Dynamic NAT

2) Os únicos packets que foram traduzidos foram os que foram enviados do PC1. Pois apenas configuramos a nat pool com uma só public address. Como o PC1 foi o primeiro a fazer o ping, então foi oque ficou com a public address associada.

3) Agora que limpamos o pool nat do roteador, o PC2 é capaz de executar ping fora da rede privada, agora ficando associado com a única public address.

4) Ao definir o tempo limite NAT para 60 segundos, após 60 segundos de inatividade do PC1, o cronômetro inicia e ao atingir 0, o PC2 agora pode assumir a public address.

5) As vantagens são que muitos terminais de uma rede privada podem utilizar o mesmo endereço público, distinguindo cada ligação pela respetiva porta, preservando a segurança e a privacidade.

6) As ligações UDP são registadas, mesmo que a porta já tenha sido usada, mas ao usar TCP através de uma porta já em uso, a ligação anterior é substituída.

7) O PCA não consegue enviar um ping para nenhum terminal na rede privada.

8) Depois de configurar o endereço público estático para o PC1, o PCA consegue agora enviar um ping para ele.

O NAT/PAT é frequentemente necessário em cenários onde um dispositivo dentro de uma rede privada precisa de ser acessível a partir da internet pública. Por exemplo, se uma empresa hospedar o seu próprio site num servidor dentro da sua rede privada, usaria NAT/PAT estático para permitir que utilizadores da internet acedam a esse site. Também pode ser útil para redes domésticas, pois preserva o endereço privado de um terminal.

10) **ip dhcp**  
Inicialmente, temos um pacote DHCP Discovery, utilizado para verificar se o endereço IP está disponível, ao solicitar um pacote ARP. Em seguida, temos outro pacote DHCP Discovery, desta vez para validar se o endereço está mesmo disponível. Depois, temos um pacote DHCP Offer para informar o terminal de que pode usar esse endereço. A seguir, ocorre um pacote DHCP Request do terminal para o router, indicando que deseja usar aquele endereço. Por fim, há um pacote DHCP ACK (acknowledge) enviado pelo router ao terminal, confirmando que este utilizará o endereço.

**ip dhcp -r**  
Desta vez, temos apenas um DHCP Discovery, pois provém de um terminal que o serviço DHCP já conhece e ao qual já está associado um endereço IP. Os outros passos e pacotes são os mesmos que no comando anterior. Este comando é utilizado para renovar a concessão do IP.

**ip dhcp -x**  
O único pacote trocado é o DHCP Release, que informa o router de que o endereço IP em uso será libertado.

**ip dhcp**  
O procedimento é o mesmo que na primeira execução deste comando, mas agora o endereço IP é incrementado em 1 (de 192.168.1.101 para 192.168.1.102)

IPv6 Basic Mechanisms

1. Existem dois tipos de pacotes exibidos: ICMPv6 (IPv6) e MDNS. Primeiro, há uma solicitação da VM para o Switch em relação a um endereço IPv6 específico. Em seguida, o Switch "liberta" esse endereço IPv6, o que é mostrado através dos pacotes MDNS. O Switch tenta comunicar com um Router (através de uma Solicitação de Router), mas, como não há nenhum Router conectado, nada acontece.
2. Os pacotes capturados são semelhantes aos encontrados no exercício anterior, mas desta vez, como há um router para comunicar, obtemos pacotes de Router Advertisement e pacotes CDP, que indicam onde o Router está conectado e confirmam que há ligação entre a VM e o Router.
3. O endereço IPv6 foi obtido pelos seguintes passos:

O Router envia uma mensagem para a VM

Uma solicitação do Router para a VM em relação a esse endereço IPv6 específico;

Outra mensagem do Router indicando que o endereço está disponível e pode ser utilizado;

Um anúncio da VM para o Router para confirmar que o endereço IPv6 será utilizado pela VM.

1. 1ª **Protocolo de Descoberta de Vizinhos (NDP)**: Substitui o ARP do IPv4 e é responsável por várias funções, incluindo a resolução de endereços e a descoberta de vizinhos.

2º **Solicitação de Vizinhos (Neighbor Solicitation)**:

Quando um dispositivo precisa saber o endereço MAC de outro dispositivo na mesma rede local, envia uma mensagem de Solicitação de Vizinhos.

Esta mensagem contém o endereço IPv6 do destino.

3º **Resposta de Vizinhos (Neighbor Advertisement)**:

O dispositivo que recebe a Solicitação de Vizinhos responde com uma mensagem de Resposta de Vizinhos, que inclui o seu endereço MAC.

**4º) Atualização da Tabela de Vizinhos**:

O dispositivo que fez a solicitação atualiza a sua tabela de vizinhos com o endereço MAC recebido, permitindo a comunicação direta.

**5º) Deteção de Endereços Duplicados (DAD)**:

Antes de um dispositivo usar um endereço IPv6, verifica se já está em uso por outro dispositivo na rede.