



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

**Лабораторна робота №10**  
*з дисципліни «Комп'ютерні мережі»*

**«Організація доступу до комп'ютерної мережі  
Технології VLAN та NAT»**

Виконала студентка групи: КВ-11  
ПІБ: Михайліченко Софія Віталіївна

Перевірив: \_\_\_\_\_

## ***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 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 VLAN4.
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 до лабораторної роботи***

1. Побудувати модель комп'ютерної мережі, яка зображена на рисунку
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 VLAN4 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.
5. Із сервера Server1 виконайте http-запит до Web-сервера Server0. Отриманий результат занесіть у звіт.

## ***Короткі теоретичні відомості:***

VLAN (Virtual Local Area Network) VLAN - це технологія в маршрутизаторах і комутаторах, яка дозволяє на одному фізичному мережевому інтерфейсі створювати кілька віртуальних локальних мереж. VLAN використовують для створення логічної топології мережі, яка не залежить від фізичної топології.

VLAN дозволяє:

- Об'єднувати на каналному рівні в єдину мережу комп'ютери, які під'єднані до різних комутаторів.
- Розділяти в різні підмережі комп'ютери, які під'єднані до одного комутатора.
- Розділяти гостьові Wi-Fi мережі і Wi-Fi мережі підприємства.

Переваги використання VLAN:

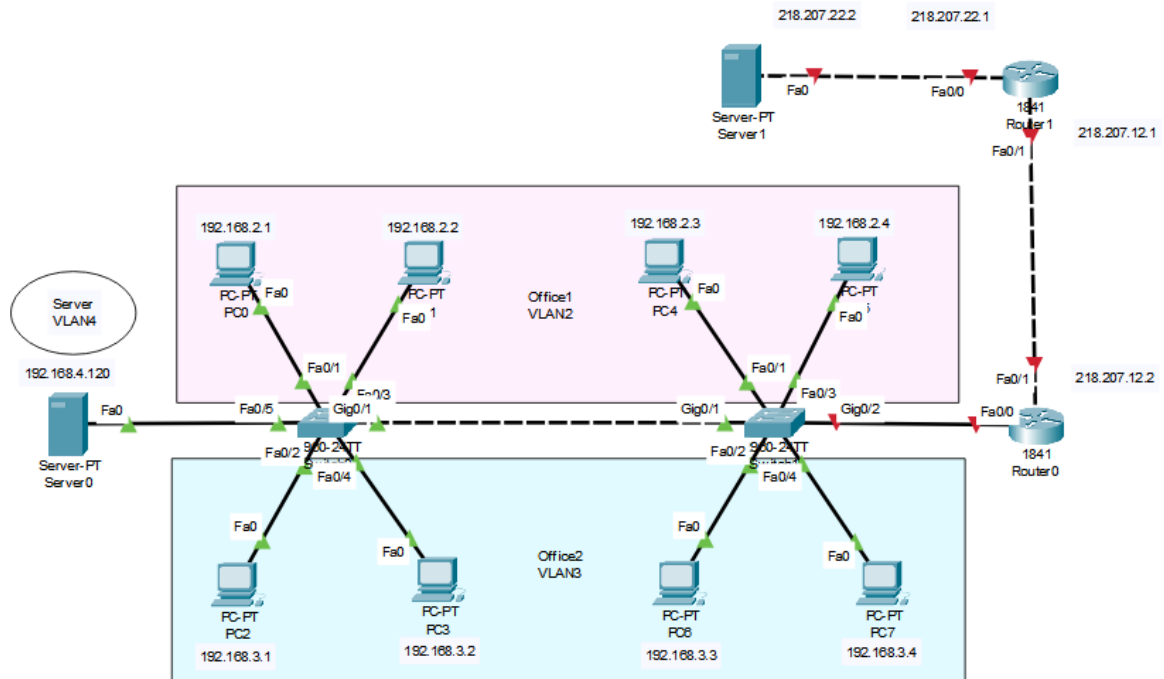
- Гнучке розділення мережевих пристроїв на групи.
- Зменшення широкомовного трафіку в мережі.
- Підвищення безпеки і керованості в мережі.
- Зменшення кількості обладнання і мережевого кабелю.

Ідентифікація VLAN. Тегований і нетегований VLAN Кожний VLAN-домен ідентифікується за допомогою числової мітки - VLAN ID. Порти комутатора поділяються на нетеговані (access) і теговані (trunk). Тегований трафік містить інформацію про належність до VLAN.

Технологія перетворення мережевих адрес NAT NAT - це технологія, яка дозволяє перетворювати приватні IP-адреси у публічні (зовнішні) IP-адреси. Основні типи NAT: статична адресна трансляція, динамічна адресна трансляція, Port Address Translation (NAT Overload). NAT дозволяє забезпечити пряму взаємодію хостів в Інтернеті з маршрутизатором, який підтримує NAT, а не з хостом в локальній мережі.

## Порядок виконання роботи:

### Побудова досліджуваної топології



Виконаємо всі налаштування користуючись інтерфейсом командного рядка(CLI).

Створимо два VLAN з іменами Office1 та Office2 з одним комутатором і налаштуємо на інтерфейсах порти access, до яких потім будуть підключені комп'ютери.

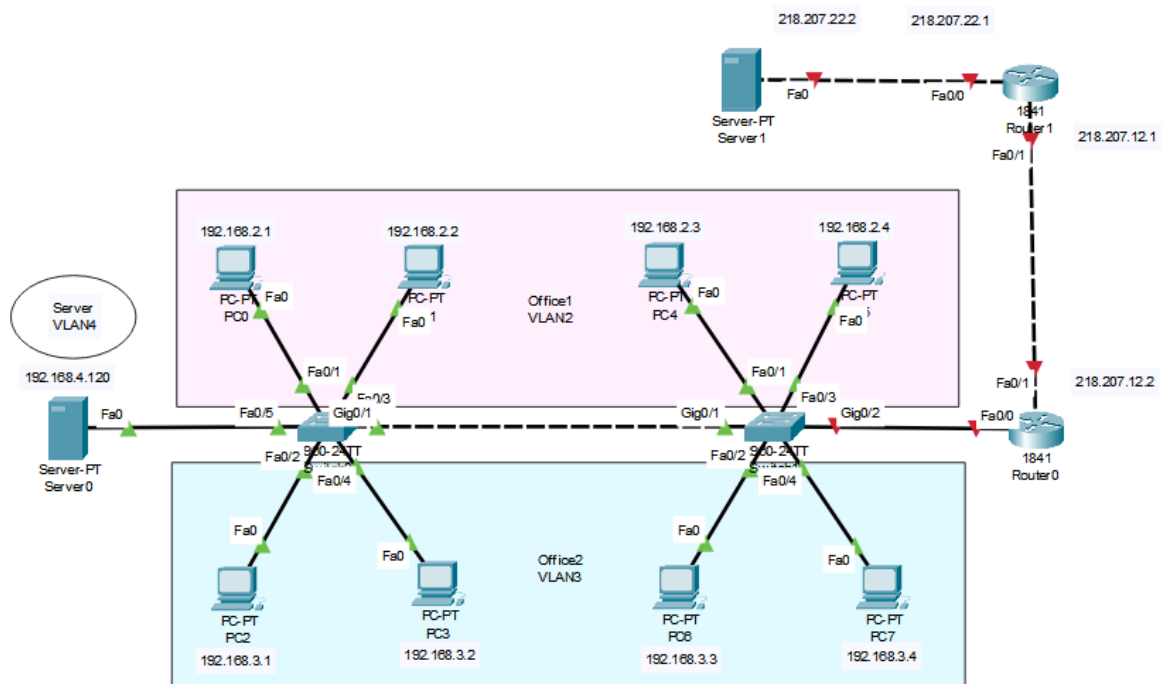
```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name Office1
Switch(config-vlan)#exit
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name Office2
Switch(config-vlan)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#int fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Перевіряємо виконані налаштування:

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
2	Office1	active	Fa0/1, Fa0/3
3	Office2	active	Fa0/2, Fa0/4
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Switch#



Потім виконаємо мережеві налаштування комп'ютерів PC0÷PC3:

PC0

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.2.1

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

PC1

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.2.2

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

PC2

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.3.1

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

PC3

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

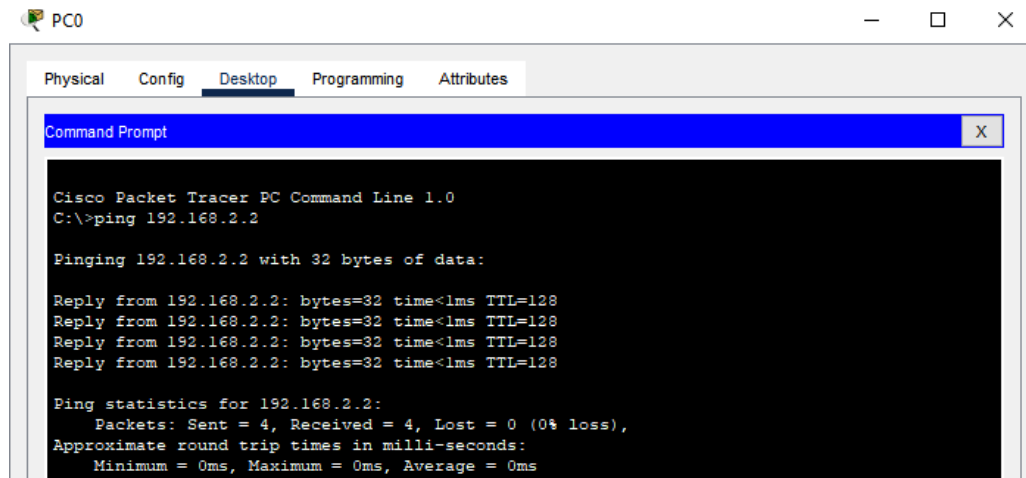
IPv4 Address 192.168.3.2

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

Перевіримо доступність комп'ютера, який розташований в тому ж VLAN, що і комп'ютер PC0. Із командного рядка PC0 виконаємо команду ping:



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

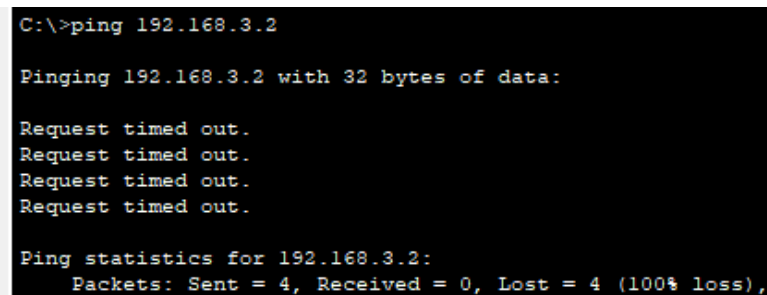
Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Перевіримо доступність комп'ютера, який розташований в іншому VLAN. Із командного рядка PC0 виконаємо команду ping.

Маємо спостерігати, що комп'ютер з іншого VLAN недоступний:



```
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

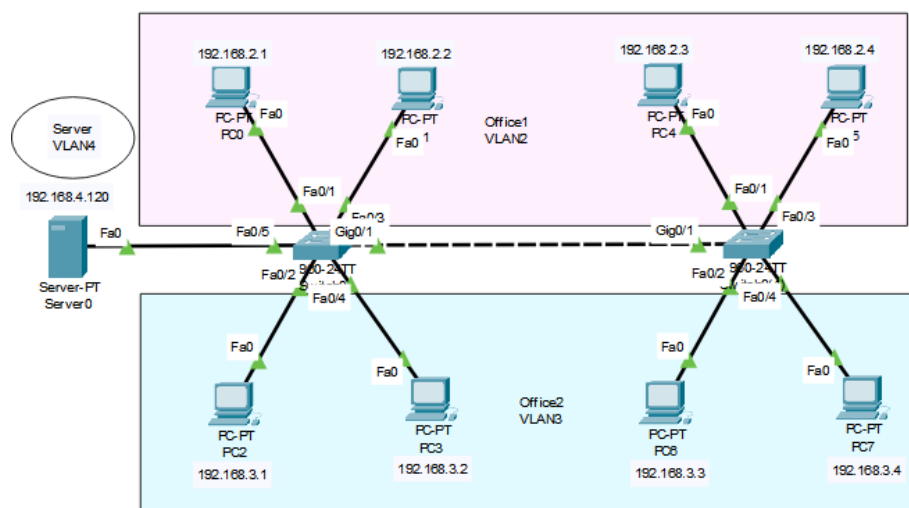
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Наступним перевіримо таблицю комутації:

```
Switch>enable
Switch#show mac address-table
      Mac Address Table
-----
Vlan  Mac Address      Type      Ports
---  -
1     000a.f3c1.e819     DYNAMIC   Gig0/1
2     0003.e40b.a53d     DYNAMIC   Fa0/1
2     0004.9a21.9e9a     DYNAMIC   Fa0/3
```

Додамо до досліджуваної схеми ще кілька сегментів: комутатор Switch0(1) з комп'ютерами PC4÷ PC7 та сервер Server0. Сервер Server0 виділяємо в окрему підмережу VLAN4.



Комутатори Switch0 та Switch0(1) з'єднуємо через швидкісні порти Gigabit, а сервер Server0 із VLAN4 підключаємо до порту fa0/5 комутатора Switch0. Виконуємо налаштування на комутаторі Switch0. Спочатку до інтерфейсу fa0/5 підключимо Server0:

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

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

Тепер налаштуємо гігабітний порт gig0/1. Через цей порт буде проходити трафік усіх підмереж: VLAN2, VLAN3 та VLAN4. В термінології Cisco такі порти називаються магістральними або транковими (trunk).

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int gig0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Switch(config-if)#switchport trunk allowed vlan 2,3,4
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

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

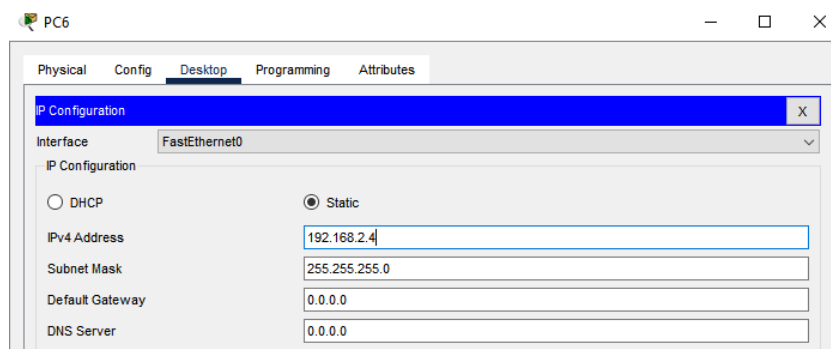
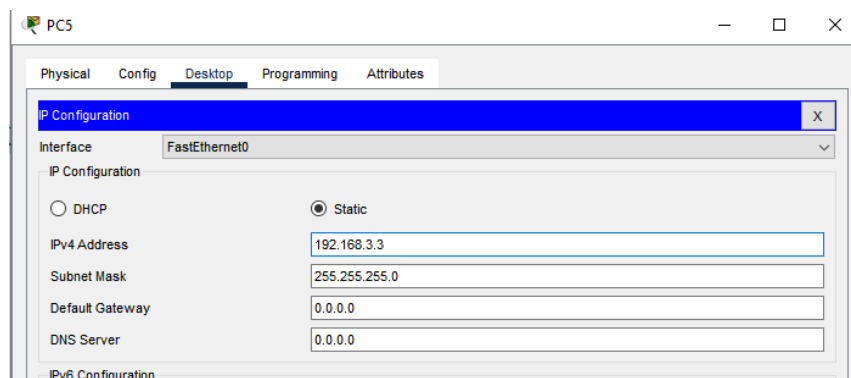
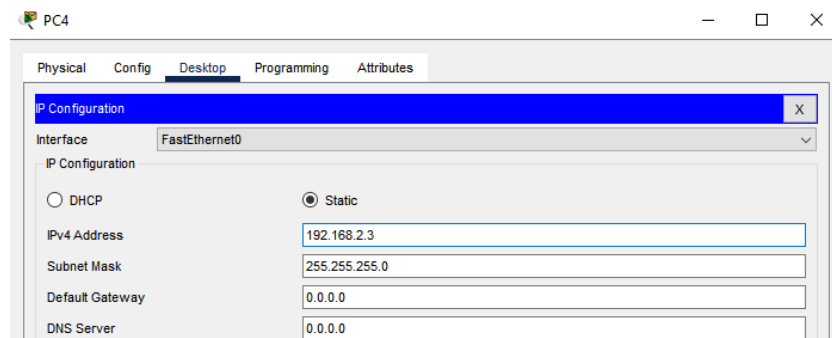


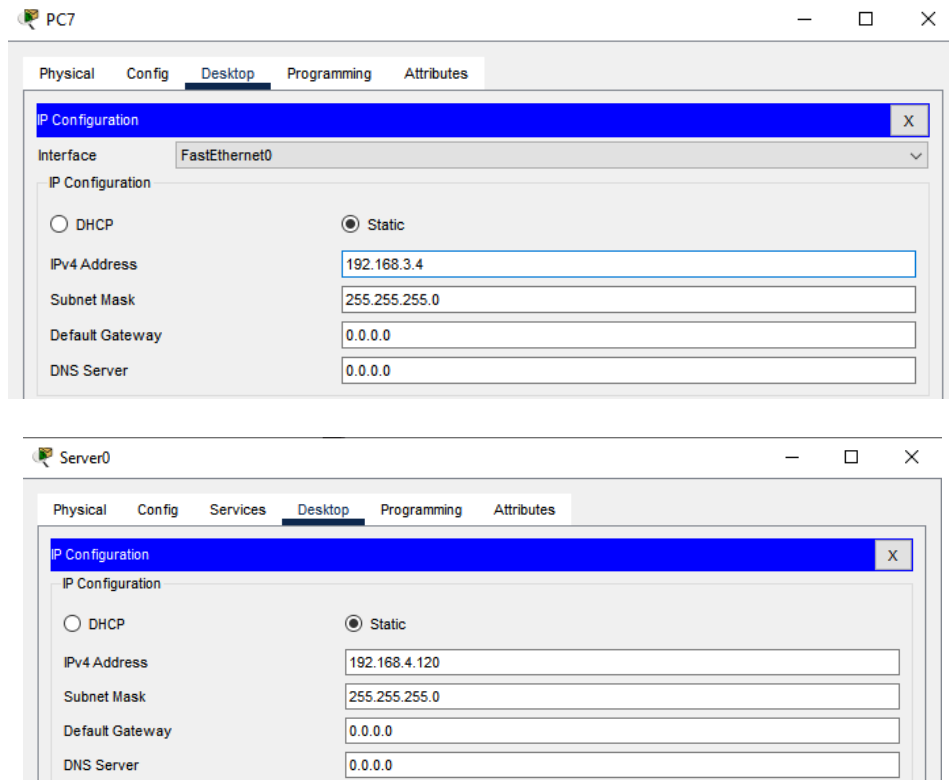
Такі ж налаштування виконаємо на порту gig0/1 комутатора Switch0(1):

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 4
Switch(config-vlan)#exit
Switch(config)#int gig0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 2,3,4
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

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

Виконаємо мережеві налаштування комп'ютерів PC4÷PC7 та сервера Server0:





Налаштування портів fa0/1, fa0/2, fa0/3 і fa0/4 комутатора Switch0(1) виконується аналогічно налаштуванням відповідних інтерфейсів комутатора Switch0:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name Office1
Switch(config-vlan)#exit
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name Office2
Switch(config-vlan)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport sccess vlan 3
      ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#int fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

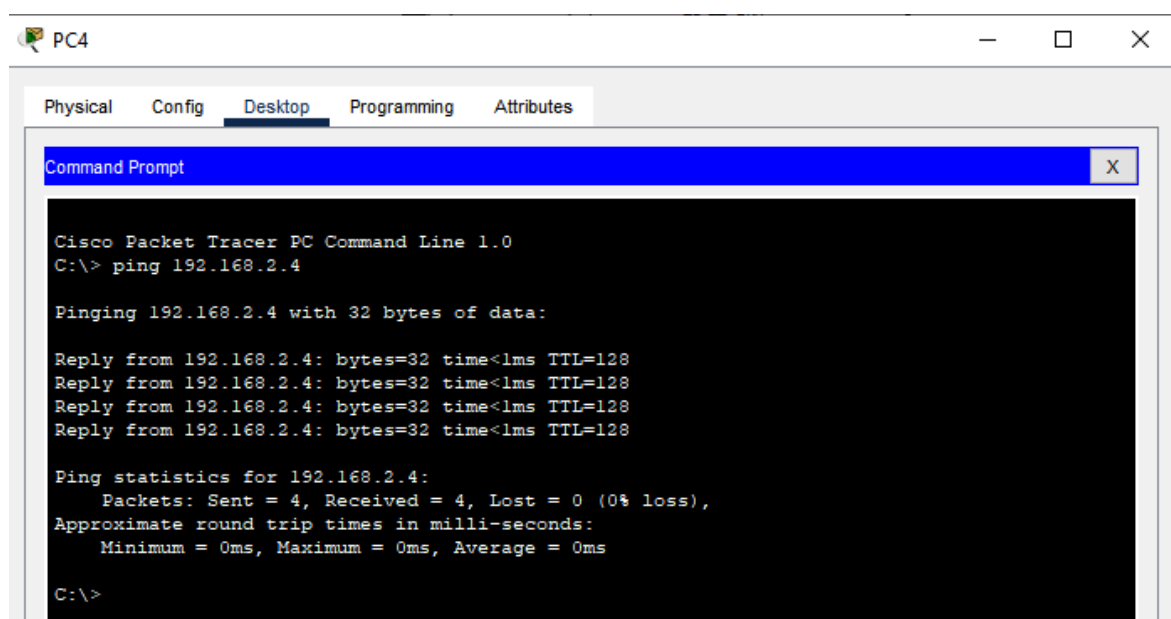
Перевірка виконаних налаштувань шляхом виклику команди `show vlan brief`, що показує створені моделі VLAN:

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/2
2	Officel	active	Fa0/1, Fa0/3
3	Office2	active	Fa0/2, Fa0/4
4	VLAN0004	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
Switch#
```

Перевіримо доступність комп'ютера, який розташований в тому ж VLAN, що і комп'ютер PC4. Із командного рядка PC4 виконаємо команду `ping`:



```
PC4
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\> ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Перевіримо доступність комп'ютера, який розташований в іншому VLAN. Із командного рядка PC4 виконаємо команду `ping`:

```
C:\> ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

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

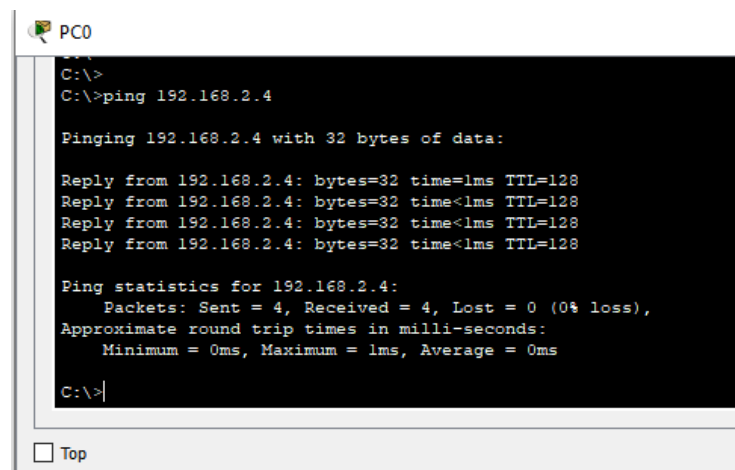
Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Спостерігаємо, що комп'ютер з іншого VLAN недоступний.

Перевіримо тепер таблицю комутації:

```
Switch>enable
Switch#show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0001.43b6.c919    DYNAMIC   Gig0/1
2       0001.43b6.c919    DYNAMIC   Gig0/1
2       000c.cfc8.e597    DYNAMIC   Fa0/1
2       0030.f2b9.6cde    DYNAMIC   Fa0/3
3       0001.43b6.c919    DYNAMIC   Gig0/1
4       0001.43b6.c919    DYNAMIC   Gig0/1
Switch#
```

Отже, створена схема складається із трьох VLAN'ів. Доступність комп'ютерів, які входять до складу одного VLAN перевіряємо за допомогою утиліти ping.



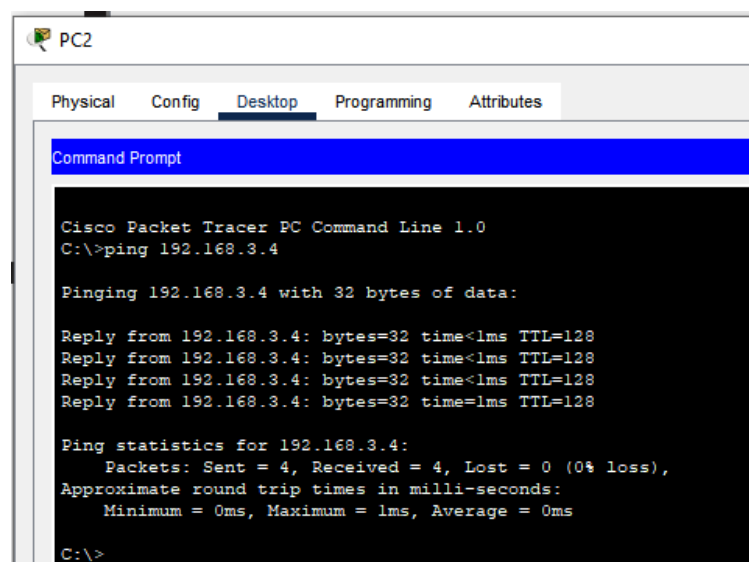
```
PC0
C:\>
C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```



```
PC2
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.4

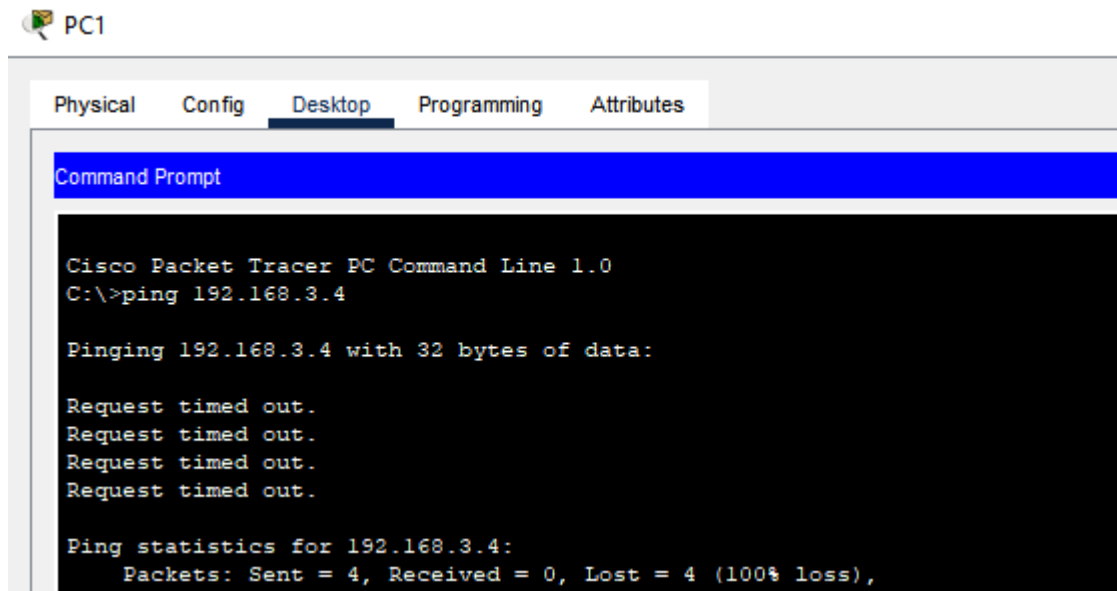
Pinging 192.168.3.4 with 32 bytes of data:

Reply from 192.168.3.4: bytes=32 time<1ms TTL=128
Reply from 192.168.3.4: bytes=32 time<1ms TTL=128
Reply from 192.168.3.4: bytes=32 time<1ms TTL=128
Reply from 192.168.3.4: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

За допомогою утиліти ping можна впевнитися, що комп'ютери, які знаходяться у різних підмережах (VLAN) не можуть обмінюватися пекетами. Для їхньої взаємодії потрібний пристрій, що працює на мережевому рівні (маршрутизатор).



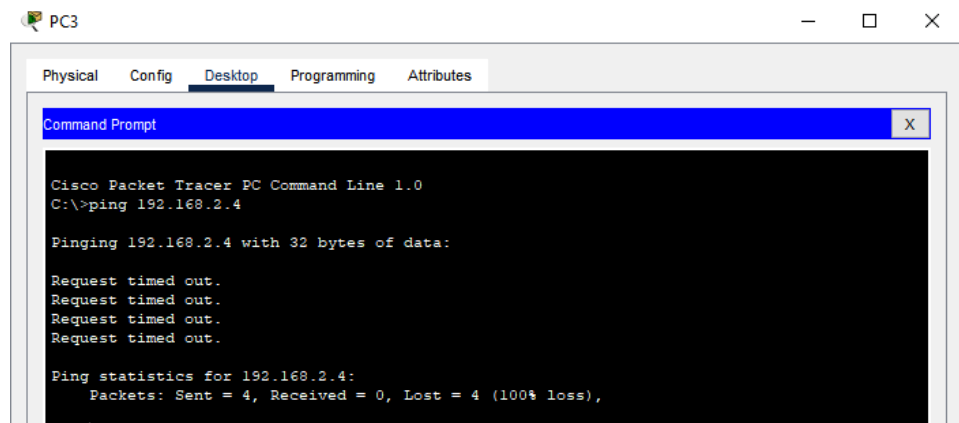
The screenshot shows the 'PC1' window in Cisco Packet Tracer. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The text in the command prompt is as follows:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

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

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



The screenshot shows the 'PC3' window in Cisco Packet Tracer. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The text in the command prompt is as follows:

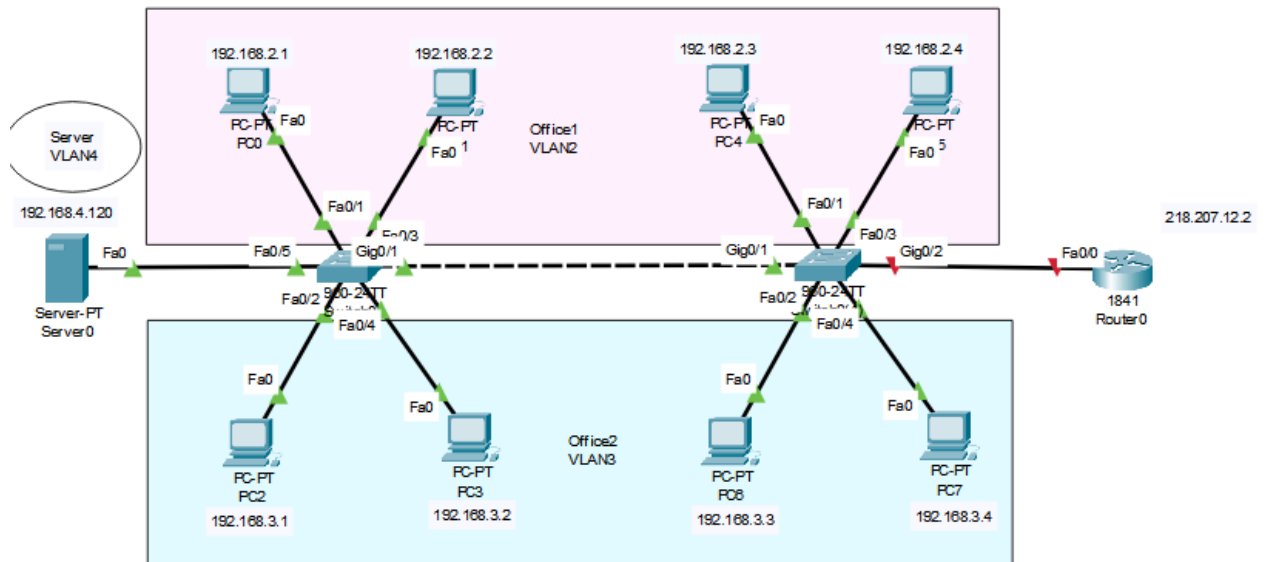
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

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

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Щоб забезпечити доступ комп'ютерів різних VLAN один до одного, додамо до нашої схеми маршрутизатор Router0 Cisco 1841:



Виконуємо налаштування інтерфейсу gig0/2 на комутаторі Switch0(1):

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int gig0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 2,3,4
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

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

Виконуємо налаштування інтерфейсу fa0/0 маршрутизатора Router0. Переходимо на маршрутизатор. По замовчуванню всі інтерфейси маршрутизатора відключені, тому спочатку потрібно включити інтерфейс fa0/0 командою no shutdown (скорочено no shut).

Через інтерфейс fa0/0 маршрутизатора проходить трафік VLAN2, VLAN3 і VLAN4. Тому на інтерфейсі fa0/0 потрібно створити три підінтерфейси (subinterfaces):

```

Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#int fa0/0.2
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up

Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 192.168.2.10 255.255.255.0
Router(config-subif)#no shut
Router(config-subif)#exit
Router(config)#int fa0/0.3
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up

Router(config-subif)#encapsulation dot1
Router(config-subif)#encapsulation dot1Q q
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 192.168.3.10 255.255.255.0
Router(config-subif)#no shut
Router(config-subif)#exit
Router(config)#int fa0/0.4
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.4, changed state to up

Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ip address 192.168.4.10 255.255.255.0
Router(config-subif)#no shut
Router(config-subif)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
Building configuration...
[OK]

```

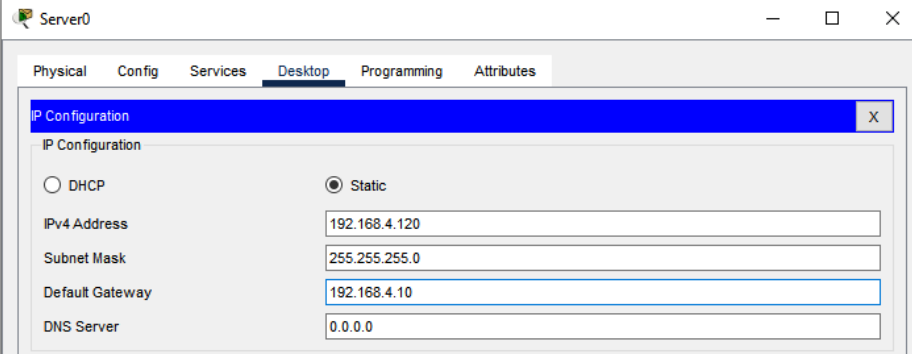
Перевіряємо виконані налаштування:

```

!
!
!
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
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.10 255.255.255.0
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.10 255.255.255.0
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!

```

Тепер потрібно повернутися до мережевих налаштувань сервера Server0 і комп'ютерів PC0÷PC7 і вказати в налаштуваннях IP-адресу шлюзу по замовчуванню – це IP-адреси відповідних підінтерфейсів маршрутизатора Router0:



Server0

Physical Config Services **Desktop** Programming Attributes

IP Configuration

IP Configuration

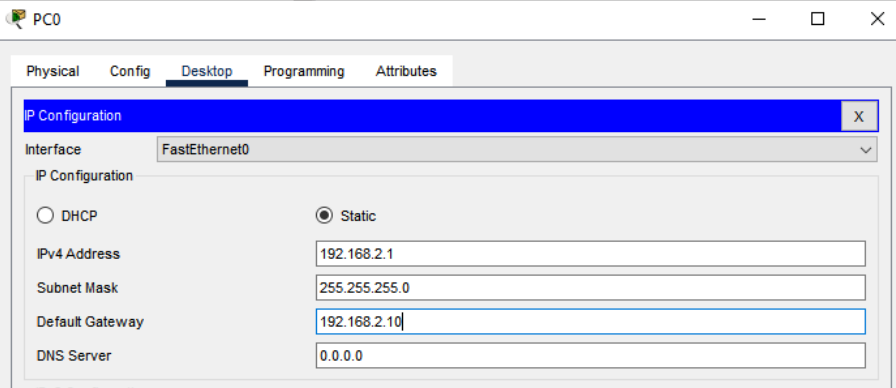
☐ DHCP ☒ Static

IPv4 Address 192.168.4.120

Subnet Mask 255.255.255.0

Default Gateway 192.168.4.10

DNS Server 0.0.0.0



PC0

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

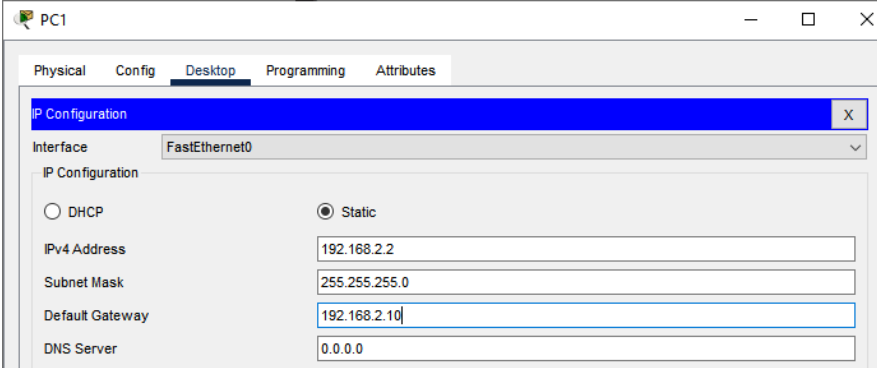
☐ DHCP ☒ Static

IPv4 Address 192.168.2.1

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.10

DNS Server 0.0.0.0



PC1

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

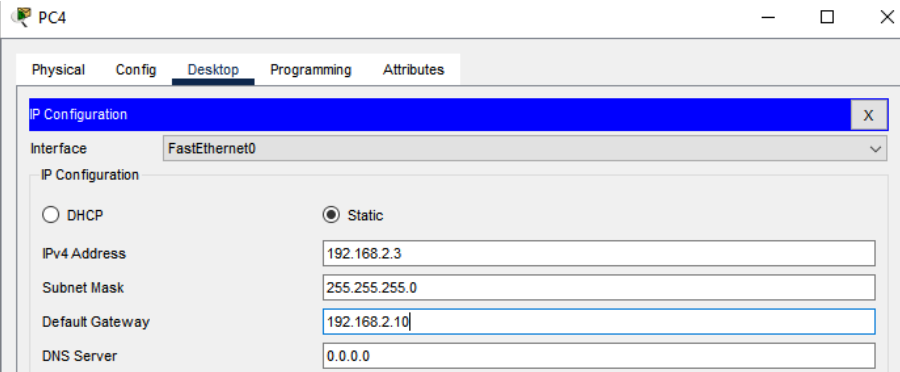
☐ DHCP ☒ Static

IPv4 Address 192.168.2.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.10

DNS Server 0.0.0.0



PC4

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.2.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.10

DNS Server 0.0.0.0



PC5

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.2.4

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.10

DNS Server 0.0.0.0

PC2

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.3.1

Subnet Mask 255.255.255.0

Default Gateway 192.168.3.10

DNS Server 0.0.0.0

PC3

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.3.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.3.10

DNS Server 0.0.0.0

PC6

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

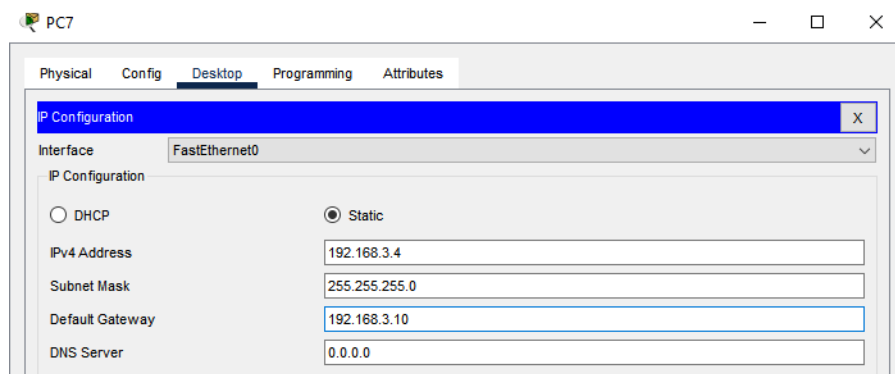
☐ DHCP ☒ Static

IPv4 Address 192.168.3.3

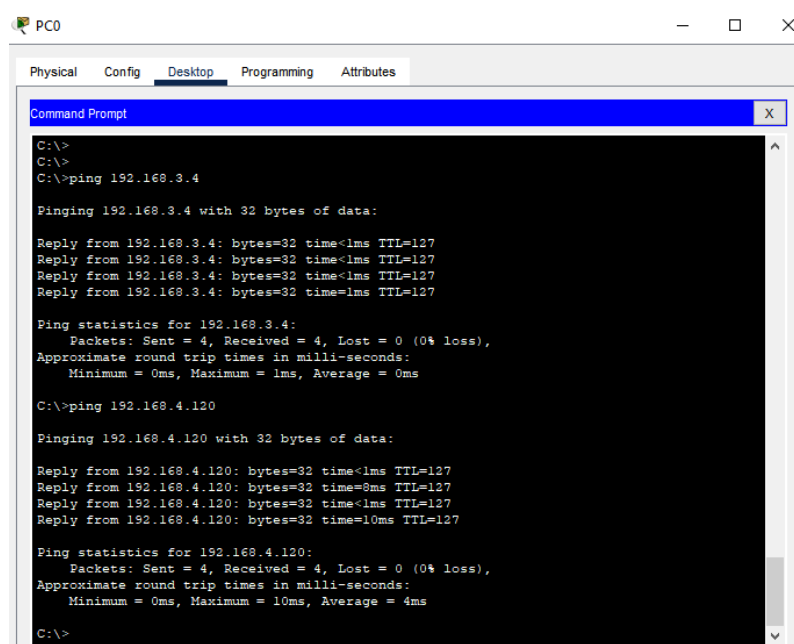
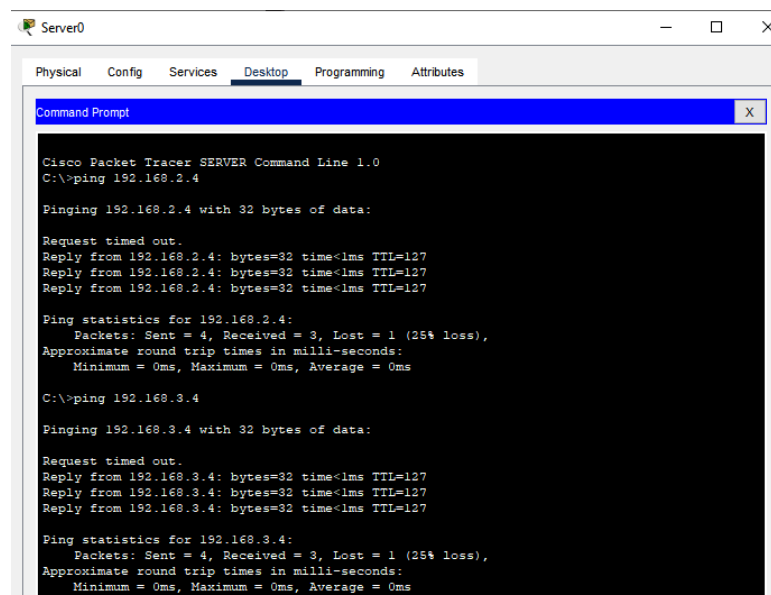
Subnet Mask 255.255.255.0

Default Gateway 192.168.3.10

DNS Server 0.0.0.0



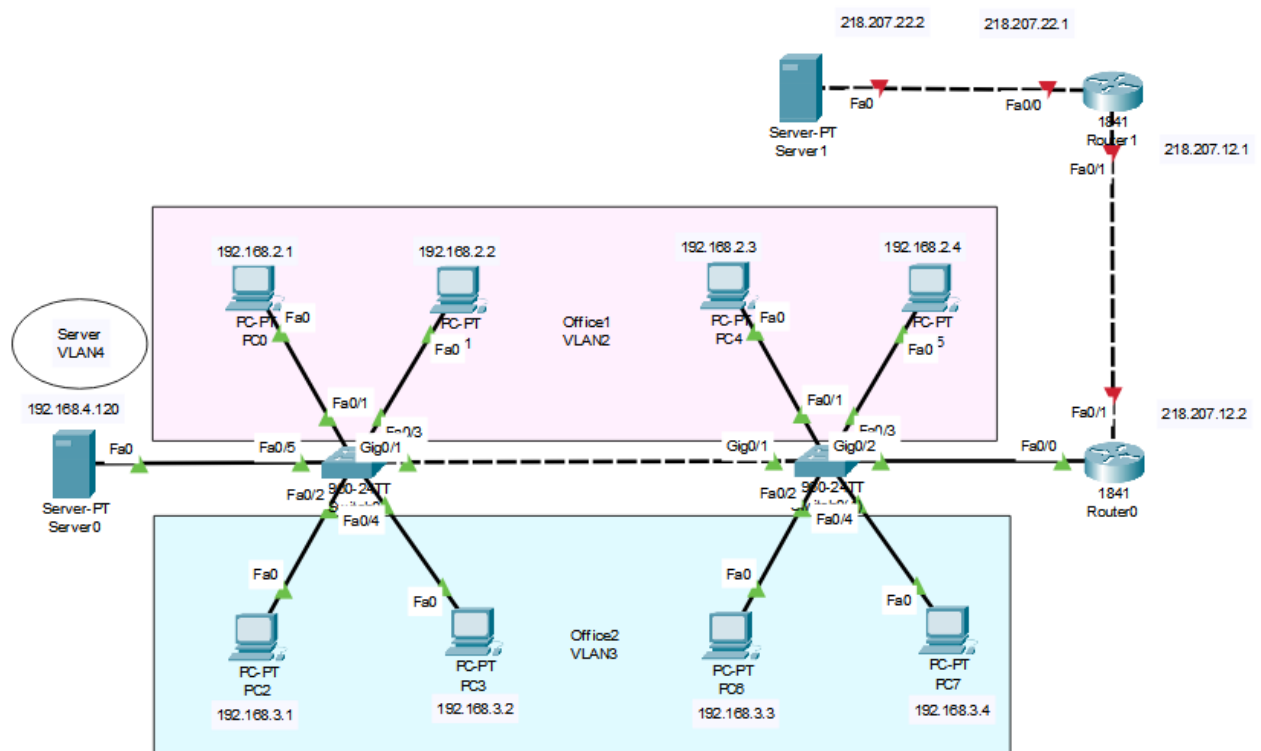
За допомогою утиліти ping знову перевіряємо доступність комп'ютерів, які входять до складу різних VLAN і впевнюємось, що комп'ютери всіх VLAN доступні один для одного.



```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
C:\>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.4.120
Pinging 192.168.4.120 with 32 bytes of data:
Reply from 192.168.4.120: bytes=32 time<1ms TTL=127
Reply from 192.168.4.120: bytes=32 time<1ms TTL=127
Reply from 192.168.4.120: bytes=32 time<1ms TTL=127
Reply from 192.168.4.120: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.4.120:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Тепер змодельюємо ситуацію підключення створеної локальної мережі до зовнішнього сервера Server1 в Інтернеті за допомогою маршрутизатора Router1, який має публічну IP-адресу 218.207.22.2. Для такого підключення нам виділена публічна IP-адреса 218.207.12.2.

Початковий вигляд:



Виконаємо налаштування маршрутизатора провайдера Router1, який має два інтерфейси і відповідно дві IP-адреси: зовнішню fa0/0 218.207.22.1, яка

звернена в напрямку зовнішнього сервера провайдер Server1, і внутрішню fa0/1 218.207.12.1, яка звернена до маршрутизатора Router0.

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip address 218.207.22.1 255.255.255.252
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#int fa0/1
Router(config-if)#ip address 218.207.12.1 255.255.255.252
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

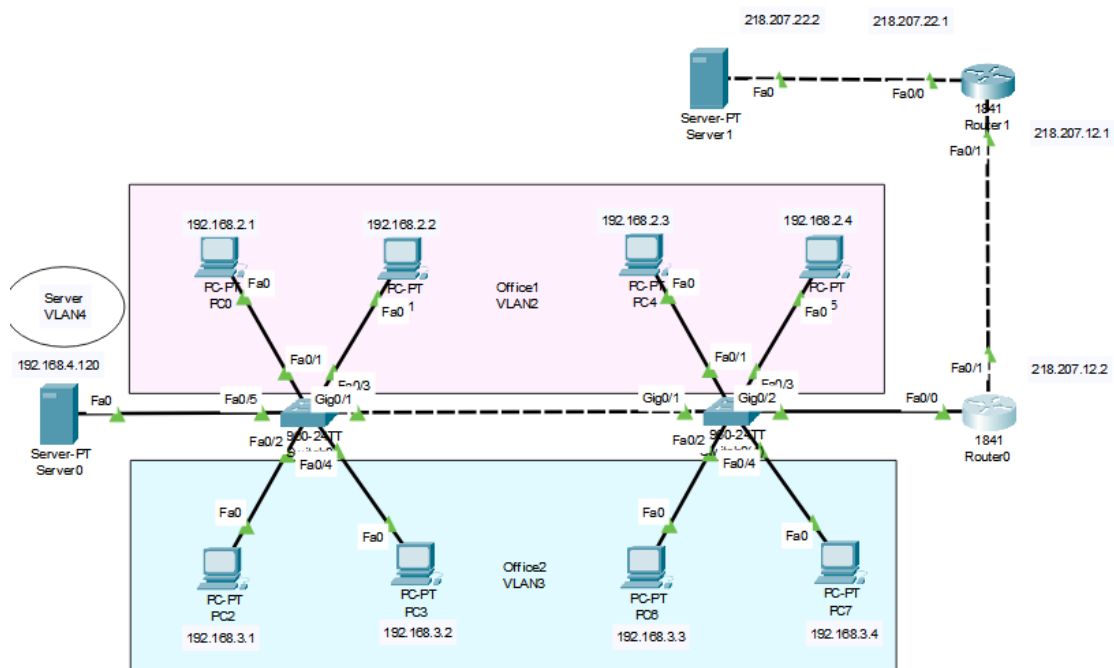
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

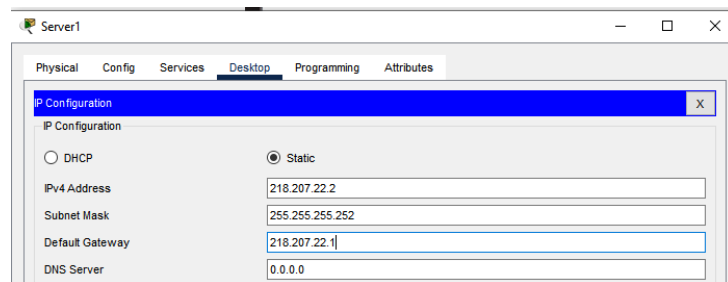
Виконаємо налаштування інтерфейсу fa0/1 маршрутизатора Router0:

```
[OK]
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#ip address 218.207.12.2 255.255.255.252
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 218.207.12.1
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

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



Виконаємо мережеві налаштування зовнішнього сервера Server1:



Перевіряємо зв'язок Router0 з провайдером та доступність сервера Server1:



## Налаштування NAT (Network Address Translation)

Тепер спробуємо зв'язатися з публічним сервером Server1 з локального комп'ютера (наприклад, з Server0), пінг не проходить, тому що ми використовуємо внутрішні IP-адреси, а маршрутизатор не має ніякої інформації про локальну мережу.

```
C:\>ping 218.207.22.2

Pinging 218.207.22.2 with 32 bytes of data:

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

Ping statistics for 218.207.22.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

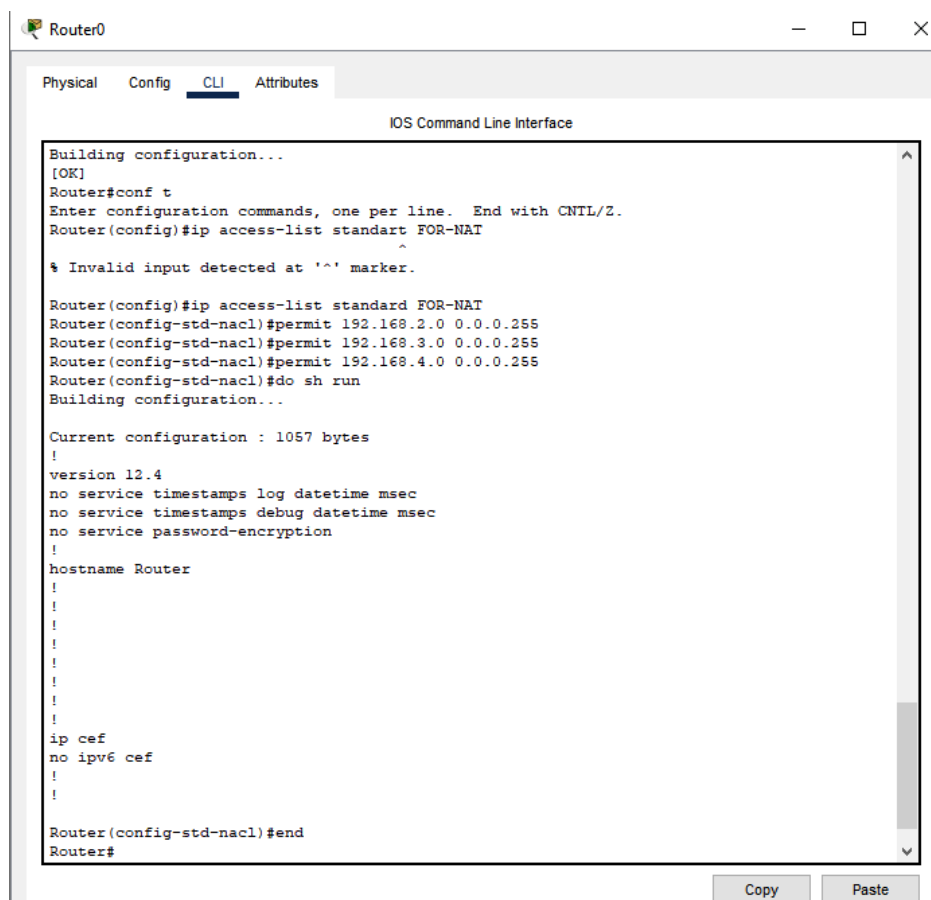
C:\>
```

За допомогою технології NAT налаштуємо доступ локальних комп'ютерів і WEB-сервера до мережі Інтернет. Спочатку вказуємо маршрутизатору Router0 який інтерфейс буде для NAT зовнішнім, а який внутрішнім:

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#int fa0/0.2
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#int fa0/0.3
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#int fa0/0.4
Router(config-subif)#ip nat inside
Router(config-subif)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

Тепер створюємо access-list. Який містить перелік IP-адрес усіх підмереж внутрішньої мережі для яких необхідно буде виконувати трансляцію адрес:



The screenshot shows a window titled "Router0" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and responses:

```
Building configuration...
[OK]
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list standart FOR-NAT
^
% Invalid input detected at '^' marker.

Router(config)#ip access-list standard FOR-NAT
Router(config-std-nacl)#permit 192.168.2.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.3.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.4.0 0.0.0.255
Router(config-std-nacl)#do sh run
Building configuration...

Current configuration : 1057 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!

Router(config-std-nacl)#end
Router#
```

At the bottom of the window, there are "Copy" and "Paste" buttons.

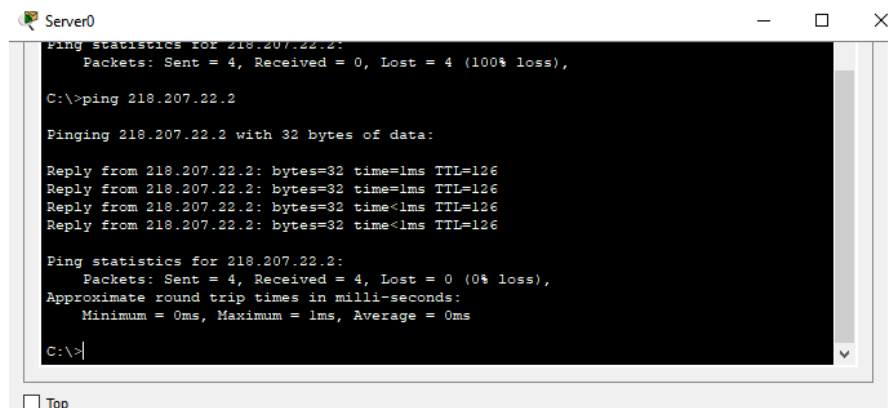
Останньою командою включаємо режим роботи NAT, який дозволяє відображати кілька внутрішніх IP-адрес в одну зовнішню, використовуючи різні порти (NAT overload):

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip nat inside source list FOR-NAT interface fa0/1 overload
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

Ця команда говорить маршрутизатору, що у всіх пакетів, отриманих на внутрішній інтерфейс і дозволених списком доступу FOR-NAT, адреса відправника буде транслюватися в адресу інтерфейсу fa0/1. Ключ overload вказує, що трансляції будуть перезавантажені, що дозволить кільком внутрішнім вузлам транслюватися на одну IP-адресу. Тепер NAT налаштований.

Перевіримо можливість виходу в Інтернет із будь-якого комп'ютера, тобто перевіримо доступ до сервера 218.207.22.2.



```
Server0
Ping statistics for 218.207.22.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

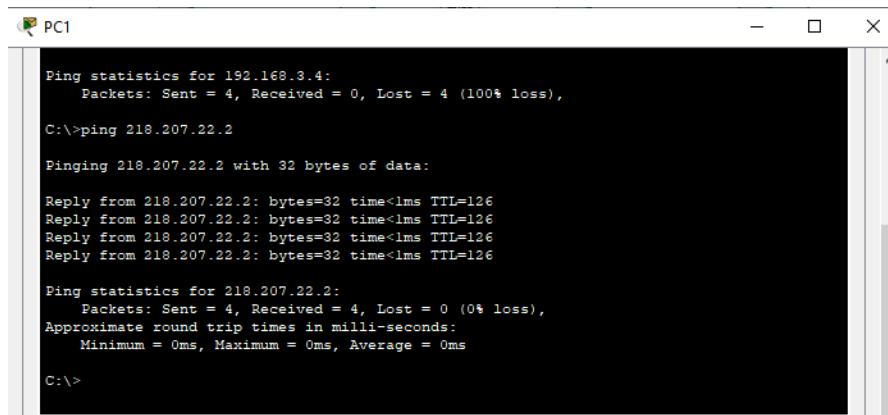
C:\>ping 218.207.22.2

Pinging 218.207.22.2 with 32 bytes of data:

Reply from 218.207.22.2: bytes=32 time<1ms TTL=126
Reply from 218.207.22.2: bytes=32 time<1ms TTL=126
Reply from 218.207.22.2: bytes=32 time<1ms TTL=126
Reply from 218.207.22.2: bytes=32 time<1ms TTL=126

Ping statistics for 218.207.22.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```



```
PC1
Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 218.207.22.2

Pinging 218.207.22.2 with 32 bytes of data:

Reply from 218.207.22.2: bytes=32 time<1ms TTL=126
Reply from 218.207.22.2: bytes=32 time<1ms TTL=126
Reply from 218.207.22.2: bytes=32 time<1ms TTL=126
Reply from 218.207.22.2: bytes=32 time<1ms TTL=126

Ping statistics for 218.207.22.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

```
PC3
C:\>ping 218.207.22.2

Pinging 218.207.22.2 with 32 bytes of data:

Reply from 218.207.22.2: bytes=32 time<1ms TTL=126
Reply from 218.207.22.2: bytes=32 time<1ms TTL=126
Reply from 218.207.22.2: bytes=32 time<1ms TTL=126
Reply from 218.207.22.2: bytes=32 time<1ms TTL=126

Ping statistics for 218.207.22.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

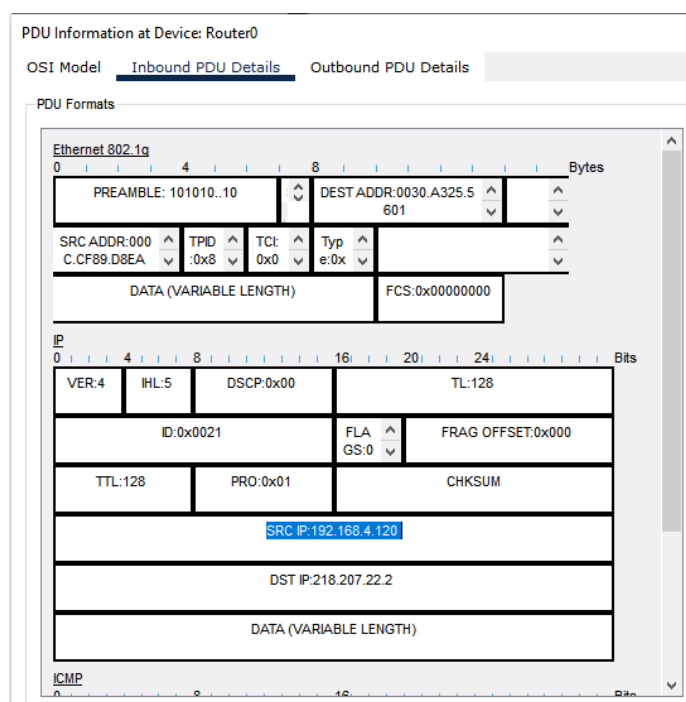
C:\>|
```

На маршрутизаторі Router0 виконаємо команду:

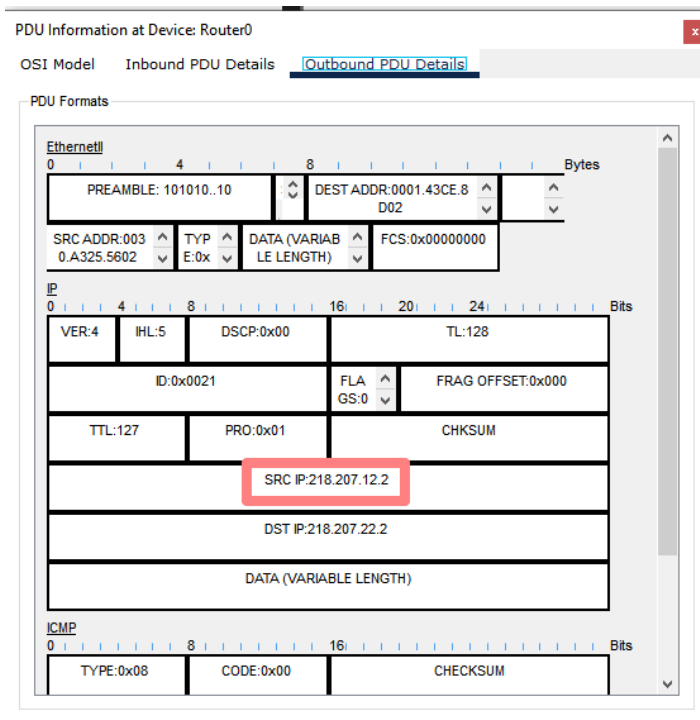
```
Router#wr mem
Building configuration...
[OK]
Router#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 218.207.12.2:13    192.168.3.2:13    218.207.22.2:13    218.207.22.2:13
icmp 218.207.12.2:14    192.168.3.2:14    218.207.22.2:14    218.207.22.2:14
icmp 218.207.12.2:15    192.168.3.2:15    218.207.22.2:15    218.207.22.2:15
icmp 218.207.12.2:16    192.168.3.2:16    218.207.22.2:16    218.207.22.2:16

Router#
```

Розглянемо, як працює NAT у нашому прикладі. Комп'ютер із внутрішньої мережі (наприклад, Server0) відправляє дейтаграму в напрямку маршрутизатора Router0. Маршрутизатор отримує дейтаграму, замінює в ній IP-адресу відправника 192.168.4.120 на IP-адресу 218.207.12.2, розташовану в глобальній мережі, також відбувається заміна старого номеру порту призначення на новий.







На сервері Server0 запустимо сервіс HTTP. Сервіс HTTP дозволяє будувати нескладні веб-сторінки і перевіряти проходження пакетів на порт 80 сервера.

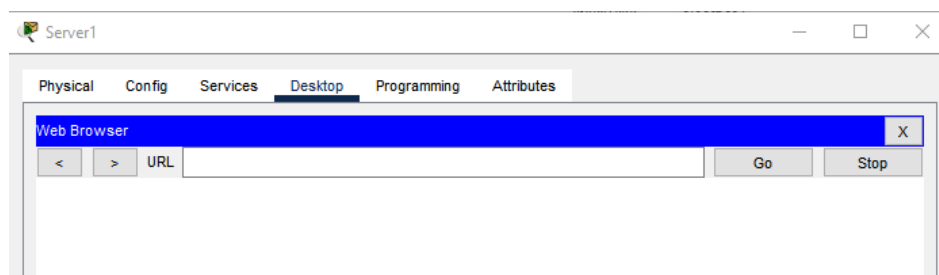
Виконаємо http-запит із зовнішнього сервера Server1 до внутрішнього Web-сервера Server0.

Для цього на Router0 необхідно налаштувати правило для статичного перетворення IP-адрес (Static NAT):

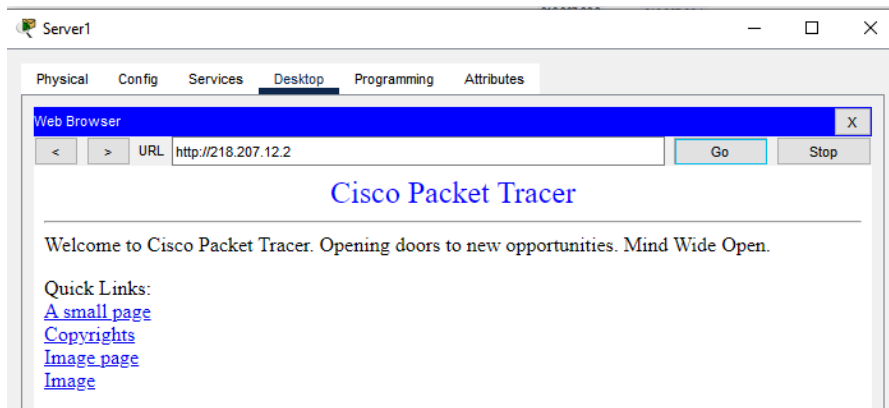
```
Router>enabl
Translating "enabl"...domain server (255.255.255.255)
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip nat inside source static tcp 192.168.4.120
% Unknown command or computer name, or unable to find computer address

Router(config)#ip nat inside source static tcp 192.168.4.120 80 218.207.12.2 80
Router(config)#
```

Заходимо на Server1, відкриваємо вкладку Desktop. Запускаємо на сервері Web-браузер:



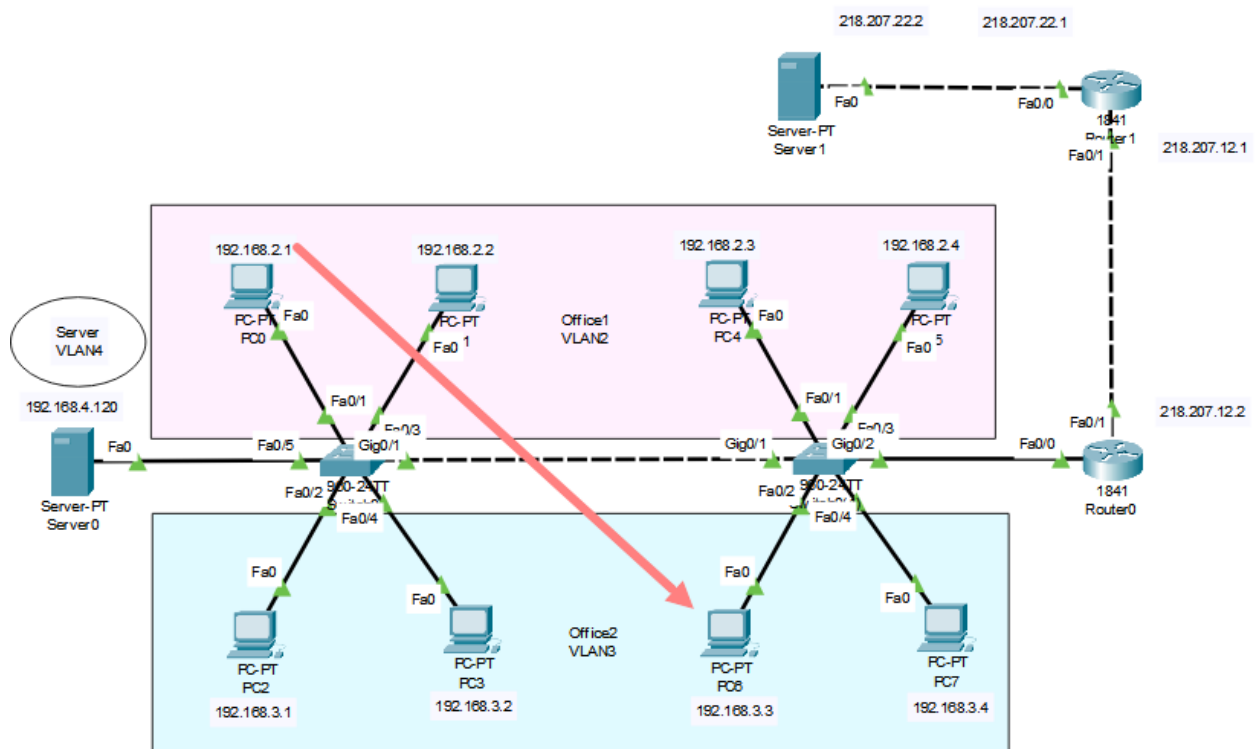
В полі URL вказуємо глобальну IP-адресу NAT-маршрутизатора 218.207.12.2 і натискаємо клавішу GO.



*У режимі симуляції за допомогою утиліти ping дослідити рух службових пакетів по створеній мережі*

- від хоста у VLAN2 до хоста у VLAN3;

Виконання команди ping в командному рядку до пристрою за адресою 192.168.3.4 у віртуальній мережі VLAN3 :



```
PC0
C:\>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Reply from 192.168.3.4: bytes=32 time=20ms TTL=127
Reply from 192.168.3.4: bytes=32 time=10ms TTL=127
Reply from 192.168.3.4: bytes=32 time=10ms TTL=127
Reply from 192.168.3.4: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 20ms, Average = 12ms

C:\>|
```

Проходження пакетів першого ICMP-запиту:

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.000	--	PC0	ARP
	0.001	PC0	Switch0	ARP
	0.002	Switch0	PC1	ARP
	0.002	Switch0	Switch...	ARP
	0.003	Switch0(1)	PC4	ARP
	0.003	Switch0(1)	PC5	ARP
	0.003	Switch0(1)	Router0	ARP
	0.004	Router0	Switch...	ARP
	0.005	Switch0(1)	Switch0	ARP
	0.006	Switch0	PC0	ARP
	0.006	--	PC0	ICMP
	0.007	PC0	Switch0	ICMP
	0.008	Switch0	Switch...	ICMP
	0.009	Switch0(1)	Router0	ICMP
	0.010	Router0	Switch...	ICMP
	0.011	Switch0(1)	PC7	ICMP
	0.011	--	PC7	ARP
	0.012	PC7	Switch...	ARP
	0.013	Switch0(1)	PC6	ARP
	0.013	Switch0(1)	Switch0	ARP
	0.013	Switch0(1)	Router0	ARP
	0.014	Switch0	PC2	ARP
	0.014	Switch0	PC3	ARP
	0.014	Router0	Switch...	ARP
	0.015	Switch0(1)	PC7	ARP
	0.015	--	PC7	ICMP
	0.016	PC7	Switch...	ICMP
	0.017	Switch0(1)	Router0	ICMP
	0.018	Router0	Switch...	ICMP
	0.019	Switch0(1)	Switch0	ICMP
	0.020	Switch0	PC0	ICMP

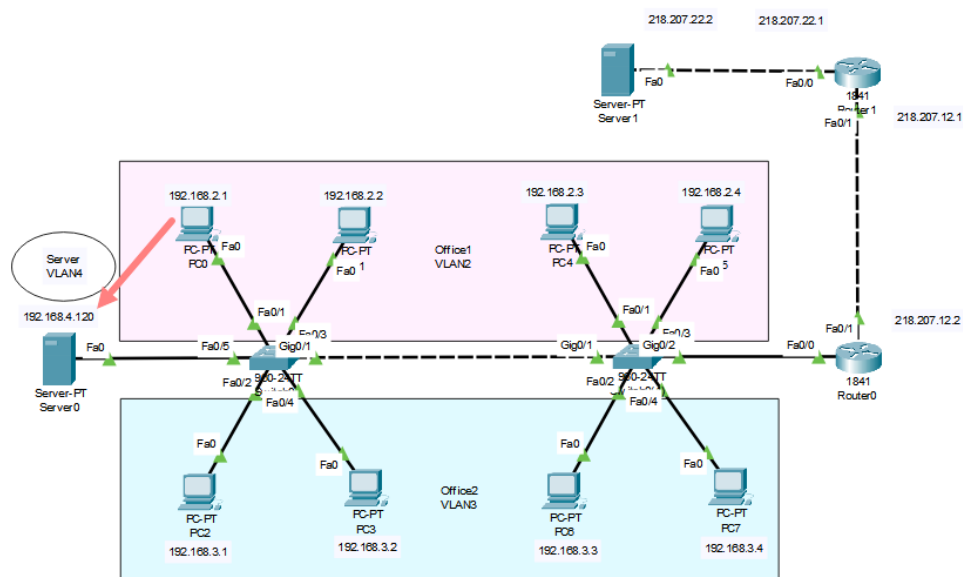
Виконання команди ping починається з відправки запиту echo-request до пристрою за адресою шлюзу 192.186.2.10. Оскільки в ARP-таблиці відсутня інформація про фізичну адресу, то здійснюється пошук та перетворення логічної адреси в MAC-адресу за допомогою таблиці ARP. Надсилається широкомовний запит, який проходить через комутатор Switch0, комутатор

Switch1 до роутера Router0, де адреса призначення співпадає з адресою маршрутизатора. Назад же відправляється відповідь з MAC-адресою Router0. Після цього відбувається продовження проходження ICMP-пакету до маршрутизатора Router0, в таблиці маршрутизації знаходиться маршрут призначення та викликається ARP-протокол для знаходження MAC-адреси пристрою PC7 й відправляється назад до маршрутизації ARP-відповідь з фізичною адресою PC7.

Далі створюється наступний ICMP-запит, який надсилає echo-request. IP-адреса місця призначення знаходиться не в одній підмережі та запит не є широкомовним. В результаті адресою призначення встановлюється адреса 18 дефолтного шлюзу. Маршрутизатор Router0 перенаправляє пакет до пристрою PC7, який формує echo-request, що надсилається назад до пристрою PC0.

1.023	--	PC0	ICMP
1.024	PC0	Switch0	ICMP
1.025	Switch0	Switch0(1)	ICMP
1.026	Switch0(1)	Router0	ICMP
1.027	Router0	Switch0(1)	ICMP
1.028	Switch0(1)	PC7	ICMP
1.029	PC7	Switch0(1)	ICMP
1.030	Switch0(1)	Router0	ICMP
1.031	Router0	Switch0(1)	ICMP
1.032	Switch0(1)	Switch0	ICMP
1.033	Switch0	PC0	ICMP

- від хоста у VLAN2 до хоста у VLAN4;

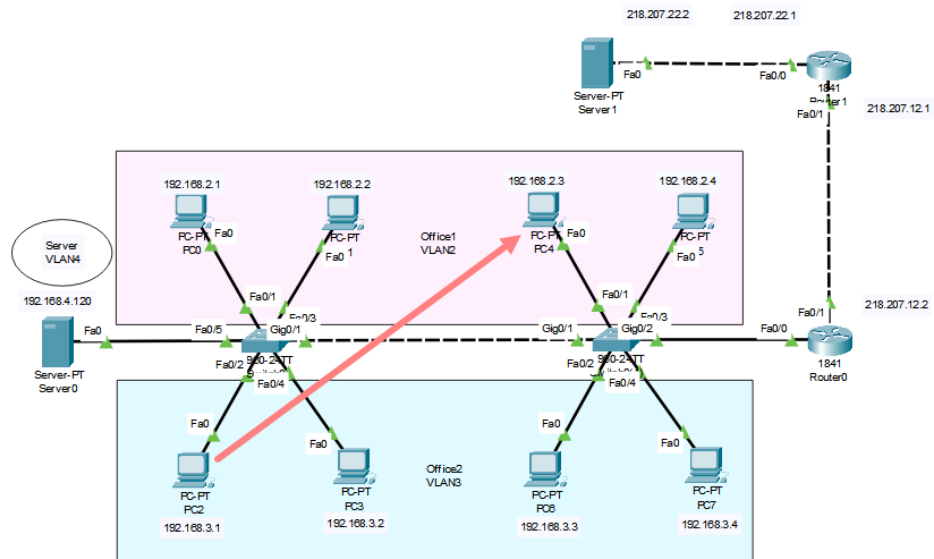


Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.000	--	PC0	ARP
	0.001	PC0	Switch0	ARP
	0.002	Switch0	PC1	ARP
	0.002	Switch0	Switch0(1)	ARP
	0.003	Switch0(1)	PC4	ARP
	0.003	Switch0(1)	PC5	ARP
	0.003	Switch0(1)	Router0	ARP
	0.004	Router0	Switch0(1)	ARP
	0.005	Switch0(1)	Switch0	ARP
	0.006	Switch0	PC0	ARP
	0.006	--	PC0	ICMP
	0.007	PC0	Switch0	ICMP
	0.008	Switch0	Switch0(1)	ICMP
	0.009	Switch0(1)	Router0	ICMP
	0.010	Router0	Switch0(1)	ICMP
	0.011	Switch0(1)	Switch0	ICMP
	0.012	Switch0	Server0	ICMP
	0.012	--	Server0	ARP
	0.013	Server0	Switch0	ARP
	0.014	Switch0	Switch0(1)	ARP
	0.015	Switch0(1)	Router0	ARP
	0.016	Router0	Switch0(1)	ARP
	0.017	Switch0(1)	Switch0	ARP
	0.018	Switch0	Server0	ARP
	0.018	--	Server0	ICMP
	0.019	Server0	Switch0	ICMP
	0.020	Switch0	Switch0(1)	ICMP
	0.021	Switch0(1)	Router0	ICMP
	0.022	Router0	Switch0(1)	ICMP
	0.023	Switch0(1)	Switch0	ICMP
	0.024	Switch0	PC0	ICMP

Як можна помітити під час надсилання серії пакетів від хосту у VLAN2 до хоста у VLAN3 було визначено MAC-адресу маршрутизатора Router0, що дає змогу надіслати ICMP-запит за адресою дефолтного шлюзу. Маршрутизатор у свою чергу займається визначенням фізичної адреси сервера Server0 за допомогою ARP-протоколу й echo-запит зазнає невдачі під час передачі. Подальша передача та прийом ICMP-пакетів відбувається у відповідності до алгоритму, описаного в попередньому сеансі зв'язку.

1.027	--	PC0	ICMP
1.028	PC0	Switch0	ICMP
1.029	Switch0	Switch0(1)	ICMP
1.030	Switch0(1)	Router0	ICMP
1.031	Router0	Switch0(1)	ICMP
1.032	Switch0(1)	Switch0	ICMP
1.033	Switch0	Server0	ICMP
1.034	Server0	Switch0	ICMP
1.035	Switch0	Switch0(1)	ICMP
1.036	Switch0(1)	Router0	ICMP
1.037	Router0	Switch0(1)	ICMP
1.038	Switch0(1)	Switch0	ICMP
1.039	Switch0	PC0	ICMP

- від хоста у VLAN3 до хоста у VLAN2;



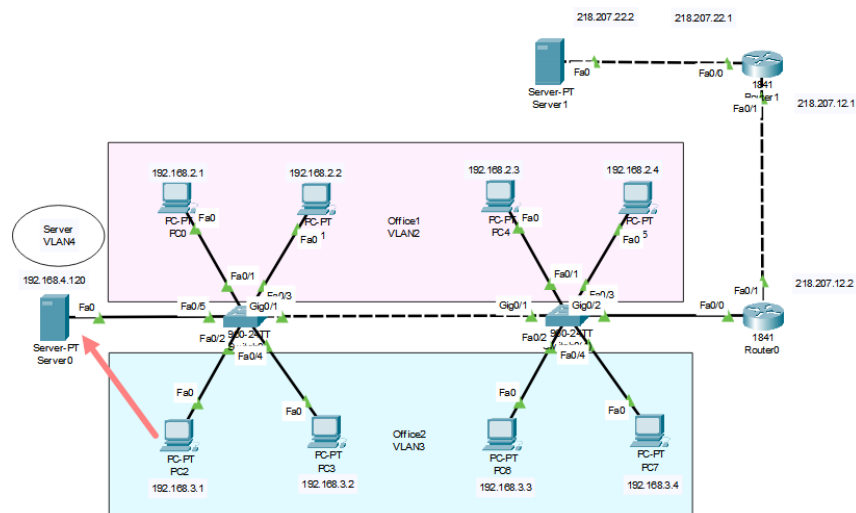
Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC2	ICMP
	0.000	--	PC2	ARP
	0.001	PC2	Switch0	ARP
	0.002	Switch0	PC3	ARP
	0.002	Switch0	Switch0(1)	ARP
	0.003	Switch0(1)	PC6	ARP
	0.003	Switch0(1)	PC7	ARP
	0.003	Switch0(1)	Router0	ARP
	0.004	Router0	Switch0(1)	ARP
	0.005	Switch0(1)	Switch0	ARP
	0.006	Switch0	PC2	ARP
	0.006	--	PC2	ICMP
	0.007	PC2	Switch0	ICMP
	0.008	Switch0	Switch0(1)	ICMP
	0.009	Switch0(1)	Router0	ICMP
	0.010	Router0	Switch0(1)	ICMP
	0.011	Switch0(1)	PC4	ICMP
	0.011	--	PC4	ARP
	0.012	PC4	Switch0(1)	ARP
	0.013	Switch0(1)	PC5	ARP
	0.013	Switch0(1)	Switch0	ARP
	0.013	Switch0(1)	Router0	ARP
	0.014	Switch0	PC0	ARP
	0.014	Switch0	PC1	ARP
	0.014	Router0	Switch0(1)	ARP
	0.015	Switch0(1)	PC4	ARP
	0.015	--	PC4	ICMP
	0.016	PC4	Switch0(1)	ICMP
	0.017	Switch0(1)	Router0	ICMP
	0.018	Router0	Switch0(1)	ICMP
	0.019	Switch0(1)	Switch0	ICMP
	0.020	Switch0	PC2	ICMP

1.022	--	PC2	ICMP
1.023	PC2	Switch0	ICMP
1.024	Switch0	Switch0(1)	ICMP
1.025	Switch0(1)	Router0	ICMP
1.026	Router0	Switch0(1)	ICMP
1.027	Switch0(1)	PC4	ICMP
1.028	PC4	Switch0(1)	ICMP
1.029	Switch0(1)	Router0	ICMP
1.030	Router0	Switch0(1)	ICMP
1.031	Switch0(1)	Switch0	ICMP
1.032	Switch0	PC2	ICMP

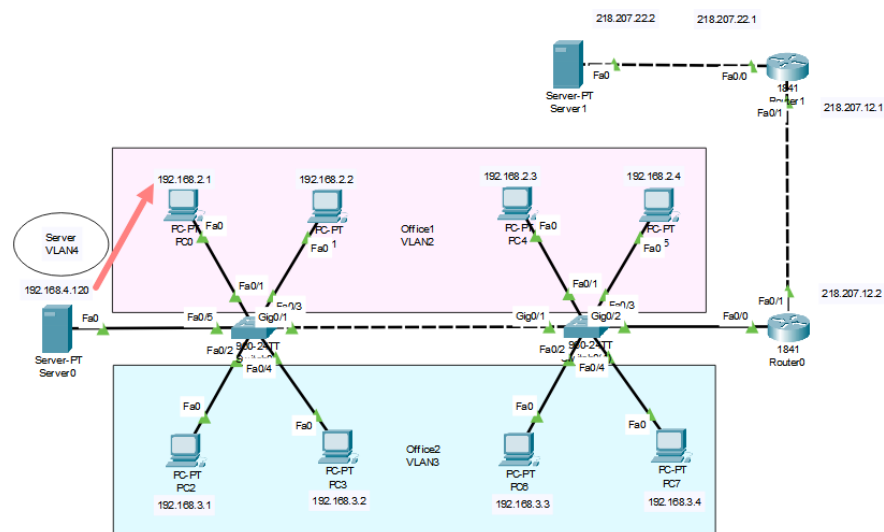
- від хоста у VLAN3 до хоста у VLAN4;



Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC2	ICMP
	0.000	--	PC2	ARP
	0.001	PC2	Switch0	ARP
	0.002	Switch0	PC3	ARP
	0.002	Switch0	Switch0(1)	ARP
	0.003	Switch0(1)	PC6	ARP
	0.003	Switch0(1)	PC7	ARP
	0.003	Switch0(1)	Router0	ARP
	0.004	Router0	Switch0(1)	ARP
	0.005	Switch0(1)	Switch0	ARP
	0.006	Switch0	PC2	ARP
	0.006	--	PC2	ICMP
	0.007	PC2	Switch0	ICMP
	0.008	Switch0	Switch0(1)	ICMP
	0.009	Switch0(1)	Router0	ICMP
	0.010	Router0	Switch0(1)	ICMP
	0.011	Switch0(1)	Switch0	ICMP
	0.012	Switch0	Server0	ICMP
	0.012	--	Server0	ARP
	0.013	Server0	Switch0	ARP
	0.014	Switch0	Switch0(1)	ARP
	0.015	Switch0(1)	Router0	ARP
	0.016	Router0	Switch0(1)	ARP
	0.017	Switch0(1)	Switch0	ARP
	0.018	Switch0	Server0	ARP
	0.018	--	Server0	ICMP
	0.019	Server0	Switch0	ICMP
	0.020	Switch0	Switch0(1)	ICMP
	0.021	Switch0(1)	Router0	ICMP
	0.022	Router0	Switch0(1)	ICMP
	0.023	Switch0(1)	Switch0	ICMP
	0.024	Switch0	PC2	ICMP

1.025	--	PC2	ICMP
1.026	PC2	Switch0	ICMP
1.027	Switch0	Switch0(1)	ICMP
1.028	Switch0(1)	Router0	ICMP
1.029	Router0	Switch0(1)	ICMP
1.030	Switch0(1)	Switch0	ICMP
1.031	Switch0	Server0	ICMP
1.032	Server0	Switch0	ICMP
1.033	Switch0	Switch0(1)	ICMP
1.034	Switch0(1)	Router0	ICMP
1.035	Router0	Switch0(1)	ICMP
1.036	Switch0(1)	Switch0	ICMP
1.037	Switch0	PC2	ICMP

- від хоста у VLAN4 до хоста у VLAN2;

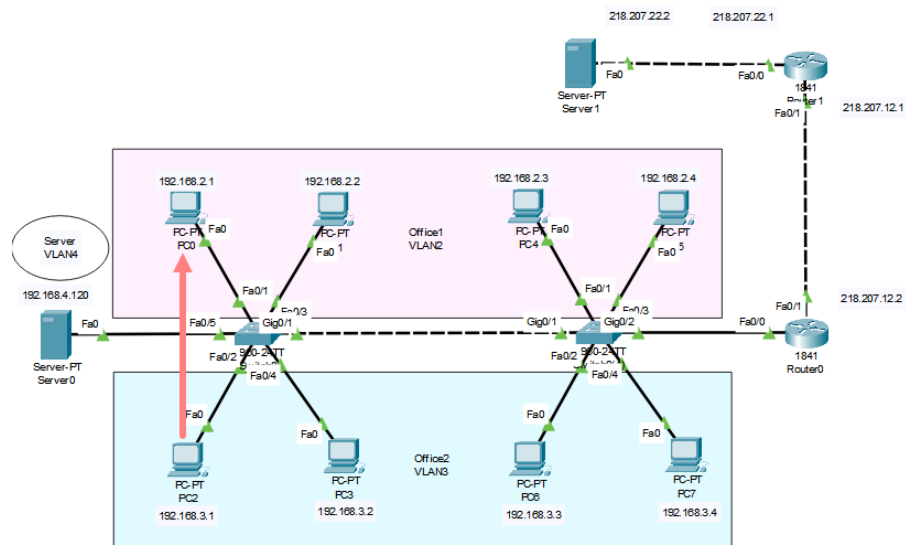


Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Server0	ICMP
	0.000	--	Server0	ARP
	0.001	Server0	Switch0	ARP
	0.002	Switch0	Switch0(1)	ARP
	0.003	Switch0(1)	Router0	ARP
	0.004	Router0	Switch0(1)	ARP
	0.005	Switch0(1)	Switch0	ARP
	0.006	Switch0	Server0	ARP
	0.006	--	Server0	ICMP
	0.007	Server0	Switch0	ICMP
	0.008	Switch0	Switch0(1)	ICMP
	0.009	Switch0(1)	Router0	ICMP
	0.010	Router0	Switch0(1)	ICMP
	0.011	Switch0(1)	Switch0	ICMP
	0.012	Switch0	PC0	ICMP
	0.012	--	PC0	ARP
	0.013	PC0	Switch0	ARP
	0.014	Switch0	PC1	ARP
	0.014	Switch0	Switch0(1)	ARP
	0.015	Switch0(1)	PC4	ARP
	0.015	Switch0(1)	PC5	ARP
	0.015	Switch0(1)	Router0	ARP
	0.016	Router0	Switch0(1)	ARP
	0.017	Switch0(1)	Switch0	ARP
	0.018	Switch0	PC0	ARP
	0.018	--	PC0	ICMP
	0.019	PC0	Switch0	ICMP
	0.020	Switch0	Switch0(1)	ICMP
	0.021	Switch0(1)	Router0	ICMP
	0.022	Router0	Switch0(1)	ICMP
	0.023	Switch0(1)	Switch0	ICMP
	0.024	Switch0	Server0	ICMP

1.026	--	Server0	ICMP
1.027	Server0	Switch0	ICMP
1.028	Switch0	Switch0(1)	ICMP
1.029	Switch0(1)	Router0	ICMP
1.030	Router0	Switch0(1)	ICMP
1.031	Switch0(1)	Switch0	ICMP
1.032	Switch0	PC0	ICMP
1.033	PC0	Switch0	ICMP
1.034	Switch0	Switch0(1)	ICMP
1.035	Switch0(1)	Router0	ICMP
1.036	Router0	Switch0(1)	ICMP
1.037	Switch0(1)	Switch0	ICMP
1.038	Switch0	Server0	ICMP



- від хоста у VLAN3 до хоста у VLAN2.



Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC2	ICMP
	0.000	--	PC2	ARP
	0.001	PC2	Switch0	ARP
	0.002	Switch0	PC3	ARP
	0.002	Switch0	Switch0(1)	ARP
	0.003	Switch0(1)	PC6	ARP
	0.003	Switch0(1)	PC7	ARP
	0.003	Switch0(1)	Router0	ARP
	0.004	Router0	Switch0(1)	ARP
	0.005	Switch0(1)	Switch0	ARP
	0.006	Switch0	PC2	ARP
	0.006	--	PC2	ICMP
	0.007	PC2	Switch0	ICMP
	0.008	Switch0	Switch0(1)	ICMP
	0.009	Switch0(1)	Router0	ICMP
	0.010	Router0	Switch0(1)	ICMP
	0.011	Switch0(1)	Switch0	ICMP
	0.012	Switch0	PC0	ICMP
	0.012	--	PC0	ARP
	0.013	PC0	Switch0	ARP
	0.014	Switch0	PC1	ARP
	0.014	Switch0	Switch0(1)	ARP
	0.015	Switch0(1)	PC4	ARP
	0.015	Switch0(1)	PC5	ARP
	0.015	Switch0(1)	Router0	ARP
	0.016	Router0	Switch0(1)	ARP
	0.017	Switch0(1)	Switch0	ARP
	0.018	Switch0	PC0	ARP
	0.018	--	PC0	ICMP
	0.019	PC0	Switch0	ICMP
	0.020	Switch0	Switch0(1)	ICMP
	0.021	Switch0(1)	Router0	ICMP
	0.022	Router0	Switch0(1)	ICMP
	0.023	Switch0(1)	Switch0	ICMP
	0.024	Switch0	PC2	ICMP

1.024	--	PC2	ICMP
1.025	PC2	Switch0	ICMP
1.026	Switch0	Switch0(1)	ICMP
1.027	Switch0(1)	Router0	ICMP
1.028	Router0	Switch0(1)	ICMP
1.029	Switch0(1)	Switch0	ICMP
1.030	Switch0	PC0	ICMP
1.031	PC0	Switch0	ICMP
1.032	Switch0	Switch0(1)	ICMP
1.033	Switch0(1)	Router0	ICMP
1.034	Router0	Switch0(1)	ICMP
1.035	Switch0(1)	Switch0	ICMP
1.036	Switch0	PC2	ICMP

## ***Висновок:***

У результаті виконання лабораторної роботи було створено модель комп'ютерної мережі, що складається з трьох віртуальних локальних мереж (VLAN2, VLAN3, VLAN4). Комп'ютери PC0, PC1, PC4, PC6 були об'єднані у VLAN2, комп'ютери PC2, PC3, PC6, PC7 - у VLAN3, а Web-сервер Server0 - у VLAN4.

Було виконано налаштування мережевих пристроїв, зокрема комутаторів та маршрутизатора, для забезпечення взаємодії комп'ютерів різних віртуальних мереж. Продемонстровано, що комп'ютери, які знаходяться в різних VLAN, не можуть безпосередньо взаємодіяти один з одним, оскільки вони ізольовані на каналному рівні. Для забезпечення їх взаємодії необхідно використовувати маршрутизатор.

Також було налаштовано технологію NAT (Network Address Translation) на маршрутизаторі Router0 для забезпечення доступу комп'ютерів локальної мережі до зовнішнього сервера Server1 в мережі Інтернет. Крім того, було налаштовано статичне перетворення адрес для забезпечення доступу до Web-сервера Server0 із зовнішньої мережі.

В ході виконання лабораторної роботи було детально досліджено процес передачі ICMP-пакетів між комп'ютерами, що належать до різних VLAN, та між локальною мережею та зовнішнім сервером. Отримані результати дозволяють зробити висновок про ефективність застосування технологій VLAN та NAT для організації доступу до комп'ютерної мережі.