Network Address Translation

NAT

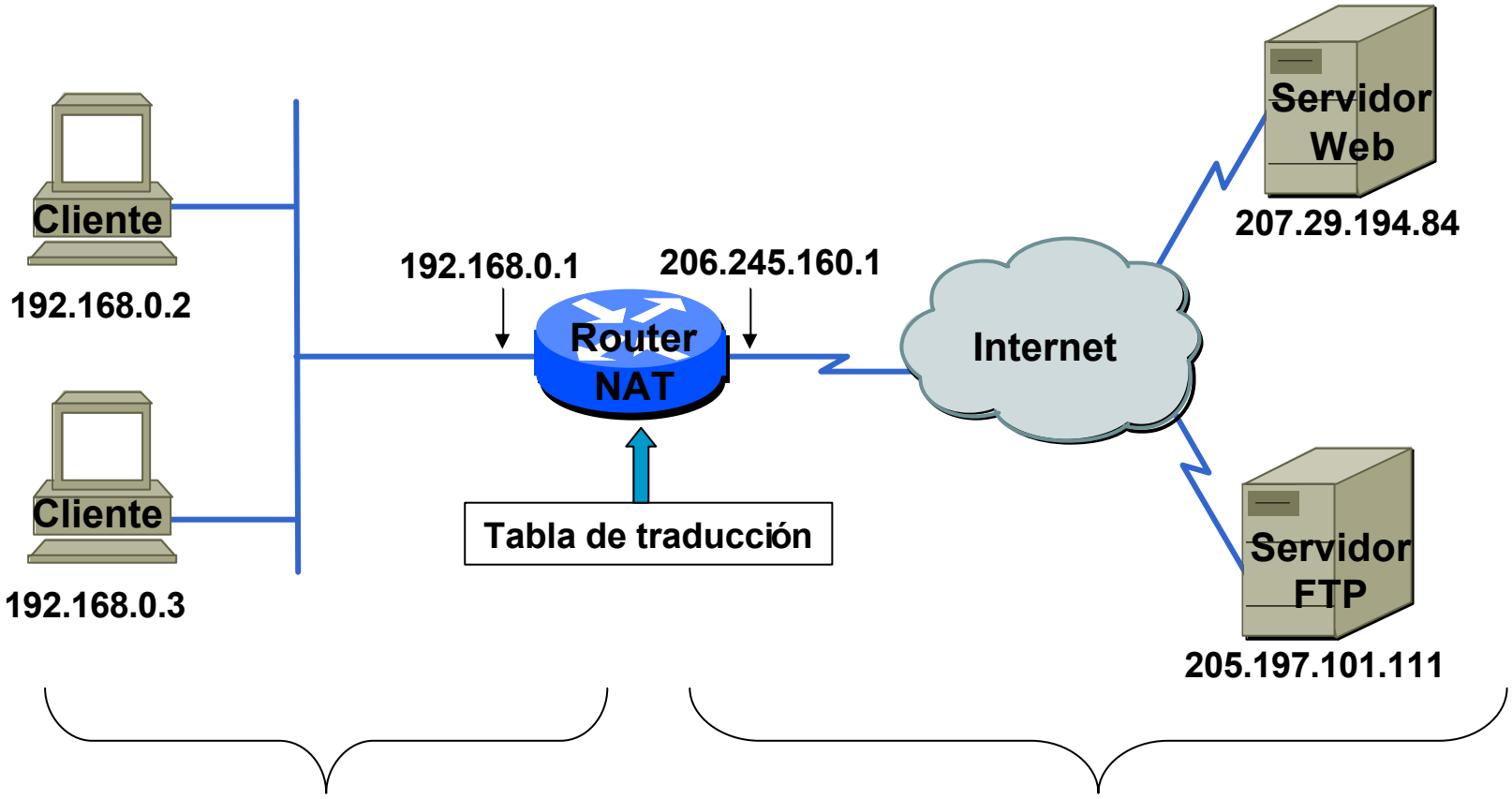
(conectar una red privada (dir. IP privadas – “no enrutables”)

con una red pública (dir. IP públicas): Internet)

Traducción de direcciones (NAT). RFC 1631

- Consiste en traducir una dirección IP en otra de acuerdo con cierta tabla de equivalencias.
- Se utiliza mucho como mecanismo para ‘extender’ el rango de direcciones disponible en una red. Por ejemplo usar una sola IP pública para dar acceso a cientos de ordenadores.
- NAT se suele utilizar para conectar a Internet redes IP que utilizan rangos privados (RFC 1918): 10.*.*.*, 172.16-31.*.* y 192.168.0-255.*.
- Normalmente la traducción la realiza el dispositivo (router) que conecta la red al exterior.

Uso de NAT



Direccionamiento privado
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16

Direccionamiento público

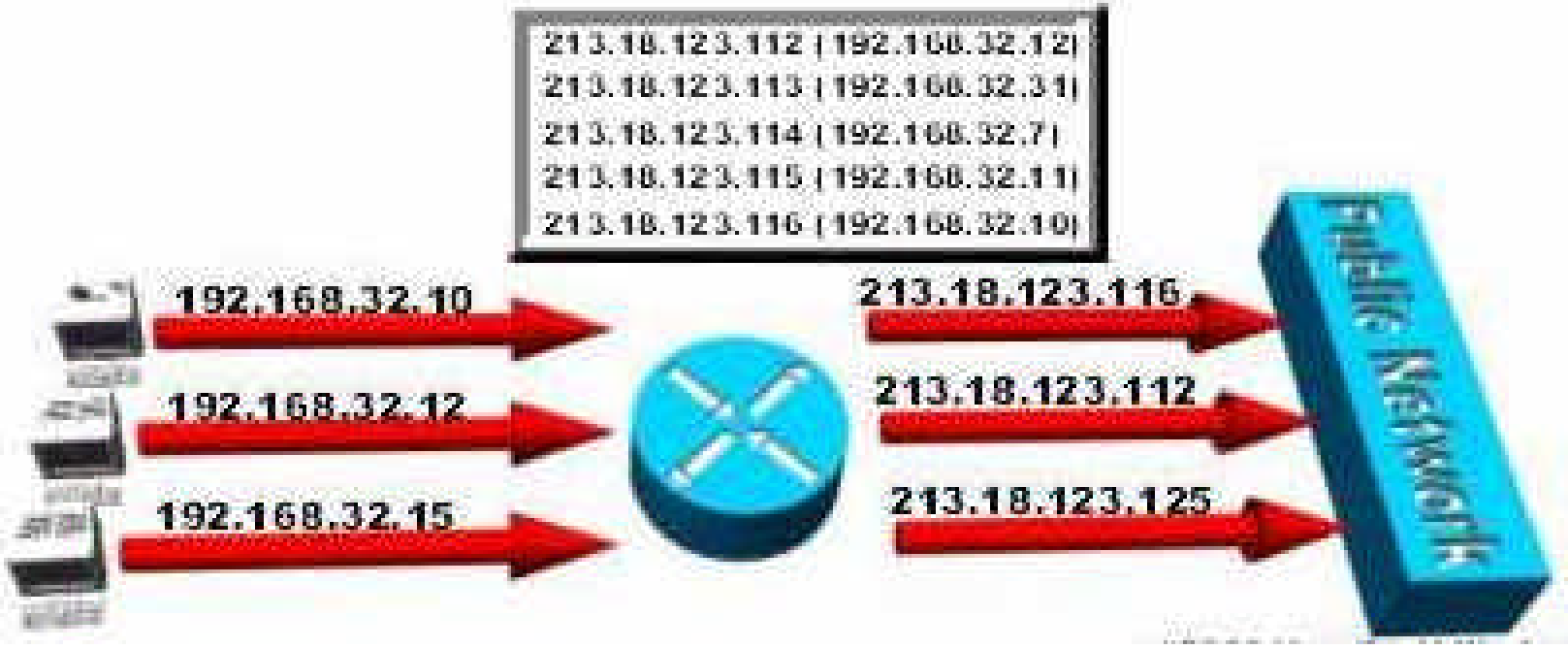
Sobre NAT

- Si se usa NAT es conveniente que la conexión al exterior se haga sólo en un router.
- NAT sólo permite paquetes TCP, UDP e ICMP. No se intercambia información de routing a través de un NAT.
- Según los campos que se modifican el NAT puede ser:
  - NAT Básico: sólo se cambia la dirección IP.
  - NAPT (Network Address Port Translation): se modifica la dirección IP y el número de puerto (TCP o UDP). También se llama Overloading NAT o simplemente PAT.
- Según la temporalidad de correspondencia entre la dirección privada y la pública el NAT puede ser:
  - Estático: la tabla de conversión de direcciones (y puertos) se carga al arrancar el equipo que hace NAT y el tráfico no la modifica
  - Dinámico: la tabla de conversión se construye y modifica en función del tráfico recibido. Las direcciones pueden reutilizarse. Requiere mantener en el NAT información de estado. Normalmente es unidireccional.

- **NAT Estático** – mapeado uno a uno. ***Particularmente interesante cuando el host debe ser accesible desde el exterior-***

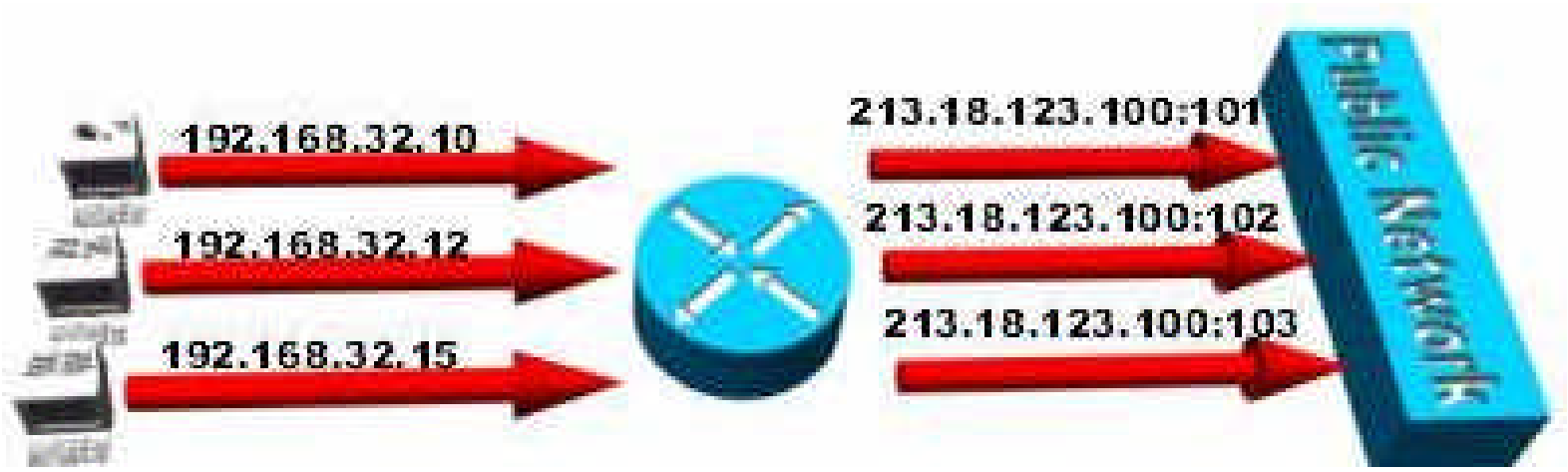
El host 192.168.32.10 siempre se traduce en 213.18.123.110.

- **NAT dinámico** – mapea de forma dinámica direcciones inside en un pool o conjunto de direcciones globales (registradas)



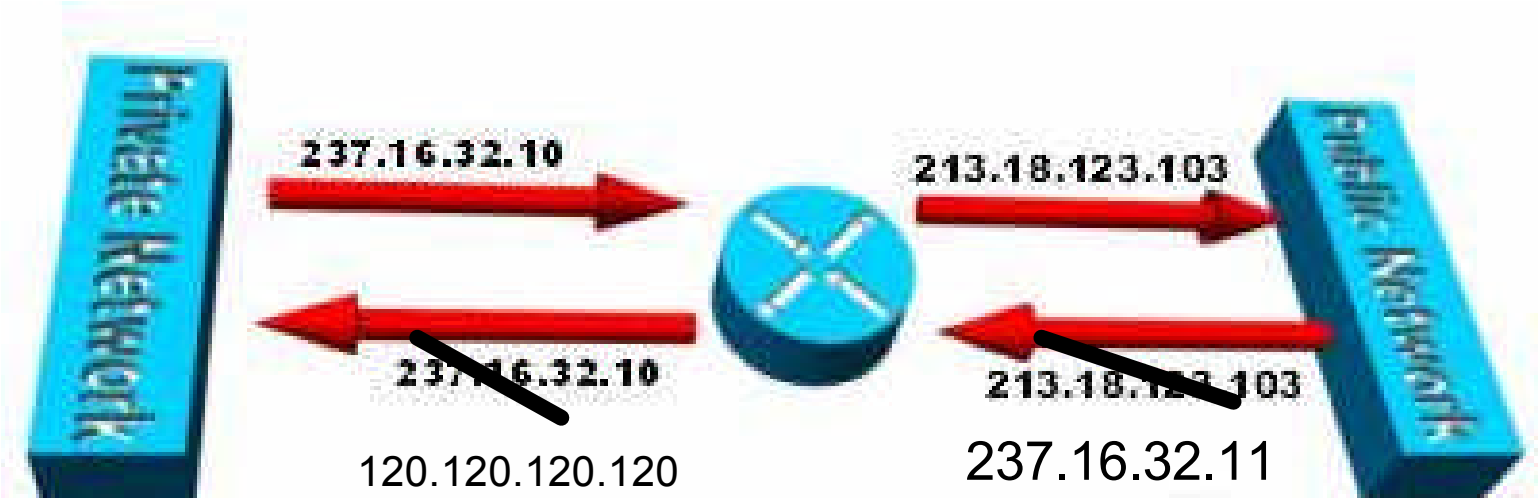
El host 192.168.32.10 se traducirá a la primera dirección libre de las IP registradas del rango o pool 213.18.123.100 to 213.18.123.150.

- **Overloading** – también conocido como ***PAT (Port Address Translation),*** con multiplexación a nivel de puerto



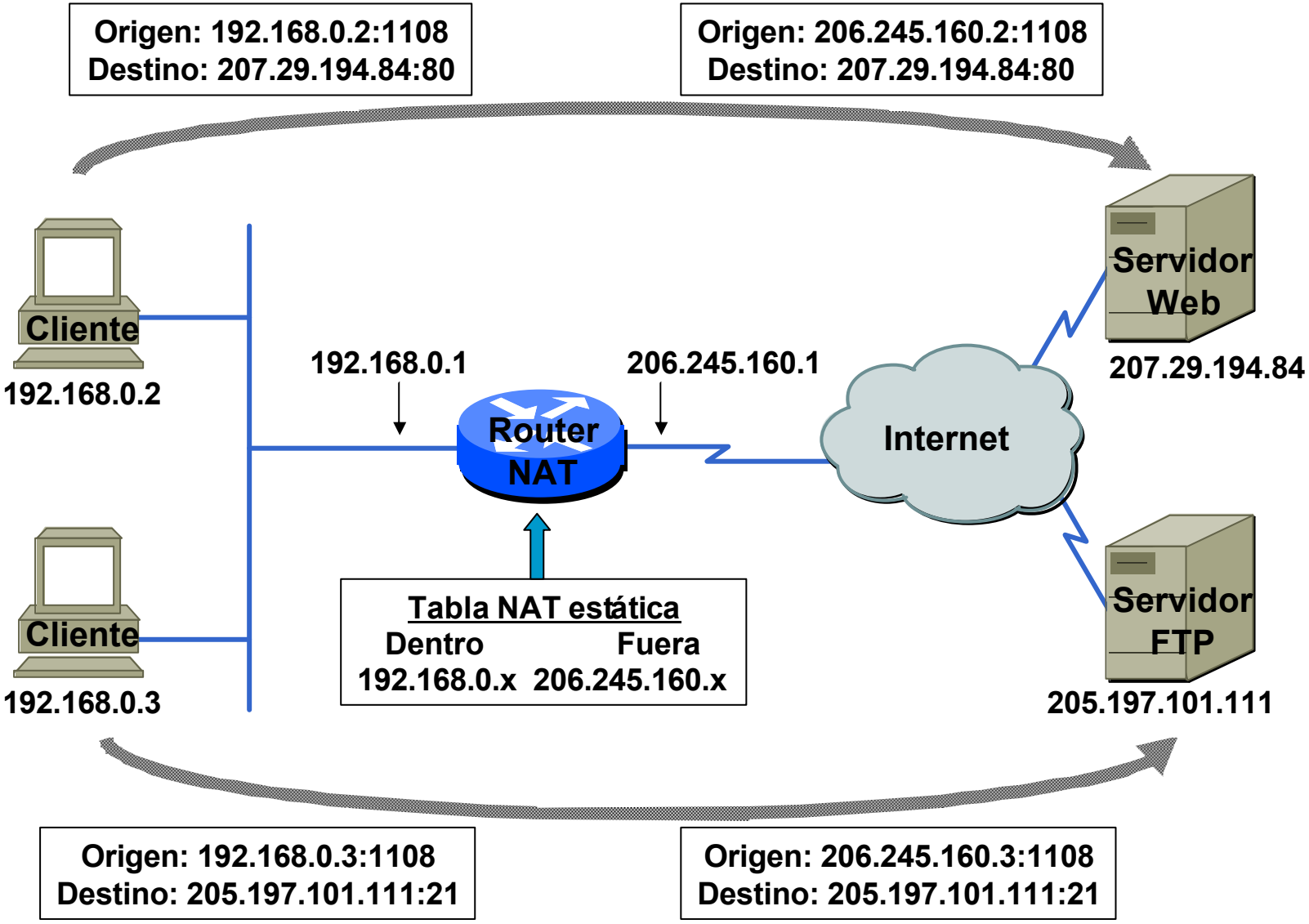
Un host de la zona inside se traduce siempre con la misma IP (213.18.123.100) pero con puertos diferentes.

- **Overlapping** – utilizado cuando el uso de direcciones internas de la LAN del router, la subred utilizada por el router, coincide con las de otra LAN en otro router, utilizan la misma subred, e interesa respetar el direccionamiento.

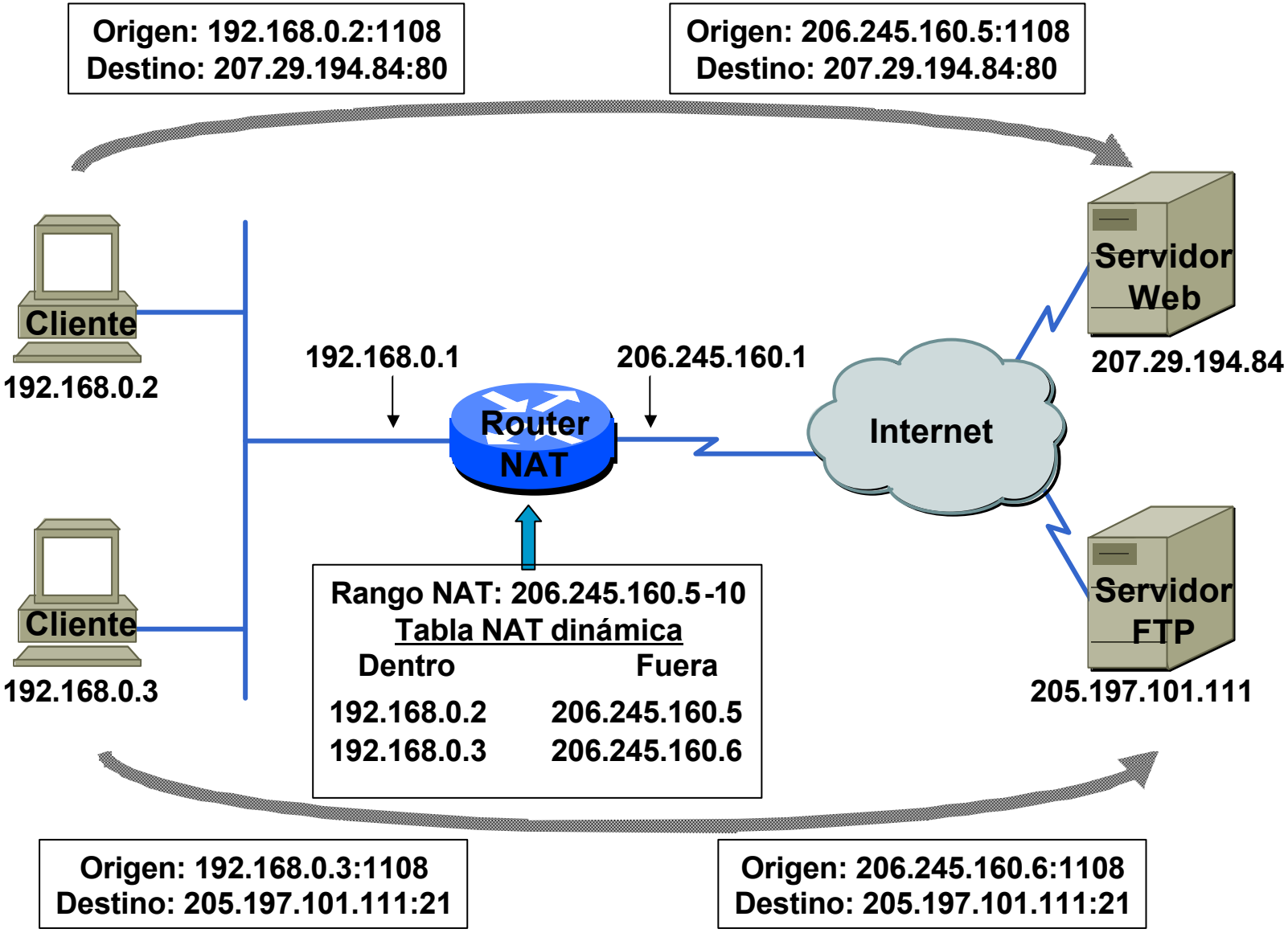


Ejemplo, la subred (237.16.32.x) está registrada por otra red, de esta forma el router traduce las direcciones para evitar conflicto de IP duplicadas. De esta forma, el router tendrá que cambiar las direcciones externas para distiguir de las internas evitando el solape. Veremos un ejemplo.

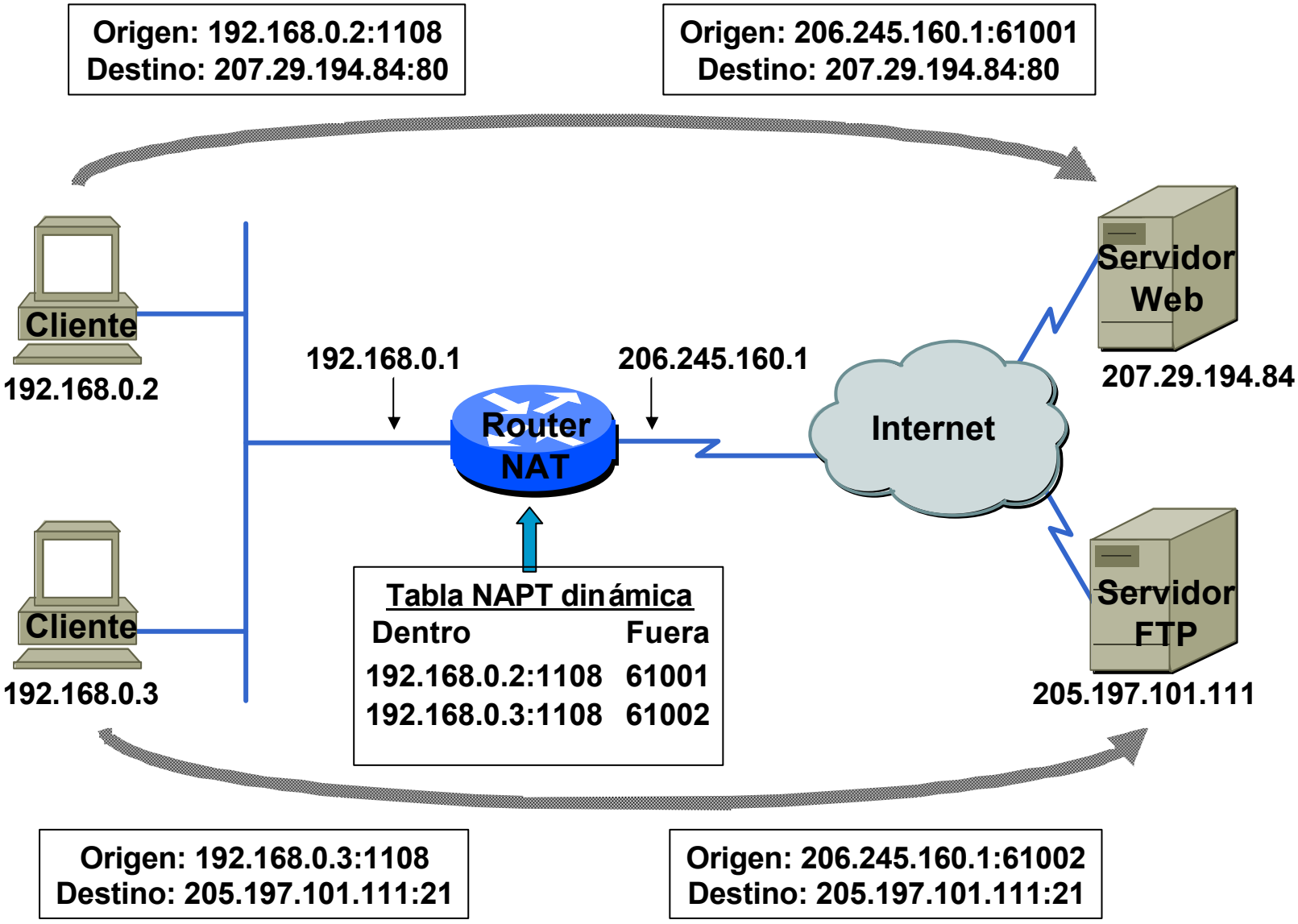
NAT básico estático



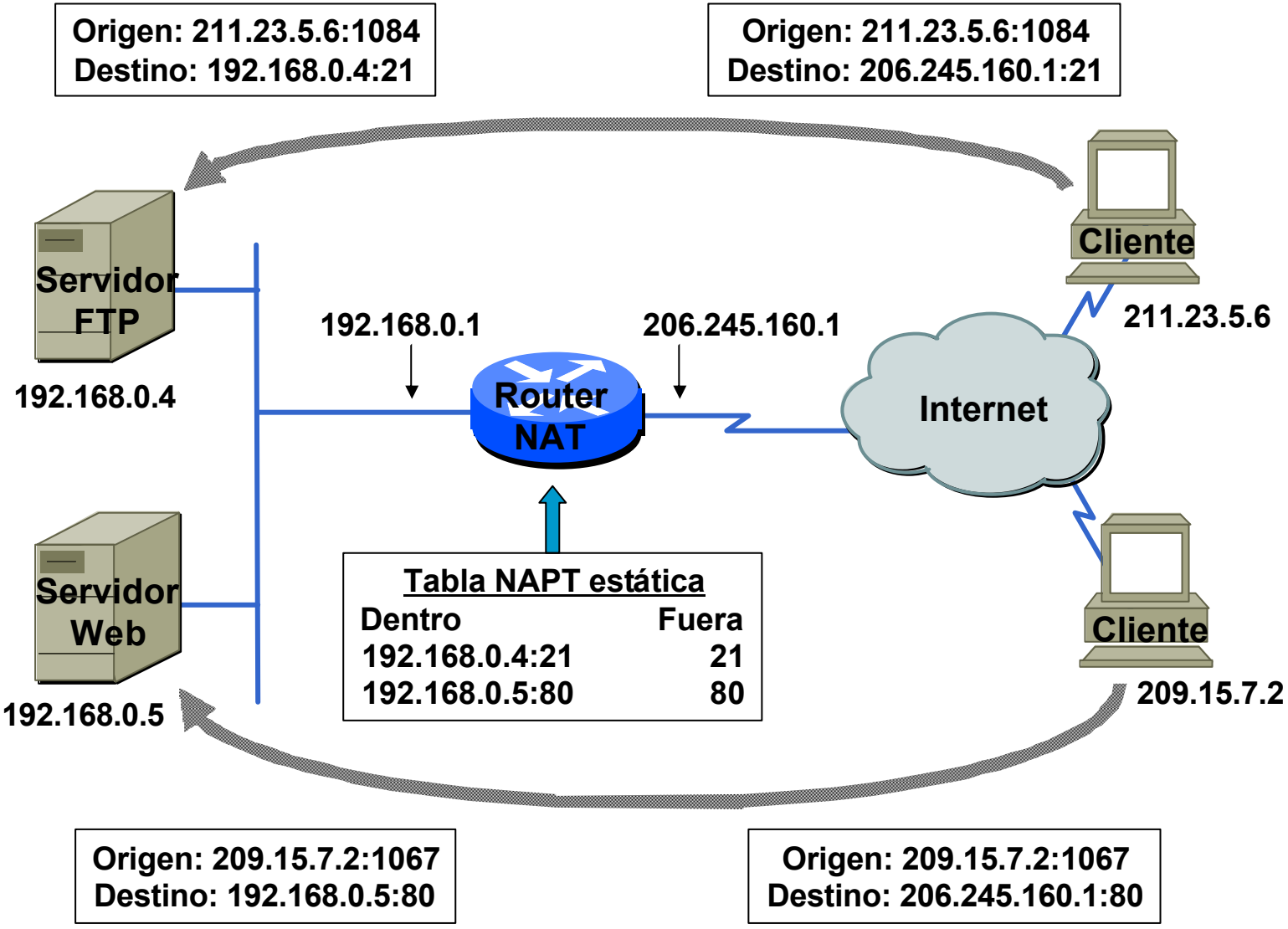
NAT básico dinámico



NAT overload dinámico



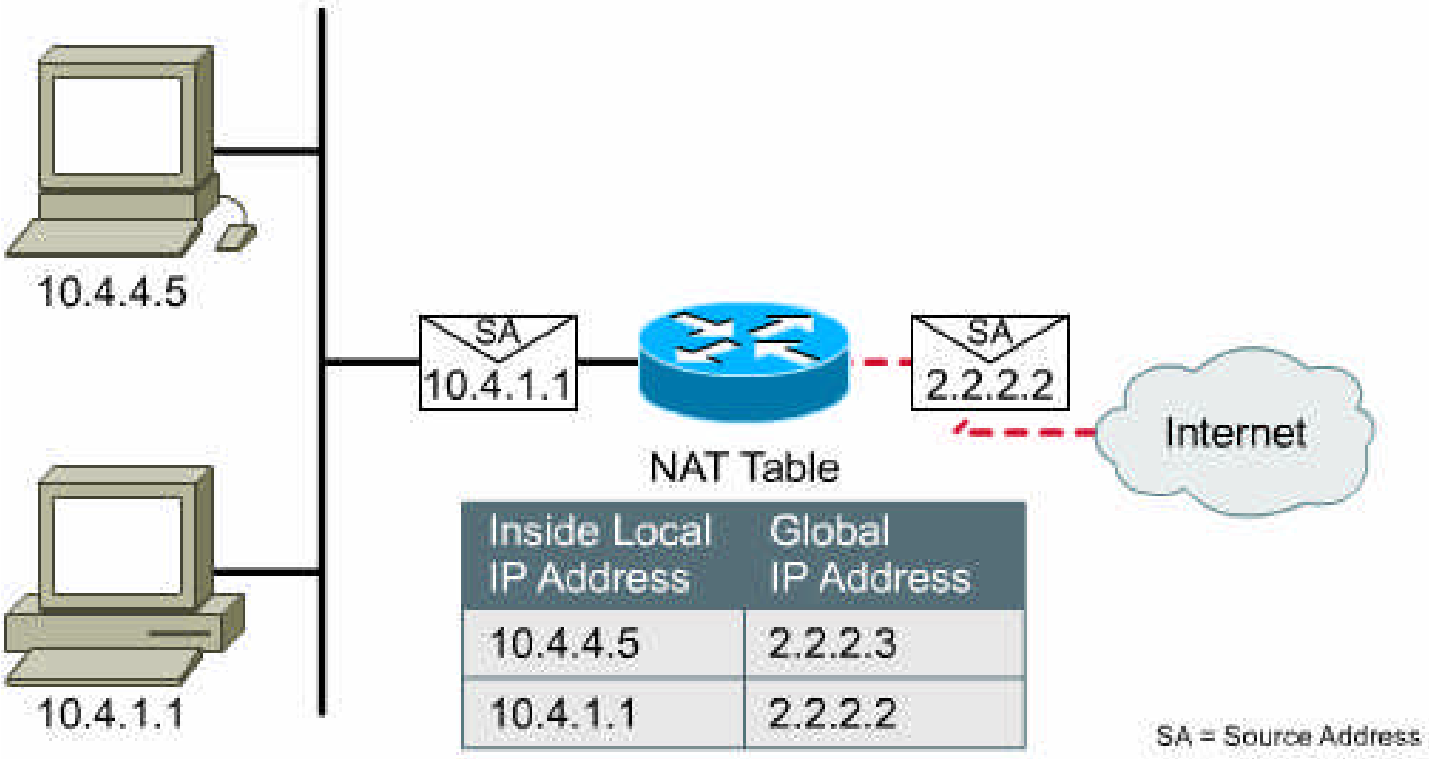
NAT overload estático



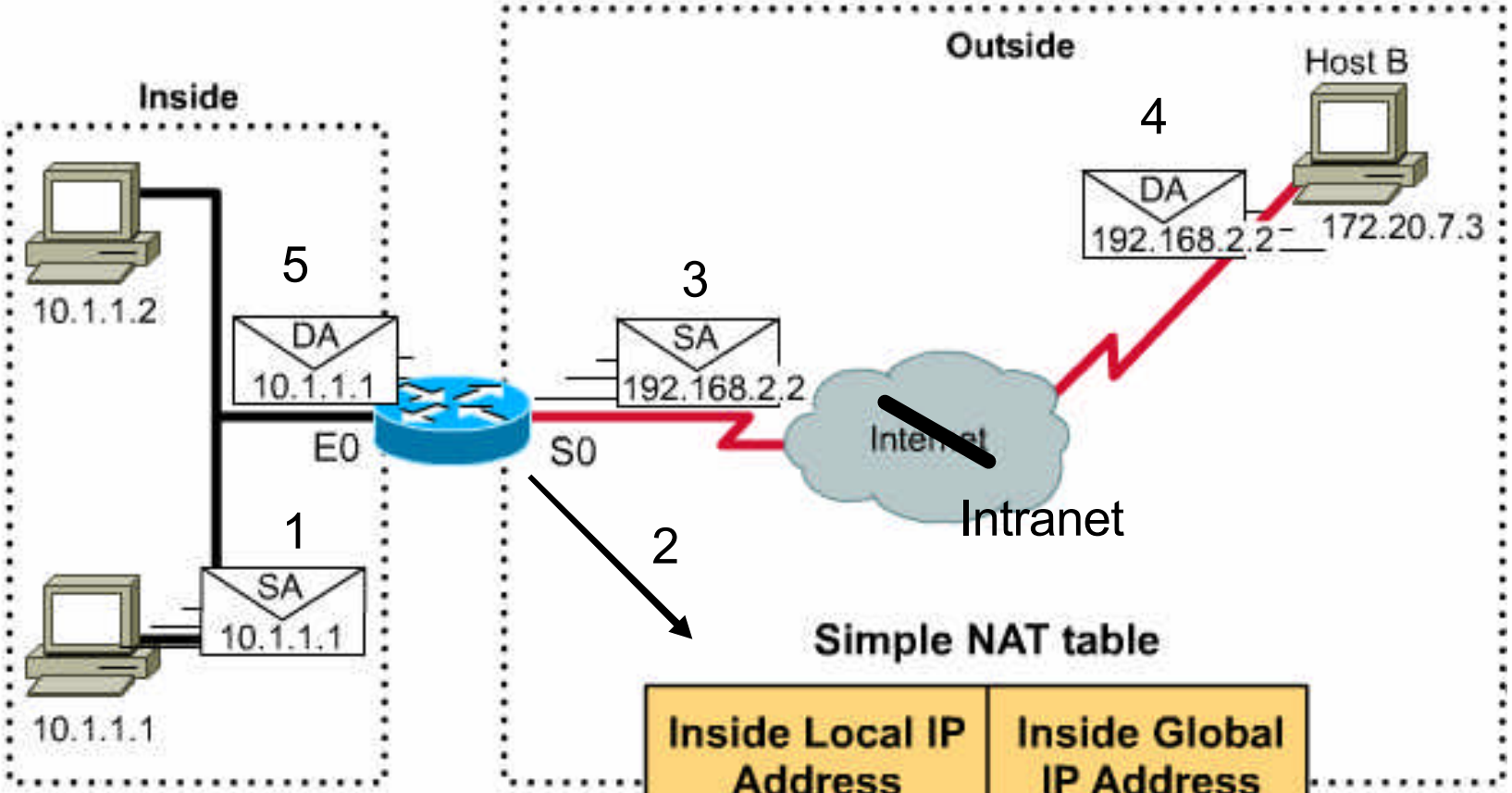
NAT: inside vs outside, local vs global

- **Inside vs outside:** Cisco define en los routers 2 zonas o lugares donde se aplicará NAT de una zona a otra: **inside y outside.** Las direcciones que utilizas en la LAN, internas son de la zona **inside,** independientemente del tipo de dirección. Las direcciones fuera de esta zona son consideradas **outside**.
- **Local vs global:** Una dirección es **local**, si sólo el router en cuestión conoce su traducción, es una dirección local al router y es **global** si puede ser encaminada fuera del router. Por tanto, para salir a Internet sólo podremos utilizar direcciones globales.

NAT: Local vs Global



Ejemplo de operación NAT



Simple NAT table

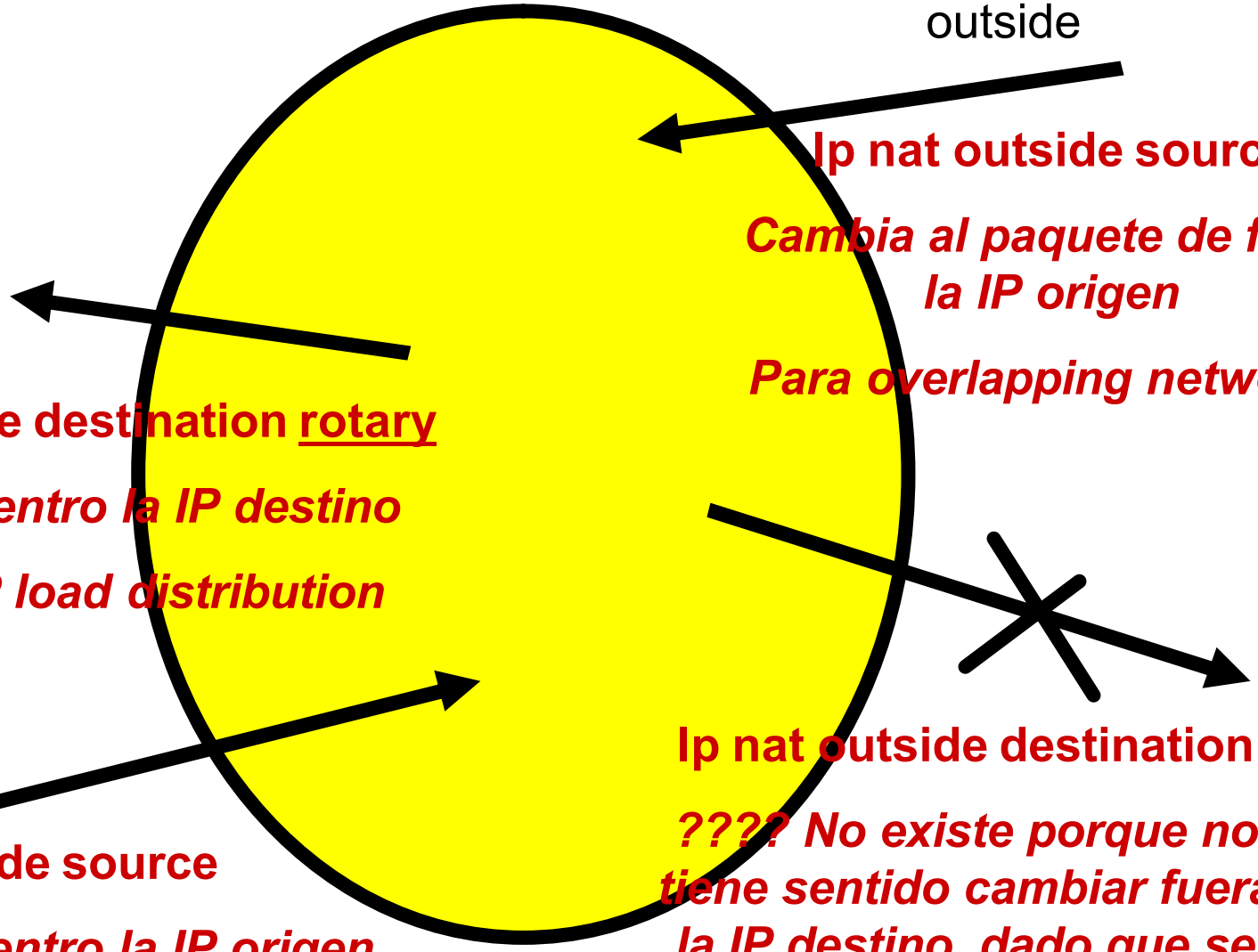
Inside Local IP Address	Inside Global IP Address
10.1.1.2 10.1.1.1	192.168.2.3 192.168.2.2

* 192.168.2.0/24

*** Esta red debe ser enrutable en el exterior (outside)**

SA: source address, dirección origen

Definiciones de NAT en el router con CISCO Systems



Ip nat outside source

Cambia al paquete de fuera la IP origen

Para overlapping networks

Ip nat inside destination rotary

Cambia dentro la IP destino

Para TCP load distribution

Ip nat outside destination

???? No existe porque no tiene sentido cambiar fuera la IP destino, dado que se debería reenviar a otro sitio el paquete

Ip nat inside source

Cambia dentro la IP origen

Para salir desde redes privadas

NAT: clientes primero!!

- Porque en outside no conocen la traducción de una dirección inside, el cliente debe iniciar la conexión para que el router realice la tabla de traducción, asignando a una “inside local” una “inside global”. De no ser así, desde fuera no podremos contectarnos a dentro.

- De esta forma, se oculta al exterior el mapa de direcciones IP y host disponibles, previniendo que hosts de fuera se conecten sin antes haber iniciado la conexión desde dentro.

- En el caso de tratarse de un servidor interno (dado que el servidor no inicia la conexión sino el cliente), para poderse conectar desde el exterior debe de estar traducido en NAT previamente y de forma permanente, es decir, debe existir un mapeo estático.

NAT Configuracion estático

De inside local a inside global!!

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

Especificar en las interfaces las zonas ***Inside*** *o* ***Outside***

```
RTA(config)#interface type number
RTA(config-if)#ip nat inside
RTA(config)#interface type number
RTA(config-if)#ip nat outside
```

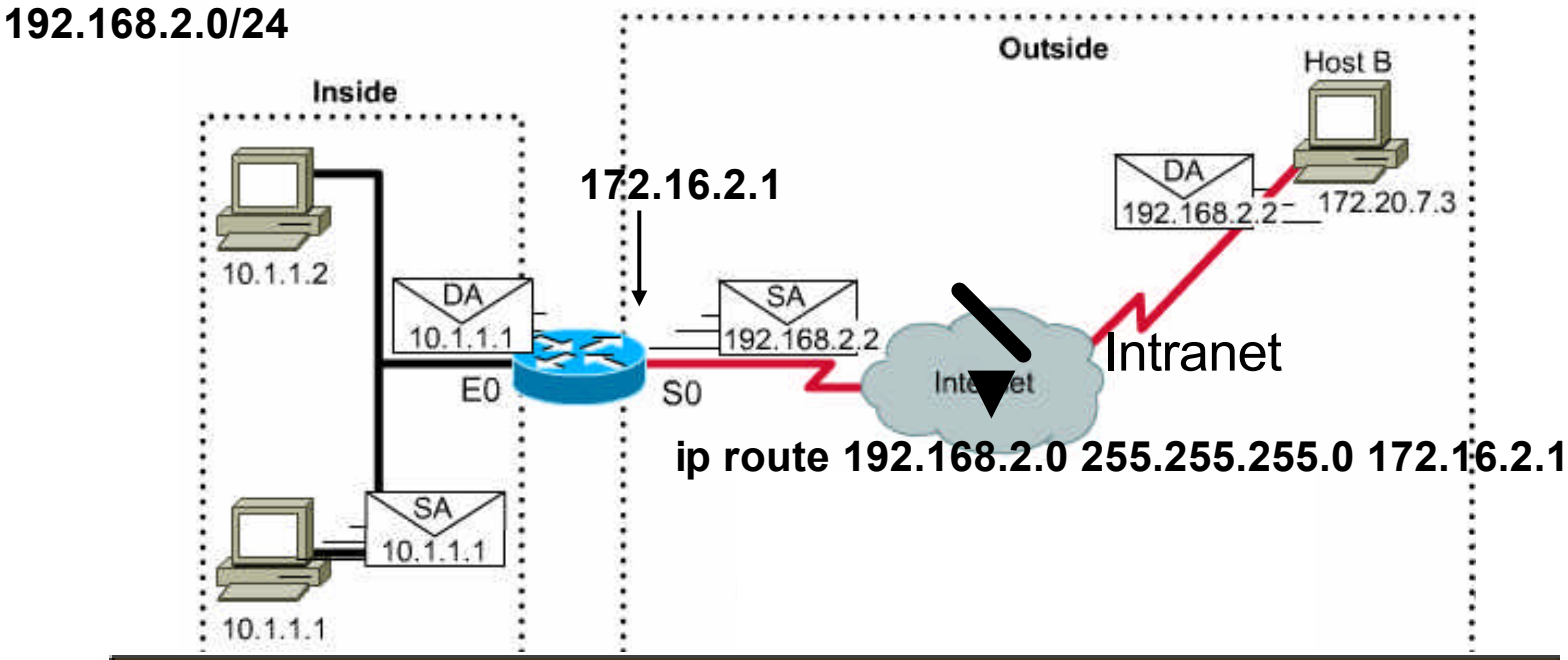
Sintaxis:

```
ip nat inside source {static {tcp | udp local-ip local-port
   global-ip global-port}
```

Ejemplo:

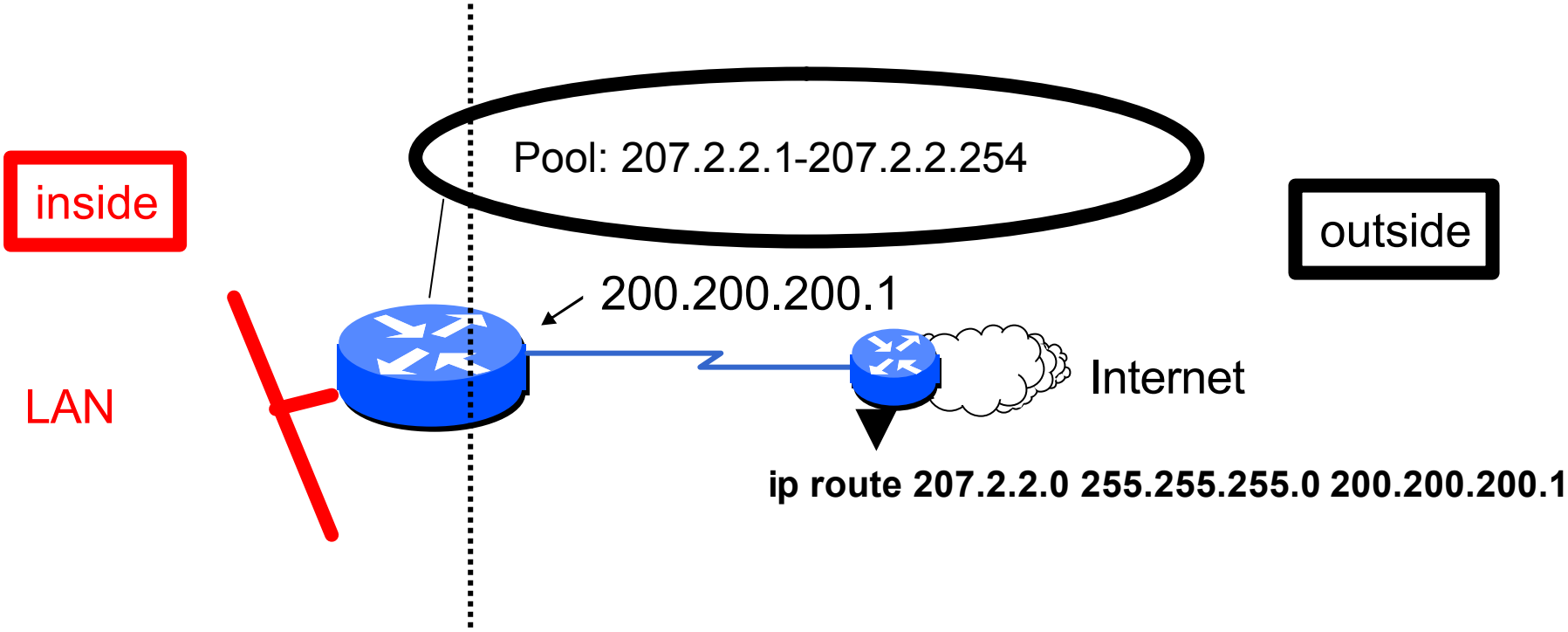
```
ip nat inside source static tcp 192.168.0.5 80 171.68.1.1 80
```

NAT Configuracion estático




```
ip nat inside source static 10.1.1.1 192.168.2.2
!
interface Ethernet0
ip address 10.1.1.10 255.255.255.0
ip nat inside
!
interface Serial0
ip address 172.16.2.1 255.255.255.0
ip nat outside
```

NAT Configuración dinámica (1/4)



Direccionamiento inside (LAN):

- **192.168.1.0/24 (*permitir que salga a Internet*)**
- **192.168.2.0/24 (*no permitir*)**

NAT Configuración dinámica (2/4)

1.- Definir el pool :

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

RTA(config)#**ip nat pool MYPOOL 207.2.2.0 207.2.2.255**
netmask 255.255.255.0

Direcciones disponibles

Nota: 207.2.2.0 - 207.2.2.255 deben ser Internet Public Addresses y serán utilizadas para Inside Global Address.

NAT Configuración dinámica(3/4)

2.- Definir direcciones IP permitidas para el NAT:

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

Router(config)# ip nat inside source {list
   {access-list-number | name} pool name
   [overload] | static local-ip global-ip}
```

Direcciones a ser traducidas

```
RTA(config)#access-list 1 permit 192.168.1.0 0.0.0.255
RTA(config)#ip nat inside source list 1 pool MYPOOL
```

Nota: 192.168.1.0/24 son Internal Local Address

NAT Configuración dinámica(4/4)

3.- Definir interfaces inside/outside:

```
Router(config)#interface type number
Router(config-if)#ip nat inside
```

```
Router(config)#interface type number:
Router(config-if)#ip nat outside
```

RTA(config)#**interface serial0**

RTA(config-if)#**ip nat outside**

RTA(config)#**interface ethernet0**

RTA(config-if)#**ip nat inside**

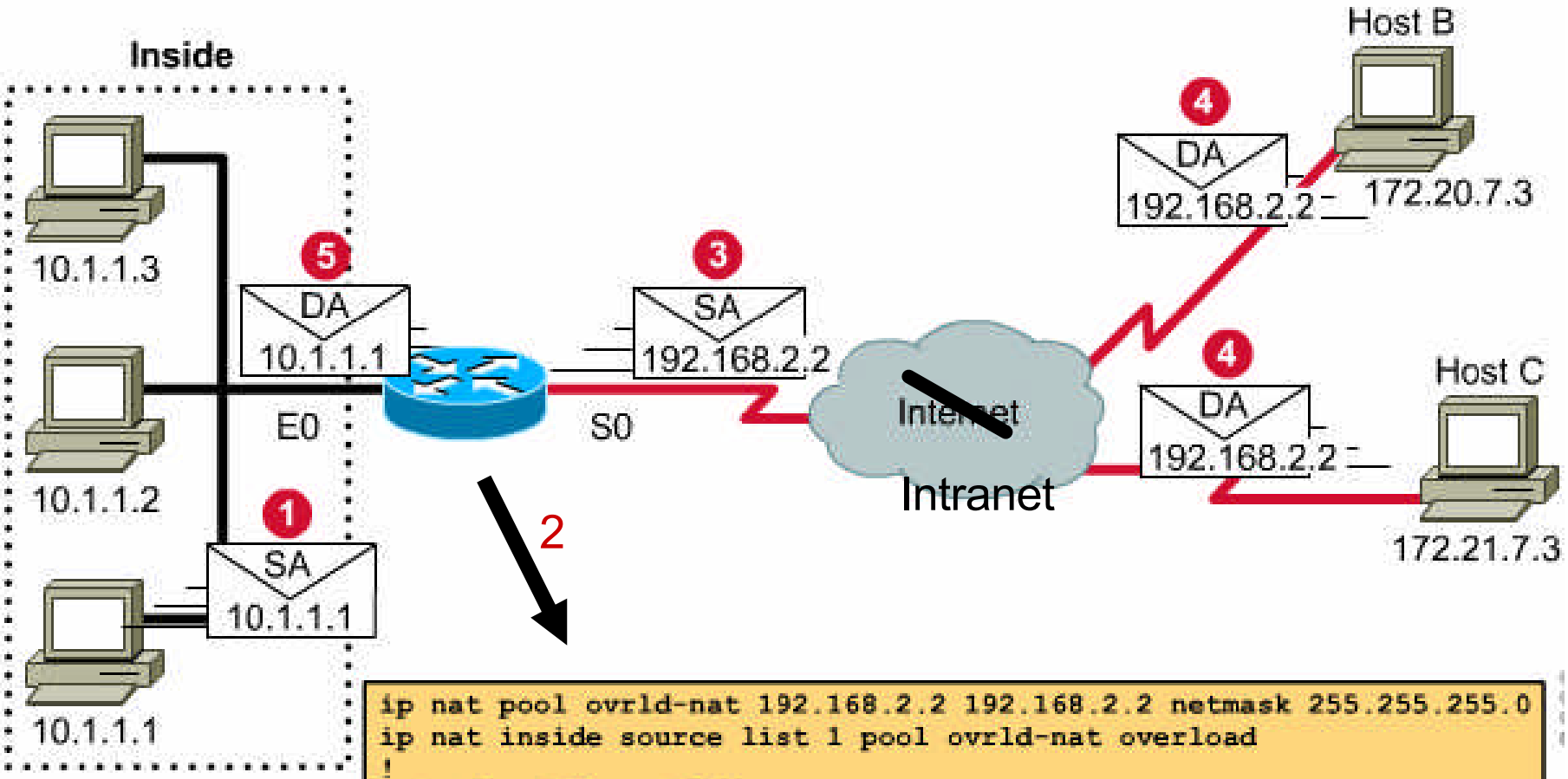
PAT Configuración

Router(config)#**ip nat inside source list 24 {pool *natpool*|interface *serial0*} overload**

RTA(config)#**ip nat inside source list 24 pool natpool overload**

Nota: el pool de NAT puede ser de sólo una IP, por ejemplo la IP pública de la interfaz de salida.

PAT Configuración




```
ip nat pool ovrld-nat 192.168.2.2 192.168.2.2 netmask 255.255.255.0
ip nat inside source list 1 pool ovrld-nat overload
!
interface Ethernet0/0
ip address 10.1.1.10 255.255.255.0
ip nat inside
!
interface Serial0/0
ip address 172.16.2.1 255.255.255.0
ip nat outside
!
access-list 1 permit 10.1.1.0 0.0.0.255
```

NAT Overlapping

las direcciones internas de la LAN del router

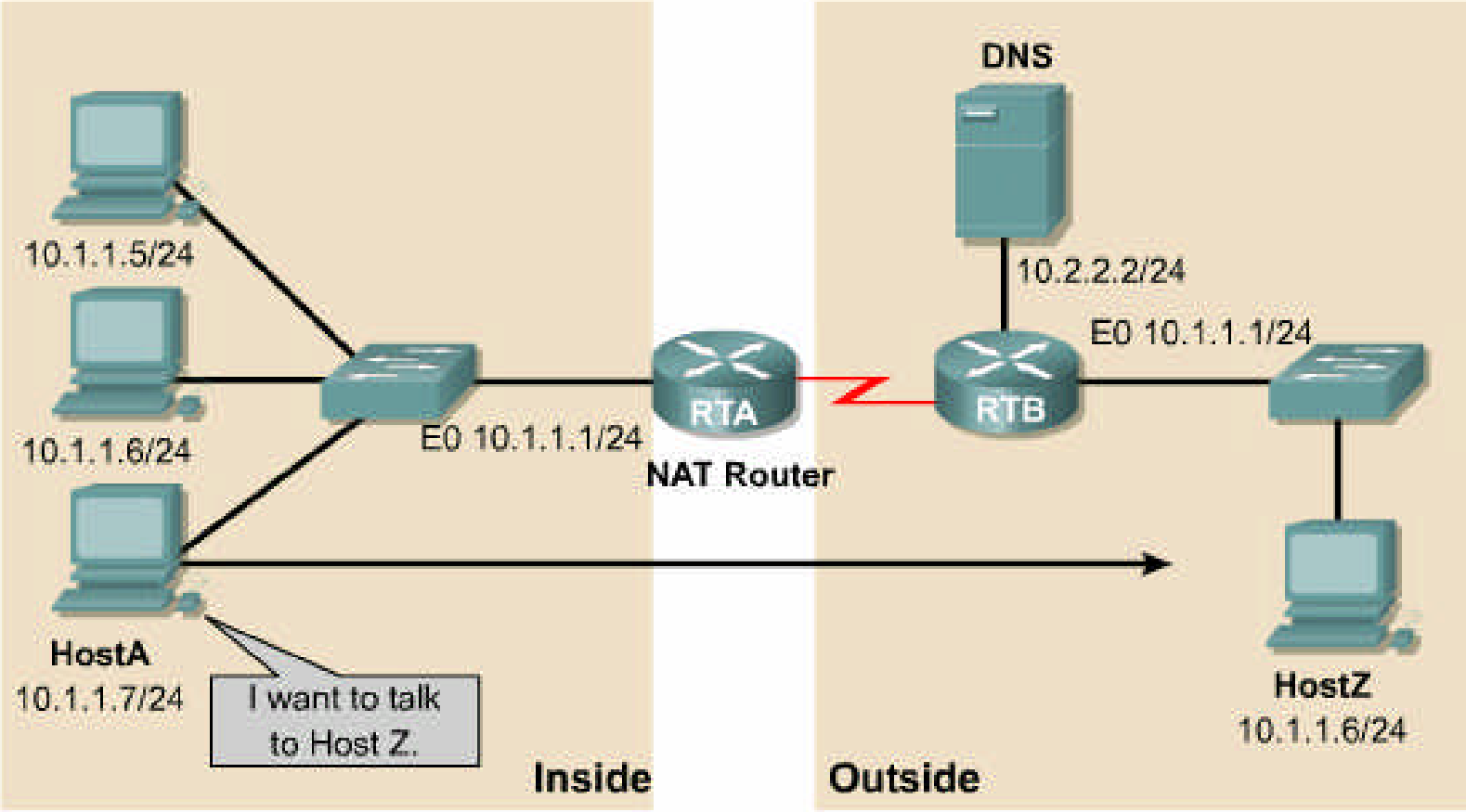
coinciden (son las mismas)

con las direcciones de otra LAN en otro router

Casos de NAT Overlapping

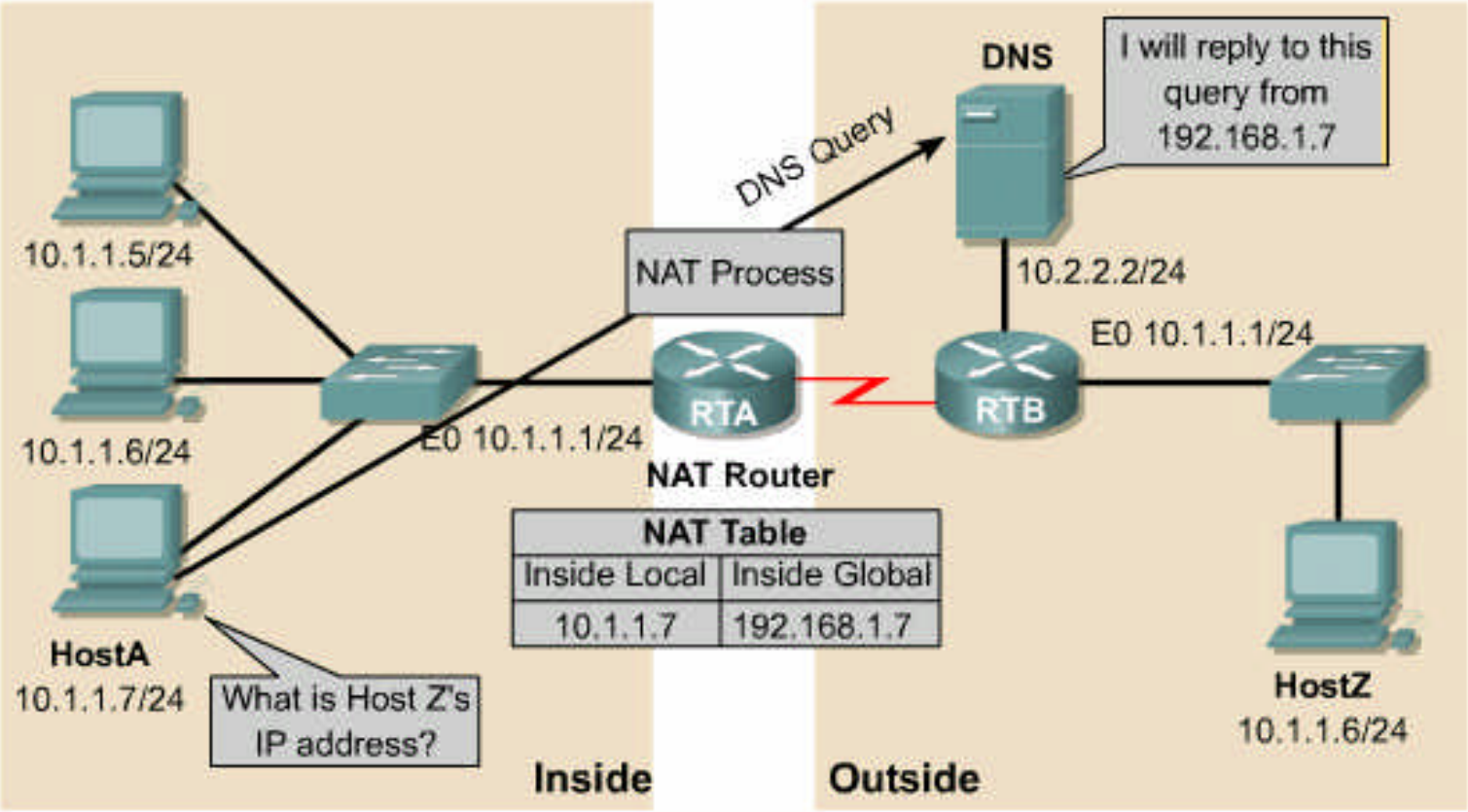
- Se intentan conectar 2 redes privadas
- Se intenta conectar a Internet una red que inicialmente se planeó como privada pero se está usando direcciones públicas (ejemplo 147.156.0.0 como red privada)
- Reasignación de direcciones públicas y no se quiere abandonar las direcciones viejas (que se han dado a otra entidad)

NAT overlapping (1/5)



HostA wants to establish an IP connection with HostZ, but cannot use the IP address 10.1.1.6 of HostZ.

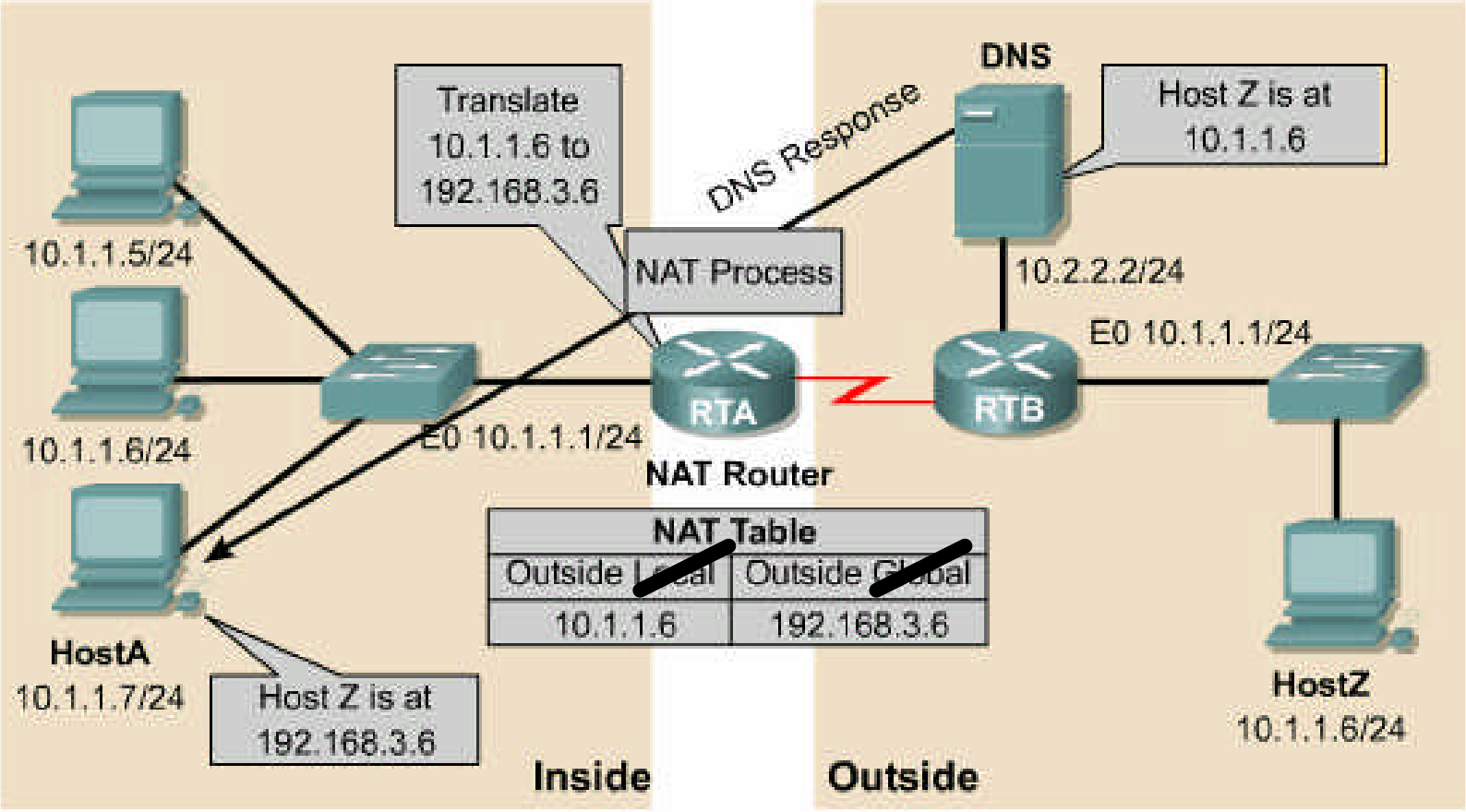
NAT overlapping (2/5)



HostA's DNS request is translated by NAT.

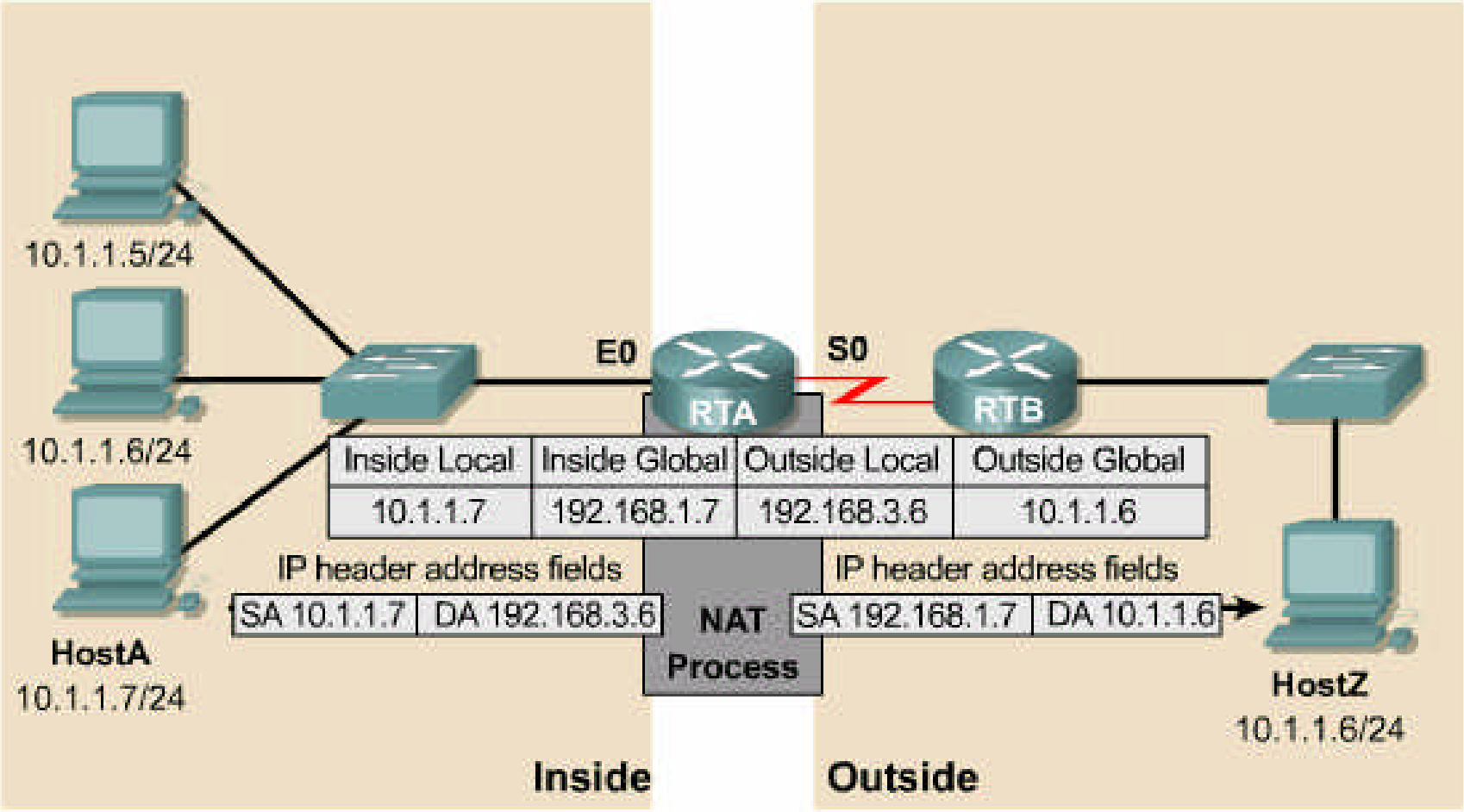
Note: Host A needs a Host Z IP address outside its own network, because if not, it will never send to the router.

NAT overlapping (3/5)



In an overlapping networks scenario, DNS responses are translated by NAT.

NAT overlapping (4/5)



NAT overlapping (5/5): Configuración

```
RTA(config)# ip nat pool inGlobal 192.168.1.1 192.168.1.254
prefix-length 24

RTA(config)#ip nat pool outGlobal 192.168.3.1 192.168.3.254
prefix-length 24
```

Configuración NAT dinámica

NAT overlapping (5/5): Configuración

```
RTA(config)# ip nat pool inGlobal 192.168.1.1 192.168.1.254
prefix-length 24

RTA(config)#ip nat pool outGlobal 192.168.3.1 192.168.3.254
prefix-length 24
```

Nombre que le hemos dado al Pool: inGlobal, outGlobal

NAT overlapping (5/5): Configuración

```
RTA(config)# ip nat pool inGlobal 192.168.1.1 192.168.1.254
prefix-length 24

RTA(config)#ip nat pool outGlobal 192.168.3.1 192.168.3.254
prefix-length 24
```

Direcciones IP que puede coger para salir al exterior

NAT overlapping (5/5): Configuración

```
RTA(config)# ip nat pool inGlobal 192.168.1.1 192.168.1.254
prefix-length 24

RTA(config)#ip nat pool outGlobal 192.168.3.1 192.168.3.254
prefix-length
```

Máscara de red o número de bits de máscara de red

NAT overlapping (5/5): Configuración

```
RTA(config)#ip nat inside source list 2 pool inGlobal

RTA(config)#ip nat outside source list 2 pool outGlobal

RTA(config)#access-list 2 permit 10.1.1.0 0.0.0.255
```

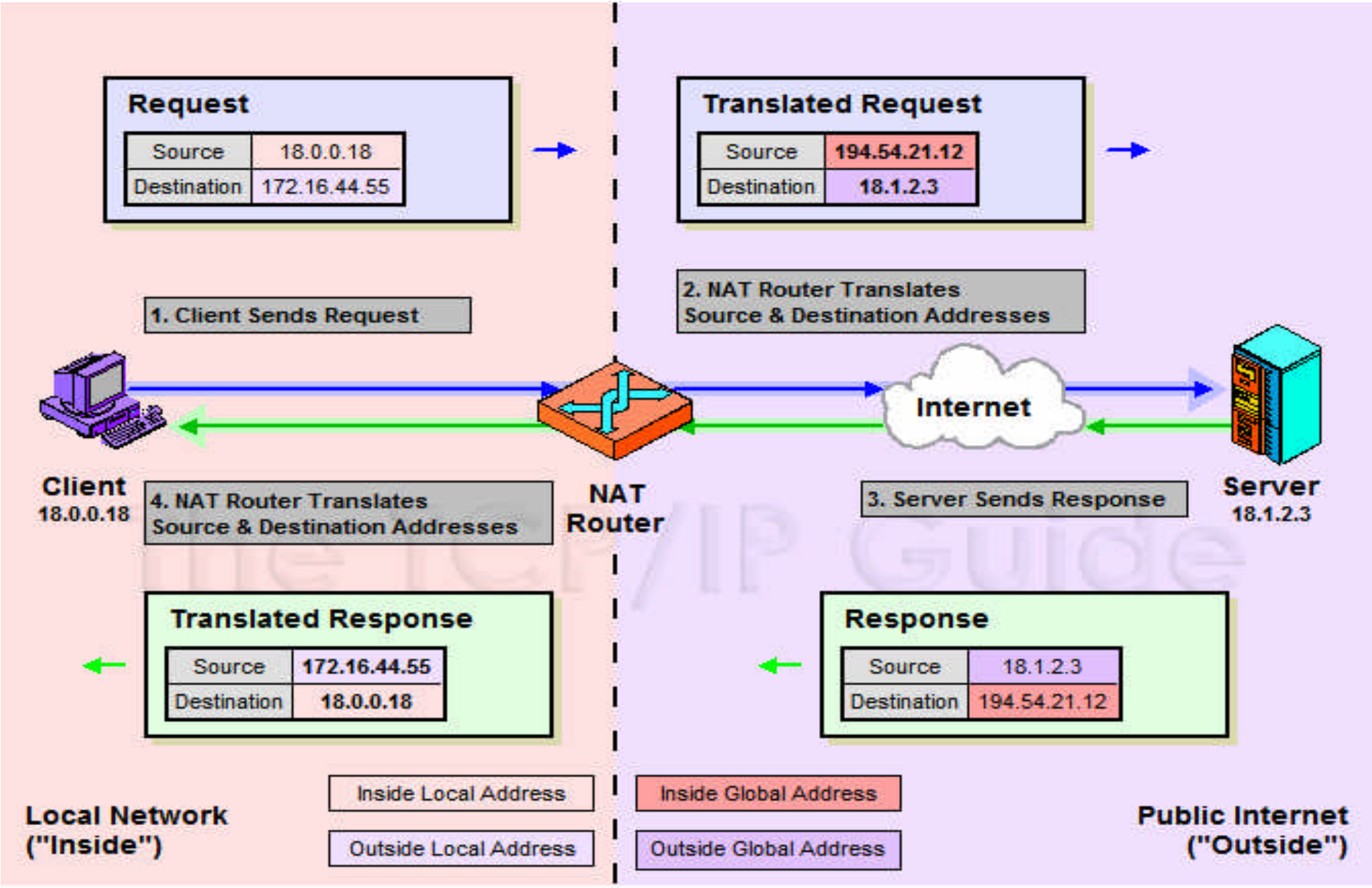
Direcciones internas que van a ser traducidas

NAT overlapping (5/5)

```
RTA(config)#ip nat pool inGlobal 192.168.1.1 192.168.1.254
prefix-length 24

RTA(config)#ip nat pool outGlobal 192.168.3.1 192.168.3.254
prefix-length 24

RTA(config)#ip nat inside source list 2 pool inGlobal

RTA(config)#ip nat outside source list 2 pool outGlobal

RTA(config)#access-list 2 permit 10.1.1.0 0.0.0.255

RTA(config)#interface ethernet0

RTA(config-if)#ip nat inside

RTA(config)#interface serial0

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

Qué es inside y outside

```
RTA#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 192.168.1.7        10.1.1.7           ---                ---
--- ---                ---                192.168.3.6        10.1.1.6
--- 192.168.1.7        10.1.1.7           192.168.3.6        10.1.1.6
```

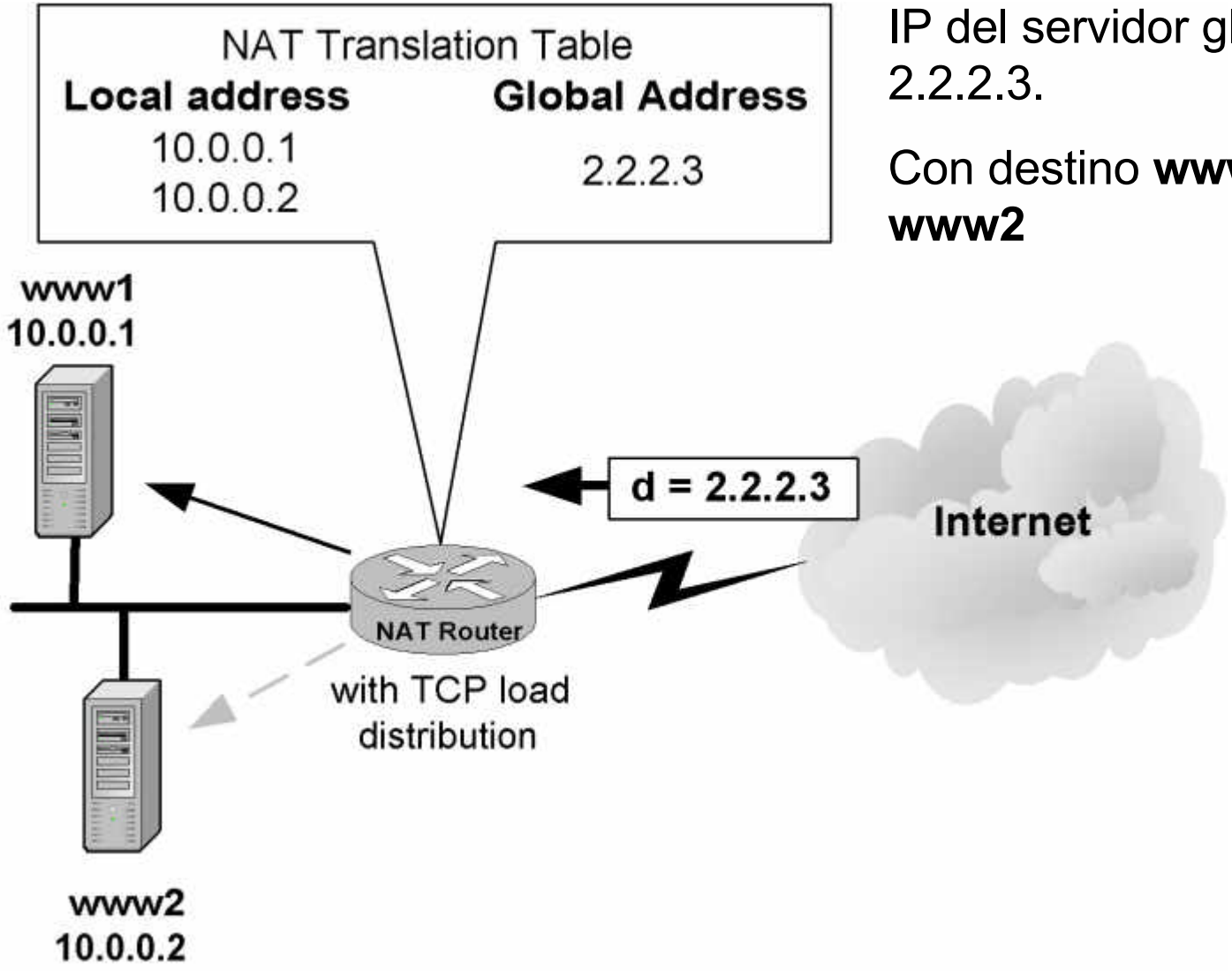


Se le llama también “Doble NAT (NAT TWICE)”

Otros: TCP Load distribution

- Cisco routers soportan **TCP load distribution**, una funcionalidad del NAT para permitir mapear una dirección global bajo varias direcciones “inside” con el propósito de distribuir la carga computacional (balanceo de carga)
- Esto permite tener un servidor virtual con una IP determinada, ser gestionado por varias máquinas internamente, varias IP. Esos servidores son “mirrored” hosts.

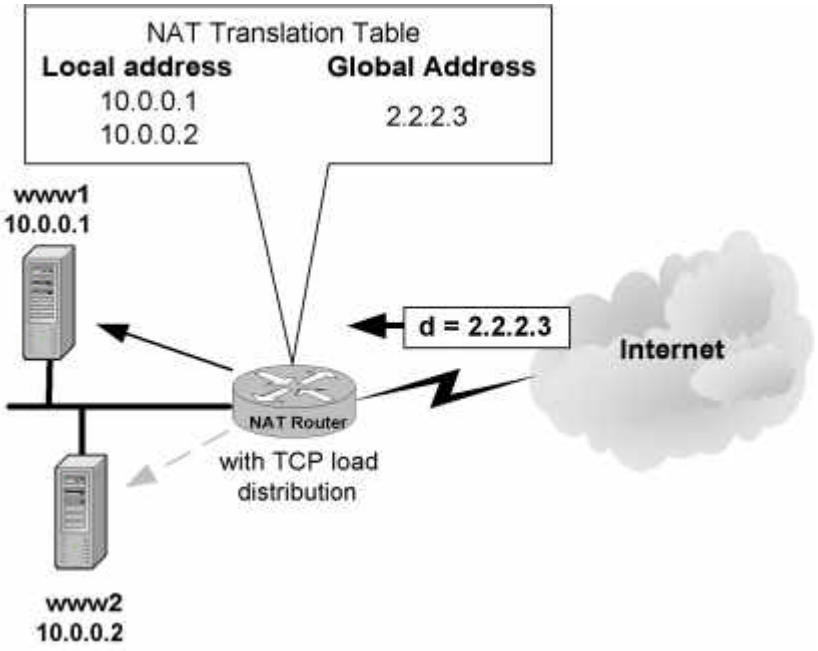
TCP Load Distribution



IP del servidor global 2.2.2.3.

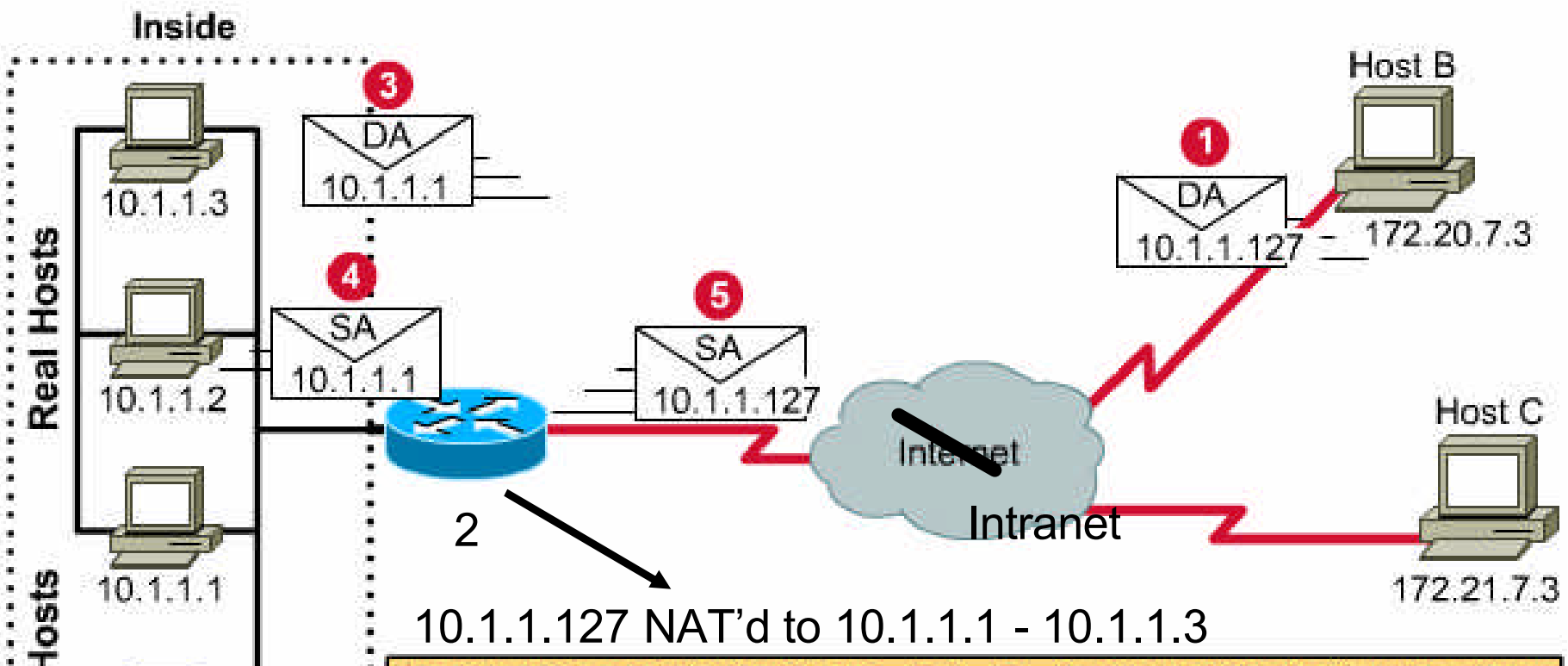
Con destino **www1 y www2**

NAT Configuración Rotary (ejemplo 1)




```
RTA(config)#ip nat pool webservers 10.0.0.1
  10.0.0.2 netmask 255.0.0.0 type rotary
RTA(config)#access-list 46 permit host 2.2.2.3
RTA(config)#ip nat inside destination list 46 pool
  webservers
RTA(config)#interface ethernet0
RTA(config-if)#ip nat inside
RTA(config)#interface serial0
RTA(config)#ip nat outside
```

NAT Configuración: Rotary (ejemplo 2)



10.1.1.127 NAT'd to 10.1.1.1 - 10.1.1.3

```
ip nat pool real-hosts 10.1.1.1 10.1.1.3 prefix-length 24 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial0
ip address 192.168.1.129 255.255.255.224
ip nat outside
!
interface ethernet0
ip address 10.1.1.254 255.255.255.0
ip nat inside
!
access-list 2 permit 10.1.1.127
```

Verificación y modificación NAT

```
Router#show ip nat translations [verbose]
Router#show ip nat statistics
Router#clear ip nat *
Router#clear ip nat {inside|outside} *
Router#debug ip nat
```

Timeouts: por defecto el préstamo de IP son 24 hours (86400 sec) en TCP y 5 minutos (300 sec) en UDP. Para modificar:

```
Router#ip nat translation timeout sec
Router#ip nat translation tcp-timeout sec
Router#ip nat translation udp-timeout sec
```

Consecuencias de NAT

- Al cambiar la dirección IP es preciso:
  - Modificar la dirección origen o destino de la cabecera IP. También hay que recalcular el checksum
  - Recalcular el checksum de la cabecera TCP o UDP (ya que la dirección IP, que aparece en la pseudocabecera, se utiliza para calcularlo).
  - En caso de utilizar NAPT hay que modificar el número de puerto TCP/UDP origen o destino.
  - Los mensajes ICMP contienen en la parte de datos la cabecera del mensaje al que hacen referencia. Con NAT el router ha de buscar esas cabeceras y modificarlas.
  - Los mensajes SNMP incluyen direcciones IP entre los datos del paquete que hay que cambiar.

Limitaciones y problemas de NAT

- Algunos protocolos de aplicación (ej. H.323, NetBIOS) incluyen las direcciones IP en diversos sitios de los datos del paquete. Esto requiere pasarelas del nivel de aplicación para funcionar a través de NAT.
- Generalmente las implementaciones de NAT van incorporando soporte para los nuevos protocolos estándar que aparecen y que utilizan direcciones IP en la parte de datos. Por eso cuando se usa NAT es especialmente importante utilizar las versiones de software más recientes.
- El uso de NAPT (PAT, overload) plantea problemas adicionales, por ejemplo generalmente no se pueden enviar mensajes ICMP (comandos ping o traceroute), ya que no incluye información de capa 4 o puertos.
- Con NAT no puede utilizarse la función AH de IPSec, salvo que se utilice IPSec en modo túnel y el NAT se haga antes, o en el mismo dispositivo donde se hace el túnel IPSec. Esto es por que AH, Authentication Header de IPsec corrobora la integridad de la cabecera, pero si se modifica con NAT (IPsec en modo transporte) esta función no puede implementarse.

NAT, IOS y compatibilidad

Cisco ISO NAT soporta:

- Cualquier tráfico TCP/UDP que no transporte IP en los datos
- HTTP, FTP, TFTP, NTP, NFS
- Telnet, Archie, Finger, rlogin, rsh, rcp

Cisco IOS NAT también soporta aunque transporten IP en los datos:

- ICMP
- NetBIOS over TCP/IP para servicios
- RealAudio
- CuSeeMe
- DNS "A" and "PTR" queries
- H.323/NetMeeting versions >12.0(1)/12.0(1)T
- VDOLive versions >11.3(4)11.3(4)T
- Vxtreme versions >11.3(4)11.3(4)T
- IP multicast version >12.0(1)T para direcciones origen sólo

Cisco IOS NAT NO soporta:

- Routing y sus tablas
- Transferencias de zona DNS
- BOOTP, SNMP
- talk, ntalk, NetShow