

Tìm hiểu cơ chế hoạt động của NAT (Network Address Translation)

Kết nối **Internet** hiện đại ngày nay đều phải sử dụng đến kỹ thuật **NAT (Network Address Translation)**. **NAT (Network Address Translation)** cho phép một hay nhiều **địa chỉ IP** nội miền được ánh xạ với một hay nhiều **địa chỉ IP** ngoại miền. Để hiểu thêm về **NAT** cũng như cơ chế hoạt động của **NAT**, các bạn cùng tham khảo bài viết dưới đây.

Mạng **Internet** ngày càng phát triển hơn so với tưởng tượng của chúng ta. Mặc dù không thể thông kê con số chính xác là bao nhiêu nhưng chúng ta có thể ước tính được con số là hơn 100 triệu Host và hơn 350 triệu người truy cập **Internet** hàng ngày. Trên thực tế, tỉ lệ này tăng gấp đôi theo mỗi năm .

Kết nối **Internet** hiện đại ngày nay đều phải sử dụng đến kỹ thuật **NAT (Network Address Translation)**. **NAT** cho phép một (hay nhiều) **địa chỉ IP** nội miền được ánh xạ với một (hay nhiều) **địa chỉ IP** ngoại miền.

Địa chỉ IP (IP – Internet Protocol) là chuỗi số có chiều dài 32 bit (**IPv4**) hoặc 128 bit (**IPv6**) dùng để định danh một thiết bị mạng trên hệ thống mạng giúp chúng nhận diện và liên lạc với nhau. Trong một mô hình mạng, mỗi một thiết bị mạng chỉ có một **địa chỉ IP** duy nhất. Có thể hiểu nôm na **địa chỉ IP** giống như địa chỉ nơi bạn sinh sống. Người khác có thể tìm ra bạn và gửi thông tin cho bạn thông qua địa chỉ đó.

Cùng với sự bùng nổ **Internet** như hiện nay và nhu cầu sử dụng hệ thống mạng ngày càng gia tăng, không gian **địa chỉ IPv4** bắt đầu bị giới hạn. Giải pháp đưa ra là thiết kế lại định dạng **địa chỉ IP**, cho phép nhiều **địa chỉ IP** hơn nữa (cụ thể là **IPv6**). Tuy nhiên giải pháp này vẫn đang trong giai đoạn nghiên cứu và phát triển và phải mất nhiều năm để thực hiện.

Do đó giải pháp tốt nhất là sử dụng đến kỹ thuật **NAT (Network Address Translation)**. **NAT** hay **Network Address Translation** cho phép một thiết bị như **Router** hoạt động như một người đại diện trung gian giữa **Internet** (hoặc **Public Network**: hệ thống mạng công cộng) và **Local** (hoặc **Private**: hệ thống mạng nội bộ). Điều này có nghĩa là một máy tính chỉ có một **địa chỉ IP** duy nhất.

NAT (Network Address Translation) là gì?

Hiểu nôm na, **NAT** cũng giống như một nhân viên lễ tân tại một văn phòng lớn. Nếu bạn muốn gặp một ai đó trong công ty đều phải thông qua và làm theo hướng dẫn của nhân viên lễ tân. Hoặc nếu bạn muốn gọi điện nói chuyện với một ai đó nhưng người đó không có mặt ở công ty hoặc họ đang bận họp,... bạn có thể để lại tin nhắn cho lễ tân sau đó họ sẽ chuyển tiếp tin nhắn tới người mà bạn cần nói

chuyện để thông báo. Trong một trường hợp khác bạn có thể nói chuyện với lễ tân và yêu cầu họ nối máy đến người bạn cần gặp.

Hay có thể hiểu khi một người muốn nói chuyện với bạn, nhưng họ chỉ biết số điện thoại văn phòng nơi bạn làm việc. Họ sẽ gọi điện đến văn phòng của bạn và yêu cầu nhân viên lễ tân chuyển tiếp cuộc gọi đến bạn. Lúc này nhân viên lễ tân sẽ tiến hành kiểm tra trên bảng tra cứu để tìm ra tên của bạn và các thông tin mở rộng khác. Và sau đó họ sẽ chuyển tiếp cuộc gọi đến cho bạn trên phần mở rộng của bạn.

NAT (Network Address Translation) làm nhiệm vụ gì?

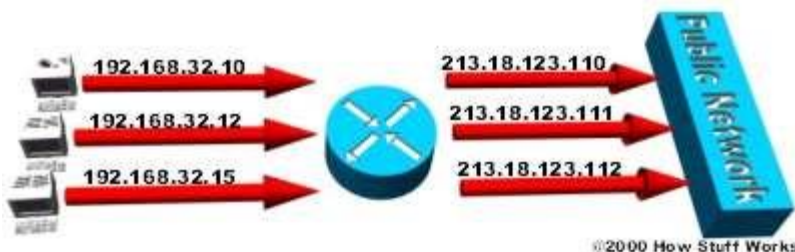
NAT (Network Address Translation) giống như một **Router**, chuyển tiếp các gói tin giữa những lớp mạng khác nhau trên một mạng lớn. **NAT** dịch hay thay đổi một hoặc cả hai địa chỉ bên trong một gói tin khi gói tin đó đi qua một **Router**, hay một số thiết bị khác. Thông thường **NAT** thường thay đổi địa chỉ thường là địa chỉ riêng (**IP Private**) của một kết nối mạng thành địa chỉ công cộng (**IP Public**). **NAT** cũng có thể coi như một **Firewall** (tường lửa) cơ bản. **NAT** duy trì một bảng thông tin về mỗi gói tin được gửi qua. Khi một máy tính trên mạng kết nối đến 1 website trên **Internet header** của **địa chỉ IP nguồn** được thay thế bằng địa chỉ **Public** đã được cấu hình sẵn trên **NAT sever**, sau khi có gói tin trở về **NAT** dựa vào bảng record mà nó đã lưu về các gói tin, thay đổi **địa chỉ IP đích** thành địa chỉ của **PC** trong mạng và chuyển tiếp đi. Thông qua cơ chế đó quản trị mạng có khả năng lọc các gói tin được gửi đến hay gửi từ một **địa chỉ IP** và cho phép hay ngăn truy cập đến một port cụ thể.

NAT (Network Address Translation) được phát triển bởi **Cisco**. **NAT** bao gồm một số loại cơ bản dưới đây:

Static NAT (NAT tĩnh)

Static NAT (NAT tĩnh) là phương thức **NAT** một đôi một. Một **địa chỉ IP Private** sẽ được map với một **địa chỉ IP Public**.

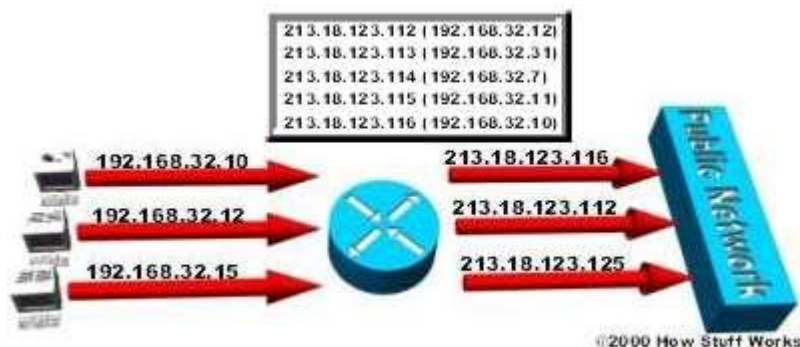
NAT tĩnh được sử dụng khi thiết bị cần truy cập từ bên ngoài mạng.



Trong **Static NAT (NAT tĩnh)**, địa chỉ IP của máy tính là 192.168.32.10 luôn được **Router** biên dịch đến địa chỉ IP 213.18.123.110.

Dynamic NAT (NAT động)

Một địa chỉ IP Private sẽ được map với một địa chỉ IP Public trong nhóm địa chỉ IP Public.



Trong **Dynamic NAT (NAT động)**, máy tính có địa chỉ IP 192.168.32.10 luôn được **Router** biên dịch đến địa chỉ đầu tiên 213.18.123.100 trong dãy địa chỉ IP từ 213.18.123.100 đến 213.18.123.150.

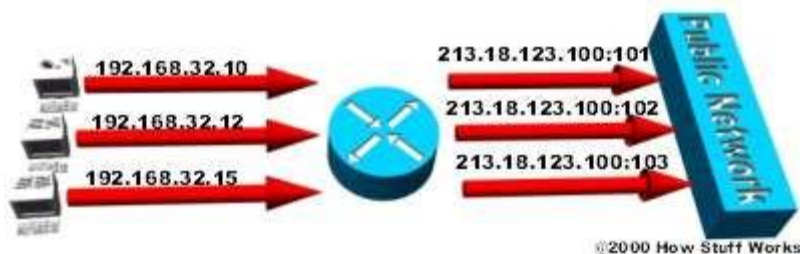
Xem thêm: Thủ thuật thay đổi cấu hình dynamic NAT

Overloading NAT

NAT Overloading là một dạng thức của **NAT động (Dynamic Overload)**.

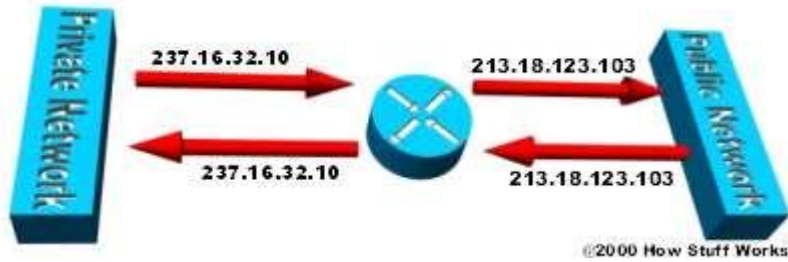
Nhiều địa chỉ IP Private sẽ được map với một địa chỉ IP Public qua các **Port (cổng)** khác nhau.

Cũng giống như **PAT (Port Address Translation)**, một địa chỉ NAT hoặc **Port** sẽ có nhiều mức độ NAT khác nhau.



Trong **Overloading NAT**, mỗi máy tính trong mạng nội bộ (**Private Network**) được **Router** biên dịch đến cùng một địa chỉ IP 213.18.123.100 nhưng trên các cổng giao tiếp khác nhau.

Overlapping NAT



Khi **địa chỉ IP** trong hệ thống mạng nội bộ là **IP Public** đang sử dụng trên một hệ thống mạng khác, **Router** phải duy trì một bảng tìm kiếm các địa chỉ này để ngăn và thay thế bằng một **IP Public** duy nhất.

Điều quan trọng cần lưu ý rằng **NAT router** phải biên dịch địa chỉ "nội bộ" thành một **địa chỉ IP Public** duy nhất cũng như biên dịch địa chỉ "ngoài" thành một địa chỉ **IP Private** duy nhất. Bạn có thể sử dụng **NAT tĩnh** hoặc sử dụng kết hợp **DNS** và **NAT động**.

Hệ thống mạng nội bộ thông thường là **LAN (Local Area Network)**, hay còn gọi là **Stub Domain**. Một **Stub Domain** là một **LAN** sử dụng **địa chỉ IP nội bộ**.

Hầu hết các **Network Traffic** (là lưu lượng mạng ổn định, không bị gián đoạn trong quá trình truyền) trong **Stub Domain** mang tính chất cục bộ, do đó hệ thống mạng nội bộ không bao giờ bị lộ ra bên ngoài.

Một **Stub Domain** có thể bao gồm cả **địa chỉ IP Public** và **IP Private**. Bất kỳ máy tính nào sử dụng **địa chỉ IP Private** đều phải dùng **NAT (Network Address Translation)** để trao đổi thông tin với các máy tính khác.

Trong phần tiếp theo Quản trị mạng sẽ giới thiệu cho bạn **cấu hình NAT**.