



CANTHO UNIVERSITY

THIẾT KẾ CÀI ĐẶT MẠNG MÁY TÍNH

GV: Phạm Hữu Tài - 001128

Mã số học phần: CT335



Chương 6:

Dịch địa chỉ mạng IPv4 (Network Address Translation-NAT)



ĐỊA CHỈ RIÊNG IPv4

(IPv4 Private Address)

- Địa chỉ riêng IPv4 được sử dụng cho các nhánh mạng, máy tính trong mạng của công ty, tổ chức mà không cần phải đăng ký hay trả chi phí

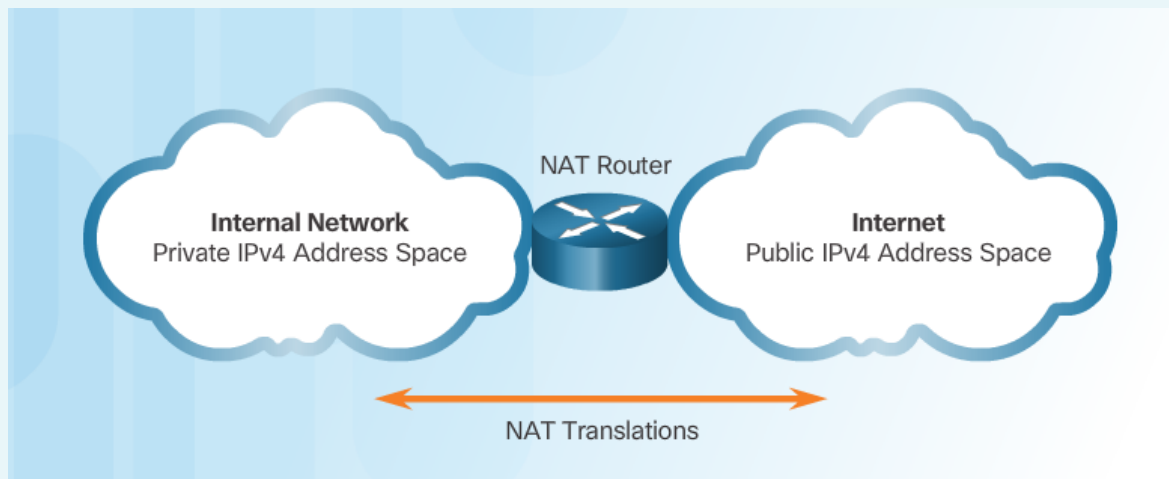
Private Internet Addresses are Defined in RFC 1918

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16



ĐỊA CHỈ RIÊNG IPv4 (IPv4 Private Address)

- Các ISP không định tuyến các địa chỉ riêng nên các máy tính dùng địa chỉ này không thể truy cập đến được các dịch vụ mạng Internet.
- NAT được sử dụng để dịch các địa chỉ IP riêng thành các địa chỉ IP công cộng (IP public) có thể được định tuyến qua Internet.
- Một địa chỉ IPv4 công cộng có thể được sử dụng cho hàng nghìn thiết bị mang địa chỉ IP riêng.





CANTHO UNIVERSITY

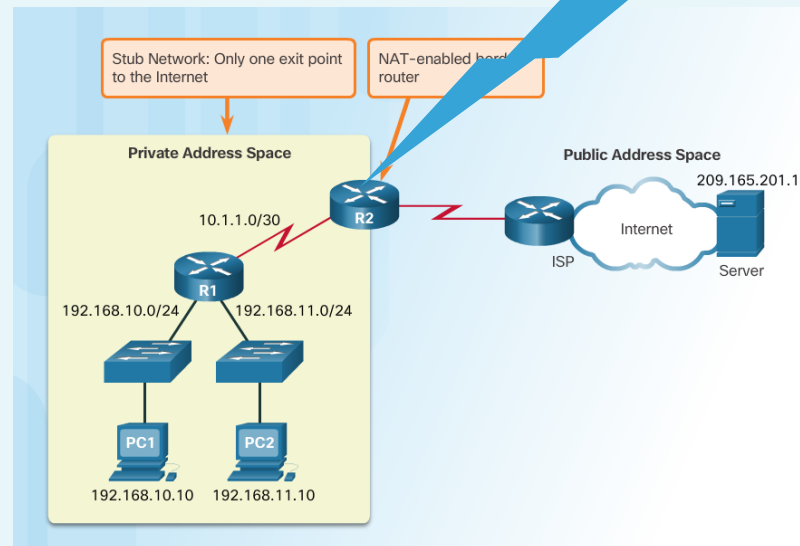
GIỚI THIỆU VỀ NAT

- Địa chỉ IP riêng không được ISP định tuyến qua Internet.
- NAT được sử dụng để dịch các địa chỉ IP riêng (được sử dụng trong mạng LAN) thành các địa chỉ công cộng có thể được định tuyến qua Internet.
- NAT ẩn địa chỉ IPv4 mạng LAN khỏi các mạng bên ngoài.

Các công ty sử dụng cùng một địa chỉ IPv4 riêng nên các thiết bị bên ngoài không thể phân biệt mạng 10.x.x.x của một công ty với mạng 10.x.x.x của công ty khác.

- Hầu hết các router đều hỗ trợ NAT, qua đó có thể được định cấu hình bằng địa chỉ IPv4 công cộng.
- Router có thể được định cấu hình với nhiều địa chỉ IPv4 công cộng để được sử dụng trong một thiết bị hoặc một các thiết bị trong mạng LAN đang được định cấu hình bằng địa chỉ riêng.

NAT thường được cấu hình trên Router biên





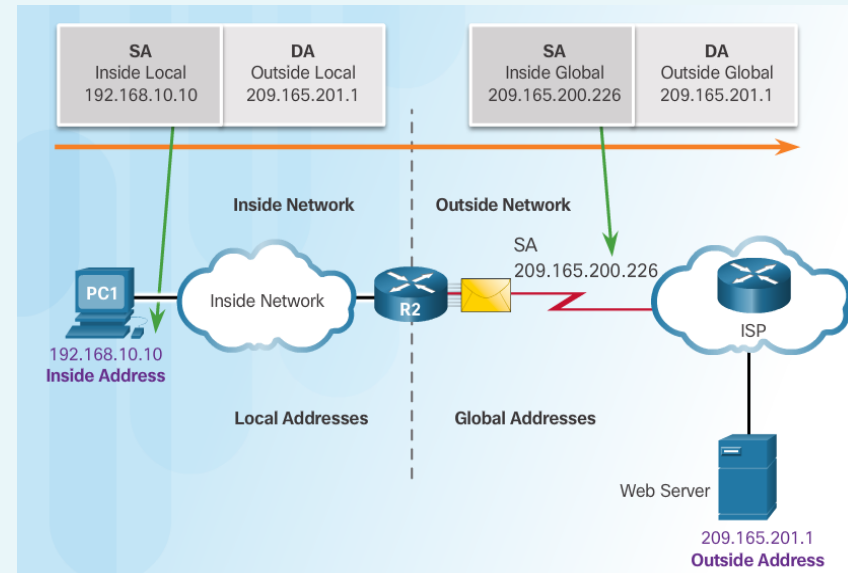
CANTHO UNIVERSITY

THUẬT NGỮ DÙNG BỞI NAT

Có 4 thuật ngữ liên quan đến địa chỉ dùng bởi NAT: *inside*, *outside*, *local* and *global*

Quan sát hình bên phải, R2 là Router biên:

- *Inside address* – địa chỉ được dùng trong LAN, là địa chỉ riêng đặt cho các thiết bị, địa chỉ này sẽ được dịch bởi NAT
- *Outside address* – địa chỉ IP đích của thiết bị trên mạng Internet, thường là địa chỉ Public



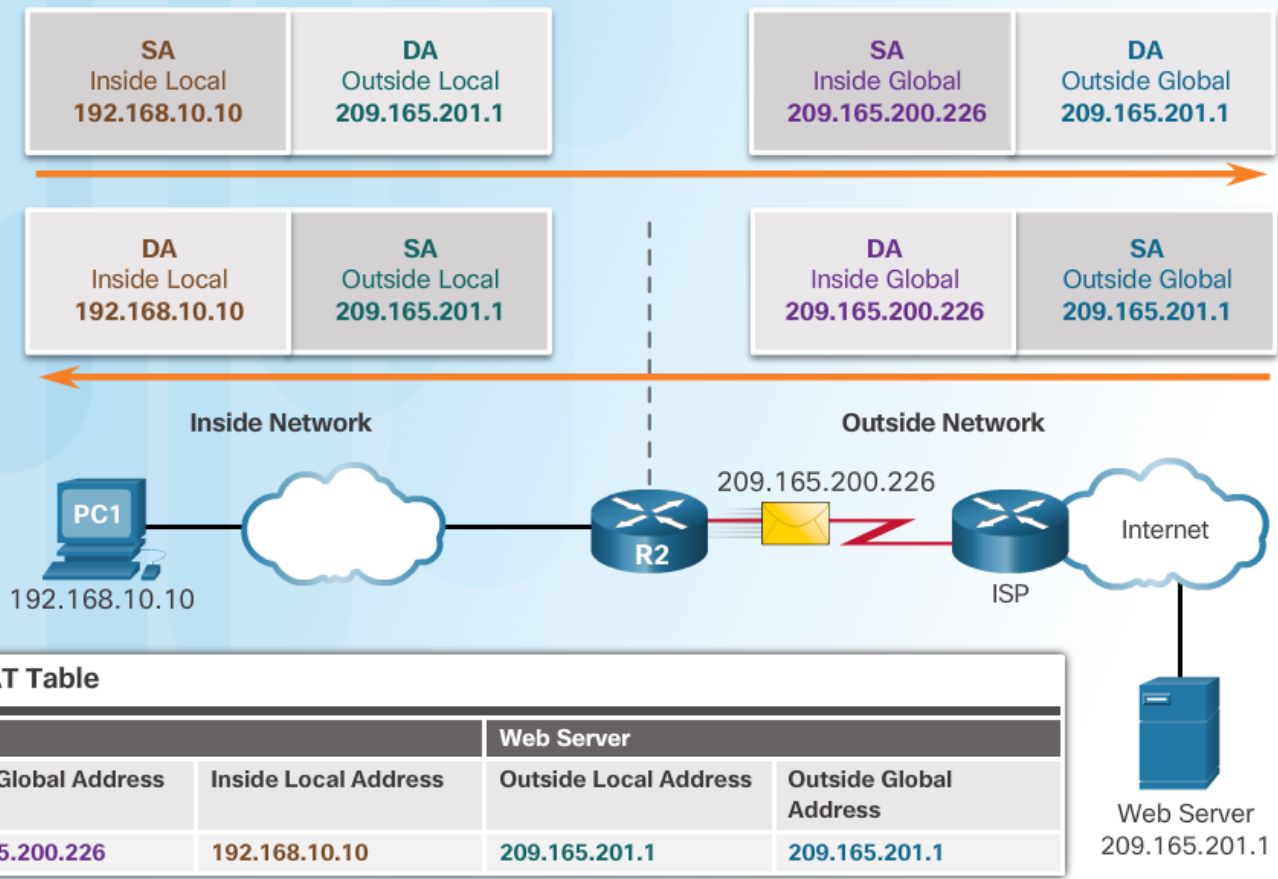
- ✓ *Inside local address* – là địa chỉ private, đặt cho các máy trong LAN
- ✓ *Inside global address* – là địa chỉ địa chỉ public, nằm ở mạng bên ngoài Internet. Đây là địa chỉ đại diện cho các địa chỉ trong LAN ra ngoài Internet
- ✓ *Outside global address* – là địa chỉ đích nằm trên Internet
- ✓ *Outside local address* – là địa chỉ thực đặt của máy đích nằm trên Internet



THUẬT NGỮ DÙNG BỞI NAT

Ví dụ

NAT Address Examples

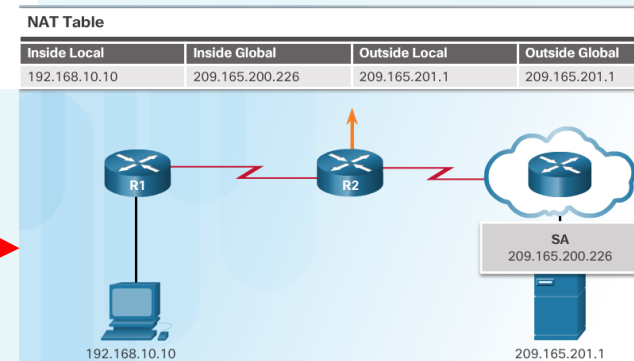
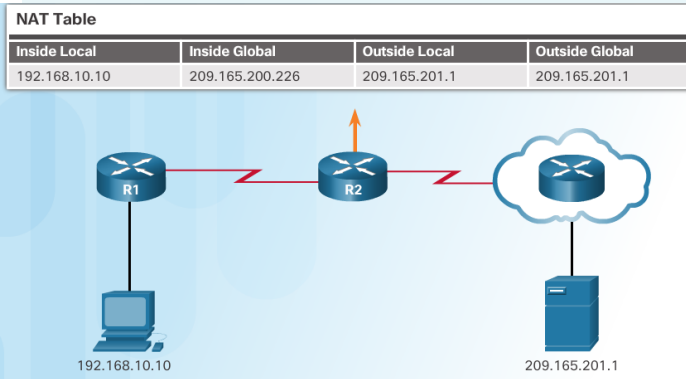
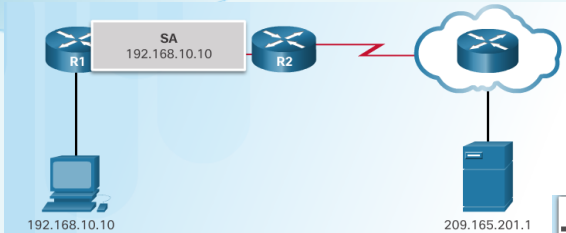




CANTHO UNIVERSITY

HOẠT ĐỘNG CỦA NAT

1. Địa chỉ riêng của thiết bị trong LAN được dịch sang địa chỉ IP công cộng để được ISP định tuyến đến Server bên ngoài mạng.



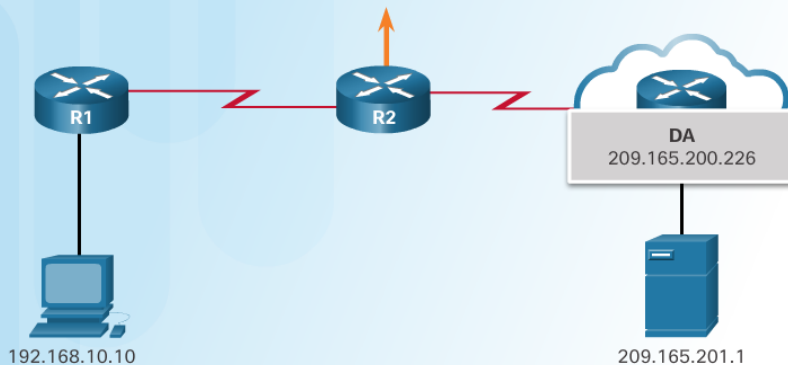


CANTHO UNIVERSITY

HOẠT ĐỘNG CỦA NAT

NAT Table

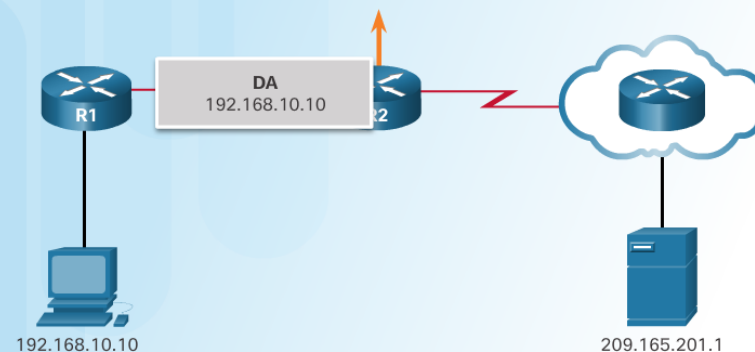
Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



2. Server mạng bên ngoài trả lời yêu cầu với địa chỉ máy nhận là địa chỉ công cộng.

NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



3. Router biên xem trong bảng dịch để biết máy nào đã yêu cầu dữ liệu và dịch lại địa chỉ từ công cộng sang địa chỉ riêng của thiết bị và chuyển gói tin đến thiết bị đó

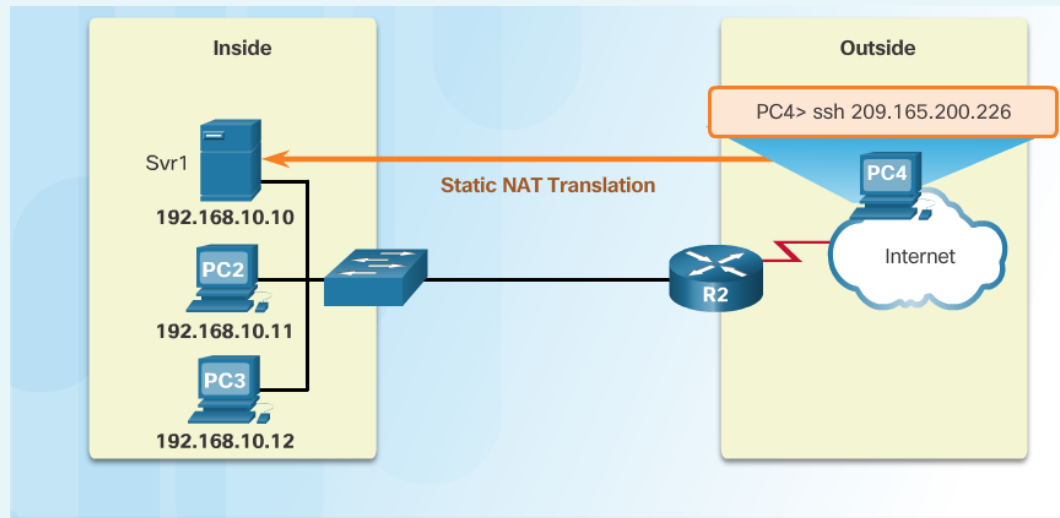


CANTHO UNIVERSITY

Các kiểu NAT

NAT tĩnh (Static NAT)

- NAT tĩnh là ánh xạ một địa chỉ IP riêng sang địa chỉ công cộng để có thể 'thấy' được bởi các máy từ mạng Internet
- NAT tĩnh thường được sử dụng cho các máy chủ có các truy cập từ bên ngoài hoặc cho các thiết bị cần được quản trị từ bên ngoài



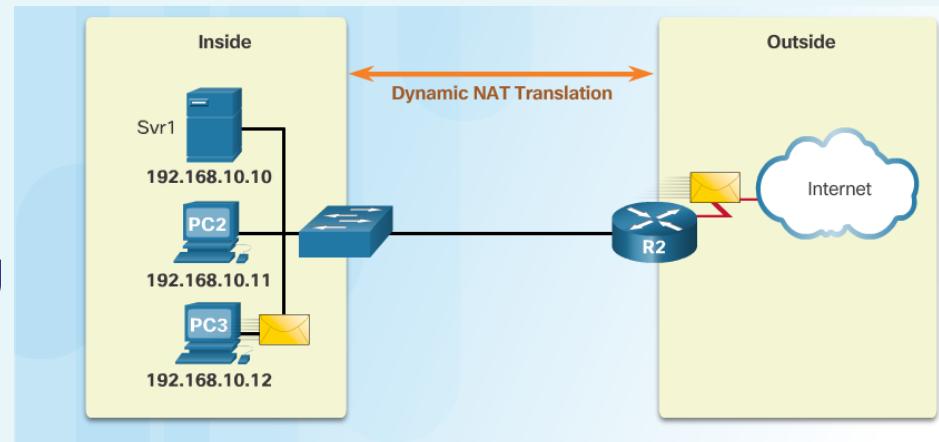
Static NAT Table

Inside Local Address	Inside Global Address - Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



NAT động (Dynamic NAT)

- NAT động gán một hay một dãy địa chỉ IP công cộng (được khai báo trước) cho mỗi gói tin xuất phát từ một thiết bị có địa chỉ là IP riêng (trong LAN) khi gói tin gửi đến một máy trên mạng công cộng (Internet).
 - Địa chỉ được gán trên nguyên tắc FIFO (First In First Out)
 - Số lượng thiết bị mạng LAN được dịch để gói tin truyền ra mạng ngoài bị giới hạn tùy theo số lượng địa chỉ được khai báo trong nhóm địa chỉ công cộng trước đó



IPv4 NAT Pool

Inside Local Address	Inside Global Address Pool - Addresses reachable via R2
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230



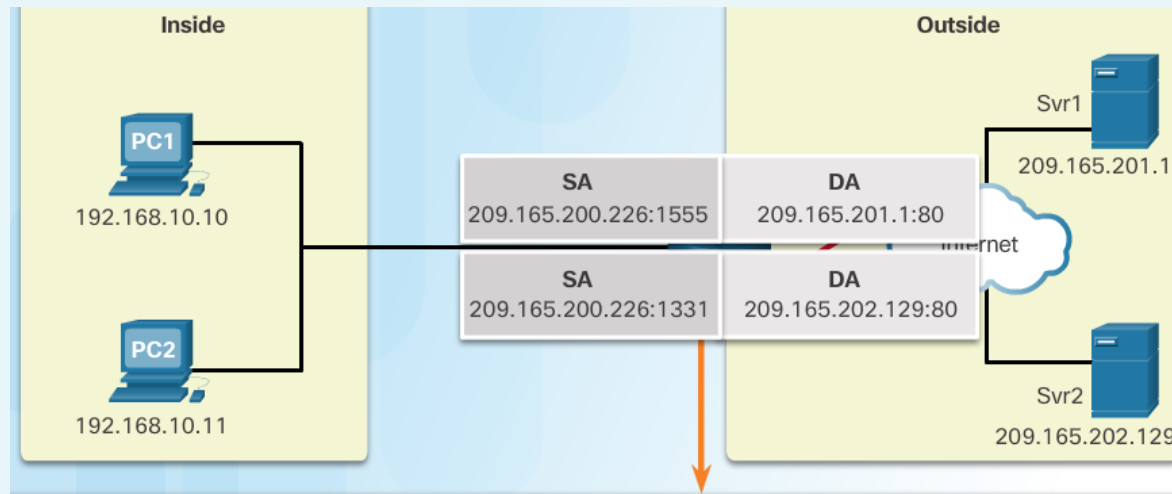
CANTHO UNIVERSITY

Các kiểu NAT

Dịch cổng²

(Port Address Translation-PAT)

- PAT (cách gọi khác là *NAT overload*) có thể dùng 01 địa chỉ IPv4 để cho phép số lượng lớn các máy bên trong mạng liên lạc với các máy bên ngoài mạng.
- PAT dùng số hiệu cổng dịch vụ để theo vết các giao dịch (dịch cổng)



NAT Table with Overload

Inside Global IP Address	Inside Local IP Address	Outside Local IP Address	Outside Global IP Address
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.11:1331	209.165.202.129:80	209.165.202.129:80



CANTHO UNIVERSITY

Các kiểu NAT

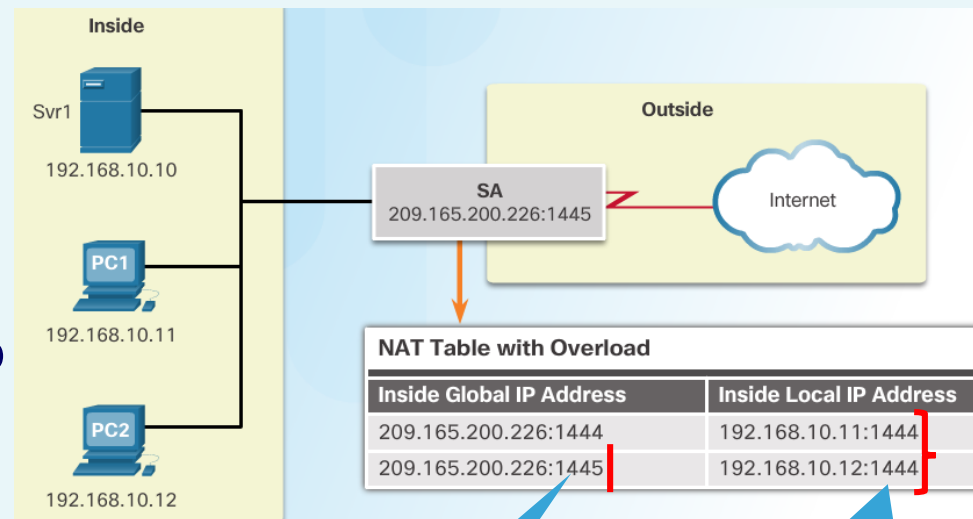
PAT - Cổng khả dụng kế tiếp

Trong quá trình dịch, PAT cố gắng bảo toàn số hiệu của cổng nguồn ban đầu:

– Nếu số hiệu của một cổng đã được sử dụng trước đó, PAT sẽ dịch số hiệu cổng sang cổng khả dụng kế tiếp đầu tiên cho nhóm cổng thích hợp:

- ✓ 0 – 511
- ✓ 512 – 1023
- ✓ 1024 - 65,535

– Khi không còn số hiệu cổng nào có thể dịch được nữa, PAT sẽ chuyển đến địa chỉ IP công cộng tiếp theo trong nhóm (nếu có khai báo nhóm địa chỉ công cộng).



2. PAT sẽ dịch sang cùng 01 địa chỉ công cộng nhưng cổng nguồn sẽ dịch sang cổng khả dụng đầu tiên

1. Khi bản dịch phát hiện nhiều hơn một bản dịch có số hiệu cổng nguồn trùng nhau



CANTHO UNIVERSITY

Các kiểu NAT

So sánh NAT tĩnh và PAT

NAT

Inside Global Address Pool	Inside Local Address
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

PAT

Inside Global Address	Inside Local Address
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

- NAT tĩnh dịch địa chỉ 1:1
- PAT sử dụng một địa chỉ công cộng với nhiều số hiệu cổng của để có thể được dịch được cho nhiều thiết bị trong LAN đang dùng địa chỉ riêng khác nhau



Lợi ích của NAT

- Bảo tồn các địa chỉ công cộng hợp pháp
- Mọi công ty đều có thể sử dụng địa chỉ IP riêng để tăng tính linh hoạt khi kết nối với mạng công cộng (Internet)
- Với nhiều nhóm địa chỉ được NAT, nhóm địa chỉ dự phòng và cân bằng tải trên các nhóm NAT
- Cung cấp tính nhất quán cho sơ đồ địa chỉ mạng nội bộ đang ổn định
- Không cần thiết đặt lại địa chỉ cho các thiết mạng nếu thay đổi ISP hoặc địa chỉ IP công cộng
- Cung cấp cơ chế bảo mật mạng, ẩn địa chỉ IPv4 riêng của người dùng mạng LAN khỏi người dùng mạng bên ngoài



Bất lợi của NAT

- Hiệu suất bị giảm sút
 - Router biên cấu hình NAT phải theo dõi và xử lý từng phiên kết nối ra các máy hay thiết bị bên ngoài mạng.
- Chức năng của các giao dịch end-to-end bị ảnh hưởng
 - Việc dịch địa chỉ IPv4 trong header của gói tin làm *tăng* thời gian xử lý gói tin.
 - Khả năng truy xuất nguồn gốc IP đầu-cuối bị mất
- Một số ứng dụng yêu cầu địa chỉ end-to-end thì không thể sử dụng với NAT.
- Đôi khi có thể sử dụng ánh xạ NAT tĩnh.
- Khắc phục sự cố mạng có thể khó khăn hơn.
- Các giao thức đường hầm (trong VPN) cấu hình phức tạp hơn
- Việc khởi tạo kết nối TCP có thể bị gián đoạn.

Hết chương 6