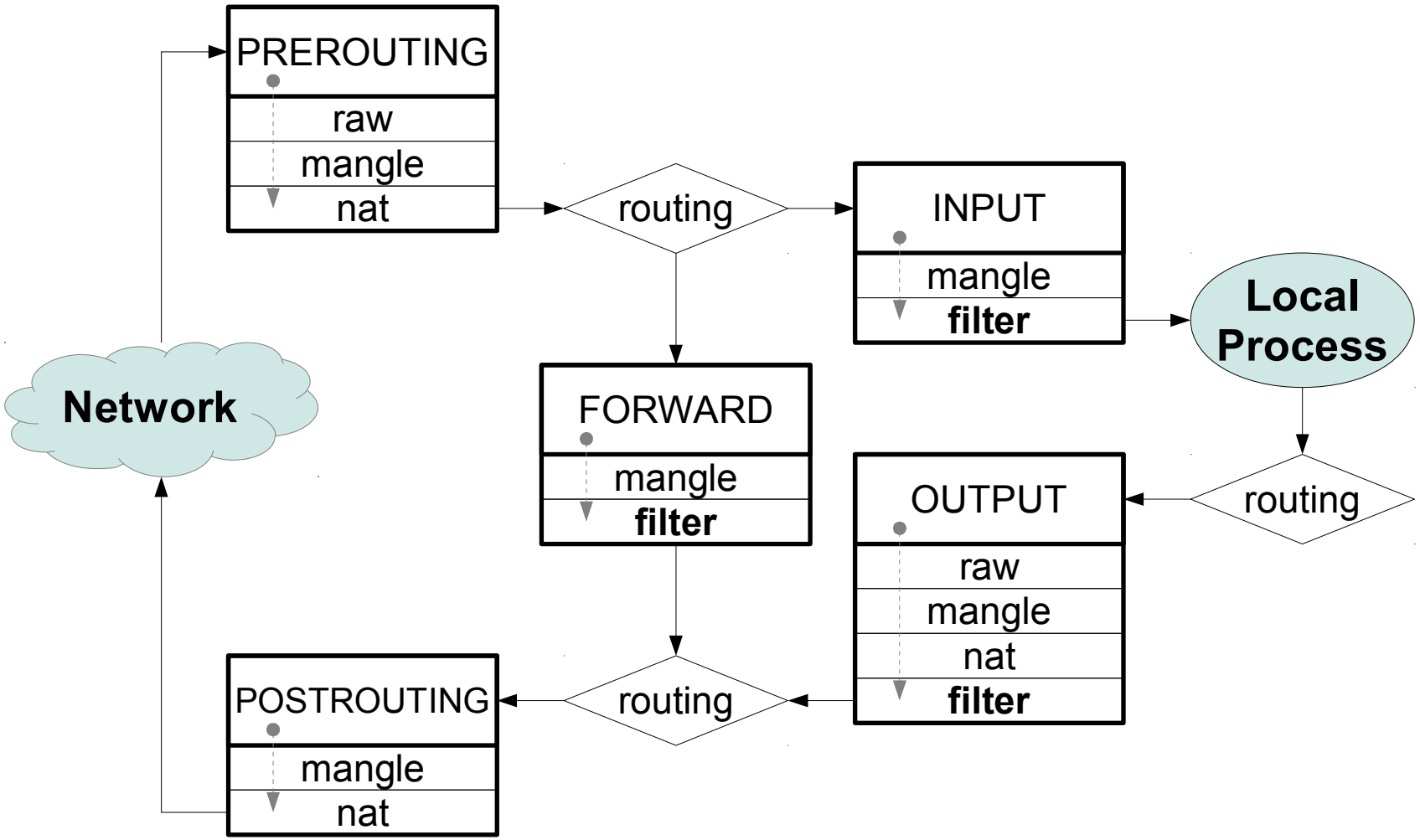
# Viagem dos pacotes no *iptables*

Miguel Frade

Departamento de Engenharia Informática
Instituto Politécnico de Leiria

October 23, 2012

# Viagem dos pacotes no iptables



# Tabelas

O iptables tem as seguintes tabelas:

- `raw` para configurar excepções ao sistema de monitorização dos estados `connection tracking`
- `mangle` para fazer alterações especializadas nos pacotes, nomeadamente:
  - `TOS` (type of service)
  - `TTL` (time to live)
- `nat` serve para fazer *Network Address Translation*
- `filter` onde se colocam as regras de filtragem, tabela pré-definida quando se omite a opção `-t`
  - `iptables [-t <tabela>]`

# Listas

E as seguintes listas (*chains*):

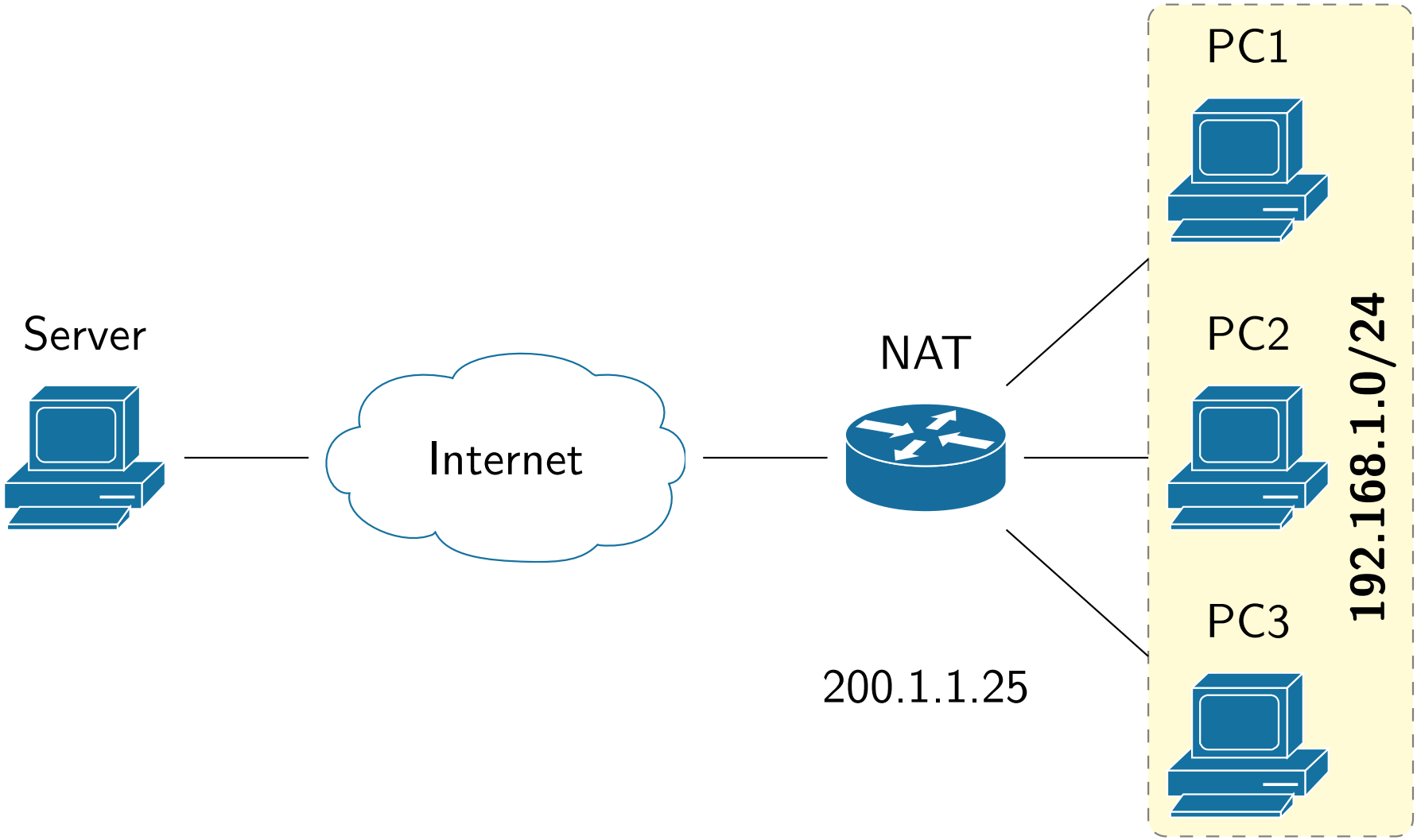
- `PREROUTING` antes de encaminhar
- `FORWARD` pacotes reencaminhados
- `INPUT` entrada de pacotes para um processo
- `OUTPUT` saída de pacotes de um processo
- `POSTROUTING` depois de encaminhar

# *Network Address Translation (NAT)*

Permite que vários computadores partilhem o mesmo IP

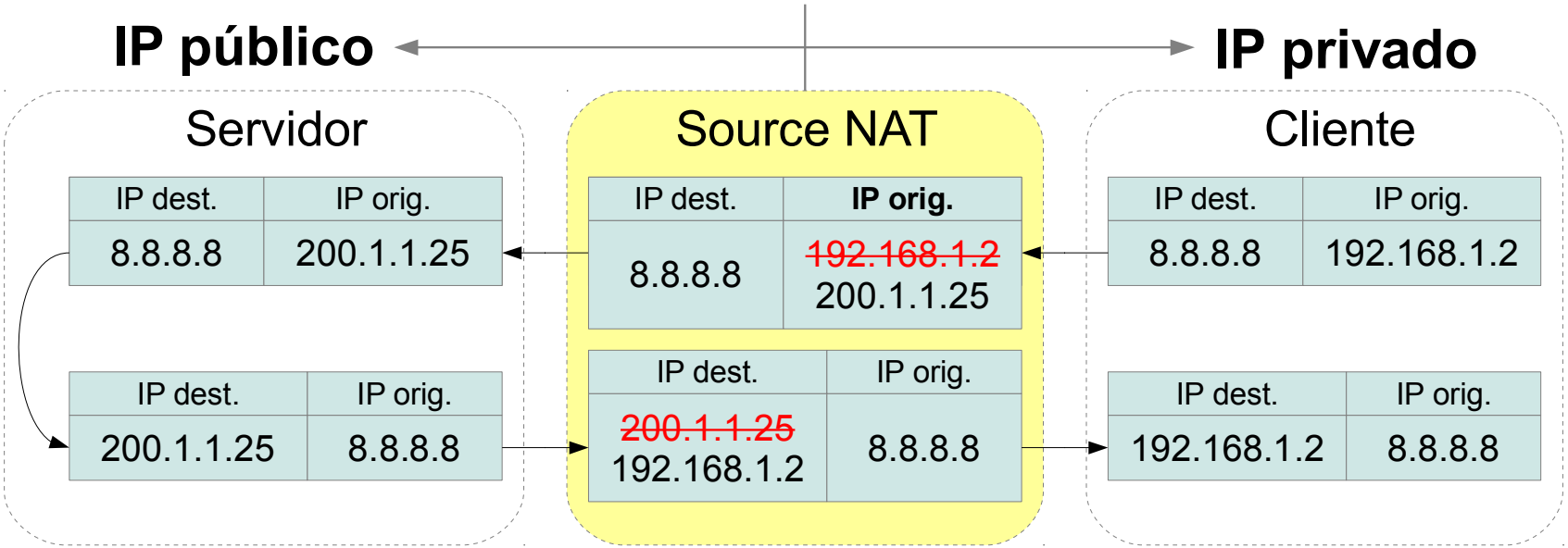
- muda os endereços IP de origem e/ou destino
- recalcula o `checksum` dos pacotes
- dois tipos de NAT
  - *Source Network Address Translation* (SNAT)
  - *Destination Network Address Translation* (DNAT)
  - estes nomes não são universais e existem mais designações, consultar ▸ Wikipedia: NAT

# Esquema NAT



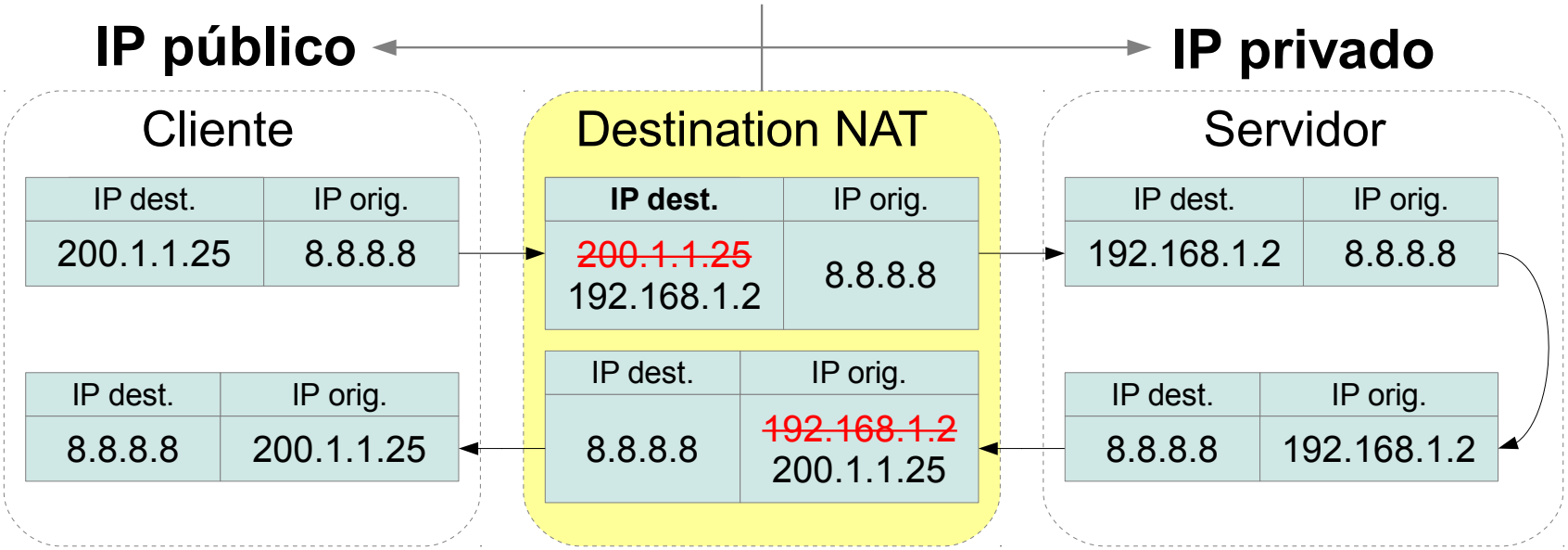
# Source NAT

- O cliente tem um endereço **IP privado**
- Liga-se a um servidor com endereço **IP público**
- O equipamento NAT troca o **IP de origem** do 1º pacote pelo seu **IP público**



# Destination NAT

- O cliente tem um endereço **IP público**
- Liga-se ao **IP público** do equipamento de NAT
- O equipamento NAT troca o **IP de destino** e reencaminha para o **IP privado** do servidor



# Alvo SNAT

`-j SNAT`

- Só é válido na tablea `nat` da lista `POSTROUTING`
- Especifica que o IP de origem deve ser mudado
- Suporta as seguintes opções
  - `--to-source ipaddr[-ipaddr][:port[-port]]` permite especificar um endereço IP e opcionalmente uma gama de portos se for especificado `-p tcp` ou `-p udp`
  - `--random` o mapeamento de portas será aleatório
  - `--persistent` dá ao cliente o mesmo endereço origem/destino para todas as ligações

# Alvo MASQUERADE

`-j MASQUERADE`

- Só é válido na tablea `nat` da lista `POSTROUTING`
- Equivalente ao `SNAT`, mas
- Só deve ser usado com IP dinâmicos, e.g. dialup (`ppp0`)
- Com IP estático deve-se usar o alvo `SNAT`
- Suporta as seguintes opções:
  - `--to-ports port[-port]` especifica uma gama de portas a usar, só é válido se for especificado `-p tcp` ou `-p udp`
  - `--random` o mapeamento de portas será aleatório

# Alvo DNAT

`-j DNAT`

- Só é válido na tabela `nat` das listas `PREROUTING` e `OUTPUT`
- Especifica que o IP de destino deve ser mudado
- Suporta as seguintes opções
  - `--to-destination [ipaddr][-ipaddr][:port[-port]]` permite especificar um endereço IP e opcionalmente uma gama de portos se for especificado `-p tcp` ou `-p udp`
  - `--random` o mapeamento de portas será aleatório
  - `--persistent` dá ao cliente o mesmo endereço origem/destino para todas as ligações

# Alvo REDIRECT

`-j REDIRECT`

- Só é válido na tabela `nat` das listas `PREROUTING` e `OUTPUT`
- Redirecciona os pacotes dirigidos à própria máquina para uma porta `TCP`/`UDP` diferente
- Usado para configurar proxies transparentes
- Suporta as seguintes opções:
  - `--to-ports port[-port]` especifica a porta de destino a usar, só é válido se for especificado `-p tcp` ou `-p udp`
  - `--random` as portas serão escolhidas aleatoreamente

## Exemplo

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT
    --to-port 8080
```

# Configurar sNAT no IPTABLES

Requisitos:

- Duas placas de rede `eth0` (ligada à Internet) e `eth1` (ligada à rede privada)
- Dizer ao kernel para permitir encaminhamento de pacotes

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

- Depois configurar o `iptables` para encaminhar os pacotes da interface interna para a externa

```
# Activar Source NAT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
# Reencaminhar pacotes, deixa sair TUDO
iptables -A FORWARD -i eth0 -o eth1 -m state --state
    RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -m state --state NEW -j
    ACCEPT
```

# Configurar dNAT no IPTABLES

Requisitos:

- Duas placas de rede `eth0` (ligada à Internet) e `eth1` (ligada à rede privada)
- Dizer ao kernel para permitir encaminhamento de pacotes (ver slide anterior)
- Depois configurar o `iptables` para encaminhar os pacotes da interface externa para a interna

```
# Activar NAT

iptables -t nat -A PREROUTING --dst ${EXTERNIP} -p tcp --dport
    22 -j DNAT --to-destination ${SSHHOST}
```