Protocolos de Comunicação
2019-2020

Ficha prática 2 – Network Address Translation

Objetivos e organização

A presente ficha prática tem por objetivo tomar contacto com um tópico de grande importância nas redes de hoje em dia, nomeadamente com a utilização de endereços privados em redes internas como forma de preservar o espaço de endereçamento IPv4.

A ficha poderá ser preparada em ambiente de emulação (utilizando o simulador GNS3), antes de ser testada em ambiente laboratorial na aula. A ficha é composta por exercícios guiados, para os quais se indicam os comandos a executar, e por exercícios abertos, isto é, exercícios cuja resolução exigirá pesquisa e concretização autónomas.

Nesta ficha serão abordados os seguintes tópicos

- Configuração e utilização de Network Address Translation (NAT) em redes locais com *routers* Cisco

Ao longo da execução da ficha deverão ser guardados os resultados dos comandos digitados e os ficheiros de configuração elaborados, de forma a possibilitar a sua análise pelo docente. Para além desses resultados, deverá dar especial atenção à interpretação e análise decorrentes não só do trabalho realizado nas aulas como do estudo extra-aula subjacente a esta ficha.

Deve ter em atenção que a execução das fichas práticas pode exigir a colaboração entre grupos de trabalho, de modo a serem construídos cenários com dimensão e funcionalidades adequadas ao estudo das questões em análise. Mais importante do que a simples configuração individual dos *routers* dos diversos cenários é a interpretação dos resultados obtidos, quer no(s) *router*(s) sob direta responsabilidade do seu grupo quer no conjunto das redes, interpretação essa que constitui um fator fundamental na avaliação.

A avaliação da ficha terá em conta as seguintes componentes e pesos:

- Preparação prévia da ficha – 10%
- Conhecimento da matéria – 30%
- Execução dos exercícios – 50%
- Autonomia – 10%

1. Network Address Translation

O *Network Address Translation* (NAT) foi definido em 1994 no RFC 1631 (http://www.ietf.org/rfc/rfc1631.txt), com o objectivo de dar resposta à crescente escassez de endereços IPv4. A ideia básica do NAT é a de permitir que máquinas de redes locais que utilizem as gamas de endereços privados definidas no RFC 1918 (http://www.ietf.org/rfc/rfc1918.txt) possam comunicar com o exterior. Para tal, o *router* (ou *firewall*) de acesso ao exterior substitui o endereço privado das máquinas da rede interna por um endereço público.

Subjacente ao NAT, estão os conceitos de 'inside', 'outside', endereço local e endereço global. O 'inside' é a rede na qual são utilizados os endereços privados. O 'outside' corresponde, normalmente, à rede com endereços públicos, embora também se possa fazer NAT entre duas ou mais redes com endereços privados (como faremos durante a execução da presente ficha).

Os endereços do tipo 'inside local' são utilizados pelas máquinas da rede interna, para comunicação entre si. Sempre que uma máquina interna pretende comunicar com uma máquina externa, o seu endereço 'inside local' é traduzido para um endereço 'outside local'. Se uma máquina externa pretender comunicar com uma máquina interna tem que utilizar um endereço de destino 'inside global'. As máquinas externas comunicam entre si utilizando endereços 'outside global'.

Salienta-se, ainda, que o mapeamento entre endereços inside→outside pode ser de um para um, de N para um, de N para M, estático, ou dinâmico. Numa dada configuração poderemos ter mapeamentos de vários tipos (como veremos ao longo da execução da presente ficha).

1.1 Configuração básica de NAT

Analise o seguinte exemplo de configuração básica de NAT num *router*:

```
R1#config t
R1(config)#access-list 25 permit 192.168.100.0 0.0.0.255
R1(config)#ip nat inside source list 25 interface Ethernet0 overload
R1(config)#interface FastEthernet0
R1(config-if)#ip address 192.168.100.1 255.255.255.0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface Ethernet0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#ip nat outside
R1(config-if)#end
R1#
```

Neste exemplo é utilizada uma 'access list' que controla quais das máquinas da rede interna verão o seu endereço traduzido para um endereço externo. Neste caso, todas as máquinas da rede 192.168.100.0/24 serão alvo de tradução.

O comando 'ip nat inside source list 25 interface Ethernet0 overload' especifica, ainda, que o endereço externo a utilizar é o da interface Ethernet0 do *router* (ou seja, 172.16.1.1) e que todos os endereços 'inside local' serão convertidos no mesmo endereço 'outside local' que, neste caso, será o endereço 172.16.1.1. Tal é especificado através da *keyword* 'overload'. Visto que existe 'overload', o *router* faz distinção entre as máquinas internas através da utilização de diferentes portos (chama-se a isto *Port Address Translation*, PAT).

Ainda no exemplo acima, a interface FastEthernet0 é declarada como sendo 'inside' e a interface Ethernet0 é declarada como sendo 'outside'.

Exercício 1 – Com base no exemplo acima, configure o seu *router* de forma a que este funcione como servidor de NAT para a sua rede local, no cenário ilustrado na Figura 1. A configuração deverá ser elaborada de acordo com o seguinte:

- Solicite ao docente o valor a usar para as variáveis X e N, sendo N o número do seu grupo.
- A rede 'inside' tem o endereço 192.168.X.0/24.
- A interface Ethernet0 do router deve ser a interface 'inside' e deverá ter o endereço 192.168.X.254.
- A interface FastEthernet0 do router deve ser a interface 'outside' e deverá ter o endereço 10.254.0.N. Esta interface deve ser ligada à rede do laboratório, que tem o endereço 10.254.0.0/24.
- A access list deve permitir que todas as máquinas da rede interna tenham acesso ao NAT
- Deve ser utilizado um único endereço 'outside local'.
- O computador a ligar à rede 'inside' deverá ser manualmente configurado com o endereço 192.168.X.100.
- Verifique a conectividade do computador para o exterior, fazendo 'ping' desde este computador para o servidor do laboratório (cujo endereço IP é 10.254.0.254). Na consola deste servidor verifique qual o endereço IP 'outside local' usado pela sua máquina.
- Com base nas suas observações, explique quais as ações executadas pelo router, em termos de endereçamento, ao receber e reencaminhar os pacotes ICMP gerados pelo 'ping'.

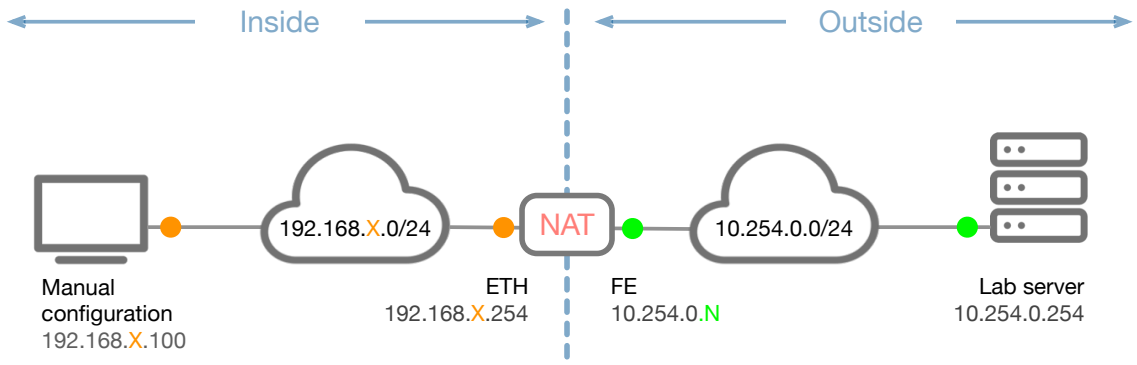


Figura 1 – Cenário básico de NAT

1.2 Atribuição estática e dinâmica de endereços

Analise o seguinte exemplo de configuração de NAT num *router*, onde alguns endereços são atribuídos de forma estática e outros de forma dinâmica:

```
R1#config t
R1(config)#access-list 25 deny 192.168.100.35 0.0.0.0
R1(config)#access-list 25 deny 192.168.100.36 0.0.0.0
R1(config)#access-list 25 permit 192.168.100.0 0.0.0.255
R1(config)#ip nat inside source static 192.168.100.35 172.16.1.50
R1(config)#ip nat inside source static 192.168.100.36 172.16.1.51
R1(config)#ip nat pool POOLB 172.16.1.100 172.16.1.120 netmask
255.255.255.0
R1(config)#ip nat inside source list 25 pool POOLB overload
R1(config)#interface FastEthernet0
R1(config-if)#ip address 192.168.100.1 255.255.255.0
R1(config-if)#ip nat inside
```

```
R1(config-if)#exit
R1(config)#interface Ethernet0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#ip nat outside
R1(config-if)#end
R1#
```

A *access list* começa por excluir os endereços que vão ser alvo de mapeamento estático. Note-se que tal não seria necessário, pois o mapeamento estático de NAT tem precedência sobre o mapeamento dinâmico. No entanto, normalmente isso é feito por questões de clareza.

De seguida, são especificados os mapeamentos estáticos. O mapeamento dinâmico é feito com base na definição de uma *pool* de endereços (172.16.1.100 a 172.16.1.120) que será *overloaded* (isto é, se os endereços da *pool* se esgotarem vão ser reutilizados, encarregando-se o *router* de os distinguir com base no mecanismo de PAT).

Exercício 2 – Altere a configuração de NAT efectuada no exercício anterior, de forma a que sejam definidos mapeamentos estáticos e dinâmicos, de acordo com o seguinte:

- A máquina com o endereço 192.168.X.200 da rede interna deve ter um mapeamento estático para o endereço 10.254.0.(N*16+1);
- Defina uma *pool* de endereços, de nome net-TESTE, com os endereços 10.254.0.(N*16+2) a 10.254.0.(N*16+5). Essa *pool* deve ser do tipo 'overload'.
- Todas as máquinas com endereço interno diferente de 192.168.X.200 devem ser mapeadas para a *pool* net-TESTE.
- Configure o seu PC com o endereço 'inside local' estático que definiu. Faça 'ping' para o servidor do laboratório. Na consola desse servidor verifique qual o endereço IP 'outside local' usado pela sua máquina.
- Re-configure o seu PC com um endereço diferente do endereço 'inside local' estático e repita o 'ping'. Qual o endereço IP usado pela sua máquina?

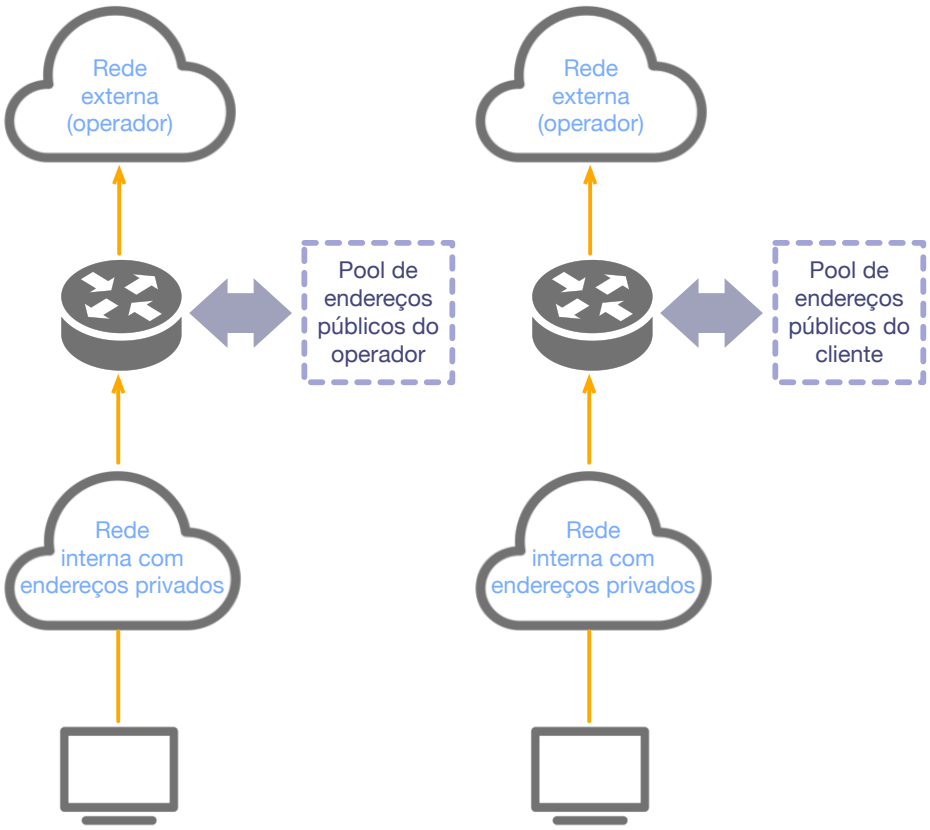
1.3 NAT com endereços públicos do cliente

Nos dois exercícios anteriores os endereços 'outside local' eram endereços da rede de *backbone* do laboratório, ou seja, num cenário real seriam endereços da rede de um ISP fornecidos por este a um seu cliente. Neste caso, representado esquematicamente na Figura 2a), todas as máquinas da rede do cliente aparecem como se fossem máquinas da rede do ISP (pois usam endereços dessa rede).

Nalguns casos, as organizações clientes já dispõem de endereços públicos e pretendem que as comunicações de a para as suas máquinas apareçam como ligações de e para as suas gamas de endereços. Neste caso, representado esquematicamente na Figura 2b), a *pool* de NAT a utilizar no *router* deve ser uma *pool* de endereços públicos do cliente, e não uma *pool* de endereços públicos do ISP. Assim, todas as máquinas da rede do cliente aparecem como se fossem máquinas dessa rede e não da rede do ISP (pois usam endereços da rede do cliente).

No exemplo seguinte é apresentada uma configuração para NAT estático e NAT dinâmico, onde se assume que os endereços privados do cliente são mapeados para endereços públicos também do cliente. As diversas gamas de endereços utilizadas são as seguintes:

- 192.168.0.0/24 – rede interna do cliente
- 172.16.1.0/27 – rede de endereços válidos do cliente (nota: para efeitos do exemplo, considera-se que os endereços desta gama representam endereços válidos embora, de facto, sejam endereços RFC 1918)
- 10.254.0.0/24 – rede do operador



a) NAT com endereços públicos do ISP b) NAT com endereços públicos do cliente

Figura 2 – NAT com endereços públicos do ISP ou do cliente

```
!
! R1: Configuracao que combina NAT estático e dinâmico
! ================================================================
!
! Rede interna: 192.168.0.0/255.255.255.0
!      Enderecos fixos internos: 192.168.0.1 a 192.168.0.24
!
! Rede valida:  172.16.0.0/255.255.255.224
!      Enderecos validos fixos: 172.16.0.1 a 172.16.0.28
!      Enderecos validos para saida por PAT: 172.16.0.29 a 172.16.0.30
!
!

interface f0
   desc Rede interna onde ligam os PCs
   ip address 192.168.0.1 255.255.255.0
   ip nat inside

interface e0
   desc Rede externa
   ip address 10.0.0.1 255.0.0.0
   ip nat outside
   ip access-group 120 in

!
! Configuracao de NAT/PAT
! PAT para os PCs internos
ip nat pool net-TESTE 172.16.0.29 172.16.0.30 netmask 255.255.255.0
ip nat inside source list 1 pool net-TESTE overload
access-list 1 permit 192.168.x.0 0.0.0.255
```

No exemplo acima pode observar-se que os endereços 'outside local' são os do cliente (rede 172.16.0.0/24) e não os do operador (rede 10.0.0.0/24).

Exercício 3 – Adapte o exemplo anterior ao caso da sua rede interna, de acordo com o seguinte:

- Utilize como rede válida do cliente a rede 172.16.(X+N).0/24.
- Utilize como rede inválida (interna) do cliente a rede 192.168.X.0/24, tal como nos exercícios anteriores.
- Utilize como rede do operador a rede 10.254.0.0/24, existente no laboratório, tal como nos exercícios anteriores.
- Faça 'ping' para o servidor do laboratório. Na consola desse servidor verifique qual o endereço IP 'outside local' usado pela sua máquina.
- Explique o que se passa em termos de tradução de endereços neste cenário.

1.4 Informação de estado e de *debugging*

Existem vários comandos úteis que fornecem informação de estado e de *debugging*. Referem-se alguns deles no que se segue.

```
R1#show ip nat translation

R1#clear ip nat translation *

R1#show ip nat statistics

R1#clear ip nat statistics

R1#debug ip nat

R1#debug ip nat detailed
```

Exercício 4 – Experimente estes comandos. Observe e interprete os respetivos *outputs*.
