CANTHO UNIVERSITY

THIẾT KẾ CÀI ĐẶT MẠNG MÁY TÍNH

MÃ SỐ HỌC PHẦN: CT335

CHƯƠNG 6
DỊCH ĐỊA CHỈ MẠNG IPv4
NETWORK ADDRESS TRANSLATION – NAT

CANTHO UNIVERSITY

ĐỊA CHỈ RIÊNG IPv4 (IPv4 Private Address)

- Địa chỉ riêng IPv4 được sử dụng cho các mạng con, máy tính trong mạng của công ty, tổ chức, tập đoàn mà không cần phải đăng ký với nhà cung cấp dịch vụ (ISP), không phải trả chi phí thuê địa chỉ

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

CANTHO UNIVERSITY

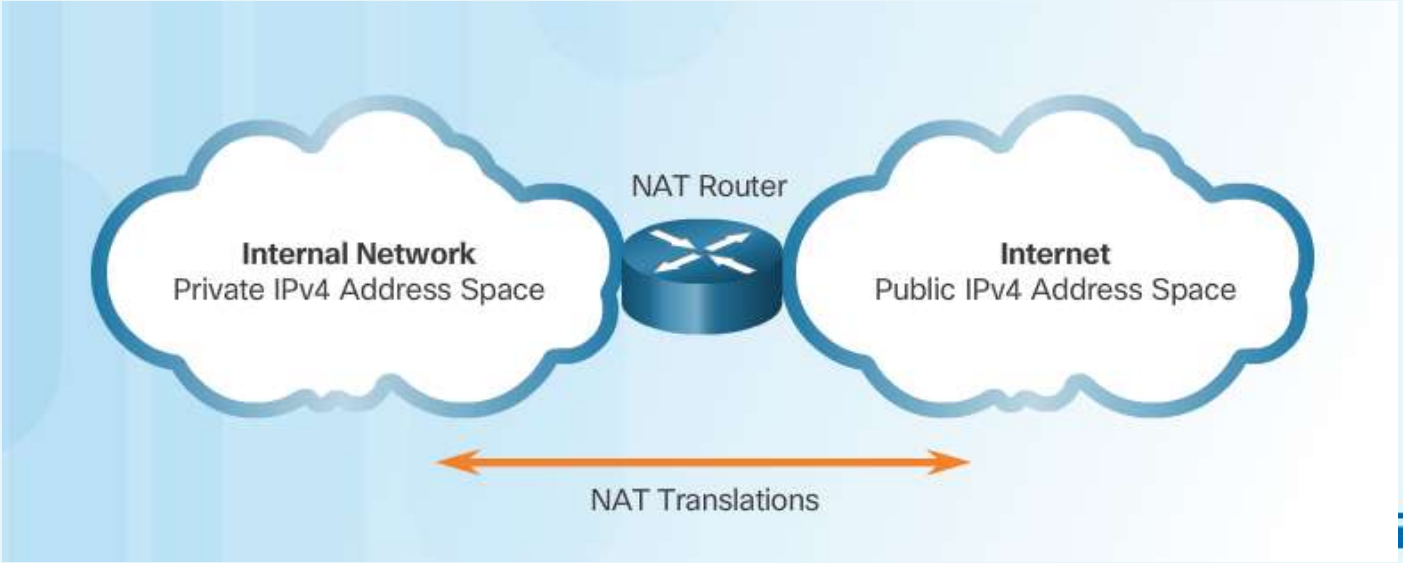
ĐỊA CHỈ RIÊNG IPv4 (IPv4 Private Address)

RFC 1918 name	IP address range	Number of addresses	Largest CIDR block (subnet mask)	Host ID size	Mask bits	Classful description
24-bit block	10.0.0.0 – 10.255.255.255	16,777,216	10.0.0.0/8 (255.0.0.0)	24 bit	8 bit	single class A network
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576	172.16.0.0/12 (255.240.0.0)	20 bit	12 bit	16 contiguous class B networks
16-bit block	192.168.0.0 – 192.168.255.255	65,536	192.168.0.0/16 (255.255.0.0)	16 bit	16 bit	256 contiguous class C networks

CANTHO UNIVERSITY

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 cài đặt trên router biên (router giữa mạng bên trong và mạng bên ngoài) để dịch các địa chỉ IP riêng thành các địa chỉ IP công cộng (public IP) có thể được định tuyến trên Internet
- Một địa chỉ IPv4 công cộng có thể được sử dụng cho hàng nghìn thiết bị mang địa chỉ IP riêng



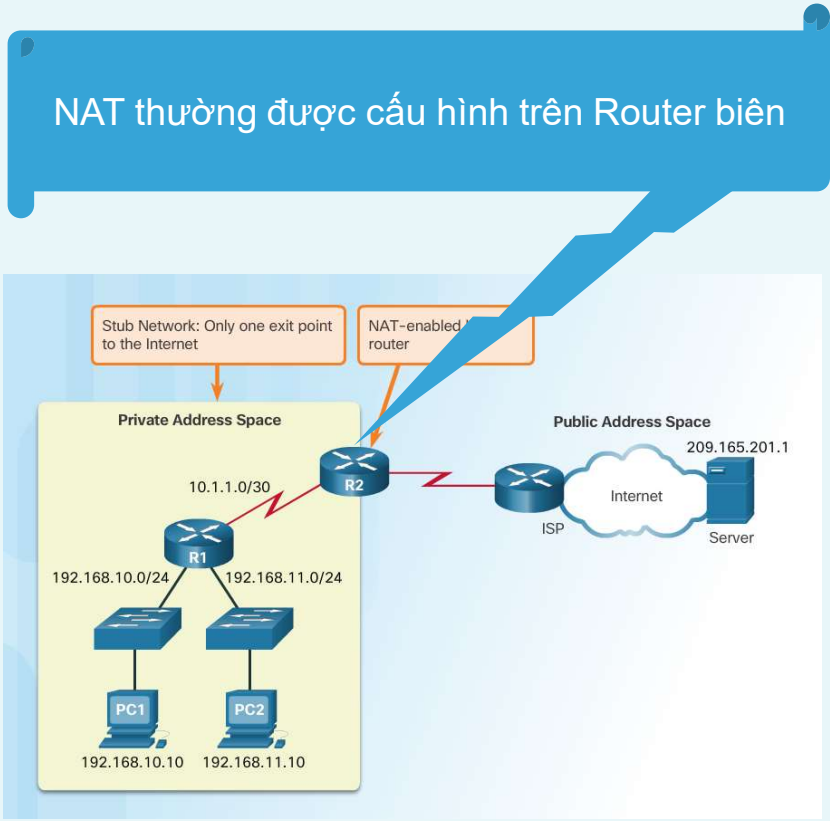
CANTHO UNIVERSITY

GIỚI THIỆU VỀ NAT

- NAT được sử dụng để dịch các địa chỉ IP riêng (được sử dụng trong mạng LAN) thành các địa chỉ IP công cộng có thể được định tuyến trên Internet
- NAT che dấu địa chỉ IPv4 mạng LAN khỏi các mạng bên ngoài

Ví dụ: Các công ty khác nhau 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 này với mạng 10.x.x.x của công ty khác

- Hầu hết các router đều hỗ trợ NAT
- Router có thể được cấu hình với nhiều kiểu dịch (với một hay nhiều địa chỉ IP công cộng) để áp dụng cho một hoặc nhiều thiết bị trong mạng LAN đang được cấu hình bằng địa chỉ riêng



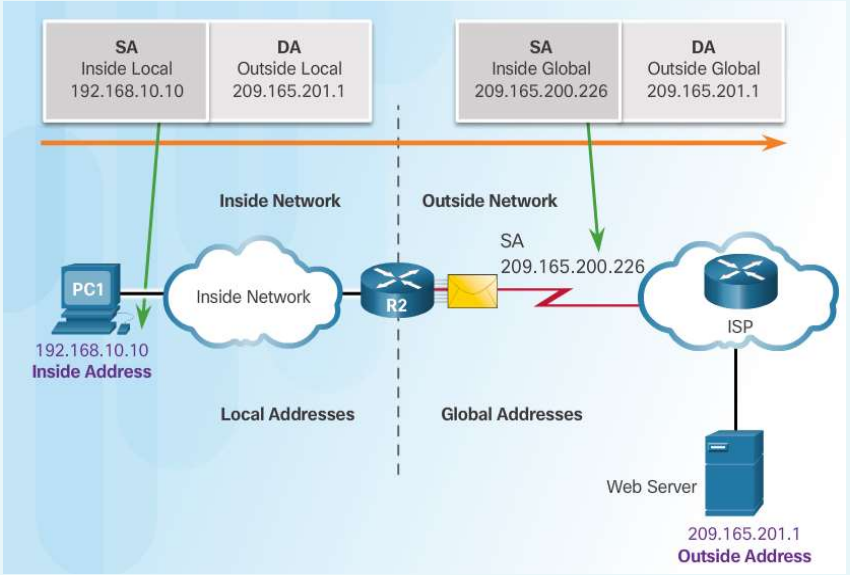
CANTHO UNIVERSITY

THUẬT NGỮ NAT

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

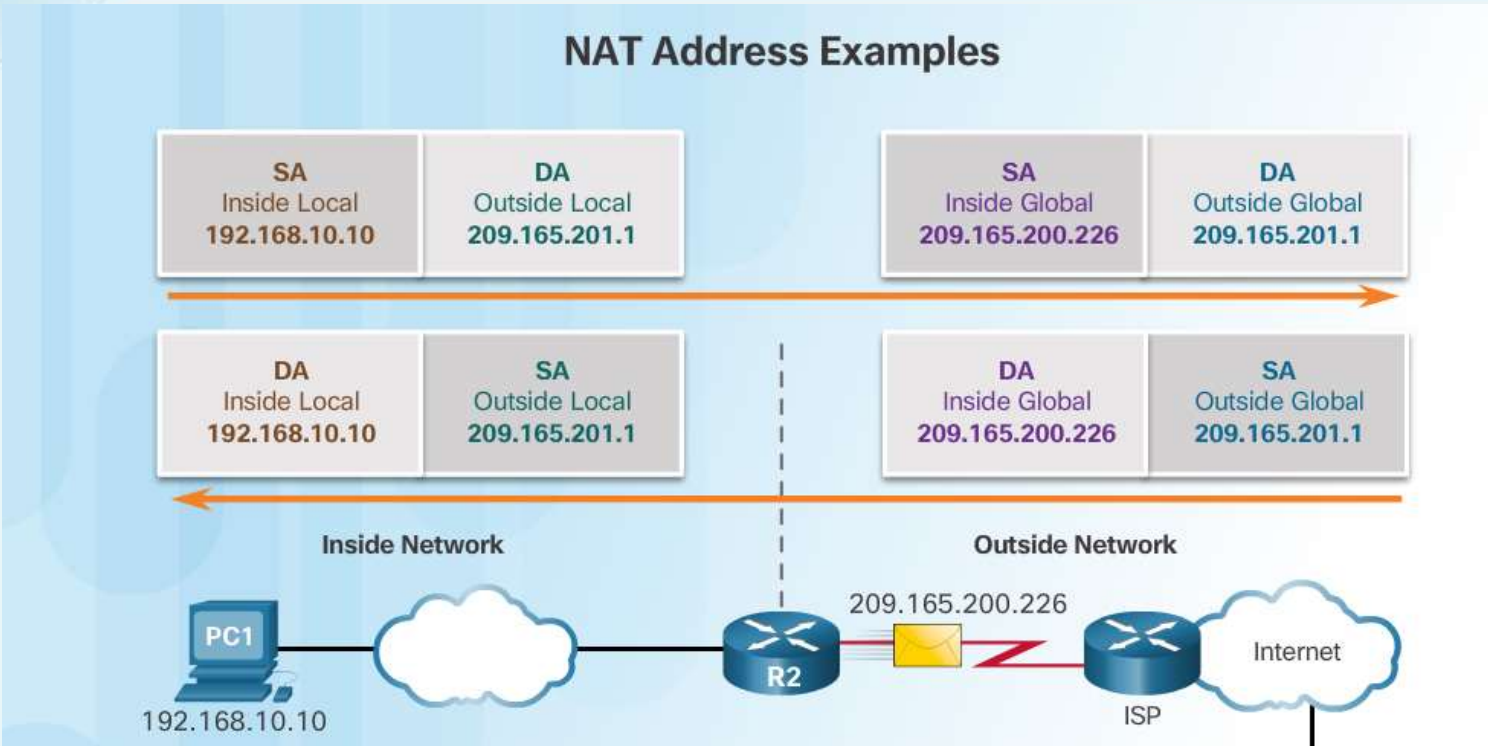
Quan sát hình bên phải, R2 là router biên:

- *Inside address:* địa chỉ được dùng trong LAN, là địa chỉ riêng đặt cho các thiết bị, host, địa chỉ này sẽ được NAT dịch
- *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 trên Internet. Đây là địa chỉ đại diện cho các địa chỉ trong LAN ra ngoài Internet
- ✓ *Outside global address:* là địa chỉ đích, kiểu public IP trên Internet
- ✓ *Outside local address:* là địa chỉ thực đặt của máy đích nằm trên Internet (có thể là địa chỉ dạng private hoặc public)

THUẬT NGỮ NAT



R2 NAT Table

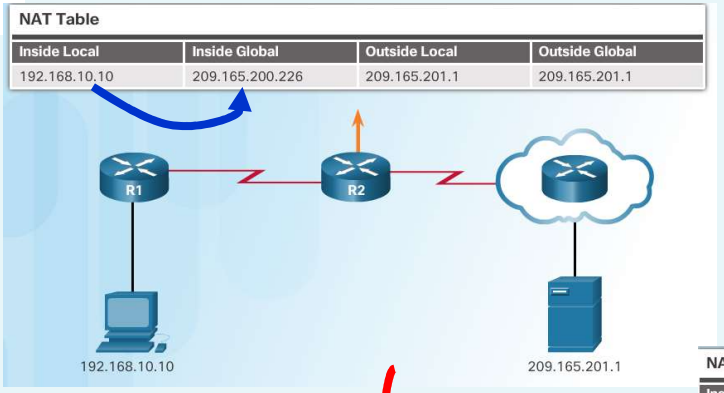
PC1		Web Server	
Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

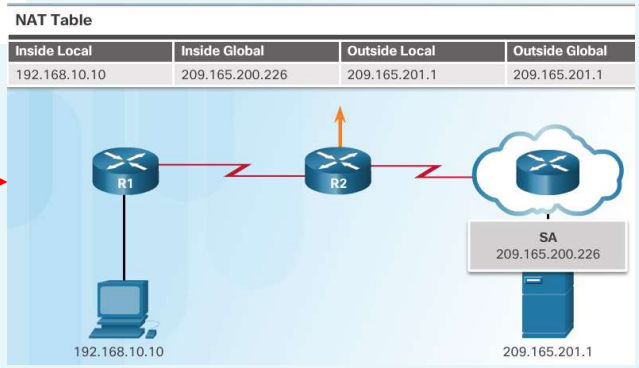
CANTHO UNIVERSITY

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 trên Internet

Địa chỉ được dịch sẽ ghi vào bảng NAT để tham khảo sau đó



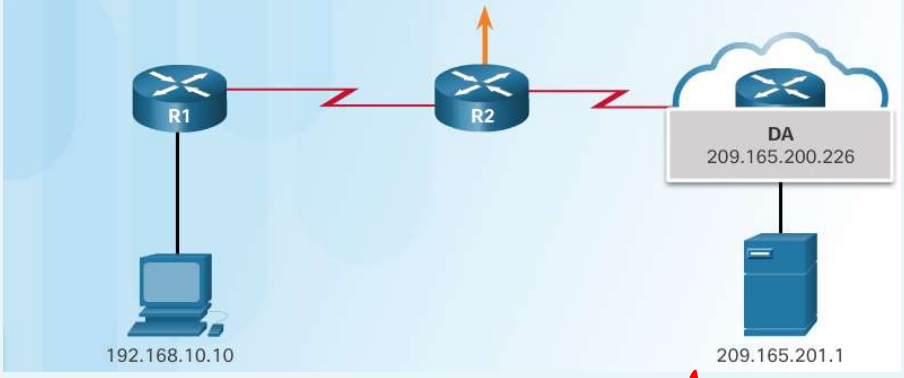


CANTHO UNIVERSITY

HOẠT ĐỘNG CỦA NAT

NAT Table

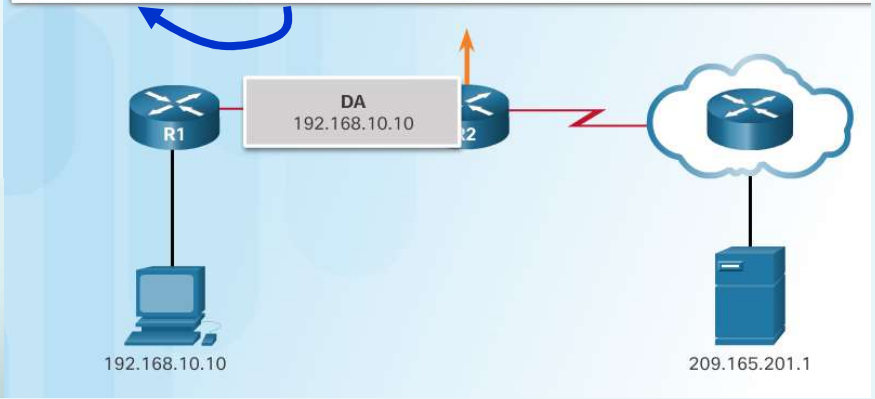
Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



2. Server mạng bên ngoài trên Internet 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

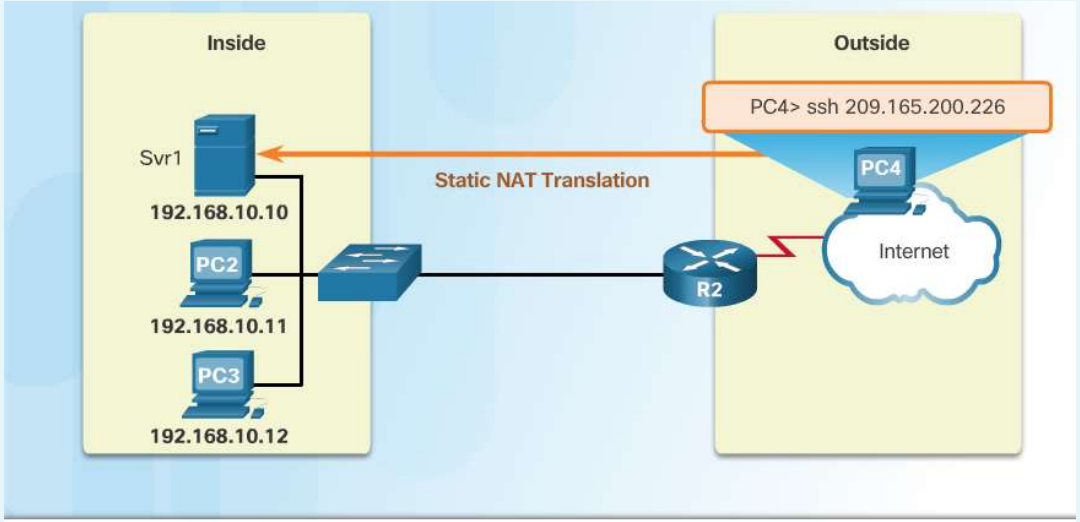


3. Router biên xem trong bảng dịch NAT để biết máy tính nào đã yêu cầu dữ liệu và dịch lại địa chỉ từ công cộng sang địa chỉ riêng của thiết bị và chuyển gói tin đến thiết bị đó

CANTHO UNIVERSITY

CÁC KIỂU NAT
NAT TĨNH – STATIC NAT

- NAT tĩnh là ánh xạ một địa chỉ *IP riêng* sang địa chỉ *IP công cộng* để các host từ Internet có thể giao tiếp
- NAT tĩnh thường được sử dụng cho các server có các truy cập từ bên ngoài hoặc cho các thiết bị cần được quản trị từ bên ngoài

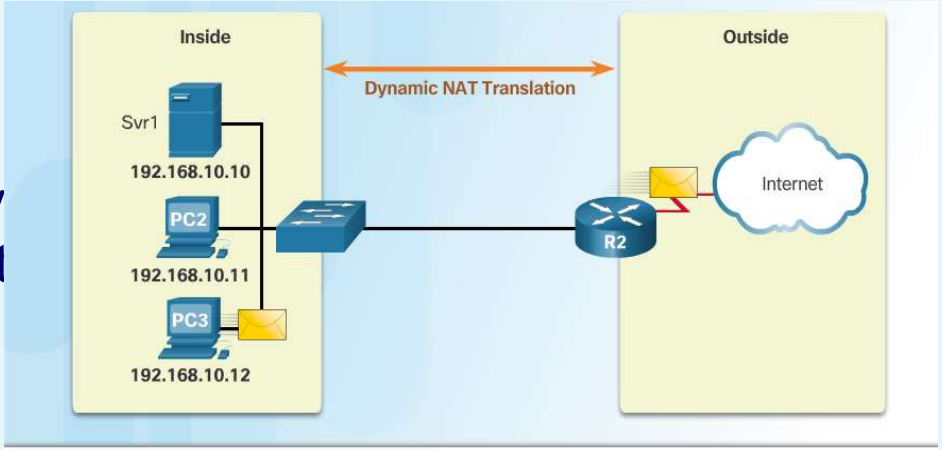


Static NAT Table

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

CÁC KIỂU NAT
NAT ĐỘNG – DYNAMIC NAT

- NAT động được dùng gán một hay một dãy địa chỉ IP công cộng (được khai báo trước). Thường được dùng để dịch địa chỉ các thiết bị (không phải là server) sử dụng địa chỉ riêng để truy cập các địa chỉ công cộng trên 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 nếu các máy trong LAN truy cập ra *cùng một IP công cộng bên ngoài* (tùy theo số lượng địa chỉ được khai báo trong nhóm địa chỉ công cộng dùng để dịch đi ra ngoài mạng)



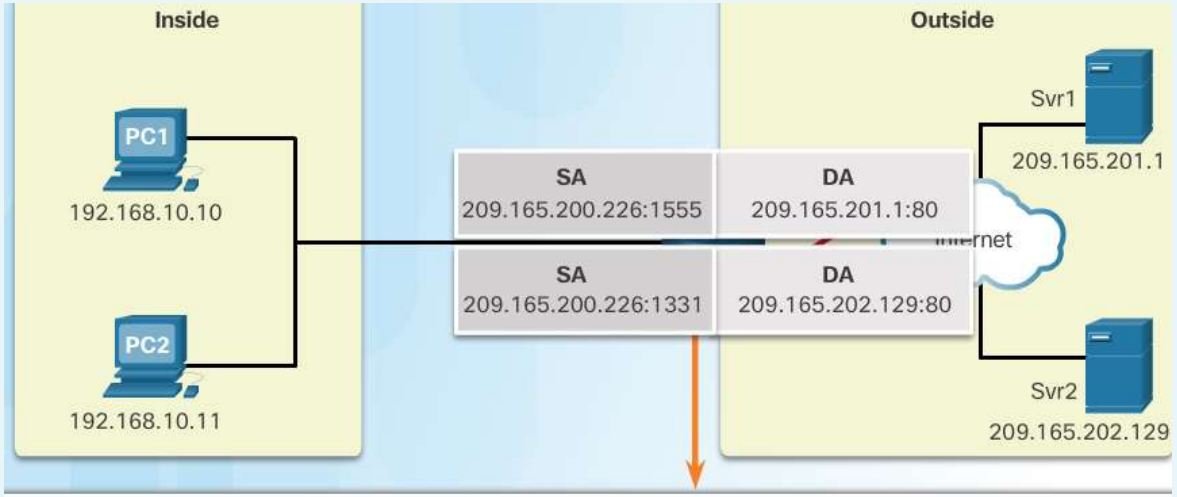
IPv4 NAT Pool

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

DỊCH ĐỊA CHỈ CỔNG – PAT
PORT ADDRESS TRANSLATION

- PAT (cách gọi khác là *NAT overload*) có thể dùng 1 địa chỉ IPv4 để cho phép số lượng lớn các host bên trong mạng giao tiếp với các host trên mạng Internet
- 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

CÁC KIỂU NAT
PAT – CỔNG KHẢ DỤNG KẾ TIẾP

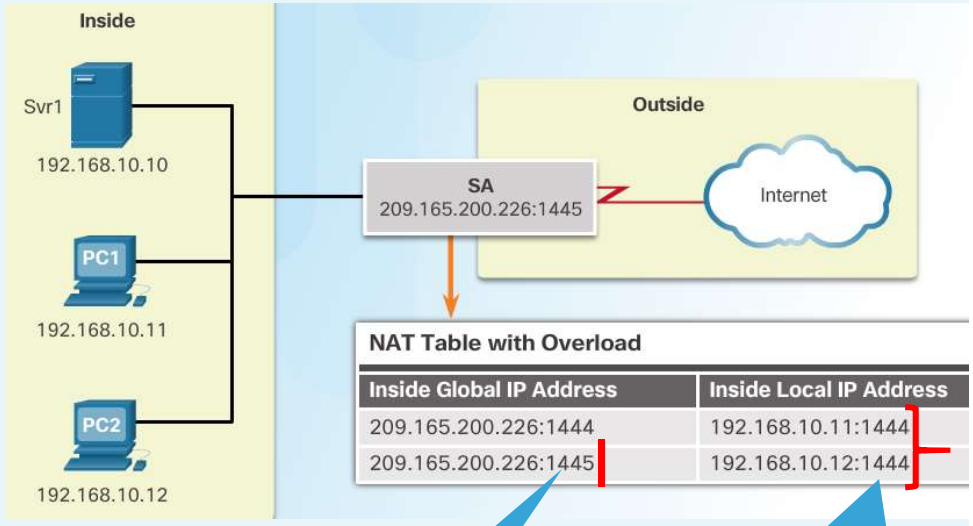
CANTHO UNIVERSITY

Trong tiến 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
- ✓ 1,024 - 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)



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

2. PAT sẽ dịch sang cùng 1 địa chỉ công cộng nhưng cổng nguồn sẽ dịch sang cổng khả dụng đầu tiên

CANTHO UNIVERSITY

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

- NAT tĩnh dịch địa chỉ 1:1

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

- PAT sử dụng một địa chỉ công cộng với nhiều số hiệu cổng để có thể dịch cho nhiều thiết bị trong LAN (không phải là server) đang dùng địa chỉ riêng khác nhau

CANTHO UNIVERSITY

LỢI ÍCH CỦA NAT

- Bảo tồn các địa chỉ IP công cộng
- 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)
- 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