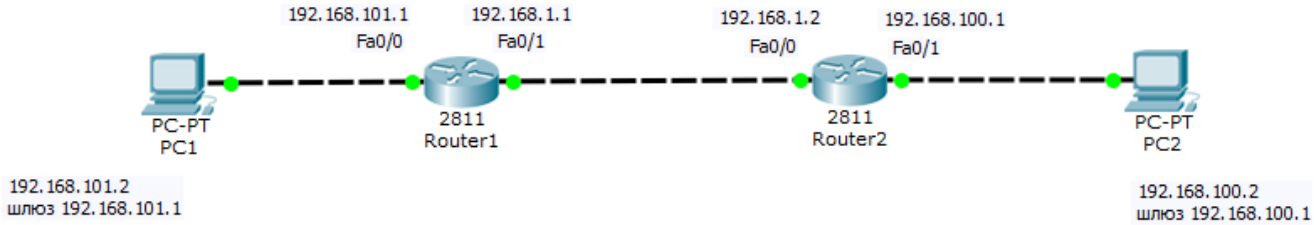


Рис.6.12.Схема для конфігурації протоколу OSPF

Налаштування роутерів

Виконаємо конфігурування R1 (рис. 6.13).

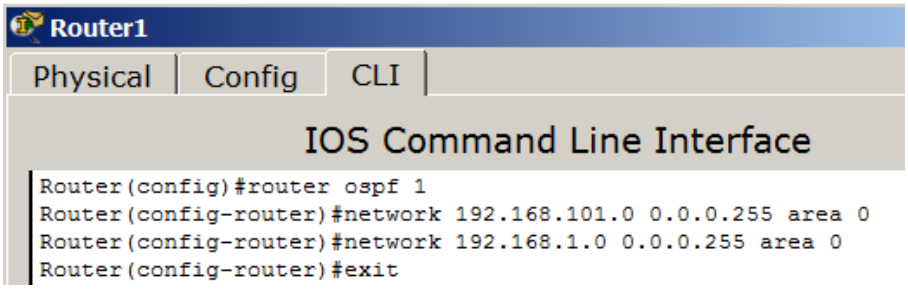


Рис. 6.13.Налаштування R1

Тепер виконаємо налаштування R2 (рис. 6.14).

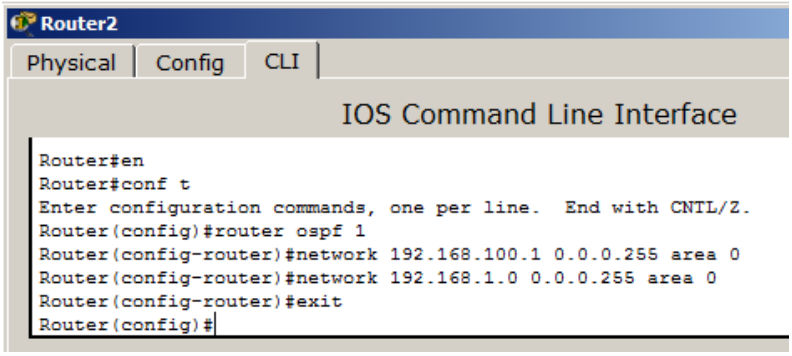


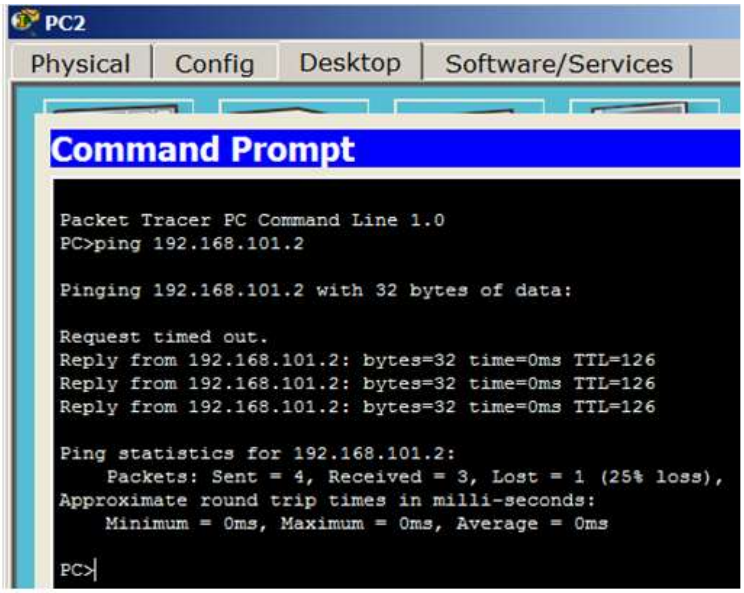
Рис. 6.14.Налаштування R2

Порада

Якщо буде потрібно в CPT скинути налаштування роутера, то слід вимкнути його тумблер живлення, а потім знову включити.

Перевірка результату

Для перевірки маршрутизації пропінгуємо ПК з різних мереж (рис. 6.15).



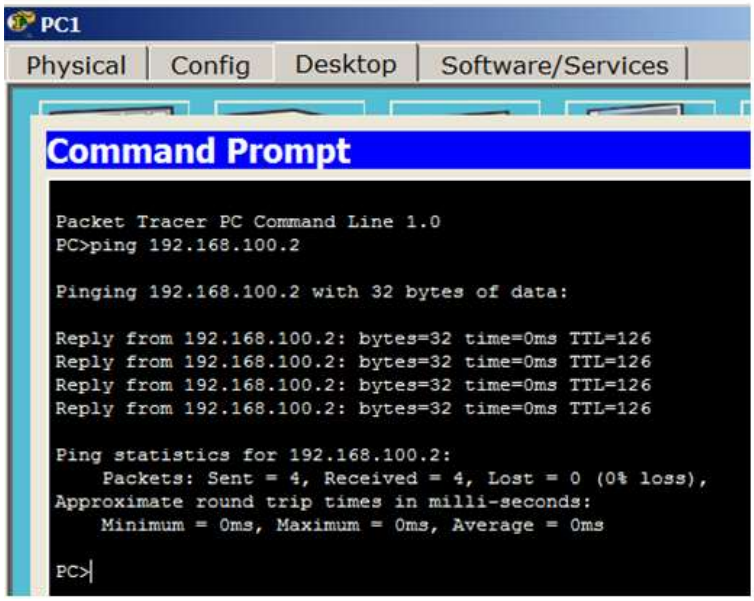


Рис. 6.15.Результат перевірки працездатності OSPF

Завдання 6.5. Налаштування маршрутизації по протоколу OSPF для 6 пристроїв

Побудуйте наступну схему(рис. 6.16).

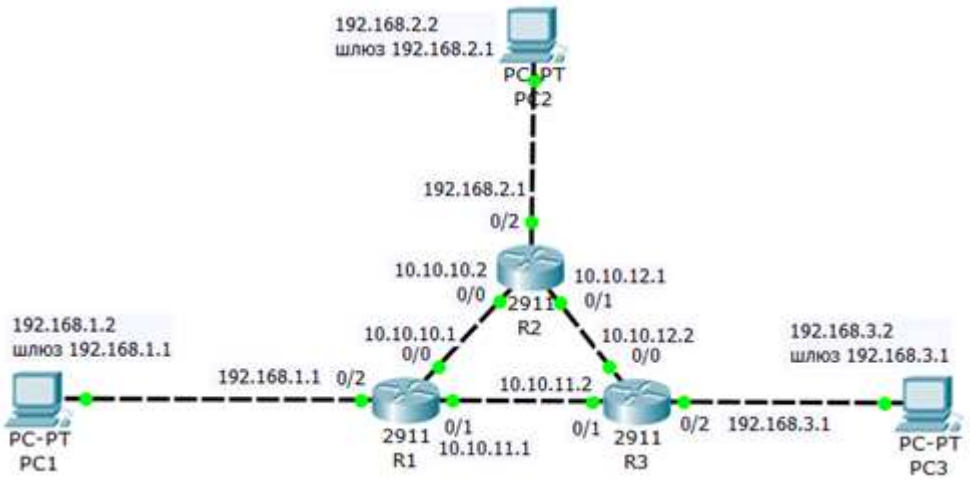


Рис. 6.16. Початкова схема мережі для нашої роботи

Мета роботи - налаштувати маршрутизацію в даній мережі по протоколу OSPF.

Налпштування loopback інтерфейс на R1

На R1 налаштуємо програмний **loopback інтерфейс** - алгоритм, який направляє отриманий сигнал (або дані) назад відправнику (рис. 6.17).

Примітка

*IPv4-адреса, призначена loopback-інтерфейсу, може бути необхідна для процесів маршрутизатора, в яких використовується IPv4-адрес інтерфейсу з метою ідентифікації. Один з таких процесів - алгоритм найкоротшого шляху (**OSPF**). При включенні інтерфейсу loopback для ідентифікації маршрутизатор буде використовувати завжди доступну адресу інтерфейсу loopback, а не IP-адреса, призначена фізичному порту, робота якого може бути порушена. На маршрутизаторі можна активувати кілька інтерфейсів loopback. IPv4-адреса для кожного інтерфейсу loopback повинна бути унікальною і не має бути задіяна іншим інтерфейсом.*

Рис. 6.17.Налаштовуємо інтерфейс *loopback* на R1

Налаштовуємо протокол OSPF на R1

Включаємо OSPF на R1, всі маршрутизатори повинні бути в одній зоні **area 0** (рис. 6.18).

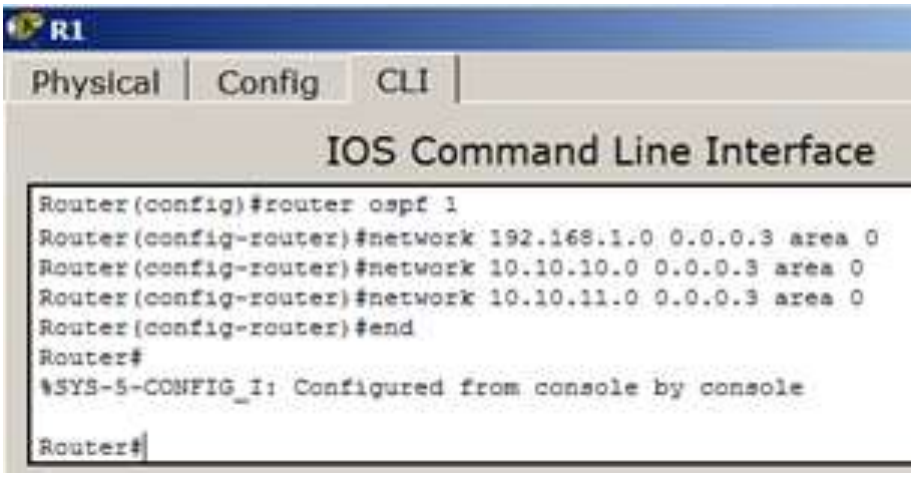
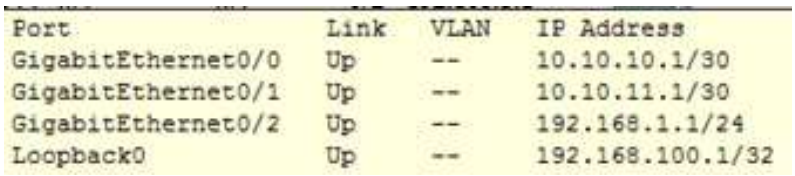


Рис. 6.18.Включаємо протокол OSPF на R1

Підводимо курсор миші до R1 і спостерігаємо результат наших налаштувань (рис. 6.19).



Port	Link	VLAN	IP Address
GigabitEthernet0/0	Up	--	10.10.10.1/30
GigabitEthernet0/1	Up	--	10.10.11.1/30
GigabitEthernet0/2	Up	--	192.168.1.1/24
Loopback0	Up	--	192.168.100.1/32

Рис. 6.19.Маршрутизатор R1 налаштований

Примітка
Зверніть увагу, що фізично порта 192.168.100.1 немає, він існує тільки логічно (програмно).

Налаштуємо loopback інтерфейс на R2

На R2 налаштуємо програмний loopback інтерфейс за аналогією з R1 (рис. 6.20).

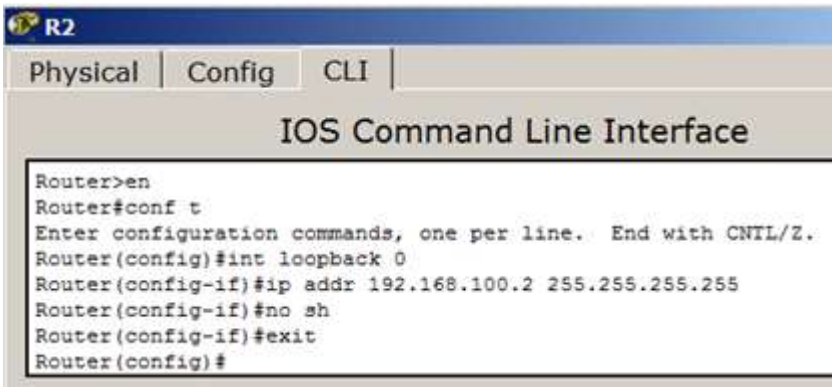


Рис. 6.20.Налаштуємо логічний інтерфейс loopback на R2

Налаштуємо OSPF на R2

Включаємо протокол OSPF на R2, все маршрутизатори повинні бути в одній зоні area 0 (рис. 6.21).

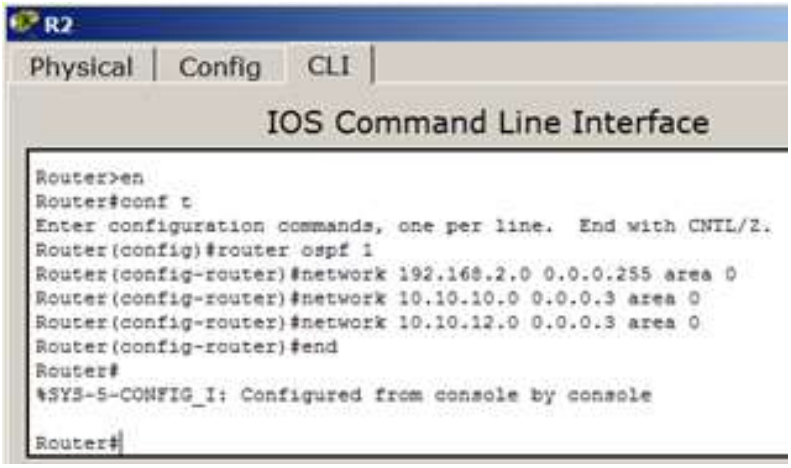
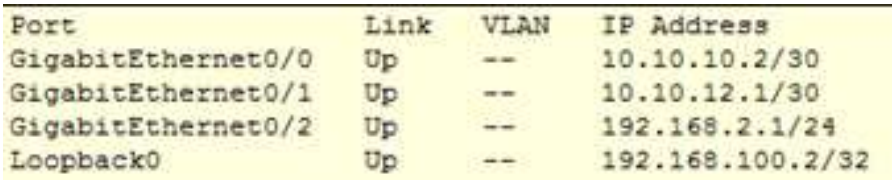


Рис. 6.21. Включаємо протокол OSPF на R2

Підводимо курсор миші до R2 і спостерігаємо результат наших налаштувань (рис. 6.22).



Port	Link	VLAN	IP Address
GigabitEthernet0/0	Up	--	10.10.10.2/30
GigabitEthernet0/1	Up	--	10.10.12.1/30
GigabitEthernet0/2	Up	--	192.168.2.1/24
Loopback0	Up	--	192.168.100.2/32

Рис. 6.22.Маршрутизатор R2 налаштований

Налаштуємо loopback інтерфейс на R3

Робимо все аналогічно (рис. 6.23).

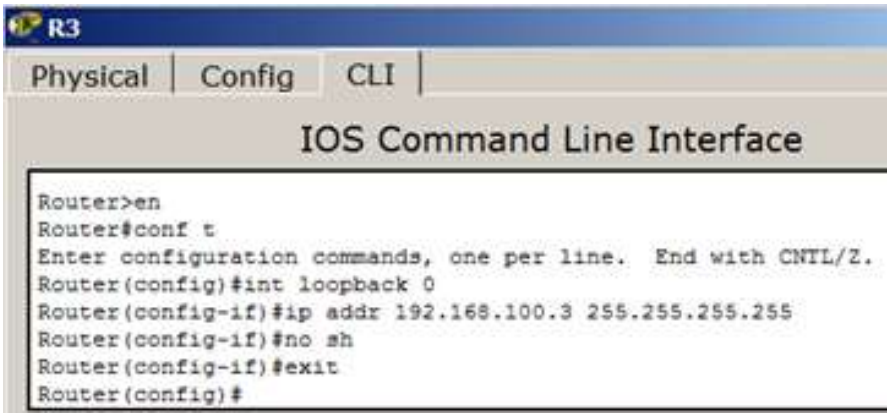


Рис. 6.23.Налаштуємо логічний інтерфейс *loopback* на R3

Налаштуємо протокол OSPF на R3

Тут робимо все, як раніше (рис. 6.24).

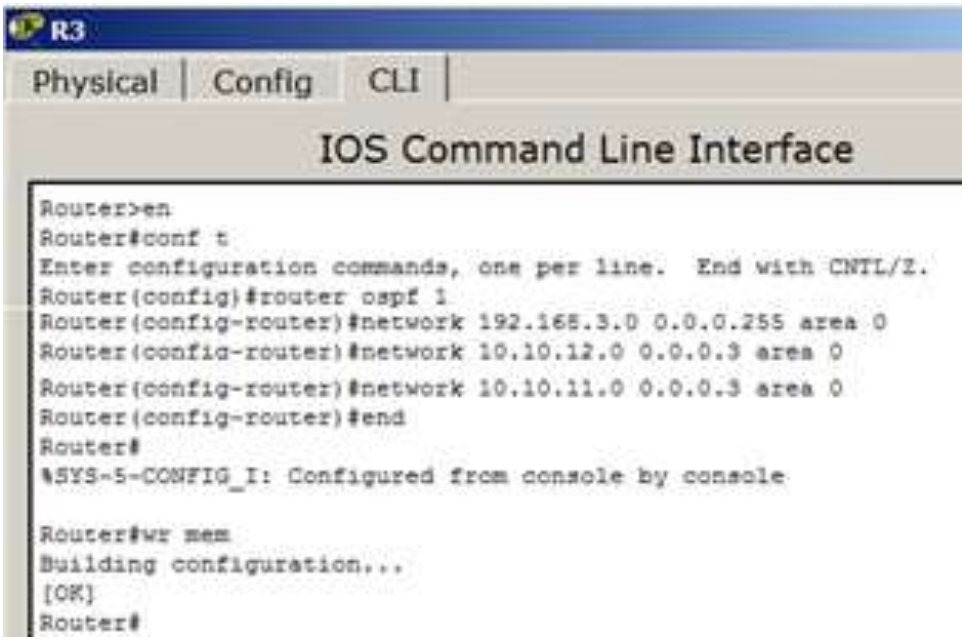


Рис. 6.24.Включаємо протокол OSPF на R2

Перевіряємо результат (рис. 6.25).

Port	Link	VLAN	IP Address
GigabitEthernet0/0	Up	--	10.10.12.2/30
GigabitEthernet0/1	Up	--	10.10.11.2/30
GigabitEthernet0/2	Up	--	192.168.3.1/24
Loopback0	Up	--	192.168.100.3/32

Рис. 6.25.Маршрутизатор R3 налаштований

Перевіряємо роботу мережі

Впевнюємося, що роутер R3 бачить R2 і R1 (рис. 6.26).

```
R3
Physical | Config | CLI
IOS Command Line Interface
Router#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
Interface
192.168.100.2     1   FULL/BDR        00:00:31    10.10.12.1
GigabitEthernet0/0
192.168.100.1     1   FULL/BDR        00:00:31    10.10.11.1
GigabitEthernet0/1
Router#
```

Рис. 6.26.Роутер R3 бачить своїх сусідів

Тепер подивимось таблицю маршрутизації для R3 (рис. 6.27).

```
R3
Physical | Config | CLI
IOS Command Line Interface
Router#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O       10.10.10.0/30 [110/2] via 10.10.11.1, 01:09:30,
GigabitEthernet0/1
                      [110/2] via 10.10.12.1, 01:09:30,
GigabitEthernet0/0
C       10.10.11.0/30 is directly connected, GigabitEthernet0/1
L       10.10.11.2/32 is directly connected, GigabitEthernet0/1
C       10.10.12.0/30 is directly connected, GigabitEthernet0/0
L       10.10.12.2/32 is directly connected, GigabitEthernet0/0
O    192.168.1.0/24 [110/2] via 10.10.11.1, 01:09:30, GigabitEthernet0/1
O    192.168.2.0/24 [110/2] via 10.10.12.1, 01:09:30, GigabitEthernet0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/2
L       192.168.3.1/32 is directly connected, GigabitEthernet0/2
 --More--
```

Рис. 6.27.Таблиця маршрутизації для R3

Примітка

У цій таблиці запис з буквою "O" говорить про те, що даний маршрут прописаний протоколом OSPF. Ми бачимо, що мережа 192.168.1.0 доступна для R3 через адреса 10.10.11.1 (це порт gig0 / 1 маршрутизатора R1). Аналогічно, мережа 192.168.2.0 доступна для R3 через адреса 10.10.12.1 (це порт gig0 / 1 маршрутизатора R2).

Тепер перевіряємо доступність різних мереж (рис. 6.28).

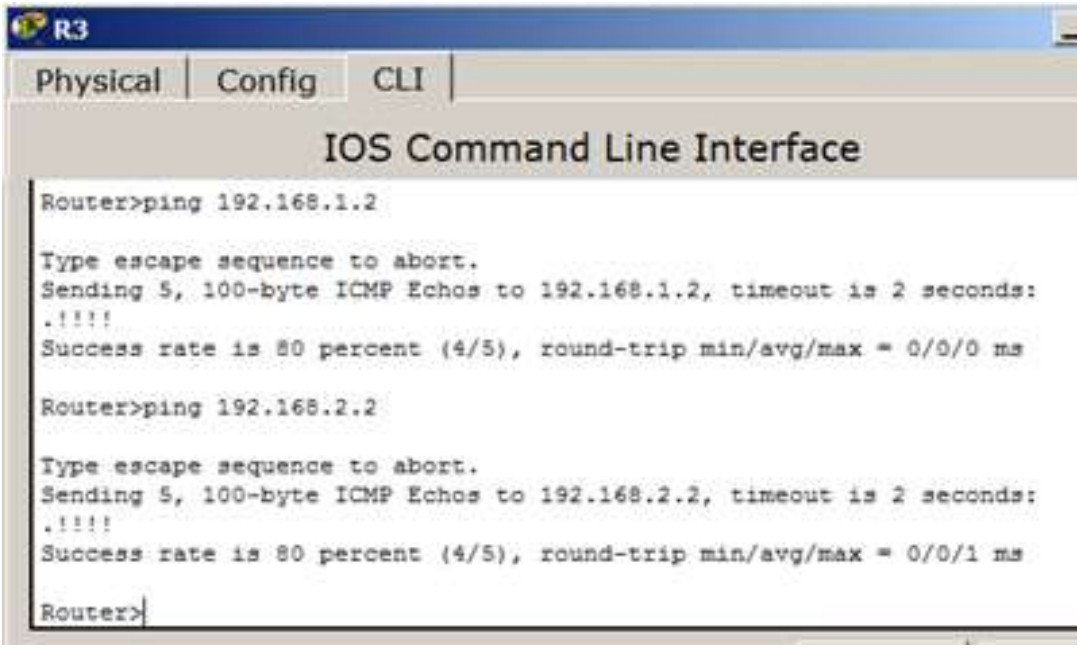


Рис. 6.28.Мережі 192.168.1.0 і 192.168.2.0 доступні

Склад звіту лабораторної роботи

В звіті повинно бути відображено:

1. Тема роботи.
2. Мета роботи.
3. Виконання завдання 6.1 з відповідними скріншотами.
4. Виконання завдання 6.2 з відповідними скріншотами.
5. Виконання завдання 6.3 з відповідними скріншотами.
6. Висновки

Контрольні питання

1. Наведіть визначення поняття «маршрутизація».
2. Наведіть визначення поняття «протокол маршрутизації».
3. На яких критерія базується побудова маршруту до мереж призначення.
4. Динамічна маршрутизація.
5. Категорії алгоритмів маршрутизації
6. Дистанційно-векторний протокол.
7. Протокол з врахуванням стану каналу.
8. Концепція дистанційно-векторної маршрутизації
9. Алгоритм вибору маршруту за станом каналу
10. Протокол RIP.
11. Протокол OSPF.
12. Протокол EIGRP. Особливості роботи.
13. Переваги протоколу EIGRP.
14. Таблиці протоколу EIGRP.

Лабораторна робота № 7

Тема: СТВОРЕННЯ СПИСКІВ ДОСТУПУ ACL

***Мета заняття*:** вивчити принципи побудови списків доступу, застосувати отримані знання при виконанні практичних завдань.

Теоретичні відомості

ACL (Access Control List) - це набір текстових виразів, які щось дозволяють, або щось забороняють. Зазвичай ACL дозволяє або забороняє IP-пакети, але крім усього іншого він може заглядати всередину IP-пакета, переглядати тип пакету, TCP і UDP порти. Також ACL існує для різних мережевих протоколів (IP, IPX, AppleTalk і так далі). В основному застосування списків доступу розглядають з точки зору пакетної фільтрації, тобто пакетна фільтрація необхідна в тих ситуаціях, коли у вас коштує обладнання на кордоні Інтернет і вашої приватної мережі і потрібно відфільтрувати непотрібний трафік.

Розміщується ACL на вхідному напрямку і блокує надлишкові види трафіку.

Функціонал ACL складається в класифікації трафіку, потрібно його перевірити спочатку, а потім щось з ним зробити в залежності від того, куди ACL застосовується. ACL застосовується скрізь, наприклад:

- На інтерфейсі: пакетна фільтрація
- На лінії Telnet: обмеження доступу до маршрутизатора
- VPN: який трафік потрібно шифрувати
- QoS: який трафік обробляти в першу чергу
- NAT: які адреси транслювати

Для застосування ACL для всіх цих компонентів потрібно зрозуміти як вони працюють. І в першу чергу будемо торкатися пакетної фільтрації. Стосовно до пакетної фільтрації, ACL розміщуються на інтерфейсах, самі вони створюються незалежно, а вже потім вони прикручуються до інтерфейсу. Як тільки ви його прикрутили до інтерфейсу маршрутизатор починає переглядати трафік. Маршрутизатор розглядає трафік як вхідний і вихідний. Той трафік, який входить в маршрутизатор називається входять, той який з нього виходить - вихідний. Відповідно ACL розміщуються на вхідному або на вихідному напрямі.

З вашої приватної мережі приходить пакет на інтерфейс маршрутизатора fa0 / 1, маршрутизатор перевіряє чи є ACL на інтерфейсі чи ні, якщо він є, то далі обробка ведеться за правилами списку доступу строго в тому порядку, в якому записані вирази, якщо список доступу дозволяє проходити пакету, то в даному випадку маршрутизатор відправляє пакет провайдеру через інтерфейс fa0 / 0, якщо список доступу не дозволяє проходити пакету, пакет знищується. Якщо списку доступу немає - пакет пролітає без всяких обмежень. Перед тим як відправити пакет провайдеру, маршрутизатор ще перевіряє інтерфейс fa0 / 0 на наявність вихідного ACL. Справа в тому, що ACL може бути прикріплений на інтерфейсі як вхідний чи. Наприклад у нас є ACL з правилом заборонити всім вузлам в Інтернеті посилати в нашу мережу пакети.

Так на який інтерфейс прикріпити дану ACL? Якщо ми прикріпимо ACL на інтерфейс fa0 / 1 як вихідний, це буде не зовсім вірно, хоча і ACL працювати буде. На маршрутизатор приходить луна-запит для якогось вузла в приватній мережі, він перевіряє на інтерфейсі fa0 / 0 є ACL, його немає, далі перевіряє інтерфейс fa0 / 1, на даному інтерфейсі є ACL, він налаштований як вихідний, все вірно пакет не проникає в мережу, а знищується маршрутизатором. Але якщо ми прикріпимо ACL за інтерфейсом fa0 / 0 як вхідний, то пакет буде знищаться відразу як прийшов на

маршрутизатор. Останнє рішення є правильним, так як маршрутизатор менше навантажує свої обчислювальні ресурси. Розширені ACL потрібно розміщувати як можна ближче до джерела, стандартні ж якомога ближче до одержувача. Це потрібно для того, щоб не ганяти пакети по всій мережі даремно.

Сам же ACL являє собою набір текстових виразів, в яких написано **permit** (дозволити) або **deny** (заборонити), і обробка ведеться строго в тому порядку в якому задані вирази. Відповідно коли пакет потрапляє на інтерфейс він перевіряється на першу умову, якщо перша умова збігається з пакетом, подальша його обробка припиняється. Пакет або перейде далі, або знищиться.

Ще раз, якщо пакет збігся з умовою, далі він не обробляється. Якщо перша умова не співпало, йде обробка другого умови, якщо воно співпало, обробка припиняється, якщо немає, йде обробка третього умови і так далі поки не перевірятися всі умови, якщо жодне з умов не збігається, пакет просто знищується. Пам'ятайте, в кожному кінці списку стоїть неявний deny any (заборонити весь трафік). Будьте дуже уважні з цими правилами, які я виділив, тому що дуже часто відбуваються помилки при конфігурації.

ACL поділяються на два типи:

• ***Стандартні (Standard):*** можуть перевіряти тільки адреси джерел

• ***Розширені (Extended):*** можуть перевіряти адреси джерел, а також адреси отримувачів, в разі IP ще тип протоколу і TCP / UDP порти.

Позначаються списки доступу або номерами, або символьними іменами. ACL також використовуються для різних мережевих протоколів. Ми в свою чергу будемо працювати з IP. Позначаються вони в такий спосіб, нумеровані списки доступу:

• Стандартні: від 1 до 99

• Розширені: від 100 до 199

Символьні ACL поділяються теж на *стандартні* і *розширені.**Розширені*** можуть перевіряти набагато більше, ніж стандартні, а й працюють вони повільніше, так як доведеться заглядати всередину пакета, на відміну від стандартних де ми дивимося тільки поле *Source Address (Адреса відправника).*При створенні ACL кожен запис списку доступу позначається порядковим номером, за замовчуванням в рамках десяти (10, 20, 30 і т.д). Завдяки чому, можна видалити певний запис і на її місце вставити іншу, але ця можливість з'явилася в Cisco IOS 12.3, до 12.3 доводилося ACL видаляти, а потім створити заново повністю. Не можна розмістити понад 1 списку доступу на інтерфейс, на протокол, на напрям. Пояснюю: якщо у нас є маршрутизатор і у нього є інтерфейс, ми можемо на вхідне напрямок для IP-протоколу розмістити тільки один список доступу, наприклад під номером 10. Ще одне правило, яке стосується самих маршрутизаторів, ACL не діє на трафік, згенерований самим маршрутизатором.

Для фільтрації адрес в ACL використовується WildCard-маска. Цезворотня маска. Беремо шаблонний вираз: 255.255.255.255 тавідіднімаємовід шаблона звичайну маску.

255.255.255.255-255.255.255.0, у нас виходить маска 0.0.0.255, що є звичайною маски 255.255.255.0, тільки 0.0.0.255 є WildCard маскою.

Види ACL

Динамічний (Dynamic ACL)

Дозволяє зробити наступне, наприклад у вас є маршрутизатор, який підключений до якогось сервера і нам потрібно закрити доступ до нього з зовнішнього світу, але в той же час є кілька людей, які можуть підключатися до сервера.

Налаштовуємо динамічний список доступу, прикріплюємо його на

вхідному напрямку, а далі людям, яким потрібно підключитися, підключатися через Telnet Цей пристрій, в результаті динамічний ACL відкриває прохід до сервера, і вже людина може зайти скажімо через HTTP потрапити на сервер. За замовчуванням через 10 хвилин цей прохід закривається і користувач змушений ще раз виконати Telnet щоб підключитися до пристрою.

Рефлексивний (Reflexive ACL)

Тут ситуація дещо відрізняється, коли вузол в локальній мережі відправляє TCP запит в Інтернет, повинен бути відкритий прохід, щоб прийшов TCP відповідь для установки з'єднання. Якщо проходу не буде - не зможемо встановити з'єднання, і ось цим проходом можуть скористатися зловмисники, наприклад проникнути в мережу. Рефлексивні ACL працюють таким чином, блокується повністю не пройшли ідентифікацію (deny any) але формується ще один спеціальний ACL, який може читати параметри сесії користувачів, які сгенерірованни з локальної мережі і для них відкривати прохід в *deny any*, в результаті виходить що з Інтернету не зможуть встановити з'єднання. А на сесії сгенеровані з локальної мережі будуть приходити відповіді.

Обмеження за часом (Time-based ACL)

Звичайний ACL, але з обмеженням по часу, можливо ввести спеціальний розклад, який активує ту чи іншу запис списку доступу. І зробити такий фокус, наприклад пишемо список доступу, в якому забороняємо HTTP-доступ протягом робочого дня і вішаємо його на інтерфейс маршрутизатора, тобто, співробітники підприємства прийшли на роботу, їм закривається HTTP-доступ, робочий день закінчився, HTTP-доступ відкривається,будь

ласка, якщо хочете - сидите в Інтернеті.

Списки доступу (***access-lists***) використовуються в цілому ряді випадків і є механізмом завдання умов, які роутер перевіряє перед виконанням будь-яких дій.

Маршрутизаторперевіряє кожен пакет і на підставі перерахованих вище критеріїв, зазначених в *ACL* визначає, що потрібно зробити з пакетом, пропустити або відкинути. Типовими критеріями є адреси відправника і одержувача пакету, тип протоколу. Кожен критерій в списку доступу записується окремим рядком.

Список доступу в цілому являє собою набір рядків з критеріями, що мають один і той же номер (або ім'я). Порядок завдання критеріїв в списку істотний. Перевірка пакету на відповідність списку проводиться послідовним застосуванням критеріїв з даного 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 назначено тільки один ***список*** доступу. Як наприклад нижче приведена *таблиця* списку управління доступом за замовчуванням:

№ правила	**Підмережа**	**Кінцева точка**	**Дозволити або заборонити**
100	0.0.0.0/0	3389	Заборонити

Без ACL - за замовчуванням при створенні кінцевої точки їй все дозволено.

Дозволити- при додаванні одного або декількох діапазонів "дозволу" всі інші діапазони за замовчуванням забороняються. Тільки пакети з дозволеного діапазону IP-адрес зможуть досягти кінцевої точки віртуальної машини.

Заборонити- при додаванні одного або декількох діапазонів "заборонити" всі інші діапазони трафіку за замовчуванням дозволяються.

Поєднання дозволу і заборони - можна використовувати поєднання (комбінацію) правил "дозволити" і "заборонити", щоб вказати вкладений дозволений або заборонений ***діапазон*** *IP*-адрес.

Розглянемо два приклади стандартних списків:

 # access-list 1 permithost 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.

Завдання на лабораторну роботу

Завдання 7.1.Створення стандартного списку доступу.

Завдання 7.2.Розширені списки доступу ACL.

Завдання 7.1. Створення стандартного списку доступу

Списки доступу бувають декількох видів: стандартні, розширені, динамічні та інші. У стандартних ACL є можливість задати лише IP ***адресу*** джерела пакетів для їх заборони або дозволів.

На рис. 7.1 показано дві підмережі: 192.168.0.0 та 10.0.0.0.

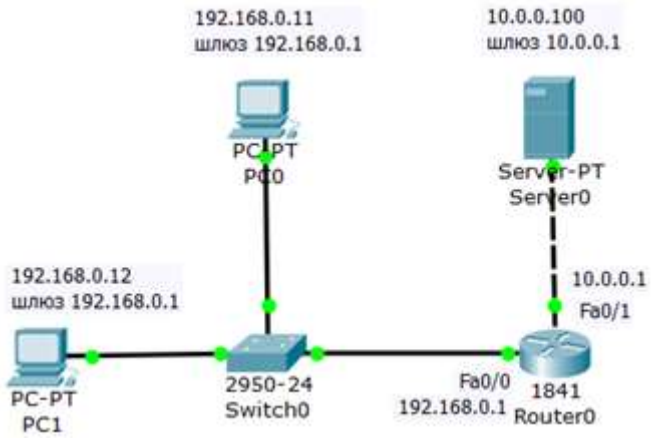


Рис. 7.1.Схема мережі

Постановка задачі

Потрібно дозволити доступ на сервер PC1 з адресою 192.168.0.12, а PC0 з адресою 192.168.0.11 - заборонити (рис. 7.2).

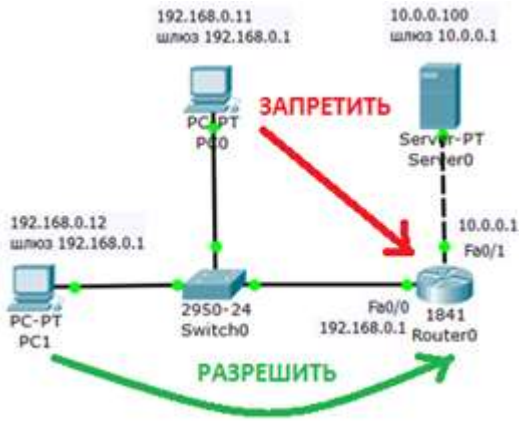


Рис. 7.2.Постановка задачі

Зберемо дану схему і налаштуємо її. Налаштування PC0 і PC1 виконайте самостійно.

Налаштування R0

Інтерфейс 0/0 маршрутизатора 1841 налаштуємо на адресу 192.168.0.1 і

включимо наступними 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 також включимо:

Router (config)#intfa0/1

Router (config-if)#ip addr 10.0.0.1 255.255.255.0

Router (config-if)#no shut

Налаштування сервера

Налаштування сервера наведені нарис. 7.3.

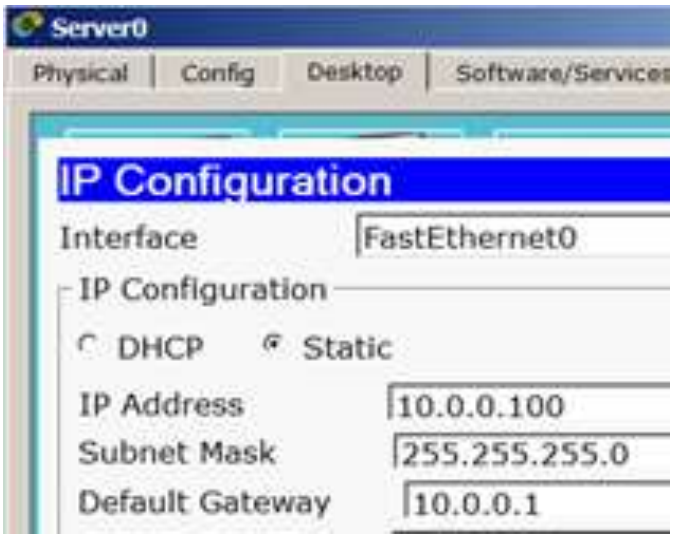


Рис. 7.3. Конфігурування S0

Діагностика мережі

Перевіряємо зв'язок ПК з різних мереж (рис. 7.4).

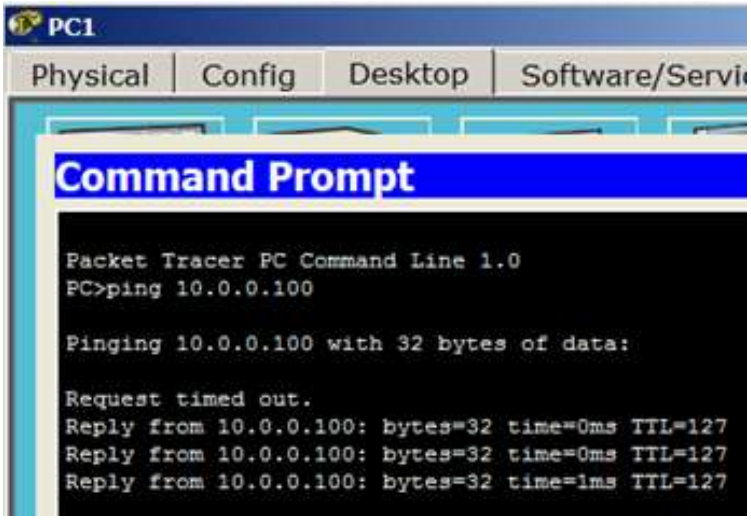


Рис. 7.4.ПК з різних мереж можуть спілкуватися

Переходимо до вирішення завдання. Правило заборони і дозволу доступу будемо складати з використанням стандартних списків доступу (ACL). Поки не заданий список доступу на інтерфейсі все дозволено (**permit**). Але, варто створити список, відразу діє механізм "Все, 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 R0 пропустити пакети з вузла 192.168.0.12 на сервер (рис. 7.5).

Рис. 7.5.Створюємо на R0 дозволяє ACL

Застосовується дане правило на інтерфейс в залежності від напрямку (PC1 розташований з боку порту Fa0 / 0) - рис. 7.6. Ця установка означає, що список доступу (правило з номером 1) діятиме на інтерфейсі fa0 / 0 на вхідному (in) від PC1 напрямку.

Рис. 7.6.Застосовуємо правило до порту Fa0/0

Примітка

Вхідний трафік (in) - цей той, який приходить на інтерфейс ззовні.

Вихідний трафік(out) - той, який відправляється з інтерфейсу зовні.

Список доступу ви можете застосувати або на вхідний трафік, тоді небажані пакети не будуть навіть потрапляти на маршрутизатор і відповідно, далі в мережу, або на вихідний, тоді пакети приходять на маршрутизатор, обробляються ним, доходять до цільового інтерфейсу і тільки на ньому обробляються. Як правило, списки застосовують на вхідний трафік (in).

Перевіряємо зв'язок ПК з сервером (рис. 7.7 і рис. 7.8).

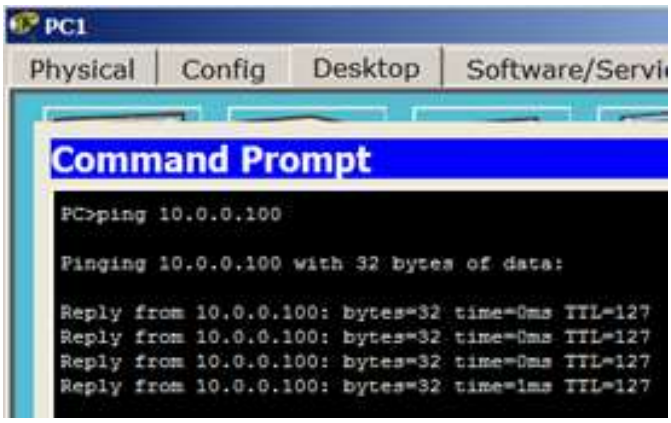


Рис. 7.7. Для PC1 сервер доступний

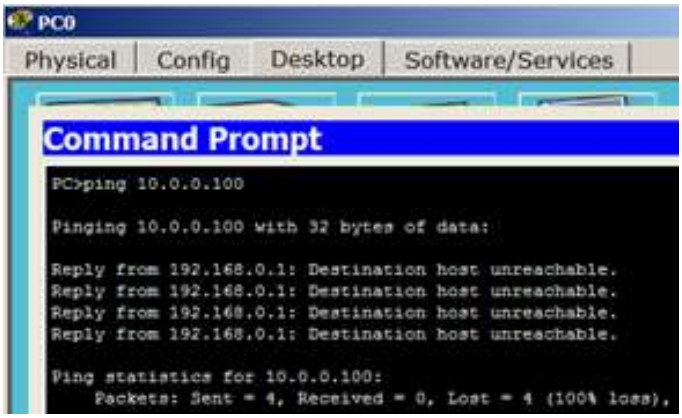


Рис. 7.8. Для PC0 сервер не доступний

Подивимось ACL (рис. 7.9).

Рис. 7.9.Вузол 192.168.0.12 дозволено

Примітка

Припустимо, потрібно додати новий вузол, наприклад, PC2 з адресою 192.168.0.13 в розділ "дозволених". Пишемо команду ***Router (config)#access-list 1 permit host 192.168.0.13****. Тепер адреса 192.168.0.12 і 192.168.0.13 можуть спілкуватися з сервером, а 192.168.0.11 – ні. А для відміни будь-якого правила – повторюємо його з приставкою "no". Тоді це правило виключається з конфігурації. Наприклад, якщо виконати команду* ***Router (config-if)#no ip access-group 1 in****, то ACL буде відмінено і знову всі ПК можуть пінгувати сервер.*

Розширені списки доступу ACL

Стандартні ***права*** не так гнучкі, як хотілося б. На відміну від стандартних списків, розширені списки фільтрують трафік більш "тонко". При створенні розширених списків в правилах доступу можна включати фільтрацію трафіку по протоколах і портам. Для вказівки портів в правилі доступу вказуються такі позначення (таблиця 7.1):

Таблиця 7.1. Позначення портів в ACL

Позначення портів в ACL	
позначення	дія
lt n	Усі номера портів, меньші n.
gt n	Усі номера портів, більшіі n.
eq n	Порт n
neq n	Усі порти, за виключенням n.
range n m	Усі портивід n до m включно.

Завдання 7.2. Розширені списки доступу ACL

Зберіть схему мережі, показану нарис. 7.10.

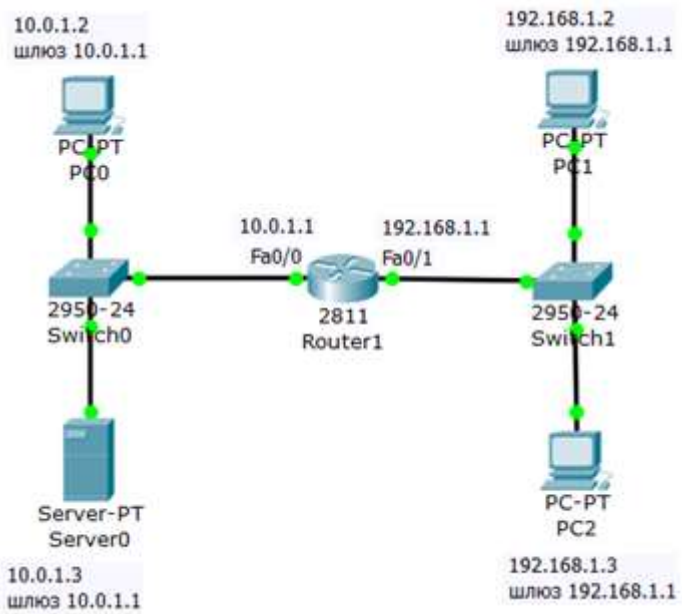


Рис. 7.10.Схема підмережі

Завдання: дозволити ***доступ*** до FTP-сервера 10.0.1.3 для вузла 192.168.1.2 і заборонити для вузла 192.168.1.3.

Створюємо розширені списки доступу і забороняємо FTP трафік. Постановка завдання графічно зображена нарис. 7.11.

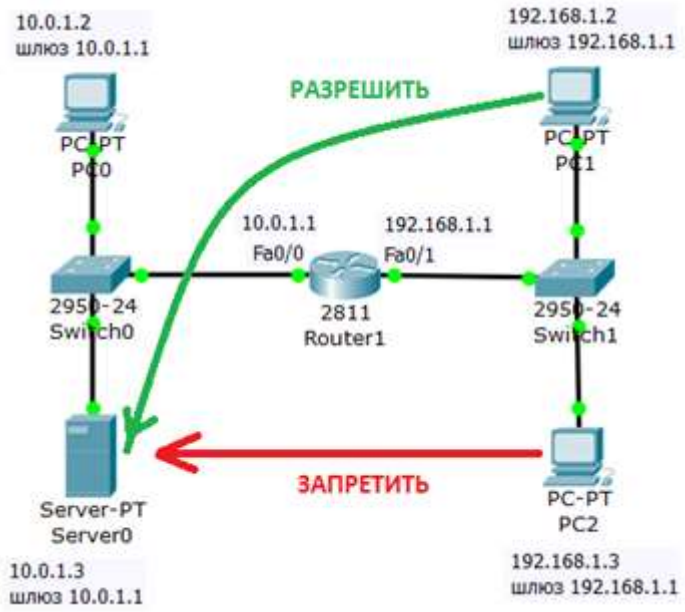


Рис. 7.11. Стрілками показана мета нашої роботи

Спочатку на сервері 10.0.1.3 FTP сервіс піднято за замовчуванням зі значеннями ім'я користувача Cisco, пароль Cisco. Переконаємося, що вузол S0 доступний і FTP працює, для цього заходимо на PC1 і зв'язуємося з сервером (рис. 7.12). Виконуємо будь-які команди, наприклад, DIR - читання директорії.

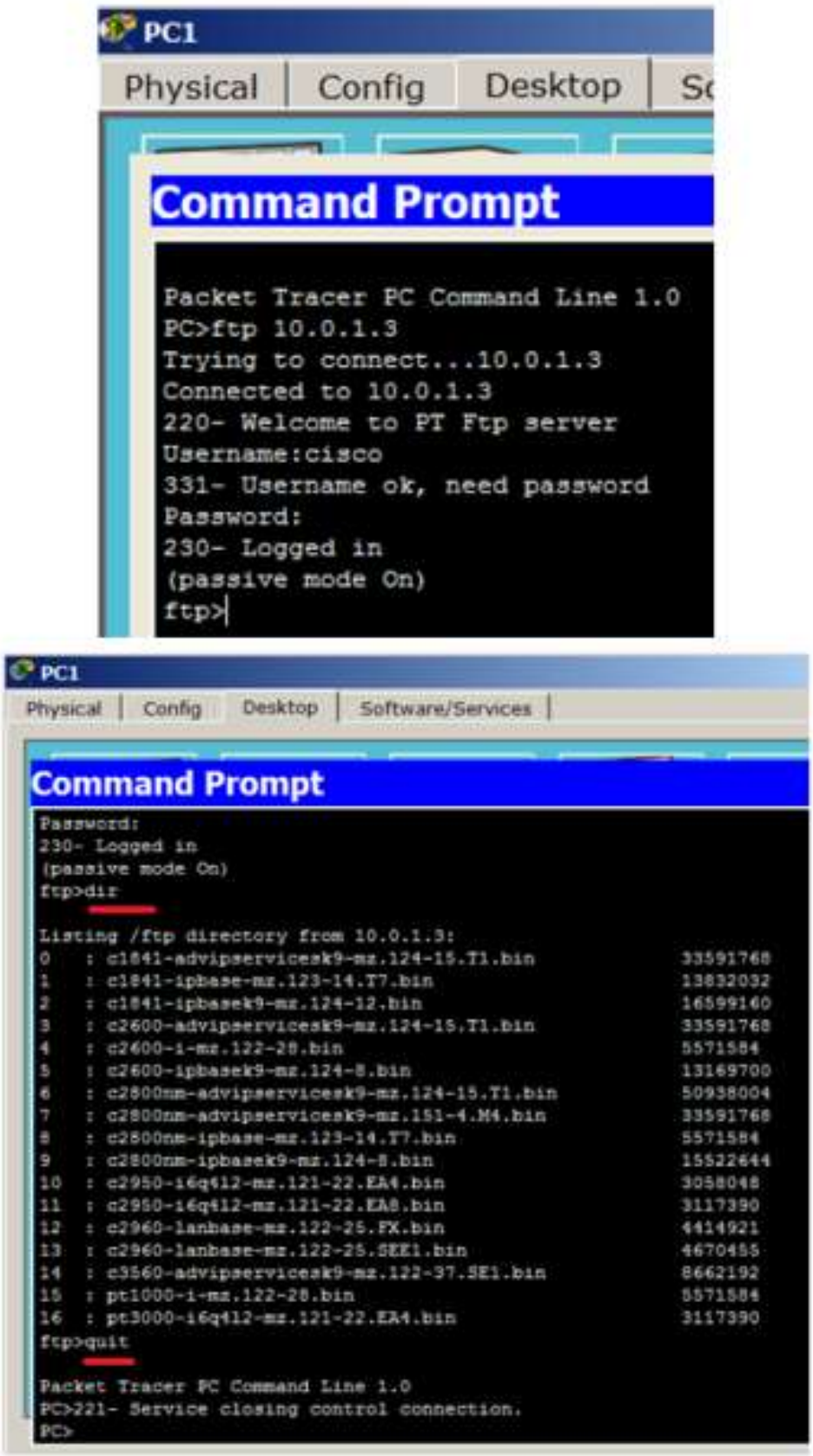


Рис. 7.12. FTP сервер доступний

Примітка

При наборі пароля на екрані нічого не відображається.Тепер створимо список правил з номером 101 в якому вкажемо 2 дозволяючих і по 2 забороняючих правила для портів сервера 21 і 20 (Ці порти служать для FTP - передачі команд і даних) – рис. 7.13.

```
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)#
```

Рис. 7.13.Складаємо розширені списки доступу

А тепер застосовуємо наш список з номером 101 на вхід (in) Fa0 / 1 тому, що трафік входить на цей порт роутера з боку мережі 192.168.1.0 (рис. 7.14).

```
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#
```

Рис. 7.14.Застосовуємо правило з номером 101 до порту 0/1 роутера

Перевіряємо зв'язок сервера з PC2 (рис. 7.15).

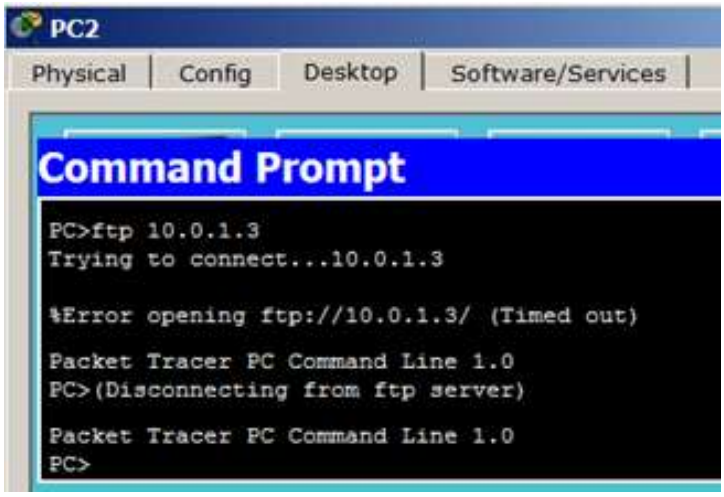


Рис. 7.15. Для PC2 FTP сервер недоступний

Перевіряємо зв'язок сервера з PC1 (рис. 7.16).

Рис. 7.16.Для PC1 FTP сервер доступний

Склад звіту комп’ютерного практикуму

В звіті повинно бути відображено:

1. Тема роботи.
2. Мета роботи.
3. Виконання завдання 7.1 з відповідними скріншотами.
4. Виконання завдання 7.2 з відповідними скріншотами.
5. Висновки

Контрольні питання

1. Що таке списки доступу, навіщо вони потрібні.
2. Де застосовуються списки доступу (ACL).
3. На які типи поділяються ACL.
4. Стандартні та розширені списки доступу.
5. Види списків доступу.
6. Динамічний список доступу (Dynamic ACL).
7. Рефлексивний список доступу (Reflexive ACL).
8. Обмеження за часом (Time-based ACL).

Лабораторна робота № 8

Тема: НАЛАШТУВАННЯ СТАТИЧНИХ ТА ДИНАМІЧНИХ ТРАНСЛЯЦІЙ МЕРЕЖНИХ АДРЕС (NAT)

***Мета заняття*:** вивчити принципи налаштування статичних та динамічних трансляцій мережних адрес, застосувати отримані знання при виконанні практичних завдань.

Теоретичні відомості

Розширення адресного простору існуючої системи IP-адресації версії 4 було здійснено за рахунок упровадження спеціальної технології заміни адрес ***NAT (Network Address Translation).*** Дана технологія і нині широко застосовується і розвивається.

Перехід на нову систему IP-адресації, яка отримала назву IP- адресація версії 6, був здійснений у межах розробки нової, більш продуктивної та ефективної версії протоколу IP – версії 6. Довжину IP-адреси версії 6 було збільшено до 128 бітів, що надало можливість позбутися проблеми дефіциту IP-адрес на тривалий період.

Класова IP-адресація

У класовому підході діапазон можливих IP-адрес поділяється на п’ять класів. У кожному з класів формуються діапазони IP-адрес мереж за правилами, які визначають структуру адреси та структуру старшого її байта (табл. 8.1).

Таблиця 8.1**Правила формування класів IP-адрес**

Клас	Правило I (структура IP-адреси)	Правило II (структура старшого байта)				
		Значення двійкове			Значення десяткове	
		Загальний вигляд	Мінімальне	Максимальне	Мінімальне	Максимальне
A	N.H.H.H	0xxxxxxx	00000000	01111111	0	127
B	N.N.H.H	10xxxxxx	10000000	10111111	128	191
C	N.N.N.H	110xxxxx	11000000	11011111	192	223
D	Multicast	1110xxxx	11100000	11101111	224	239
E	Reserved	11110xxx	11110000	11110111	240	247

Примітка: *N*, Network – байт(и) IP-адреси мережі; *H*, Host – байт(и) IP-адреси вуз- ла.

Правило I визначає структуру адреси, тобто показує, яка частина IP-адреси є IP-адресою (номером) мережі та яка частина – IP-адресою (номером) вузла. У класі A на IP-адресу мережі виділяється один байт, а на IP-адресу вузла – три байти. У класі B як на IP-адресу мережі, так і на IP-адресу вузла виділяється по два байти. У класі C на IP-адресу мережі виділяється три байти, а на IP-адресу вузла – один байт. IP-адреси класу D застосовуються як групові. IP- адреси класу E зарезервовані для експериментального використан- ня. На практиці застосовуються адреси всіх класів, крім класу E.

Правило II стосується лише старшого байта. За його допомогою формується і відображається структура цього байта у двійковій фо- рмі для кожного класу. Правило II дає змогу сформувати різні за розміром діапазони IP-адрес мереж, що належать певним класам.

Інформацію про діапазони IP-адрес мереж відповідних класів та їх кількісні параметри наведено у табл. 8.2. Слід зазначити, що у ході формування діапазону класу A дві IP-адреси мереж були вилу- чені. Під час формування класу E було вилучено діапазон 248.0.0.0 – 255.255.255.255.

Інформацію про згадані IP-адреси ви- лучення та їх призначення наведено у табл. 8.3.

Таблиця 8.2**Класи IP-адрес**

Клас	Мінімальна IP-адреса мережі	Максимальна IP-адреса мережі	Кількість IP-мереж	Кількість IP-адрес вузлів у мережі
A	**1**.0.0.0	**126**.0.0.0	126 (2^7–2)*	16777214 (2^{24}–2)**
B	**128.0**.0.0	**191.255**.0.0	16384 (2^{14})	65534 (2^{16}–2)**
C	**192.0.0**.0	**223.255.255**.0	2097152 (2^{21})	254 (2^8–2)**
D	224.0.0.0	239.255.255.255	–	–
E	240.0.0.0	247.255.255.255	–	–

*Примітка: * – дві IP-адреси мереж класу A (0.0.0.0 та 127.0.0.0) вилучено із звичайного застосування; ** – дві IP-адреси з діапазону окремої мережі (нульова й остання) зарезе- рвовані для спеціальних цілей і не можуть бути призначені вузлам: нульова IP-адреса – це IP-адреса мережі; остання IP-адреса – це широкомовна IP-адресамережі.*

Таблиця 8.3**IP-адреси вилучення та їх призначення**

№ з/п	IP-адреса вилучення	Назва	Застосування
1	0.0.0.0	Невизначена IP-адреса (Unknown IP-Address)	Позначення поточного вузла. Адреса відправника повідомлення увипадку, коли вузол не має адресної інформації
2	127.0.0.1 (127.x.x.x)	IP-адреса зворотної петлі (Loopback, Localhost IP-Address)	Тестування роботи стеку TCP/IP, а також організація роботи клієнтсь- кої і серверної частин додатка, які функціонують на одному

			вузлі
3	255.255.255.255	Обмежена широкомовна IP-адреса (Limited Broadcast IP-Address)	Пересилання повідомлення всім вузлам поточної мережі, без пересилання через маршрутизатори

На початковому етапі впровадження класової IP-адресації передбачалося, що всі IP-адреси класів A, B та C будуть застосовуватися для адресації вузлів у глобальній мережі Інтернет, однак із часом деякі IP-адреси мереж були вилучені для спеціального застосування. Серед них слід згадати так звані приватні IP-адреси (Private IP-Addresses), які були виділені для застосування у локальних мережах, що взагалі не мають підключення до глобальної мережі Інтернет або підключаються за допомогою технології заміни адрес NAT.

Налаштування статичного NAT

NAT* (*Network Address Translation*) —*трансляція мережевих адрес, технологія, яка дозволяє перетворювати (змінювати) IP адреси і порти в мережевих пакетах. NAT використовується найчастіше для здійснення доступу пристроїв з локальної мережі підприємства в ***Інтернет,*** або навпаки для доступу ***з Інтернет*** на який-небудь ресурс всередині мережі. ***Локальна мережа*** підприємства будується на приватних ***IP адресах***:

- 10.0.0.0 — 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))
- 172.16.0.0 — 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))
- 192.168.0.0 — 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Ці адреси не маршрутизируются в Інтернеті, і провайдери повинні відкидати пакети з такими *IP* адресами відправників або одержувачів. Для перетворення приватних адрес в Глобальні (маршрутизовані в Інтернеті) застосовують *NAT*.

NAT — технологія трансляції мережевих адрес, тобто підміни адрес (або портів) в заголовку IP-пакета. Іншими словами, пакет, проходячи через маршрутизатор, може поміняти свою адресу джерела і / або призначення. Подібний механізм служить для забезпечення доступу з LAN, де використовуються приватні IP-адреси, в Internet, де використовуються глобальні IP-адреси.

Існує три види трансляції *StaticNAT,DynamicNAT, Overloading* (*PAT*).

- **Static NAT** (**статичний NAT**) здійснює перетворення IP адреси один до одного, тобто порівнюється одна адреса з внутрішньої мережі з однією адресою з зовнішньої мережі. Іншими словами, при проходженні через маршрутизатор, адреса (и) змінюються на строго задану адресу, один-до-одного (Наприклад, 10.1.1.5 завжди замінюється на 11.1.1.5 і назад). Запис про таку трансляцію зберігається необмежено довго, поки є відповідний рядок в конфігурації роутера.
- **Dynamic NAT** (**динамічний NAT**) проводить перетворення внутрішньої адреси / ів в одну з групи зовнішніх адрес. Тобто, перед використанням динамічної трансляції, потрібно задати nat-пул зовнішніх адрес. В цьому випадку при проходженні через маршрутизатор, нова адреса вибирається динамічно з деякого діапазону адрес, званого пулом (pool). Запис про трансляцію зберігається деякий час, щоб відповідні пакети могли бути доставлені адресату. Якщо протягом деякого часу трафік по цій трансляції

відсутній, трансляція видаляється і адреса повертається в пул. Якщо потрібно створити трансляцію, а вільних адрес в пулі немає, то пакет відкидається. Іншими словами, добре б, щоб число внутрішніх адрес було ненабагато більше числа адрес в пулі, інакше висока ймовірність проблем з виходом в WAN.

- **Overloading (PAT)** дозволяє перетворювати кілька внутрішніх адрес в один зовнішній. Для здійснення такої трансляції використовуються порти, тому такий *NAT* називають *PAT (Port Address Translation).* За допомогою PAT можна перетворювати внутрішні адреси в зовнішню адресу, заданий через пул або через адресу на зовнішньому інтерфейсі.

Завдання на лабораторну роботу

Завдання 8.1. Статична трансляція адрес NAT.

Завдання 8.2. Визначити можливість роботи схеми.

Завдання 8.3. Налаштування статичного NAT.

Завдання 8.4. Налаштування динамічного NAT.

Завдання 8.5. Налаштування PAT.

Завдання8.1.Статична трансляція адрес NAT

На рис. 8.1 є зовнішня *адреса* 20.20.20.20 (зовнішній інтерфейс *інтерфейс*fa0/1) і внутрішня*мережа* 10.10.10.0 (внутрішній і*нтерфейс* fa0/0). Потрібно налаштувати *NAT*. Передбачається, що адреси вже прописані, і *мережа*піднята (робоча).

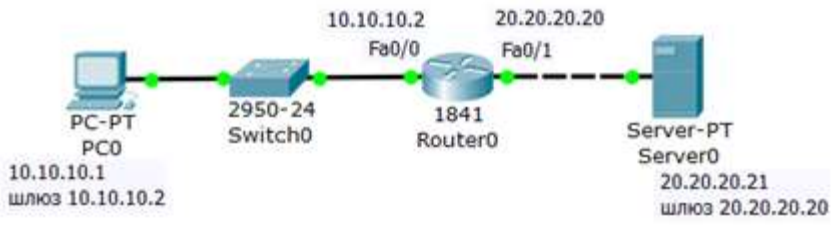


Рис. 8.1**.** Схема мережі

На R0 додаємо *access-list*, дозволяємо все (*any*)

Дозволяємо весь трафік, тобто, будь-яку IP адресу (рис. 8.2).

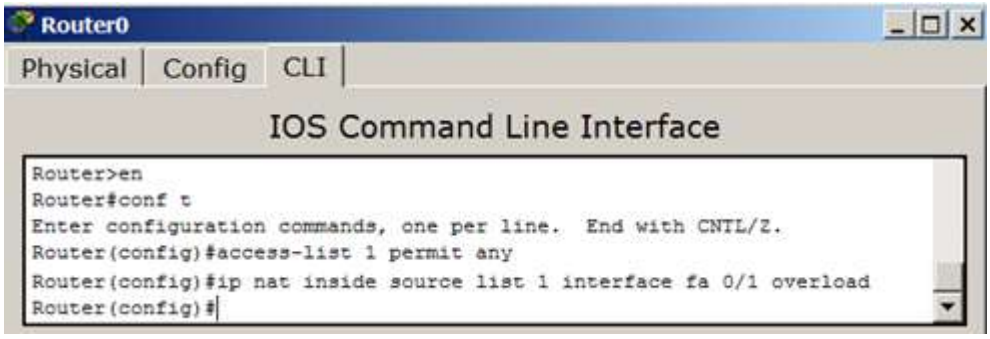


Рис. 8.2.Складаємо лист допуску

Створюємо правило трансляції

Тепер налаштуємо трансляцію на інтерфейсах (на внутрішньому inside, на зовнішньому - *outside*), тобто, для R0 вказуємо внутрішній і зовнішній порти (рис. 8.3).

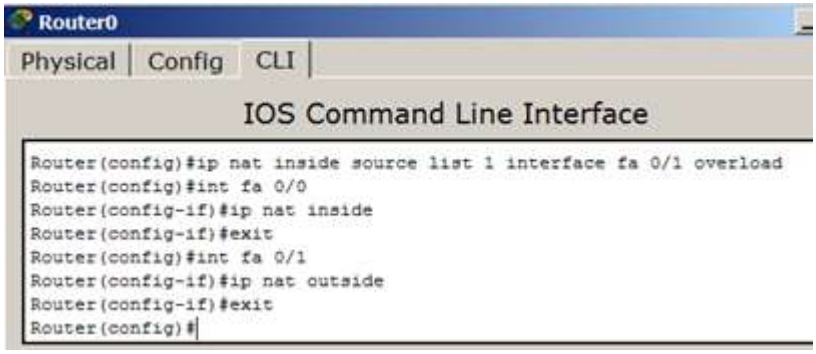


Рис. 8.3.Для R0 назначаємо внутрішній і зовнішній порти

Налаштування роутера (рис.8.4). «*int fa0/0*» -- переходимо до налаштування інтерфейсу fa0/0, «*ip addr 10.10.10.1 255.0.0.0*» - налаштовуємо адресу, «*ip nat inside*» - вказуємо, що саме вхідні в цей інтерфейс повідомлення будуть транслюватися, «*no sh*» -- вмикаємо інтерфейс, аналогічно для інтерфейсу fa0/1 за винятком «*ip nat outside*» - вказуємо, що саме вихідні з цього інтерфейсу повідомлення будуть транслюватися. Далі командою «*ip nat inside source static 10.10.10.2 20.20.20.22*» задаємо статичну трансляцію адреси 10.10.10.2 в адресу 20.20.20.22.

Пінгуючи сервер, переконуємось, що мережа працює коректно (рис.8.5). В режимі симуляції відправимо з ПК0 на сервер повідомлення. Бачимо, що по дорозі до серверу, адреса відповідно змінилася (рис.8.6), і повертаючись змінилася на початкову (рис.8.7)

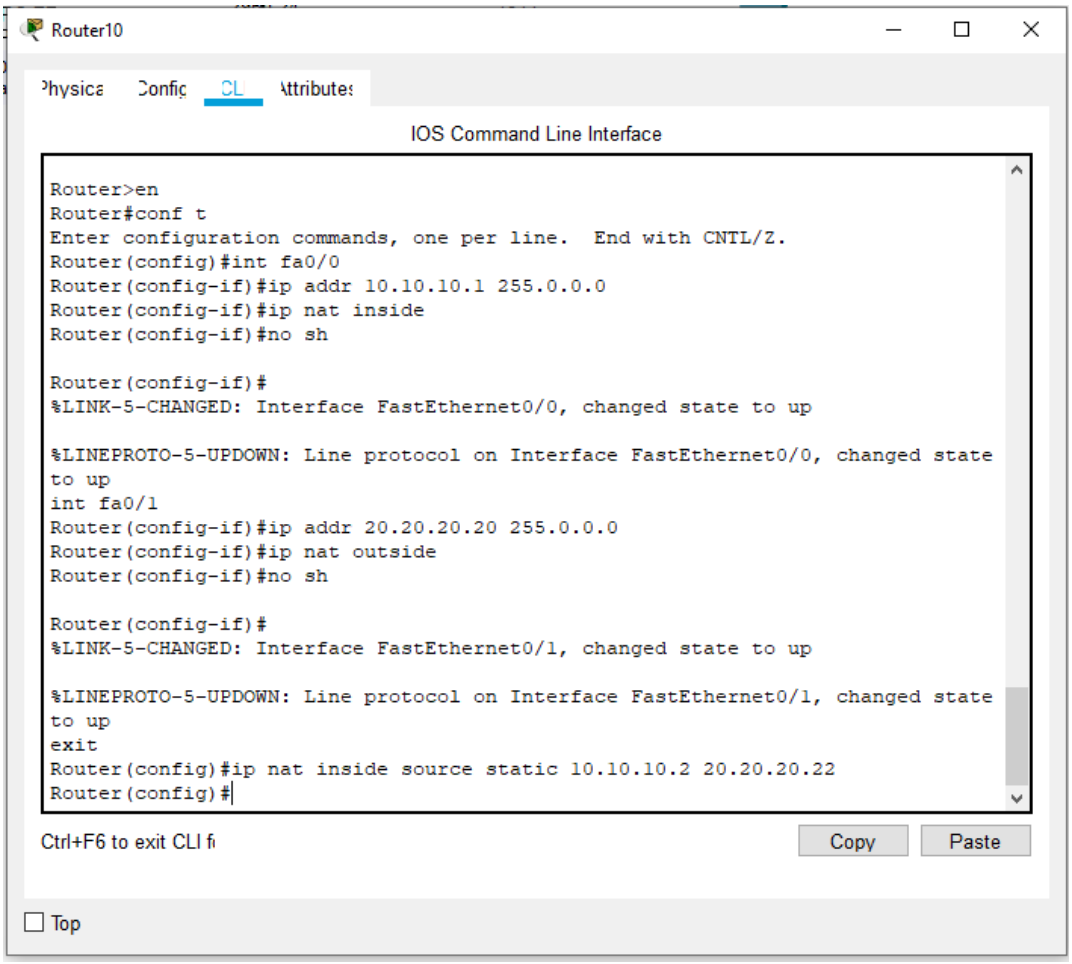


Рис.8.4. Налаштування статичної трансляції на роутері 0

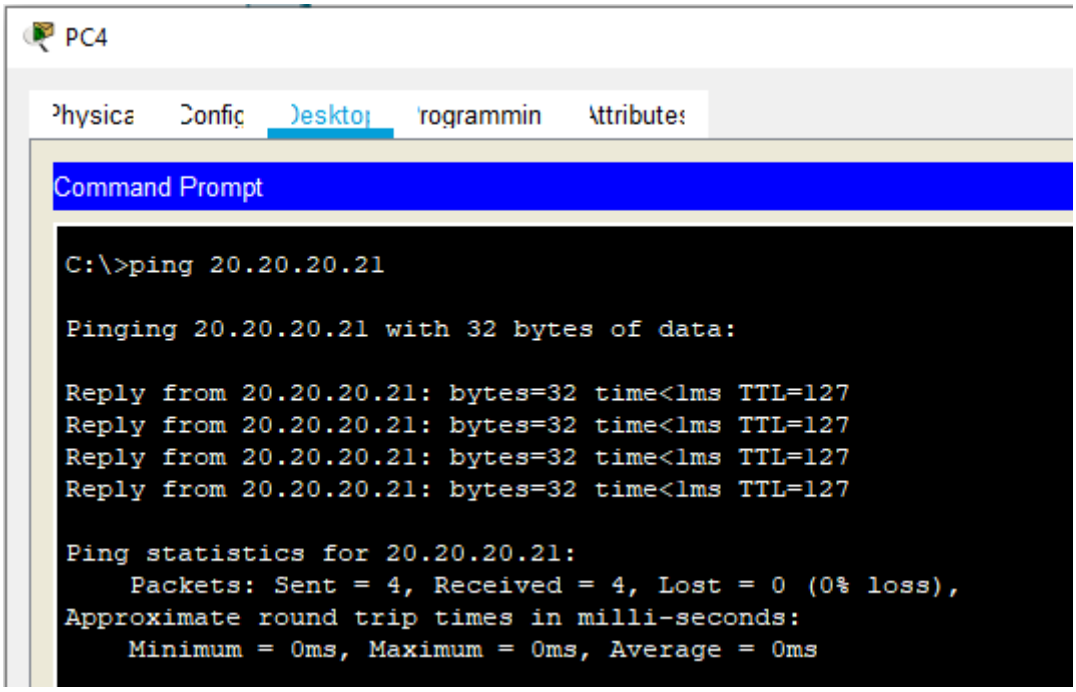


Рис. 8.5. Пінгування серверу з ПК4

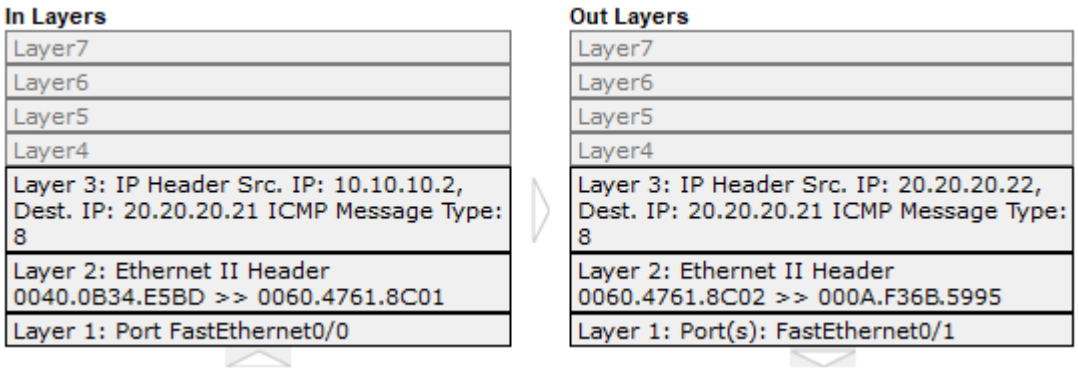


Рис. 8.6.Транслювання адреси при проходженні повідомлення до серверу

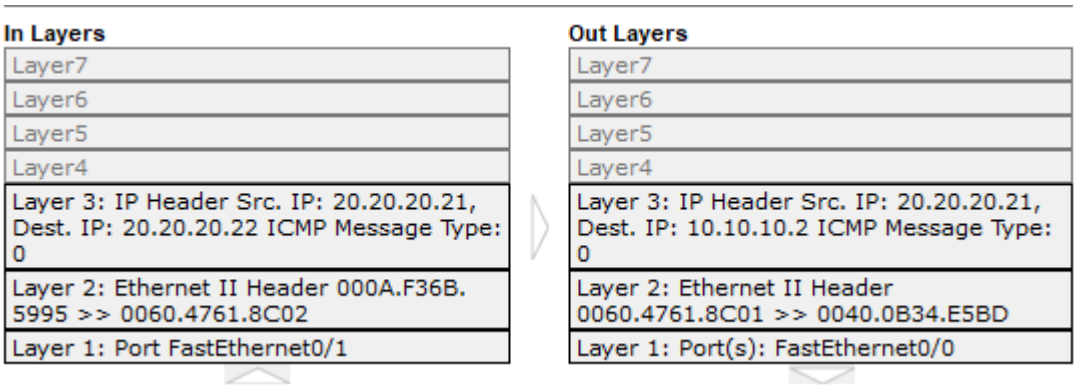


Рис. 8.7.Зворотнє транслювання адреси.

Виходимо з режиму глобального конфігурування і записуємо настройки

роутера в мікросхему пам'яті (рис. 8.8).

Рис. 8.8.Зберігаємо налаштування в ОЗУ

Перевіряємо роботу мережі (перегляд стану таблиці NAT)

З PC0 пінгуем провайдера і переконуємося, що PC1 і сервер можуть спілкуватися (рис. 8.9).

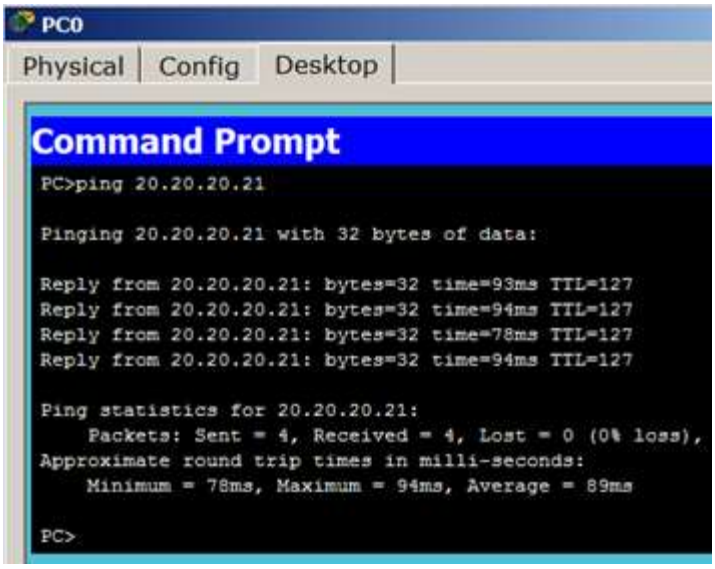


Рис. 8.9.З внутрішньої мережі пінгуемо зовнішню мережу

Для перегляду стану таблиці NAT, одночасно з пінгом використовуйте команду **Router#sh ip nat translations**(пінг з машини 10.10.10.1, тобто, з PC1

на адресу 20.20.20.21, тобто., на S0) – рис. 8.10.

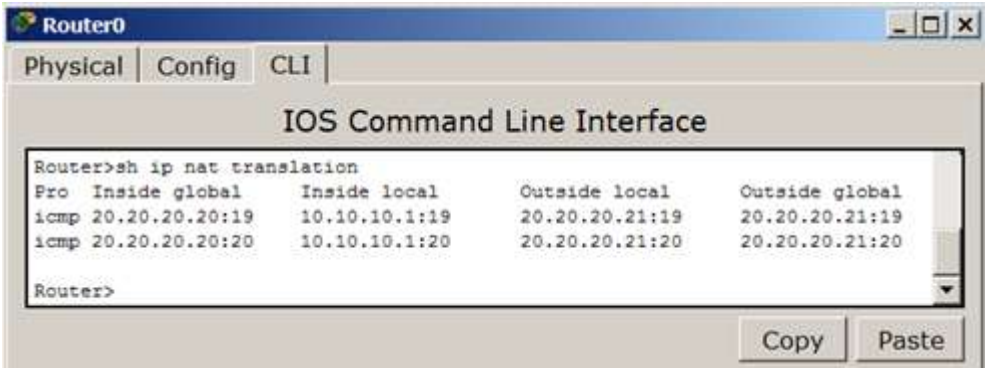


Рис. 8.10. Під час пінга переглядаємо стан таблиці NAT

Переконуємося в успішній маршрутизації в режимі симуляції (рис. 8.11).

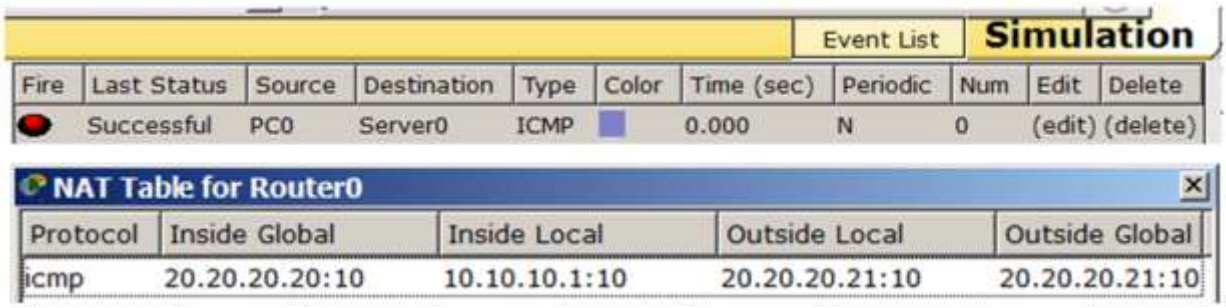


Рис. 8.11.Зв’язок PC0 і S0 працює

Завдання 8.2. Визначити можливість роботи схеми

Якщо в схему додати PC1 (рис. 8.12), то чи буде працювати статичний NAT між ним і S0?

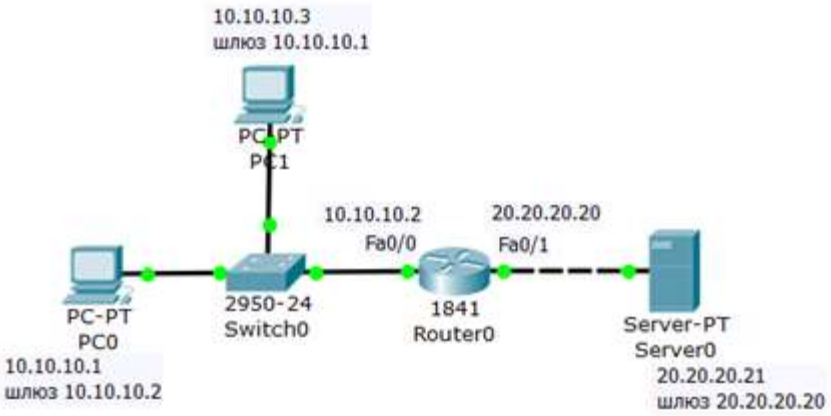


Рис. 8.12. Завдання для самостійної роботи

Завдання 8.3. Налаштування статичного NAT

Статичний NAT - порівнює один NAT inside (внутрішній = приватна локальна ip-адреса) з одним NAT outside (глобальним = публічною зовнішньою ip-адресою) – рис. 8.13. Тут *ISP* (*Internet Service Provider*) - постачальник *Інтернет*-послуг (*Інтернет-провайдер*).

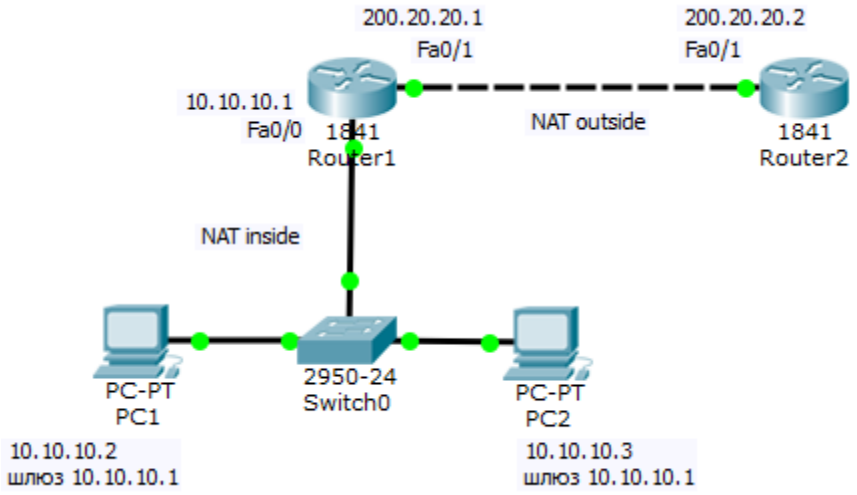


Рис. 8.13. Схема мережі

Алгоритм налаштування R1

Нижче наведена послідовність команд конфігурування маршрутизатора R1 по кроках.

Крок 1. Налаштування дефолту на R1

R1(config)# ip route 0.0.0.0 0.0.0.0 200.20.20.2

Крок 2. Налаштування внутрішнього інтерфейсу по відношенню NAT

R1(config)# interface fastethernet 0/0
R1(config-if)# ip nat inside

Крок 3. Налаштування зовнішнього інтерфейсу по відношенню NAT

R1(config)# interface fastethernet 0/1
R1(config-if)# ip nat outside

Крок 4. Налаштування порівняння ip-адрес.

R1(config)# ip nat inside source static 10.10.10.2 200.10.21.5

В результаті цієї команди ip-адресі 200.10.21.5 завжди буде відповідати внутрішня ip-адреса 10.10.10.2, тобто якщо ми будемо звертатися до адреси 200.10.21.5 то відповідати буде PC1.

Повний лістинг команд наведено на рис. 8.14.

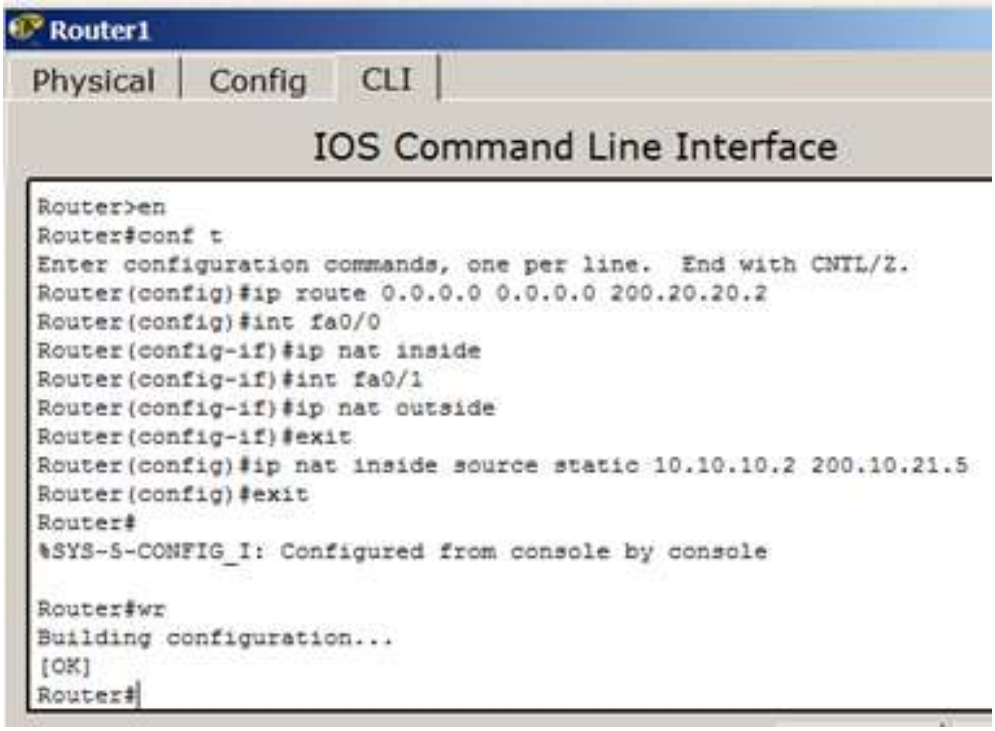


Рис. 8.14. Повний лістинг команд по налаштуванню R1

Команди для перевірки роботи NAT

Перевіряємо зв'язок PC1 і R2 (рис. 8.15).

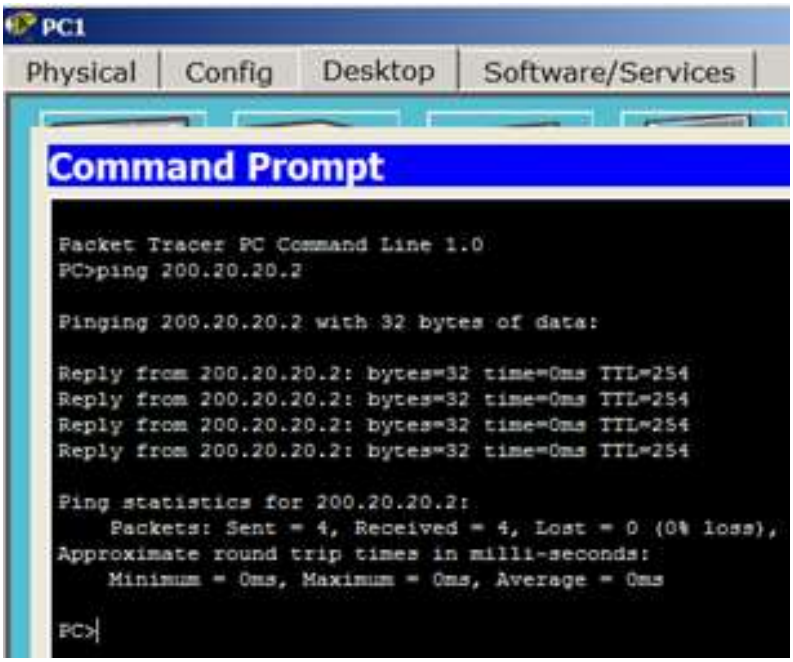


Рис. 8.15.PC1 бачить R2

Перевіримо, що R1 бачить сусідні мережі (рис. 8.16).

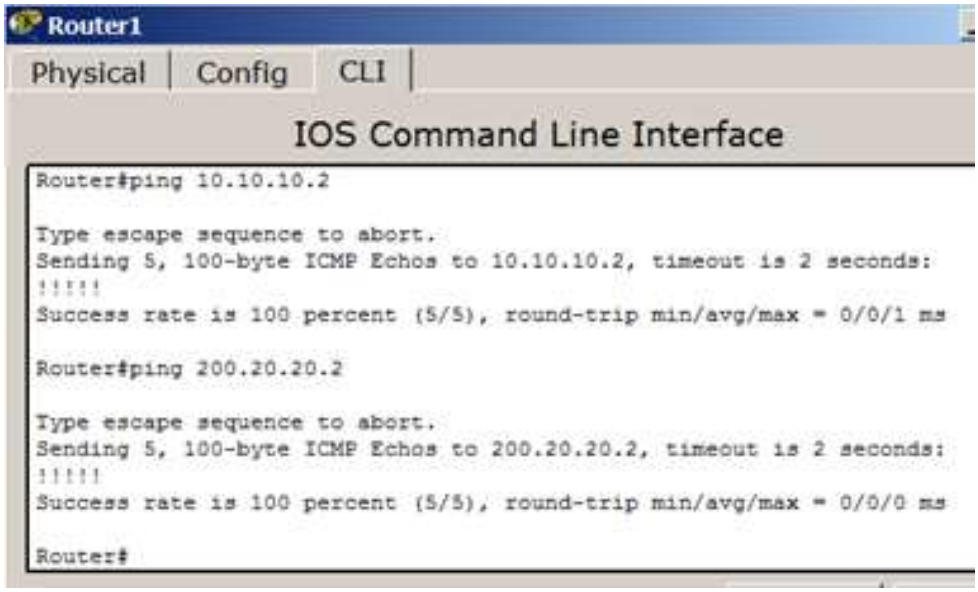


Рис. 8.16.R1 бачить PC1 і R2

Перевіримо механізм роботи статичного NAT: команда **show ip nat translations** виводить активні перетворення, а команда **show ip nat statistics** виводить статистику по NAT перетворенням (рис. 8.17).

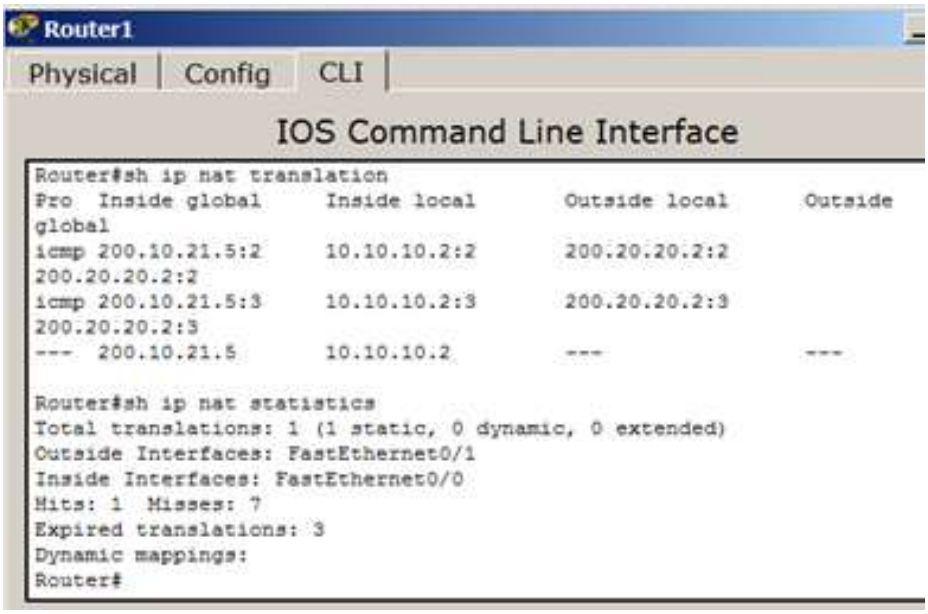


Рис. 8.17.Перевірка механізму роботи статичного NAT

З ілюстрації бачимо, що глобальній ip-адресі 200.10.21.5 відповідає локальна ip-адреса 10.10.10.2, а також, який інтерфейс є зовнішнім, а який-внутрішнім.

Динамична трансляція адрес. Настройка динамічного NAT

Динамічний NAT - використовує пул доступних глобальних (публічних) ip-адрес і призначає їх внутрішнім локальним (приватним) адресам. Схема для нашої роботи приведена на рис.8.18.

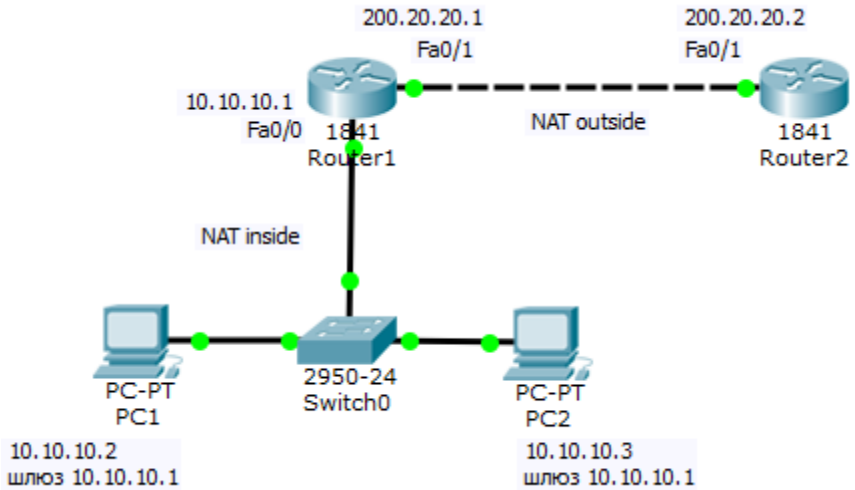


Рис. 8.18.Схема мережі

Завдання 8.4. Налаштування динамічного NAT

Крок 1. Налаштування на R1 списку доступу, відповідного адресам LAN

R1 (config)# access-list 1 permit 10.10.10.0 0.0.0.255

Тут 0.0.0.225 – зворотна (інверсна) *маска* для адреси 10.10.10.0.

Крок 2. Налаштування пулу адрес

R1 (config)# ip nat pool white-address 200.20.20.1 200.20.20.30 netmask 255.255.255.0

Крок 3. Налаштування трансляції

R1 (config)# ip nat inside source list 1 pool white-address

Крок 4. Налаштування внутрішнього інтерфейсу по відношенню NAT

R1 (config)# interface fastethernet 0/0

R1 (config-if)# ip nat inside

Крок 5. Настройка внешнего интерфейса в отношение NAT

R1 (config)# interface fastethernet 0/1

R1 (config-if)# ip nat outside

Нижче дан повний лістинг команд по налаштуванню R1 (рис. 8.19).

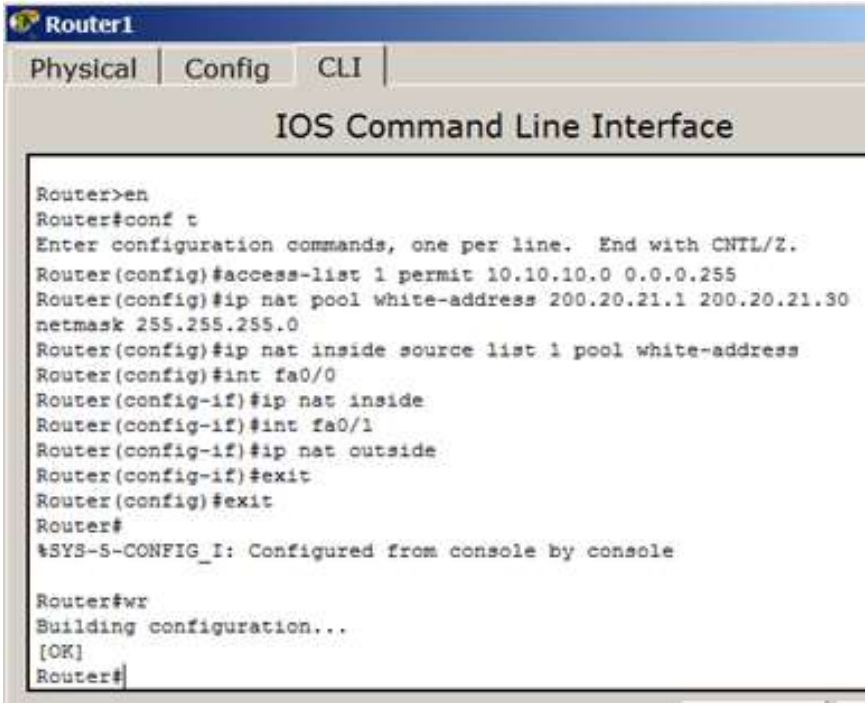


Рис. 8.19.Повний лістинг команд по конфігурації R1

Команди для перевірки роботи динамічного NAT

Перевіримо зв'язок PC1 і R2 (рис. 8.20).

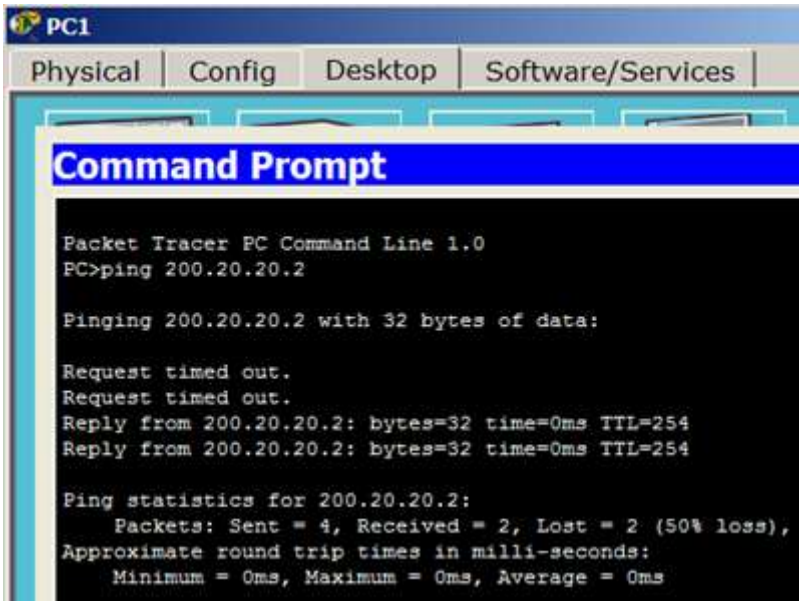


Рис. 8.20.PC1 бачить R2

Перевіримо, що R1 бачить сусідні мережі (рис. 8.21).

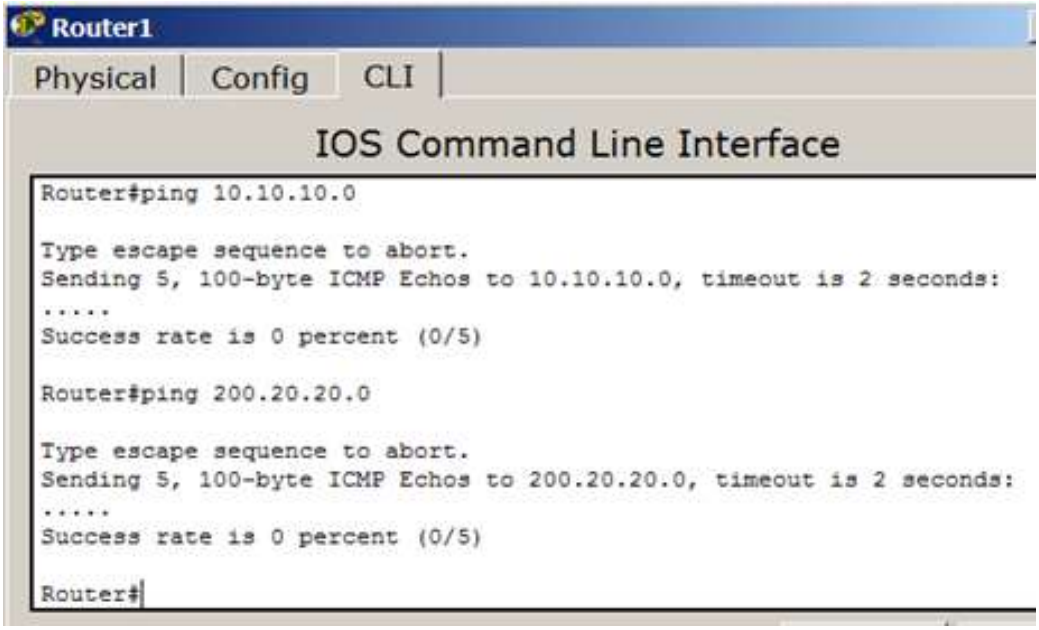


Рис. 8.21. R1 бачить підмережі 10.10.10.0 и 200.20.20.0

Перевіримо механізм роботи динамічного NAT: для цього виконаємо одночасно (паралельно) команди **pingishow ip nat translations**(рис. 8.22).

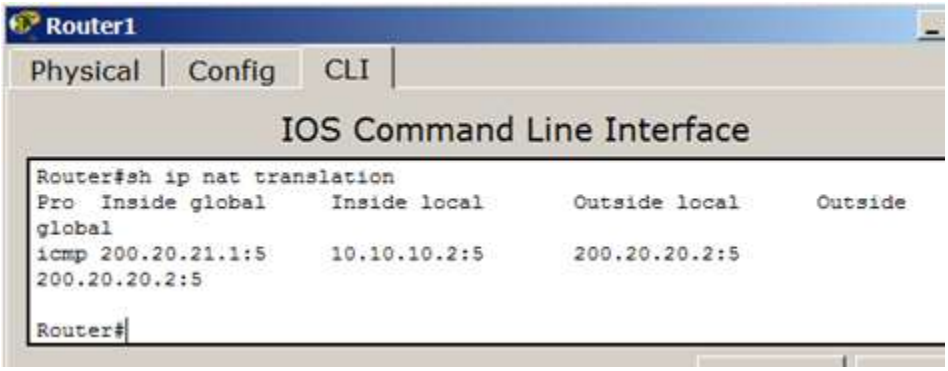


Рис. 8.22. Адреси: глобальна, внутрішня, зовнішня

Командою **show ip nat statistics** виведемо статистику по *NAT* перетворенням (рис. 8.23).

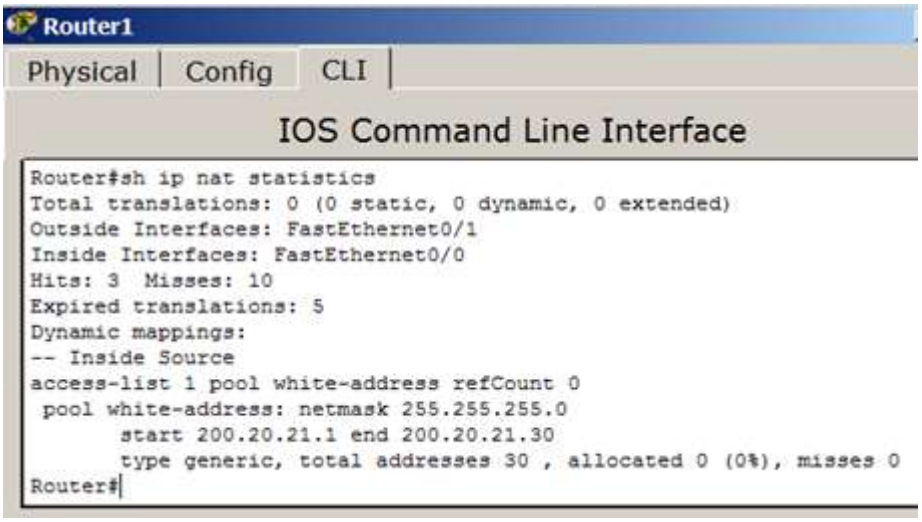


Рис. 8.23.Статистика роботи динамічного NAT

З ілюстрації бачимо, що локальним адресам відповідає пул зовнішніх адрес від 200.20.20.1 до 20.20.20.30.

Завдання 8.5. Динамічний *NAT Overload*: налаштування PAT (маскарадінг)

***PAT* (*Port AddressTranslation*)** - відображає кілька локальних (приватних) ip-адрес в глобальну ip-адресу, скориставшись різними портами

(рис. 8.24).

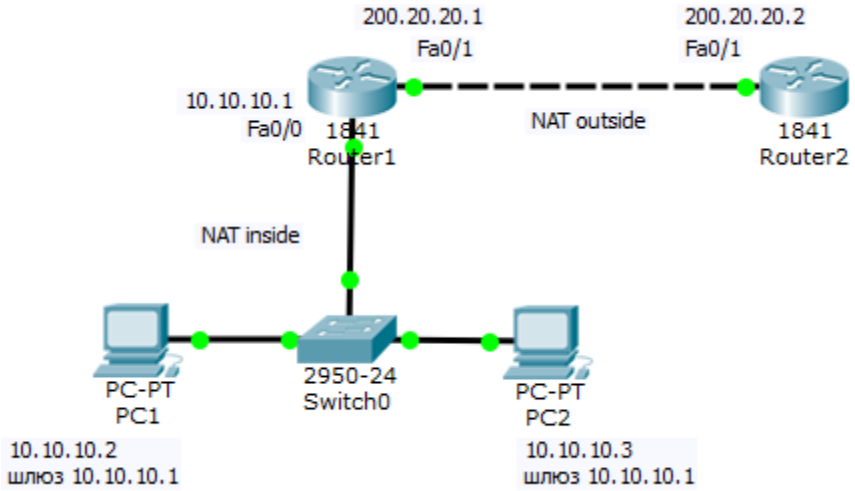


Рис. 8.24. Схема мережі на налаштування трансляції адрес PAT

Розглянемо алгоритм нашої роботи по кроках.

Крок 1. Налаштування списку доступу, відповідного внутрішнім приватним адресам

R1(config)# access-list 1 permit 10.10.10.0 0.0.0.255

Крок 2. Налаштування трансляції

R1(config)# ip nat inside source list 1 interface fastethernet 0/1 overload

Крок 3. Налаштування внутрішнього інтерфейсу по відношенню NAT

R1(config)# interface fastethernet 0/0

R1(config-if)# ip nat inside

Крок 4. Налаштування NAT на інтерфейсі

R1(config)# interface fastethernet 0/1

R1(config-if)# ip nat outside

Нижче дано повний лістинг команд по конфігурації R1 (рис. 8.25).

Рис. 8.25.Лістинг команд з конфігурування R1

Команди для перевірки роботи маскарадінгу (PAT)

Перевіримо зв'язок PC1 і R2 (рис. 8.26).

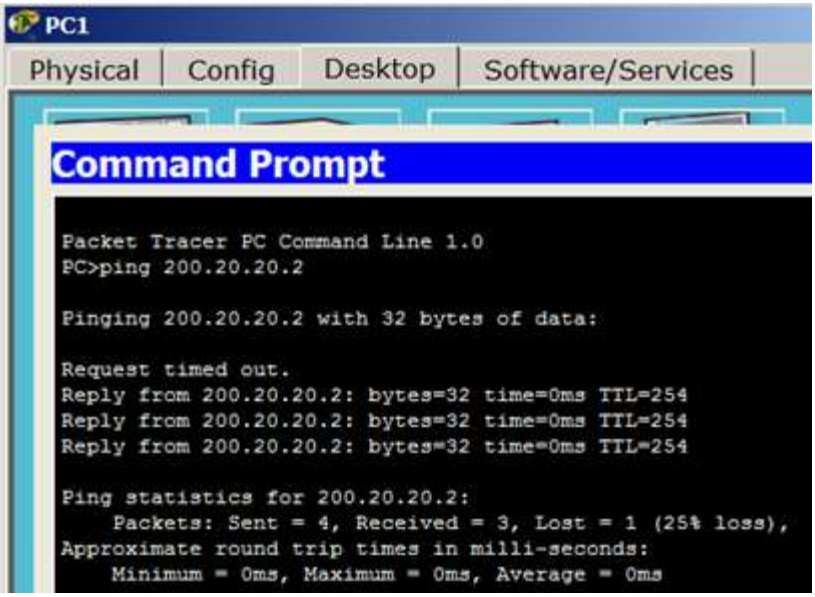


Рис. 8.26.PC1 бачить R2

Перевіримо, що R1 бачить сусідні мережі (рис. 8.27).

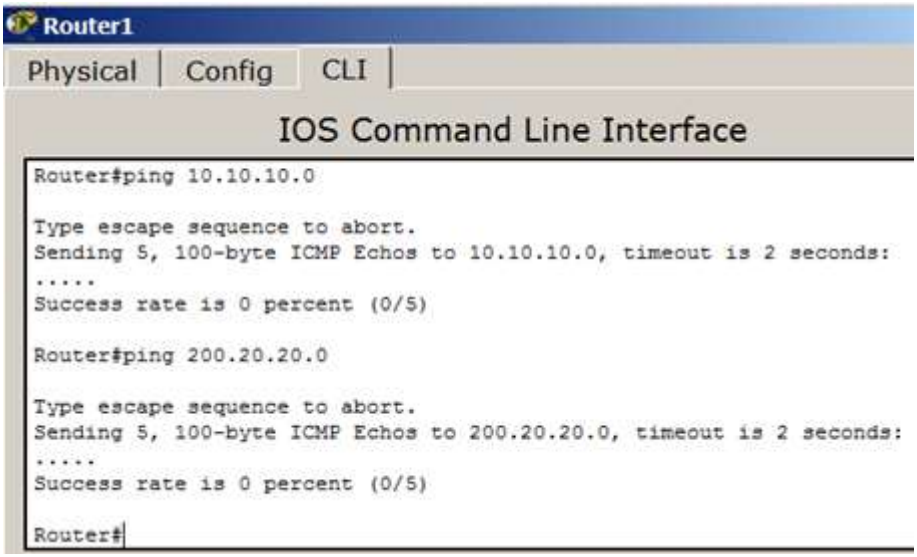


Рис. 8.27.R1 бачить підмережі 10.10.10.0 и 200.20.20.0

Перевіримо механізм роботи динамічного NAT: для цього виконаємо одночасно (паралельно) команди **ping и show ip nat translations** (рис. 8.28).

Рис. 8.28.Адреси: глобальна, внутрішня, зовнішня

Перевіримо роботу мережі в режимі симуляції (рис. 8.29).

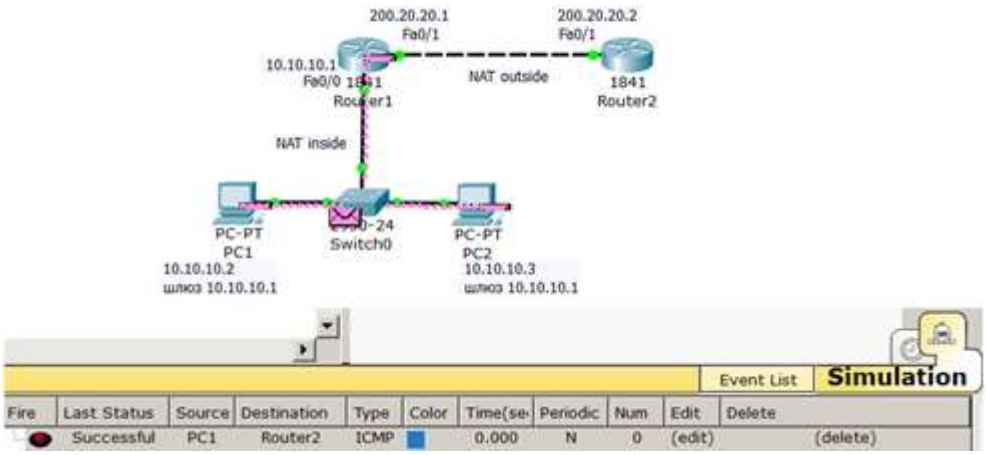


Рис. 8.29.PAT працює, PC1 і R2 відправляють і отримують пакети *Successful*

Склад звіту лабораторної роботи

В звіті повинно бути відображено:

1. Тема роботи.
2. Мета роботи.
3. Виконання завдання 8.1 з відповідними скріншотами
4. Виконання завдання 8.2 з відповідними скріншотами.
5. Виконання завдання 8.3 з відповідними скріншотами.
6. Виконання завдання 8.4 з відповідними скріншотами.
7. Виконання завдання 8.5 з відповідними скріншотами.
8. Висновки

Контрольні питання

1. Класова IP-адресація.
2. Безкласова IP-адресація.
3. Приватні IP-адреси версії4.
4. Налаштування статичного NAT
5. Динамическая трансляция адресов.
6. Налаштування динамичного NAT.
7. Динамічний NAT Overload: налаштування PAT (маскарадінг)

Лабораторна робота № 9

Тема: СТВОРЕННЯ ТА НАЛАШТУВАННЯ БЕЗПРОВОДОВОЇ МЕРЕЖІ.

***Мета заняття*:** ознайомитися із загальними принципами створення та налаштування безпроводових мереж, отримати практичні навички аналізу та визначення параметрів безпроводових мереж; застосувати отримані знання при виконанні практичних завдань.

Теоретичні відомості

Варіанти побудови мережі радіодоступу та види послуг, що надаються

Можливі наступні варіанти організації доступу та надаваємих послуг:

- радіомережа для об’єднання по радіоканалу двох точок в умовах прямого бачення або при його відсутності;
- радіомережа для об’єднання по радіоканалу трьох й більше точок при різних умовах бачення;
- радіомережа з доступом в Інтернет для місць публічного користування;
- радіомережа передачі даних з інтеграцією IP-телефонії и доступа в Інтернет в масштабі окремого района, селища;
- радіомережа передачі даних з інтеграцією IP-телефонії, передачі даних телематичних послуг, включачи й відеоінформаційні

Створення нової бездротової мережі починається безпосередньо з конфігурації точки доступу - безпроводового маршрутизатора (роутера) підключення до неї комп'ютерів та іншого безпроводового обладнання. Класичний спосіб настройки такий: спочатку проводиться підключення до

точки доступу обладнання, а потім потрібно задати вручну ***ім'я***безпроводової мережі і ***ключ*** безпеки. У цій лабораторній роботі далі ми розглянемо різні варіанти безпроводових мереж і способи їх налаштування в програмі CPT.

Ключ безпеки безпроводової мережі - унікальний код (***пароль***), який закриває ***доступ*** до вашої мережі. При цьому важливим є не стільки сам ***ключ***, скільки тип шифрування. Справа в тому, що вся *інформація*, яка протікає між роутером і ПК шифрується. І якщо ви ввели неправильний ***ключ***, то ваш пристрій просто не зможе розкодувати її. Це зроблено для підвищення безпеки. Варто зазначити, що на сьогоднішній день існує три типи шифрування *Wi-Fi* підключень:*WPA. WPA2. WEP.*

Wi-Fi **-** це система короткої дії, що зазвичай покриває десятки метрів, яка використовує неліцензовані діапазони частот для забезпечення доступу до мережі.Зазвичай *Wi-Fi* використовується користувачами для доступу до їх власної локальної мережі, яка може бути і не підключена до Інтернету.

WEP (Wired Equivalent Privacy) - алгоритм для забезпечення безпеки мереж *Wi-Fi*. Використовується для забезпечення захисту, переданих даних

Завдання на лабораторну роботу

Завдання 9.1. Налаштувати безпроводової мережіWEP.

Завдання 9.2. Налаштування безпроводової мережі WPA.

Завдання 9.3. Безпроводова мережа з точкою доступу.

Завдання 9.4. Безпроводова мережа між офісами.

Завдання 9.5. Налаштування комутованого WI-FI з'єднання.

Завдання 9.6. Безпроводовий зв'язок в Packet Tracer з безпроводовим роутером.

Завдання 9.1. Налаштувати безпроводової мережі WEP

Схема для роботи показана на рис. 9.1.

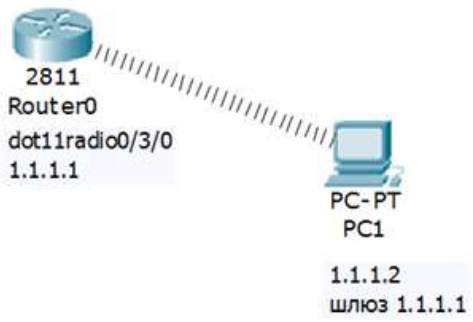


Рис. 9.1. Схема мережі

Оснастимо ***маршрутизатор*** радіоточкою доступу HWIC-AP-AG-B (рис. 9.2).

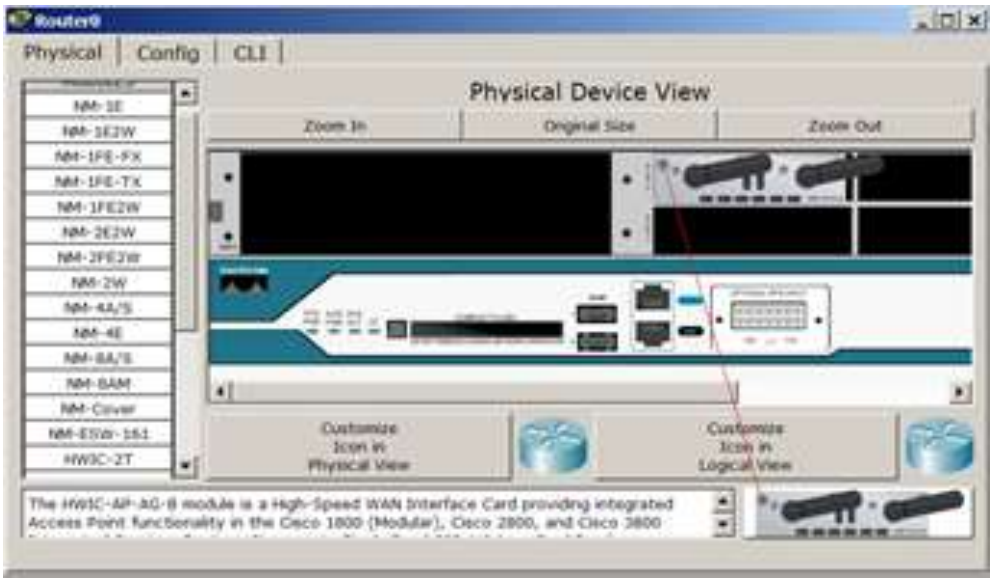


Рис. 9.2. Радіоточка доступу HWIC-AP-AG-B

Вставимо в ПК бездпроводовий ***адаптер*** WMP300N. Для цього спочатку вимкнемо ПК і приберемо з нього ***модуль*** PT-HOST-NM-1CFE (рис. 9.3).

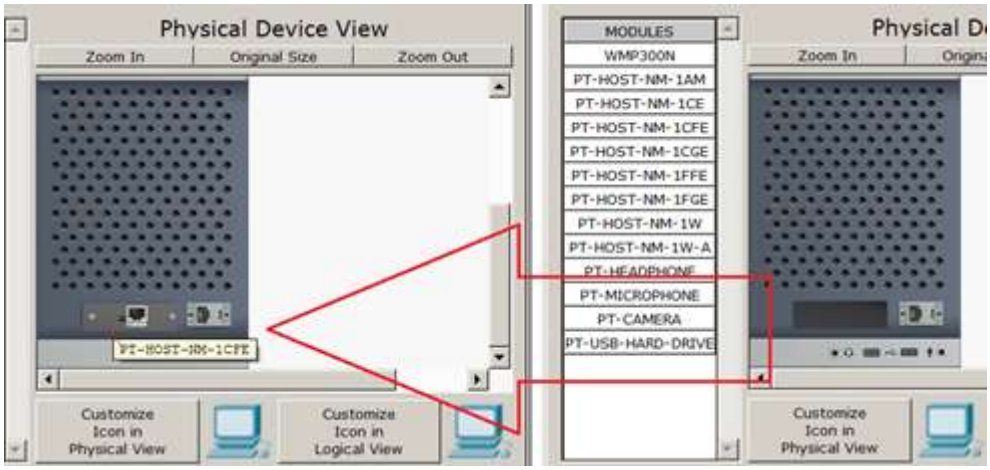


Рис. 9.3.Видаляємо модуль PT-HOST-NM-1CFE

Від’єднуємо безпроводовий *адаптер* WMP300N (рис. 9.4).

Рис. 9.4. Обладнуємо ПК безпроводовим адаптером

Реальний вигляд безпроводового адаптера WMP300N наведено на рис. 9.5.

Рис. 9.5.Безпроводовий адаптер WMP300N

Налаштуємо безпроводовий *адаптер* на PC1 (рис. 9.6).

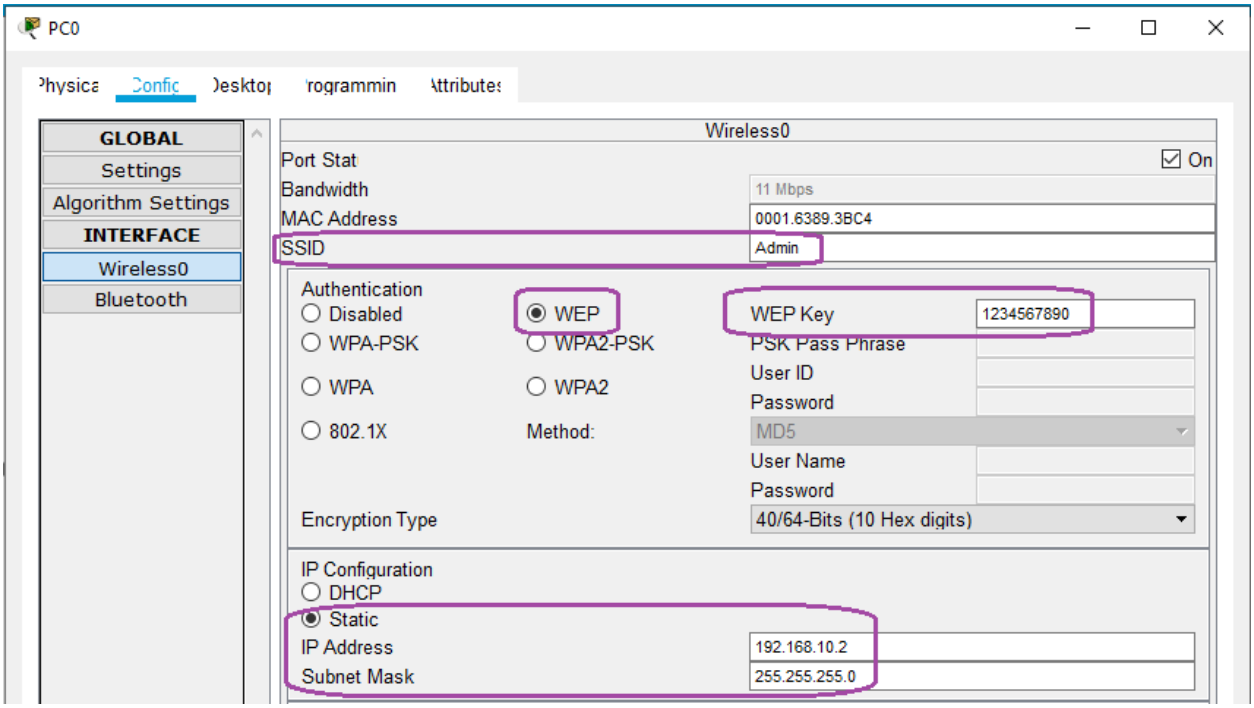


Рис. 9.6.Налаштування ПК

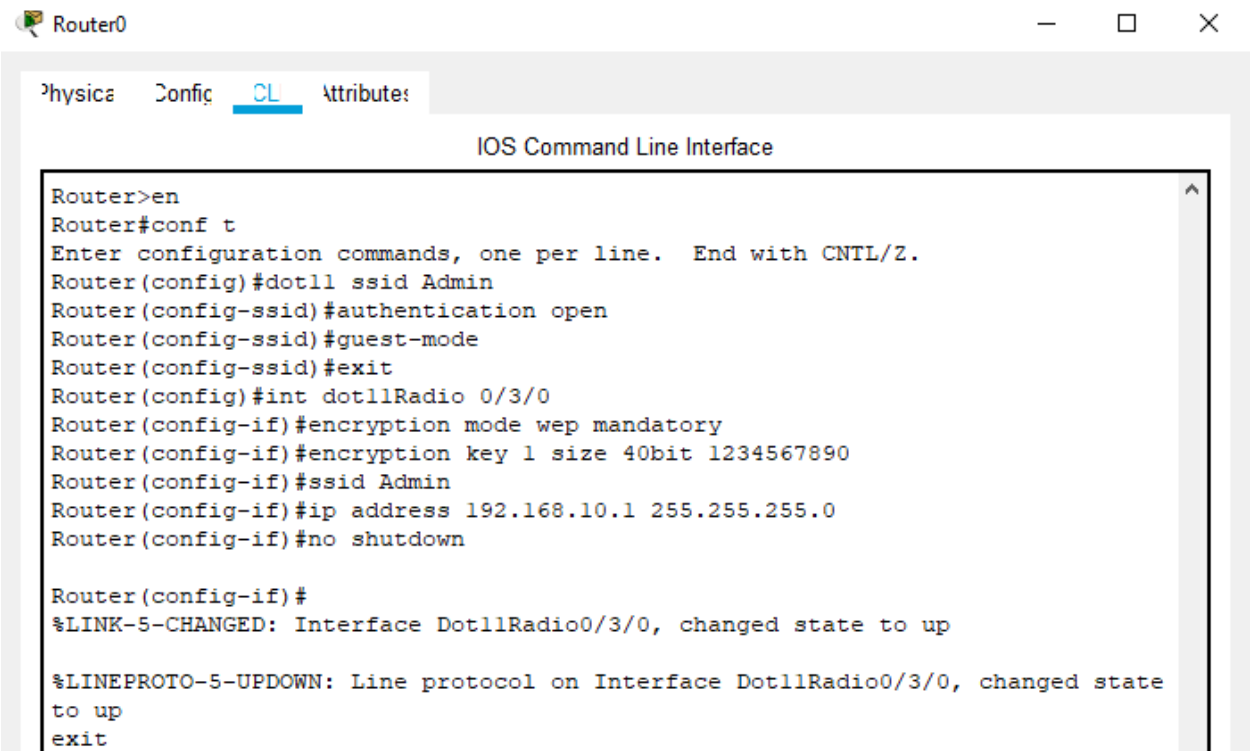


Рис.9.7. Налаштування точки доступу на роутері.

Перевіримо результат (рис. 9.8ірис. 9.9).

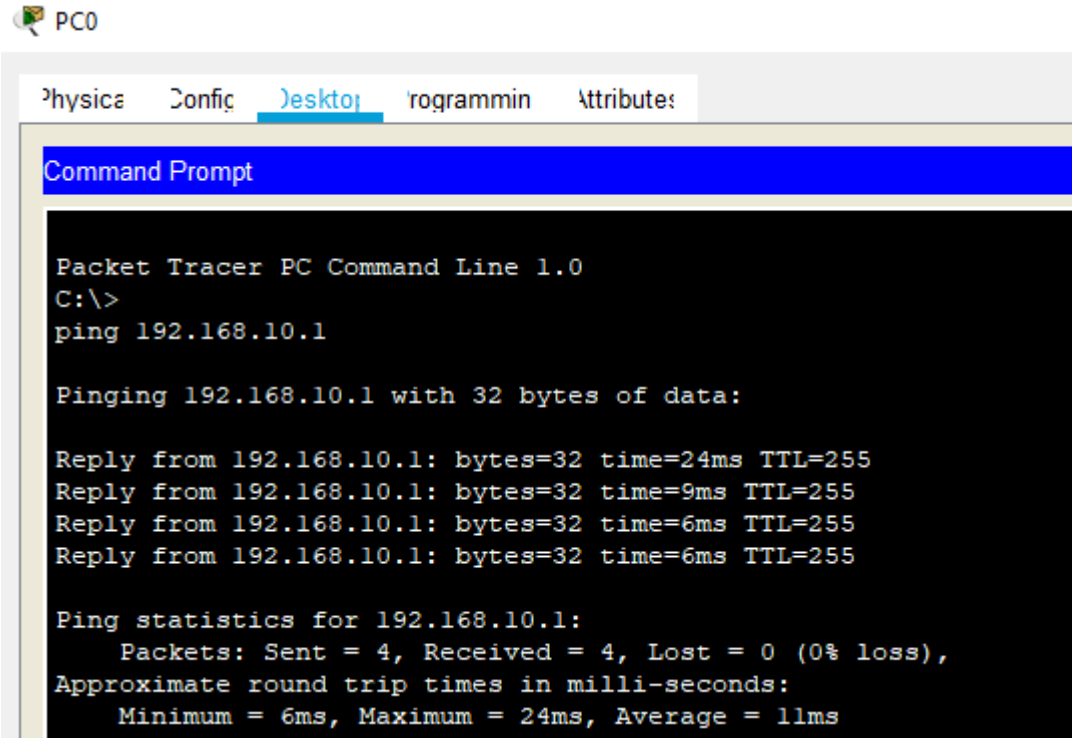


Рис. 9.8.Перевірка зв’язку ПК і маршрутизатора

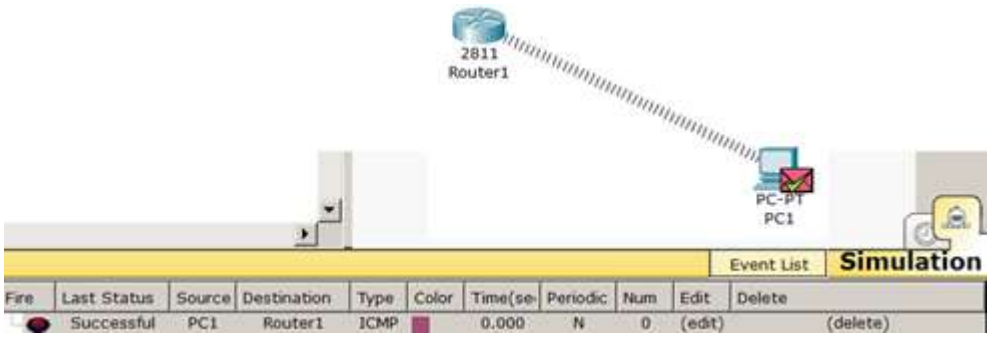


Рис. 9.9. Перевірка зв’язку ПК і маршрутизатора в режиме симуляції

Безпроводова мережа WPA

Типи шифрування мережі WPA і WPA2 вимагають від абонентів введення унікального пароля. Без нього ви просто не зможете виконати підключення. Після перевірки введеного ключа всі дані, які передаються між учасниками мережі, шифруються. Сучасні роутери підтримують обидві технології. Але, WPA2 все ж надає більш високий захист. Тому по можливості слід вибирати саме його.

WPA

WPA (Wi-Fi Protected Access) - являє собою технологію захисту безпроводової Wi-Fi мережі. Плюсами WPA є посилена безпека даних і посилений контроль доступу до безпроводових мереж, а також - сумісність між безліччю безпроводових пристроїв як на апаратному рівні, так і на програмному.

Завдання 9.2. Налаштування безпроводової мережі WPA

Розглянемо ***мережу***, зображену нарис. 9.9.

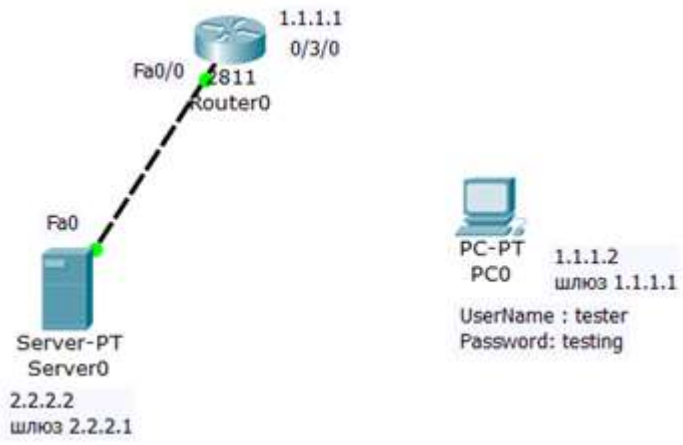


Рис. 9.9.Схема мережі

Перейдемо до налаштувань. Для початку налаштуємо сервер IP 2.2.2.2/8 шлюз 2.2.2.1/8. Далі перейдемо до налаштування роутера інтерфейсу fa0/0 встановим адресу 2.2.2.1/8 і підключив витою парою до нього сервер. Роутер та пк не мають бездротового мережного адаптеру, його слід встановити (Рис.9.10 – 9.11). Далі налаштуємо роутер:

```
Router1(config)#dot11 ssid Adm
Router1(config-ssid)#authentication open
Router1(config-ssid)#authentication key-management wpa
Router1(config-ssid)#wpa-psk ascii 0 12345678
Router1(config-ssid)#guest-mode
Router1(config-ssid)#exit

Router1(config)#interface dot11radio0/2/0
Router1(config-if)#ip address 192.168.90.1 255.255.255.0
Router1(config-if)#ssid Adm
Router1(config-if)#encryption mode ciphers aes-ccm
Router1(config-if)#no shutdown

Router1(config)#interface fa0/0
Router1(config-if)#ip address 2.2.2.1 255.0.0.0
Router1(config-if)#no shutdown
```

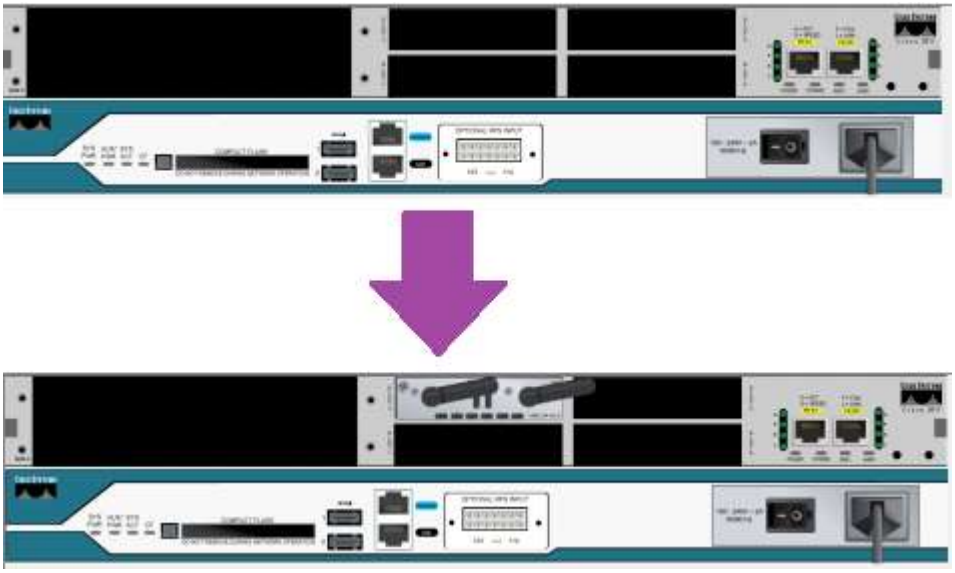


Рис.9.10. Встановлення HWIC-AP-AG-B на роутер

Рис. 9.11. Встановлення PT-HOST-NM-1W на ПК

Тут для нас нічого нового, крім налаштувань адаптера ПК (рис. 9.12).

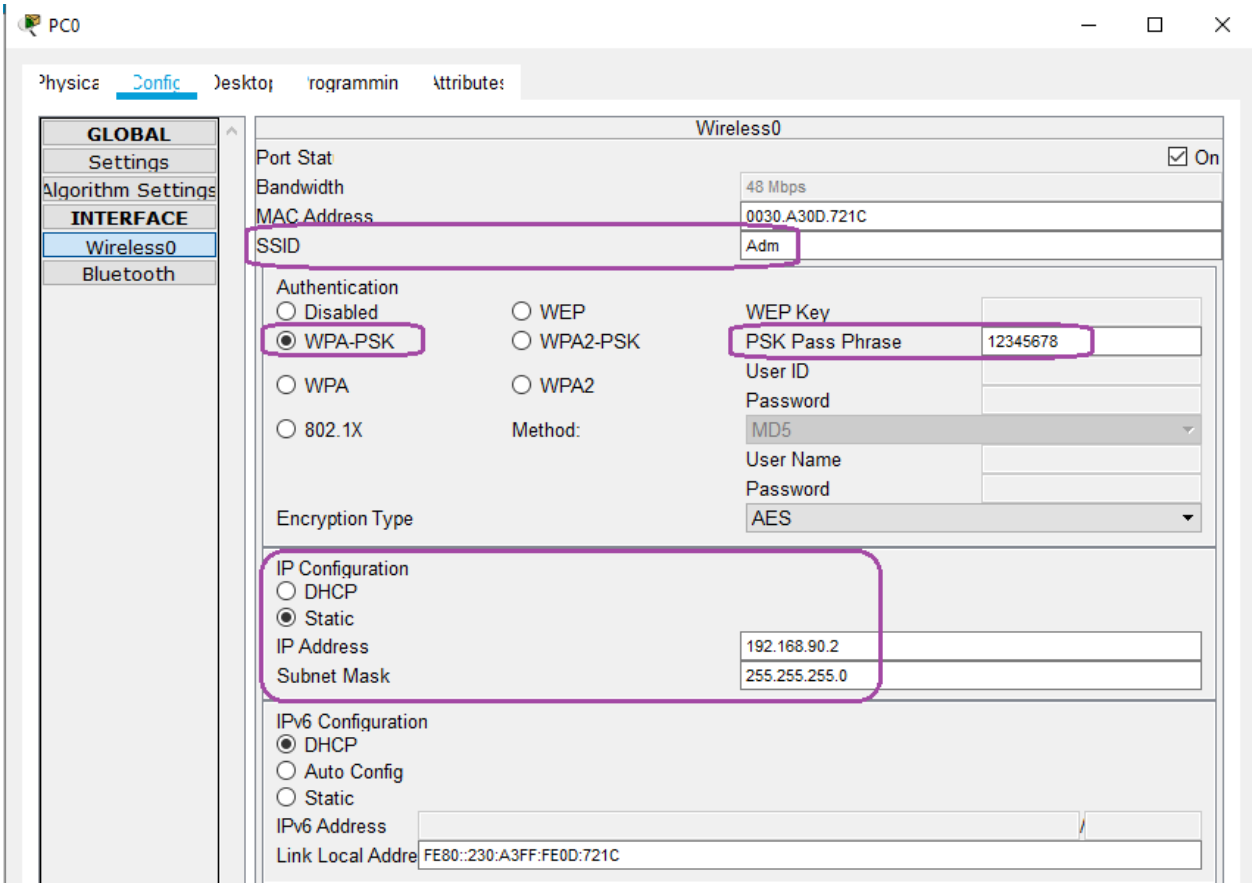


Рис. 9.12. Включаємо технологію захисту WPA

Тепер зайдемо *маршрутизатор* (рис. 9.13) і, щоб включити бепроводовий ***зв'язок***, наберемо *логін* і *пароль*(рис. 9.14).

Рис. 9.13.Роутер потребує провести автентифікацію

UserName : tester
Password: testing

Рис. 9.14. Логін і пароль для зв’язку безпроводових пристроїв

Після проведення автентифікації зв’язок буде встановлено (рис. 9.15).

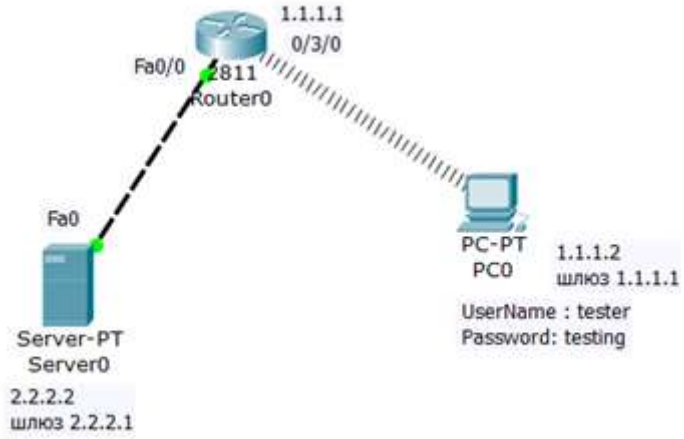


Рис. 9.15.Наявність з'єднання в мережі

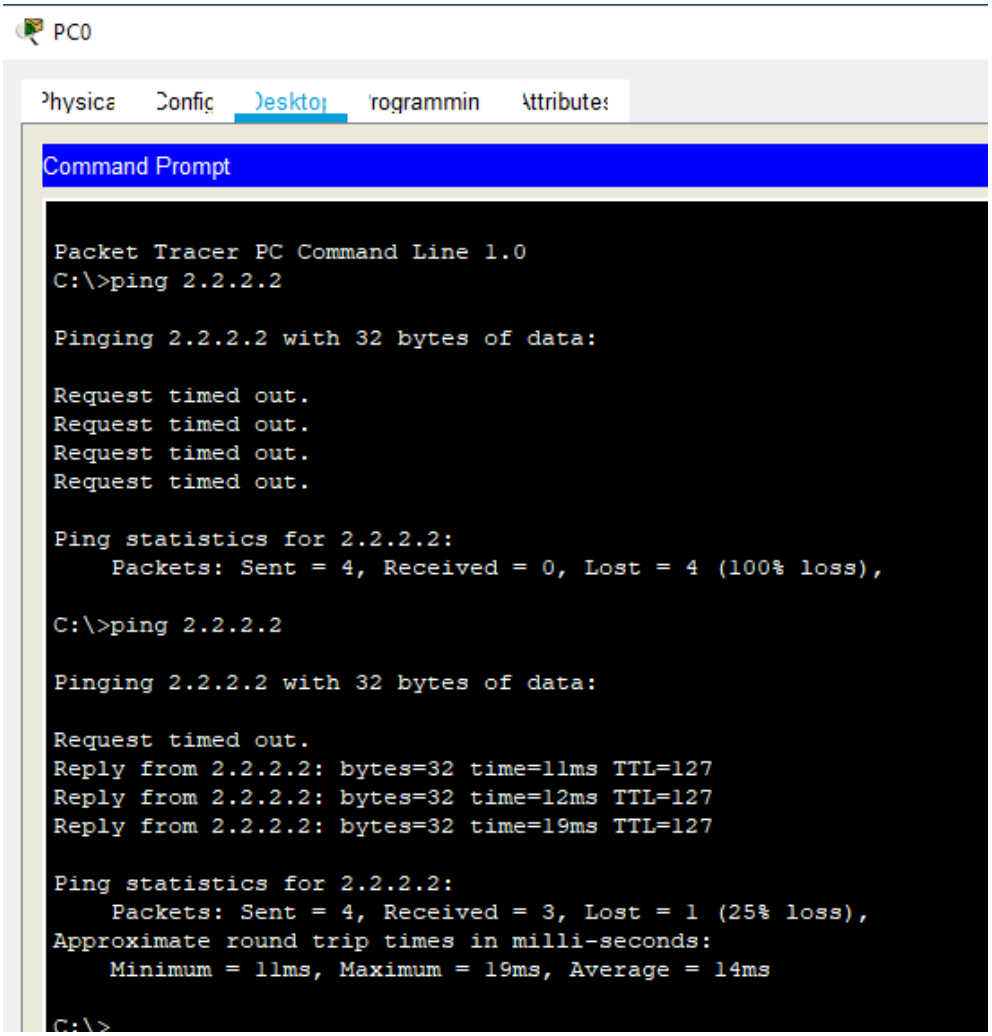


Рис.9.16. Пінгування серверу з ПК

Безпроводова мережа з точкою доступу

Нижче розглянемо два приклади налаштування безпроводових WI-FI мереж.

Завдання 9.3. Безпроводова мережа з точкою доступу

Зберіть схему мережі, представлену нарис. 9.17.

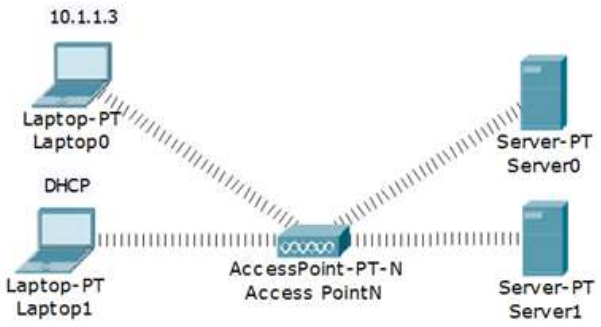


Рис. 9.17.Схема мережі

Рис.9.18. Встановлення бездротового мережевого адаптера на сервер

Рис.9.19. Встановлення бездротового мережевого адаптера на ноутбук

Wireless Access Point

Точка доступу в англійській термінології – **Wireless Access Point**. Розглянемо налаштування точки доступу, вони такі самі за замовчуванням (рис. 9.20).

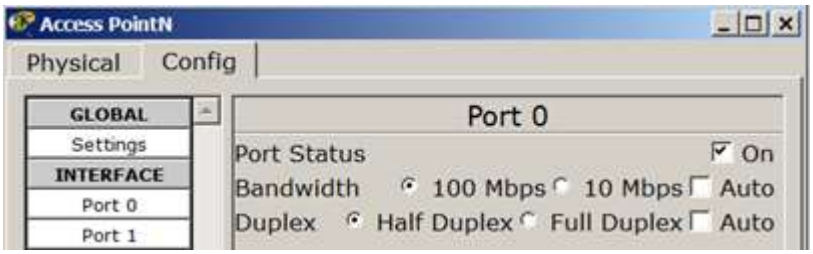


Рис. 9.20.Налаштування точки доступу

Статичне налаштування ноутбука (рис. 9.21).

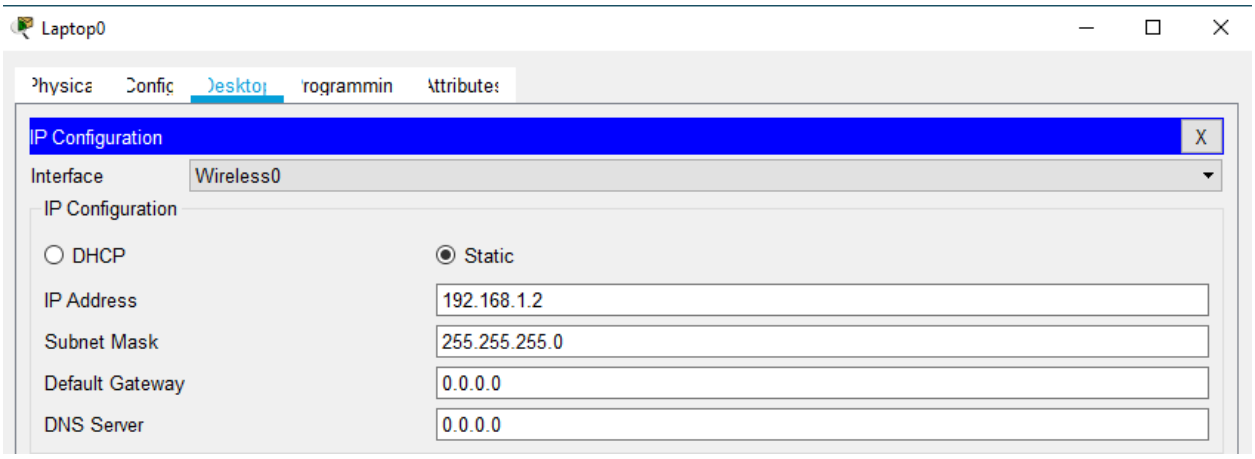


Рис. 9.21.Задаємо IP адресу для L0

Динамічне налаштування ноутбука (рис. 9.22).

Рис. 9.22.Включаємо перемикач DHCP для L1

Налаштування серверів (рис. 9.23).

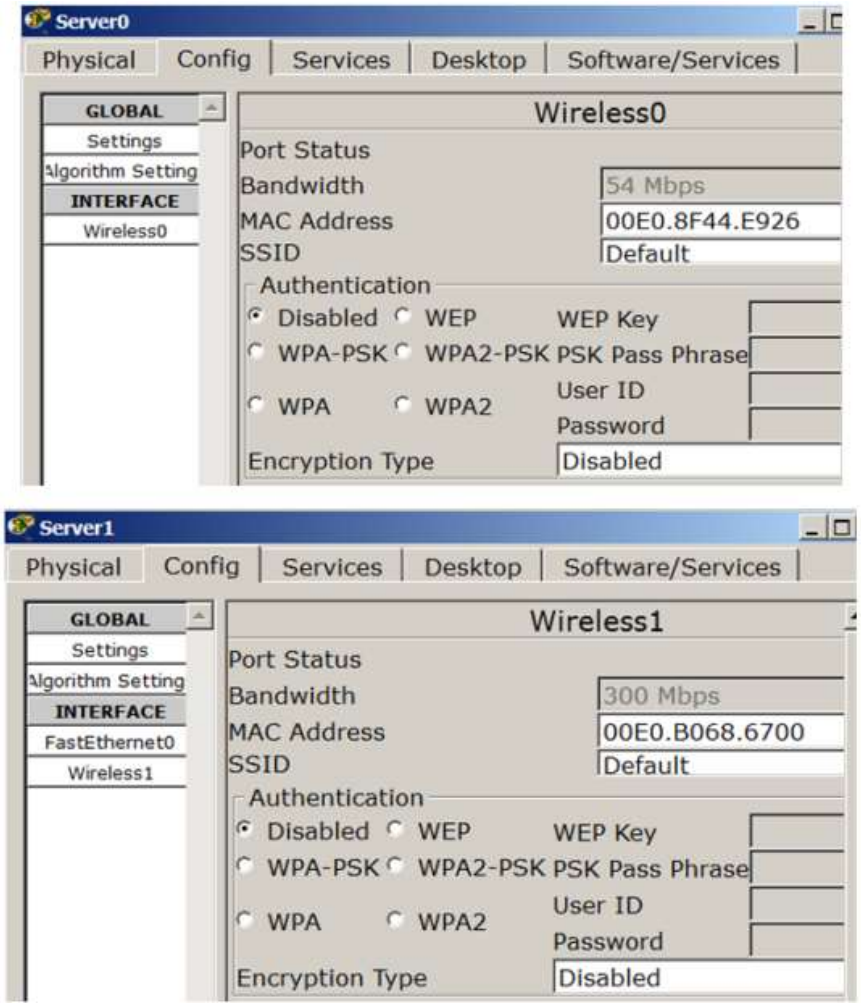


Рис. 9.23.Сервера налаштовані за замовчуванням

Точку доступу *POINT N* можете замінити на *POINT 0*, при цьому налаштування хостів можна не міняти (рис. 9.24).

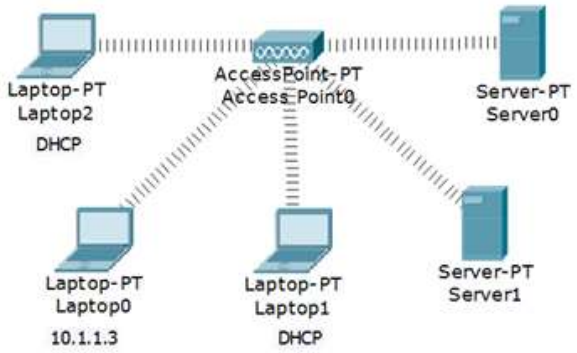


Рис. 9.24.Безпроводовий зв’язок встановлено

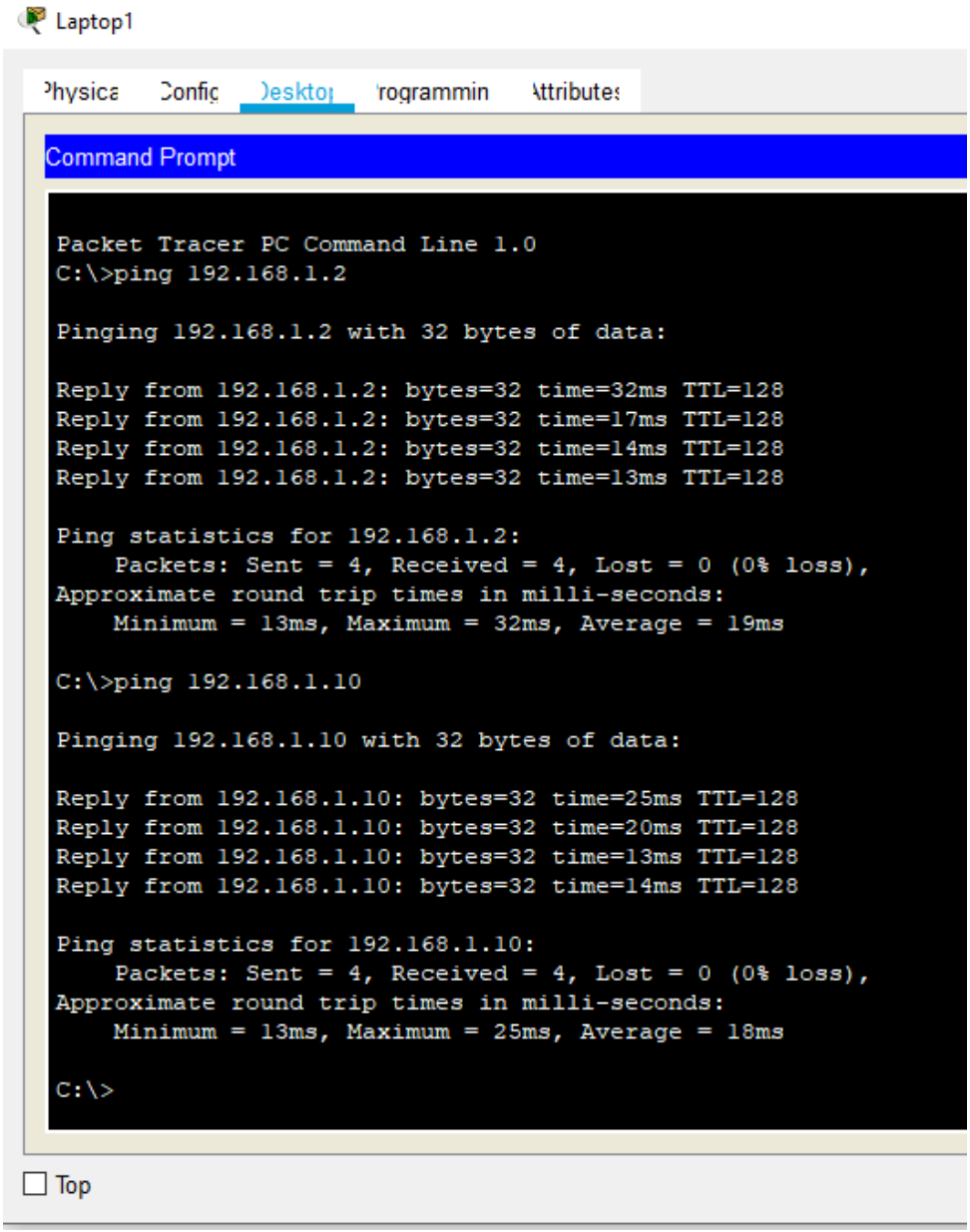


Рис.9.25. Пінгування ноутбука 0 та серверу 0

Завдання 9.4. Безпроводова мережа між офісами

Налаштуємо наступну безпроводову мережу (рис. 9.26).

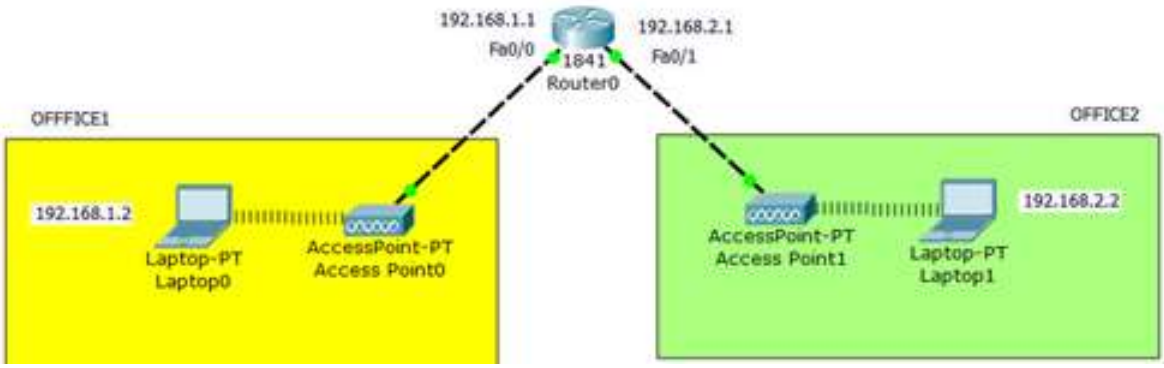


Рис. 9.26. WI-FI мережа між офісами

Облаштовуємо ноутбуки *wi-fi* адаптерами WPC300N. Налаштування обох ноутбуків аналогічні (рис. 9.27).

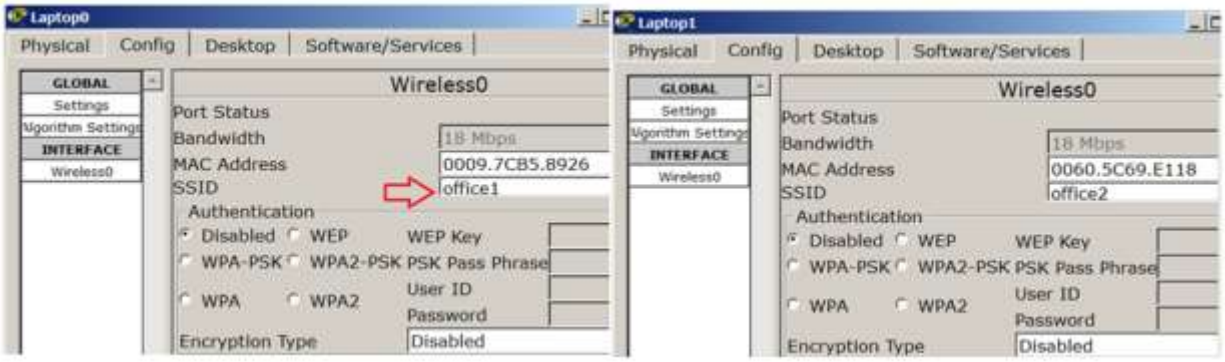


Рис. 9.27.Налаштування ноутбуків

Примітка

Кожна безпроводова локальна мережа використовує унікальне мережеве ім'я для ідентифікації мережі. Це ім'я також називається ідентифікатором обслуговування мережі - SSID. Коли встановлюється адаптер Wi-Fi, потрібно вказати SSID. Якщо потрібно підключитися до існуючої бездротової мережі, необхідновикористовувати ім'я цієї мережі. Ім'я може мати довжину до 32 символів і містити букви і цифри.

Крім SSID на ноутбуках налаштовується шлюз (рис. 9.28).

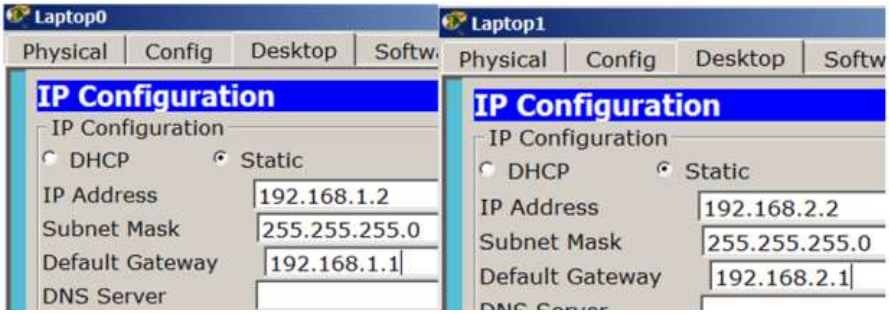


Рис. 9.28. На L0 і L1 вказуємо адресу шлюзу

SSID задаємо на обох точках доступу (рис. 9.29).

Рис. 9.29. Задаємо SSID на точках доступу

Перевіряємо зв'язок ПК з різних офісів (рис. 9.30).

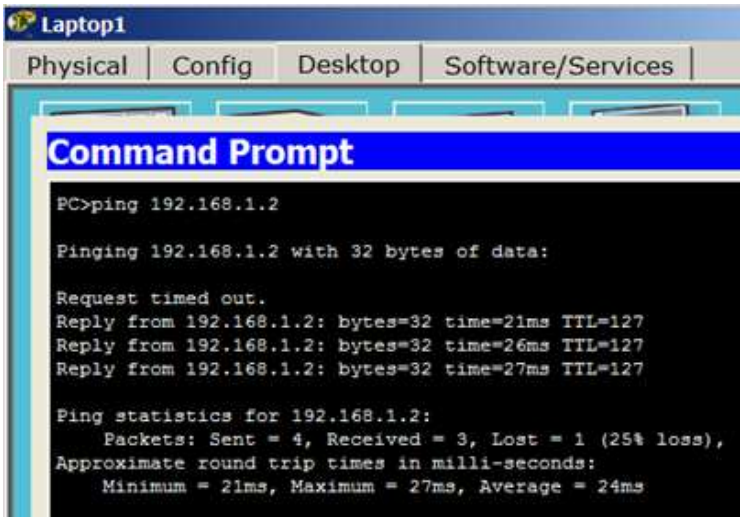


Рис. 9.30.Зв’язок L1 і L0 присутній

Налаштування комутованого WI-FI з'єднання

Завдання 9.5. Налаштування комутованого WI-FI з'єднання

Зберемо і налаштуємо мережу, зображену на рис. 9.31.

Рис. 9.31.WI-FI мережа

Спочатку задаємо ім’я мережі (SSID) на точці доступу (рис. 9.32).

Рис. 9.32.Задаємо SSID на точці доступу

В обидва ПК вставляємо безпроводовий адаптер Linksys-WPM-300N (рис.9.33).

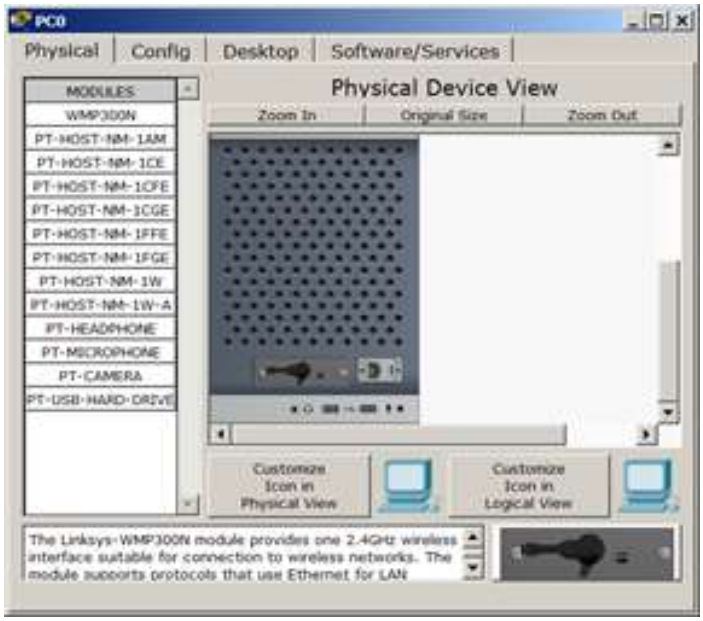


Рис. 9.33.Адаптер Linksys-WPM-300N вставлений в PC0

Встановлюємо зв'язок точки доступу і PC0, для цього натискаємо на кнопку PC Wireless (рис. 9.34).

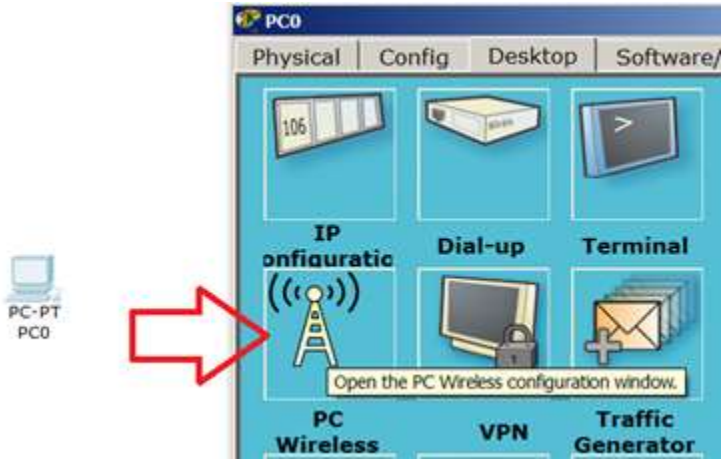


Рис. 9.34.Натискаємо на кнопку PC Wireless

Тепер відкриваємо вкладку Connect і натискаємо на кнопку Connect (рис.9.35).

Рис. 9.35.Підключення ноутбука до доточки доступу

В результаті у нас виходить динамічний зв'язок PC0 і Access Point-PT (рис.9.36).

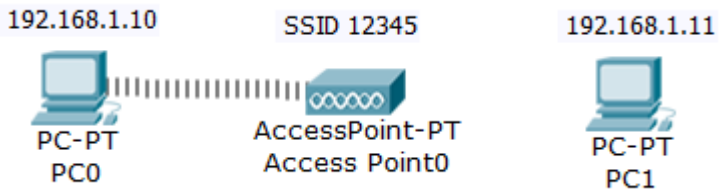


Рис. 9.36. Динамічний зв'язок точки доступу і безпроводового адаптера

Міняємо динамічну адресу на статичну (рис. 9.37).

Рис. 9.37. Міняємо динамічну адресу на статичну

Тепер аналогічно налаштовуємо PC1 і перевіряємо зв’язок між ПК (рис. 9.38).

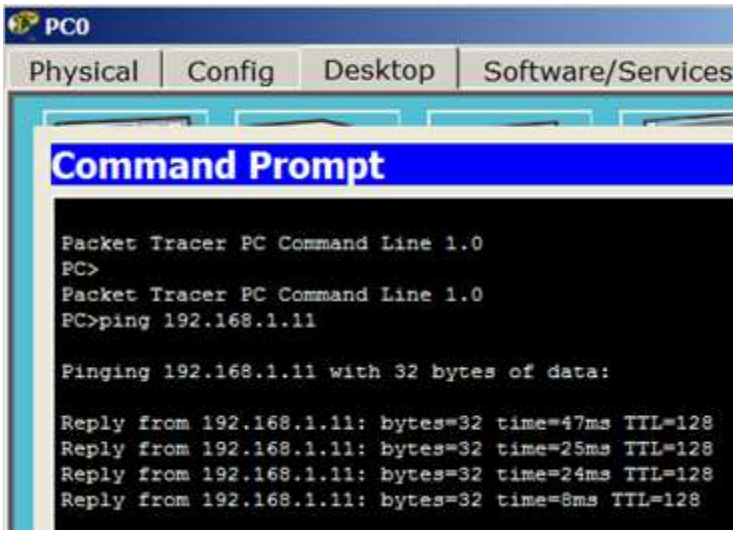


Рис. 9.38. Зв'язок між ПК відмінний

Завдання 9.6.Безпроводовий зв'язок в Packet Tracer з безпроводовим роутером

Нарис. 9.39 приведена схема мережі з безпроводовим роутером.

Рис. 9.39. Схема мережі з безпроводовим роутером

Якщо забезпечимо обидва ПК безпроводовим модулем, то в даній мережі можемо спостерігати появу WIFI зв'язку (рис. 9.40).

Рис. 9.40. Мы можем спостерігати появу WIFI зв'язку

Зайдемо на роутер і подивимося на його IP address. Як бачимо, включений DHCP service і роутер отримує IP адресу автоматично (рис. 9.41).

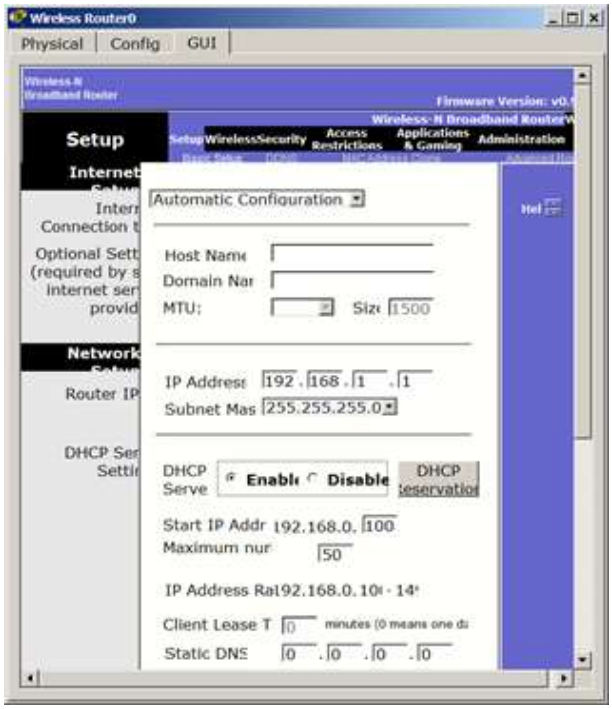


Рис. 9.41.Автоматичне конфігурування роутера

Тепер на вкладці Config налаштуємо автентифікацію роутера (рис.9.42).

Рис. 9.42. Вводимо SSID і WPA2-PSK

Тепер для PC0 заходимо в меню PC Wireless (рис. 9.43).

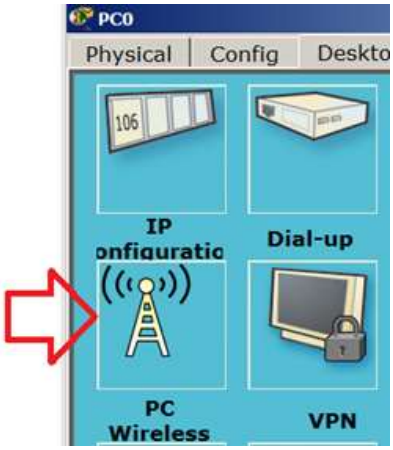


Рис. 9.43.Заходимо в меню PC Wireless

Встановлюємо з’єднання PC0 і роутера (рис. 9.44).

Рис. 9.44. На вкладці Connect натискаємо на кнопку Connect

Для автентифікації необхідний WPA2-PSK пароль, тобто 1234567890 (рис.9.45).

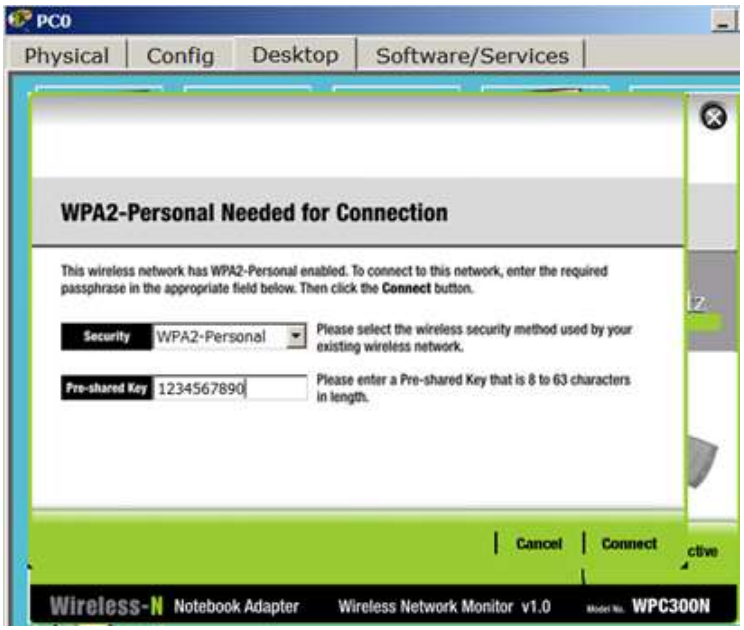


Рис. 9.45. Вводимо пароль і натискаємо на кнопку Connect

Примітка

Протокол безпеки WPA2-PSK - спрощений варіант WPA2. Технології захисту

бездротових мереж WPA2 є найкращою на сьогоднішній день. Але, з міркувань сумісності на маршрутизаторах можна зустріти її варіант WPA2-PSK.

Отже, ми пред'явили наш "пропуск" на вхід користувача в мережу і зв'язок пристроїв встановлена (рис. 9.46).

Рис. 9.46.Зв’язок PC0 і роутера налаштовано

Тепер вводимо пароль на PC1 (рис. 9.47).

Рис. 9.47.З’явився зв’язок роутера і PC1

Дізнаємося динамічну IP адресу для PC1

```
Port        Link   IP Address
Wireless0   Up     192.168.0.101/24

Gateway: 192.168.0.1
DNS Server:  <not set>
Line Number:  <not set>
```

і пінгуємо її з PC0 (рис. 9.48).

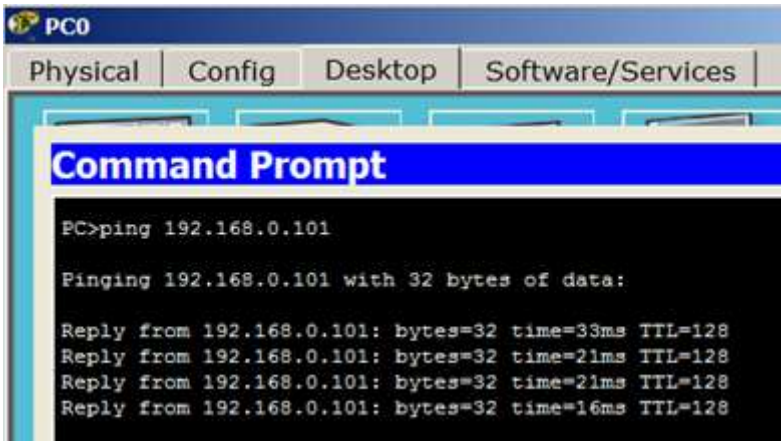


Рис. 9.48.Зв’язок між PC0 і PC1 є

Склад звіту лабораторної роботи

В звіті повинно бути відображено:

1. Тема роботи.
2. Мета роботи.
3. Виконання завдання 9.1 з відповідними скріншотами.
4. Виконання завдання 9.2 з відповідними скріншотами.
5. Виконання завдання 9.3 з відповідними скріншотами.
6. Виконання завдання 9.4 з відповідними скріншотами.
7. Виконання завдання 9.5 з відповідними скріншотами.
8. Виконання завдання 9.6 з відповідними скріншотами.
9. Висновки

Контрольні питання

1. Варіанти побудови мережі радіодоступу та види послуг, що надаються.
2. Етапи створення нової бездротової мережі.
3. Ключ безпеки безпроводової мережі.
4. Дайте визначення Wi-Fi.
5. Що собою представляє WEP (Wired Equivalent Privacy).
6. Технологія WPA (Wi-Fi Protected Access).

Література

1. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 4-е изд. — СПб.: Питер, 2010. — С. 438. — 4500 экз. — ISBN 978-5-49807-389-7.
2. Компьютерные сети. 4-е изд./ *И. Таненбаум*. – СПб.: Питер, 2003. – 992 с.
3. *Жураковский Б. Ю.* Комп'ютерні мережі. Частина 1. Навчальний посібник [Електронний ресурс] / *Б. Ю. Жураковский, І. О. Зенів* // КПІ ім. Ігоря Сікорського. – 2020. – 336 с. – Режим доступу до ресурсу: https://ela.kpi.ua/handle/123456789/36615.
4. *Жураковський Б. Ю.* Комп'ютерні мережі. Частина 2 Навчальний посібник [Електронний ресурс] / *Б. Ю. Жураковский, І. О. Зенів* // КПІ ім. Ігоря Сікорського. – 2020. – 372 с. – Режим доступу до ресурсу: https://ela.kpi.ua/handle/123456789/36641
5. *Уэнделл Одом*. Компьютерные сети. Первый шаг // Computer Networking First-step. – М.: «Вильямс», 2005. – С. 432.
6. *Новиков Ю. В., Кондратенко С. В.* Основы локальных сетей. Курс лекций. – М.: Интернет-университет информационных технологий, 2005. – ISBN 5-9556-0032-9.
7. *Амато Вито* Основы организации сетей Cisco, Том 1, Пер. с англ. – М.: Издательский дом «Вильяме», 2004. - 512 с.
8. *Амато Вито* Основы организации сетей Cisco, Том 2, Пер. с англ. – М.: Издательский дом «Вильяме», 2004. - 464 с.
9. *Zhurakovskiy B.* Assessment. Technique and Selection of Interconnecting Line of Information Networks [Електронний ресурс] / *B. Zhurakovskiy, N. Tsopa* // 3rd International Conference on Advanced Information and Communications Technologies (AICT). – 2019. – Режим доступу до ресурсу: DOI: 10.1109/AIACT.2019.8847726. *Proceedings (2019) 71-75.*