

## Комп'ютерний практикум № 8

### Налаштування статичних та динамічних трансляцій мережних адрес (NAT). Налаштування статичного NAT

*NAT (Network Address Translation)* — трансляція мережевих адрес, технологія, що дозволяє перетворювати (змінювати) *IP*-адреси і порти у мережевих пакетах. NAT використовується найчастіше для здійснення доступу пристроїв з локальної мережі підприємства в Інтернет, або навпаки для доступу з Інтернет на який-небудь ресурс усередині мережі. Локальна мережа підприємства будується на приватних *IP*-адресах:

10.0.0.0 — 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))

172.16.0.0 — 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))

192.168.0.0 — 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Ці адреси не маршрутизуються в Інтернеті, і провайдери повинні відкидати пакети з такими *IP*-адресами відправників або одержувачів. Для перетворення приватних адрес у глобальні (маршрутизовані в Інтернеті) застосовують NAT.

**NAT** — технологія трансляції мережевих адрес, тобто підміни адрес (чи портів) у заголовку *IP*-пакету. Іншими словами, пакет, проходячи через маршрутизатор, може змінити свою адресу джерела та/чи призначення. Подібний механізм служить для забезпечення доступу з LAN, де використовуються приватні *IP*-адреси, у Internet, де використовуються глобальні *IP*-адреси.

Існує три види трансляції:

1. **Static NAT (статичний NAT)** здійснює перетворення *IP*-адреси один до одного, тобто зіставляється одна адреса з внутрішньої мережі з однією адресою з зовнішньої мережі. Іншими словами, при проходженні через маршрутизатор, адреса змінюється на строго задану адресу, один-до-одного (Наприклад, 10.1.1.5 завжди замінюється на 11.1.1.5 і назад). Запис про таку трансляцію зберігається необмежено довго, поки є відповідний рядок в конфігурації роутера.
2. **Dynamic NAT (динамічний NAT)** виконує перетворення внутрішньої адреси в одну з групи зовнішніх адрес. Тобто, перед використанням динамічної трансляції, потрібно задати nat-пул зовнішніх адрес. У цьому випадку при проходженні через

маршрутизатор, нова адреса вибирається динамічно з деякого діапазону адрес, званого пулом (pool). Запис про трансляцію зберігається деякий час, щоб відповідні пакети могли бути доставлені адресату. Якщо протягом деякого часу трафік по цій трансляції відсутній, трансляція видаляється і адреса повертається в пул. Якщо потрібно створити трансляцію, а вільних адрес в пулі немає, то пакет відкидається. Іншими словами, добре б, щоб число внутрішніх адрес було ненабагато більше числа адрес в пулі, інакше висока ймовірність проблем з виходом в WAN.

3. Overloading(чи **PAT**) дозволяє перетворювати кілька внутрішніх адрес в одну зовнішню. Для здійснення такої трансляції використовуються порти, тому такий NAT називають PAT (Port Address Translation). За допомогою PAT можна перетворювати внутрішню адресу в зовнішню адресу, задану через пул або через адресу на зовнішньому інтерфейсі.

### Хід роботи

#### Завдання №1

#### Статична трансляція адрес NAT

На рис. 8.1 є зовнішня адреса 20.20.20.20 (зовнішній інтерфейс fa0/1) і внутрішня мережа 10.10.10.0 (внутрішній інтерфейс fa0/0). Потрібно налаштувати NAT. Передбачається, що адреси вже прописані, і мережа піднята (робоча).

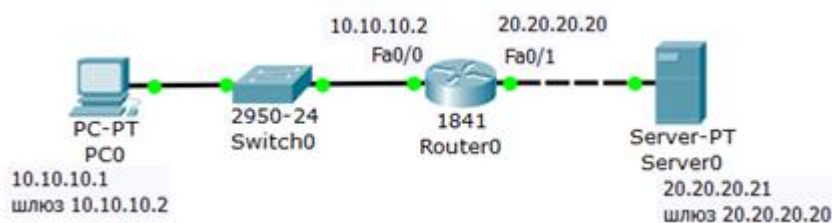
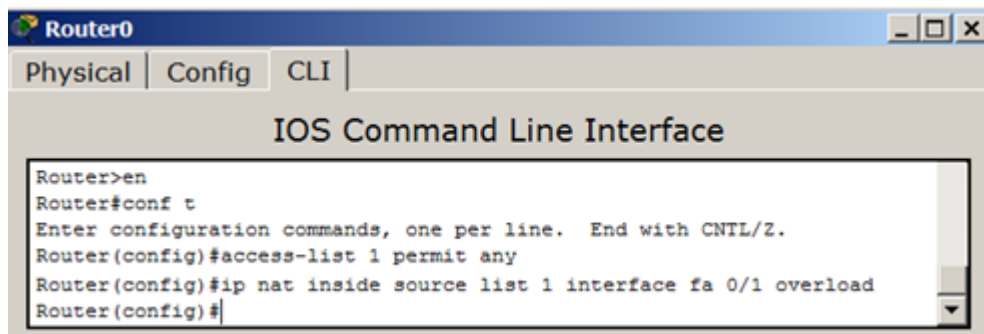


Рис. 8.1. Схема мережі

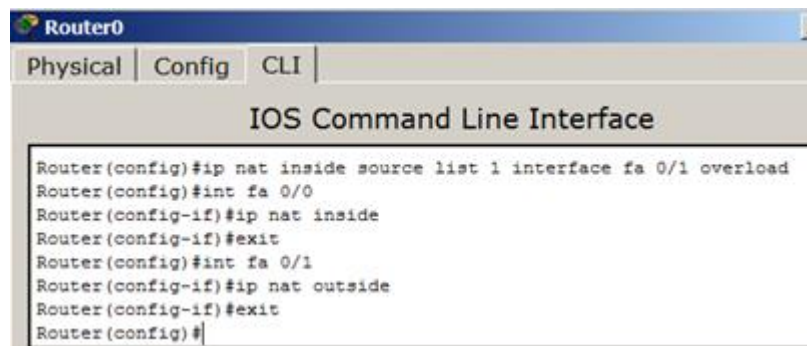
На R0 додаємо access-list, дозволяємо всі (any). Дозволяємо весь трафік, тобто, будь-яку IP-адресу (рис. 8.2).



**Рис. 8.2** Складаємо лист допуску

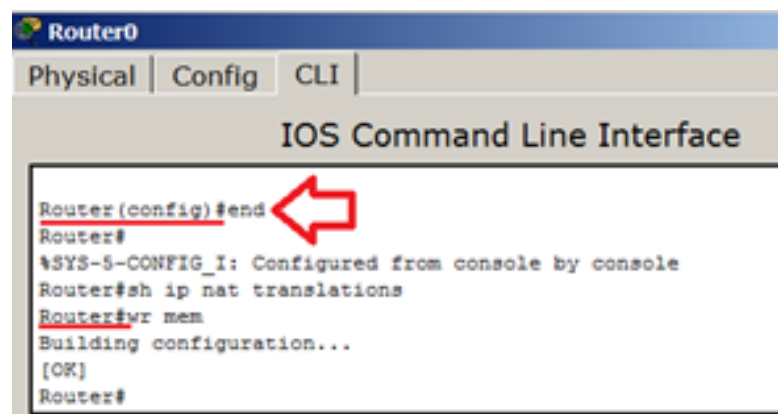
### Створюємо правило трансляції

Налаштуємо трансляцію на інтерфейсах (на внутрішньому inside, на зовнішньому – outside), тобто, для R0 вказуємо внутрішній і зовнішній порти (рис. 8.3)



**Рис. 8.3.** Для R0 призначаємо внутрішній і зовнішній порти

Виходимо з режиму глобального конфігурування і записуємо налаштування роутера у мікросхему пам'яті (рис. 8.4).



**Рис. 8.4.** Зберігаємо налаштування в ОЗУ

### Перевіряємо роботу мережі (перегляд стану таблиці NAT)

З PC0 пінгуємо провайдера і переконуємося, що PC1 і сервер можуть спілкуватися (рис. 8.5).

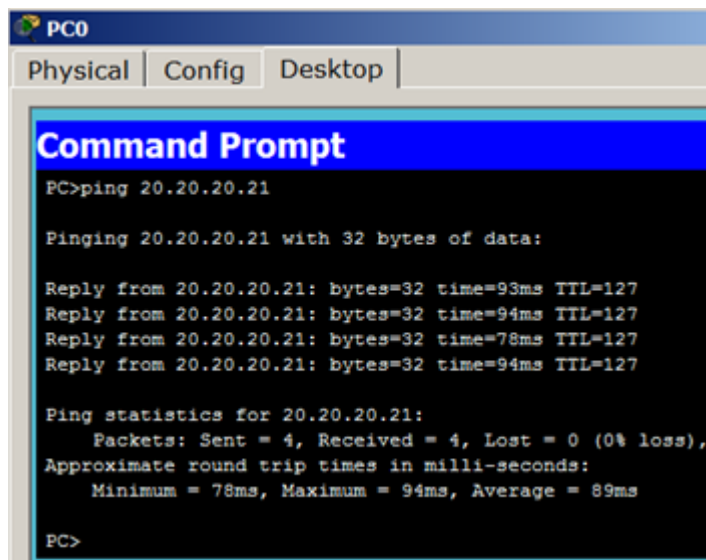


Рис. 8.5. З внутрішньої мережі пінгуємо зовнішню мережу

Для перегляду стану таблиці NAT, одночасно з пінгом використовуйте команду **Router # sh ip nat translations** (у прикладі запущено пінг з машини 10.10.10.1, тобто, з PC1 на адресу 20.20.20.21, тобто, на S0) – рис. 8.6.

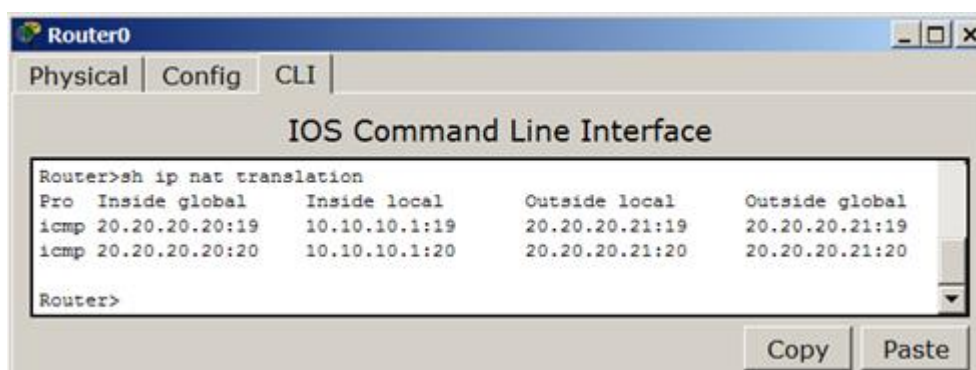


Рис. 8.6. Під час пінгу переглядаємо стан таблиці NAT

Переконаємося в успішній маршрутизації в режимі симуляції(рис. 8.7).

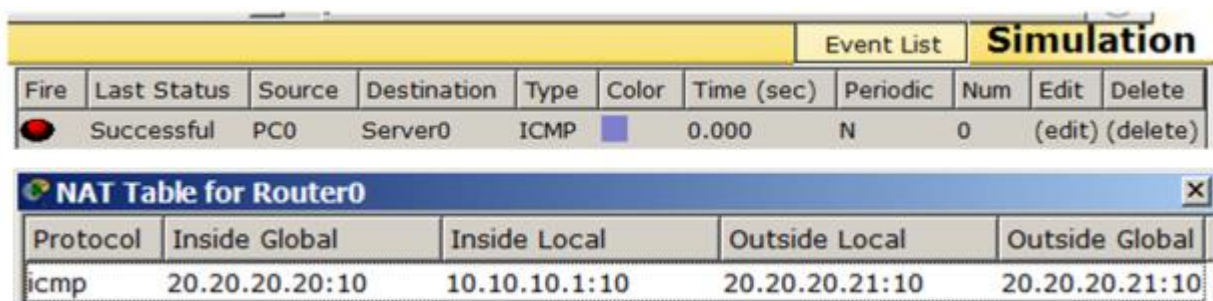
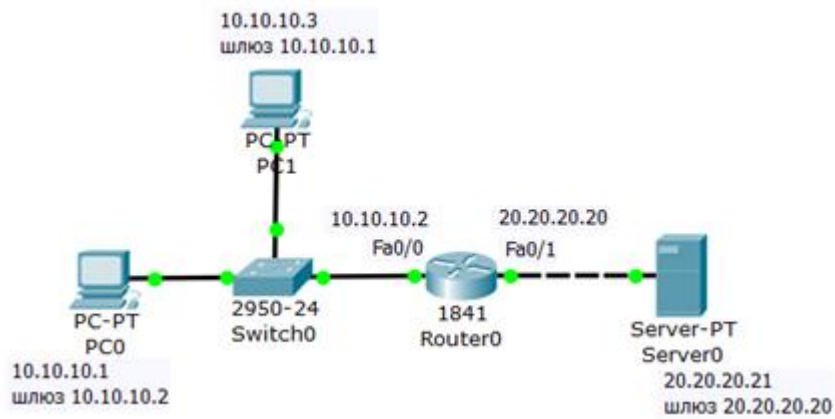



Рис. 8.7. Зв'язок PC0 і S0 працює

**Самостійно:** якщо в схему додати PC1(рис. 8.8), то чи працюватиме статичний NAT між ним і S0?



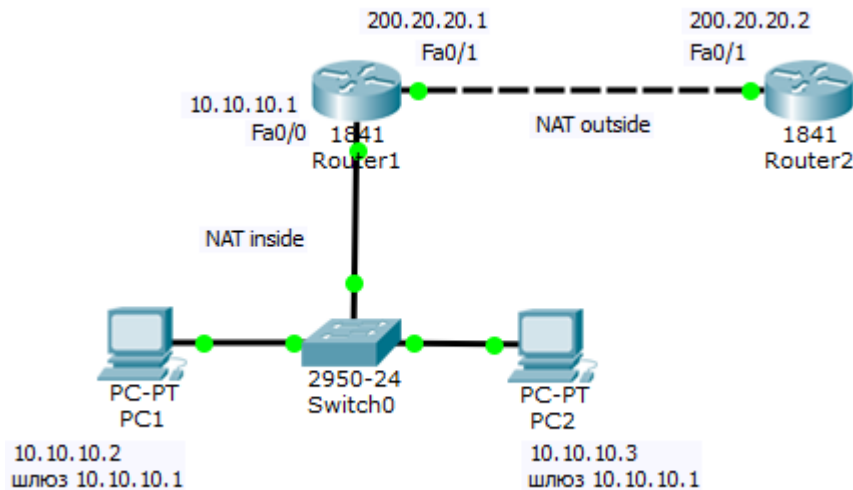
**Рис. 8.8.** Завдання для самостійної роботи

Вирішення задачі наведено у  файлу task-9-3.pkt.

## Завдання №2

### Налаштування статичного NAT

Статичний NAT - зіставляє один NAT inside (внутрішній = приватна локальна ір-адреса) з одним NAT outside (глобальним = публічною зовнішньою ір-адресою) - рис. 8.9. Тут ISP (Internet Service Provider) - постачальник Інтернет-послуг (Інтернет-провайдер).



**Рис. 8.9.** Схема мережі

### Алгоритм налаштування R1

Нижче приведена послідовність команд конфігурування маршрутизатора R1 покроково.

#### Крок 1. Налаштування дефолту на R1

**R1(config)# ip route 0.0.0.0 0.0.0.0 200.20.20.2**

## Крок 2. Налаштування внутрішнього інтерфейсу у відношення NAT

```
R1(config)# interface fastethernet 0/0
```

```
R1(config-if)# ip nat inside
```

## Крок 3. Налаштування зовнішнього інтерфейсу у відношення NAT

```
R1(config)# interface fastethernet 0/1
```

```
R1(config-if)# ip nat outside
```

## Крок 4. Налаштування зіставлення IP-адрес.

```
R1(config)# ip nat inside source static 10.10.10.2 200.10.21.5
```

У результаті цієї команди IP-адресі 200.10.21.5 завжди буде відповідати внутрішня IP-адреса 10.10.10.2, тобто якщо звертатимемося за адресою 200.10.21.5 то відповідати буде PC1.

Повний лістинг команд наведений на рис. 8.10.



```
Router1
Physical | Config | CLI |
IOS Command Line Interface

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 200.20.20.2
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat inside source static 10.10.10.2 200.10.21.5
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

**Рис. 8.10.** Повний лістинг команд по налаштуванню R1

## Команди для перевірки роботи NAT

Перевіримо зв'язок PC1 і R2(рис. 8.11).

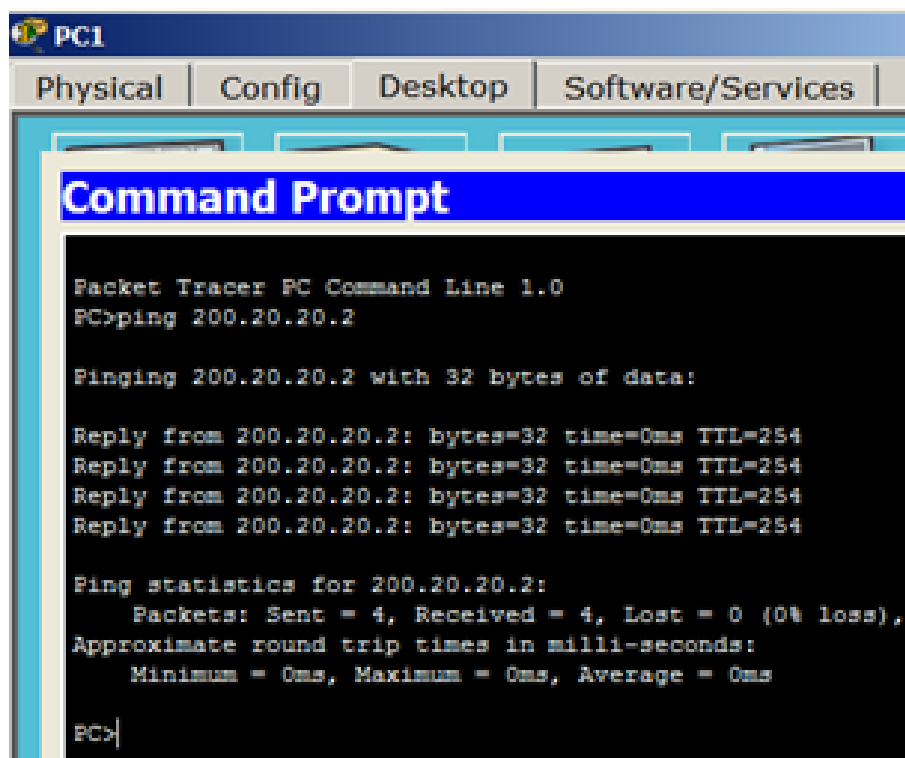


Рис. 8.11. PC1 бачить R2

Перевіримо, що R1 бачить сусідні мережі (рис. 8.12).

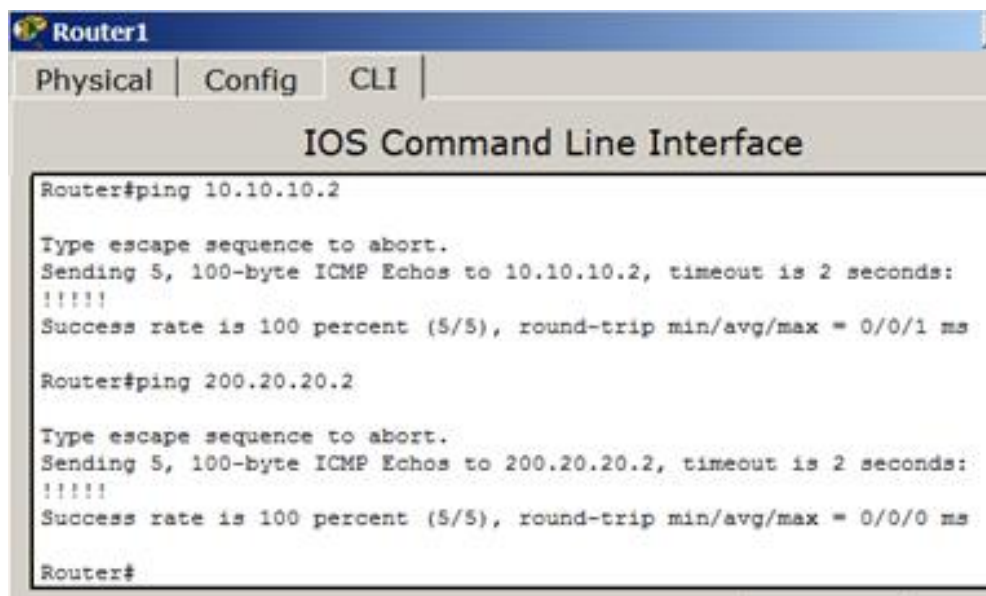


Рис. 8.12. R1 бачить PC1 і R2

Перевіримо механізм роботи статичного NAT: команда **show ip nat translations** виводить активні перетворення, а команда **show ip nat statistics** виводить статистику по NAT перетворенням (рис. 8.13).







## Завдання №3

### Налаштування динамічного NAT на маршрутизаторі R1 покроково

**Крок 1. Налаштування на R1 списку доступу, що відповідає адресам LAN**

```
R1 (config) # access-list 1 permit 10.10.10.0 0.0.0.255
```

Тут 0.0.0.255 - зворотна (інверсна) маска для адреси 10.10.10.0.

**Крок 2. Налаштування пулу адрес**

```
R1 (config) # ip nat pool white-address 200.20.20.1 200.20.20.30 netmask  
255.255.255.0
```

**Крок 3. Налаштування трансляції**

```
R1 (config) # ip nat inside source list 1 pool white-address
```

**Крок 4. Налаштування внутрішнього інтерфейсу у відношення NAT**

```
R1 (config) # interface fastethernet 0/0
```

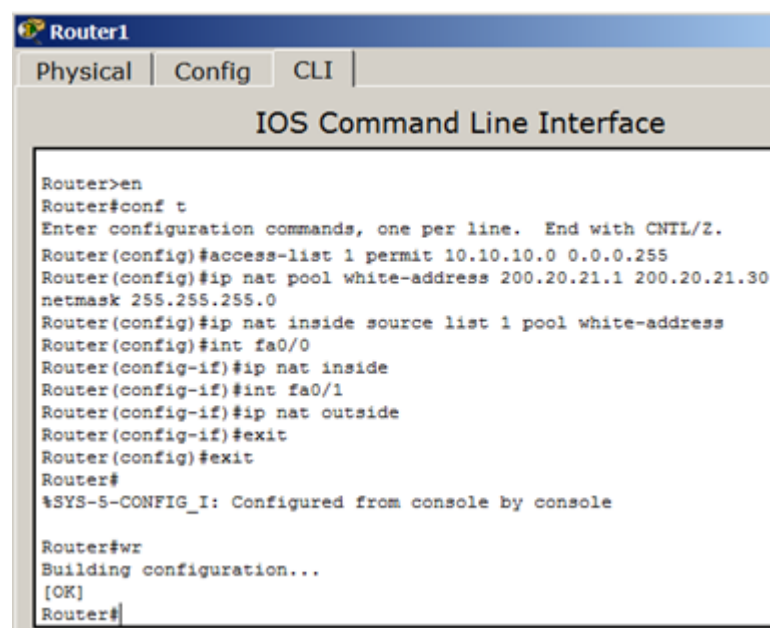
```
R1 (config-if) # ip nat inside
```

**Крок 5. Налаштування зовнішнього інтерфейсу в відношення NAT**

```
R1 (config)# interface fastethernet 0/1
```

```
R1 (config-if)# ip nat outside
```

Нижче продемонстровано повний лістинг команд по налаштуванню R1 (рис.8.15).



```
Router1
Physical | Config | CLI |
IOS Command Line Interface

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 10.10.10.0 0.0.0.255
Router(config)#ip nat pool white-address 200.20.21.1 200.20.21.30
netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool white-address
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

**Рис. 8.15.** Повний лістинг команд по конфігуруванню R1

## Команди для перевірки роботи динамічного NAT

Перевіримо зв'язок PC1 і R2 (рис. 8.16).

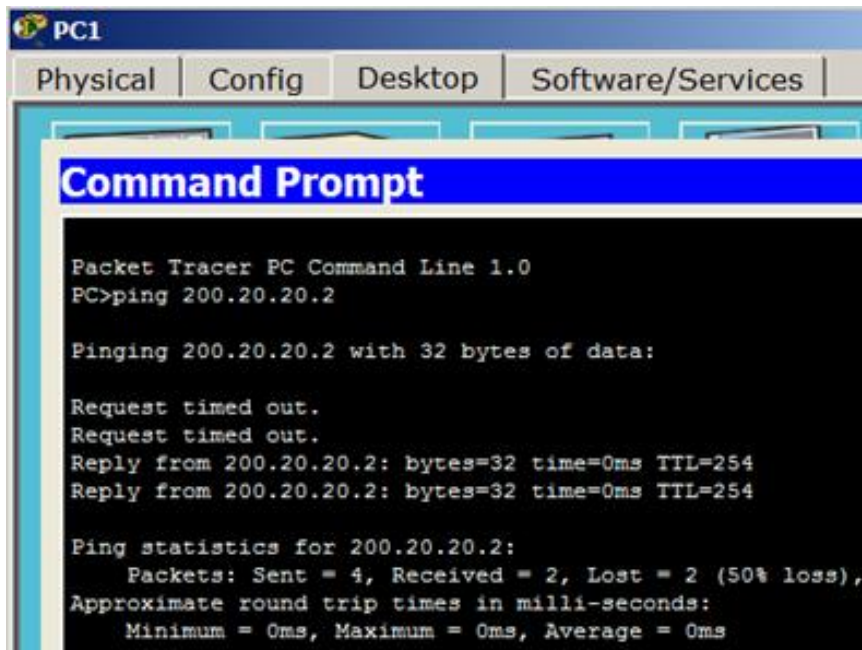


Рис. 8.16. PC1 бачить R2

Перевіримо, що R1 бачить сусідні мережі(рис. 8.17).

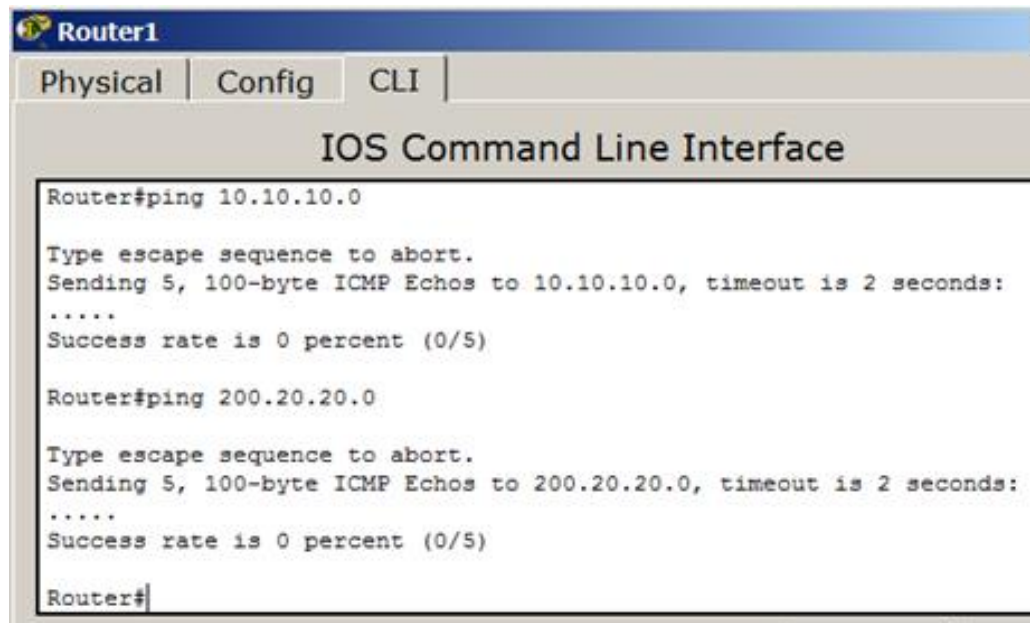
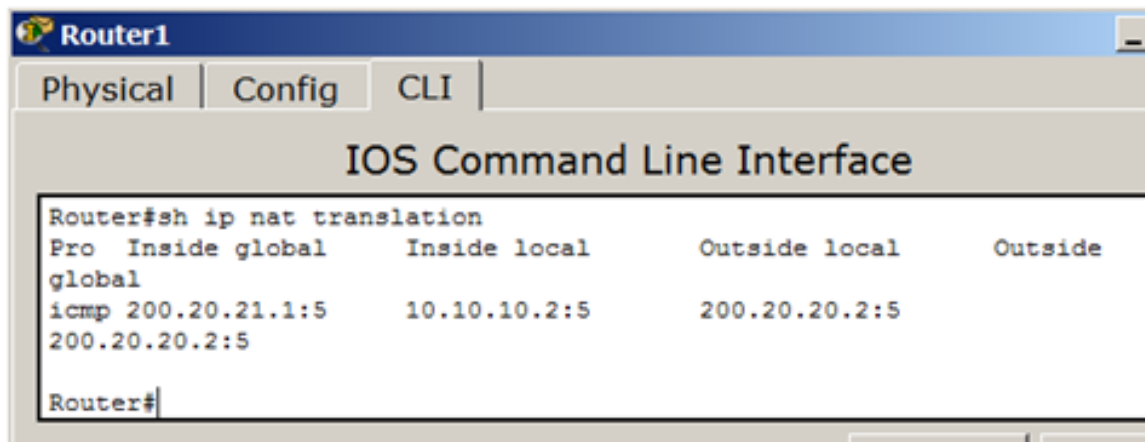


Рис. 8.17. R1 бачить підмережі 10.10.10.0 і 200.20.20.0

Перевіримо механізм роботи динамічного NAT: для цього виконаємо одночасно(паралельно) команди **ping** і **show ip nat translations** (рис. 8.18).

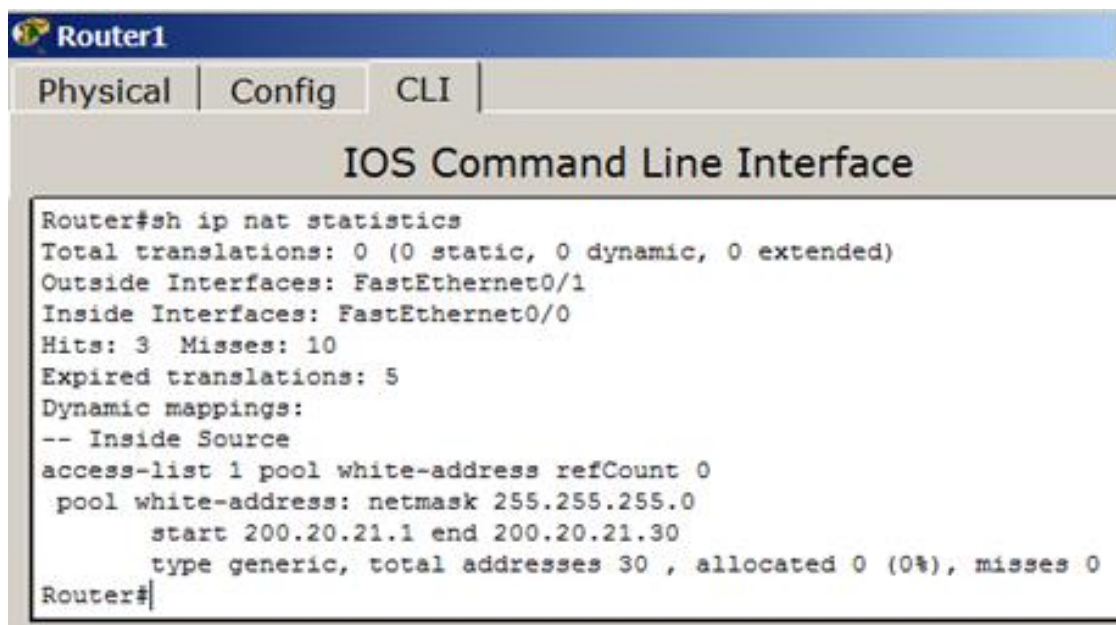


```
Router1
Physical | Config | CLI |
IOS Command Line Interface

Router#sh ip nat translation
Pro Inside global      Inside local      Outside local      Outside
global
icmp 200.20.21.1:5      10.10.10.2:5      200.20.20.2:5
200.20.20.2:5
Router#
```

**Рис. 8.18.** Адреси: глобальна, внутрішня, зовнішня

Командою **show ip nat statistics** виведемо статистику по NAT перетворенням (рис. 8.19).



```
Router1
Physical | Config | CLI |
IOS Command Line Interface

Router#sh ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: FastEthernet0/1
Inside Interfaces: FastEthernet0/0
Hits: 3 Misses: 10
Expired translations: 5
Dynamic mappings:
-- Inside Source
access-list 1 pool white-address refCount 0
 pool white-address: netmask 255.255.255.0
   start 200.20.21.1 end 200.20.21.30
   type generic, total addresses 30 , allocated 0 (0%), misses 0
Router#
```

**Рис. 8.19.** Статистика роботи динамічного NAT

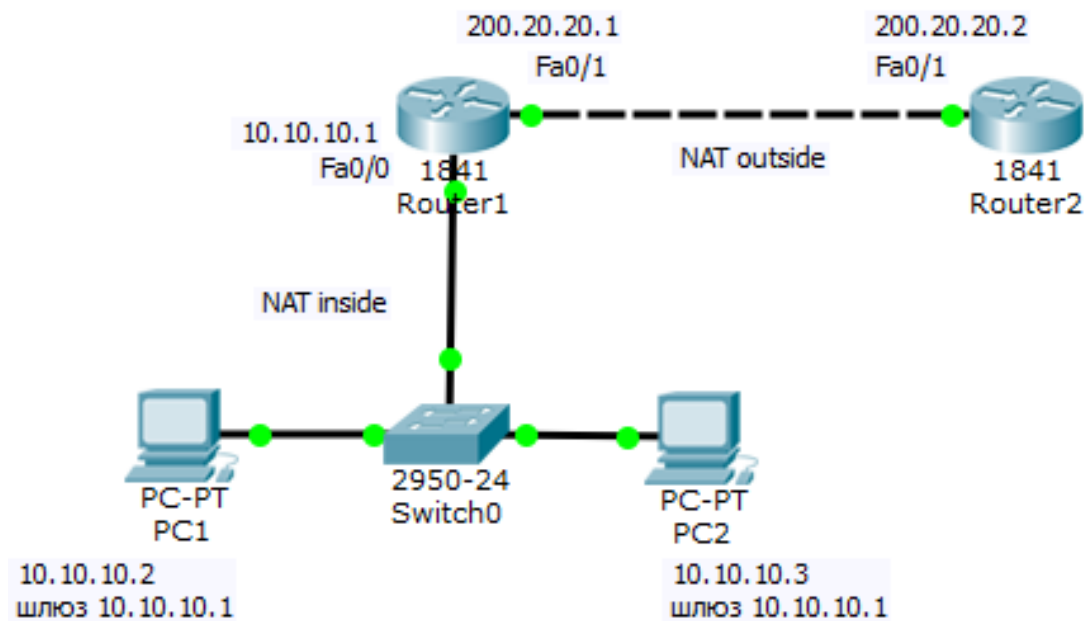
З ілюстрації бачимо, що локальним адресам відповідає пул зовнішніх адрес від 200.20.20.1 до 20.20.20.30.

Робоча мережа даного прикладу додається до курсу у вигляді файлу  [task-9-5.pkt](#)

## Завдання №4

### Динамічний NAT Overload: налаштування PAT (маскарадинг)

*PAT (Port Address Translation)* - відображає декілька локальних (приватних) IP-адрес у глобальну IP-адресу, скориставшись різними портами (рис. 8.20).



**Рис. 8.20.** Схема мережі на налаштування трансляції адрес NAT

Розглянемо *алгоритм* роботи покроково.

**Крок 1.** Налаштування списку доступу, що відповідає внутрішнім приватним адресам

```
R1(config)# access-list 1 permit 10.10.10.0 0.0.0.255
```

**Крок 2.** Налаштування трансляції

```
R1(config)# ip nat inside source list 1 interface fastethernet 0/1 overload
```

**Крок 3.** Налаштування внутрішнього інтерфейсу у відношенні NAT

```
R1(config)# interface fastethernet 0/0
```

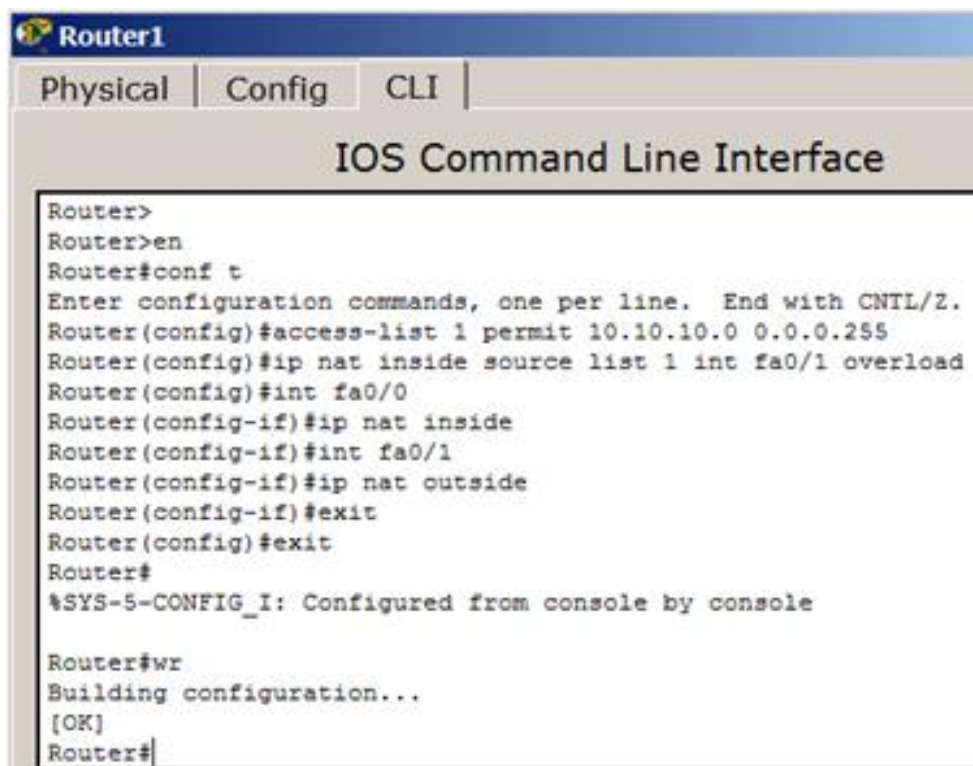
```
R1(config-if)# ip nat inside
```

**Крок 4.** Налаштування NAT на інтерфейсі

```
R1(config)# interface fastethernet 0/1
```

```
R1(config-if)# ip nat outside
```

Нижче дано повний лістинг команд по конфігуруванню R1(рис. 8.21).



```
Router1
Physical | Config | CLI |
IOS Command Line Interface

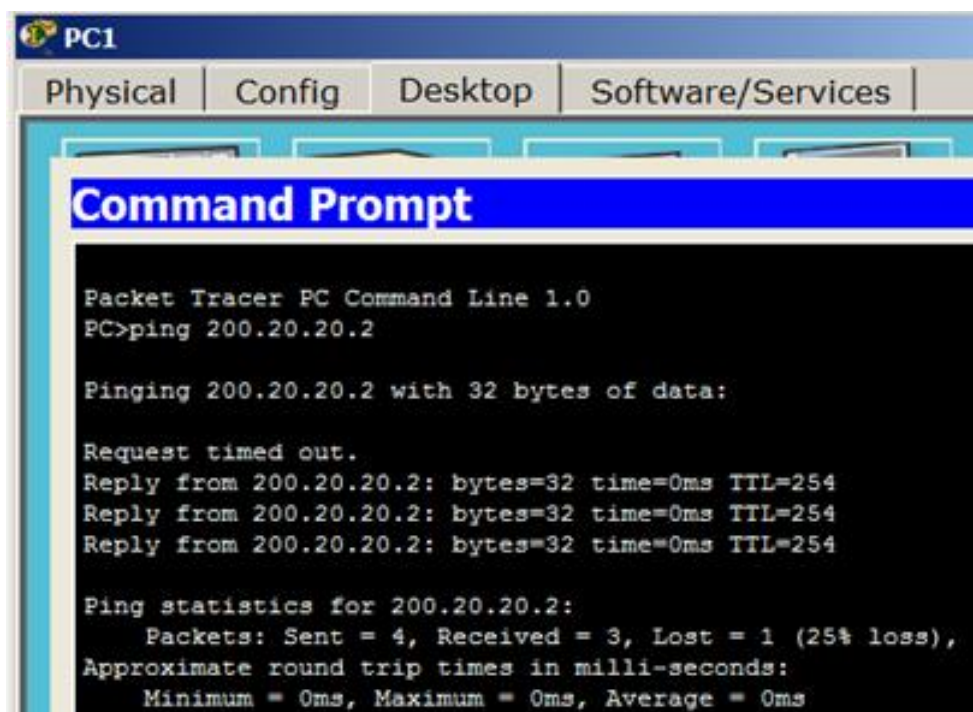
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 10.10.10.0 0.0.0.255
Router(config)#ip nat inside source list 1 int fa0/1 overload
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

**Рис. 8.21.** Лістинг команд по конфігуруванню R1

### Команди для перевірки роботи маскування (PAT)

Перевіримо зв'язок PC1 і R2 (рис. 8.22).



```
PC1
Physical | Config | Desktop | Software/Services |
Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 200.20.20.2

Pinging 200.20.20.2 with 32 bytes of data:

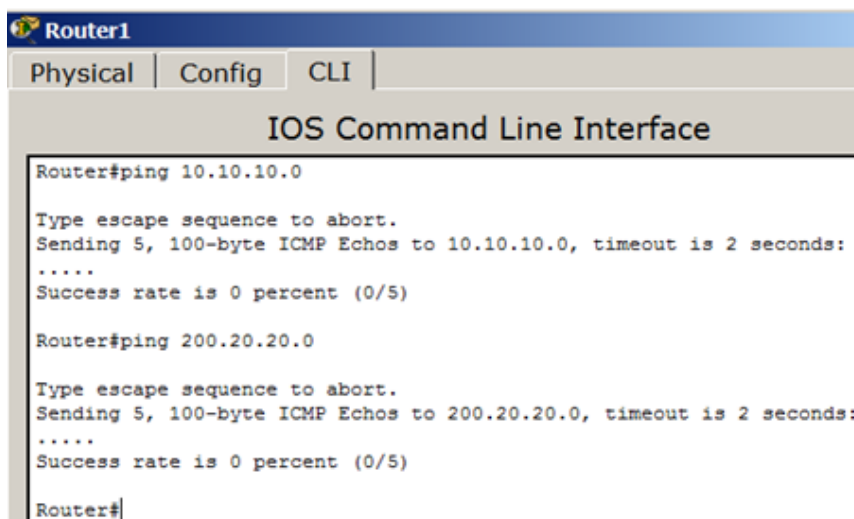
Request timed out.
Reply from 200.20.20.2: bytes=32 time=0ms TTL=254
Reply from 200.20.20.2: bytes=32 time=0ms TTL=254
Reply from 200.20.20.2: bytes=32 time=0ms TTL=254

Ping statistics for 200.20.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

**Рис. 8.22.** PC1 бачить R2

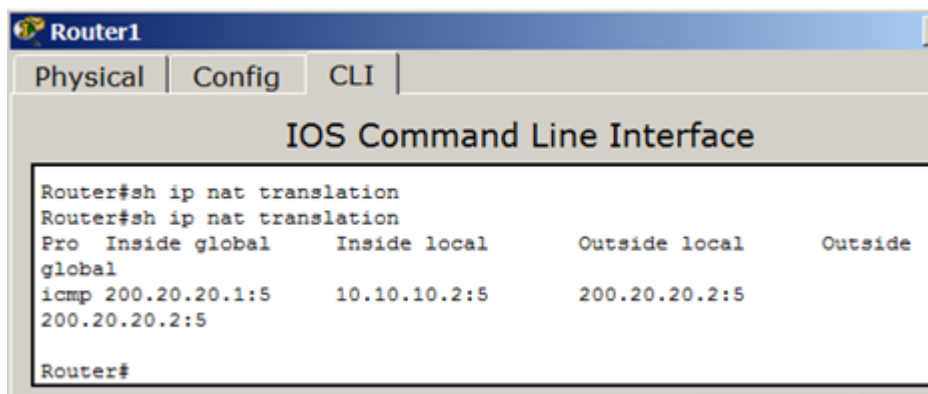
Перевіримо, що R1 бачить сусідні мережі(рис. 8.23).





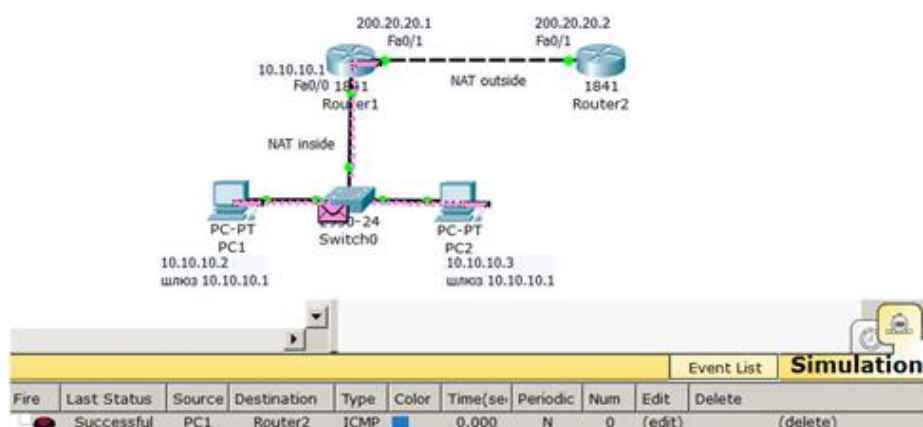
**Рис.8.23.** R1 бачить підмережі 10.10.10.0 і 200.20.20.0

Перевіримо механізм роботи динамічного NAT: для цього виконаємо одночасно(паралельно) команди **ping** і **show ip nat translations** (рис. 8.24).



**Рис. 8.24.** Адреси: глобальна, внутрішня, зовнішня

Перевіримо роботу мережі в режимі симуляції(рис. 8.25).



**Рис. 8.25.** NAT працює, PC1 і R2 надсилають та отримують пакет Successful

Робоча мережа даного прикладу додається до курсу у вигляді файлу  [task-](#)

[9-6.pkt](#)