IP Protocol

NAT & NATP

PEDRO MARTINS

April 25, 2018

Contents

1 NAT

- NEtwork Address Translation
- efetua a tradução entre endereços privados e endereços públicos
  - permite mapear endereços privados, internos a uma rede, em endereços públicos, acessíveis através da Internet
- A associação entre endereços públicos e privados pode ser:
  - **estática**
  - **dinâmica**
- Os endereços NAT são **endereços privados**
  - Os pacotes enviados para estes destinos não são reencaminhados para as redes públicas
  - O BGP não anuncia estes endereços
  - RIP e OSPF sim

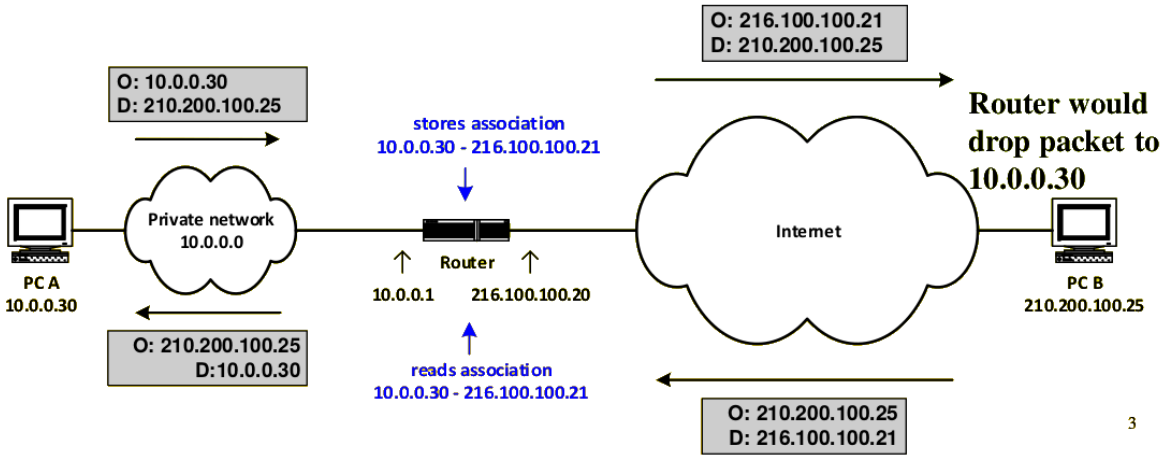


Figure 1: Exemplo de uma associação entre endereços públicos e privados

1.1 Associação Estática

- O mapeamento entre endereços NAT e endereços públicos é configurada estaticamente no router
- Permite que sejam iniciadas sessões nas duas direções

1.2 Associação Dinâmica

- O mapeamento entre endereços NAT e endereços públicos é efetuada automaticamente quando o primeiro pacote privado chega ao router NAT

1.3 Address Blocks

Table 1: Endereços NAT

Prefix	Endereço Mínimo	Endereço Máximo
10/8	10.0.0.0	10.255.255.255
172.16/12	172.16.0.0	172.31.255.255
192.168/16	192.168.0.0	192.168.255.255
169.254/16	169.254.0.0	169.254.255.255

1.4 Exemplo

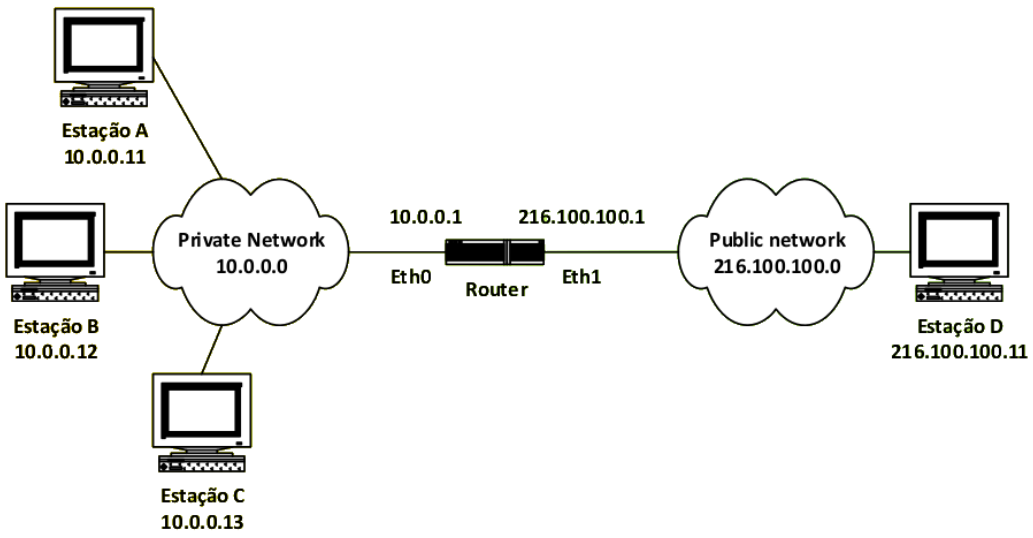
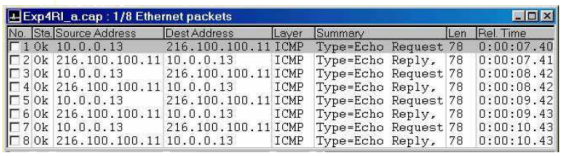


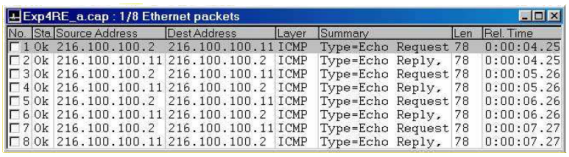
Figure 2: Exemplo de Associação Dinâmica em endereços NAT. Os endereços IP públicos utilizados são 216.100.100.2 e 216.100.100.3 para as associações NAT e 216.100.100.1 para a interface do router.

Se as estações tentarem fazer ping, acontece o seguinte:


Exp4RI_a.cap : 1/8 Ethernet packets

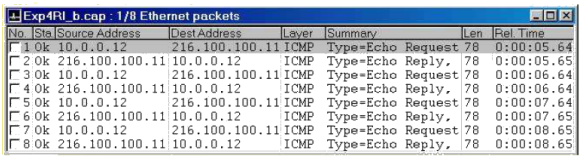
No.	Sta.	Source Address	Dest Address	Layer	Summary	Len	Rel. Time
1	Ok	10.0.0.13	216.100.100.11	ICMP	Type=Echo Request	78	0:00:07.40
2	Ok	216.100.100.11	10.0.0.13	ICMP	Type=Echo Reply,	78	0:00:07.41
3	Ok	10.0.0.13	216.100.100.11	ICMP	Type=Echo Request	78	0:00:08.42
4	Ok	216.100.100.11	10.0.0.13	ICMP	Type=Echo Reply,	78	0:00:08.42
5	Ok	10.0.0.13	216.100.100.11	ICMP	Type=Echo Request	78	0:00:09.42
6	Ok	216.100.100.11	10.0.0.13	ICMP	Type=Echo Reply,	78	0:00:09.43
7	Ok	10.0.0.13	216.100.100.11	ICMP	Type=Echo Request	78	0:00:10.43
8	Ok	216.100.100.11	10.0.0.13	ICMP	Type=Echo Reply,	78	0:00:10.43

(a) Ping de 10.0.0.13 para 216.100.100.11. *Snipping* da rede Interna


Exp4RE_a.cap : 1/8 Ethernet packets

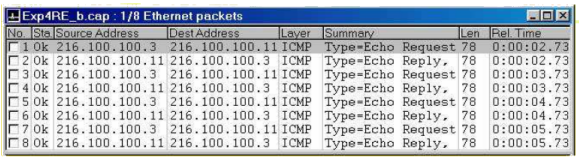
No.	Sta.	Source Address	Dest Address	Layer	Summary	Len	Rel. Time
1	Ok	216.100.100.2	216.100.100.11	ICMP	Type=Echo Request	78	0:00:04.25
2	Ok	216.100.100.11	216.100.100.2	ICMP	Type=Echo Reply,	78	0:00:04.25
3	Ok	216.100.100.2	216.100.100.11	ICMP	Type=Echo Request	78	0:00:05.26
4	Ok	216.100.100.11	216.100.100.2	ICMP	Type=Echo Reply,	78	0:00:05.26
5	Ok	216.100.100.2	216.100.100.11	ICMP	Type=Echo Request	78	0:00:06.26
6	Ok	216.100.100.11	216.100.100.2	ICMP	Type=Echo Reply,	78	0:00:06.26
7	Ok	216.100.100.2	216.100.100.11	ICMP	Type=Echo Request	78	0:00:07.27
8	Ok	216.100.100.11	216.100.100.2	ICMP	Type=Echo Reply,	78	0:00:07.27

(b) Ping de 10.0.0.13 para 216.100.100.11. *Snipping* da rede Externa


Exp4RI_b.cap : 1/8 Ethernet packets

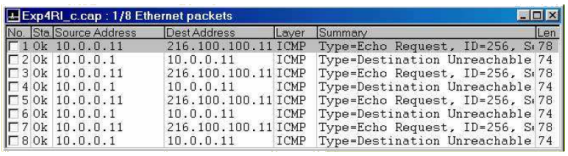
No.	Sta.	Source Address	Dest Address	Layer	Summary	Len	Rel. Time
1	Ok	10.0.0.12	216.100.100.11	ICMP	Type=Echo Request	78	0:00:05.64
2	Ok	216.100.100.11	10.0.0.12	ICMP	Type=Echo Reply,	78	0:00:05.65
3	Ok	10.0.0.12	216.100.100.11	ICMP	Type=Echo Request	78	0:00:06.64
4	Ok	216.100.100.11	10.0.0.12	ICMP	Type=Echo Reply,	78	0:00:06.64
5	Ok	10.0.0.12	216.100.100.11	ICMP	Type=Echo Request	78	0:00:07.64
6	Ok	216.100.100.11	10.0.0.12	ICMP	Type=Echo Reply,	78	0:00:07.65
7	Ok	10.0.0.12	216.100.100.11	ICMP	Type=Echo Request	78	0:00:08.65
8	Ok	216.100.100.11	10.0.0.12	ICMP	Type=Echo Reply,	78	0:00:08.65

(c) Ping de 10.0.0.12 para 216.100.100.11. *Snipping* da rede Interna


Exp4RE_b.cap : 1/8 Ethernet packets

No.	Sta.	Source Address	Dest Address	Layer	Summary	Len	Rel. Time
1	Ok	216.100.100.3	216.100.100.11	ICMP	Type=Echo Request	78	0:00:02.73
2	Ok	216.100.100.11	216.100.100.3	ICMP	Type=Echo Reply,	78	0:00:02.73
3	Ok	216.100.100.3	216.100.100.11	ICMP	Type=Echo Request	78	0:00:03.73
4	Ok	216.100.100.11	216.100.100.3	ICMP	Type=Echo Reply,	78	0:00:03.73
5	Ok	216.100.100.3	216.100.100.11	ICMP	Type=Echo Request	78	0:00:04.73
6	Ok	216.100.100.11	216.100.100.3	ICMP	Type=Echo Reply,	78	0:00:04.73
7	Ok	216.100.100.3	216.100.100.11	ICMP	Type=Echo Request	78	0:00:05.73
8	Ok	216.100.100.11	216.100.100.3	ICMP	Type=Echo Reply,	78	0:00:05.73

(d) Ping de 10.0.0.12 para 216.100.100.11. *Snipping* da rede Externa


Exp4RI_c.cap : 1/8 Ethernet packets

No.	Sta.	Source Address	Dest Address	Layer	Summary	Len
1	Ok	10.0.0.11	216.100.100.11	ICMP	Type=Echo Request, ID=256, S	78
2	Ok	10.0.0.1	10.0.0.11	ICMP	Type=Destination Unreachable	74
3	Ok	10.0.0.11	216.100.100.11	ICMP	Type=Echo Request, ID=256, S	78
4	Ok	10.0.0.1	10.0.0.11	ICMP	Type=Destination Unreachable	74
5	Ok	10.0.0.11	216.100.100.11	ICMP	Type=Echo Request, ID=256, S	78
6	Ok	10.0.0.1	10.0.0.11	ICMP	Type=Destination Unreachable	74
7	Ok	10.0.0.11	216.100.100.11	ICMP	Type=Echo Request, ID=256, S	78
8	Ok	10.0.0.1	10.0.0.11	ICMP	Type=Destination Unreachable	74

(e) Ping de 10.0.0.11 para 216.100.100.11. *Snipping* da rede Interna

Figure 3: Exemplo de ping de estações numa rede interna para uma estação na rede externa e tradução de endereços NAT privados em endereços públicos. A figura 3e mostra o que acontece quando o router não possui mais endereços públicos para os quais possa transferir o endereço NAT privado.

O router possui um número fixo de endereços públicos, por isso é que a estação `10.0.0.11` não consegue aceder à rede pública porque todos os endereços públicos disponíveis estão a ser utilizados por outras máquinas.

As associações entre endereços privados e endereços públicos possuem um tempo máximo de vida (`timeout`), que no caso de inatividade de uma estação, garante a desassociação do endereço e respetiva libertação. # NATP - `NEtwork Address Port Translation` - para além da tradução de endereços (efetuada pelo `NAT`), efetua a tradução de portas UDP e TCP entre portas privadas e públicas - A associação entre endereços públicos ou privados por ser: - estática - dinâmica - É responsável por processar as mensagens de protocolos da camada de aplicação que usam endereços IP e portas TCP/UDP - p.e., o protocolo ftp - Só utiliza um endereço IP público - a multiplexagem é efetuada no uso das diferentes portas - O router é capaz de efetuar a distribuição dos pedidos por diferentes portas de destino para diferentes máquinas - O número da porta só é traduzido se for necessário e as estações não estão cientes do processo - A tradução de endereços IP tem de ser efetuada no interior de vários `application protocols` que referem as portas das ligações

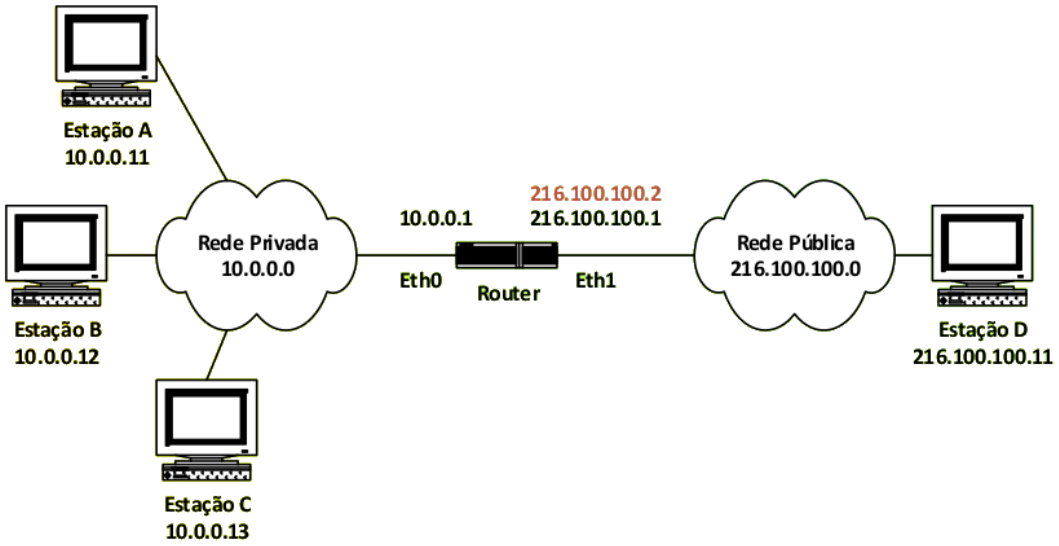
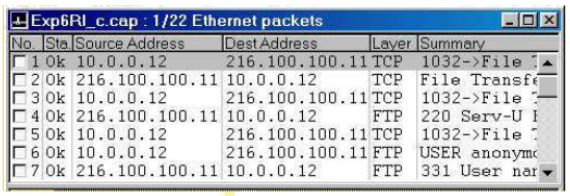
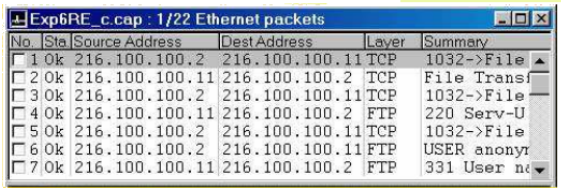


Figure 4: Exemplo de rede a correr o protocolo NATP. A estação D foi configurada como um servidor FTP ativo e os endereços públicos que estão a ser usados são `216.100.100.2` para as associações NAPT e `216.100.100.1` para a interface do router

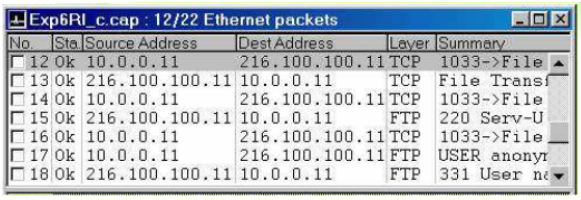
1.5 Exemplo sem necessidade de tradução de portas



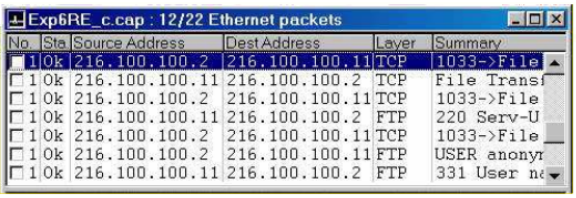
(a) Estação A acede o servidor FTP (estação D). *Snipping* da rede Interna



(b) Estação A acede o servidor FTP (estação D). *Snipping* da rede Externa



(c) Estação B acede o servidor FTP (estação D). *Snipping* da rede Interna



(d) Estação B acede o servidor FTP (estação D). *Snipping* da rede Externa

Figure 5: Exemplo da tradução de endereços no acesso de várias estações de uma rede interna para um servidor ftp externo, usando o protocolo NAPT. Nestas imagens não é mostrada a tradução de portas da rede interna para a rede externa, uma vez que as portas na rede interna são diferentes para as diferentes estações.

```
1 Router#show ip nat translation verbose
```

```
Pro Inside global         Inside local      Outside local       Outside global
tcp 216.100.100.2:1032    10.0.0.12:1032    216.100.100.11:21   216.100.100.11:21
    create 00:00:35, use 00:00:24, left 23:59:35,
    flags:
extended, use_count: 0

tcp 216.100.100.2:1033    10.0.0.11:1033    216.100.100.11:21   216.100.100.11:21
    create 00:00:12, use 00:00:06, left 23:59:53,
    flags:
extended, use_count: 0
```

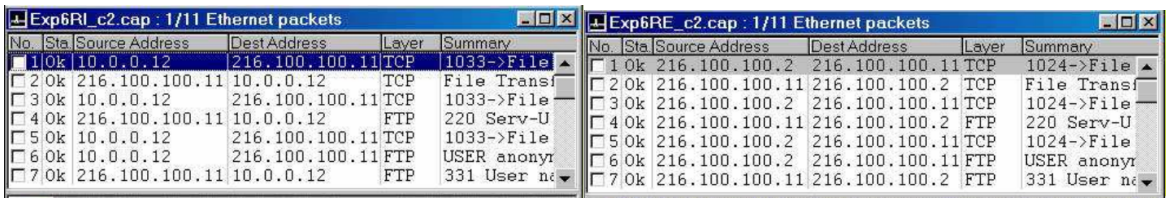
No exemplo apresentado não existe a necessidade de traduzir as portas do `sender`, porque elas já são diferentes na rede interna:

- A estação A está a usar a porta 1032
- A estação B está a usar a porta 1033

Só a porta de destino é que é a mesma, e pertence às *Well-known ports (wkp)*

Se estão duas máquinas a aceder ao mesmo serviço e o servidor de envio é o mesmo. Uma vez que o IP de envio (IP público) é o mesmo, os portos de ligação de cada uma delas têm de ser diferentes.

1.6 Exemplo com necessidade de tradução de portas



(a) Estação B acede pela segunda vez o servidor FTP (estação D). *Snipping* da rede Interna

(b) Estação B acede pela segunda vez o servidor FTP (estação D). *Snipping* da rede Externa

Figure 6: Exemplo da tradução de endereços no 2º acesso da estação B ao servidor ftp externo, usando o protocolo NAPT. Nestas imagens é mostrada a tradução de portas da rede interna para a rede externa, uma vez que as porta usada pela estação B na transação passada ainda está ativa, o router é obrigado a efetuar a tradução de portas entre a rede rede interna e a rede externa, uma vez que a porta 1033 já foi usada em conexões passadas.

A estação B não sabe que a sua porta foi traduzida.

```
Router#show ip nat translation verbose
Pro Inside global         Inside local      Outside local       Outside global
tcp 216.100.100.2:1024    10.0.0.12:1033    216.100.100.11:21   216.100.100.11:21
create 00:00:49, use 00:00:42, left 23:59:17,
    flags:
```

```
6       extended, use_count: 0
7
8   tcp 216.100.100.2:1032   10.0.0.12:1032   216.100.100.11:21   216.100.100.11:21
9   create 00:02:42, use 00:02:31, left 23:57:28,
10      flags:
11      extended, use_count: 0
12
13  tcp 216.100.100.2:1033   10.0.0.11:1033   216.100.100.11:21   216.100.100.11:21
14  create 00:02:18, use 00:02:13, left 23:57:46,
15      flags:
16      extended, use_count: 0
```

- O uso da opção verbose permite mostrar o `creation time`