Network Services 1

2019-2020

Licenciatura em Engenharia Informática

Ramo de Redes e Administração de Sistemas

NAT- Network Address Translation

School Year 2019-2020

Public Addresses

- Any institution or company may purchase or lease IP addresses or ranges of IPs for assignment to equipment that has the need for public access.
  - Address rental can be requested from ISPs.
  - IP addresses are made available to ISPs by regional entities to which this competence has been delegated.

Public Internet addresses are regulated by five Regional Internet Registries (RIRs):

- ARIN
- RIPE
- APNIC
- LACNIC
- AfriNIC

Private Addresses

- There are 3 sets of addresses that can not be assigned specifically to a client and are reserved for use on private networks:
  - They are called "private addresses".
  - They can be used by millions of devices simultaneously.
  - Packages containing these addresses **can not** be forwarded to the Internet.

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:

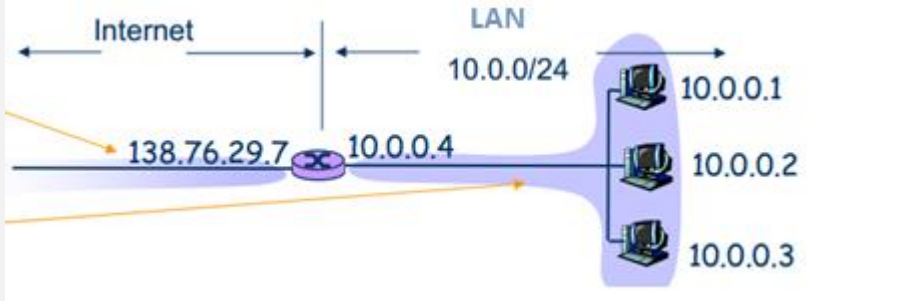
Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Public and private addresses

- Machines with private addresses can not directly access the internet.
- Public addresses are a limited and currently scarce resource.
  - There are not enough addresses to deal with the amount of equipment that is interconnected.
- However machines have to be accessed and accessed through the internet.
- Solutions:
  - IP V6
  - Intermediate machines to provide the intended services indirectly (eg Proxys).
  - Translation of private addresses into public addresses (NAT).

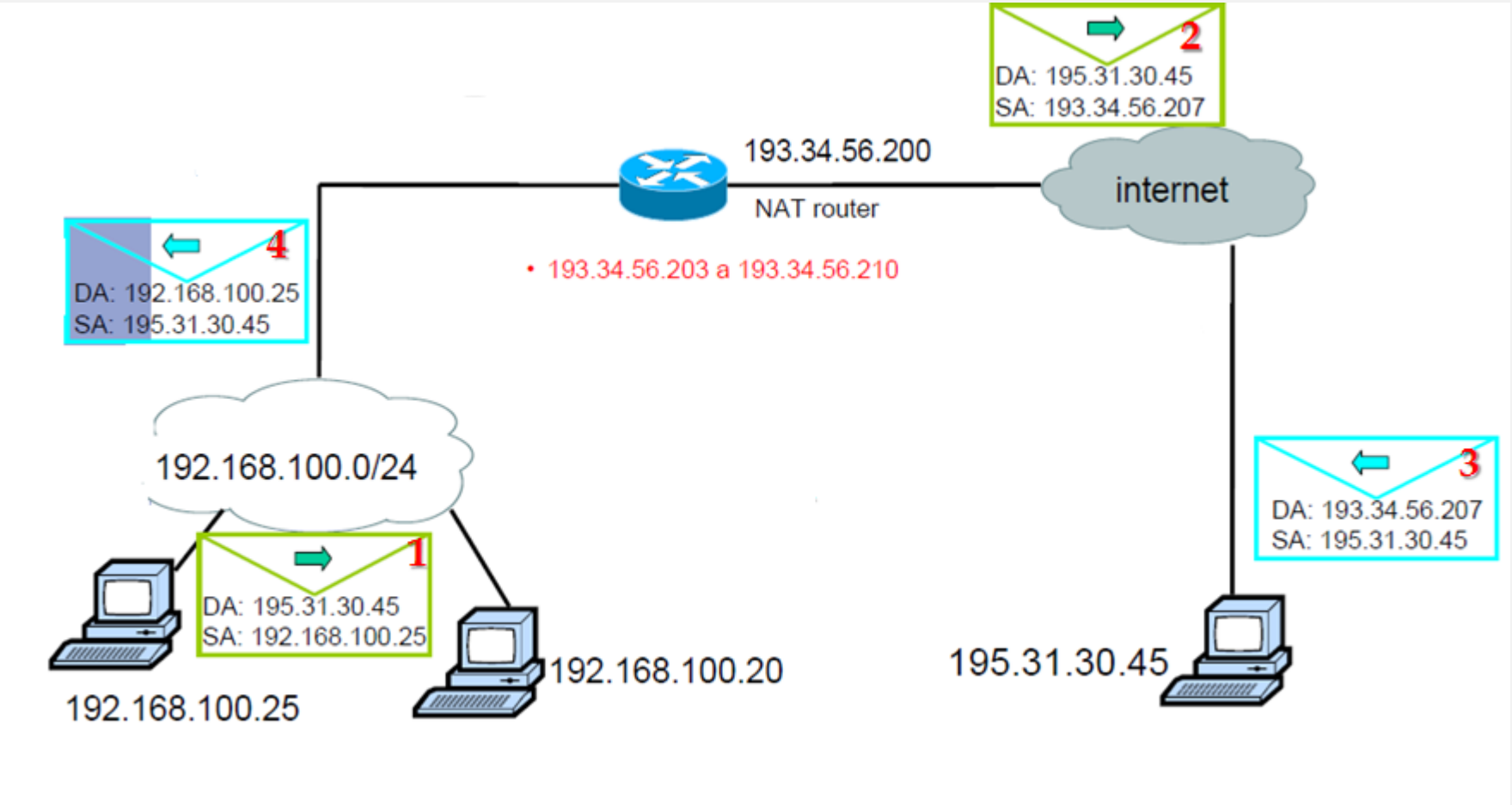
Network Address Translation (NAT)

- With NAT (Network Address Translation) you can expand the IP address space through the use of private addresses.



- It is regulated and defined in the following RFCs:
  - 3022 - Traditional IP Address Translator (NAT)
  - 1918 - Address Allocation for Private Internets

NAT


2
DA: 195.31.30.45
SA: 193.34.56.207
193.34.56.200
NAT router
internet
4
DA: 192.168.100.25
SA: 195.31.30.45
• 193.34.56.203 a 193.34.56.210
192.168.100.0/24
3
DA: 193.34.56.207
SA: 195.31.30.45
1
DA: 195.31.30.45
SA: 192.168.100.25
192.168.100.20
195.31.30.45
192.168.100.25

Benefits

- Ensures that private addresses are not passed to the public domain.
- Ensure greater address space management capacity.
- It increases the flexibility of access to public networks.
- It ensures a more rational and efficient management of public address.
- Easy to change ISP.
- It enables the creation of safer networks and with greater guarantee of privacy of data.

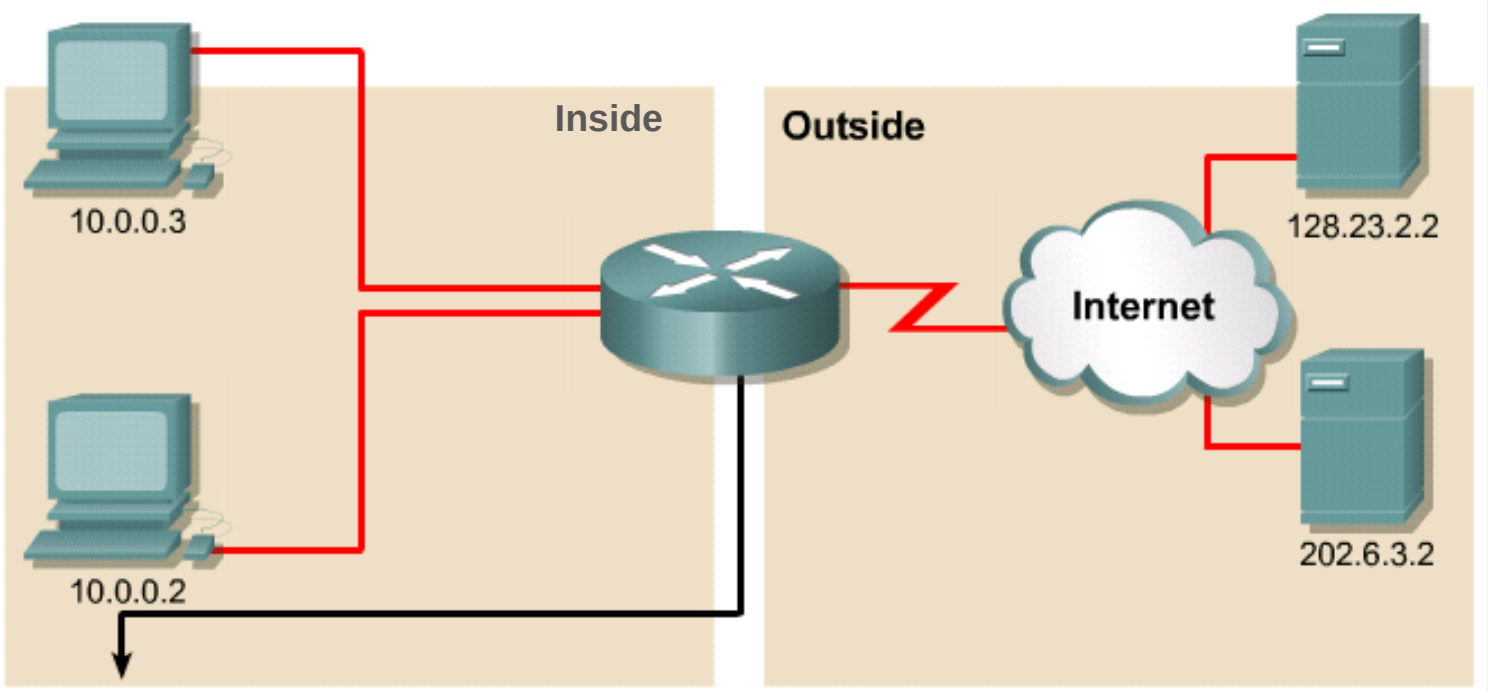
Disadvantages

- Not all protocols support and / or work well with NAT.
- Decreases the performance of the communication system:
  - Increases process delay;
  - The first packet is always translated more slowly;
  - As the CPU has to analyze each package to see if it should translate it or not it will cause delay and greater need of processing;
- You must change the IP address each time you translate.
- The NAT table consumes memory.
- We are no longer able to "rebuild" the entire route of the data packets.
- It is more complicated to the creation of tunnels.

Terms

- **Internal local address -** IP address assigned to a host on the internal network. This address is probably private.
- **Internal global address -** A legitimate IP address assigned by your ISP and representing one or more public IP addresses.
- **External local address -** The IP address of an external host, as known by the internal network hosts.
- **Outside global address -** The IP address assigned to a host on the external network. The host owner assigns this address.

Terms

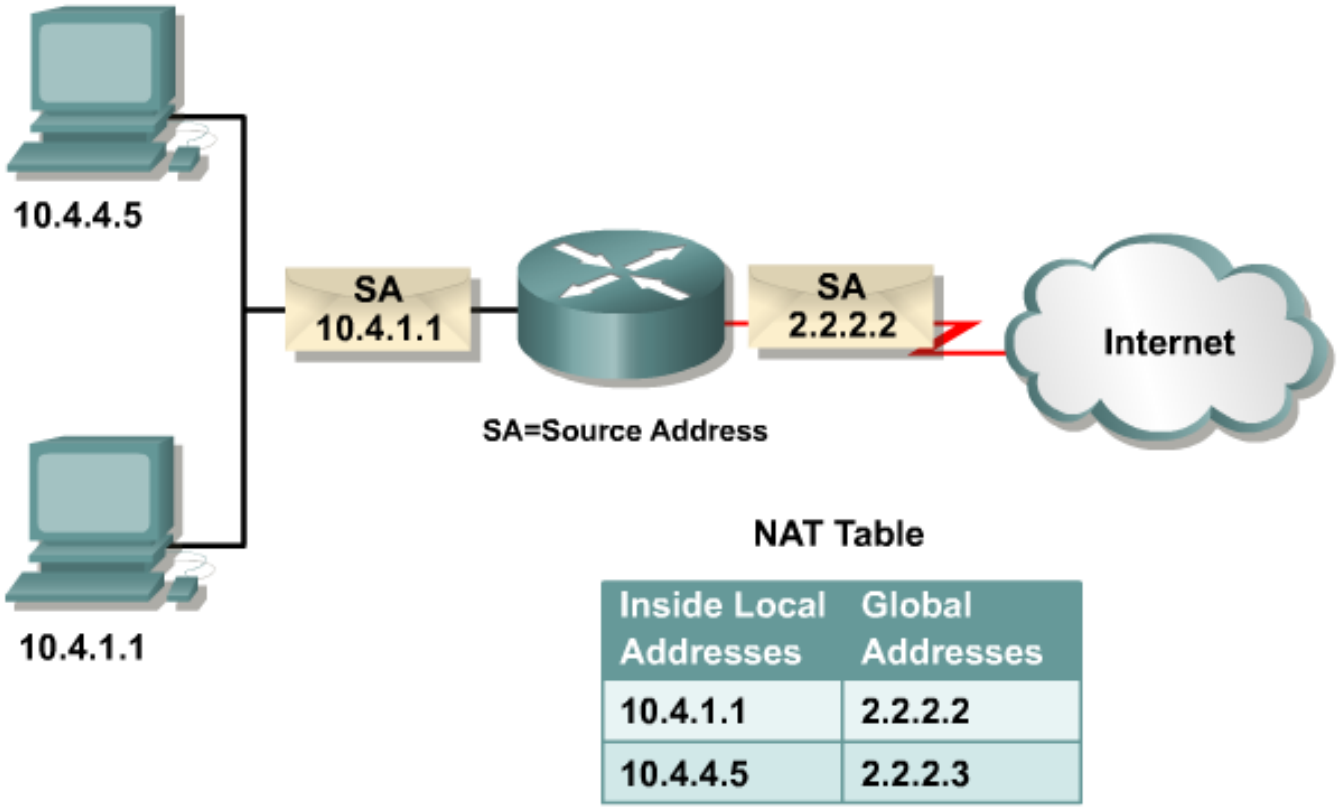


NAT Table

Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global Address
10.0.0.2:1331 10.0.0.4:1444	179.9.8.20:1331 179.9.8.80:1445	202.6.3.2:80 128.23.2.2:80	202.6.3.2:80 128.23.2.2:80

Table

- The device that is having the NAT function registers an association between internal and external addresses.



Inside Local Addresses	Global Addresses
10.4.1.1	2.2.2.2
10.4.4.5	2.2.2.3

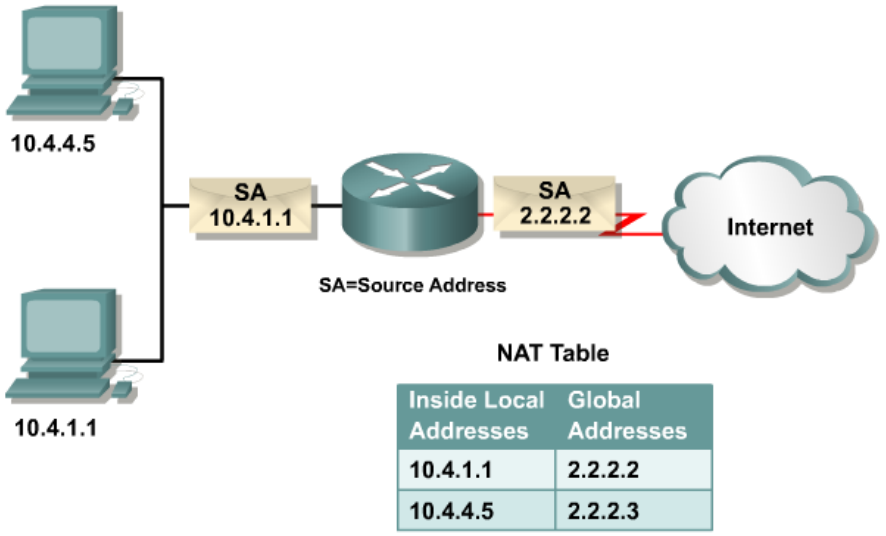
Types

- There are the following NAT types:
  - **Static NAT** - A public IP address for a private IP address.
  - **Dynamic NAT** - There is a set of public addresses (pool), which machines that use private addresses can use.
  - **PAT (Network Address Port Translation) or NAT Overload** - A public IP address for "n" private IP addresses. This is certainly the most commonly used technique.
  - **Twice NAT** - public address is provided under internal or external conditions or conditions.
  - **Destination NAT** - give a private address to a machine with the public address (almost a "reverse NAT").

Static NAT

- Static NAT directly maps private addresses to public addresses. A private IP will always be associated with the same public IP ('one-to-one' rule).
- This type of NAT is useful when you want to reference a certain device with a consistent and constant IP address.
- However, it does not allow management and “saving” of the available public addresses since a private address corresponds to a public address.
- Used when a machine with a private address is required to “leave” always with the same public address.

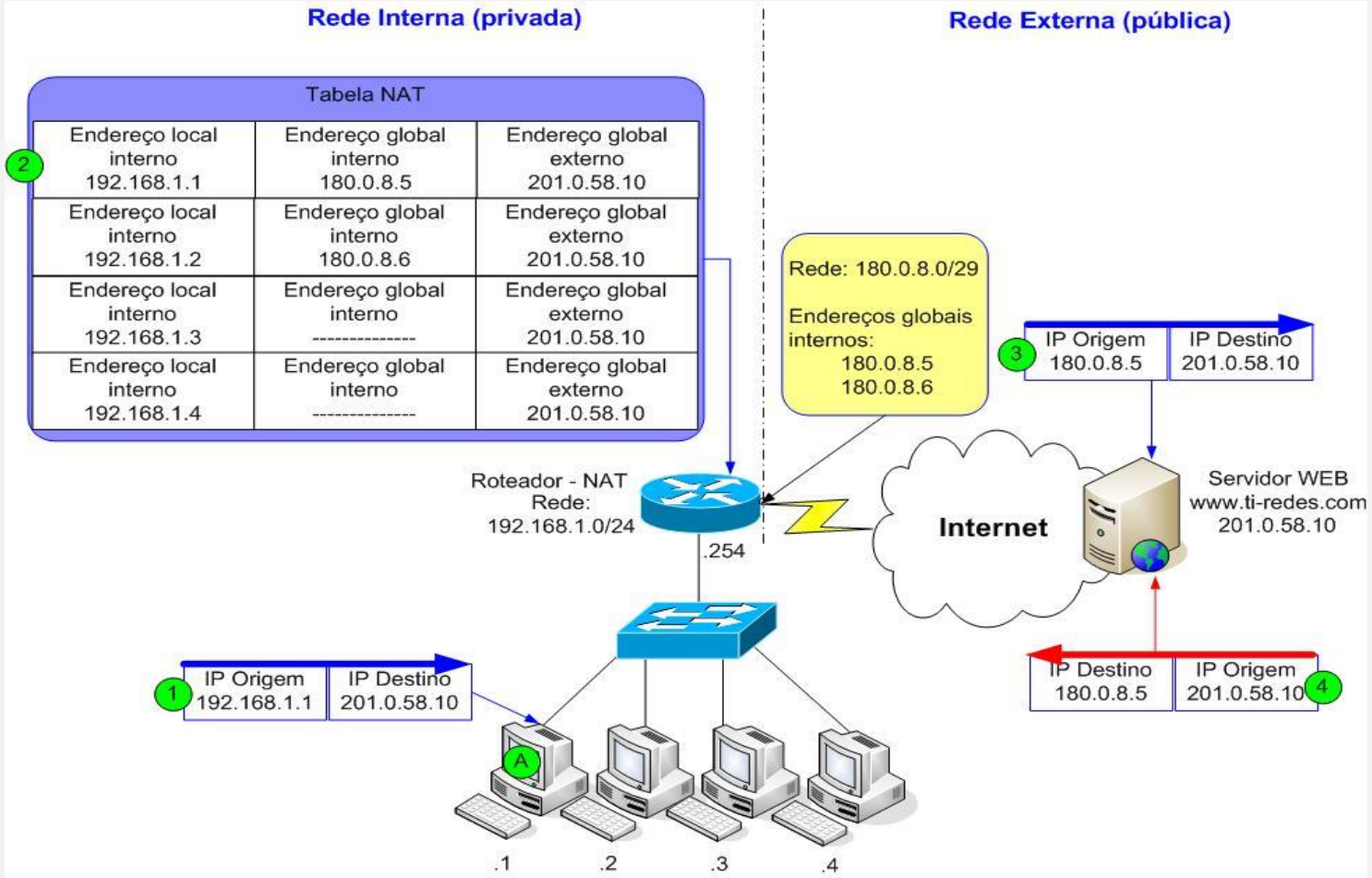
Static NAT



NAT Table

Inside Local Addresses	Global Addresses
10.4.1.1	2.2.2.2
10.4.4.5	2.2.2.3

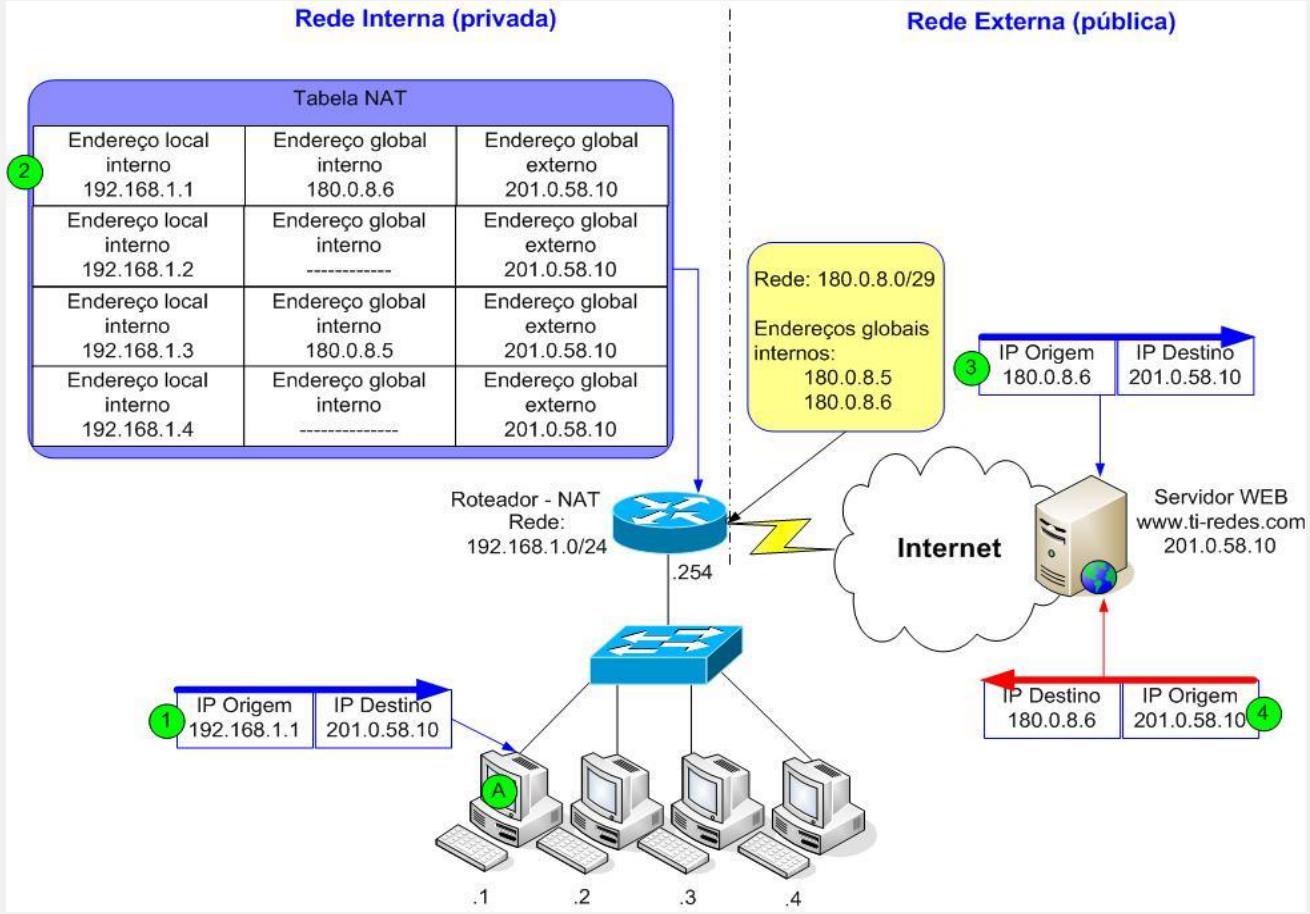
Static NAT


Rede Interna (privada)
Rede Externa (pública)
Tabela NAT
Endereço local interno 192.168.1.1
Endereço global interno 180.0.8.5
Endereço global externo 201.0.58.10
Endereço local interno 192.168.1.2
Endereço global interno 180.0.8.6
Endereço global externo 201.0.58.10
Endereço local interno 192.168.1.3
Endereço global interno ----------
Endereço global externo 201.0.58.10
Endereço local interno 192.168.1.4
Endereço global interno ----------
Endereço global externo 201.0.58.10
Rede: 180.0.8.0/29
Endereços globais internos:
180.0.8.5
180.0.8.6
IP Origem 180.0.8.5
IP Destino 201.0.58.10
Roteador - NAT
Rede:
192.168.1.0/24
.254
Internet
Servidor WEB
www.ti-redes.com
201.0.58.10
IP Origem 192.168.1.1
IP Destino 201.0.58.10
IP Destino 180.0.8.5
IP Origem 201.0.58.10
.1
.2
.3
.4

Dynamic NAT

- Dynamic NAT dynamically maps private addresses to public addresses.
- Thus, any private address can be translated to a range of public addresses dynamically.
- Unlike Static NAT, internal addresses are not always translated into the same public address.
- It allows to make a more efficient management of the available public addresses.

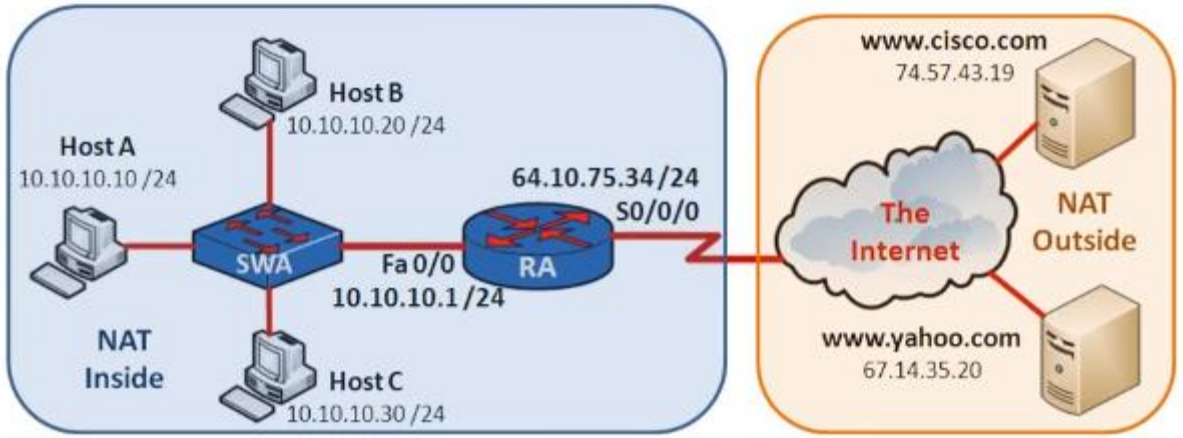
Dynamic NAT


Rede Interna (privada)
Rede Externa (pública)
Tabela NAT
Endereço local interno 192.168.1.1
Endereço global interno 180.0.8.6
Endereço global externo 201.0.58.10
Endereço local interno 192.168.1.2
Endereço global interno ----------
Endereço global externo 201.0.58.10
Endereço local interno 192.168.1.3
Endereço global interno 180.0.8.5
Endereço global externo 201.0.58.10
Endereço local interno 192.168.1.4
Endereço global interno ----------
Endereço global externo 201.0.58.10
Rede: 180.0.8.0/29
Endereços globais internos:
180.0.8.5
180.0.8.6
IP Origem 180.0.8.6
IP Destino 201.0.58.10
Roteador - NAT
Rede:
192.168.1.0/24
.254
Internet
Servidor WEB
www.ti-redes.com
201.0.58.10
IP Origem 192.168.1.1
IP Destino 201.0.58.10
IP Destino 180.0.8.6
IP Origem 201.0.58.10
A
.1
.2
.3
.4

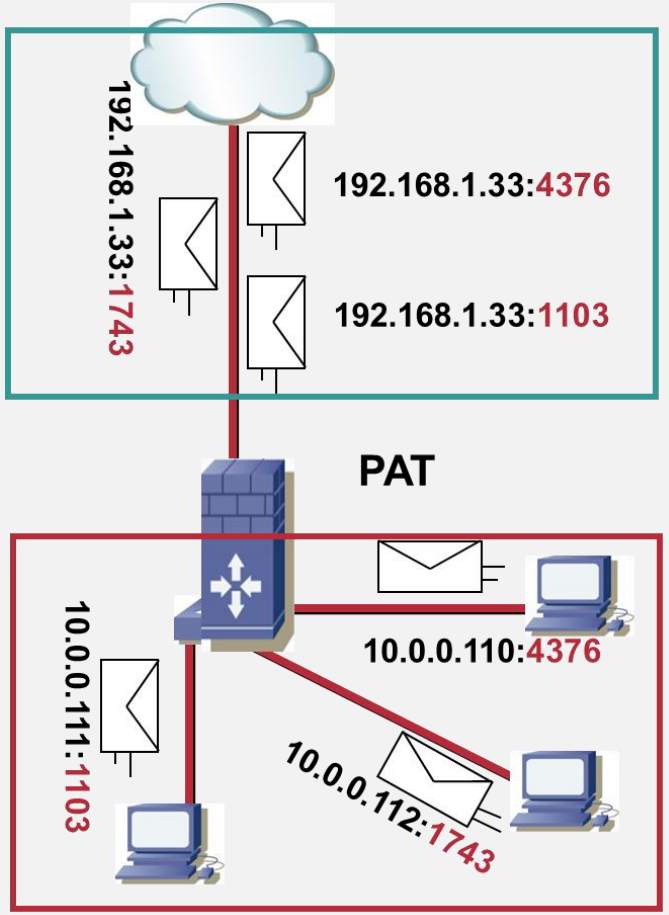
PAT - Network Address Port Translation or NAT Overload

- The PAT or NAT Overload appears as the most used solution since it does not require as many public addresses as the equipment that intends to communicate with the outside.
- In this way, numerous devices can use the same public address, as they will be differentiated by the port number used.
- The distinction between communications is made on the basis of port origin:
  - When two devices intend to communicate using the same value for the source port, the NAT service uses the next port that is free.
  - If there are no free ports but a pool with multiple IP addresses has been configured, the next IP address is used, trying to respect the originally chosen port.

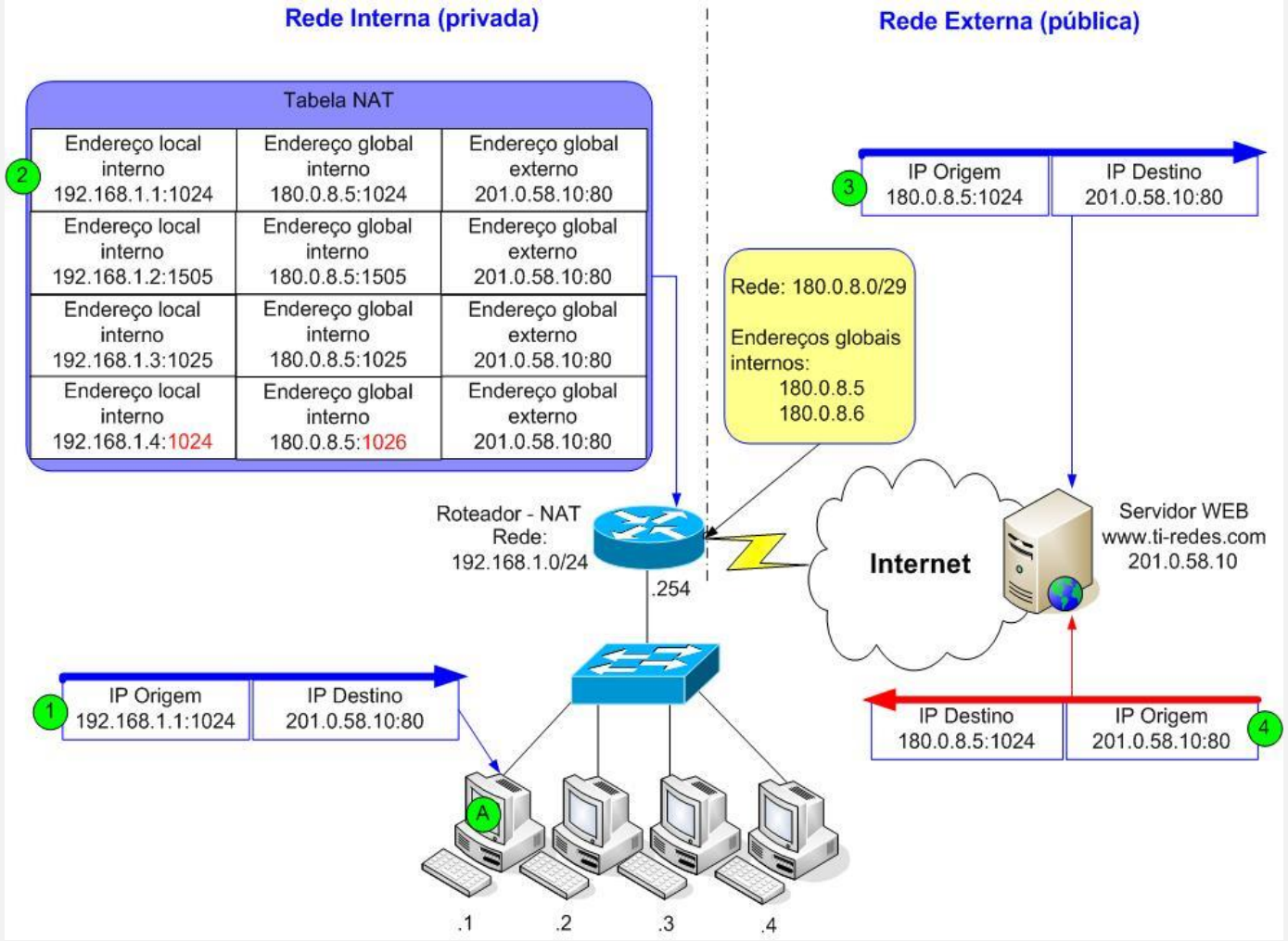
PAT or NAT Overload



Inside Local	Inside Global	Outside Global
10.10.10.10::5097	64.10.75.34::5097	74.57.43.19::80
10.10.10.30::5097	64.10.75.34::6021	67.14.35.20::80
10.10.10.10::9000	64.10.75.34::8701	67.14.35.20::80



PAT or NAT Overload

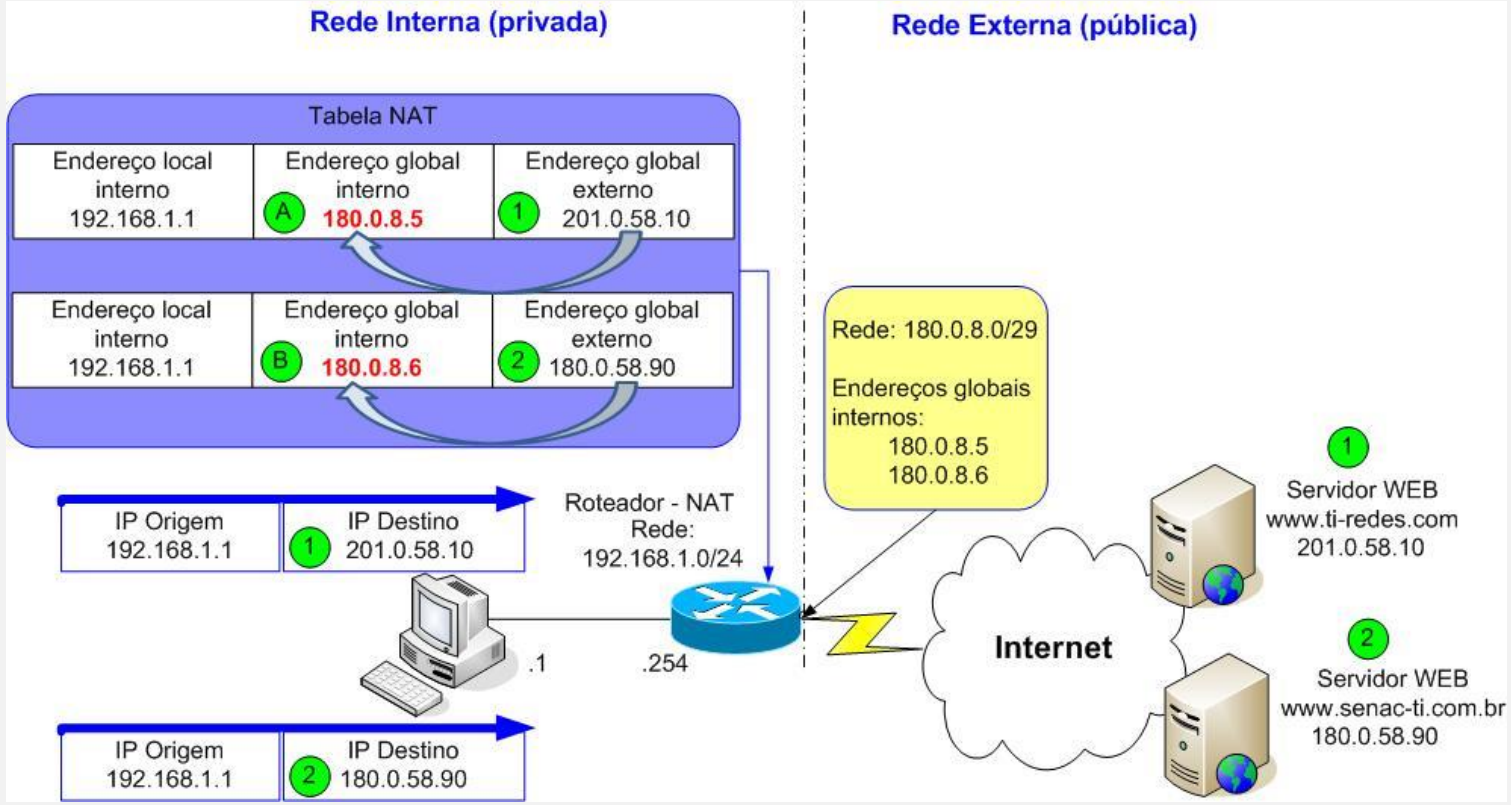


Twice NAT

- Twice NAT allows you to decide which public address will be used in the mapping process, based on the destination IP or the destination port number.
- You can create rules to determine that an internal address is translated to a particular public address, taking as its determinant its destination.
- Or in the case of ports, the determinant will be the destination port number.

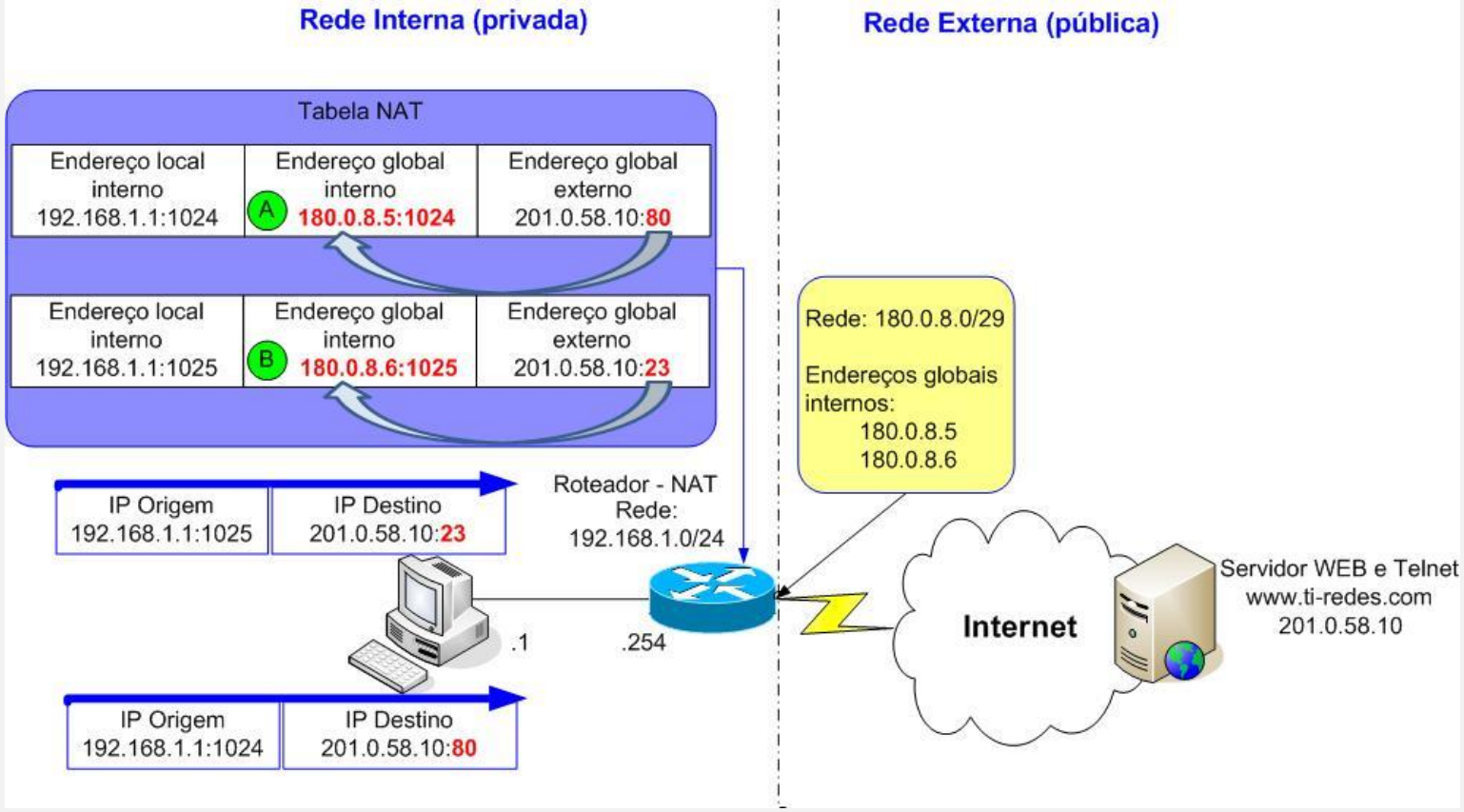
Twice NAT

- **Determiner:** Destination IP address



Twice NAT

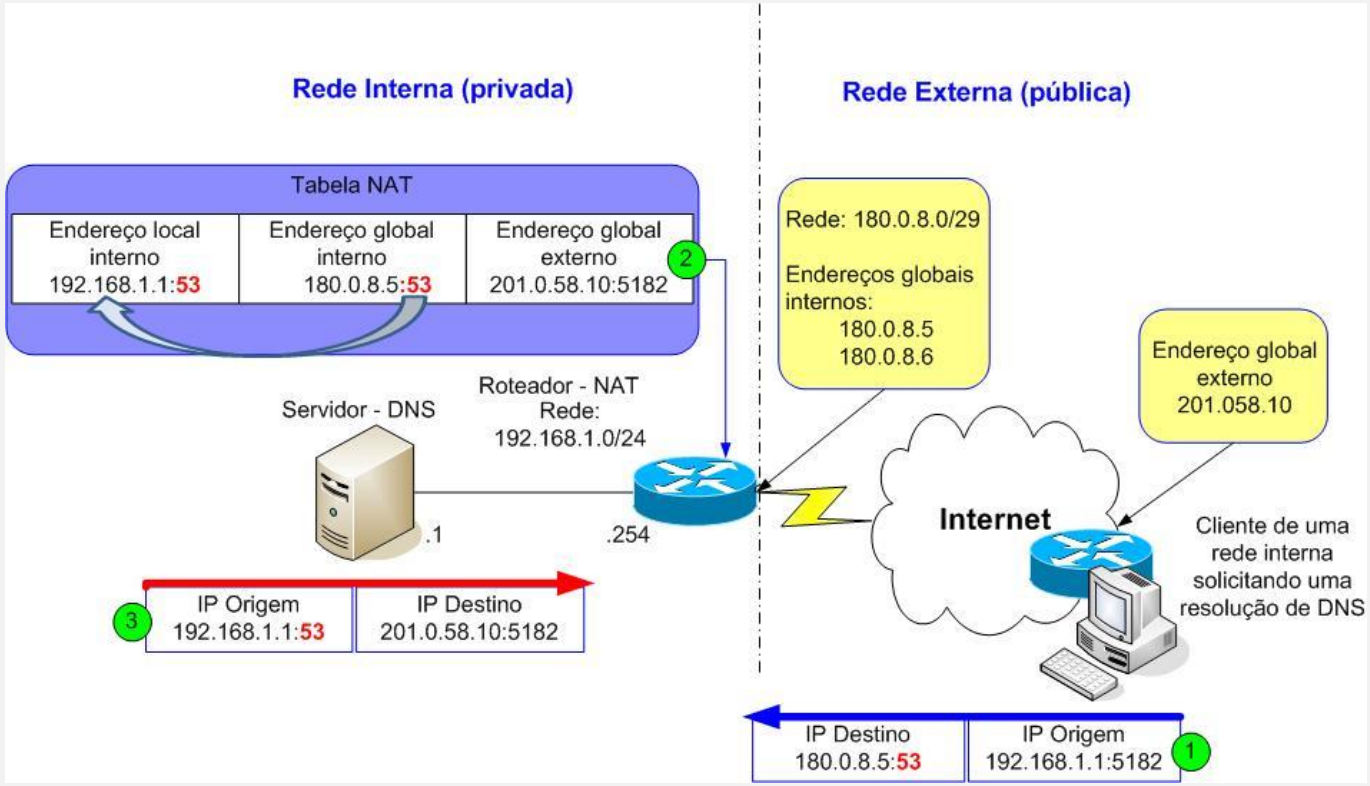
- **Determiner:** Destination port number.



Destination NAT

- With Destination NAT, connections are initiated from public network (Internet) hosts.
- This feature has been incorporated into NAT to enable more advanced capabilities / functionality.
- Because, the external network hosts do not know the IP address of hosts on the internal network, so they could not access a resource that was located internally. For this to happen we have to do a "Reverse NAT".

Destination NAT



NAT - Fases

- **output datagrams:** replace (private source IP address, port) of each output datagram by (public IP address, new port)
  - Remote clients / servers respond using the destination address (public IP address, new port).
- **save** in the NAT translation table all pairs (source private IP address, port), (public IP address, new port).
- **Input datagrams:** Replace (public IP address, new port) in the destination address field of each input datagram the corresponding value in the translation table NAT (source private IP address, port).

Network Address Translation (NAT) - Cisco

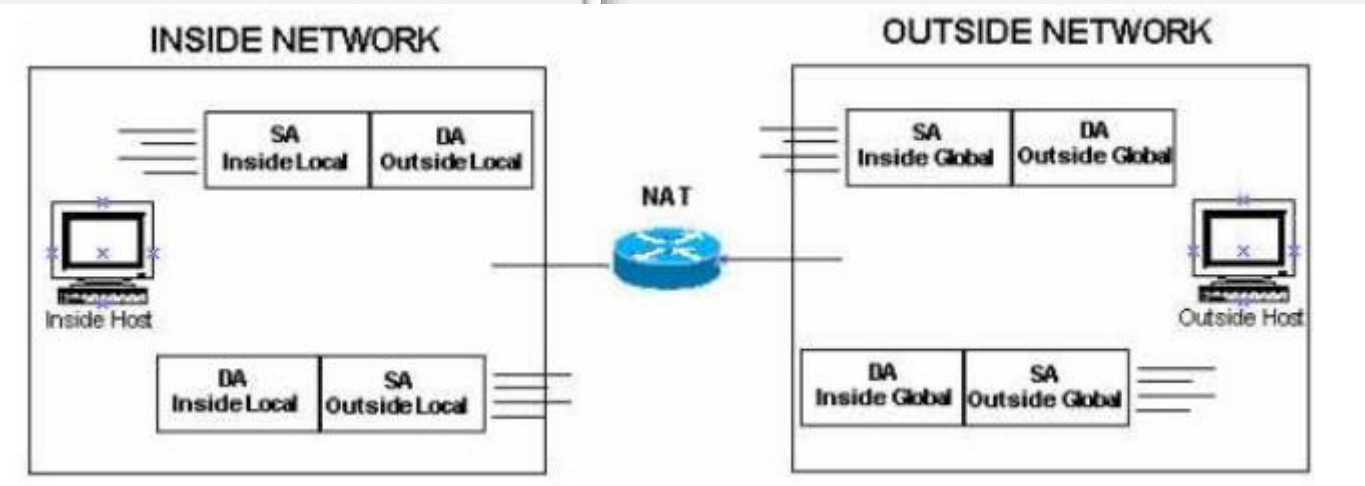
Network Services 1

School Year 2019-2020

Static NAT: configuration

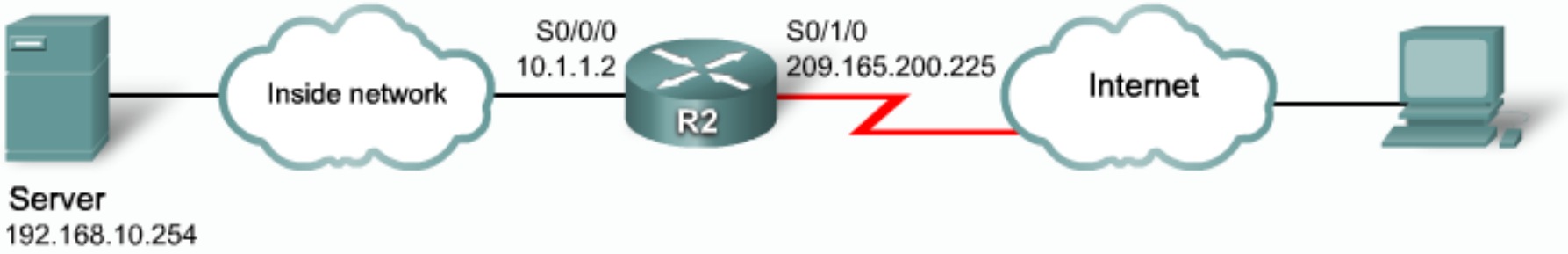
Configuring Static NAT

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



Static NAT: configuration

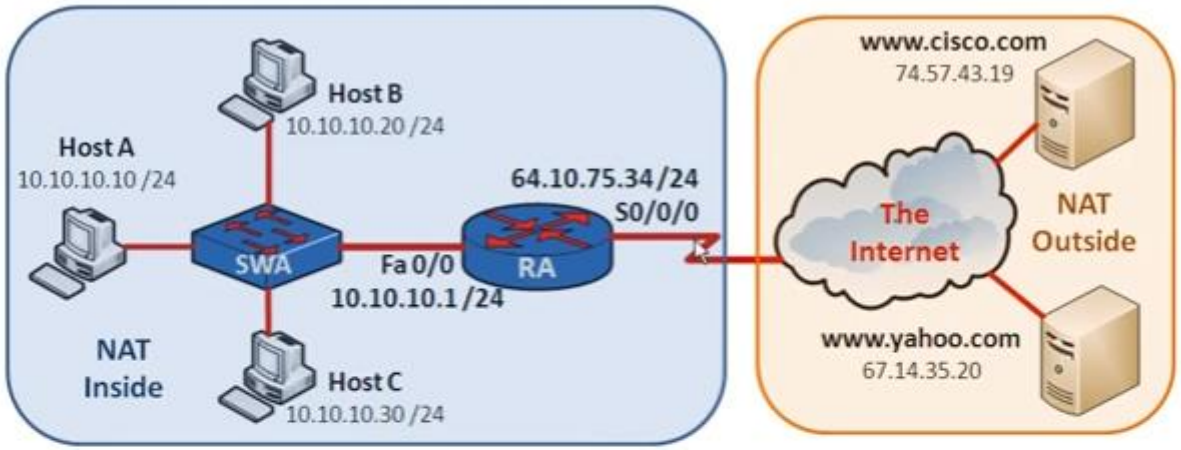
Configuring Static NAT




```
ip nat inside source static 192.168.10.254 209.165.200.254
!–Establishes static translation between an inside local address and an inside global address.
interface serial 0/0/0
ip nat inside
!—Identifies Serial 0/0/0 as an inside NAT interface.
interface serial 0/1/0
ip nat outside
!—Identifies Serial 0/1/0 as an outside NAT interface.
```

With this configuration, 192.168.10.254 will always translate to 209.165.200.254

Static NAT: configuration



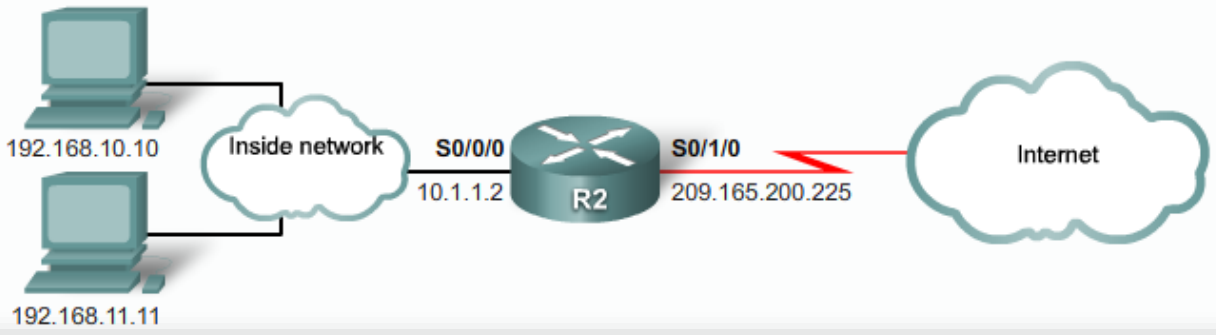

```
RA(config)#      ip nat inside source static 10.10.10.10 64.10.75.99
RA(config)#      interface Fa 0/0
RA(config-if)#   ip nat inside
RA(config-if)#   exit
RA(config)#      interface S 0/0/0
RA(config-if)#   ip nat outside
```

Dynamic NAT: configuration

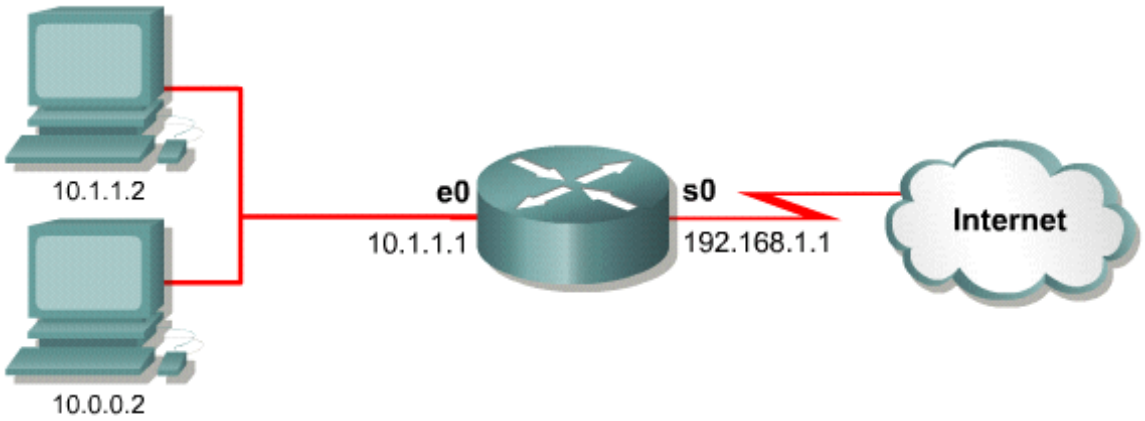
Configuring Dynamic NAT

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

Dynamic NAT: configuration

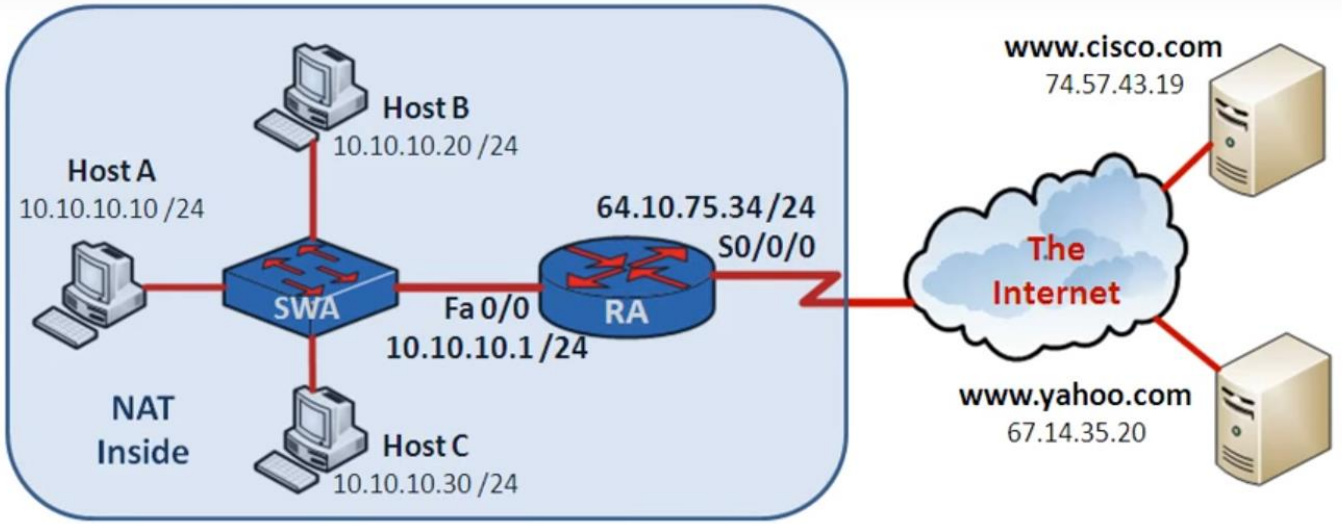



```
ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
!—Defines a pool of public IP addresses under the pool name NAT-POOL1
access-list 1 permit 192.168.0.0 0.0.255.255
!—Defines which addresses are eligible to be translated
ip nat inside source list 1 pool NAT-POOL1
!—Binds 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
```

Dynamic NAT: configuration




```
RA(config)#      ip nat pool test 64.10.75.80 64.10.75.99 netmask 255.255.255.0
RA(config)#      access-list 10 permit 10.10.10.0 0.0.0.255
RA(config)#      ip nat inside source list 10 pool test
RA(config)#      interface Fa 0/0
RA(config-if)#   ip nat inside
RA(config-if)#   exit
RA(config)#      interface S 0/0/0
RA(config-if)#   ip nat outside
```

NAT overload: configuration

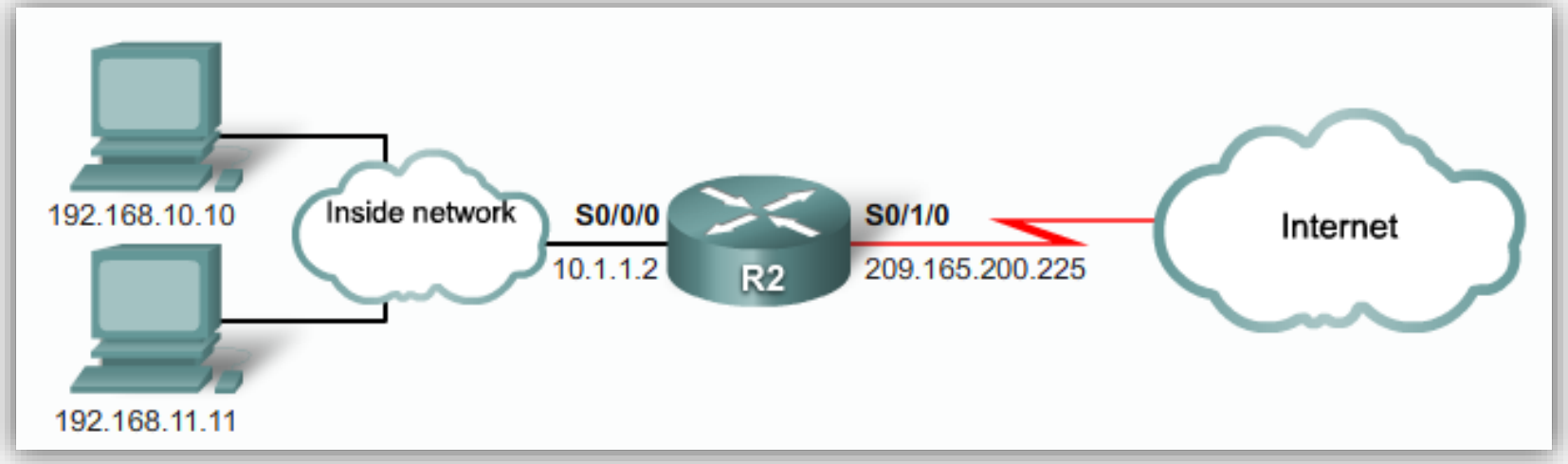
We can configure using a range of IP address:

Step	Action	Notes
1	Define a standard access list permitting those addresses that are to be translated. `Router(config)#access-list acl-number permit source [source-wildcard]`	Enter the global command `no access-list access-list-number` to remove the access list.
2	Specify the global address, as a pool, to be used for overloading. `Router(config)#ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}.`	
3	Establish overload translation. `Router {config} #ip nat inside source list acl-number pool name overload.`	

4	Specify the inside interface.
	`Router(config)#interface type number`
	`Router(config-if)#ip nat inside`
		Enter the `interface` command. The CLI prompt will change from `(config)#` to `(config-if)#`.

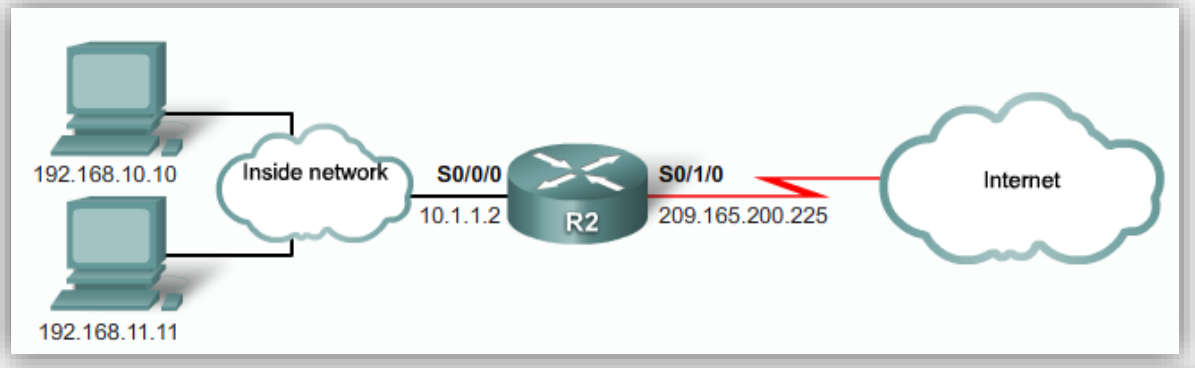
5	Specify the outside interface.
	`Router(config-if)#interface type number`
	`Router(config-if)#ip nat outside`	

NAT overload: configuration



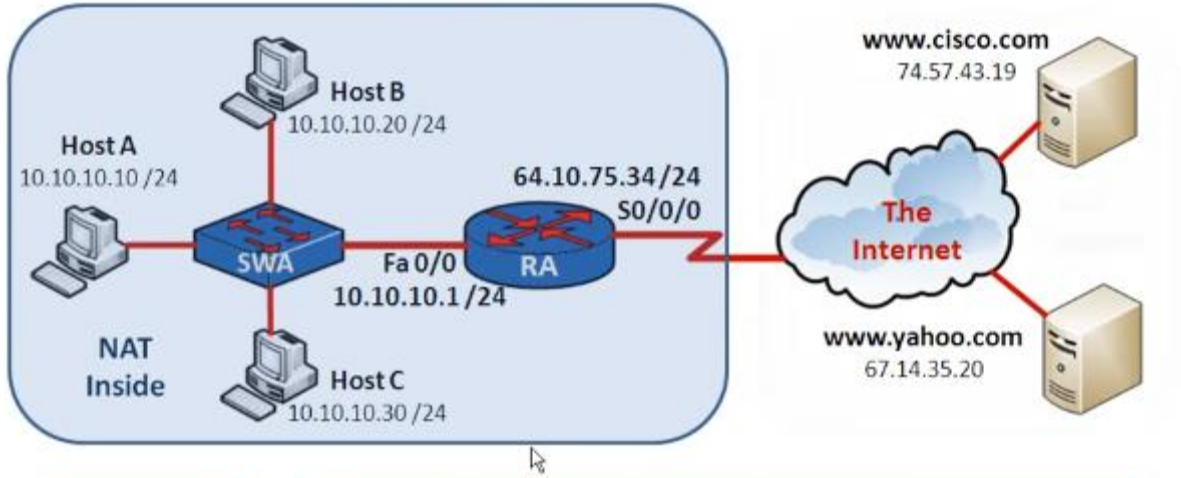

```
access-list 1 permit 192.168.0.0 0.0.255.255
!—Defines which addresses are eligible to be translated
ip nat inside source list 1 interface serial 0/1/0 overload
!—Identifies the outside interface Serial 0/1/0 as the inside global address to be overloaded
interface serial 0/0/0
  ip nat inside
!—Identifies 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
```

NAT overload: configuration



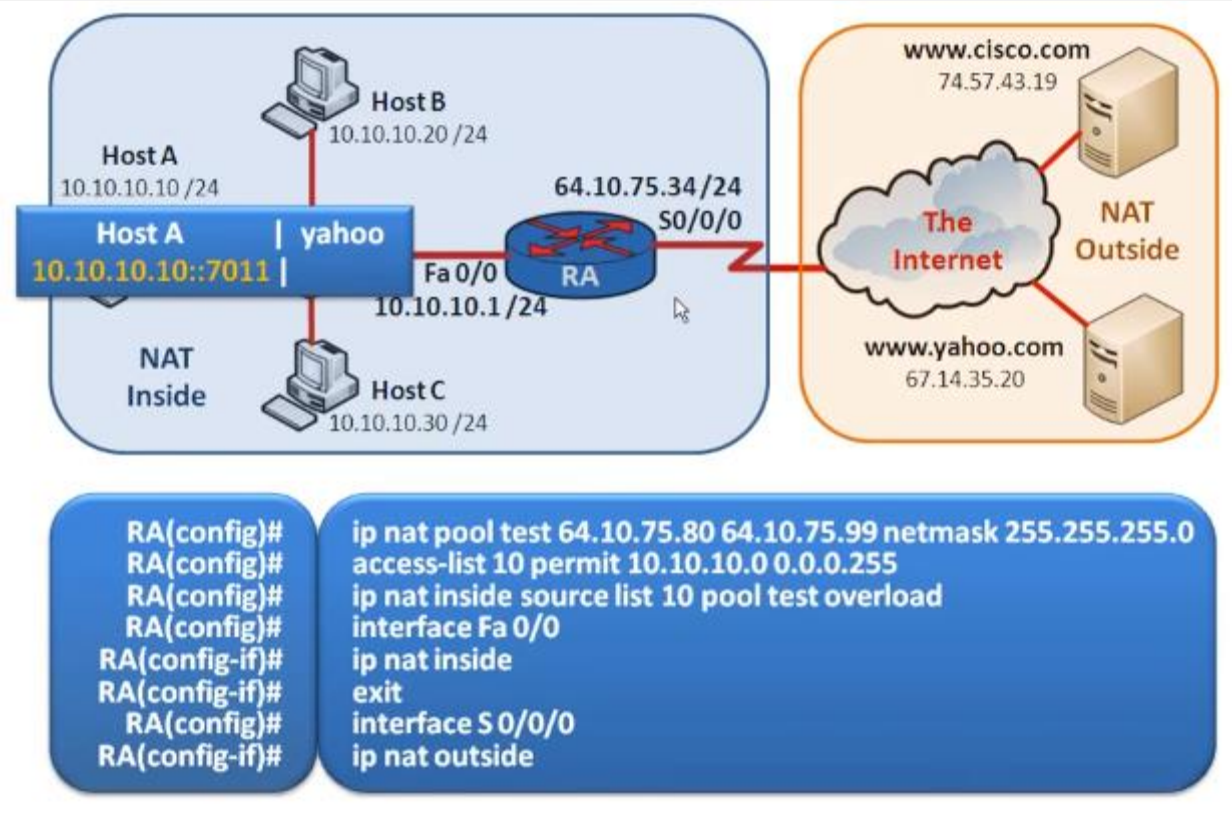

```
access-list 1 permit 192.168.0.0 0.0.255.255
! – Defines which addresses are eligible to be translated
ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240
! – Defines a pool of addresses named NAT-POOL2 to be used in NAT translation
ip nat inside source list 1 pool NAT-POOL2 overload
! – Binds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

NAT overload: configuration



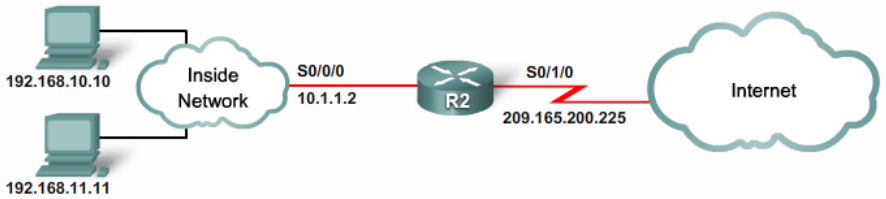

```
RA(config)#      access-list 10 permit 10.10.10.0 0.0.0.255
RA(config)#      ip nat inside source list 10 interface S 0/0/0 overload
RA(config)#      interface Fa 0/0
RA(config-if)#   ip nat inside
RA(config-if)#   exit
RA(config)#      interface S 0/0/0
RA(config-if)#   ip nat outside
```

NAT overload: configuration



NAT Configuration Check

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#
```

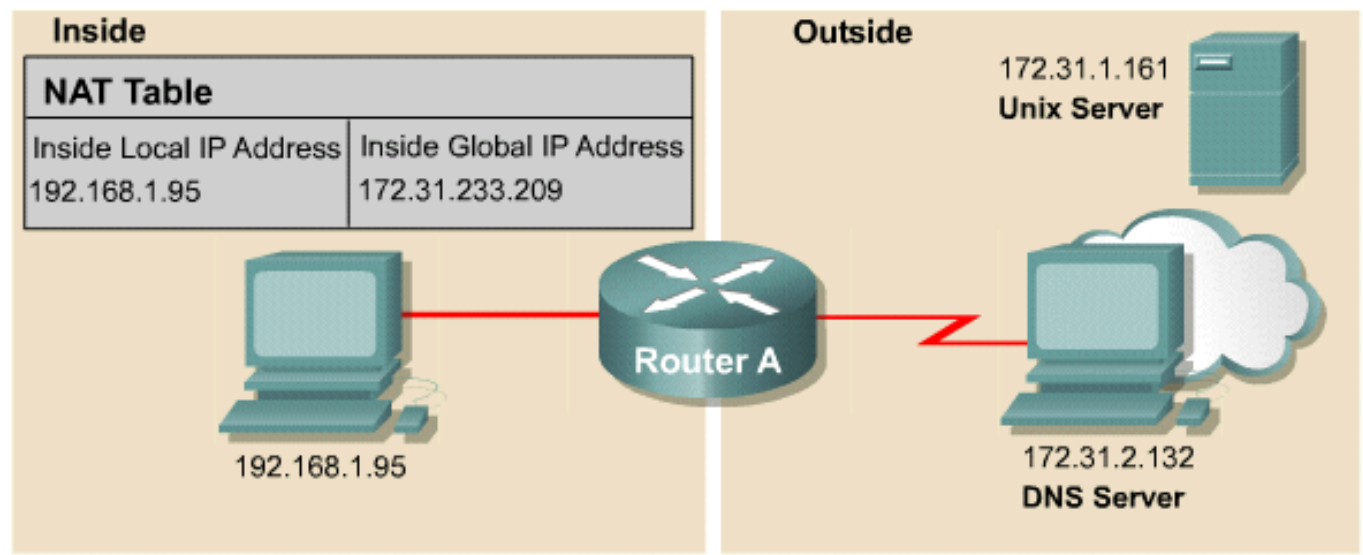
Clearing NAT Translations

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

R2#
```

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

NAT Configuration Check



outgoing

incoming

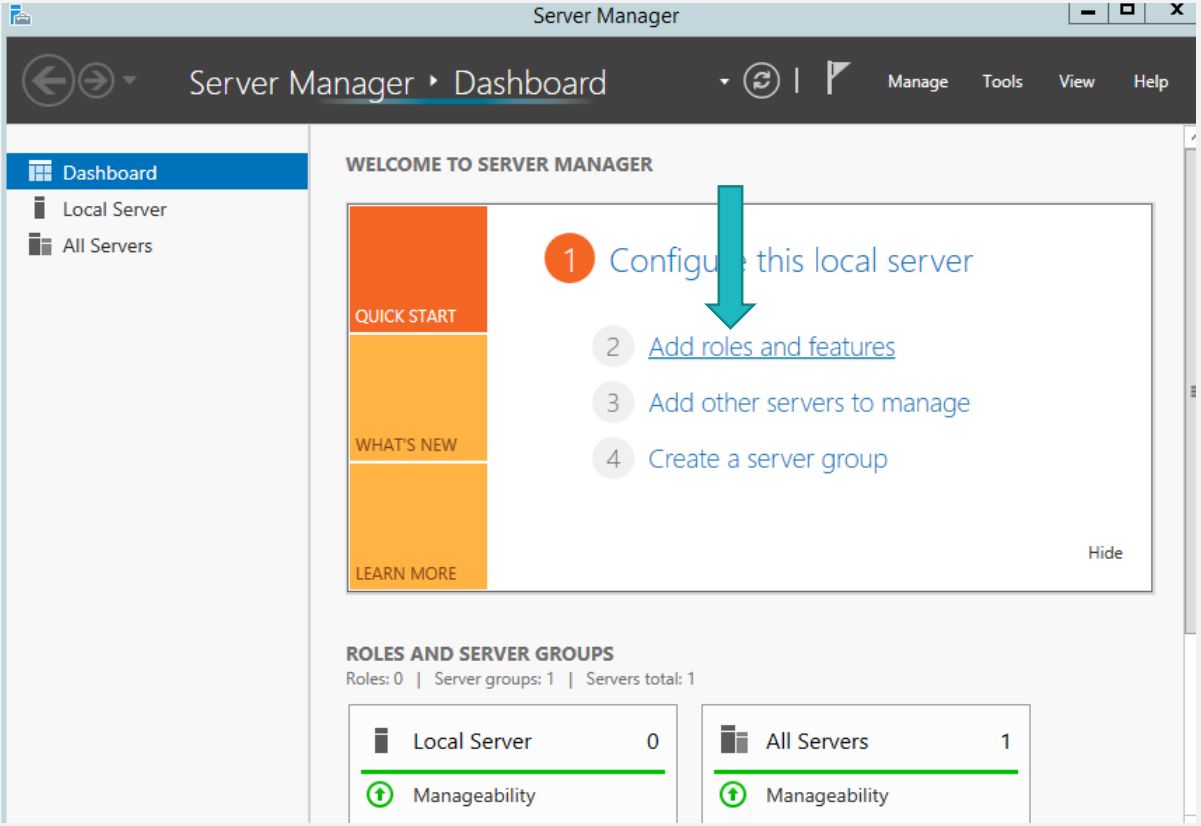
```
RouterA#debug ip nat
NAT:   s= 192.168.1.95    → 172.31.233.209,      d=172.31.2.132 [6825]
NAT:   s= 172.31.2.132,     d=172.31.233.209,    → 192.168.1.95 [21852]
NAT:   s= 192.168.1.95    → 172.31.233.209,      d=172.31.1.161 [6826]
NAT*:  s= 172.31.1.161,     d=172.31.233.209,    → 192.168.1.95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

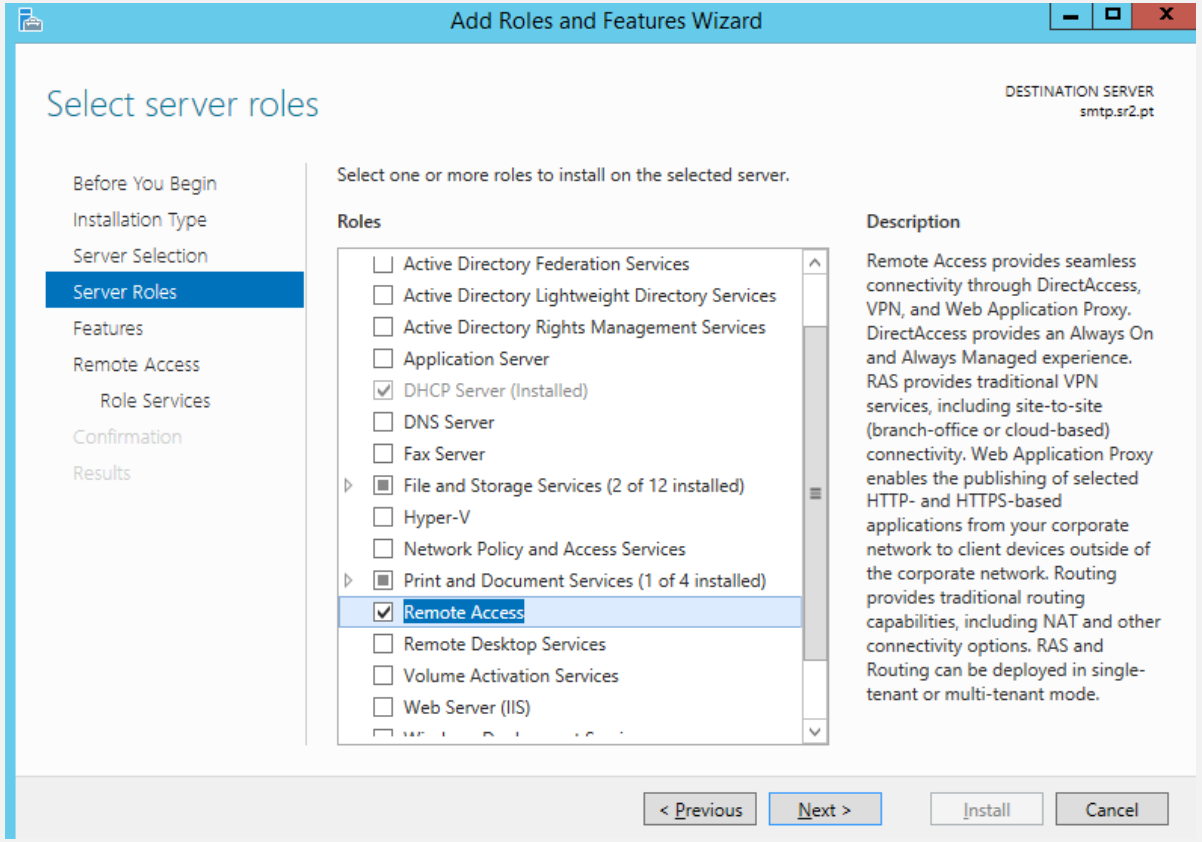
Network Address Translation (NAT) - Windows

Network Services 1

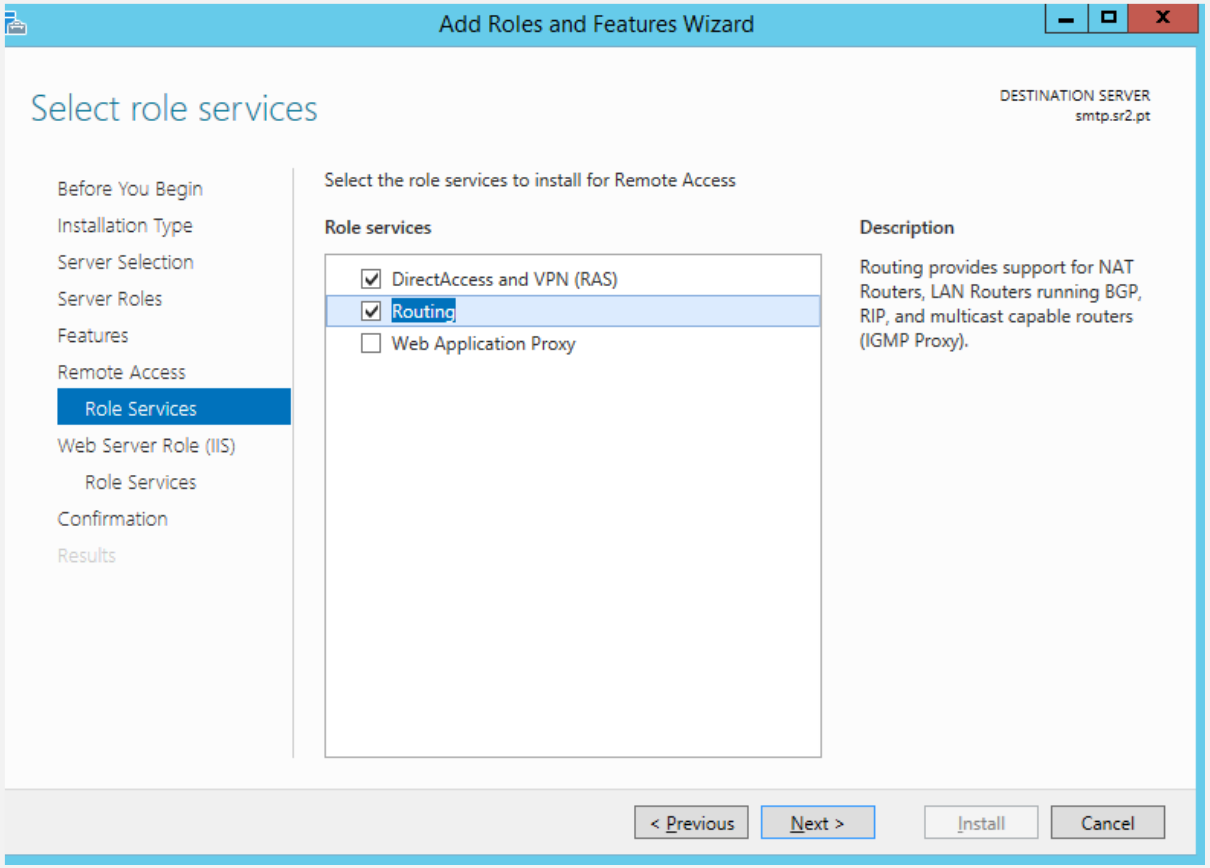
School Year 2019-2020

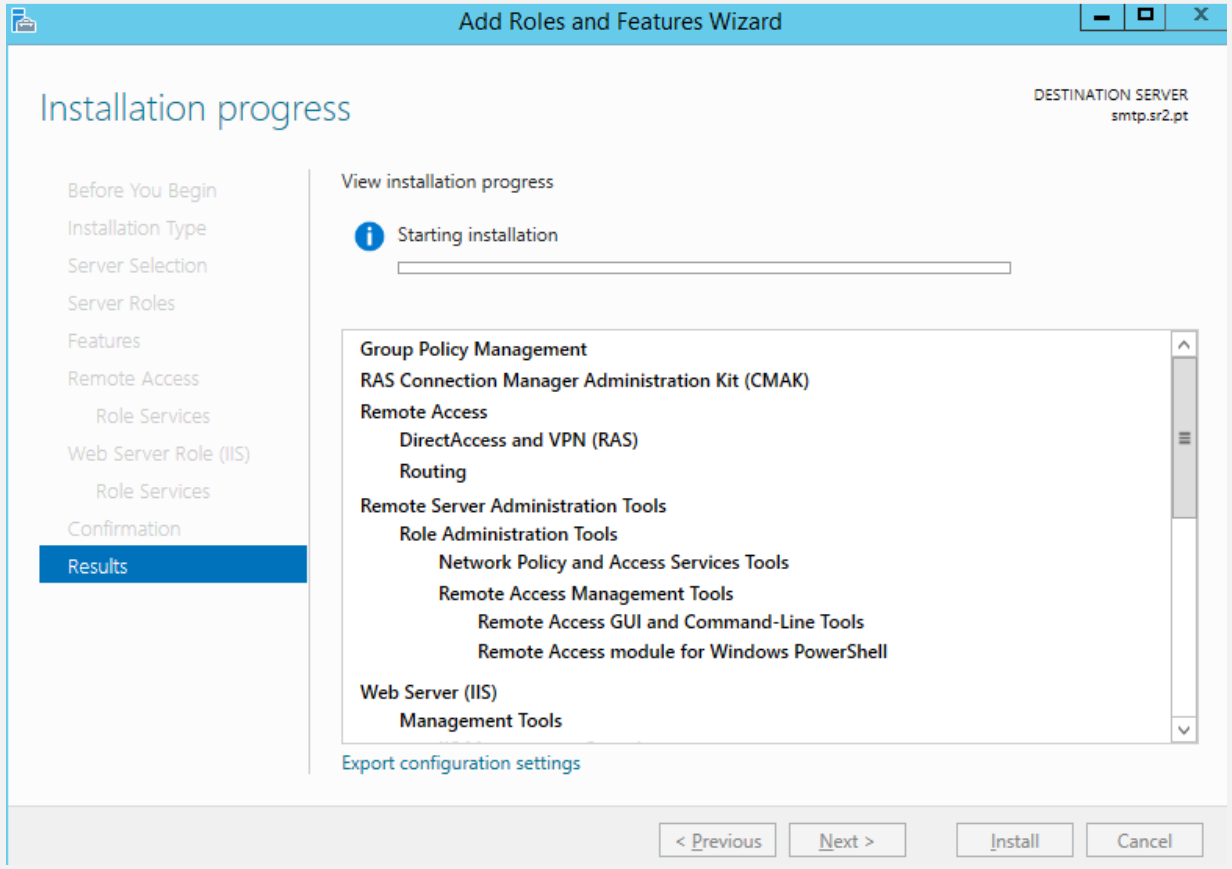
Service installation



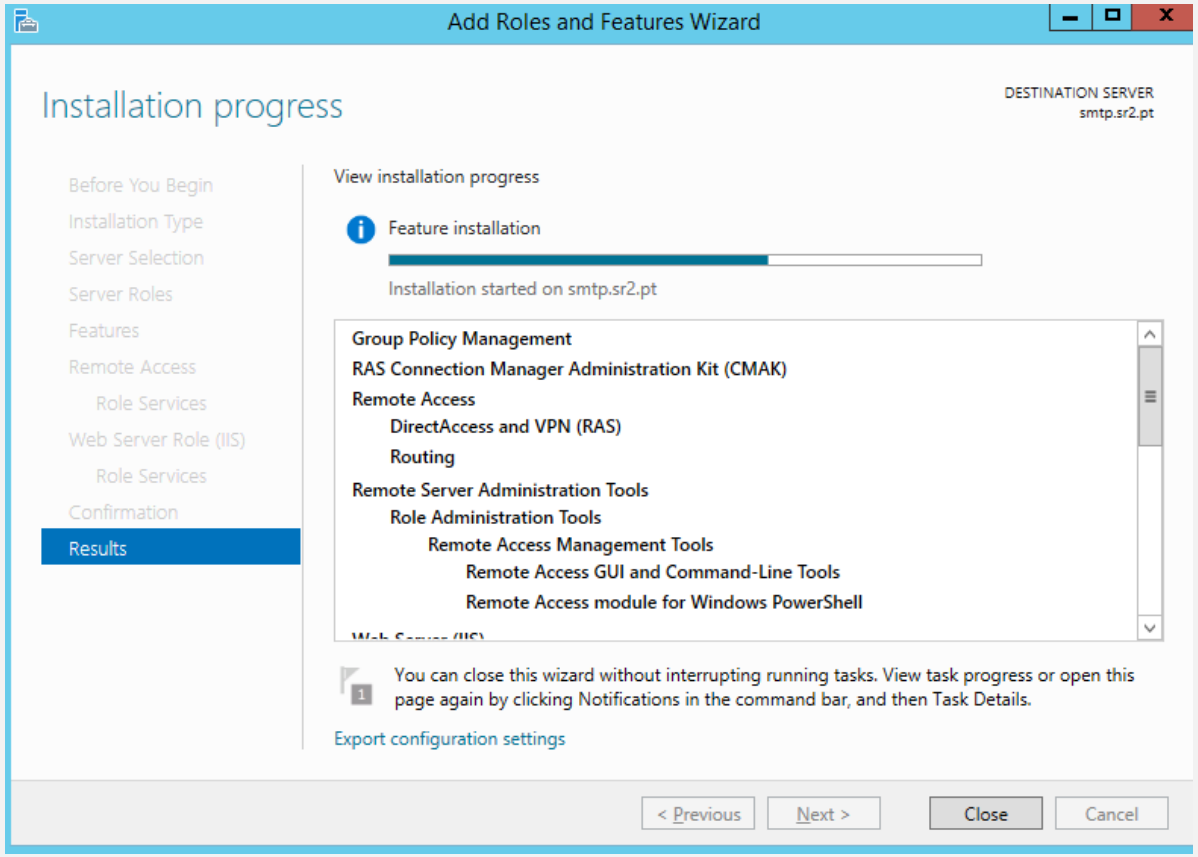


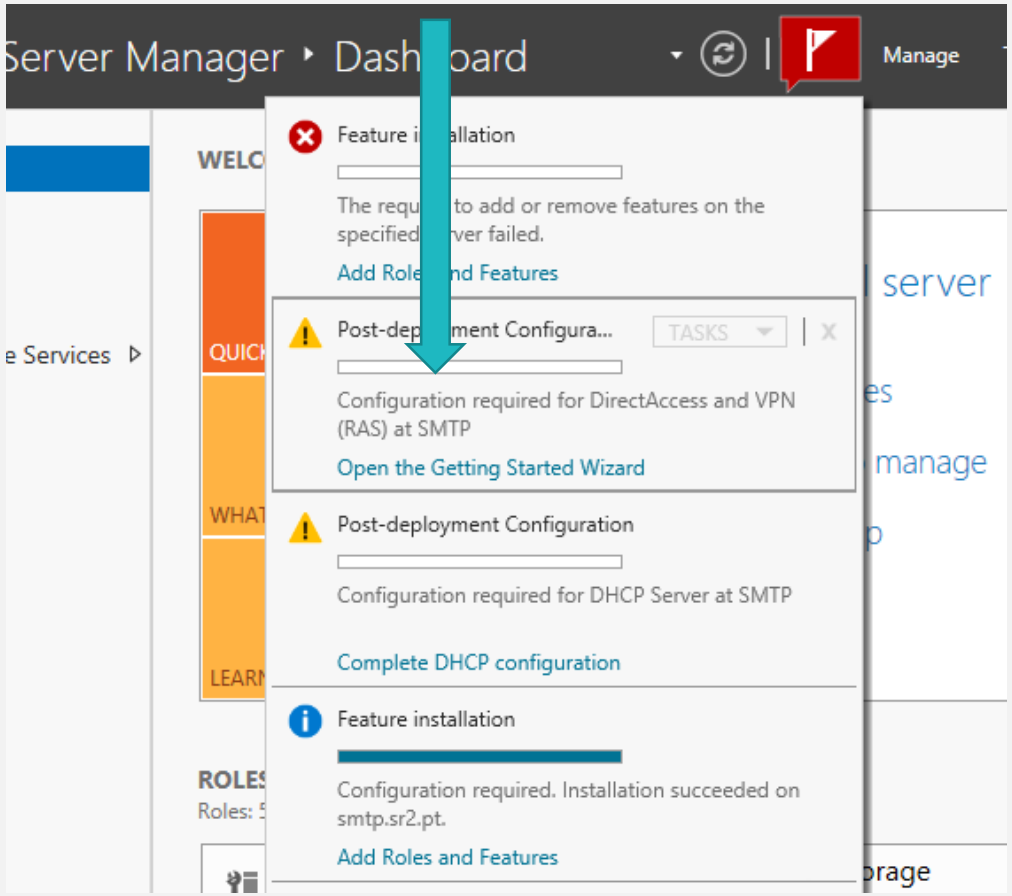
Service installation



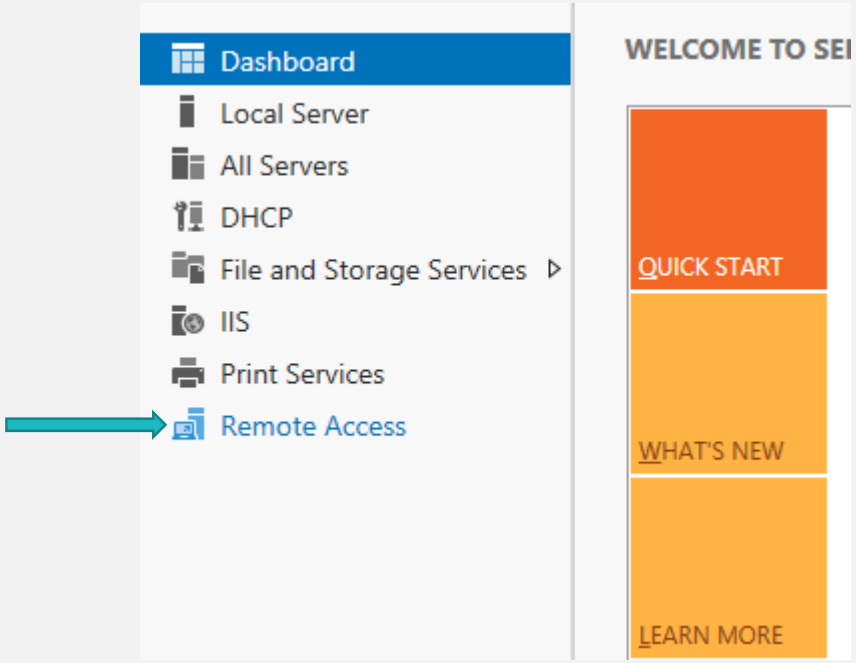


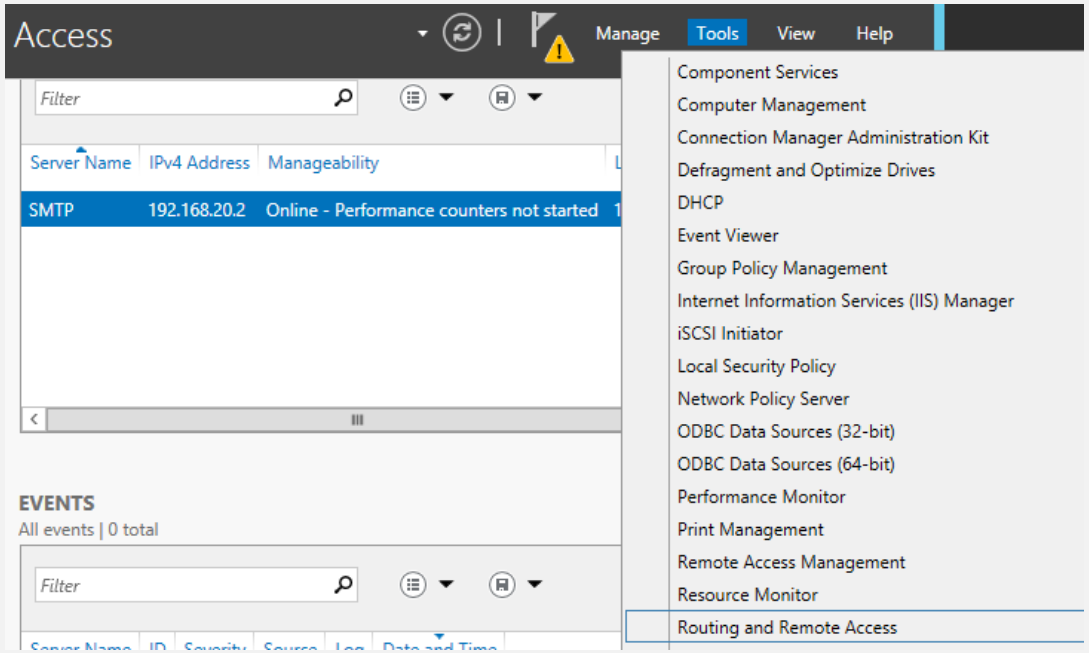
Service installation



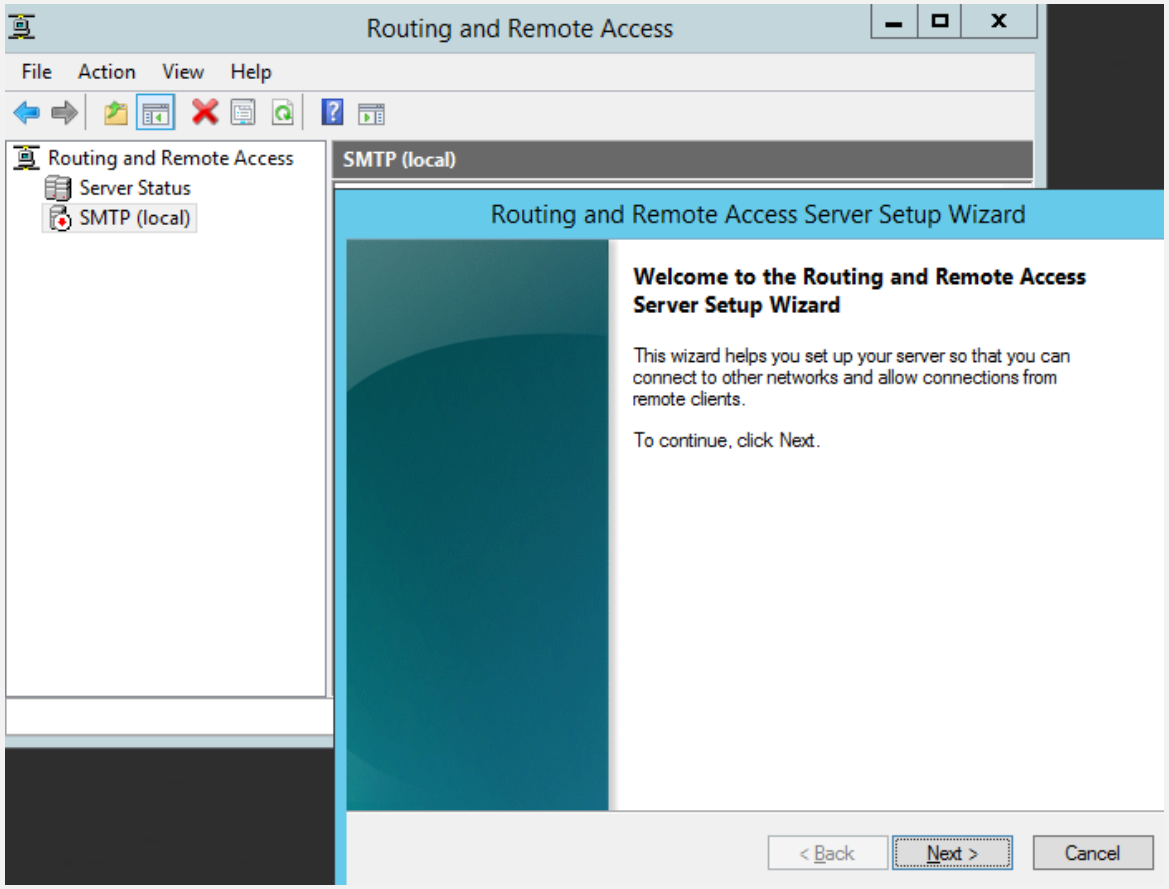


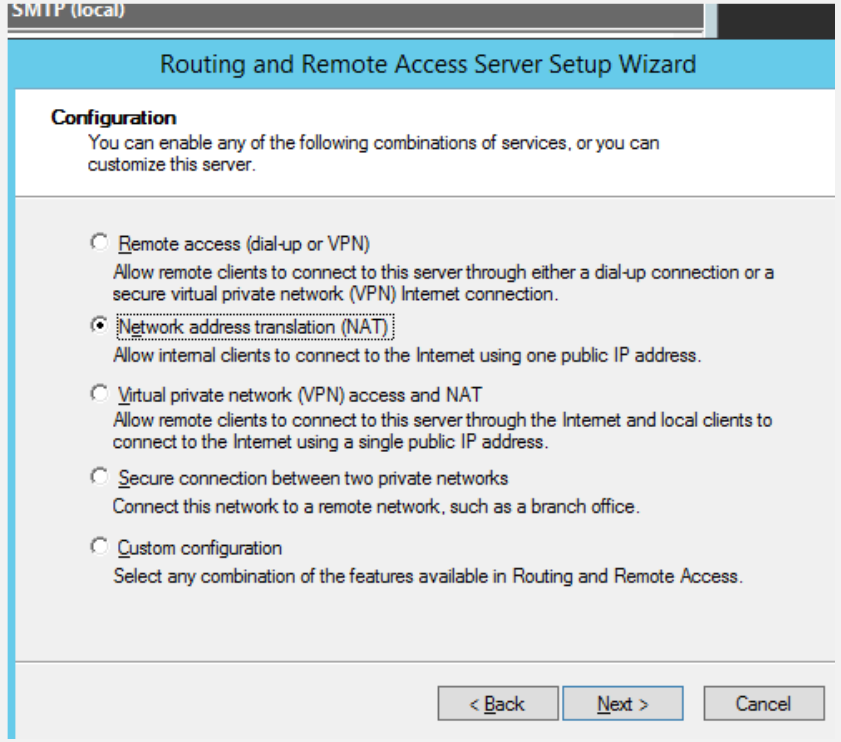
Service installation





Service installation





Doubts

References

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