Netwok Address Translation
NAT
and Port Address Translation
PAT

Giới thiệu

Trên thực tế, có vài loại NAT khác nhau nhưng tôi muốn tập trung nói đến loại có ưu điểm nổi bật là NAT/PAT (Network Address Translation combined with Port Address Translation) và được gọi tắt là "NATPT"

NAT: Địa chỉ IP riêng của mạng LAN được dịch chuyển tới 1 địa chỉ công cộng, do đó chỉ nhìn thấy địa chỉ công cộng của mạng từ Internet.

PAT: Trong các phiên truyền dữ liệu từ các máy trạm đã đều sử dụng chung 1 địa chỉ IP công cộng và chức năng PAT sẽ dịch chuyển các địa chỉ cổng trên mạng LAN nội bộ thành địa chỉ cổng khác trên Internet để tránh các tấn công của các Hacker

Dynamic NAT mapping - bản đồ NAT động : Định tuyến NAT (NAT router) sẽ "nhớ" các yêu cầu đã gửi từ các máy trạm trên mỗi port gọi là "bản đồ NAT động" khi server trả lời các yêu cầu xuất phát từ định tuyến NAT, nó sẽ gửi lại dữ liệu trên cùng cổng mà đã được sử dụng với yêu cầu tương tự trước đó và NAT router sử dụng bản đồ NAT đó để quyết định gửi dữ liệu tới các máy trạm trên các cổng nào khi có yêu cầu.

Unsolicited data -Dữ Nếu NAT server nhận được dữ liệu từ Internet trên cổng không được sử dụng trong thời gian gần đây và được yêu cầu chuyển tới 1 máy trạm nào đó thì dữ liệu này sẽ bị loại bỏ và không được chuyển tới máy trạm trên mạng LAN nội bộ để đảm bảo an ninh mạng.

Định nghĩa các thuật ngữ

Cisco.com

Cisco định nghĩa các thuật ngữ được sử dụng trong NAT & PAT như sau:

- **Inside local address - Địa chỉ IP được gán cho một host của mạng trong. Đây là địa chỉ được cấu hình như là một tham số của hệ điều hành trong máy tính hoặc được gán một cách tự động thông qua các giao thức như DHCP. Địa chỉ này không phải là những địa chỉ IP hợp lệ được cấp bởi NIC (Network Information Center) hoặc nhà cung cấp dịch vụ Internet.**

- **Inside global address - Là một địa chỉ hợp lệ được cấp bởi NIC hoặc một nhà cung cấp dịch vụ trung gian. Địa chỉ này đại diện cho một hay nhiều địa chỉ IP inside local trong việc giao tiếp với mạng bên ngoài.**

- **Outside local address - Là địa chỉ IP của một host thuộc mạng bên ngoài, các host thuộc mạng bên trong sẽ nhìn host thuộc mạng bên ngoài thông qua địa chỉ này. Outside local không nhất thiết phải là một địa chỉ hợp lệ trên mạng IP (có thể là địa chỉ private).**

- **Outside global address - Là địa chỉ IP được gán cho một host thuộc mạng ngoài bởi người sở hữu host đó. Địa chỉ này được gán bằng một địa chỉ IP hợp lệ trên mạng Internet.**

Định nghĩa các thuật ngữ

Trên đây là các định nghĩa kinh điển của Cisco, tuy nhiên nó không được dễ hiểu cho lắm và đôi khi gây cho chúng ta không ít nhầm lẫn. Trước khi đi vào các ví dụ, ta định nghĩa lại các thuật ngữ trên theo một cách dễ hiểu hơn. Trước hết bạn phải nhớ kỹ rằng khái niệm khái niệm "inside" và "outside" của NAT là các giao diện được cấu hình bởi câu lệnh ip nat inside and ip nat outside. Các mạng nào nối đến các giao diện này sẽ có vai trò inside và outside tương ứng.

Định nghĩa các thuật ngữ

Cisco.com

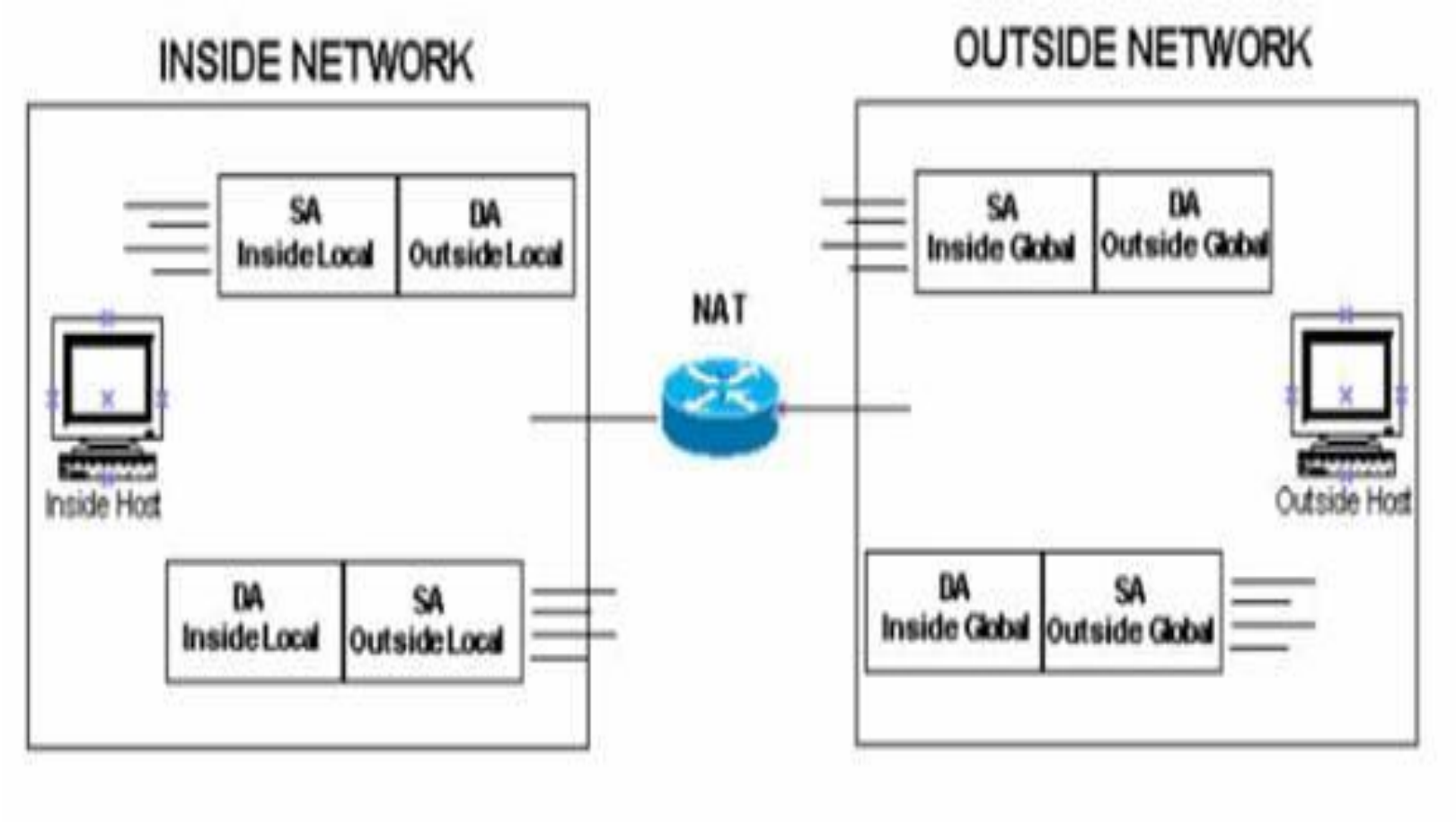
- Local address - Là địa chỉ xuất hiện trong phần “inside” của một network.
- Global address - Là địa chỉ xuất hiện trong phần “outside” của một network.

Các gói tin bắt nguồn từ phần mạng “inside” sẽ có địa chỉ source IP là địa chỉ kiểu “inside local” và destination IP là “ouside local” khi nó còn ở trong phần mạng “inside”. Cũng gói tin đó, khi được chuyển ra mạng “outside” source IP address sẽ được chuyển thành "inside global address" và địa destination IP của gói tin sẽ là “outside global address”

Ngược lại, khi một gói tin bắt nguồn từ một mạng “outside”, khi nó còn đang ở mạng “outside” đó, địa chỉ source IP của nó sẽ là "outside global address", địa chỉ destination IP sẽ là "inside global address". Cũng gói tin đó khi được chuyển vào mạng “inside”, địa chỉ source sẽ là "outside local address" và địa chỉ destination của gói tin sẽ là "inside local address".

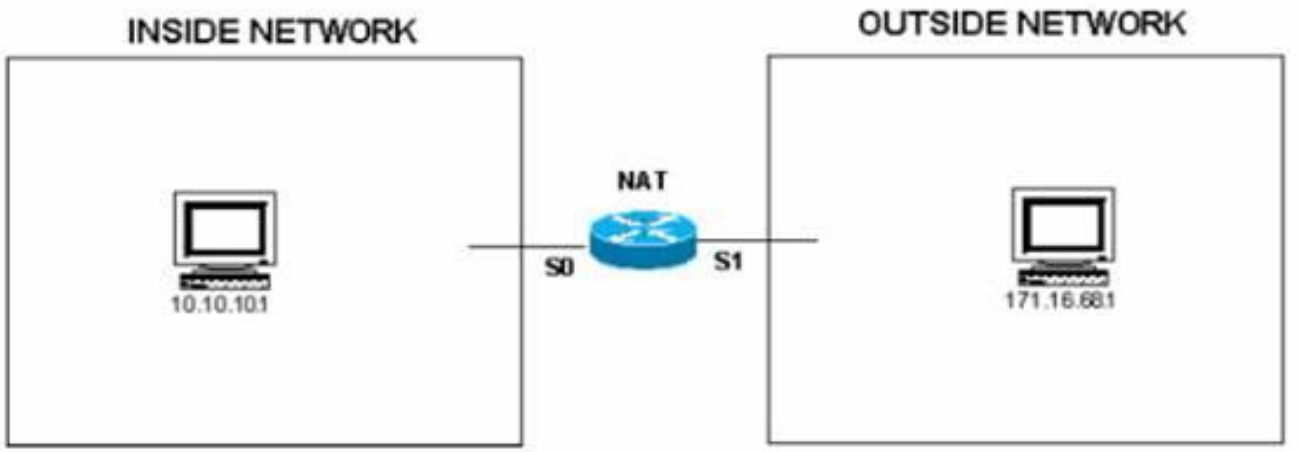
Định nghĩa các thuật ngữ

Chúng ta hãy quan sát ví dụ trong hình sau



Các ví dụ minh họa

Các phần sau đây sẽ tìm hiểu sâu hơn các thuật ngữ trên sử dụng topo đơn giản như sau:



Định nghĩa các địa chỉ inside local và inside global

Trong ví dụ này ở giữa sẽ được cấu hình NAT để phiên dịch địa chỉ . Khi nhận được một gói tin từ mạng trong đi ra ngoài có địa chỉ source IP là 10.10.10.1 thì địa chỉ này sẽ được router đổi thành 171.16.68.5 trước khi đi ra ngoài. Và ngược lại khi router nhận được gói tin có địa chỉ destination IP là 171.16.68.5 đi từ mạng ngoài vào thì nó sẽ phiên dịch thành địa chỉ destination IP là 10.10.10.1

Các ví dụ minh họa

ip nat inside source static 10.10.10.1 171.16.68.5

!--- Inside device A is known by the outside cloud as 171.16.68.5.

interface s 0

ip nat inside

interface s 1

ip nat outside

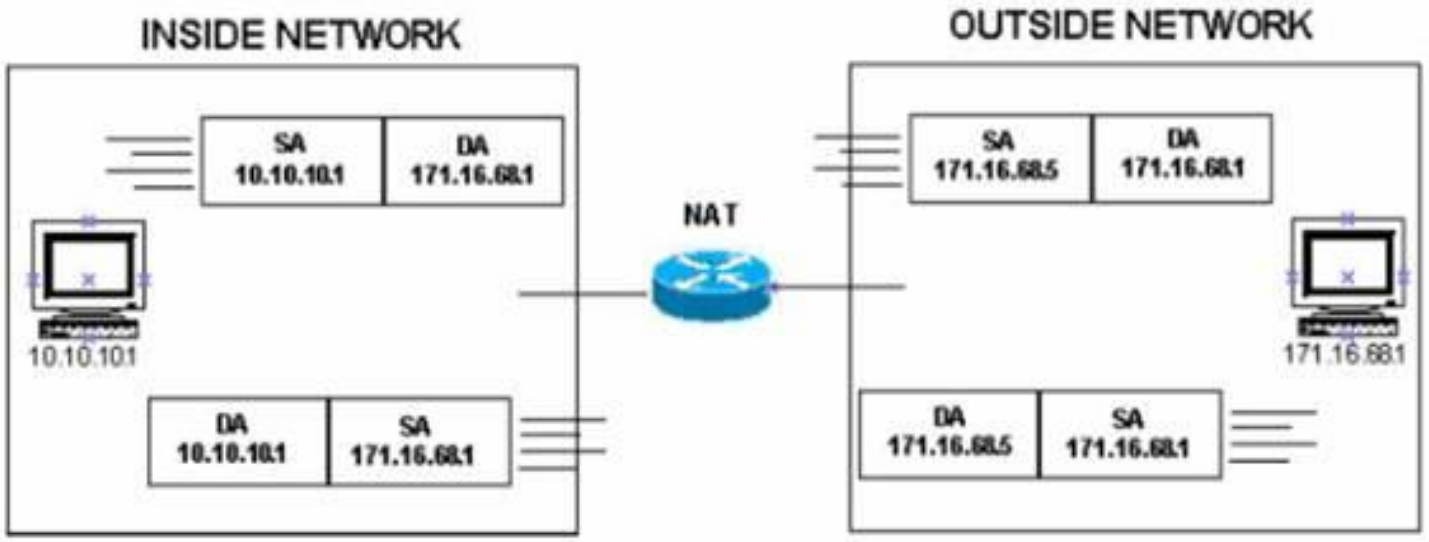
Khi thiết bị bên trong giao tiếp với thiết bị bên ngoài, các địa chỉ được định nghĩa như sau:

Inside Global	Inside Local	Outside Local	Outside Global
171.16.68.5	10.10.10.1	171.16.68.1	171.16.68.1

Các ví dụ minh họa

Như đã nói ở trên, các địa chỉ là địa chỉ xuất hiện trong đám mây mạng inside. Các địa chỉ global là địa chỉ xuất hiện trong đám mây outside. Do cách NAT được cấu hình trong ví dụ này chỉ để phiên dịch các địa chỉ inside, địa chỉ "inside local" sẽ khác địa chỉ "inside global" trong khi địa chỉ "outside local" và "outside global" thì hoàn toàn giống nhau.

Hình sau minh họa gọi tin khi nó ở trong mạng inside và outside.



Các ví dụ minh họa

Định nghĩa các địa chỉ outside local và outside global

Trong ví dụ cấu hình tiếp theo, khi NAT router nhận một packet ở giao diện outside với địa chỉ source là 171.16.68.1, địa chỉ này sẽ được phiên dịch là 10.10.10.5. Điều này cũng có nghĩa là nếu router NAT nhận được một packet trên giao diện inside của nó với một địa chỉ destination là 10.10.10.5, địa chỉ đích đó sẽ được phiên dịch thành 171.16.68.1

```
ip nat outside source static 171.16.68.1 10.10.10.5
!--- Outside device A is known to the inside cloud as 10.10.10.5.

interface s 0
ip nat inside

interface s 1
ip nat outside
```

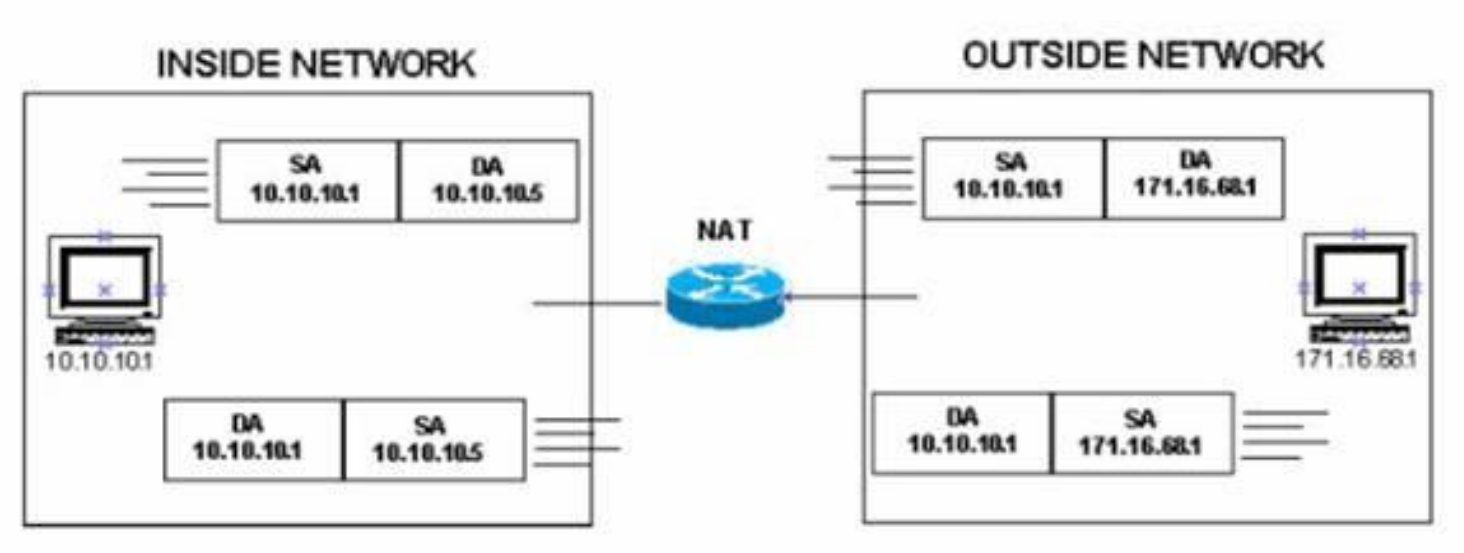
Khi thiết bị bên trong giao tiếp với thiết bị bên ngoài, các địa chỉ được định nghĩa như sau:

Inside Global	Inside Local	Outside Local	Outside Global
10.10.10.1	10.10.10.1	10.10.10.5	171.16.68.1

Các ví dụ minh họa

Các địa chỉ là địa chỉ xuất hiện trong đám mây mạng inside. Các địa chỉ global là địa chỉ xuất hiện trong đám mây outside. Do cách NAT được cấu hình trong ví dụ này chỉ để phiên dịch các địa chỉ outside, địa chỉ "outside local" sẽ khác địa chỉ "outside global" trong khi địa chỉ "inside local" và "inside global" thì hoàn toàn giống nhau.

Hình sau minh họa gọi tin khi nó ở trong mạng inside và outside.



Các ví dụ minh họa

Định nghĩa cả địa chỉ Local và Global

Trong ví dụ cấu hình cuối cùng này, router NAT được cấu hình để thực hiện việc phiên dịch địa chỉ như sau: khi router này nhận được một packet ở giao diện inside với địa chỉ source là 10.10.10.1, địa chỉ này sẽ được phiên dịch thành 171.16.68.5. Khi NAT router này nhận được một gói tin ở giao diện outside với địa chỉ source là 171.16.68.1, địa chỉ này sẽ được phiên dịch thành 10.10.10.5.

Điều này cũng có nghĩa là khi NAT router nhận được một gói tin ở giao diện outside với địa chỉ destination là 171.16.68.5, địa chỉ này sẽ được phiên dịch thành 10.10.10.1. Đồng thời, khi NAT nhận được một gói tin ở giao diện inside của nó với một địa chỉ destination là 10.10.10.5 thì địa chỉ này sẽ được phiên dịch thành 171.16.68.1.

Các ví dụ minh họa


```
ip nat inside source static 10.10.10.1 171.16.68.5
!--- Inside device A is known to the outside cloud as 171.16.68.5.

ip nat outside source static 171.16.68.1 10.10.10.5
!--- device A is known to the inside cloud as 10.10.10.5.

interface s 0
ip nat inside

interface s 1
ip nat outside
```

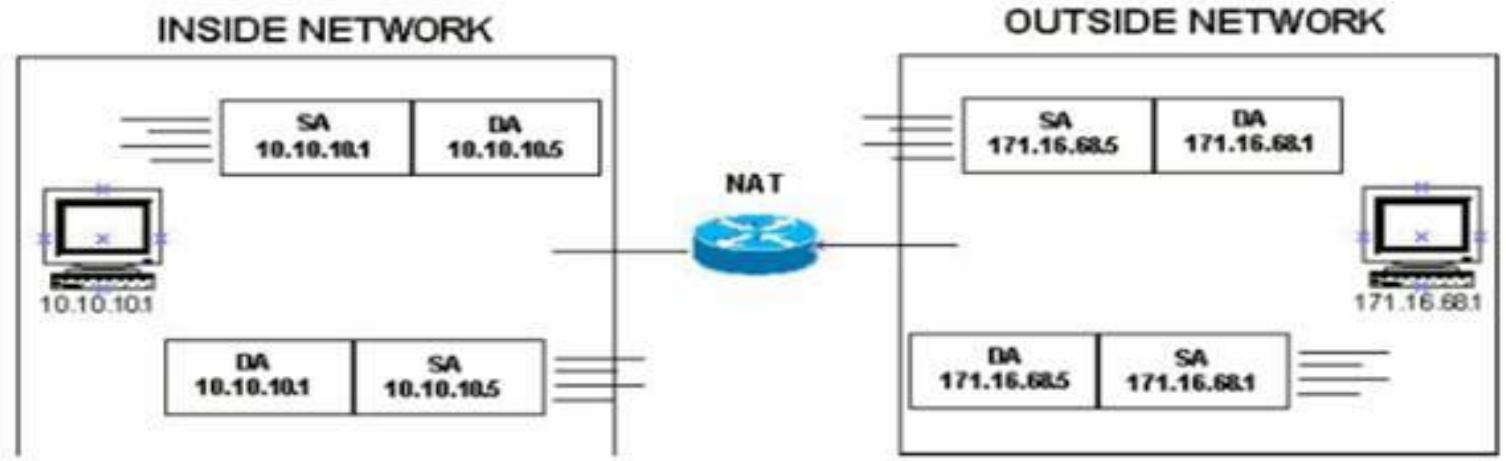
Khi thiết bị bên trong giao tiếp với thiết bị bên ngoài, các địa chỉ được định nghĩa như sau:

Inside Global	Inside Local	Outside Local	Outside Global
171.16.68.5	10.10.10.1	10.10.10.5	171.16.68.1

Các ví dụ minh họa

Một lần nữa chúng ta để ý rằng địa chỉ local là các địa chỉ xuất hiện trong mạng inside và địa chỉ global là địa chỉ xuất hiện trong mạng outside. Trong trường hợp đặc biệt này, do cách cấu hình NAT, cả địa chỉ "inside" và địa chỉ "outside" đều được phiên dịch do vậy địa chỉ "inside local" sẽ khác địa chỉ "inside global" và địa chỉ "outside local" cũng sẽ khác địa chỉ "outside global"

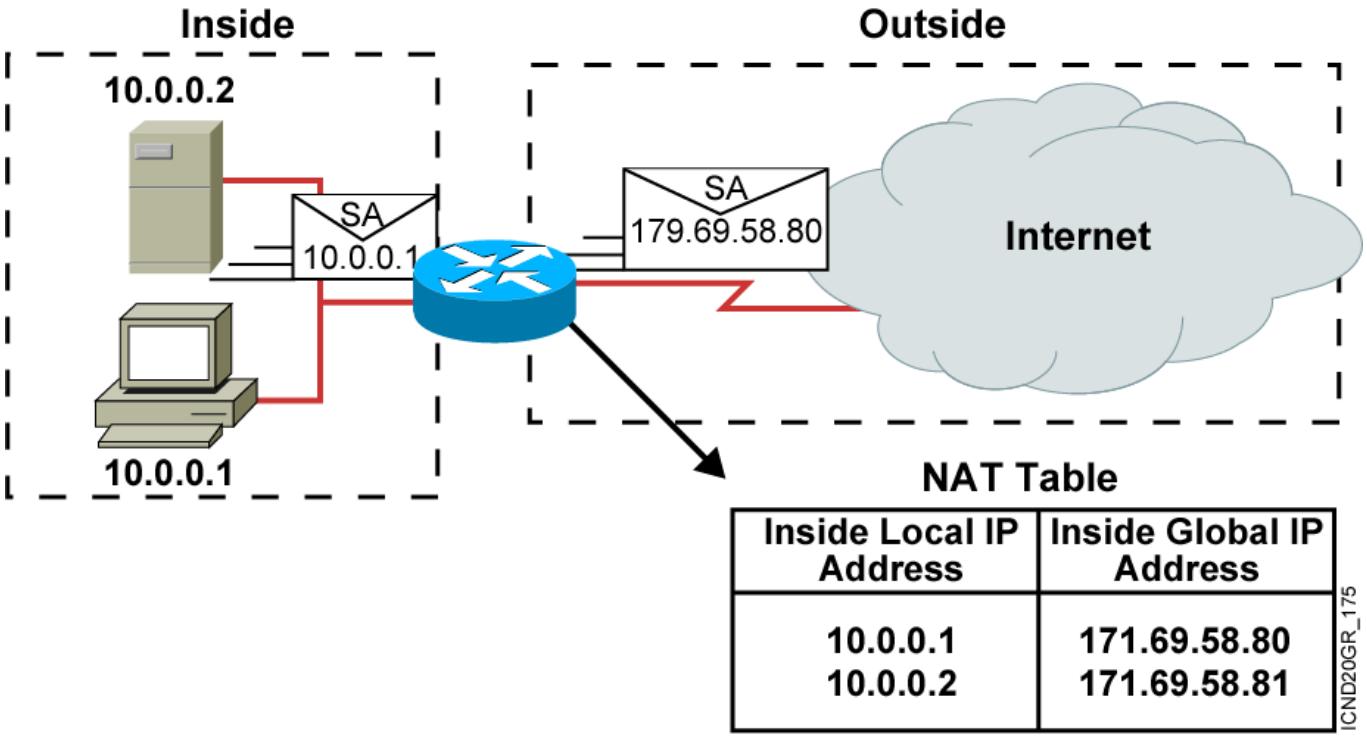
Hình sau minh họa gọi tin khi nó ở trong mạng inside và outside.



Các ví dụ minh họa

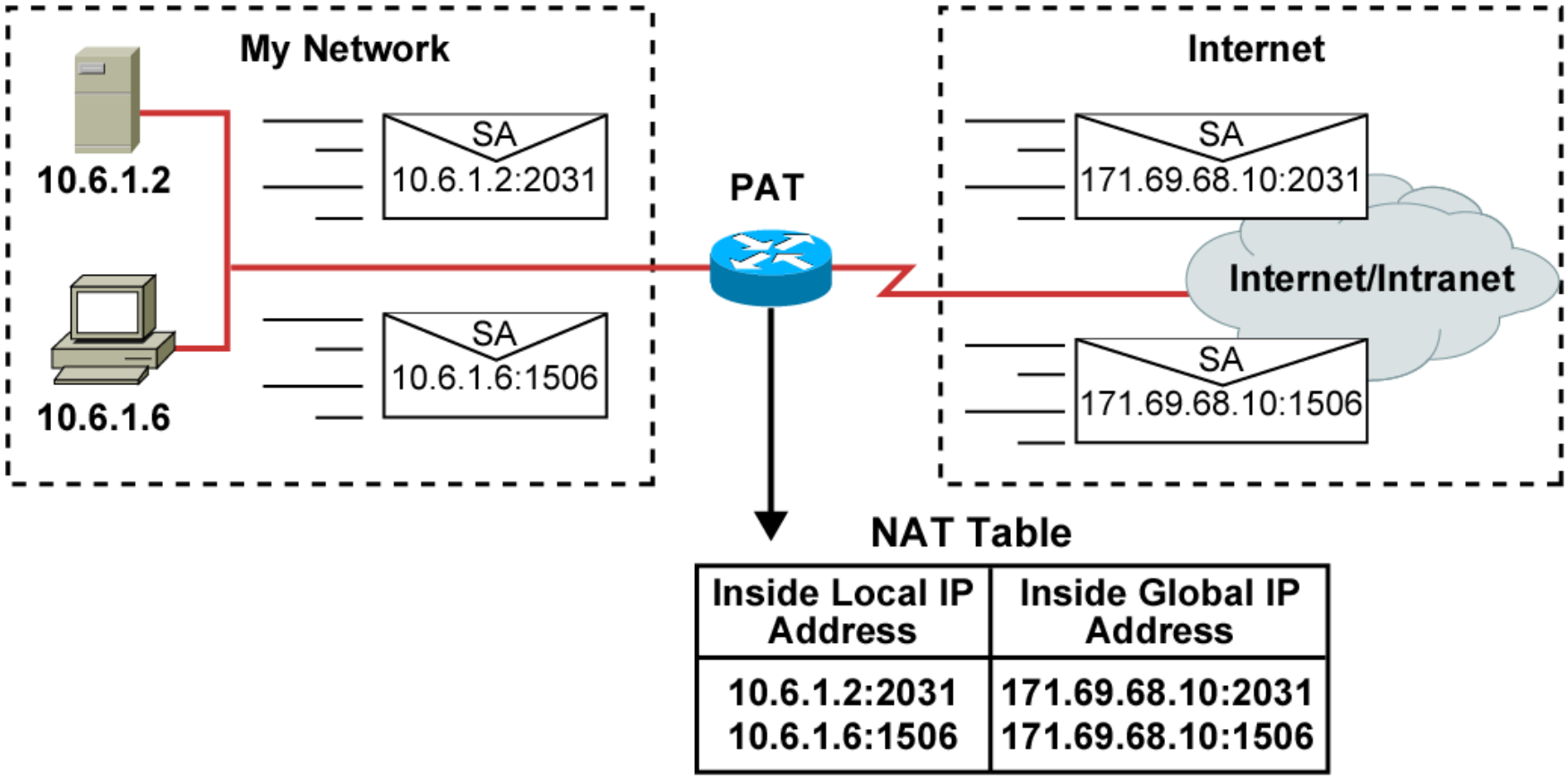
Nói tóm lại, các thuật ngữ “local” và “global” sẽ dễ hiểu hơn rất nhiều nếu chúng ta xem xét đến vị trí của nó khi xuất hiện trong mạng. Địa chỉ local chỉ xuất hiện trong phần “inside” của mạng trong khi địa chỉ global chỉ xuất hiện trong phần “outside” của mạng. Đồng thời phụ thuộc vào cách mà NAT được cấu hình, các địa chỉ global và local trên mỗi giao diện (inside hay outside) sẽ có thể giống hoặc không giống nhau.

Network Address Translation

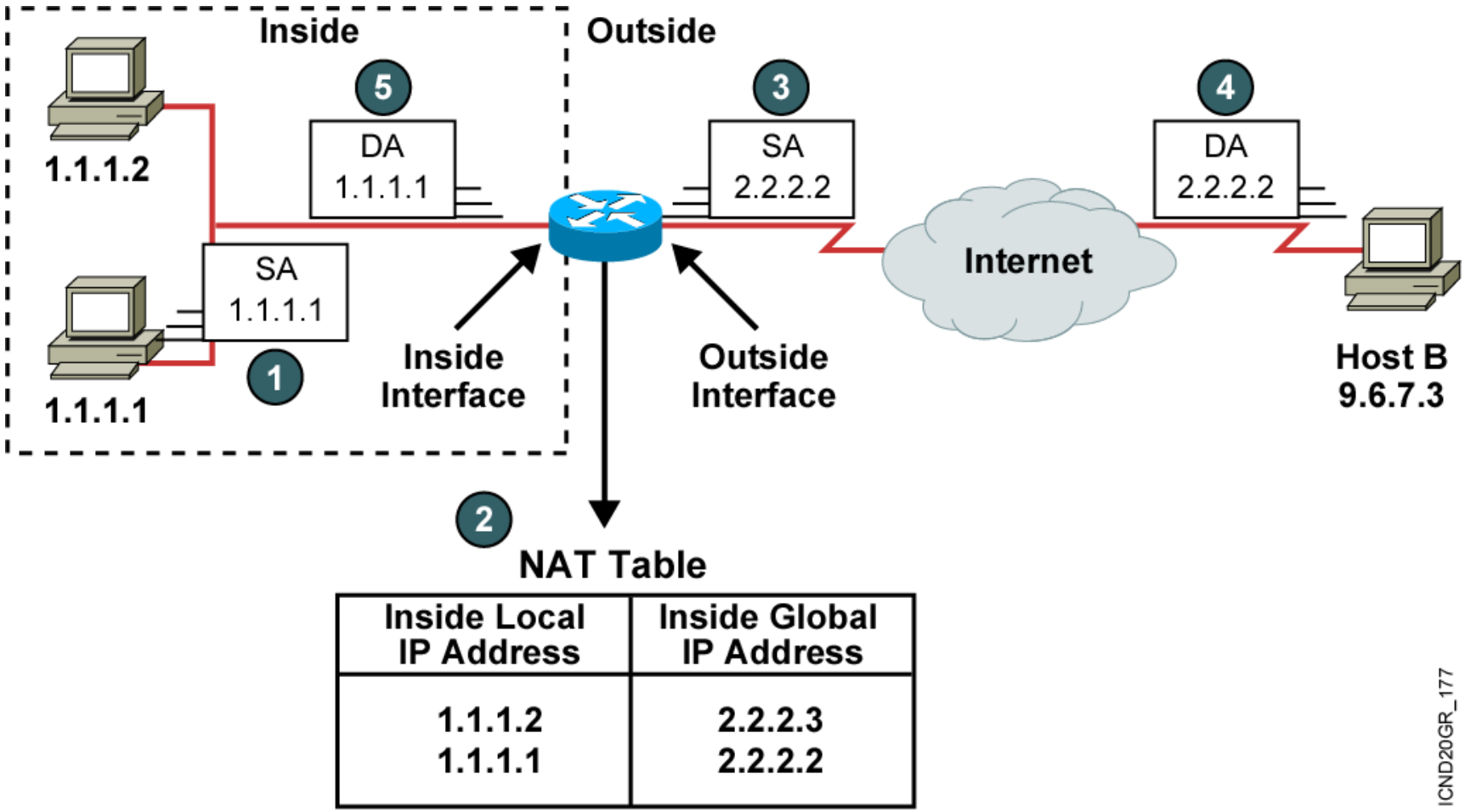


- An IP address is either local or global.
- Local IP addresses are seen in the inside network.

Port Address Translation



Translating Inside Source Addresses



Configuring Static Translation

Cisco.com

```
Router(config)#ip nat inside source static local-ip global-ip
```

- **Establishes static translation between an inside local address and an inside global address**

```
Router(config-if)#ip nat inside
```

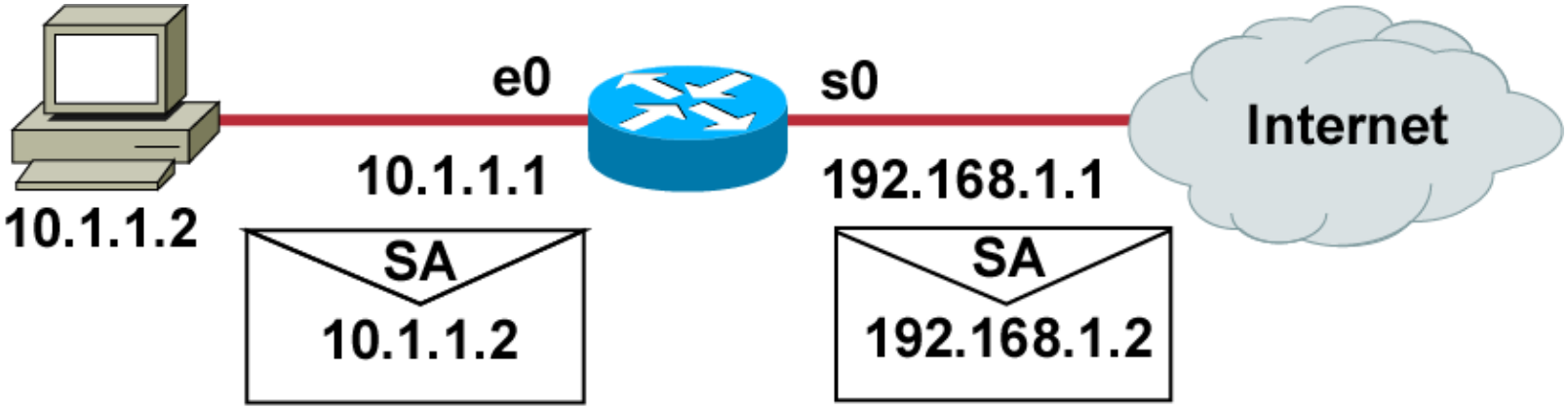
- **Marks the interface as connected to the inside**

```
Router(config-if)#ip nat outside
```

- **Marks the interface as connected to the outside**

Enabling Static NAT Address Mapping Example

Cisco.com




```
interface s0
ip address 192.168.1.1 255.255.255.0
ip nat outside
!
interface e0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
ip nat inside source static 10.1.1.2 192.168.1.2
```

ICND20GR_282

Configuring Dynamic Translation

Cisco.com

```
Router(config)#ip nat pool name start-ip end-ip
{netmask netmask | prefix-length prefix-length}
```

- Defines a pool of global addresses to be allocated as needed

```
Router(config)#access-list access-list-number permit
source [source-wildcard]
```

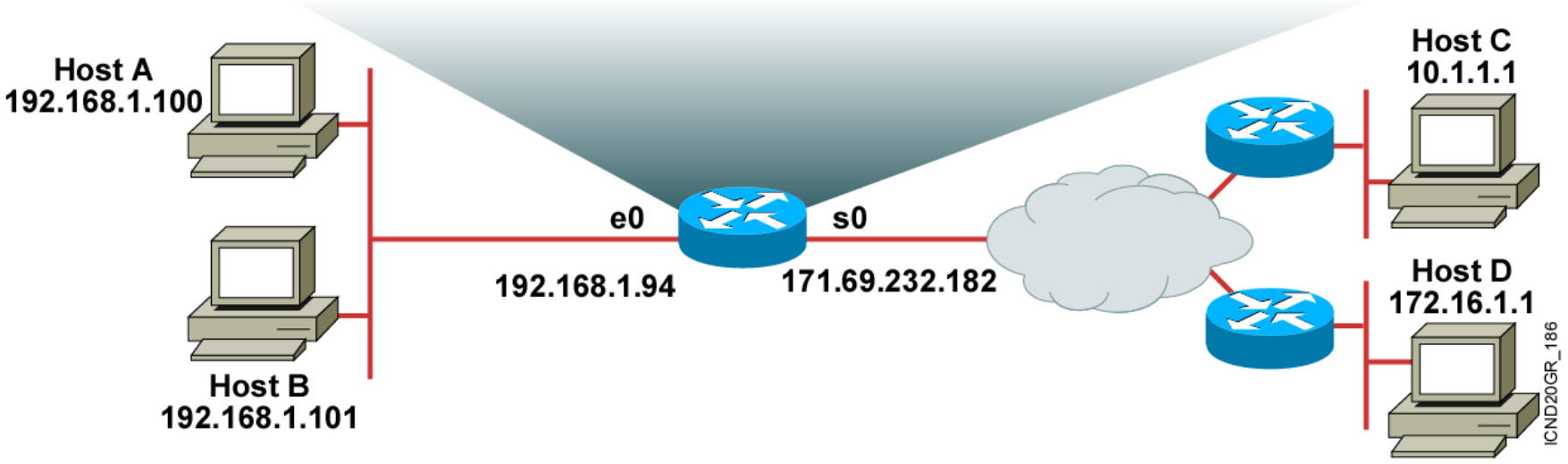
- Defines a standard IP access list permitting those inside local addresses that are to be translated

```
Router(config)#ip nat inside source list
access-list-number pool name
```

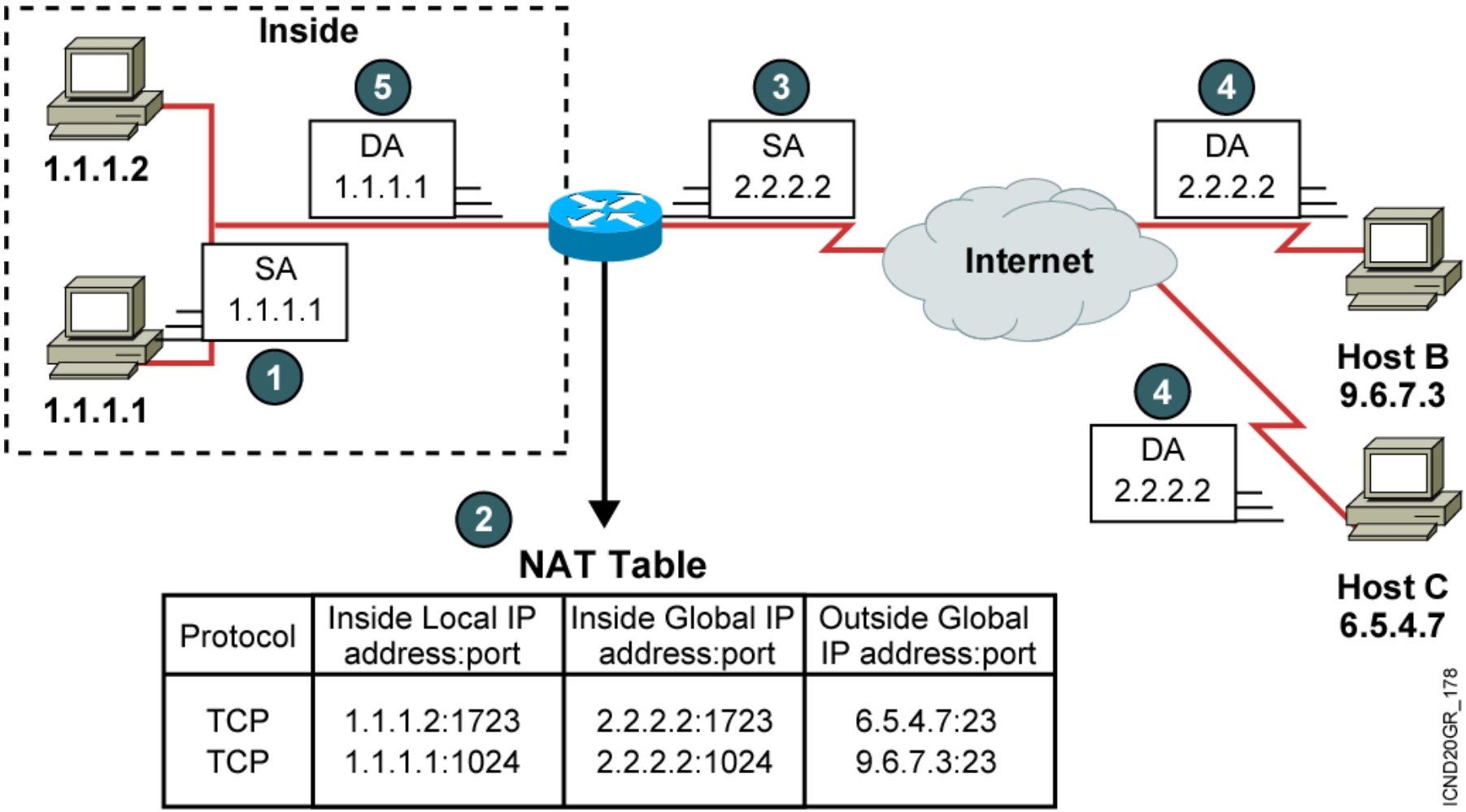
- Establishes dynamic source translation, specifying the access list defined in the prior step

Dynamic Address Translation Example


```
ip nat pool net-208 171.69.233.209 171.69.233.222 netmask
255.255.255.240
ip nat inside source list 1 pool net-208
!
interface serial 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 0
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```



Overloading an Inside Global Address



Protocol	Inside Local IP address:port	Inside Global IP address:port	Outside Global IP address:port
TCP	1.1.1.2:1723	2.2.2.2:1723	6.5.4.7:23
TCP	1.1.1.1:1024	2.2.2.2:1024	9.6.7.3:23

ICND20GR_178

Configuring Overloading

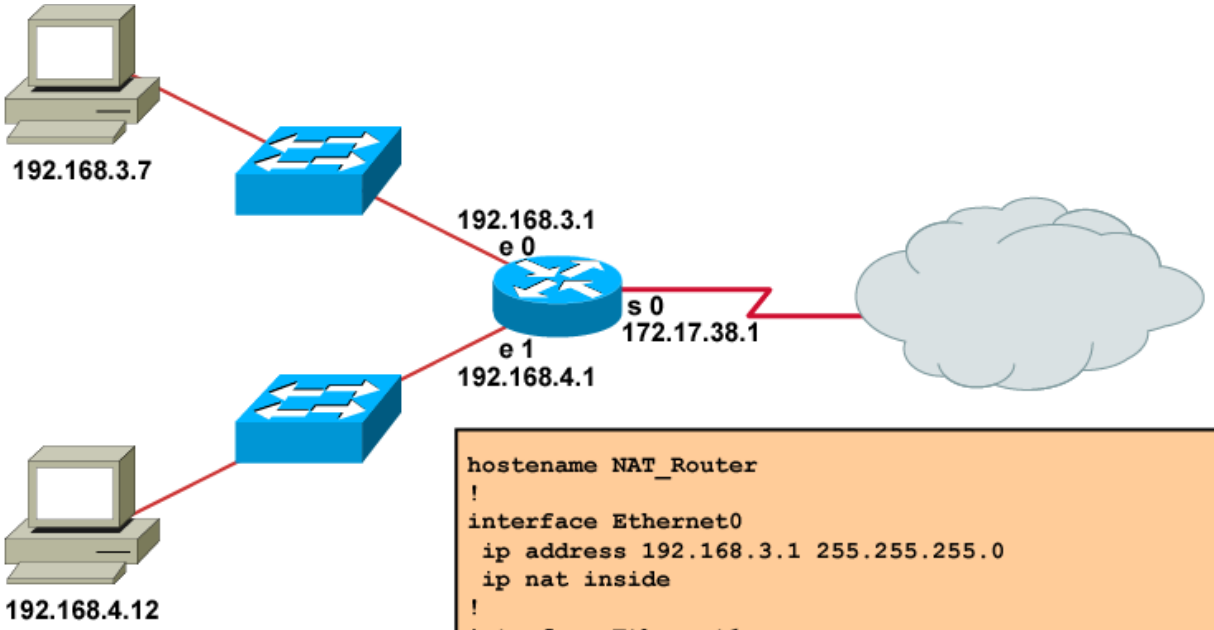

```
Router(config)#access-list access-list-number permit
source source-wildcard
```

- **Defines a standard IP access list permitting those inside local addresses that are to be translated**

```
Router(config)#ip nat inside source list
access-list-number interface interface_name overload
```

- **Establishes dynamic source translation, specifying the access list defined in the prior step**

Overloading an Inside Global Address Example




```
hostename NAT_Router
!
interface Ethernet0
 ip address 192.168.3.1 255.255.255.0
 ip nat inside
!
interface Ethernet1
 ip address 192.168.4.1 255.255.255.0
 ip nat inside
!
interface Serial0
 description To ISP
 ip address 172.17.38.1 255.255.255.0
 ip nat outside
!
ip nat inside source list 1 interface Serial0 overload
!
ip route 0.0.0.0 0.0.0.0 Serial0
!
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
!
```

ICND2_0GR_260

Clearing the NAT Translation Table

Cisco.com

```
Router#clear ip nat translation *
```

- Clears all dynamic address translation entries

```
Router#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

```
Router#clear ip nat translation outside
local-ip global-ip
```

- Clears a simple dynamic translation entry containing an outside translation

```
Router#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

Displaying Information with show Commands


```
Router#show ip nat translations
```

- Displays active translations

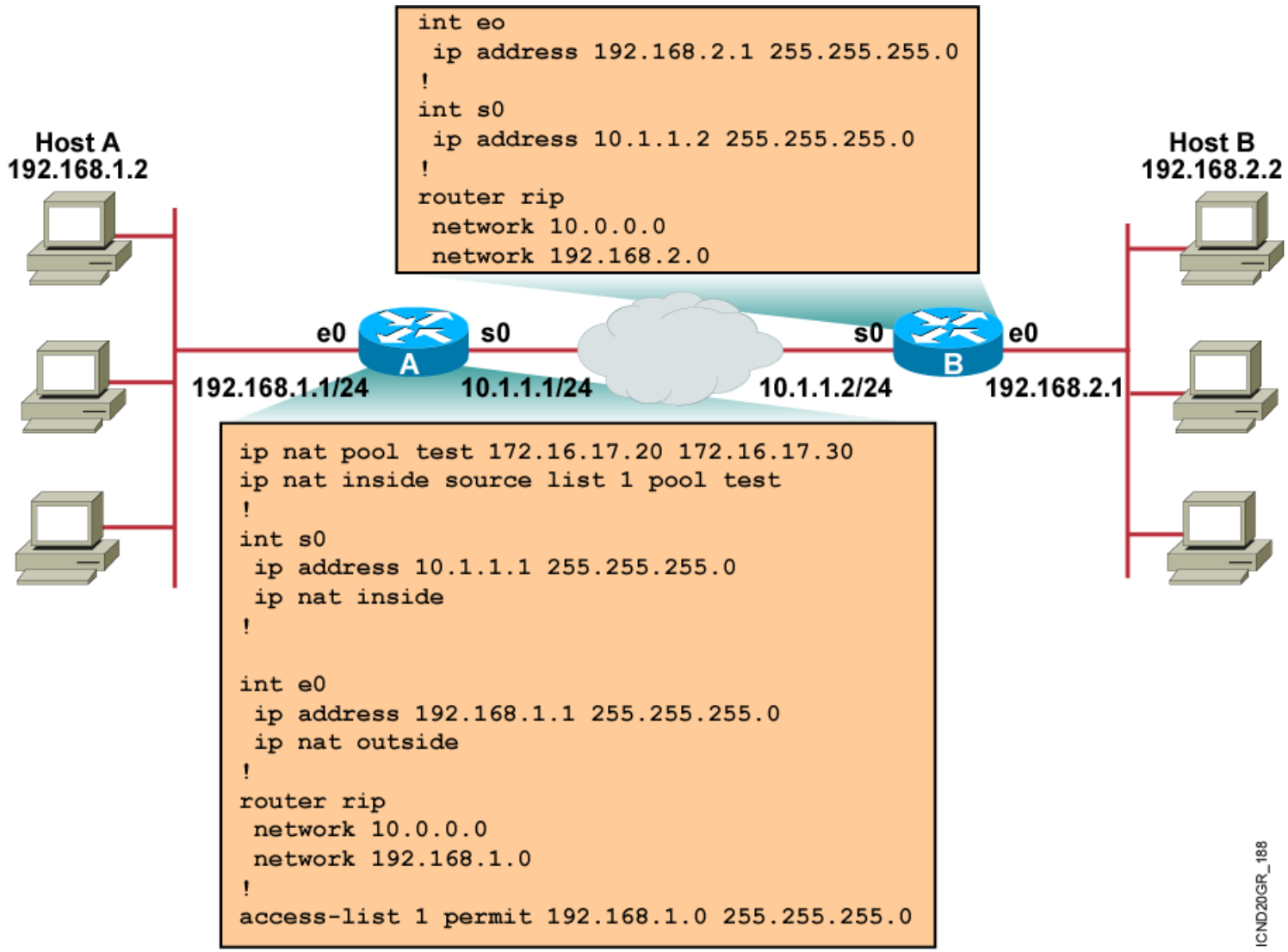
```
Router#show ip nat translation
     Pro Inside global      Inside local       Outside local      Outside global
     --- 172.16.131.1        10.10.10.1         ---                ---
```

```
Router#show ip nat statistics
```

- Displays translation statistics

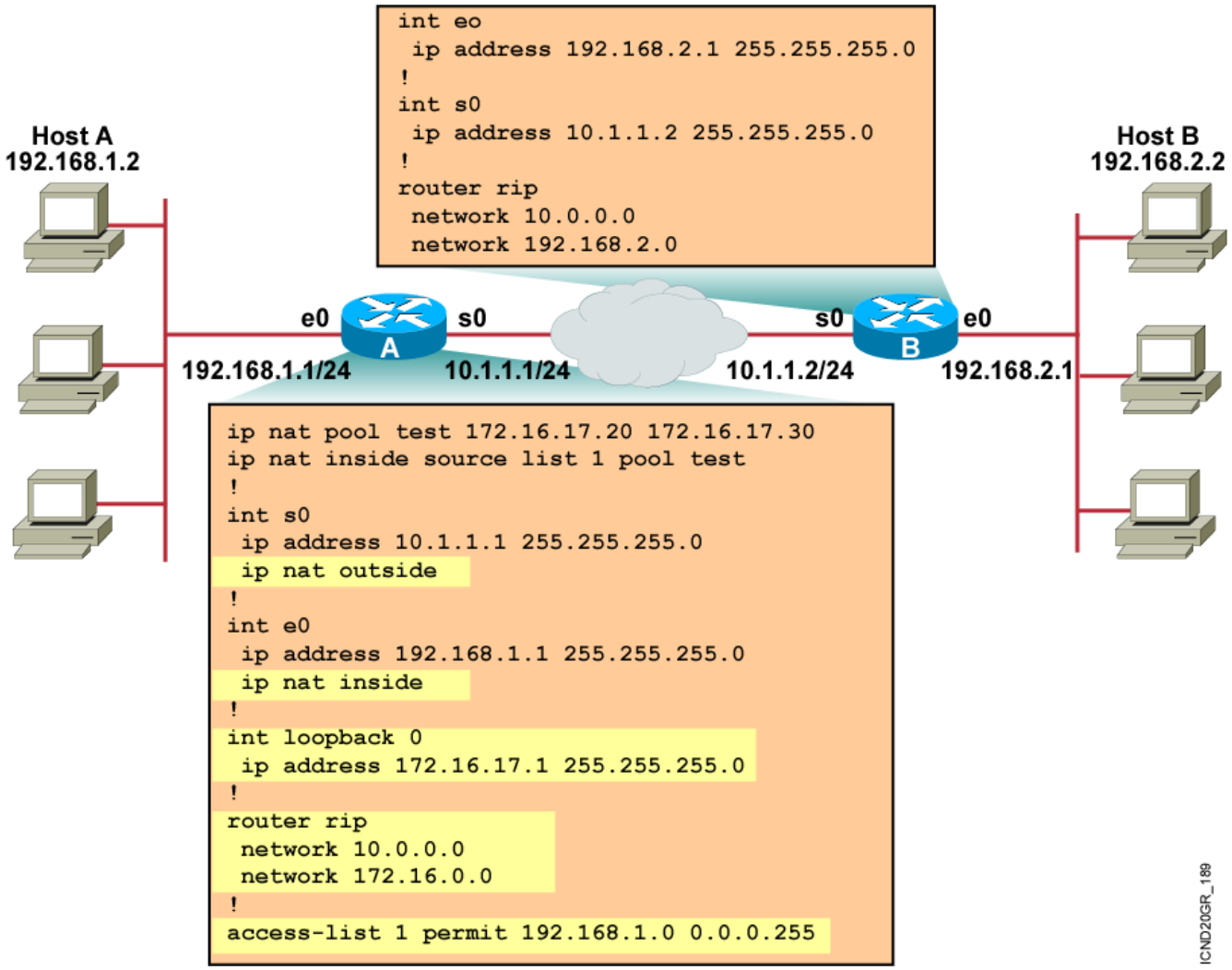
```
Router#show ip nat statistics
      Total active translations: 1 (1 static, 0 dynamic; 0 extended)
      Outside interfaces:
      Ethernet0, Serial2.7
      Inside interfaces:
      Ethernet1
      Hits: 5  Misses: 0
      …
```

Sample Problem: Cannot Ping Remote Host



ICND20GR_188

Solution: New Configuration



Using the debug ip nat Command

Cisco.com

```
Router#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 [23325]
```

Translation Not Installed in the Translation Table?

- Verify that:
  - The configuration is correct.
  - There are not any inbound access lists denying the packets from entering the NAT router.
  - The access list referenced by the NAT command is permitting all necessary networks.
  - There are enough addresses in the NAT pool.
  - The router interfaces are appropriately defined as NAT inside or NAT outside.

Summary

Cisco.com

- Cisco IOS NAT allows an organization with unregistered private addresses to connect to the Internet by translating those addresses into globally registered IP addresses.
- You can translate your own IP addresses into globally unique IP addresses when communicating outside of your network.
- Overloading is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address (many-to-one) by using different ports, known also as PAT.
- Once you have configured NAT, verify that it is operating as expected using the clear and show commands.
- Sometimes NAT is blamed for IP connectivity problems when there is actually a routing problem.


CISCO SYSTEMS
EMPOWERING THE
INTERNET GENERATION