

Зміст

Лабораторна робота №0. Знайомство з Cisco Packet Tracer. Конфігурація початкових налаштувань комутатора.	3
Лабораторна робота №1. Вивчення моделей TCP/IP і OSI у дії	12
Лабораторна робота №2. Побудова мережі. Визначення MAC- та IP-адрес	20
Лабораторна робота №3. Вивчення таблиці ARP	25
Лабораторна робота №4. Аналіз трафіку одноадресної та загальної розсилки	31

Лабораторна робота №0. Знайомство з Cisco Packet Tracer.

Конфігурація початкових налаштувань комутатора.

Топологія:



Завдання:

1. Огляд програми Cisco Packet Tracer.
2. Знайомство з IOS.
3. Налаштування початкових параметрів комутатора.
4. Збереження файлів конфігурації в NVRAM.

Загальні відомості:

Packet Tracer – проста, універсальна програма для домашнього користування, яка допоможе вам у вивченні комп'ютерних мереж. За допомогою Packet Tracer можна експериментувати, створюючи та тестуючи моделі, а також проводити аналіз «а що, якщо» без страху щось вивести з ладу. У цій вправі ви детально познайомитеся з функціоналом Packet Tracer, при цьому ви дізнаєтесь, як користуватися довідкою та навчальними керівництвами. Окрім цього, ви навчитесь проводити базові налаштування комутатора за допомогою командного рядка (CLI) і зберігати ці налаштування.

ЧАСТИНА 1. ЗНАЙОМСТВО З CISCO PACKET TRACER

У першій частині лабораторної роботи ви побачите, як влаштований Packet Tracer та познайомитеся з його функціоналом.

Крок 1: Отримання довідки та навчальних матеріалів

Робота з будь-якої програмою має починатися з вивчення функціоналу цієї програми. Для цього часто використовується документація або навчальні посібники. Packet Tracer пропонує цілий набір навчальних матеріалів та туторіалів, які допоможуть вам опанувати базові навички та швидко розпочати роботу.

- а. Доступ до розділів з навчальними матеріалами можна отримати двома способами.
 - Клікнути знак питання в правому верхньому куту меню панелі інструментів.
 - Відкрити пункт меню **Help** і обрати **Contents** (або **Tutorials** для отримання доступу до навчальних відео)

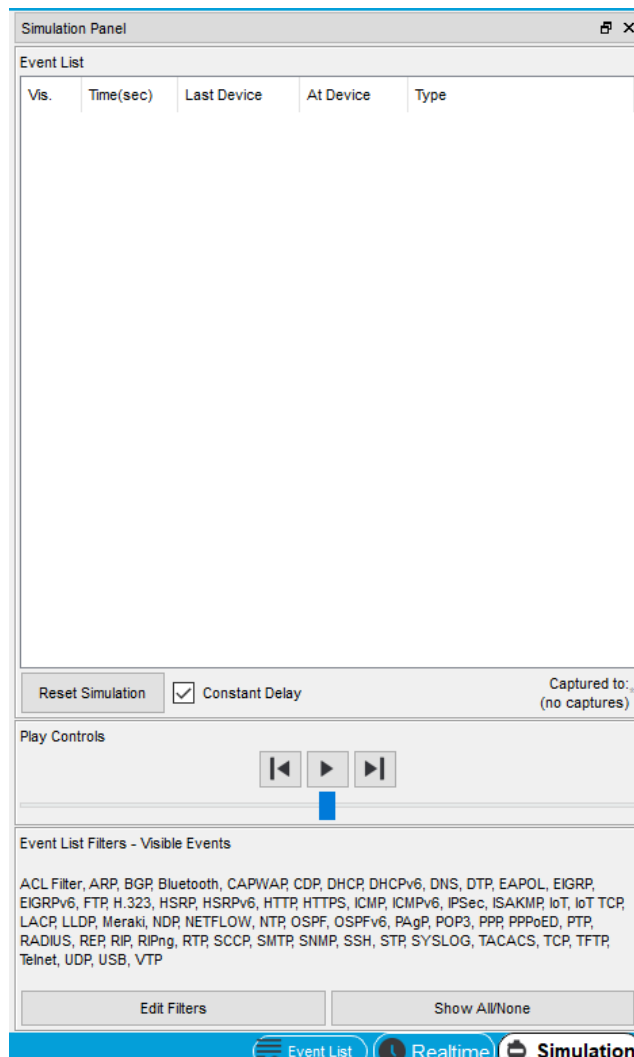
- b. Перед тим, як продовжити роботу над завданням, необхідно отримати уявлення про інтерфейс програми та режим симуляції. Для цього рекомендується переглянути наступні відео, які доступні у вищезгаданих туторіалах.
- 1) **Interface Overview** в розділі **Getting Started**.
 - 2) **Simulation Environment** в розділі **Realtime and Simulation Modes**.
 - 3) **Desktop Tab** в розділі **Configuring Devices**.

Крок 2: Виконайте перемикання між режимами реального часу та симуляції

- a. Знайдіть слово **Realtime** в правому нижньому кутку інтерфейсу Packet Tracer. В режимі реального часу мережа завжди діє як справжня незалежно від того, працюєте ви з нею чи ні. Налаштування при цьому застосовуються в реальному часі і мережа реагує на них практично миттєво.



- b. Перейдіть на вкладку **Simulation**, яка знаходиться поряд з вкладкою **Realtime**. В цьому режимі мережа працює повільно, що дозволяє спостерігати за шляхами передачі даних і детально вивчати пакети даних.
- c. Панель, що відкрилася при переході в режим симуляції, дозволяє виконувати будь-які дії покроково, зберігаючи при цьому кожну подію з можливістю повернутися назад до неї. Окрім цього в цій панелі можна здійснити фільтрування, зазначивши в ньому за якими пакетами яких протоколів ми хочемо спостерігати.



Крок 3: Виконайте перемикання між логічним та фізичним представленнями

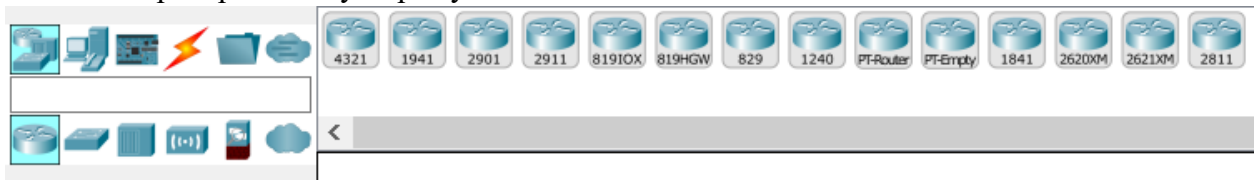
- a. Знайдіть слово **Logical** у верхньому лівому кутку інтерфейсу Packet Tracer. Даний режим дозволяє будувати логічні топології мереж, не пов'язуючи їх з географією місцевості або фізичним розташуванням в будівлі (кількох будівлях чи навіть цілого міста).



- b. Перейдіть на вкладку **Physical**. Цей режим дозволяє переглядати фізичне відображення логічної топології мережі. Тут можна оцінити масштаб і розташування елементів мережі.

Крок 4: Робота з елементами мережі

- a. У лівому нижньому кутку інтерфейсу Packet Tracer можна знайти меню з пристроями та елементами мережі. Тут знаходяться як проміжні (**Network devices**), так і кінцеві (**End devices**) пристрої мережі. Також саме тут знаходяться з'єднання (**Connections**), які ми будемо використовувати, щоб об'єднати усі пристрої в одну мережу.

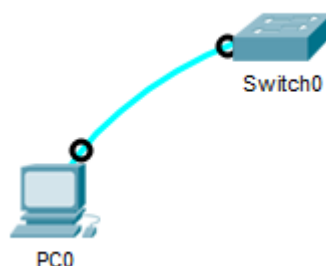


ЧАСТИНА 2. ВСТАНОВЛЕННЯ З'ЄДНАННЯ ТА ЗНАЙОМСТВО З IOS

У другій частині лабораторної роботи ви створите свою першу систему, яка буде складатися лише з одного комп'ютера та комутатора, після чого ви познайомитеся з інтерфейсом командного рядку (CLI).

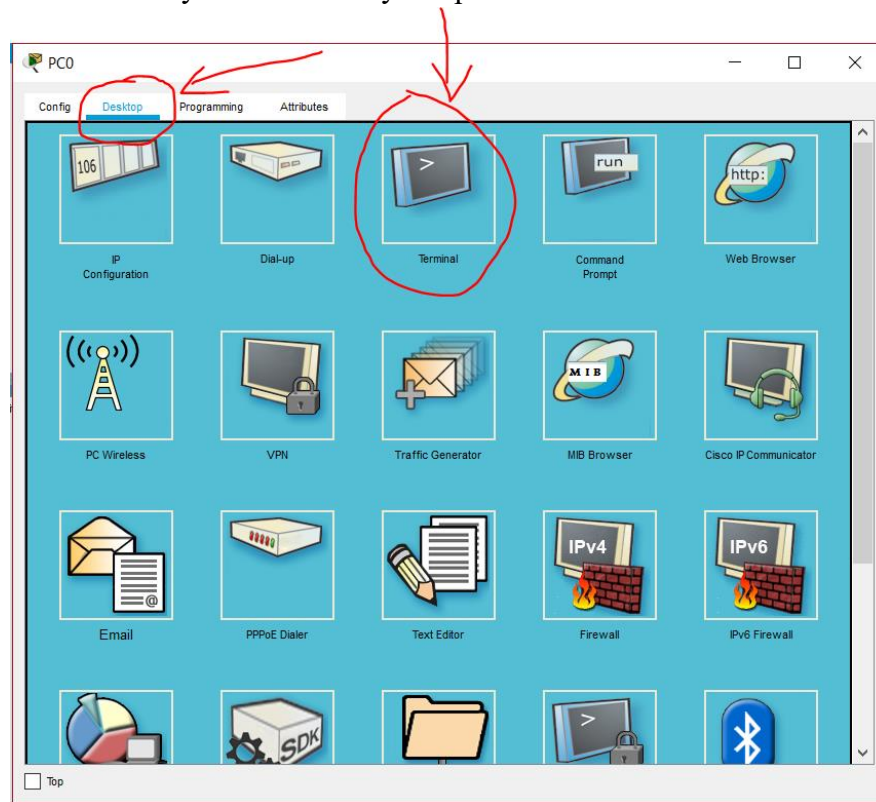
Крок 1: Створіть з'єднання

- a. Для того, щоб створити систему, зображену на топології, необхідно просто перетягнути пристрої з області елементів мережі на робочу область (найбільша область, поки що порожня, знаходиться в самому центрі програми). В даному випадку нам треба комутатор та ПК (можна обрати перші із списку запропонованих пристроїв).
- b. Виберіть світло-блакитний консольний кабель із розділу **Connections**. Натисніть на ПК та оберіть варіант для підключення **RS-232**. Потім натисніть на комутатор і оберіть порт **Console**, щоб завершити підключення. Тепер ви маєте доступ до комутатора з комп'ютера і можете проводити певні операції.

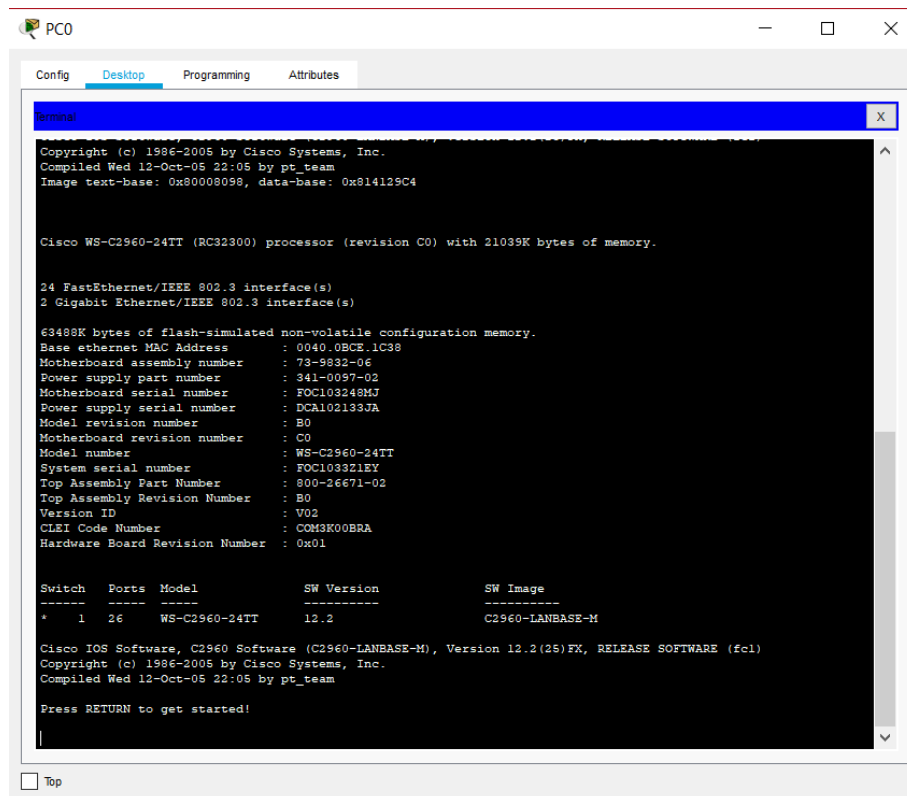


Крок 2: Встановіть сеанс діалогу з комутатором

- а. Клікніть на ПК і відкрийте вкладку **Desktop**. Оберіть значок **Terminal** та натисніть кнопку OK – запуситься командний рядок, за допомогою якого ми будемо налаштовувати наш комутатор.



- б. Коли командний рядок повністю завантажиться, має з'явитися напис **Press RETURN to get started!**, що означає що можна починати роботу. Натискаємо **ENTER**.



Крок 3: Вивчіть довідку IOS

- a. В IOS доступна довідка по командам в залежності від рівня роботи. В даний момент відображається запрошення **User EXEC** (користувацький режим **EXEC**) і пристрій очікує введення команди. Найлегший спосіб отримання довідки – ввести знак питання. Як відповідь командний рядок видає список команд.
- b. Можна почати вводити одну або декілька літер, після чого ввести знак питання (наприклад, **te?**). Як результат будуть виведені команди, що починаються на ці літери (в даному випадку на **te**).

Крок 4: Вивчіть методи переходу між режимами

- a. Режим **User EXEC** є оглядовим та не дозволяє робити будь-які зміни з пристроєм. Для цього потрібно увійти у привілейований режим. Команда **enable** дозволяє це зробити.
- b. Увійшовши у привілейований режим введіть знак питання та вивчіть команди, що доступні в даному режимі. Можна побачити, що тут їх набагато більше і вони дозволяють робити певні маніпуляції з комутатором. Проте це ще не все. Існує режим глобальної конфігурації, з якого і здійснюються всі налаштування. Щоб увійти в цей режим потрібно ввести команду **configure terminal**.
- c. Для виходу з режиму глобальної конфігурації потрібно ввести команду **exit**, з привілейованого режиму – **disable**.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#disable
Switch>
```

Окрім того: існують також і інші режими, які використовуються для конфігурування певних інтерфейсів та ліній. Для того, щоб перейти в такий режим, потрібно в режимі глобальної конфігурації ввести назву та порядковий номер інтерфейсу (лінії) – наприклад, **line console 0**.

Зверніть увагу: у кожному режимі строка, що пропонує ввести команду, має інший вигляд. Наприклад, на користувачькому рівні вона має вигляд **Switch>**, на привілейованому: **Switch#**, в режимі глобальної конфігурації: **Switch(config)**. Це полегшує роботу з командним рядком, постійно нагадуючи, в якому режимі ви знаходитесь.

Підказка: при введенні команди, у випадку, якщо введених символів достатньо для унікального визначення команди, можна натиснути клавішу **TAB**, яка закінчить введення команди автоматично (наприклад, в користувачькому режимі є тільки одна команда, що починається на **en**, тому, ввівши ці дві літери, можна скористатися табом, що пришвидшить та полегшить роботу). Окрім того, не завжди обов'язково дописувати команди до кінця. Якщо введених літер вистачає для унікальної ідентифікації команди, можна просто натиснути на **ENTER**, після чого виконається відповідна команда.

ЧАСТИНА 3. КОНФІГУРАЦІЯ ПОЧАТКОВИХ НАЛАШТУВАНЬ КОМУТАТОРА

У третій частині лабораторної роботи ви налаштуєте початкові параметри комутатора, використовуючи інтерфейс командного рядка (CLI).

Крок 1: Налаштуйте годинник

- Використайте команду **show clock** привілейованого режиму, щоб отримати час і дату. Як бачите, ці час та дата не відповідають дійсності. Спробуємо налаштувати годинник.
- Вивчіть команду **clock**, викликавши для неї довідку. Для цього введіть команду **clock ?**. Як бачимо, щоб установити потрібний нам час, необхідно ввести команду **clock set**. Проте ця команда не спрацює (можете спробувати), тому що потрібно ввести ще деякі дані. Щоб дізнатися які саме, введіть команду **clock set ?**.
- Система показала формат введення часу. Спробуємо ввести **clock set 15:00:00**. Ця команда знову не відпрацювала. Розбираємось в чому справа (вводимо команду **clock set 15:00:00 ?**), бачимо, що потрібно ввести дату. Вводимо **clock set 15:00:00 30 Apr 2019**. Тепер при виконанні команди **show clock** виведеться реальний час та дата.

```
Switch#show clock
*0:7:58.20 UTC Mon Mar 1 1993
Switch#clock ?
  set  Set the time and date
Switch#clock set
% Incomplete command.
Switch#clock set ?
  hh:mm:ss  Current Time
Switch#clock set 15:00:00
% Incomplete command.
Switch#clock set 15:00:00 ?
  <1-31>   Day of the month
  MONTH    Month of the year
Switch#clock set 15:00:00 30 Apr 2019
Switch#show clock
15:0:4.159 UTC Tue Apr 30 2019
Switch#
```

Крок 2: Перевірте поточну конфігурацію комутатора

- Для цього в привілейованому режимі введіть команду **show running-config**. Інформація, що вивелась, показує які інтерфейси та лінії є у комутатора, IP-адреси, ім'я пристрою та інше.

```
Switch#show running-config
Building configuration...

Current configuration : 1078 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
--More--
```

Крок 3: Налаштуйте ім'я комутатора

- a. Для цього потрібно увійти в режим глобальної конфігурації та ввести команду **hostname name**, де *name* – бажане ім'я.

```
Switch(config)#hostname ourSwitch
```

- b. Переглядаючи тепер файл конфігурації, можна побачити, що ім'я нашого комутатора змінилося з імені за замовчуванням (**Switch**) на ім'я, яке ми щойно встановили.

```
ourSwitch#show run
Building configuration...

Current configuration : 1081 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ourSwitch
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
--More-- |
```

Крок 4: Забезпечте безпечний доступ до консолі

- a. Для забезпечення безпечного доступу до консолі варто поставити пароль, що дозволить доступ лише тим, хто знає цей пароль. Для встановлення такого паролю потрібно для початку увійти в режим **config-line** за допомогою команди в глобальному режимі конфігурації **line console 0**.
- b. Для встановлення самого паролю потрібно ввести команду **password**, після якої потрібно одразу вказати бажаний пароль (наприклад, **password cisco**).

```
ourSwitch(config)#line console 0
ourSwitch(config-line)#pass
ourSwitch(config-line)#password cisco
ourSwitch(config-line)#login
ourSwitch(config-line)#
```

- c. Але поки що цей пароль ще не захищає наш комутатор, він лише існує. Щоб запитувався пароль потрібно це явно вказати за допомогою команди **login**, після чого можна вийти з режиму конфігурації лінії консолі. Тепер кожного разу, коли ми будемо підключатися до комутатора (ще до входження в користувацький режим) система буде запитувати у нас пароль.

```
Press RETURN to get started.

User Access Verification
Password: |
```


Крок 5: Забезпечте безпечний доступ до привілейованого режиму

- а. Окрім паролю до консолі ми можемо захистити привілейований режим від небажаних змін. Це може стати у нагоді, коли у нас є користувачі, які можуть під'єднуватися до комутатора, проте не мають права змінювати в ньому якісь налаштування. Для встановлення такого паролю потрібно в режимі глобальної конфігурації ввести команду **enable password**, після якої потрібно одразу вказати бажаний пароль (наприклад, **enable password mypassword**).

```
ourSwitch(config)#enable password mypassword
```

- б. Тепер кожного разу при введенні команди **enable** (для входу до привілейованого режиму) необхідно буде ввести даний пароль.

```
ourSwitch>enable
Password: |
```

Окрім того: пароль можна зробити зашифрованим. Чому це важливо? Якщо ввести команду **show running-config**, можна побачити, що наші паролі в цьому файлі зберігаються у вигляді звичайного тексту. Тобто будь-хто, хто має доступ до користувацького режиму, зможе переглянути цей файл і дізнатись пароль до привілейованого режиму. Щоб уникнути цього, можна замінити команду налаштування паролю до привілейованого режиму на **enable secret**, після чого ввести бажаний пароль (наприклад, **enable secret mysecret**). Тепер, якщо подивитися в файл конфігурації, можна побачити, що пароль зберігається у зашифрованому вигляді.

```
ourSwitch#show run
Building configuration...

Current configuration : 1133 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ourSwitch
!
enable password mypassword
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
--More--
```

```
ourSwitch#show run
Building configuration...

Current configuration : 1180 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ourSwitch
!
enable secret 5 $1$mERr$/x9VUDEedbC1BA8DhbGj0
enable password mypassword
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
```

Зверніть увагу: тепер наш пароль до привілейованого режиму зашифрований. Те ж саме можна зробити з іншими паролями, які ми встановили. Для цього використовується команда **service password-encryption**, яка вводиться в режимі глобальної конфігурації. Тепер, передивившись файл конфігурації, ми нарешті можемо побачити всі наші паролі в безпечному зашифрованому вигляді.

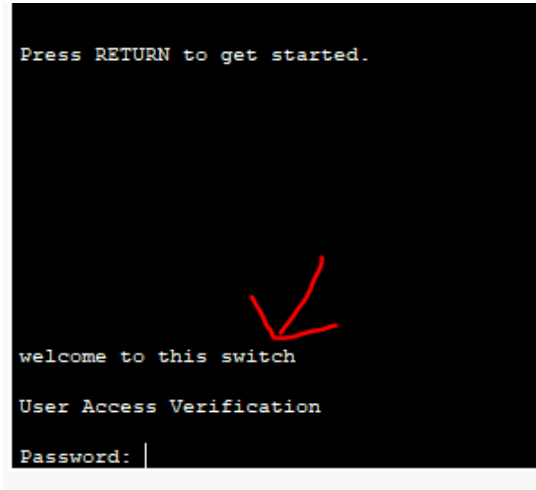
Крок 6: Встановіть банер MOTD (Message Of The Day)

- а. Іноді, перед використанням комутатора, потрібно передати якусь інформацію тому, хто збирається працювати з пристроєм. Це може бути попередження або порада. Для цього використовується банер **MOTD**. Це повідомлення буде виводитися кожного разу при під'єднанні до комутатора (ще до входу в користувацький режим). Для створення такого повідомлення необхідно в режимі

глобальної конфігурації ввести команду **banner motd**, після якої ми розміщаємо наше повідомлення між двох ідентичних символів, які не зустрічаються в самому повідомленні (наприклад, **banner motd \$welcome to the switch\$**)

```
ourSwitch(config)#banner motd $welcome to this switch$
```

- b. Тепер, якщо ви двічі введете команду **exit**, тобто повністю вийдете з усіх режимів, то зможете побачити своє повідомлення.



```
Press RETURN to get started.  
  
welcome to this switch  
User Access Verification  
Password: |
```

Крок 7: Збережіть файл конфігурації в NVRAM

- a. Тепер, коли всі параметри налаштовані, потрібно їх зберегти, щоб вони не втрапились при перезавантаженні комутатора або у випадку відключення живлення. Для цього використовується команда **copy running-config startup-config**, тобто це команда, яка копіює вміст теперішнього файлу конфігурації у файл, який читається системою при початку роботи. Цей файл зберігається в **NVRAM (nonvolatile RAM)**, ця область є енергонезалежною, що запобігає втраті налаштувань при будь-яких збоях системи.

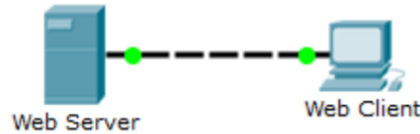
```
ourSwitch#copy running-config startup-config  
Destination filename [startup-config]?  
Building configuration...  
[OK]  
ourSwitch#
```

Завдання: повторити кроки, описані вище. Як результат виконання роботи продемонструвати побудовану систему з налаштованим комутатором.

Підсумок: У даній лабораторній роботі ми познайомились з інтерфейсом програми Cisco Packet Tracer, побудували нашу першу топологію, а також виконали початкову конфігурацію комутатора.

Лабораторна робота №1. Вивчення моделей TCP/IP і OSI у дії

Топологія:



Завдання:

1. Вивчення HTTP-трафіку
2. Відображення елементів пакета протоколів TCP/IP

Загальні відомості:

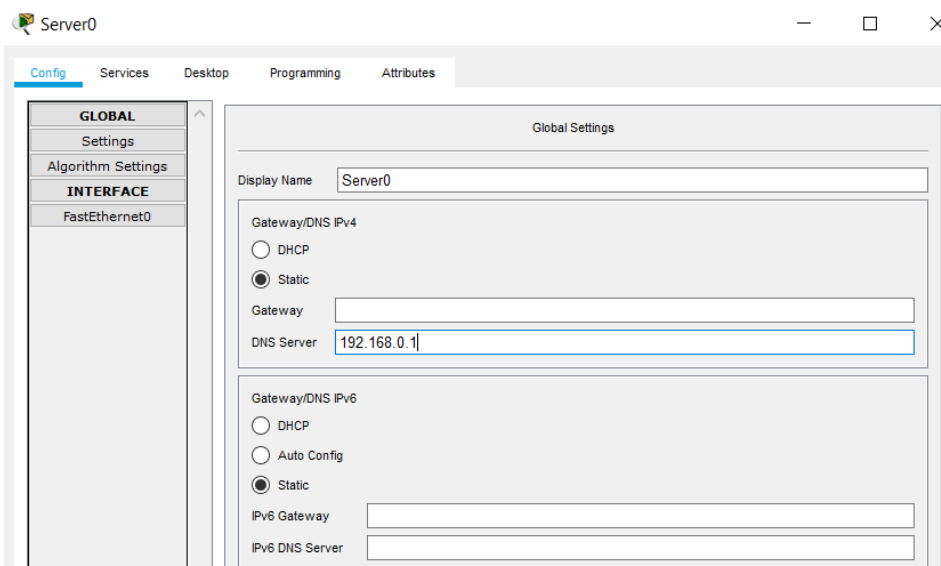
Дана вправа по симуляції - перший крок на шляху до розуміння принципів роботи пакета протоколів **TCP / IP** і його взаємозв'язку з моделлю **OSI**. Режим симуляції дозволяє переглядати вміст даних, що переміщуються по мережі на кожному з рівнів.

При передачі даних по мережі вони розбиваються на більш дрібні фрагменти і ідентифікуються таким чином, щоб їх можна було з'єднати по прибуттю в пункт призначення. Кожен фрагмент отримує власне ім'я (**protocol data unit** - PDU) і асоціюється з конкретним рівнем моделей TCP / IP і OSI. Режим симуляції програми **Packet Tracer** дозволяє переглядати всі рівні і пов'язані з ними PDU. Нижче описана послідовність кроків користувача для запиту веб-сторінки з веб-сервера за допомогою встановленого на клієнтському ПК веб-браузера.

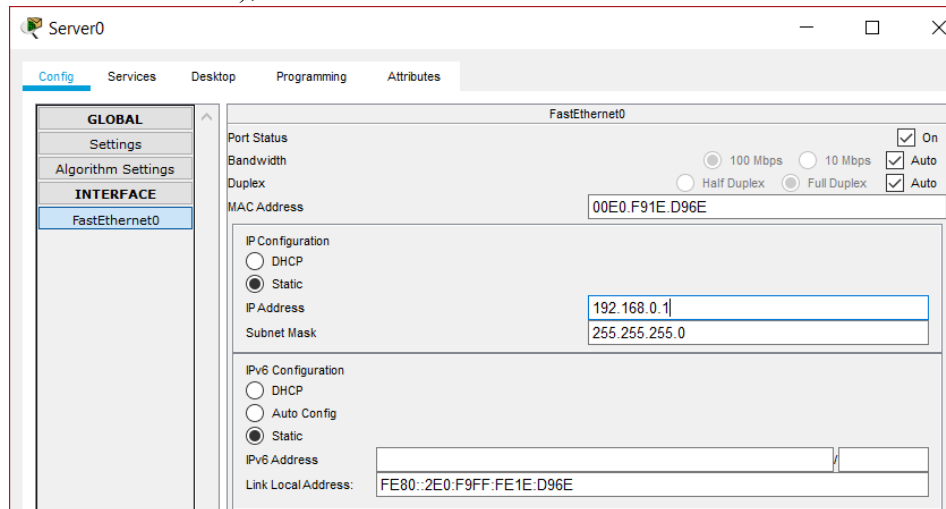
Дана лабораторна робота дасть вам можливість ознайомитися з можливостями програми **Packet Tracer**, а також наочно розглянути процес інкапсуляції.

Для виконання лабораторної роботи потрібно спочатку створити систему, що відповідає наведеній вище топології, а потім – додати наступні налаштування:

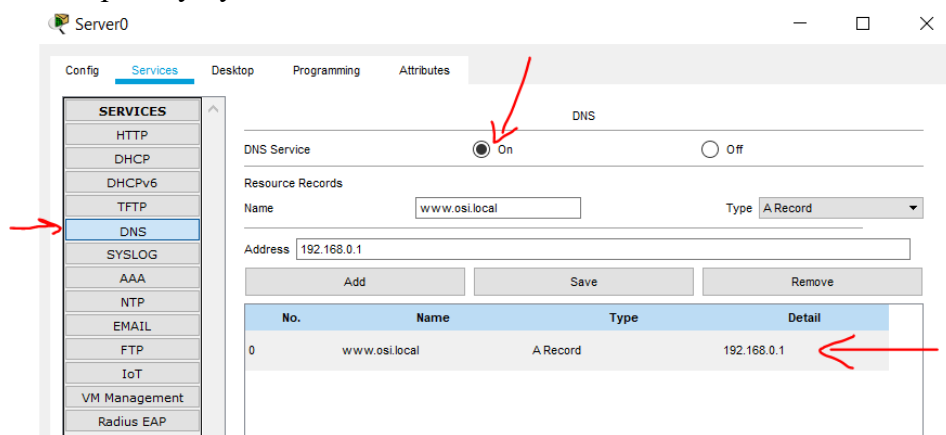
- Для веб-сервера:
 1. на вкладці **Config**, розділ **Settings** в полі **DNS Server** задати будь-яку **IP-адресу** (наприклад, 192.168.0.1);



- цю саму IP-адресу задати в полі **IP-Address** на вкладці **Config**, розділ **FastEthernet0** (після цього поле **Subnet Mask** має автоматично заповнитись);

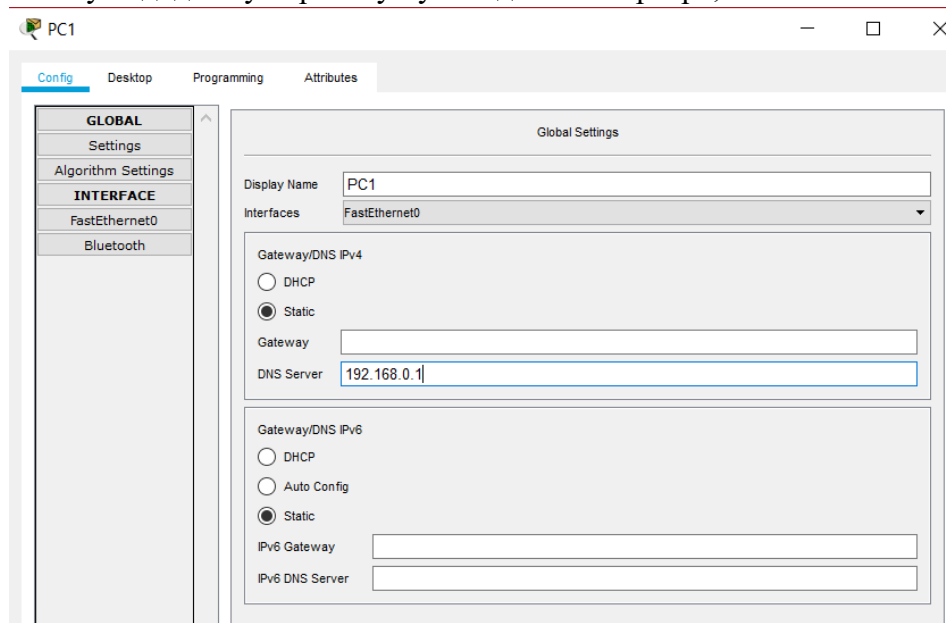


- на вкладці **Services** в розділі **DNS** потрібно увімкнути **DNS Service** (On) та додати новий домен з ім'ям **www.osi.local** та адресою, що була задана в першому пункті.

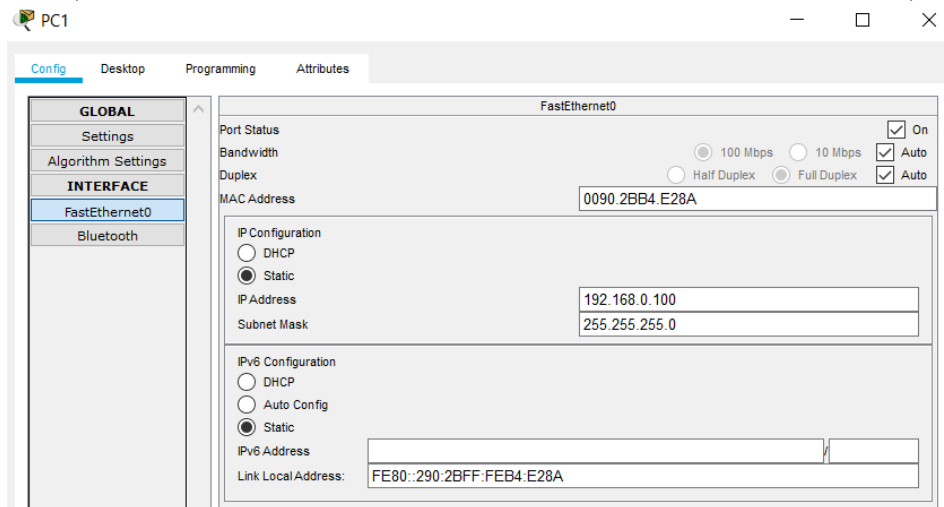


- Для веб-клієнта:

- на вкладці **Config**, розділ **Settings** в полі **DNS Server** задати адресу, що було додано у першому пункті для веб-сервера;



2. задати будь-яку адресу (наприклад 192.168.0.100), відмінну від адреси DNS Сервера, в полі **IP-Address** на вкладці **Config**, розділ **FastEthernet0** (після цього поле **Subnet Mask** має автоматично заповнитись).



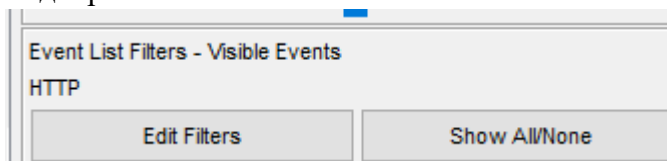
ЧАСТИНА 1. ВИВЧЕННЯ HTTP-ТРАФІКУ

У першій частині лабораторної роботи ви будете використовувати програму **Packet Tracer** (PT) в режимі симуляції для генерування веб-трафіку і вивчення протоколу HTTP.

Крок 1: Перейдіть з режиму реального часу в режим симуляції

У правому нижньому кутку інтерфейсу **Packet Tracer** знаходяться вкладки для перемикання між режимами **Realtime** (режим реального часу) і **Simulation** (режим симуляції). PT завжди запускається в режимі **Realtime**, в якому мережеві протоколи працюють з реальними значеннями часу. Однак широкі можливості **Packet Tracer** дозволяють користувачеві «Зупинити час», переключившись в режим симуляції. У режимі симуляції користувачі можуть покроково переходити від одної мережевої події до іншої.

- a. Натисніть на значок режиму **Simulation** для перемикання з режиму реального часу в режим симуляції.
- b. Виберіть в списку **Event List Filters** (Фільтри списку подій) пункт **HTTP**
 - 1) HTTP в цей момент вже може бути єдиною видимою подією. Натисніть кнопку **Edit Filters** (Змінити фільтри), і Ви побачите видимі події. Встановіть або зніміть прапорець **Show All / None** (Показати всі / нічого) і зверніть увагу на те, як зміниться стан встановлених і знятих прапорців.
 - 2) Натискайте на прапорець **Show All / None** до тих пір, поки всі прапорці не будуть зняті, а потім виберіть **HTTP**. Натисніть на будь-яке місце за межами поля **Edit Filters**, щоб приховати його. У розділі видимих подій тепер відображається тільки HTTP.

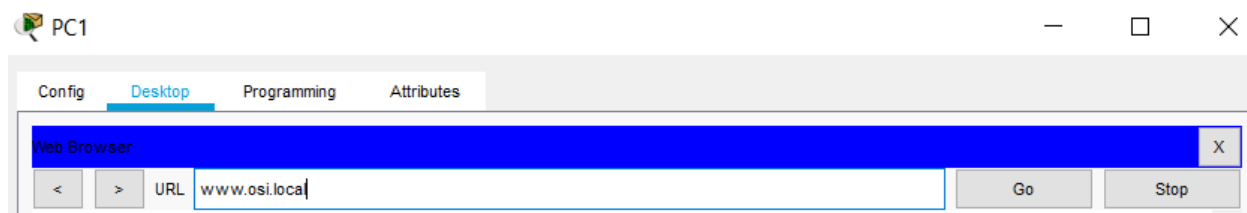


Крок 2: Згенеруйте веб-трафік (HTTP).

На даний момент панель симуляції порожня. У верхній частині панелі симуляції видно найменування п'яти стовпців списку подій. У міру генерації і просування трафіку в списку будуть з'являтися події.

Примітка. Веб-сервер і веб-клієнт показані на лівій панелі. Розмір панелі можна змінити, якщо навести покажчик на смугу прокрутки і, коли він набуде вигляду двобічної стрілки, перетягнути його вліво або вправо.

- Натисніть **Web Client** (Веб-клієнт) на крайній лівій панелі.
- Натисніть вкладку **Desktop** (Робочий стіл), потім клацніть на значок **Web Browser**, щоб відкрити веб-браузер.
- У полі **URL** введіть адресу **www.osi.local** і натисніть кнопку **Go**.



Оскільки час в режимі симуляції прив'язаний до подій, то для відображення подій в мережі необхідно використовувати кнопку **Capture / Forward** (Захоплення / вперед).

- Натисніть кнопку **Capture / Forward** чотири рази. У списку подій повинні бути чотири події.

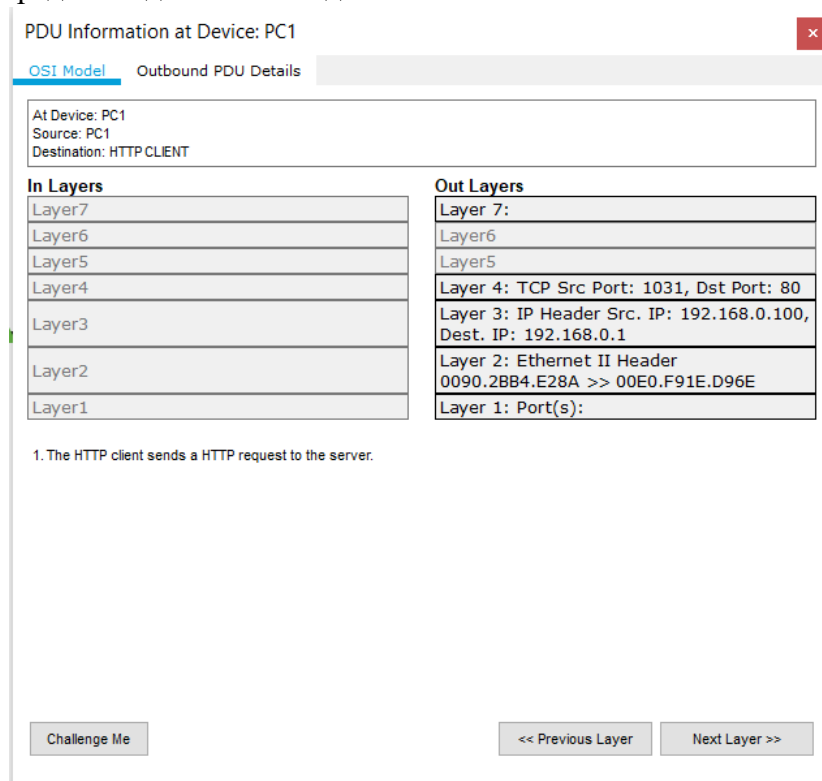
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.004	--	PC1	HTTP
	0.005	--	PC1	HTTP
	0.006	PC1	Server0	HTTP
Visible	0.007	Server0	PC1	HTTP

Подивіться на сторінку веб-клієнта в веб-браузері. Що-небудь змінилося?

Тут має бути відповідь

Крок 3: Вивчення змісту HTTP-пакету

- а. Натисніть на перший кольоровий квадрат в списку подій **Event List**. Вам може знадобитися розгорнути панель симуляції або використовувати смугу прокрутки безпосередньо під списком подій **Event List**.



Відкриється вікно **PDU Information at Device: Web Client** (Інформація про PDU на пристрої: веб-клієнт). У цьому вікні є тільки дві вкладки: **OSI Model** (Модель OSI) і **Outbound PDU Details** (Відомості про вихідну PDU), оскільки це тільки початок передачі. По мірі вивчення нових подій стануть видні три вкладки, включаючи нову вкладку **Inbound PDU Details** (Відомості про вхідну PDU). Коли подія є останньою в потоці трафіку, відображаються тільки вкладки **OSI Model** і **Inbound PDU Details**.

- б. Переконайтеся, що обрана вкладка **OSI Model**. Переконайтеся, що в стовпці **Out Layers** (Вихідні рівні) виділено поле **Layer 7** (Рівень 7).

Яка інформація перерахована в пронумерованих кроках безпосередньо під полями **In Layers** (Вхідні рівні) і **Out Layers** (Вихідні рівні)?

Тут має бути відповідь

- с. Натисніть кнопку **Next Layer** (Наступний рівень). Має бути виділений 4 рівень. Яке призначення Має параметр **DST Port** (Порт призначення)?

Тут має бути відповідь

- д. Натисніть **Next Layer** (Наступний рівень). Має бути виділений 3 рівень. Яке призначення Має параметр **Dest. IP** (IP-адреса призначення)?

Тут має бути відповідь

- e. Натисніть **Next Layer** (Наступний рівень). Яка інформація відображається на цьому рівні?

Тут має бути відповідь

- f. Натисніть на вкладку **Outbound PDU Details** (Відомості про вихідну PDU). Відомості на вкладці **PDU Details** (Відомості про PDU) відображають рівні моделі TCP / IP.

Примітка. Відомості в розділі **Ethernet II** містять ще більш докладні дані, ніж показані в розділі рівня 2 на вкладці **OSI Model**. Вкладка **Outbound PDU Details** містить більш описові і докладні відомості. Значення **DEST MAC** (MAC-адресу призначення) і **SRC MAC** (MAC-адресу джерела) в розділі **Ethernet II** на вкладці **PDU Details** відображаються на вкладці **OSI Model** в розділі Layer 2, але не вказані в якості таких.

Якщо порівняти відомості в розділі **IP** вкладки **PDU Details** з відомостями на вкладці **OSI Model**, яка інформація є для них загальною? До якого рівня вона відноситься?

Тут має бути відповідь

Якщо порівняти відомості в розділі **TCP** вкладки **PDU Details** з відомостями на вкладці **OSI Model**, яка інформація є для них загальною і до якого рівня вона відноситься?

Тут має бути відповідь

- g. Натисніть на наступний кольоровий квадрат в списку **Event List**. Активний тільки рівень 1 (не відображається сірим кольором). Пристрій витягує кадр з буфера і поміщає його в мережу.
- h. Перейдіть до наступного поля в списку подій **Event List** і натисніть на кольоровий квадрат. У цьому вікні є два стовпці: **In Layers** і **Out Layers**. Зверніть увагу на напрямок стрілки безпосередньо під стовпцем **In Layers**. Вона дивиться вгору, показуючи напрямок переміщення даних. Прокрутіть ці рівні, звертаючи увагу на переглянуті раніше елементи. У верхній частині стовпчика стрілка вказує вправо. Це означає, що сервер тепер відправляє дані назад клієнту.

Порівняйте дані в стовпці **In Layers** з даними в стовпці **Out Layers** і скажіть, в чому полягає основна відмінність між ними.

Тут має бути відповідь

ЧАСТИНА 2. ВІДОБРАЖЕННЯ ЕЛЕМЕНТІВ ПАКЕТУ ПРОТОКОЛІВ TCP/IP

У другій частині лабораторної роботи ви будете використовувати режим симуляції Packet Tracer для спостереження і вивчення роботи деяких протоколів, що входять в пакет TCP/IP.

Крок 1: Продивіться додаткові події

- b. Закрийте всі вікна з відомостями про PDU.
- c. У розділі **Event List Filters > Visible Events** (Фільтри списку подій > Видимі події) натисніть на кнопку **Show All** (показати все).
Які додаткові типи подій з'явилися в **Event List**?

Тут має бути відповідь

Ці додаткові записи грають різні ролі в пакеті протоколів **TCP / IP**. Якщо в списку вказано **ARP** (Address Resolution Protocol), то цей протокол здійснює пошук MAC-адреси. Протокол **DNS** відповідає за перетворення імен (наприклад, **www.osi.local**) в IP-адреси.

Додаткові події TCP пов'язані з встановленням з'єднань, узгодженням параметрів зв'язку і роз'єднанням сеансів зв'язку між пристроями.

В даний час Packet Tracer дозволяє охоплювати більше 35 протоколів (типів подій).

- d. Натисніть на першу подію DNS в **Event List**. Перегляньте вкладки **OSI Model** і **PDU Details** і зверніть увагу на процес інкапсуляції. На вкладці **OSI Model** з виділеним полем **Layer 7** безпосередньо під стовпцями **In Layers** і **Out Layers** відображається опис того, що відбувається. ("1. The DNS client sends a DNS query to the DNS server." [DNS-клієнт відправляє DNS-запит на DNS-сервер]) Це дуже корисна інформація, яка допомагає зрозуміти, що відбувається під час процесу зв'язку.
- e. Клацніть вкладку **Outbound PDU Details** (Відомості про вихідну PDU). Які відомості показані в полі **NAME**: в розділі DNS QUERY?

Тут має бути відповідь

- f. Натисніть на останній кольоровий квадрат DNS у списку подій. Який пристрій відображений та чому?

Тут має бути відповідь

Яке значення показано біля поля **IP**: у розділі DNS ANSWER на вкладці **Inbound PDU Details**?

Тут має бути відповідь

- g. Знайдіть першу подію **HTTP** у списку і натисніть на кольоровий квадрат події **TCP** відразу після цієї події. Виділіть **Layer 4** на вкладці **OSI Model**. Які відомості відображаються під пунктами 4 і 5 в пронумерованому списку безпосередньо під стовпцями **In Layers** і **Out Layers**?

Тут має бути відповідь

TCP поміж іншого управляє підключенням і відключенням каналу зв'язку. Ця конкретна подія показує, що канал зв'язку був встановлений.

- h. Натисніть на останню подію TCP. Виділіть Layer 4 на вкладці **OSI Model**. Перевірте дії, перелічені безпосередньо під стовпцями **In Layers** і **Out Layers**. Яка дія наведена в останньому пункті списку (4).

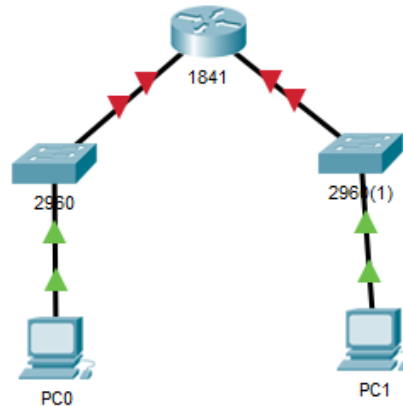
<i>Тут має бути відповідь</i>

Завдання: повторити кроки, описані вище. Як результат виконання роботи продемонструвати побудовану систему та відповіді на запитання.

Підсумок: в даній лабораторній роботі ми познайомились з такими мережевими протоколами як TCP/IP, DNS, HTTP, з рівнями моделі OSI, з хедерами та їхнім вмістом для кожного рівня моделі OSI, а також поспостерігали за рухом пакетів в мережі.

Лабораторна робота №2. Побудова мережі. Визначення MAC- та IP-адрес

Топологія:



Завдання:

1. Побудова простої мережі
2. Визначення MAC- та IP-адрес під час тестування з'єднання

Загальні відомості:

У даній вправі ми навчимося створювати просту мережу: з'єднувати між собою кінцеві та проміжні пристрої та налаштовувати їх так, щоб можна було надсилати дані. Після цього, за допомогою простої команди **ping**, ми будемо спостерігати за рухом пакета по мережі та визначимо **MAC**- та **IP**-адреси, зазначені в хедері пакета даних на кожному етапі його руху по мережі.

IP-адреса – це логічна адреса мережевого рівня (**network layer**), яка необхідна для доставки пакету даних до місця призначення.

IP-адреса складається з мережевої частини (ліва частина адреси, яка визначає, до якої мережі належить ця IP-адреса) і вузлової частини (права частина адреси, яка визначає конкретний пристрій в мережі). Мережева частина однакова для всіх пристроїв в межах однієї мережі, в той час як вузлова частина є унікальною.

Маска підмережі (**Subnet Mask**) відділяє мережеву частину адреси від вузлової. За допомогою маски підмережі здійснюється поділ на підмережі, що дозволяє «економити» IP-адреси.

Наприклад, є IP-адреса та її маска: 168.192.0.1 255.255.255.0. В даному випадку 192.168.0 визначає мережу (це мережева частина), а 1 – унікальна адреса пристрою в цій мережі (вузлова частина).

Окрім того, IP-адреса може бути статичною та динамічною. Статична адреса задається вручну, в той час як динамічна призначається автоматично DHCP сервером. Зазвичай використовується саме динамічне присвоєння адреси, проте в лабораторних роботах ми будемо користуватися статичним присвоєнням. Це полегшить навчання і допоможе уникнути певних можливих плутанин.

MAC-адреса (Media Access Control) – фізична адреса мережевої інтерфейсної плати.

Під час руху по мережі, якщо пристрої знаходяться в одній локальній мережі, пошук і транспортування здійснюється саме по MAC-адресі. IP-адреса використовується, коли пристрої знаходяться в різних мережах. У такому випадку пакет даних спочатку автоматично доправляється до маршрутизатора, а вже звідки відправляється далі. IP-адреси протягом всього руху по мережі залишаються сталими, в той час як MAC-адреси відправника і отримувача змінюються на кожній окремій ділянці транспортування.

ЧАСТИНА 1. ПОБУДОВА МЕРЕЖІ

У першій частині лабораторної роботи ви побудуєте та налаштуєте свою першу робочу мережу.

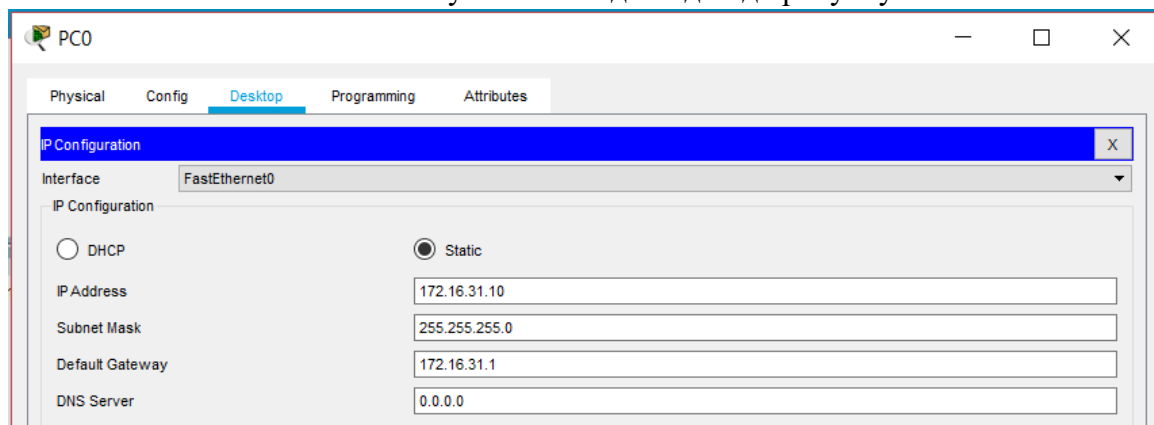
Крок 1: Створіть систему за наданою вище топологією

Зверніть увагу: обирайте саме такі маршрутизатор і комутатори, які вказані на топології, тобто маршрутизатор 1841 та комутатори 2960. Це допоможе уникнути складнощів з портами (на різних пристроях присутні різні порти. Їх можна додавати і забирати, проте це не є метою лабораторної роботи).

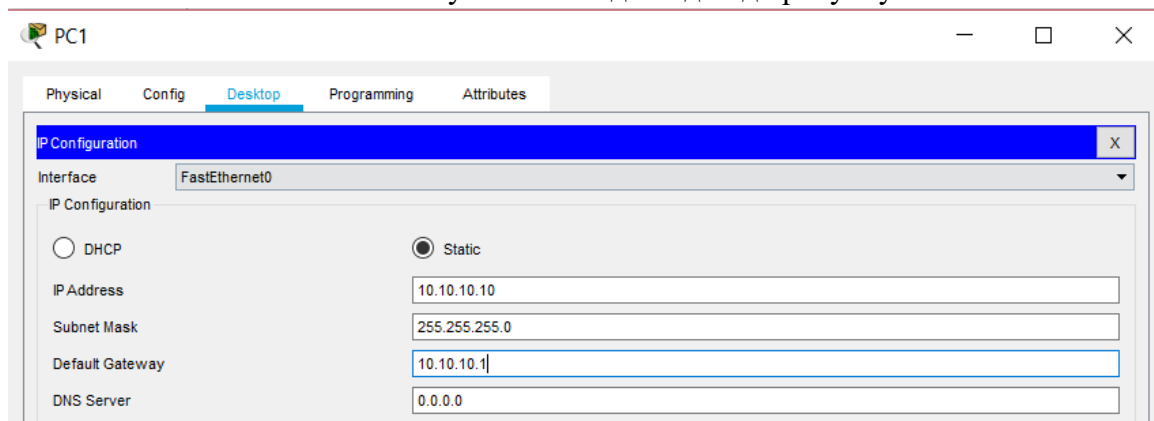
Крок 2: Налаштуйте мережу.

На даний момент, якщо ви спробуєте надіслати дані з одного ПК на інший, у вас нічого не вийде, так як ні в одного з пристроїв мережі немає адрес. Для того, щоб можна було передавати дані між пристроями, необхідно присвоїти кожному з них унікальну **IP-адресу**.

а. Клікніть на PC0. Налаштуйте його відповідно до рисунку



б. Клікніть на PC1. Налаштуйте його відповідно до рисунку



Зверніть увагу: ви щойно налаштували IP-адреси для обох ПК. Але окрім того ви приписали кожному з них адресу шлюзу за замовчуванням (**default gateway**). Це адреса інтерфейсу маршрутизатора, яка відповідає даній підмережі. Саме сюди будуть відправлятися дані, якщо адреси отримувача не знайдено в локальній мережі. Тоді це вже буде справа маршрутизатора – перенаправити пакет даних у правильному напрямку.

- с. Налаштуйте комутатори. Для цього під'єднайте один з ПК до кожного з комутаторів по черзі за допомогою консольного кабелю **Console** (як ви це робили в першій лабораторній роботі). Тепер потрібно налаштувати віртуальний інтерфейс, тобто присвоїти йому адресу. Для цього з режиму глобальної конфігурації вам потрібно перейти в режим конфігурації даного інтерфейсу. Це можна зробити за допомогою команди **interface vlan 1**. Тепер призначимо адреси за допомогою наступних команд: **ip address 172.16.31.100 255.255.255.0** та **ip address 10.10.10.100 255.255.255.0** для комутатора 2960 та 2960(1) відповідно. Далі потрібно активувати інтерфейс. Це робить за допомогою команди **no shutdown** (це потрібно зробити для обох комутаторів).

```
Switch(config)#int vl 1
Switch(config-if)#ip ad 172.16.31.100 255.255.255.0
Switch(config-if)#no sh

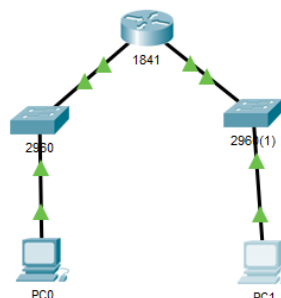
Switch(config)#int vl 1
Switch(config-if)#ip ad 10.10.10.100 255.255.255.0
Switch(config-if)#no sh
```

- д. Налаштуйте маршрутизатор. Це робиться ідентично до налаштування комутатора, тільки тепер замість введення адреси до віртуального інтерфейсу ми будемо це робити для кожного порту окремо. Під'єднайтесь за допомогою консолі до маршрутизатора та введіть наступні команди (у вас можуть відрізнятись порядкові номери інтерфейсів, все залежить від того, до якого порту який комутатор ви підключили. Головне – прослідкуйте за тим, щоб інтерфейс, якому ви назначаете IP-адресу, що починається на 172, був під'єднаний до комутатора, в якого IP-адреса віртуального інтерфейсу починається на 172. Ідентично з іншого боку – інтерфейс з початковими цифрами 10 у адресі має бути «повернутий» в сторону підмережі, в якій всі пристрої мають адреси, що починаються на 10).

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface f 0/0
Router(config-if)#ip address 172.16.31.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#exit
Router(config)#interface f 0/1
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#no shutdown
```

Тепер мережа повністю налаштована і має виглядати ось так:

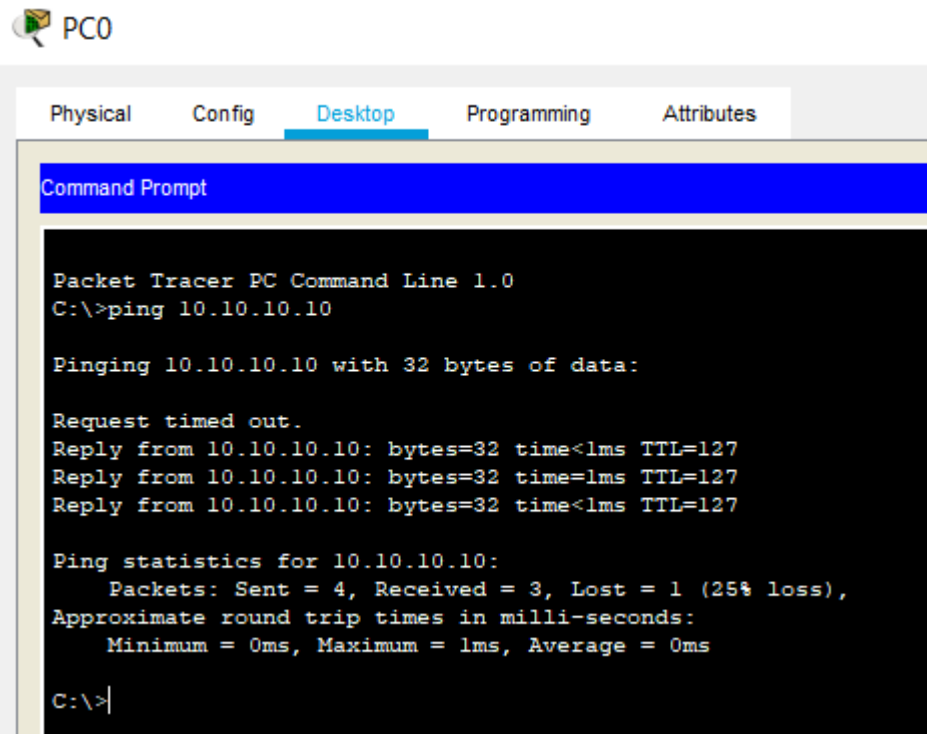


ЧАСТИНА 2. ВИЗНАЧЕННЯ MAC- ТА IP-АДРЕС

У другій частині лабораторної роботи ви протестуєте створену мережу, намагаючись пропінувати один ПК з іншого. Окрім цього, ви вивчите, як пересуватиметься пакет даних по мережі та визначите адреси на кожному етапі транспортування.

Крок 1: Пропінуйте один комп'ютер з іншого

- Клікніть на **PC0** та відкрийте вікно **Command Prompt** (Командний рядок)
- Введіть команду **ping 10.10.10.10** та дочекайтесь відповіді. Вона має мати наступний вигляд



```
Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Request timed out.
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time=1ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Таким чином ми перевірили з'єднання між двома комп'ютерами (так як пакет, відправлений одним ПК, досяг іншого і повернувся). Тепер можна перейти до збирання інформації про **MAC-** та **IP-**адреси.

- Перейдіть в режим симуляції та повторіть команду пінгування. Поряд з **PC0** має з'явитися одиниця даних протоколу (**PDU**). Натисніть на **PDU** та запишіть в таблицю, наведену в кінці лабораторної роботи, наступні дані на вкладці **Outbound PDU Layer**.
 - MAC-адреса призначення
 - MAC-адреса відправника
 - IP-адреса призначення
 - IP-адреса відправника
- Натисніть кнопку **Capture/Forward** на панелі симуляції для переміщення до наступного пристрою. Зберіть тут аналогічні дані. Повторюйте цю процедуру до тих пір, поки **PDU** не досягне **PC1**.

Команда «ping 10.10.10.10» з PC0	Пристрій	MAC-адреса призначення	MAC-адреса відправника	IP-адреса призначення	IP-адреса відправника
	PC0				
	2960				
	1841				
	2960(1)				
	PC1				

е. Дайте відповіді на наступні запитання:

Чому IP-адреси залишались сталими, в той час як MAC-адреси постійно змінювались?

Тут має бути відповідь

Чому на етапі комутаторів MAC-адреси залишились такими ж, як і на попередньому етапі,

Тут має бути відповідь

Навіщо потрібна MAC-адреса?

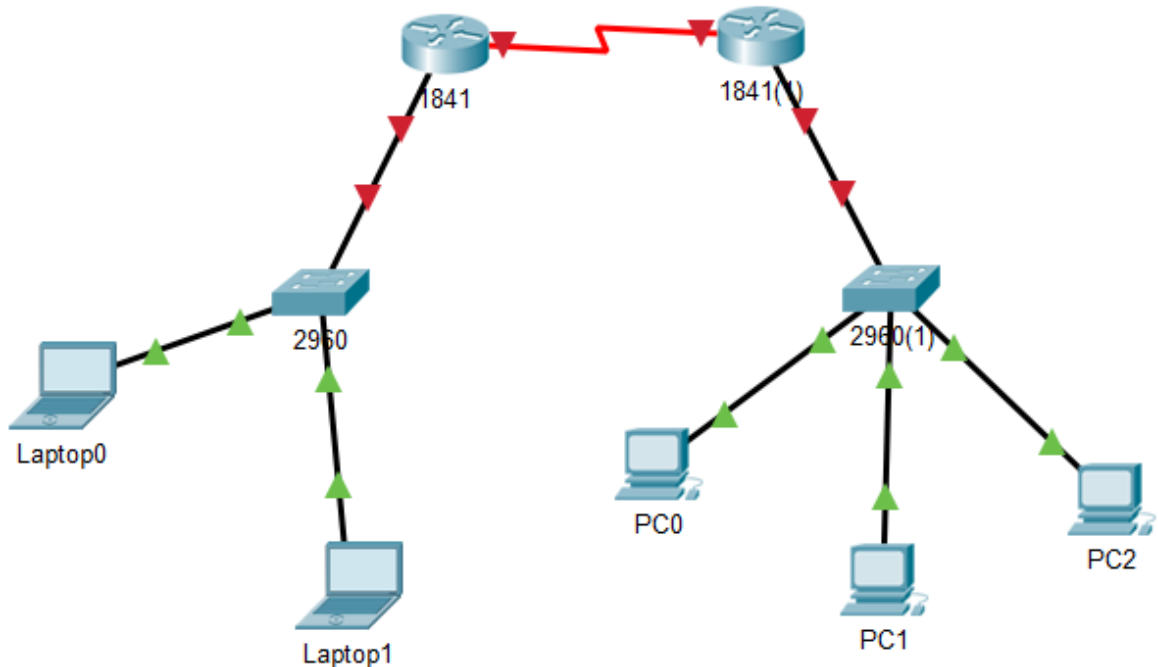
Тут має бути відповідь

Завдання: повторити кроки, описані вище. Як результат виконання роботи продемонструвати побудовану систему, заповнену таблицю та відповіді на запитання.

Підсумок: у даній лабораторній роботі ми побудували свою першу мережу, протестували її, а також спостерігали за рухом пакету даних в ній. На основі спостережень визначили IP-адреси та MAC-адреси пристроїв в мережі, а також розібрались, в чому між ними різниця.

Лабораторна робота №3. Вивчення таблиці ARP

Топологія:



Завдання:

1. Побудова складної мережі
2. Аналіз ARP-запиту

Загальні відомості:

У даній вправі ми навчимося створювати вже складнішу мережу: тут вже будуть присутні два маршрутизатора, що ускладнює рух по мережі. Навчимося налаштовувати пристрої, щоб вони могли відправляти та отримувати дані в такій мережі, окрім того, на прикладі маршрутизатора дізнаємося, як можна змінювати фізичний стан пристрою, додаючи до нього нові потрібні нам порти. Після цього, за допомогою простої команди `ping`, ми будемо спостерігати за процесом **ARP-запиту**, дізнаємося, як відбувається вивчення пристроями **MAC-адрес** інших пристроїв та вивчимо **таблицю ARP**.

ARP (address resolution protocol) – протокол, який пристрої використовують для визначення **MAC-адреси** отримувача. У цього протоколу є дві основні функції: співставлення IP-адрес з MAC-адресами та створення таблиці співставлень. Ця таблиця називається **ARP-таблицею**. Вона створюється поступово кожним пристроєм окремо по мірі відправлень пакетів даних цим пристроєм до інших пристроїв. Тобто MAC-адресу кожен пристрій дізнається при першому надсиланні даних. Цей процес називається **ARP-запитом**. Коли відповідне значення вже існує в таблиці, пристрій одразу може відправляти пакет з даними. Якщо ж отримувача немає в даній локальній мережі, дані перенаправляються на шлюз за замовчуванням (**default gateway**).

ARP-запит в своєму заголовку окрім IP-адреси призначення, MAC-адреси відправника та типу повідомлення (яке інформує, що це ARP-запит) містить MAC-адресу

призначення, яка є загальною, тобто призначається для всіх інтерфейсів Ethernet в мережі. Кожен пристрій, який отримав такий ARP-запит, мусить його обробити. Для цього він звіряє свою власну IP-адресу з тою, яка міститься в запиті, і якщо вони однакові, відправляє свою MAC-адресу пристрою, який відправив запит.

Після отримання MAC-адреси, пристрій поміщає її в свою ARP-таблицю і тепер може використовувати ці дані в майбутньому. Варто відмітити, що дані в ARP-таблиця не є постійними і мусять постійно оновлюватись.

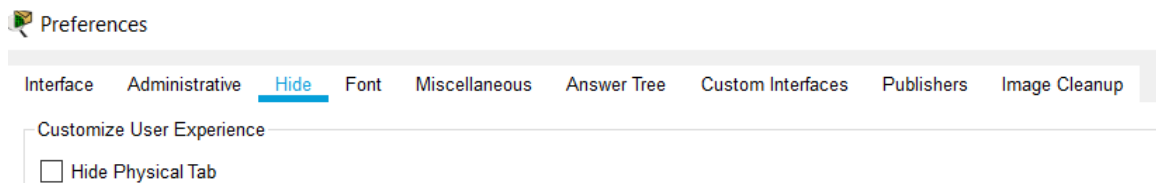
ЧАСТИНА 1. ПОБУДОВА МЕРЕЖІ

У першій частині лабораторної роботи ви побудуєте та налаштуєте мережу.

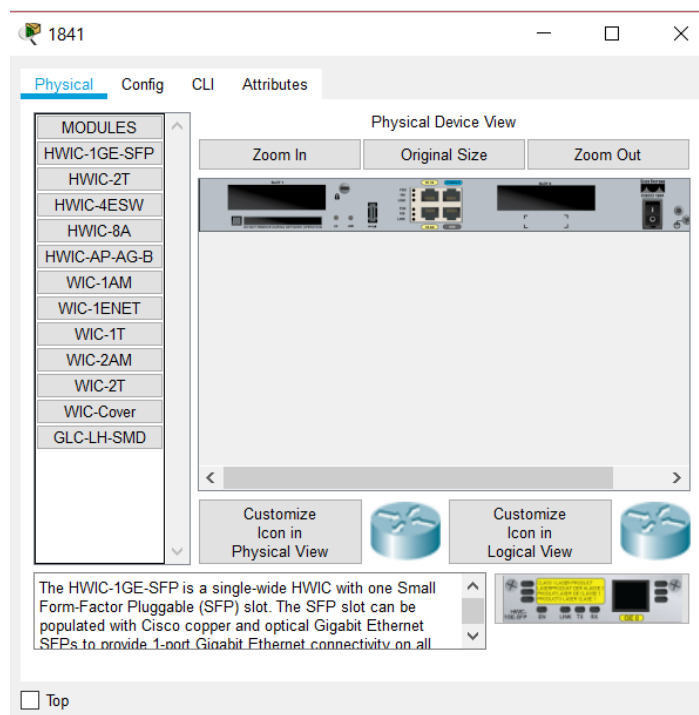
Крок 1: Створіть систему за наданою вище топологією

Зверніть увагу: обирайте саме такі маршрутизатор і комутатори, які вказані на топології, тобто маршрутизатори **1841** та комутатори **2960**. Для того, щоб з'єднати між собою два маршрутизатори необхідно використати **Serial DTE** підключення. Проте маршрутизатори за замовчуванням можуть не мати потрібних нам портів. Треба їх додати вручну. Для цього:

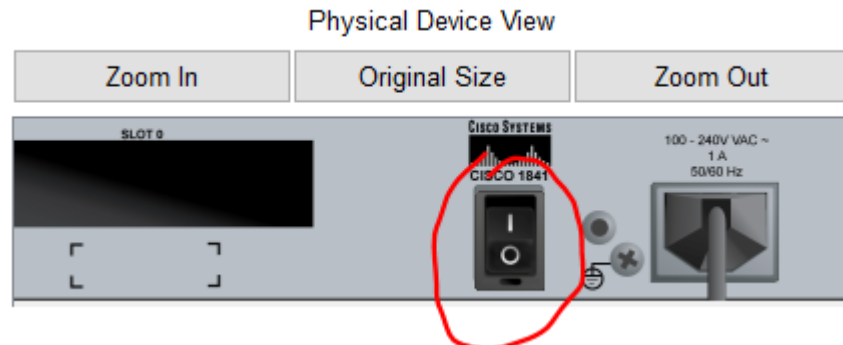
- Клікніть на маршрутизатор та перейдіть на вкладку **Physical** (ця вкладка може бути прихована, відкрити її можна, забравши галочку з **Hide Physical Tab** в **Options-Preferences-Hide**)



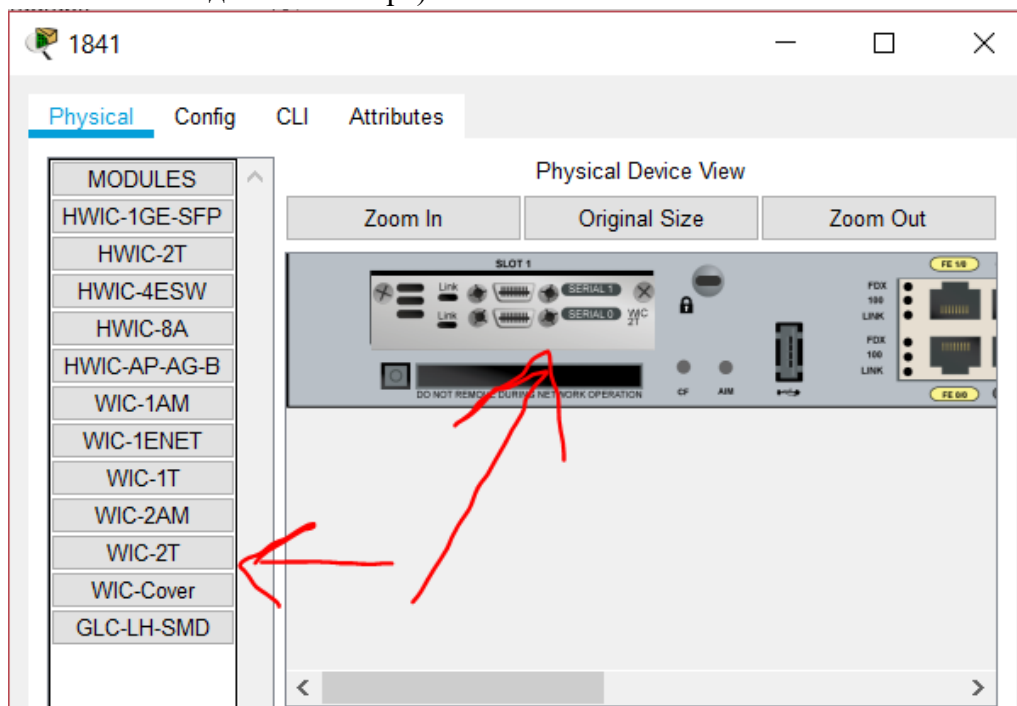
- Коли ви клікнули на вкладку **Physical**, ви можете побачити реальний фізичний вигляд маршрутизатора зі всім портами, що на ньому є. Нам потрібно додати порт **Serial**, щоб ми мали змогу використати необхідний кабель для передачі даних.



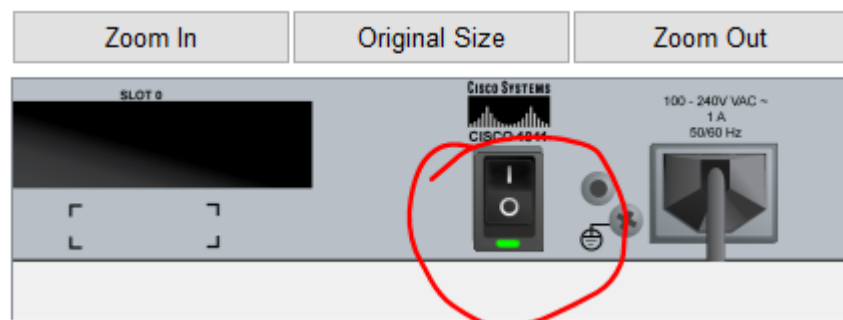
- Ви можете приближати та віддаляти рисунок для зручності, використовуючи кнопки **Zoom in** і **Zoom out**.
- Для того, щоб додати необхідні порти, треба для початку вимкнути живлення. Для цього просто натисніть на перемикач. Погасне зелений світлодіод, що розташований під ним.



- Тепер, власне, додамо порти: перенесіть модуль **WIC-2T** зі списку модулів, що розташований зліва від рисунку на рисунок маршрутизатора. Цей модуль містить два **Serial** порти (можна використати також модуль **WIC-1T**, який має лише один такий порт).



- Увімкніть живлення



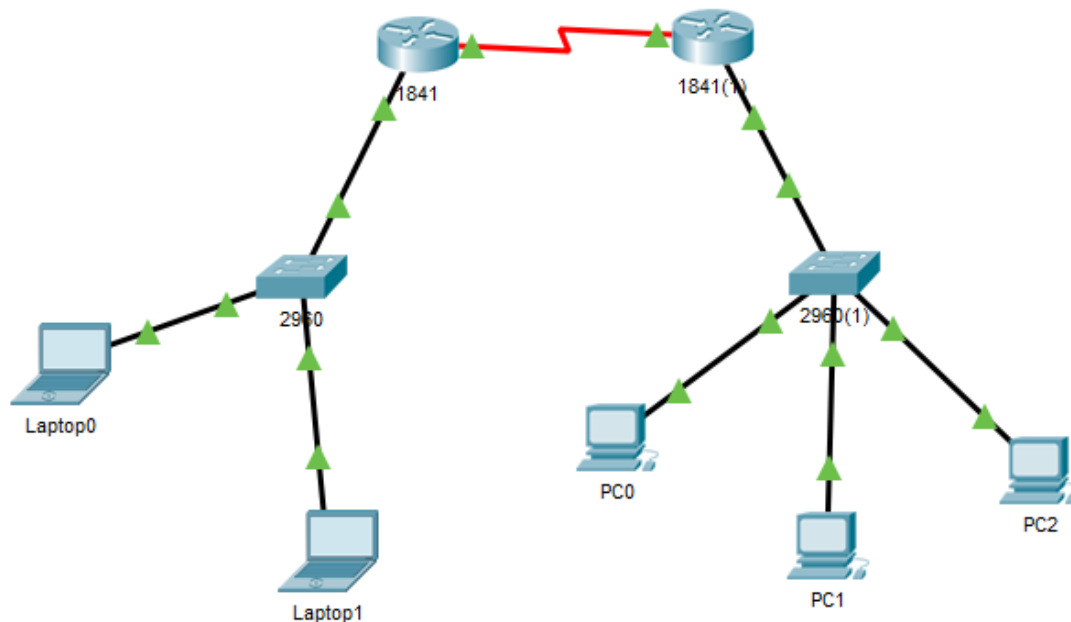
Крок 2: Налаштуйте мережу.

Використовуючи знання, набуті в попередніх лабораторних роботах, налаштуйте пристрої в мережі відповідно до наступної таблиці.

Пристрій	Порт (для проміжних пристроїв) / IP-адреса шлюзу за замовчуванням (для кінцевих пристроїв)	IP-адреса
1841	Serial	192.168.0.2 255.255.255.0
	FastEthernet0/0	172.16.31.1 255.255.255.0
1841(1)	Serial	192.168.0.1 255.255.255.0
	FastEthernet0/0	10.10.10.1 255.255.255.0
2960	Vlan 1	172.16.31.100 255.255.255.0
2960(1)	Vlan 1	10.10.10.100 255.255.255.0
Laptop0	172.16.31.1	172.16.31.10 255.255.255.0
Laptop1	172.16.31.1	172.16.31.11 255.255.255.0
PC0	10.10.10.1	10.10.10.10 255.255.255.0
PC1	10.10.10.1	10.10.10.11 255.255.255.0
PC2	10.10.10.1	10.10.10.12 255.255.255.0

Увага: не забудьте активувати інтерфейс після присвоєння йому IP-адреси (команда **no shutdown**). Окрім того, у вас не обов'язково порт на маршрутизаторі буде саме 0/0. Ви можете обрати будь-який порт **FastEthernet**.

Тепер ваша мережа має мати такий вигляд (зверніть увагу: усі позначення на з'єднаннях мають зелений колір, тобто сигнал присутній):



Залишився один крок – вказати маршрутизаторам, що робити, коли до них приходить пакет, який потрібно передати комусь з іншої мережі. Для цього необхідно клікнути на маршрутизатор та обрати вкладку **Config**. Далі переходимо на пункт **Static** в розділі **Routing**. Вказуємо наступні значення для маршрутизаторів 1841 та 1841(1) відповідно:

Static Routes		Static Routes	
Network	0.0.0.0	Network	0.0.0.0
Mask	0.0.0.0	Mask	0.0.0.0
Next Hop	192.168.0.1	Next Hop	192.168.0.2
<input type="button" value="Add"/>		<input type="button" value="Add"/>	

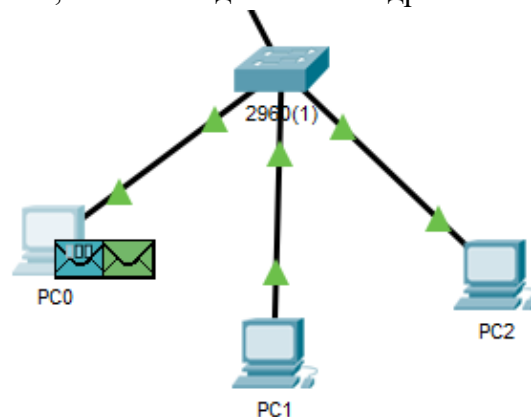
Далі натискаємо кнопку **Add** і закриваємо налаштування маршрутизатора. Готово! Тепер наша мережа є абсолютно дієспроможною. Це можна перевірити за допомогою, наприклад, команди **ping**.

ЧАСТИНА 2. АНАЛІЗ ARP-ЗАПИТУ

У другій частині лабораторної роботи ви протестуєте створену мережу, намагаючись пропінувати один ПК з іншого. Окрім цього, ви вивчите, як працює протокол **ARP**, як здійснюється **ARP-запит** та як виглядає **ARP-таблиця**.

Крок 1: Пропінуйте один комп'ютер з іншого

- Клікніть на PC0 та відкрийте вікно **Command Prompt** (Командний рядок).
- Введіть команду **arp -d**, щоб очистити **ARP**-таблицю.
- Перейдіть в режим симуляції та введіть команду **ping 172.16.31.10**. Мають з'явитися дві одиниці даних: протоколу **ARP** та протоколу **ICMP**. **ICMP**-пакет не може бути відправлений, так як невідома MAC-адреса.



- Натисніть кнопку **Capture/Forward** на панелі симуляції для переміщення до наступного пристрою. Як бачимо, ARP-пакет перемістився далі, в той час як **ICMP**-пакет зник. Насправді він просто очікує, поки повернеться ARP-пакет з потрібною MAC-адресою.
- Натисніть кнопку **Capture/Forward** на панелі симуляції для переміщення до наступного пристрою. Скільки копій запиту створив комутатор та чому?

Тут має бути відповідь

- Натискайте кнопку **Capture/Forward** поки пакет не повернеться до відправника. До якого пристрою дійшов запит? Скільки копій пакету зробив комутатор цього разу?

Тут має бути відповідь

- g. Зверніть увагу, що знову з'явився **ICMP** пакет. Натисніть на **ARP**-пакет, зайдіть у вкладку **Inbound PDU Details** та подивіться на **Source Mac**. А тепер натисніть на маршрутизатор, вкладка **Config**, та оберіть серед інтерфейсів той, до якого підключений комутатор. Чи співпадає MAC-адреса цього інтерфейсу з з тою, яка зазначена у відповіді **ARP**-запиту? Що це означає?

Тут має бути відповідь

- h. Поверніться назад в режим реального часу – команда **ping** завершиться. Натисніть на ПК, з якого був відправлений запит та виконайте в командному рядку команду **arp -a**. IP- та MAC-адреси якого пристрою містяться у виведеній таблиці?

Тут має бути відповідь

- i. Тепер виконайте команду **ping 10.10.10.11**, а потім знову **arp -a**. Що змінилося в таблиці?

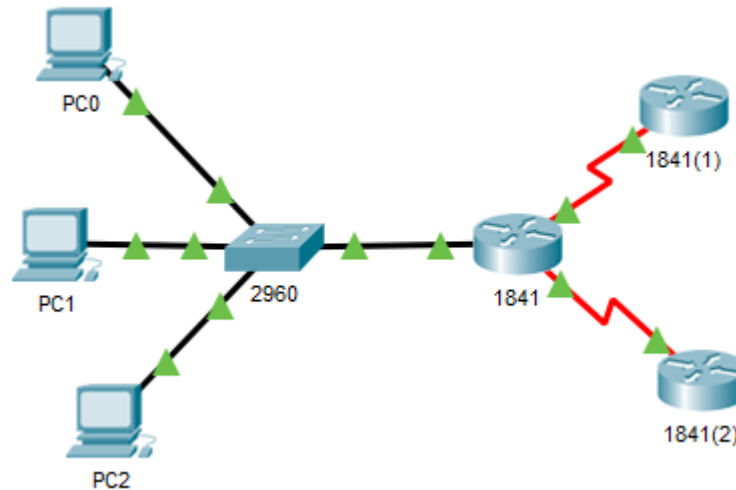
Тут має бути відповідь

Завдання: повторити кроки, описані вище. Як результат виконання роботи продемонструвати побудовану систему та відповіді на запитання.

Підсумок: у даній лабораторній роботі ми побудували мережу, що складається з кількох підмереж та протестували з'єднання між пристроями з різних мереж. У процесі тестування ми познайомилися з **ARP** протоколом та вивчили навіщо він потрібен і як працює.

Лабораторна робота №4. Аналіз трафіку одноадресної та загальної розсилки

Топологія:



Завдання:

1. Побудувати мережу
2. Генерація трафіку одноадресної розсилки
3. Генерація трафіку загальної розсилки

Загальні відомості:

В даній вправі ми дізнаємось, що таке одноадресна, багатоадресна та загальна розсилка та проаналізуємо перші дві з них. Ми навчимося генерувати комплексні пакети даних та за допомогою одного такого створимо загальну розсилку.

Пристрої в мережі можуть обмінюватись даними один з одним трьома різними способами:

- Одноадресною розсилкою
- Багатоадресною розсилкою
- Загальною розсилкою

Одноадресна розсилка (**Unicast**) – процес відправлення пакету з одного вузла на інший конкретний вузол. Використовується для самої звичайної передачі даних між двома вузлами.

Багатоадресна розсилка (**Multicast**) – процес відправлення пакету з одного вузла групі вузлів, які можуть знаходитись в різних мережах. В якості отримувача вказується IP-адреса групи, для якої зарезервовані адреси від 224.0.0.0 до 239.255.255.255, з яких з 224.0.0.0 до 224.0.0.255 – для багатоадресної розсилки в межах однієї мережі. Вузол отримує пакет, адресований на групову адресу, якщо підписується на відповідну групу.

Загальна розсилка (**Broadcast**) – процес відправлення пакету з одного вузла всім іншим вузлам в мережі. Для цього в якості адреси отримувача використовується 255.255.255.255. Маршрутизатори за замовчуванням не пересилають загальні розсилки.

ЧАСТИНА 1. ПОБУДОВА МЕРЕЖІ

У першій частині лабораторної роботи ви побудуєте та налаштуєте мережу.

Крок 1: Створіть та налаштуйте систему

Використовуючи отримані в минулих лабораторних роботах знання, побудуйте та налаштуйте систему відповідно до топології та наступної таблиці адрес:

Пристрій	Порт (для проміжних пристроїв) / IP-адреса шлюзу за замовчуванням (для кінцевих пристроїв)	IP-адреса
1841	Serial 0/1/0	10.0.2.1 255.255.255.0
	Serial 0/1/1	10.0.3.1 255.255.255.0
	FastEthernet0/0	10.0.1.1 255.255.255.0
1841(1)	Serial 0/1/0	10.0.2.2 255.255.255.0
1841(2)	Serial 0/1/1	10.0.3.2 255.255.255.0
2960	Vlan 1	10.0.1.100 255.255.255.0
PC0	10.0.1.1	10.0.1.2 255.255.255.0
PC1	10.0.1.1	10.0.1.3 255.255.255.0
PC2	10.0.1.1	10.0.1.4 255.255.255.0

Увага: не забудьте активувати інтерфейси після присвоєння їм IP-адреси (команда **no shutdown**). Окрім того, у вас не обов'язково порти на маршрутизаторах будуть мати саме наведені у таблиці номери. Ви можете обрати будь-які доступні порти. Окрім того, не забудьте вказати для маршрутизаторів дані про наступну зупинку, як це було показано в попередній лабораторній роботі (частина 1 крок 2).

ЧАСТИНА 2. АНАЛІЗ ОДНОАДРЕСНОЇ ТА ЗАГАЛЬНОЇ РОЗСИЛОК

У другій частині лабораторної роботи ви протестуєте створену мережу, намагаючись пропінувати один ПК з іншого. Окрім цього, ви вивчите, як працює протокол ARP, як здійснюється ARP-запит та як виглядає ARP-таблиця.

Крок 1: Проаналізуйте одноадресну розсилку

- Клікніть на PC0 та відкрийте вікно **Command Prompt** (Командний рядок).
- Введіть команду **ping 10.0.3.2**. Виконання має закінчитися успішно.
- Перейдіть в режим симуляції, у фільтрі (**Edit Filters**) на панелі симуляції оберіть **ICMP** та введіть на PC0 команду **ping 10.0.3.2**. Натискайте кнопку **Capture/Forward** поки пакет не повернеться до відправника. Через які пристрої пройшов пакет? Натисніть на пакет та подивіться інформацію про нього. З якого рівня починається передача (які рівні моделі **OSI** є доступними) та чому?

Тут має бути відповідь

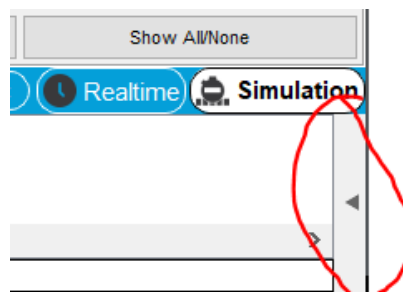
- Натисніть кнопку **Reset Simulation**.

Крок 2: Проаналізуйте загальну розсилку

- a. Додамо складну **PDU**. Для цього натисніть кнопку **Add Complex PDU** в панелі інструментів зверху.



- b. Натисніть на PC0, відкриється діалогове вікно **Create Complex PDU**.
- c. У вікні, яке відкриється, введіть наступні значення:
- IP-адреса призначення (**Destination IP Address**): 255.255.255.255
 - Порядковий номер (**Sequence Number**): 1
 - Час одноразової події (**One Shot Time**): 0
- d. Натисніть **Create PDU**. Вікно зачиниться, а біля ПК з'явиться пакет даних. Окрім цього цей пакет повинен з'явитися в **Event List** та у вікні **PDU List** (якщо у вас такого вікна немає, його можна відкрити за допомогою стрілки в нижньому лівому краю)



- e. Двічі натисніть кнопку **Capture/Forward**. Спочатку пакет переміститься на комутатор, а потім утвориться три копії, кожна з яких піде в різному напрямку: на два ПК та на маршрутизатор. Вивчіть дані третього рівня для всіх подій. Якою є IP-адреса отримувача у кожного з них та чому?

Тут має бути відповідь

- f. Ще раз натисніть кнопку **Capture/Forward**. Чи пересилається пакет на інші маршрутизатори? Чому?

Тут має бути відповідь

- g. Видалити пакет після його вивчення можна, натиснувши на **Delete** під **Scenario 0** в **PDU List**.

Завдання: повторити кроки, описані вище. Як результат виконання роботи продемонструвати побудовану систему та відповіді на запитання.

Підсумок: у даній лабораторній роботі згенерували одноадресну та загальну розсилку та вивчили як і навіщо вона використовується. Окрім того, ми навчилися створювати складні PDU в Cisco Packet Tracer.