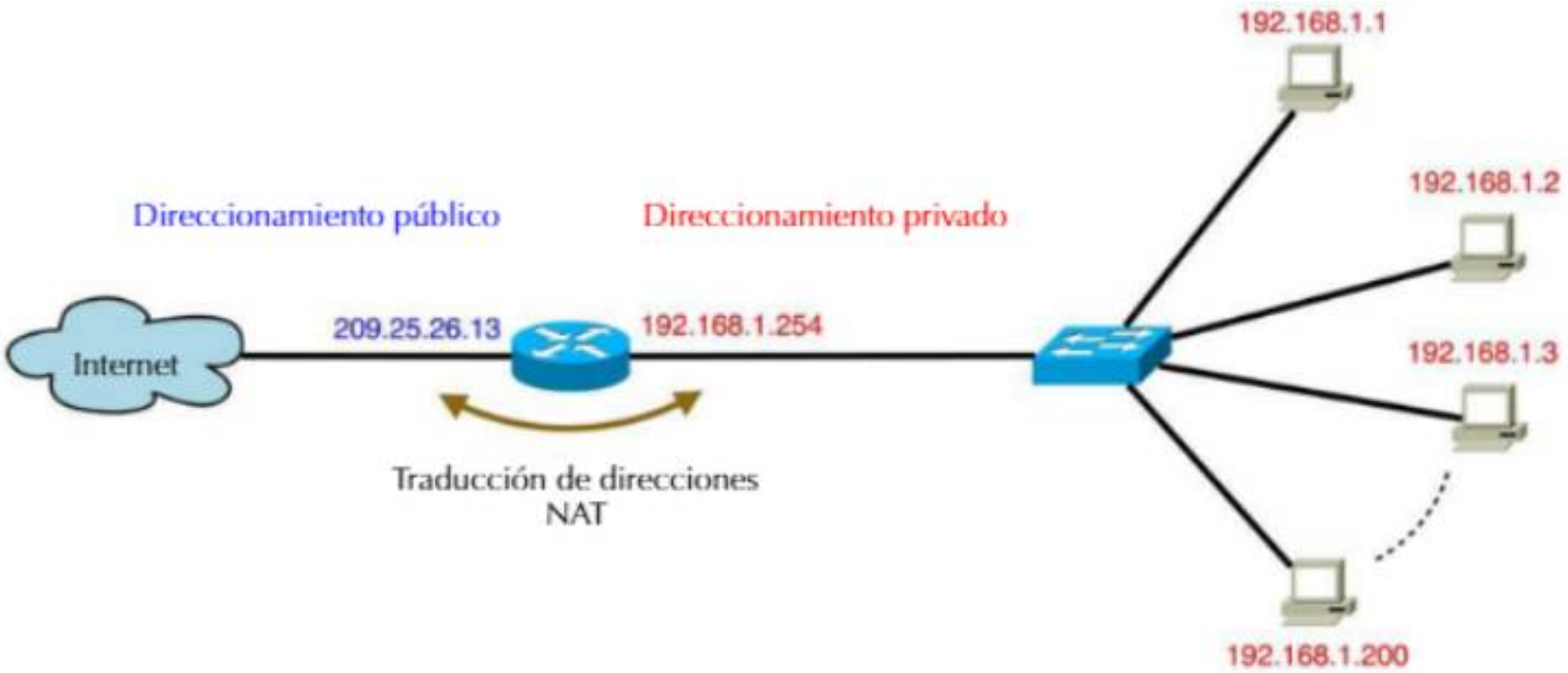
NAT

el rango de direccionamiento en la red interna es privado, concretamente, 192.168.1.0/24, pero cuando los paquetes enviados por los dispositivos locales son encaminados por el router hacia el exterior, este transforma las direcciones privadas en la misma dirección pública 209.25.26.13



NAT ESTÁTICO

Consiste básicamente en un tipo de NAT en el que se mapea una dirección IP privada con una dirección IP pública de forma estática. De esta manera, cada equipo en la red privada debe tener su correspondiente IP pública asignada para poder acceder a Internet. La principal desventaja de este esquema es que, por cada equipo que se desee que tenga acceso a Internet, se debe contratar una IP pública. Para configurar este tipo de NAT en Cisco hay que utilizar los siguientes comandos:

R(config)# ip nat inside source static [ip-privada][ip-pública]
R(config)# interface [nombre][número]
R(config-if)# ip nat inside
R(config)# interface [nombre][número]
R(config-if)# ip nat outside

Se usa principalmente para que se pueda entrar desde fuera y no tanto para poder salir desde dentro.

NAT DINÁMICO

En este caso se utiliza un rango (pool) de IP públicas y otro rango (pool) de IP privadas, que serán transformadas de forma dinámica y a petición de los clientes.
La principal ventaja es que se garantiza el acceso a Internet de todas las IP privadas, siempre y cuando el número de máquinas encendidas en la red privada no supere al número de IP públicas disponibles. Para configurar este tipo de NAT en Cisco se utilizan los siguientes comandos:

R(config)# ip nat pool [nombre] [IPinicial] [IPfinal] netmask [máscara]
R(config)# access-list [número] permit [IP] [wildcard]
R(config)# ip nat inside source list [número] pool [nombre]
R(config)# interface [nombre] [número]
R(config-if)# ip nat inside
R(config)# interface [nombre] [número]
R(config-if)# ip nat outside

NAT CON SOBRECARGA O PAT

El caso de NAT con sobrecarga es el más común de todos y el más usado en los hogares.
Consiste en utilizar una única dirección IP pública para mapear múltiples direcciones IP privadas

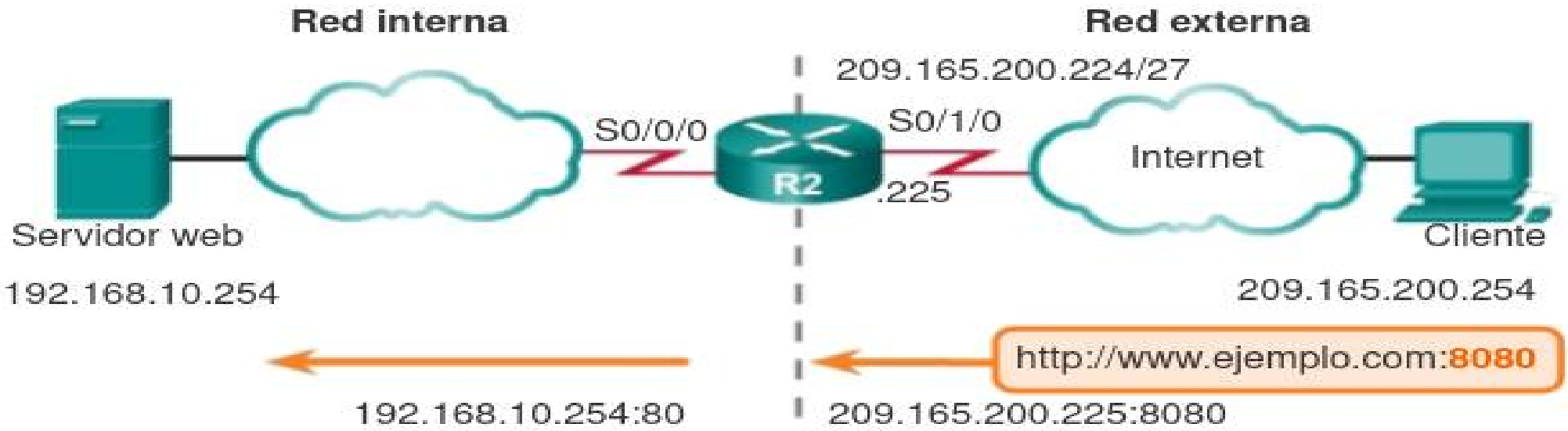
La arquitectura TCP/IP permite direccionar hasta 65.536 números de puerto diferentes, de tal forma que, combinando una IP pública con el número de puerto, se permitirán hasta un total de 65.536 accesos concurrentes a Internet; aunque si se dispone de dos direccio-nes públicas, se podrán permitir el doble de accesos simultáneos y así sucesivamente.
Para configurar este tipo de traducción de direcciones PAT en Cisco se dispone de los siguientes comandos:

ip inside

R(config)# **access-list [n] permit [IP] [wildcard]**
R(config)# **ip nat inside source list [n] interface [nombre] [número] overload**
interface outside
R(config)# **interface [nombre] [número]**
R(config-if)# **ip nat inside**
R(config)# **interface [nombre] [número]**
R(config-if)# **ip nat outside**

PORT FORWARDING
GAMING
TUNNELING
APERTURA DE PUERTOS

Ejemplo de reenvío de puertos con IOS



Establece la traducción estática entre una dirección local interna y un puerto local, y entre una dirección global interna y un puerto global.

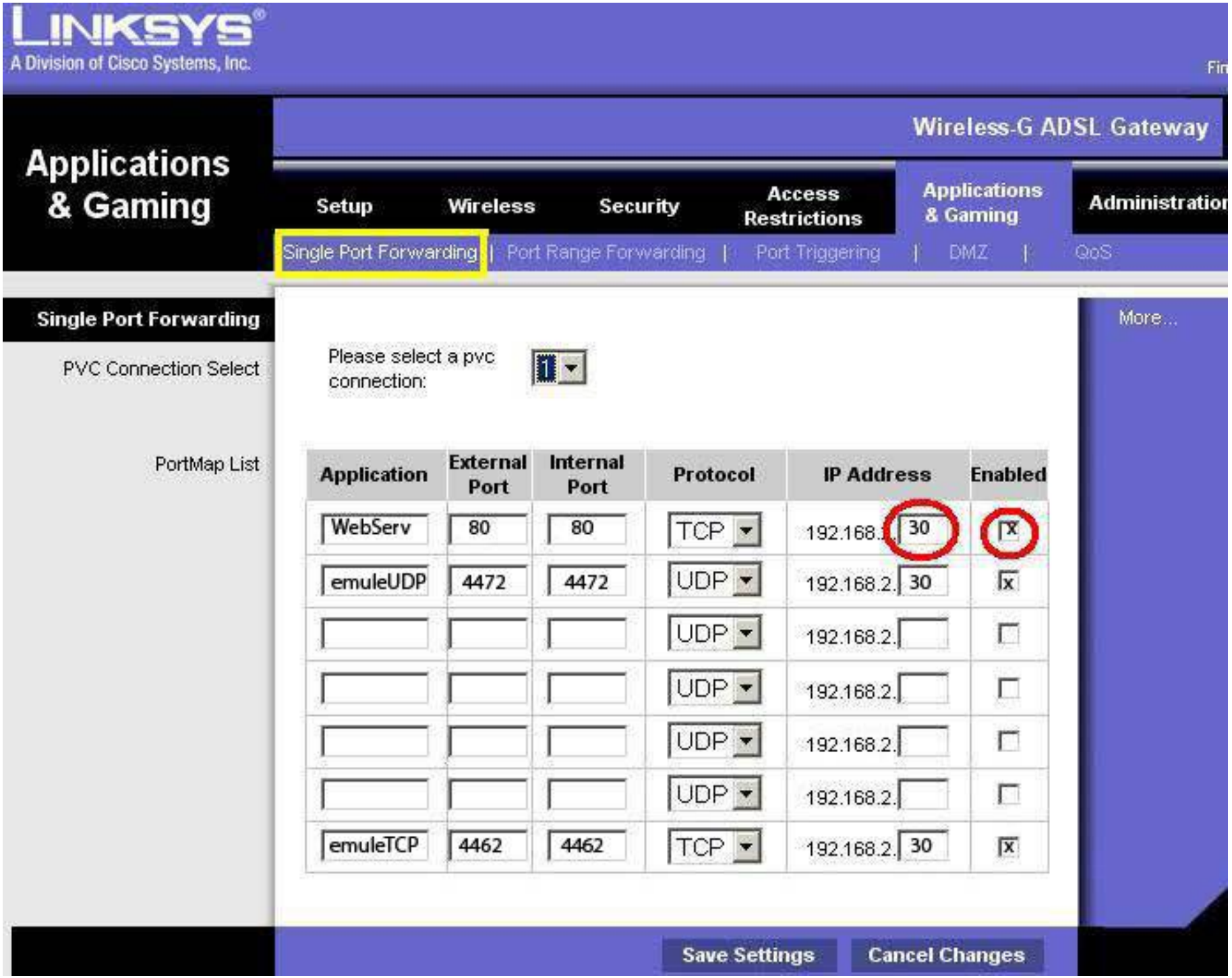
```
R2(config)# ip nat inside source static tcp
192.168.10.254 80 209.165.200.225 8080
```

Identifica la interfaz serial 0/0/0 como interfaz NAT interna.

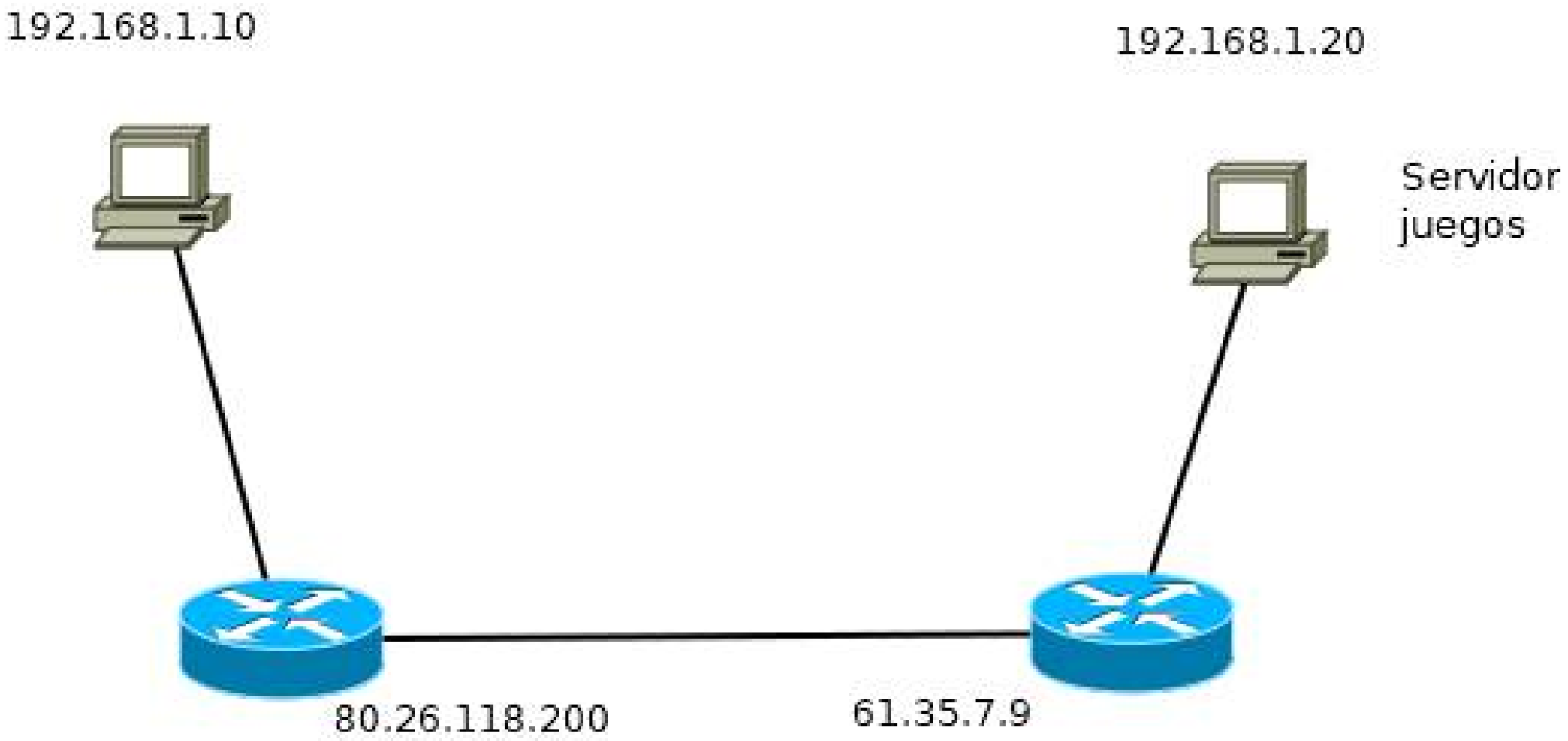
```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

Identifica la interfaz serial 0/1/0 como interfaz NAT externa.

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

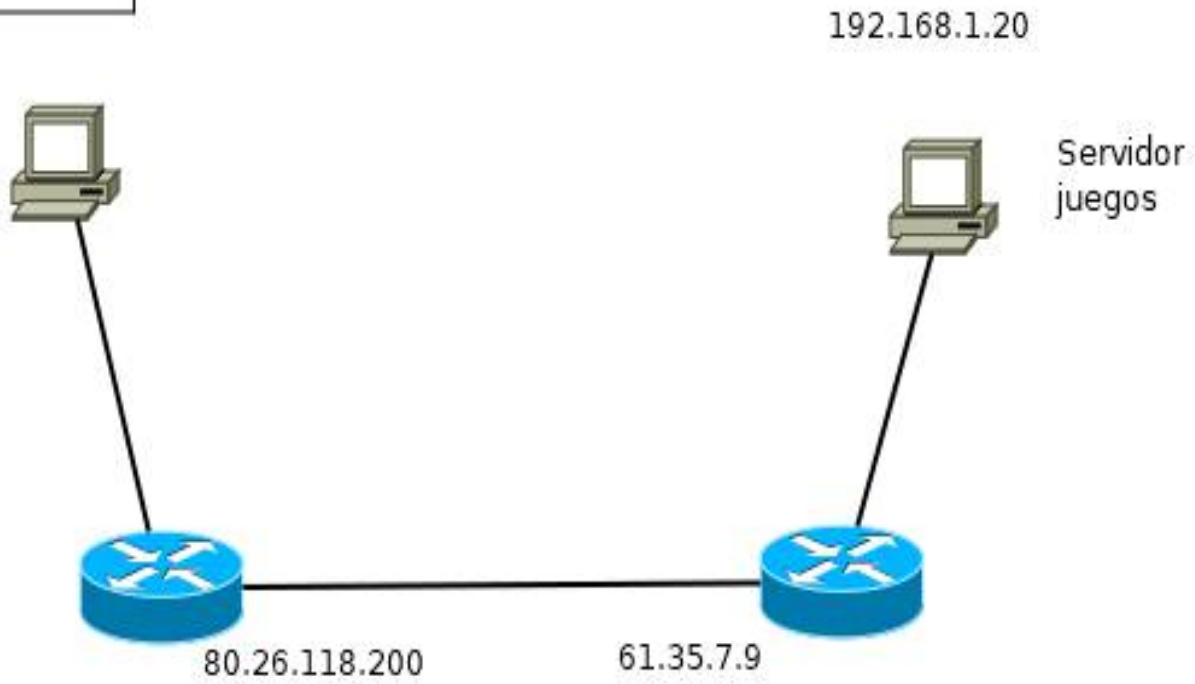

LINKSYS
A Division of Cisco Systems, Inc.
Wireless-G ADSL Gateway
Applications & Gaming
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Single Port Forwarding | Port Range Forwarding | Port Triggering | DMZ | QoS
Single Port Forwarding
PVC Connection Select
PortMap List
More...
Please select a pvc connection:
1
Application
External Port
Internal Port
Protocol
IP Address
Enabled
WebServ 80 80 TCP 192.168.2. 30 X
emuleUDP 4472 4472 UDP 192.168.2. 30 X
UDP 192.168.2.
UDP 192.168.2.
UDP 192.168.2.
UDP 192.168.2.
emuleTCP 4462 4462 TCP 192.168.2. 30 X
Save Settings
Cancel Changes

Paso 1: un usuario quiere iniciar una conexión y conectarse a un servidor en otro lugar remoto.

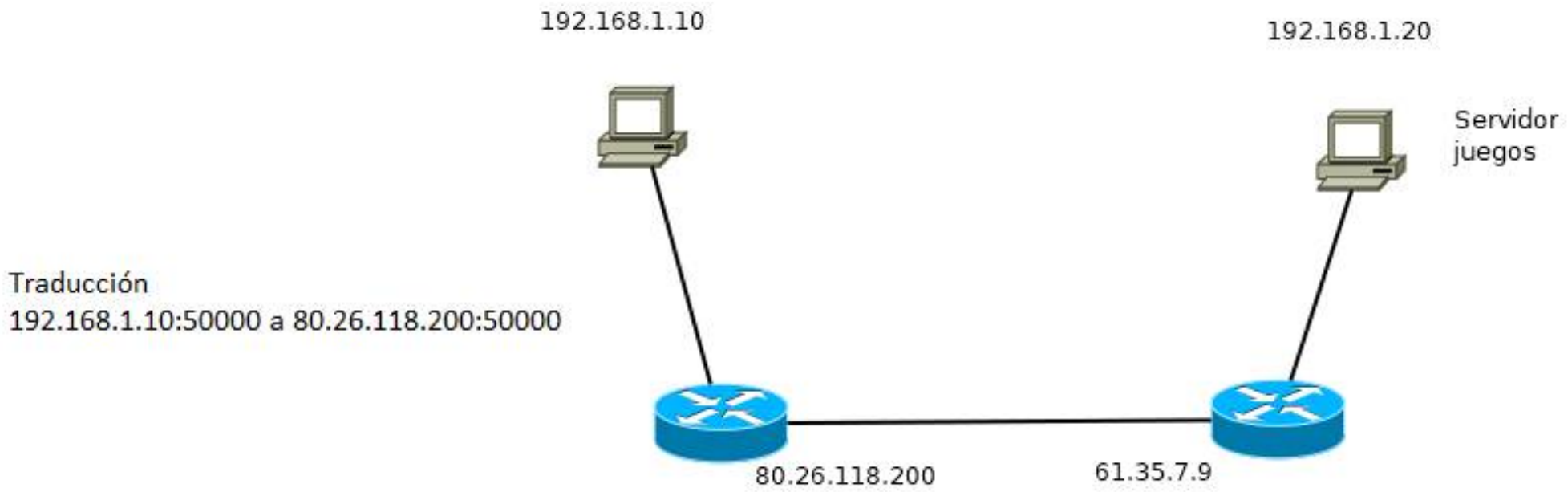


Paso 2: el usuario pide al servidor la IP pública de su router y usando su programa intenta conectarse a la IP pública del otro router y al puerto del juego o servicio. El puerto de origen se elige al azar.

IP Origen	192.168.1.10
Puerto origen	50000
IP Destino	61.35.7.9
Puerto destino	6003

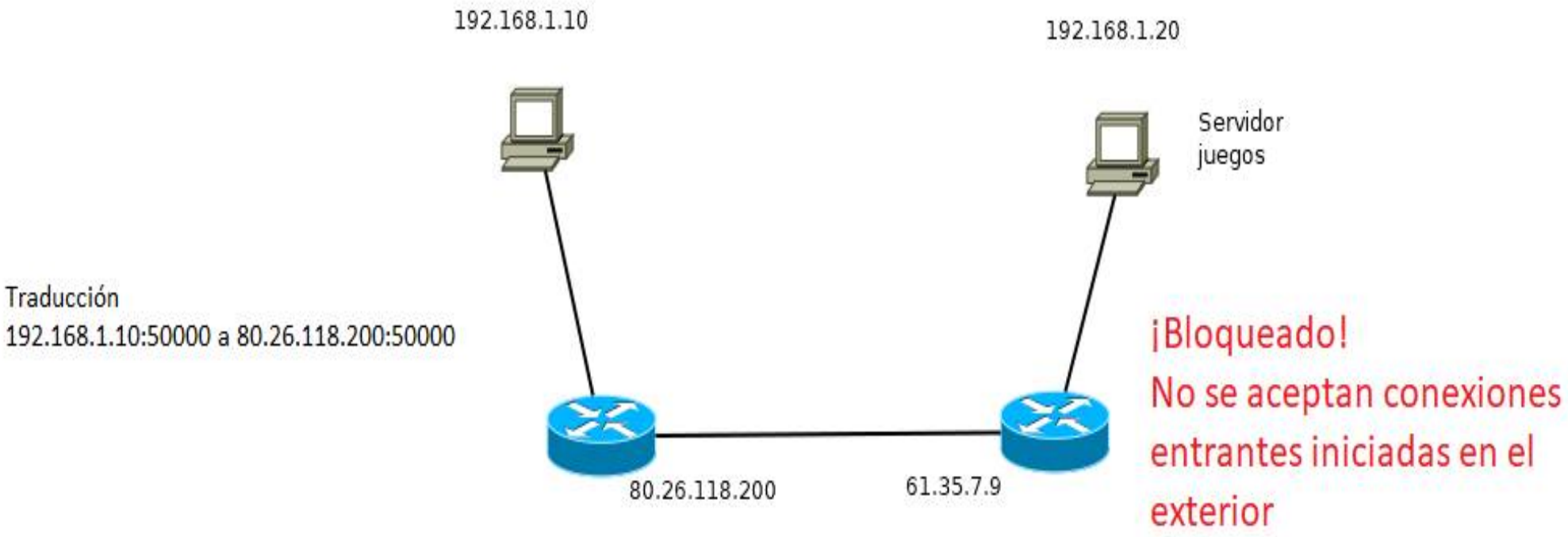


Paso 3: el paquete llega al router. El router observa que el paquete va al exterior. Como no se pueden usar IPs privadas en el exterior, el router CAMBIA LA IP DE ORIGEN Y TOMA NOTA DE ESA TRADUCCIÓN POR SI EN EL FUTURO SE NECESITA ESA INFORMACIÓN.



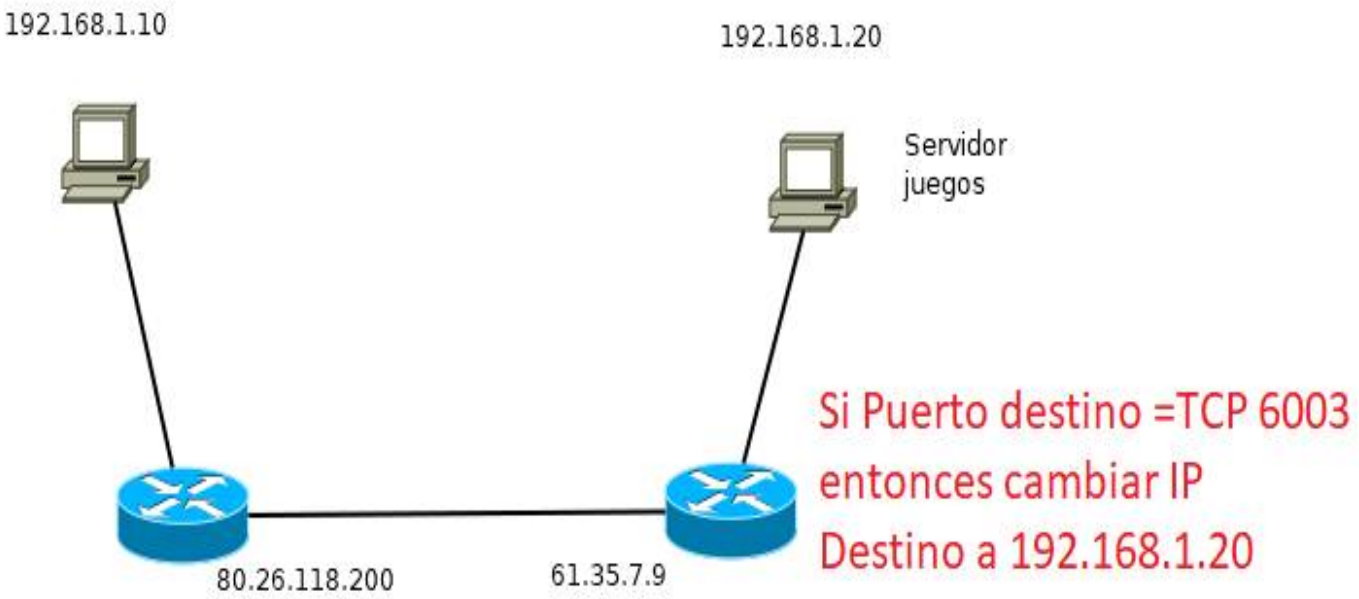
IP Origen	~~192.168.1.10~~ → 80.26.118.200
Puerto origen	50000
IP Destino	61.35.7.9
Puerto destino	6003

Paso 4: el paquete (con la IP de origen cambiada) viaja por la red y llega al router de destino. Como los router por defecto no aceptan conexiones entrantes, en principio el paquete no entraría Es necesario que primero el router derecho tenga el puerto 6003 abierto. Abrir un puerto consiste en poner una regla que indique que si llega una conexión entrante iniciada en el exterior se va a dejar pasar enviando el paquete a una cierta IP.



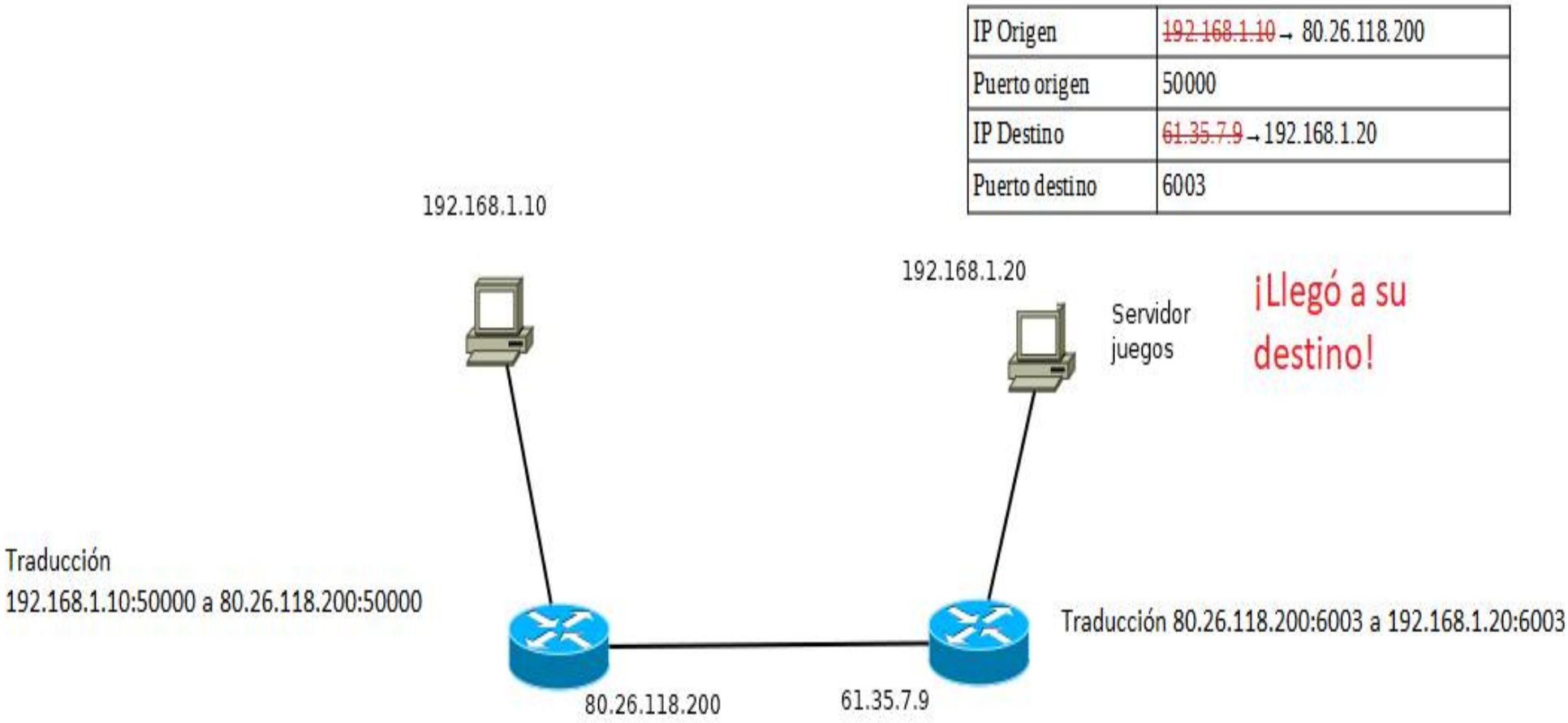
IP Origen	~~192.168.1.10~~ → 80.26.118.200
Puerto origen	50000
IP Destino	61.35.7.9
Puerto destino	6003

Paso 5: si hubiera la regla correcta, el paquete entrará pero con la IP de destino modificada.



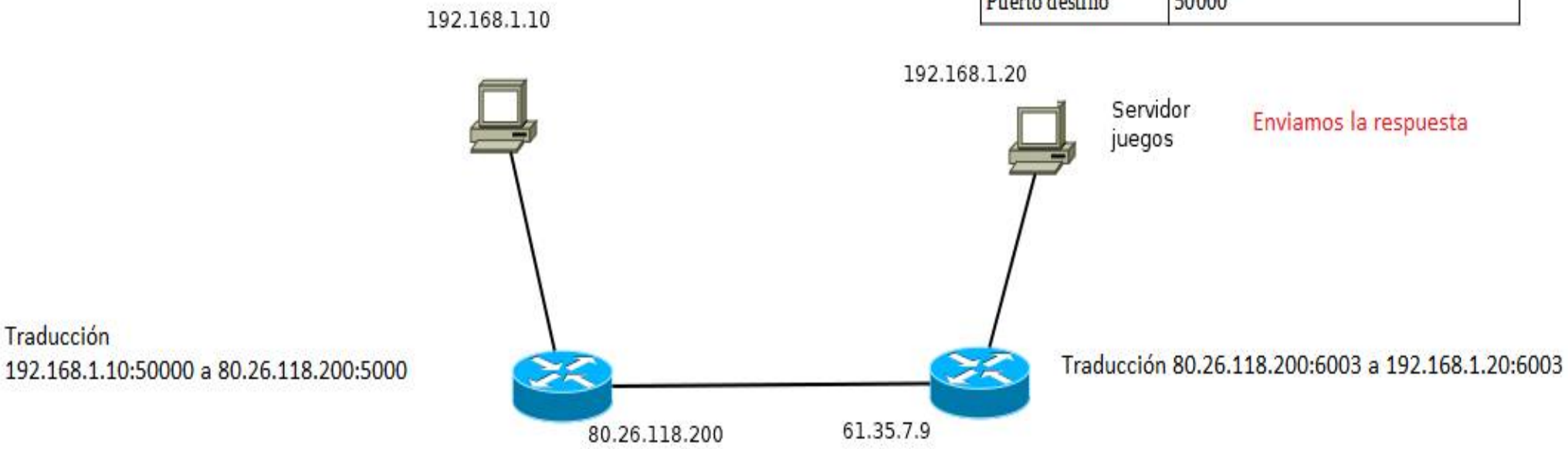
IP Origen	~~192.168.1.10~~ → 80.26.118.200
Puerto origen	50000
IP Destino	~~61.35.7.9~~ → 192.168.1.20
Puerto destino	6003

Paso 6: el paquete que intentaba iniciar la conexión llega correctamente a su destino.

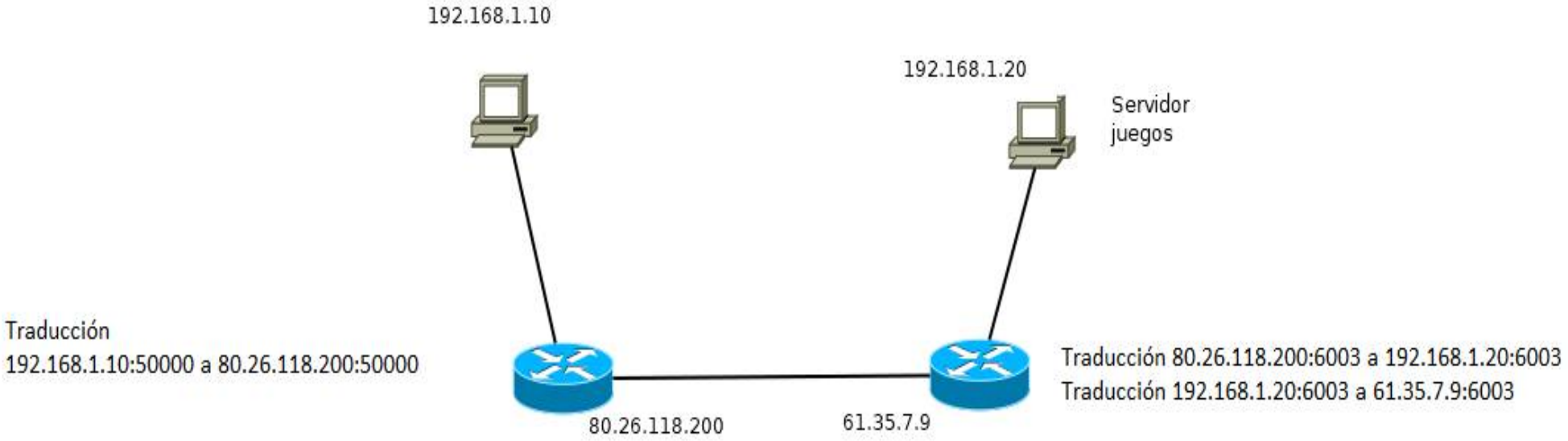


Paso 7: el servidor va a responder y genera un paquete de respuesta.

IP Origen	192.168.1.20
Puerto origen	6003
IP Destino	80.26.118.200
Puerto destino	50000

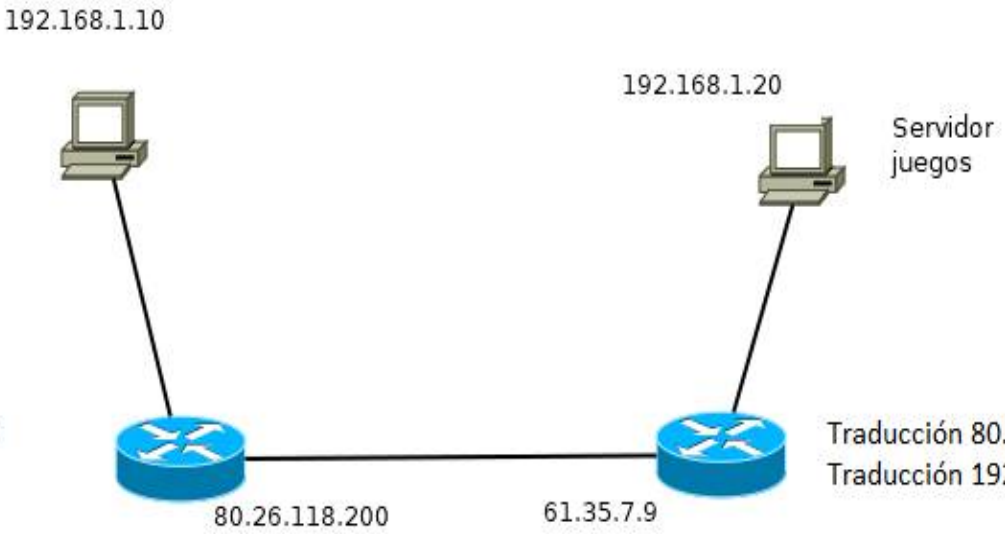


Paso 8: el paquete llega al router que vuelve a modificar la IP de origen porque no se aceptan IPs privadas en Internet. Por supuesto, el router vuelve a apuntar esa traducción.



IP Origen	~~192.168.1.20~~ → 61.35.7.9
Puerto origen	6003
IP Destino	80.26.118.200
Puerto destino	50000

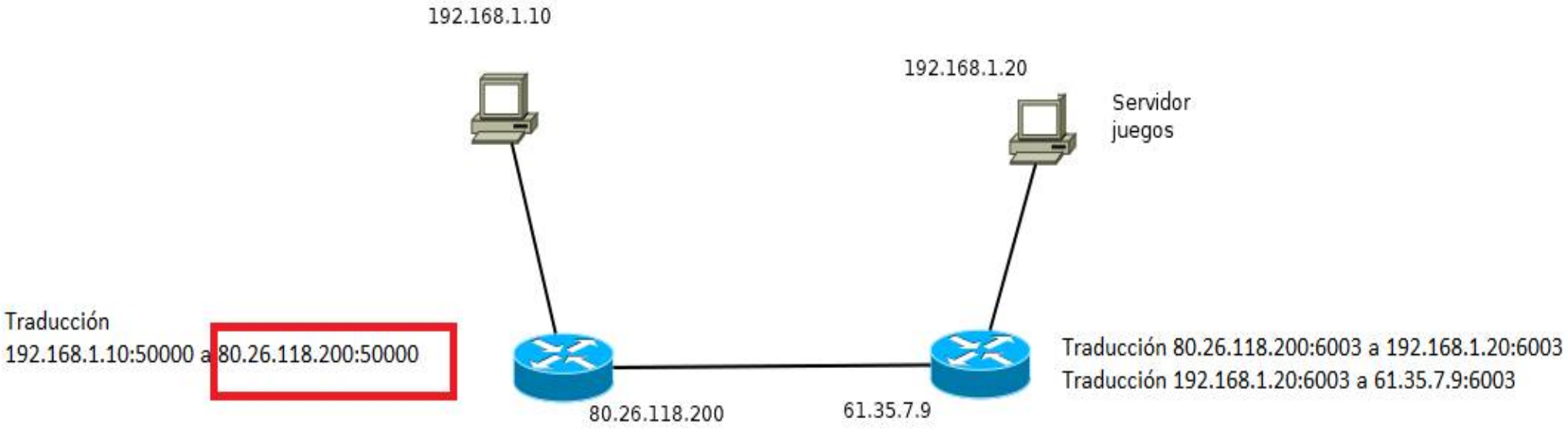
Paso 9: el paquete intenta entrar. Lo primero que podríamos pensar es que el paquete no entrará, sin embargo SÍ VA A CONSEGUIR ENTRAR



¡Un paquete intenta entrar!

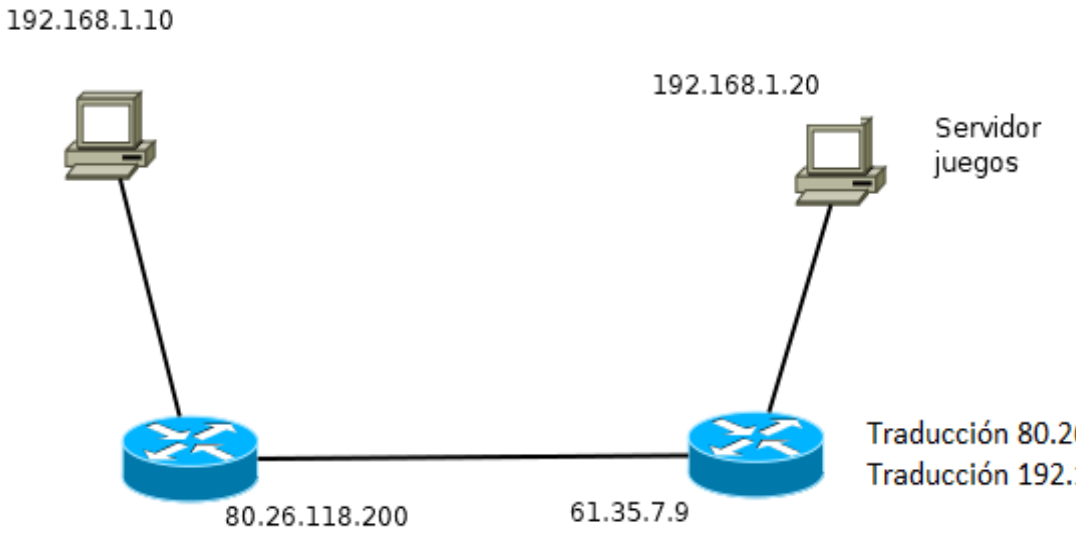
IP Origen	~~192.168.1.20~~ → 61.35.7.9
Puerto origen	6003
IP Destino	80.26.118.200
Puerto destino	50000

Paso 10: el router observa que el paquete coincide perfectamente con la información de una traducción que se hizo en el pasado. Es decir el paquete puede pasar. De nuevo, se vuelve a cambiar la IP de destino y el paquete se inyecta en la



IP Origen	~~192.168.1.20~~ → 61.35.7.9
Puerto origen	6003
IP Destino	80.26.118.200
Puerto destino	50000

Paso 10b: se modifica la IP y se envía al interior.



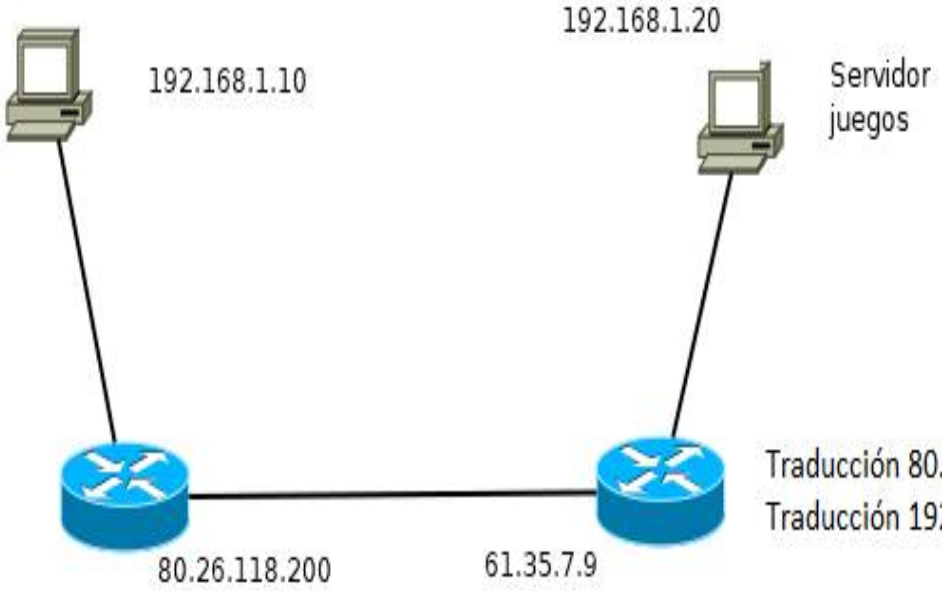
IP Origen	~~192.168.1.20~~ → 61.35.7.9
Puerto origen	6003
IP Destino	~~80.26.118.200~~ → 192.168.1.10
Puerto destino	50000

¡Se autoriza su entrada, pues es una respuesta a una conexión abierta!.
Se modifica la IP de destinto y el paquete entra hacia su destino

Paso 11: el paquete llega a su destino

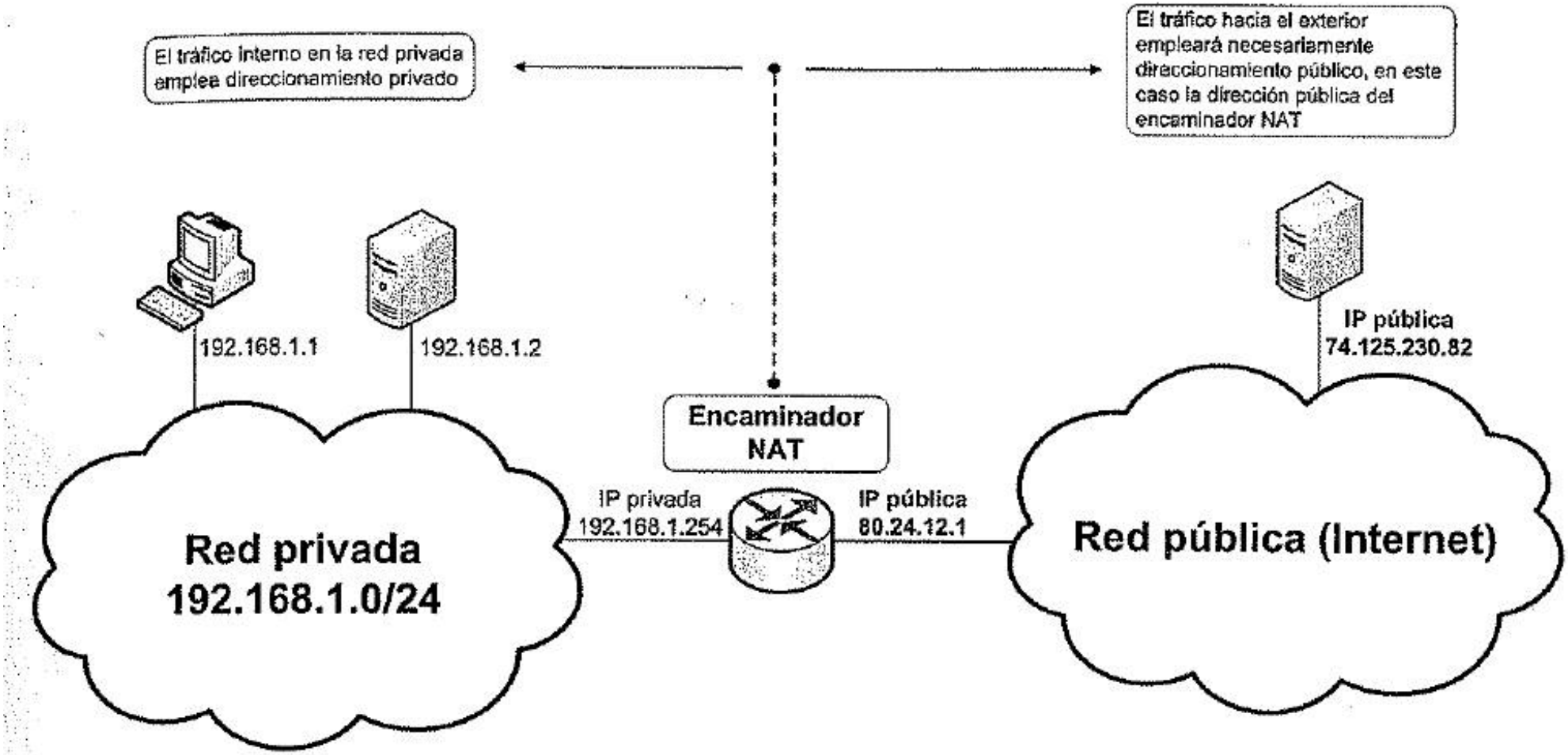
IP Origen	~~192.168.1.20~~ → 61.35.7.9
Puerto origen	6003
IP Destino	~~80.26.118.200~~ → 192.168.1.10
Puerto destino	50000

¡El paquete llega a su destino!



Traducción
192.168.1.10:50000 a 80.26.118.200:50000

Traducción 80.26.118.200:6003 a 192.168.1.20:6003
Traducción 192.168.1.20:6003 a 61.35.7.9:6003


El tráfico interno en la red privada emplea direccionamiento privado
El tráfico hacia el exterior empleará necesariamente direccionamiento público, en este caso la dirección pública del encaminador NAT
192.168.1.1
192.168.1.2
IP pública
74.125.230.82
Encaminador NAT
IP privada
192.168.1.254
IP pública
80.24.12.1
Red privada
192.168.1.0/24
Red pública (Internet)

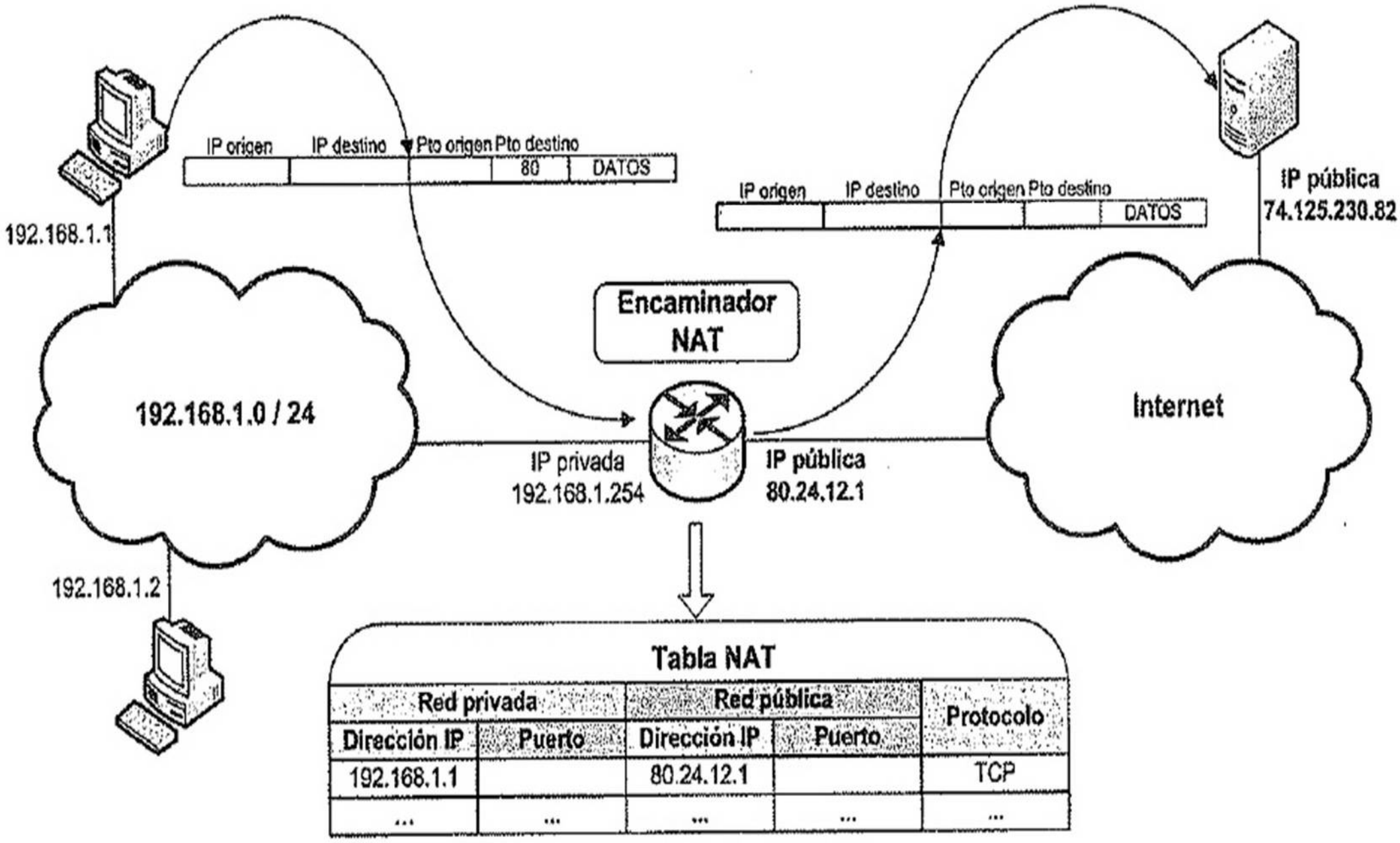


Tabla NAT

Red privada		Red pública		Protocolo
Dirección IP	Puerto	Dirección IP	Puerto	
192.168.1.1		80.24.12.1		TCP
...	...	...	...	...

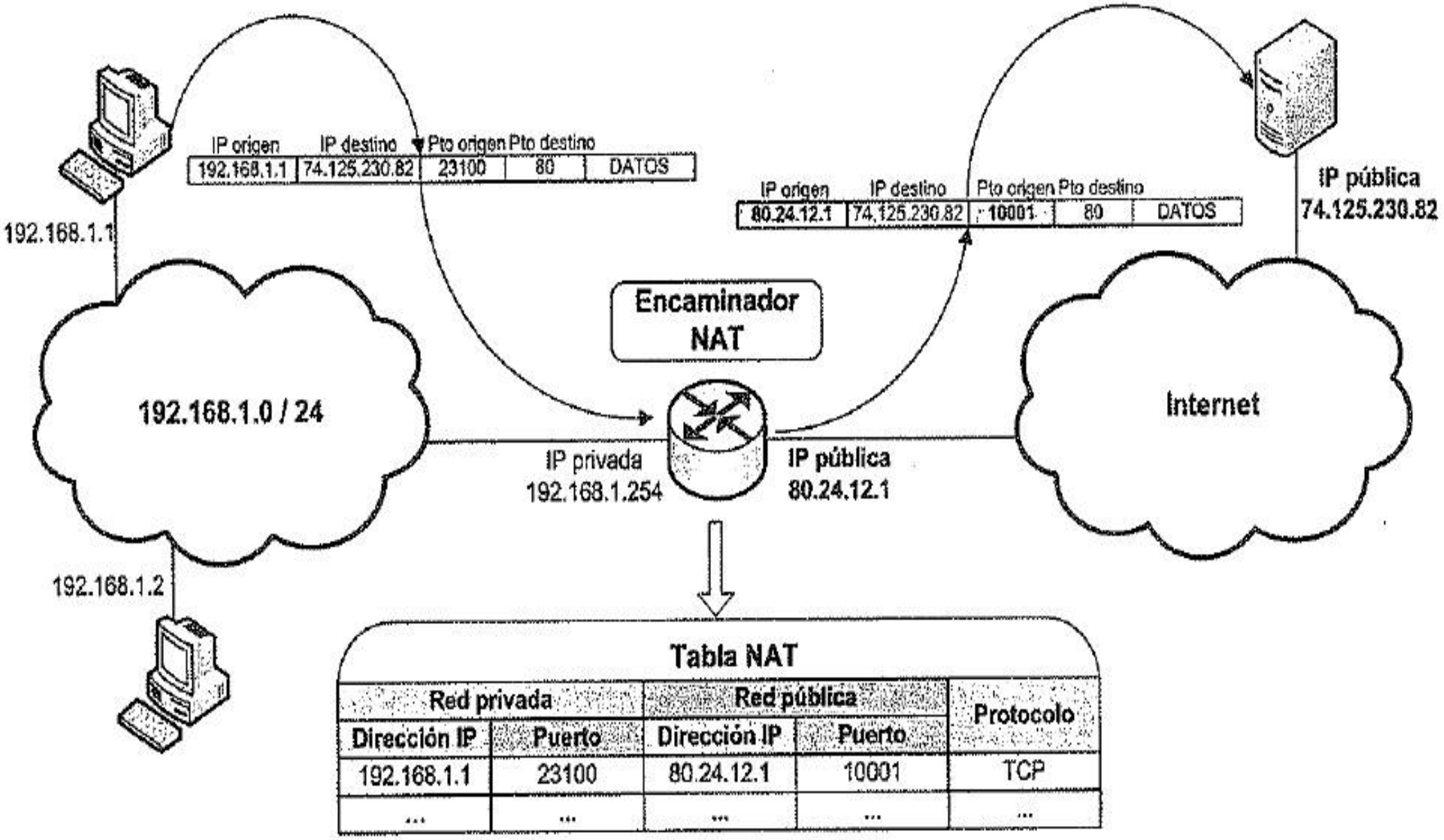


Tabla NAT

Red privada		Red pública		Protocolo
Dirección IP	Puerto	Dirección IP	Puerto	
192.168.1.1	23100	80.24.12.1	10001	TCP
...	...	...	...	...

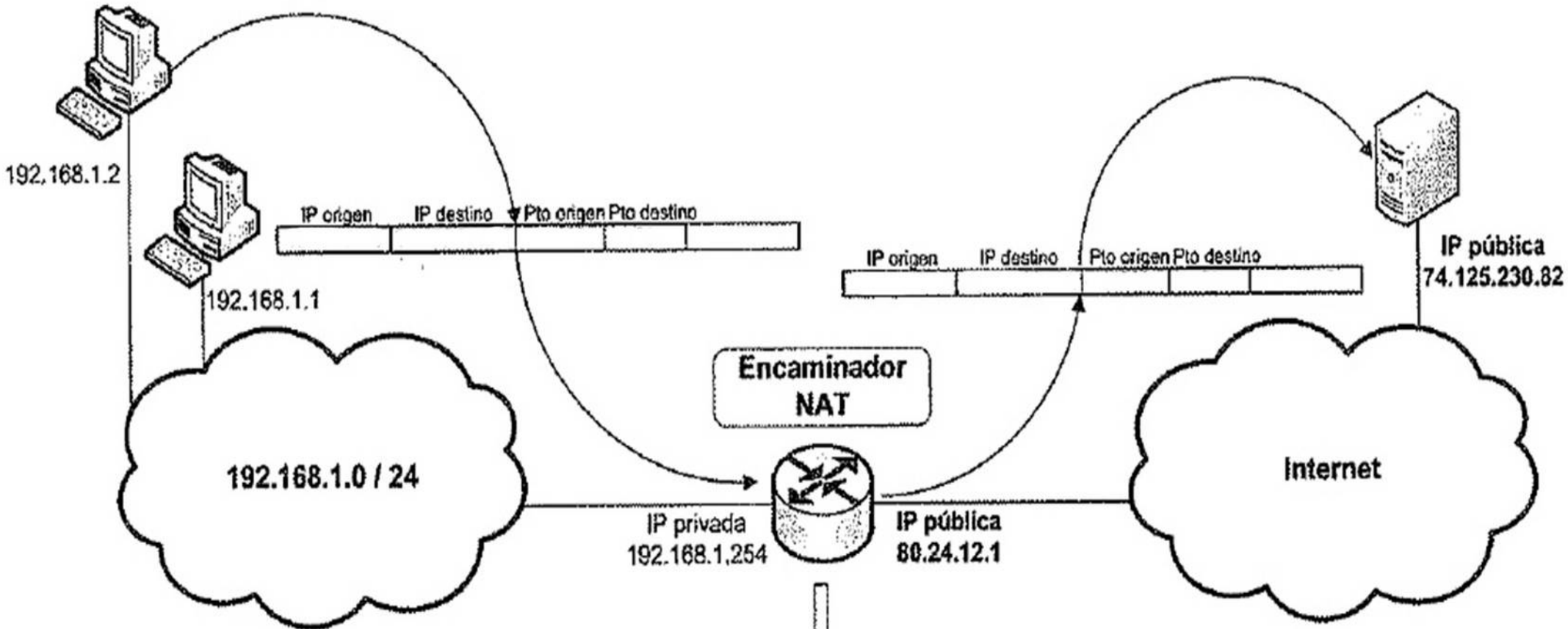


Tabla NAT

Red privada		Red pública		Protocolo
Dirección IP	Puerto	Dirección IP	Puerto	
192.168.1.1				TCP
				TCP

Entrada de la tabla NAT añadida

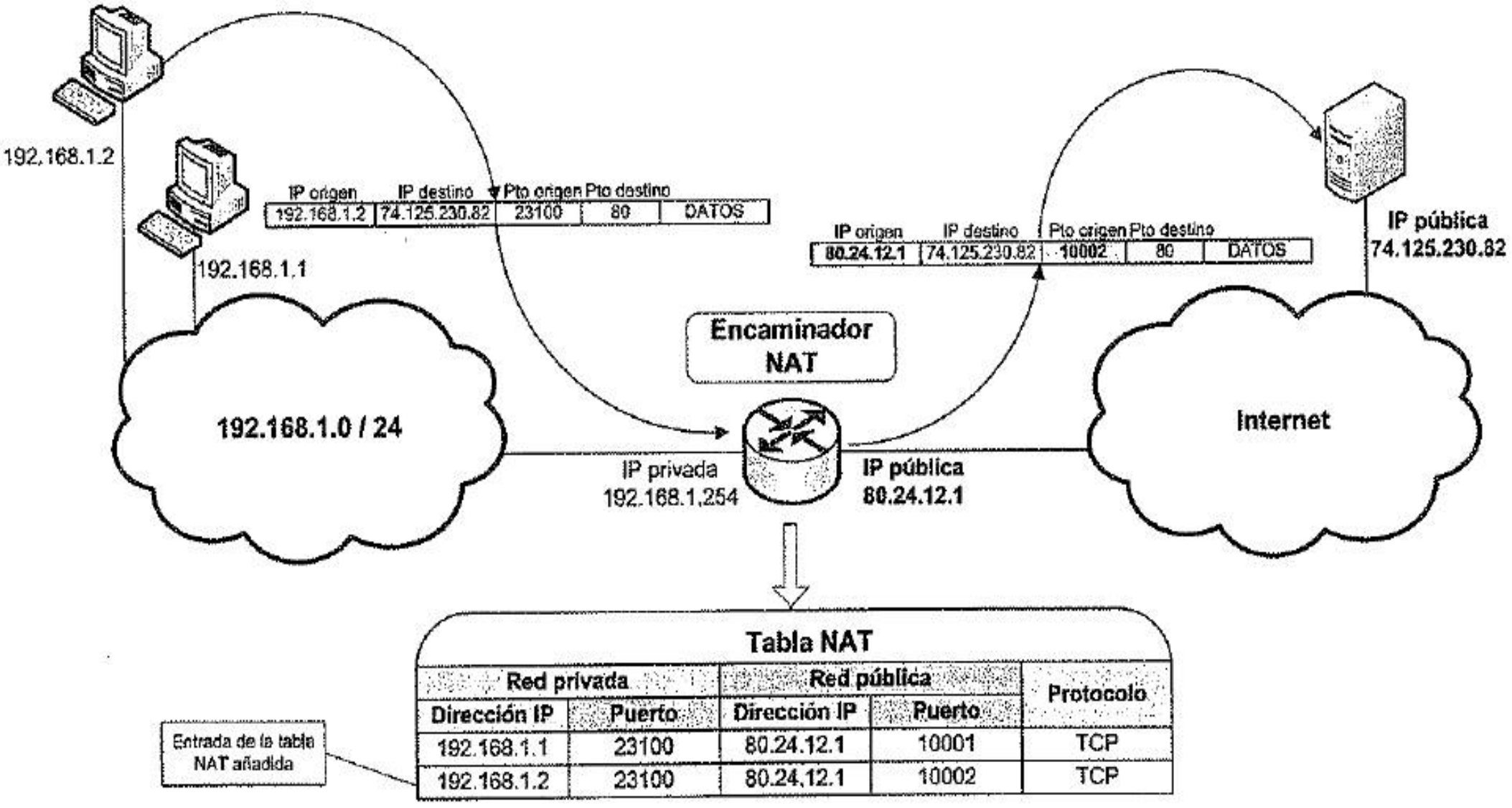
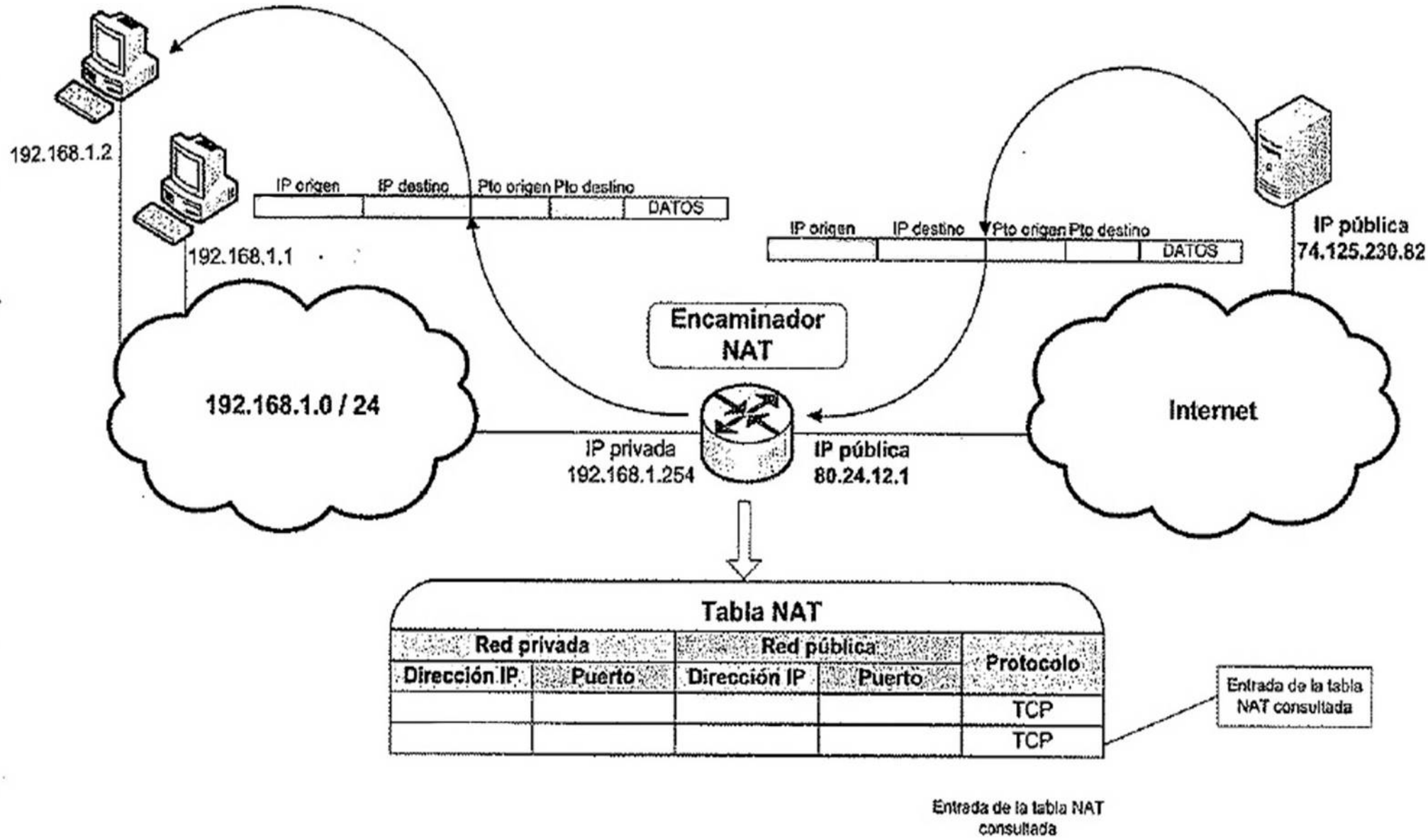


Tabla NAT

Red privada		Red pública		Protocolo
Dirección IP	Puerto	Dirección IP	Puerto	
192.168.1.1	23100	80.24.12.1	10001	TCP
192.168.1.2	23100	80.24.12.1	10002	TCP

Entrada de la tabla NAT añadida



Entrada de la tabla NAT consultada

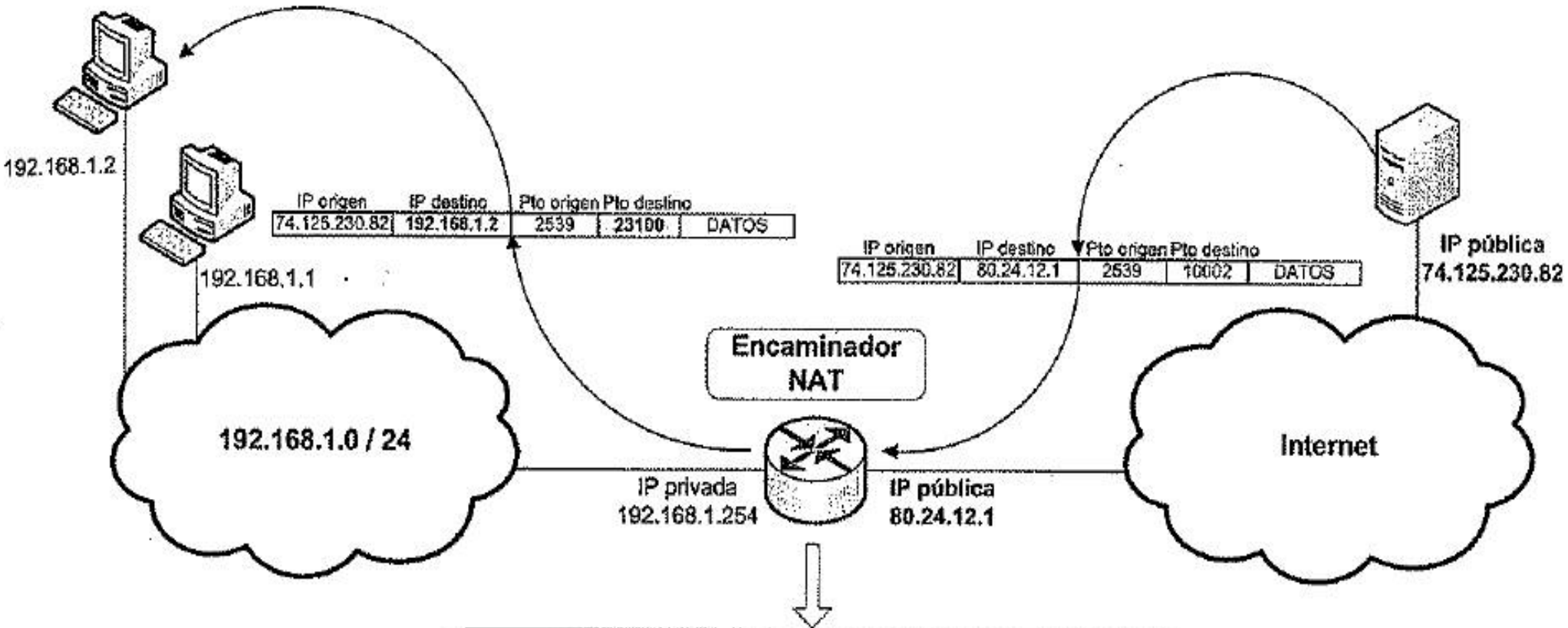


Tabla NAT

Red privada		Red pública		Protocolo
Dirección IP	Puerto	Dirección IP	Puerto	
192.168.1.1	23100	80.24.12.1	10001	TCP
192.168.1.2	23100	80.24.12.1	10002	TCP

Entrada de la tabla NAT consultada

Entrada de la tabla NAT consultada

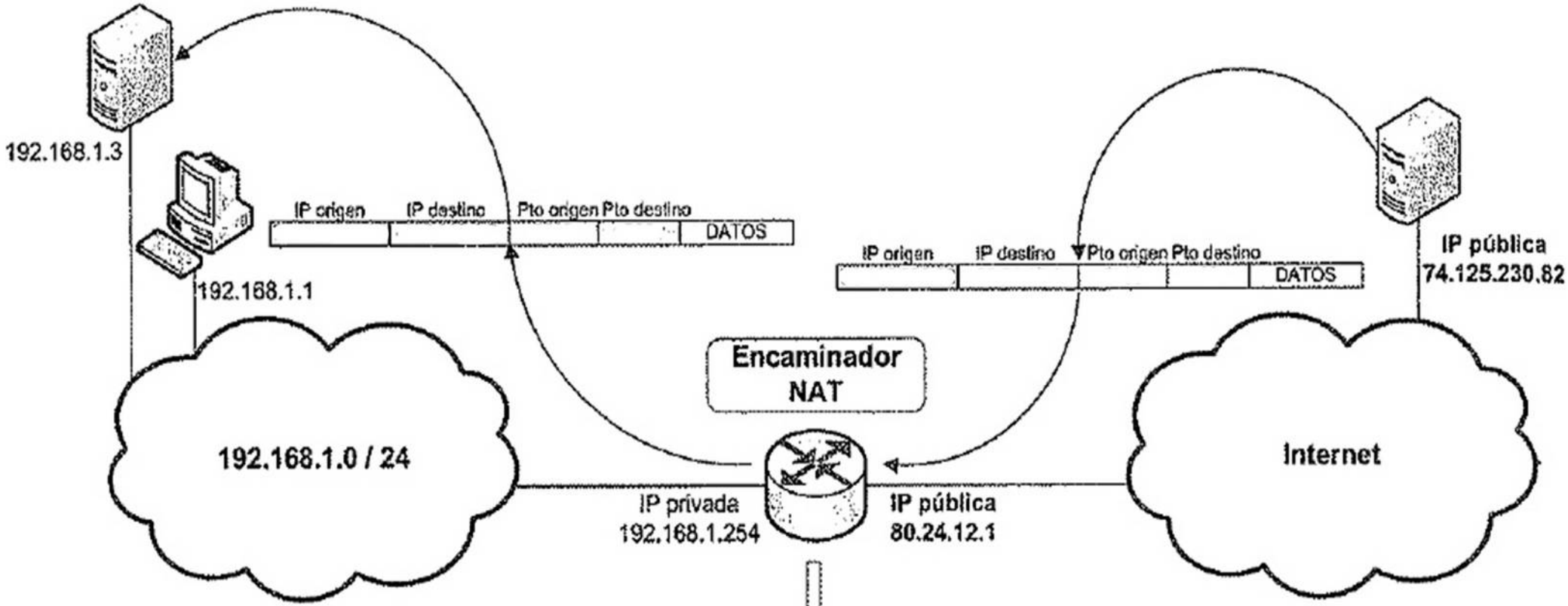


Tabla NAT

Red privada		Red pública		Protocolo
Dirección IP	Puerto	Dirección IP	Puerto	
192.168.1.1		80.24.12.1		TCP
192.168.1.2		80.24.12.1		TCP
192.168.1.3		80.24.12.1	80	TCP

Entrada de la tabla NAT añadida manualmente
Redirige la conexión al puerto 800 del servidor interno

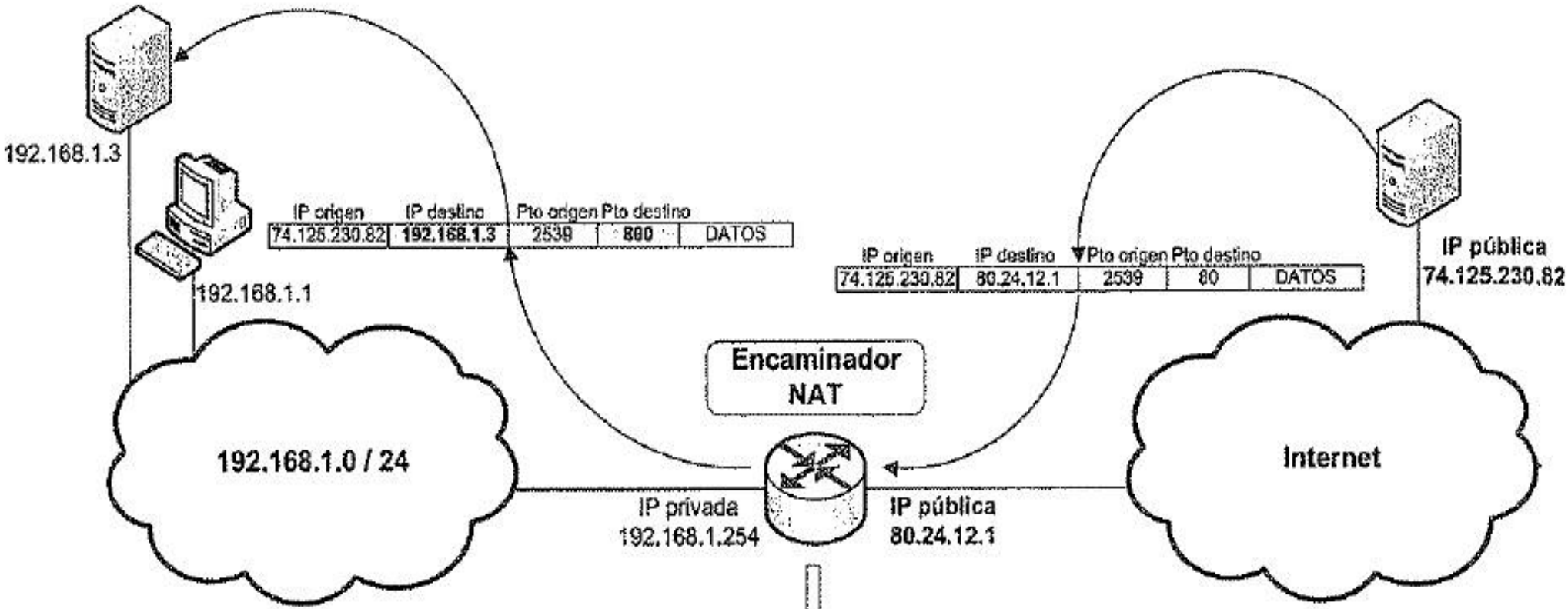


Tabla NAT

Red privada		Red pública		Protocolo
Dirección IP	Puerto	Dirección IP	Puerto	
192.168.1.1	23100	80.24.12.1	10001	TCP
192.168.1.2	23100	80.24.12.1	10002	TCP
192.168.1.3	800	80.24.12.1	80	TCP

Entrada de la tabla NAT añadida manualmente
Redirige la conexión al puerto 800 del servidor interno