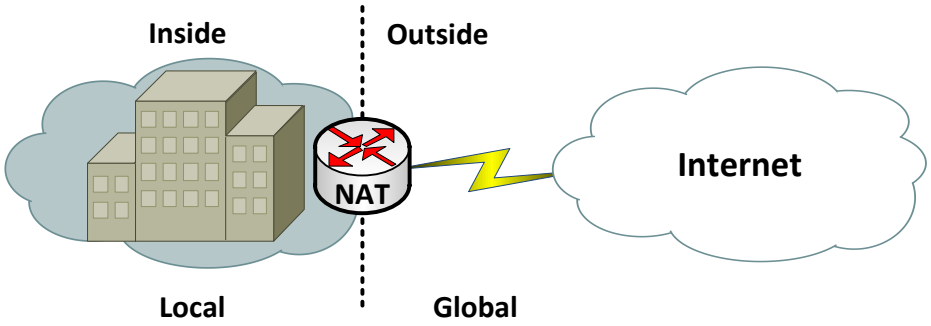
CHƯƠNG . NAT

Chương này trình bày một số đặc điểm của NAT, phân loại và cấu hình trên thiết bị Cisco. Học xong chương này, người học có khả năng:

- *Trình bày được một số khái niệm dùng trong kỹ thuật NAT*
- *Phân loại và trình bày được đặc điểm của mỗi loại NAT*
- *Cấu hình NAT*

1. Giới thiệu

NAT *(Network Address Translation)* là một kỹ thuật cho phép chuyển đổi từ một địa chỉ IP này thành một địa chỉ IP khác. Thông thường, NAT được dùng phổ biến trong mạng sử dụng địa chỉ cục bộ, cần truy cập đến mạng công cộng (Internet). Vị trí thực hiện NAT là router biên kết nối giữa hai mạng.

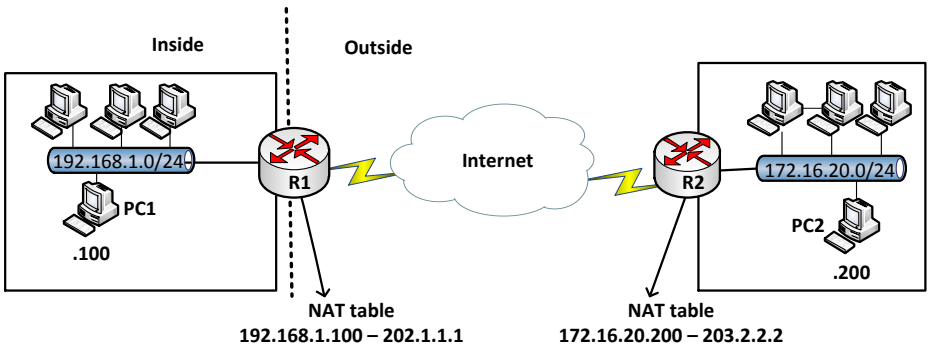


***Hình 4.1** Mô hình thực hiện NAT*

❖ **Địa chỉ *private* và địa chỉ *public***

- Địa chỉ private: được định nghĩa trong RFC 1918
  - ✓ 10.0.0.0 – 10.255.255.255
  - ✓ 172.16.0.0 – 172.31.255.255
  - ✓ 192.168.0.0 – 192.168.255.255
- Địa chỉ public: các địa chỉ còn lại. Các địa chỉ public là các địa chỉ được cung cấp bởi các tổ chức có thẩm quyền.

❖ **Một số thuật ngữ**



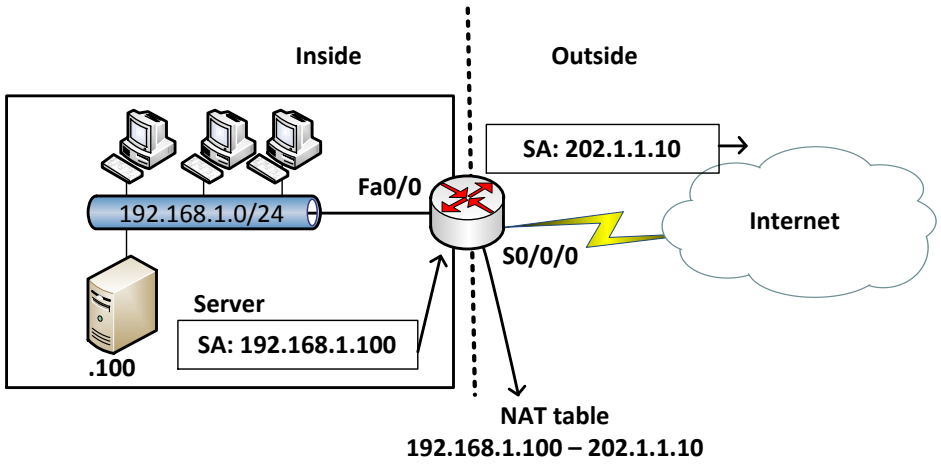
***Hình 4.2** Địa chỉ inside và outside*

- Địa chỉ **inside local**: là địa chỉ IP gán cho một thiết bị ở mạng bên trong. Địa chỉ này hầu như không phải địa chỉ được cấp bởi NIC (Network Information Center) hay nhà cung cấp dịch vụ.
- Địa chỉ **inside global**: là địa chỉ đã được đăng ký với NIC, dùng để thay thế một hay nhiều địa chỉ IP *inside local*.
- Địa chỉ **outside local**: là địa chỉ IP của một thiết bị bên ngoài khi nó xuất hiện bên trong mạng. Địa chỉ này không nhất thiết là địa chỉ được đăng ký, nó được lấy từ không gian địa chỉ bên trong.
- Địa chỉ **outside global**: là địa chỉ IP gán cho một thiết bị ở mạng bên ngoài. Địa chỉ này được lấy từ địa chỉ có thể dùng để định tuyến toàn cầu hay từ không gian địa chỉ mạng.

2. Static NAT

Static NAT được dùng để chuyển đổi một địa chỉ IP này sang một địa chỉ khác một cách cố định, thông thường là từ một địa chỉ cục bộ sang một địa chỉ công cộng và quá trình này được cài đặt thủ công, nghĩa là địa chỉ ánh xạ và địa chỉ được ánh xạ được chỉ định rõ ràng tương ứng duy nhất.

Static NAT rất hữu ích trong trường hợp những thiết bị cần phải có địa chỉ cố định để có thể truy cập từ bên ngoài Internet. Những thiết bị này phổ biến là những Server như Web, Mail,...



Hình 4.3 *Chuyển dịch địa chỉ dạng tĩnh*

❖ Cấu hình Static -NAT

✓ Thiết lập mối quan hệ chuyển đổi giữa địa chỉ nội bộ bên trong và địa chỉ đại diện bên ngoài.

```
Router(config)#ip nat inside source static local-ip global-ip
```

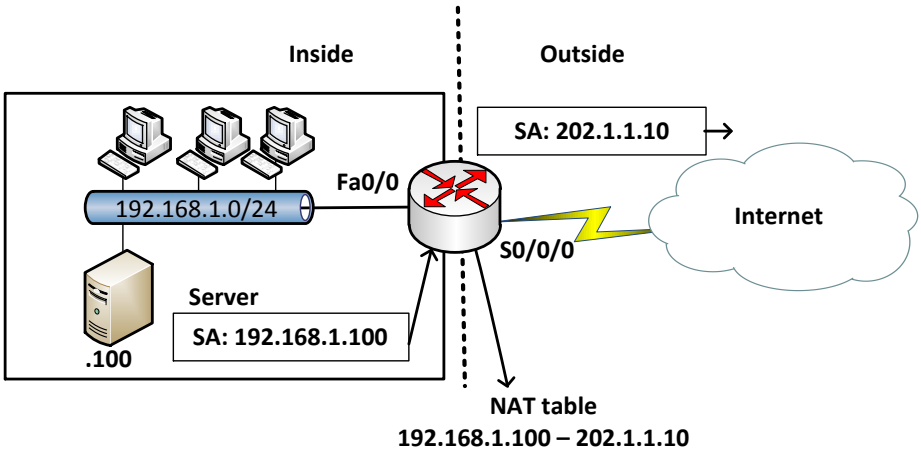
✓ Xác định các cổng kết nối vào mạng bên trong và thực hiện lệnh

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

✓ Xác định các cổng kết nối ra mạng công cộng bên ngoài và thực hiện lệnh

```
Router(config-fi)#ip nat outside
```

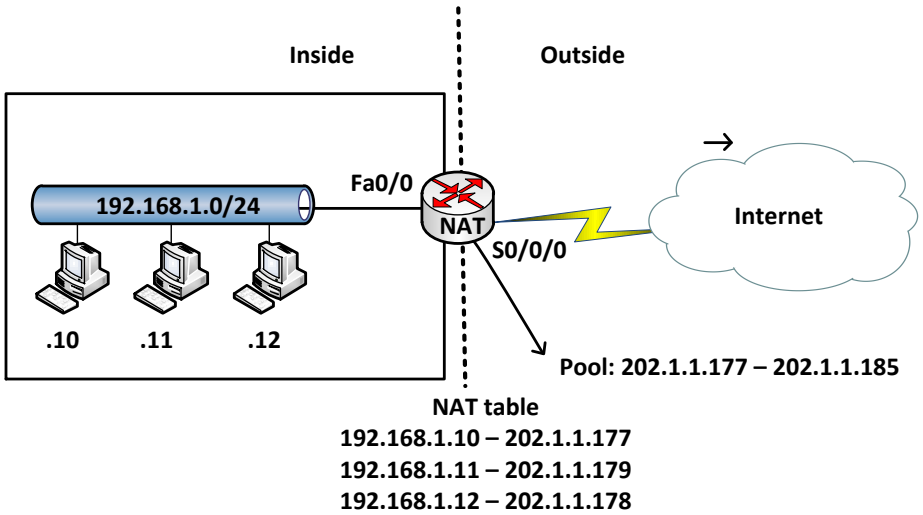
Ví dụ:




```
Router(config)#ip nat inside source static 192.168.1.100 202.1.1.10
Router(config)#interface fa0/0
Router(config-if)#ip nat inside
Router(config)#interface S0/0/0
Router(config-if)#ip nat outside
```

3. Dynamic NAT

Dynamic NAT được dùng để ánh xạ một địa chỉ IP này sang một địa chỉ khác một cách tự động, thông thường là ánh xạ từ một địa chỉ cục bộ sang một địa chỉ được đăng ký. Bất kỳ một địa chỉ IP nào nằm trong dải địa chỉ IP công cộng đã được định trước đều có thể được gán cho một thiết bị bên trong mạng.



❖ Cấu hình Dynamic NAT

✓ Xác định dải địa chỉ đại diện bên ngoài (public): các địa chỉ NAT

```
Router(config)#ip nat pool name start-ip end-ip [netmask
netmask/prefix-length prefix-length]
```

- ✓ Thiết lập ACL cho phép những địa chỉ nội bộ bên trong nào được chuyển đổi: các địa chỉ được NAT

  `Router(config)#access-list access-list-number pertmit source [source-wildcard]`

- ✓ Thiết lập mối quan hệ giữa địa chỉ nguồn đã được xác định trong ACL với dải địa chỉ đại diện ra bên ngoài

  `Router(config)#ip nat inside source list <acl-number> pool <name>`

- ✓ Xác định các cổng kết nối vào mạng nội bộ

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

- ✓ Xác định các cổng kết nối ra bên ngoài

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

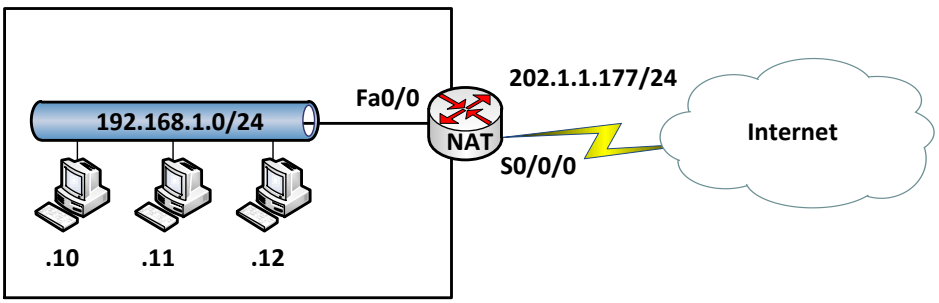
Ví dụ: Cấu hình cho mô hình trong hình trên

```
Router(config)#ip nat pool abc 202.1.1.177 202.1.1.185 netmask
255.255.255.0

Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Router(config)#ip nat inside source list 1 pool abc

Router(config)#interface fa0/0

Router(config-if)#ip nat inside

Router(config)#interface S0/0/0

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

4. NAT overload

NAT Overload là một dạng của *Dynamic NAT*, nó thực hiện ánh xạ nhiều địa chỉ IP thành một địa chỉ (many – to – one) và sử dụng các chỉ số cổng khác nhau để phân biệt cho từng chuyển đổi. NAT Overload còn có tên gọi là PAT *(Port Address Translation).*

Chỉ số cổng được mã hóa 16 bit, do đó có tới 65536 địa chỉ nội bộ có thể được chuyển đổi sang một địa chỉ công cộng.



NAT table
192.168.1.10 – 202.1.1.177:**1030**
192.168.1.11 – 202.1.1.177:**1031**
192.168.1.12 – 202.1.1.177:**1032**

❖ **Cấu hình NAT Overload**

✓ Xác định dãy địa chỉ bên trong cần chuyển dịch ra ngoài *(private ip addresses range)*

```
Router(config)#access-list <ACL-number> permit <source>
<wildcard>
```

✓ Cấu hình chuyển đổi địa chỉ IP sang cổng nối ra ngoài

```
Router(config)#ip nat inside source list <ACL-number> interface
<interface>  overload
```

✓ Xác định các cổng nối vào mạng bên trong và nối ra mạng bên ngoài

Đối với các cổng nối vào mạng bên trong:

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

Đối với nối ra mạng bên ngoài:

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

Ví dụ:

Giả sử hệ thống mạng công ty mô tả như sơ đồ trên, công ty thuê một đường kết nối Internet qua cổng S0/0/0 của router. Công ty muốn tất cả các thành viên trong công ty đều có thể truy cập được Internet.

Trong trường hợp này, người quản trị mạng thực hiện cấu hình PAT (NAT Overload) trên router để cho phép người dùng trong công ty có thể truy cập ra ngoài bằng địa chỉ được đăng ký trên cổng *S0/0/0* của router.

Các lệnh cấu hình NAT như sau:

```
Rconfig)#access-list 1 permit 192.168.1.0 0.0.0.255

R(config)#ip nat inside source list 1 interface s0/0/0 overload

Rconfig)#interface fa0/0

R(config-if)#ip nat inside

R(config)#interface S0/0/0

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

❖ **Các lệnh kiểm tra cấu hình**

`R#show ip nat translation` → hiển thị bảng NAT đang hoạt động

`R#show ip nat statistics` → hiển thị trạng thái hoạt động của NAT

`R#clear ip nat translation *` → xóa bảng NAT

`R#debug ip nat` → kiểm tra hoạt động của NAT, hiển thị các thông tin chuyển đổi NAT bởi router.

5. Tổng kết chương

Cisco IOS NAT cho phép một tổ chức với những địa chỉ không đăng ký (địa chỉ local) có thể kết nối Internet bằng cách chuyển những địa chỉ này thành những địa chỉ đã được đăng ký (public).

NAT có ưu điểm là tiết kiệm địa chỉ đăng ký (public). Tuy nhiên, sử dụng NAT cũng có khuyết điểm là làm tăng thời gian trễ do phải thực hiện việc chuyển đổi địa chỉ trong các gói dữ liệu.

Ba kỹ thuật NAT được dùng là: *Static NAT, Dynamic NAT* và *NAT Overload (PAT).* *Static NAT* được sử dụng để ánh xạ địa chỉ theo kiểu "*one-to-one"* và được chỉ định bởi người quản trị. *Dynamic NAT* là kiểu chuyển dịch địa chỉ dạng "*one-to-one"* một cách tự động. *NAT Overload* là kiểu chuyển dịch địa chỉ dạng "*many-to-one"* một cách tự động, sử dụng các chỉ số cổng (port) để phân biệt cho từng chuyển dịch.

6. Câu hỏi và bài tập

6.1. Địa chỉ "Inside Global" trong cấu hình NAT có ý nghĩa gì?

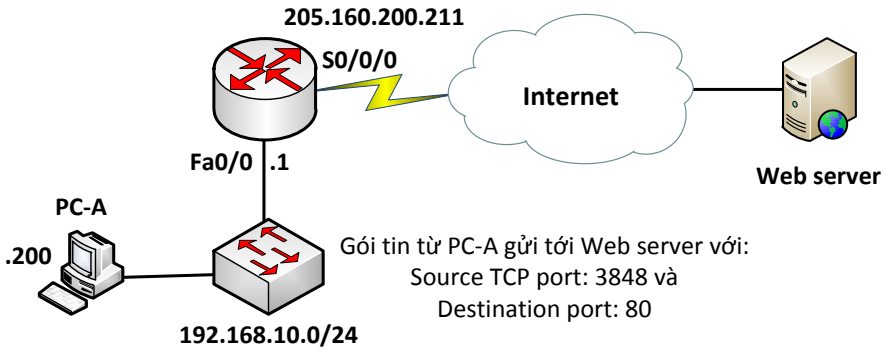
A. Là địa chỉ MAC được các máy tính sử dụng để kết nối ra ngoài.

B. Là địa chỉ tóm tắt đại diện cho tất cả các mạng bên trong.

C. Là địa chỉ cục bộ gán cho máy tính ở mạng bên trong.

D. Là địa chỉ được đăng ký (public) đại diện cho các máy tính bên trong khi đi ra mạng bên ngoài.

6.2. Cho mô hình mạng



NAT Overload đã được cấu hình trên router, phát biểu nào sau đây là đúng khi máy tính PC-A giao tiếp với Web server?

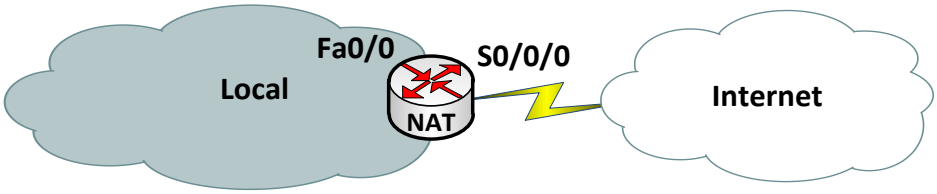
A. Web server sử dụng địa chỉ IP đích là 205.160.200.211 và port đích là 80 khi gửi gói tin đến cho PC-A

B. Máy tính PC-A sử dụng địa chỉ IP đích là 192.168.10.1 và port nguồn là 80 khi gửi các gói tin đến Web server.

C. Web server sử dụng địa chỉ IP đích là 205.160.200.211 và port đích là 3848 khi gửi gói tin đến cho PC-A

D. Máy tính PC-A sử dụng địa chỉ IP đích là 205.160.200.211 và port đích là 3848 khi gửi các gói tin đến Web server.

6.3. Cho mô hình mạng



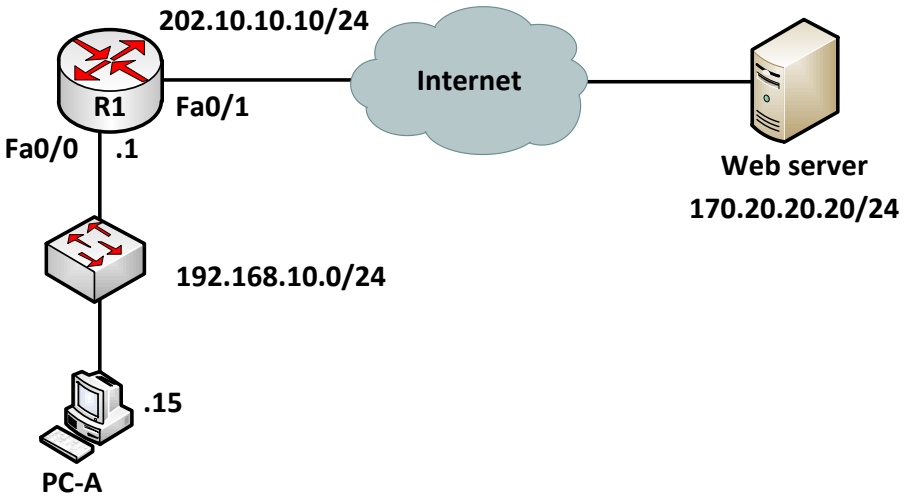
Lệnh nào sau đây được cấu hình trên cổng S0/0/0 của Router NAT khi cấu hình NAT trên router này?

A. `ip nat inside`
B. `ip nat outside`
C. `ip pat inside`
D. `ip pat outside`

6.4. Hai phát biểu nào sau đây là đúng cho loại Static NAT

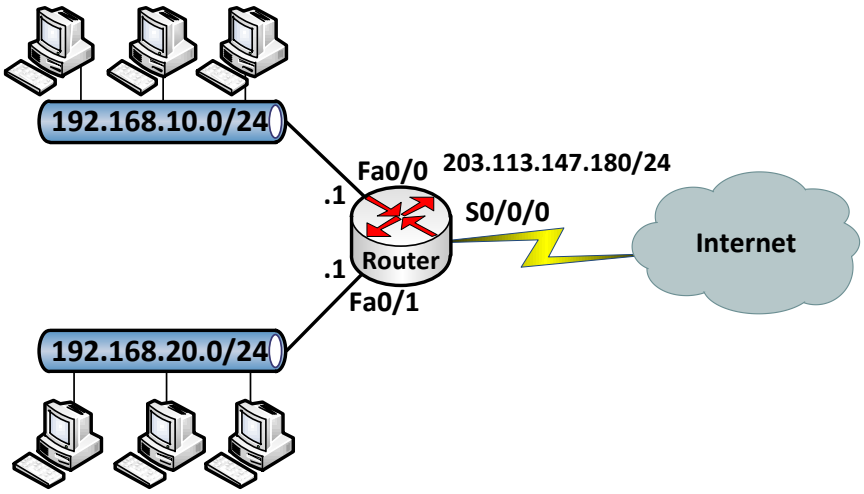
A. Loại này cho phép từ bên ngoài có thể khởi tạo kết nối vào bên trong
B. Loại này không yêu cầu phải chỉ ra cổng nào gắn với mạng ngoài và cổng nào gắn với mạng bên trong ở router thực hiện NAT
C. Loại này có thể dùng ACL để cho phép nhiều kết nối khởi tạo từ mạng bên ngoài
D. Loại này luôn được hiển thị trong bảng NAT

6.5. Cho mô hình mạng



Trong mô hình trên đã cấu hình NAT overload trên router R1. PC-A đang truy cập tới Web server. Hãy cho biết các địa chỉ: *inside local, inside global, outside local, outside globlal*.

6.6. Cho mô hình mạng



Router được cấu hình như sau:

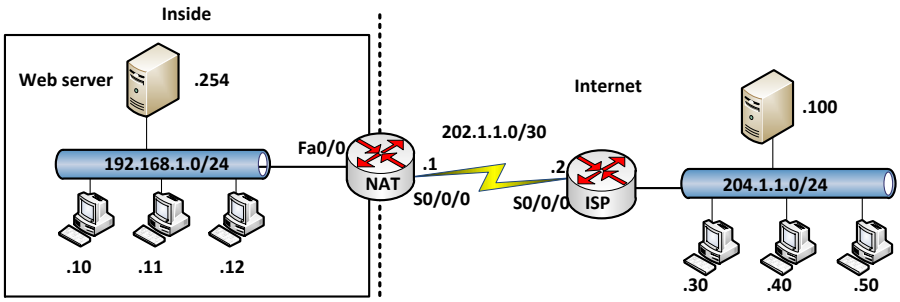
```
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 203.113.147.180 255.255.255.0
 ip nat inside
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 shutdown
!
```

```
interface Vlan1
 no ip address
!
ip nat inside source list 1 interface Serial0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
```

Trên Router đã cấu hình NAT sai ở đâu?

A. ACL cấu hình chưa đúng
B. Cổng S0/0/0 và Fa0/0
C. Cổng Fa0/1
D. Lệnh default route cấu hình sai

6.7. Cho sơ đồ mạng



❖ **Mô tả yêu cầu**

Công ty thuê một IP public để dùng cho local Web serber là 202.2.2.254 và đang kết nối ra Internet qua cổng S0/0/0 của Router. Yêu cầu cấu hình để cho các máy bên ngoài Internet có thể truy cập vào Web server và các máy bên trong có thể ra ngoài Internet net.

❖ **Hướng dẫn cấu hình**

- Các máy tính đặc địa chỉ IP và **default gateway** cho phù hợp
- Giữa router NAT và ISP không cấu hình bất kỳ giao thức định tuyến nào
- Router NAT tạo đường "default route" lên ISP

```
NAT(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
```

- Cấu hình public cho Web server

```
NAT(config)#ip nat inside source static 192.168.1.254
202.1.1.254
```

- Cấu hình cho phép các máy tính bên trong ra ngoài Internet

```
NAT(config)#access-list 1 permit 192.168.1.0 0.0.0.255

NAT(config)#ip nat inside source list 1 interface S0/0/0
overload

NAT(config-if)#int Fa0/0

NAT(config-if)#ip nat inside

NAT(config-if)#int S0/0/0

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

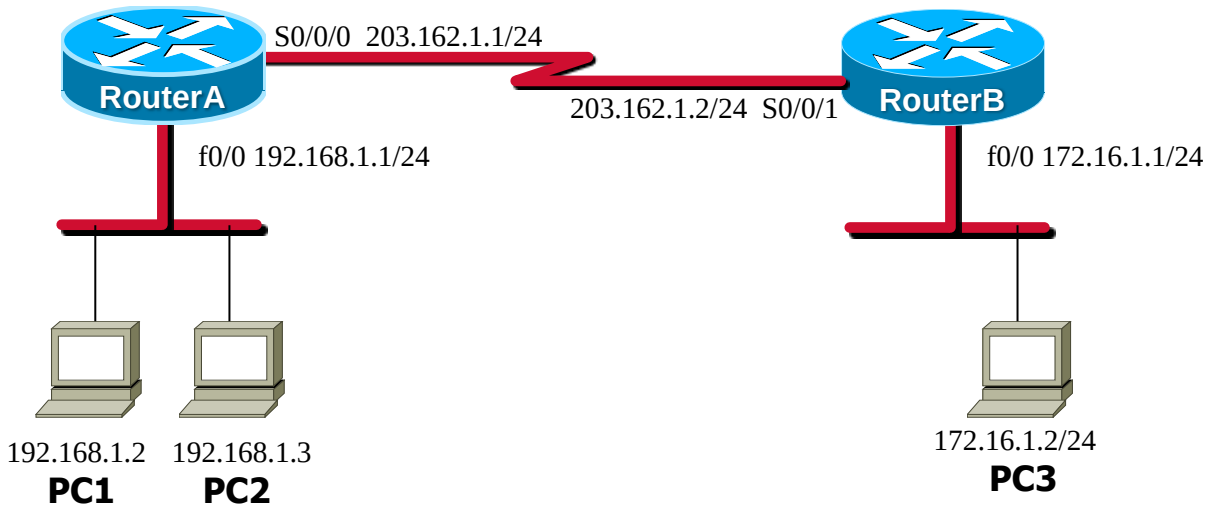
❖ **Kiểm tra cấu hình bằng các lệnh đã học**

✓ Thực hiện ping giữa các máy tính, phân tích các gói truyền nhận bằng lệnh *debug ip packet* trên router trước khi thực hiện lệnh *ping*.

Sử dụng lệnh *debug ip nat* để xem quá trình hoạt động của quá trình NAT

7. Lab NAT

Lab 6-1. STATIC NAT



❖ **Mô tả**

Bài thực hành này mô tả cách cấu hình static NAT đơn giản trên router: đổi địa chỉ 192.168.1.2 (PC1) thành địa chỉ 203.162.1.3 khi gói tin đi từ PC1 ra khỏi cổng S0/0/0 trên RouterA.

❖ **Cấu hình**

- Cấu hình RouterA

```
router(config)#hostname RouterA

RouterA(config)#interface fa0/0
```

```
RouterA(config-if)#ip address 192.168.1.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config)#interface serial 0/0/0
RouterA(config-if)#ip address 203.162.1.1  255.255.255.0
RouterA(config-if)#clock rate 64000
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config)#ip nat inside source static  192.168.1.2   203.162.1.3
RouterA(config)#interface fa0/0
RouterA(config-if)#ip nat inside
RouterA(config-if)#interface Serial 0/0/0
RouterA(config-if)#ip nat outside
```

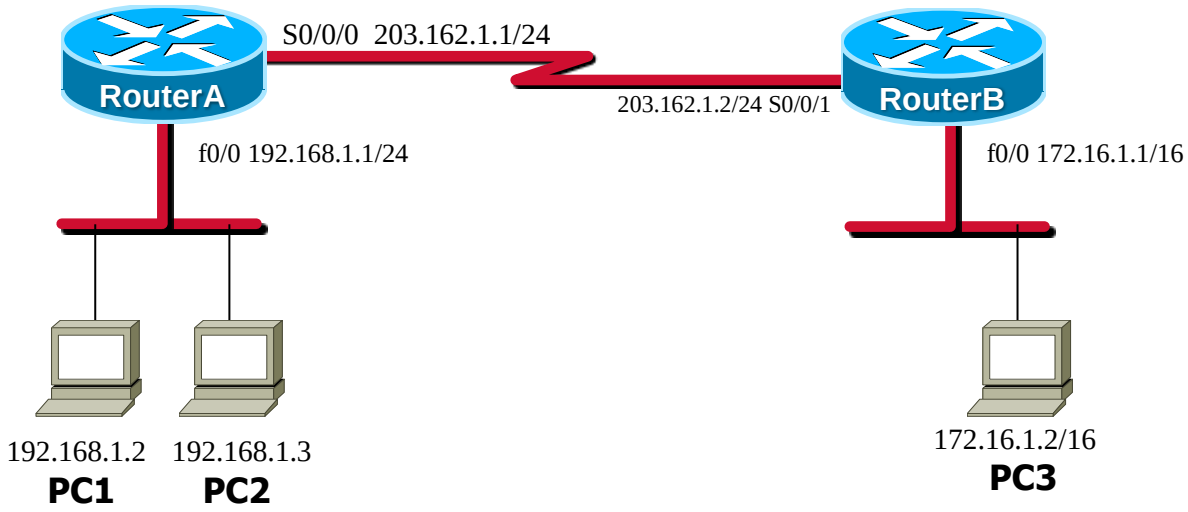
- Cấu hình RouterB

```
router(config)#hostname RouterB
RouterB(config)#interface  fa0/0
RouterB(config-if)#ip address 172.16.1.1 255.255.255.0
RouterB(config-if)#no shutdown

RouterB(config-if)#interface serial 0/0/1
RouterB(config-if)#ip address 203.162.1.2 255.255.255.0
RouterB(config-if)#no shutdown
```

❖ **Kiểm tra**

- ✓ Thực hiện ping từ PC1 đến PC3, phân tích các gói truyền nhận bằng lệnh `debug ip packet` trên router trước khi ping
- ✓ Sử dụng lệnh `debug ip nat` để xem quá trình hoạt động của quá trình NAT

Lab 6-2. DYNAMIC NAT



Bài thực hành này trình bày cách chuyển đổi động các địa chỉ inside thành địa chỉ outside. RouterA sẽ chuyển đổi các địa chỉ nguồn trong mạng 19.168.1.0/24 thành các địa chỉ global được xác định trong vùng (pool) địa chỉ "globalpool: 203.162.1.5 - 203.162.1.8".

RouterA được cấu hình NAT động, chuyển đổi các địa chỉ nguồn inside thành các địa chỉ global; các địa chỉ inside được xác định bởi access-list 1.

❖ Cấu hình

- Cấu hình RouterA

```
router(config)#hostname RouterA
```

```
RouterA(config)#int f0/0
RouterA(config-if)#ip add 192.168.1.1 255.255.255.0
RouterA(config-if)#no shut
RouterA(config-if)#exit
RouterA(config)#int s0/0/0
RouterA(config-if)#ip add 203.162.1.1 255.255.255.0
RouterA(config-if)#no shut
RouterA(config-if)#exit
RouterA(config)#ip nat pool globalpool 203.162.1.5
                                203.162.1.8 netmask 255.255.255.0
RouterA(config)#access-list 1 permit 192.168.1.0 0.0.0.255
RouterA(config)#ip nat inside source list 1 pool globalpool
RouterA(config)#int f0/0
RouterA(config-if)#ip nat inside

RouterA(config-if)#int s0/0/0
RouterA(config-if)#ip nat outside
RouterA(config-if)#end
RouterA#
```

- **Cấu hình RouterB**

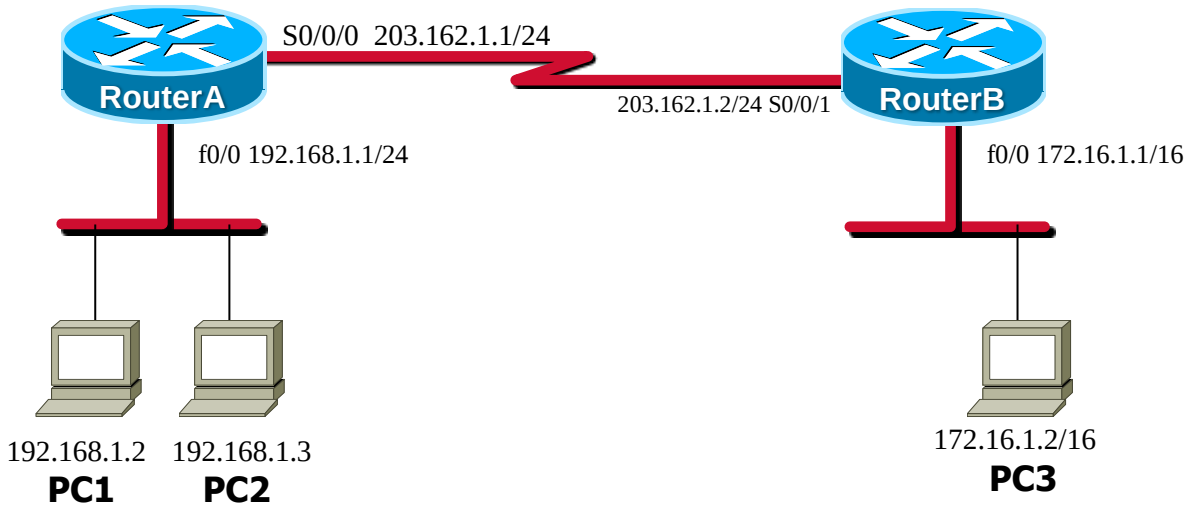
```
router(config)#hostname RouterB
RouterB(config)#interface s0/0/1
RouterB(config-if)#ip address 203.162.1.2 255.255.255.0
RouterB(config-if)#clock rate 64000
RouterB(config-if)#no shutdown
RouterB(config-if)#exit

RouterB(config)#interface fa0/0
RouterB(config-if)#ip address 172.16.1.1 255.255.255.0
RouterB(config-if)#no shutdown
RouterB(config-if)#exit
RouterB(config)#
```

- **Kiểm tra**

✓ Từ RouterA, thực hiện lệnh ping mở rộng đến RouterB (172.16.1.1), với địa chỉ nguồn lần lượt là 192.168.1.2, 192.168.1.3, 192.168.1.4, ...

✓ Kiểm tra NAT đã thực hiện bằng lệnh `Router#debug ip nat` trên RouterA

Lab 6-3. DYNAMIC NAT WITH OVERLOAD



❖ Yêu cầu

NAT overloading là cơ chế cho phép chuyển đổi tất cả các địa chỉ IP thành một địa chỉ global (địa chỉ IP thật). Các địa chỉ trong sẽ được phân biệt dựa trên port number.

RouterA được cấu hình NAT và sẽ tự động chuyển dịch bất kỳ địa chỉ trong nào thuộc mạng 192.168.1.0/24 thành 203.162.1.3

❖ Cấu hình

- **Cấu hình RouterA**

```
Router(config)#hostname RouterA
RouterA(config)#interface  fastEthernet 0/0
```

```
RouterA(config-if)#ip add 192.168.1.1 255.255.255.0
RouterA(config-if)#no shutdown

RouterA(config)#int S0/0/0
RouterA(config-if)#ip add 203.162.1.1 255.255.255.0
RouterA(config-if)#no shutdown

RouterA(config)#access-list 1 permit 192.168.1.0 0.0.0.255
RouterA(config)#ip nat pool globalpool 203.162.1.3 203.162.1.3
                                              netmask 255.255.255.0
RouterA(config)#ip nat inside source list 1 pool globalpool overload
```

- **Cấu hình trên RouterB**

```
Router(config)#hostname RouterB
RouterB(config)#interface  fastEthernet 0/0
RouterB(config-if)#ip address 172.16.1.1 255.255.255.0
RouterB(config-if)#no shutdown

RouterB(config)#interface  serial 0/0/1
RouterB(config-if)#ip address 203.162.1.2
RouterB(config-if)#clock rate 64000
RouterB(config-if)#no shutdown
```

❖ **Kiểm tra**

Từ RouterA, thực hiện lệnh ping mở rộng đến RouterB, source từ 192.168.1.2 và 192.168.1.3. Kiểm tra chuyển dịch bằng lệnh debug ip nat → các địa chỉ này sẽ được chuyển dịch thành 203.162.1.3

Để xem bảng chuyển đổi NAT trên RouterA dùng lệnh show ip nat translation. Lưu ý port number sau mỗi địa chỉ IP, số thứ tự các port này là chìa khóa để chuyển các gói đúng về địa chỉ IP *inside local*.