

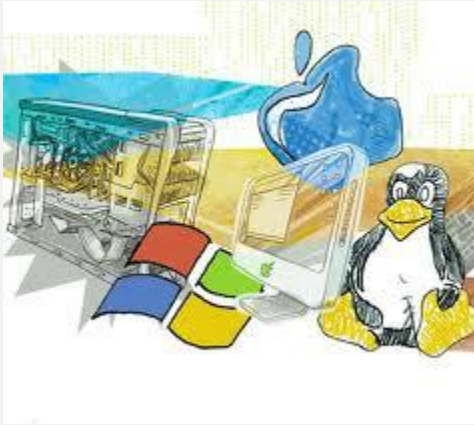
# Serviços de Rede 1

2019-2020

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática





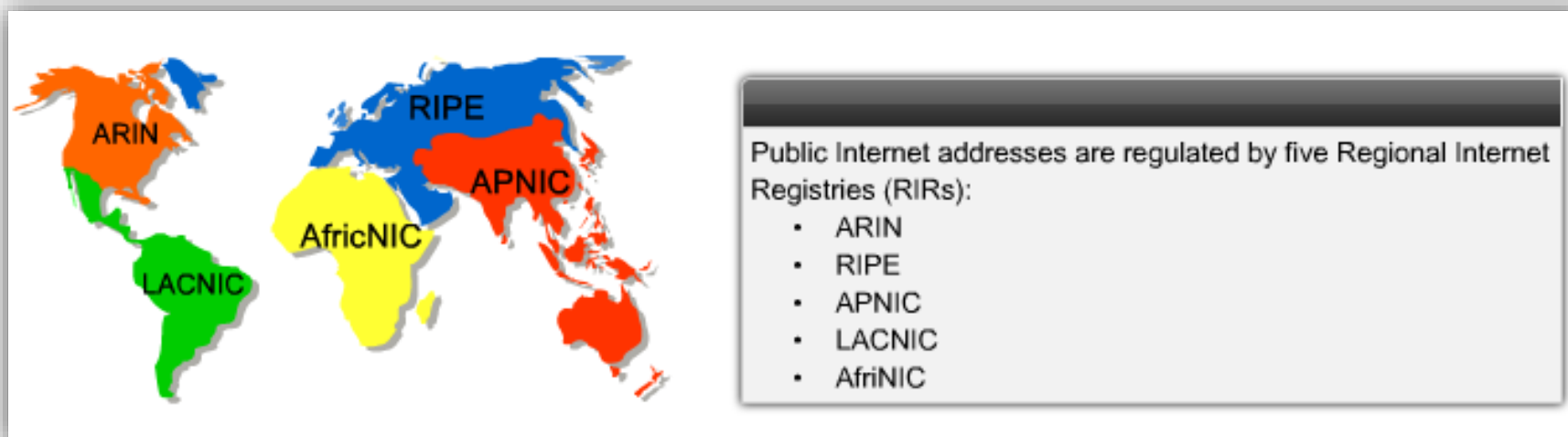
# Serviços de Rede 1

*NAT- Network Address Translation*

© - Pedro Geirinhas

# Endereços públicos

- Qualquer instituição ou empresa pode comprar ou alugar endereços IP ou gamas de IPs para atribuição a equipamentos que tenham a necessidade de acesso público.
  - O aluguer dos endereços pode ser solicitado aos ISP.
  - Os endereços IPs são disponibilizados aos ISP por entidades regionais a quem foi delegada essa competência.



# Endereços privados

- Existem 3 conjuntos de endereços que não podem ser atribuídos especificamente a um cliente, estando reservados para utilização em redes privadas:
  - São designados por “endereços privados”.
  - Podem ser usados por milhões de equipamentos em simultâneo.
  - Os pacotes contendo esses endereços **não podem** ser encaminhados para o exterior.

Class	Private IP Address Range	Public IP Address Range
Class A	10.0.0.0 – 10.255.255.255	1.0.0.0 – 9.255.255.255 11.0.0.0 – 126.255.255.255
Class B	172.16.0.0 – 172.31.255.255	128.0.0.0 – 172.15.255.255 172.32.0.0 – 191.255.255.255
Class C	192.168.0.0 – 192.168.255.255	192.0.0.0 – 192.167.255.255 192.169.0.0 – 223.255.255.255

Private Internet addresses are defined in RFC 1918:

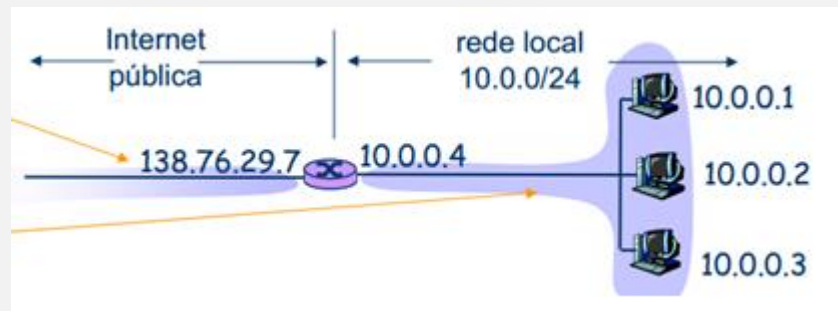
Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

# Endereços públicos e privados

- As máquinas com endereços privados não podem aceder directamente à internet.
- Os endereços públicos são um recurso limitado e atualmente escasso.
  - Não existem endereços suficientes para fazer face à quantidade de equipamentos que se encontram interligados.
- Contudo, as máquinas têm de aceder e ser acedidas através da internet.
- Soluções:
  - IP V6.
  - Máquinas intermédias a prestar os serviços pretendidos de forma indirecta (ex. *Proxys*).
  - **Tradução de endereços privados em endereços públicos (NAT).**

# Network Address Translation (NAT)

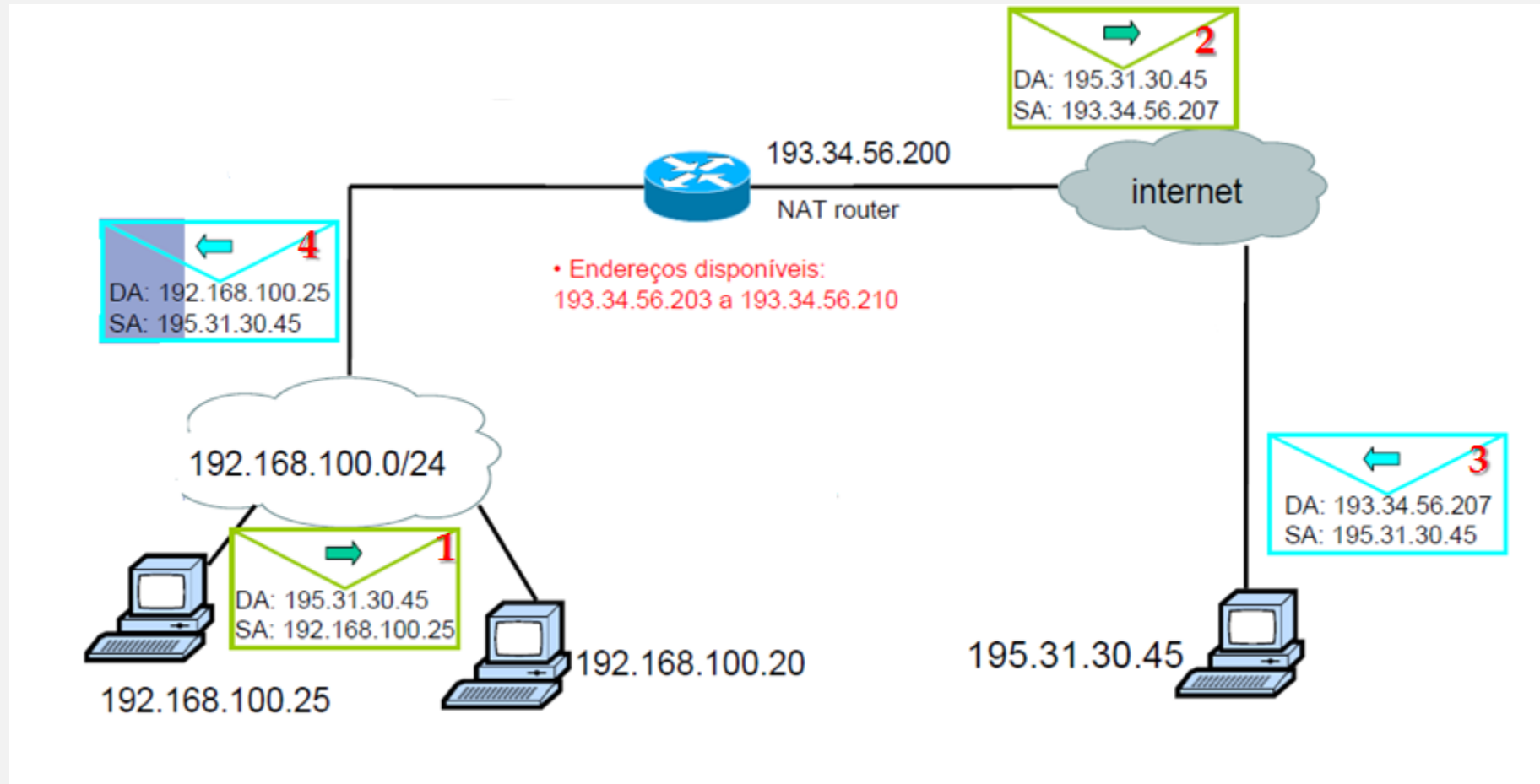
- Com o NAT (*Network Address Translation*) pode-se expandir o espaço de endereçamento IP através da utilização de endereços privados.



- Está regulamentado e definido nos seguintes RFCs:
  - 3022 – Traditional IP Network Address Translator (NAT).
  - 1918 – Address Allocation for Private Internet.



# NAT



# Vantagens

---

- Garante que os endereços privados não são passados para o domínio público.
- Garantem maior capacidade de gestão do espaço de endereçamento.
- Aumenta a flexibilidade do acesso a redes publicas.
- Garante uma gestão mais racional e eficiente do endereçamento público.
- Facilidade de mudança de ISP.
- Permite a criação de redes mais seguros e com maior garantia de privacidade de dados.



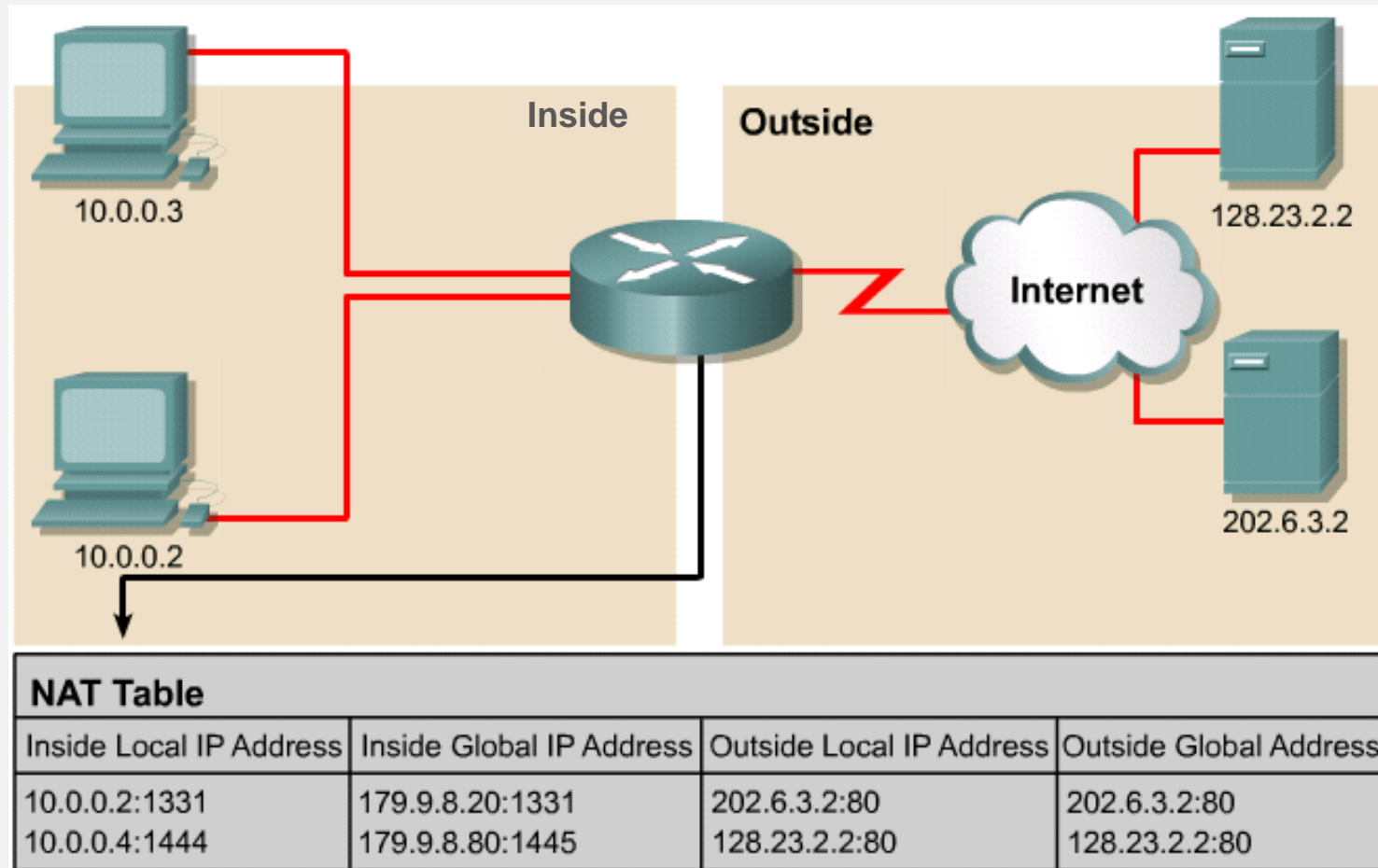
# Desvantagens

- Nem todos os protocolos suportam e/ou trabalham bem com o NAT.
- Diminui a performance do sistema de comunicação:
  - Aumenta o atraso do processo;
  - O primeiro pacote é traduzido sempre de forma mais lenta;
  - Como a CPU tem de analisar cada pacote para perceber se deve traduzi-lo ou não vai provocar atraso e maior necessidade de processamento;
  - É preciso alterar o endereço IP sempre que vai traduzir.
- A tabela NAT consome memória.
- Deixamos de conseguir “reconstruir” toda a rota dos pacotes de dados.
- Dificulta a criação de tuneis.

# Termos

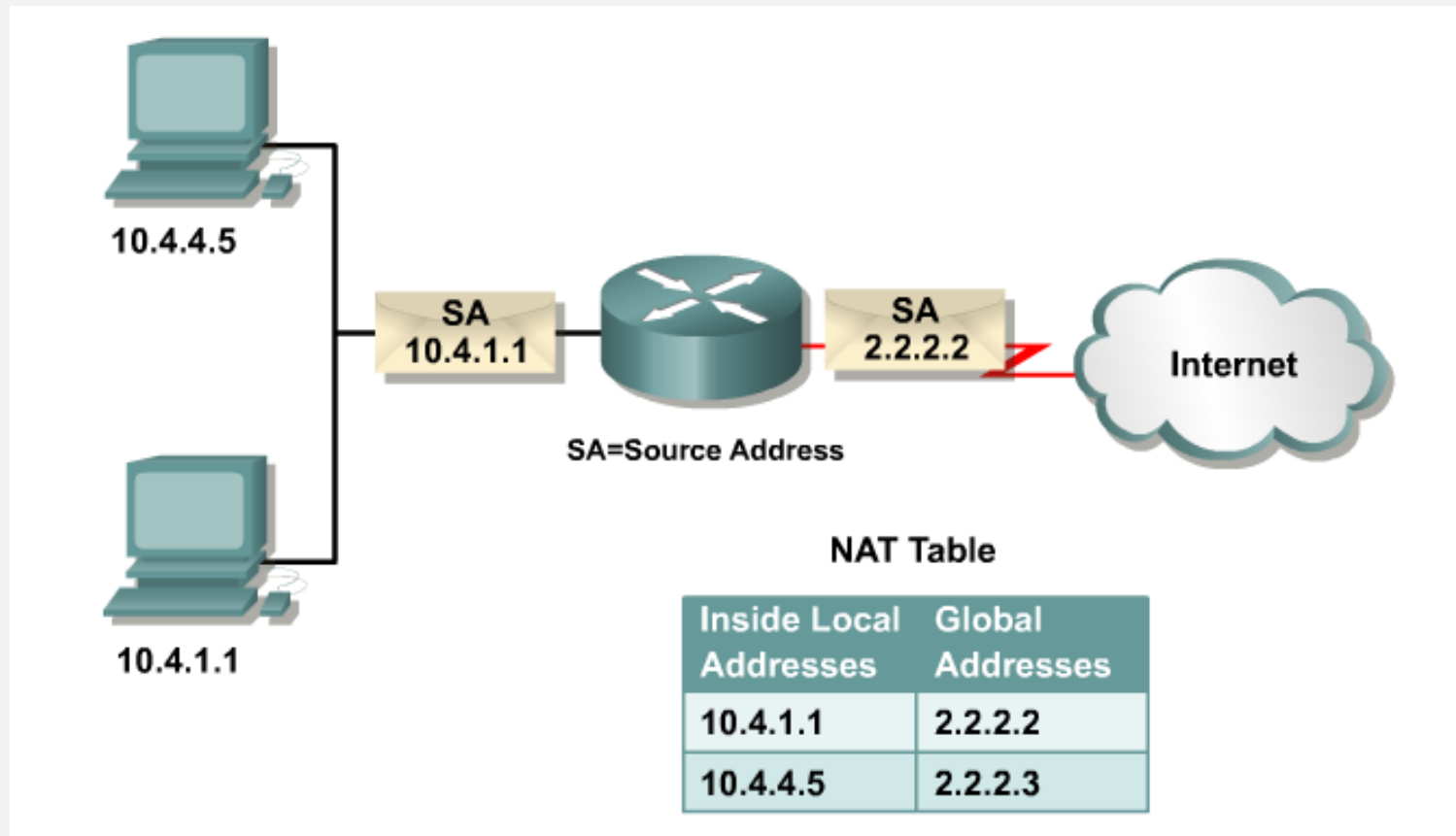
- **Endereço local interno** (*Inside local address*) – Endereço IP atribuído a um *host* da rede interna. Provavelmente, esse endereço é privado.
- **Endereço global interno** (*Inside global address*) – Um endereço IP legítimo atribuído pelo ISP e que representa um ou mais endereços IP públicos.
- **Endereço local externo** (*Inside local address*) – Endereço IP de um *host* externo, tal como é conhecido pelos *hosts* da rede interna.
- **Endereço global externo** (*Outside global address*) – Endereço IP atribuído a um *host* da rede externa. O proprietário do *host* atribui esse endereço.

# Termos



# Tabela

- O equipamento que está a ter a função de NAT, regista numa a associação entre os endereços internos e externos.



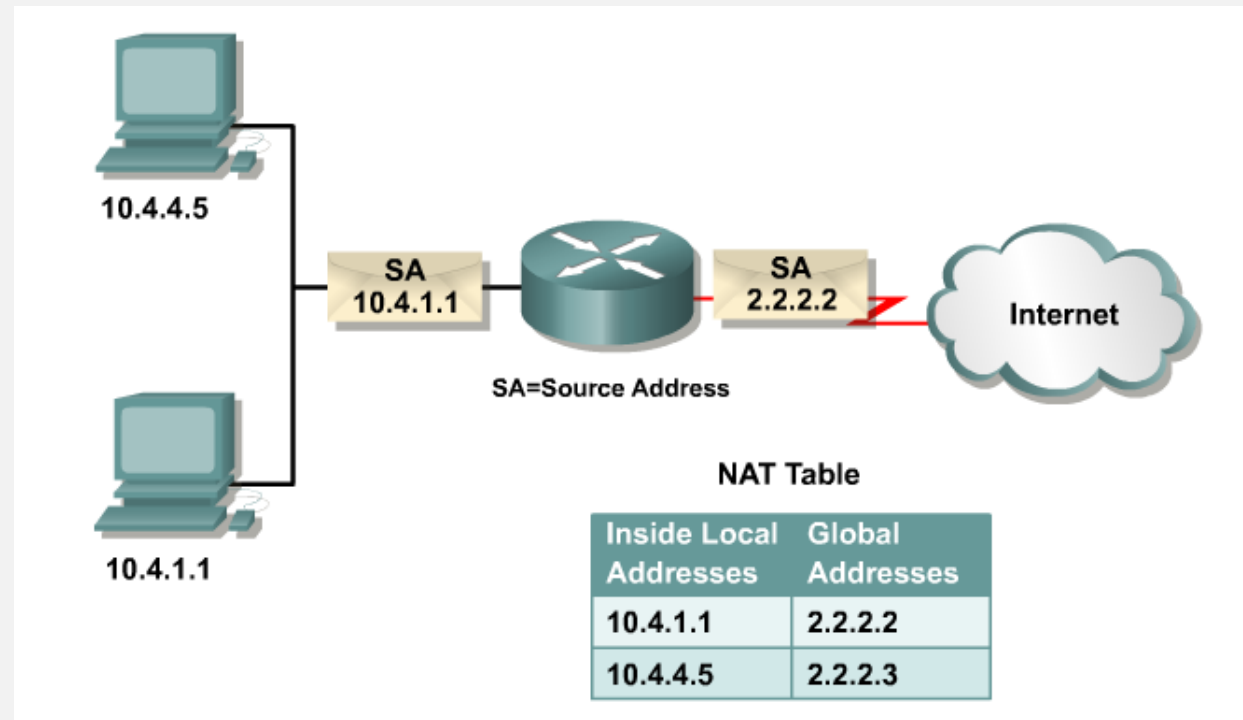
# Tipos

- Existem os seguintes tipos de NAT:
  - **NAT Estático** - um endereço IP público para um endereço IP privado.
  - **NAT Dinâmico** - existe um conjunto de endereços públicos (*pool*), que as máquinas que usam endereços privados podem usar.
  - **PAT (Network Address Port Translation) ou NAT Overload** - Um endereço IP público para “n” endereços IP privados. Esta é certamente a técnica mais usada.
  - **Twice NAT** – o endereço publico é fornecido mediante condição ou condições internas ou externas.
  - **Destination NAT**– dar um endereço privado a uma maquina com o endereço público (quase um “reverse NAT”).

# NAT Estático

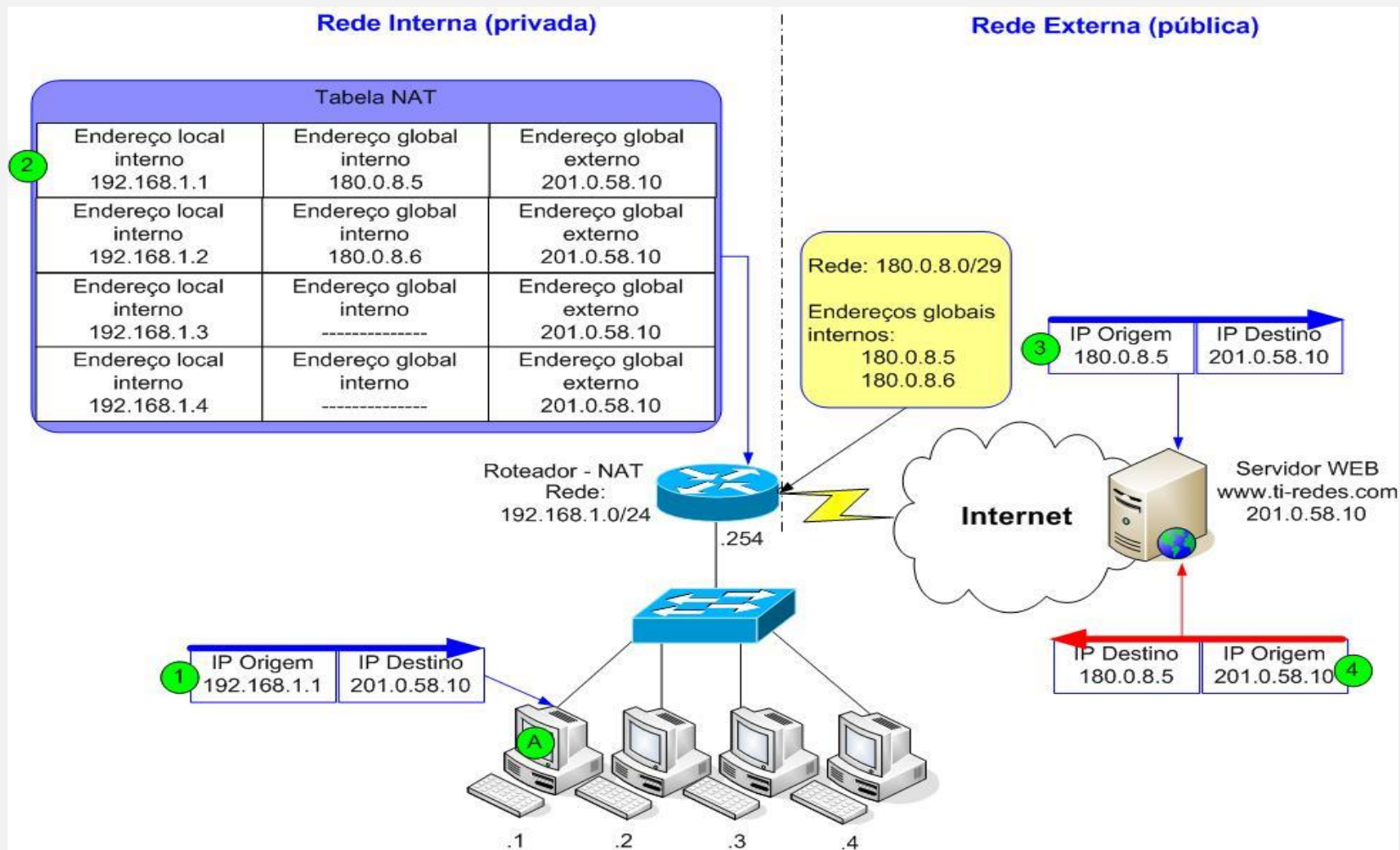
- O NAT Estático faz o mapeamento direto de **endereços privados** para **endereços públicos**. Um IP privado será sempre associado ao mesmo IP público (regra de ‘um para um’).
- Este tipo de NAT é útil quando se quer fazer a referência de determinado dispositivo com um endereço IP consistente e constante.
- Não permite contudo fazer gestão e “poupança” dos endereços públicos disponíveis já que a um endereço privado corresponde um endereço público.
- Usado quando se necessita que uma máquina com um endereço privado “saia” sempre com o mesmo endereço publico.

# NAT Estático





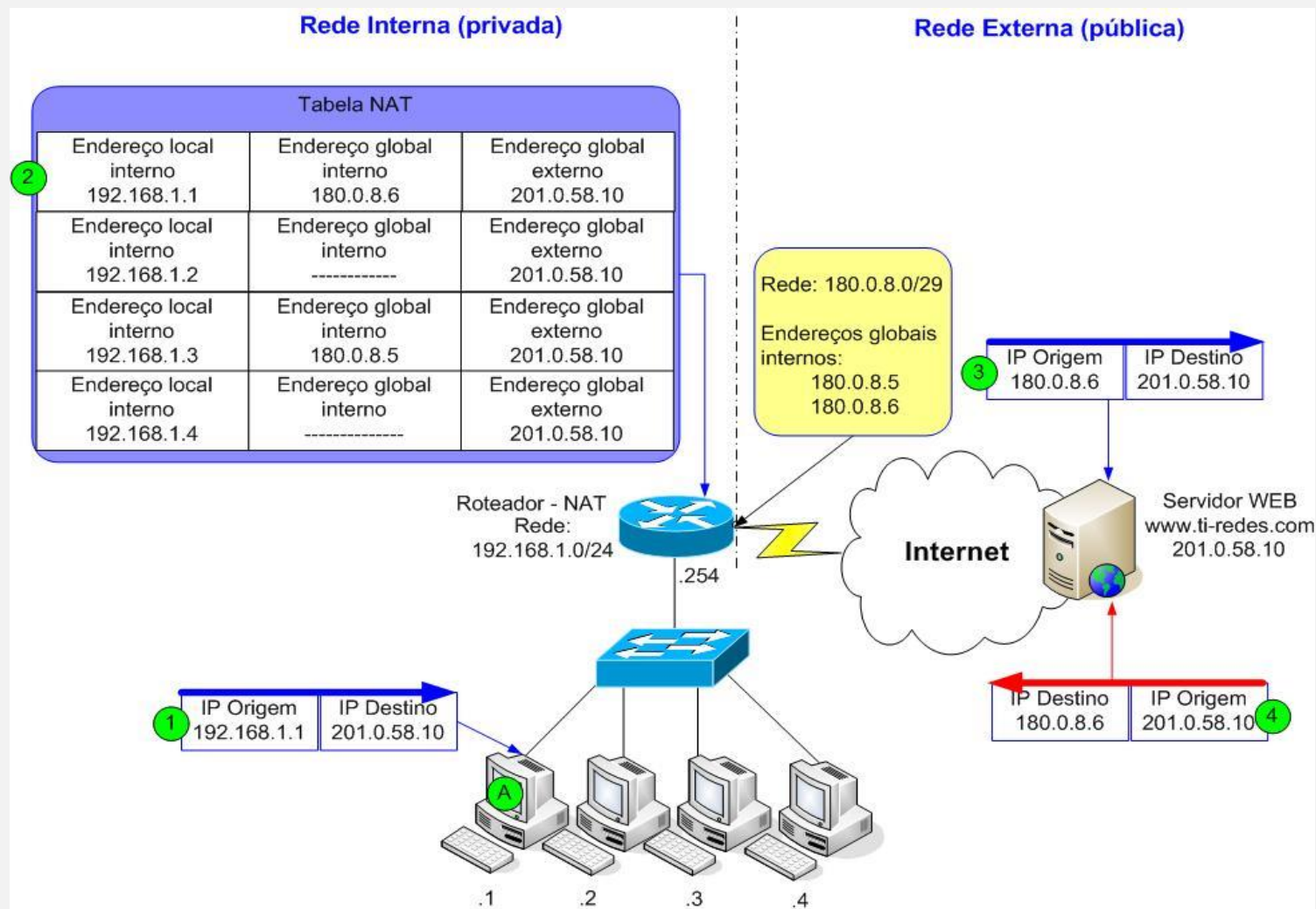
# NAT Estático



# NAT Dinâmico

- O NAT Dinâmico faz o mapeamento de endereços privados para endereços públicos de forma dinâmica.
- Assim, qualquer endereço privado pode ser traduzido para uma gama de endereços públicos de forma dinâmica.
- Contrariamente ao NAT Estático, os endereços internos nem sempre vão ser traduzidos para o mesmo endereço público.
- Permite fazer uma gestão mais eficiente dos endereços públicos disponíveis.

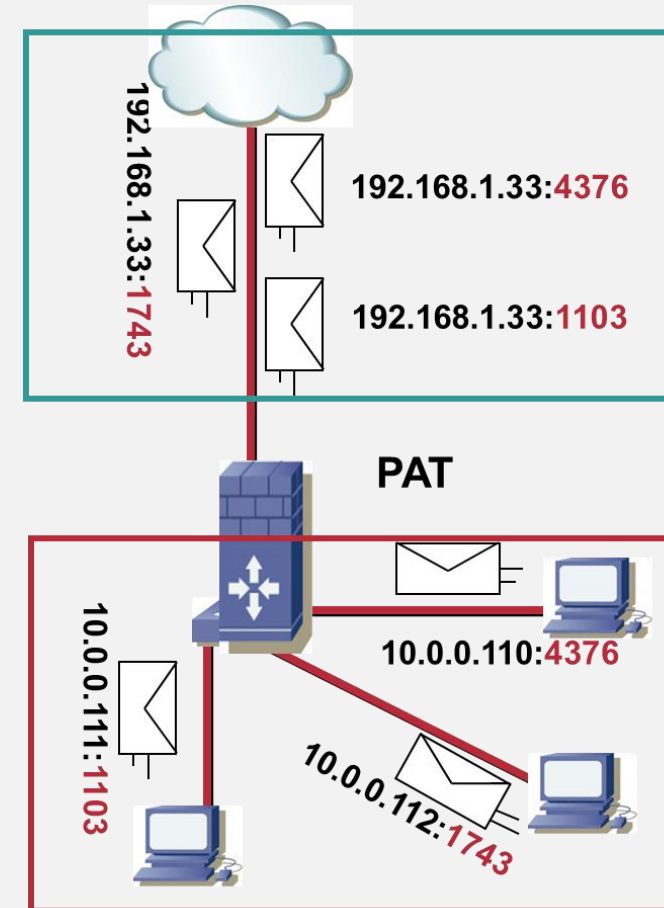
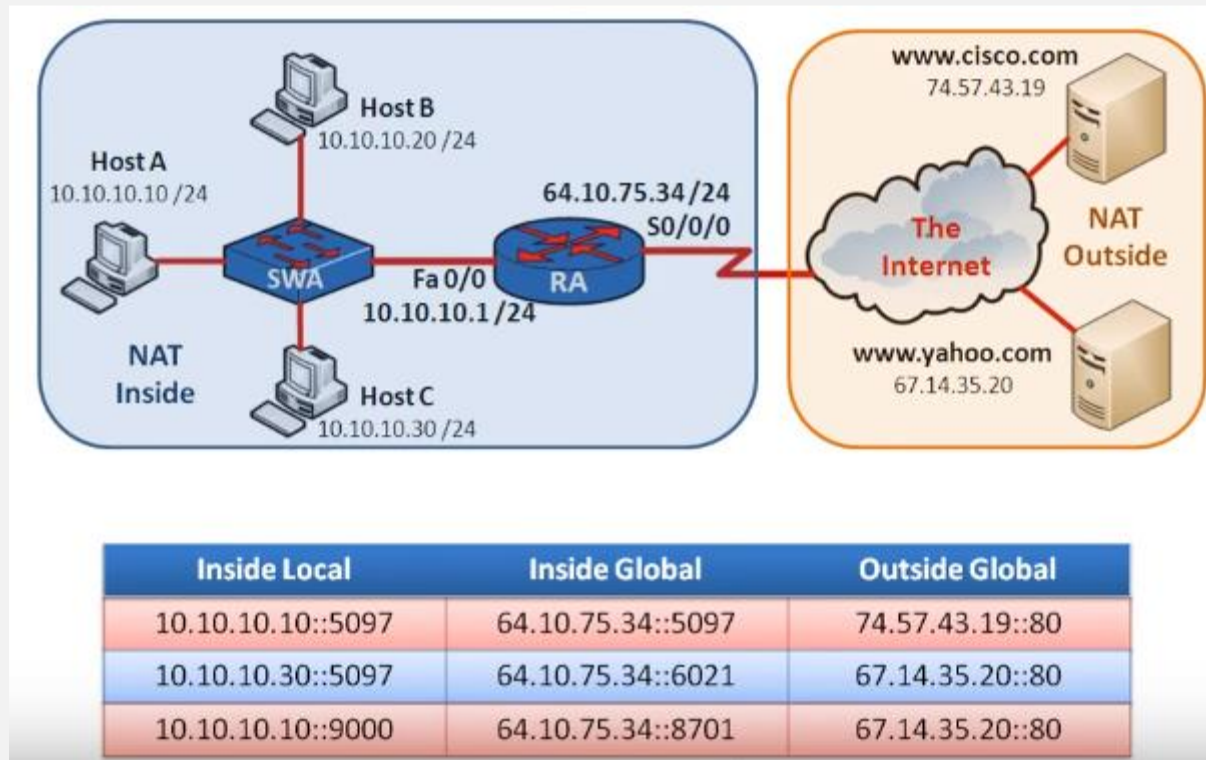
# NAT Dinâmico



## PAT - Network Address Port Translation ou NAT Overload

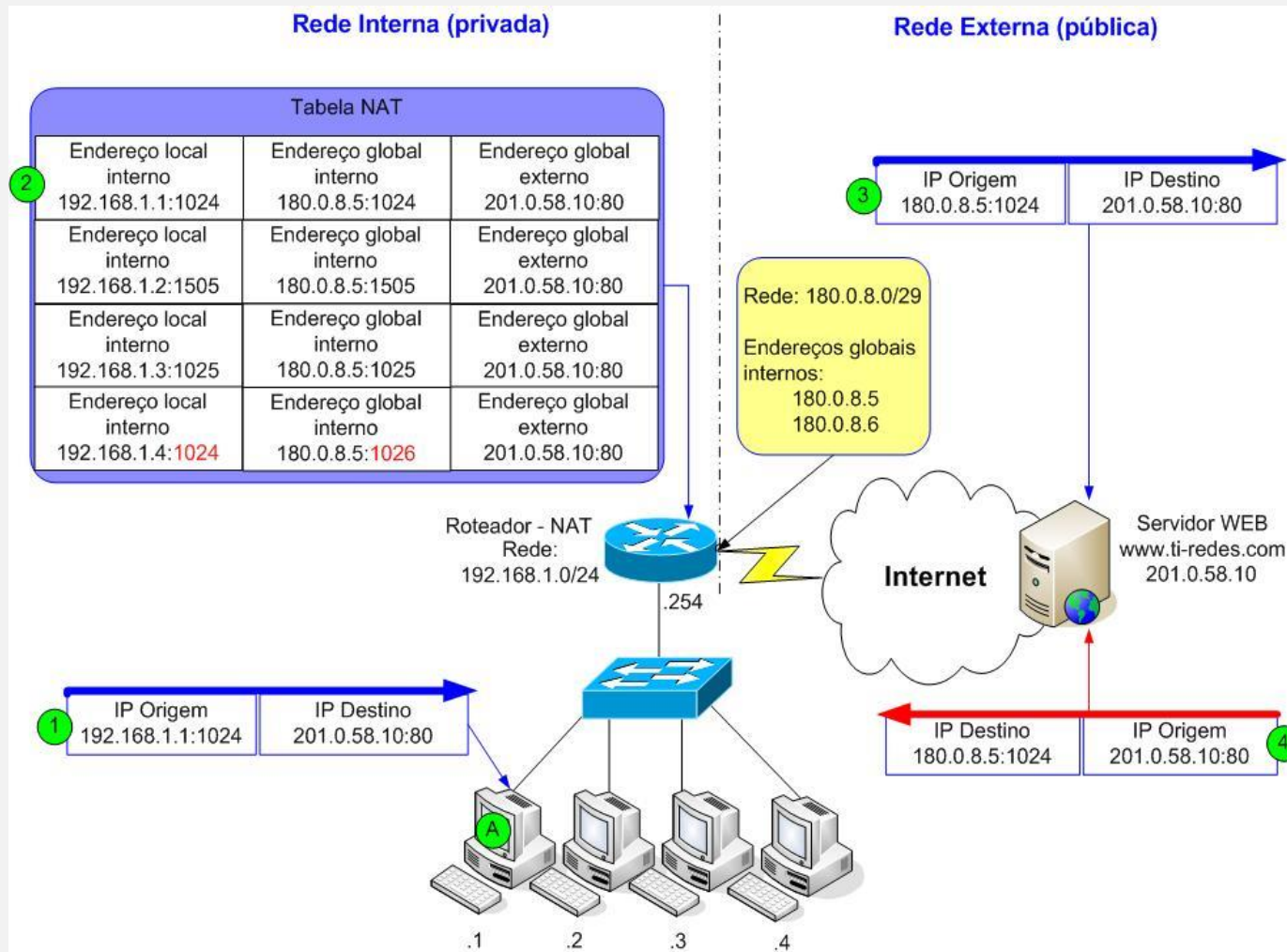
- O PAT ou *NAT Overload* surge como solução mais utilizada já que assim não são necessários tantos endereços públicos quantos os equipamentos que pretendem comunicar com o exterior.
- Desta forma, inúmeros dispositivos podem utilizar o mesmo endereço público, pois serão diferenciados pelo número do porto utilizado.
- A distinção entre as comunicações é realizada com base no porto origem:
  - Quando dois equipamentos pretendem comunicar usando o mesmo valor para o porto origem, o serviço de NAT utiliza o porto seguinte que esteja livre.
  - Caso não existam portos livres mas tenha sido configurada uma *pool* com vários endereços IP, é usado o próximo endereço IP, tentando respeitar o porto originalmente escolhido.

# Network Address Port Translation





# Network Address Port Translation



# Twice NAT

---

O Twice NAT permite que se decida qual o endereço público que será utilizado no processo de mapeamento, baseado no IP de destino ou pelo número da porta de destino.

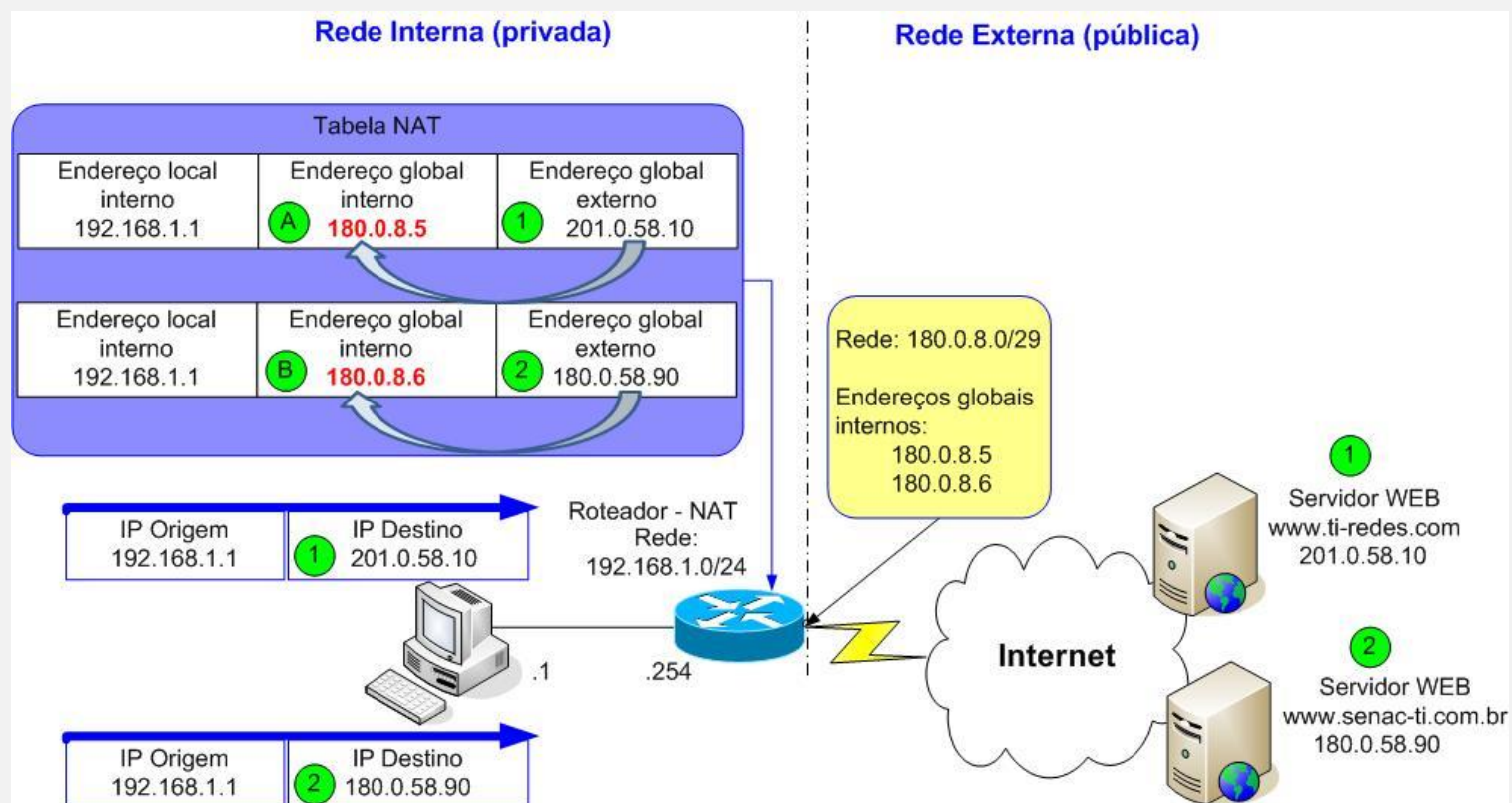
Pode-se criar regras para determinar que um endereço interno seja traduzido para determinado endereço público, tomando como determinante o seu destino.

Ou no caso de portas, o determinante será o número da porta de destino.



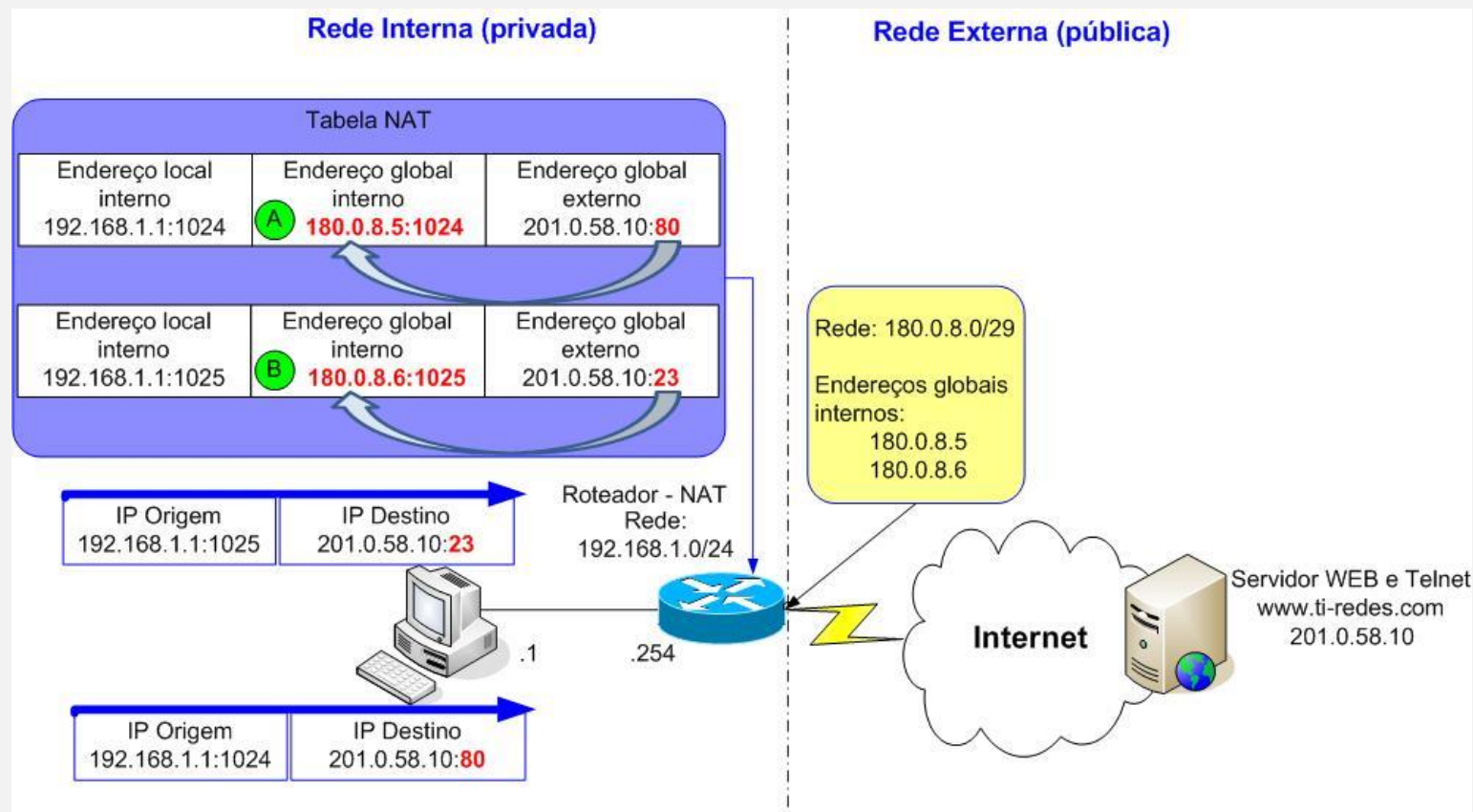
# Twice NAT

- **Determinante:** Endereço IP do destino.



# Twice NAT

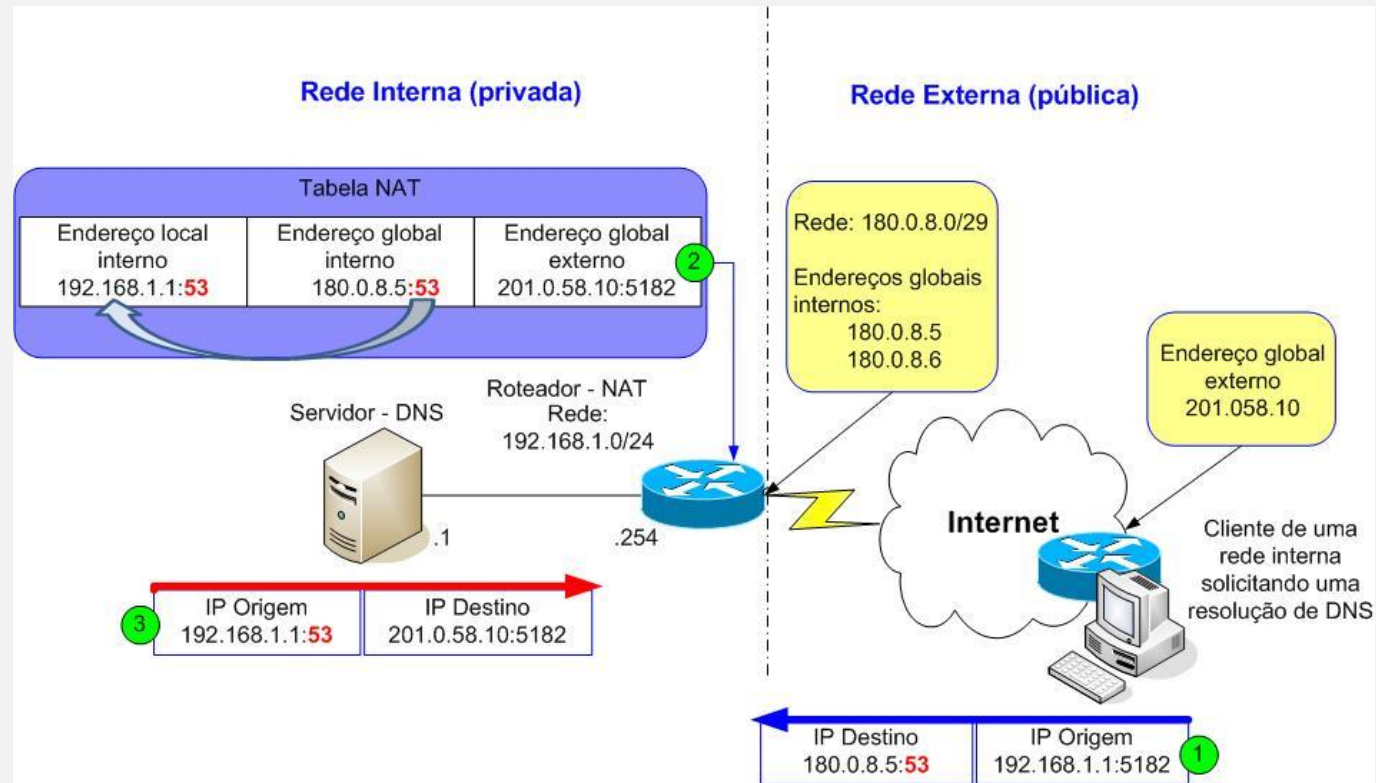
- **Determinante:** Número da porta do destino.



# Destination NAT

- Com o Destination NAT as ligações são iniciadas a partir de hosts da rede pública (Internet).
- Esta característica foi incorporada no NAT para possibilitar capacidades/funcionalidades mais avançadas.
- Como, os *hosts* das redes externas não sabem o endereço IP de *hosts* da rede interna, então não podiam aceder a um recurso que estivesse localizado internamente. Para que isso aconteça temos de fazer um “Reverse NAT”.

# Destination NAT



# NAT - Fases

- **datagramas de saída:** substituir (*endereço IP privado de origem, porto*) de cada datagrama de saída por (*endereço NAT IP público, novo porto*)
  - Os clientes/servidores remotos respondem usando como endereço de destino (*endereço NAT IP público, novo porto*).
- **guardar** na tabela de tradução NAT todos os pares (*endereço IP privado de origem, porto*), (*endereço NAT IP público, novo porto*).
- **datagramas de entrada:** substituir (*endereço NAT IP público, novo porto*) no campo de endereço de destino de cada datagrama de entrada o valor correspondente na tabela de tradução NAT (*endereço IP privado de origem, porto*).



Network Address Translation (NAT) - Cisco

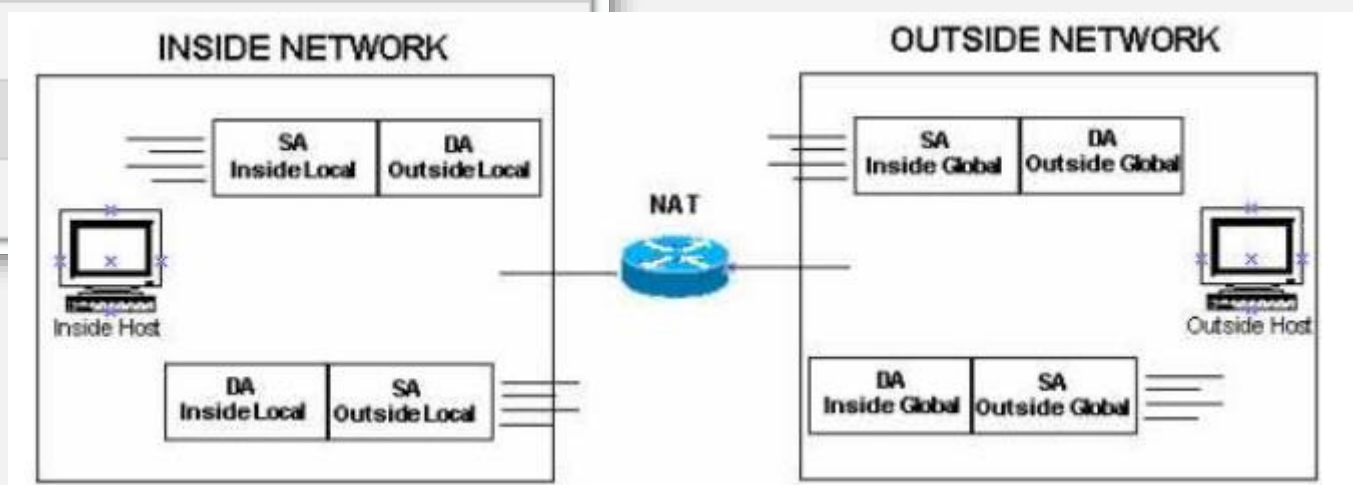
# Serviços de Rede 1

Ano Letivo 2019-2020

# NAT estático: configuração

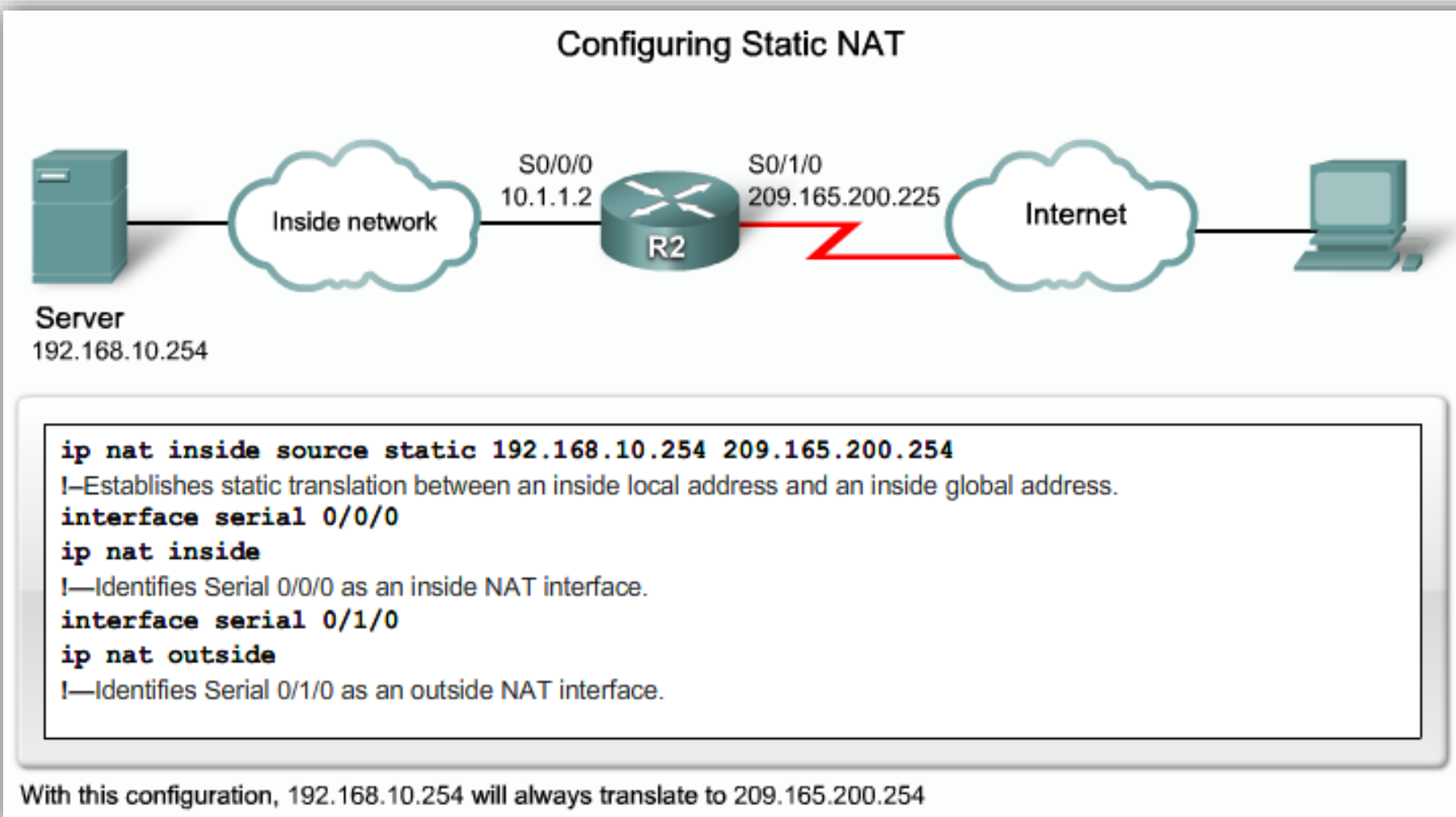
## Configuring Static NAT

Step	Action	Notes
1	Establish static translation between an inside local address and an inside global address. <code>Router(config)#ip nat inside source static local-ip global-ip</code>	Enter the global command <code>no ip nat inside source static</code> to remove the static source translation.
2	Specify the inside interface. <code>Router(config)#interface type number</code>	Enter the <code>interface</code> command. The CLI prompt will change from <code>(config)#</code> to <code>(config-if)#</code> .
3	Mark the interface as connected to the inside. <code>Router(config-if)#ip nat inside</code>	
4	Exit interface configuration mode. <code>Router(config-if)# exit</code>	
5	Specify the outside interface. <code>Router(config)#interface type number</code>	
6	Mark the interface as connected to the outside. <code>Router(config-if)#ip nat outside</code>	

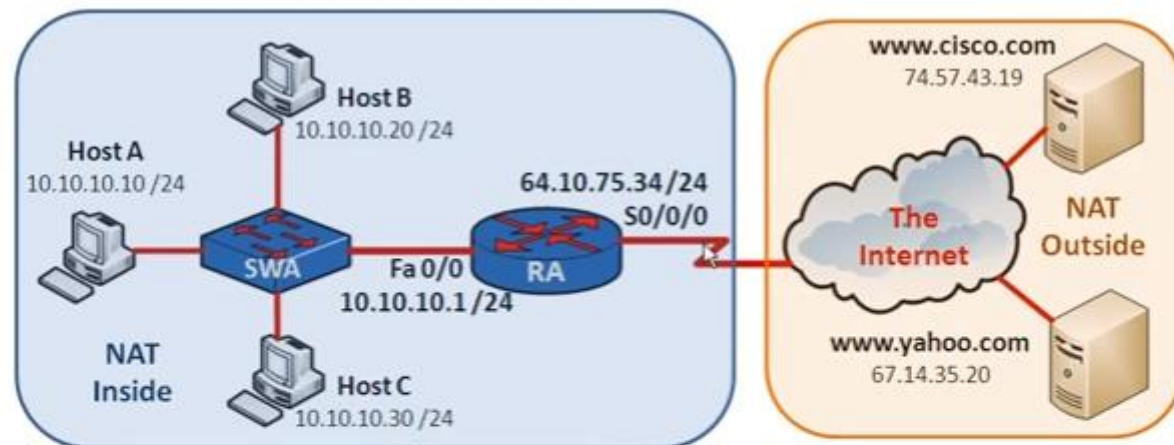




# NAT estático: configuração



# NAT estático: configuração



```
RA(config)#  
RA(config)#  
RA(config-if)#  
RA(config-if)#  
RA(config)#  
RA(config-if)#
```

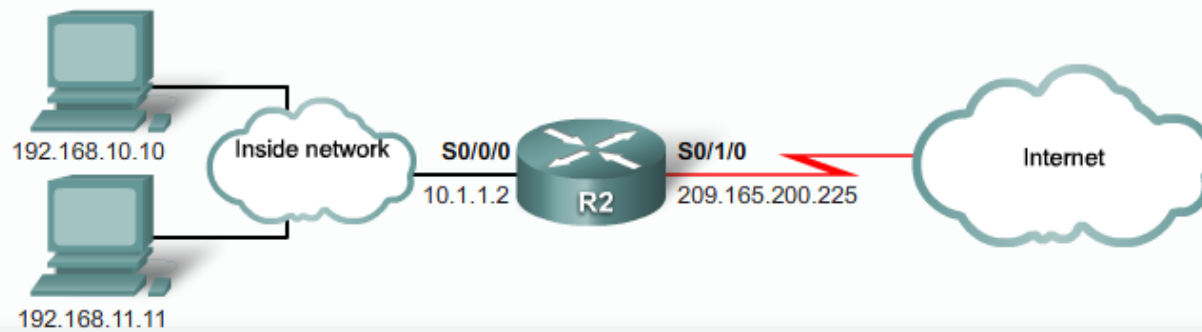
```
ip nat inside source static 10.10.10.10 64.10.75.99  
interface Fa 0/0  
ip nat inside  
exit  
interface S0/0/0  
ip nat outside
```

# NAT dinâmico: configuração

## Configuring Dynamic NAT

Step	Action	Notes
1	Define a pool of global addresses to be allocated as needed. Router(config)# <b>ip nat pool name start-ip end-ip</b> { <b>netmask netmask</b>   <b>prefix-length prefix-length</b> }	Enter the global command <b>no ip nat pool name</b> to remove the pool of global addresses.
2	Define a standard access list permitting those addresses that are to be translated. Router(config)# <b>access-list access-list-number permit</b> source [ source-wildcard]	Enter the global command <b>no access-list access-list-number</b> to remove the access list.
3	Establish dynamic source translation, specifying the access list defined in the prior step. Router(config)# <b>ip nat inside source list access-list-number pool name</b>	Enter the global command <b>no ip nat inside source</b> to remove the dynamic source translation.
4	Specify the inside interface. Router(config)# <b>interface type number</b>	Enter the <b>interface</b> command. The CLI prompt will change from (config)# to (config-if)#.
5	Mark the interface as connected to the inside. Router(config-if)# <b>ip nat inside</b>	
6	Specify the outside interface. Router(config)# <b>interface type number</b>	
7	Mark the interface as connected to the outside. Router(config-if)# <b>ip nat outside</b>	
8	Exit interface configuration mode. Router(config-if)# <b>exit</b>	

# NAT dinâmico: configuração



```
ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
```

!—Defines a pool of public IP addresses under the pool name NAT-POOL1

```
access-list 1 permit 192.168.0.0 0.0.255.255
```

!—Defines which addresses are eligible to be translated

```
ip nat inside source list 1 pool NAT-POOL1
```

!—Binds the NAT pool with ACL 1

```
interface serial 0/0/0
```

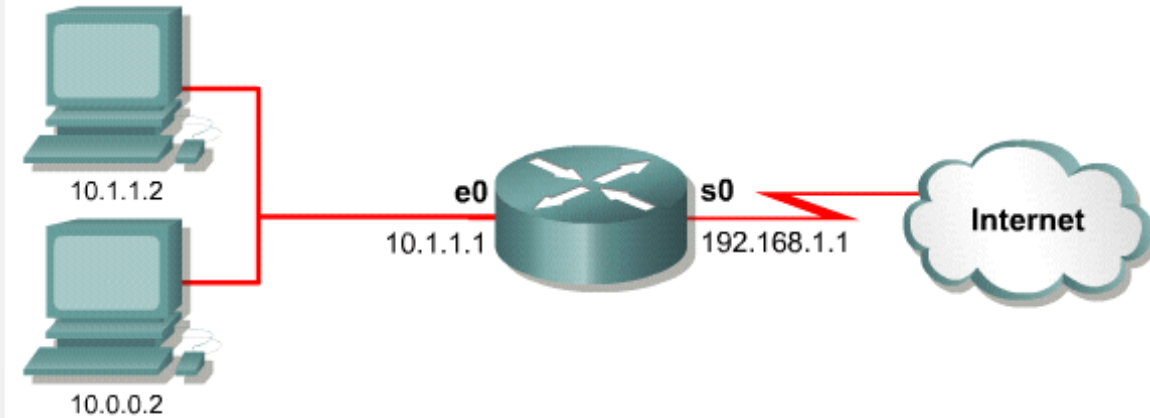
```
ip nat inside
```

!—Identifies interface Serial 0/0/0 as an inside NAT interface

```
interface serial 0/1/0
```

```
ip nat outside
```

!—Identifies interface Serial 0/1/0 as the outside NAT interface



```
ip nat pool nat-pool 1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
```

```
ip nat inside source list 1 pool nat-pool1
```

!

```
interface ethernet 0
```

```
ip address 10.1.1.1 255.255.255.0
```

```
ip nat inside
```

!

```
interface serial 0
```

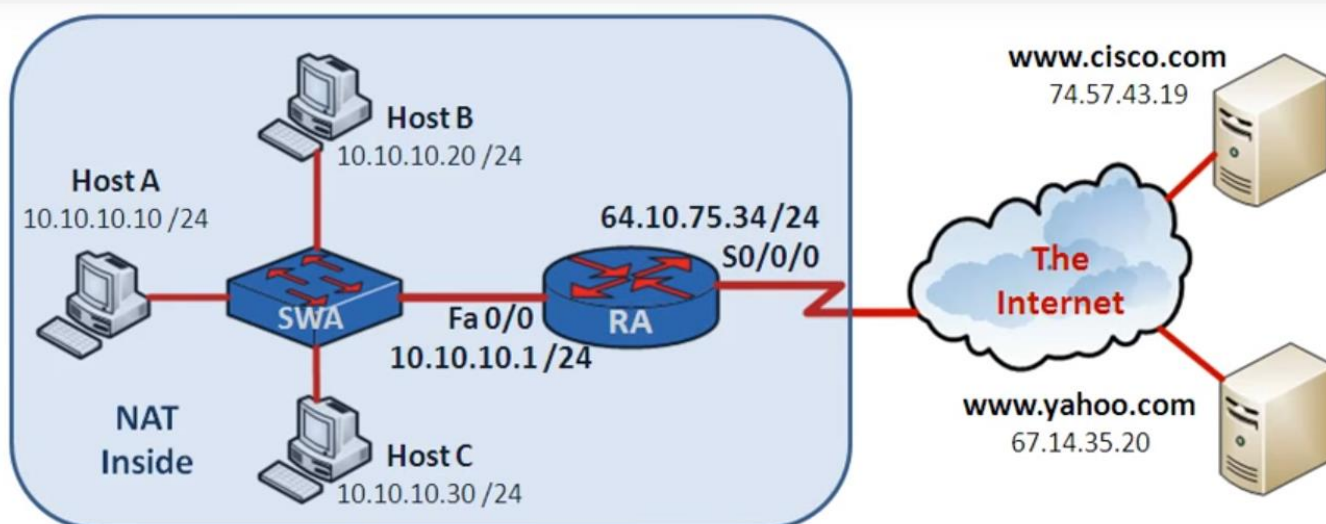
```
ip address 192.168.1.1 255.255.255.0
```

```
ip nat outside
```

!

```
access-list 1 permit 10.0.0.0.0.0.255.255
```

# NAT dinâmico: configuração



```
RA(config)#  
RA(config)#  
RA(config)#  
RA(config)#  
RA(config-if)#  
RA(config-if)#  
RA(config)#  
RA(config-if)#
```

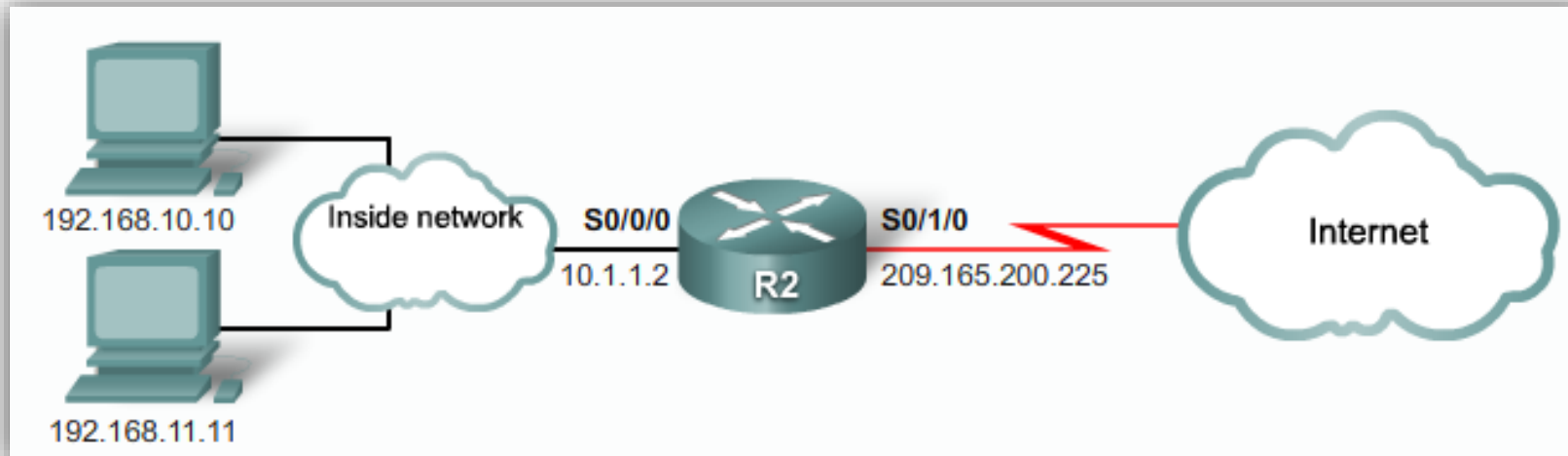
```
ip nat pool test 64.10.75.80 64.10.75.99 netmask 255.255.255.0  
access-list 10 permit 10.10.10.0 0.0.0.255  
ip nat inside source list 10 pool test  
interface Fa 0/0  
ip nat inside  
exit  
interface S0/0/0  
ip nat outside
```

# PAT - configuração

Podemos configurar utilizando uma gama de endereço IP:

Step	Action	Notes
1	Define a standard access list permitting those addresses that are to be translated. Router(config)# <b>access-list</b> <i>acl-number</i> <b>permit</b> <i>source</i> [ <i>source-wildcard</i> ]	Enter the global command <b>no access-list</b> <i>access-list-number</i> to remove the access list.
2	Specify the global address, as a pool, to be used for overloading. Router(config)# <b>ip nat pool</b> <i>name</i> <i>start-ip</i> <i>end-ip</i> { <b>netmask</b> <i>netmask</i>   <b>prefix-length</b> <i>prefix-length</i> }.	
3	Establish overload translation. Router { config} # <b>ip nat inside source list</b> <i>acl-number</i> <b>pool</b> <i>name</i> <b>overload</b> .	
4	Specify the inside interface. Router(config)# <b>interface</b> <i>type</i> <i>number</i> Router(config-if)# <b>ip nat inside</b>	Enter the <b>interface</b> command. The CLI prompt will change from (config)# to (config-if)#.
5	Specify the outside interface. Router(config-if)# <b>interface</b> <i>type</i> <i>number</i> Router(config-if)# <b>ip nat outside</b>	

# PAT - configuração



```
access-list 1 permit 192.168.0.0 0.0.255.255
```

*!—Defines which addresses are eligible to be translated*

```
ip nat inside source list 1 interface serial 0/1/0 overload
```

*!—Identifies the outside interface Serial 0/1/0 as the inside global address to be overloaded*

```
interface serial 0/0/0
```

```
    ip nat inside
```

*!—Identifies interface Serial 0/0/0 as an inside NAT interface*

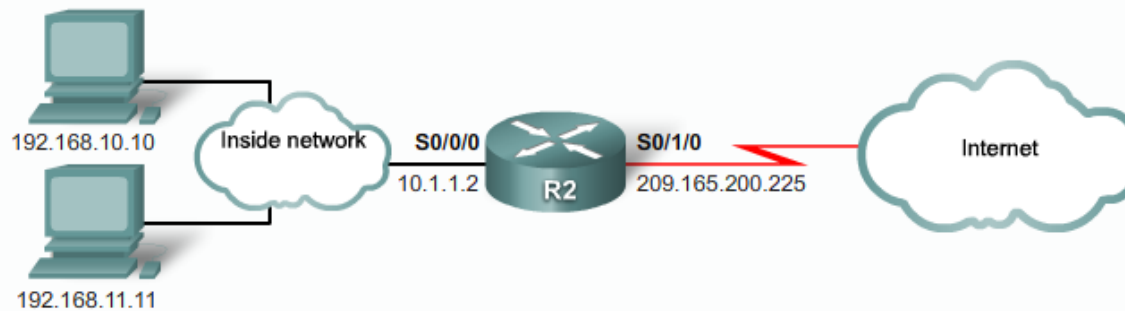
```
interface serial 0/1/0
```

```
    ip nat outside
```

*!—Identifies interface Serial 0/1/0 as the outside NAT interface*

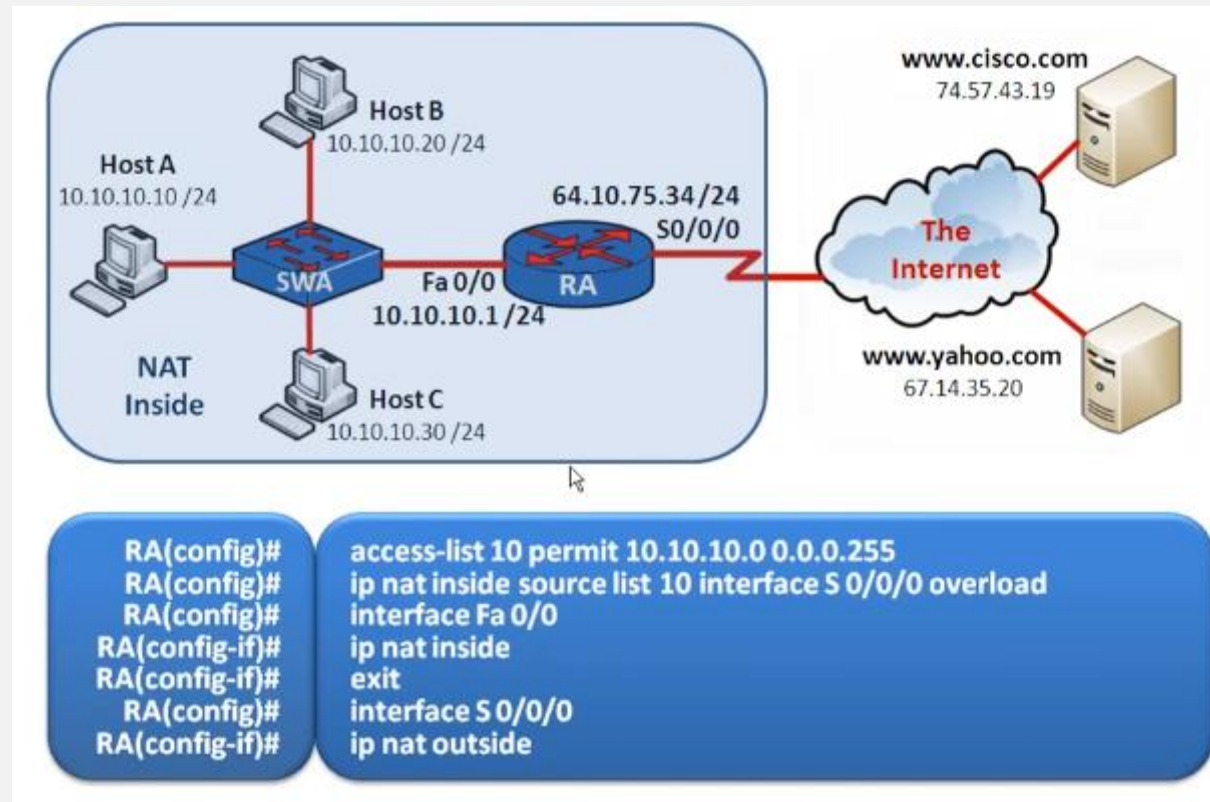


# PAT - configuração

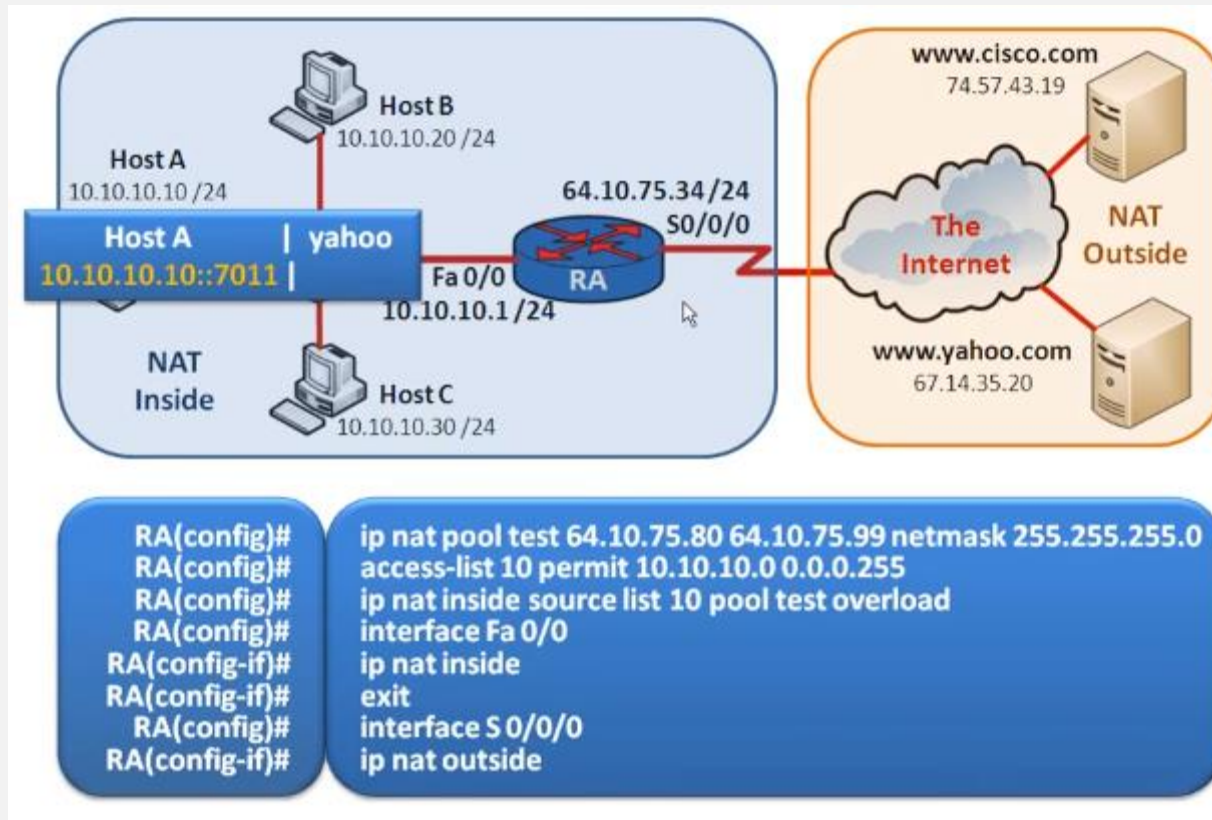


```
access-list 1 permit 192.168.0.0 0.0.255.255
! - Defines which addresses are eligible to be translated
ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240
! - Defines a pool of addresses named NAT-POOL2 to be used in NAT translation
ip nat inside source list 1 pool NAT-POOL2 overload
! - Binds the NAT pool with ACL 1
interface serial 0/0/0
ip nat inside
! - Identifies interface Serial 0/0/0 as an inside NAT interface
interface serial 0/1/0
ip nat outside
! - Identifies interface Serial 0/1/0 as an outside NAT interface
```

# PAT - configuração

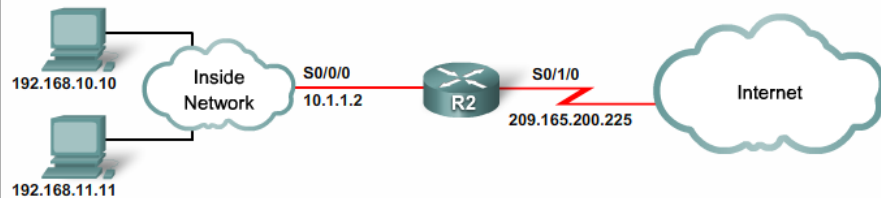


# PAT - configuração



# Verificação da configuração NAT

NAT Overload Configuration Example



```
access-list 1 permit 192.168.0.0 0.0.255.255
ip nat inside source list 1 interface serial 0/1/0 overload
interface serial 0/0/0
 ip nat inside
interface serial 0/1/0
 ip nat outside
```

NAT Translations Example

```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:3 192.168.10.10:3   209.165.200.254:3 209.165.200.254:3
tcp  209.165.200.225:11679 192.168.10.10:11679 209.165.200.254:80 209.165.200.254:80
icmp 209.165.200.225:0   192.168.11.10:0   209.165.200.254:0 209.165.200.254:0
tcp  209.165.200.225:14462 192.168.11.10:14462 209.165.200.254:80 209.165.200.254:80
```

```
R2#show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0, Serial0/0/1
Hits: 173 Misses: 9
CEF Translated packets: 182, CEF Punted packets: 0
Expired translations: 6
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Serial0/1/0 refcount 3
Queued Packets: 0
R2#
```

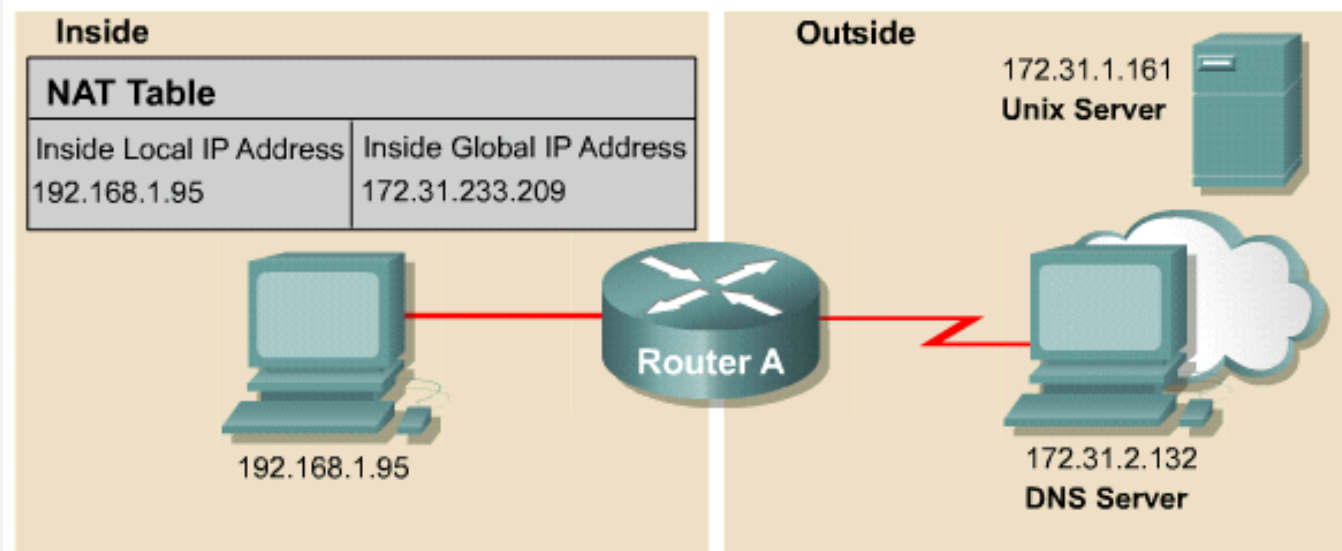
Clearing NAT Translations

```
R2#clear ip nat translation *
R2#show ip nat translations

R2#
```

Command	Description
<code>clear ip nat translation *</code>	Clears all dynamic address translation entries from the NAT translation table
<code>clear ip nat translation inside global-ip local-ip [ outside local-ip global-ip ]</code>	Clears a simple dynamic translation entry containing an inside translation or both inside and outside translation
<code>clear ip nat translation protocol inside global-ip global-port local-ip local-port [ outside local-ip local-port global-ip global-port ]</code>	Clears an extended dynamic translation entry

# Verificação da configuração NAT



outgoing  
incoming

```
RouterA#debug ip nat
NAT: s= 192.168.1.95 → 172.31.233.209, d=172.31.2.132 [6825]
NAT: s= 172.31.2.132, d=172.31.233.209, → 192.168.1.95 [21852]
NAT: s= 192.168.1.95 → 172.31.233.209, d=172.31.1.161 [6826]
NAT*: s= 172.31.1.161, d=172.31.233.209, → 192.168.1.95 [23311]
NAT*: s= 192.168.1.95 → 172.31.233.209, d=172.31.1.161 [6827]
NAT*: s= 192.168.1.95 → 172.31.233.209, d=172.31.1.161 [6828]
NAT*: s= 172.31.1.161 d=172.31.233.209, → 192.168.1.95 [23313]
NAT*: s= 172.31.1.161, d=172.31.233.209, → 192.168.1.95 [23313]
```

# Reencaminhamento de portos

- É possível reencaminhar portos através do *router* de acesso de modo a podermos aceder a determinados serviços presentes em máquinas internas

- Usar o comando

```
ip nat inside source static {tcp|udp} \ <ip_inside_local>  
    <porto_interno> \ <ip_inside_global> <porto_externo>
```

- Exemplo

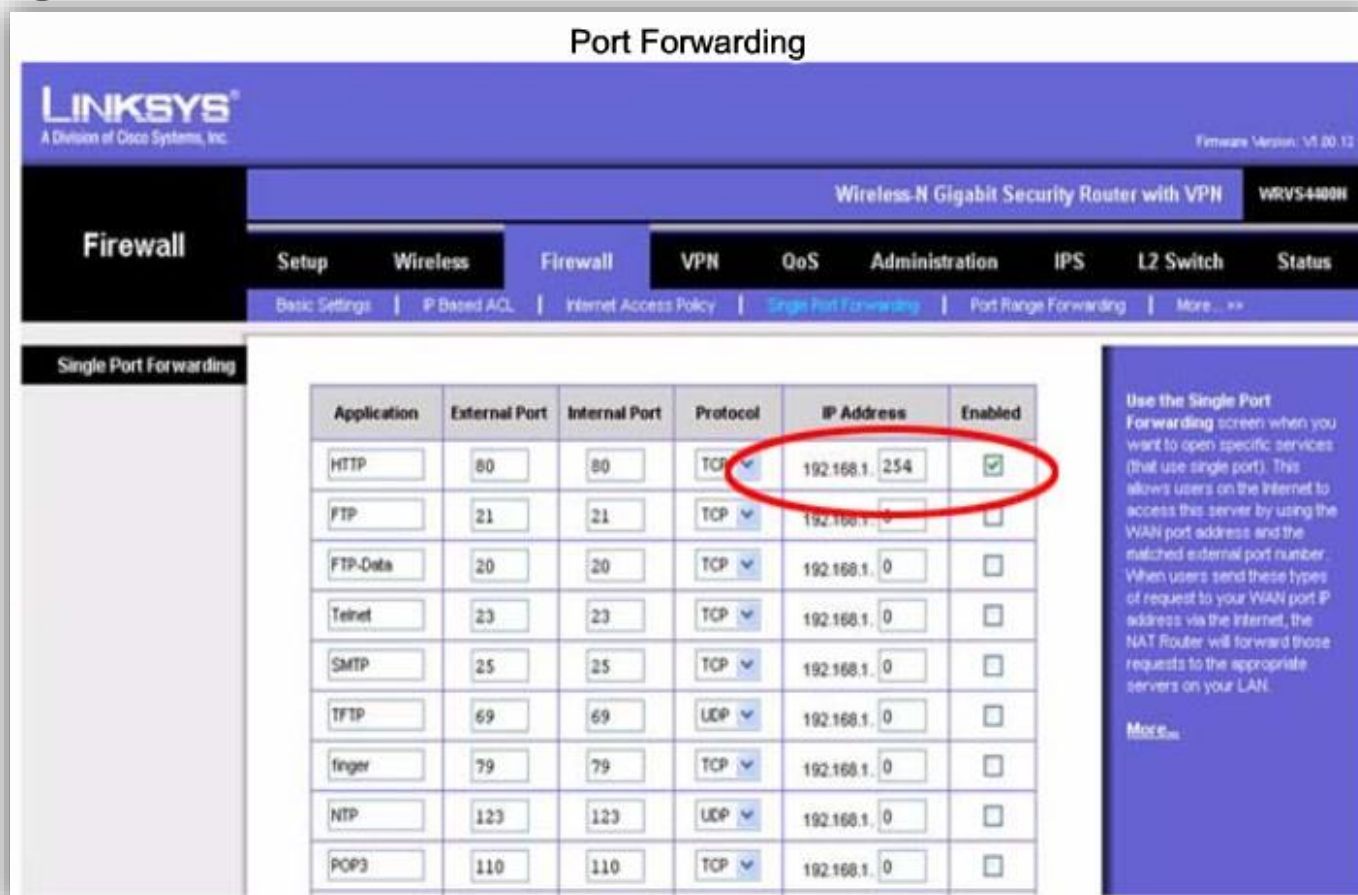
- Assumindo que uma instituição tem um router com IP público 193.137.78.254 e se pretende dar acesso ao servidor *web* interno (IP 192.168.15.1) através do porto 9988, fazer

```
ip nat inside source static tcp 192.168.15.1 80 193.137.78.254 9988
```

- Usar este comando no contexto de uma configuração completa do serviço de NAT

# Reencaminhamento de portos

- Nos routers domésticos existe uma interface *web* que facilita a configuração



**Port Forwarding**

LINKSYS®  
A Division of Cisco Systems, Inc.

Wireless-N Gigabit Security Router with VPN WRT54GL

Firewall

Setup Wireless Firewall VPN QoS Administration IPS L2 Switch Status

Basic Settings | IP Based ACL | Internet Access Policy | **Single Port Forwarding** | Port Range Forwarding | More... >>

**Single Port Forwarding**

Application	External Port	Internal Port	Protocol	IP Address	Enabled
HTTP	80	80	TCP	192.168.1.254	<input checked="" type="checkbox"/>
FTP	21	21	TCP	192.168.1.0	<input type="checkbox"/>
FTP-Data	20	20	TCP	192.168.1.0	<input type="checkbox"/>
Telnet	23	23	TCP	192.168.1.0	<input type="checkbox"/>
SMTP	25	25	TCP	192.168.1.0	<input type="checkbox"/>
TFTP	69	69	UDP	192.168.1.0	<input type="checkbox"/>
finger	79	79	TCP	192.168.1.0	<input type="checkbox"/>
NTP	123	123	UDP	192.168.1.0	<input type="checkbox"/>
POP3	110	110	TCP	192.168.1.0	<input type="checkbox"/>

Use the Single Port Forwarding screen when you want to open specific services (that use single port). This allows users on the Internet to access this server by using the WAN port address and the matched external port number. When users send these types of request to your WAN port IP address via the Internet, the NAT Router will forward those requests to the appropriate servers on your LAN.

More...





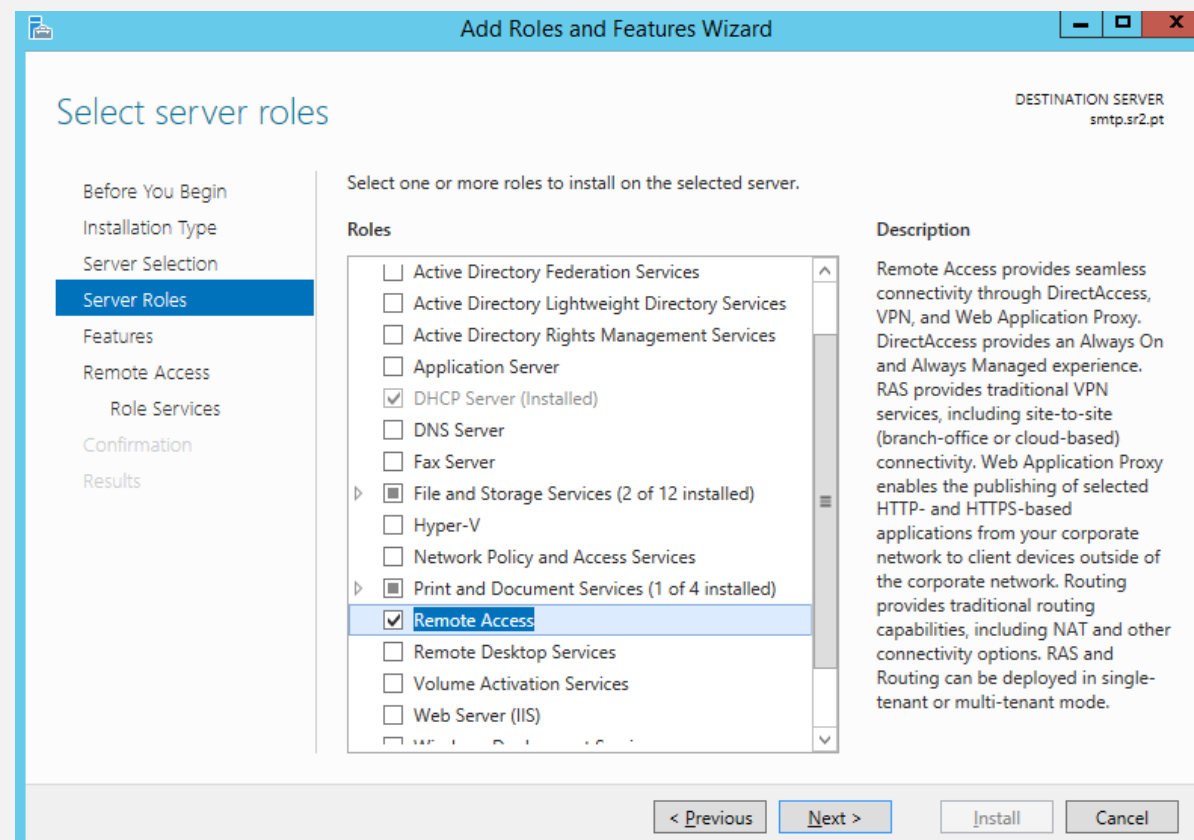
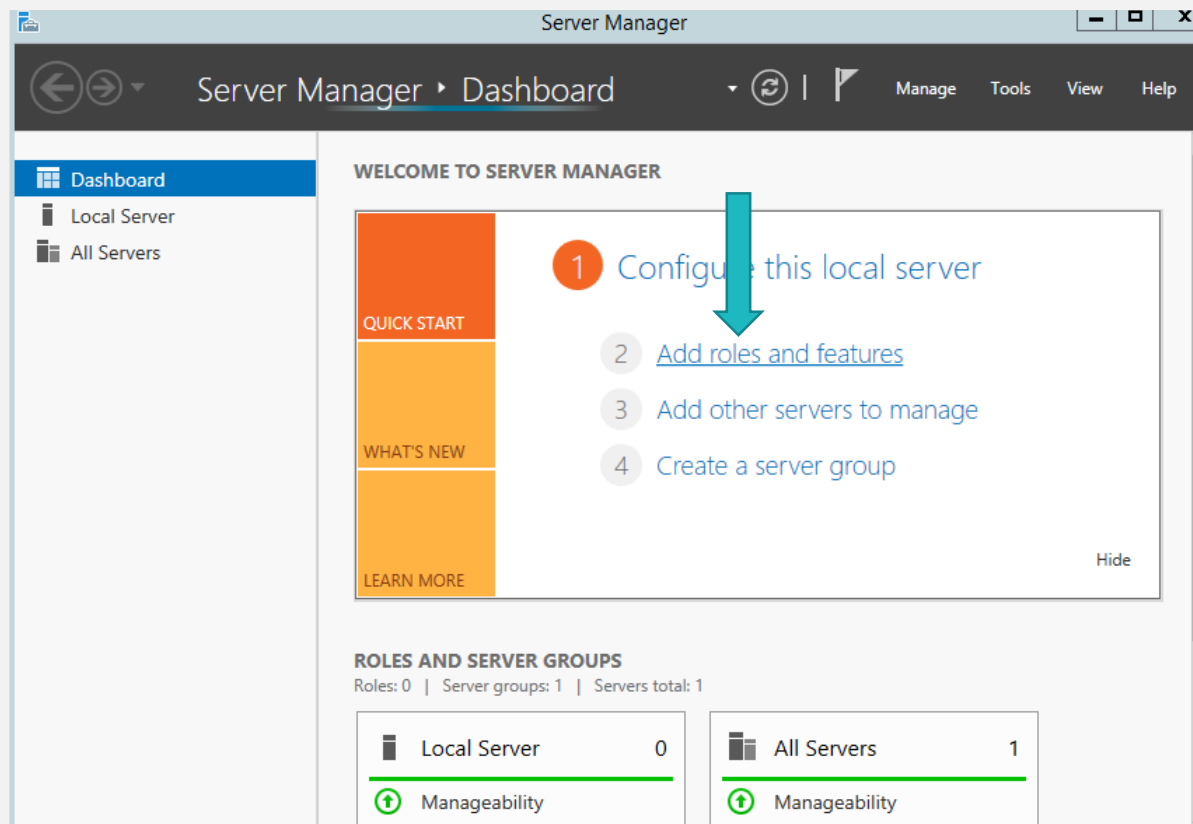
Network Address Translation  
(NAT) - Windows

# Serviços de Rede 1

**Ano Letivo 2019-2020**



# Instalação do serviço



# Instalação do serviço

Add Roles and Features Wizard

DESTINATION SERVER  
smtp.sr2.pt

## Select role services

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
Remote Access  
**Role Services**  
Web Server Role (IIS)  
Role Services  
Confirmation  
Results

Select the role services to install for Remote Access

Role services

<input checked="" type="checkbox"/> DirectAccess and VPN (RAS)
<input checked="" type="checkbox"/> <b>Routing</b>
<input type="checkbox"/> Web Application Proxy

Description

Routing provides support for NAT Routers, LAN Routers running BGP, RIP, and multicast capable routers (IGMP Proxy).

< Previous   Next >   Install   Cancel

Add Roles and Features Wizard

DESTINATION SERVER  
smtp.sr2.pt

## Installation progress

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
Remote Access  
Role Services  
Web Server Role (IIS)  
Role Services  
Confirmation  
**Results**

View installation progress

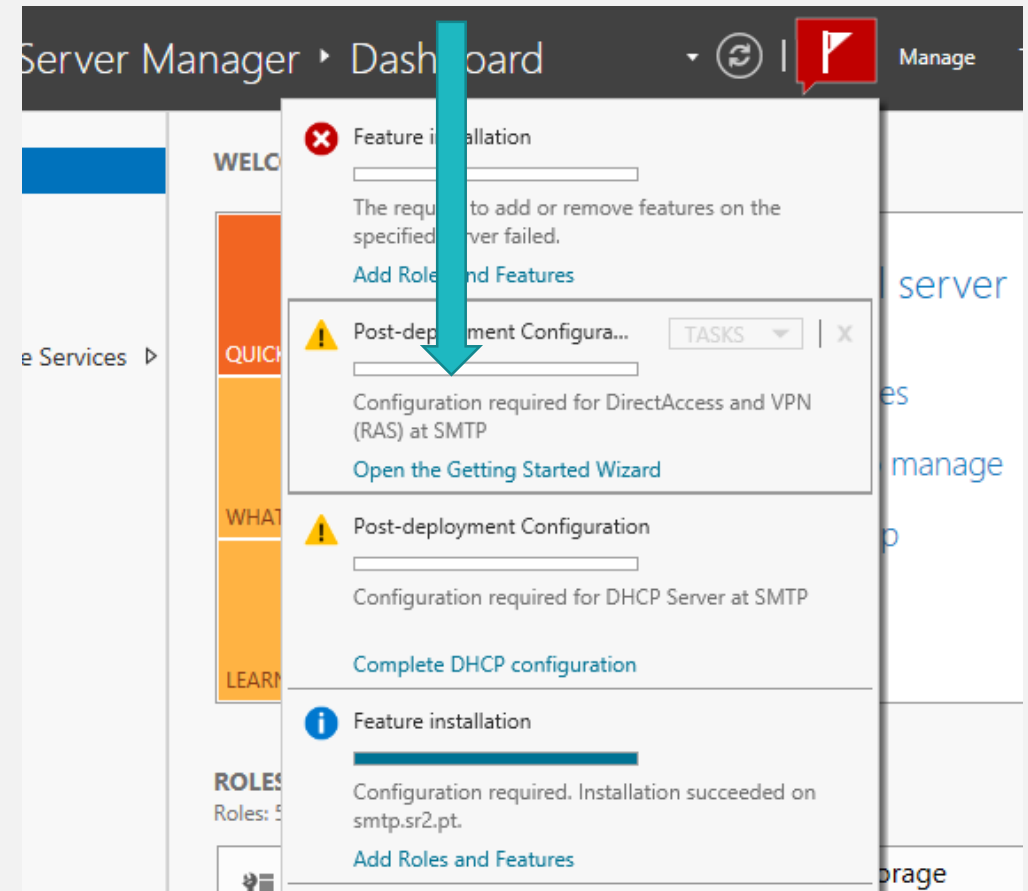
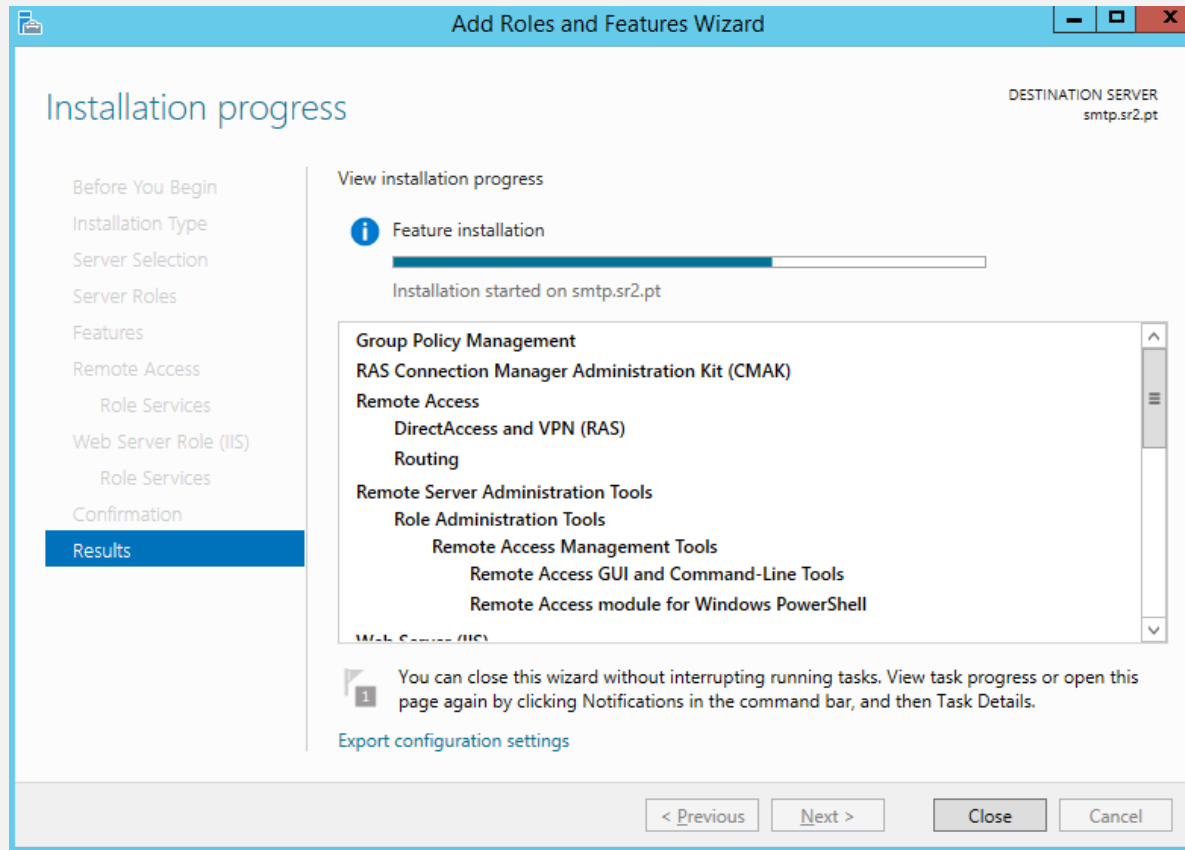
**i** Starting installation

Group Policy Management  
RAS Connection Manager Administration Kit (CMAC)  
Remote Access  
    DirectAccess and VPN (RAS)  
    Routing  
Remote Server Administration Tools  
    Role Administration Tools  
        Network Policy and Access Services Tools  
        Remote Access Management Tools  
        Remote Access GUI and Command-Line Tools  
        Remote Access module for Windows PowerShell  
Web Server (IIS)  
    Management Tools

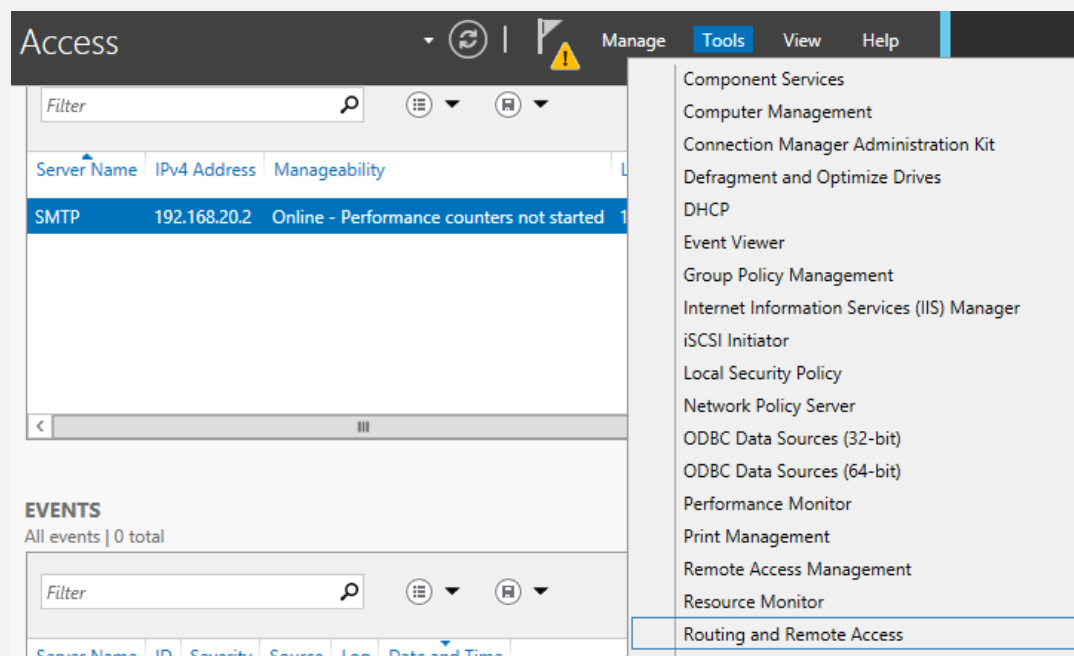
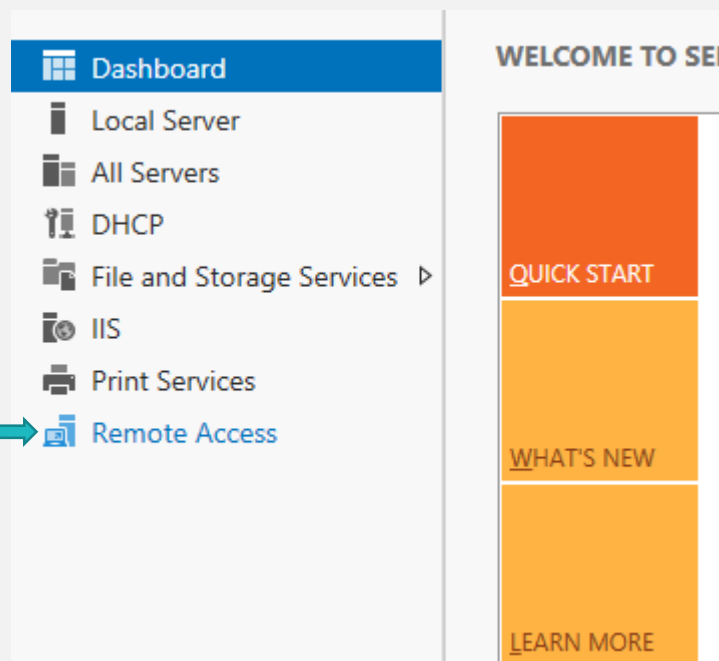
Export configuration settings

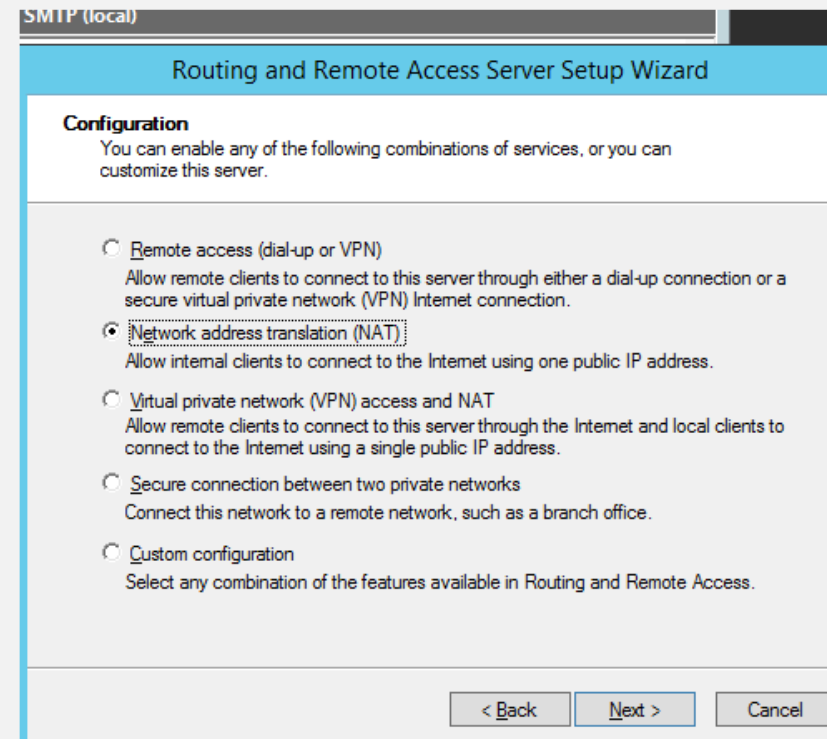
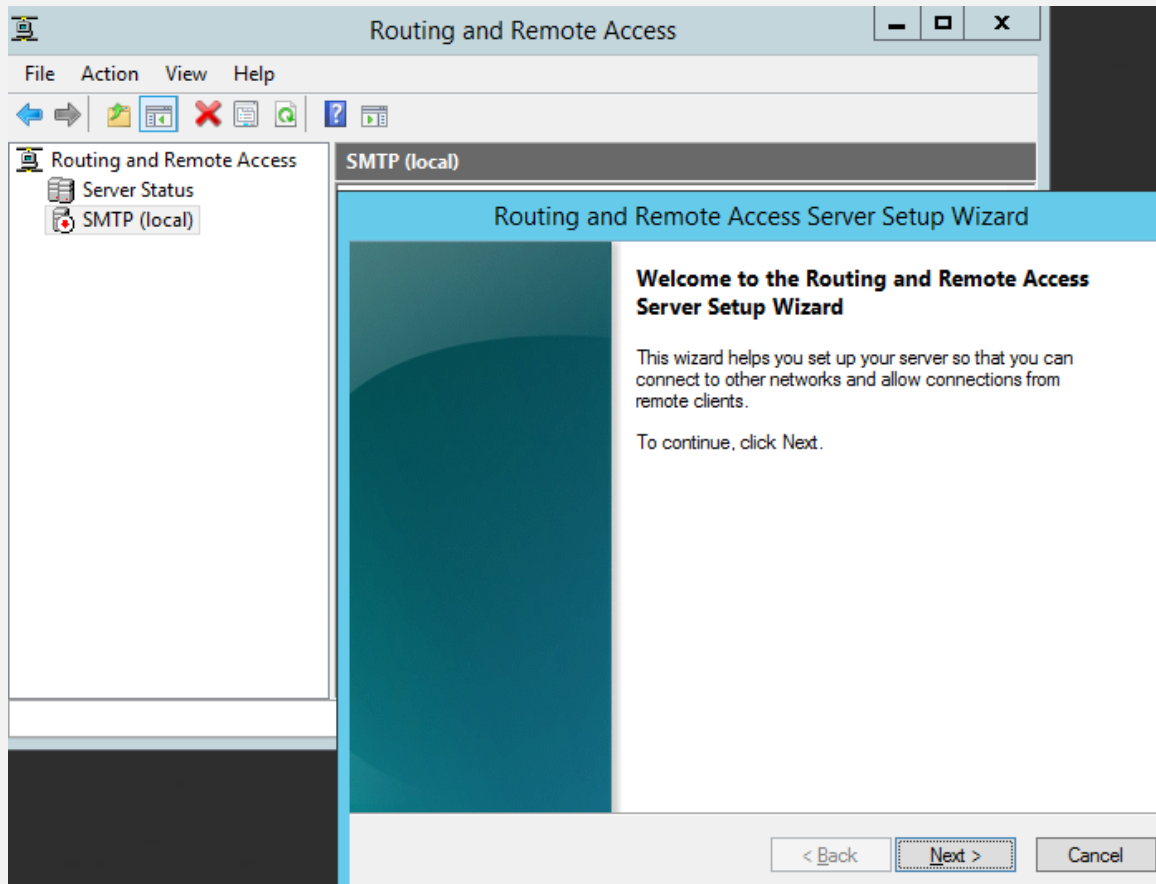
< Previous   Next >   Install   Cancel

# Instalação do serviço



# Instalação do serviço





# Dúvidas



# Referencias

- <http://pt.scribd.com/doc/111360368/NAT-Network-Address-Translation>
- <https://www.youtube.com/watch?v=QBqPzHEDzvo>
- <https://www.youtube.com/watch?v=xkCgYaJXDSk>