

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 пристройів 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 проходжені через маршрутизатор, адреса змінюються 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 проходжені 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.

- 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).

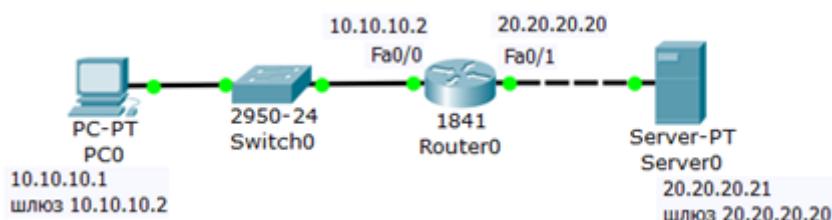


Рис. 8.1. Схема мережі

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

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit any
Router(config)#ip nat inside source list 1 interface fa 0/1 overload
Router(config)#

```

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)

```

Router(config)#ip nat inside source list 1 interface fa 0/1 overload
Router(config)#int fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int fa 0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#

```

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).

```

Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#sh ip nat translations
Router#wr mem
Building configuration...
[OK]
Router#

```

Рис. 8.4. Зберігаємо налаштування в ОЗУ

Перевіряємо роботу мережі (перегляд стану таблиці NAT)

З PC0 пінгуюмо провайдера і переконаємося, що PC1 і сервер можуть спілкуватися (рис. 8.5).

```

PC>ping 20.20.20.21

Pinging 20.20.20.21 with 32 bytes of data:

Reply from 20.20.20.21: bytes=32 time=93ms TTL=127
Reply from 20.20.20.21: bytes=32 time=94ms TTL=127
Reply from 20.20.20.21: bytes=32 time=78ms TTL=127
Reply from 20.20.20.21: bytes=32 time=94ms TTL=127

Ping statistics for 20.20.20.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 78ms, Maximum = 94ms, Average = 89ms

PC>

```

Рис. 8.5. З внутрішньої мережі пінгуюмо 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.

```

Router>sh ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
icmp 20.20.20.20:19    10.10.10.1:19    20.20.20.21:19    20.20.20.21:19
icmp 20.20.20.20:20    10.10.10.1:20    20.20.20.21:20    20.20.20.21:20

Router>

```

Рис. 8.6. Під час пінгу переглядаємо стан таблиці NAT

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

Event List	Simulation									
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
Successful	PC0	Server0	ICMP			0.000	N	0	(edit)	(delete)

NAT Table for Router0				
Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	20.20.20.20:10	10.10.10.1:10	20.20.20.21:10	20.20.20.21:10

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?

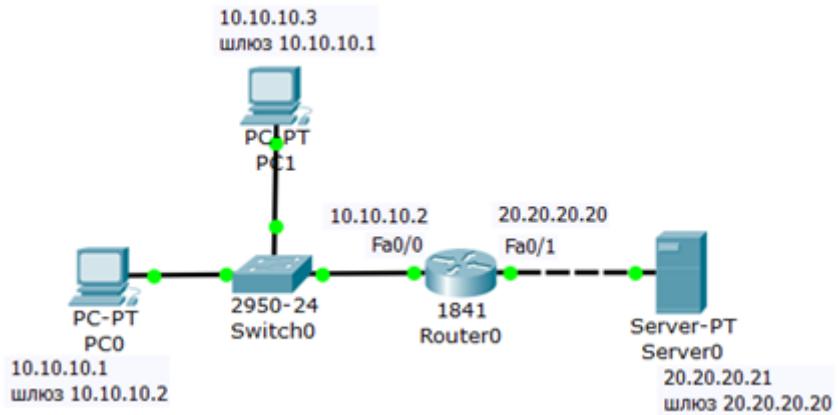


Рис. 8.8. Завдання для самостійної роботи

Вирішення задачі наведено

Завдання №2

Налаштування статичного NAT

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

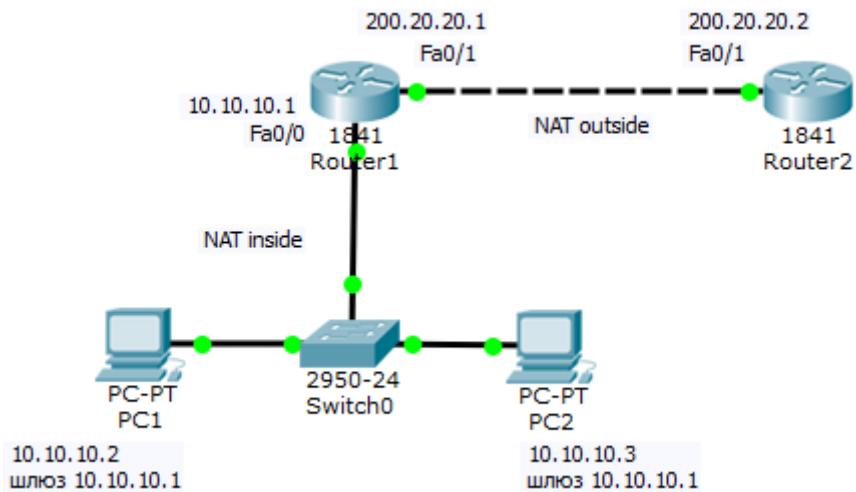


Рис. 8.9. Схема мережі

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 відношенні NAT

R1(config)# interface fastethernet 0/0

R1(config-if)# ip nat inside

Крок 3. Налаштування зовнішнього інтерфейсу у відношенні 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.

The screenshot shows the Cisco IOS CLI interface for Router1. The window title is "Router1". The tabs at the top are "Physical", "Config" (which is selected), and "CLI". The main area is titled "IOS Command Line Interface". The command history is as follows:

```
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).

The screenshot shows a 'Command Prompt' window from Packet Tracer. The title bar says 'pc1'. The menu bar includes 'Physical', 'Config', 'Desktop', and 'Software/Services'. The main window title is 'Command Prompt'. The command entered is 'ping 200.20.20.2'. The output shows the ping process: 'Pinging 200.20.20.2 with 32 bytes of data', four replies from 200.20.20.2, and ping statistics: 'Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)', 'Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms'. The prompt 'PC>' is at the bottom.

```

Packet Tracer PC Command Line 1.0
PC>ping 200.20.20.2

Pinging 200.20.20.2 with 32 bytes of data:

Reply from 200.20.20.2: bytes=32 time=0ms TTL=254

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

PC>

```

Рис. 8.11. PC1 бачить R2

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

The screenshot shows the 'IOS Command Line Interface' for 'Router1'. The menu bar includes 'Physical', 'Config', and 'CLI'. The main window title is 'IOS Command Line Interface'. The commands entered are 'ping 10.10.10.2' and 'ping 200.20.20.2'. The output for the first ping shows success: 'Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms'. The output for the second ping also shows success: 'Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms'. The prompt 'Router#' is at the bottom.

```

Router#ping 10.10.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router#ping 200.20.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.20.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Router#

```

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).

Router1

Physical | Config | CLI |

IOS Command Line Interface

```

Router#sh ip nat translation
Pro Inside global      Inside local      Outside local      Outside
global
icmp 200.10.21.5:2    10.10.10.2:2     200.20.20.2:2
200.20.20.2:2
icmp 200.10.21.5:3    10.10.10.2:3     200.20.20.2:3
200.20.20.2:3
--- 200.10.21.5       10.10.10.2       ---           ---
Router#sh ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: FastEthernet0/1
Inside Interfaces: FastEthernet0/0
Hits: 1 Misses: 7
Expired translations: 3
Dynamic mappings:
Router#

```

Рис. 8.13. Перевірка механізму роботи статичного NAT

З ілюстрації бачимо, що глобальний IP-адресі 200.10.21.5 відповідає локальному IP-адреса 10.10.10.2, а також, який інтерфейс є зовнішнім, а який - внутрішнім.

Робоча схема мережі даного прикладу представлена

Динамічна трансляція адрес.

Налаштування динамічного NAT

Динамічний *NAT* - використовує пул доступних глобальних (публічних) IP-адрес і назначає їх внутрішнім локальним (приватним) адресам. Схема роботи приведена на рис. 8.14.

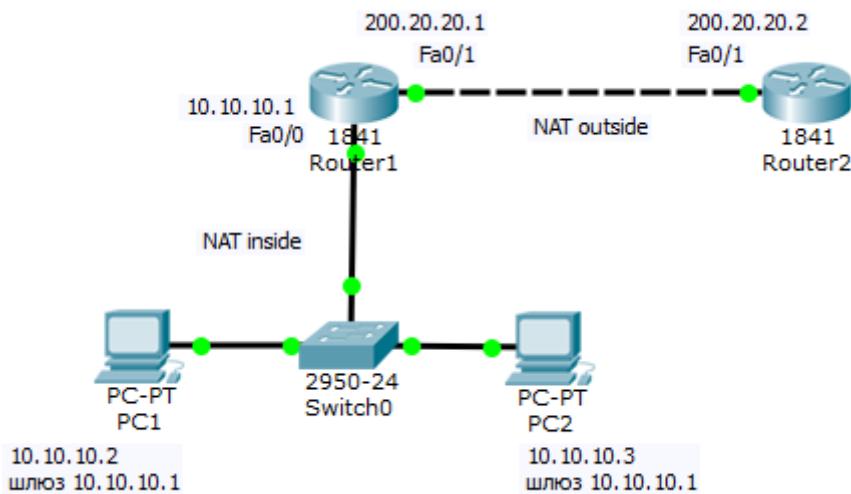


Рис. 8.14. Схема мережі

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 відношенні NAT

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

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

Крок 5. Налаштування зовнішнього інтерфейсу в відношенні NAT

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

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

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

The screenshot shows the Router1 CLI interface. The title bar says "Router1". Below it is a menu bar with "Physical", "Config" (which is selected), and "CLI". The main window is titled "IOS Command Line Interface". The command history is as follows:

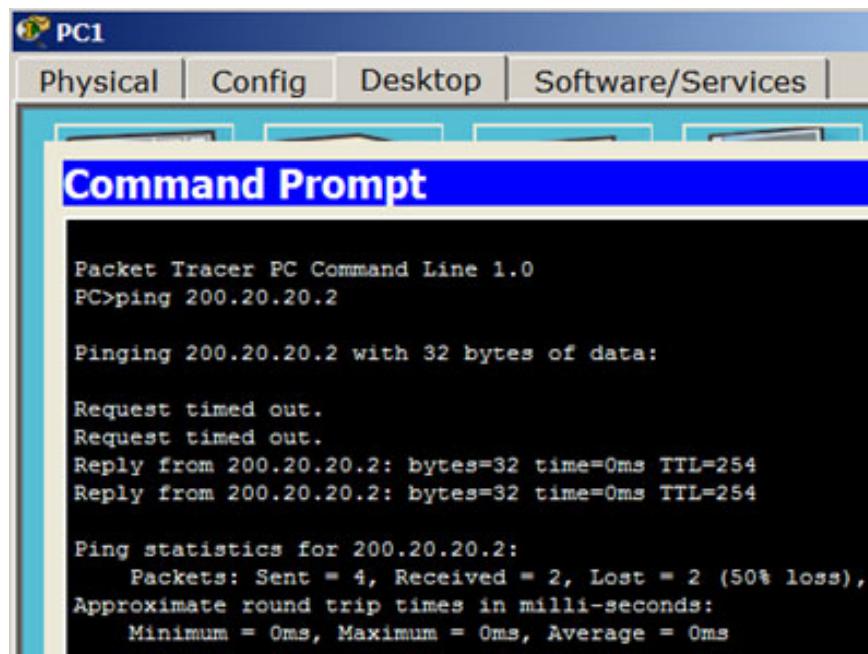
```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 10.10.10.0 0.0.0.255
Router(config)#ip nat pool white-address 200.20.20.1 200.20.20.30
netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool white-address
Router(config)#int 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).



The screenshot shows a 'Command Prompt' window in the Packet Tracer interface. The title bar says 'PC1'. The menu bar includes 'Physical', 'Config', 'Desktop', and 'Software/Services'. The main window title is 'Command Prompt'. The command entered is 'ping 200.20.20.2'. The output shows the ping process, receiving two replies from 200.20.20.2, and concluding with ping statistics.

```
Packet Tracer PC Command Line 1.0
PC>ping 200.20.20.2

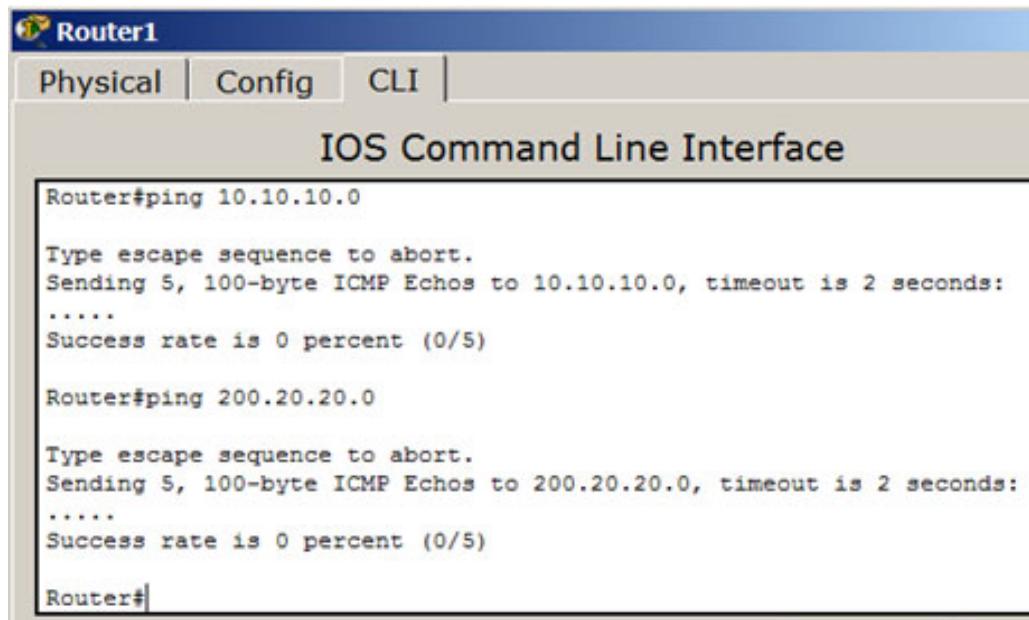
Pinging 200.20.20.2 with 32 bytes of data:

Request timed out.
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

Ping statistics for 200.20.20.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рис. 8.16. PC1 бачить R2

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



The screenshot shows the 'IOS Command Line Interface' on Router1. The title bar says 'Router1'. The menu bar includes 'Physical', 'Config', and 'CLI'. The main window title is 'IOS Command Line Interface'. The user enters 'ping 10.10.10.0' and 'ping 200.20.20.0', both of which show 0% success rate.

```
Router#ping 10.10.10.0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.0, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Router#ping 200.20.20.0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.20.20.0, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Router#
```

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).

Router#sh ip nat translation

Protocol	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).

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

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).

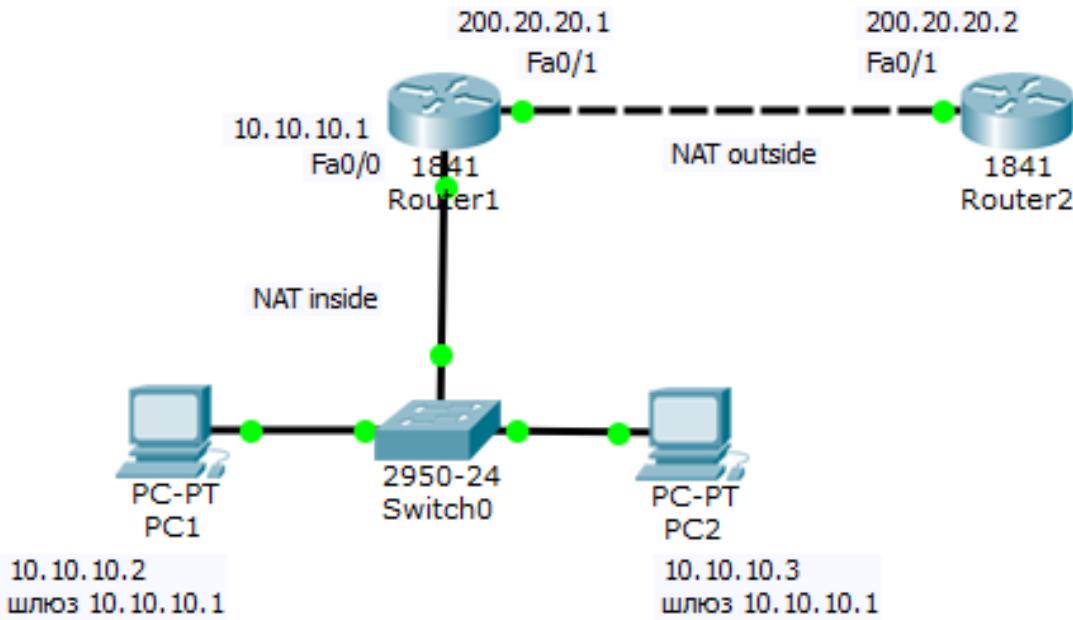


Рис. 8.20. Схема мережі на налаштування трансляції адрес РАТ

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).

```

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 маскарадингу (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).

```

Router#ping 10.10.10.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.0, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Router#ping 200.20.20.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.20.20.0, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Router#

```

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).

```

Router#sh ip nat translation
Router#sh ip nat translation
Pro Inside global      Inside local      Outside local      Outside
global
icmp 200.20.20.1:5    10.10.10.2:5    200.20.20.2:5
200.20.20.2:5

Router#

```

Рис. 8.24. Адреси: глобальна, внутрішня, зовнішня

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

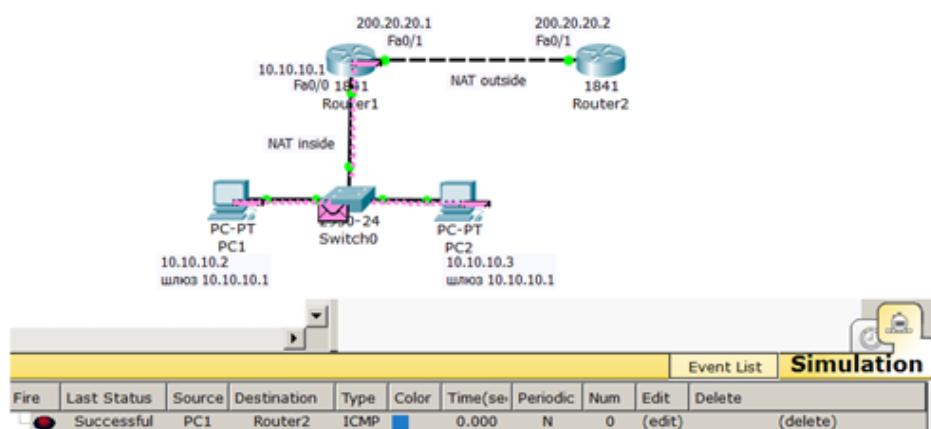


Рис. 8.25. ПАТ працює, PC1 і R2 надсилають та отримують пакет Successful

Робоча мережа даного прикладу додається до курсу у вигляді