

Redes Privadas NAT & NAT

Redes e Serviços

**Licenciatura em Engenharia Informática
DETI-UA**

NAT (Network Address Translation) e NAPT (Network Address Port Translation)

Port

Em casa utilizamos muitos, mas
quando sai de casa ele fica com
o router de saída

- NAT – faz a tradução entre endereços privados e públicos
- NAPT – para além dos endereços, faz a tradução entre números de porto UDP ou TCP
- As associações entre endereços públicos e privados podem ser estáticas ou dinâmicas
- É necessário processar também as mensagens dos protocolos de aplicação que passam endereços IP e números de porto UDP ou TCP (é o caso do FTP)

↳ Para além de troca no
cabeçalho precisa de
troca no pacote



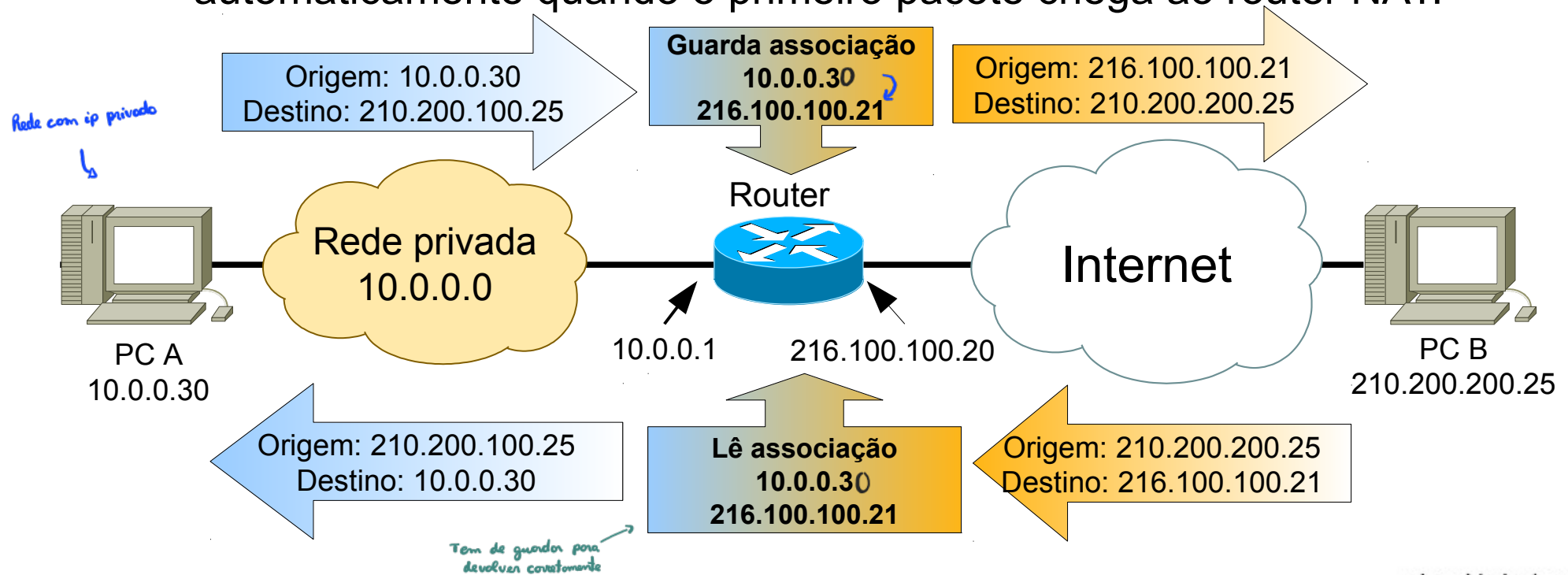
Associações NAT

- Associação estática:

- a correspondência entre endereço NAT e endereço público é configurada estaticamente no router NAT → Assim pode ser feita nos dois sentidos!,,
* e.g.: ter um servidor em casa
 - permite que as sessões possam ser iniciadas nos dois sentidos
- Se precisarmos da comunicação de fora para dentro a associação tem de ser estática!,,

- Associação dinâmica:

- a correspondência entre endereço NAT e endereço público é feita automaticamente quando o primeiro pacote chega ao router NAT:



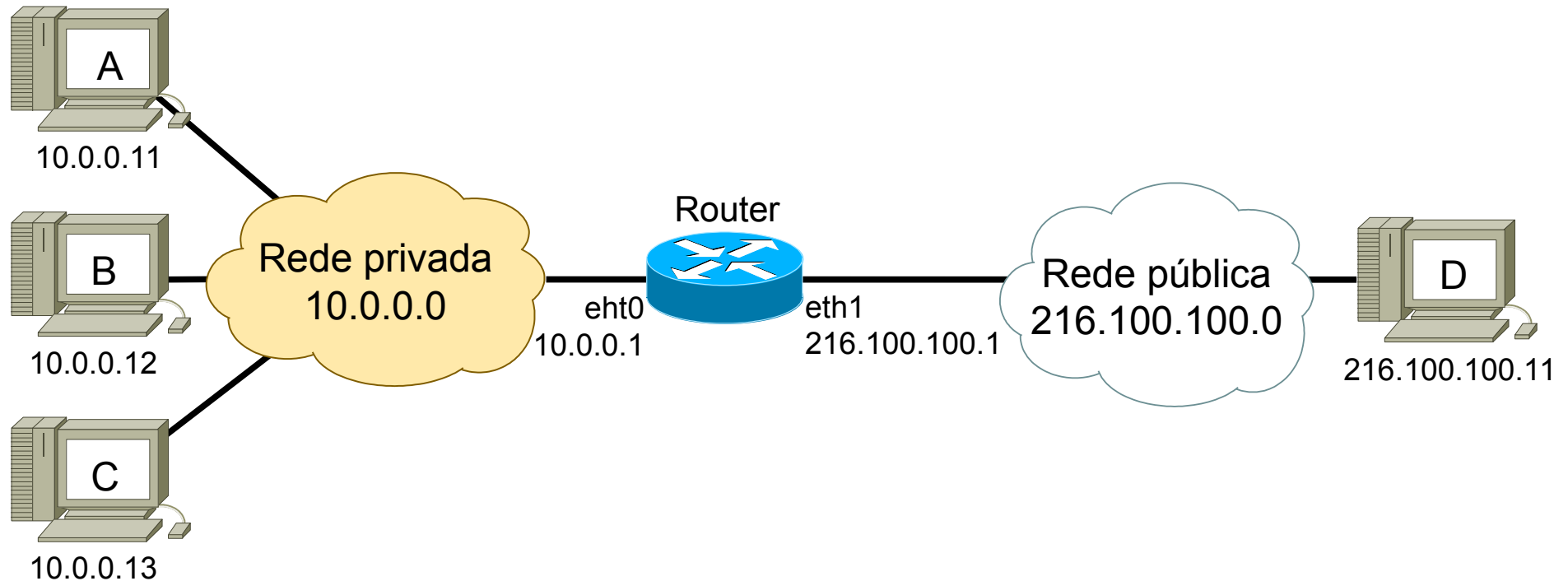
Blocos de endereços NAT

Prefixo	Endereço mais baixo	Endereço mais alto
10.0.0.0/8	10.0.0.0	10.255.255.255
172.16.0.0/12	172.16.0.0	172.31.255.255
192.168.0.0/16	192.168.0.0	192.168.255.255
169.254.0.0/16	169.254.0.0	169.254.255.255

- Os endereços NAT são endereços privados *{ os endereços privados nunca podem ir para a internet*
- Os pacotes para estes destinos não são encaminhados na rede pública



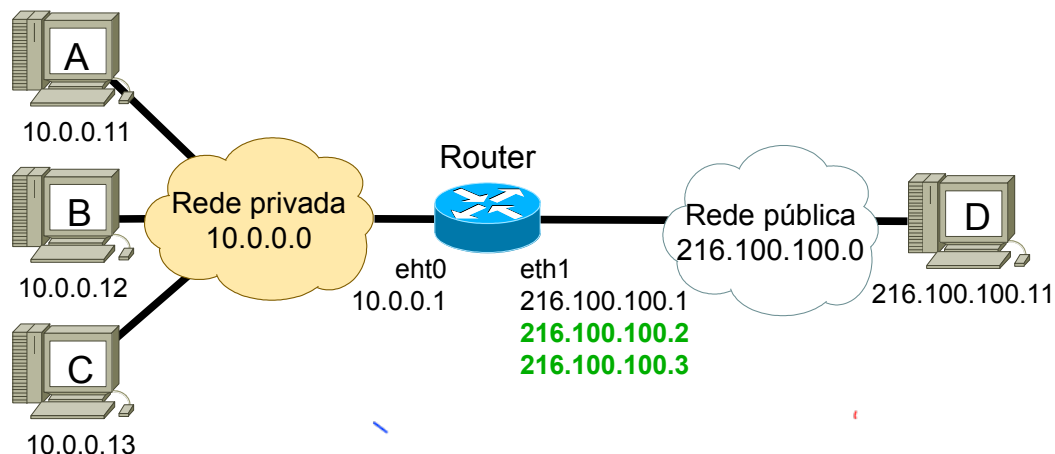
Exemplos – NAT (I)



- Router configurado com associação dinâmica de endereços
- Endereços IP públicos usados: *Pode com 2 endereços ! //*
 - ♦ 216.100.100.2 e 216.100.100.3 para associações NAT
 - ♦ 216.100.100.1 para a interface do router

Exemplos – NAT (II)

Ping de 10.0.0.13 para 216.100.100.11:



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

rede privada

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

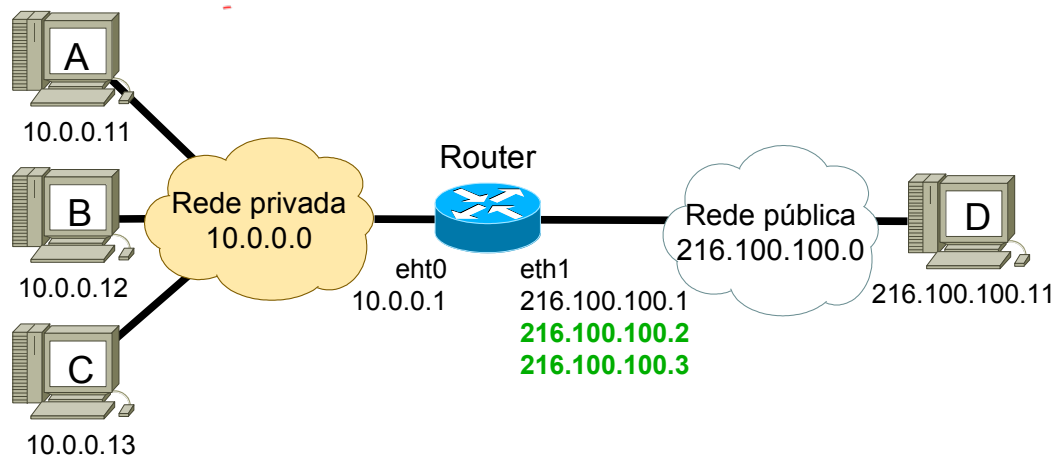
→ Ele comunica com o Router!

rede pública



Exemplos – NAT (III)

Ping de 10.0.0.12 para 216.100.100.11:



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

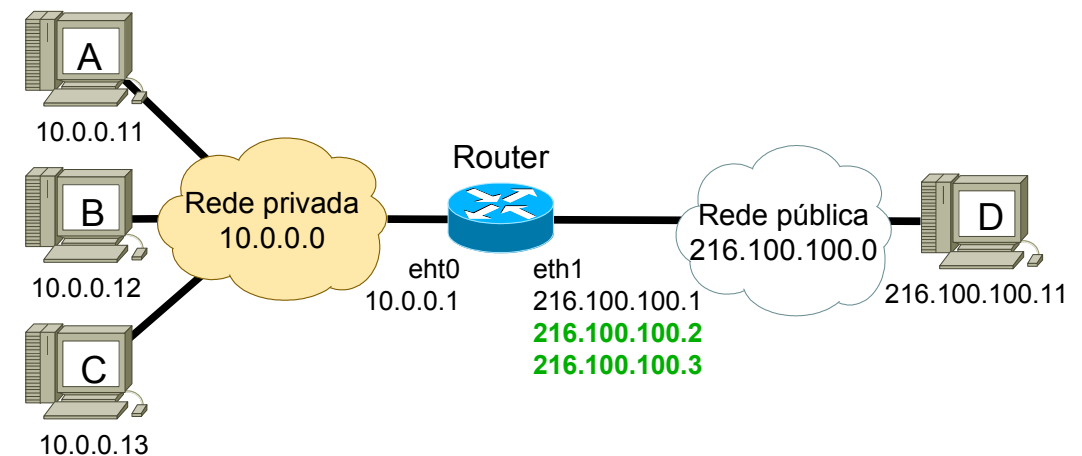
rede privada

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

rede pública

Exemplos – NAT (IV)



Ping de 10.0.0.11 para 216.100.100.11:

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	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	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	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	78
8	Ok	10.0.0.1	10.0.0.11	ICMP	Type=Destination Unreachable	74

Não existem endereços disponíveis!

rede privada

Acabou a Pool de endereços!!

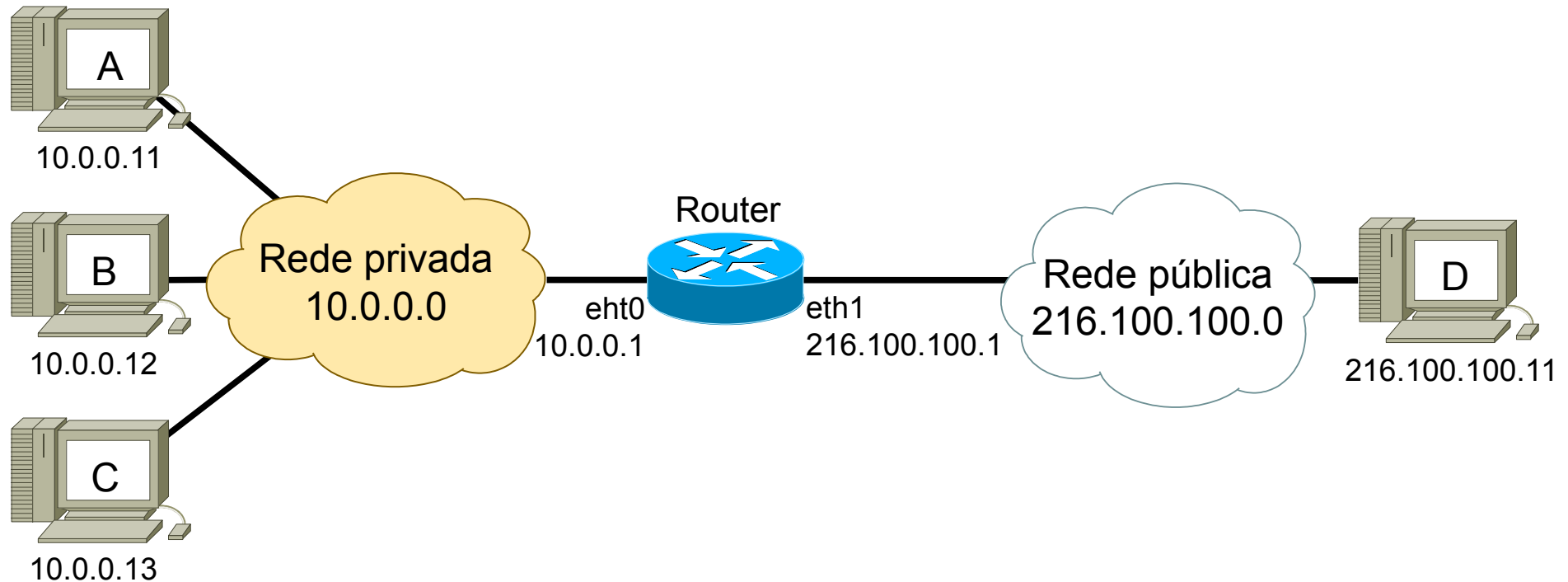
- A estação 10.0.0.11 não consegue aceder à rede pública porque todos os endereços disponíveis foram previamente associados
- As associações têm um tempo de vida (*timeout*) máximo de inactividade ao fim do qual são anuladas

*Nota que: endereços públicos custam dinheiro ...
→ esta solução não é muito económica!!*



Exemplos – NAPT (I)

with Port Translation



- Estação D configurada com um servidor FTP activo
- Endereços IP públicos usados:
 - 216.100.100.2 para associações NAPT
 - 216.100.100.1 para a interface do router

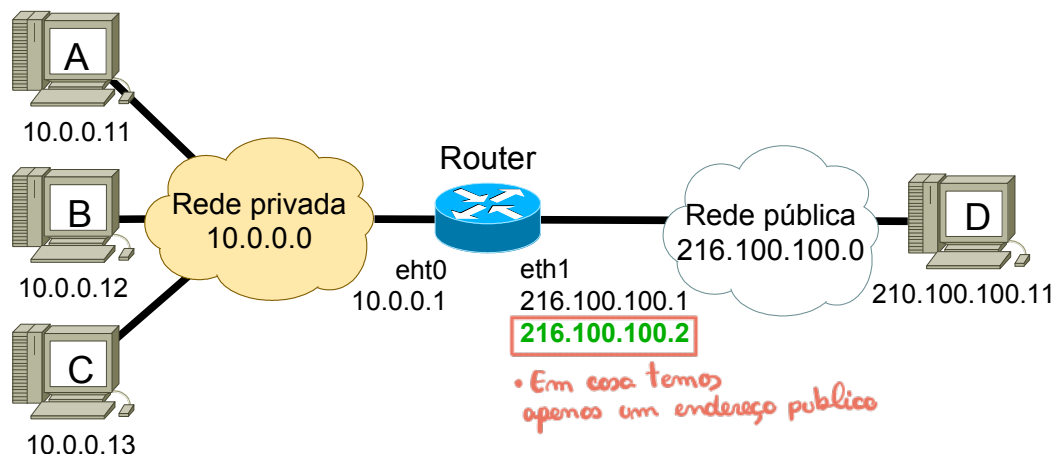
→ Apenas 1 endereço disponível ! Ele fez a distinção com os portos

← é recomendado !



Exemplos – NAT (II)

Acesso das estações B e A ao servidor FTP na estação D:



• Em casa temos apenas um endereço público

Mesmo ip mas portas diferentes

Porta diferente!!

No.	Sta.	Source Address	Dest Address	Layer	Summary
1	Ok	10.0.0.12	216.100.100.11	TCP	1032->File
2	Ok	216.100.100.11	10.0.0.12	TCP	File Transf
3	Ok	10.0.0.12	216.100.100.11	TCP	1032->File
4	Ok	216.100.100.11	10.0.0.12	FTP	220 Serv-U
5	Ok	10.0.0.12	216.100.100.11	TCP	1032->File
6	Ok	10.0.0.12	216.100.100.11	FTP	USER anonym
7	Ok	216.100.100.11	10.0.0.12	FTP	331 User nar

No.	Sta.	Source Address	Dest Address	Layer	Summary
12	Ok	10.0.0.11	216.100.100.11	TCP	1033->File
13	Ok	216.100.100.11	10.0.0.11	TCP	File Transf
14	Ok	10.0.0.11	216.100.100.11	TCP	1033->File
15	Ok	216.100.100.11	10.0.0.11	FTP	220 Serv-U
16	Ok	10.0.0.11	216.100.100.11	TCP	1033->File
17	Ok	10.0.0.11	216.100.100.11	FTP	USER anonym
18	Ok	216.100.100.11	10.0.0.11	FTP	331 User na

rede privada

No.	Sta.	Source Address	Dest Address	Layer	Summary
1	Ok	216.100.100.2	216.100.100.11	TCP	1032->File
2	Ok	216.100.100.11	216.100.100.2	TCP	File Transf
3	Ok	216.100.100.2	216.100.100.11	TCP	1032->File
4	Ok	216.100.100.11	216.100.100.2	FTP	220 Serv-U
5	Ok	216.100.100.2	216.100.100.11	TCP	1032->File
6	Ok	216.100.100.2	216.100.100.11	FTP	USER anonym
7	Ok	216.100.100.11	216.100.100.2	FTP	331 User na

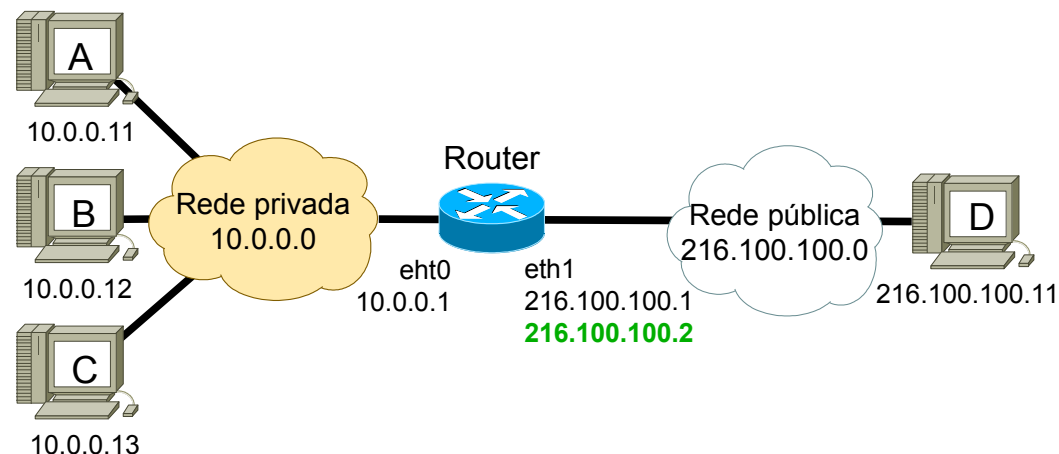
No.	Sta.	Source Address	Dest Address	Layer	Summary
10k	Ok	216.100.100.2	216.100.100.11	TCP	1033->File
10k	Ok	216.100.100.11	216.100.100.2	TCP	File Transf
10k	Ok	216.100.100.2	216.100.100.11	TCP	1033->File
10k	Ok	216.100.100.11	216.100.100.2	FTP	220 Serv-U
10k	Ok	216.100.100.2	216.100.100.11	TCP	1033->File
10k	Ok	216.100.100.2	216.100.100.11	FTP	USER anonym
10k	Ok	216.100.100.11	216.100.100.2	FTP	331 User na

rede pública



Exemplos – NAT (III)

Acesso das estações B e A ao servidor FTP na estação D:



```
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
```

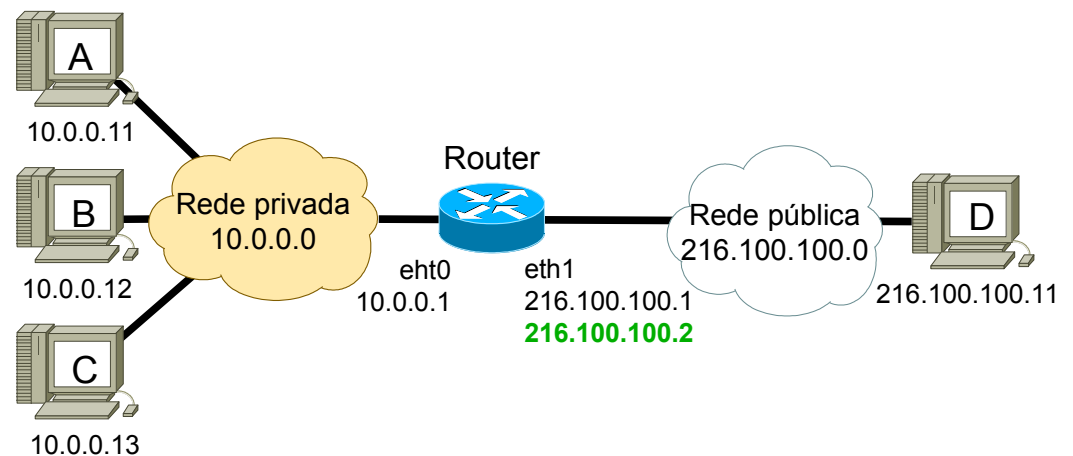
→ Não existe NAT aqui

↑
Porta do servidor

- Neste caso, não é necessário traduzir os números de porta origem porque eles são diferentes
 - ♦ A estação B usou o número de porta 1032
 - ♦ A estação A usou o número de porta 1033

Exemplos – NATP (IV)

Segundo acesso da estação B a servidor FTP na estação D:



O router vê que existe um conflito ip: porta e ele troca para outra porta...

```
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:				
extended, use_count: 0				
tcp	216.100.100.2:1032	10.0.0.12:1032	216.100.100.11:21	216.100.100.11:21
create 00:02:42, use 00:02:31, left 23:57:28, 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 00:02:18, use 00:02:13, left 23:57:46, flags:				
extended, use_count: 0				

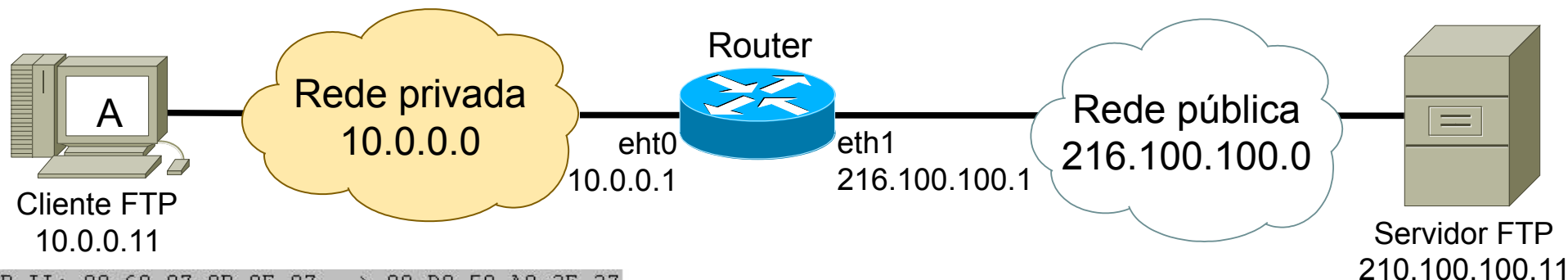
Escolhe um número do porto de saída!

A opção *verbose* permite mostrar o instante de criação e o instante da última utilização de cada entrada da tabela de tradução.

- Neste caso, é necessário traduzir o número de porto 1033 pois este número é presentemente usado numa ligação TCP anterior



Exemplos – NAT (V)



Tradução de endereços IP no interior de pacotes FTP:

```
ETHER-II: 00-60-97-9B-9E-07 ==> 00-D0-58-A9-3E-37
Internet Protocol
  Version(MSB 4 bits): 4
  Header length(LSB 4 bits): 5 (32-bit word)
  Service type: Preced=Routine,Delay=Normal,Thrput=Normal,Reli=Normal
  Total length: 61 (Octets)
  Fragment ID: 14595
  Flags: Do not fragment,Last fragment,Offset=0 (0x00)
  Time to live: 128 seconds/hops
  IP protocol type: TCP (0x06)
  Checksum: 0x7B3D
  IP address 10.0.0.11 ->216.100.100.11
  No option
TCP: 1036->File Transfer (Control),S=82367,A=171360,W=86
File Transfer Protocol
  PORT 10,0,0,11,4,13 -> Porta: 0000 0100:0000 1101, = 1024 + 13 = 1037
Sliced Packet( Data Length = 75)
```

IP

rede privada

12-se byte
a byte

Tivemos de ir
dentro do próprio
pacote e mudar
o IP

```
ETHER-II: 00-D0-58-A9-3E-38 ==> 00-60-97-D4-9F-9A
Internet Protocol
  Version(MSB 4 bits): 4
  Header length(LSB 4 bits): 5 (32-bit word)
  Service type: Preced=Routine,Delay=Normal,Thrput=Normal,Reli=Normal
  Total length: 65 (Octets)
  Fragment ID: 14595
  Flags: Do not fragment,Last fragment,Offset=0 (0x00)
  Time to live: 127 seconds/hops
  IP protocol type: TCP (0x06)
  Checksum: 0x49DD
  IP address 216.100.100.2 ->216.100.100.11
  No option
TCP: 1036->File Transfer (Control),S=82367,A=171360,W=8610
File Transfer Protocol
  PORT 216,100,100,2,4,13
Sliced Packet( Data Length = 79)
```

Ip muda e a porta
mantém-se

rede pública