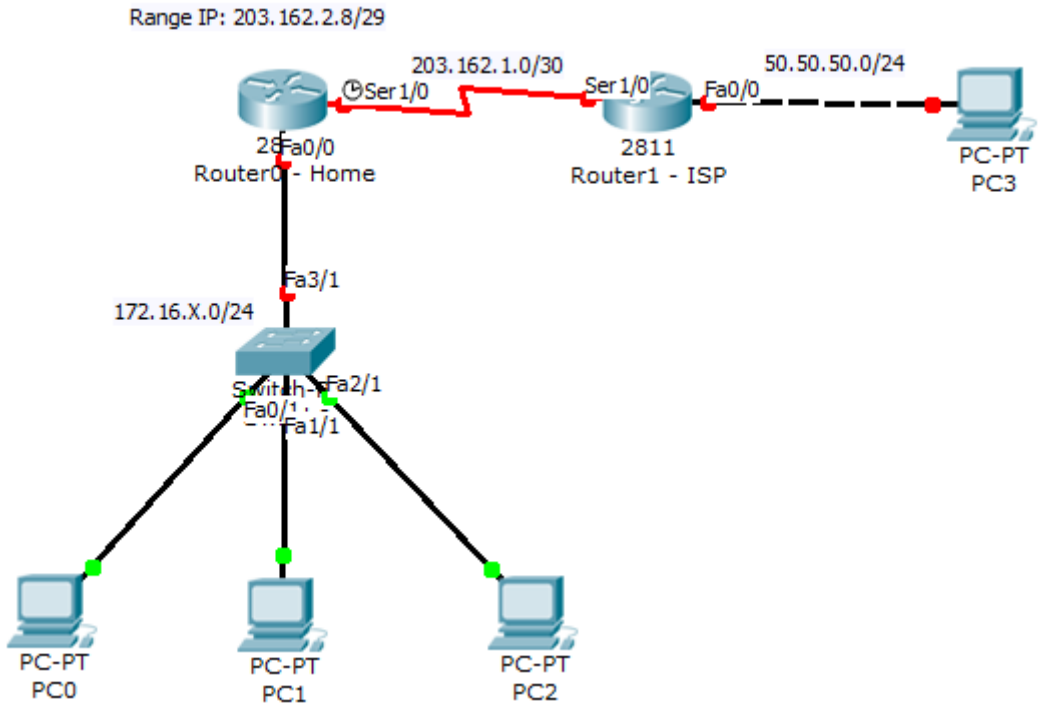
Network Address Translation (NAT)

Các dạng NAT xem xét trong bài:

- Static NAT
- Dynamic NAT
- NAT Port (interface/pool)
- Static NAT + Port

1. Thiết lập hệ thống mạng như hình vẽ



Trong đó:

- R1 tượng trưng cho ISP
- R0 là một doanh nghiệp thuê đường truyền của ISP (mô hình này thường dùng trong kiểu kết nối lease line).
- Doanh nghiệp đã mua 1 gói địa chỉ gồm 6 địa chỉ IP public **203.162.2.8/29**

Cấu hình IP cho các thiết bị:

R0:

```
R0#show ip int br
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        172.16.1.1      YES manual up                    up

FastEthernet0/1        unassigned      YES manual administratively down down

Serial1/0              203.162.1.1     YES manual up                    up

Serial1/1              unassigned      YES manual administratively down down

Serial1/2              unassigned      YES manual administratively down down

Serial1/3              unassigned      YES manual administratively down down

Vlan1                  unassigned      YES manual administratively down down
R0#
```

R1:

```
R1#show ip int br
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        50.50.50.1      YES manual up                    up

FastEthernet0/1        unassigned      YES manual administratively down down

Serial1/0              203.162.1.2     YES manual up                    up

Serial1/1              unassigned      YES manual administratively down down

Serial1/2              unassigned      YES manual administratively down down

Serial1/3              unassigned      YES manual administratively down down

Vlan1                  unassigned      YES manual administratively down down
R1#
```

Routing: Giữa doanh nghiệp này và ISP sẽ không chạy bất kì dynamic routing protocol nào cả. Doanh nghiệp đơn thuần chỉ default route lên ISP và ISP dùng static route xuống hướng doanh nghiệp.

R0:

```
R0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#ip route 0.0.0.0 0.0.0.0 203.162.1.2
R0(config)#
```

R1:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 203.162.2.8 255.255.255.248 s1/0
R1(config)#
```

2. NAT Tĩnh (Static NAT):

Đây là hình thức NAT thủ công, từ 1 địa chỉ trong mạng LAN thành 1 địa chỉ public IP. Cách này thường dùng để NAT các server trong hệ thống mạng như Web server, FTP server, Mail server…

Giả sử ở đây chúng ta có yêu cầu:

NAT tĩnh cho ip máy tính PC1 172.16.1.3 trở thành ip 203.162.2.9 đối với mạng bên ngoài.

Câu lệnh cần dùng:

- **ip nat inside source static**
- **ip nat inside**
- **ip nat outside**

Cụ thể: *Diễn ra hoàn toàn ở Router R0.*

NAT tĩnh 172.16.1.3 thành 203.162.2.9 bằng câu lệnh IP nat inside source static.

Sau đó lên cổng mạng LAN (fa0/0) gõ câu lệnh ip nat inside; cổng mạng WAN s1/0 gõ câu lệnh ip nat outside.

```
R0(config)#ip nat inside source static 172.16.1.3 203.162.2.9
R0(config)#int fa0/0
R0(config-if)#ip nat inside
R0(config-if)#int s1/0
R0(config-if)#ip nat outside
R0(config-if)#
```

Ngay lập tức thao tác NAT được ghi nhận.

Câu lệnh

#show ip nat translation

```
R0#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
---  203.162.2.9       172.16.1.3         ---                ---

R0#
```

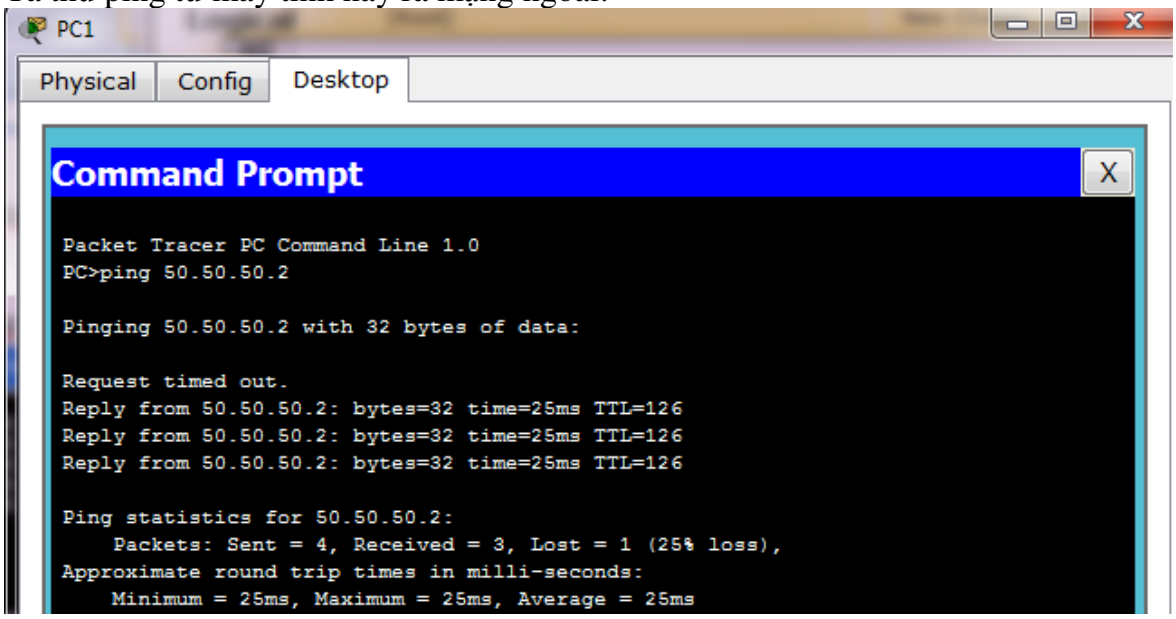
Giải thích ý nghĩa:

- Inside local: Địa chỉ trong mạng LAN trước khi NAT
- Inside global: Địa chỉ trong mạng LAN sau khi đã được NAT, trước khi truyền ra mạng ngoài.
- Global inside: Địa chỉ máy tính bên ngoài trước khi NAT
- Global outside: Địa chỉ máy tính bên ngoài sau khi NAT.

Ở các dạng NAT trong bài này, global inside và global outside luôn như nhau, vì ta chỉ nat inside (mạng LAN).

Theo câu lệnh show bên trên, máy tính 172.16.1.3 trước khi ra ngoài sẽ được đổi thành 203.162.2.9

Ta thử ping từ máy tính này ra mạng ngoài:

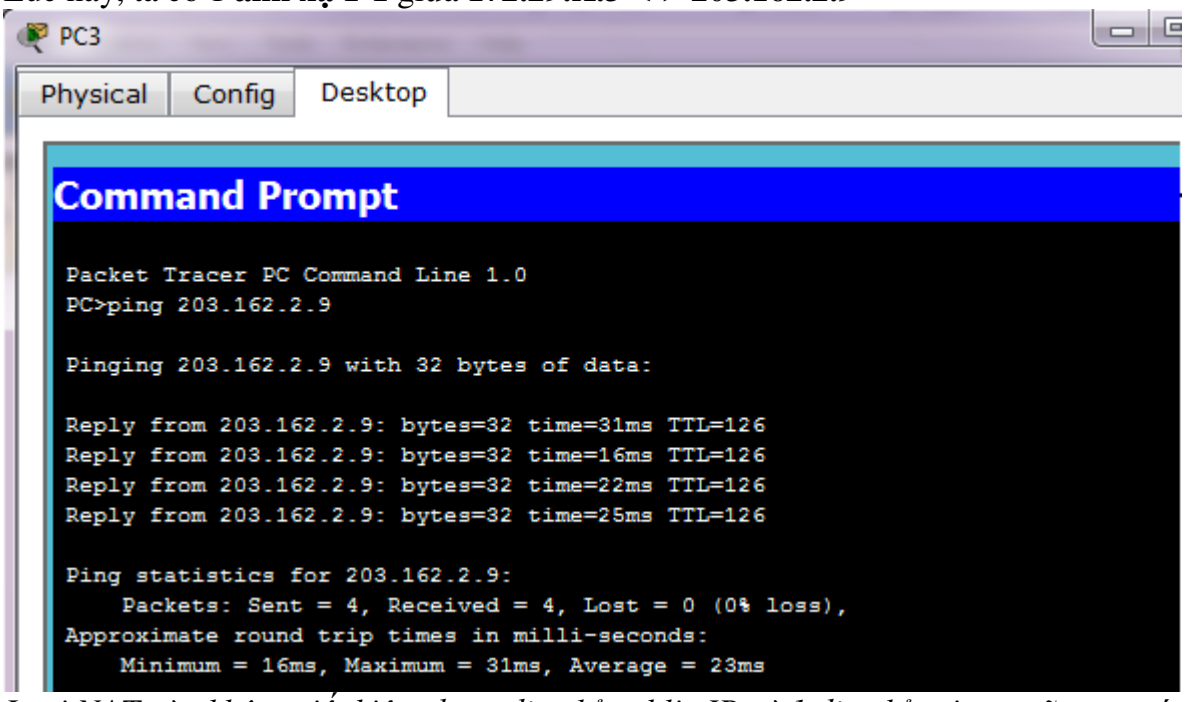


Bật câu lệnh **debug ip nat** và **ping** lại lần nữa, quan sát trên router:

```
R0>
R0>en
R0#debug ip nat
IP NAT debugging is on
R0#
NAT: s=172.16.1.3->203.162.2.9, d=50.50.50.2[0]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.3[0]
NAT: s=172.16.1.3->203.162.2.9, d=50.50.50.2[0]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.3[0]
NAT: s=172.16.1.3->203.162.2.9, d=50.50.50.2[0]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.3[0]
NAT: s=172.16.1.3->203.162.2.9, d=50.50.50.2[0]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.3[0]
R0#
```

Khi gói tin đi ra ngoài (echo request), **source ip = 172.16.X.3** sẽ được chuyển thành **203.162.2.9**
Khi gói tin đi vào (echo reply), **dest ip = 203.162.2.9** sẽ được chuyển trở lại thành **172.16.X.3** và đưa vào mạng LAN.
Lúc này, ISP không hề biết có sự tồn tại của network **172.29.X.0/24**.

Từ PC bên ngoài (**50.50.50.2**) cũng dễ dàng liên lạc vào máy tính trên theo địa chỉ ip **203.162.2.9**
Lúc này, ta có 1 **ánh xạ 1-1** giữa **172.29.X.3 <-> 203.162.2.9**



Loại NAT này không tiết kiệm được địa chỉ public IP, vì 1 địa chỉ private sẽ tương ứng 1 địa chỉ public.

3. NAT động (Dynamic NAT):

NAT tĩnh ta phải tự thiết lập ánh xạ **private <-> public** cho từng cặp.
Ta có thể định nghĩa tất cả ip private và tất cả ip public trên router. Khi 1 gói tin private ip đến router, nó sẽ tự lựa 1 địa chỉ public ip còn rảnh để NAT.
Cấu hình: Câu lệnh ip nat inside và ip nat outside trên fa0/0 và s1/0 vẫn giữ nguyên trong suốt bài học.

- Các địa chỉ mạng LAN cho phép ra ngoài: bằng **access-list**
- Các địa chỉ public IP dùng để NAT: câu lệnh **ip nat pool <địa chỉ đầu> <địa chỉ cuối> netmask <subnet mask>**
- Câu lệnh nat: **ip nat inside source list … pool …**

Ví dụ: *Cho phép các máy trong LAN 172.16.X.0/24 ra ngoài internet, các địa chỉ này sẽ được nat bằng range 203.162.2.10 -> 203.162.2.14 (địa chỉ 203.162.2.9 đã dùng để NAT tĩnh, mặc dù ta vẫn có thể dùng lại địa chỉ này).*

```
R0(config)#access-list 1 permit 172.16.1.0 0.0.0.255
R0(config)#ip nat pool ADSL 203.162.2.10 203.162.2.14 netmask 255.255.255.248
R0(config)#ip nat inside source list 1 pool ADSL
R0(config)#
R0(config)#
```

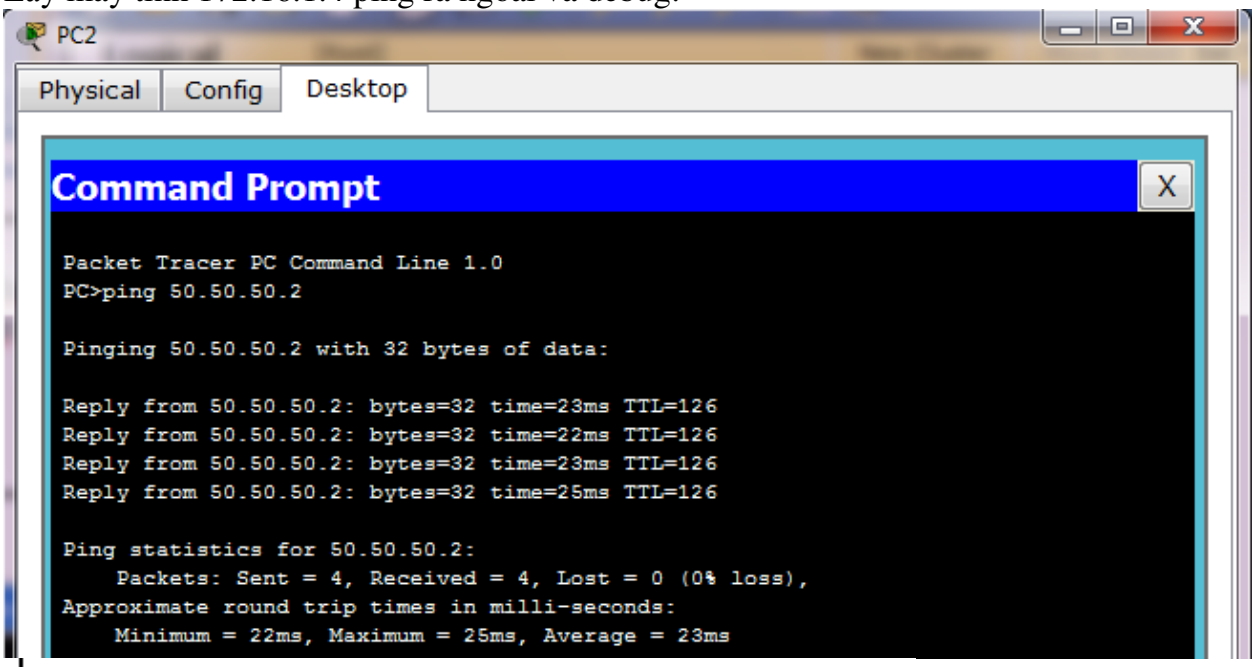
Đặc điểm của dynamic nat:

Khi chưa có gói tin đi ra, quá trình NAT chưa thực thi. Do đó bảng NAT chưa tồn tại các record mới này, chỉ tồn tại record static nat ở bước trước.

```
R0#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
---  203.162.2.9       172.16.1.3         ---                ---

R0#
```

Lấy máy tính 172.16.1.4 ping ra ngoài và debug:



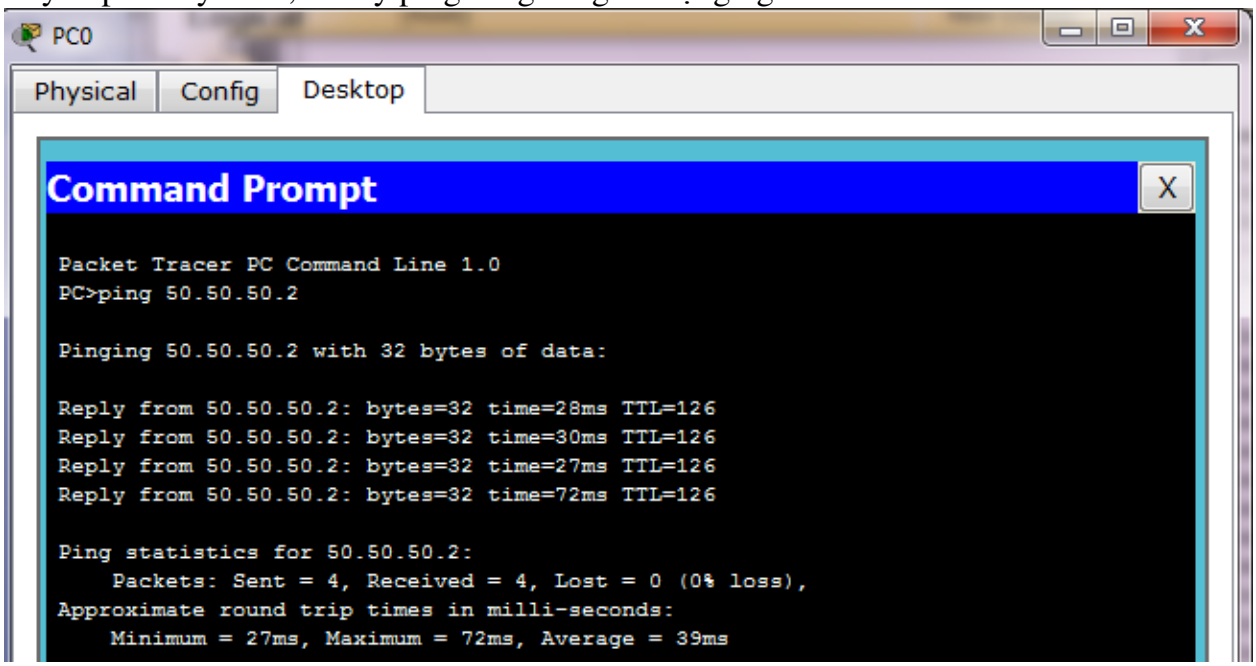

```
R0#debug ip nat
IP NAT debugging is on
R0#
NAT: s=172.16.1.4->203.162.2.10, d=50.50.50.2[1]
NAT*: s=50.50.50.2, d=203.162.2.10->172.16.1.4[1]
NAT: s=172.16.1.4->203.162.2.10, d=50.50.50.2[1]
NAT*: s=50.50.50.2, d=203.162.2.10->172.16.1.4[1]
NAT: s=172.16.1.4->203.162.2.10, d=50.50.50.2[1]
NAT*: s=50.50.50.2, d=203.162.2.10->172.16.1.4[1]
NAT: s=172.16.1.4->203.162.2.10, d=50.50.50.2[1]
NAT*: s=50.50.50.2, d=203.162.2.10->172.16.1.4[1]
```

Xem lại bảng NAT: Đã tồn tại record này.

```
R0#
R0#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  203.162.2.9       172.16.1.3         ---                ---
---  203.162.2.10      172.16.1.4         ---                ---

R0#
```

Lấy tiếp 1 máy khác, 2 máy ping song song ra mạng ngoài:



Bảng NAT: Router tự động lấy thêm địa chỉ 203.162.2.11 cho máy 172.16.1.5

```
R0#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  203.162.2.11      172.16.1.2         ---                ---
---  203.162.2.9       172.16.1.3         ---                ---
---  203.162.2.10      172.16.1.4         ---                ---

R0#
```

Có thể xem các thống kê về NAT:

```
R0#show ip nat sta
R0#show ip nat statistics
Total translations: 3 (1 static, 2 dynamic, 0 extended)
Outside Interfaces: Serial1/0
Inside Interfaces: FastEthernet0/0
Hits: 61  Misses: 2
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool ADSL refCount 2
 pool ADSL: netmask 255.255.255.248
       start 203.162.2.10 end 203.162.2.14
       type generic, total addresses 5 , allocated 2 (40%), misses 0
R0#
```

NAT động thường không thể dùng để nat các server vì:

- *Chỉ khi nào có gói tin bên trong đi ra mới xuất hiện giao tác, và chỉ duy trì 1 khoảng thời gian ngắn.*
- *Do tính chất động, ta không biết private ip address sẽ được nat thành public ip address nào. Điều này hoàn toàn do router quyết định.*

Ngoài ra, dạng NAT này cũng chưa tiết kiệm địa chỉ ip, **1 private <-> 1 public**. Khi pool có 5 địa chỉ public, chỉ có 5 máy tính trong mạng LAN có thể ra internet cùng lúc.

4. NAT overload trên interface:

Đây là dạng NAT dùng nhiều nhất ở mô hình ADSL. **Overload** ở đây có nghĩa là khái niệm NAT ***kèm theo port***.

Ví dụ:

Giả sử router dùng ip 203.162.2.10 để NAT
*Ứng dụng trên máy 172.16.1.4, sử dụng port **10000** (từ giờ về sau sẽ viết là 172.16.1.4:10000) khi đến Router sẽ được NAT thành 203.162.2.10:**10000** và ra internet.*
*Cùng lúc đó, gói tin 172.16.1.5:**10001** đến router sẽ được NAT thành 203.162.2.10:**10001** để ra internet.*

Khi có gói tin từ internet trả về router, router sẽ xem xét Destination port: nếu là 203.162.2.10:10000 sẽ chuyển thành 172.16.1.4:10000 và trả về mạng LAN; nếu là 203.162.2.10:10001 sẽ chuyển thành 172.16.1.5:10001 và trả về mạng LAN.

Với cách thức này, dù chỉ dùng 1 địa chỉ public IP router có thể NAT được cùng lúc cho nhiều máy khác nhau.
Port trong hệ thống mạng là số 2 byte : 0 -> 65535

Trong trường hợp sử dụng IP động (ADSL), ta không biết trước IP của cổng mạng WAN. Ta sẽ dùng từ khóa interface. Tùy vào lúc chạy, ip của cổng WAN cụ thể là bao nhiêu sẽ được dùng để NAT.

Cấu hình:

Trước hết ta tắt tính năng NAT dynamic ở bước trước
(config)# no ip nat inside source list 1 pool ADSL
Sau đó cấu hình câu lệnh nat overload:
Chú ý từ interface và overload.

```
R0(config)#no ip nat inside source list 1 pool ADSL
R0(config)#ip nat inside source list 1 int s1/0 overload
ipnat_add_dynamic_cfg: id 6, flag 5, range 0
id 6, flags 0, domain 0, lookup 0, aclnum 1 ,
        aclname 1 , mapname idb 000040B2
R0(config)#
R0(config)#
```

Ping từ máy 172.16.1.4 và kiểm tra:
debug:

```
R0#debug ip nat
IP NAT debugging is on
R0#
NAT: s=172.16.1.4->203.162.1.1, d=50.50.50.2[7]
NAT*: s=50.50.50.2, d=203.162.1.1->172.16.1.4[7]
NAT: s=172.16.1.4->203.162.1.1, d=50.50.50.2[8]
NAT*: s=50.50.50.2, d=203.162.1.1->172.16.1.4[8]
NAT: s=172.16.1.4->203.162.1.1, d=50.50.50.2[9]
NAT*: s=50.50.50.2, d=203.162.1.1->172.16.1.4[9]
NAT: s=172.16.1.4->203.162.1.1, d=50.50.50.2[10]
NAT*: s=50.50.50.2, d=203.162.1.1->172.16.1.4[10]
```

Bảng nat: Có thêm **port** cụ thể.

```
R0#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 203.162.1.1:21    172.16.1.4:21      50.50.50.2:21      50.50.50.2:21
icmp 203.162.1.1:22    172.16.1.4:22      50.50.50.2:22      50.50.50.2:22
icmp 203.162.1.1:23    172.16.1.4:23      50.50.50.2:23      50.50.50.2:23
icmp 203.162.1.1:24    172.16.1.4:24      50.50.50.2:24      50.50.50.2:24
---  203.162.2.9       172.16.1.3         ---                ---

R0#
```

5. NAT Overload Pool:

Trong các tổ chức lớn, 1 địa chỉ dùng để NAT overload đôi khi không đủ phục vụ. Do đó chúng ta sẽ NAT overload trên một POOL.
Ở đây chúng ta sẽ sử dụng lại POOL ADSL đã định nghĩa ở **phần 2**.

Trước hết bỏ câu lệnh NAT interface ở bước làm trước.
Sau đó áp câu lệnh nat pool và kèm theo từ khóa Overload.

```
R0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#no ip nat inside source list 1 int s1/0 overload
R0(config)#ip nat inside source list 1 pool ADSL overload
ipnat_add_dynamic_cfg: id 7, flag 5, range 0
poolstart 203.162.2.10 poolend 203.162.2.14
id 7, flags 0, domain 0, lookup 0, aclnum 1 ,
        aclname 1 , mapname idb 0
R0(config)#
```

Ping từ nhiều máy ra ngoài:

```
R0#debug ip nat
IP NAT debugging is on
R0#
NAT: s=172.16.1.2->203.162.2.10, d=50.50.50.2[15]
NAT*: s=50.50.50.2, d=203.162.2.10->172.16.1.2[15]
NAT: s=172.16.1.3->203.162.2.9, d=50.50.50.2[15]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.3[15]
NAT: s=172.16.1.4->203.162.2.10, d=50.50.50.2[16]
NAT*: s=50.50.50.2, d=203.162.2.10->172.16.1.4[16]
NAT: s=172.16.1.2->203.162.2.10, d=50.50.50.2[17]
NAT*: s=50.50.50.2, d=203.162.2.10->172.16.1.2[17]
NAT: s=172.16.1.4->203.162.2.10, d=50.50.50.2[18]
NAT*: s=50.50.50.2, d=203.162.2.10->172.16.1.4[18]
NAT: s=172.16.1.2->203.162.2.10, d=50.50.50.2[19]
NAT*: s=50.50.50.2, d=203.162.2.10->172.16.1.2[19]
NAT: s=172.16.1.4->203.162.2.10, d=50.50.50.2[20]
NAT*: s=50.50.50.2, d=203.162.2.10->172.16.1.4[20]
NAT: s=172.16.1.2->203.162.2.10, d=50.50.50.2[21]
NAT*: s=50.50.50.2, d=203.162.2.10->172.16.1.2[21]
NAT: s=172.16.1.4->203.162.2.10, d=50.50.50.2[22]
NAT*: s=50.50.50.2, d=203.162.2.10->172.16.1.4[22]
NAT: s=172.16.1.3->203.162.2.9, d=50.50.50.2[22]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.3[22]
NAT: s=172.16.1.3->203.162.2.9, d=50.50.50.2[22]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.3[22]
NAT: s=172.16.1.3->203.162.2.9, d=50.50.50.2[22]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.3[22]
```

Bảng NAT:

```
R0#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 203.162.2.10:5    172.16.1.2:5       50.50.50.2:5       50.50.50.2:5
icmp 203.162.2.10:6    172.16.1.2:6       50.50.50.2:6       50.50.50.2:6
icmp 203.162.2.10:7    172.16.1.2:7       50.50.50.2:7       50.50.50.2:7
icmp 203.162.2.10:8    172.16.1.2:8       50.50.50.2:8       50.50.50.2:8
icmp 203.162.2.10:25   172.16.1.4:25      50.50.50.2:25      50.50.50.2:25
icmp 203.162.2.10:26   172.16.1.4:26      50.50.50.2:26      50.50.50.2:26
icmp 203.162.2.10:27   172.16.1.4:27      50.50.50.2:27      50.50.50.2:27
icmp 203.162.2.10:28   172.16.1.4:28      50.50.50.2:28      50.50.50.2:28
---  203.162.2.9       172.16.1.3         ---                ---

R0#
```

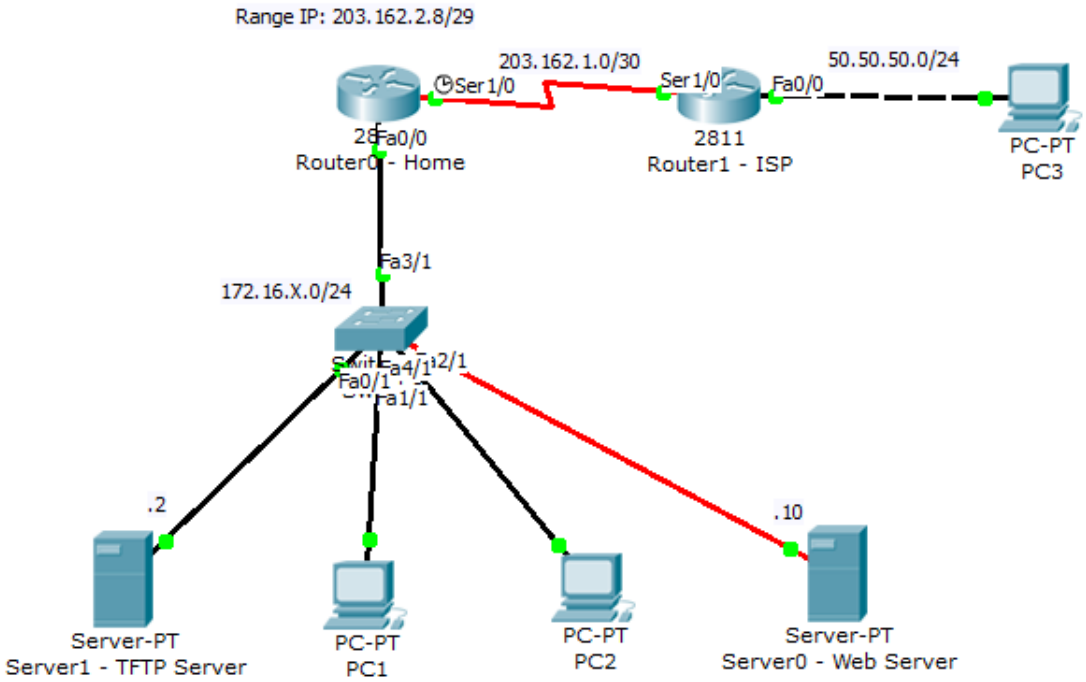
6. Static NAT + Port:

Như chúng ta đã nói, static NAT là loại NAT duy nhất phù hợp cho việc NAT các server như web, ftp, mail…

Tuy nhiên, nếu chúng ta có 10 servers, với hình thức static nat truyền thống sẽ cần đến 10 public ip addresses -> Quá lãng phí.

Ta có thể kết hợp NAT tĩnh nhưng chỉ theo 1 port cụ thể. Do đó, cùng 1 địa chỉ public IP có thể NAT cho nhiều servers, dựa theo số port khác nhau.

Thay đổi mô hình thành như sau:



Ví dụ: *dịch vụ http (tcp: 80) nằm trên máy tính 172.16.1.10; tftp (udp: 69) nằm ở máy tính 172.16.1.2.*

Ta có thể NAT 2 servers này thành cùng địa chỉ IP 203.162.2.9

Cấu hình:

Trước hết bỏ câu lệnh static nat đã cấu hình ở **mục 1**.

Sau đó gõ câu lệnh static nat kết hợp port.

```
R0(config)#
R0(config)#no ip nat inside source static 172.16.1.3 203.162.2.9

ipnat_remove_static_cfg: id 20, flag AR0(config)#
R0(config)#ip nat inside source static tcp 172.16.1.10 80 203.162.2.9 80
R0(config)#ip nat inside source static udp 172.16.1.2 69 203.162.2.9 69
R0(config)#
R0(config)#
```

Bảng NAT:

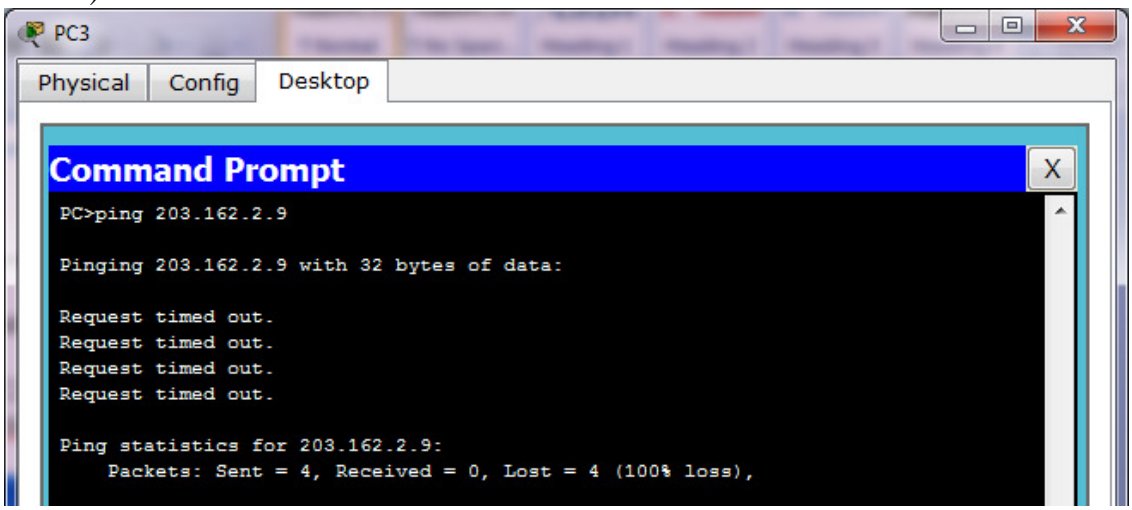
```
R0#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
udp 203.162.2.9:69     172.16.1.2:69      ---                ---
tcp 203.162.2.9:80     172.16.1.10:80     ---                ---

R0#
```

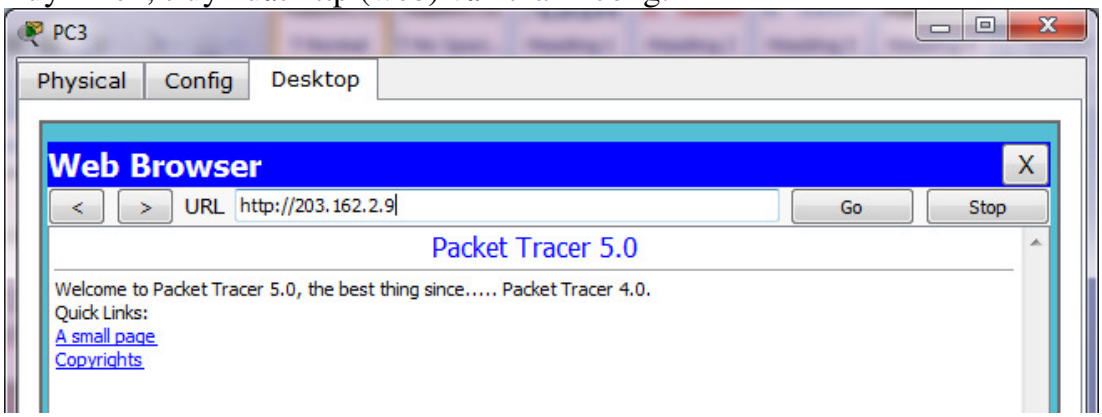
Kiểm tra:

Truy xuất thử web server trên máy 172.16.1.10.

Do ta chỉ NAT udp 172.16.1.2:69 thành 203.162.2.9:69 và tcp 172.16.1.10:80 thành 203.162.2.9:80 nên từ PC3 ping địa chỉ 203.162.2.9 không được (ta không nat giao thức ICMP).



Tuy nhiên, truy xuất http (web) vẫn thành công:



Debug trên R0:

```
R0#debug ip nat
IP NAT debugging is on
R0#
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.10[0]
NAT: s=172.16.1.10->203.162.2.9, d=50.50.50.2[0]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.10[0]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.10[0]
NAT: s=172.16.1.10->203.162.2.9, d=50.50.50.2[0]
NAT: s=172.16.1.10->203.162.2.9, d=50.50.50.2[0]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.10[0]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.10[0]
NAT: s=172.16.1.10->203.162.2.9, d=50.50.50.2[0]
NAT: s=172.16.1.10->203.162.2.9, d=50.50.50.2[0]
NAT*: s=50.50.50.2, d=203.162.2.9->172.16.1.10[0]
R0#
R0#
```

Khi có các server khác, ta có thể dùng cùng ip 203.162.2.9 này để NAT.
Khuyết yếu: *Không thể kiểm tra sự "liên thông" với server bằng câu lệnh ping.*
Ưu điểm: *Tiết kiệm địa chỉ IP tối đa.*