NAT e PAT

Network Address Translation e Port Address Translation

Versão 1.2
Outubro de 2018

Prof. Jairo

jairo@uni9.pro.br
professor@jairo.pro.br

http://www.jairo.pro.br/

O NAT é um método de remapear o endereço IP no datagrama. Atua na camada 3 do RM-OSI.

Porém, a aplicabilidade do conceito NAT é muito extensa, diversificada e em muitos casos pode envolver também camadas 4 (transporte) e 7 (aplicação).

PAT está relacionado ao NAT, mas trata de tradução de portas TCP e não de endereços.

1 – NAT, DNAT e SNAT

1.1 – Descrição

O NAT (*Network Address Translation, tradução de endereço de rede*), é um método de tradução de endereço de rede que opera na camada 3, e que remapeia o endereço IP no pacote. O funcionamento básico consiste em modificar o endereço IP no cabeçalho do datagrama IP e/ou a porta TCP/UDP no cabeçalho de camada de transporte, quando este estiver sendo roteado.

Porém, a aplicabilidade do conceito NAT é muito extensa, diversificada e, em muitos casos, além da camada 3 pode envolver também camadas 4 (transporte) e 7 (aplicação). Muitas vezes DNAT (*Destination* NAT) e SNAT (*Source* NAT) também são tratados como NAT.

Por sua vez PAT está relacionado ao NAT, mas trata de tradução de portas TCP e não de endereços.

1.2 – NAT

O principal motivador da criação do NAT foi a percepção de que estava esgotando a disponibilidade dos endereços ipv4 para a internet (IPs públicos), isso em meados dos anos 1990.

Já naquela época, nas redes internas, passaram então a usar endereços IP das faixas reservadas (IPs privados). Com isto, para acesso à internet foi necessário NAT, técnica em que o roteador modifica o endereço IP do remetente no datagrama para que o pacote possa ser roteável na internet mesmo tendo origem numa LAN com endereços IP da faixa reservada.

Inicialmente, o conceito NAT era usado para a técnica de mascarar (*masquerade*) um endereço IP privado (LAN) num endereço IP público do roteador (IP externo). A tradução era de um para um, então para cada usuário na LAN que quisesse navegar na internet, era necessário também haver disponível um endereço público no roteador. Uma vez esgotados os endereços públicos, ninguém mais na LAN conseguia navegar na internet até que fosse liberado um IP público. A liberação do IP público ocorria automaticamente quando o usuário ficasse um determinado intervalo de tempo sem navegar na internet.

Na figura 1, abaixo. É mostrado uma única máquina da rede interna, com IP da faixa privada, navegando na internet com o IP externo (público) do roteador.

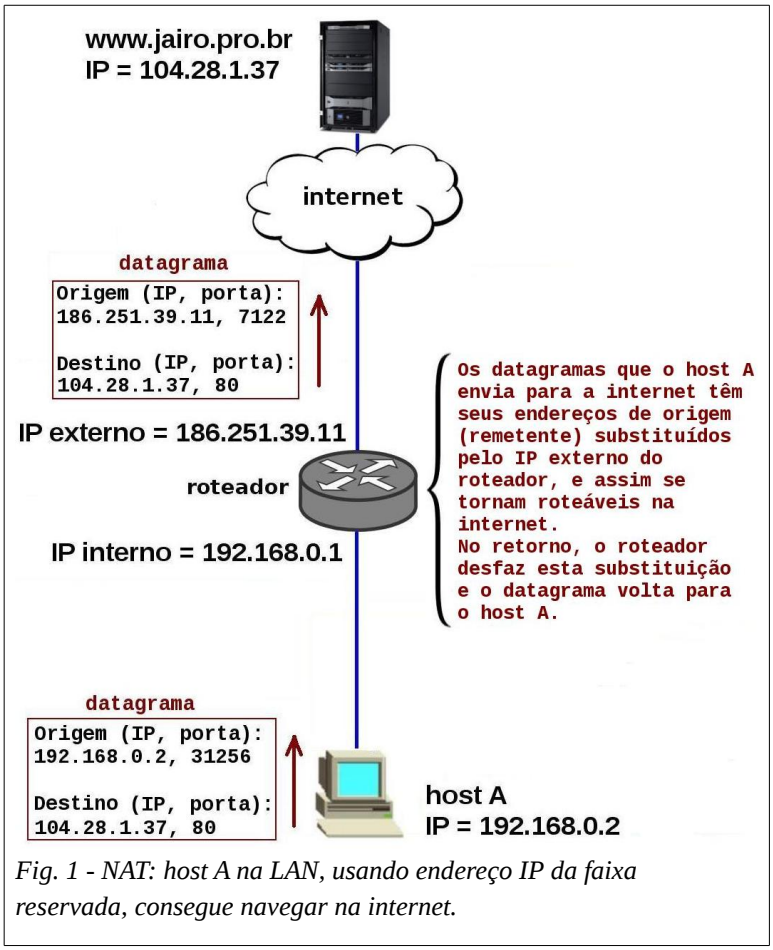

Fig. 1 - NAT: host A na LAN, usando endereço IP da faixa reservada, consegue navegar na internet.

Atualmente, o mapeamento de um para um é conhecido por *static* NAT (NAT estático).

Na figura 1, acima, no roteador as regras são um para um, portanto cada usuário na LAN irá navegar na internet com um endereço IP público diferente do outro.

Posteriormente, o conceito avançou e permitiu traduzir muitos para um, e assim foi possível traduzir todos os endereços IP privados na LAN para um único endereço IP público (IP externo).

Na figura 2, abaixo, nos datagramas com destino à internet os endereços IP da rede privada (LAN) são traduzidos para o endereço IP externo do roteador.

Atualmente, o mapeamento de muitos para um é conhecido por *dinamic* NAT (NAT dinâmico).

Um aspecto interessante sobre o NAT atualmente, é que ele impossibilita a comunicação fim a fim. Mas por outro lado, torna transparente a comunicação tanto para o *host* interno (na LAN), quanto externo (na internet). O *host* interno não sabe qual o IP público que está sendo usado na internet, e o *host* externo só vê o endereço IP público (externo) do roteador NAT. O único que sabe da conversão de endereços IP que está ocorrendo nos datagramas é o roteador NAT.

NAT, conforme apresentado acima, só vale para a versão 4 do protocolo IP, pois o que existe atualmente para ipv6 é muita discussão.

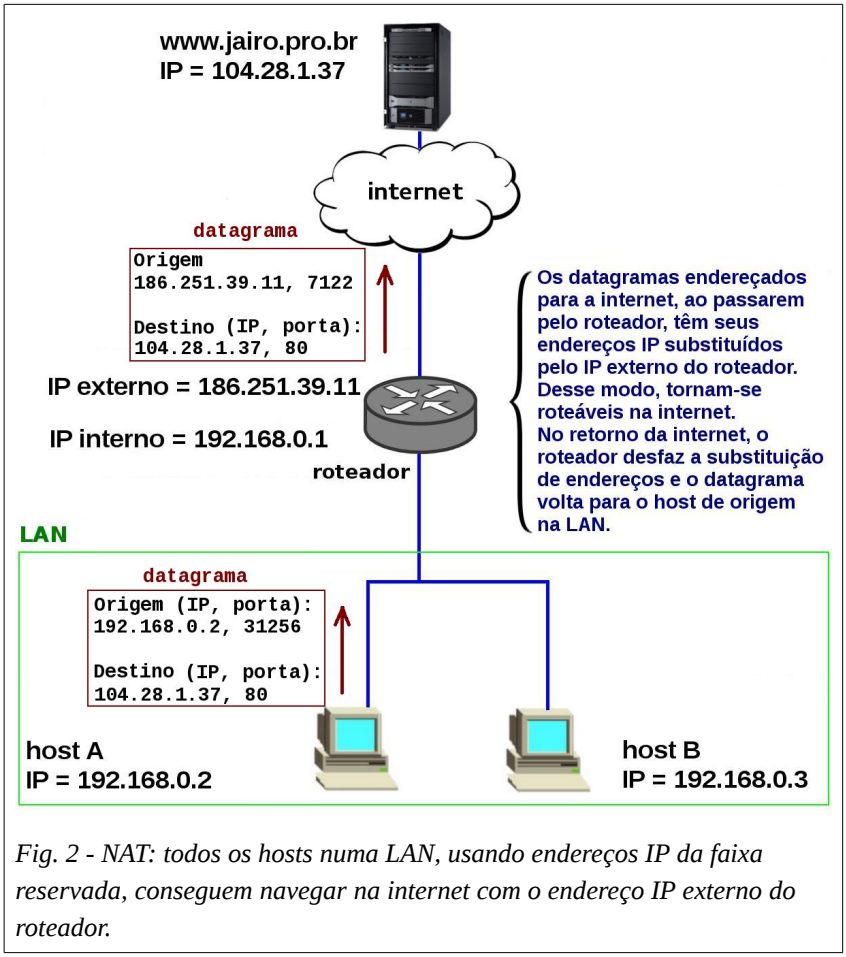

Fig. 2 - NAT: todos os hosts numa LAN, usando endereços IP da faixa reservada, conseguem navegar na internet com o endereço IP externo do roteador.

No passado, a ampla adoção do NAT ocorreu sem a contrapartida de padronização desta técnica, por isso existe hoje um grande número de produtos NAT que seguem definições diferentes entre si. Esta falta de padronização foi devido ao foco estar mais centrado na nova versão do protocolo IP (ipv6), que resolveria o problema de rápido crescimento da internet. O surpreendente é ver que hoje, transcorridos cerca de 20 anos, o ipv6 ainda está numa fase inicial de implantação e é o NAT que tem garantido o crescimento da internet.

E pior, a mesma resistência que houve no passado para padronizar o NAT está ocorrendo de novo agora, quando se busca interconectar as LANs em ipv4 com a internet em ipv6.

1.3 – Conceitos adicionais: *masquerading*, DNAT, SNAT

Masquerading: *IP masquerade* (IP mascarado) é uma técnica de mascaramento de endereço IP similar ao NAT um para muitos. É basicamente apenas uma questão de nomenclatura diferente.

DNAT: *Destination Network Address Translation* (*tradução de endereço de rede de destino*) é uma técnica para transparentemente alterar o endereço IP de destino (e não o endereço de origem

como no NAT) do datagrama ao passar pelo roteador, e depois, quando do retorno do datagrama, desfazer esta alteração. Tem semelhança com *port forward*, a diferença é que atua no endereço IP de destino e não na porta do serviço. No entanto, em muitos casos, DNAT também pode modificar a porta de destino. A figura 3, abaixo, ilustra um caso de uso do DNAT, onde o host C tenta acessar o serviço web em 172.16.1.8 mas é transparentemente redirecionado para o serviço web em 10.10.1.5.

SNAT: *Source Network Address Translation* (tradução de endereço de rede na origem) é também uma técnica de NAT conforme descrito acima, porém normalmente somente é usada para modificar o endereço de destino do datagrama originado dentro de uma rede interna que esteja sendo encaminhado para a internet.

Nos conceitos acima para DNAT e SNAT, é importante notar que a definição é dependente do referencial, faz diferença se a conexão parte de um *host* dentro de uma LAN ou o oposto.

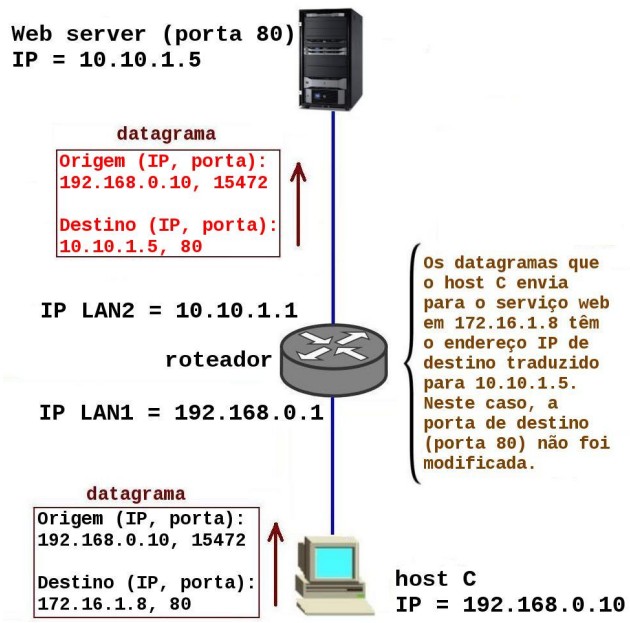

Fig. 3 - DNAT: o host C endereça o datagrama para o IP de destino 172.16.1.8, porém o roteador faz DNAT e modifica o endereço de destino para 10.10.1.5.

2 – PAT ou NAPT (*Port Address Translation*)

Um conceito relacionado a NAT, porém ligeiramente diferente, é o PAT (*Port Address Translation*, tradução de endereço de porta) ou NAPT (*Network Address Port Translation*, tradução de endereço de porta de rede).

PAT é técnica de tradução de endereço de porta. No exemplo ao lado, o host D tenta acessar o servidor web no IP 10.10.1.6:80 (porta web padrão, 80), porém na realidade o serviço está na porta 8000.

Para que o cliente possa então acessar o serviço, ao passarem pelo roteador os pacotes de dados têm a porta traduzida de 80 para 8000.

É importante notar que, na prática, muitas vezes a tarefa de tradução pode envolver simultaneamente NAT e PAT, ou seja, o roteador pode alterar tanto o endereço IP de destino quanto a porta de destino do datagrama.

Outro aspecto a ser considerado, é que as portas de origem e de destino são definidas em campos do cabeçalho TCP ou UDP (camada 4), e não do cabeçalho IP (camada 3).

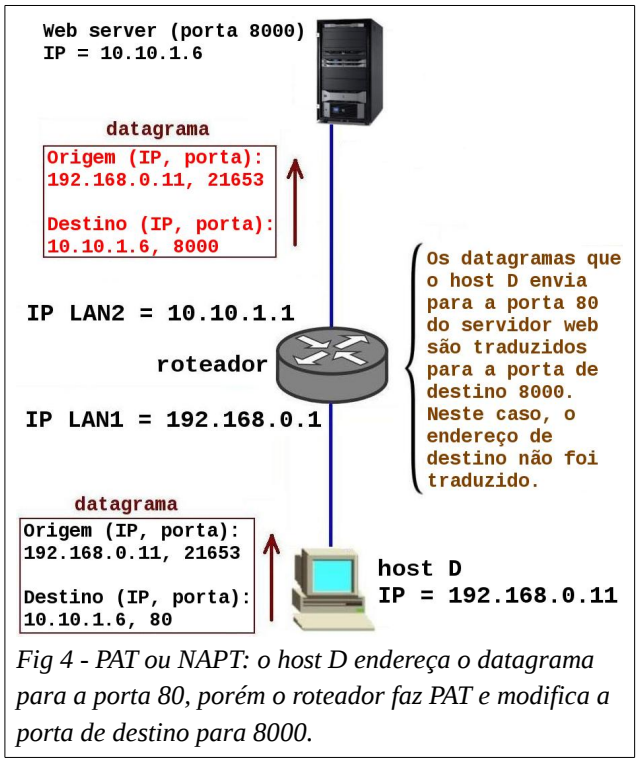

Fig 4 - PAT ou NAPT: o host D endereça o datagrama para a porta 80, porém o roteador faz PAT e modifica a porta de destino para 8000.