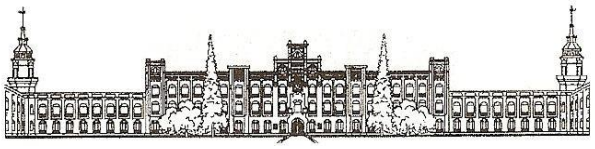

Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
Факультет прикладної математики
Кафедра системного програмування та спеціалізованих комп’ютерних систем

Лабораторна робота №10

з дисципліни «Комп’ютерні мережі»

«Організація доступу до комп’ютерної мережі. Технології VLAN та NAT»

Виконав
студент 4-го курсу
групи КВ-11
Терентьєв Іван Дмитрович

Перевірив: _____

Київ 2024

Мета роботи

Навчити студентів створювати віртуальні комп'ютерні мережі на основі керованих комутаторів та маршрутизаторів, а також впроваджувати віртуальні мережі на базі запропонованої топології.

План виконання лабораторної роботи

1. У межах запропонованої топології (рис 10.1) створити та налаштувати три віртуальні мережі: VLAN2, VLAN3, VLAN4. Комп'ютери PC0, PC1, PC4 та PC6 помістити в VLAN2 комп'ютери PC2, PC3, PC6 та PC7 помістити в VLAN3, Web-сервер Server0 помістити в VLAV4.
2. Виконати мережеві налаштування комп'ютерів PC0 ÷ PC7 та сервера Server0. На сервері Server0 встановити службу HTTP.
3. Виконати налаштування маршрутизатора Router0 для забезпечення взаємодії комп'ютерів різних віртуальних мереж.
4. Виконати підключення створеної локальної мережі до зовнішнього сервера Server1, забезпечивши при цьому перетворення зовнішніх IP-адрес у внутрішні IP-адреси і внутрішніх IP-адрес у зовнішні IP-адреси.
5. Виконати налаштування маршрутизатора Router0 для забезпечення доступу до Web-сервера Server0 із зовнішньої мережі.

Завдання

1. Побудувати модель комп'ютерної мережі, яка зображена на рисунку 10.1.
2. Покроково виконати необхідні мережеві налаштування мережевих пристроїв. Рекомендується після кожного кроку перевіряти виконані налаштування
3. У режимі симуляції за допомогою утиліти ping дослідити рух службових пакетів по створеній мережі:

- від хоста у VLAN2 до хоста у VLAN3;
- від хоста у VLAN2 до хоста у VLAN4;
- від хоста у VLAN3 до хоста у VLAN2;
- від хоста у VLAN3 до хоста у VLAN4;
- від хоста у VLAN4 до хоста у VLAN2;
- від хоста у VLAN2 до хоста у VLAN3.

Результати спостережень занесіть у звіт.

4. У режимі симуляції за допомогою утиліти ping дослідіть рух службових пакетів із внутрішньої мережі до сервера Server1 і в зворотному напрямку. Звернути увагу на заміну внутрішньої IP-адреси на зовнішню і зовнішньої на внутрішню при проходженні пакету через маршрутизатор Router0.

Результати спостережень занесіть у звіт.

5. Із сервера Server1 виконайте http-запит до Web-сервера Server0.

Отриманий результат занесіть у звіт.

Теоретичні відомості

VLAN (Virtual Local Area Network)

VLAN – це технологія, яка дозволяє розділяти одну фізичну мережу на кілька віртуальних, ізолюючи трафік між різними групами пристроїв.
Основні переваги VLAN:

- **Логічне розділення мережі** – пристрої в різних VLAN працюють, як ніби вони підключені до окремих комутаторів.
- **Безпека** – обмежується небажаний доступ між сегментами мережі.
- **Оптимізація трафіку** – зменшується навантаження на мережу за рахунок розділення широкомовного домену.

Типи VLAN-портів:

- **Access-порт** – підключає кінцеві пристрої (ПК, принтери) до певного VLAN.
- **Trunk-порт** – передає трафік одразу декількох VLAN між комутаторами або між комутатором і маршрутизатором.

Для ідентифікації VLAN використовується тегування кадрів (стандарт 802.1Q).

NAT (Network Address Translation)

NAT – це технологія, яка використовується для перетворення приватних IP-адрес у публічні для доступу до Інтернету.

Типи NAT:

- **Статичний NAT** – одна внутрішня IP-адреса постійно відображається на одну зовнішню.
- **Динамічний NAT** – внутрішні IP-адреси зіставляються із пулом зовнішніх.
- **PAT (NAT Overload)** – багато внутрішніх IP-адрес використовують одну зовнішню, розрізняючись за номерами портів.

Основні переваги NAT:

- **Економія публічних IP-адрес**.
- **Забезпечення безпеки** – внутрішні IP-адреси залишаються прихованими.
- **Гнучкість у керуванні доступом**.

Для налаштування NAT маршрутизатор розділяє інтерфейси на внутрішні (ip nat inside) і зовнішні (ip nat outside) та виконує трансляцію адрес.

Хід роботи

Побудуємо модель комп'ютерної мережі, результат можна побачити на рисунку 1.

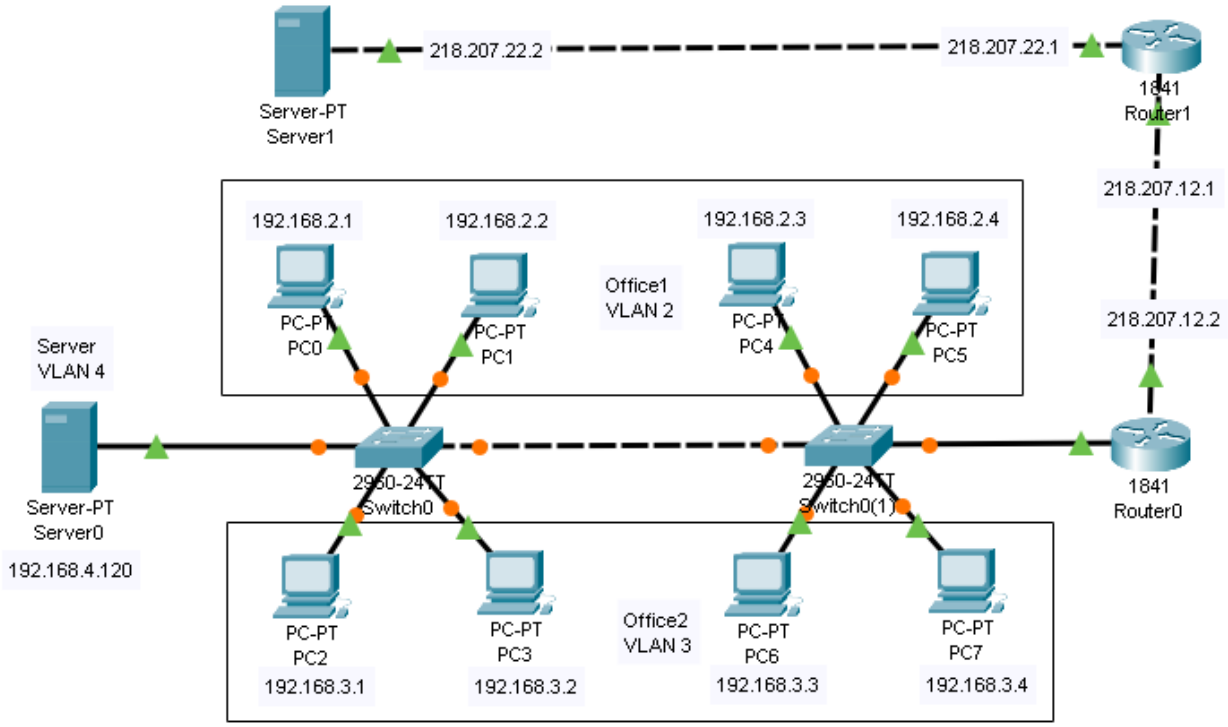

Рис. 1 – Модель комп'ютерної мережі

Далі покроково виконаємо необхідні мережеві налаштування мережевих пристроїв, перевіряючи виконані налаштування.

Спочатку створюємо VLAN з іменами Office1 та Office2, й відповідно налагоджуємо порти access до яких будуть підключені відповідні комп'ютери. Також додаємо VLAN Server до якого буде підключений сервер. Результати на рис. 2 та рис. 3.

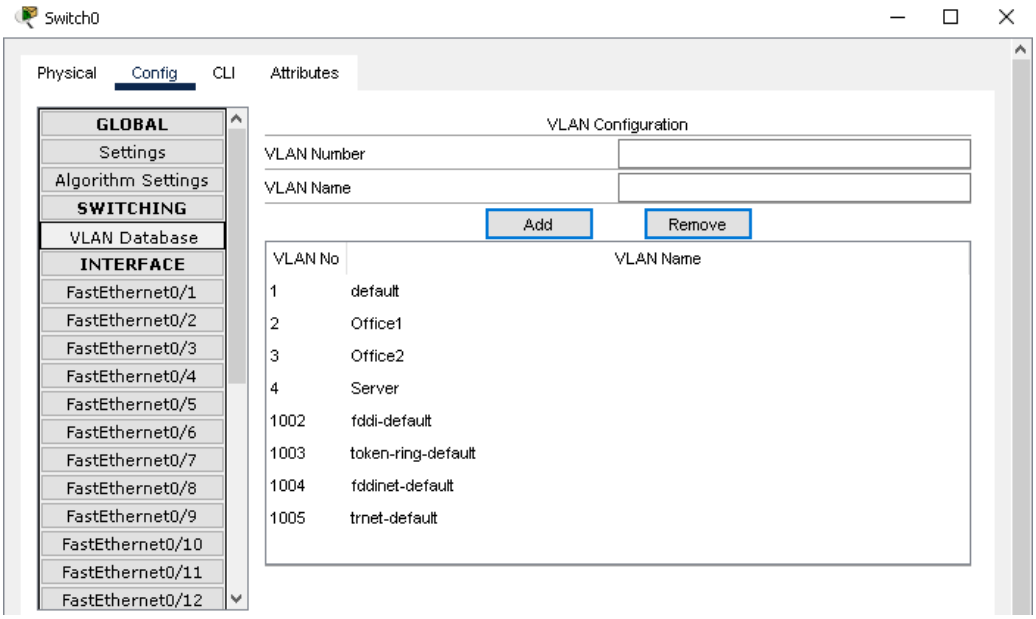

Рис. 2 – Створені VLAN (Switch0)

```
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 4
 switchport mode access
!
```

Рис. 3 – Налаштування портів access (Switch0)

Перевіримо доступність комп'ютера, що був розташований в іншому VLAN, та побачимо, що за відсутності маршрутизатора, комп'ютери з різних VLAN є недоступними один для одного, а комп'ютери в одному VLAN є доступні. Перевірка відбувалася за допомогою команди ping. Також за допомогою таблиці комутації на Switch0 можна побачити MAC-адреси пристроїв, що перевіряли з'єднання.

Далі виконаємо налаштування портів, що називаються магістральними або транковими, для того, щоб комп'ютери в одній VLAN, але підключені до різних комутаторів мали один до одного доступ. Також забезпечимо на Switch0(1) можливість з'єднання до маршрутизатора, надавши, порт gig0/2 в режимі trunk. Результати налаштувань на рисунку 4. Порти access на комутаторі Switch0(1) аналогічні до Switch0, бо Switch0(1) був створений в результаті копіювання Switch0.

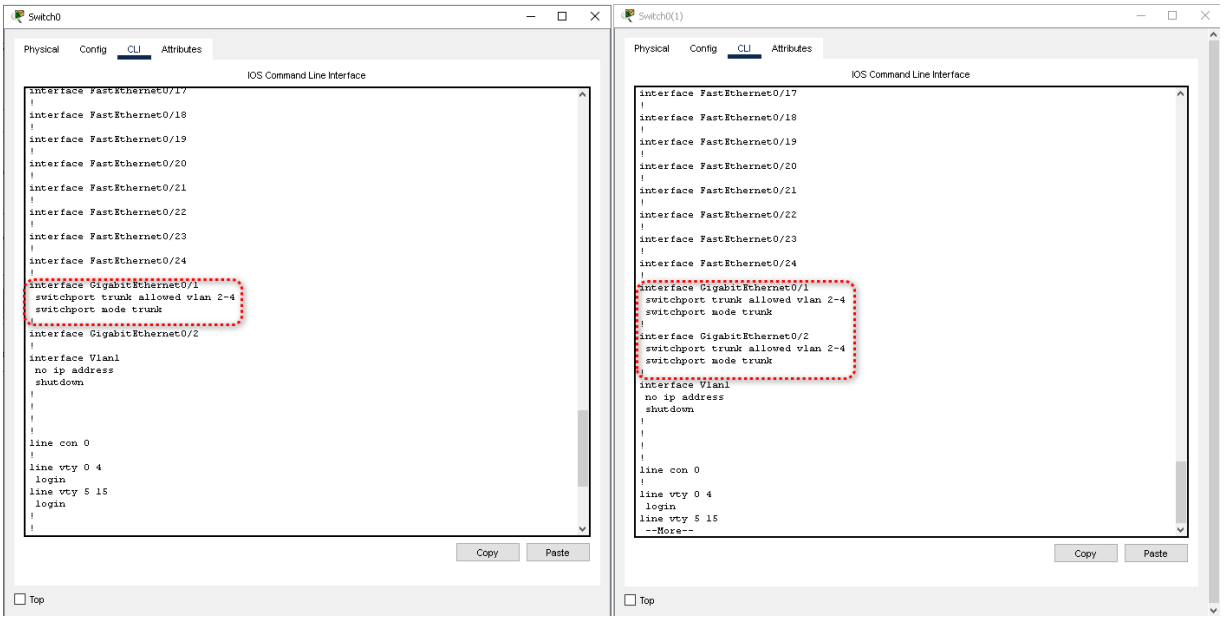

Рис. 4 – Налаштування портів trunk Switch0 та Switch0(1)

Зробимо відповідні перевірки, що комп'ютери, з'єднані через різні комутатори, але, що мають спільну VLAN мають один до одного доступ за допомогою команди ping та перейдемо на наступний крок налаштування мережі.

Далі налаштуємо Router0 та Router1, де Router1 має публічну IP-адресу 218.207.22.2, а Router0 має виділену публічну IP-адресу 218.207.12.2 та для NAT вказуємо який інтерфейс буде зовнішній, а який внутрішній. Також вказуємо перелік IP-адрес усіх підмереж внутрішньої мережі для яких необхідно буде виконувати трансляцію адрес. Результат налаштувань Router0 зображений на рисунку 5.

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.2.10 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.10 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.10 255.255.255.0
 ip nat inside
!
interface FastEthernet0/1
 ip address 218.207.12.2 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router rip
!
ip nat inside source list FOR-NAT interface FastEthernet0/1 overload
ip nat inside source static tcp 192.168.4.120 80 218.207.12.2 80
ip classless
ip route 0.0.0.0 0.0.0.0 218.207.12.1
!
ip flow-export version 9
!
!
ip access-list standard FOR-NAT
 permit 192.168.2.0 0.0.0.255
 permit 192.168.3.0 0.0.0.255
 permit 192.168.4.0 0.0.0.255
!
```

Рис. 5 – Налаштування маршрутизатора Router0

Перевіримо можливість виходу в Інтернет, тобто з’єднання будь якого комп’ютера до сервера Server1, що має IP-адресу 218.207.22.2, та продивимося таблицю трансляції NAT, що можна побачити на рисунку 6.

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 218.207.12.2:80    192.168.4.120:80   ---                ---
```

Рис. 6 – Таблиця трансляції NAT

Відкриємо Web-браузер на Server1 та вказуємо глобальну IP-адресу NAT-маршрутизатора 218.207.12.2. Отримаємо відповідь, що зображена на рисунку 7.

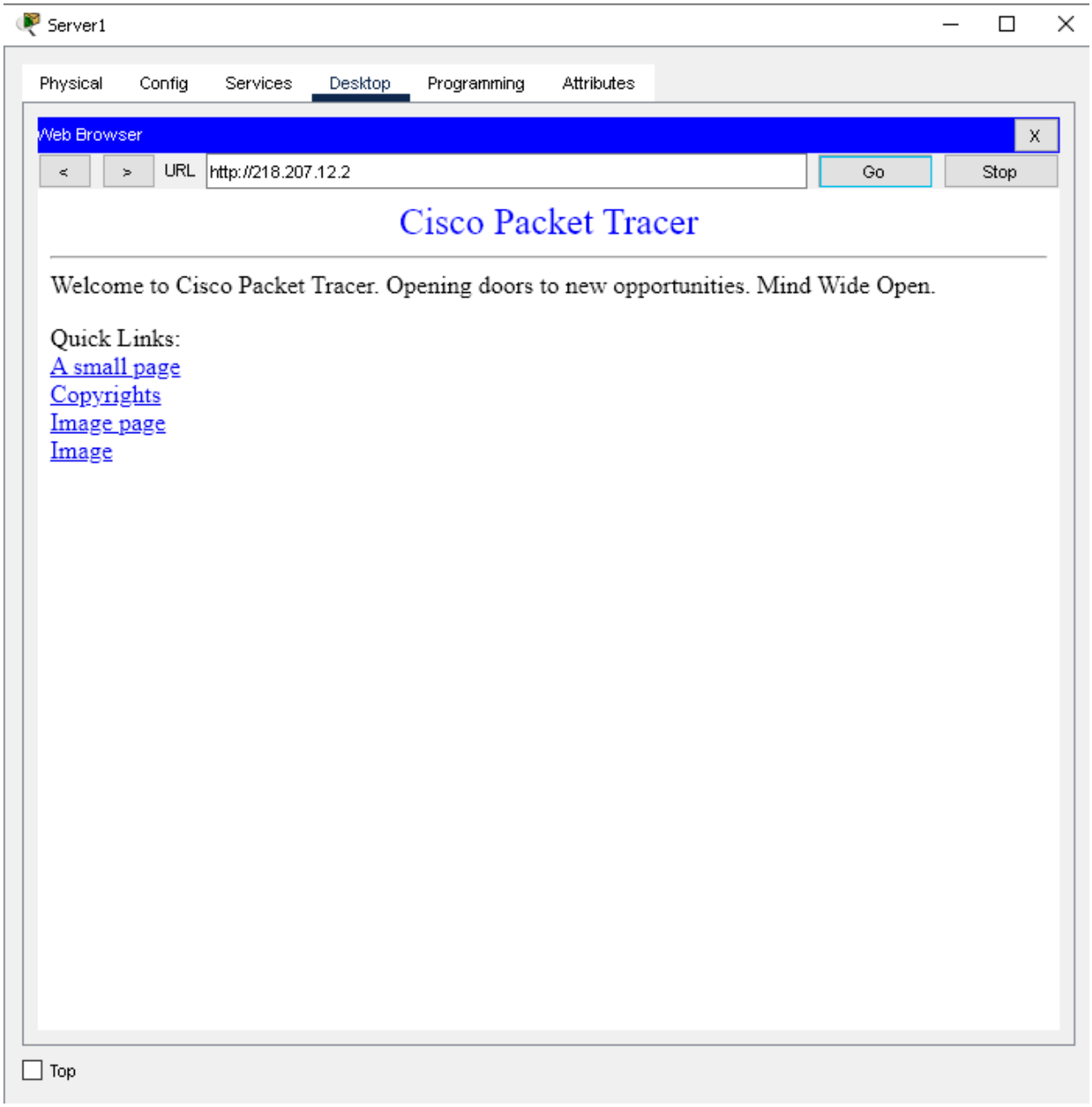

Рис. 7 – HTTP-запит із сервера Server1 до Web-сервера Server0

Далі у режимі симуляції за допомогою утиліти ping дослідимо рух службових пакетів по створеній мережі:

- від хоста у VLAN2 до хоста у VLAN3
- від хоста у VLAN2 до хоста у VLAN4
- від хоста у VLAN3 до хоста у VLAN2
- від хоста у VLAN3 до хоста у VLAN4
- від хоста у VLAN4 до хоста у VLAN2

Та розглянемо результати спостережень нижче.

У всіх випадках при виконанні ping з однієї VLAN мережі до іншої спостерігається один й той же алгоритм. Результати симуляції зображені на рисунку 8.

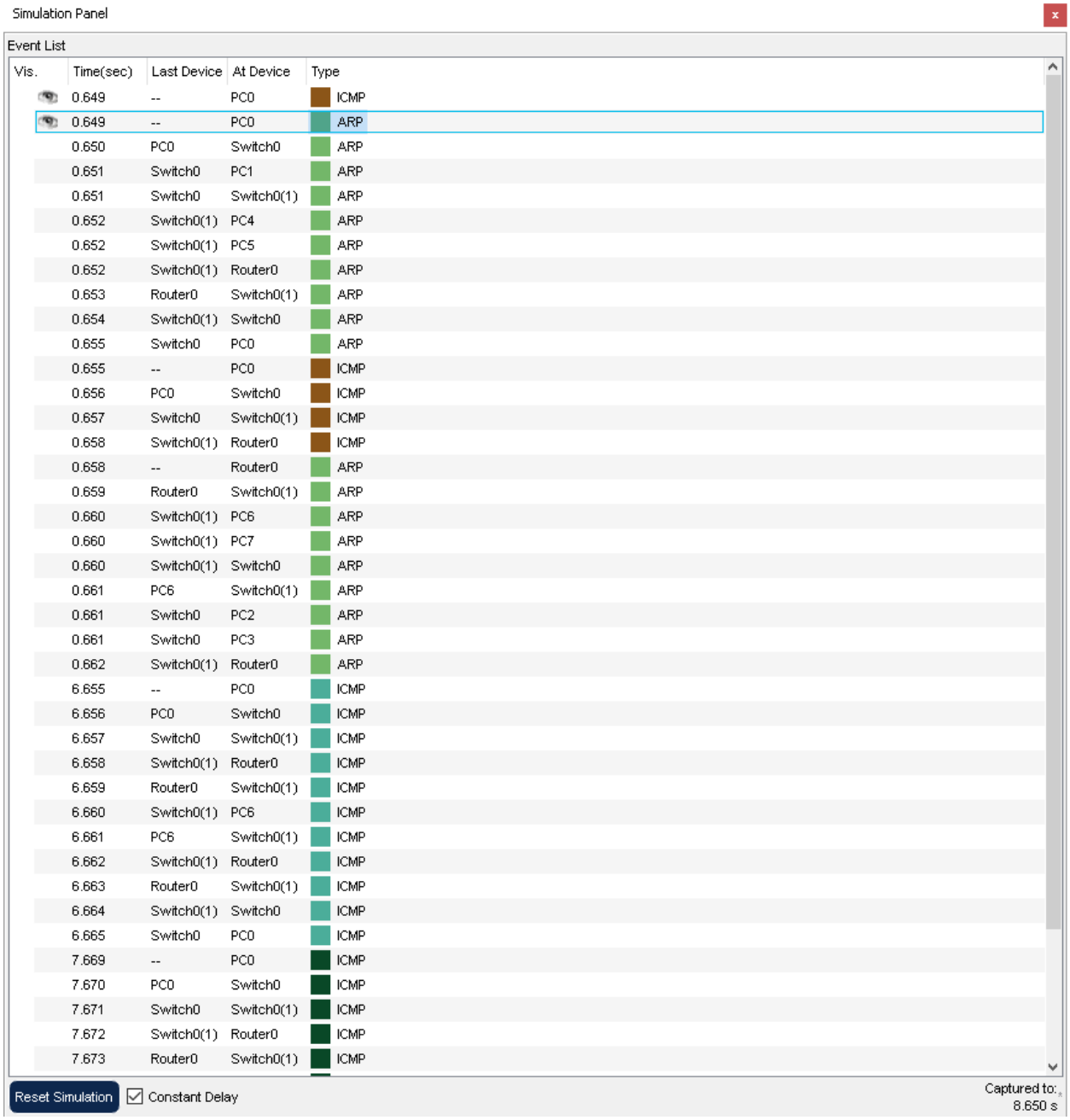

Рис. 8 – Симуляція ping від PC0 до PC6

Початково створюється два пакети, ICMP та ARP на PC0, та ICMP пакет утримується поки ARP пакет знаходить Router0. Далі коли з’ясована адреса маршрутизатора, туди надсилається ICMP пакет. Після надходження ICMP пакету, маршрутизатор надсилає ARP-пакет з метою знайти PC6. Після з’ясування адреси PC6, відбувається повторна відправка ICMP пакету від PC0. Надалі етап з’ясування адреси Router0 від PC0 не потрібен та з’ясування адреси PC6 від Router0 не потрібен для всіх наступних ping. Алгоритм виконання ping надалі можна детально й покроково роздивитися на рисунку 9.

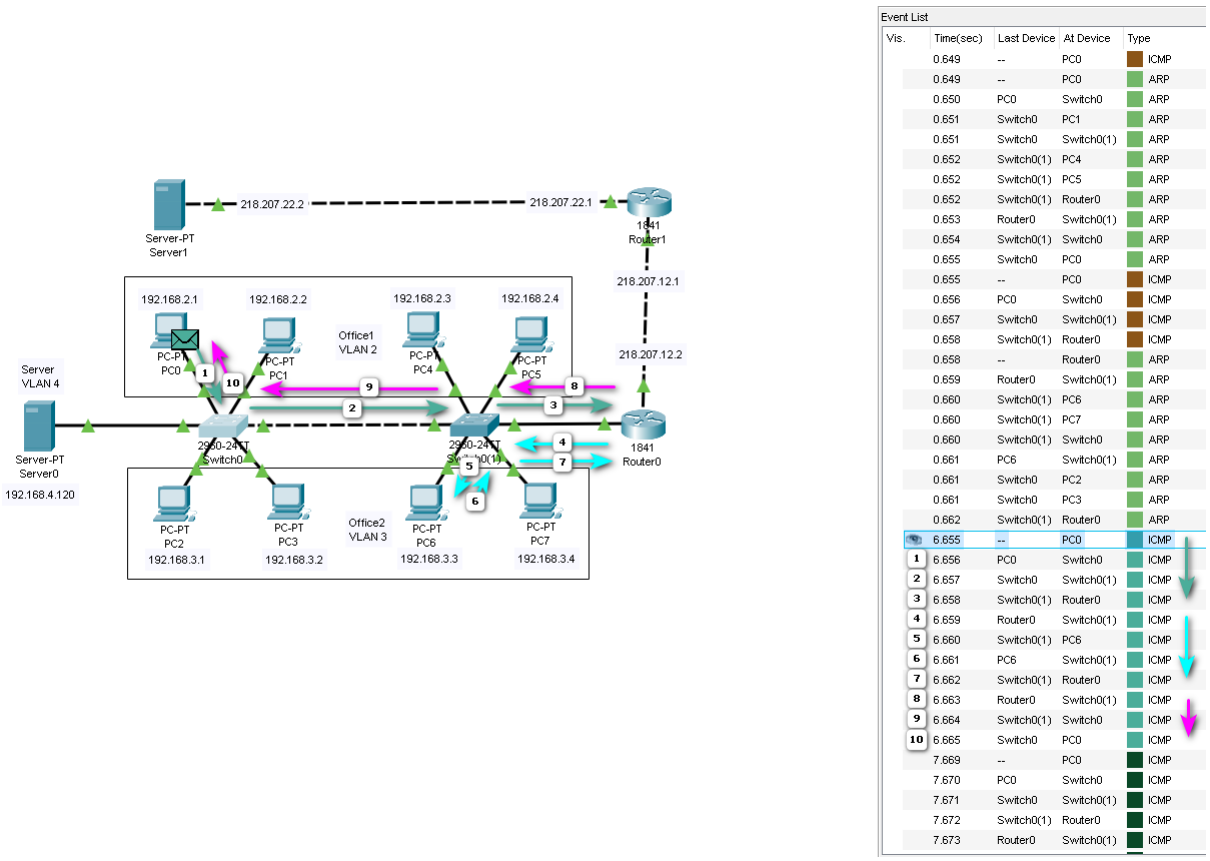

Рис. 9 – Виконання команди ping від PC0 до PC6 покроково

Як можна побачити, пакет початково відправляється на маршрутизатор, далі досягає PC6, повертається відповідь на маршрутизатор, а далі на PC0.

Вміст пакету ICMP, що надсилав PC0 зображений на рисунку 10.

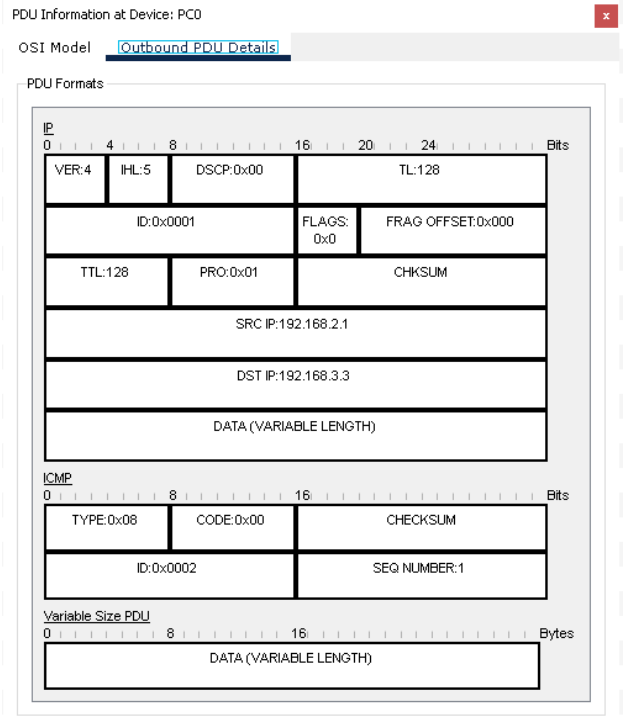

Рис. 10 – Вміст пакету ICMP

Також, подивимося на вміст пакету ARP, що надсилав маршрутизатор, коли бажав знайти PC6 на рисунку 11.

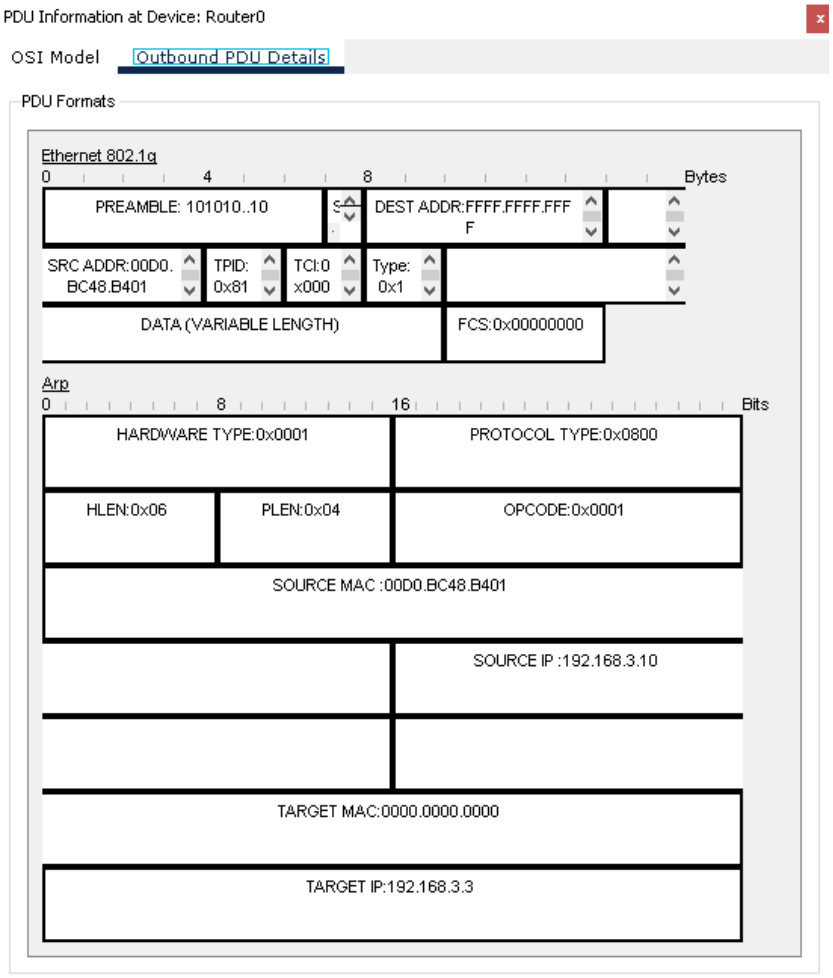

Рис. 11 – Вміст пакету ARP

Надалі у режимі симуляції за допомогою утиліти ping дослідимо рух службових пакетів із внутрішньої мережі до сервера Server1 і в зворотному напрямку.

Почнемо з розгляду ping від Server0 до Server1, що зображено на рисунку 12.

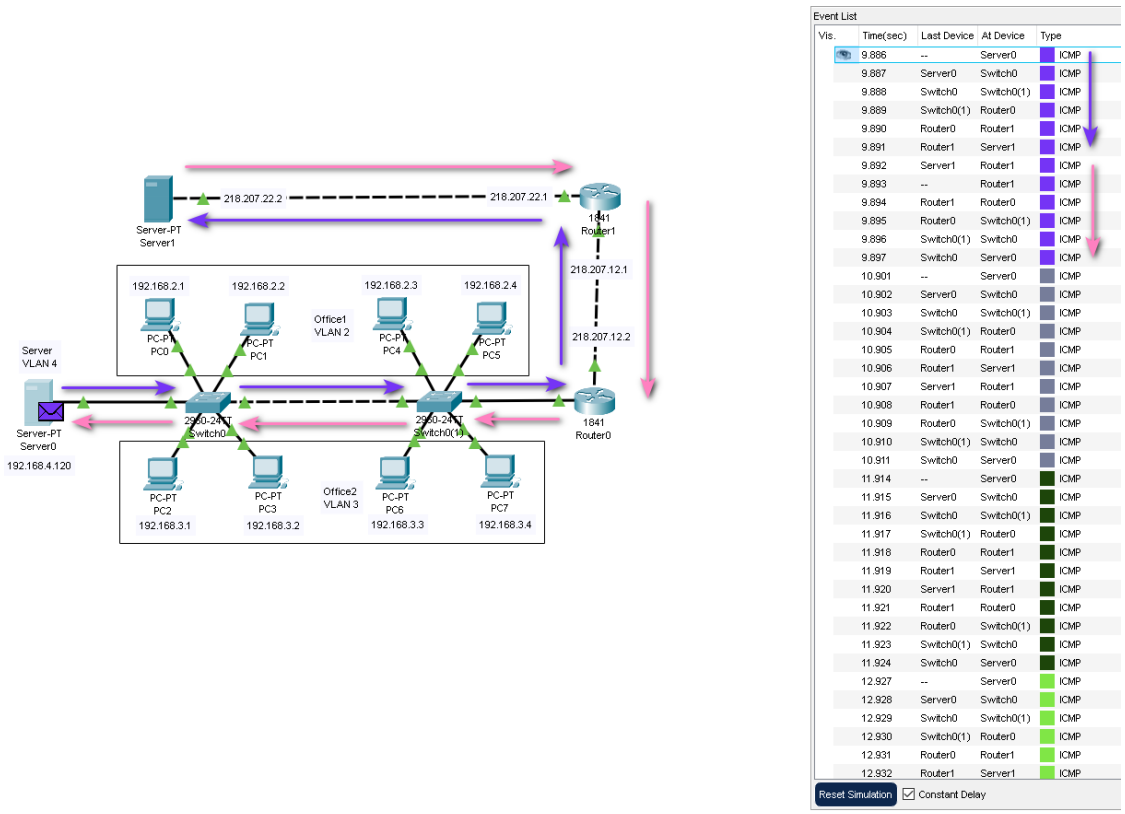

Рис. 12 – ping від Server0 до Server1

Звернемо увагу на пакет ICMP до та після проходження Router, що відповідно зображені на рисунках 13 та 14.

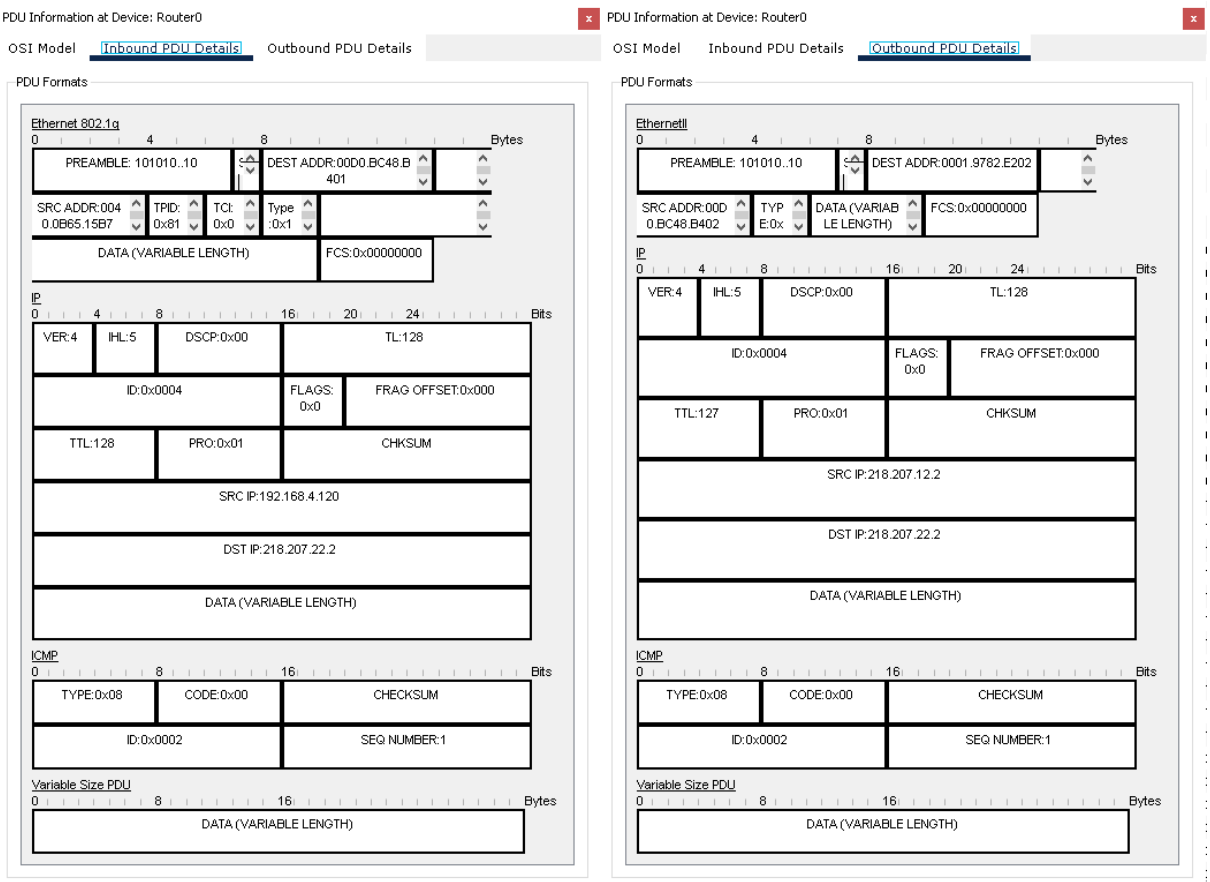

Рис. 13 – Вміст ICMP пакету до проходження Router0

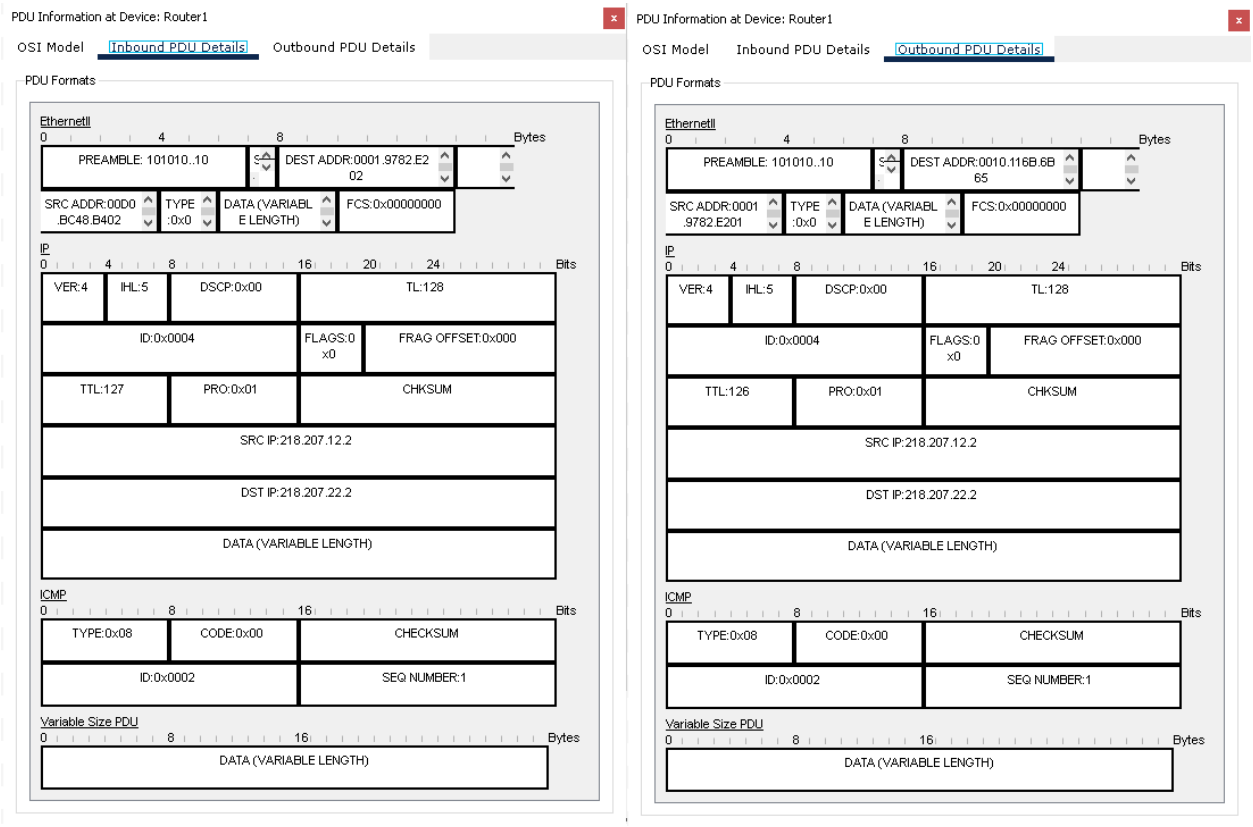

Рис. 14 – Вміст ICMP пакету після проходження Router0

Відповідно можна побачити як відбувається трансляція IP-адреси із внутрішньої у зовнішню.

Аналогічним чином відправимо ping від Server1 до Server0 та побачимо, що при звертанні на внутрішню адресу серверу, пакет не доходить до отримувача, а при звертанні на виділену публічну адресу відповідь надсилає не Server0, а маршрутизатор Router0.

Щоб побачити відповідь від Server0 до Server1 виконаємо HTTP-запит за допомогою Web-браузера на публічну адресу. Результат на рисунку 15.

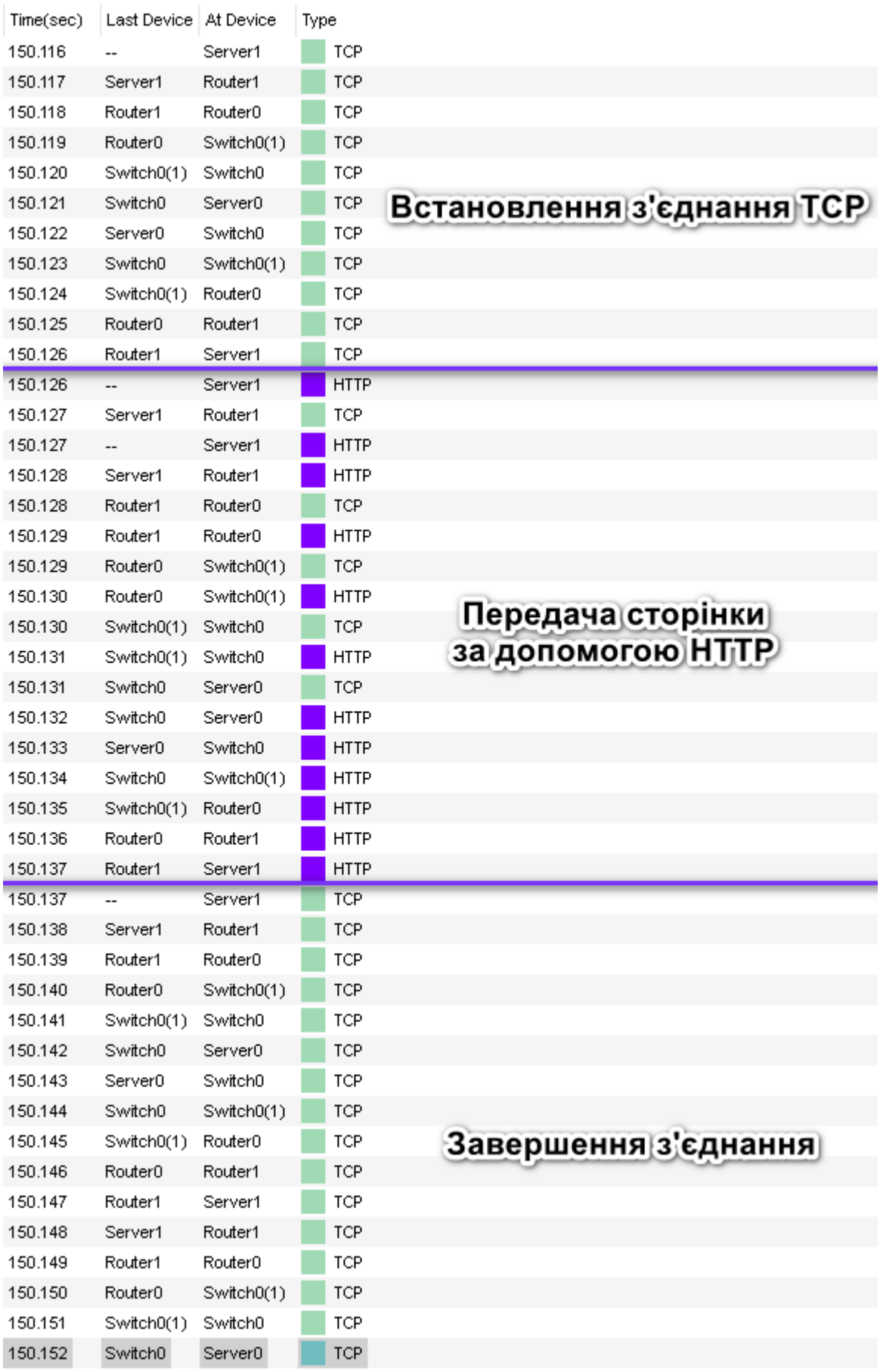

Рис. 15 – HTTP-запит із сервера Server1 до Web-сервера Server0 у режимі симуляції

Розглянемо TCP пакет, що був відправлений від Server1 на публічну адресу та побачимо трансляцію адреси з публічної у локальну IP-адресу серверу Server0 на рисунку 16.

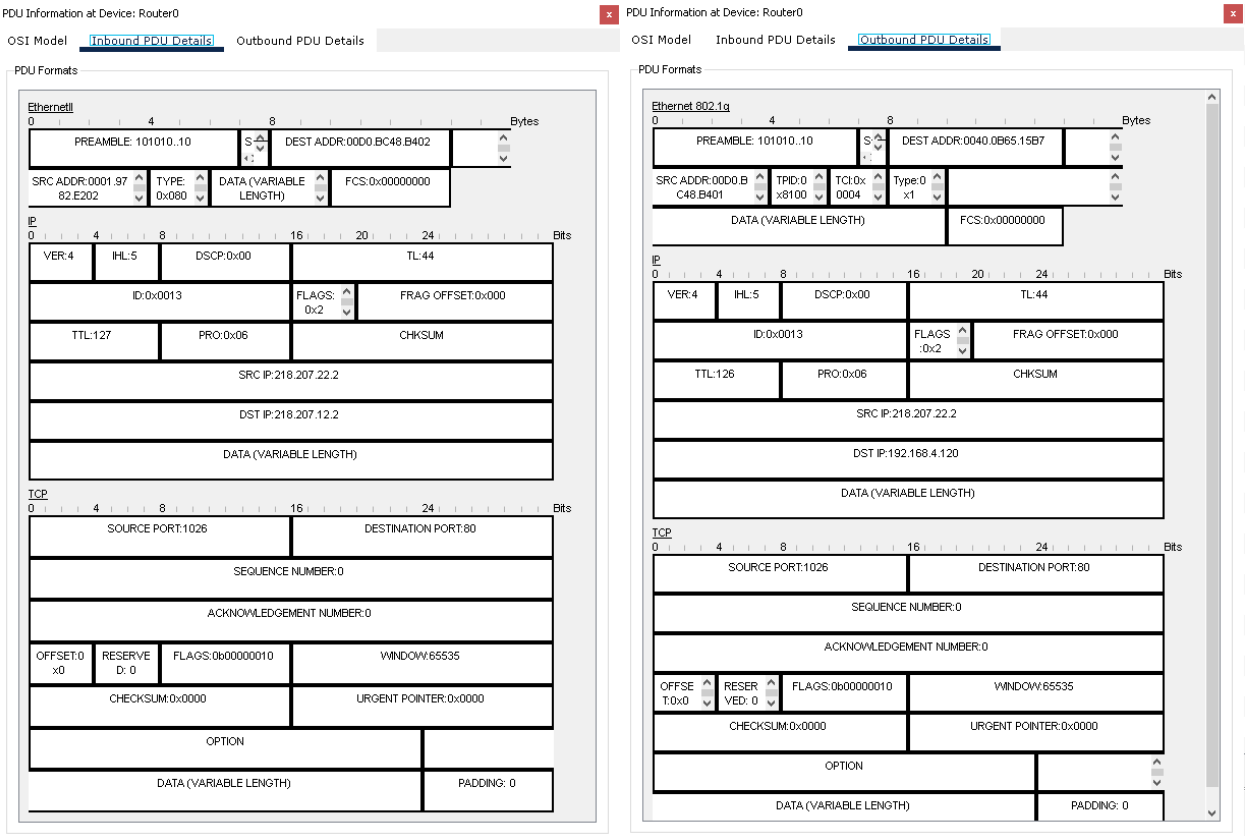

Рис. 16 – TCP пакет при проходженні Router0 від Server1 до Server0

Висновок

У ході виконання лабораторної роботи було розглянуто принципи роботи технологій VLAN і NAT, їх застосування та налаштування у мережі.
Було виконано:

1. **Налаштування VLAN** – створені віртуальні мережі, призначені порти Access і Trunk, перевірено ізоляцію між VLAN.
2. **Налаштування маршрутизатора** – реалізована маршрутизація між VLAN через підінтерфейси.
3. **Налаштування NAT** – створені правила трансляції, перевірена передача пакетів між локальною мережею та Інтернетом.
4. **Аналіз трафіку** – проведено тестування доступності між пристроями за допомогою ping та аналізу таблиць комутації, маршрутизації та трансляції.

За результатами роботи було підтверджено, що VLAN забезпечує логічне розділення мережі без зміни фізичної структури, а NAT дозволяє комп’ютерам локальної мережі отримувати доступ до зовнішньої мережі без використання реальних публічних IP-адрес. Усі налаштування працюють коректно, що підтверджено перевірками та симуляцією трафіку.