**BÀI TÂP LÝ THUYẾT 2**

**Câu 1: Trình bày cơ chế NAT, so sánh dynamic NAT và static NAT kèm ứng dụng cụ thể của từng loại?**

- Cơ chế NAT:

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 sử dụng 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 2 mạng.

NAT sử dụng IP của chính nó làm IP công cộng cho mỗi máy con (client) với IP riêng. Khi một máy con thực hiện kết nối hoặc gửi dữ liệu tới một máy tính nào đó trên Internet, dữ liệu sẽ được gửi tới NAT, sau đó NAT sẽ thay thế địa chỉ IP gốc của máy con đó rồi gửi gói dữ liệu đi với địa chỉ IP của NAT. Máy tính từ xa hoặc máy tính nào đó trên Internet khi nhận được tín hiệu sẽ gửi gói tin trở về cho NAT computer bởi chúng nghĩ rằng NAT computer là máy đã gửi những gói dữ liệu đi. NAT ghi lại bảng thông tin của những máy tính đã gửi những gói thông tin ra ngoài trên mỗi cổng dịch vụ và gửi những gói tin nhận được về đúng client đó.

NAT xử lý một gói tin xuất phát từ bên trong đi ra bên ngoài một mạng theo cách thức sau:

- Khi NAT nhận một gói tin từ một cổng bên trong, gói tin này đáp ứng các tiêu chuẩn để NAT, Router sẽ tìm kiếm trong bảng NAT địa chỉ bên ngoài của gói tin. Nói cách khác, tiến trình NAT tìm kiếm một hàng ở trong bảng NAT trong đó địa chỉ outside local address bằng với địa chỉ đích của gói tin. Nếu không có phép so sánh trùng nào được tìm thấy, gói tin đó sẽ bị loại bỏ.

- Nếu có một hàng trong bảng NAT là tìm thấy, trong hàng này địa chỉ đích của gói tin bằng với địa chỉ outside local, NAT sẽ thay thế địa chỉ đích trong gói tin bằng địa chỉ outside global theo thông tin trong bảng NAT.

- Tiến trình NAT tiếp tục tìm kiếm bảng NAT để xem có một địa chỉ Inside local nào bằng với địa chỉ nguồn của gói tin hay không. Nếu có một hàng là tìm thấy, NAT tiếp tục thay thế địa chỉ nguồn của gói tin bằng địa chỉ Inside global. Nếu không có một hàng nào được tìm thấy, NAT sẽ tạo ra một hàng mới trong bảng NAT và chèn địa chỉ mới vào trong gói tin.

- Nếu không có hàng nào trong bảng NAT được tìm thấy, gói tin sẽ bị loại bỏ. Nếu có một hàng tìm thấy trong bảng NAT thì nó sẽ thay thế địa chỉ đích bằng địa chỉ Inside local từ bảng NAT.

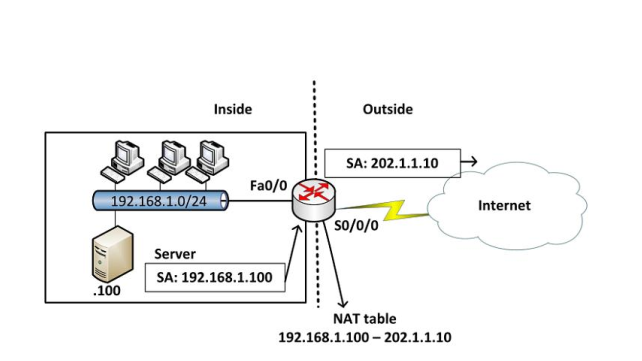
- Router tìm kiếm bảng NAT để tìm ra địa chỉ Outside global bằng với địa chỉ nguồn của gói tin. Nếu có một hàng là tìm thấy, NAT sẽ thay thế địa chỉ đích bằng địa Outside local từ bảng NAT. Nếu NAT không tìm thấy một hàng nào, nó sẽ tạo ra một hàng mới trong bảng NAT và cũng thực hiện như ở bước 2.

- So sánh NAT động và NAT tĩnh:

- NAT tĩnh - Static NAT

NAT tĩnh hay còn gọi là Static NAT là phương thức NAT một đổi một. Nghĩa là một địa chỉ IP cố định trong LAN sẽ được ánh xạ ra một địa chỉ IP Public cố định trước khi gói tin đi ra Internet. Phương pháp này không nhằm tiết kiệm địa chỉ IP mà chỉ có mục đích ánh xạ một IP trong LAN ra một IP Public để ẩn IP nguồn trước khi đi ra Internet làm giảm nguy cơ bị tấn công trên mạng.

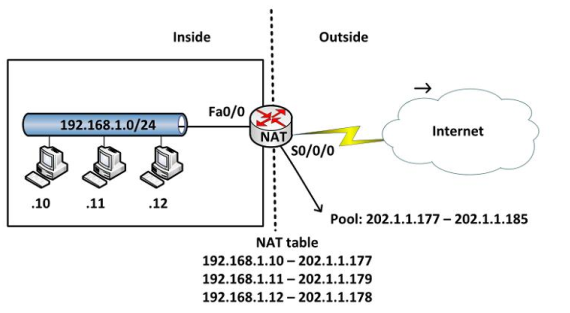
Kỹ thuật này thường được sử dụng để chuyển đổi từ địa chỉ IP này sang địa chỉ khác một cách cố định, và thường là từ một địa chỉ private sang một địa chỉ public. Toàn bộ quá trình này được cài đặt thủ công, địa chỉ IP được ánh xạ tĩnh với nhau thông qua các lệnh cấu hình.



- NAT động - Dynamic NAT

NAT được thực hiện 1 cách tự động. Trên Router, người quản trị cấu hình 1 danh sách các địa chỉ bên trong cần đi ra ngoài Internet và 1 danh sách các địa chỉ bên ngoài đại diện cho các địa chỉ bên trong. Tiếp theo, người quản trị cấu hình yêu cầu Router NAT danh sách bên trong thành danh sách bên ngoài. Bảng NAT của Router sẽ không có bất kỳ 1 dòng thông tin NAT nào được tạo sẵn mà các dòng thông tin NAT sẽ chỉ được tạo ra khi có gói tin đến Router ra Internet.

Dynamic NAT phức tạp hơn so với Static, chúng phải lưu giữ các thông tin kết nối và thậm chí phải tìm thông tin của TCP trong packet. Do mức độ phức tạp cao hơn, nên Dynamic NAT chỉ dùng thay Static NAT với mục đích bảo mật. Những người bên ngoài không thể tìm ra IP kết nối với host chỉ định vì tại thời điểm tiếp theo host này có thể nhận một IP hoàn toàn khác.



**Câu 2: So sánh địa chỉ IPv4 và IPv6 và ý nghĩa sử dụng của địa chỉ Ipv6?**

- So sánh địa chỉ IPv4 và IPv6

|  |  |  |
| --- | --- | --- |
| Điểm khác biệt | IPv4 | IPv6 |
| Khả năng tương thích với các thiết bị di động | Địa chỉ sử dụng ký hiệu dấu thập phân, không phù hợp với mạng di động | Địa chỉ được phân tách bằng dấu hai chấm – thập lục phân. Giúp cho nó tương thích tốt hơn với các mạng di động |
| Ánh xạ | Address Resolution Protocol dùng để ánh xạ đến các địa chỉ MAC | Neighbor Discovery Protocol dùng để ánh xạ đến địa chỉ MAC |
| DHCP | Khi kết nối mạng, clients được yêu cầu tiếp cận với DHCP | Clients được cung cấp địa chỉ, không cần phải liên hệ bắt buộc với máy chủ nào khác |
| Bảo mật IP | Tùy chọn | Bắt buộc |
| Các trường tùy chọn | Có | Không. Thay vào đó là các tiêu đề tiện ích mở rộng. |
| Quản lý nhóm mạng con cục bộ | Sử dụng Internet Group Management Protocol (GMP) | Sử dụng Multicast Listener Discovery (MLD) |
| Phân giải IP thành MAC | Broadcasting ARP | Multicast Neighbor Solicitation |
| Cấu hình địa chỉ | Thực hiện thủ công hoặc qua DHCP | Sử dụng tự động cấu hình địa chỉ không trạng thái bằng ICMP hoặc DHCP6. |
| DNS Record | Ở địa chỉ A | Ở địa chỉ AAAA |
| Packet Header | Không xác định được packet flow để xử lý QoS. Bao gồm cả các tùy chọn kiểm tra checksum. | Flow Label Fields chỉ định luồng gói để xử lý QoS |
| Packet Fragmentation | Cho phép từ các router truyền đến máy chủ | Chỉ truyền được đến máy chủ |
| Kích thước gói | Tối thiểu là 576 byte | Tối thiểu là 1208 byte |
| Bảo mật | Chủ yếu dựa vào tầng Ứng dụng | Có giao thức Bảo mật riêng được gọi là IPSec |
| Tính di động và khả năng tương tác | Các cấu trúc liên kết mạng tương đối hạn chế. Do đó, làm giảm tính di động và khả năng tương tác | Cung cấp tính di động và khả năng tương tác được nhúng trong các thiết bị mạng |
| SNMP | Hỗ trợ | Không hỗ trợ |
| Address Mask | Dùng cho mạng được chỉ định từ phần máy chủ | Không được sử dụng |
| Address Features | Network Address Translation được sử dụng, cho phép NAT một địa chỉ đại diện cho hàng ngàn địa chỉ non-routable. | Direct Addressing là khả thi vì không gian địa chỉ rộng lớn. |
| Cấu hình mạng | Được cấu hình thủ công hoặc với DHCP | Cấu hình tự động |
| Giao thức định tuyến thông tin (RIP) | Hỗ trợ | Không hỗ trợ |
| Phân mảnh | Được thực hiện trong quá trình routing. | Được thực hiện bởi người gửi |
| VLSM | Hỗ trợ | Không hỗ trợ |
| Cấu hình | Để giao tiếp với các hệ thống khác, một hệ thống mới phải được cấu hình | Tùy chọn cấu hình |
| Số lớp | Năm lớp (A-E) | Không giới hạn lưu trữ địa chỉ IP |
| Loại địa chỉ | Multicast, Broadcast và Unicat | Anycast, Unicast và Multicast |
| Trường Checksum | Có | Không |
| Chiều dài Header | 20 | 40 |
| Số lượng Header field | 12 | 8 |
| Address method | Địa chỉ số | Địa chỉ chữ và số |
| Kích thước địa chỉ | 32 bit | 128 bit |

- Ý nghĩa sử dụng của IPv6

IPv6 đã bù đắp được mọi lỗ hổng trong kỹ thuật ở IPv4. Việc cung cấp địa chỉ 128 bit (16 byte) đã làm cho tổng số lượng địa chỉ lên đến khoảng 340 nghìn nghìn tỷ.

Rõ ràng, nó lớn hơn rất nhiều so với IPv4 vì được tạo nên bởi 16 bit. Đây là lý do để các mạng nên bắt đầu sử dụng IPv6 ngay từ lúc này. Tuy nhiên, việc thực hiện việc đó đến nay vẫn chưa dễ dàng. Các nhà triển khai mạng đã quen với IPv4, và cũng chưa có động thái rõ ràng về cách tiếp cận với IPv6. Nhiều người cho rằng IPv4 vẫn tốt cho tương lai gần. Nhưng rõ ràng là việc sử dụng IPv4 chỉ càng làm cho số lượng của nó giảm đi mà thôi.

Một ví dụ đơn giản về khả năng vượt trội của IPv6 so với IPv4 là việc nó không cần phải chia sẻ địa chỉ IP và nhận một địa chỉ riêng biệt cho các thiết bị. Việc sử dụng IPv4 đồng nghĩa với việc một nhóm các máy tính muốn dùng chung một địa chỉ IP công cộng sẽ phải dùng đến NAT.

Sau đó là vấn đề truy cập trực tiếp vào một trong số chúng. Bạn sẽ cần thiết lập các cấu hình phức tạp. Có thể gồm chuyển tiếp, thay đổi tường lửa…Đối với IPv6, sẽ có nhiều địa chỉ để sử dụng hơn. Do đó, các máy tính sử dụng IPv6 có thể truy cập công khai mà không cần cấu hình bổ sung, tiết kiệm được tài nguyên.

**Câu 3: Trình bày sự giống và khác nhau giữa mô hình OSI và mô hình TCP/IP**

- Điểm giống nhau giữa mô hình OSI và TCP/IP

+ *Chia sẻ kiến trúc chung*

Cả 2 mô hình đều là mô hình logic và có kiến trúc tương tự vì cả 2 mô hình đều được xây dựng dựa trên các lớp

+ *Xác định tiêu chuẩn*

Cả 2 lớp đều có các tiêu chuẩn xác định và chúng cũng cung cấp khuôn khổ được sử dụng để thực hiện các tiêu chuẩn và thiết bị

+ *Quy trình khắc phục sự cố được đơn giản hóa*

Cả 2 mô hình đã đơn giản hóa quá trình khắc phục sự cố bằng cách chia nhỏ chức năng phức tạp thành các thành phần đơn giản hơn

+ *Các tiêu chuẩn được xác định trước*

Các tiêu chuẩn và giao thức đã được xác định trước, những mô hình này không xác định lại chúng, chỉ tham khảo hoặc sử dụng lại chúng. Ví dụ, các tiêu chuẩn Ethernet đã được IEEE xác định trước khi phát triển các mô hình

+ *Cả 2 đều có chức năng tương tự của các lớp Transport và Network*

Chức năng được thực hiện giữa lớp Presentation và lớp Network tương tự như chức năng được thực hiện ở lớp Transport

- Điểm khác nhau giữa mô hình OSI và TCP/IP

|  |  |  |
| --- | --- | --- |
| **Nội dung** | **Mô hình OSI** | **Mô hình TCP/IP** |
| **Độ tin cậy và phổ biến** | Nhiều người cho rằng đây là mô hình cũ, chỉ để tham khảo, số người sử dụng hạn chế hơn so với TCP/IP | Được chuẩn hóa, nhiều người tin cậy và sử dụng phổ biến trên toàn cầu |
| **Phương pháp tiếp cận** | Tiếp cận theo chiều dọc | Tiếp cận theo chiều ngang |
| **Sự kết hợp giữa các tầng** | Mỗi tầng khác nhau sẽ thực hiện một nhiệm vụ khác nhau, không có sự kết hợp giữa bất cứ tầng nào | Trong tầng ứng dụng có tầng trình diễn và tầng phiên được kết hợp với nhau |
| **Thiết kế** | Phát triển mô hình trước sau đó sẽ phát triển giao thức | Các giao thức được thiết kế trước sau đó phát triển mô hình |
| **Số lớp (Tầng)** | 7 | 4 |
| **Truyền thông** | Hỗ trợ cả kết nối định tuyến và không dây | Hỗ trợ truyền thông không kết nối từ tầng mạng |
| **Tình phụ thuộc** | Giao thức độc lập | Phụ thuộc vào giao thức |