МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ МІСЬКОГО ГОСПОДАРСТВА імені О. М. БЕКЕТОВА

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

до проведення практичних занять та організації самостійної роботи
з навчальної дисципліни

«КОМП'ЮТЕРНІ МЕРЕЖІ»

(для здобувачів першого (бакалаврського) рівня вищої освіти
денної та заочної форм навчання
зі спеціальності 122 – Комп'ютерні науки,
освітньо-професійна програма «Комп'ютерні науки»)

Харків
ХНУМГ ім. О. М. Бекетова
2023

Методичні рекомендації до проведення практичних занять та організації самостійної роботи з навчальної дисципліни «Комп’ютерні мережі» (для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання зі спеціальності 122 – Комп’ютерні науки, освітньо-професійна програма «Комп’ютерні науки» / Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова ; уклад. К. В. Плахотніков. – Харків : ХНУМГ ім. О. М. Бекетова, 2023. – 115 с.

Укладач канд. техн. наук, доц. К. В. Плахотніков

Рецензент

Н. Д. Сізова, доктор фізико-математичних наук, професор, професор кафедри комп’ютерних наук та інформаційних технологій Харківського національного університету міського господарства імені О. М. Бекетова

Рекомендовано кафедрою комп’ютерних наук та інформаційних технологій, протокол № 9 від 27 січня 2023 р.

Методичні рекомендації призначені для здобувачів спеціальності 122 – Комп’ютерні науки. Подано засоби та послідовність виконання завдань, запитання для самопідготовки, список рекомендованих джерел тощо.

ЗМІСТ

ВСТУП

Метою навчальної дисципліни «Комп'ютерні мережі» є формування у здобувачів вищої освіти здатності володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення, застосовувати знання у практичних ситуаціях та вчитися й оволодівати сучасними знаннями.

Завдання навчальної дисципліни «Комп'ютерні мережі» є теоретична й практична підготовка здобувачів вищої освіти щодо організації робіт із створення та налаштування комп'ютерних мереж.

Тематика практичних занять включає розгляд реальних ситуацій у комп'ютерних мережах, вирішення завдань, пов'язаних з налаштування пристроїв різних рівнів The open systems interconnection model (OSI), опитування з теоретичної частини прочитаних викладачем лекцій, перевірку знань щодо запитань для самопідготовки.

Заняття включає проведення попереднього контролю знань, удосконалення вмінь і навичок здобувачів вищої освіти, постановку загальної проблеми викладачем та її обговорення за участю здобувачів вищої освіти, розв'язування завдань з їх обговоренням, перевіркою і оцінюванням.

Під час проведення практичних занять організовується дискусія щодо попередньо визначених тем, до яких здобувачі готують доповіді, а також обговорюються проблемні питання, на які мають бути знайдені відповіді в результаті дискусії. На практичних заняттях у здобувачів мають сформуватися вміння і навички розробки, організації та впровадження комп'ютерних мереж.

У процесі проведення практичного заняття здобувачі самостійно вирішують запропоновані завдання різного рівня складності, проектують елементи комп'ютерних мереж.

З метою виявлення рівня засвоєння матеріалу викладачем проводиться перевірка і обговорення роботи, яку виконували здобувачі, а також підведення

підсумків з одержанням здобувачами вищої освіти відповідної оцінки залежно від результатів виконаної роботи.

Варто зазначити, що проведення практичних занять вимагає наявності попередньо підготовленого матеріалу. За кожне практичне заняття фіксуються оцінки, що враховуються при виставленні модульної оцінки з даної навчальної дисципліни.

Самостійна робота над засвоєнням навчального матеріалу з дисципліни може виконуватися в домашніх умовах. Виконання завдань із самостійної та роботи є обов'язковим для кожного здобувача вищої освіти.

Заключною формою самостійної роботи є підготовка до поточного контролю зі змістових модулів. Вона базується на систематичному вивченні лекційного матеріалу, питань, розглянутих на заняттях, а також проблемних питань, досліджених самостійно, й умінні логічно викладати їх суть.

Таким чином, практичні заняття разом з лекційним курсом і самостійною роботою формують професійну складову здобувачів вищої освіти, завдяки чому вони можуть швидше адаптуватися в умовах Європейської інтеграції.

1 ПРАКТИЧНА РОБОТА

Практичне заняття №1

СТВОРЕННЯ НАЙПРОСТІШОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Мета заняття – опанувати навички підключення двох комп'ютерів у єдину комп'ютерну мережу.

Для початку роботи встановлюємо програму «Cisco Packet Tracer» (CPT), яку надає викладач. Після встановлення програми повинно відкритися стартове вікно програми (рис. 1.1).

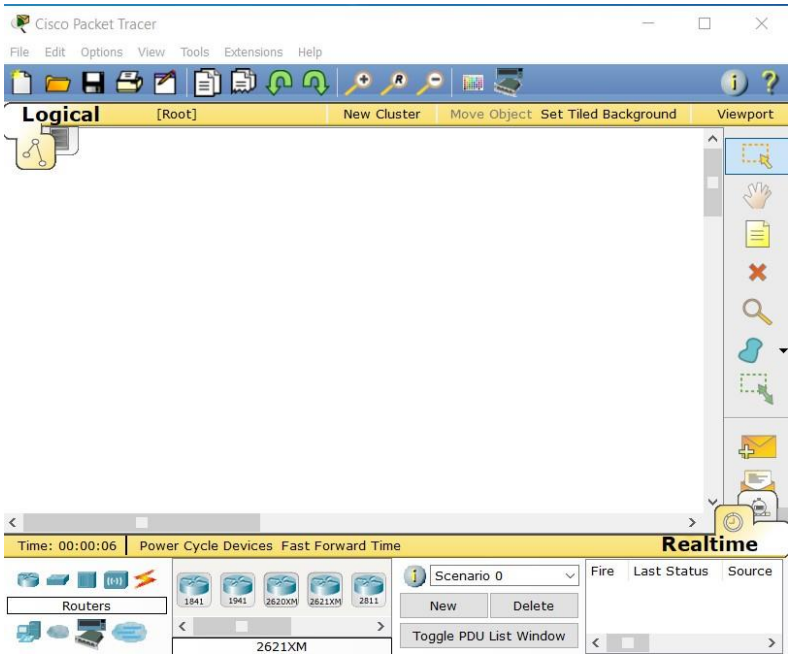


Рисунок 1.1 – Стартове вікно програми Cisco Packet Tracer після інсталяції

Для виконання лабораторної роботи необхідні два комп'ютери та комутаційний кабель (патч-корд) (рис. 1.2).

Рисунок 1.2 – Зовнішній вигляд патч-корду

У випадку відсутності патч-корду нам знадобиться кабель вітої пари та два конектори. Зауважимо, що існують два види комутаційних кабелів, такі як, прямий кабель (для з'єднання комп'ютер-комутатор та комутатор-маршрутизатор, тобто для приладів різного рівня сітьової моделі OSI) та перехресний кабель (для з'єднання комп'ютер з комп'ютером, комутатор з комутатором та маршрутизатор з маршрутизатором).

Прямий кабель може бути обжатий по стандарту А та стандарту Б.

У подальшому переходимо у вкладку «End devices», обираємо комп'ютер та перетягуємо його у робочу область. Так само перетягуємо ще один комп'ютер (рис. 1.3).

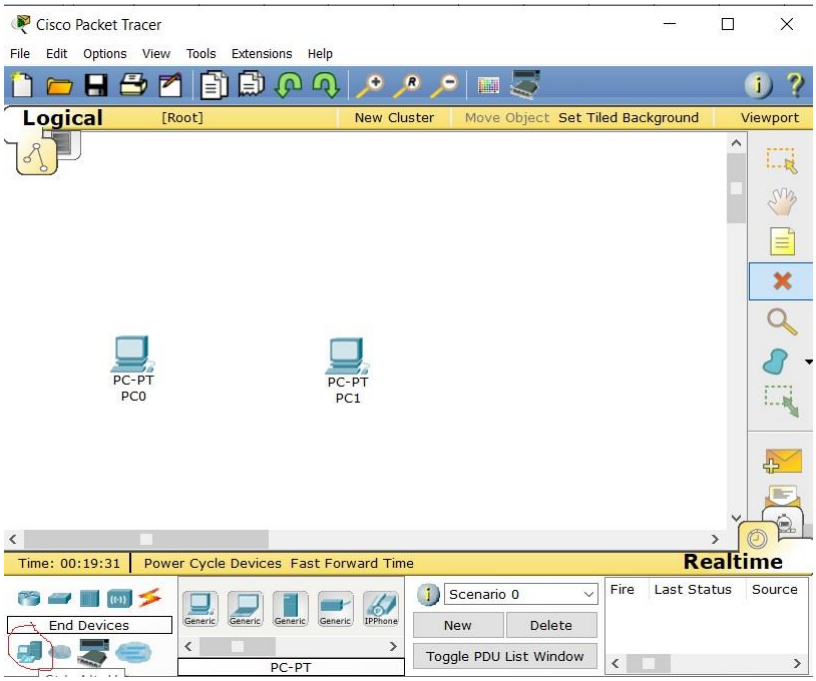


Рисунок 1.3 – Розміщення двох комп'ютерів на робочому аркуші

Переходимо у вкладку «Connections » та обираємо тип кабелю. Маємо на увазі, що сучасні сітьові карти комп'ютера вміють визначати тип кабелю і підлаштовуватися під нього, тобто у реальному житті підійде як прямий, так і перехресний кабель. Однак програма потребує дотримуватися використання перехресного кабелю для з'єднання приладів одного рівня сітьової моделі OSI.

Натискаємо піктограму та лівою кнопкою миші клацаємо на комп'ютері PC0, обравши FastEthernet. Далі за тим же принципом обираємо комп'ютер PC1, отримуючи з'єднання, лінки загоряться зеленим кольором. Для

прикладу можна спробувати з’єднати два комп’ютери прямим кабелем , при цьому ми побачимо некоректність підключення (рис. 1.4).

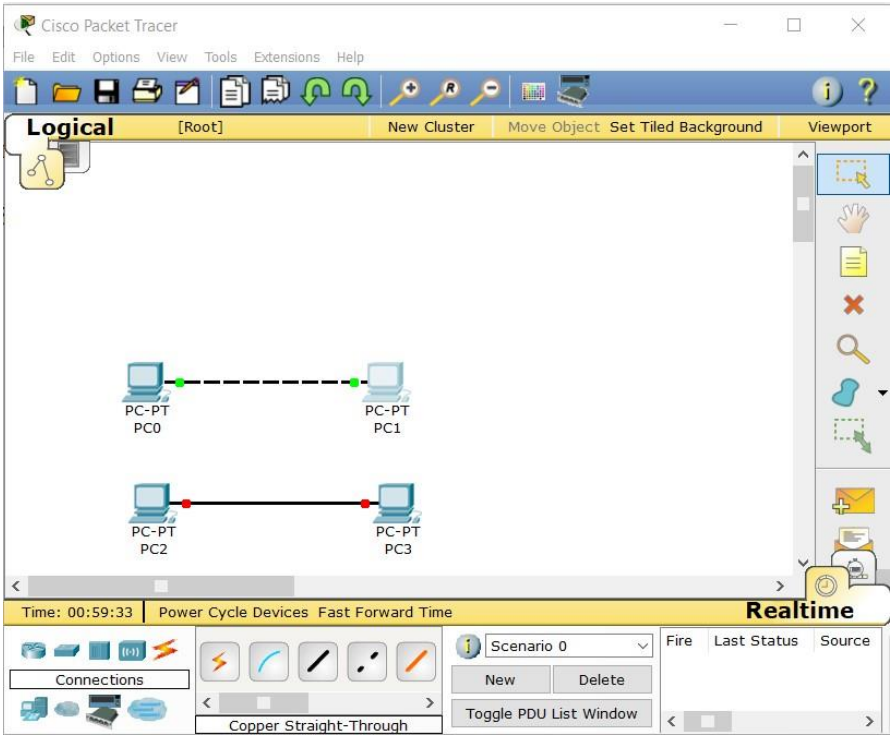


Рисунок 1.4 – Приклад коректного та хибного застосування типу кабелю

Переходимо до налаштування самого комп’ютера. Одинарним натисканням лівої клавіші мишки на ньому, відкриваємо його налаштування та переходимо до вкладки «Desktop» та обираємо пункт «Internet protocol (IP) Configuration» і прописуємо два параметри, наведених на рисунку 1.5.

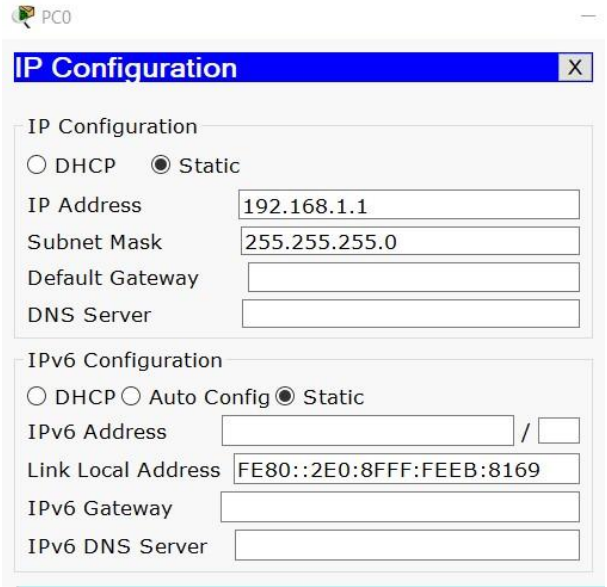


Рисунок 1.5 – Введення параметрів IP Configuration 192.168.1.1 та 255.255.255.0

Для другого комп’ютера також проводимо відповідні налаштування, а саме 192.168.1.2 та 255.255.255.0. Далі перевіряємо з’єднання. Натискаємо лівою кнопкою миші на першому комп’ютері, виконуємо команду Desktop-Command Prompt, вводимо 192.168.1.2, після чого перевіряємо, що з’єднання встановлено (рис. 1.6).

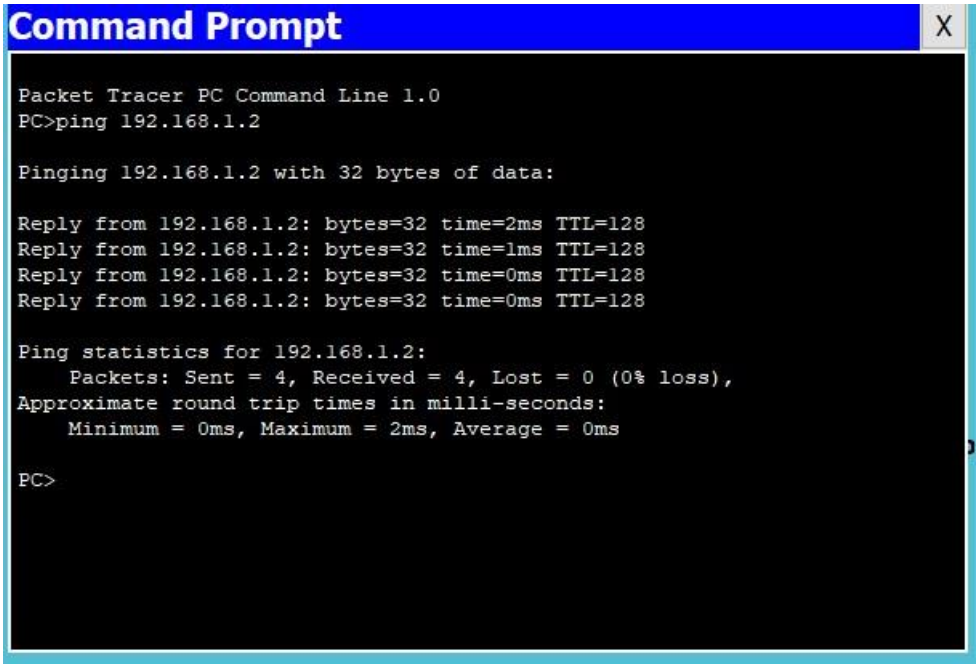


Рисунок 1.6 – Результат успішного встановлення з’єднання

Запитання для самопідготовки

1. У чому різниця обжимання кабелю по стандарту А та стандарту Б?
2. Що вам відомо про перехресний кабель?
3. Опишіть повний функціонал IP Configuration.
4. Яким чином перевірити коректність підключення кабелю?
5. Наведіть відомі вам види конекторів.

Практичне заняття №2
РОБОТА З КОМУТАТОРАМИ

Мета заняття – опанувати навички підключення комп’ютерів до хабу та комутатору, налаштувати передачу пакету даних від одного комп’ютера до іншого в рамках створеної комп’ютерної мережі.

Розглянемо ситуацію, коли у мережі, що ви створюєте, з’являється більше двох комп’ютерів, нам необхідний спеціальний прилад для підключення. Цей прилад або мережний концентратор – хаб (перевага лише у його вартості), який функціонує на першому рівні моделі OSI або комутатор (switch), який функціонує на другому рівні моделі OSI. Хаб відправляє пакти у всі порти, окрім порта джерела, а комутатор відправляє пакет лише у визначений порт за рахунок використання таблиці Media access control address (MAC-адреса).

Створюємо мережу з чотирьох комп’ютерів. Спочатку розміщуємо один комп’ютер та настоюємо йому Internet Protocol Address (IP-адресу) 192.168.1.2. Потім, виділивши його рамкою, зажав клавішу ctrl, перетягуємо у бік і створюємо копію існуючого комп’ютера. Причому копіюється комп’ютер з властивостями і налаштуваннями першоджерела. Лише у налаштуваннях змінюємо останню цифру IP-адреси з 2 на 3. Відповідні дії робимо ще для двох комп’ютерів (рис. 2.1).

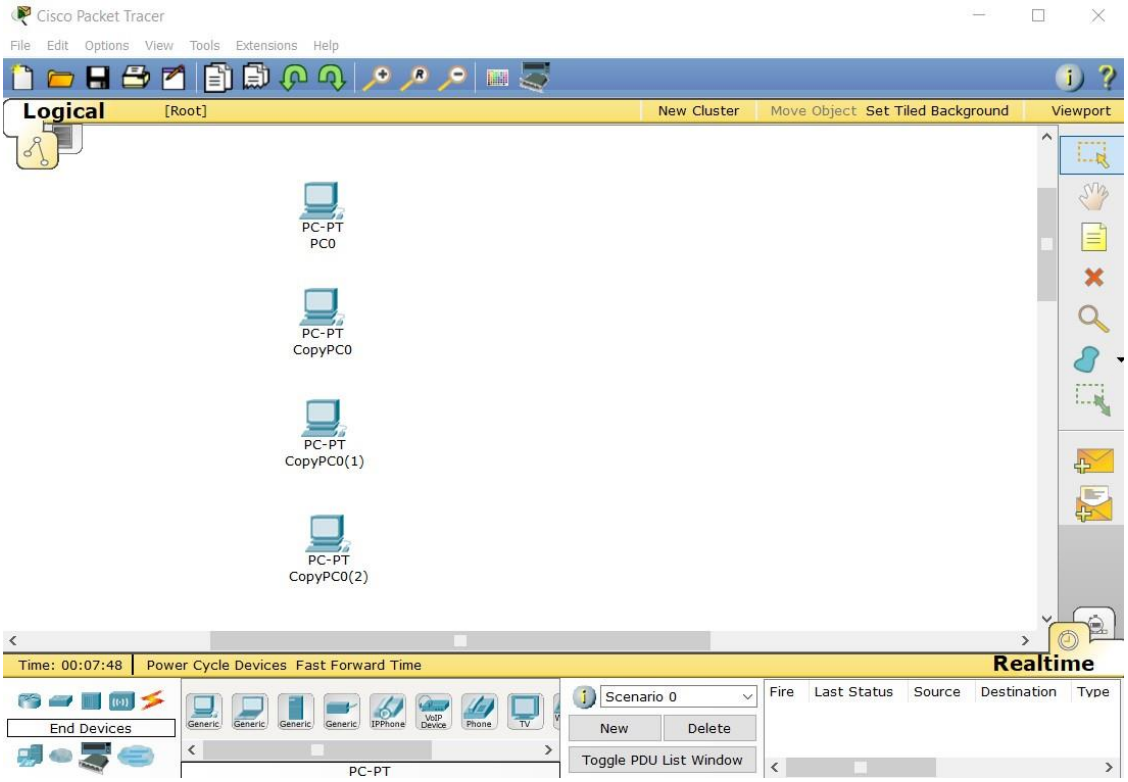


Рисунок 2.1 – Розміщення комп’ютерів за допомогою копіювання

У категорії Switches обираємо комутатор, наприклад 2960, після розміщення дивимося його властивості, наприклад, кількість портів (рис. 2.2).

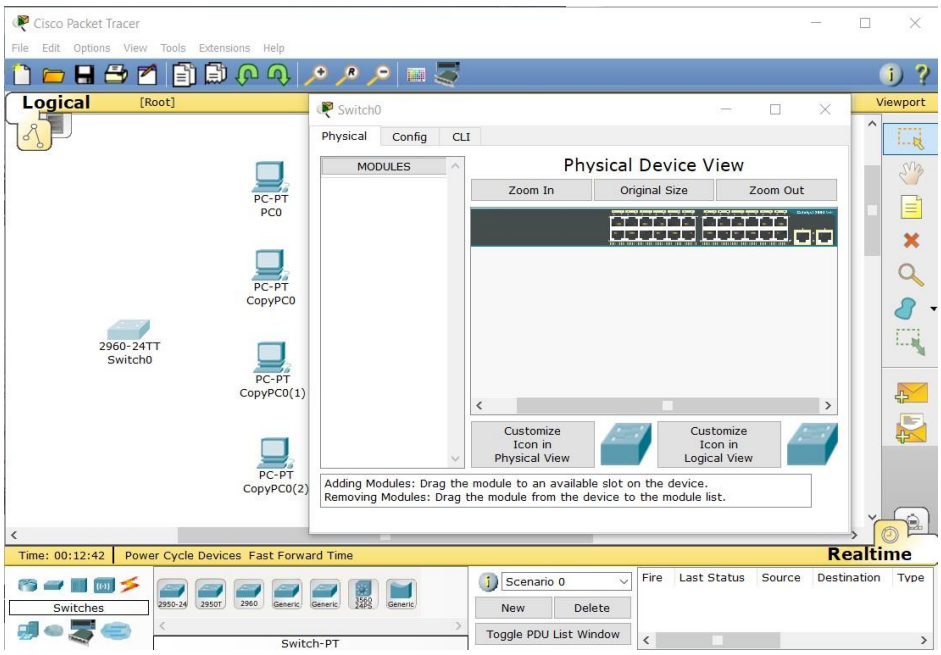


Рисунок 2.2 – Перегляд властивостей обраного комутатора

За допомогою прямого кабелю підключаємо комп’ютери до комутатора у послідовності Personal computer (PC) 0 до першого порту, CopyPC0 до другого порту. На комп’ютерах лінки не одразу загоряться зеленим, комутатору необхідно для цього деякий час. Далі перевіряємо з першого комп’ютера пінгування другого, третього та четвертого (рис. 2.3).

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

Рисунок 2.3 – Перевірка коректності підключення комп’ютерів до мережі

Далі перевіримо, як проходить пакет через комутатор та хаб. Для цього копіюємо чотири налаштовані комп'ютери, додаємо хаб (перший у переліку). Використаємо автоматичний підбір кабелю програми за допомогою піктограми  і з'єднаємо у мережу.

Перевіримо проходження пакету за допомогою AddSimplePDU  з першого на четвертий комп'ютера у мережі з комутатором та у мережі з хабом. Натискаємо піктограму і клацаємо лівою кнопкою миші спочатку на перший, потім на четвертий комп'ютер. Вмикаємо симуляцію комбінацією клавіш «Shift+S» або використовуємо піктограму  .

У вікні перетягуємо курсор у крайню ліву позицію і натискаємо Capture-Forward (рис. 2.4).

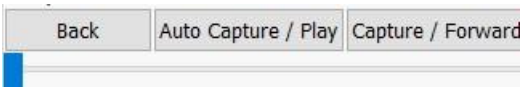


Рисунок 2.4 – Запуск відправки пакету при використання комутатора та хабу

При цьому пакет відправлено з першого комп'ютера, натиснувши ще раз, можемо побачити різницю між відправленням з комутатора та хабу (рис. 2.5).

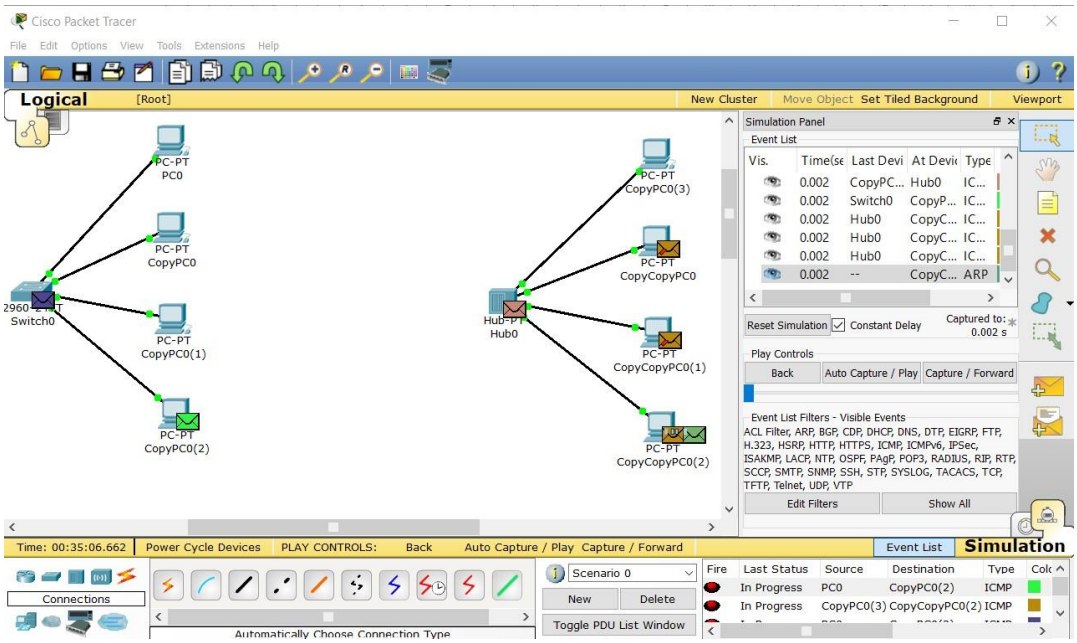


Рисунок 2.5 – Відправлення та отримання пакетів у мережі

Також можна переглянути дані пакету. Наприклад, у мережу з комутатором, натиснувши на пакеті з четвертого комп'ютера, отримуємо про нього інформацію (рис. 2.6).

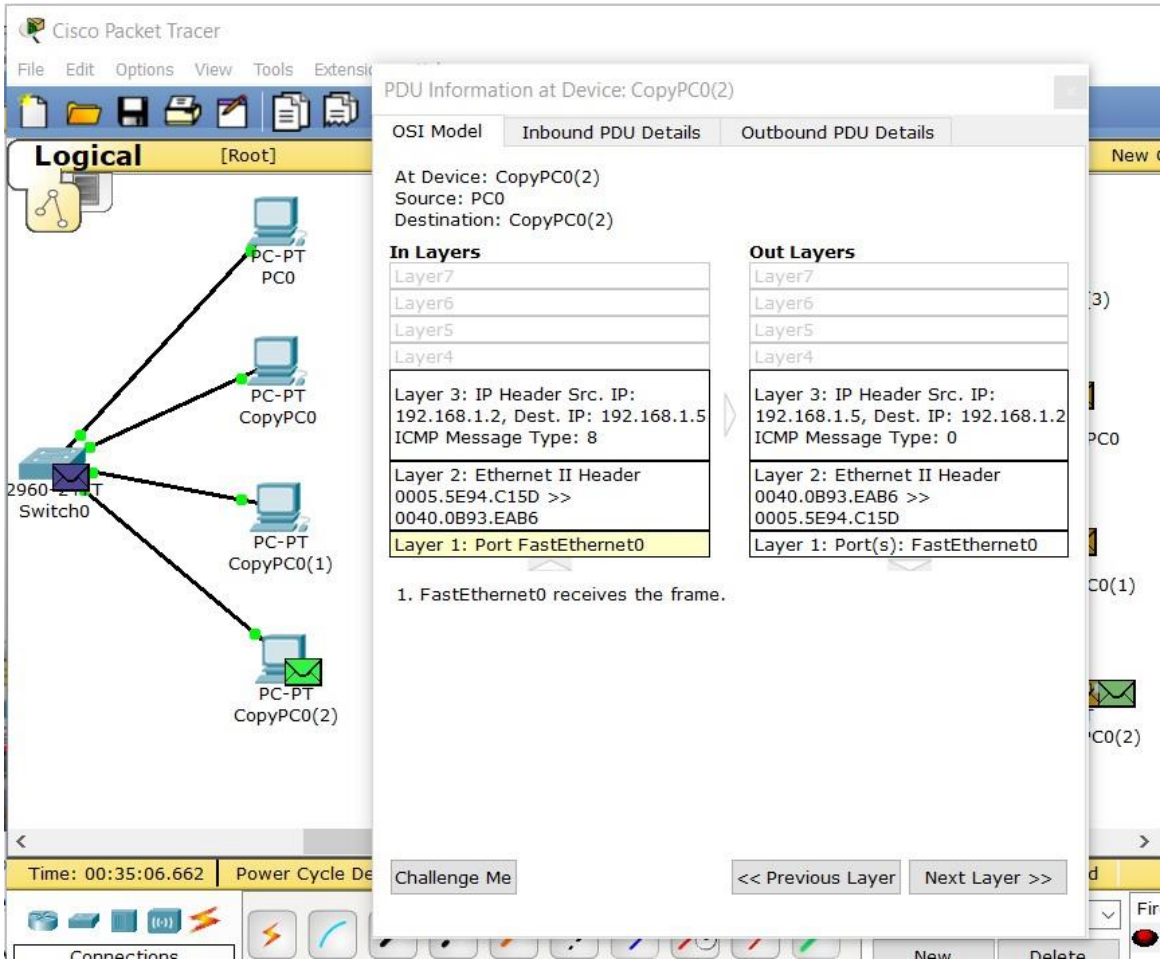


Рисунок 2.6 – Перегляд властивостей пакета

Далі, повторюючи дії, переглядаємо зворотне відправлення пакету.

Запитання для самопідготовки

1. У чому полягає різниця між першим та другим рівнем моделі OSI?
2. Наведіть основні недоліки використання хабу порівняно з комутатором.
3. Наведіть найбезпечніший пристрій між хабом та комутатором.
4. Яким чином проходить перевірка працездатності мережі при підключенні хабом та комутатором? Які спільні риси та відмінності?
5. Яка різниця між створенням нового комп’ютера у програмі CPT та копіюванням за допомогою клавіші ctrl?
6. Наведіть основні технічні характеристики комутатора.
7. Який тип кабелю застосовують при підключенні хабу та комутатора до мережі?

Практичне заняття №3

ПІДКЛЮЧЕННЯ ДО МЕРЕЖНОГО ОБЛАДНАННЯ

Мета заняття – проаналізувати існуючі методи підключення комп'ютерної техніки до комутатора та налаштування комутатора.

Для виконання даного завдання використовуємо комутатор Cisco 2960 (рис. 3.1).

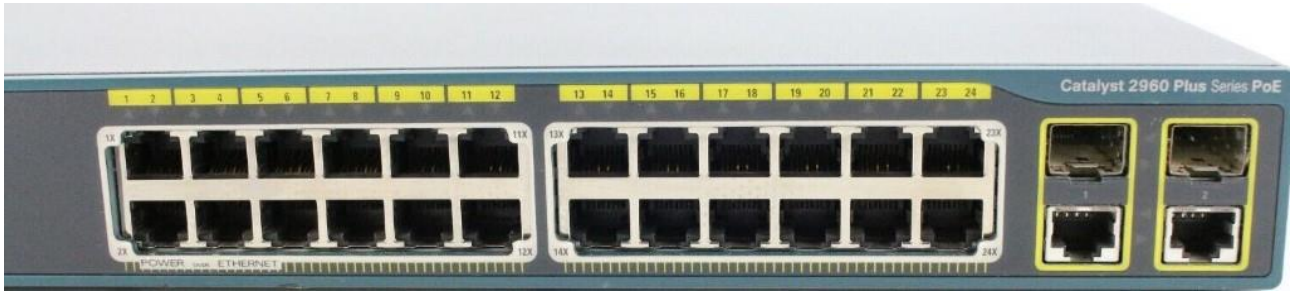


Рисунок 3.1 – Зовнішній вигляд комутатора Cisco 2960

Необхідно налаштувати даний комутатор. Це можна зробити за допомогою консольного кабелю, з використанням протоколу «Telnet», протоколу «Secure SHell» (SSH), web-інтерфейсу, спеціалізованого програмного забезпечення тощо. Розглянемо підключення за допомогою консольного кабелю. Для цього у комутаторі існує консольний порт (рис. 3.2).

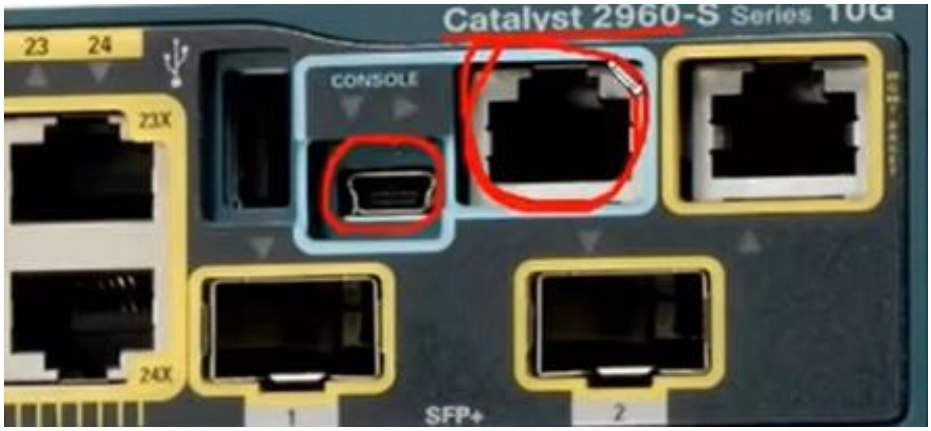


Рисунок 3.2 – Зовнішній вигляд консольних портів

Для першого підключення знадобиться комп'ютер (з наявністю com-порту), консольний кабель (рис. 3.3), перехідник «Universal Serial Bus - Communications port» (USB-COM) (рис. 3.4) та відповідне програмне забезпечення (наприклад putty, secure srt).

Рисунок 3.3 – Зовнішній вигляд консольних кабелів

Рисунок 3.4 – Зовнішній вигляд перехідника USB-COM

У програмі CPT спочатку підключаємося по консолі. Для цього Розміщуємо комп’ютер та комутатор 2960, за допомогою консольного кабелю , проводимо з’єднання через порт RS232 на комп’ютері до порту консоль на комутаторі. Потім виконуємо команду на комп’ютері «Desktop-terminal» і бачимо основні властивості порта, а саме швидкість, дата біт тощо, вони нам підходять, тому ми їх залишаємо (рис. 3.5), натискаємо OK і потрапляємо до нашого комутатора.

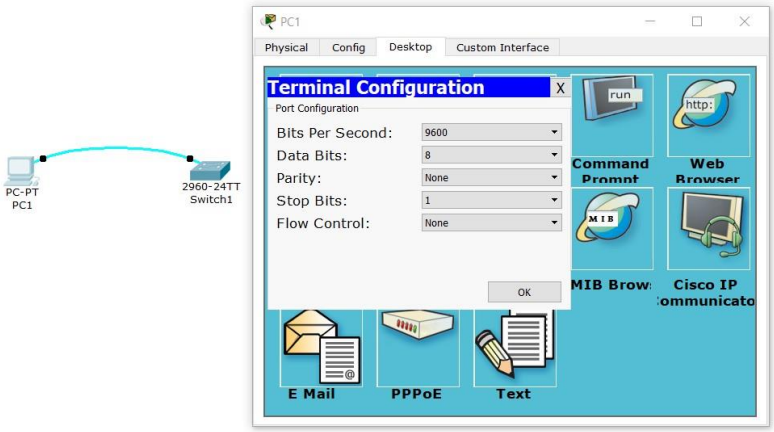


Рисунок 3.5 – Властивості com-порту комп’ютера

Натиснувши знак питання можна отримати список команд операційної системи комутатора, але не у повній кількості, оскільки ми працюємо у користувацькому режимі. Для входу у розширений режим виконуємо *enable*. Після цього знов вводимо знак питання і бачимо розширений список команд, використовуючи пробіл для гортання сторінок. Для повернення у користувацький режим вводимо *disable*. (можна ввести dis і система автоматично допише необхідну вам команду).

Далі входимо в режим глобального конфігурування у розширеному режимі ввівши *conf t (configure terminal)*. Задаємо власний пароль (наприклад CPT) вводом *enable password CPT*. Тепер, ввійшовши у користувацький режим, пробуємо зайти у розширений. Програма буде вимагати пароль, який ми створили раніше. За допомогою *show run* можемо переглянути конфігурацію (рис. 3.6).

```
Switch#show run
Building configuration...

Current configuration : 1059 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
enable password CPT
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
```

Рисунок 3.6 – Використання *show run* для перегляду створеного паролю

Але проблема полягає у тому, що ми пароль бачимо. Для усунення цього недоліку заходимо в режим глобального конфігурування та вводимо *Switch(config)#service password-encryption*. Для виходу з режиму конфігурації вводимо exit. Тепер, виконавши *Switch#show run*, замість нашого паролю ми побачимо запис, наприклад, *enable password 7 08027C7A*, і не побачимо реальний пароль СРТ.

Також існує ще один засіб захисту, а саме *Switch(config)#enable secret CPT1*. Переглянувши конфігурацію з поточного режиму *Switch(config)#do show run*, ми бачимо *enable secret 5 1mERr$V4mZ0oKYwV8oJv28VA7qT1*.

Зауважимо, що саме цей пароль має пріоритет.

Далі навчимося створювати користувача. Для цього у режимі глобального конфігурування набираємо *user* і натискаємо клавішу табуляції, отримуємо *username*. Клавішу табуляції ми натискаємо завжди для отримання повної команди за введеними початковими літерами. У імені користувача вводимо ваше Прізвище (у тестовому прикладі Ivanov). Якщо на кожному етапі натискати знак питання, система буде Вам виводити підказки (рис. 3.7).

```
Switch(config)#user
Switch(config)#username ?
  WORD  User name
Switch(config)#username Ivanov?
WORD
Switch(config)#username Ivanov ?
  password   Specify the password for the user
  privilege  Set user privilege level
  secret     Specify the secret for the user
  <cr>
Switch(config)#username Ivanov
```

Рисунок 3.7 – Надання підказок під час роботи

Є опція, щоб задати пароль та рівень привілегії (від 0 до 15). Для цього необхідно ввести з клавіатури *Switch(config)#username Ivanov privilege 15 password CPT*. Таким чином, в нас є користувач з правами адміністратора та відповідним паролем.

Далі встановлюємо авторизацію на підключення до консолі. Для цього заходимо в режим конфігурації термінальних ліній за допомогою *line c tab ?*, виводячи список команд. Нас цікавить login (рис. 3.8).

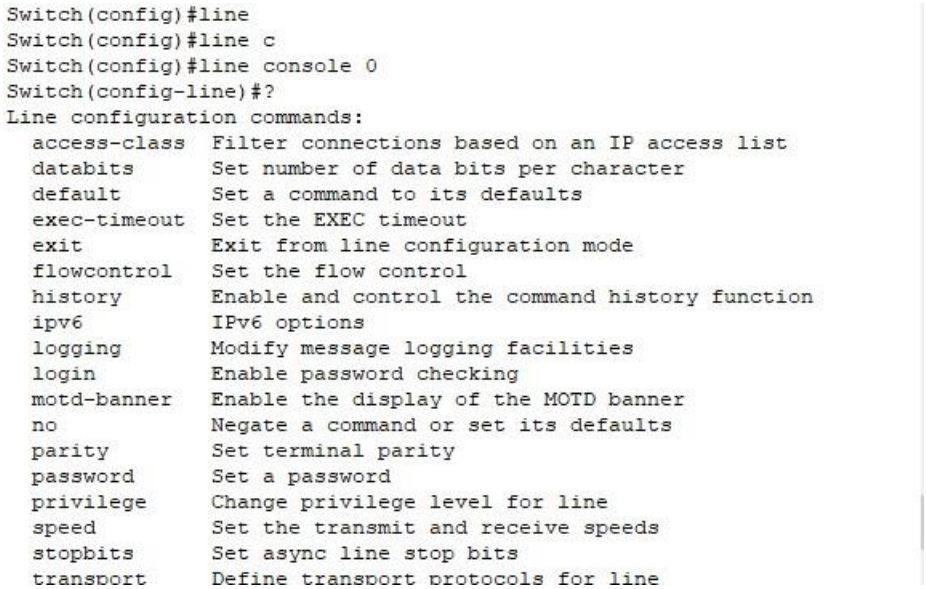


Рисунок 3.8 – Список команд config-line

Вводимо login і вказуємо що ми будемо використовувати локальну базу при перевірці. Рядок матиме вигляд: *Switch(config-line)#login local*. Щоб вийти одразу зі всіх режимів конфігурації можна набрати end (або по черзі exit).

Задаємо IP-адресу пристрою. Виконавши у консолі запис *Switch#show run*, можна побачити фізичні інтерфейси, від 0 до 24. В комутаторі за замовчуванням всі порти підключені до Virtual local area network (VLAN) 1. В комутаторі IP-адреси завжди налаштовуються на логічних інтерфейсах, а не на фізичних. Заходимо в режим глобального конфігурування та конфігурування інтерфейсів *Switch(config)#interface Vlan1*. Переглядаємо доступні нам команди, натиснувши знак питання. Вводимо строку *Switch(config-if)#ip address 192.168.0.1 255.255.255.0*. Для підняття нашого інтерфейсу вводимо *Switch(config-if)#no shutdown* і виходимо.

Тепер налаштовуємо віртуальні термінальні лінії. Входимо в режим конфігурування термінальних ліній *Switch(config)#line vty 0 4*. Дивимося налаштування де визначаємо транспортний протокол, а саме вхідний telnet: *Switch(config-line)#transport input telnet*. Після цього одразу необхідно задати пароль на вхід *Switch(config-line)#login local*. Натискаємо *end*. Write memory – команда, яку використовуємо для збереження стану системи *Switch#write memory*.

Перевіряємо. Для цього підключимо комп'ютер через Ethernet. Після вводимо IP-адреси з тієї ж мережі, що і IP-адреса комутатора, а саме 192.168.0.2. Перевіряємо пінгом *PC>ping 192.168.0.1*, пінгування пішло, потім перевіряємо telnet 192.168.0.1, вводимо логін і пароль і заходимо віддалено на наш комутатор.

Ми провели у підсумку дії, які проводяться при першому підключенні до реального комутатора. Також можна увійти з меню комутатора, а саме за допомогою вкладки «CLI» входимо в ту ж консоль.

Запитання для самопідготовки

1. Які існують формати консольних портів у комутаторі?
2. Яким чином підключити ноутбук без com-порту до комутатора?
3. Яка різниця між користувацьким та розширеним режимом IOS?

Практичне заняття №4

НАЛАШТУВАННЯ VIRTUAL LOCAL AREA NETWORK

Мета заняття – навчитися проектувати віртуальні локальні мережі.

VLAN це віртуальна локальна мережа та найголовніша функція комутаторів. Дану технологію можна порівняти з комутатором всередині комутатора. VLAN допомагає об'єднати комп'ютери в одну мережу на канальному рівні (другий рівень моделі OSI), навіть якщо вони фізично під'єднані до різних комутаторів. Також VLAN допомагає повністю ізолювати трафік групи вузлів від остальної мережі.

До основних переваг VLAN можна віднести:

– структурування мережі, тобто можливість виділення в окрему мережу відділу організацій або групи комп'ютерів, використовуючи загальний комутатор. Також можна проводити виділення фрагментів серверів. VLAN це основа побудови мережі, яка має декілька інформаційних ресурсів. VLAN будує логічну структуру мережі. Таку структуру зручніше аналізувати, ніж звичайну фізичну схему, де зображені лише підключення;

– використання для забезпечення безпеки, наприклад розмежування мережі гостьових користувачів від мережі серверів. Користувачі різних сегментів можуть взаємодіяти тільки на мережевому рівні (третій рівень моделі OSI). Для цього необхідно створити спеціалізовані маршрутизатори, які функціонують на третьому рівні;

– використання для об’єднання користувачів на канальному рівні, навіть якщо вони підключені до різних фізичних комутаторів.

– зменшення кількості широкомовного трафіку. Кожен VLAN це окремий широкомовний домен. За замовчуванням всі порти на комутаторі находяться в першому VLAN, а значить в одному широкомовному домені. Широкомовний домен – це сегмент, всередині якого передаються широкомовні кадри, тобто кадри, які передаються на всю мережу даного сегменту, тобто в кожний порт комутатора. У випадку великої мережі широкомовний трафік може призвести до нераціонального використання полоси пропускання, створення додаткових VLAN на комутаторі означає розділення комутатора на декілька широкомовних доменів.

Налаштовувати VLAN можна лише на налаштовуємих комутаторах, до яких можна підключитися по консолі або віддалено за допомогою відповідних протоколів.

У комутатора може бути два вид портів, а саме access port – для підключення кінцевих пристроїв (комп’ютери, ноутбуки, відеокамери тощо) та trunk port – для з’єднання між комутаторами

Приступимо до виконання лабораторної роботи. Створимо схеми з одним комутатором та з двома комутаторами. У першому випадки ми створюємо VLAN і визначаємо access порти (комп’ютери), у другому випадку створюємо VLAN, визначаємо access порти (комп’ютери) та trunk порт, тобто порт між нашими комутаторами.

Використовуємо комутатор 2960, ставимо перший комп’ютер. Потім затискаємо ctrl і клацаємо на робочій області стільки разів, скільки комп’ютерів

нам необхідно. Аналогічні дії можна виконувати для з’єднання. Створюємо мережу (рис. 4.1).

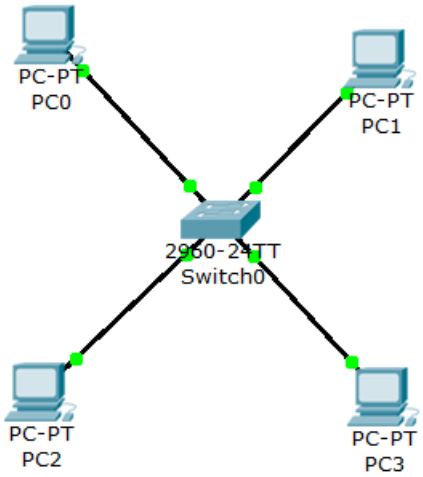


Рисунок 4.1 – Приклад мережі

Припустимо, що PC0 та PC1 це буде перший сегмент, наприклад дирекція. PC2 та PC3 віднесемо до сегменту менеджери. Обравши Draw Poligon, робимо візуалізацію сегментів дирекція та менеджери (рис. 4.2).

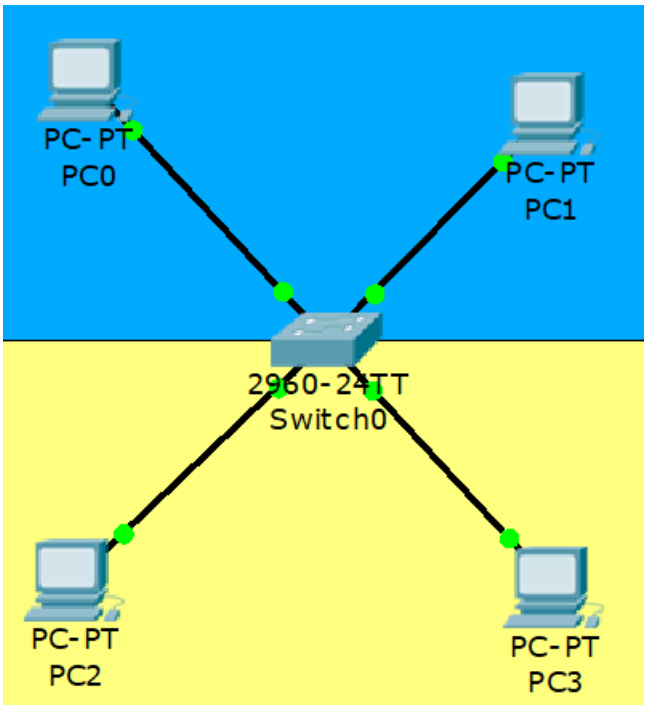


Рисунок 4.2 – Візуалізація сегментів дирекція та менеджери

Також необхідно розділити трафік сегментів. Для цього у налаштуваннях комутатора заходимо в консоль. Спочатку заходимо в розширений режим *Switch>en*, потім в режим глобального конфігурування *Switch#conf terminal*, не забуваємо користуватися при скороченому вводу клавішею табуляції. Всі порти комутатора за замовчуванням знаходяться в VLAN1, тому, ми їх визначимо в другий *Switch(config)#vlan2* і дамо йому ім'я *Switch(config-vlan)#name KN41_KNAME_Director, exit*. Переходимо до налаштування інтерфейсу. Для цього наводимо курсор на з'єднання комутатора та PC0, PC1. Як бачимо з'єднання відбувається по порту FastEthernet 0/1 та 0/2 відповідно. Відповідно дані порти нам необхідно визначити у знов створеному VLAN2. Для цього заходимо в налаштування інтерфейсу *Switch(config)#interface fastEthernet 0/1*, визначаємо що даний порт функціонує в режимі access: *Switch(config-if)#switchport mode access* і визначаємо VLAN: *Switch(config-if)#switchport access vlan 2*. На цьому завершено налаштування порта.

Аналогічно налаштовуємо FastEthernet 0/2 (рис. 4.3).

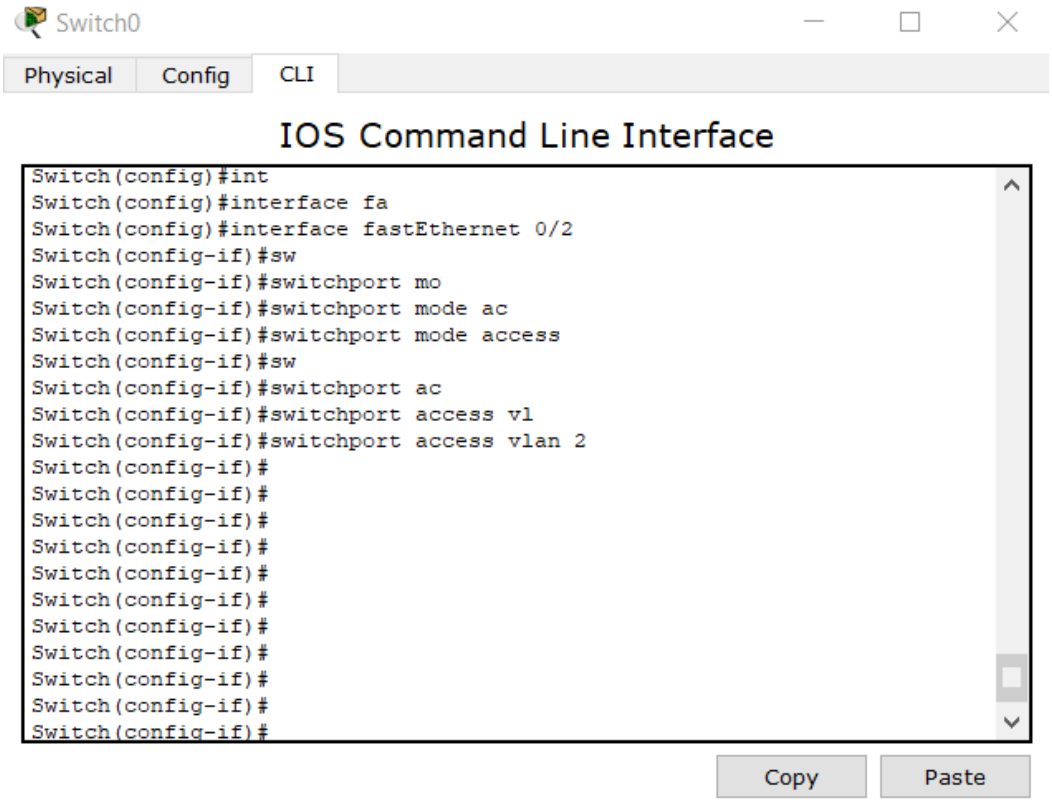


Рисунок 4.3 – Налаштування FastEthernet 0/2

Натискаємо *exit* і виконуємо *Switch#show vlan*. Перевіряємо отримані налаштування (рис. 4.4), як бачимо 1 default vlan cisco комутаторів виставлений на всіх портах, окрім наших двох. Звертаємо увагу на наступну строку: *2 KN41_KNAME_Director active Fa0/1, Fa0/2.*

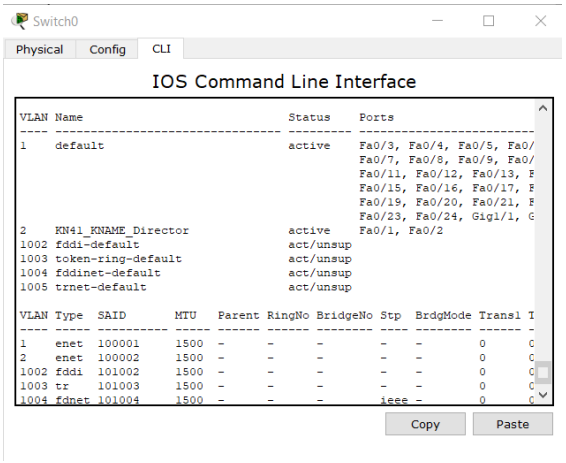


Рисунок 4.4 – Перевірка отриманих налаштувань

Також можна використовувати команду *Switch#show vlan brief* для скороченого подання інформації.

Далі аналогічні дії проводимо для сегменту менеджерів.

Switch#conf terminal

Switch(config)#vlan 3

Switch(config-vlan)#name KN_41_Manager

Switch(config-vlan)#exit

Проводимо аналогічні налаштування VLAN3 (рис. 4.5).

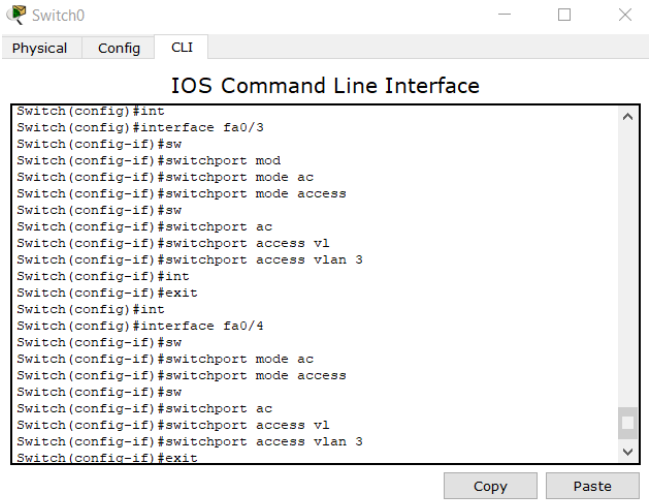


Рисунок 4.5 – Налаштування VLAN3

Перевіряємо налаштування (рис. 4.6).

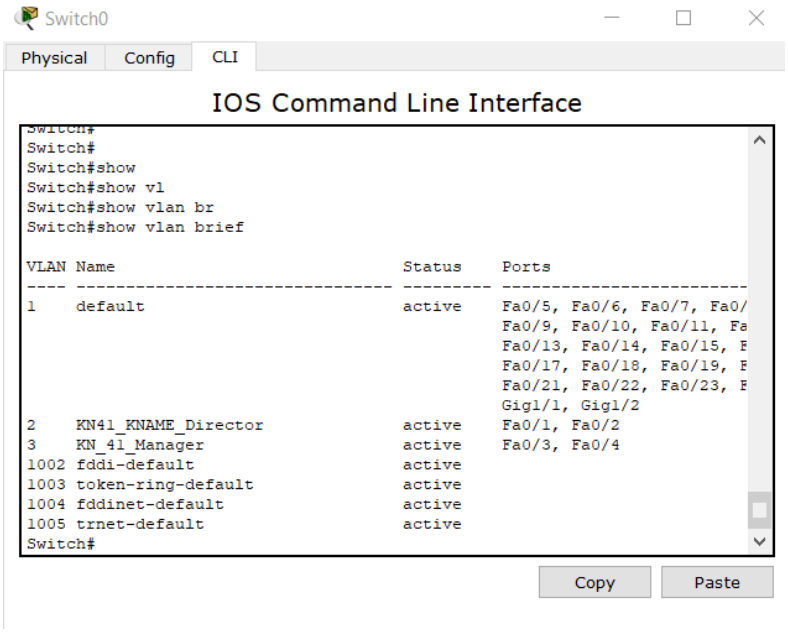


Рисунок 4.6 – Перевірка налаштувань VLAN3

Переходимо до налаштувань комп'ютера. Заходимо в PC0 та задаємо IP-адресу 192.168.2.1, для PC1 задаємо IP-адресу 192.168.2.2, для PC2 задаємо IP-адресу 192.168.3.1. та для PC3 задаємо IP-адресу 192.168.3.2 (третя цифра адреси відповідає відповідному VLAN). Перевіряємо налаштування комп'ютерів різних сегментів (рис. 4.7)

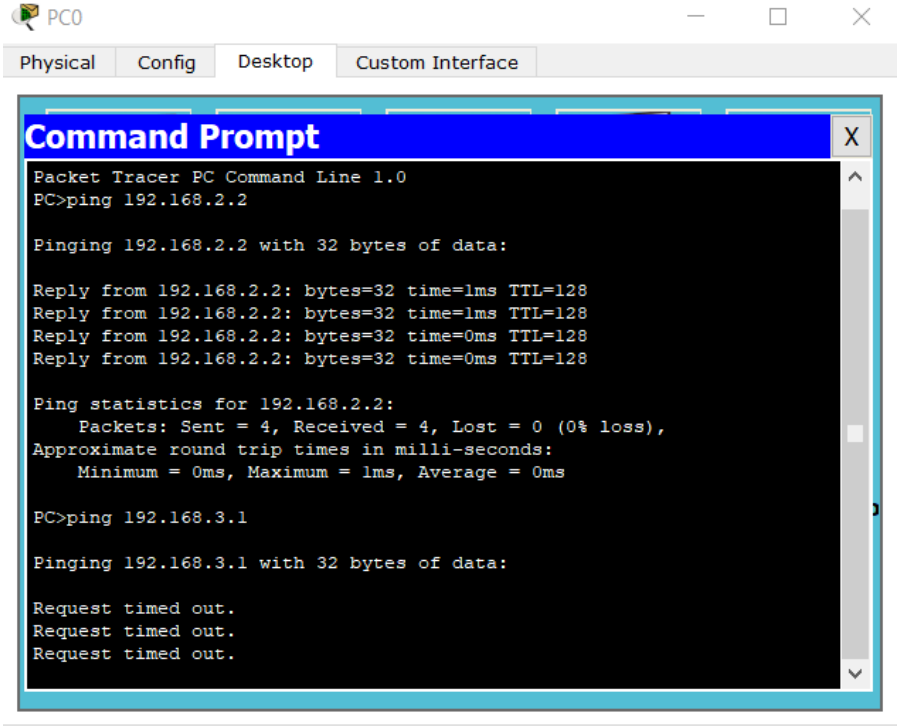


Рисунок 4.7 – Перевірка пінгу

Як ми бачимо другий комп’ютер відповідного VLAN наш комп’ютер бачить, а інші комп’ютери з VLAN3 недоступні.

Далі розглянемо модель з використанням двох комутаторів. Копіюємо наше обладнання (виділяємо, затискаємо ctrl і перетягуємо). Тепер з’єднуємо наші комутатори крос кабелем портами GigabitEthernet 1/1. Змінюємо IP-адреси знов створених комп’ютерів, а саме copyPC0 та задаємо IP-адресу 192.168.2.3, copyPC1 – 192.168.2.4, copyPC2 – 192.168.3.3. та copyPC3 – 192.168.3.4 і аналогічно об’єднуємо їх в сегменти (рис. 4.8).

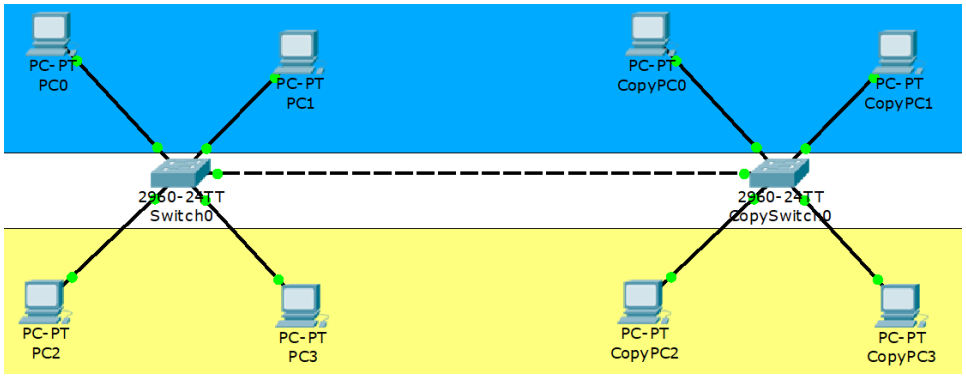


Рисунок 4.8 – Модель з двома комутаторами

У зв’язку з тим, що ми копіювали комутатори з налаштуваннями, проводимо лише перевірку налаштувань другого комутатора. Але нам необхідно налаштувати trunk порт (рис. 4.9), який дозволяє розбити фізичне з’єднання на декілька сегментів.

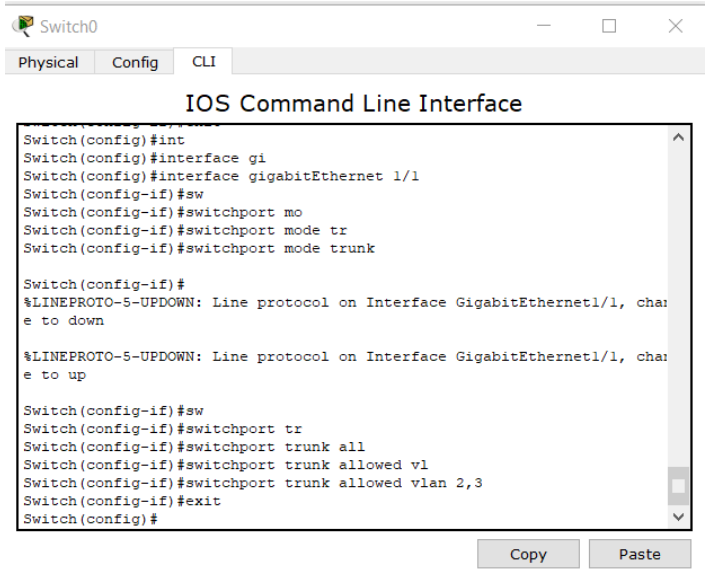


Рисунок 4.9 – Налаштування trunk порту першого комутатора

Зазначимо, що у рядку *Switch(config-if)#switchport trunk allowed vlan 2,3* вказуються VLAN, через які ми плануємо передавати наше фізичне з'єднання.

Такі ж саме дії робимо на другому комутаторі (рис. 4.10).

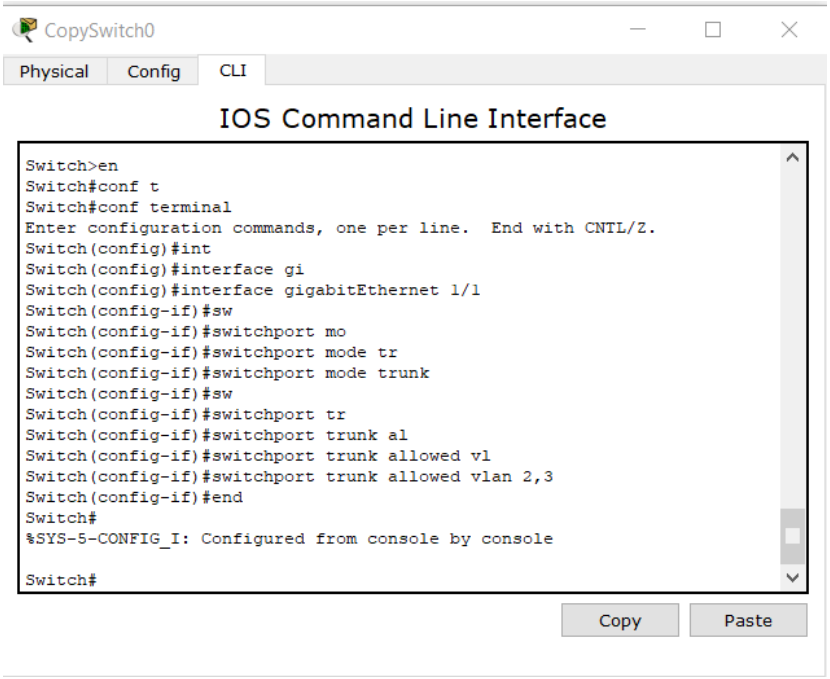


Рисунок 4.10 – Налаштування trunk порту другого комутатора

Тепер перевіримо взаємодію даних комп'ютерів. Запускаємо з комп'ютера PC0 пінгування на copyPC1, як бачимо все працює коректно (рис. 4.11).

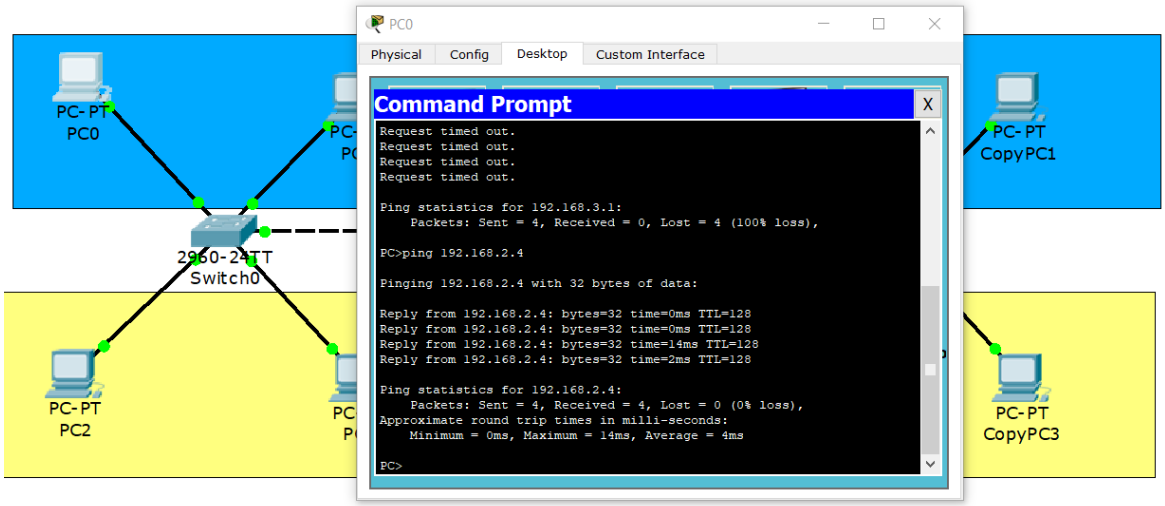


Рисунок 4.11 – Перевірка зв'язку PC0 та copyPC1

Аналогічні дії проведемо в нижньому сегменті з PC2 до copyPC3 (рис. 4.12).

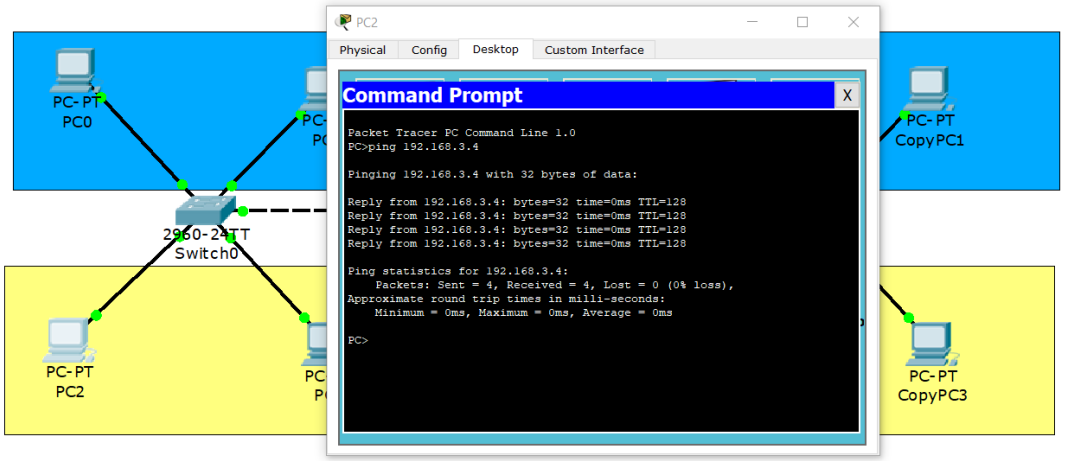


Рисунок 4.12 – Перевірка зв’язку PC2 та copyPC3

Тепер у створеній мережі на другому комутаторі відключимо VLAN3 (рис. 4.13).

```
Switch#conf t
Switch#conf terminal
Enter configuration commands, one per line.  End with CNT
Switch(config)#int
Switch(config)#interface gi
Switch(config)#interface gigabitEthernet 1/1
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk al
Switch(config-if)#switchport trunk allowed vl
Switch(config-if)#switchport trunk allowed vlan 2
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Рисунок 4.13 – Відключення VLAN3 на другому комутаторі

Якщо запустити з PC0 пінгування на copyPC1, все буде як і було, а ось якщо запустити з PC2 на copyPC3, то отримаємо за умов відключення VLAN3 з trunk порту наступне повідомлення (рис. 4.14).

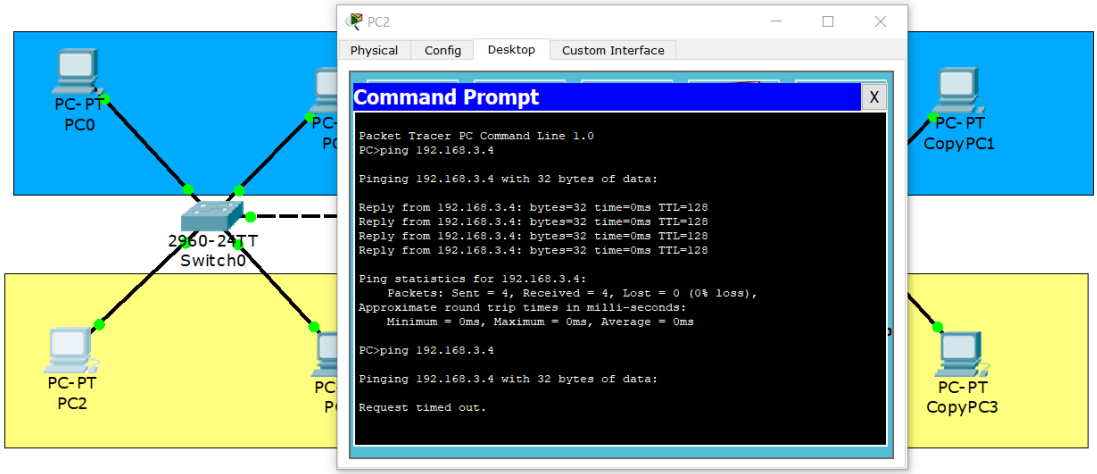


Рисунок 4.14 – Відмова пінгування з PC2 до copyPC3 за умов відключення VLAN3

Запитання для самопідготовки

1. Що таке широкомовний домен?

2. Які пристрої відносіть до 3 рівня моделі OSI?

3. Що таке широкомовні кадри?

4. Назвіть призначення основних портів комутатора.

5. Опишіть два методи перевірки налаштувань VLAN які Вам відомі? В чому їх спільні риси та відмінності?

6. Який порт є найбільш продуктивним?

7. Що являє собою trunk порт?

8. Що таке пінгування?

Практичне заняття №5

SPANNING TREE PROTOCOL

Мета заняття – організація відмовостійкої мережі за допомогою Spanning Tree Protocol.

Важливим завданням є організація відмовостійкої мережі. Для чого це потрібно? Якщо в нас є два комутатори і вони з'єднані однією мережею, то при виникненні проблем зі зв'язком по цій мережі ми не зможемо оперативно відновити зв'язок (наприклад хтось перебив кабель). Для цього використовуються резервні лінки.

Розглянемо резервні методи організації відмовостійких каналів зв'язку:

1. Резервування з'єднань (традиційна надлишкова топологія). Даний метод полягає в тому, що якщо ми маємо два лінки, то з них функціонує лише один, а другий знаходиться в резерві.

2. Агрегування каналів – об'єднання декількох фізичних каналів в один логічний. Сучасний метод, при якому, якщо ми використовуємо два канали між комутаторами, то обидва канали сприймаються як одне логічне з'єднання і інформація передається по обом лінкам і у випадку обриву одного з них, інформація не перестає передаватися.

У випадку резервування з’єднань ми отримуємо комутаційну петлю. Це створює наступні проблеми: широкомовні шторми, багаточисельні копії кадрів та багаточисельні петлі. Будь яка з цих проблем призводить до непрацездатності мережі.

Для вирішення цих проблем існує Spanning Tree Protocol (STP). Даний протокол функціонує на другому рівні моделі OSI, реалізує захист від петель в мережі, дозволяє резервувати автоматичне резервування каналів, час сходимості складає від тридцяти до п’ятдесяти секунд (у випадку падіння активного лінку переключення на резервний складає від тридцяти до п’ятдесяти секунд). Це дуже тривалий час, тому існують альтернативи, а саме протоколи Rapid STP, Manystages STP з часом сходимості менше однієї секунди.

Алгоритм роботи STP полягає в наступному. Спочатку обирається кореневий порт (root bridge), при цьому порти стають однозадачними і переходять у стан передачі. Далі обирається кореневий порт на некореневому комутаторі. Кореневий порт переходить у стан передачі. Кореневий порт обирається з розрахунку вартості шляху від некореневого комутатора до кореневого. Вартість шляху розраховується на підставі пропускної здатності каналів. Чим більше пропускна здатність, тим менша вартість. У підсумку відбувається вибір назначеного порту. У кожному сегменті (відстань між комутаторами), STP створює один призначений для зв’язку з цим сегментом порт. Порт обирається на свічі, який має найдешевший шлях до кореневого свіча. Призначений порт переходить у стан передачі.

При виборі кореневого комутатора STP ґрунтується на кількості біт. Цей параметр об’єднує в собі пріоритет комутатора та його MAC-адресу. Оскільки на всіх комутаторах Cisco за замовчуванням пріоритет однаковий, то кореневим комутатором стає комутатор з найменшим MAC-адресом. Так само відбувається і вибір призначеного порта у випадку якщо у двох комутаторів однакова вартість до кореневого комутатора. Назначеним портом буде обрано порт з мінімальним MAC-адресом.

Стан портів може бути у відповідних станах: блокування, прослуховування, навчання та передача.

Переходимо до програми, розміщуємо три комутатори та за допомогою авто підбору кабелю з'єднуємо їх між собою, емулюємо передачу по мережі і проводимо перевірку (рис. 5.1).

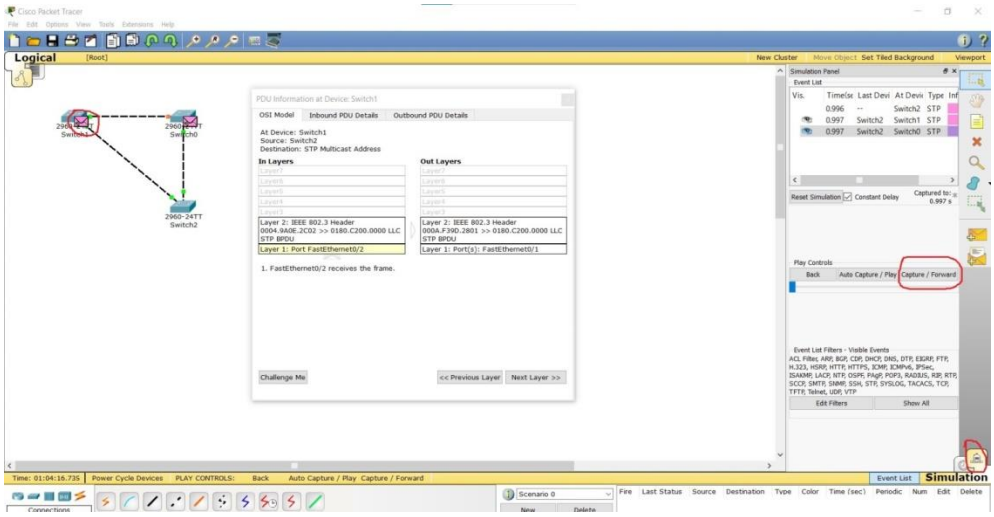


Рисунок 5.1 – З'єднання за протоколом STP

Для того, щоб визначити який комутатор буде кореневим, зайдемо в вкладку CLI, наприклад другого комутатора, та за допомогою *Switch#show spanning-tree* бачимо, що комутатор 2 є кореневим (рис. 5.2).

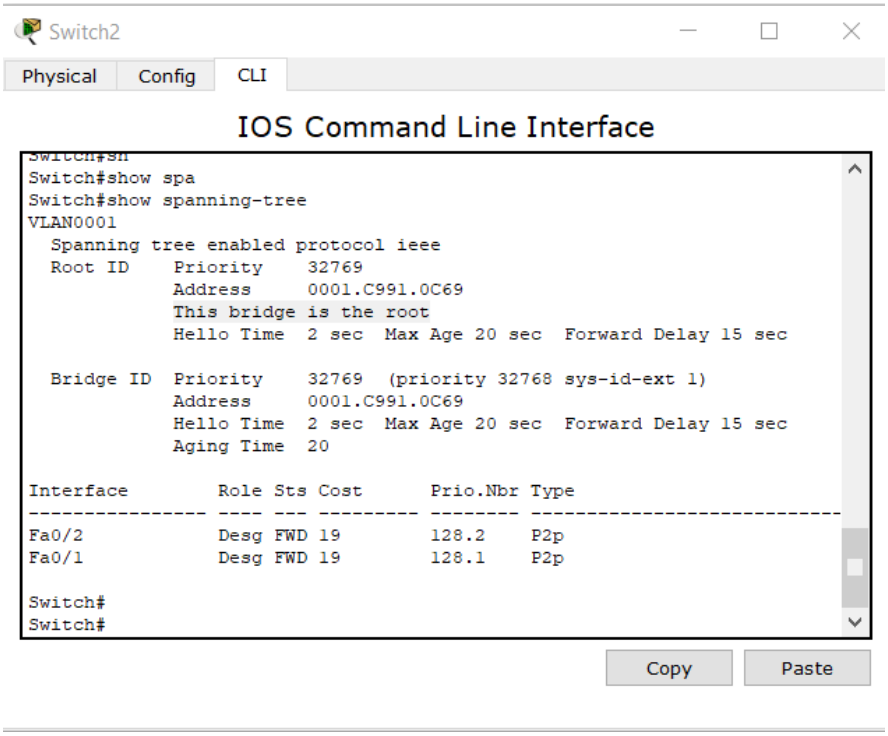


Рисунок 5.2 – Визначення у CLI комутатора 2 властивості кореневості

Надпис This bridge is the root позначає, що комутатор кореневий. Також за допомогою строк *Fa0/2 Desg FWD 19 128.2 P2p, Fa0/1 Desg FWD 19 128.1 P2p*, можна побачити, що всі його порти знаходяться в режимі передачі і є назначеними (designated).

Також подивіться аналогічну інформацію на других комутаторах. Параметр «Altn» позначає що порт заблокований, root активний та знаходиться в стані передачі.

Також подивіться на кожному комутаторі MAC-адресу. На кореневому, у вашому випадку, буде найменше значення адреси.

Уважно подивіться MAC-адреси назначеного порту.

Перевіримо роботу STP. У тестовому прикладу вимкнемо зв’язок FastEthernet 0/1 на комутаторі 2. Для цього введемо код (рис. 5.3).

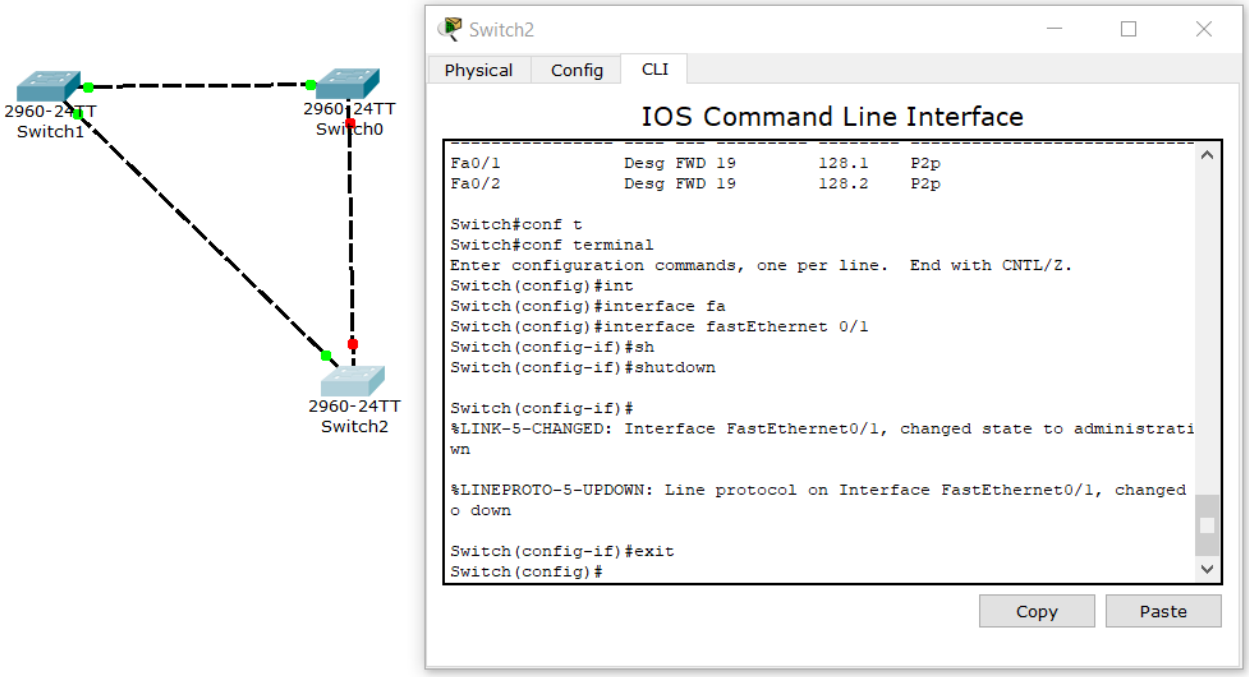


Рисунок 5.3. – Вимкнення зв’язку FastEthernet 0/1 на комутаторі 2

Як можемо бачити, спрацювала наша відмовостійкість, тобто зв’язок відновився і при падіння одного з активних лінків.

Розглянемо ще один приклад. Між комутаторами створюємо комутаційну петлю (рис. 5.4).

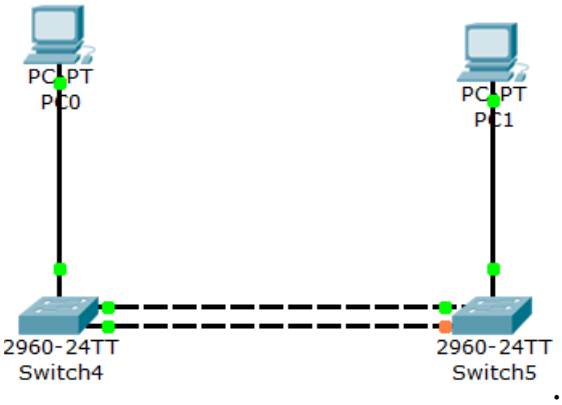


Рисунок 5.4 – Створення мережі з комутаційною петлею

На PC0 задаємо IP-адресу 192.168.1.1, на PC1 задаємо IP-адресу 192.168.1.2. Перевіряємо пінгування при реалізації протоколу STP (рис. 5.5).

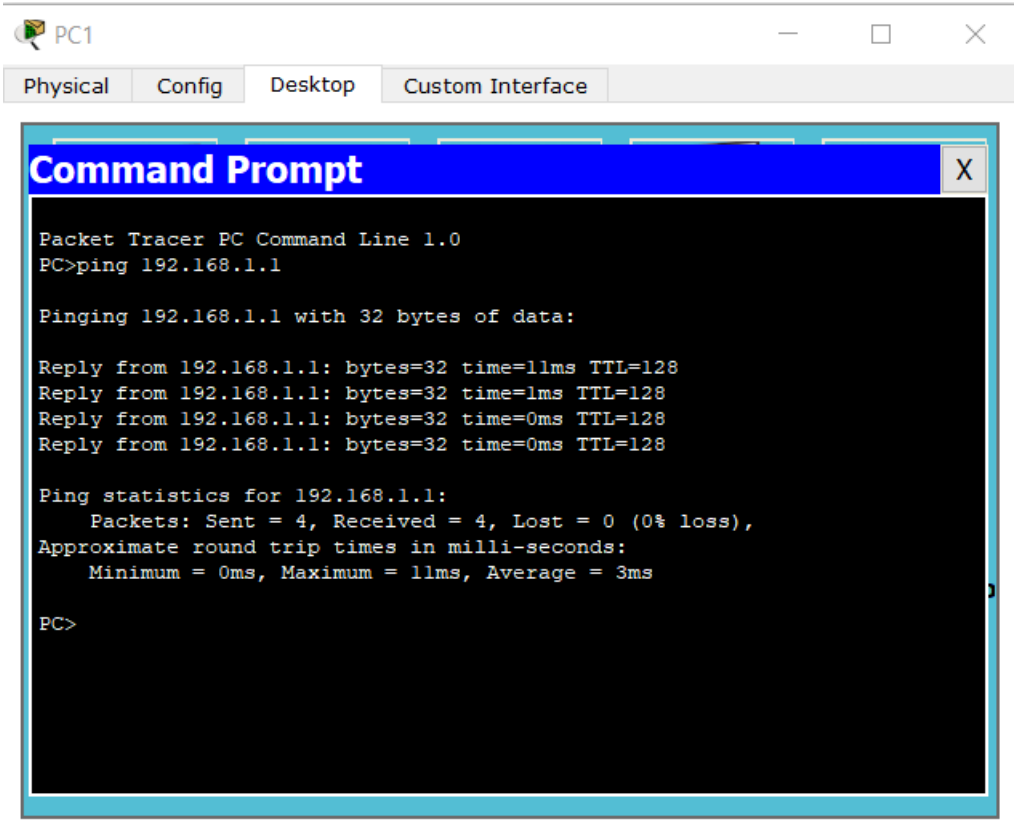


Рисунок 5.5 – Пінгування з PC1 на PC0

Як ми бачимо, STP виконав свою функцію і у нас один з портів в режимі блокування. Визначаємо за допомогою *Switch#show spanning-tree*, який комутатор є кореневим та перевіряємо на якому комутаторі який порт заблокований.

Визначимо, як на користувача вплине використання протоколу «STP», тобто час сходимості. Для цього тушимо активний порт FastEthernet 0/1 на комутаторі 4 (рис. 5.6).

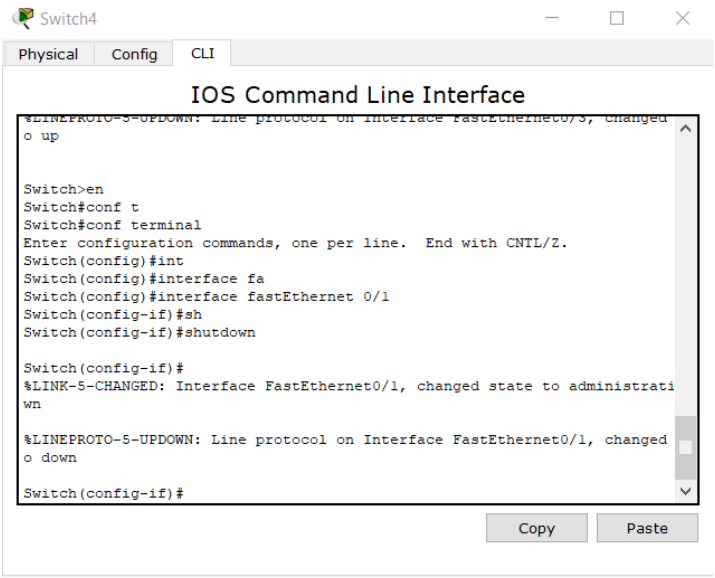


Рисунок 5.6. – Відключення активного порту

Чекаємо на переініціалізацію параметрів. Порт, який був заблокований, переходить у режим прослуховування, потім у стан навчання і тільки потім у стан передачі. У цей час зв’язок між користувачами порушений. Якщо постійно пінгувати стан мережі, можна побачити, що зв’язок був відсутні протягом шістнадцяти секунд. Реалізували відмовостійкість, але в ідеалі скоротити час непрацездатності мережі. Для цього застосовуємо Rapid STP (у коді програми pvst, тобто для кожного VLAN існує свій STP). Переходимо у режим конфігурування четвертого комутатора (рис. 5.7).

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spa
Switch(config)#spanning-tree mo
Switch(config)#spanning-tree mode ra
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#
```

Рисунок 5.7 – Налаштування на четвертому комутаторі протоколу «Rapid STP»

Аналогічні дії робимо на п’ятому комутаторі та перевіримо підключення Rapid STP (рис. 5.8).

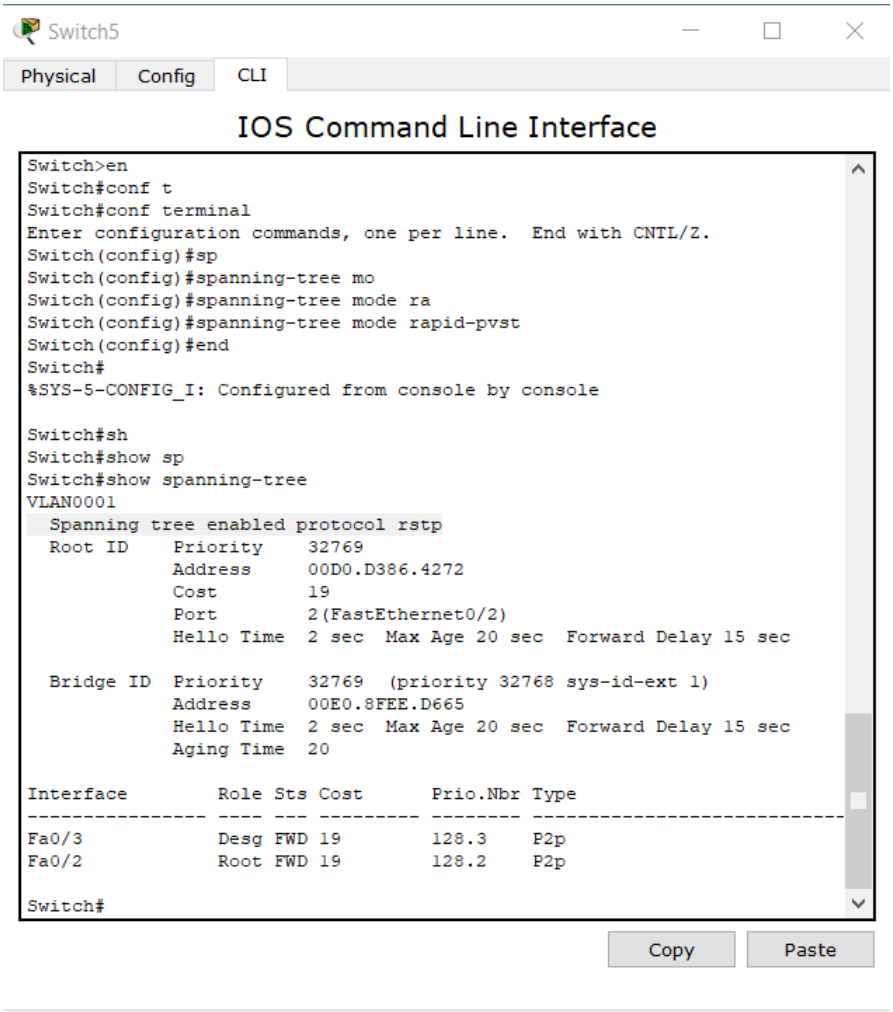


Рисунок 5.8 – Перевірка роботи Rapid STP на 5-му комутаторі

Повернемося до комутатора на якому ми заблокували роботу порту та відновимо його роботу (рис. 5.9).

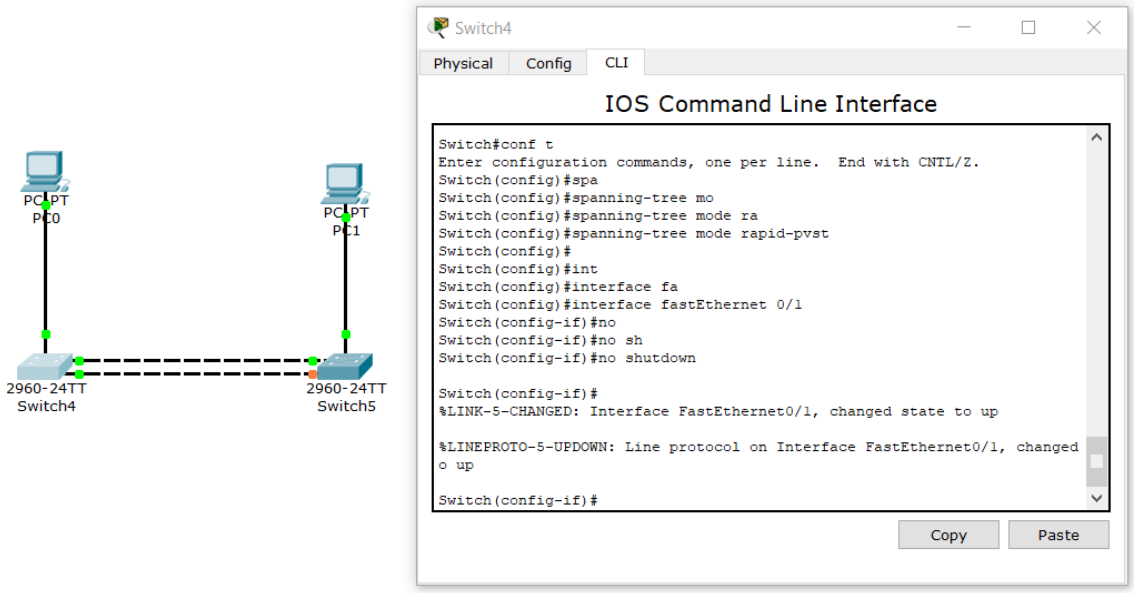


Рисунок 5.9 – Повернення до роботи заблокованого порту

Лінк при цьому відновився моментально. Перевіряємо комп'ютери на підключення. Проводимо взаємне пінгування. Пінг вдалий. При запущеному пінгу проводимо процедуру вимкнення порту. Як ми бачимо жодного пінгу не було загублено.

Запитання для самопідготовки

1. Що ви знаєте про поняття сегменту?
2. Що таке широкомовні шторми?
3. Що вам відомо про комутаційну петлю?
4. Як визначити MAC-адресу комутатора та комп'ютера?
5. Як визначити MAC-адресу порту?
6. За яким принципом у мережі з обладнанням cisco обирається кореневий комутатор?
7. Яким кабелем проводилося з'єднання комутаторів у першому прикладі?

Практичне заняття №6

АГРЕГУВАННЯ КАНАЛІВ «ETHERCHANNEL»

Мета заняття – організація відмовостійкості мережі за допомогою агрегування каналів.

Другим варіантом створення відмовостійких каналів є агрегування каналів, тобто об'єднання декількох фізичних каналів в один логічний. На думку багатьох експертів дана технологія більш ефективна, ніж STP.

Суть даного протоколу складається в об'єднанні декількох фізичних з'єднань в один логічний канал. Усі з'єднання агрегованого каналу є активними і передають інформацію, що вигідно відрізняє даний метод від традиційної надмірної моделі, де додаткові лінки є резервними і не передають інформацію.

Таким чином, використовуючи агрегацію каналів, ми не тільки організовуємо відмовостійкість, але й суттєво підвищуємо пропускну здатність

нашого каналу. При створенні агрегованого каналу існує декілька варіантів: динамічне агрегування (використовуємо два протоколи «Link Aggregation Control Protocol» (LACP), «Port Aggregation Protocol» (PAgP) та статичне агрегування.

З переваг статичного агрегування можна виділити відсутність суттєвих затримок при використанні агрегованого каналу або зміни його налаштувань. З недоліків можна мовити про відсутність налаштувань з віддаленою стороною, а помилки у налаштуваннях можуть призвести до виникнення петель.

У динамічного агрегування, наприклад з LACP, є свої переваги, а саме узгодження налаштувань з віддаленою стороною. Також є підтримка StandBy-інтерфейсів, що дозволяє агрегувати до 16-и портів, 8 з яких будуть активними. Недолік полягає у затримці при підійманні агрегованого каналу або зміни його налаштувань.

При створенні агрегованого каналу необхідно, щоб всі порти мали однакові параметри, а саме швидкість, режим дуплекса, nativeVLAN, діапазон розширених VLAN, trunking status та тип інтерфейсу.

Розглянемо приклад з використанням статичного агрегування, з'єднавши два комутатора одним агрегованим каналом, що складається з двох фізичних лінків. Розміщуємо в робочій області CPT два комутатори 2960 та два комп'ютери. З'єднуємо через порти «FastEthernet» (fe) 0/3 комутатор з відповідним комп'ютером.

Перед з'єднанням комутаторів, налаштуємо порти fe0/1 та fe0/2, саме їх будемо об'єднувати в агрегований канал (рис. 6.1).

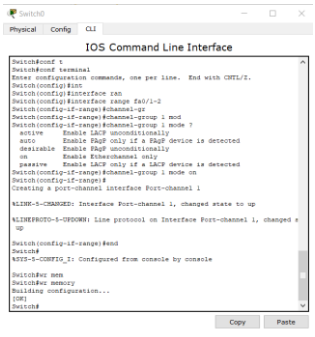


Рисунок 6.1 – Налаштування Switch0

Аналогічні налаштування проводимо на другому комутаторі (рис. 6.2), причому в кінці закінчуємо строчкою збереження стану.

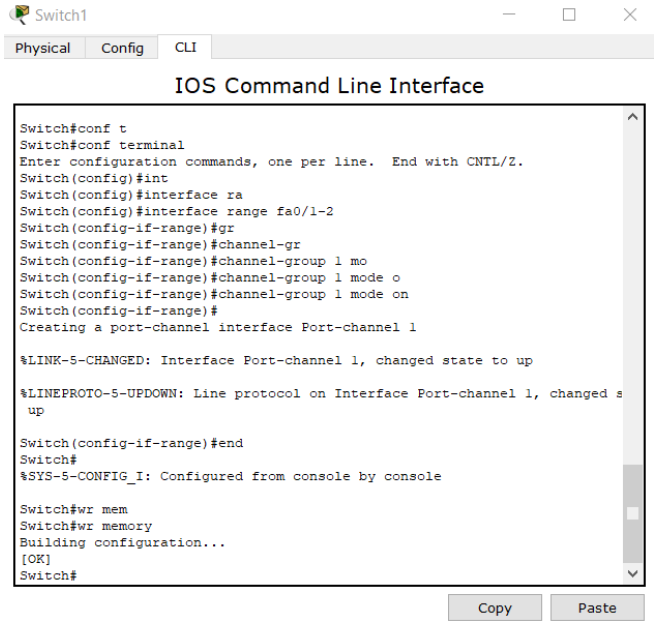


Рисунок 6.2 – Налаштування Switch1

Тепер з'єднуємо два комутатора через порти fe0/1 та fe0/2, чекаємо ініціалізацію портів. Прописуємо IP-адреси для PC0 192.168.1.1 та для PC2 192.168.1.2, маски залишаємо без змін.

Перевіримо з'єднання з PC1 (рис. 6.3).

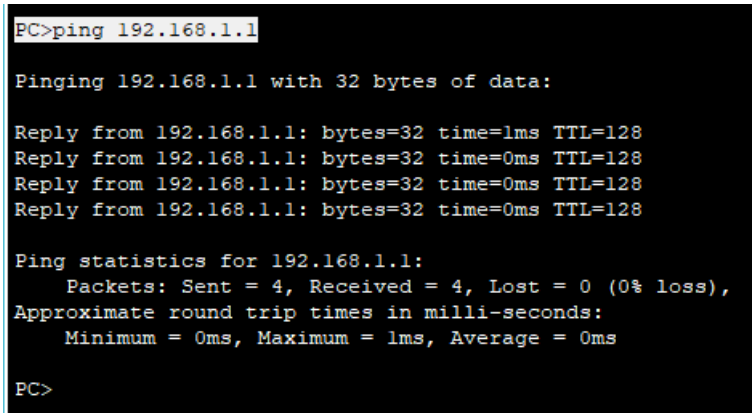


Рисунок 6.3 – Перевірка каналу по агрегованому з'єднанню

Ми отримали агрегований канал між двома комутаторами на 200 мегабіт, оскільки обидва лінки є активними. Для перевірки відмовостійкості, тушимо один з лінків, наприклад, fe0/2 на комутаторі 1 (рис. 6.4).

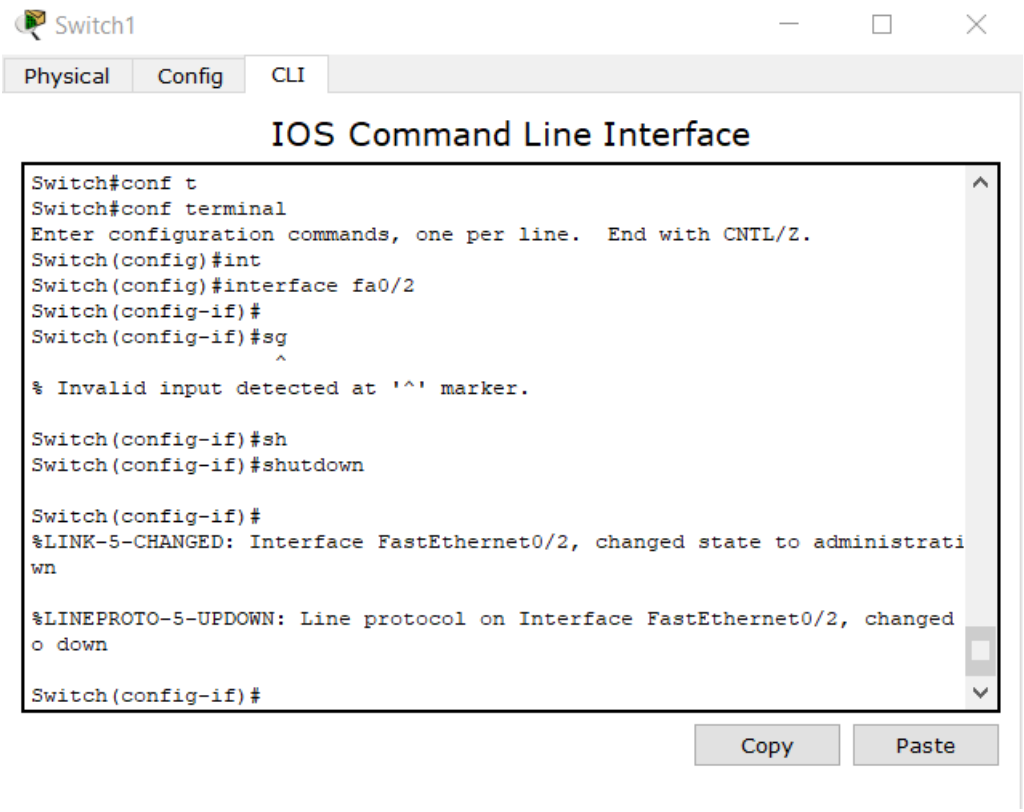


Рисунок 6.4 – Відключення у тестовому режимі, fe0/2 на комутаторі 1

Перевіримо пінг з PC1 (рис. 6.5).

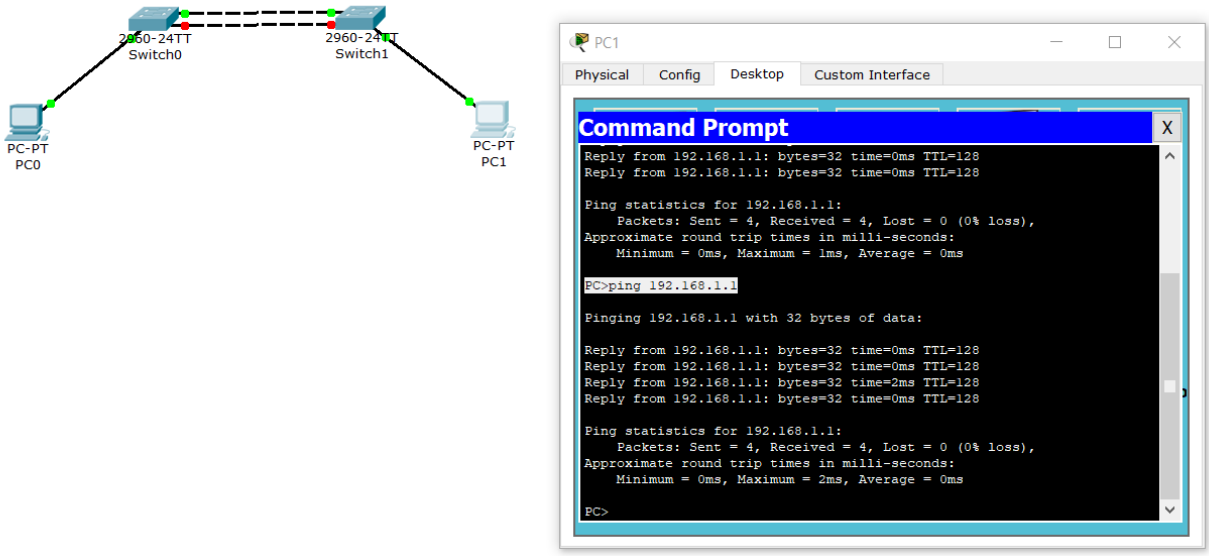


Рисунок 6.5. – Перевірка мережі на відмовостійкість

Як можна побачити з результатів перевірки на відмовостійкість, жоден з пінгів не загубився. Якщо подивитися на схему, то можна побачити, що один канал досі активний.

Якщо б на реальному обладнанні за цих умов ми підняли б інтерфейс, то зв’язок повинен був би відновитися без будь яких затримок, але у програмі при відновленні каналу йде затримка, але зв’язок з плином певного проміжку часу знов відновиться (рис. 6.6).

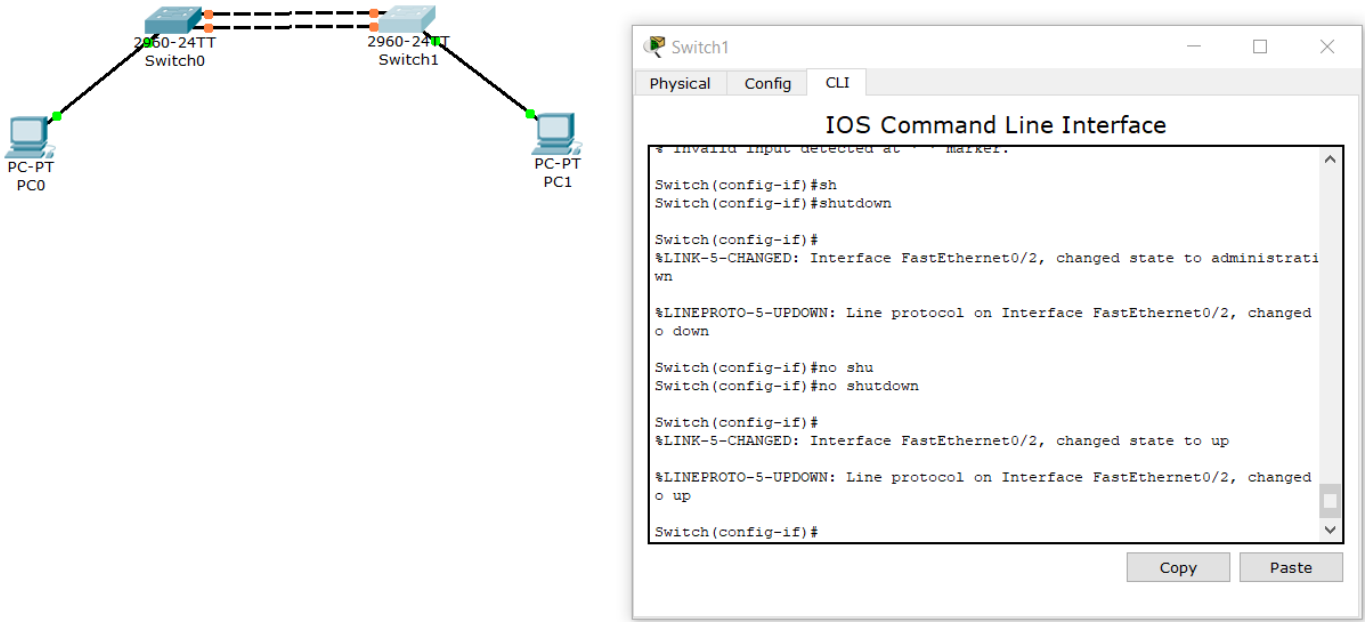


Рисунок 6.6 – Відновлення другого каналу зв’язку між комутаторами після відключення

Для перегляду статусу etherchannel-порту можна за допомогою команди *Switch#show etherchannel* або *Switch#show etherchannel summary* (не використовується жодний протокол, використовується статична агрегація), де можна подивитися, що на комутаторі 0 існує один portchannel, куди входять порти fa0/1 fa0/2. Також існує команда *Switch#show etherchannel portchannel*.

У наступному прикладі розглянемо класичну топологію «Зірка», коли комутатори другого рівня (комутатори рівня доступу) підключаються до центрального комутатора 3-го рівня (комутатора рівня розподілення). Як правило ця схема може застосовуватися у багатоповерхівках, де на кожному поверсі стоїть комутатор 2-го рівня.

Розмістимо на схемі три комутатори 2-го рівня та 1 комутатор 3-го рівня. Кожен з комутаторів 2-го рівня підключаємо двома портами до центрального комутатора, використовуючи динамічне агрегування. Для цього спочатку

переходимо в налаштування центрального комутатора 3560, не забуваючи по закінченню зберегти налаштування (рис. 6.7).

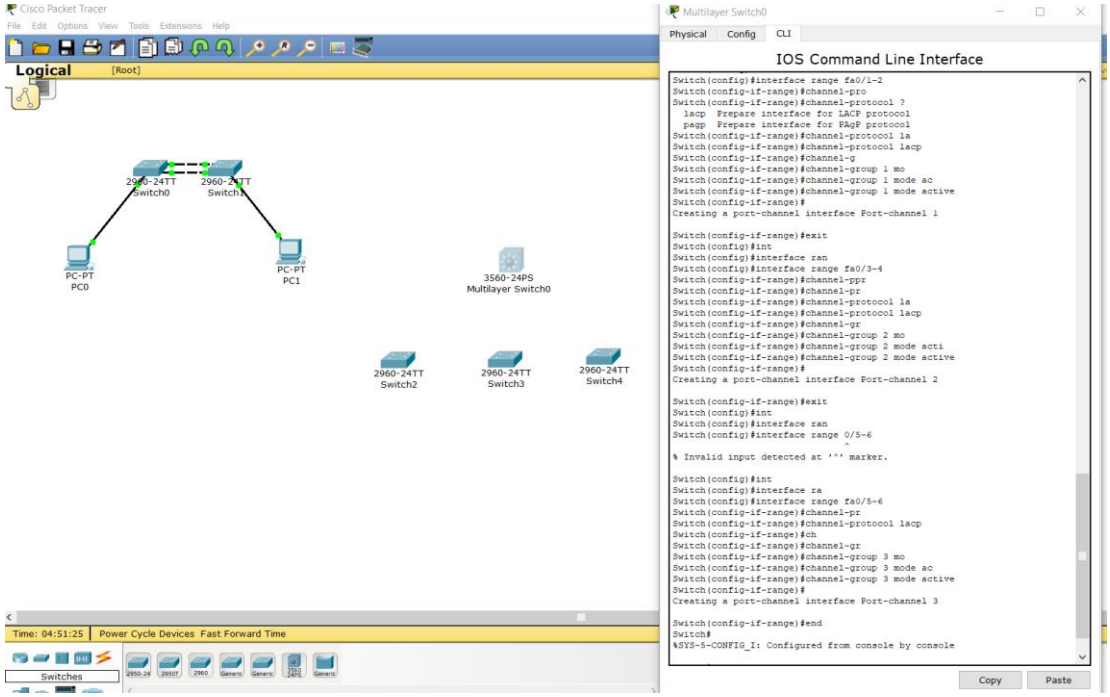


Рисунок 6.7 – Налаштування центрального комутатора

Завдяки *Switch(config)#interface range fa0/1-2* ми створюємо перший агрегований канал. Для створення інтерфейсу portchannel1 використовуємо запис *Switch(config-if-range)#channel-group 1 mode active*. Аналогічно створювали 2-й та 3-й агрегований канал.

Далі налаштовуємо комутатори рівня доступу (рис. 6.8).

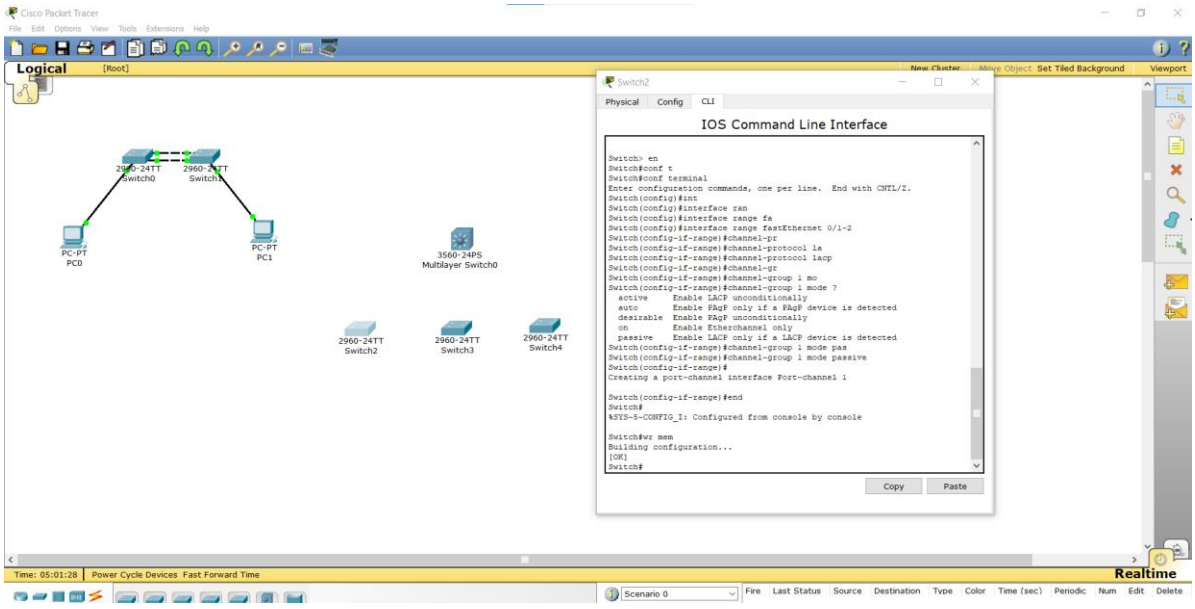


Рисунок 6.8 – Налаштування комутаторів рівня доступу

Аналогічні налаштування робимо на другому та третьому комутаторах (рис. 6.9).

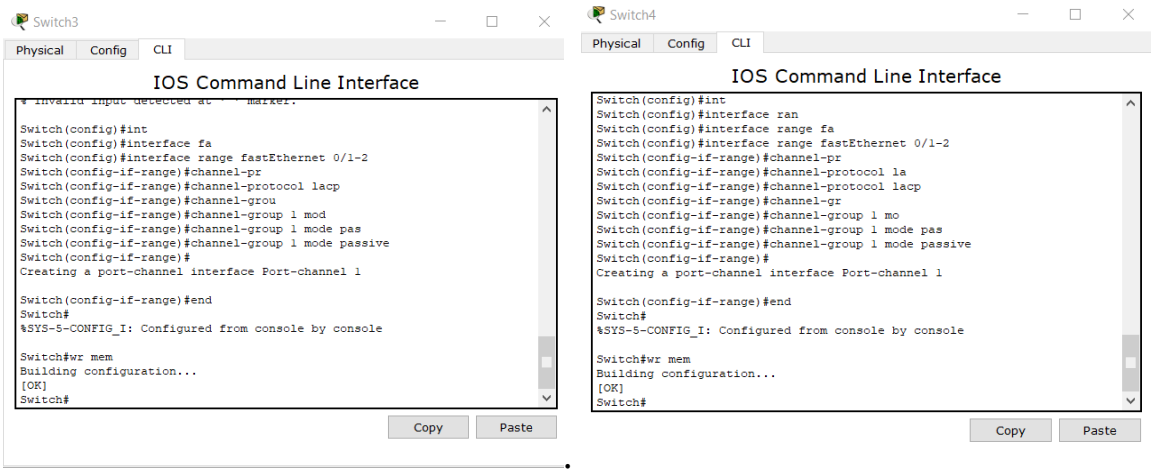


Рисунок 6.9 – Налаштування другого та третього комутаторів

Далі підключаємо fa0/1-fa0/1, fa0/2-fa0/2, fa0/1-fa0/3, fa0/2-fa0/4, fa0/1-fa0/5 та fa0/2-fa0/6.

Виконавши команду *Switch#show etherchannel summary* для головного комутатора, можна побачити, що використовується, на відміну від першої схеми, LACP (рис. 6.10).

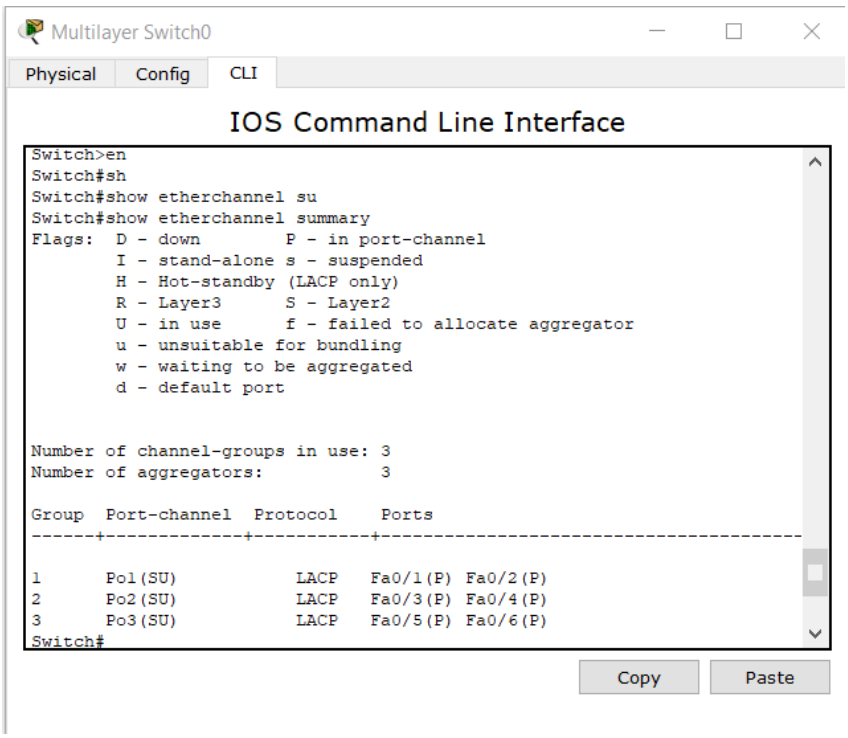


Рисунок 6.10 – Реалізація *Switch#show etherchannel summary* для комутатора третього рівня

Також, у випадку існування декількох VLAN, транкпорт налаштовується не на фізичних інтерфейсах, а на логічному (portchannel). Для того щоб створити транкпорт необхідно ввести код (рис. 6.11).

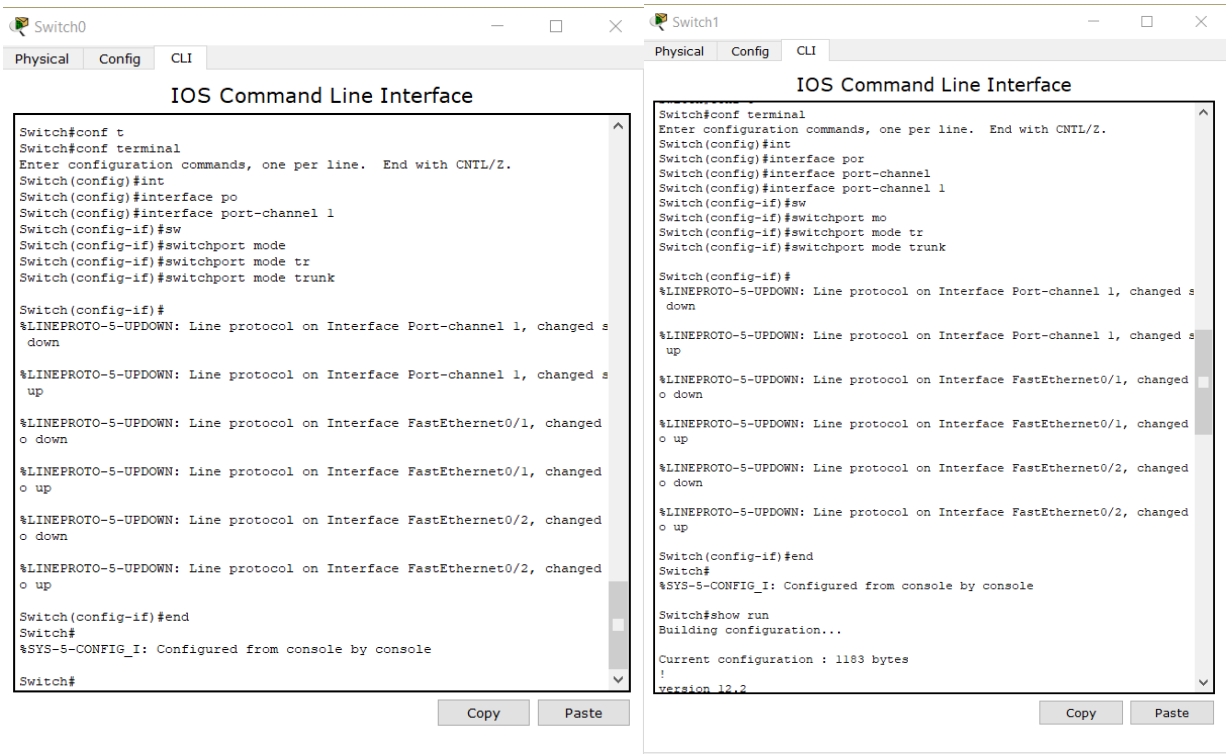


Рисунок 6.11 – Налаштування mode trunk (наприкінці після команди *Switch#show run*)

Запитання для самопідготовки

1. Обладнання фірм HP, D-Link використовують LACP або PAgP?
2. За допомогою якого запису можна зберегти стан системи?
3. Назвіть основні переваги та недоліки статичного агрегування.
4. Назвіть основний недолік протоколу LACP.
5. Яким чином позначаються неактивні канали?
6. Які канали відносяться до portchannel?
7. Що вам відомо про топологію «Зірка»?

Практичне заняття №7

КОМУТАТОРИ ТРЕТЬОГО РІВНЯ

Мета заняття – вивчити функціонування та особливості використання комутаторів третього рівня.

Комутатори третього рівня моделі OSI (L3) підтримують IP-маршрутизацію (можуть не тільки розбити мережу на декілька VLAN, а й маршрутизувати трафік між сегментами), агрегування комутаторів рівня доступу, використовуються в якості комутаторів рівня розподілу та маюсь високу продуктивність. L3 комутатори використовуються для маршрутизації трафіку тільки всередині мережі, тобто вони не можуть замінити маршрутизатор.

Створимо мережу з трьох комп'ютерів та комутатора L3. Підключаємо їх напряму. Після розбиваємо мережу на три сегменти (три мережі), щоб дані комп'ютери могли зв'язуватися між собою.

Для створення трьох VLAN на тестовій схемі необхідно ввести код (рис. 7.1).

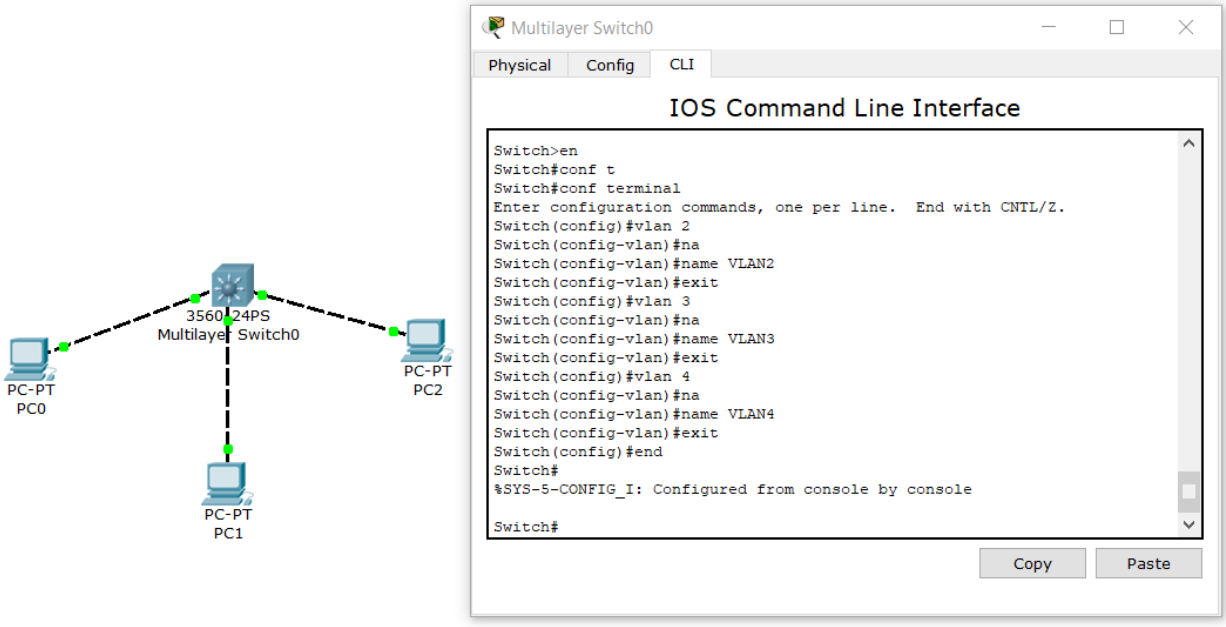


Рисунок 7.1 – Створення VLAN

Визначимо порт fe0/1 у VLAN2, fe0/2 у VLAN3 та fe0/3 у VLAN4 (рис. 7.2).

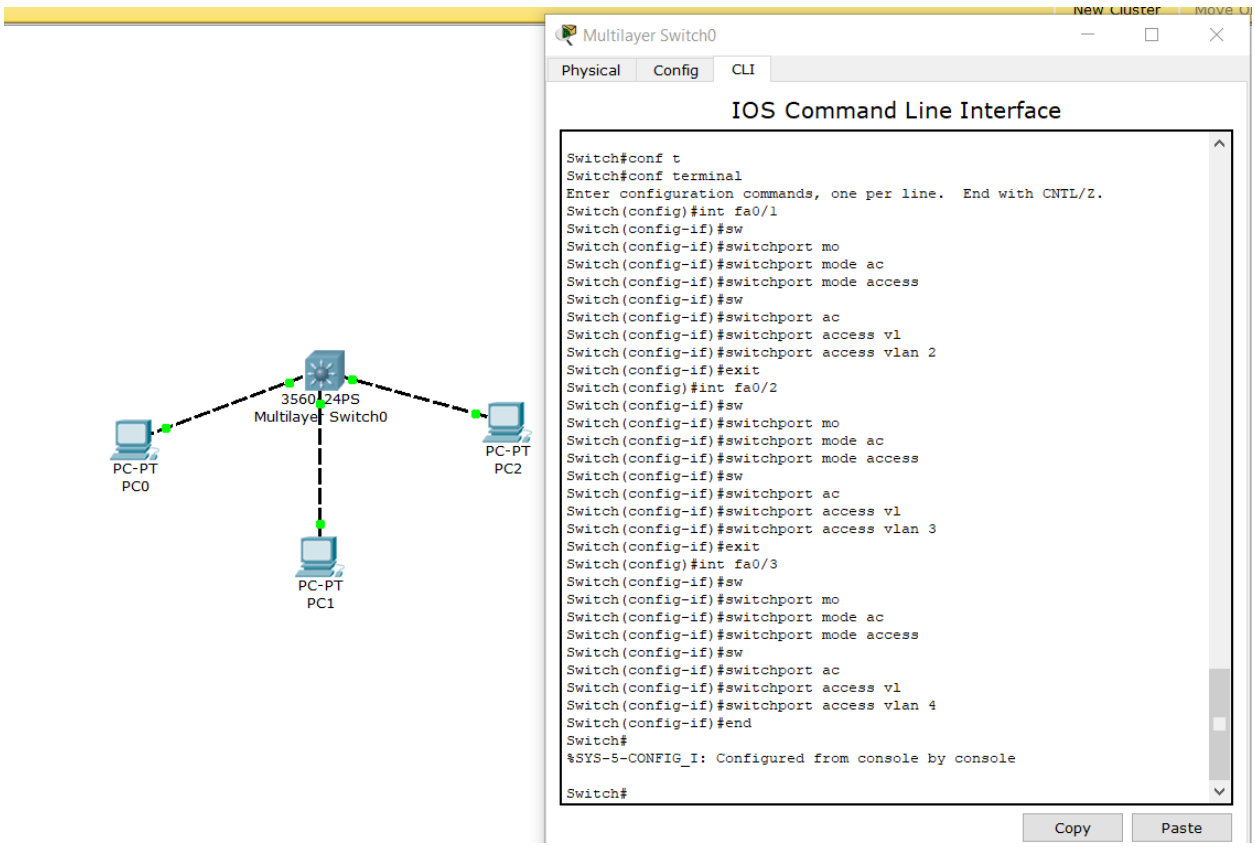


Рисунок 7.2 – Визначення портів

Перевіримо налаштування за допомогою show run (рис. 7.3).

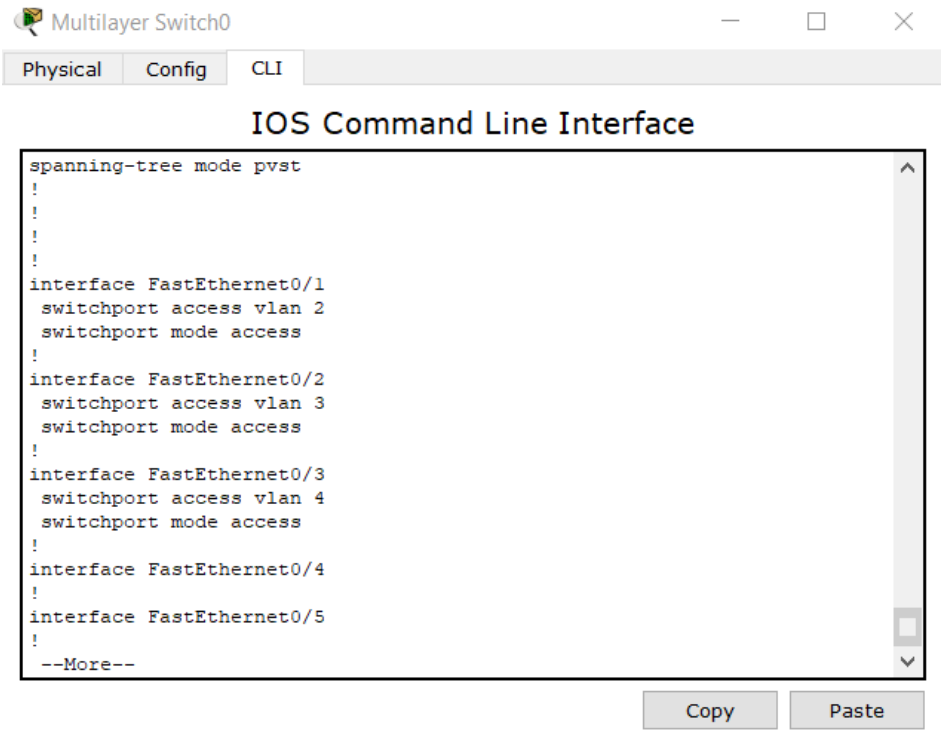


Рисунок 7.3 – Перевірка налаштувань

Як бачимо налаштування коректні. Оскільки ми використовуємо комутатор третього рівня, нам необхідно на створені сегменти призначити IP-адреси. Для цього використаємо віртуальний інтерфейс (рис. 7.4).

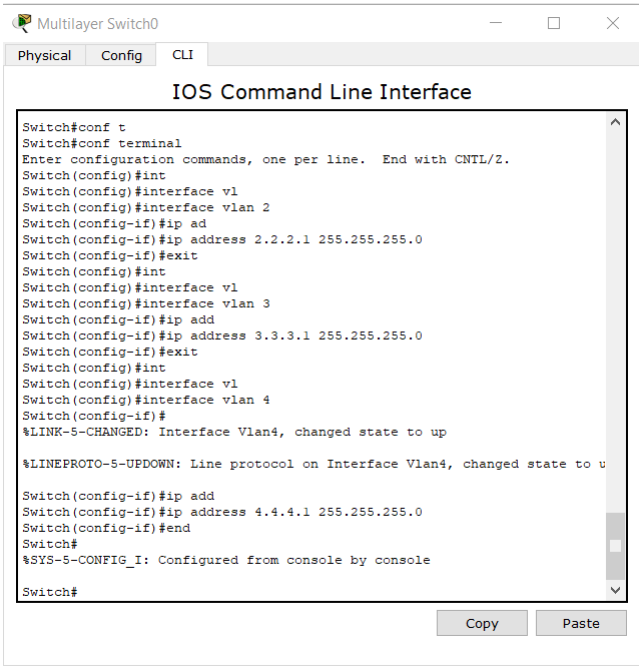


Рисунок 7.4 – Призначення IP-адрес на створені сегменти

Перевіримо налаштування за допомогою show run (рис. 7.5, рис. 7.6).

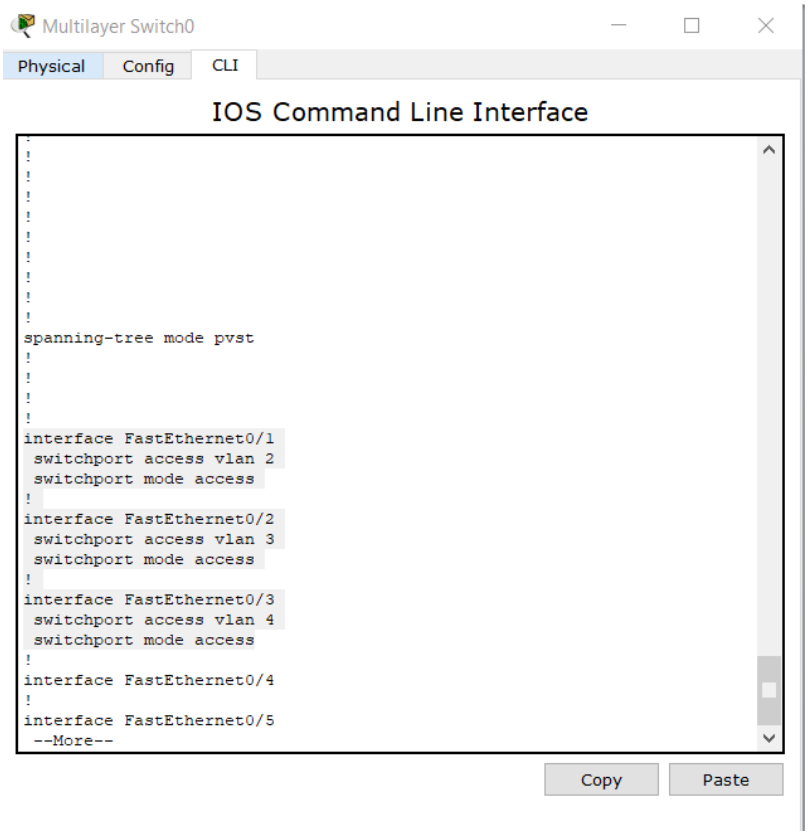


Рисунок 7.5 – Перевірка налаштувань, при якій можна побачити фізичні порти

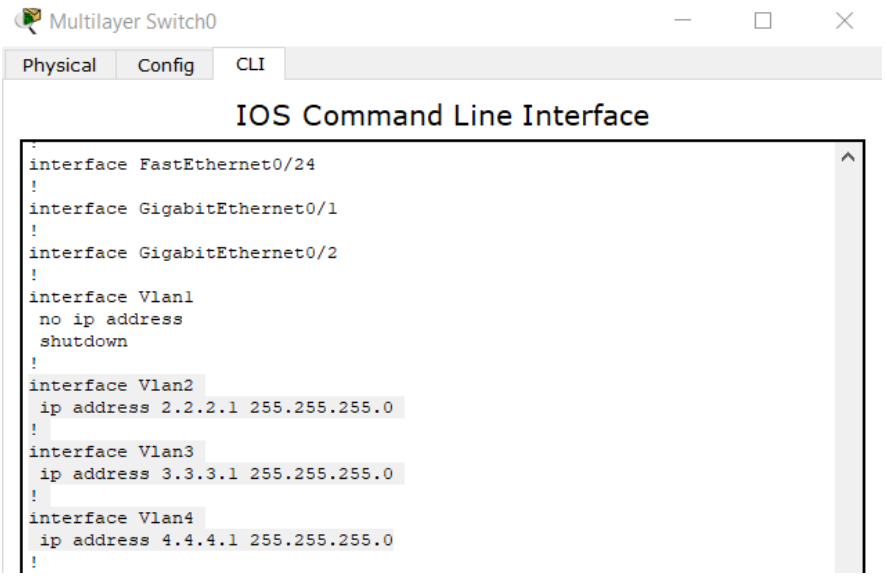


Рисунок 7.6 – Перевірка налаштувань, при якій бачимо IP-адреси, які присвоєні нашим віртуальним інтерфейсам

Далі налаштовуємо самі комп'ютери. PC0 знаходиться в VLAN2, тому задаємо IP-адресу 2.2.2.2, маску 255.255.255.0 і задаємо значення шлюзу нашого L3 комутатора 2.2.2.1 (точніше IP-адреса, яка висить на віртуальному інтерфейсі VLAN2) і перевіримо зв'язок (рис. 7.7).

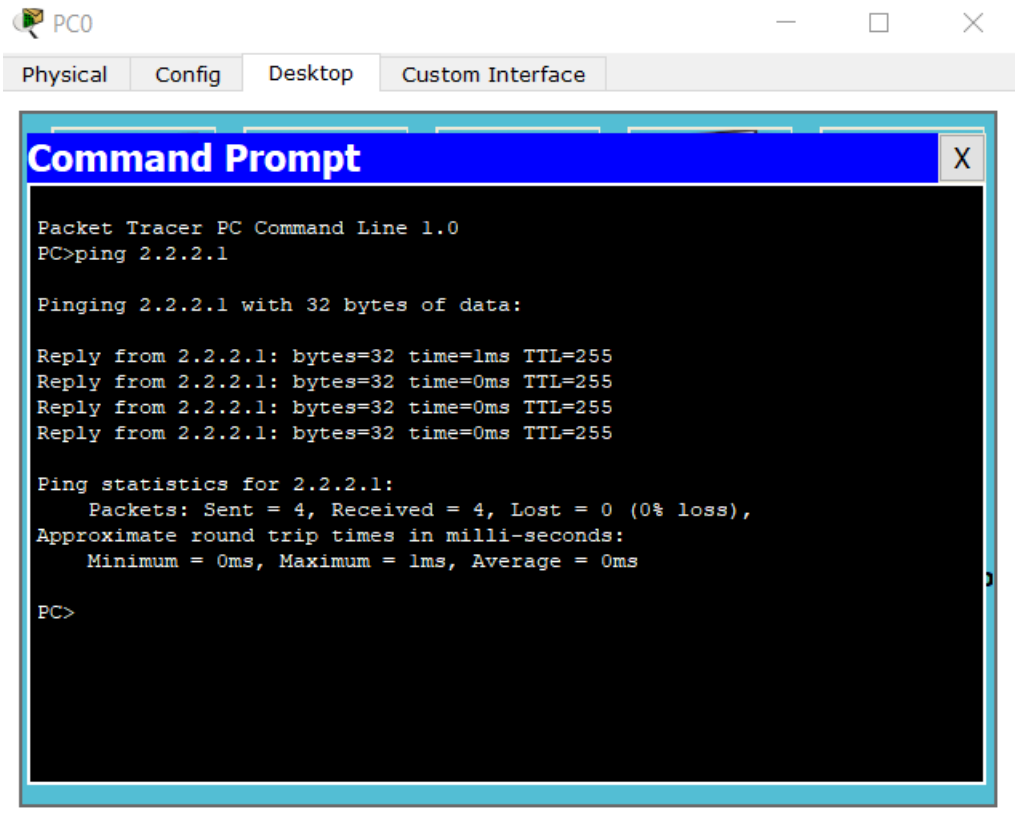


Рисунок 7.7 – Налаштування PC0-комп'ютера та перевірка зв'язку

Аналогічно налаштовуємо і перевіряємо зв’язок інших двох комп’ютерів. На PC1, що знаходиться в VLAN3, задаємо IP-адресу 3.3.3.2, маску 255.255.255.0, шлюз 3.3.3.1, PC2, що знаходиться в VLAN4, задаємо IP-адресу 4.4.4.2, маску 255.255.255.0, шлюз 4.4.4.1.

Таким чином налаштовано три сегменти, на комутаторі визначено IP-адреси, наші комп’ютери в цих сегментах видять відповідні адреси на комутаторі, тепер перевіряємо міжмережне з’єднання.

Наприклад, з комп’ютера PC2, який знаходиться в четвертому сегменті, пропінгувати комп’ютер PC0, який знаходиться в сегменті VLAN2 (рис. 7.8).

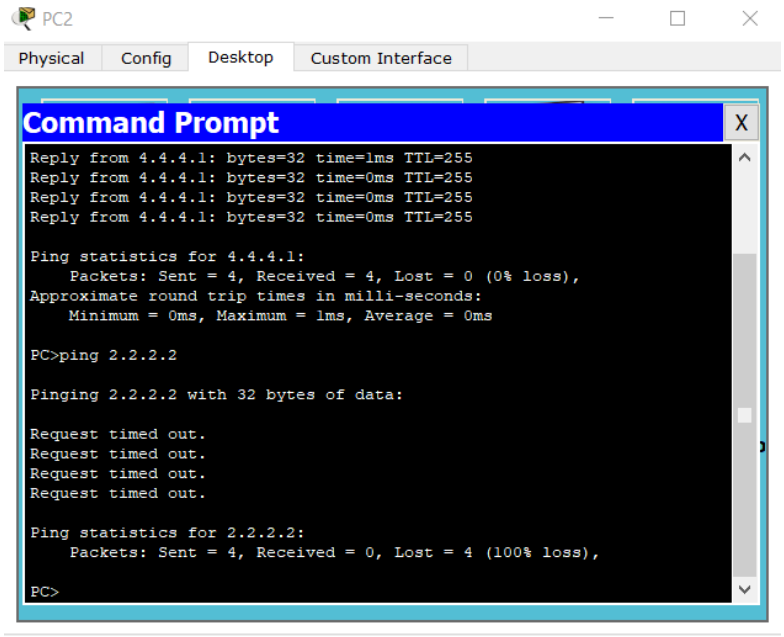


Рисунок 7.8 – Приклад невірного налаштування маршрутизатора

Дана помилка пов’язана з тим, що на комутаторі не налаштована опція маршрутизування трафіка (рис. 7.9).

```
Switch>en
Switch#conf t
Switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip rou
Switch(config)#ip routing
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

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

Рисунок 7.9 – Налаштування комутатора на маршрутизацію трафіка

Після цього перевіряємо зв’язок. Як підсумок, комутатор L3 маршрутизує три мережі.

Далі розглянемо більш розповсюджену мережу. L3 комутатор встановлюємо, коли в нас 2 і більше комутаторів рівня два. Припустимо, що PC3 та PC5 знаходяться у VLAN2, PC4 та PC6 у VLAN3.

Налаштуємо access-порти (рис. 7.10).

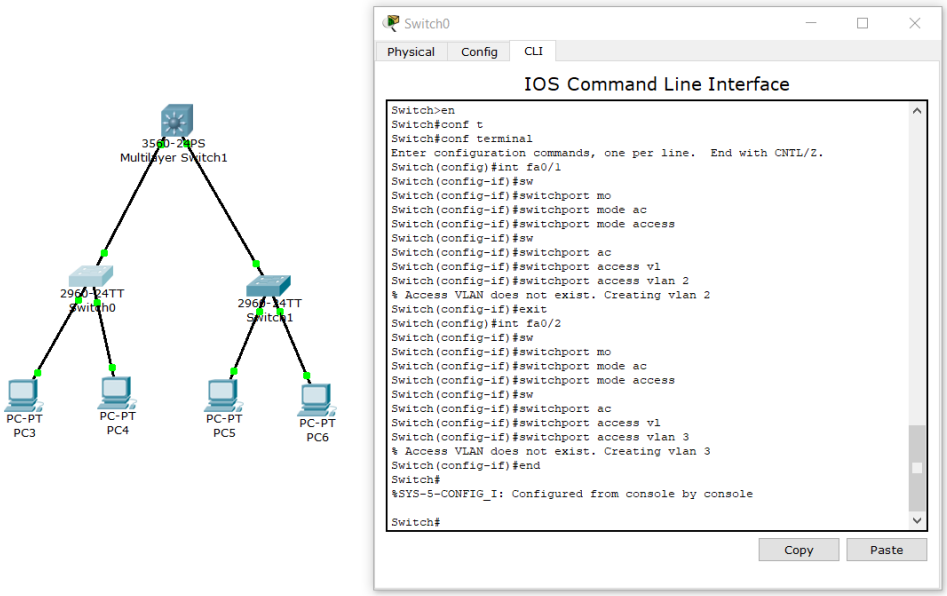


Рисунок 7.10 – Налаштування access-портів

Далі налаштовуємо транк порти. Як говорили раніше, між комутаторами краще використовувати GigabitEthernet (GE) порти, в яких найшвидші лінки.

Налаштуємо порт GE 1/1 (рис. 7.11).

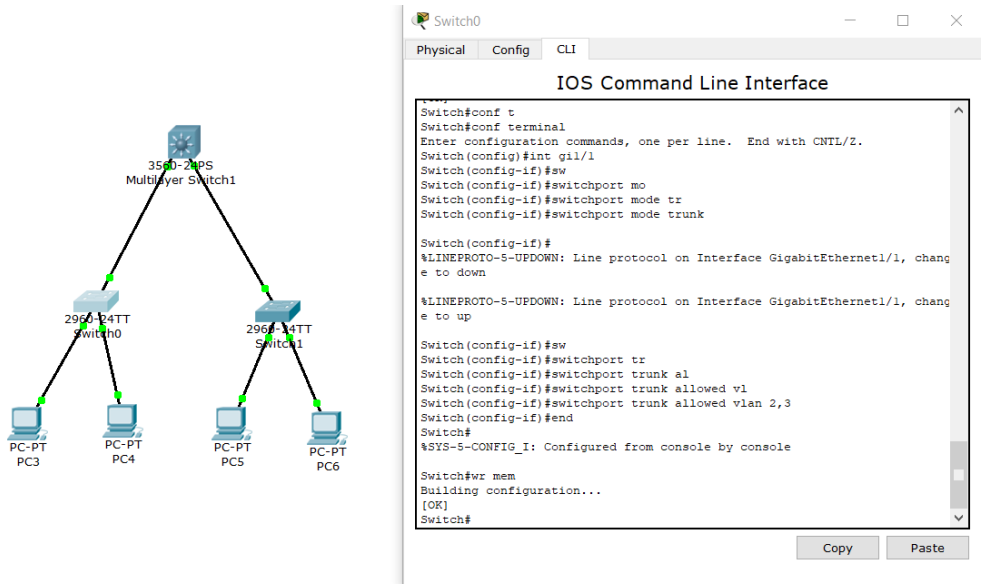


Рисунок 7.11 – Налаштування портів між комутаторами різних рівнів

Зауважимо, що порт, який ми налаштовували на Switch0, мав в статусі (підводимо мишкою до Switch0) Up.

Налаштовуємо транк порти (рис. 7.12).

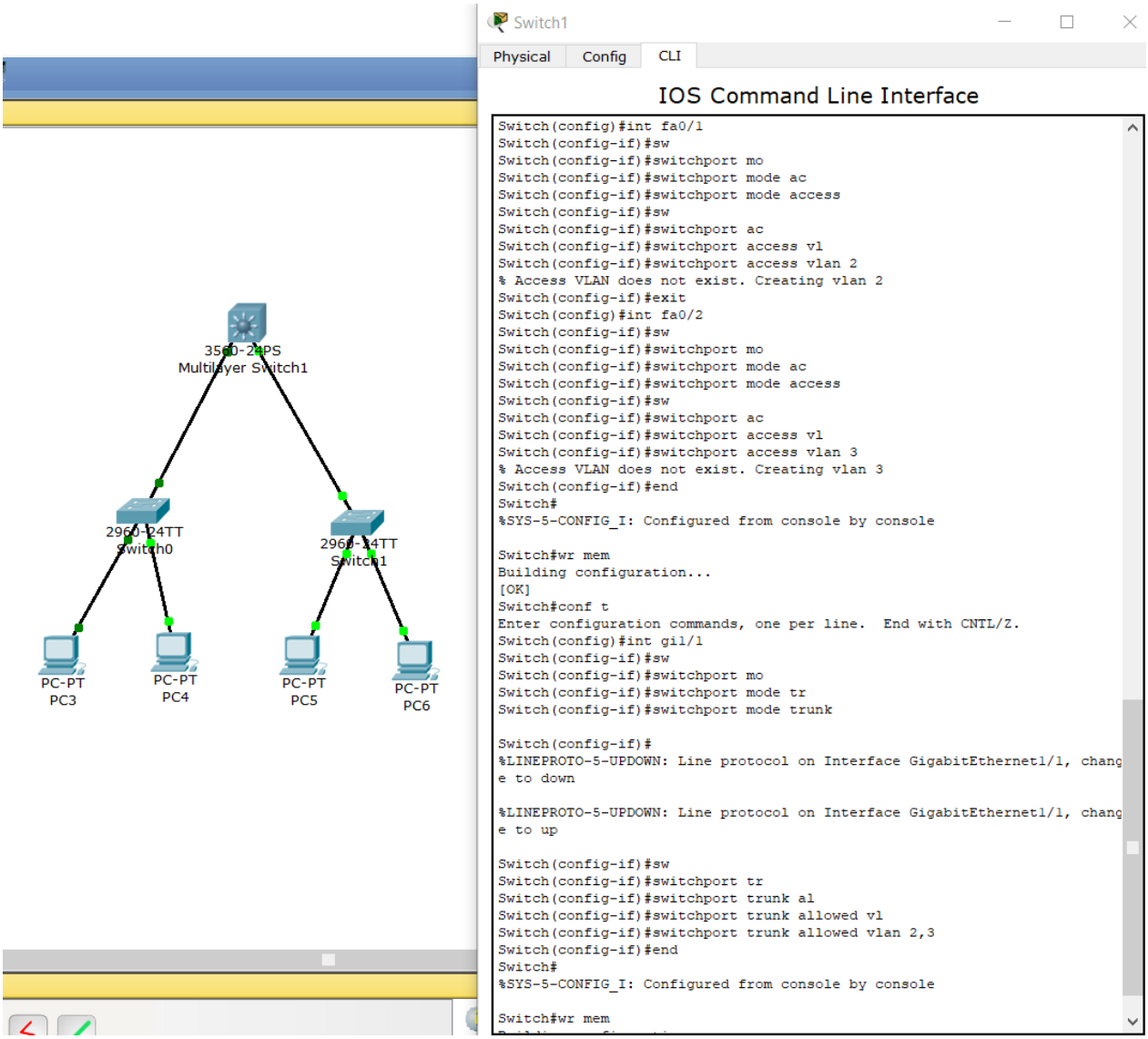


Рисунок 7.12 – Налаштування транк портів

Далі налаштовуємо L3 комутатор.

Комутатор Switch0 підключається у порт GE0/1, Switch1 підключається у порт GE0/2.

У зв’язку з тим, що це підключення між комутаторами і сюди приходить транк-лінк, налаштовуємо дані порти в транку (рис. 7.13).

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int gi0/1
Switch(config-if)#sw
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can nc
nfigured to "trunk" mode.
Switch(config-if)#?
  arp               Set arp type (arpa, probe, snap) or timeout
  bandwidth         Set bandwidth informational parameter
  cdp               Global CDP configuration subcommands
  channel-group     Etherchannel/port bundling configuration
  channel-protocol  Select the channel protocol (LACP, PAgP)
  delay             Specify interface throughput delay
  description       Interface specific description
  duplex            Configure duplex operation.
  exit              Exit from interface configuration mode
  hold-queue        Set hold queue depth
  mac-address       Manually set interface MAC address
  mdix              Set Media Dependent Interface with Crossover
  no                Negate a command or set its defaults
  power             Power configuration
  service-policy    Configure QoS Service Policy
  shutdown          Shutdown the selected interface
  spanning-tree     Spanning Tree Subsystem
  speed             Configure speed operation.
  storm-control     storm configuration
  switchport        Set switching mode characteristics
  tx-ring-limit     Configure PA level transmit ring limit
Switch(config-if)#sw
Switch(config-if)#switchport ?
  access          Set access mode characteristics of the interface
  mode            Set trunking mode of the interface
  native          Set trunking native characteristics when interface is ir
                  trunking mode
  nonegotiate     Device will not engage in negotiation protocol on this
                  interface
  port-security   Security related command
  trunk           Set trunking characteristics of the interface
  voice           Voice appliance attributes
  <cr>
Switch(config-if)#switchport
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk enc
Switch(config-if)#switchport trunk encapsulation do
Switch(config-if)#switchport trunk encapsulation dotlq
Switch(config-if)#sw
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk all
Switch(config-if)#switchport trunk allowed vl
Switch(config-if)#switchport trunk allowed vlan 2,3
Switch(config-if)#exit
Switch(config)#int
Switch(config)#interface gi0/2
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk en
Switch(config-if)#switchport trunk encapsulation do
Switch(config-if)#switchport trunk encapsulation dotlq
Switch(config-if)#sw
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk al
Switch(config-if)#switchport trunk allowed vl
Switch(config-if)#switchport trunk allowed vlan 2,3
Switch(config-if)#exit
Switch(config)#
```

Рисунок 7.13 – Налаштування транк портів L3

Далі на створені віртуальні інтерфейси розмістимо IP-адреси (рис. 7.14).

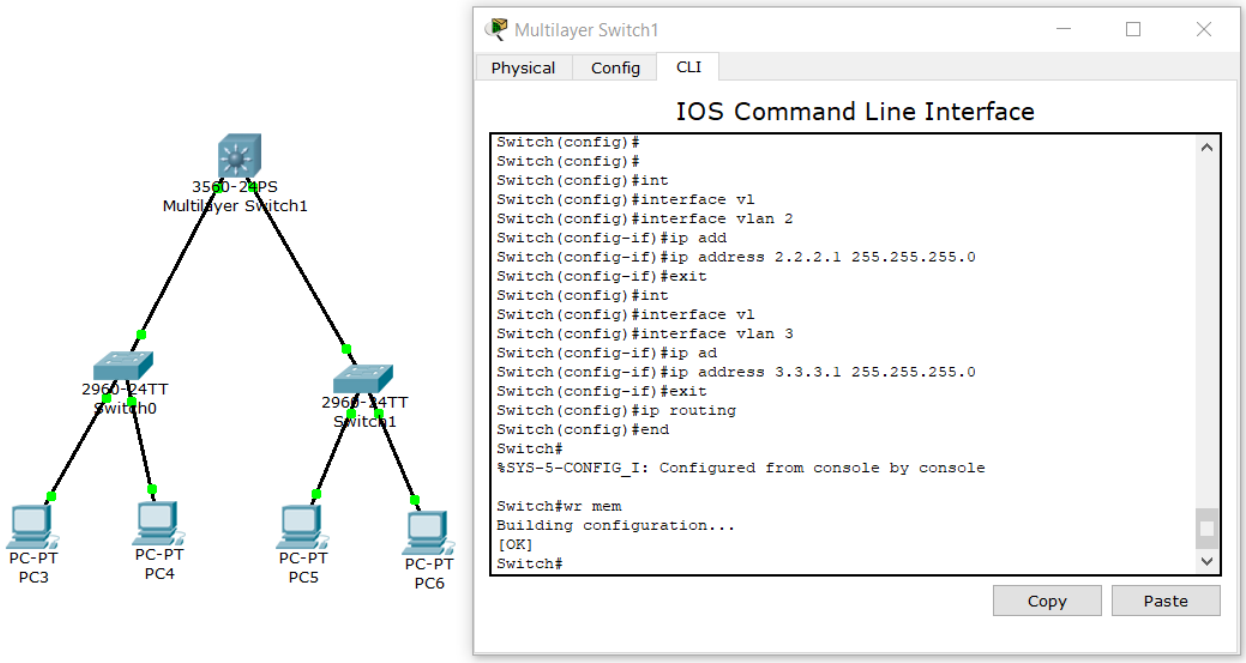


Рисунок 7.14 – Створення віртуальних інтерфейсів

Якщо комутатор автоматично не створює VLAN, вводимо наступну команду (рис. 7.15).

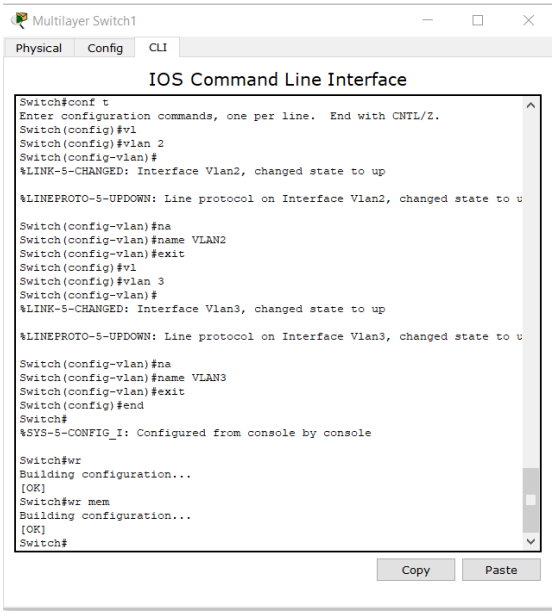


Рисунок 7.15 – створення VLAN на комутаторі L3

Далі проводимо налаштування комп'ютерів. Для PC3 задаємо IP-адресу 2.2.2.2, маску 255.255.255.0, шлюз 2.2.2.1 (IP-адреса, як на другому VLAN в комутаторі). Перевіряємо зв'язок: з PC3 пінгуємо 2.2.2.1, зв'язок повинен бути.

PC4 знаходиться у VLAN3, задаємо IP-адресу 3.3.3.2, маску 255.255.255.0, шлюз 3.3.3.1. Перевіряємо доступність мережі, ping 3.3.3.1, зв'язок має бути.

Для PC5 задаємо IP-адресу 2.2.2.3, маску 255.255.255.0, шлюз 2.2.2.1, для PC4 задаємо IP-адресу 3.3.3.3, маску 255.255.255.0, шлюз 3.3.3.1.

Перевіряємо взаємодію між мережами (рис. 7.16).

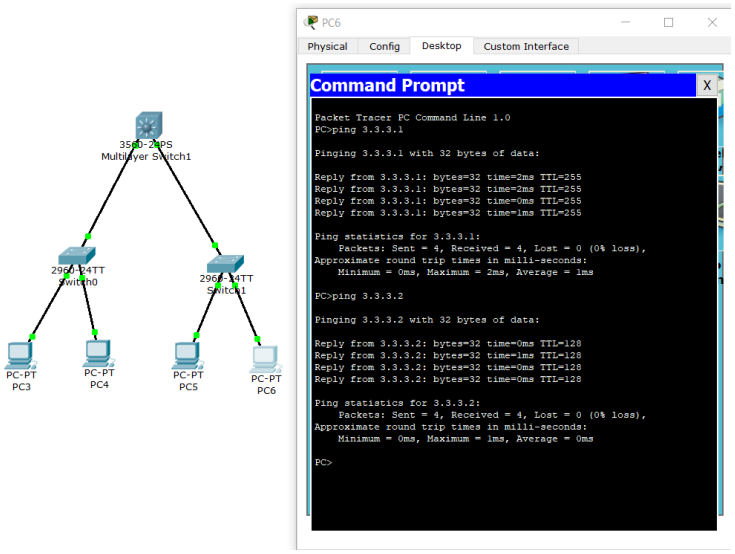


Рисунок 7.16 – Перевірка роботи мережі

Як можна побачити, з PC6 ми, подолавши три комутатори різного рівня, пропінгували PC4. Аналогічно перевіряємо VLAN2 та взаємодію між комп'ютерами різних VLAN.

Отже, ми налаштували два сегменти, обидва сегменти через транк порт йдуть на центральний комутатор.

Запитання для самопідготовки

1. У чому різниця комутаторів другого і третього рівня моделі OSI?
2. Що собою являє маска підмережі?
3. Які лінки краще використовувати між комутаторами?
4. Яку інформацію можна отримати, підвівши курсор миші до Switch0?
5. Що таке інкапсуляція?
6. Що вам відомо про dot1q?

Практичне заняття №8

ВИКОРИСТАННЯ МАРШРУТИЗАТОРІВ

Мета заняття – набути навичок використання маршрутизаторів у комп'ютерних мережах.

Коли в локальній мережі з'являються два сегменти, а саме сегмент користувачів і сегмент серверів, то виникає необхідність використання маршрутизаторів (третій рівень моделі OSI). Комутатор третього рівня це пристрій для локальної мережі, тобто даний комутатор маршрутизує трафік в локальній мережі між існуючими сегментами. Зазвичай він використовується в ієрархічній структурі мережі (рис. 8.1).

Рисунок 8.1 – Комутатор третього рівня на прикладі Catalyst 3750X

Маршрутизатор призначений, в першу чергу, для підключення локальної мережі до глобальної комп’ютерної мережі, тобто здійснює маршрутизацію трафіка у зовнішній світ (Інтернет, філіал, віддалені співробітники тощо і назад) (рис. 8.2).

Рисунок 8.2 – Зовнішній вигляд маршрутизатора

До основного функціоналу відноситься IP-маршрутизація, Network address translation (NAT), Virtual private network (VPN), іноді міжмережний екран та інше.

Комутатор третього рівня можна порівняти з швидким маршрутизатором, він вміє працювати з динамічним протоколом маршрутизації, цілком сумісний з маршрутизатором. Також доступне налаштування списків доступу (access-list). Але відмінна різниця з маршрутизатором у ціні та продуктивності. Сучасні комутатори 3-го рівня у десятки чи сотні разів переважають маршрутизатори по продуктивності. Це обумовлено використанням у комутаторах наборів спеціалізованих мікросхем, маршрутизація (обробка пакетів) проходить при цьому на апаратному рівні, а програмна підтримка залишається для процедур, які напряму не зв’язані з обробкою трафіку.

У звичайного маршрутизатора обробка пакетів реалізована програмно, і він, як правило, функціонує на процесорі загального призначення. Однак деякі сучасні маршрутизатори мають виділені мікросхеми для прискорення обробки пакетів без використання процесора (але вони в рази дорожчі комутаторів третього рівня з аналогічними характеристиками).

Наприклад, якщо в організації розташовано декілька потужних серверів і потребується маршрутизація трафіка на великих швидкостях, десятки Гігабіт за

секунду, то підійде лише комутатор третього рівня. Маршрутизатор з такою пропускною здатністю просто не впорається.

Але загалом, комутатор третього рівня програє по можливостям традиційному маршрутизатору.

Сучасні маршрутизатори можна перетворити у міжмережний екран, і головне, він має функції NAT, VPN – а це підключення віддалених філіалів, віддалених користувачів і різні функції безпеки.

У підсумку можна зазначити, що маршрутизатор ми застосовуємо у тому випадку, коли необхідно підключити наш офіс до мережі Інтернет або до регіональної мережі.

Розглянемо мережу невеликого офісу. При невеликому локальному трафіку і відсутності виділених локальних серверів, в нас немає необхідності ставити комутатор 3-го рівня, тому що, у першу чергу, це буде не рентабельно.

Тому використаємо маршрутизатор для доступу у мережу, PC0-VLAN2, PC1-VLAN3, PC2-VLAN4, (рис. 8.3).

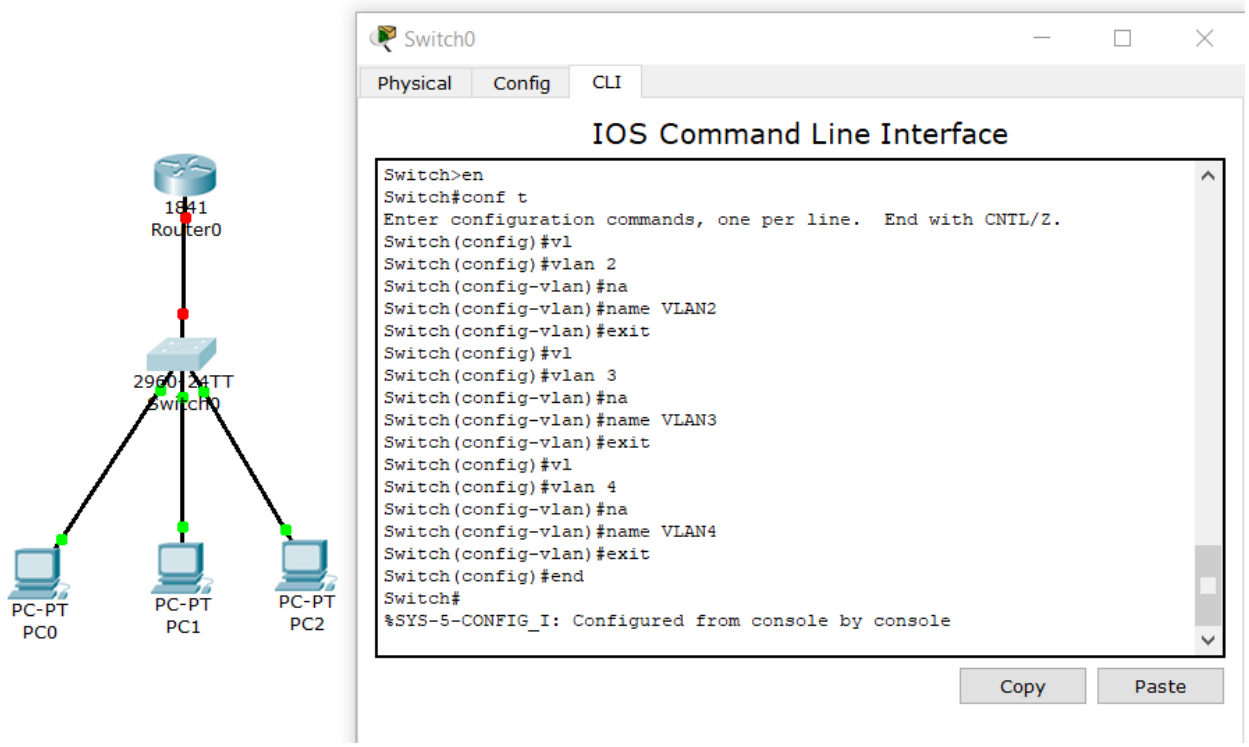


Рисунок 8.3. – Організація мережі невеликого офісу

На наступному етапі визначаємо наші комп’ютери в необхідний сегмент (рис. 8.4).

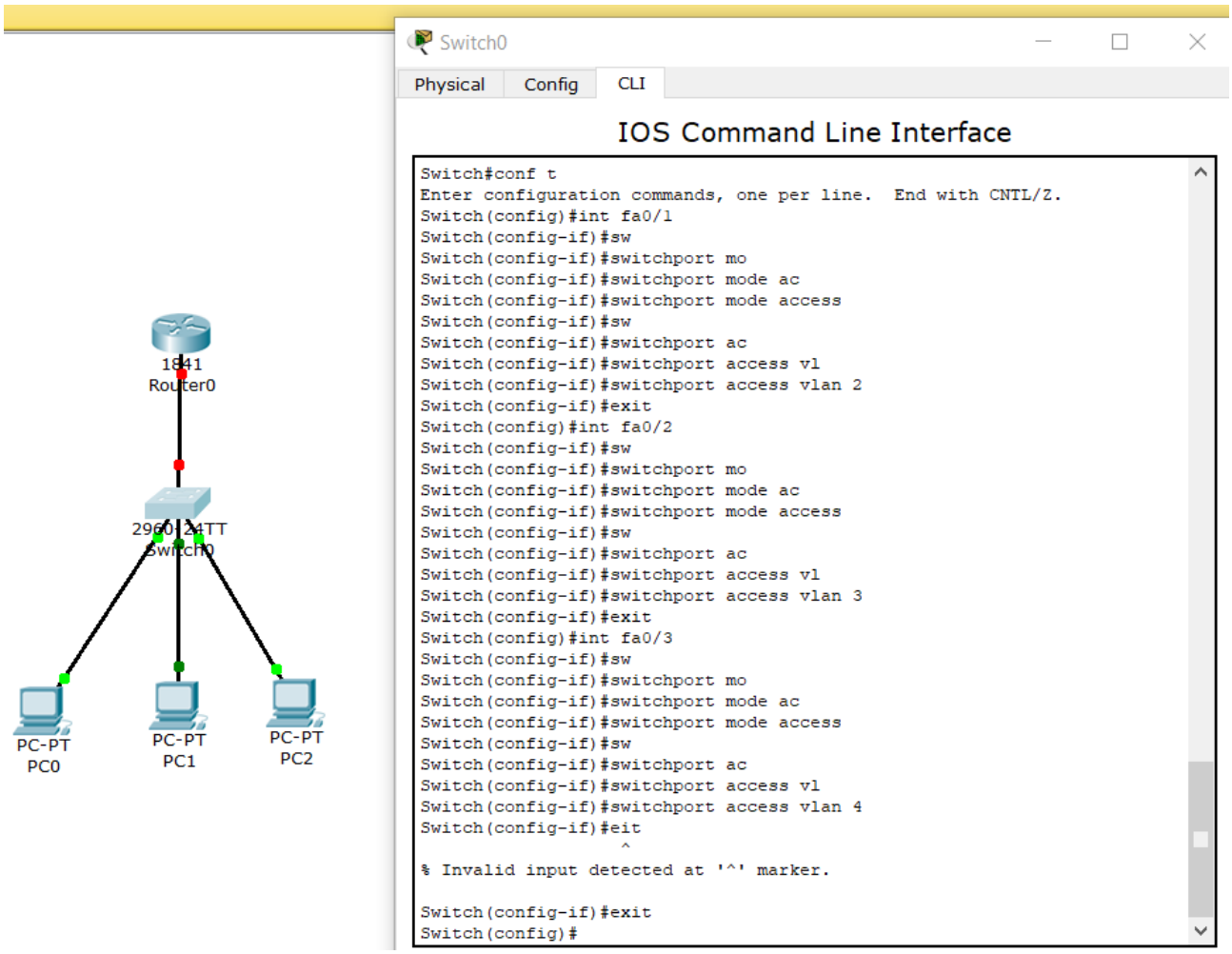


Рисунок 8.4 – Визначення комп’ютерів

Далі налаштовуємо транкпорт від комутатора до маршрутизатора (рис. 8.5).

```
Switch(config)#int fa0/4
Switch(config-if)#sw
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk vl
Switch(config-if)#switchport trunk al
Switch(config-if)#switchport trunk allowed vl
Switch(config-if)#switchport trunk allowed vlan 2,3,4
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

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

Рисунок 8.5 – Налаштування транк порту

Переходимо до налаштування маршрутизатора (роутера). Спочатку піднімемо фізичний порт (бо на відміну від маршрутизаторів, на роутерах всі порти за замовчування в режимі «down»). (рис. 8.6).

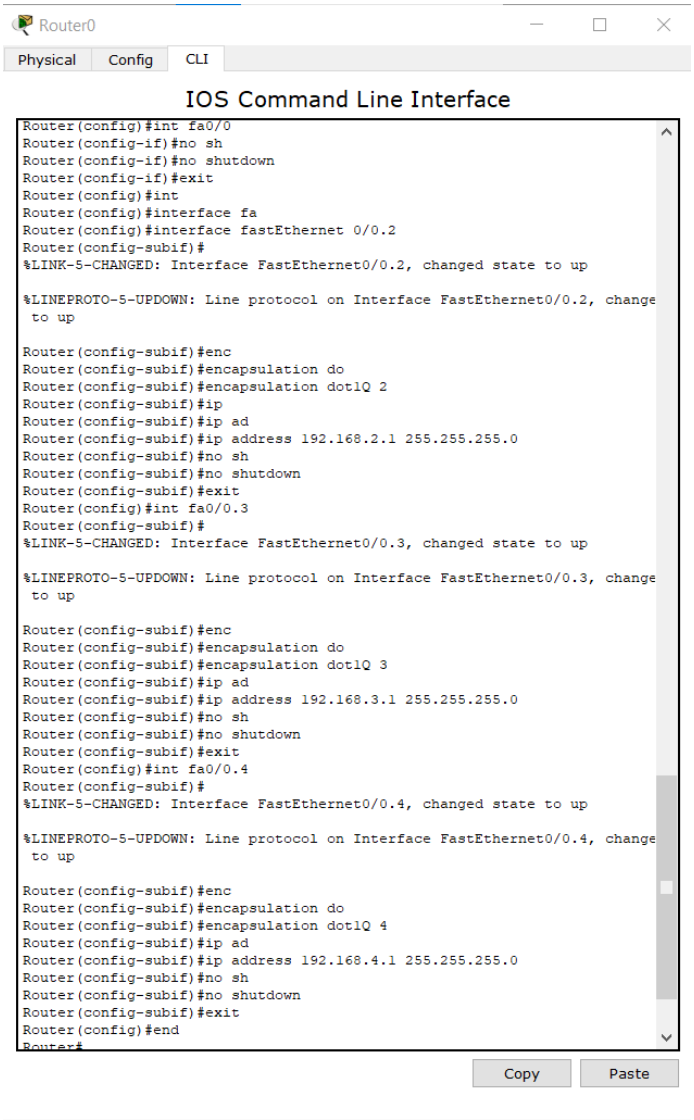


Рисунок 8.6 – Налаштування роутера

Опишемо вищенаведені опції. Оскільки на роутер приходять декілька VLAN, в нашому випадку три, ми створюємо на роутері sub-інтерфейс (під інтерфейси). Кожному під інтерфейсу відповідає окремий VLAN. У вище наведеному коді це виражається через *Router(config)#interface fastEthernet 0/0.2* (.2 це і є sub-інтерфейс). Також номер VLAN ми вказуємо командою *Router(config-subif)#encapsulation dot1Q 2.*

Далі перевіримо налаштування за допомогою show run (рис. 8.7).

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
```

Рисунок 8.7 – Перевірка налаштувань

Як ми бачимо фізичний інтерфейс це FastEthernet0/0, а нижче вказані три створені sub-інтерфейси.

Далі прописуємо на комп'ютерах відповідні мережі. PC0 (VLAN2) прописуємо IP-адресу 192.168.2.2, маску 255.255.255.0, шлюз. IP-адресу роутера 192.168.2.1. PC1 (VLAN3) прописуємо IP-адресу 192.168.3.2, маску 255.255.255.0, шлюз IP-адресу роутера 192.168.3.1. PC2 (VLAN4) прописуємо IP-адресу 192.168.4.2, маску 255.255.255.0, шлюз IP-адресу роутера 192.168.4.1.

Далі тестуємо пінгування шлюзу з PC2 (рис. 8.8).

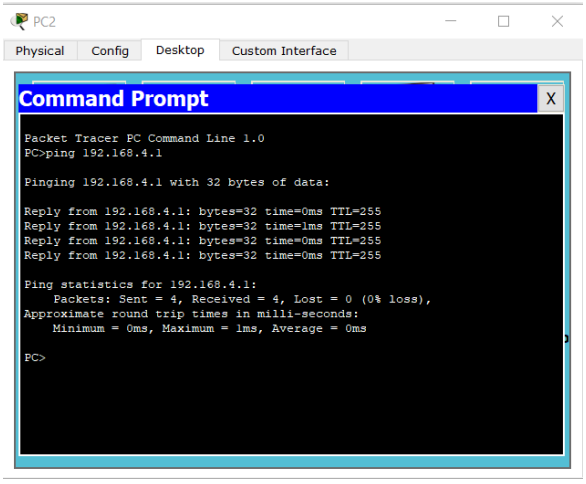


Рисунок 8.8 – Тестове пінгування шлюзу з PC2

Аналогічно спробуємо пропінгувати сусідні сегменти: ping 192.168.2.2, ping 192.168.3.2. Таким чином ми організували маршрутизацію трафіку між

трьома сегментами без використання комутатора третього рівня. Також маршрутизатор може використовуватися для маршрутизації локального трафіка в мережу Інтернет за допомогою NAT або звичайної маршрутизації.

Далі ускладнимо нашу схему, додавши комутатори 3-го рівня, сервери, додаткові комутатори другого рівня. В даному прикладі локальний трафік значний і знадобиться висока пропускна здатність до локальних серверів.

Призначимо PC3 – VLAN2, PC4 – VLAN3, PC5 – VLAN2, PC6 – VLAN3, два сервери – VLAN4.

Спочатку проведемо налаштування Switch1 (рис. 8.9).

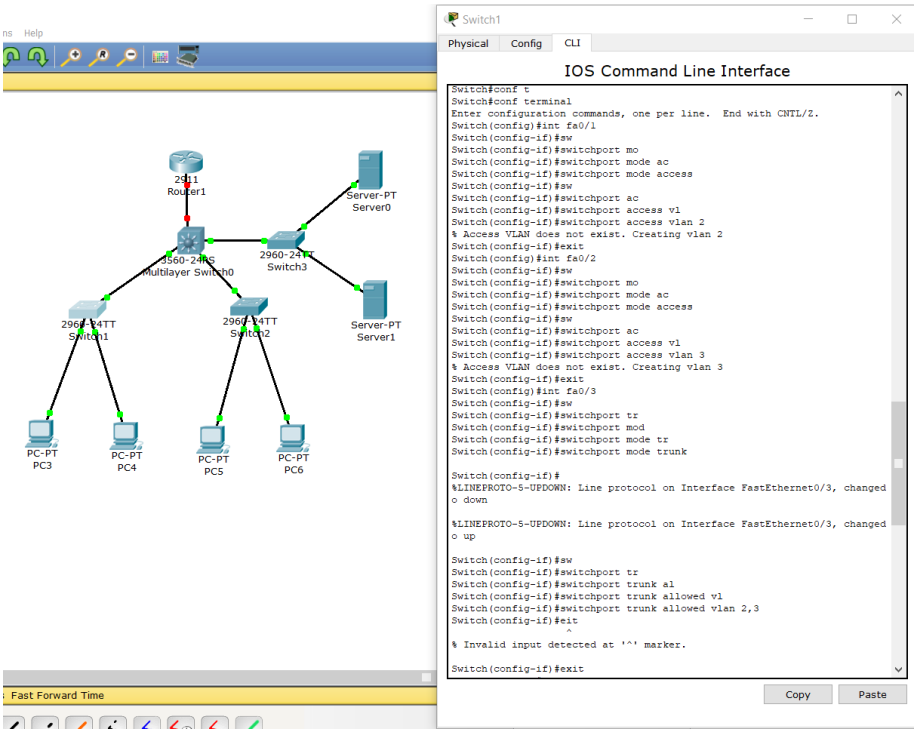


Рисунок 8.9 – Налаштування Switch1

Далі перевіряємо налаштування Switch1 (рис. 8.10).

```
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/3
 switchport trunk allowed vlan 2-3
 switchport mode trunk
```

Рисунок 8.10 – Перевірка налаштування Switch1

Аналогічні налаштування і перевірку проводимо для Switch2 (рис. 8.11).

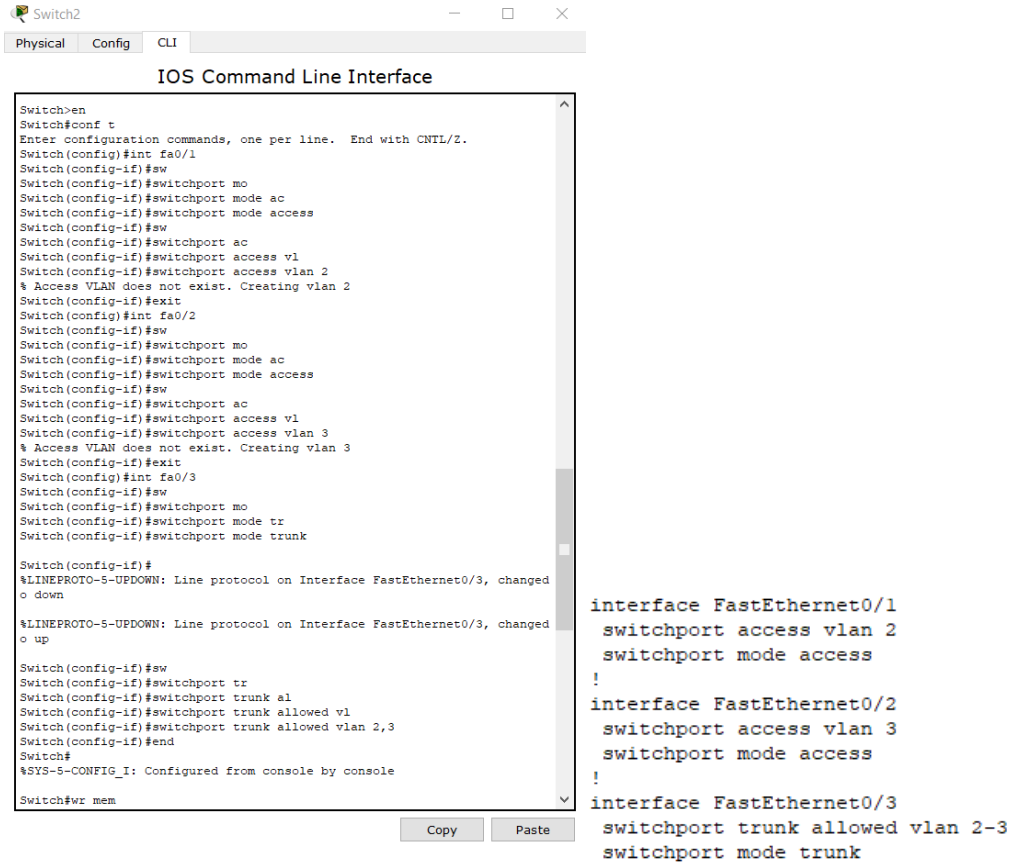


Рисунок 8.11 – Налаштування та перевірка налаштування Switch2

Налаштовуємо один VLAN4 на Switch3, де порти які направлені в сторону серверів налаштовані як access-порти, а fe0/3 це транк порт до комутатора третього рівня (рис. 8.12).

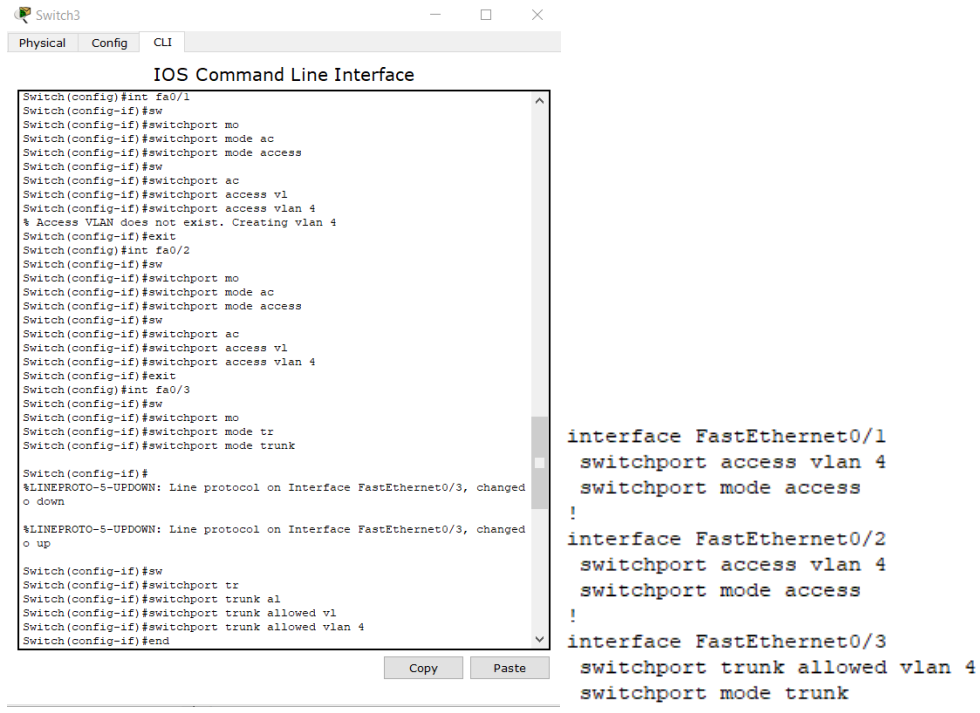


Рисунок 8.12 – Налаштування Switch3

Задаємо параметри комп’ютерів та серверів:

PC3 (VLAN2) IP-адреса 192.168.22.2, маска 255.255.255.0, шлюз 192.168.22.1.

PC5 (VLAN2) IP-адреса 192.168.22.3, маска 255.255.255.0, шлюз 192.168.22.1.

PC4 (VLAN3) IP-адреса 192.168.33.2, маска 255.255.255.0, шлюз 192.168.33.1.

PC6 (VLAN3) IP-адреса 192.168.33.3, маска 255.255.255.0, шлюз 192.168.33.1.

Server0 (VLAN4) IP-адреса 192.168.44.2, маска 255.255.255.0, шлюз 192.168.44.1.

Server1 (VLAN4) IP-адреса 192.168.44.3, маска 255.255.255.0, шлюз 192.168.44.1.

Проведемо налаштування комутатора 3-го рівня (рис. 8.13).

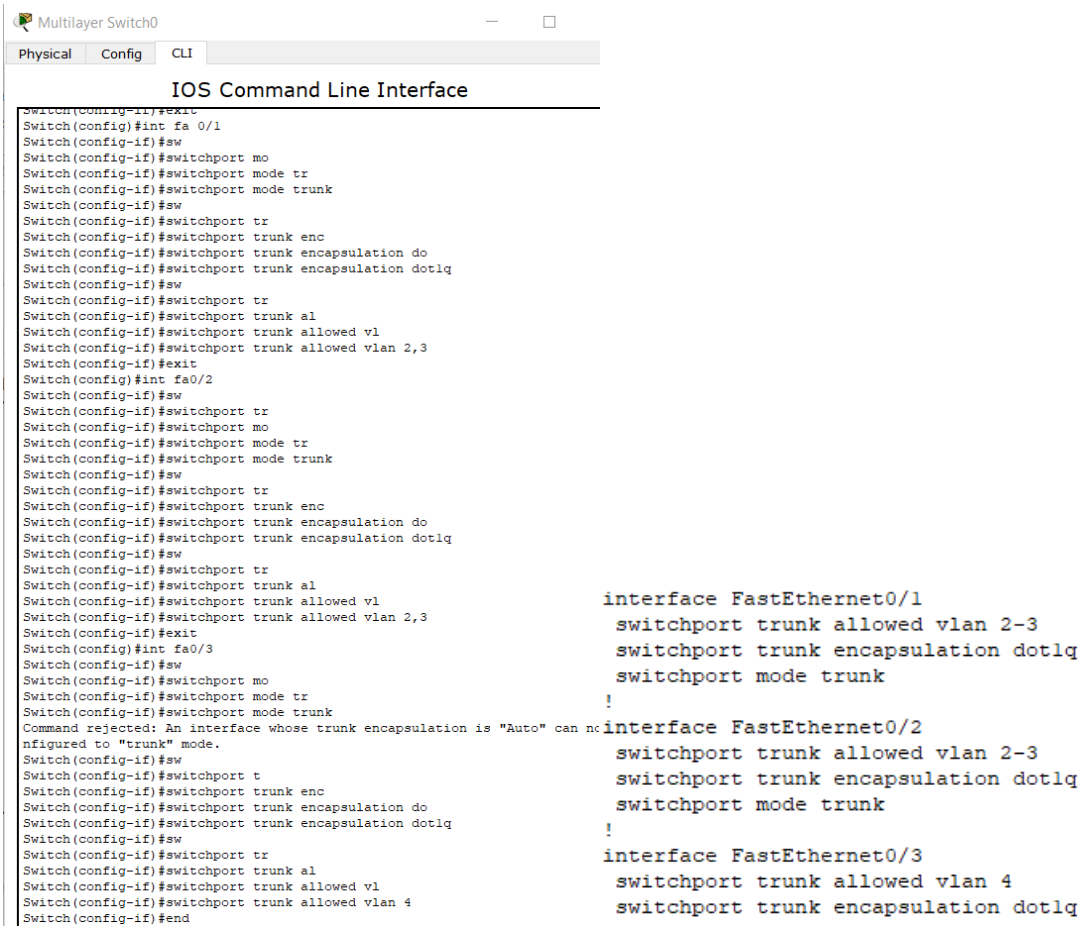


Рисунок 8.13 – Налаштування комутатора третього рівня

На рисунку 8.14 наведемо призначення IP-адрес.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int
Switch(config)#interface vl
Switch(config)#interface vlan 2
Switch(config-if)#ip ad
Switch(config-if)#ip address 192.168.22.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#int
Switch(config)#interface vl
Switch(config)#interface vlan 3
Switch(config-if)#ip ad
Switch(config-if)#ip address 192.168.33.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#int
Switch(config)#interface vl
Switch(config)#interface vlan 4
Switch(config-if)#ip ad
Switch(config-if)#ip address 192.168.44.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr mem
Building configuration...
[OK]
Switch#show run
```

```
interface FastEthernet0/1
 switchport trunk allowed vlan 2-3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk allowed vlan 2-3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk allowed vlan 4
 switchport trunk encapsulation dot1q
!
```

Рисунок 8.14 – Налаштування комутатора третього рівня: IP-адреси

Перевіряємо зв’язок, наприклад з PC3 на PC5, PC3 на PC6, PC3 на Server 0 (рис. 8.15).

```
Pinging 192.168.22.3 with 32 bytes of data:

Reply from 192.168.22.3: bytes=32 time=0ms TTL=128
Reply from 192.168.22.3: bytes=32 time=1ms TTL=128
Reply from 192.168.22.3: bytes=32 time=0ms TTL=128
Reply from 192.168.22.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.22.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.33.3

Pinging 192.168.33.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.33.3: bytes=32 time=0ms TTL=127
Reply from 192.168.33.3: bytes=32 time=0ms TTL=127
Reply from 192.168.33.3: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.33.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.44.2

Pinging 192.168.44.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.44.2: bytes=32 time=0ms TTL=127
Reply from 192.168.44.2: bytes=32 time=0ms TTL=127
Reply from 192.168.44.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.44.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 8.15 – Приклад пінгування з PC3

Якщо пінгування не йде на комп’ютери, що належать іншим VLAN, виконайте дії з комутатором 3-го рівня, описані в минулій лабораторній роботі на рисунках 7.9 та 7.15.

Далі проводимо налаштування між комутатором 3-го рівня та роутером. Припустимо, що це буде VLAN5 (рис. 8.16, 8.17).

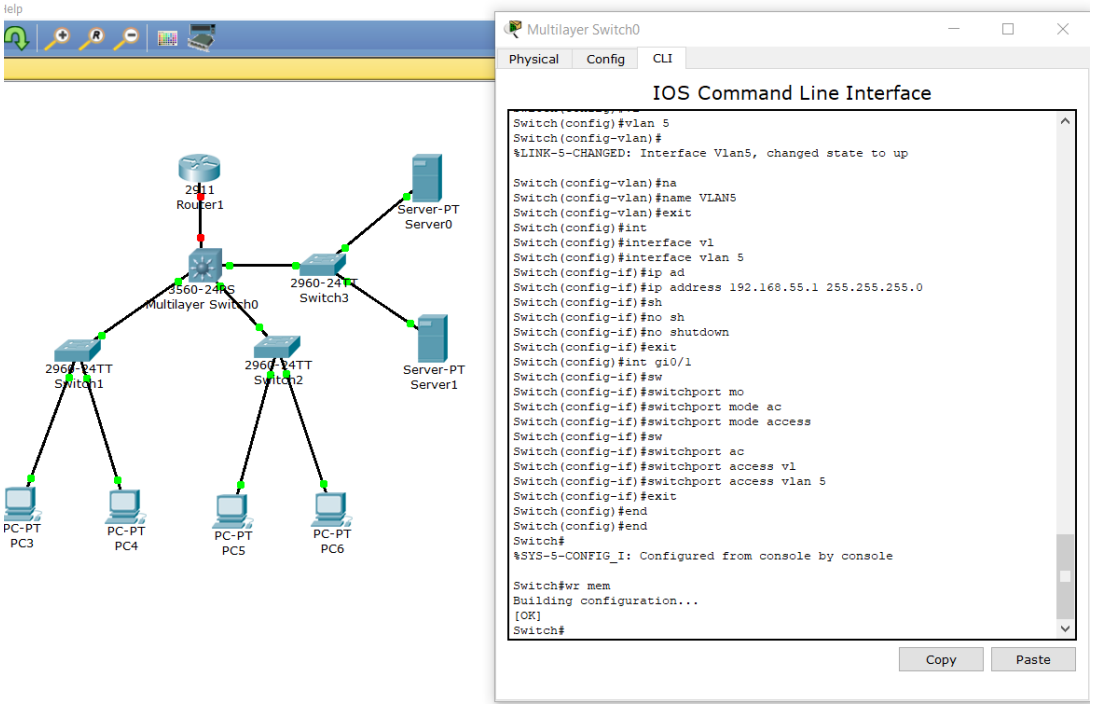


Рисунок 8.16. – Налаштування VLAN5 на комутаторі L3

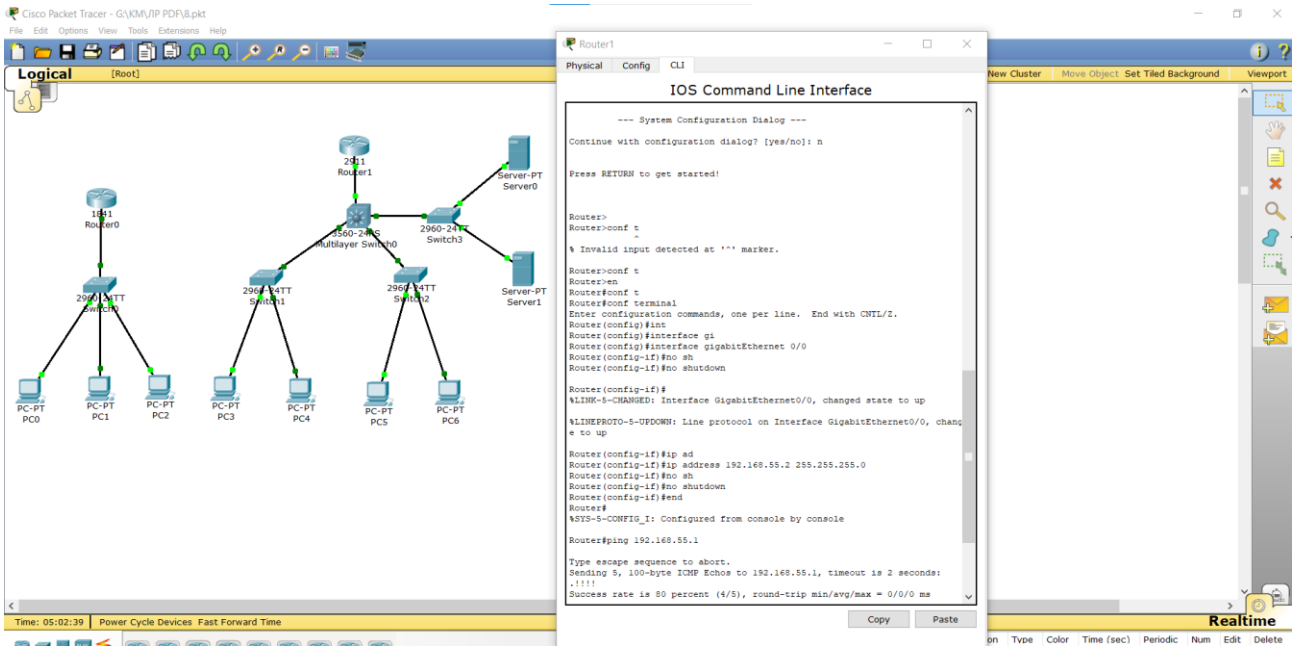


Рисунок 8.17 – Налаштування роутера 2911

Наприкінці обов’язково збережіть даний файл з налаштуваннями.

Запитання для самопідготовки

1. Наведіть спільні риси та основні відмінності комутатора 3-го рівня та маршрутизатора.

2. В чому різниця налаштування фізичних портів за замовчуванням у комутаторах 2-го рівня та маршрутизаторі?

3. Наведіть синтаксис створення sub-інтерфейсу.

4. Для чого створюються віртуальні інтерфейси?

5. Які ви знаєте способи пінгування?

Практичне заняття №9.
СТАТИЧНА МАРШРУТИЗАЦІЯ

Мета заняття – ознайомитися та впровадити методи статичної маршрутизації при проектуванні комп'ютерних мереж

Застосування маршрутизації дозволяє впорядкувати мережу будь-яких розмірів.

Статичні маршрути дуже поширені, при цьому вони не вимагають такої ж кількості обчислень і операцій, як протоколи динамічної маршрутизації. Маршрутизатор можна повідомити про віддалені мережі одним з двох способів: вручну, коли віддалені мережі вручну вводяться в таблицю маршрутизації за допомогою статичних маршрутів і динамічно віддалені маршрути, що автоматично додаються за допомогою протоколу динамічної маршрутизації.

Статична маршрутизація має свої переваги, в порівнянні з динамічною маршрутизацією в тому, що статичні маршрути не оголошуються по мережі, що робить їх більш безпечними.

Статичні маршрути використовують більш вузьку смугу пропускання, ніж протоколи динамічної маршрутизації (для розрахунку і зв'язку маршрутів цикли центрального процесора не використовуються). Шлях, який використовується статичним маршрутом для відправки даних, відомий.

Використовуючи схему минулої лабораторної роботи, згадаємо, що:

PC0 (VLAN2) IP-адреса 192.168.2.2, маска 255.255.255.0, шлюз 192.168.2.1.

PC1 (VLAN3) IP-адреса 192.168.3.2, маска 255.255.255.0, шлюз 192.168.3.1.

PC2 (VLAN4) IP-адреса 192.168.4.2, маска 255.255.255.0, шлюз 192.168.4.1.

PC3 (VLAN2) IP-адреса 192.168.22.2, маска 255.255.255.0, шлюз 192.168.22.1.

PC4 (VLAN3) IP-адреса 192.168.33.2, маска 255.255.255.0, шлюз 192.168.33.1.

PC5 (VLAN2) IP-адреса 192.168.22.3, маска 255.255.255.0, шлюз 192.168.22.1.

PC6 (VLAN3) IP-адреса 192.168.33.3, маска 255.255.255.0, шлюз 192.168.33.1.

Server0 (VLAN4) IP-адреса 192.168.44.2, маска 255.255.255.0, шлюз 192.168.44.1.

Server1 (VLAN4) IP-адреса 192.168.44.3, маска 255.255.255.0, шлюз 192.168.44.1.

Перевіримо IP-адресу, наприклад, PC0 (рис. 9.1).

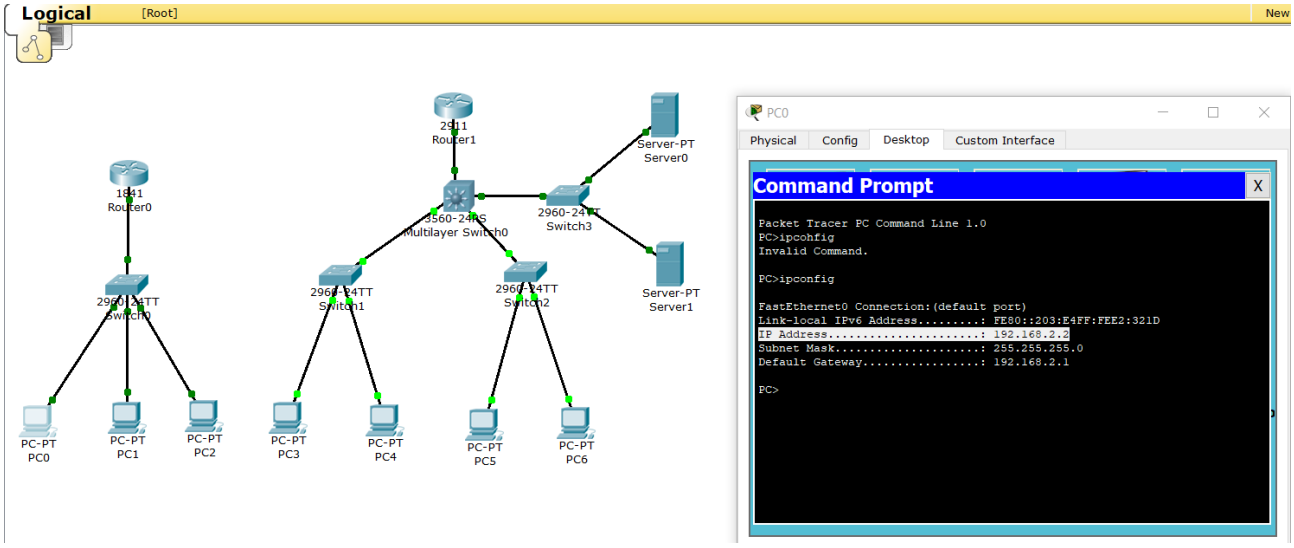


Рисунок 9.1 – Схема розміщення комп’ютерів та перевірка IP-адреси PC0

Також пінгуємо з PC0 на 192.168.3.2, з PC0 на 192.168.4.2, з PC3 на 192.168.22.3, з PC3 на 192.168.33.2, з PC3 на 192.168.44.2 тощо – зв'язок повинен бути. Якщо з роутера 2911 пропінгувати комутатор 3-го рівня *Router#ping 192.168.55.1*, то ми побачимо, що зв'язок встановлено. Але, якщо пропінгувати комп'ютер, наприклад 192.168.22.2, то зв'язку не буде. Це пов'язано з статичними маршрутами. Прямий лінк між 2911 та PC3 відсутній, доступний лише через комутатор третього рівня.

Для встановлення зв'язку необхідно прописати маршрути (рис. 9.2).

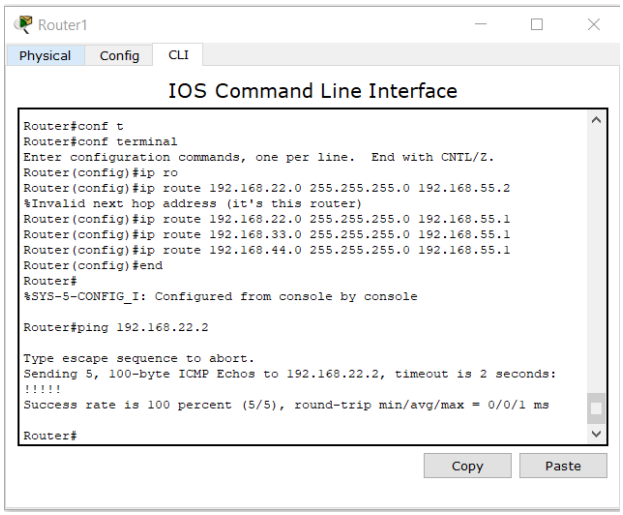


Рисунок 9.2 – Налаштування маршрутів

Як ми бачимо, тепер з роутера 2911 є зв'язок на комп'ютер 192.168.22.2. Перевіряємо доступність 192.168.33.2 та 192.168.44.2. З'єднаємо наші два комутатори кабелем за автопідбором і проведемо налаштування (рис. 9.3).

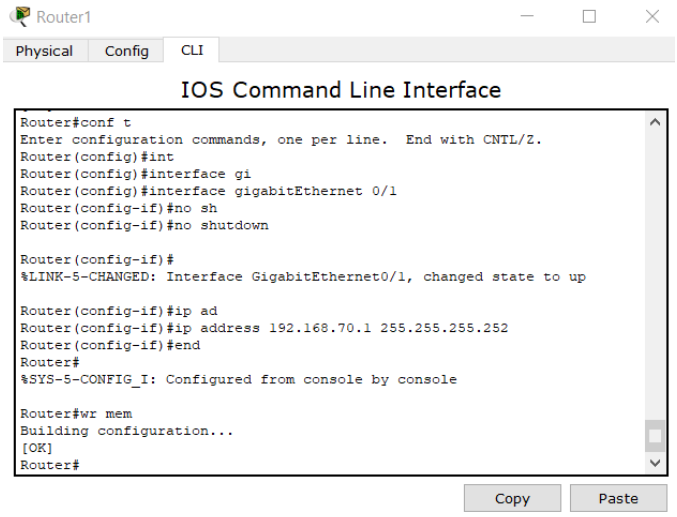


Рисунок 9.3 – Налаштування на першому роутері порту gi0/1

Налаштовуємо порт на роутері 0 (рис. 9.4).

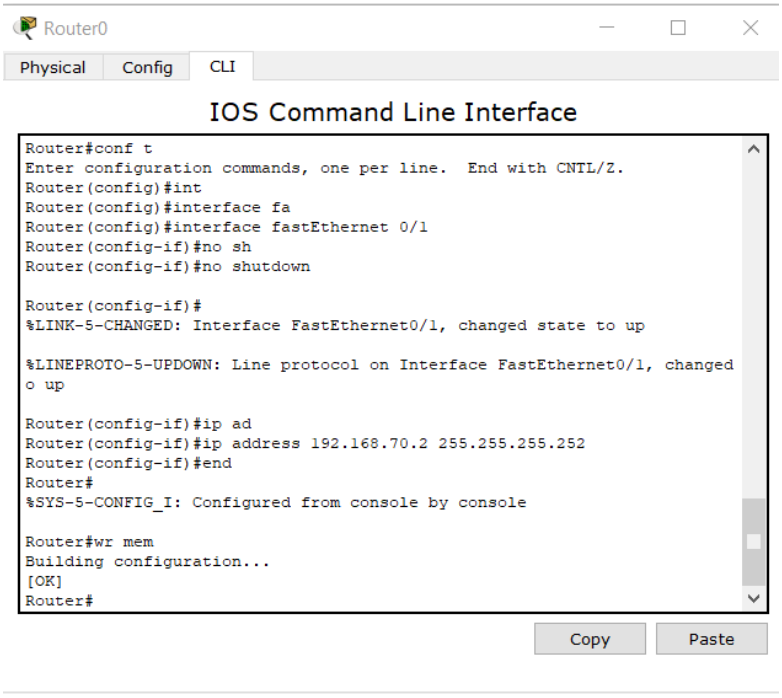


Рисунок 9.4 – Налаштування на роутері0

Лінки повинні встановитися. З роутера 0 пінгуємо роутер 1 наступним чином: *Router#ping 192.168.70.1*, зв’язок встановлено. Але необхідно розробити маршрути (рис. 9.5).

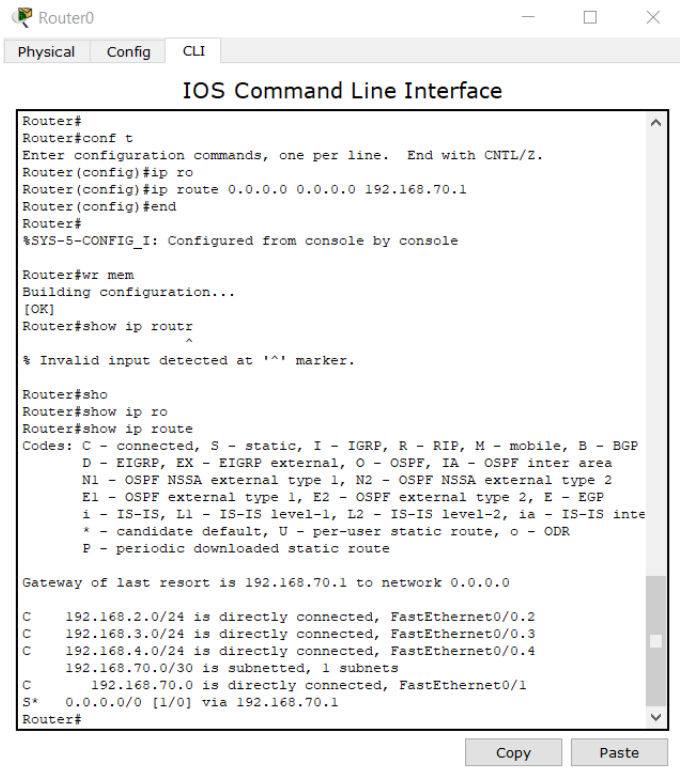


Рисунок 9.5 – Налаштування маршрутів

Але навіть за цих умов не буде зв'язку з PC0 на PC3. На даний момент пакет йде за маршрутом PC0-Switch0-Router0-Router1-Multilayer-Switch0-Switch1-PC3. Але коли пакет повертається, то він йде по маршруту PC3-Switch1-Multilayer-Switch0-далі комутатор 3-го рівня не має відомостей про мережу, де розміщений PC0. Маршрутизатор 2911 також не має відомостей про мережу PC0, а саме де її шукати. Вносимо корективи до комутатора 3-го рівня, який має лише одну точку виходу у зовнішнє середовище, задаємо дефолтний маршрут на комутаторі третього рівня *Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.55.2*.

Далі на роутері 1 пропишемо маршрут через мережу на роутер 0. *Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.70.2* і перевіримо пінгування з роутера 1 на PC0 – пінгування успішне.

Далі виконуємо пінгування з PC0 (рис. 9.6).

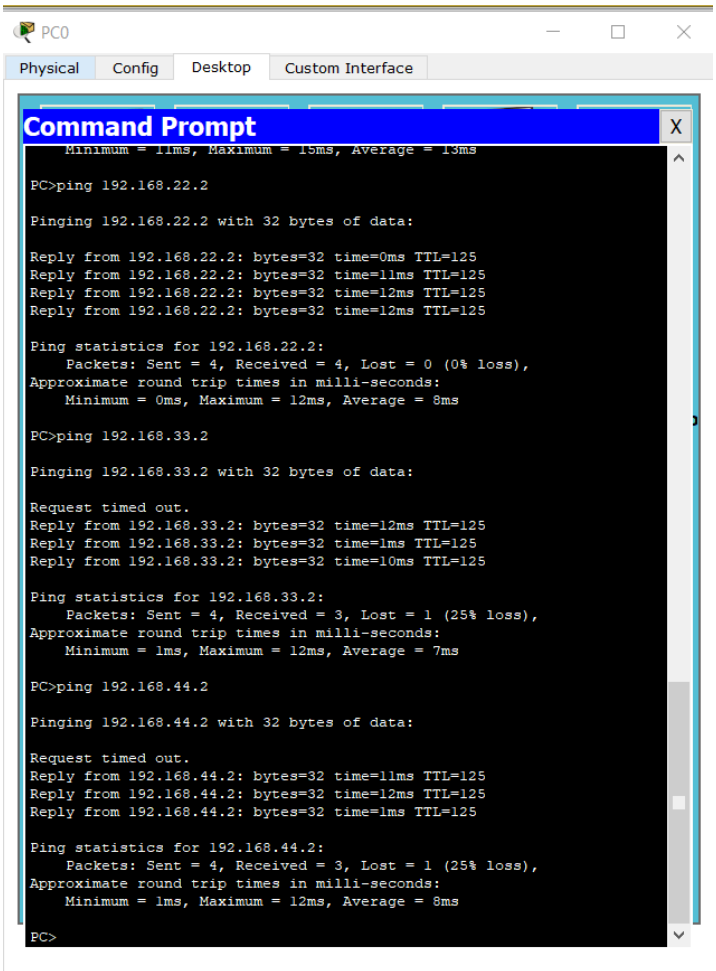


Рисунок 9.6 – Пінгування з PC0

Аналогічно перевіряємо з PC1 на 192.168.22.2 – зв'язку немає. Це пов'язано з тим, що на роутері 1 ми прописали всього один маршрут (тільки у мережу 2.0). Виправимо це (рис. 9.7).

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.70.2
Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.70.2
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
```

Рисунок 9.7 – Налаштування 1 роутера

Далі знов перевіряємо з PC1 на 192.168.22.2: *PC>ping 192.168.22.2* – зв'язок встановлено. Також перевіримо з PC2 на 192.168.22.2 – все працює.

Таким чином ми налаштували зв'язок між двома офісами засобами маршрутизації.

Запитання для самопідготовки

1. Що позначає даний запис?
2. Де використовуються статичні маршрути?
3. Наведіть переваги та недоліки статичних маршрутів.
4. Наведіть характеристики статичного маршруту за замовчуванням.
5. Які мережі вважать дистанційними?

Практичне заняття №10

DYNAMIC HOST CONFIGURATION PROTOCOL

Мета заняття – набути навичок використання Dynamic host configuration protocol.

Якщо у мережі багато комп'ютерів, то вручну незручно налаштовувати IP-адреси. Для автоматичного налаштування IP-адрес комп'ютерів використовується Dynamic host configuration protocol **(**DHCP).

У процесі налаштування задіяні DHCP клієнт (звичайний комп'ютер) та DHCP сервер (маршрутизатор або виділений DHCP сервер).

Створимо елементарну схему і налаштуємо роутер (рис. 10.1).

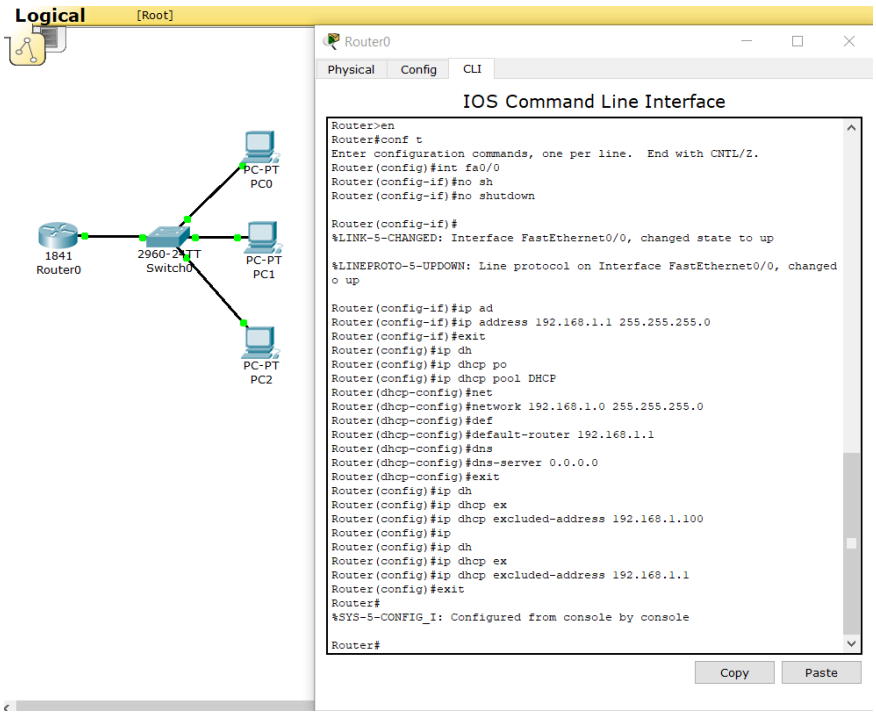


Рисунок 10.1 – Створення тестової схеми та налаштування роутера

На даному рисунку ми створили DHCP-pool – простір IP-адрес з ім'ям DHCP (*Router(config)#ip dhcp pool DHCP*). У якості DHCP сервера виступає наш роутер. Також задали з якої мережі (що і IP-адреса на інтерфейсі маршрутизатора) ми будемо роздавати IP-адреси комп'ютерам (*Router(dhcp-config)#network 192.168.1.0 255.255.255.0*).

Комп'ютерам ми повинні видати не тільки IP-адресу, а й дефолтний маршрут (*Router(dhcp-config)#default-router 192.168.1.1*). При цьому вказуємо IP-адресу нашого маршрутизатора, оскільки саме він займається маршрутизацією і буде шлюзом за замовчуванням.

Також, якщо нам необхідний буде вихід в Інтернет з нашої мережі, необхідно вказати Domain name system (DNS) сервер (*Router(dhcp-config)#dns-server 0.0.0.0*). У якості прикладу задали DNS сервер Google.

Використовуємо функцію виключення IP-адрес з пулу (наприклад для серверу або роутера) *Router(config)#ip dhcp excluded-address 192.168.1.100* – для сервера та *Router(config)#ip dhcp excluded-address 192.168.1.1* для роутера.

На всіх комп'ютерах ставимо позначку замість Static DHCP і бачимо параметри, які нам видав DHCP сервер. У реальних мережах даний параметр

змінювати не потрібно, на комп'ютерах реальних параметр DHCP стоїть за замовчуванням (рис. 10.2).

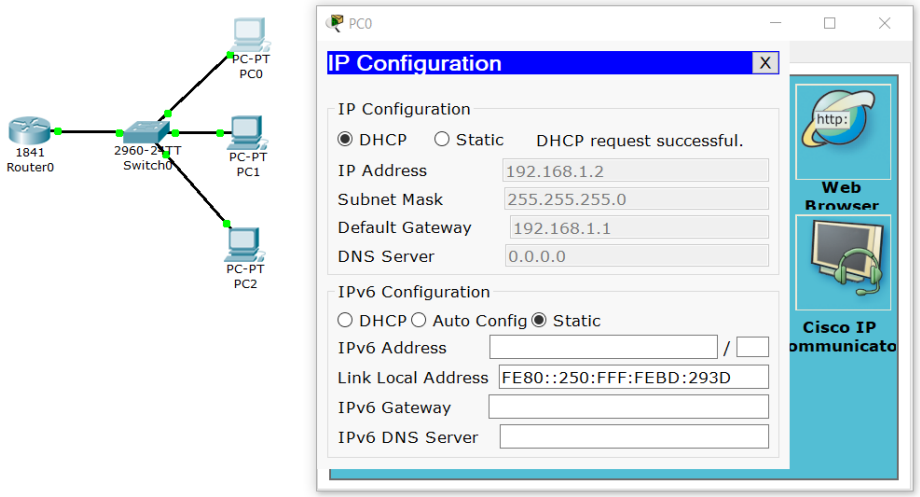


Рисунок 10.2 – Результат застосування параметрів

Далі перевіряємо взаємодію з PC0 (рис. 10.3).

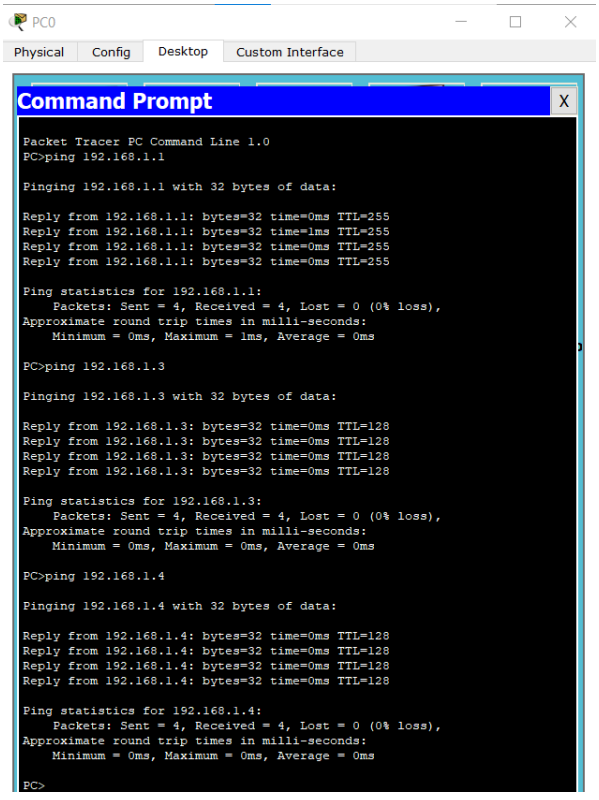


Рисунок 10.3 – Пінгування мережі

Розглянемо складнішу мережу. fa0/1 на роутер, fa0/2 на PC3, fa0/3 на PC4, fa0/4 на PC5, fa0/5 на PC6, fa0/6 на сервер (рис. 10.4).

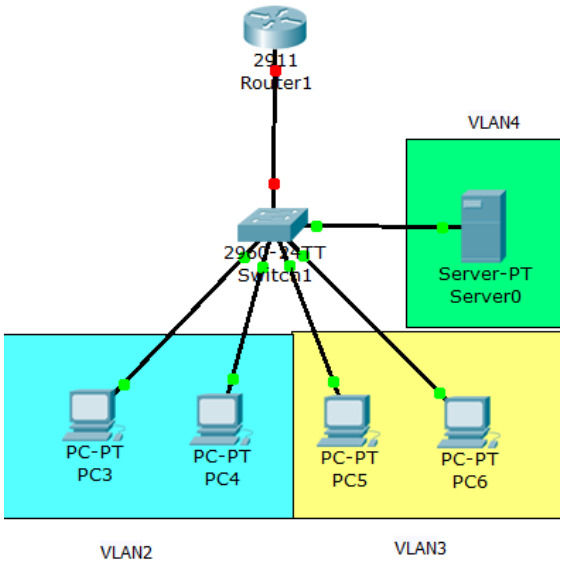


Рисунок 10.4 – Тестова схема 2

Налаштовуємо комутатор (рис. 10.5).

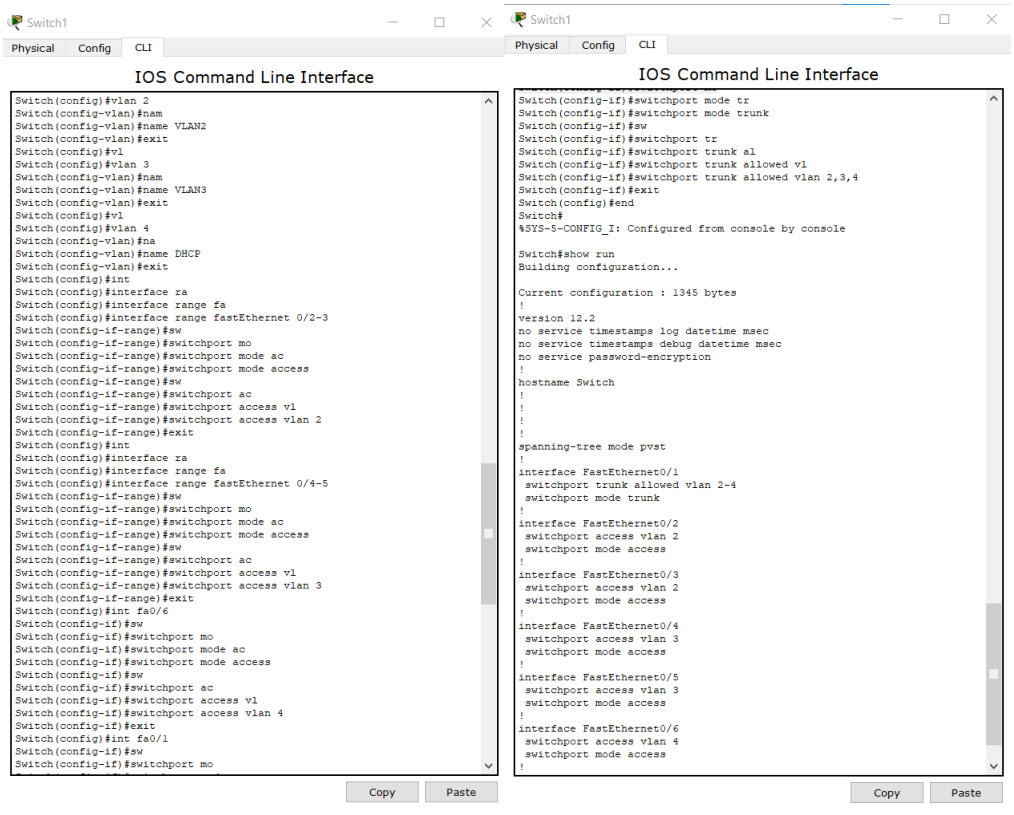


Рисунок 10.5 – Налаштування комутатора та перевірка show run

Проводимо налаштування маршрутизатора, створюючи спочатку sub-інтерфейси (рис. 10.6).

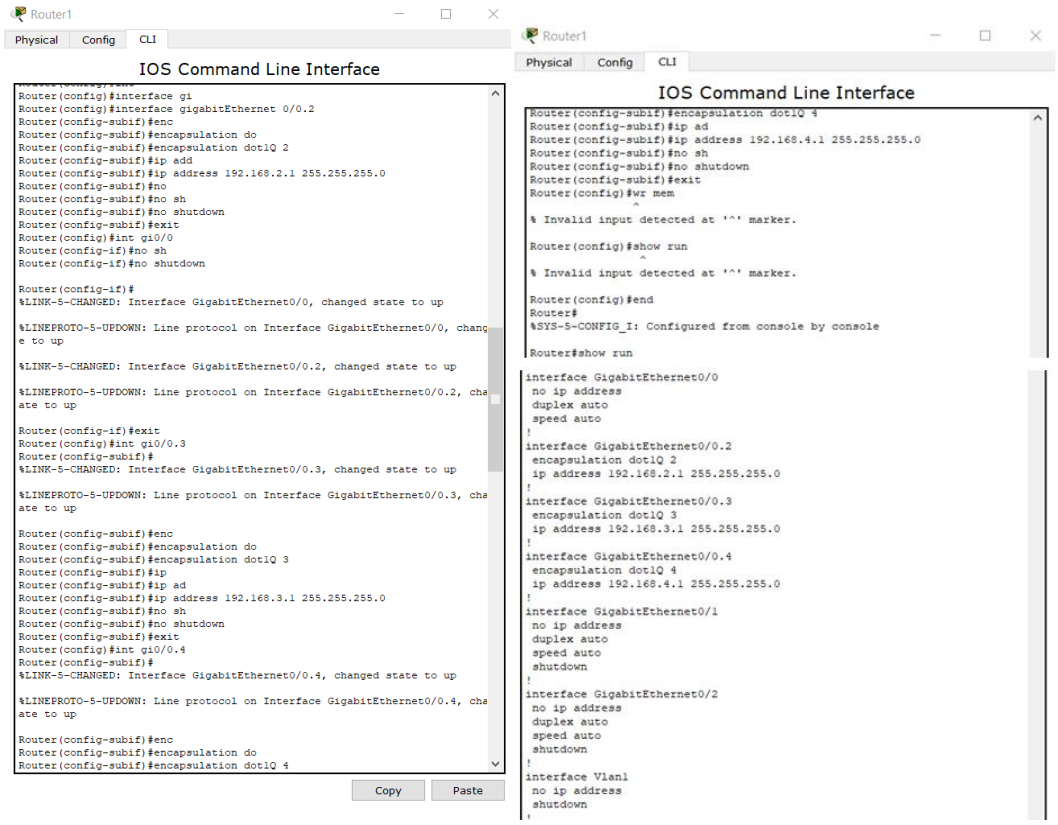


Рисунок 10.6 – Налаштування маршрутизатора та перевірка show run

Проведемо налаштування DHCP сервера. Надаємо статичну IP-адресу 192.168.4.2, маску 255.255.255.0 та шлюз 192.168.4.1 та виконаємо його налаштування. Виконуємо Config-DHCP і у нижньому вікні бачимо, що вже створений один дефолтний сервер pool. Ми його залишаємо і створюємо новий DHCPVLAN2. (рис. 10.7).

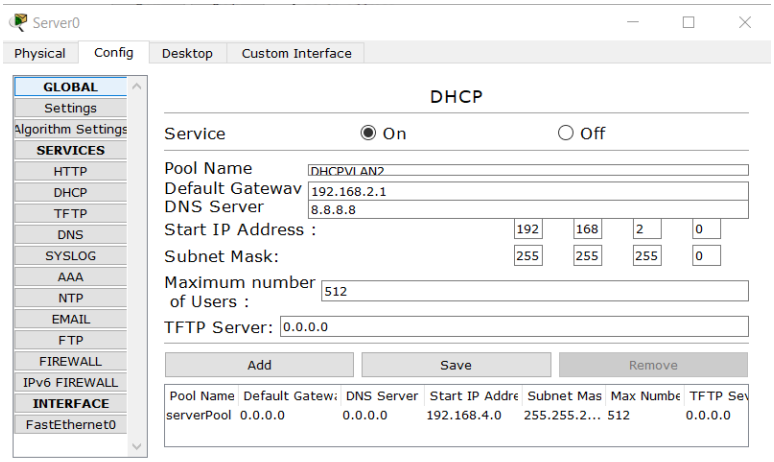


Рисунок 10.7 – Створення DHCPVLAN2

Аналогічно створимо другий пул DHCPVLAN3 (рис. 10.8).

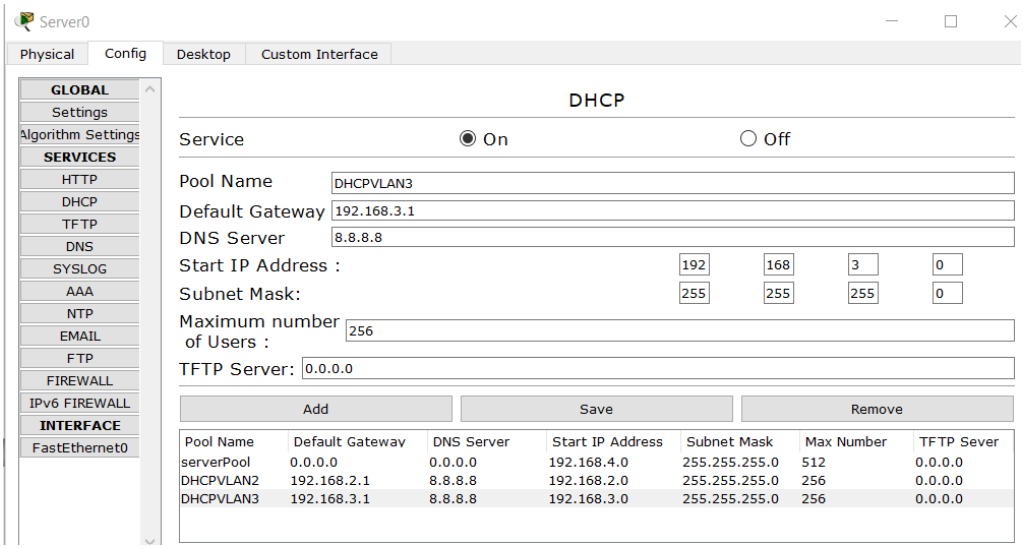


Рисунок 10.8 – Створення DHCPVLAN3

У підсумку ми створили два DHCP-pool, який буде роздавати IP-адреси відповідним сегментам. Далі необхідно переадресувати запити наших комп'ютерів на отримання IP-адрес, оскільки, на відміну від першого прикладу, у якості DHCP серверу в нас виступає Server0, а не маршрутизатор. Тому налаштуємо для кожного sub-інтерфейсу перенаправлення DHCP запитів на існуючий DHCP сервер (рис.10.9).

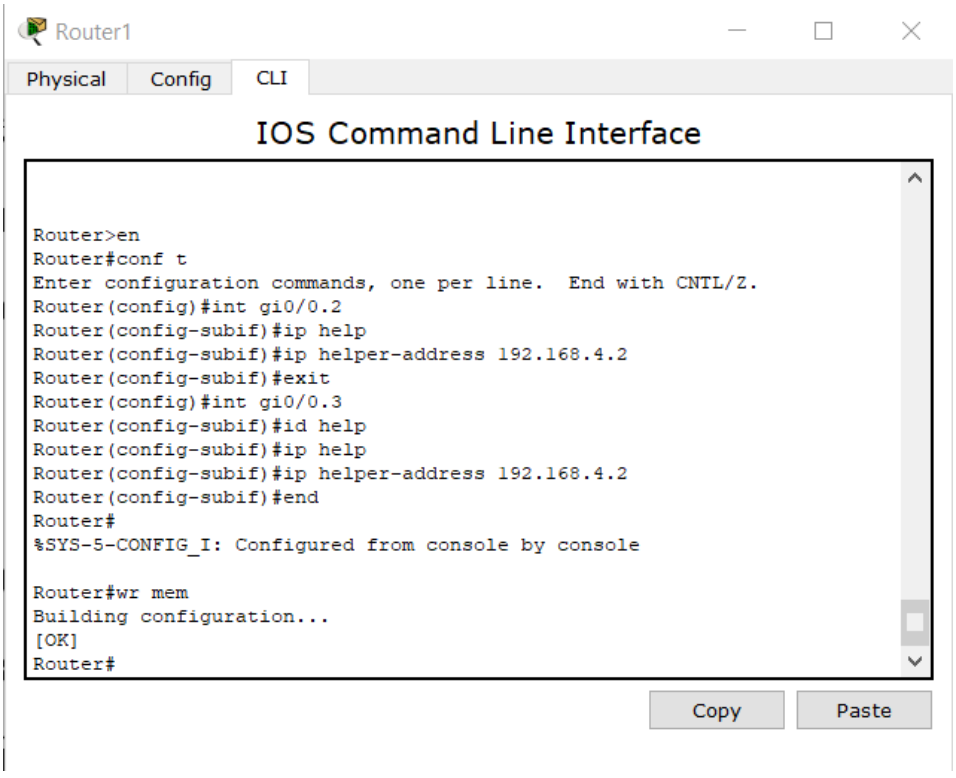


Рисунок 10.9 – Перенаправлення DHCP запитів на існуючий DHCP сервер

На всіх комп’ютерах у налаштуваннях IP-адрес ставимо позначку замість Static, DHCP, і бачимо параметри, які нам видав DHCP сервер. Також перевіряємо взаємодію з, наприклад, PC6 (рис. 10.10).

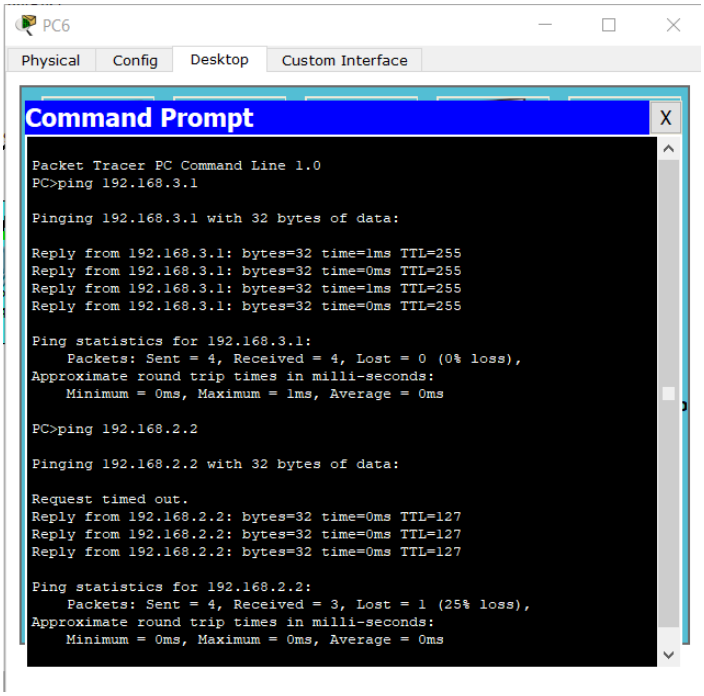


Рисунок 10.10 – Перевірка налаштувань складної мережі

Запитання для самопідготовки

1. Для чого виключається з DHCP pool IP-адреса сервера?
2. Що вам відомо про дефолтний маршрут?
3. Яка відмінність між Static та DHCP при присвоєнні IP-адрес комп’ютерам?
4. Для чого використовують перенаправлення DHCP?
5. Що позначають наведені цифри 255.255.255.0 у масці підмережі?

Практичне заняття №11

ТЕХНОЛОГІЯ «NETWORK ADDRESS TRANSLATION»

Мета заняття – опрацювання технологій виходу до Інтернету з локальних віртуальних мереж.

Біла IP-адреса – це IP-адреса, яка маршрутизується в мережі Інтернет, тобто доступна у будь-якій точці світу (отримуються у Інтернет провайдерів) та сягає приблизно 4,3 мільярди унікальних адрес.

Приватна IP-адреса (сіра IP-адреса) використовується в локальних мережах, може повторюватися але без виходу в Інтернет:

– Мережа класу A – 10.0.0.0 – 10.255.255.255 маска 255.0.0.0 (16 мільйонів адрес);

– Мережа класу B – 172.16.0.0 – 172.31.0.0 с маскою 255.255.0.0 (65 тисяч адрес);

– Мережа класу C – 192.168.0.0 – 192.168.255.255 с маскою 255.255.255.0 (256 адрес).

Ось і постає питання, як комп'ютерам з сірими адресами вийти в Інтернет. Для цього використовується технологія Network Address Translation (NAT).

Існують типи статичний, динамічний та перевантажений (Port Address Translation (PAT), який може перетворювати декілька сірих IP-адрес в один білий – можна підключити цілий офіс, використовуючи лише одну білу IP-адресу).

Однією з переваг NAT також є безпека, оскільки до локальних комп'ютерів відсутній доступ з мережі Інтернет.

Створюємо схему, підключаємо Swich0: fa-0/1 – до роутера, fa-0/2 – до сервера 0, fa-0/3 – до PC0, fa-0/4 – до PC1, fa-0/5 – до PC1.

Задаємо IP-адреси комп'ютерам PC0 – 192.168.2.2, 255.255.255.0, 192.168.2.1, PC1 – 192.168.2.3, 255.255.255.0, 192.168.2.1, PC2 – 192.168.2.4., 255.255.255.0, 192.168.2.1.

Сервери традиційно виділяємо в окремий сегмент. Server0 з параметрами 192.168.3.2., 255.255.255.0, 192.168.3.1

Створюємо сегменти за допомогою VLAN (рис. 11.1).

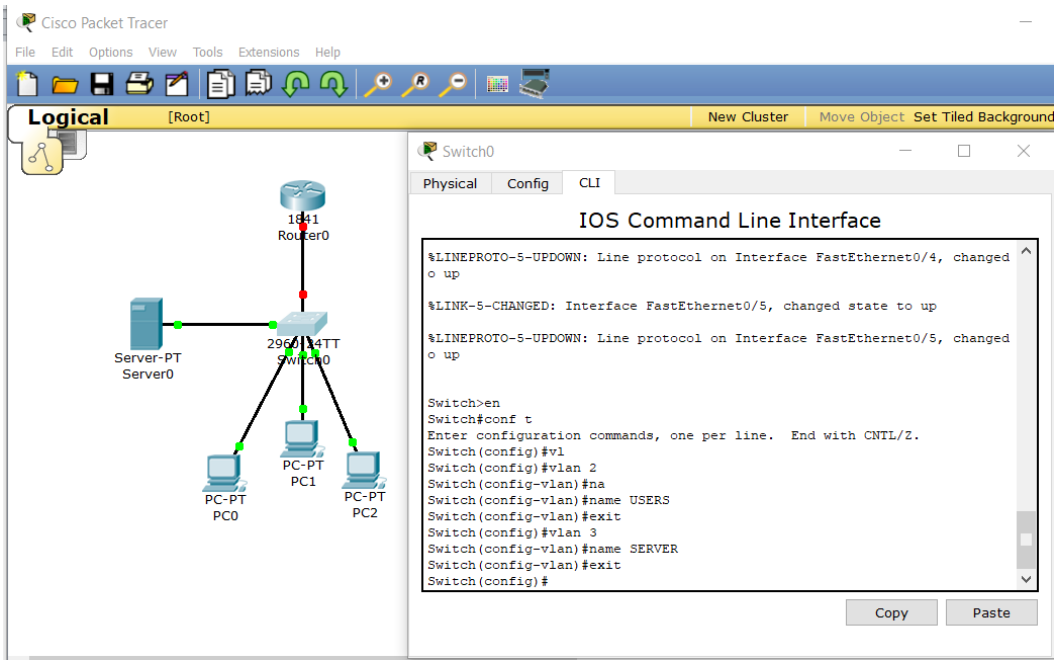


Рисунок 11.1 – Створення тестової мережі

Порт fa0/1 – транковий, fa0/2 – VLAN3, fa0/3, fa0/4, fa0/5 – VLAN2 – проведемо налаштування та перевірку налаштувань (рис. 11.2).

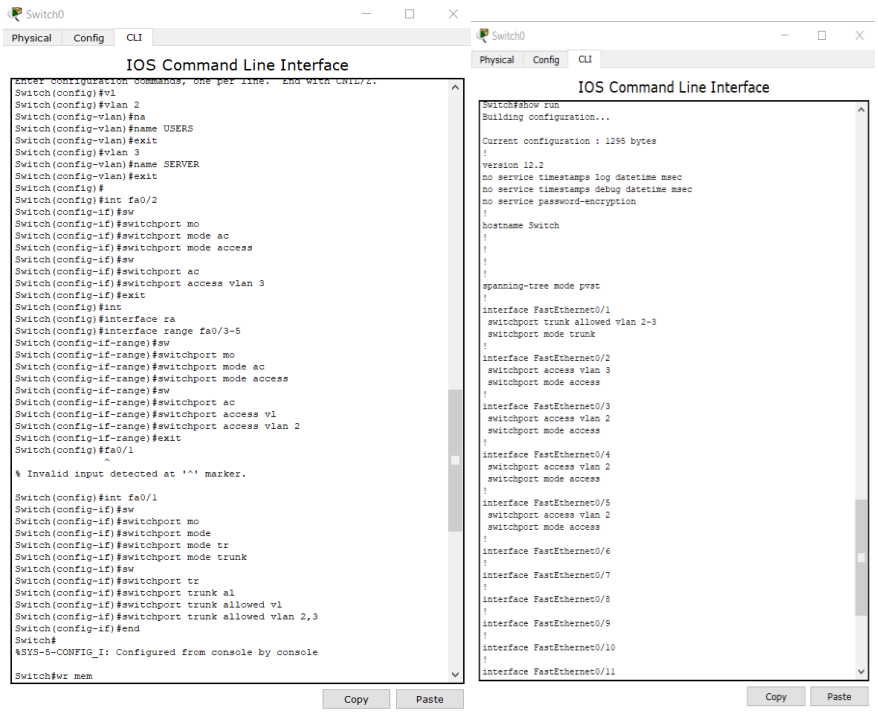


Рисунок 11.2 – Налаштування та перевірка VLAN

Наступним кроком є налаштування роутера з створенням двох сабінтерфейсів (рис. 11.3).

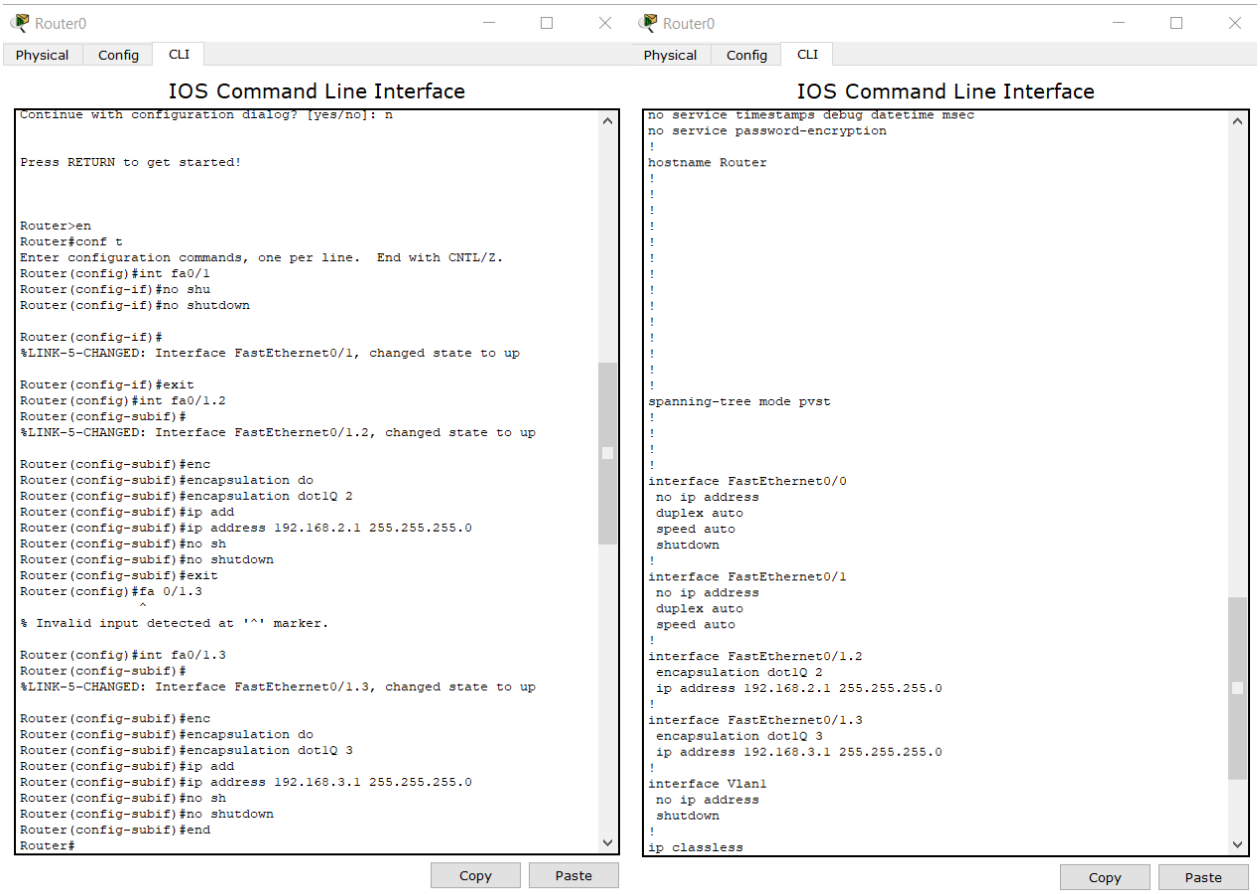


Рисунок 11.3 – Налаштування роутера

Переходимо то тестування зв’язку з PC0 (рис. 11.4).

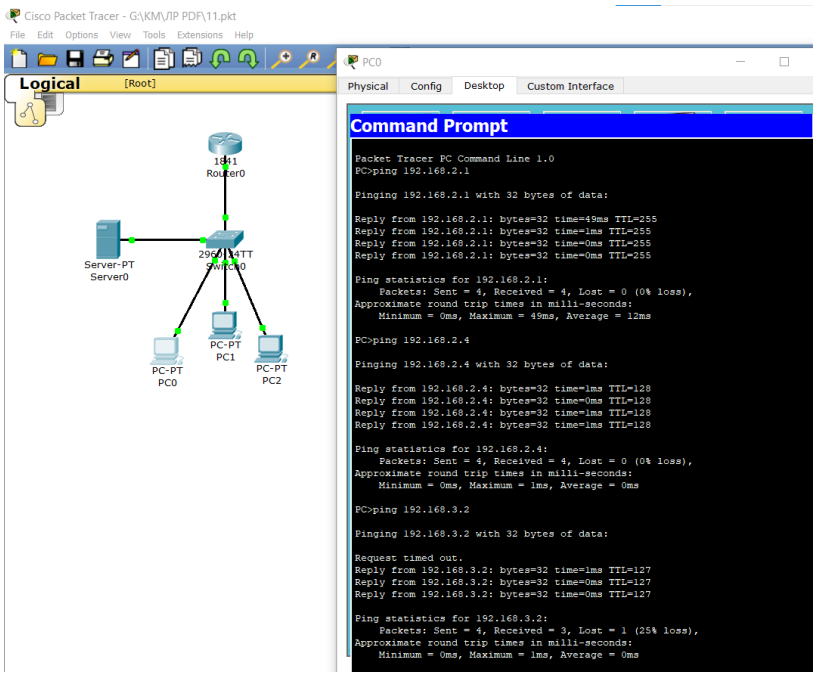


Рисунок 11.4 – Пінгування зв’язку

Таким чином ми налаштували локальну мережу, але тепер нам необхідно підключити її до мережі Інтернет. Після звернення до провайдера, нам виділили

білу IP-адресу, наприклад, статичну. Далі емулюємо вихід в Інтернет засобами роутера та сервера. Припустимо, що на роутері 1 провайдера на fa0/0, провайдер присвоїв адресу з білого діапазону 213.234.10.1 і 30-и бітну маску 255.255.255.252. На fa0/1 знаходиться деякий сервер з білою IP-адресою (рис. 11.5).

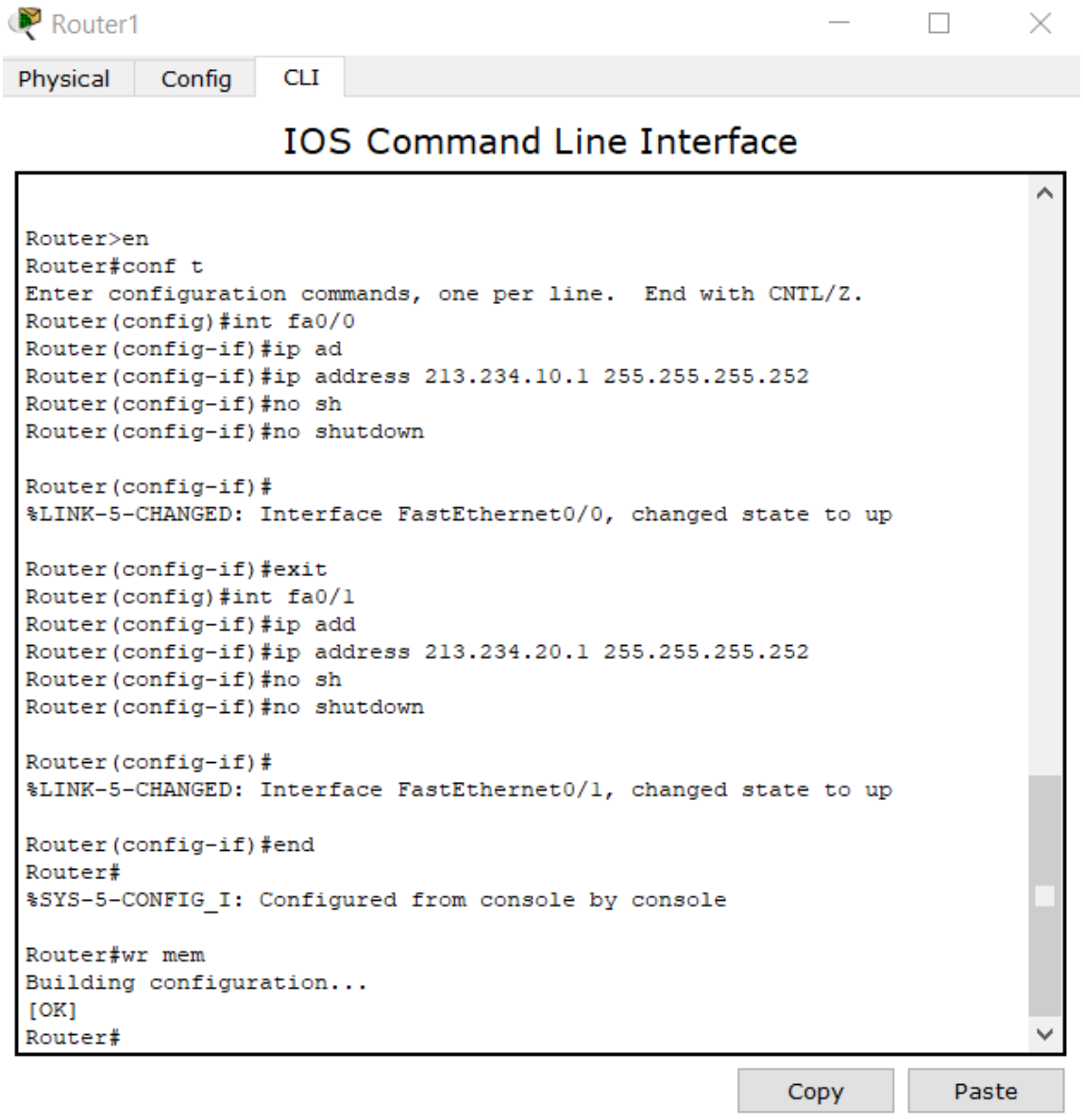


Рисунок 11.5 – Налаштування роутера 1

Далі проводимо налаштування сервера: IP-адреса 213.234.20.2, маска 255.255.255.252 і шлюз роутера 213.234.20.1

На роутері 0 прописуємо білу IP-адресу, яку надав нам провайдер 213.234.10.2 (рис. 11.6).

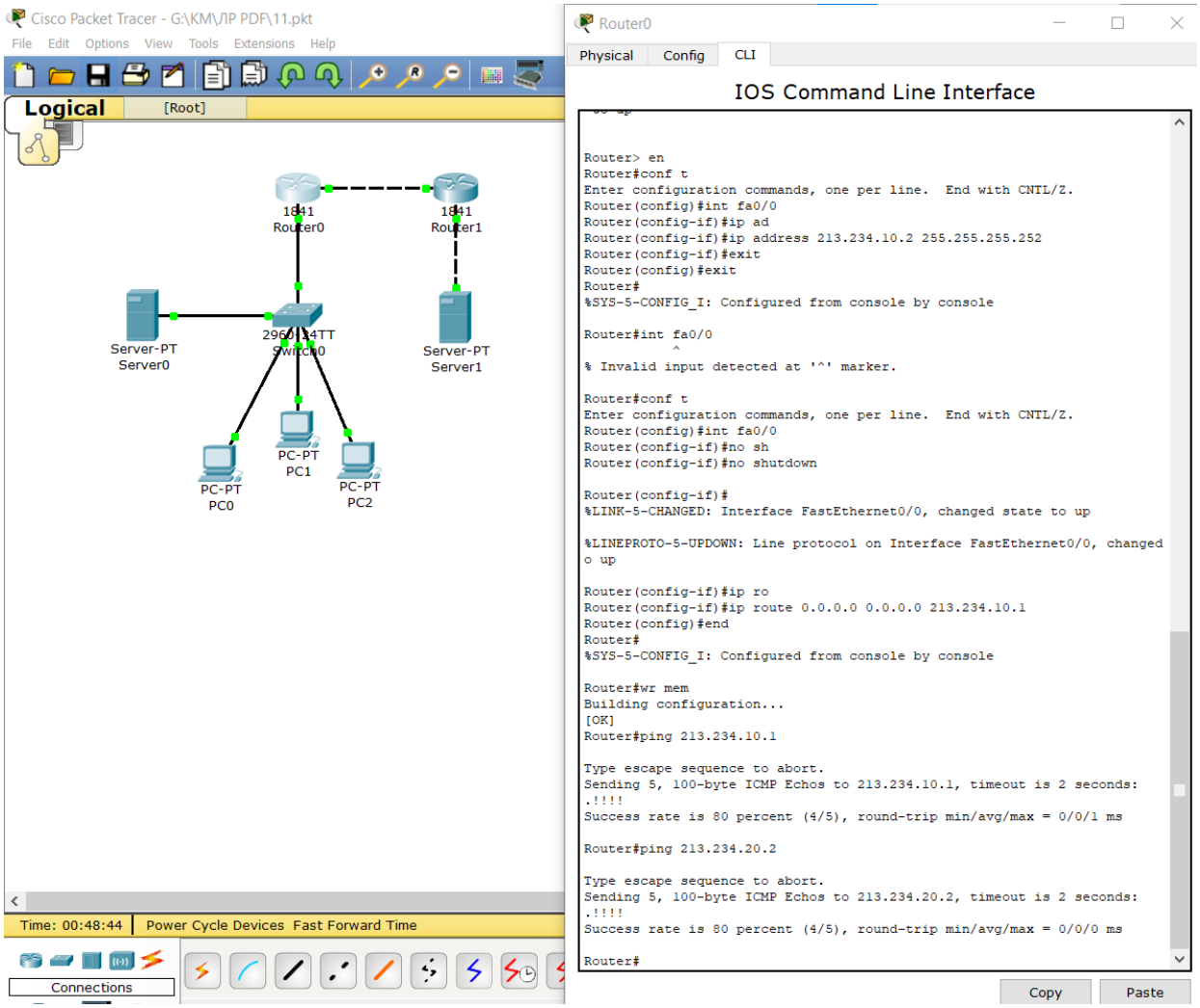


Рисунок 11.6 – Налаштування роутера 0

Наприкінці, як бачимо на рисунку 11.6, перевіряємо пінгування на Інтернет та сервер 1, зв’язок встановлено.

Зазначимо, що якщо ми перевіримо зв’язок з PC0 на сервер 1, то зв’язку не буде.

Це пов’язано з тим, що в локальній мережі використовуються сірі адреси, і маршрутизатор 1, в нашому прикладі, просто не знає про нашу мережу.

Як раз на цьому етапі нам і знадобиться технологія NAT. Визначимо, який інтерфейс буде внутрішнім, який зовнішнім.

Налаштуємо NAT (рис. 11.7).

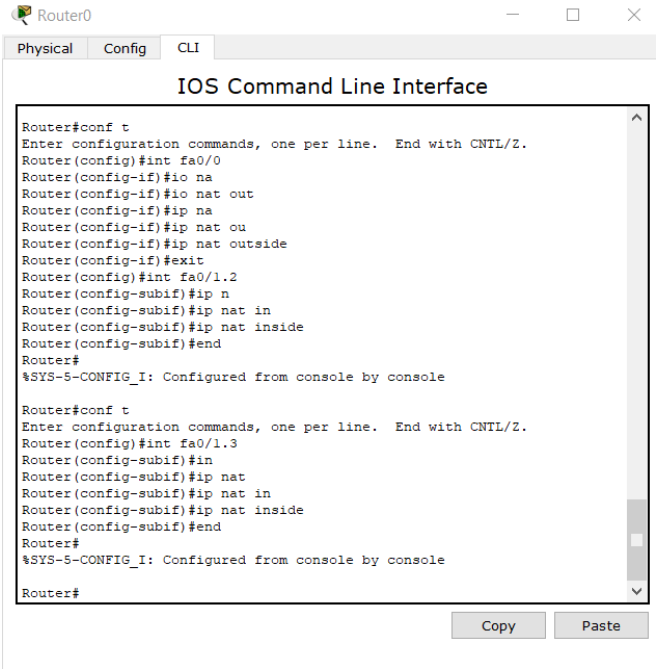


Рисунок 11.7 – Реалізація NAT

Далі створюємо access-list, тобто який трафік ми повинні натити. Наприклад, налаштування permit 192.168.2.0 0.0.0.255 говорить про те, що натити потрібно мережу 2.0 (рис.11.8).

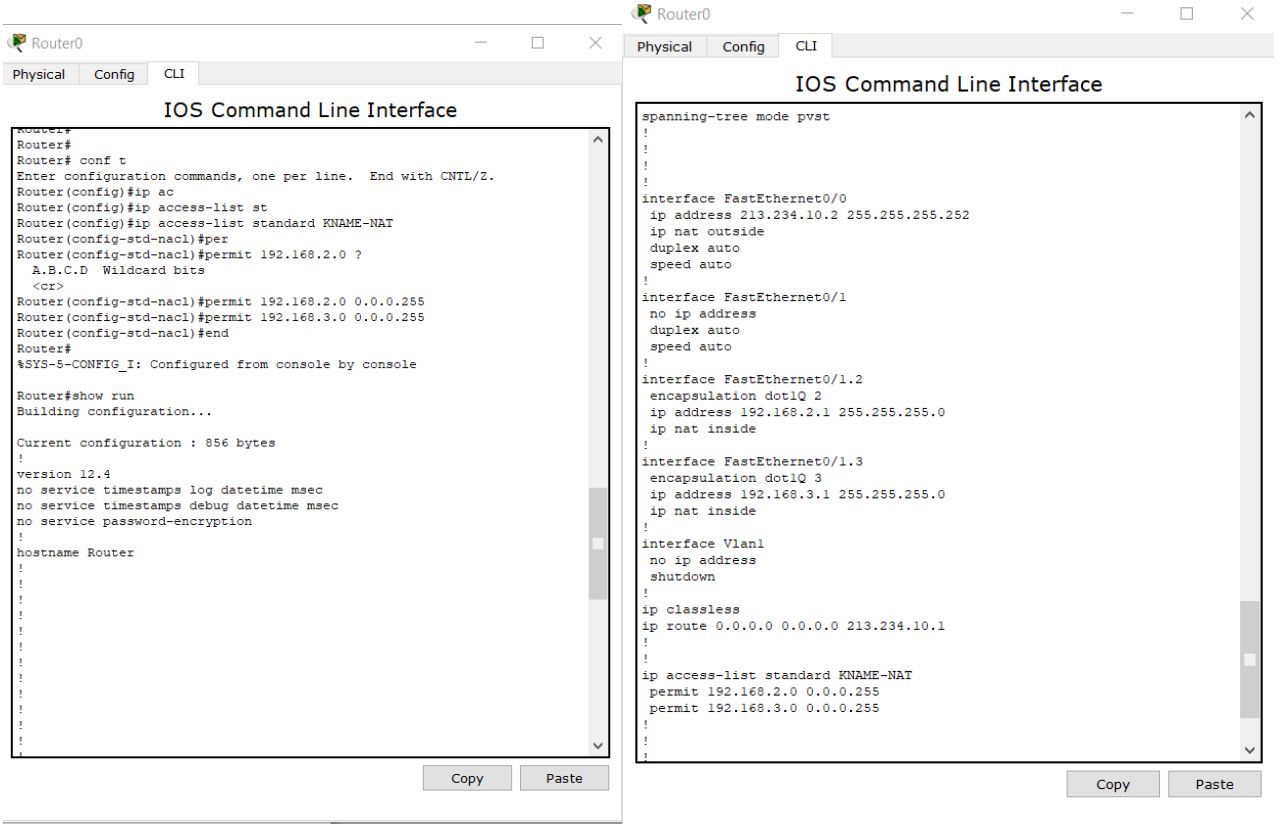


Рисунок 11.8 – Створення access-list

Налаштовуємо PAT (рис. 11.9).

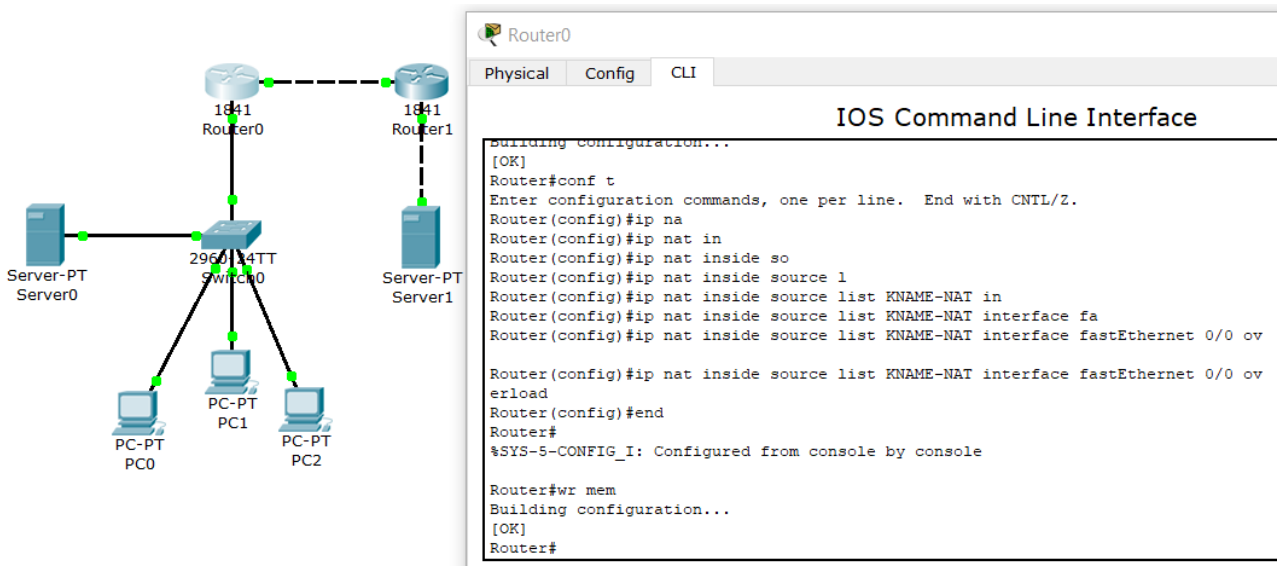


Рисунок 11.9 – Налаштування PAT

Після введення налаштувань спробуємо пінг з PC0 на сервер 1, зв'язок є. Далі у режимі симуляції запускаємо пакет по даному маршруту. Аналогічно робимо по зворотному маршруту.

Далі налаштуємо статичний NAT, тобто забезпечимо доступ до локального вебсервера 0 з зовнішньої мережі.

Переходимо в налаштування сервер 0 (рис. 11.10).

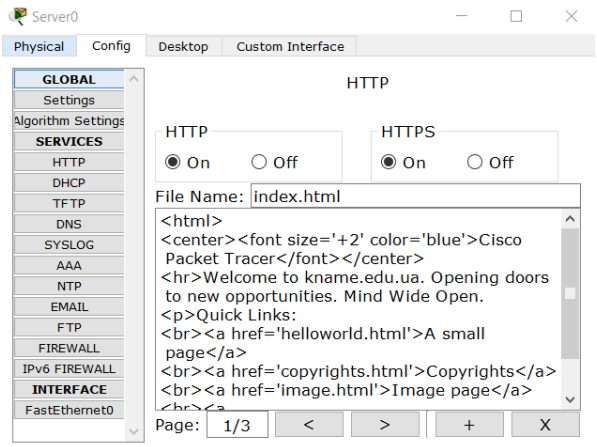


Рисунок 11.10 - Налаштування Hyper text transfer protocol (HTTP) локального сервера 0

Далі необхідно транслятувати звернення на нашу зовнішню адресу на порт 80 (на який буде транслюватися запит) і це звернення буде транслюватися на локальний сервер (рис. 11.11).

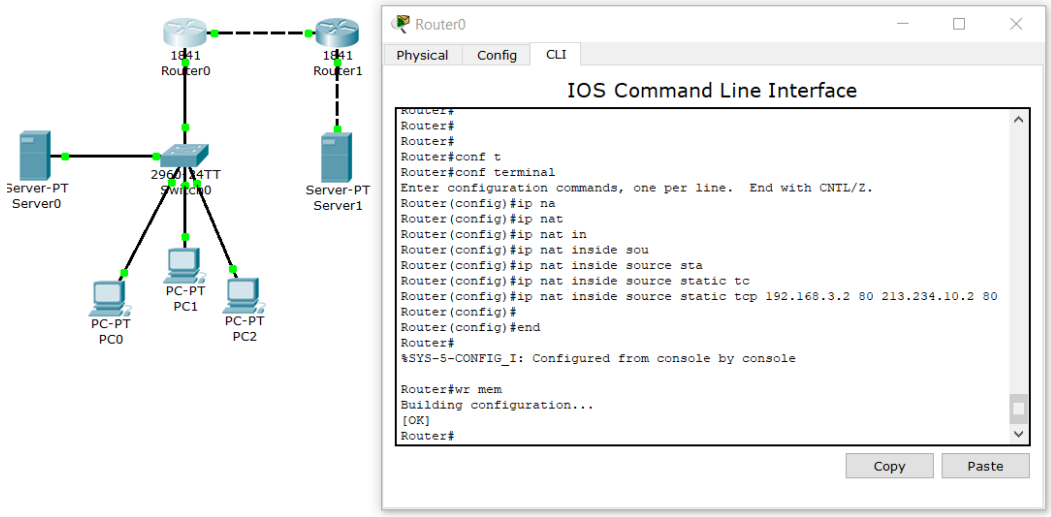


Рисунок 11.11 – Налаштування порту доступу

Заходимо на сервер 1 у браузер та спробуємо зайти на сервер 0, який має сіру адресу (рис. 11.12).

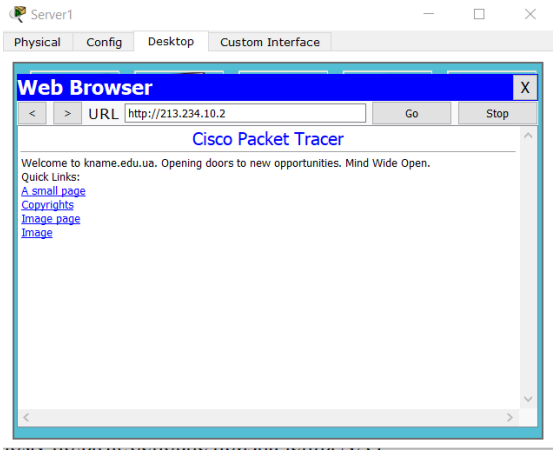


Рисунок 11.12 – реалізація static NAT

Ми бачимо при цьому сторінку нашого локального сервера 0, який не має білої IP-адреси, реалізувавши статичний NAT.

Запитання для самопідготовки

1. В чому полягає основне призначення NAT?
2. Які класи мереж вам відомі?
3. Що вам відомо про PAT?
4. Наведіть перелік помилок та некоректності вводу коду на рисунку 11.7.
5. Що значить транслювати запит?
6. Що вам відомо про static NAT?

Практичне заняття №12

ПРОТОКОЛ «OPEN SHORTEST PATH FIRST»

Мета заняття – опанувати прийоми роботи з автоматичним розподілом маршрутів.

У лабораторній роботі номер дев'ять розглядалася статична маршрутизацію, де прописували маршрути вручну на кожному з роутерів. Змоделюємо ситуацію коли 20 роутерів та декілька десятків мереж. При цьому прописати всі маршрути буде нескладно, але це займе дуже багато часу. При зміні топології також доведеться переписувати всі маршрути.

Динамічна маршрутизація є вирішенням даної проблеми – всі маршрути автоматично додаються на роутер та забезпечується організація відмовостійкості на з рівні моделі OSI.

Але є й недоліки, а саме більш висока завантаженість обчислювальних ресурсів, вимоги до високої кваліфікації при пошуку проблеми та мережа в цілому менш передбачувана.

Автоматичний розподіл маршрутів здійснюється за допомогою протоколів динамічної маршрутизації, які поділяються на зовнішні (Exterior Gateway Protocol (EGP, BGP) та внутрішні (Interior Gateway Protocol (RIP, OSPF, EIGRP, IGRP, IS-IS), які здійснюють динамічну маршрутизацію між автономними системами (AS) або доменами маршрутизації (група роутерів під загальним керуванням). AS обмінюються маршрутами, наприклад, мережа провайдера. У провайдера в наявності пул білих адрес, і окрім IP-адрес провайдеру продають номер автономної системи, який є унікальним. Як раз за допомогою номера AS та, наприклад, протоколу BGP здійснюється обмін інформацією з зовнішнім світом, тобто з іншими автономними системам.

Існують дистанційно векторні протоколи – Distance vector (RIP, EIGRP,IGRP) та протоколи станів каналів Link state (OSPF, IS-IS)

Розглянемо, наприклад, протокол Open shortest path first (OSPF).

Для початку, побудуємо дві мережі (рис. 12.1). У першому прикладі використовується три роутера та три мережі. Можна скачати файл TEST12.pkt

до практичного заняття та провести покрокове налаштування відповідно до завдання (перевіряти налаштування за допомогою show run).

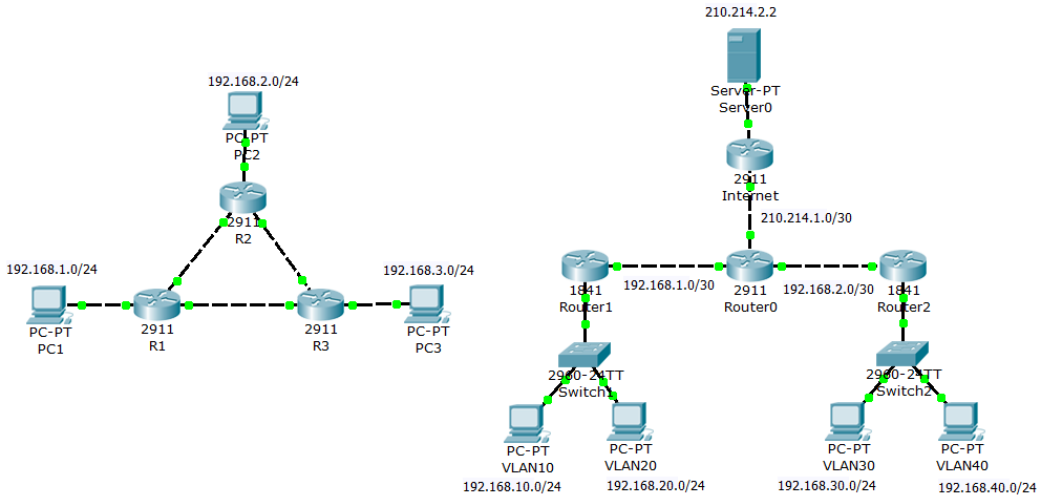


Рисунок 12.1 – Створення двох схем з файлу TEST12.pkt

Далі необхідно без статичного прописання маршрутів на роутерах зробити таким чином, щоб на комп'ютерах буди доступні всі IP-адреси.

Зауважимо, що перед налаштуванням динамічної маршрутизації необхідно налаштувати адресу на Loopback-інтерфейсі (логічний інтерфейс, який не прив'язаний до жодних інтерфейсів). При запуску самого процесу генерується роутер-id, і за замовчуванням він бере найбільшу адресу Loopback інтерфейсу і якщо його немає, бере найбільшу адресу на фізичному інтерфейсі, використовувати IP-адресу роутера на фізичному інтерфейсі не коректно.

Тому виконаємо налаштування роутерів 1,2,3 (рис. 12.2).

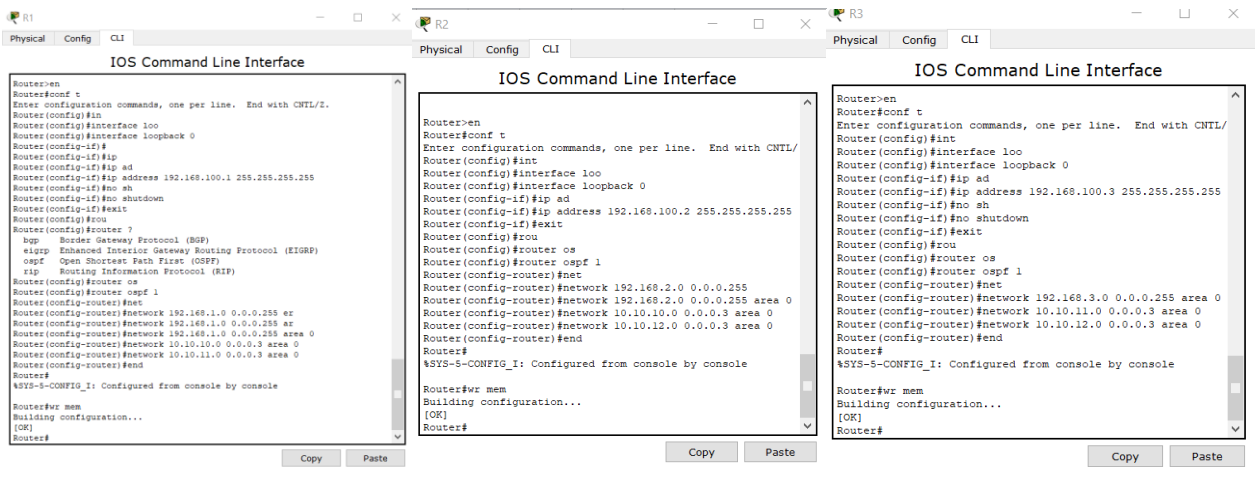


Рисунок 12.2 – Налаштування роутерів 1,2,3

Далі проводимо перевірку, як роутер 3 знайшов сусідні два роутери (рис. 12.3).

```
Router#sh
Router#show ip os
Router#show ip ospf nei
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.100.2     1   FULL/BDR        00:00:30    10.10.12.1      GigabitEtherne
t0/0
192.168.100.1     1   FULL/BDR        00:00:30    10.10.11.1      GigabitEtherne
t0/1
Router#
```

Рисунок 12.3 – Перевірка роутера 3 на пошук сусідніх роутерів

Також на рисунку 12.3 можна ознайомитися з адресами та інтерфейсами, звідки приходить пакет.

Далі перейдемо до розгляду таблиці маршрутизації на прикладі роутера 3 (рис. 12.4).

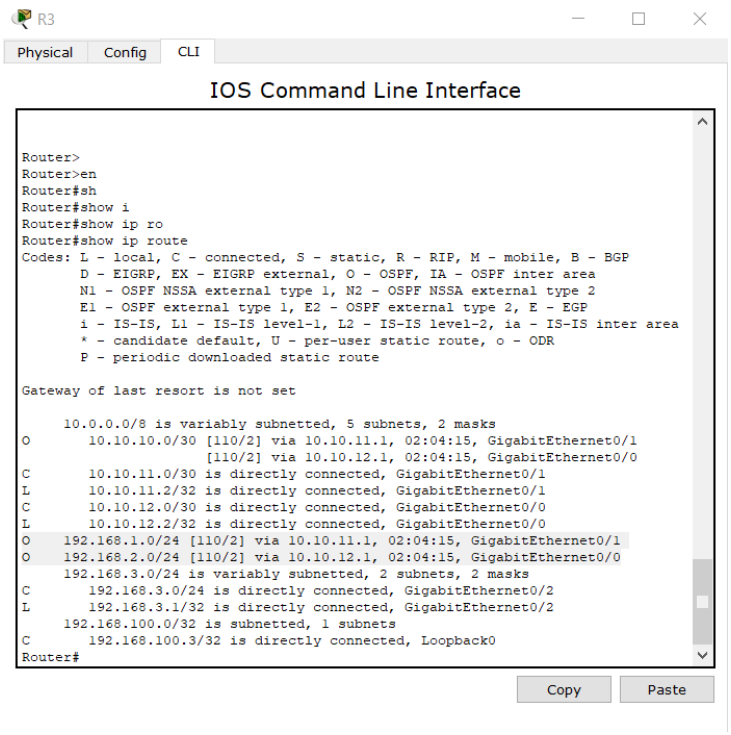


Рисунок 12.3 – Таблиця маршрутизації на прикладі роутера 3

Виділені на рисунку записи, що помічені «О», позначають, що дані маршрути прописалися автоматично за допомогою протоколу OSPF.

Далі проводимо перевірку налаштувань та пінгування, наприклад з роутера 3 на комп’ютер PC1 (рис. 12.4).

```
Router#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Рисунок 12.4 – Пінгування маршрутів

Перевіряємо відмовостійкість. Гасимо лінк на роутері 1 та з роутера 3 перевіримо таблицю маршрутизації і побачимо що пінг йде тільки через «O» 192.168.1.0/24 [110/3] via 10.10.12.1, 00:01:54, GigabitEthernet0/0 на відміну від рис.12.3. Результат наведено на рисунку 12.5.

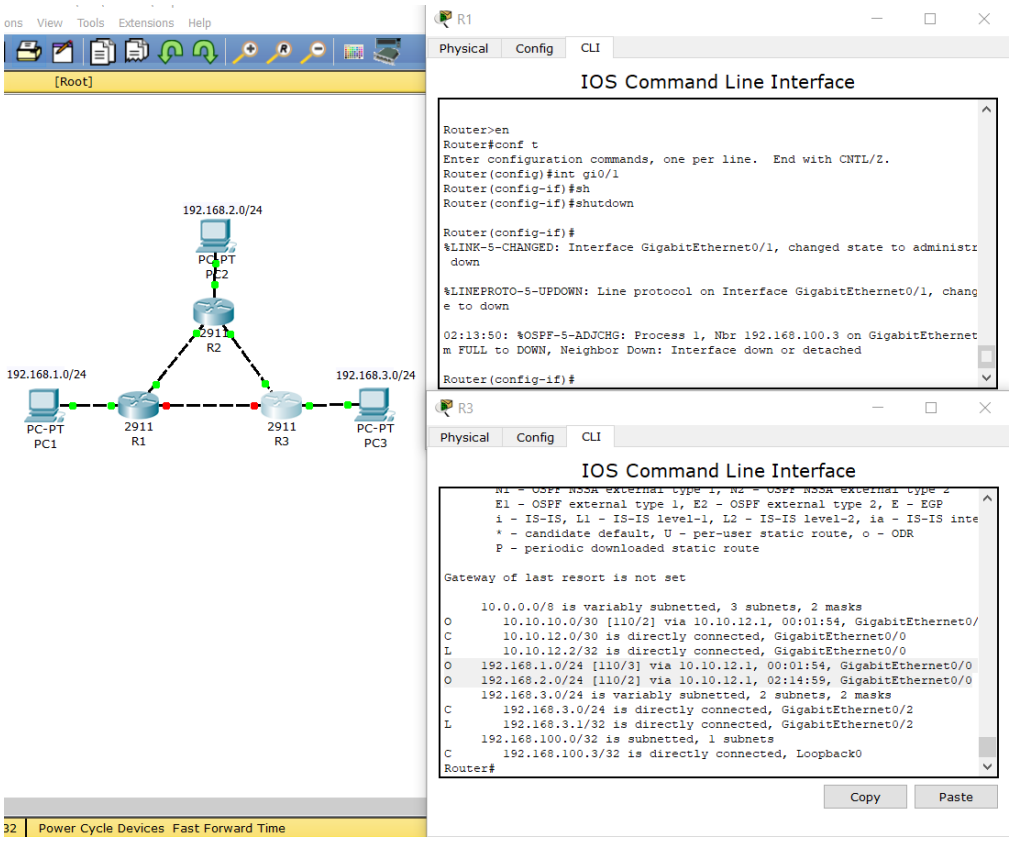


Рисунок 12.5 – Тестування відмовостійкості

Таким чином в тестовому завданні автоматично перебудувався маршрут і зв’язок відновився.

Далі перейдемо до схеми 2, біль наближеної до реальних схем. Маємо два будинки та центральний вузол зв’язку Router0, який забезпечує нам доступ до Інтернету. При цьому кожен маршрутизатор має по два сегменти (VLAN10 та 20; VLAN30 та VLAN40).

Необхідно налаштувати OSPF таким чином, щоб наші сегменти бачили один одного та могли надсилати пакети. Налаштовуємо Router1 (рис. 12.6).

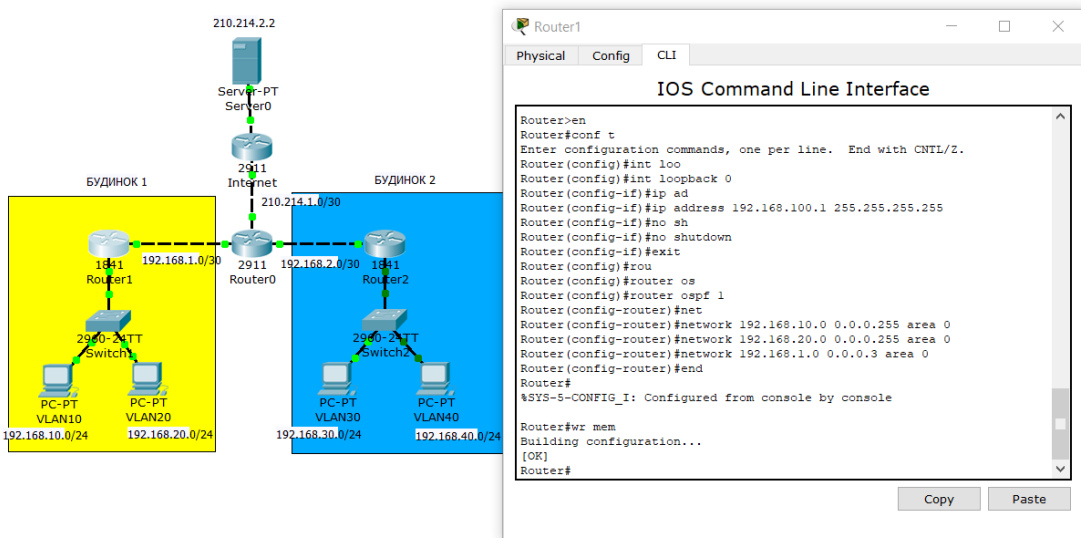


Рисунок 12.6 – Налаштування Router1

Налаштовуємо Router2 (рис. 12.7). Наприклад запис *Router(config-router)#network 192.168.30.0 0.0.0.255 area 0* називається анонсуванням мережі, тобто ми дозволяємо маршрутизатору розсилати оновлення з приводу даної мережі, те, що вона присутня.

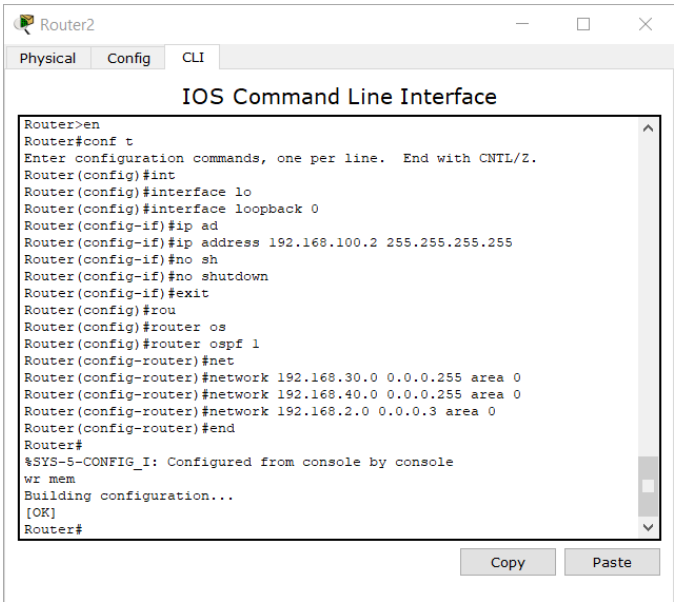


Рисунок 12.7 – Налаштування Router2

На даний момент проведено всі налаштування на роутерах обох віртуальних будинків. Далі проводимо налаштування центрального маршрутизатора (рис. 12.8).

Зауважимо, що на даному маршрутизаторі один з інтерфейсів взаємодіє з пристроєм з білою IP-адресою, тому на даному пристрої налаштовувати OSPF

не рекомендується, оскільки реальний провайдер наші пакети динамічної маршрутизації з OSPF приймати не буде. Анонсуємо лише мережі 1.0 та 2.0.

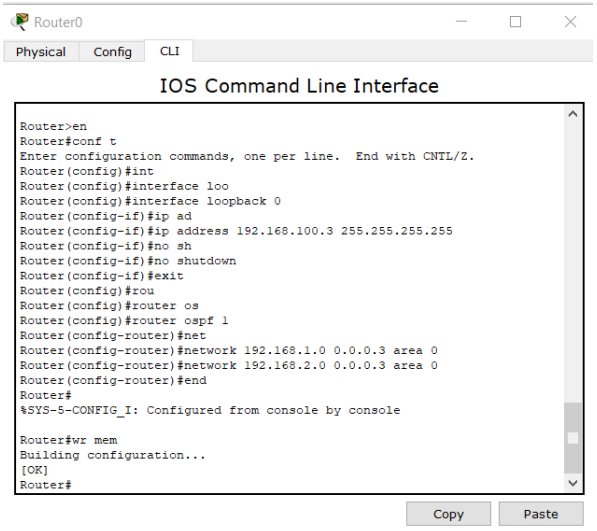


Рисунок 12.8 – Налаштування центрального маршрутизатора

Виконаємо команду *Router#show ip ospf neighbor*, та подивимось таблицю маршрутизації (рис. 12.9).

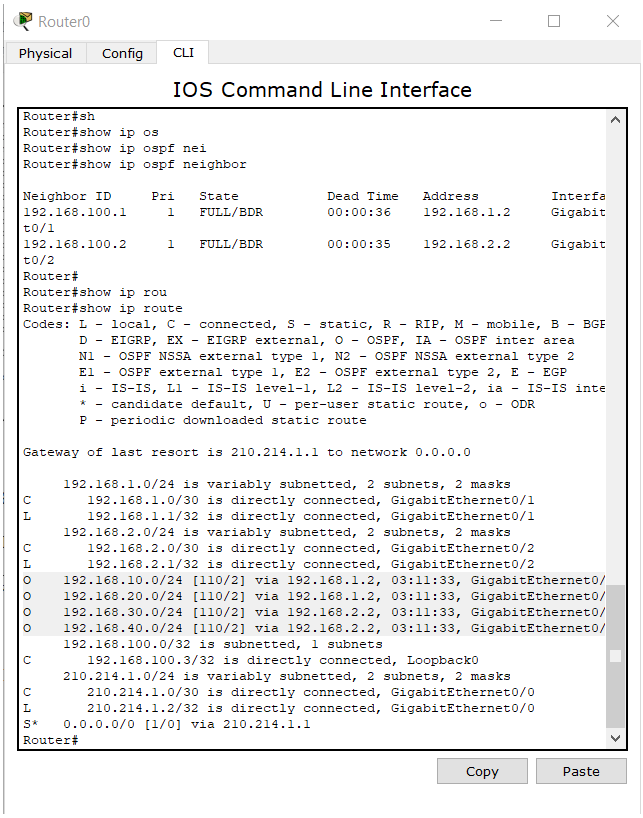


Рисунок 12.9 – Таблиця маршрутизації центрального маршрутизатора

Далі тестуємо пінгування, наприклад, з комп’ютера VLAN30 на VLAN10, інші комбінації, бачимо що зв’язок встановлено.

Також у зв’язку з тим, що ми додали маршрути лише локальних мереж, нам необхідно налагодити вихід в Інтернет. Пропишемо default gateway на Router0 (рис. 12.10).

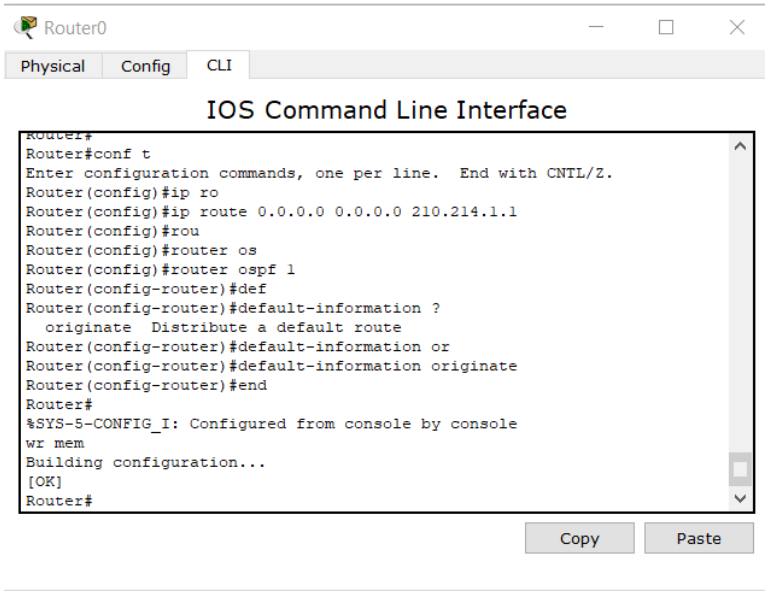


Рисунок 12.10 – Налаштування default gateway на Router0

Далі на роутері 1 перевіримо таблицю маршрутизації (рис. 12.11).

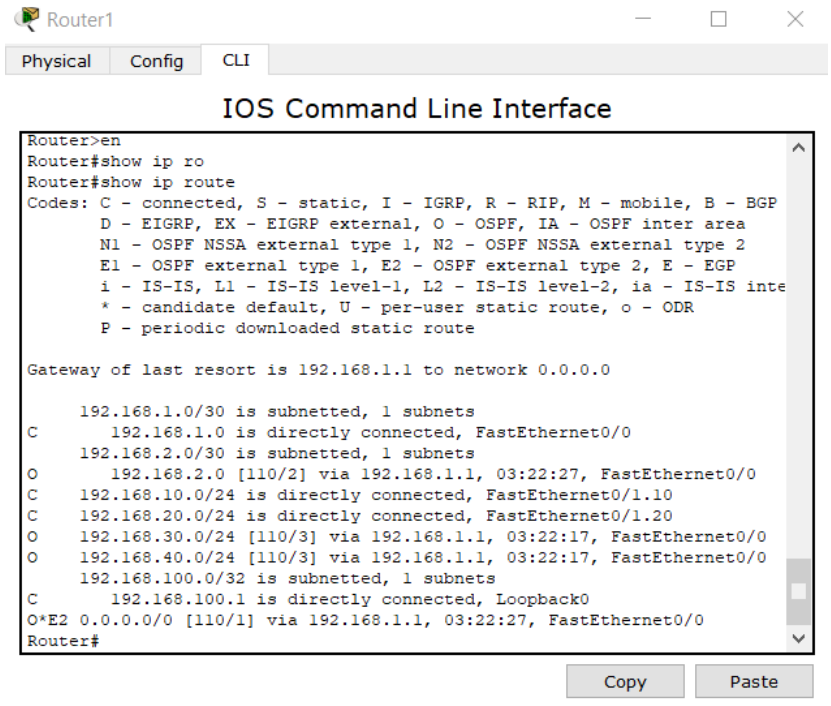


Рисунок 12.11 - Перевірка таблиці маршрутизації на роутері 1

Як бачимо, отримано дефолтний маршрут O*E2 0.0.0.0/0 [110/1] via 192.168.1.1, 03:22:27, FastEthernet0/0.

Далі використовуємо NAT на центральному маршрутизаторі. Визначаємо, що інтерфейс gi0/0 – це зовнішній інтерфейс, оскільки на ньому біла IP-адреса. На інтерфейсі gi0/1,2 – це внутрішній інтерфейс (напрямок на внутрішню мережу). Далі в access-list перераховуємо мережі, яким необхідний доступ в Інтернет (рис. 12.12).

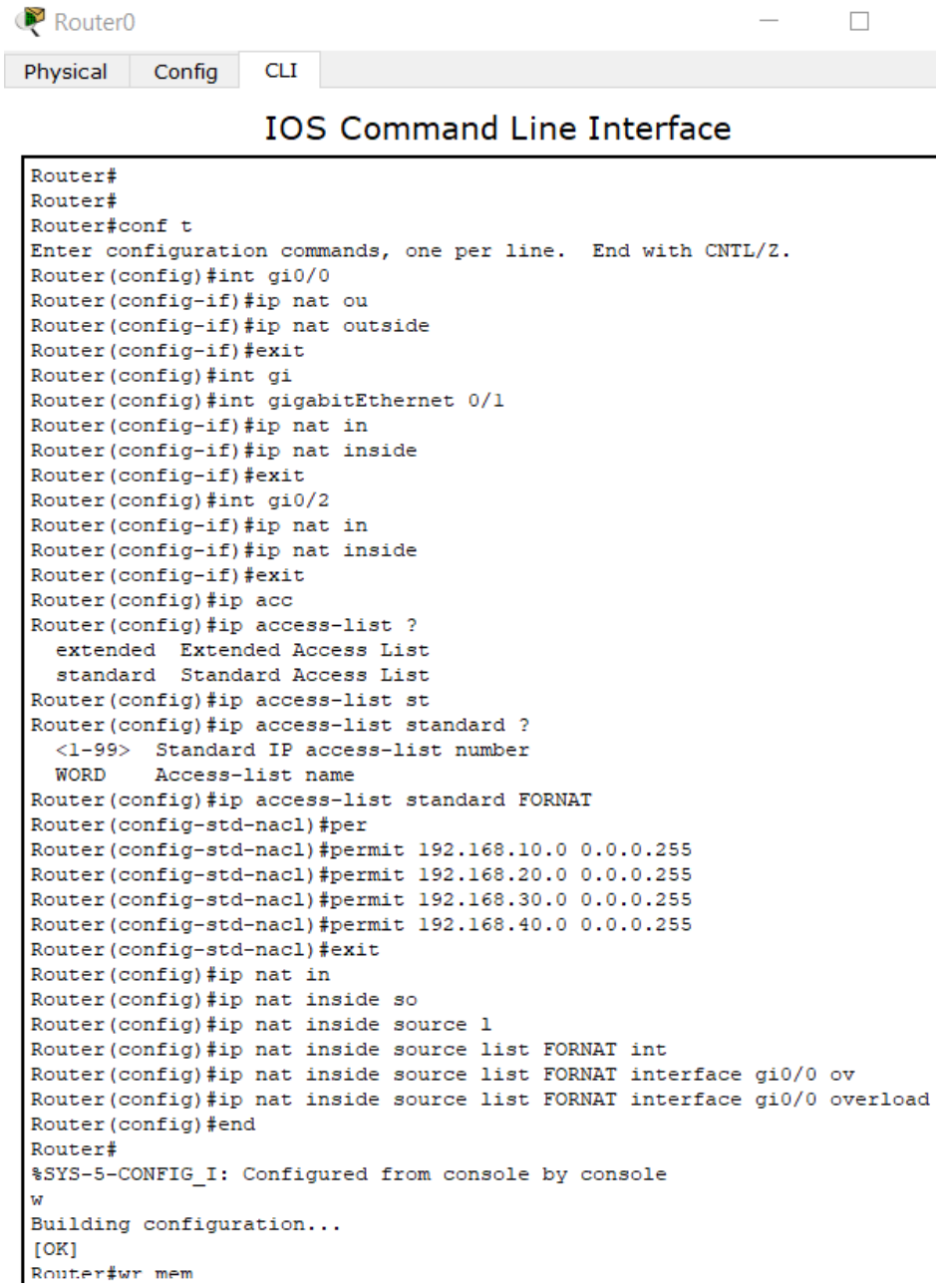


Рисунок 12.12 – Реалізація NAT

При правильному налаштуванні роутер 1 та роутер 2 мають шлюз за замовчуванням, отриманий по OSPF і на центральному маршрутизаторі в нас

налаштований NAT. Спробуємо з комп’ютера пінгувати мережу Інтернет (рис. 12.13).

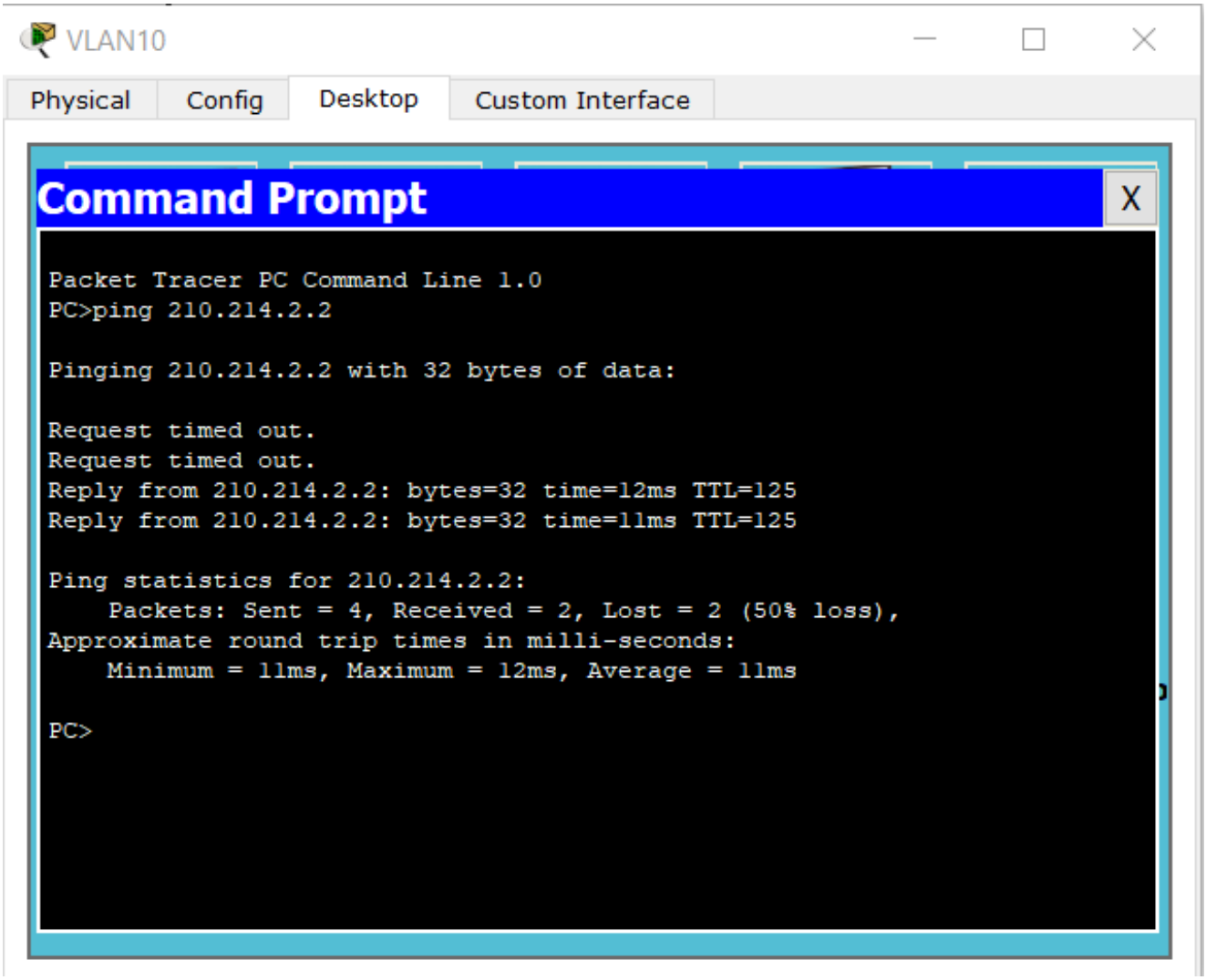


Рисунок 12.13 – Підсумок налаштування динамічної маршрутизації, при якій розповсюдили дефолтний маршрут за замовчуванням та на центральному роутері налаштовували NAT і здійснили доступ до мережі Інтернет.

Запитання для самопідготовки

1. Що вам відомо про Loopback – інтерфейс?
2. Що вам відомо про wildcard маску?
3. Як визначити по таблиці маршрутизації реалізацію протоколу OSPF?
4. Наведіть основні рекомендації використання OSPF з пристроями з білими IP-адресами.

Практичне заняття №13

ПРОТОКОЛ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ

«ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL»

Мета заняття – ознайомитися з протоколом динамічної маршрутизації.

Enhanced interior gateway routing protocol (EIGRP), у продовженні теоретичного матеріалу практичного заняття №12, є дистанційно – векторним протоколом. При його використанні маршрутизатори поділяються протоколами маршрутизації (знає лише сусідні маршрутизатори), тобто роутери, які підключені напряму. Відповідно завантаження центрального процесора та пам'яті значно нижча ніж у OSPF.

EIGRP більш легкий у налаштуваннях, оскільки відсутні області (в OSPF налаштовували area), підходе для малих та середніх мереж. Але недолік в тому, що працює лише на обладнанні Cisco.

Також з тестового файлу TEST12.pkt скористаємося схемою 1. За допомогою show run ознайомлюємося з налаштуваннями, покроково виконуємо в рамках даної лабораторної роботи. Зауважимо, що застосовується опція, що вимикає додавання маршрутів (no auto summary).

Налаштуємо роутер 1 (рис. 13.1).

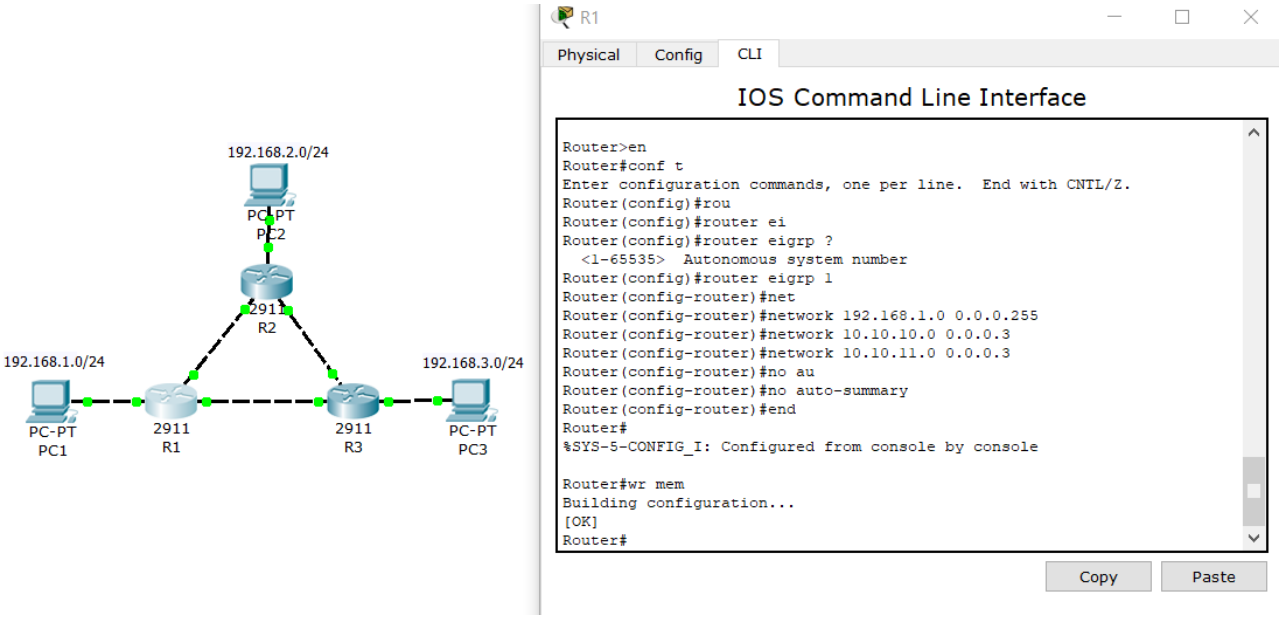


Рисунок 13.1 – Налаштування 1 роутера

Проводимо налаштування роутерів 2 та 3 (рис. 13.2).

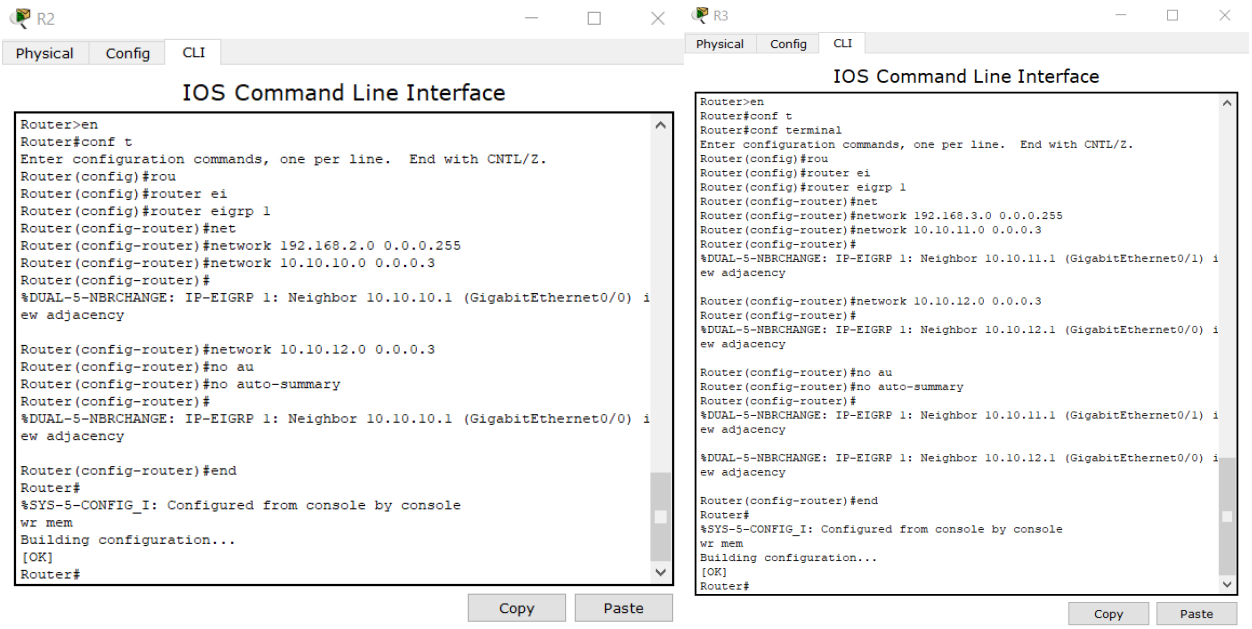


Рисунок 13.2 – Налаштування роутерів 2 та 3

Перевіряємо таблицю маршрутизації (рис. 13.3).

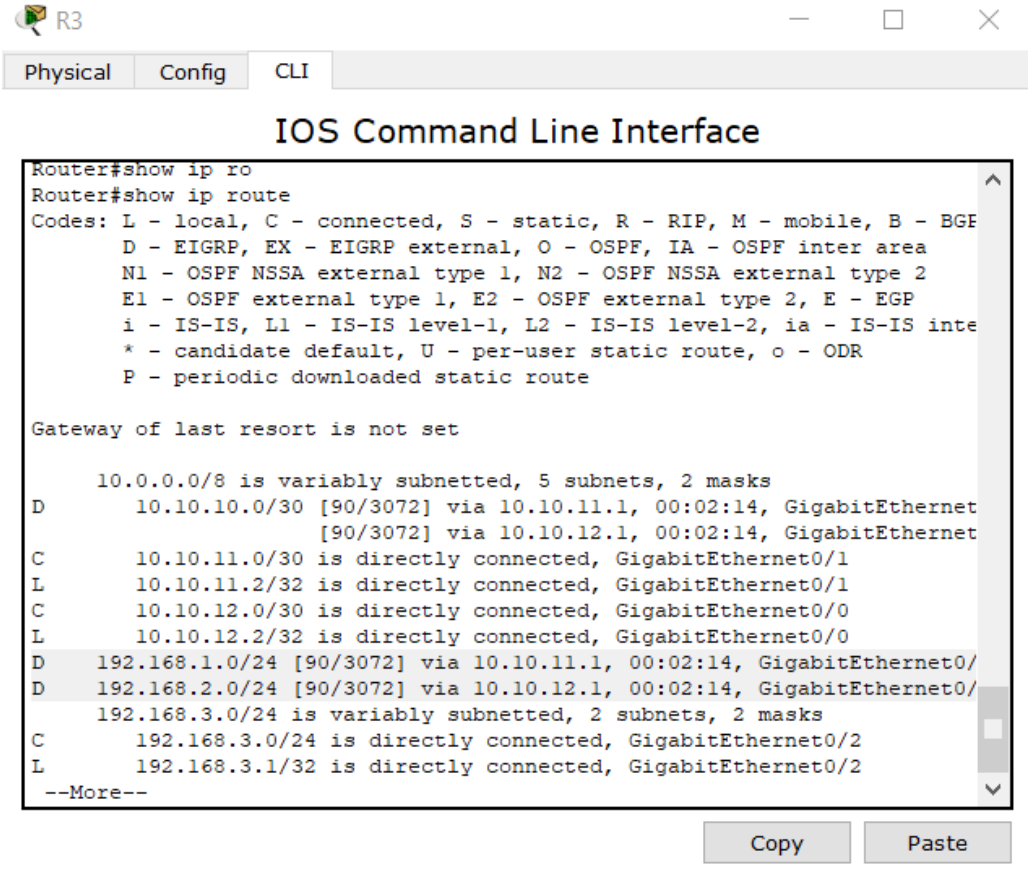


Рисунок 13.3 – Перевірка таблиці маршрутизації

Пропінгуємо з PC3 на PC2, зв’язок встановлено (рис. 13.4).

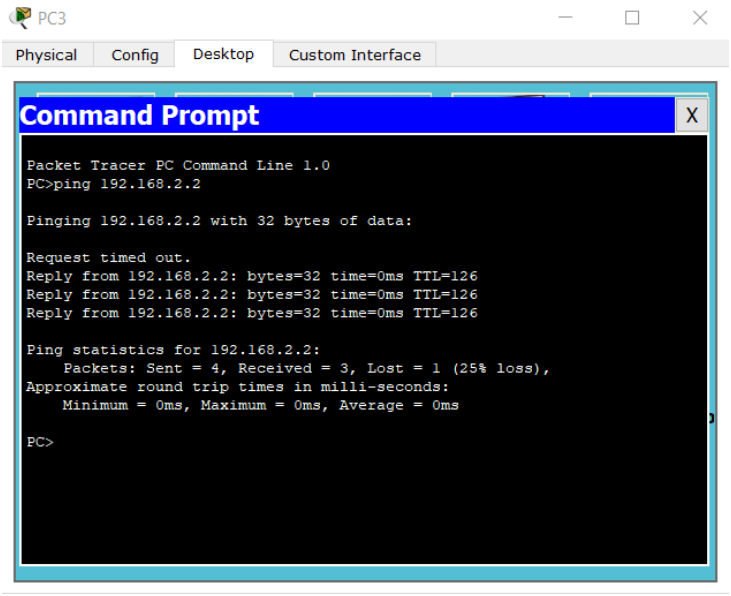


Рисунок 13.4 – Пінгування з PC3 на PC2

На PC3 запускаємо пінгування *PC>ping 192.168.2.2 -n 2000* (рис. 13.5).

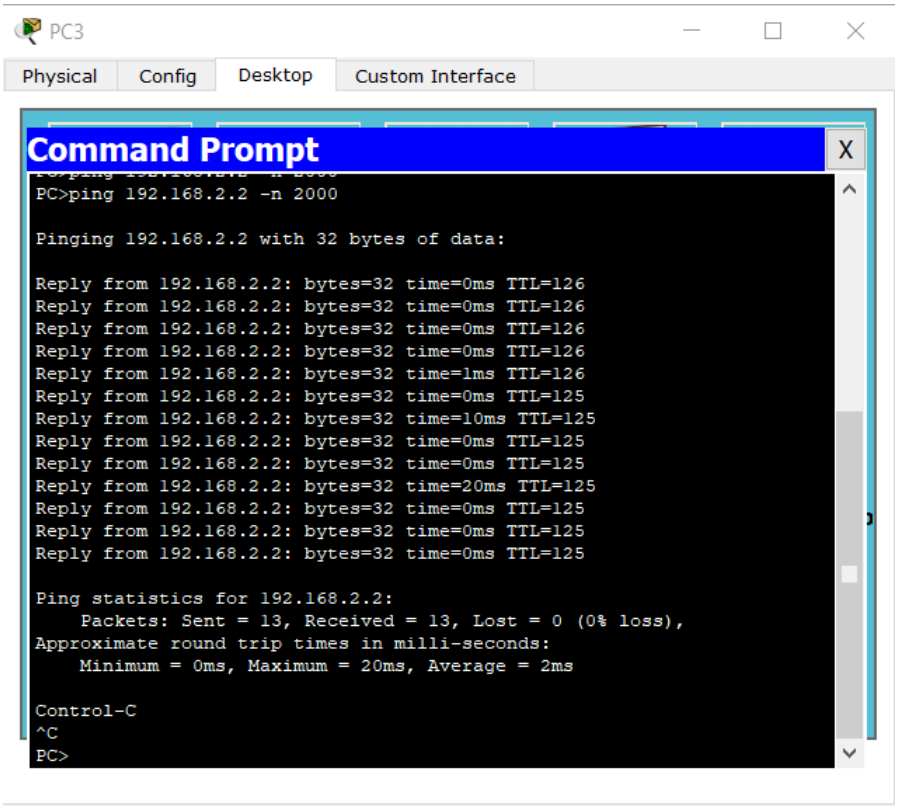


Рисунок 13.5 – Перевірка кількості втрачених пакетів при відключенні одного з портів

Далі вимикаємо gi0/1 (рис. 13.6).

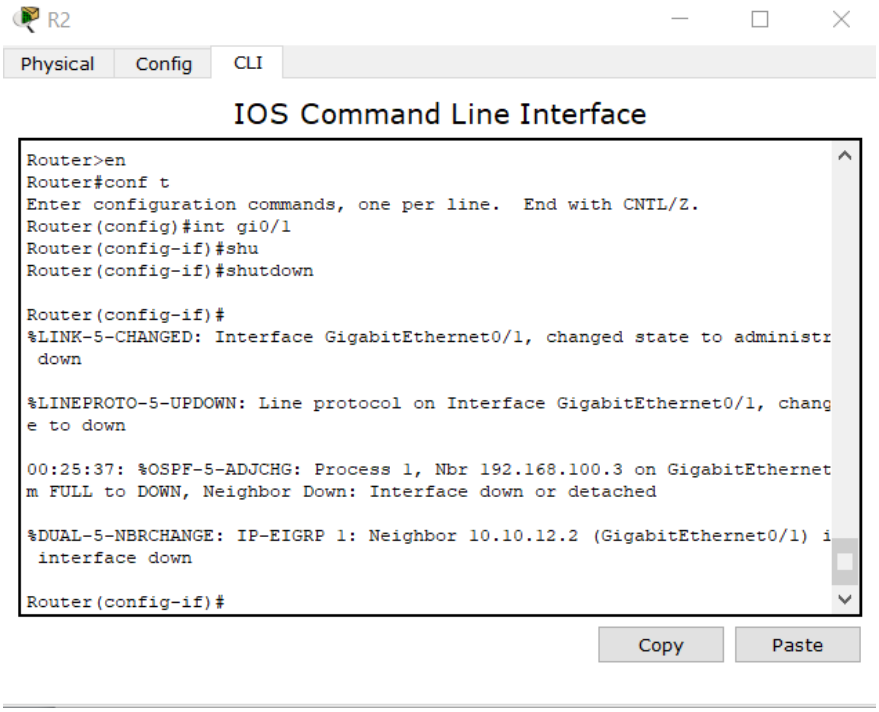


Рисунок 13.6 – Перевірка відмовостійкості

Як бачимо, жоден з пакетів не загубився. Якщо таку дію повторити з OSPF, декілька пекетів буде втрачено.

Відновимо відключений інтерфейс за допомогою команди no shutdown.

У минулому завданні ми розповсюджували дефолтний маршрут. Зробимо і для цього протоколу, припустивши що роутер 3 має дефолтний порт через IP-адресу PC3 (рис. 13.7).

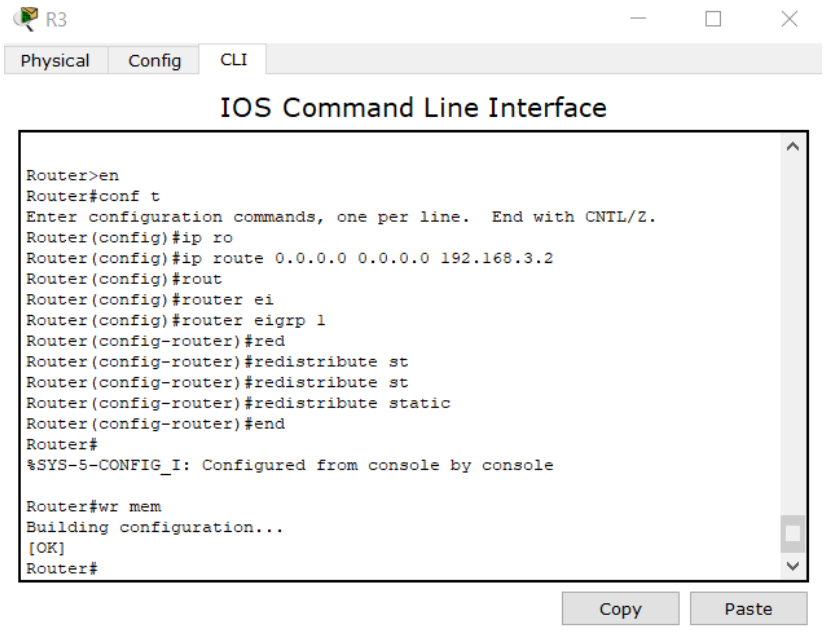


Рисунок 13.7 – Створення дефолтного маршруту

Зауважимо, що за допомогою операції *Router(config-router)#redistribute static* розповсюджується інформація про дефолтний маршрут.

Перевіряємо на роутері 2 таблицю маршрутизації (рис. 13.8).

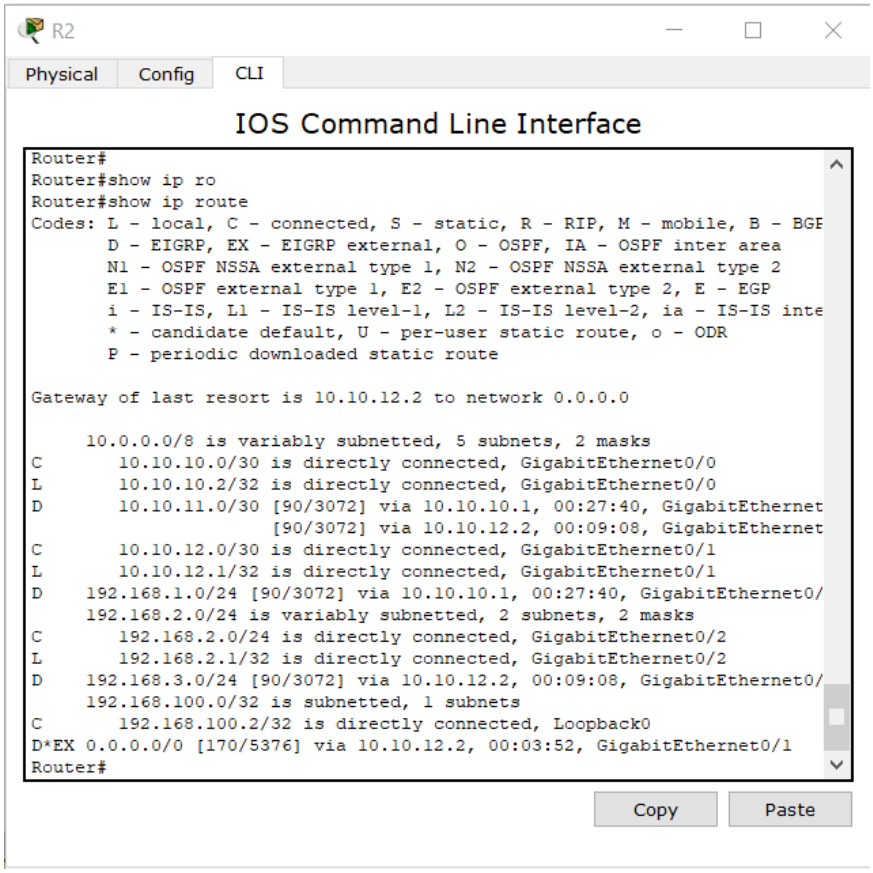


Рисунок 13.8 – Перевірка маршрутизації на роутері 2

Як бачимо, дефолтний маршрут прийшов нам по протоколу EIGRP.

Запитання для самопідготовки

1. Наведіть короткі характеристики автономної системи.
2. В чому полягають переваги та недоліки EIGRP порівняло с OSPF?
3. Для чого використовують no auto summary?

Практичне заняття №14

Домашня мережа WI-FI.

Мета заняття – ознайомлення з технологією бездротових мереж за допомогою технології WI-FI.

Розглянемо технологію бездротової передачі даних. Серед основних засобів застосування виділяють WI-FI міст, роутер (маршрутизатор) та точка доступу.

Створимо просту мережу (рис. 14.1).

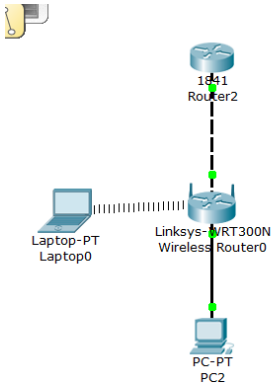


Рисунок 14.1 – Приклад простої мережі

Налаштовуємо WI-FI та роутер 2, що буде імітувати вихід в Інтернет та мати білу IP-адресу. Зауважимо, що на пристрої WI-FI використовуємо для підключення порту Ethernet (рис. 14.2).

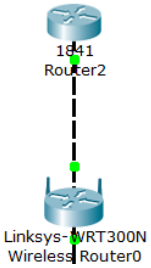


Рисунок 14.2 – З’єднання мережі

На інтерфейсі Інтернет провайдера налаштуємо IP-адресу з маскою 30 біт (рис. 14.3).

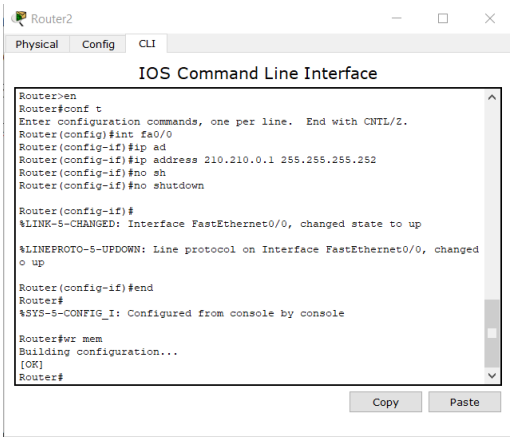


Рисунок 14.3 – Налаштування роутера Інтернет провайдера

Далі проводимо налаштування WI-FI маршрутизатора. Налаштування проведемо через симуляцію веб-інтерфейсу маршрутизатора. Зазначимо, що у вкладці «Router-IP» проводиться налаштування локальної мережі, тобто адреси, які будуть роздаватися по WI-FI або по портах для локальних підключень (за замовчуванням виставлена адреса 192.168.0.1 з маскою 24 біта, ввімкнений DHCP сервер, прописано що адреси роздаються з 100-ї адреси) (рис. 14.4).

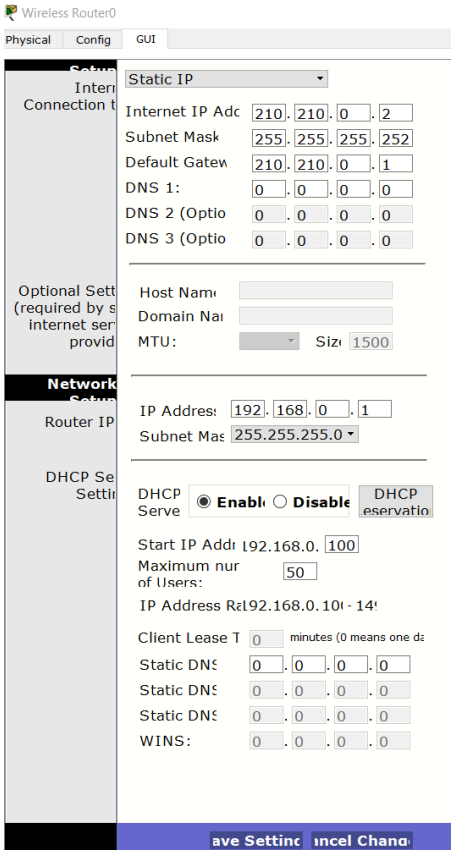


Рисунок 14.4 – Налаштування WI-FI маршрутизатора

У вкладці Wireless Network mode mixed означає, що можуть підключати всі пристрої, які підтримують режими, що знаходяться в спливаючому меню даного пункту.

Ідентифікатор мережі Service set identifier (SSID) задаємо по назві університету «KNAME», ширину та частоту каналу залишаємо на авто. SSID Broadcast для ідентифікатора мережі у режимі Enable означає, що всі пристрої з включеним WI-FI будуть бачити нашу бездротову мережу.

Також нас цікавить вкладка Wireless Security, проводимо її налаштування (рис. 14.5).

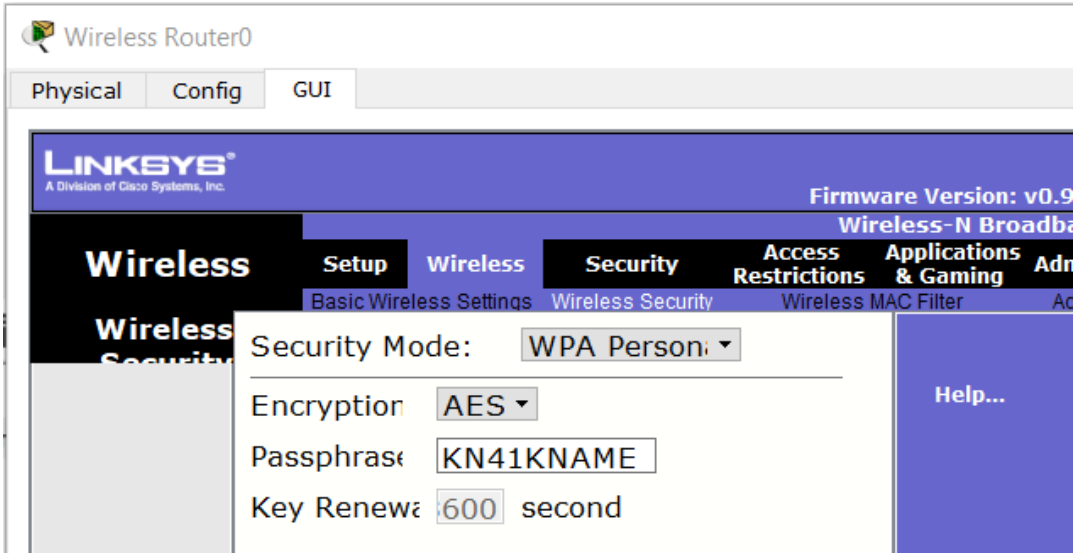


Рисунок 14.5 – Приклад налаштування у вкладці Wireless Security

Далі додаємо ноутбук. В залежності від версії CPT необхідно прибрати з ноутбуку підключений модуль для кабелю і додаємо WPC300N простим перетягування мишкою. Не забуваємо перед дією вимкнути ноутбук і потім його ввімкнути.

Далі заходимо у вкладку Wireless-Connect і дивимося доступні мережі. Бачимо KNAME, підключаємося, ввівши наш пароль KN41KNAME (рис. 14.6).

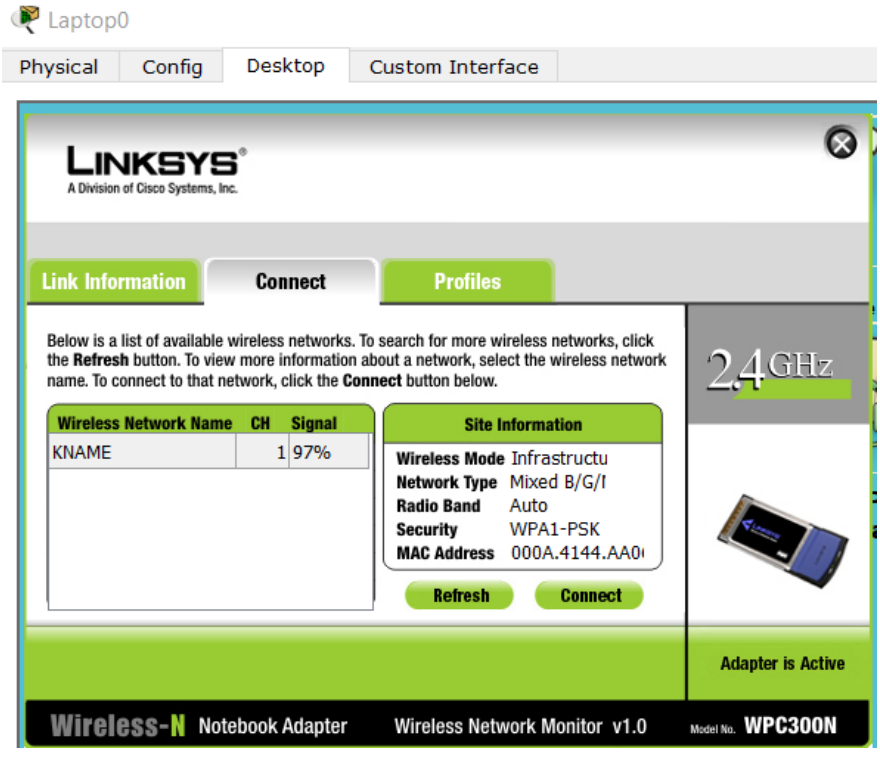


Рисунок 14.6 – Підключення ноутбука до бездротової мережі

Далі отримуємо візуальне підтвердження встановлення з’єднання (рис. 14.7).

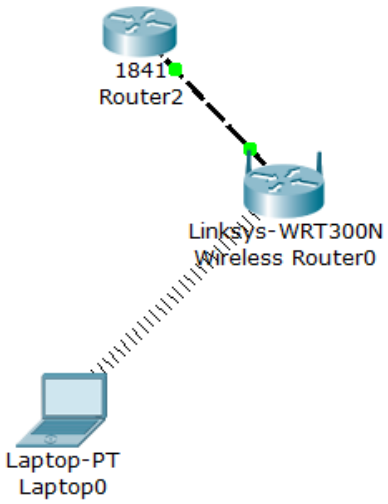


Рисунок 14.7 – Візуальне підтвердження підключення ноутбука до бездротової мережі

Перевіримо, яка IP-адреса присвоєна даному ноутбуку (рис. 14.8).

```
PC>ipconfig

Wireless0 Connection:(default port)
Link-local IPv6 Address.....: FE80::202:4AFF:FE5B:7D61
IP Address.....: 192.168.0.100
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 0.0.0.0
```

Рисунок 14.8 – Перевірка IP-адреси ноутбука

Пінгуємо шлюз, тобто WI-FI роутер (рис. 14.9).

```
PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=31ms TTL=255
Reply from 192.168.0.1: bytes=32 time=18ms TTL=255
Reply from 192.168.0.1: bytes=32 time=19ms TTL=255
Reply from 192.168.0.1: bytes=32 time=24ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 31ms, Average = 23ms
```

Рисунок 14.9 – Пінгування шлюзу з ноутбука

Пінгуємо адресу Інтернет провайдера (рис. 14.10).

```
PC>ping 210.210.0.1

Pinging 210.210.0.1 with 32 bytes of data:

Request timed out.
Reply from 210.210.0.1: bytes=32 time=24ms TTL=254
Reply from 210.210.0.1: bytes=32 time=21ms TTL=254
Reply from 210.210.0.1: bytes=32 time=19ms TTL=254

Ping statistics for 210.210.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 24ms, Average = 21ms
```

Рисунок 14.10 – Пінгування адреси Інтернет провайдера з ноутбука

Зауважимо, що можна вийти у мережу Інтернет, не налаштовуючи в цьому прикладі NAT. Це пов’язано з тим, що на WI-FI маршрутизаторах NAT налаштований автоматично.

Далі до нашої схеми можемо додати пристрій, наприклад комп’ютер. Підключаємо через порт Ethernet1? Чекаємо з’єднання, в налаштуваннях IP комп’ютера вмикаємо DHCP та бачимо налаштування (рис. 14.11).

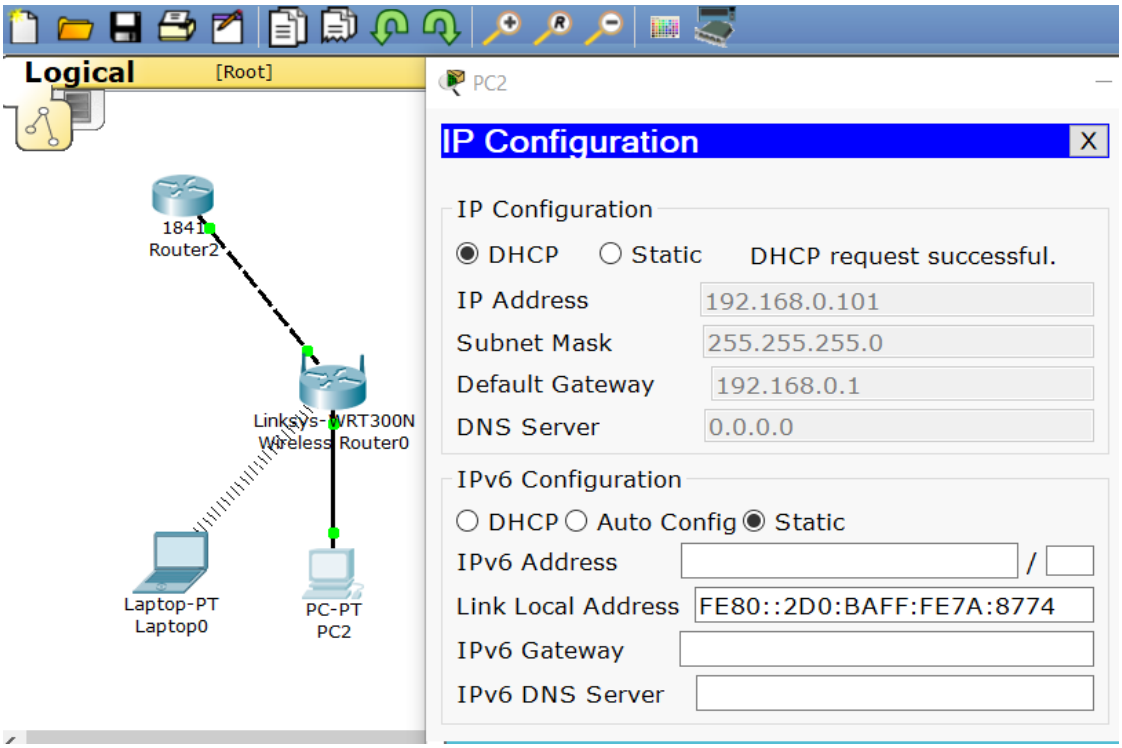


Рисунок 14.11 – Підключення комп’ютера до WI-FI маршрутизатора

Проводимо перевірку пінгування з комп’ютера (рис. 14.12).

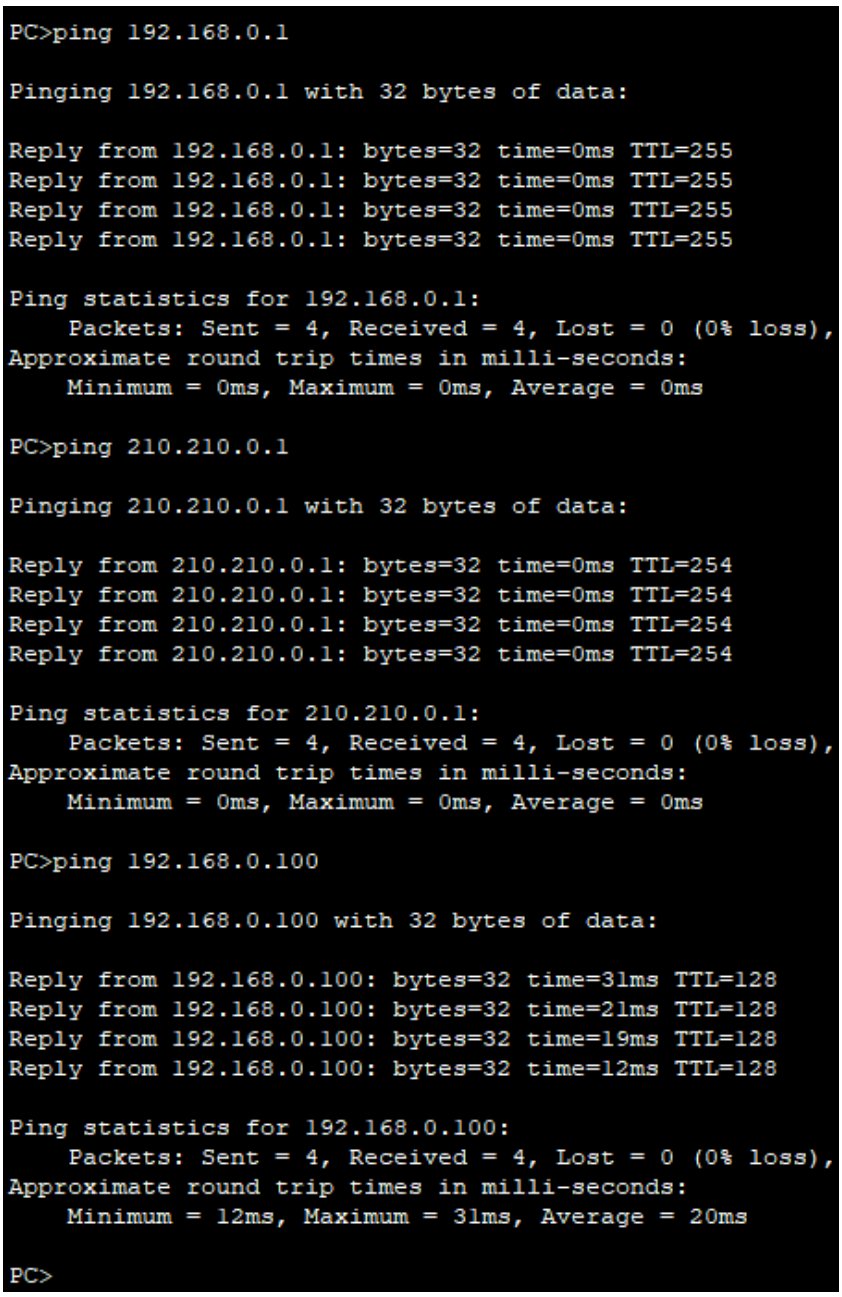


Рисунок 14.12 – Перевірка пінгування з комп’ютера

Запитання для самопідготовки

1. Яка принципова різниця між маршрутизатором та точкою доступу?
2. Наведіть приклади застосування точки доступу.
3. Які частоти мають бездротові мережі?
4. Які стандарти WI-FI вам відомі?
5. У Чому полягає основний принцип використання WI-FI мосту?

Практичне заняття №15

ТОЧКИ ДОСТУПУ

Мета заняття – налаштування точок доступу до безпровідної мережі.

Розглянемо технологію бездротової передачі даних. Серед основних засобів застосування виділяють WI-FI міст, роутер (маршрутизатор) та точку доступу.

Визначимо обидва комп'ютери (fa0/2, fa0/3) у VLAN2 Users, сервер у VLAN3 (fa0/4) Server відповідно до лабораторної роботи №4 (рис. 15.1).

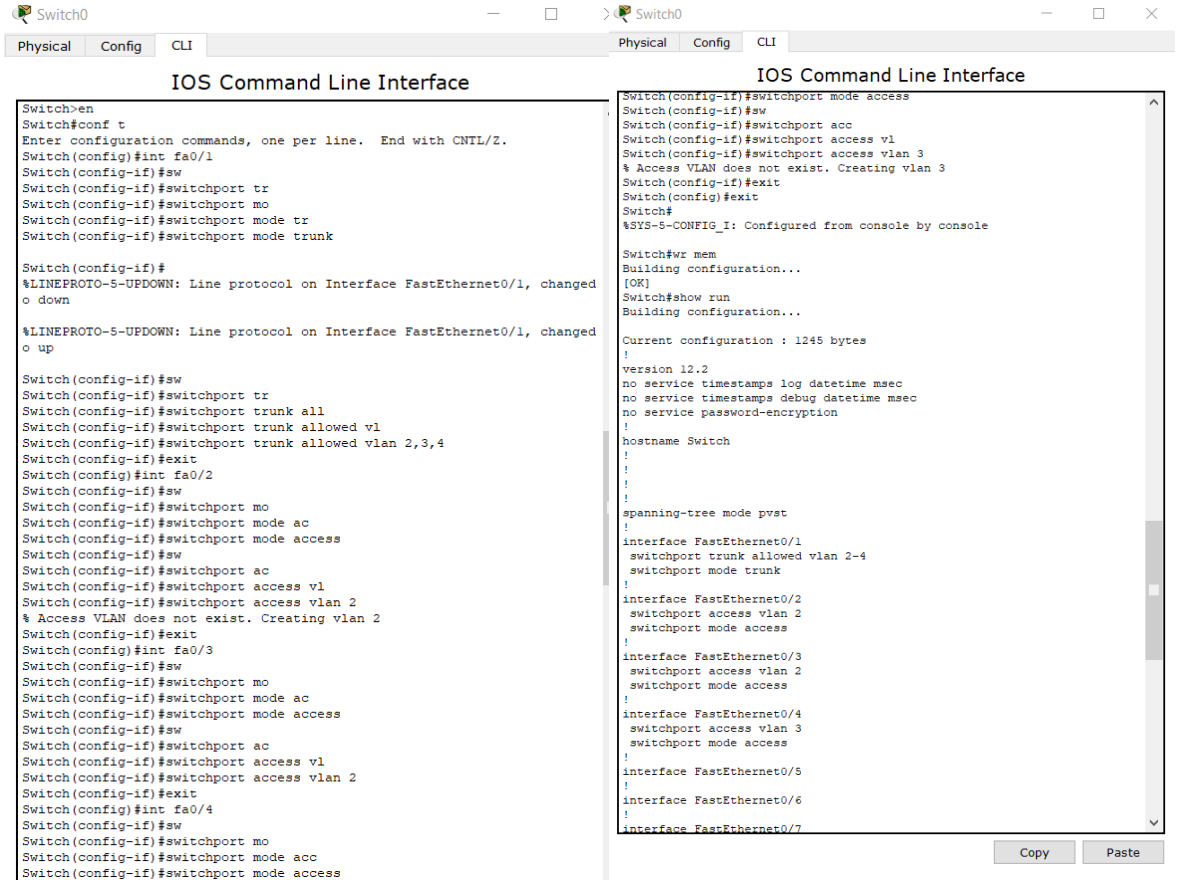


Рисунок 15.1 – Налаштування VLAN

На рисунку 15.2 наведемо найменування VLAN.

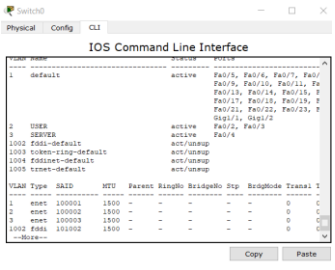


Рисунок 15.2 – Найменування VLAN

Далі, відповідно до практичних заняття №8 та №11, налаштовуємо роутер 0 з двома sub-інтерфейсами (рис. 15.3).

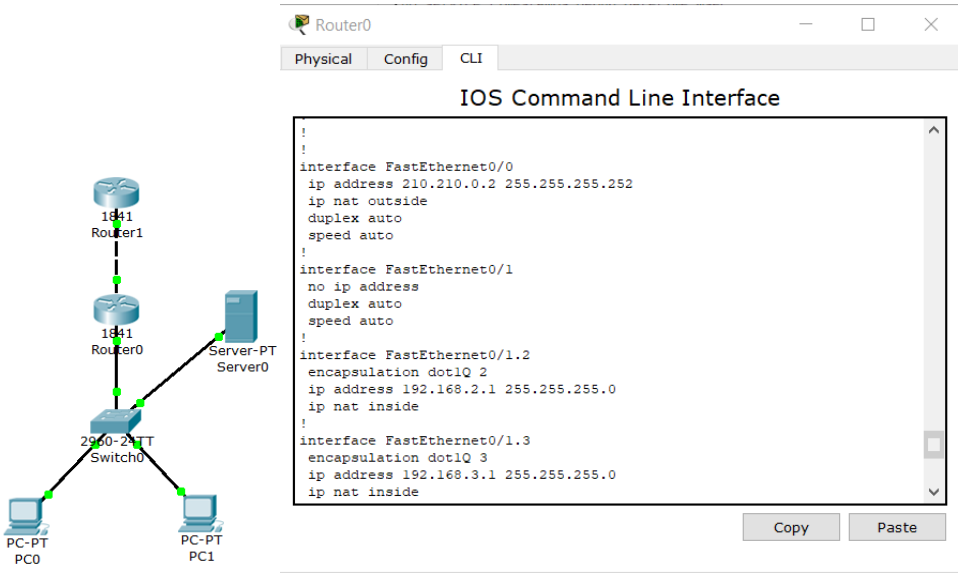


Рисунок 15.3 – Налаштування роутера 0

Також для роутера 0 створимо access-list (рис. 15.4).

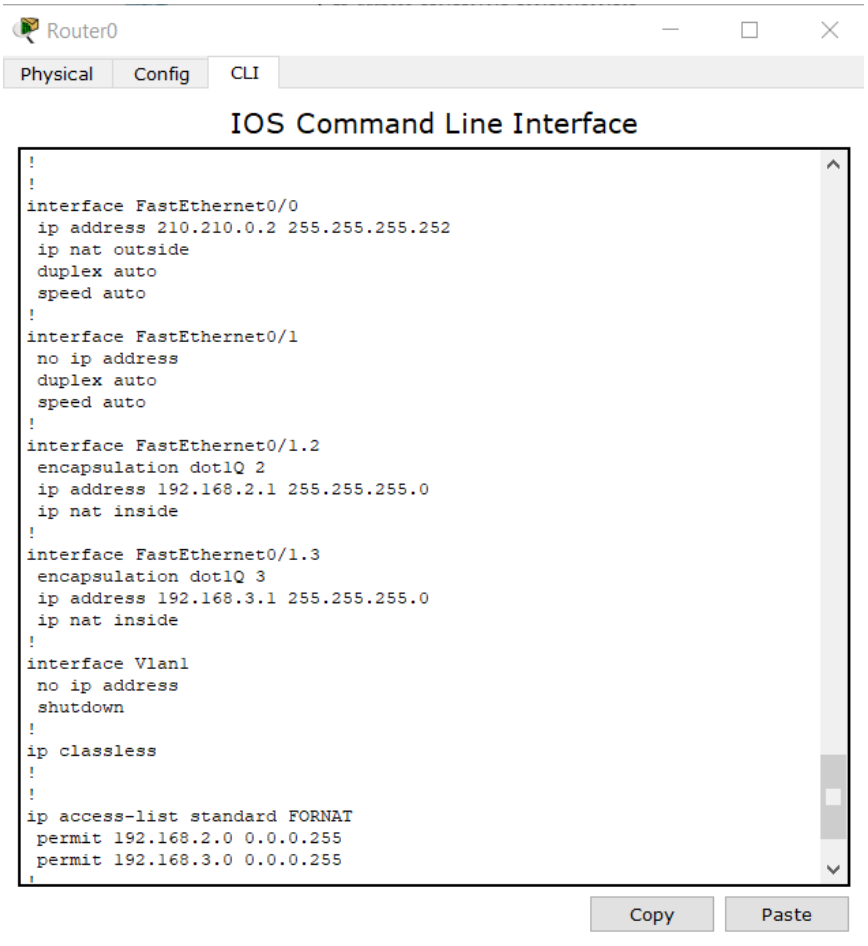


Рисунок 15.4 – Access-list для роутера 0

Необхідно виявити недоліки роботи системи та налаштувати мережу таким чином, щоб з PC0 йшов пінг на сервер та в Інтернет на 210.210.0.1.

З урахуванням масштабу мережі (наприклад три поверхи з можливістю розширення організації), встановлюємо точку доступу (в кімнатах очікування наприклад) та проводимо її налаштування (рис.15.5).

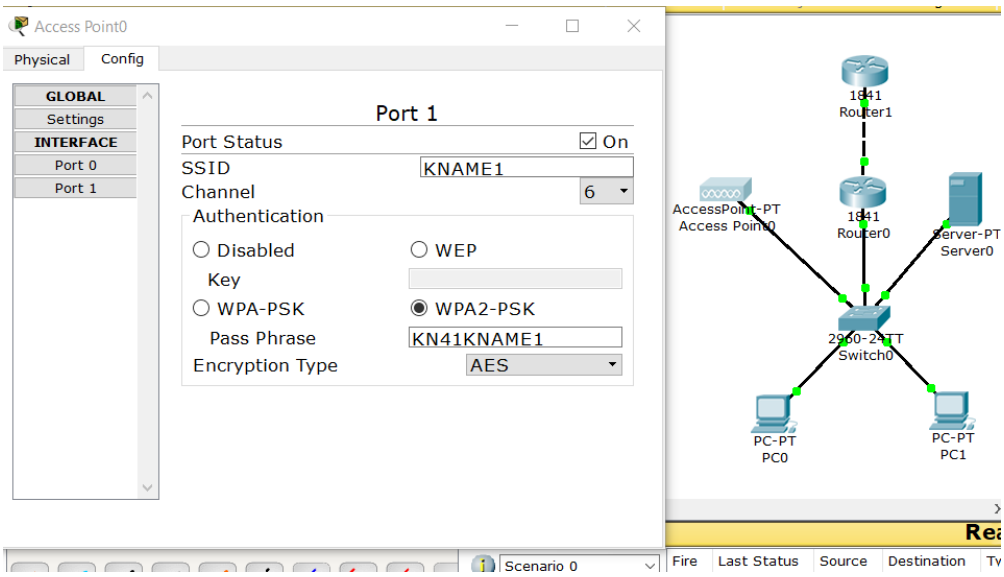


Рисунок 15.5 – Встановлення та налаштування точки доступу

Визначаємо точку доступу в окремий VLAN4 (рис. 15.6).

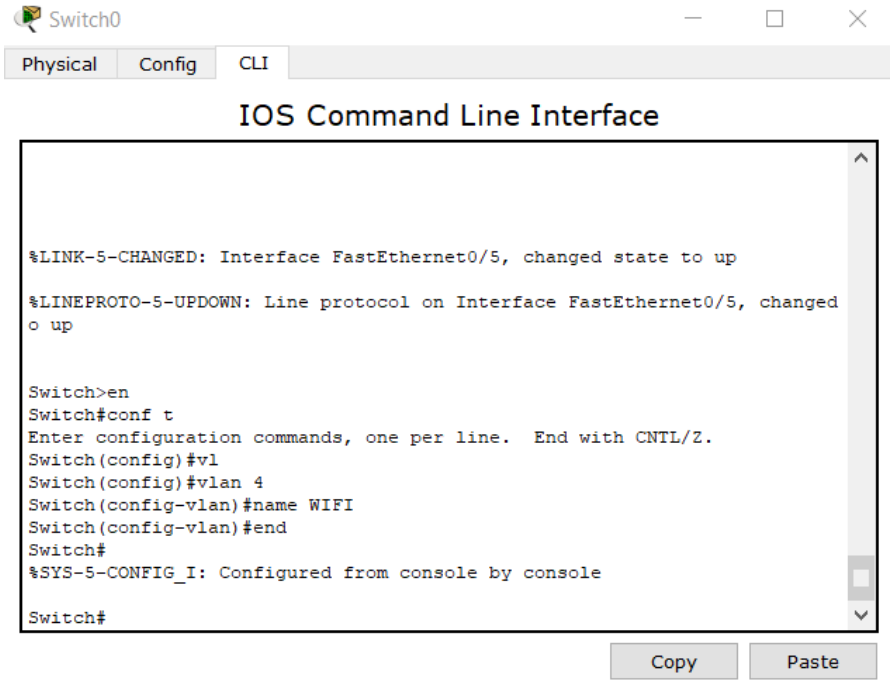


Рисунок 15.6 – Визначення точки доступу в окремий VLAN4

На рисунку 15.1 у транк порт вже додано VLAN4. Якщо на етапі рисунку 15.1 ви додали лише VLAN2 та VLAN 3, на цьому кроці необхідно додати VLAN 4.

Далі створюємо sub-інтерфейс на маршрутизаторі (рис. 15.7).

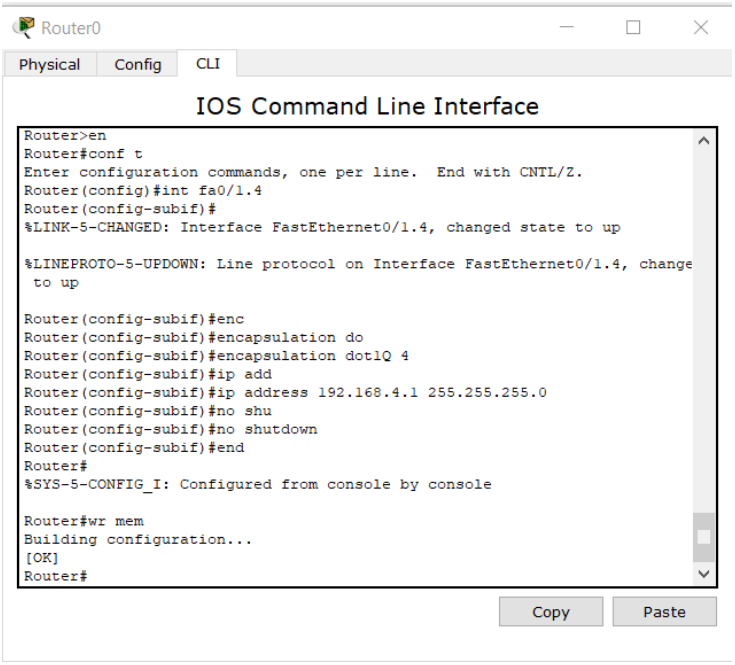


Рисунок 15.7 – Створення sub-інтерфейсу на маршрутизаторі для точки доступу

На даному етапі точка доступу не роздає IP-адреси, тому необхідно використовувати або виділений DHCP сервер або прямо з роутера роздавати адреси для користувачів WI-FI. Налаштуємо роутер 0 (рис. 15.8).

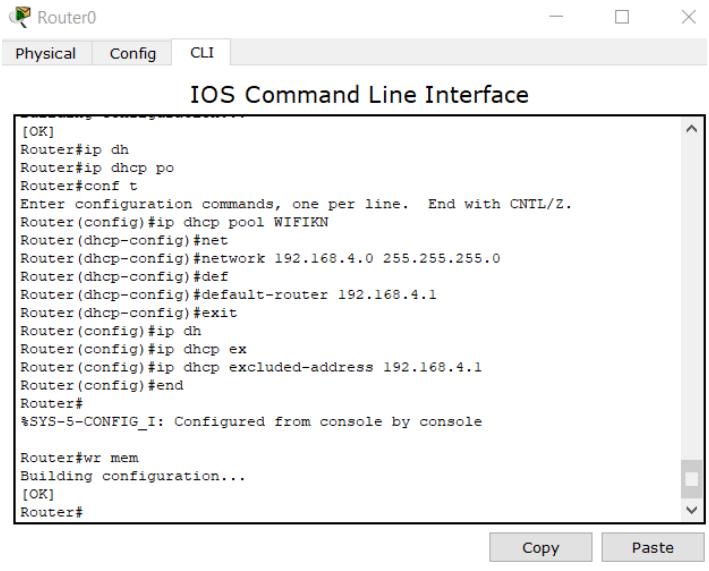


Рисунок 15.8 – Налаштування роутера 0 для генерування IP-адрес для користувачів WI-FI

Визначаємо точку доступу у VLAN4 (рис. 15.9).

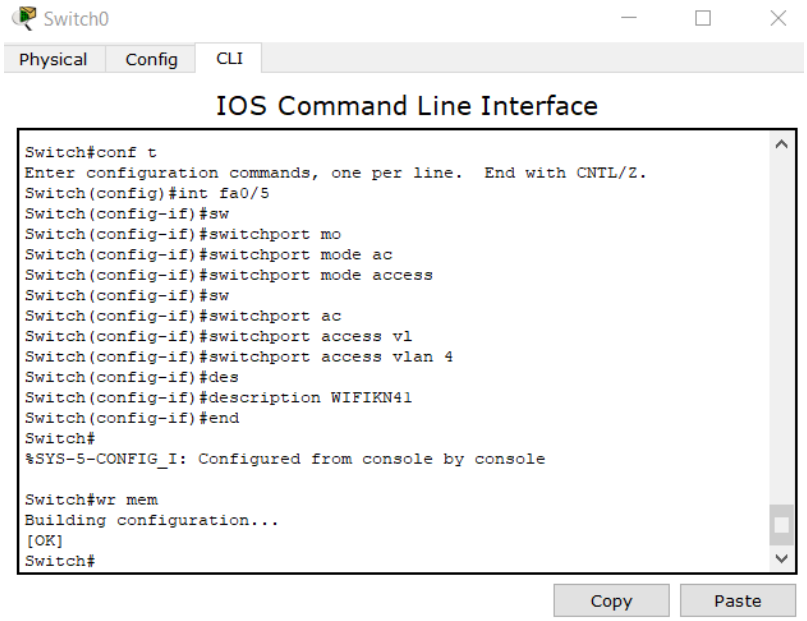


Рисунок 15.9 – Визначення точки доступу у 4 VLAN

При цьому виключаємо зі списку IP-адресу маршрутизатора. Додаємо гостьовий пристрій та тестуємо його підключення (рис. 15.10).

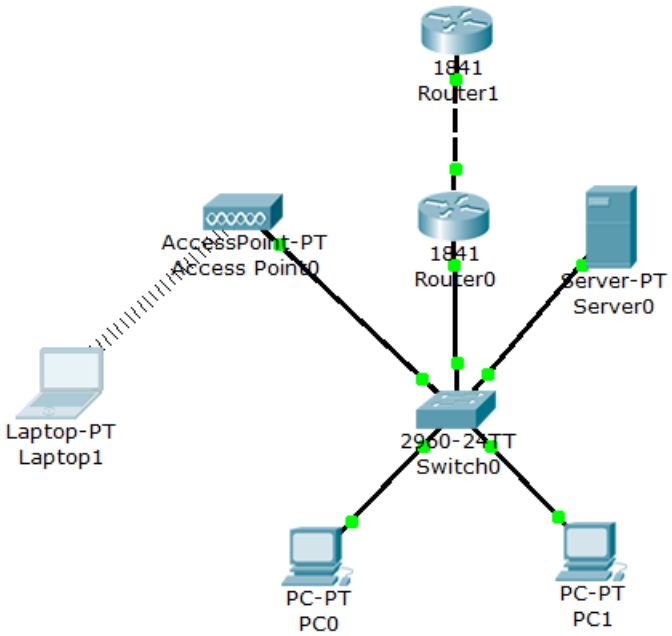


Рисунок 15.10 – Підключення гостьового пристрою до точки доступу

Наприкінці перевіряємо пінгування шлюзу, сусідніх сегментів, пінгування йде. Точка доступу, на відміну від WI-FI, не генерує NAT. Тому

проведемо відповідні налаштування, змінивши наш існуючий вже access-list (рис. 15.11).

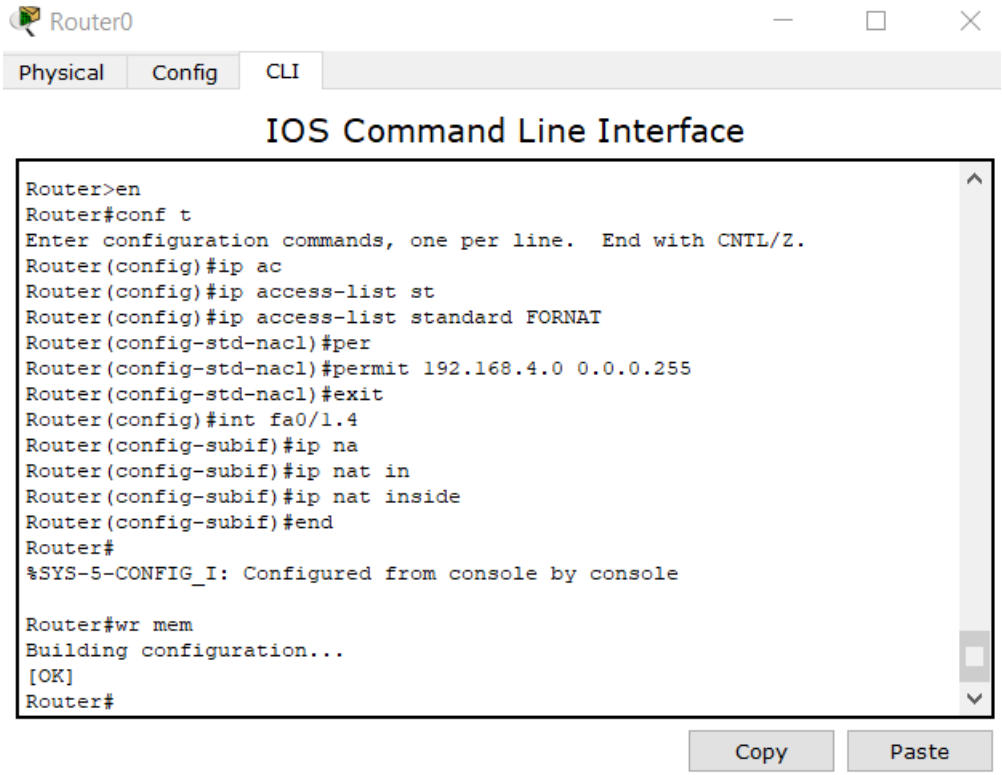


Рисунок 15.11 – Налаштування NAT для точки доступу

Підключаємо ноутбук до Інтернету. В ідеалі нам необхідно використовувати WI-FI контролер, аутентифікації користувачів заводити на окремий радіус сервер, налаштовувати access-list тощо.

Запитання для самопідготовки

1. Яка різниця між алгоритмами шифрування AES та TKIP?
2. Які мінуси підключення до точки доступу через WEP?
3. Що вам відомо про безпеку WI-FI?
4. Для чого створюються sub-інтерфейси?

2 САМОСТІЙНА РОБОТА

2.1 Загальні рекомендації щодо організації самостійної роботи

Обов'язковим елементом успішного засвоєння навчального матеріалу дисципліни «Комп'ютерні мережі» є самостійна робота здобувачів вищої освіти з вітчизняною і зарубіжною літературою з питань проектування та функціонування комп'ютерних мереж, практики проведення наукових досліджень. Самостійна робота є основним засобом оволодіння навчальним матеріалом у час, вільний від нормованих навчальних занять, тобто лекційних і практичних занять.

Основні види самостійної роботи, на які повинні звертати увагу здобувачі вищої освіти:

– вивчення лекційного матеріалу;

– робота з опрацювання та вивчення рекомендованої літератури;

– підготовка до практичних занять;

– підготовка до обговорень та інших, пропонованих викладачем, завдань;

– робота над рефератами, тезами, доповідями з тематики курсу;

– самоперевірка здобувачем вищої освіти власних знань за запитаннями для самоперевірки;

– підготовка до поточного та підсумкового контролю;

Для цього необхідно:

– розібратися в сутності кожної запропонованої теми;

– підготуватися до дискусії щодо розуміння вивченого матеріалу;

– у разі наявності декількох тлумачень кожного терміну, обґрунтувати, якої саме інтерпретації дотримується здобувач і чому, а також обґрунтувати, з чим здобувач вищої освіти не може погодитись;

– за умови, що значення якогось терміну є незрозумілим, зафіксувати запитання, а під час дискусії за запропонованими темами винести їх на обговорення або проконсультуватися у викладача.

Опрацювання лекційного матеріалу. У системі різних форм навчально-виховної роботи особливе місце належить лекції, де викладач надає здобувачу вищої освіти основну інформацію, навчає розмірковувати, аналізувати, допомагає опанувати ключові знання, а також спрямовує самостійну роботу здобувача.

Зв'язок лекції і самостійної роботи здобувача вищої освіти розглядається в таких напрямах:

– лекція як головна початкова ланка, що визначає зміст і обсяг самостійної роботи здобувача;

– методичні прийоми читання лекцій, що активізують самостійну роботу здобувачів вищої освіти;

– самостійна робота, яка сприяє поглибленому засвоєнню теми на базі прослуханої лекції.

Перший етап самостійної роботи починається з процесу слухання і записування лекції. Правильно складений конспект лекції – найефективніший засіб стимулювання подальшої самостійної роботи здобувачів вищої освіти. Здобувач вищої освіти повинен чітко усвідомити, що конспект лекцій – це короткий тезовий запис головних положень навчального матеріалу.

Конспект допомагає в раціональній підготовці до практичних занять, підсумковому контролю, у визначенні напряму і обсягу подальшої роботи з літературними джерелами. Під час підготовки до лекції здобувач вищої освіти повинен опрацювати матеріал попередньої лекції з використанням підручників та інших джерел літератури.

На лекціях висвітлюють тільки основні теоретичні положення та найбільш актуальні проблеми, тому більшість питань виноситься на самостійне опрацювання.

Підготовка до практичних занять розпочинається з опрацювання лекційного матеріалу. Здобувач вищої освіти повинен самостійно підготувати відповіді на контрольні запитання, які подані в програмі у певній послідовності згідно з логікою засвоєння навчального матеріалу.

Практичні заняття збагачують і закріплюють теоретичні знання здобувачів вищої освіти, розвиваючи їх творчу активність, допомагають у набутті практичних навичок роботи за предметом навчальної дисципліни.

У процесі підготовки до практичних занять самостійна робота здобувачів є обов'язковою частиною навчальної роботи, без якої успішне і якісне засвоєння навчального матеріалу неможливе. Це свідчить про необхідність керування самостійною роботою здобувачів з боку викладача завдяки проведенню цілеспрямованих організаційних і контрольних заходів.

Викладач у вступній лекції рекомендує здобувачам вищої освіти літературу, методичні рекомендації до самостійної роботи та до організації практичних занять з дисципліни. У методичних вказівках з кожної теми наведено перелік питань для теоретичної підготовки до заняття. У разі, коли здобувач не може самостійно розібратися в якомусь питанні, він може отримати консультацію у викладача.

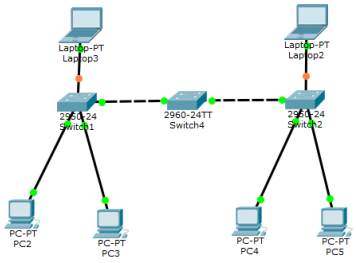
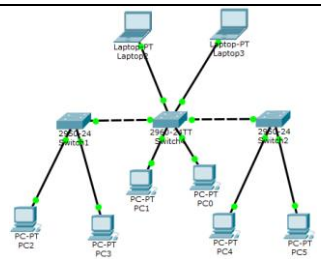
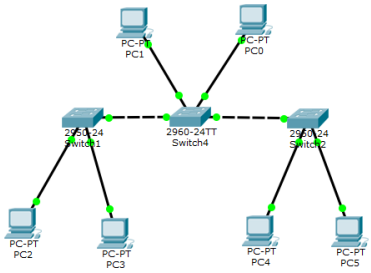
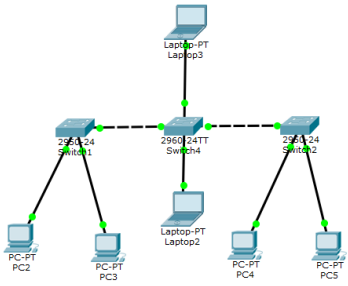
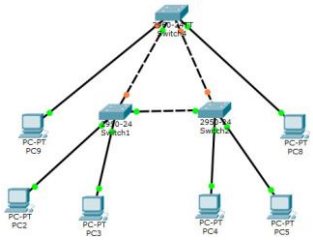
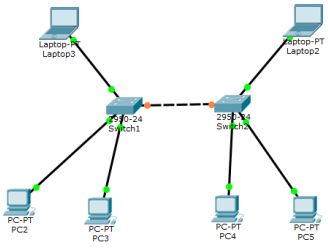
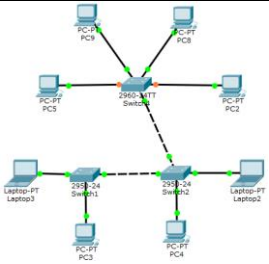
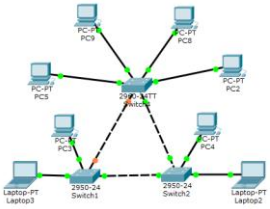
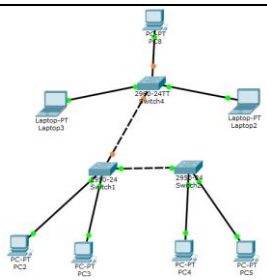
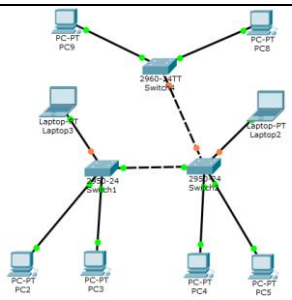
Добре організовані консультації дозволяють спрямувати самостійну роботу в потрібному напрямі, зробити раціональною і підвищити її ефективність.

2.2 Варіанти завдань до самостійної роботи

В рамках виконання самостійної роботи необхідно створити топологію комп'ютерної мережі відповідно до варіанту (табл. 2.2.1). У всіх варіантах, в якості комутаторів, використайте Switch 2960. Далі призначте комп'ютерам IP-адреси відповідно до вказаного діапазону адрес (табл. 2.2.2). Мережна маска для всіх пристроїв 255.255.255.0.

При виконанні завдання необхідно всім кінцевим вузлам надати унікальні імена (ваше ім'я за паспортом). На наступному кроці перевірте налаштування кожного кінцевого вузла за допомогою команди «ipconfig», перевірте всі з'єднання між комп'ютерами за допомогою команди «ping». У режимі симуляції надішліть запит за допомогою команди «ping» з PC3 до PC5, відстежуючи рух пакета ICMP.

Таблиця 2.2.1 – Параметри завдання топології комп’ютерної мережі

Варіант 1	Варіант 2
	
Варіант 3	**Варіант 4**
	
Варіант 5	**Варіант 6**
	
Варіант 7	**Варіант 8**
	
Варіант 9	**Варіант 10**
	

Таблиця 2.2.2 – Варіанти діапазонів адрес

Номер варіанта	Діапазон адрес
1	112.168.5.15 – 112.168.5.25
2	12.208.6.15 – 12.208.6.25
3	144.18.9.15 – 144.18.9.25
4	133.73.9.60 – 133.73.9.69
5	12.208.6.15 – 12.208.6.25
6	13.18.0.45 – 13.18.0.55
7	152.164.8.75 – 152.164.8.85
8	122.8.85.45 – 122.8.85.55
9	155.38.0.0 – 155.38.0.9
10	212.28.68.15 – 212.28.68.25

Звіт з виконаної роботи повинен містити наступні складові:

- зображення топології мережі;
- скрін роботи команди «ipconfig» кожного кінцевого вузла;
- скрін роботи команди «ping» між усіма кінцевими вузлами;с
- скрін симуляції шляху слідування одного запиту з PC3 до PC5;
- скрін кадру запиту після його отримання на PC5;
- загальні висновки по роботі.

Контрольні запитання

1. Яка максимальна кількість пристроїв у мережі підтримує CPT?
2. Які типи мережних пристроїв і з’єднань використовуються в CPT?
3. Як перейти до інтерфейсу командного рядка пристрою?
4. Як додати до топології та налаштувати новий пристрій?
5. Що таке комп’ютерна мережа?
6. Назвіть основні компоненти мережі?
7. Чим комутатор відрізняється від моста?

СПИСОК РЕКОМЕНДОВНИХ ДЖЕРЕЛ

1. Коробейнікова Т. І. Комп’ютерні мережі / Т. І. Коробейнікова, С. М. Захарченко. – Львів : Львівська політехніка, 2022. – 228 с.

2. Микитишин А. Г. Комп’ютерні мережі / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк. – Львів : Магнолія, 2021. – Кн. 1. – 256 с.

3. Конахович Г. Ф. Експлуатація телекомунікаційних систем / Г. Ф. Конахович. – Київ : Центр навчальної літератури, 2019. – 372 с.

4. Комп’ютерні мережі : навч. посіб. / О. В. Задерейко, Н. І. Логінова, А. А. Толокнов. – Одеса : Фенікс, 2022. – 249 с.

5. Жураковський Б. Ю. Комп’ютерні мережі : навч. посіб. / Б. Ю. Жураковський, І. О. Зенів. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.

6. Ромашко С. М. Конспект лекцій з дисципліни «Комп’ютерні мережі і телекомунікації» / С. М. Ромашко. – Львів : ЛРІДУ НАДУ, 2016. – 61с.

7. Комп’ютерні мережі : навч. посіб. / А. І. Блозва, Ю. В. Матус, В. В. Смолій, Б. С. Гусєв, Д. Ю. Касаткін, Т. Ю. Осипова, Я. А. Савицька. – Київ : Компрінт, 2017. – 821с.

8. Олещенко Л. М. Організація комп’ютерних мереж : навч. посіб. / Л. М. Олещенко. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 225 с.

9. Денніс Брилов. Комп’ютерні науки. Базовий курс / Денніс Брилов, Дж. Гленн Брукшир. – Київ : Діалектика, 2018. – 475 с.

10. Плахотніков К. В. Комп’ютерні мережі : конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання зі спеціальності 122 – Комп’ютерні науки) [Електрон. ресурс] / К. В. Плахотніков ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Електрон. текст. дані. – Харків : ХНУМГ ім. О. М. Бекетова, 2023. – 156 с. – Режим доступу: https://eprints.kname.edu.ua/63182/, вільний (дата звернення 29.03.2023). – Назва з екрана.

Електронне навчальне видання

Методичні рекомендації
до проведення практичних занять та організації самостійної роботи
з навчальної дисципліни

«КОМП'ЮТЕРНІ МЕРЕЖІ»

(для здобувачів першого (бакалаврського) рівня вищої освіти
денної та заочної форм навчання
зі спеціальності 122 – Комп'ютерні науки,
освітньо-професійна програма «Комп'ютерні науки»)

Укладач **ПЛАХОТНІКОВ** Кирило Валерійович

Відповідальний за випуск *М. В. Новожилова*
За авторською редакцією
Комп'ютерне верстання *К. В. Плахотніков*

План 2023, поз. 233М

Підп. до друку 28.03.2023. Формат 60 × 84/16.
Ум. друк. арк. 6,7.

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