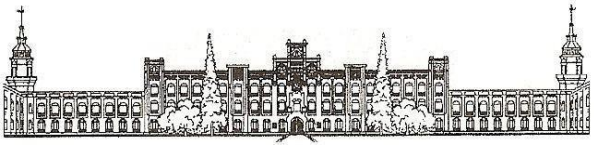


Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут»

Лабораторна робота №6

з дисципліни «Комп'ютерні мережі»

«Засвоєння принципів перетворення DNS-імен в IP-адреси»

Виконала студентка групи: КВ-11

ПІБ: Михайліченко Софія Віталіївна

Перевірив: _____

Київ 2024

Мета роботи:

Використовуючи програму моделювання комп’ютерних мереж засвоїти принципи адресації на канальному та мережевому рівнях моделі OSI, принципи динамічного призначення IP-адрес і принципів перетворення DNS-імен в IP-адреси.

План виконання лабораторної роботи:

Завдання №1. Побудова локальної мережі з двома робочими станціями.

Завдання №2. Засвоєння принципів адресації на канальному і мережевому рівнях.

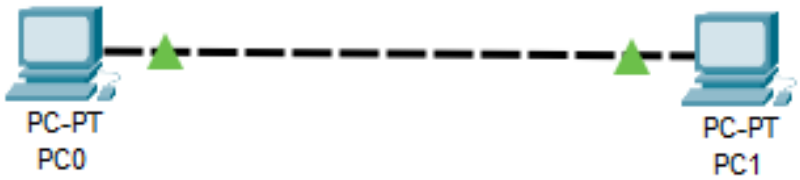
Завдання №3. Засвоєння принципів динамічного призначення IP-адрес.

Завдання №4. Засвоєння принципів перетворення DNS-імен в IP-адреси.

Завдання №5. Ознайомлення з відомостями про структуру перехресного кабеля.

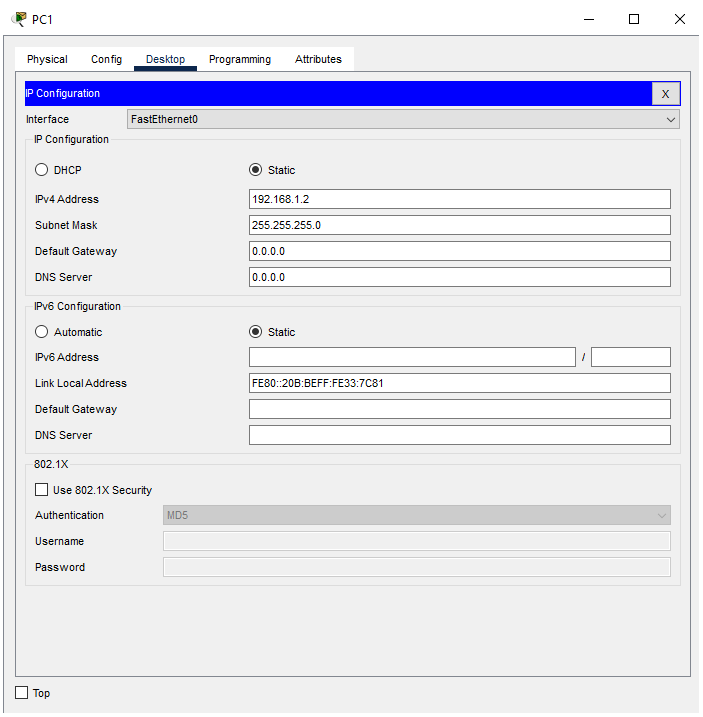
Порядок виконання роботи:

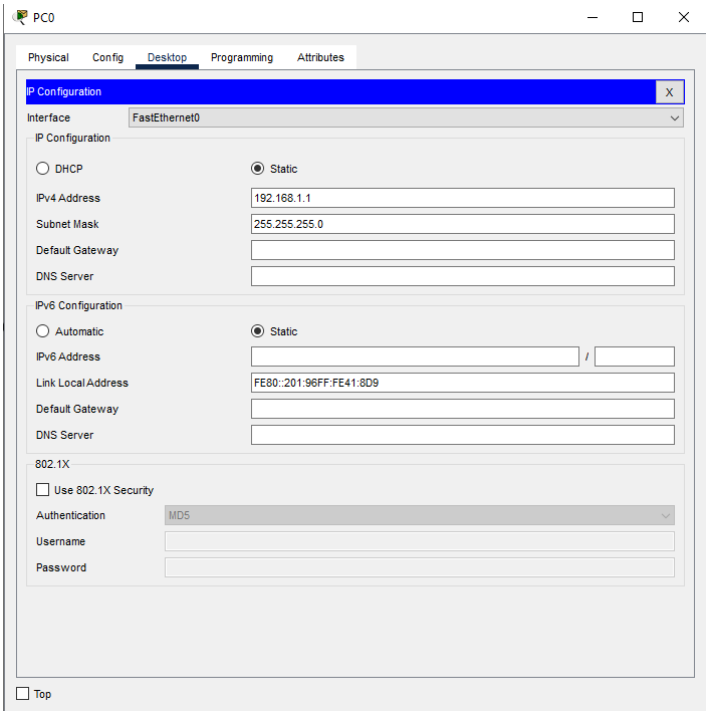
Завдання №1. Побудова локальної мережі з двома робочими станціями



Як ми можемо побачити, що з’єднання між робочими станціями відбулося, адже засвітилися зелені індикатори link.

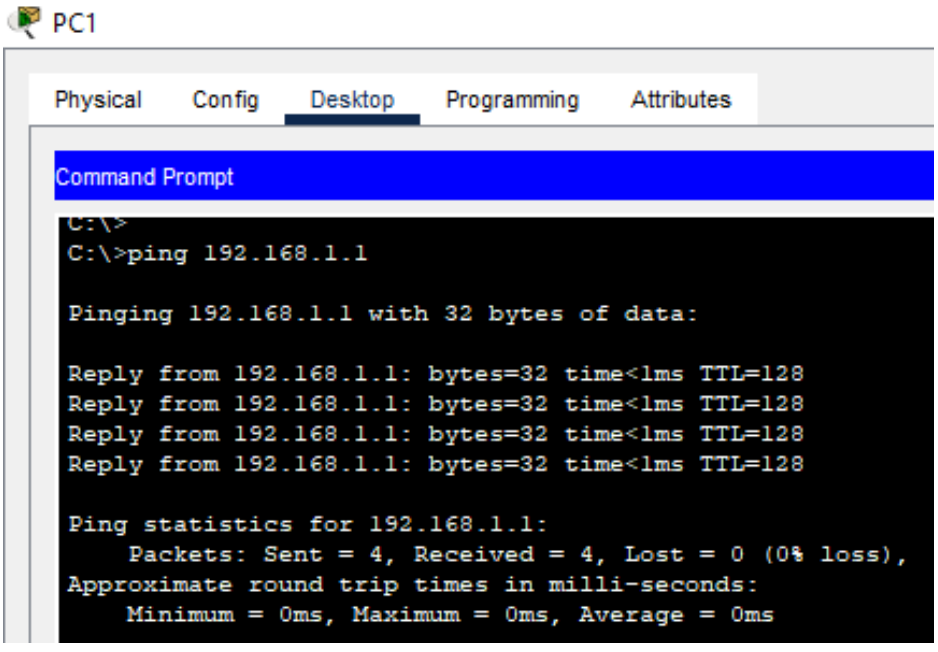
Тепер потрібно вказати статичну IP-адресу комп’ютера:



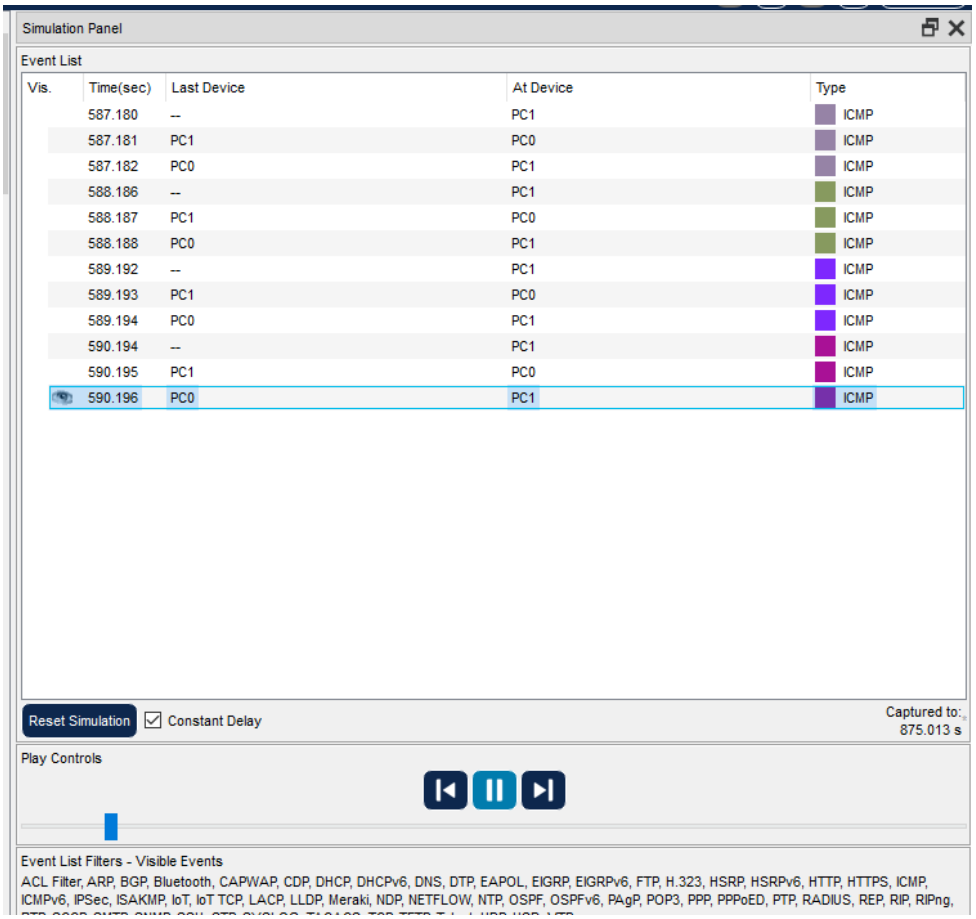


Тепер на другій робочій станції вибрати режим Command Promt:

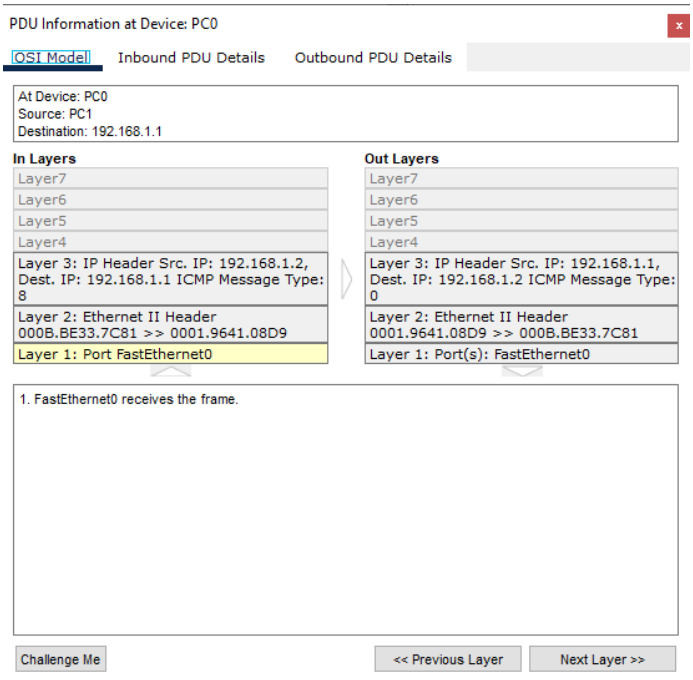
Виконаємо команду ping 192.168.1.1, в результаті виконання якої видно, що зв’язок між робочими станціями встановлений.



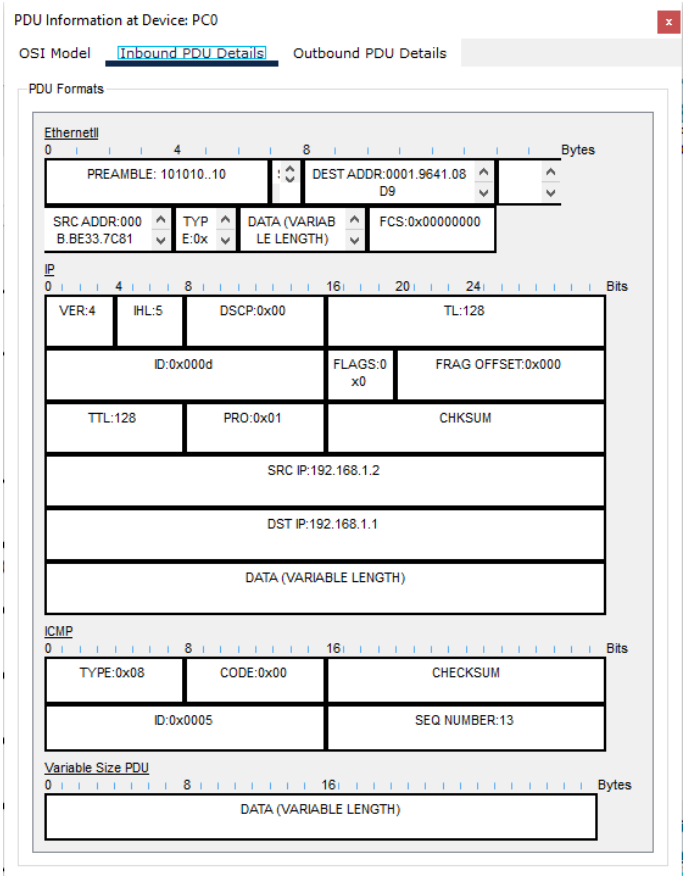
В режимі симуляції відслідковуємо протоколи, які надсилаються до PC0 за допомогою команди ping 192.168.1.1:

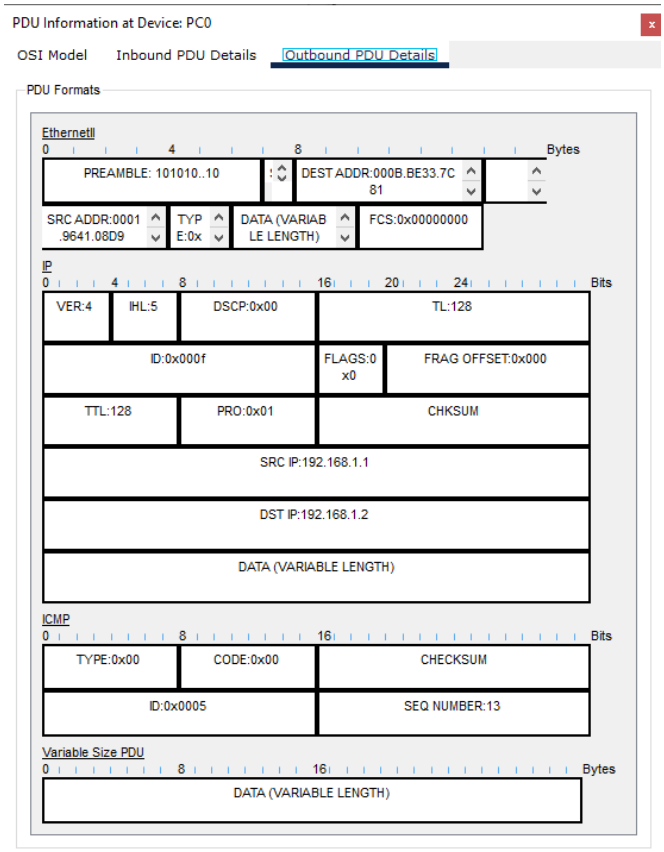


Моніторимо рух пакетів на основі моделі OSI:



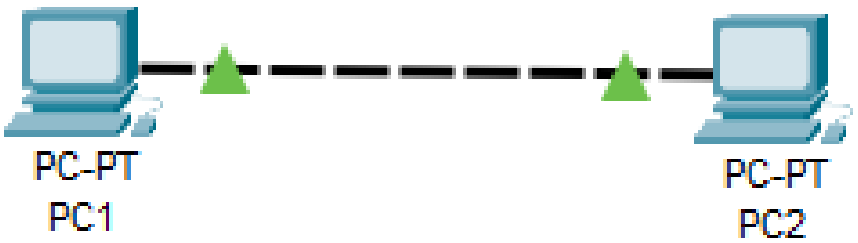
Структура вхідного і вихідного пакету:



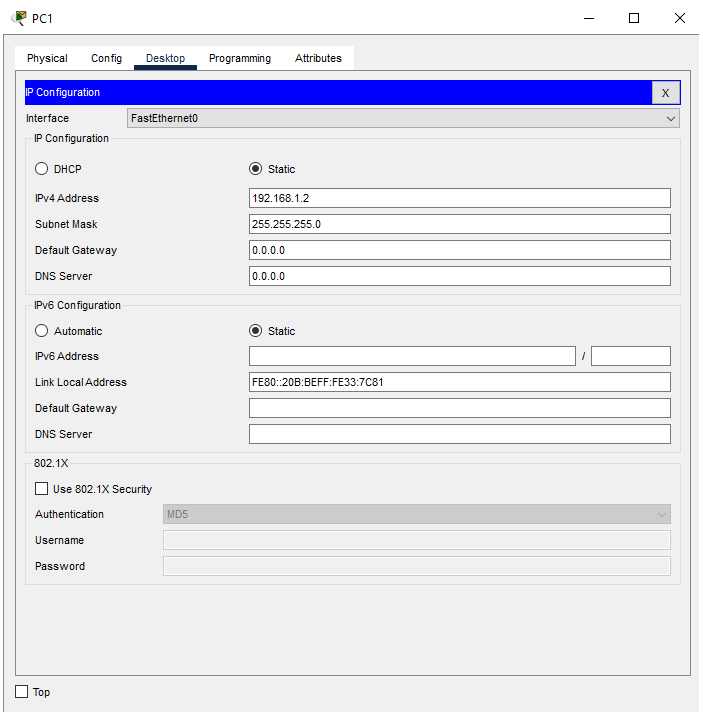


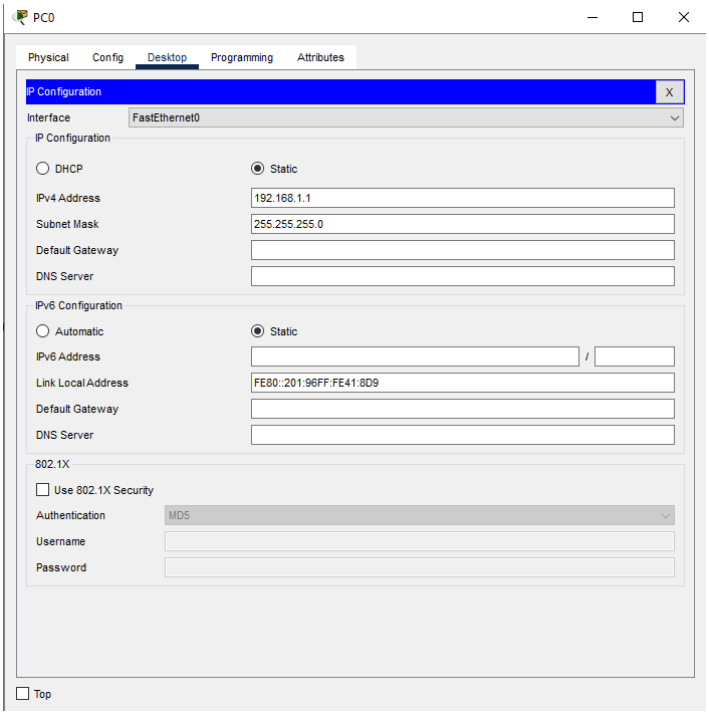
Завдання №2. Засвоєння принципів адресації на канальному і мережевому рівнях.

1. Побудова моделі мережі та присвоєння ip-адрес 192.168.1.1 та 192.168.1.2 до приладів PC1 та PC2 відповідно:

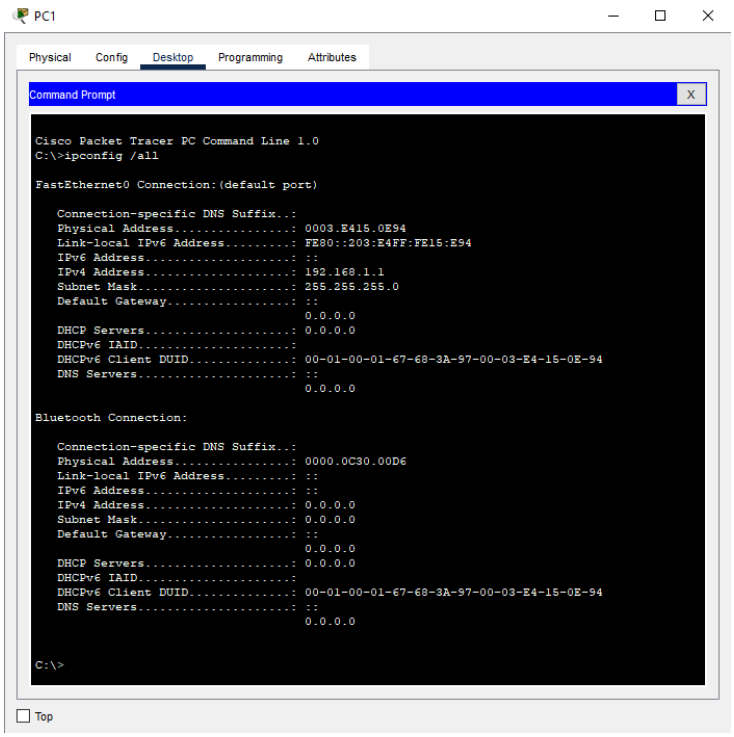


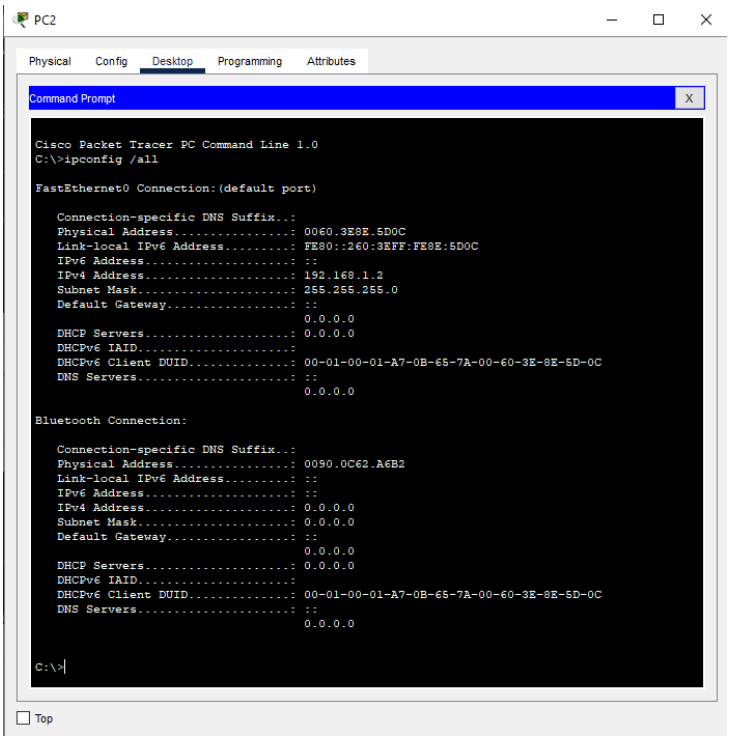
2. Призначити робочим станціям IP-адреси та маску. Перші три байти IP-адрес збігаються з адресою мережі, а останній байт дорівнює відповідно 1 та 2:





3. Визначити MAC-адресу кожної робочої станції за допомогою команди **ipconfig /all** з командного рядка:





4. На робочій станції PC1 з командного рядка виконати команду arp –a. Зафіксувати отриманий результат:

```
C:\> arp -a
No ARP Entries Found
C:\>
```

5. На робочій станції PC1 з командного рядка виконати команду ping на адресу станції PC2, після чого знову виконати команду arp –a. Пояснити отриманий результат.:

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.2           0060.3e8e.5d0c        dynamic

C:\>
```

Початкова перевірка таблиці ARP командою arp -a показала, що таблиця була порожньою: *"No ARP Entries Found"*. Це очікувано, оскільки ще не надсилалися запити до інших пристроїв у мережі, і відповідно жодних відповідностей між IP- та MAC-адресами не було збережено.

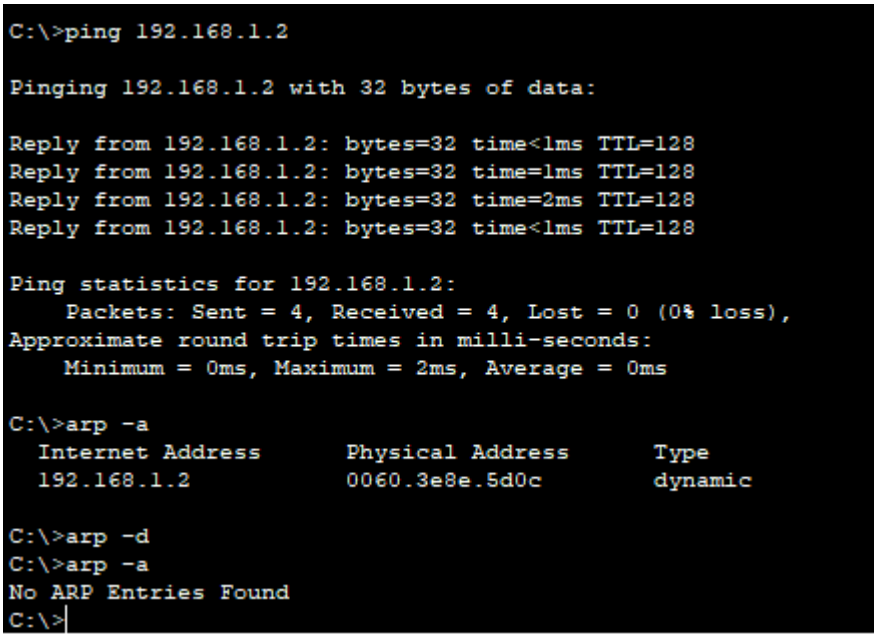
Наступним кроком було надсилання запиту до пристрою з IP-адресою 192.168.1.2 за допомогою команди ping. Результат показав, що пристрій відповів на всі чотири пакети з мінімальною затримкою (<1 мс). Це підтвердило, що пристрій доступний і знаходиться в межах локальної мережі (LAN).

Після успішного виконання ping, було виконано команду arp -a, щоб перевірити зміни у таблиці ARP. Цього разу таблиця містила запис:

- **Internet Address:** 192.168.1.2 (IP-адреса пристрою).
- **Physical Address:** 0060.3e8e.5d0c (MAC-адреса пристрою).
- **Type:** dynamic (запис було створено автоматично).

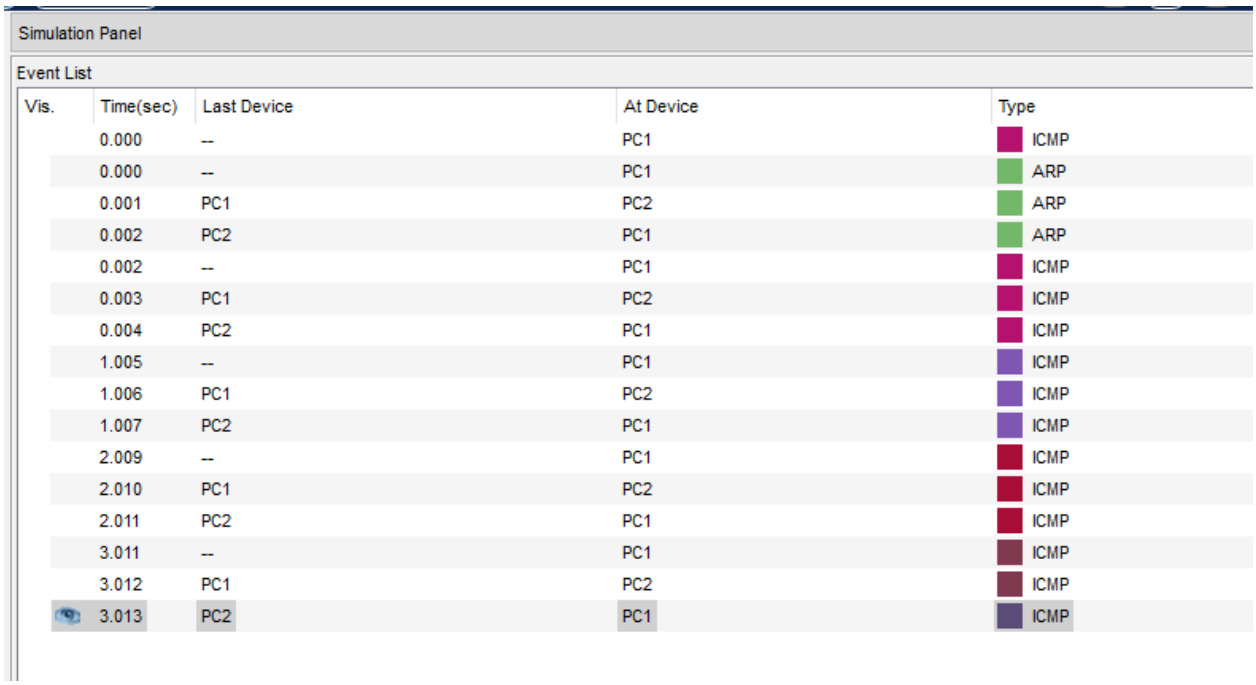
Цей результат показав, що ARP-запит спрацював, і тепер PC1 "знає", як знайти пристрій 192.168.1.2 у мережі, використовуючи його MAC-адресу.

6. На робочій станції PC1 з командного рядка виконати команду arp –d. Пояснити призначення ключа –d:



Ключ -d у команді arp використовується для видалення записів з таблиці ARP.

7. Перейти в режим Simulation. Із командного рядка робочої станції PC1 виконати команду ping на IP-адресу станції PC2. На «Simulation panel» натиснути кнопку «CaptureForward». Пояснити призначення пакетів, що відправляються зі станції PC1. Натиснути кнопкою миші на кожному із створених пакетів і переглянути їх вміст. Звернути увагу на адреси відправника та отримувача. Натискаючи на «CaptureForward» прослідкувати за формуванням та передачею створених пакетів мережею, одночасно спостерігаючи за командним рядком. Пояснити призначення ARP-пакету.



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.000	--	PC1	ARP
	0.001	PC1	PC2	ARP
	0.002	PC2	PC1	ARP
	0.002	--	PC1	ICMP
	0.003	PC1	PC2	ICMP
	0.004	PC2	PC1	ICMP
	1.005	--	PC1	ICMP
	1.006	PC1	PC2	ICMP
	1.007	PC2	PC1	ICMP
	2.009	--	PC1	ICMP
	2.010	PC1	PC2	ICMP
	2.011	PC2	PC1	ICMP
	3.011	--	PC1	ICMP
	3.012	PC1	PC2	ICMP
	3.013	PC2	PC1	ICMP

ARP-пакети

- 0.000 сек: PC1 ініціює ARP-запит, щоб визначити MAC-адресу пристрою PC2, який має відповідну IP-адресу.
- 0.001 сек: ARP-запит передається від PC1 до PC2.
- 0.002 сек: PC2 відповідає на ARP-запит, відправляючи свою MAC-адресу назад до PC1.

Призначення ARP-пакетів:

ARP (Address Resolution Protocol) використовується для встановлення відповідності між IP-адресою (рівень 3, мережевий рівень) та MAC-адресою (рівень 2, канальний рівень). Це необхідно для доставки пакетів у локальній мережі.

ICMP-пакети

- **0.002 сек:** Перший ICMP Echo Request (ping) відправляється з PC1 до PC2. Він перевіряє доступність станції PC2.
- **0.003 сек:** PC2 отримує ICMP Echo Request і відповідає ICMP Echo Reply.
- Наступні серії ICMP-пакетів (1.005, 2.009, 3.011 сек) відповідають додатковим спробам ping і обміну між PC1 та PC2.

Призначення ICMP-пакетів:

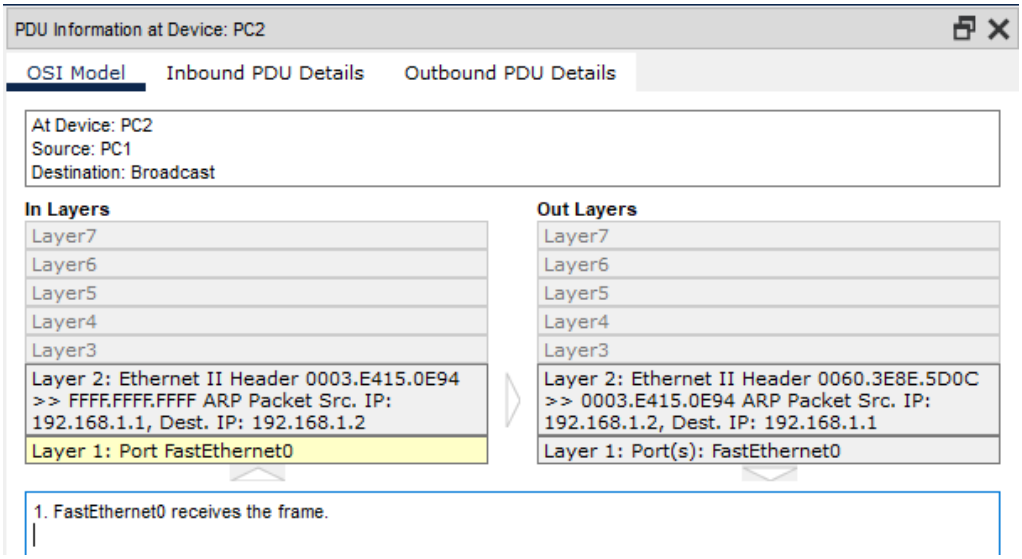
ICMP (Internet Control Message Protocol) використовується для діагностики мережевих проблем. Зокрема, ping перевіряє:

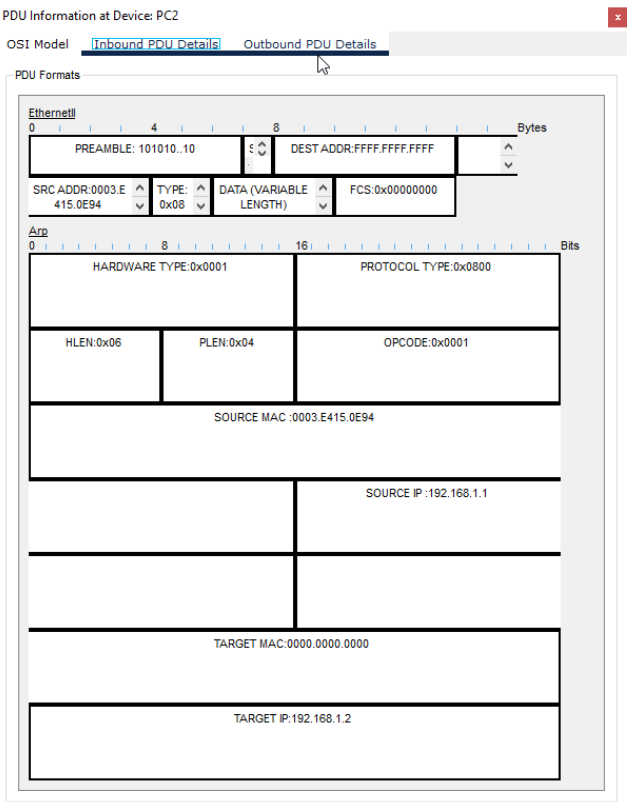
1. Доступність вузла (чи отримано відповідь).
2. Час передачі пакета (RTT - round trip time).

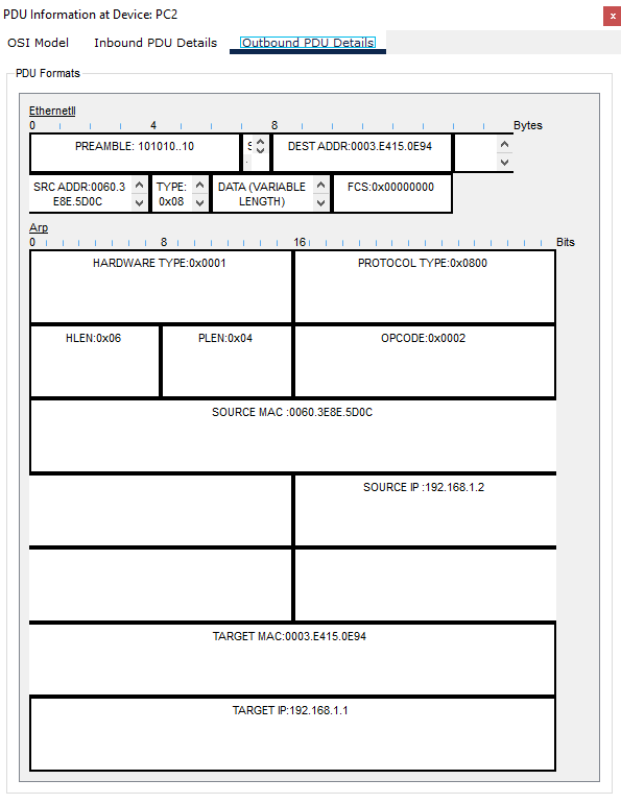
ARP-запити відбуваються лише один раз, оскільки інформація кешується в ARP-таблиці.

ICMP-пакети продовжують обмінюватися для кожного запиту ping, відображаючи затримку (RTT) між станціями.

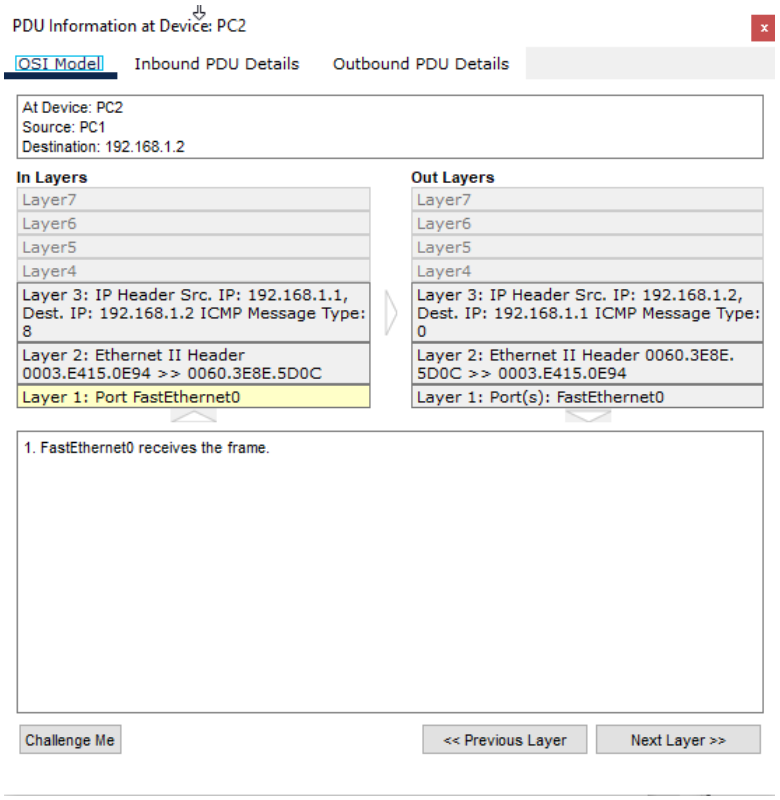
ARP:

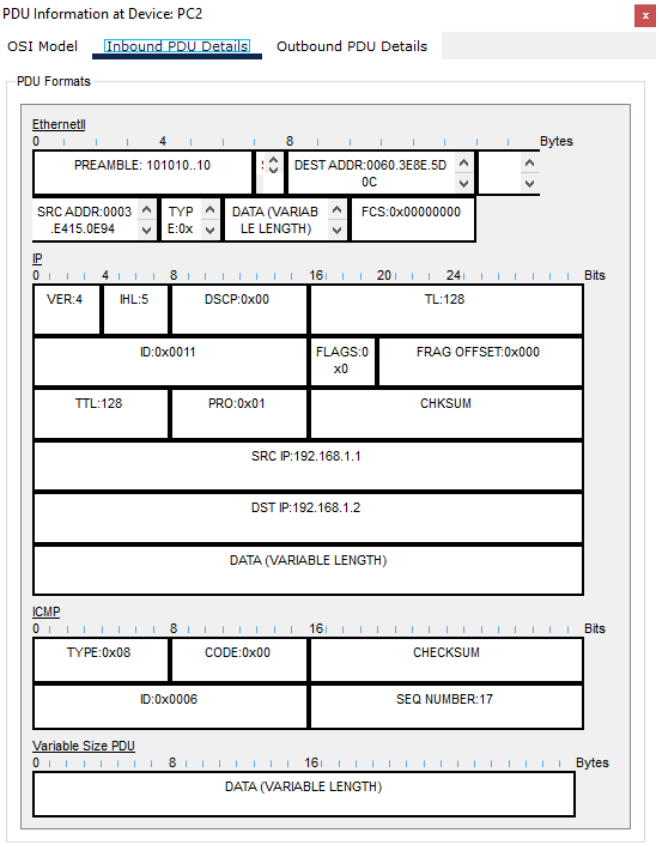


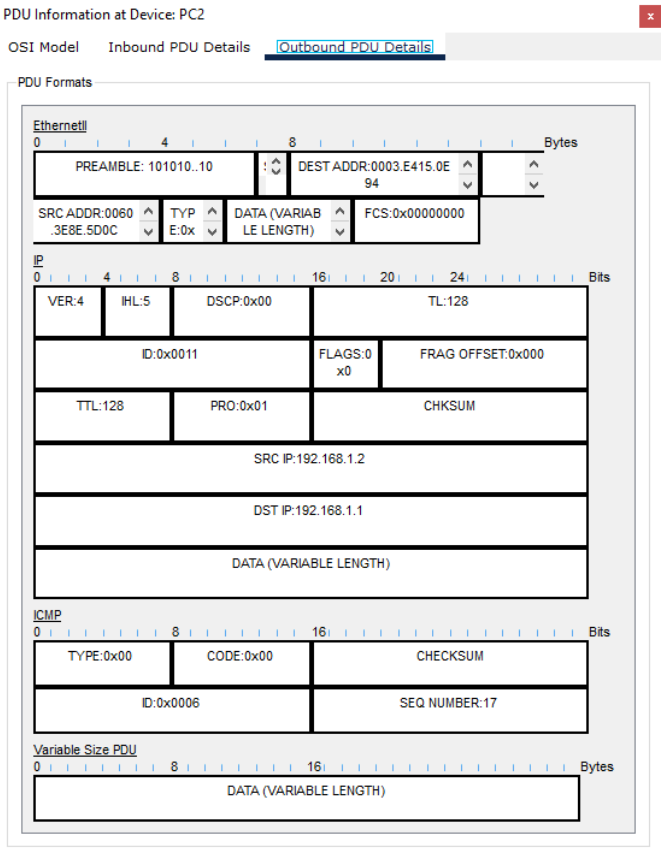




ICMP:

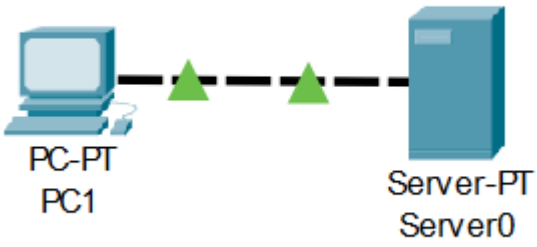

PDU Information at Device: PC2
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: PC2
Source: PC1
Destination: 192.168.1.2
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.2 ICMP Message Type: 8
Layer 2: Ethernet II Header 0003.E415.0E94 >> 0060.3E8E.5D0C
Layer 1: Port FastEthernet0
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.1.1 ICMP Message Type: 0
Layer 2: Ethernet II Header 0060.3E8E.5D0C >> 0003.E415.0E94
Layer 1: Port(s): FastEthernet0
1. FastEthernet0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>


PDU Information at Device: PC2
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
EthernetII
PREAMBLE: 101010..10
DEST ADDR:0060.3E8E.5D0C
SRC ADDR:0003.E415.0E94
TYPE:0x
DATA (VARIABLE LENGTH)
FCS:0x00000000
IP
VER:4
IHL:5
DSCP:0x00
TL:128
ID:0x0011
FLAGS:0x0
FRAG OFFSET:0x000
TTL:128
PRO:0x01
CHKSUM
SRC IP:192.168.1.1
DST IP:192.168.1.2
DATA (VARIABLE LENGTH)
ICMP
TYPE:0x08
CODE:0x00
CHECKSUM
ID:0x0006
SEQ NUMBER:17
Variable Size PDU
DATA (VARIABLE LENGTH)


PDU Information at Device: PC2
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
EthernetII
PREAMBLE: 101010..10
DEST ADDR:0003.E415.0E94
SRC ADDR:0060.3E8E.5D0C
TYPE:0x
DATA (VARIABLE LENGTH)
FCS:0x00000000
IP
VER:4
IHL:5
DSCP:0x00
TL:128
ID:0x0011
FLAGS:0x0
FRAG OFFSET:0x000
TTL:128
PRO:0x01
CHKSUM
SRC IP:192.168.1.2
DST IP:192.168.1.1
DATA (VARIABLE LENGTH)
ICMP
TYPE:0x00
CODE:0x00
CHECKSUM
ID:0x0006
SEQ NUMBER:17
Variable Size PDU
DATA (VARIABLE LENGTH)

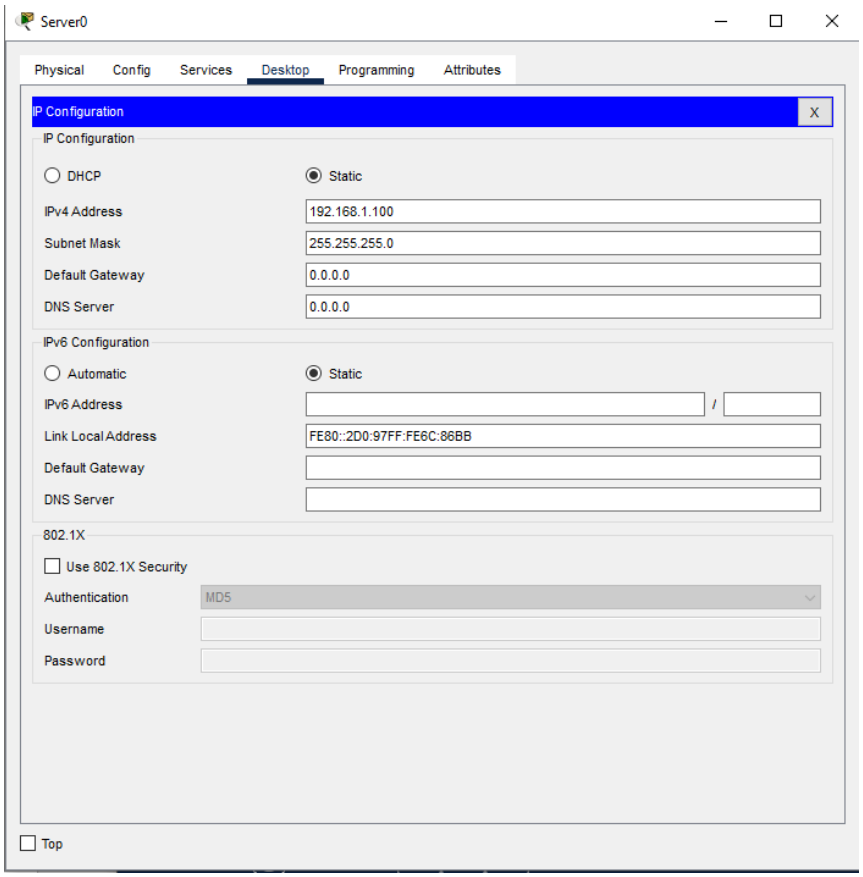
Завдання №3. Засвоєння принципів динамічного призначення IP-адрес:

1. За допомогою програми Packet Tracer побудувати мережу, структура якої наведена на рисунку:



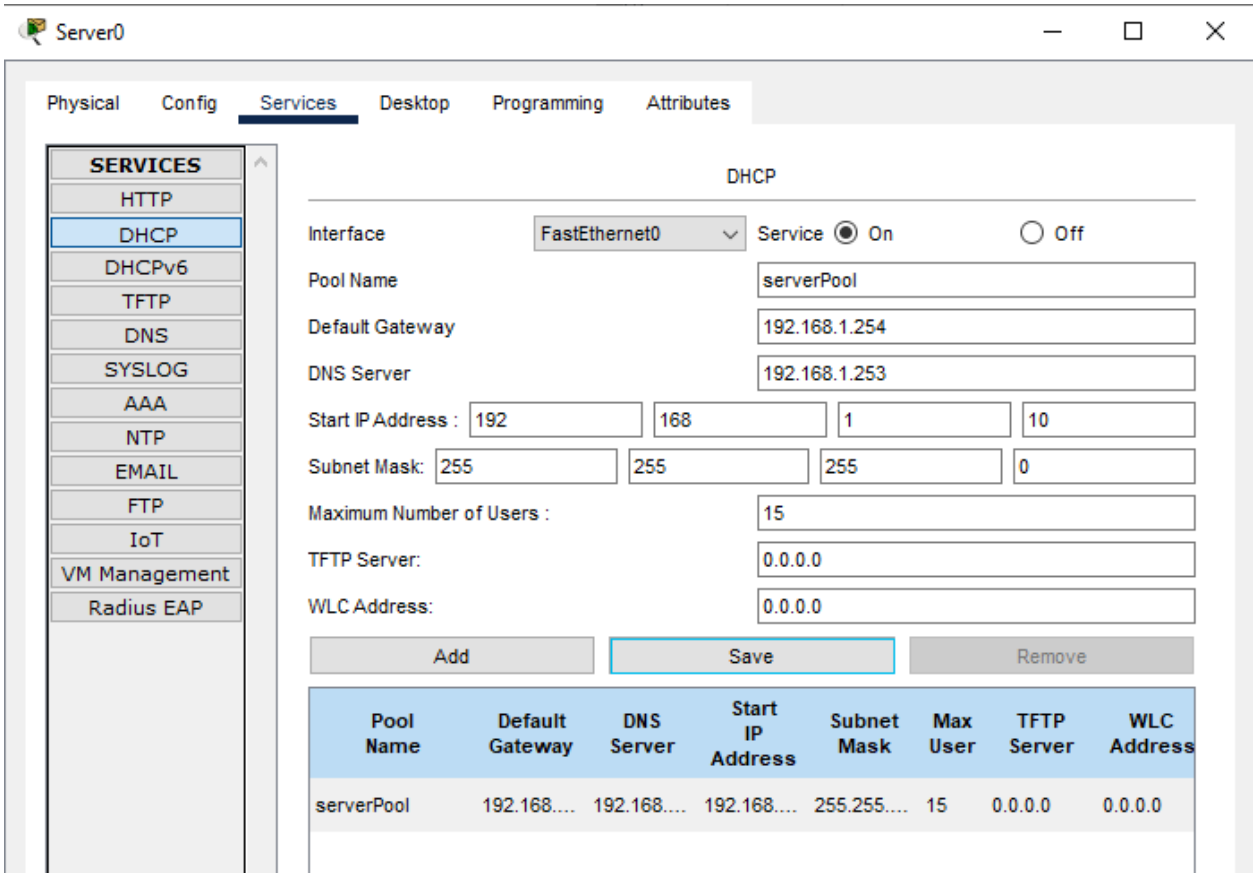
2. Перейти до режими “Simulation”.

3. Вибрати режим конфігурування сервера. Призначити IP-адресу, перші три байти якої збігаються з адресою мережі, а останній байт дорівнює 100:

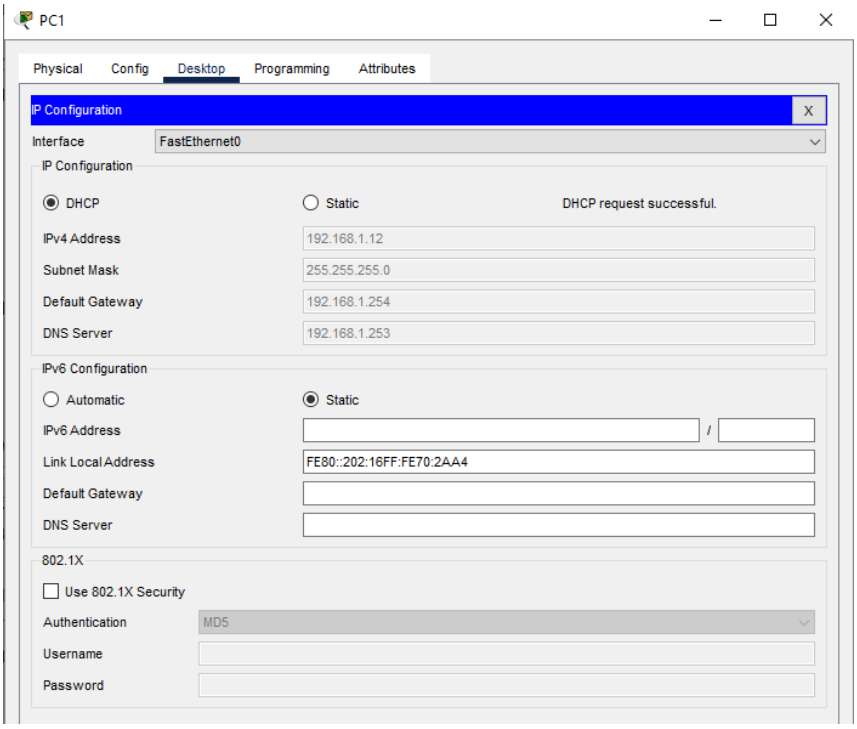


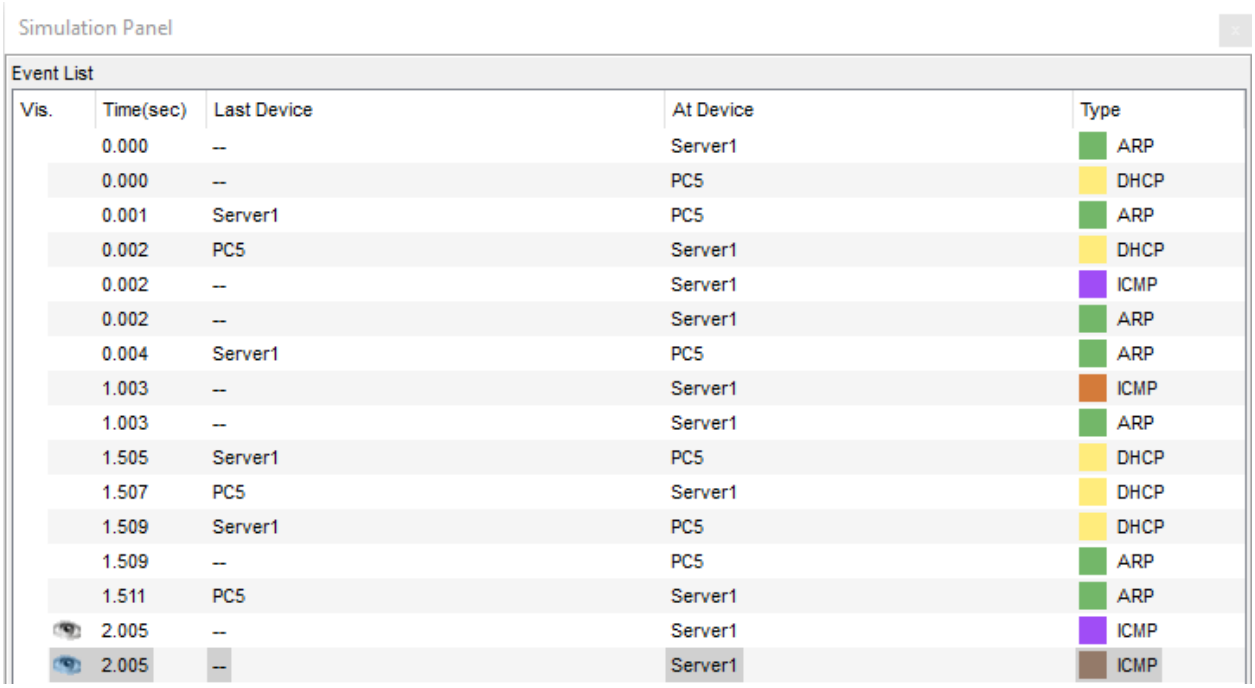
4. У режимі конфігурування перейти до вкладки DHCP і налаштувати таким чином: у полях Default Gateway та DNS Server ввести адреси, перші три байти

яких збігаються з адресою мережі, а останній байт відповідно дорівнює 254 та 253. У полі Start IP Adress ввести адресу, перші три байти якої збігаються з адресою мережі, а останній дорівнює 10. Значення поля Maximum number of Users встановити рівним 15:



5. На PC1 включити динамічний режим конфігурування адрес (DHCP). Впевнитись, що поле IP-адреси, маска підмережі, шлюз за замовчуванням та DNS-сервер порожні. Не закриваючи вікна конфігурування PC1 натиснути кнопку «CaptureForward»:

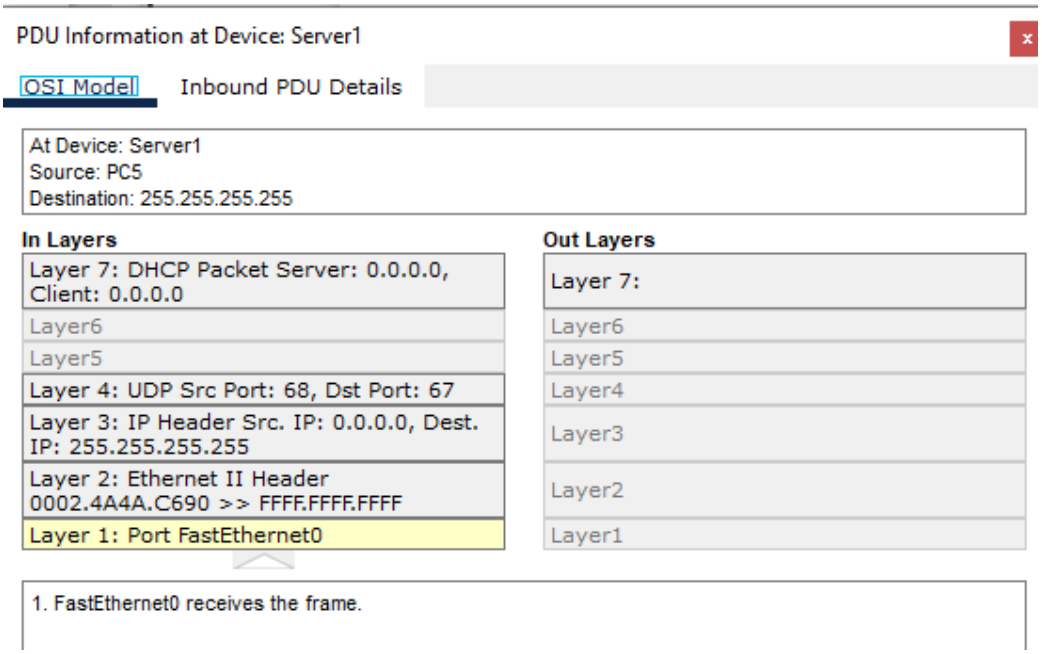




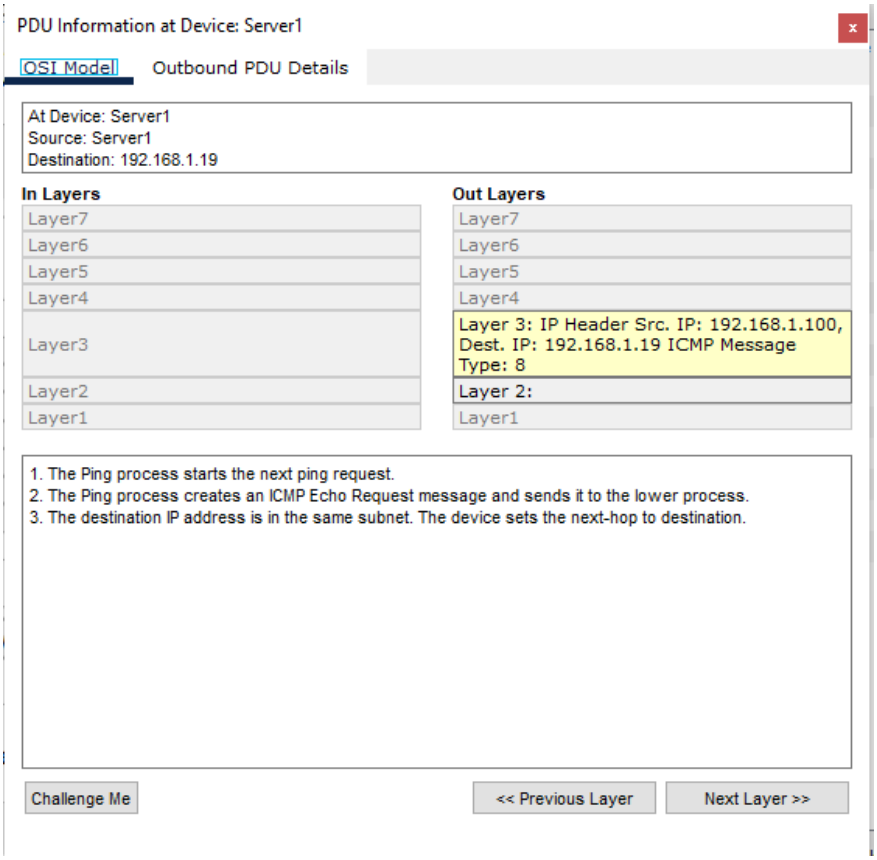
6. Переглянути вміст пакета, що передав PC1, звернути увагу, що вказано в полі адреси отримувача, порівняти вміст пакетів «Inbound PDU» та «Outbound PDU». Визначити, яку інформацію передав DHCP-сервер станції:

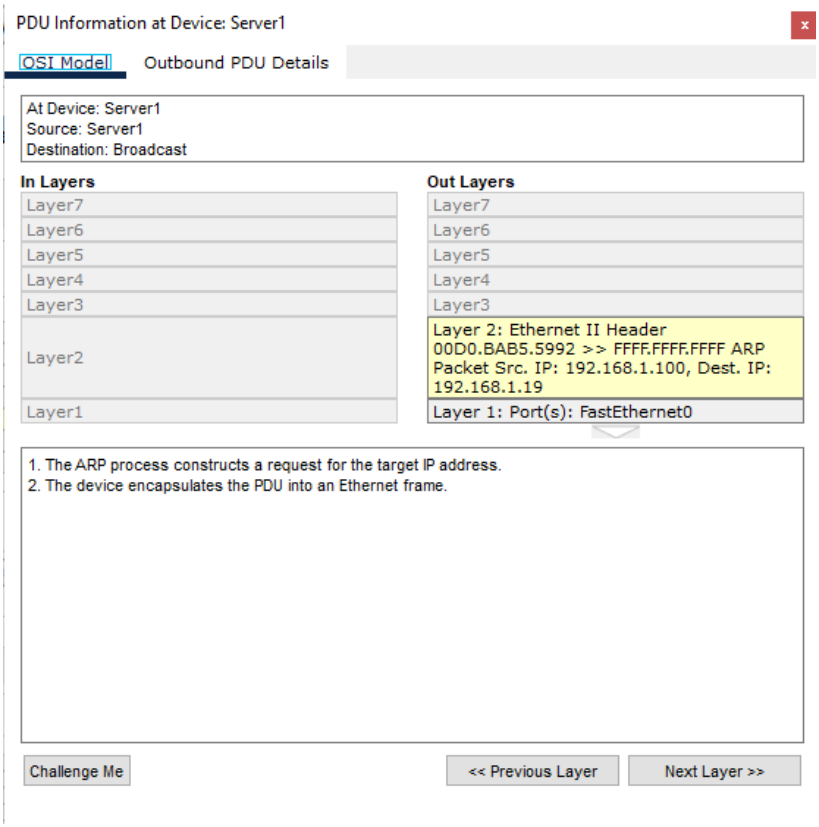
Клієнт DHCP підключається до мережі і починає пошук DHCP-сервера, для чого відправляє запит DHCPDISCOVER на широкомовну адресу 255.255.255.255. Адреса клієнта в цьому запиті 0.0.0.0, оскільки своєї адреси у

клієнта ще немає. Також в запиті клієнт вказує свою MAC-адресу.

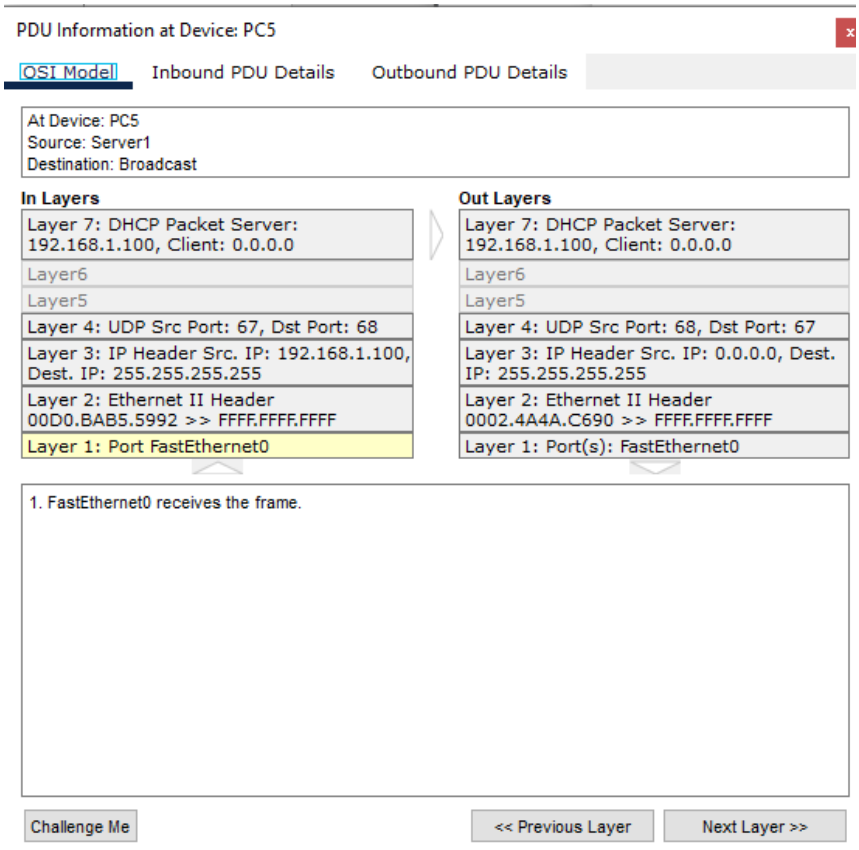


Запит надходить всім модулям, які знаходяться в даному сегменті мережі, але відповідають на нього тільки DHCP-сервери:

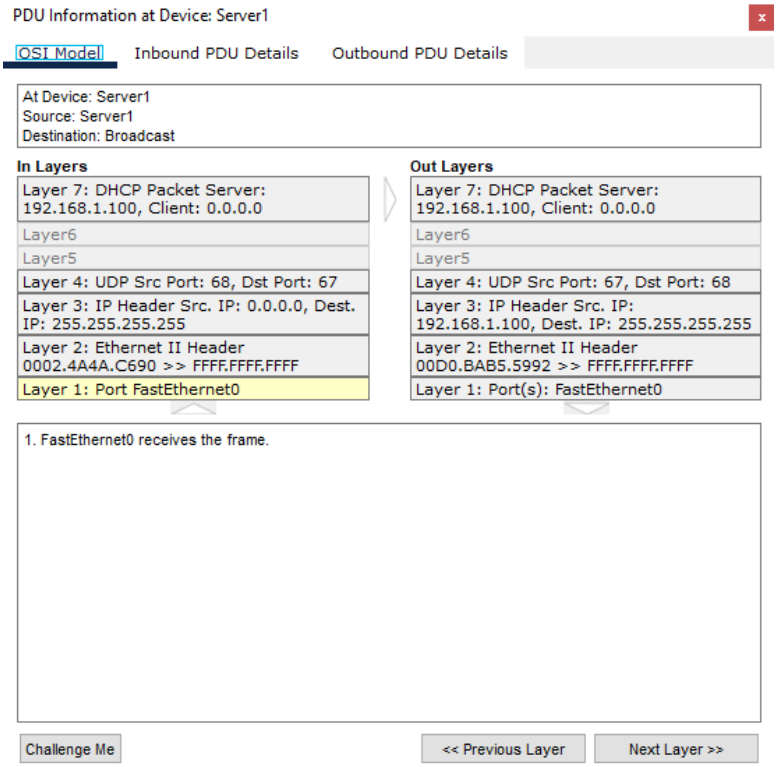




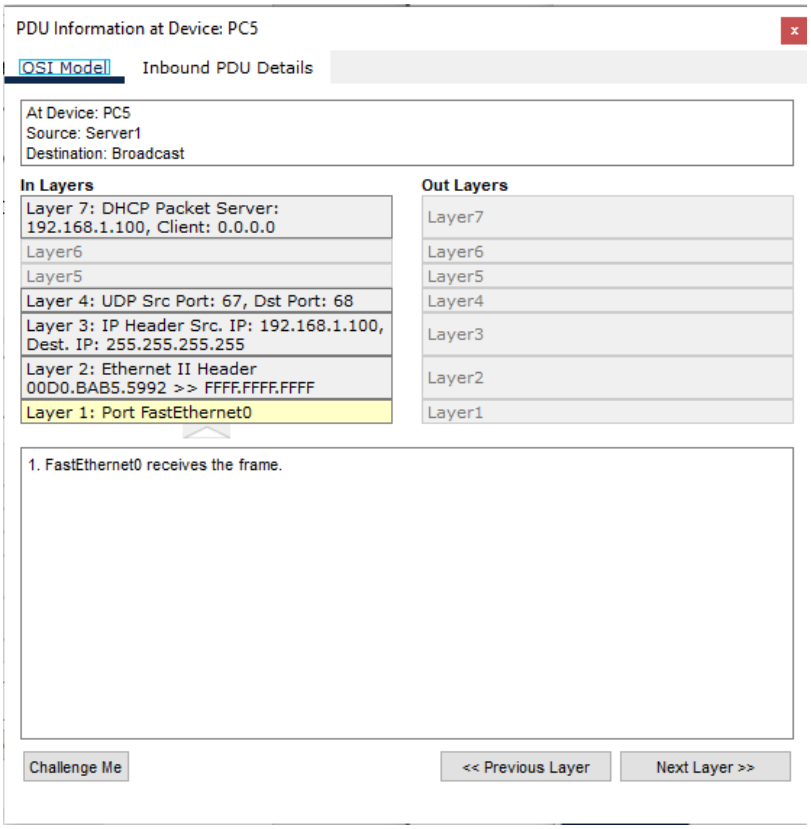
Запит надходить всім модулям, які знаходяться в даному сегменті мережі, але відповідають на нього тільки DHCP-сервери.

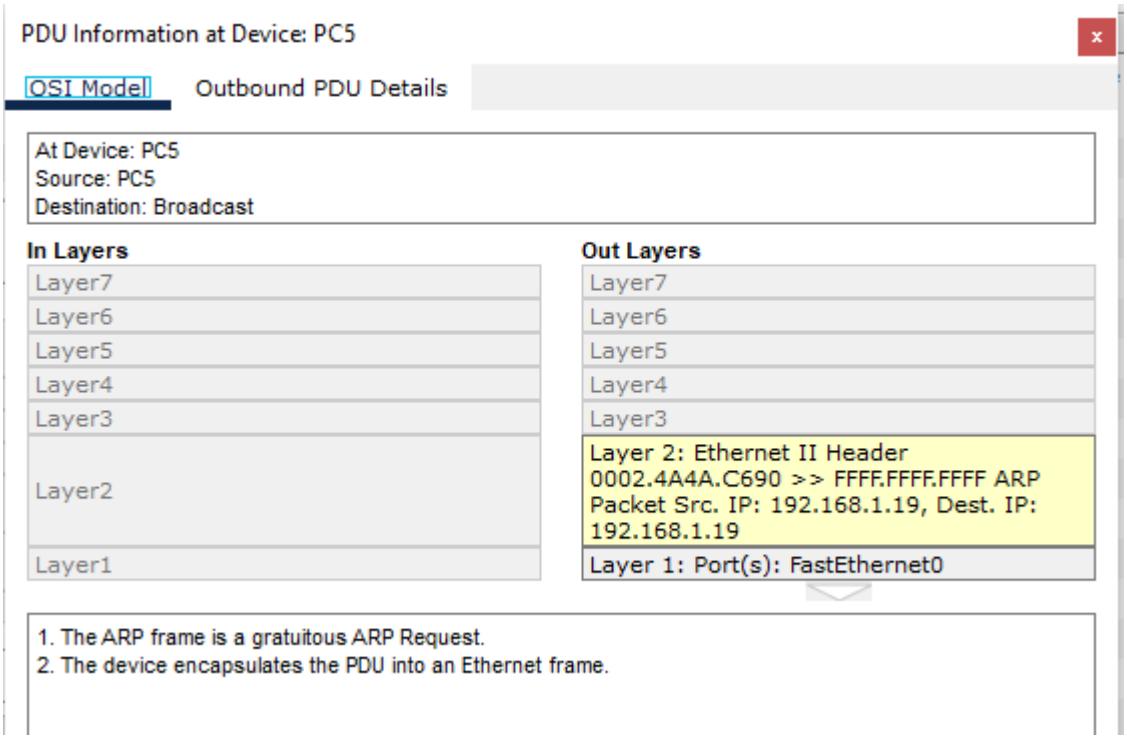


DHCP-сервер, який отримав запит **DHCPDISCOVER**, аналізує його зміст, вибирає підходящу конфігурацію мережі та відправляє її в повідомленні **DHCPOFFER**. **DHCPOFFER** відправляється на широкомовне розсилання. Якщо в мережі знаходиться кілька DHCP-серверів, то клієнт отримує кілька відповідей **DHCPOFFER** і вибирає з них одну, як правило, отриману першою.



Отримавши відповідь сервера, клієнт відповідає повідомленням **DHCPREQUEST**, в якому «офіційно» запитує у сервера надані йому налаштування. В повідомленні **DHCPREQUEST** міститься та ж інформація, що і в **DHCPDISCOVER**, а також IP-адреса вибраного DHCP-сервера. **DHCPREQUEST** надсилається на широкомовну адресу і ті DHCP-сервери, адреса яких відсутня в повідомленні, розуміють, що їхня пропозиція відкинута.



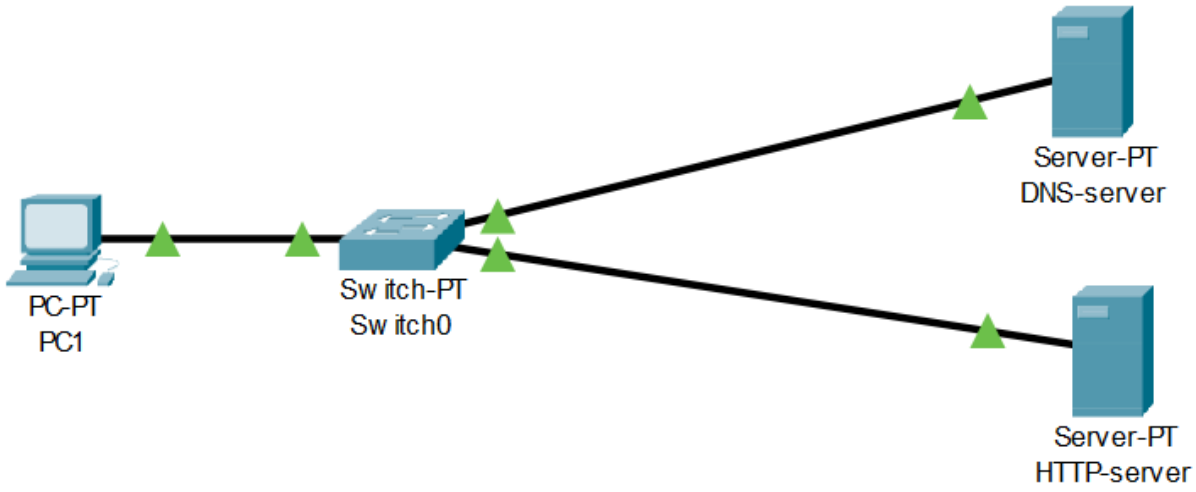


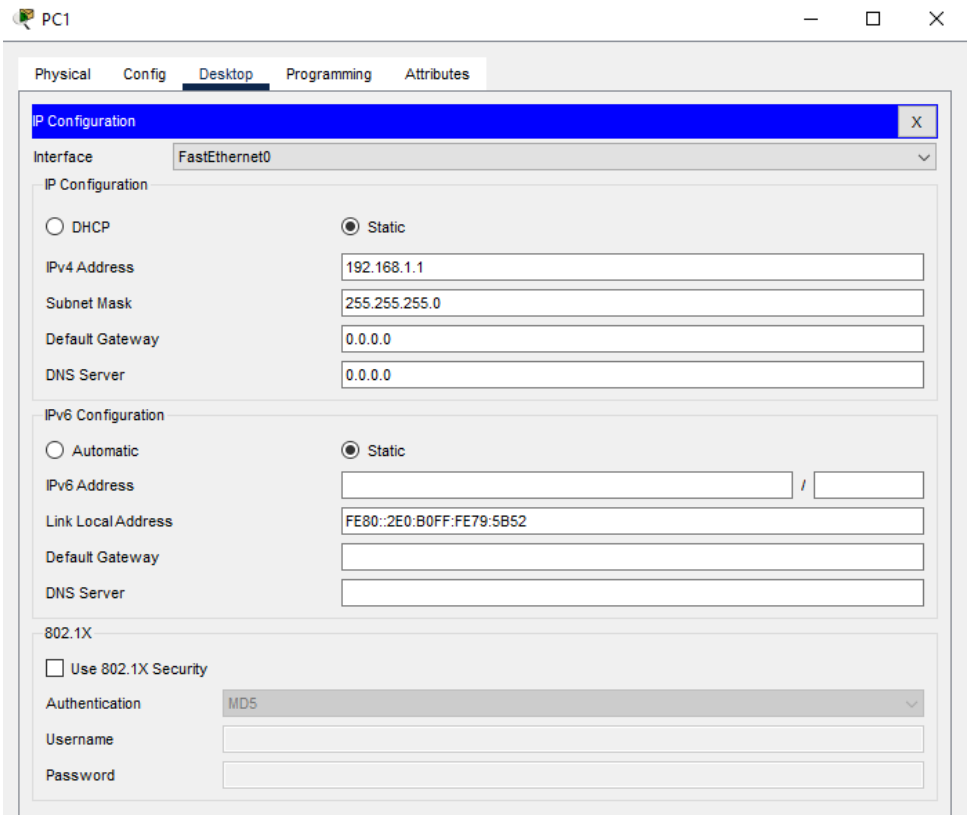
Перш ніж зрозуміти процес призначення IP-адреси, важливо знати деякі ключові технічні терміни, які використовуються в контексті сервера DHCP. Пул адрес DHCP – це віртуальний контейнер, який містить усі IP-адреси, які були налаштовані в діапазоні DHCP, щоб зробити їх доступними для клієнтських комп’ютерів. Як тільки будь-яка IP-адреса з пулу адрес

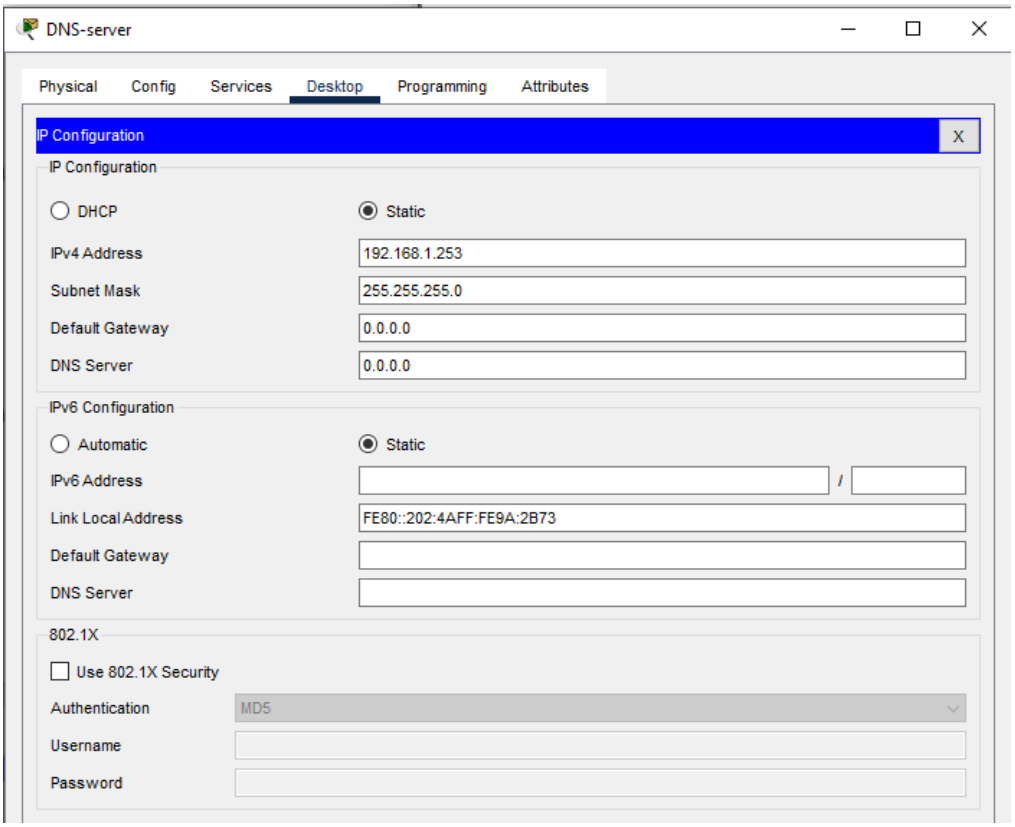
призначається клієнтському комп'ютеру, адреса тимчасово видаляється з пулу. Коли сервер DHCP призначає IP-адресу клієнтському комп'ютеру DHCP, адреса призначається на певний час. Тривалість часу, протягом якого сервер DHCP призначає IP адресу клієнтському комп'ютеру DHCP, технічно називається орендою DHCP. Коли термін оренди DHCP закінчується, IP-адреса відкликається з комп'ютера-клієнта DHCP і повертається до пулу адрес DHCP. Оскільки DHCP-сервер відіграє важливу роль у мережі, коли кількість клієнтських комп'ютерів велика, DHCP-сервер діє дуже розумно та точно, щоб уникнути будь-яких конфліктів або погіршення продуктивності. Покроковий процес, за допомогою якого DHCP-сервер призначає IP-адресу клієнтському комп'ютеру DHCP, коротко називається DORA. Після завершення всього процесу DORA сервер DHCP позначає IP-адресу як призначену в його базі даних, і клієнтський комп'ютер DHCP починає використовувати призначену IP-адресу для зв'язку з іншими комп'ютерами в мережі.

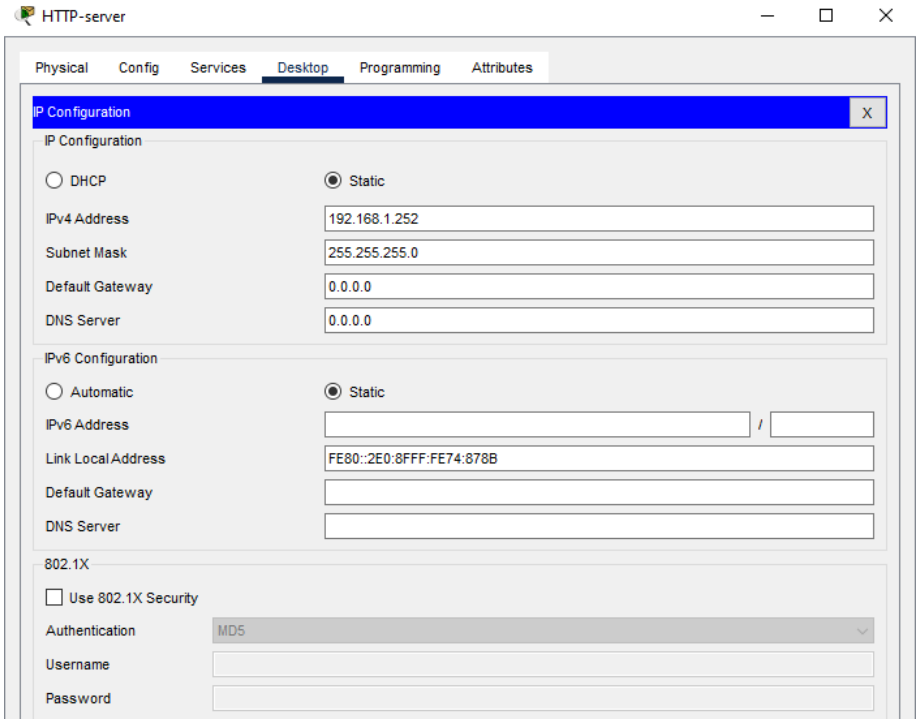
Завдання №4. Засвоєння принципів перетворення DNS-імен в IP-адреси.

1. За допомогою програми Packet Tracer побудувати мережу, структуру якої наведено на рисунку 6.18. Призначити такі IP-адреси: перші три байти всіх адрес відповідають адресі мережі, останній байт PC1 – 1; DNS- сервера – 253; HTTP-сервера – 252.

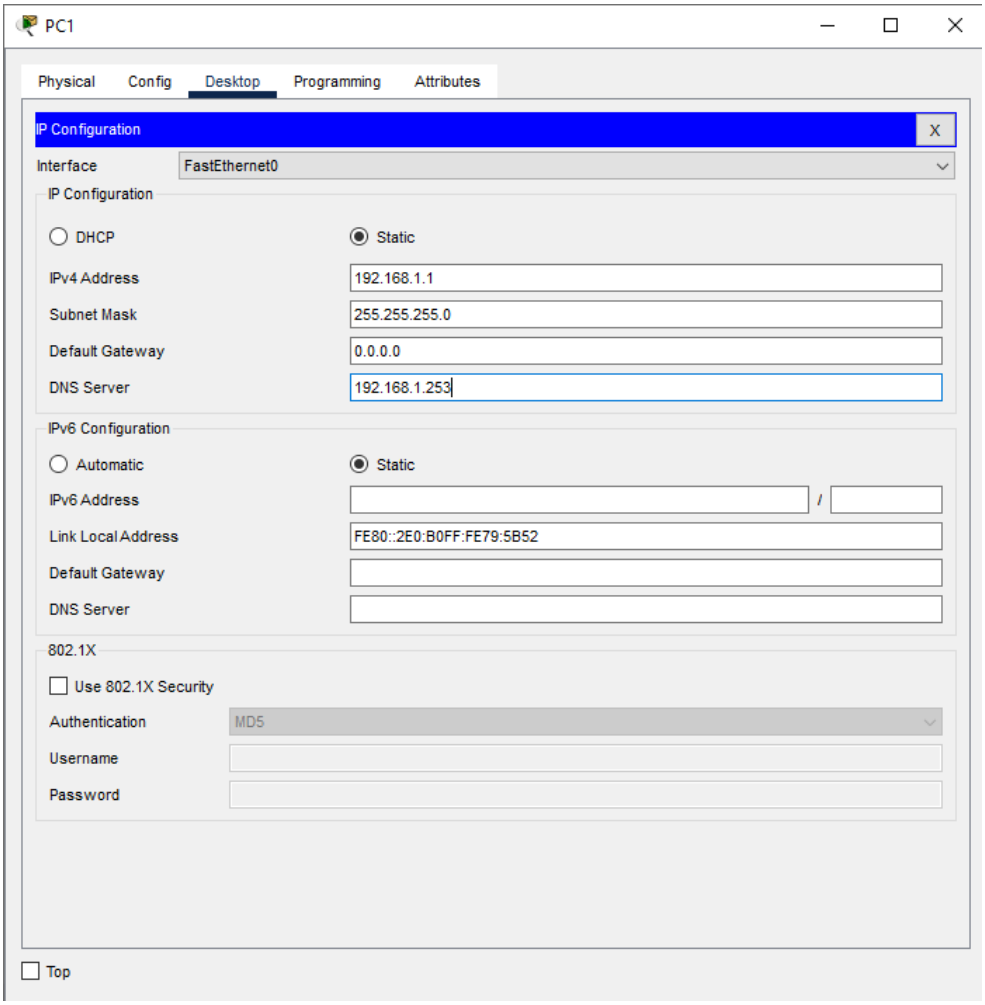



PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2E0:B0FF:FE79:5B52
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password

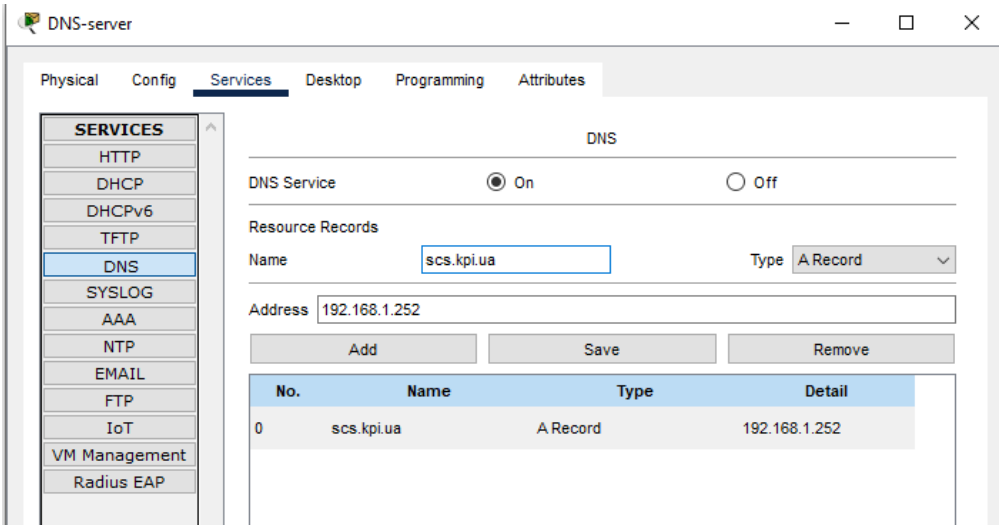

DNS-server
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.253
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::202:4AFF:FE9A:2B73
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password



2. На PC1 в полі DNS вказати відповідну адресу.



3. На DNS-сервері в вкладці DNS додати запис, в якому в полі Domain Name вказати ім’я scs.kpi.ua, а в полі IP-Address – адресу HTTP-сервера.



4. Перейти до режиму “Simulation”.

5. На PC1 в командному рядку виконати команду ping, вказавши доменне ім’я scs.kpi.ua та натиснути кнопку «Capture/Forward».

6. Натискати кнопку «Capture/Forward», поки на PC1 не буде сформований DNS-запит. Пояснити призначення ARP-пакетів, які були сформовані на попередніх кроках:

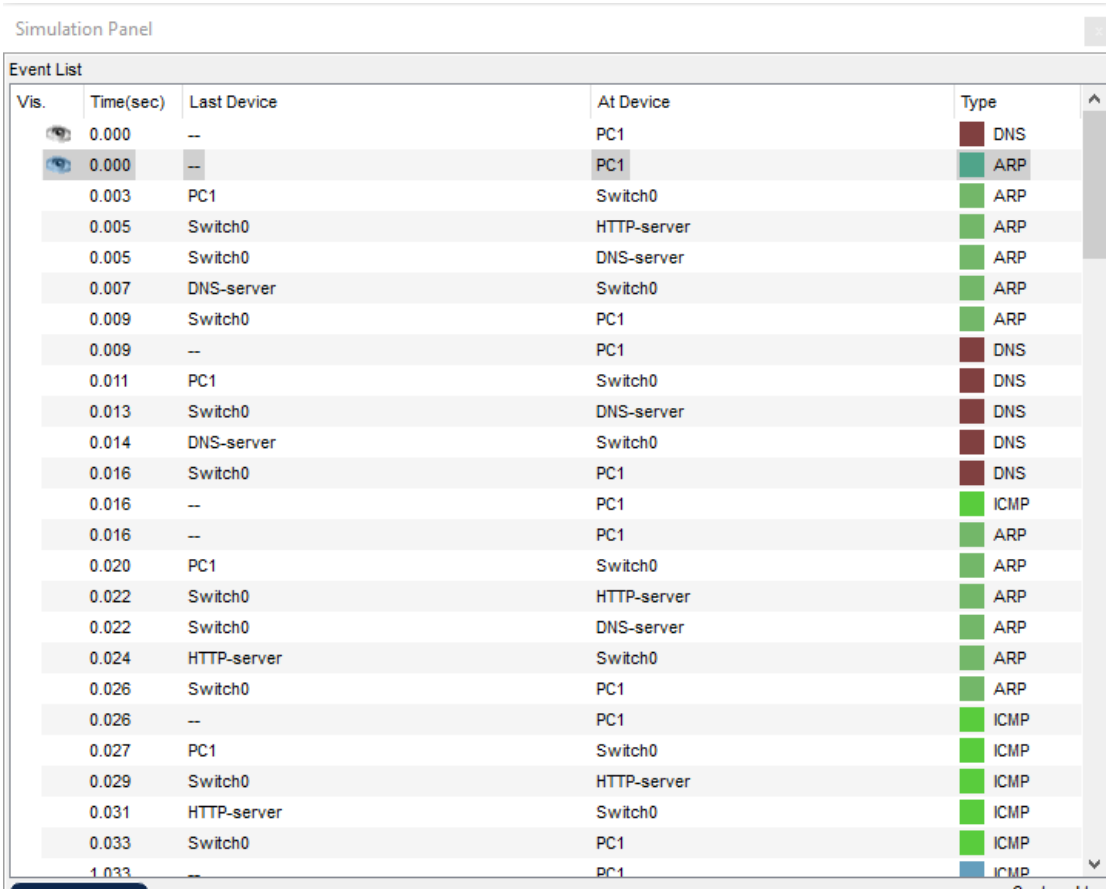
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping scs.kpi.ua

Pinging 192.168.1.252 with 32 bytes of data:

Reply from 192.168.1.252: bytes=32 time=17ms TTL=128
Reply from 192.168.1.252: bytes=32 time=9ms TTL=128
Reply from 192.168.1.252: bytes=32 time=6ms TTL=128
Reply from 192.168.1.252: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.1.252:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 17ms, Average = 10ms

C:\>
```



ARP (Address Resolution Protocol) використовується для визначення MAC-адрес пристроїв у локальній мережі. Оскільки DNS-запит передається від PC1 до DNS-сервера, а в подальшому — від PC1 до HTTP-сервера, комп'ютер PC1 спочатку має отримати MAC-адреси обох серверів. Саме для цього і використовуються ARP-запити.

На початку симуляції ми спостерігали декілька етапів формування ARP-пакетів:

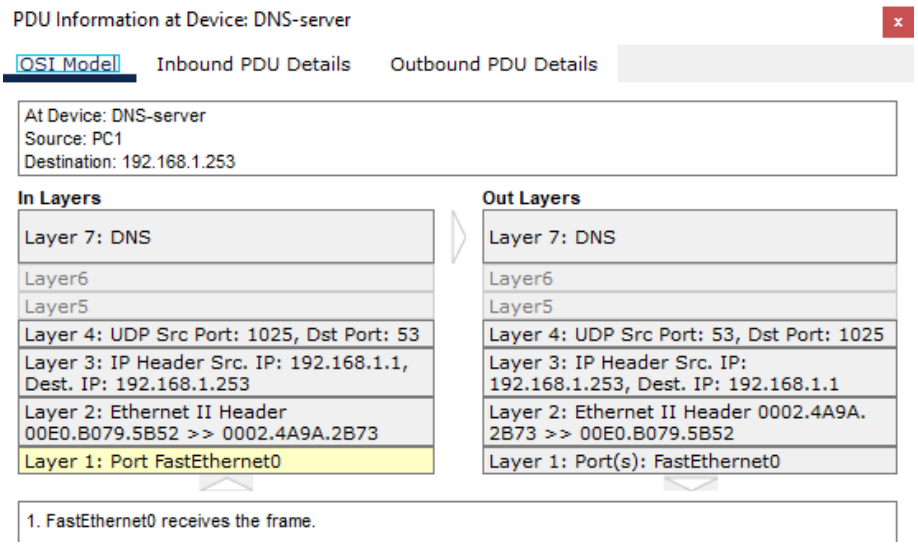
1. **Визначення MAC-адреси DNS-сервера**
    - **0.000 сек:** PC1 формує ARP-запит для визначення MAC-адреси DNS-сервера. Цей запит передається через Switch0 до всіх підключених пристроїв.
    - **0.007 сек:** DNS-сервер відповідає на запит, повідомляючи свою MAC-адресу.
    - **0.009 сек:** PC1 отримує відповідь і зберігає MAC-адресу DNS-сервера у своїй таблиці ARP.
2. **Формування DNS-запиту**

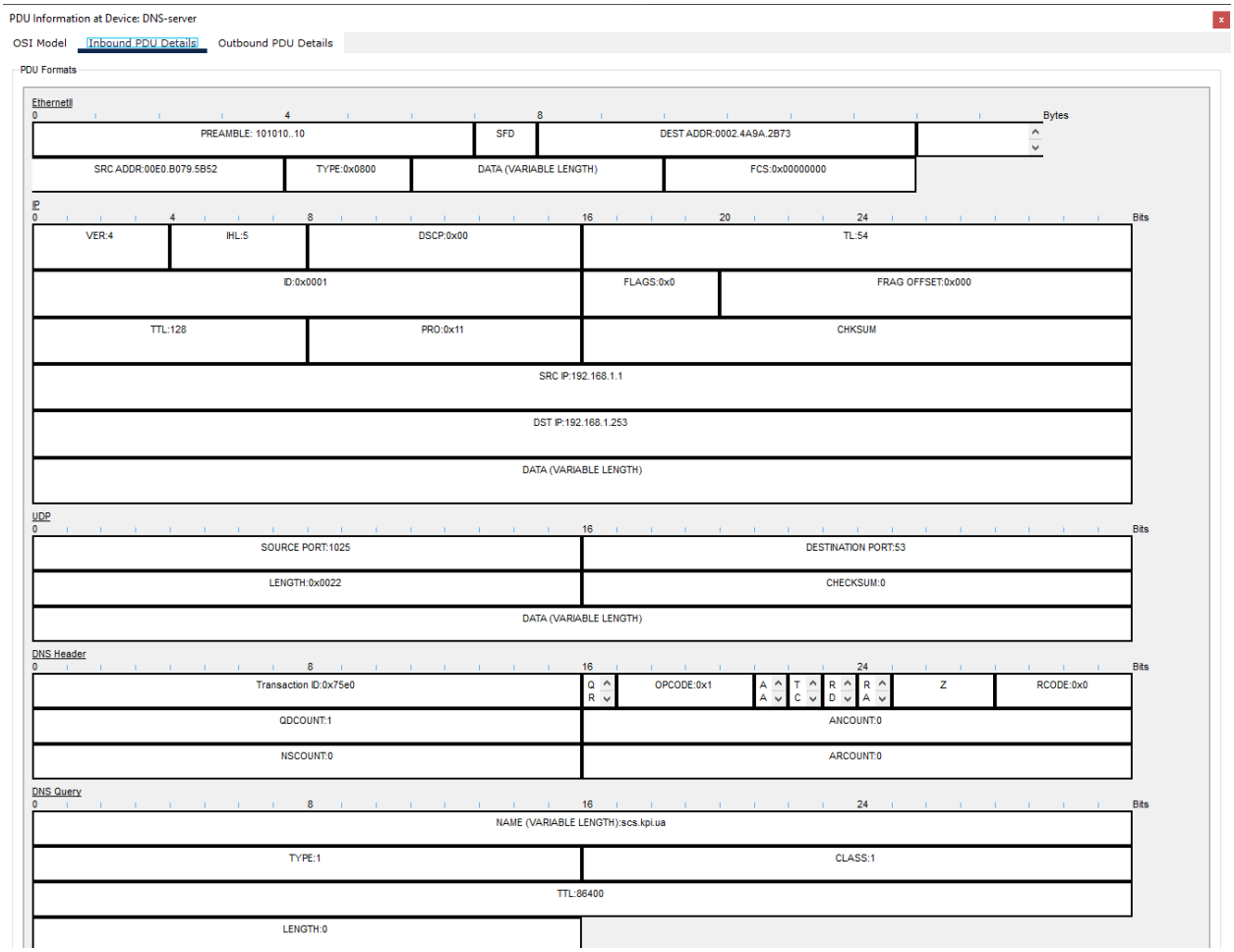
Після отримання MAC-адреси DNS-сервера PC1 формує DNS-запит і передає його до DNS-сервера. Цей запит є ключовим для отримання IP-адреси HTTP-сервера.

3. **Визначення MAC-адреси HTTP-сервера**
   - **0.016 сек:** Після отримання відповіді від DNS-сервера PC1 дізнається IP-адресу HTTP-сервера (192.168.1.252).
   - **0.020 сек:** PC1 формує новий ARP-запит, щоб визначити MAC-адресу HTTP-сервера.
   - **0.024 сек:** HTTP-сервер відповідає на ARP-запит, після чого його MAC-адреса зберігається у таблиці ARP на PC1.
4. **Передача ICMP-запиту (ping)**

   Після завершення ARP-взаємодії PC1 починає надсилати ICMP-пакети до HTTP-сервера. На цьому етапі ARP більше не використовується, оскільки всі необхідні MAC-адреси вже визначено.

7. Коли DNS-запит надійде на сервер, переглянути його вміст (Inbound PDU) та вміст відповіді (Outbound PDU). Пояснити інформацію, що міститься в цих пакетах.





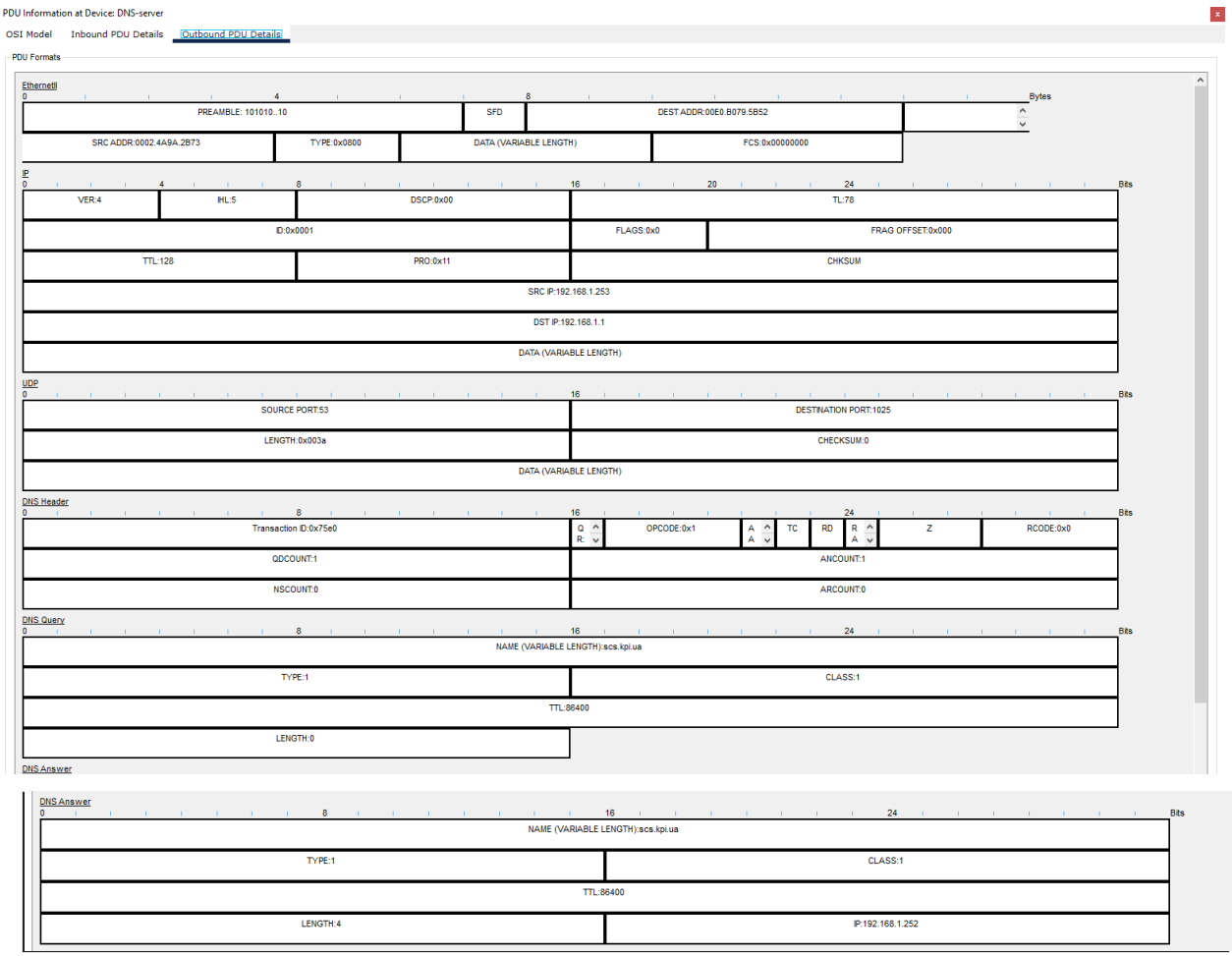
Аналіз структури DNS-запиту

1. Ethernet Header
    - SRC ADDR: 00E0.B079.5852 — MAC-адреса відправника (робочої станції PC1).
    - DEST ADDR: 0002.4A9A.2B73 — MAC-адреса одержувача (DNS-сервера).
    - TYPE: 0x0800 — Позначає, що передається IP-пакет.
2. IP Header
    - VER: 4 — Версія протоколу IP (IPv4).
    - SRC IP: 192.168.1.1 — IP-адреса відправника (PC1).
    - DST IP: 192.168.1.253 — IP-адреса отримувача (DNS-сервера).
    - PRO: 0x11 — Протокол UDP (User Datagram Protocol), який використовується для DNS-запитів.
3. UDP Header
    - Source Port: 1025 — Випадковий порт відправника (PC1),

використаний для зв'язку.

- Destination Port: 53 — Порт DNS, стандартний для отримання запитів.
- Length: 0x0022 — Довжина UDP-пакета.

4. DNS Header
    - Transaction ID: 0x75E0 — Унікальний ідентифікатор для зіставлення запиту та відповіді.
    - Opcode: 0x1 — Вказує на стандартний запит (Query).
    - QCOUNT: 1 — Кількість запитуваних доменних імен (одне доменне ім’я).
5. DNS Query
    - Name: scs.kpi.ua — Доменне ім'я, яке необхідно перетворити в IP-адресу.
    - Type: 1 — Запит для IPv4-адреси (A-запис).
    - Class: 1 — Інтернет (IN).
    - TTL: 86400 — Час життя запису в секундах (24 години).



Аналіз структури DNS-відповіді

1. Ethernet Header
    - SRC ADDR: 0002.4A9A.2B73 — MAC-адреса відправника (DNS-сервера).
    - DEST ADDR: 00E0.B079.5852 — MAC-адреса одержувача (робочої станції PC1).
    - TYPE: 0x0800 — Вказує на те, що передається IP-пакет.
2. IP Header
    - VER: 4 — Версія протоколу IP (IPv4).
    - SRC IP: 192.168.1.253 — IP-адреса відправника (DNS-сервера).
    - DST IP: 192.168.1.1 — IP-адреса одержувача (PC1).
    - PRO: 0x11 — Протокол UDP (User Datagram Protocol).
3. UDP Header
    - Source Port: 53 — Порт DNS-сервера, стандартний для відповіді на DNS-запити.
    - Destination Port: 1025 — Порт клієнта (PC1), через який був зроблений запит.
    - Length: 0x003a — Довжина UDP-пакета.
4. DNS Header
    - Transaction ID: 0x75E0 — Ідентифікатор транзакції, що відповідає запиту. Це дозволяє клієнту зрозуміти, на який запит прийшла відповідь.
    - Opcode: 0x1 — Стандартна відповідь на запит.
    - QR: 1 — Позначає, що це відповідь, а не запит.
    - RD: 1 — Встановлений біт рекурсії, що підтверджує виконання рекурсивного пошуку.
    - RA: 1 — Сервер підтримує рекурсивний пошук.
    - RCode: 0x0 — Відповідь успішна, без помилок.
5. DNS Query
    - Name: scs.kpi.ua — Доменне ім’я, запитане клієнтом.

- Type: 1 — Вказує на те, що клієнт запитував IPv4-адресу (A-запис).
- Class: 1 — Інтернет (IN).

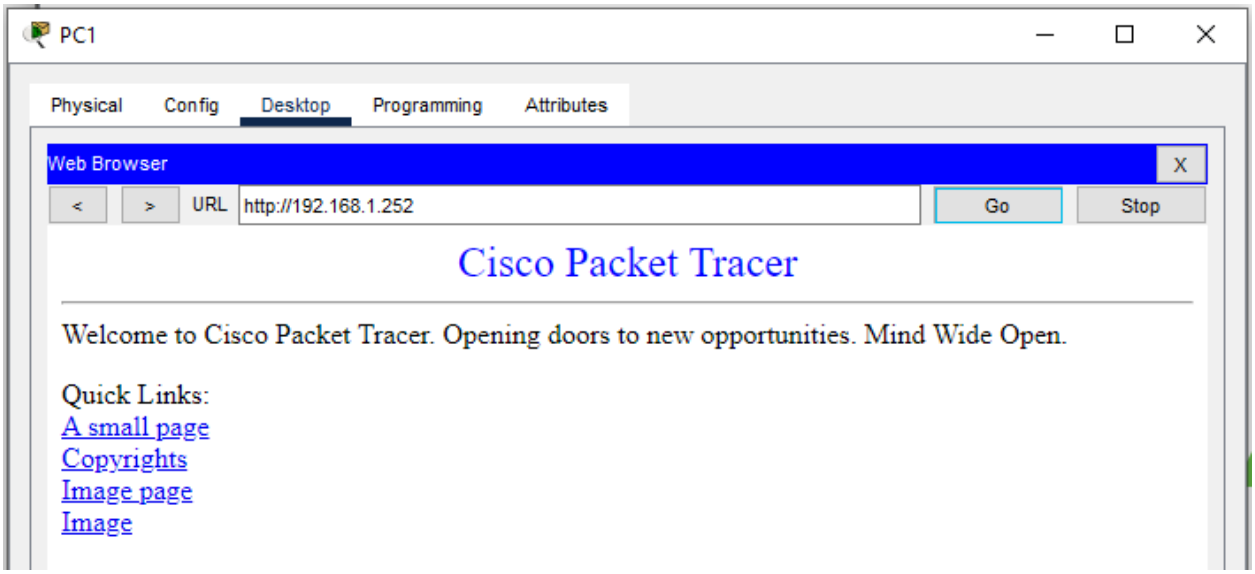
6. DNS Answer
   - Name: scs.kpi.ua — Доменне ім’я, на яке дається відповідь.
   - Type: 1 — Відповідь для IPv4-адреси (A-запис).
   - Class: 1 — Інтернет (IN).
   - TTL: 86400 — Час життя запису (24 години).
   - IP: 192.168.1.252 — Відповідна IP-адреса для доменного імені.

Роль DNS-відповіді

Ця відповідь дозволяє клієнту використовувати отриману IP-адресу (192.168.1.252) для доступу до ресурсу scs.kpi.ua. Це ключовий етап у механізмі DNS, який забезпечує перетворення доменних імен в IP-адреси для подальшого встановлення з’єднань.

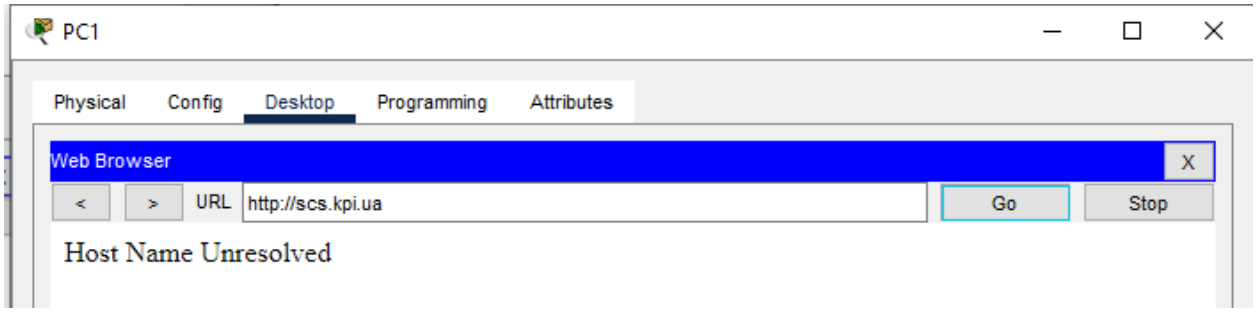
9. Перейти в режим «Real Time».

10. У налаштуваннях DNS-сервера відключити DNS-сервіс. У полі URL веб браузера на PC1 набрати IP-адресу HTTP-сервера. Зафіксувати результат. Замість IP-адреси HTTP-сервера набрати його DNS-ім’я. Пояснити отриманий результат. Не закриваючи вікна веб браузера включити DNS-сервіс. Зафіксувати зміни, що відбулися.

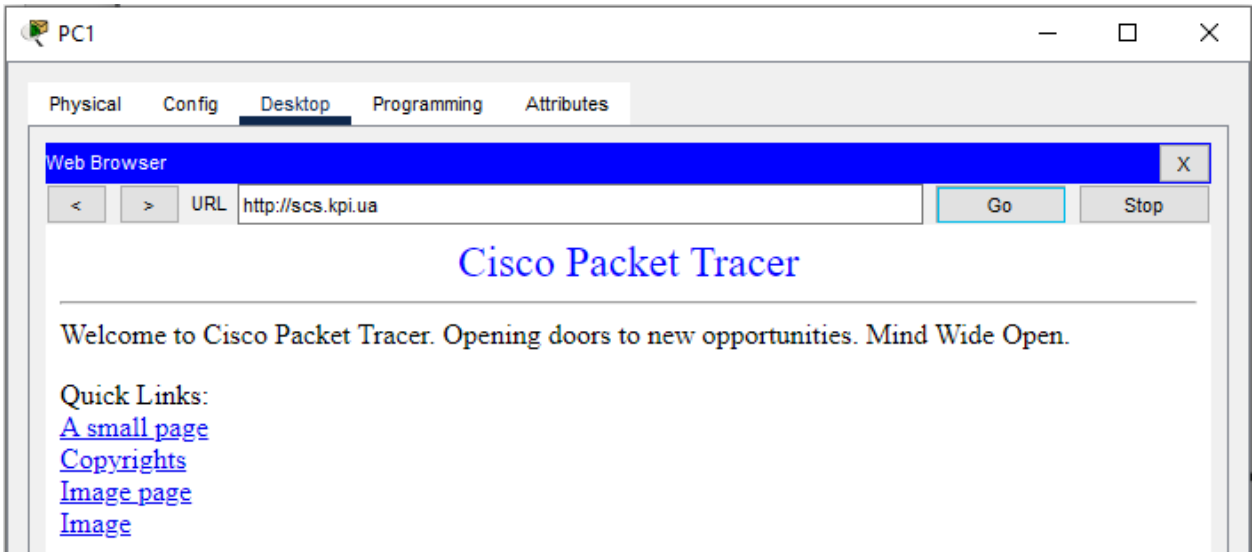


Браузер відкриє веб-сторінку HTTP-сервера, оскільки IP-адреса не потребує DNS-розв'язання. Це демонструє, що DNS є необов’язковим, якщо клієнт

знає IP-адресу.



Веб-сторінка не відкриється, оскільки відсутній DNS-сервіс для перетворення доменного імені на IP-адресу.



Веб-сторінка завантажиться успішно, оскільки DNS-сервіс тепер працює й клієнт отримує правильну IP-адресу для доменного імені.

Завдання №5. Ознайомлення з відомостями про структуру перехресного кабеля.

Кабель типу «вита пара» є основою для побудови Ethernet-мереж, які використовуються для з'єднання різних мережевих пристроїв. Його популярність пояснюється простотою використання, доступністю та ефективністю в передачі даних. У цьому есе ми розглянемо особливості використання перехресного кабелю, його роль у мережевих технологіях і принципи створення.

Вита пара складається з кількох ізольованих проводників, які скручені

попарно для зменшення електромагнітних завад. Це рішення дозволяє забезпечити надійну передачу сигналів, навіть у середовищах з високим рівнем завад. Кабелі поділяються на екрановані (STP, FTP) та неекрановані (UTP). Екрановані кабелі використовуються у складних умовах, тоді як неекрановані, через їхню гнучкість і простоту використання, підходять для офісних приміщень.

Однією з ключових характеристик кабелю є його обтискання, тобто порядок з'єднання проводів у роз'ємах RJ-45. Існує два основні стандарти обтискання – T568A та T568B, які визначають послідовність кольорових проводів. Ці стандарти дозволяють створювати два типи кабелів: прямий і перехресний.

Прямий і перехресний кабель

Прямий кабель має однаковий порядок обтискання на обох кінцях (T568A–T568A або T568B–T568B) і використовується для з'єднання пристроїв різних рівнів моделі OSI, наприклад, комп'ютера з комутатором. У перехресному кабелі один кінець обтиснутий за стандартом T568A, а інший — за T568B. Цей кабель дозволяє з'єднувати пристрої одного рівня моделі OSI, наприклад, дві робочі станції або два комутатори.

Головна мета перехресного кабелю — забезпечити передачу сигналів з контактів TX (передача) одного пристрою на контакти RX (прийом) іншого. Це досягається через «перехрещення» провідників, яке синхронізує логічні сигнали між пристроями.

Автоматизація з Auto MDI/MDI-X

Із розвитком технологій більшість сучасного мережевого обладнання підтримує функцію **Auto MDI/MDI-X**. Вона дозволяє пристроям автоматично налаштовуватися під пряме чи перехресне з'єднання, незалежно від типу кабелю. Це зменшує необхідність використання перехресного кабелю в реальних мережах. Однак у навчальних цілях, зокрема в програмі **Cisco Packet Tracer**, традиція використання перехресного кабелю для однотипного обладнання залишається актуальною.

Процес створення перехресного кабелю

Для виготовлення перехресного кабелю потрібно:

1. Один кінець кабелю обтиснути за стандартом **T568A**.
2. Інший кінець обтиснути за стандартом **T568B**. Це забезпечить правильне «перехрещення» сигналів для передачі та прийому.

На практиці кабель використовується для з'єднання двох комп'ютерів або комутаторів. У програмі Cisco Packet Tracer це дозволяє симулювати роботу однотипного обладнання.

Висновок:

Лабораторна робота №6 дала змогу не лише закріпити теоретичні знання, а й отримати практичний досвід роботи з основними механізмами функціонування комп'ютерних мереж, зокрема принципами перетворення DNS-імен в IP-адреси.

У ході виконання роботи я наочно побачила, як базові протоколи взаємодіють між собою в рамках моделі OSI, а саме на мережевому та канальному рівнях. Особливо цікавим було спостерігати, як за допомогою протоколу ARP відбувається визначення MAC-адрес для встановлення з'єднання між пристроями. Цей процес, що на перший погляд здається непомітним для кінцевого користувача, є фундаментально важливим для функціонування локальних мереж.

Динамічне призначення IP-адрес за допомогою DHCP-сервера продемонструвало ефективність автоматизації управління мережевими ресурсами. Це ще раз підкреслило важливість грамотного налаштування мережі, що дозволяє уникати конфліктів адрес та зменшувати кількість ручної роботи адміністратора. Спостерігаючи за взаємодією DHCP-сервера і клієнта, вдалося зрозуміти чотири основні етапи DORA (Discover, Offer, Request, Acknowledge), які забезпечують процес оренди адреси.

Окремим відкриттям стало розуміння ролі DNS у повсякденному житті користувачів. Виконання DNS-запиту продемонструвало, як доменні імена, що є зручними для людини, перетворюються на IP-адреси, зрозумілі

комп’ютерам. Процес перетворення є швидким і непомітним, але водночас базується на складній і багаторівневій взаємодії серверів та клієнтів.

Ця робота допомогла усвідомити, наскільки важливою є синергія між різними рівнями та протоколами мережі. Простий процес передачі даних, як-от ping або доступ до веб-сайту, є результатом злагодженої роботи десятків механізмів, від фізичного з’єднання до абстрактних протоколів.