



NAT (Network Address Translation)

A. Barbieri



Problemas con IPv4

- IPv4 tiene el espacio de direcciones “casi” agotado.
- Soluciones temporales:
 - CIDR: Tablas de ruteo.
 - DHCP: direcciones escasas, facilidad de administración.
 - NAT: direcciones escasas.
- Solución definitiva:
 - IPv6

NAT (Network Address Translation)

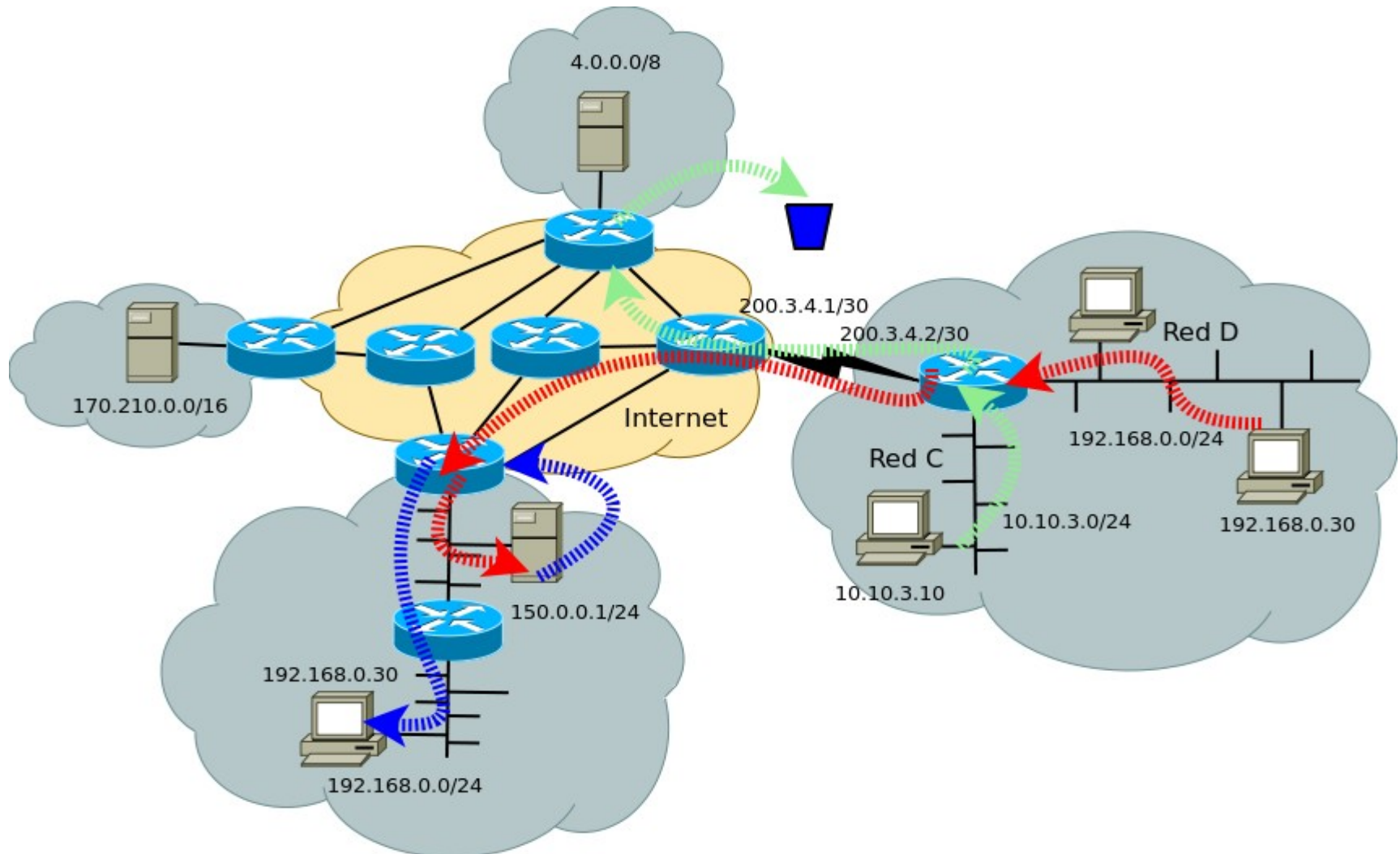
- Traslación de direcciones de un espacio privado (**no** “enrutable” en Internet) a un espacio público.
- Direcciones Privadas: RFC-1918:
 - 1 Clase A: 10.0.0.0/8
 - 16 Clases B: 172.16.0.0/12.
 - 256 Clases C: 192.168.0.0/16.
- Proceso definido en **RFC-3022**, hace obsoleta a **RFC-1631**.



Problemas con IP Privadas

- No son únicas, por lo tanto:
 - Las rutas pueden ser confundidas.
 - Habitualmente son filtradas por routers de borde.
 - Algunos protocolos no funcionan adecuadamente, FTP, VoIP, etc.

Problemas con IP Privadas



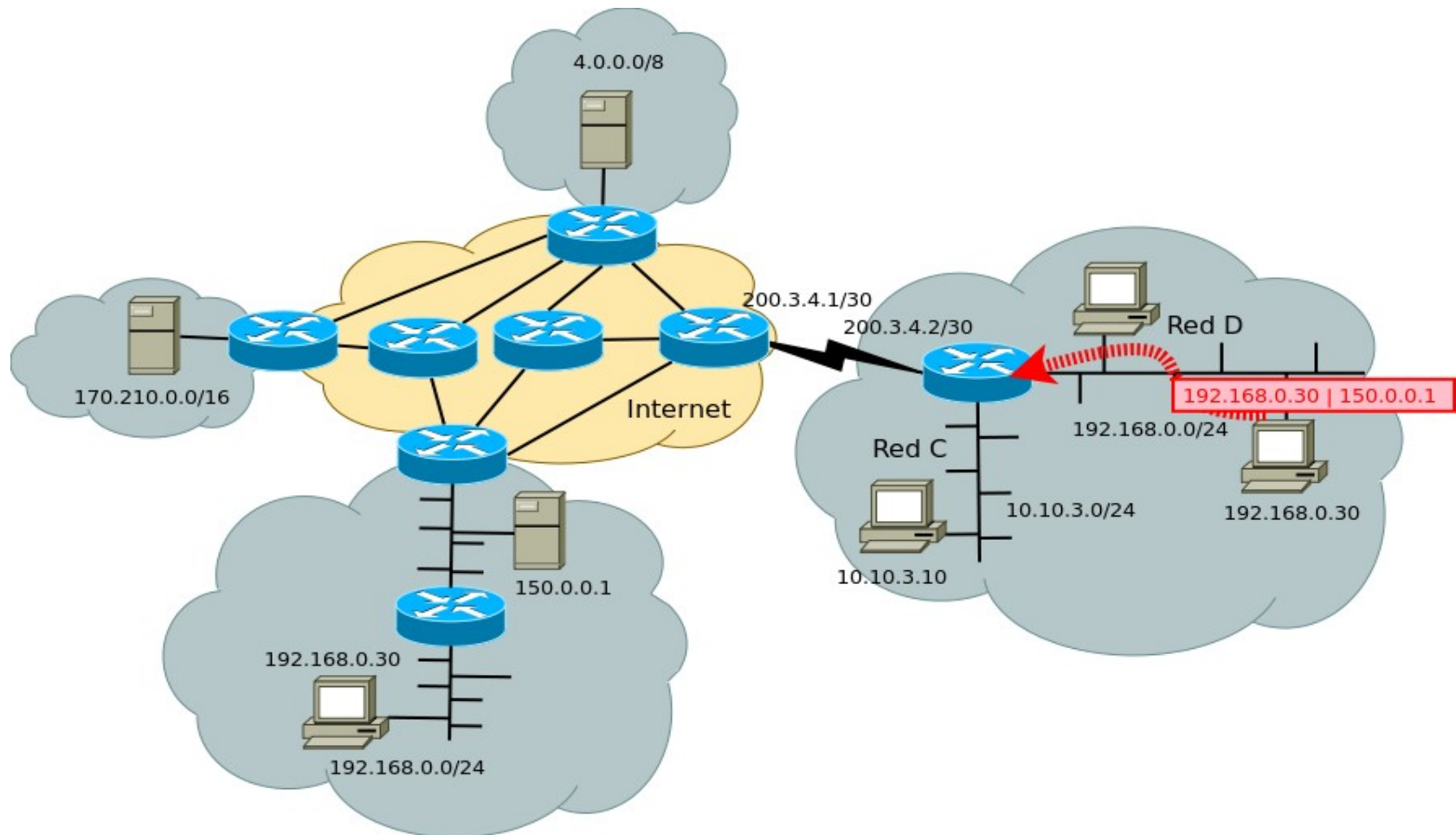
Procesos de Traslación

- Se realizan sobre redes stubs (solo una salida).
- Se deben mantener tablas de traslaciones.
- Varias formas de realizarlo:
- **NAT** (Network Address Translation):
 - Estático.
 - Dinámico.
- **NAPT** (Network Address Port Translation):
 - Dinámico sobre pool.
 - Dinámico sobre dir. overload/masquerade.
- Modificación de direcciones, ports, checksums.

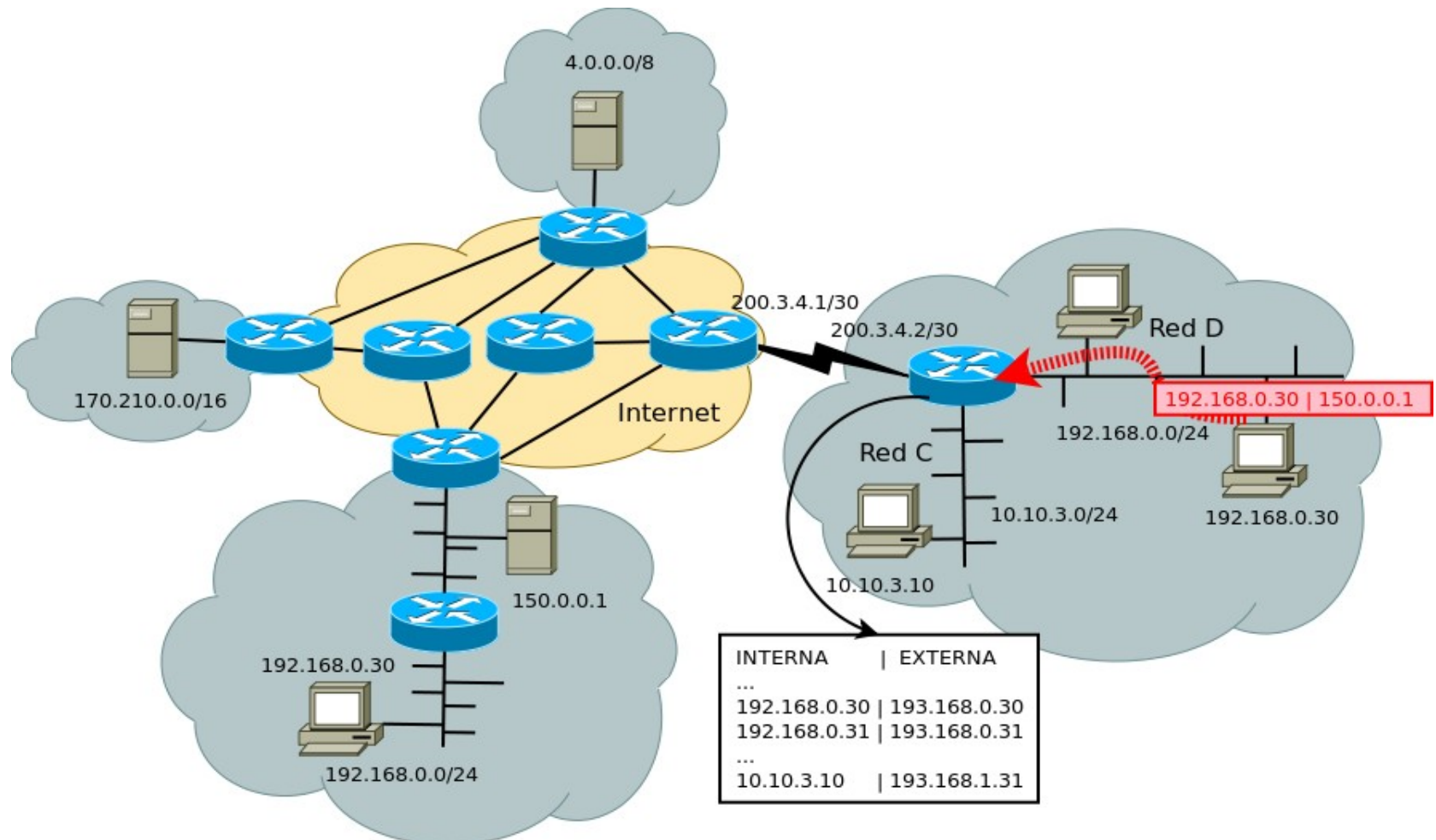
NAT (NAT básico)

- Una forma de realizarlo es: “**one-to-one**” (uno a uno), **NAT básico**:
- Se mapea una dirección IPv4 privada a una dirección IPv4 pública.
- Si se hace de forma **estática** requiere tantas direcciones públicas como privadas.
- Permite acceso en ambas direcciones.
- Si se hace de forma **dinámica** no es necesario, pero sí se requiere un timer por cada entrada. Limita acceso simultaneo de acuerdo al pool pub.

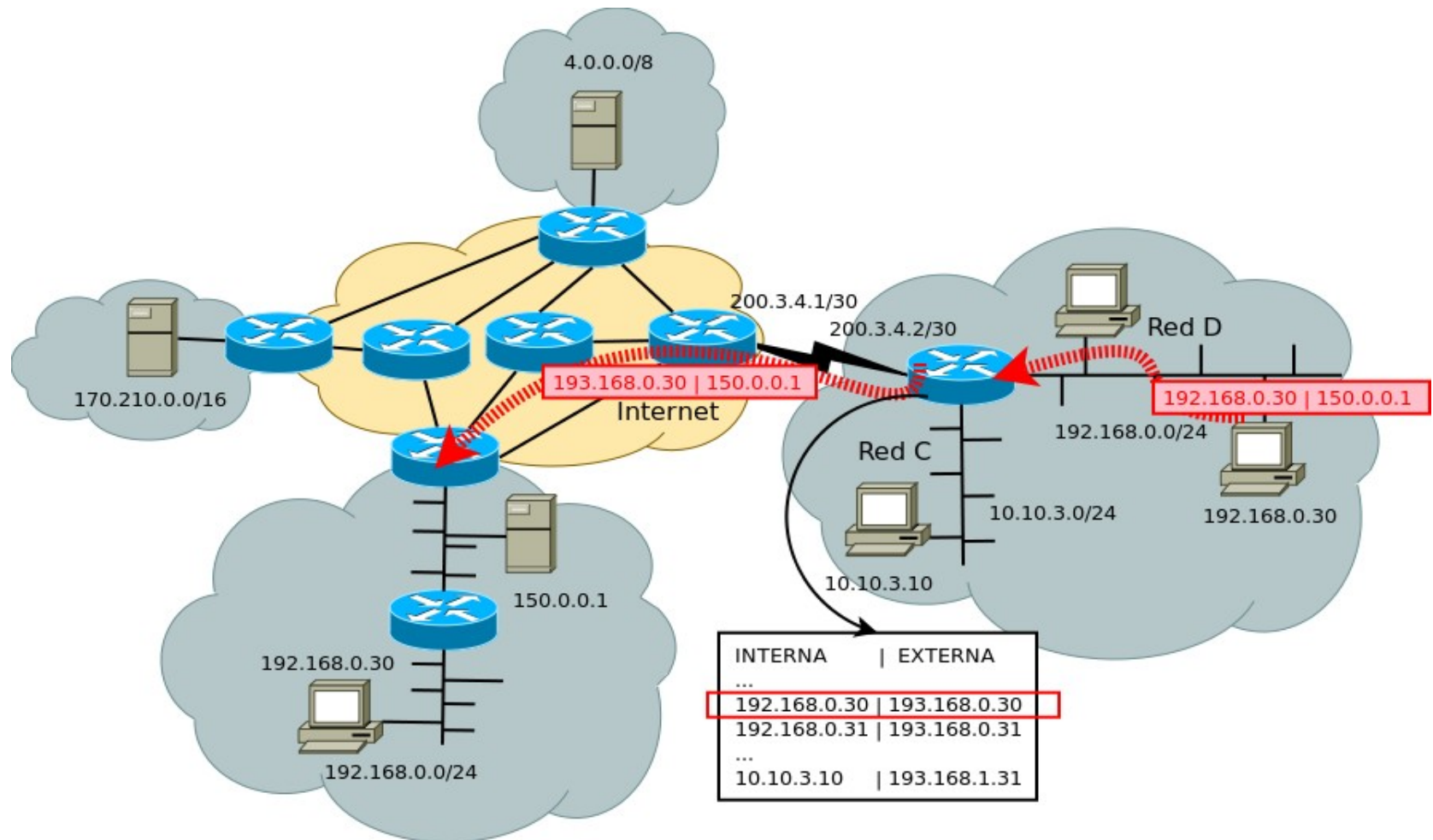
Ejemplo NAT estático (1)



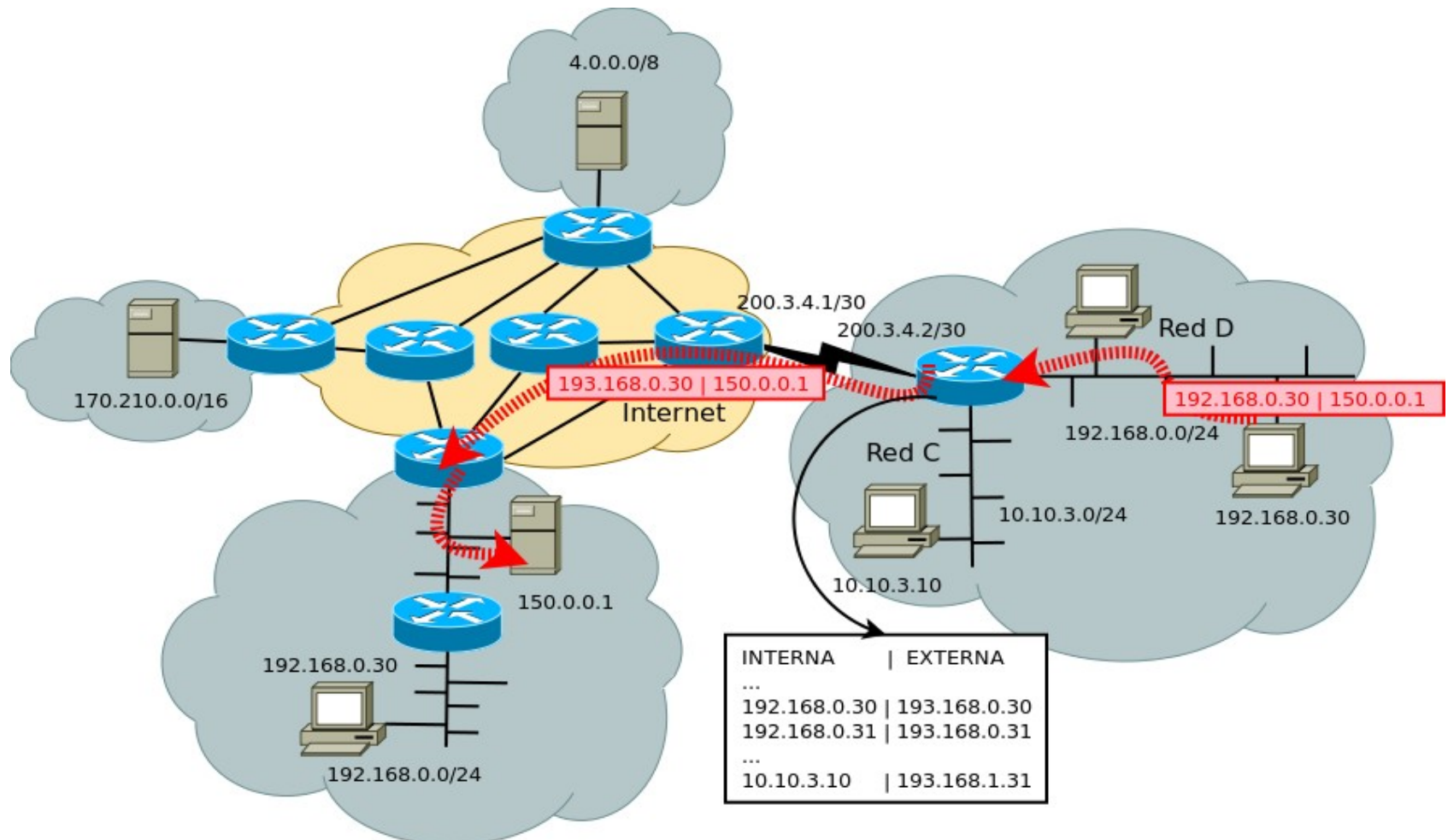
Ejemplo NAT estático (2)



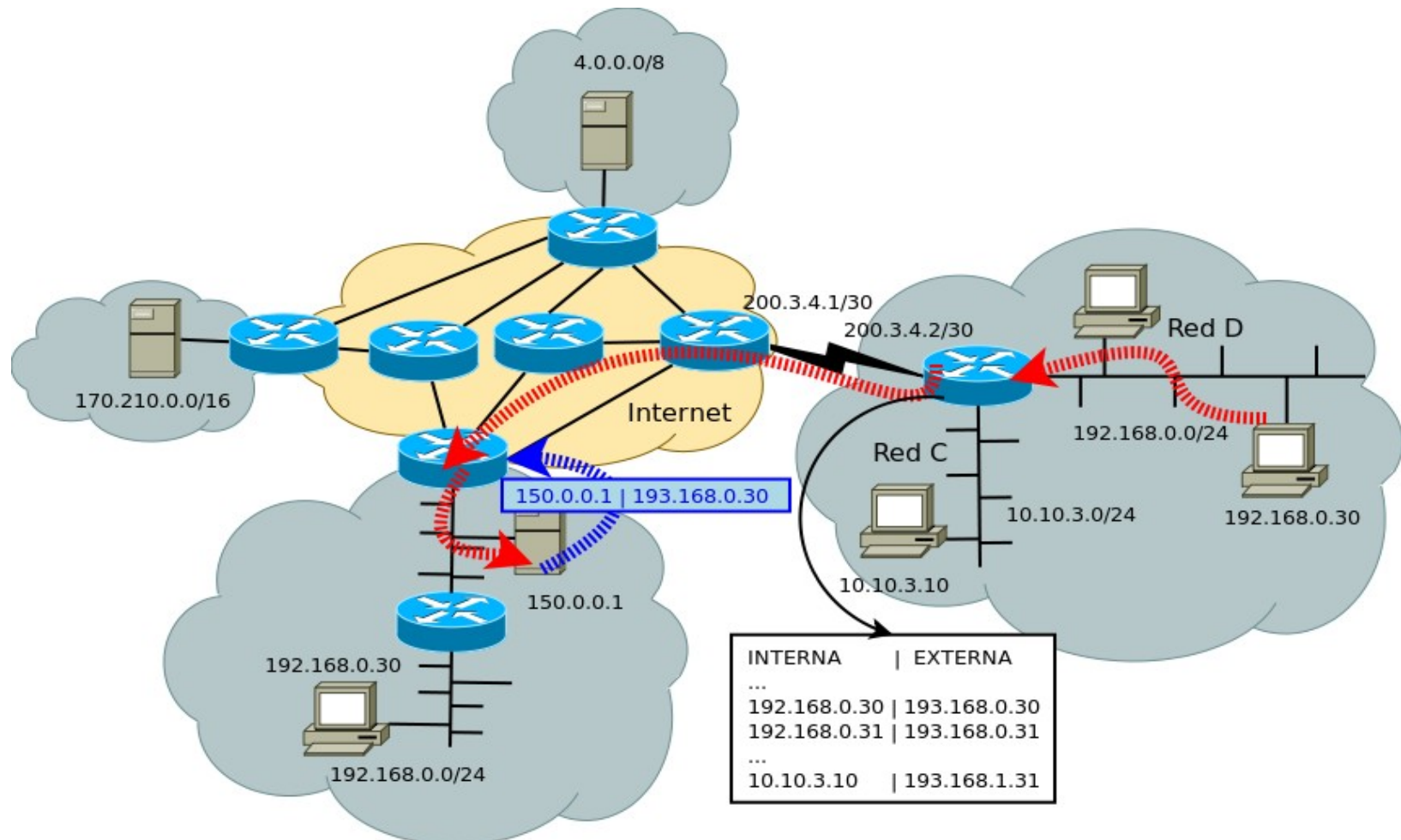
Ejemplo NAT estático (3)



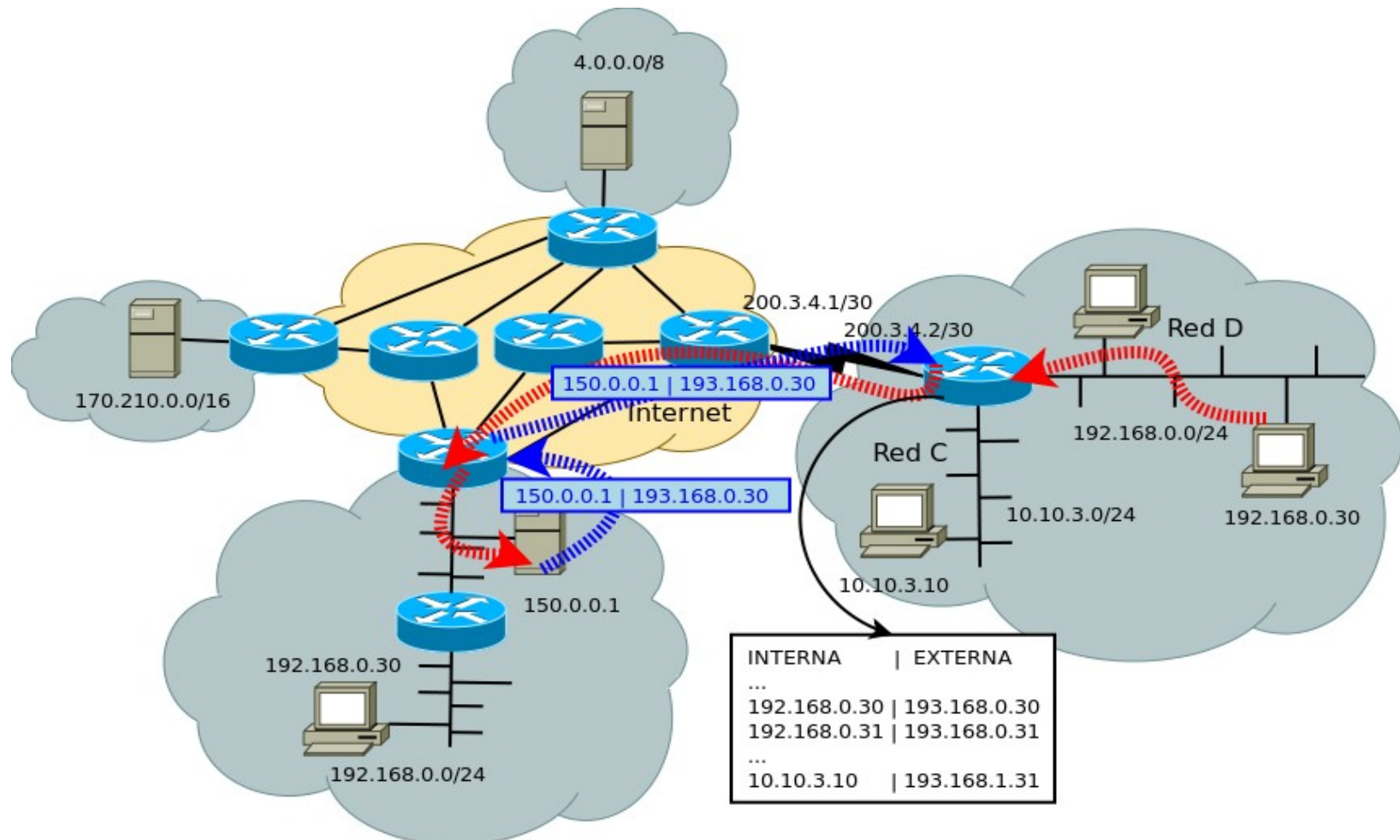
Ejemplo NAT estático (4)



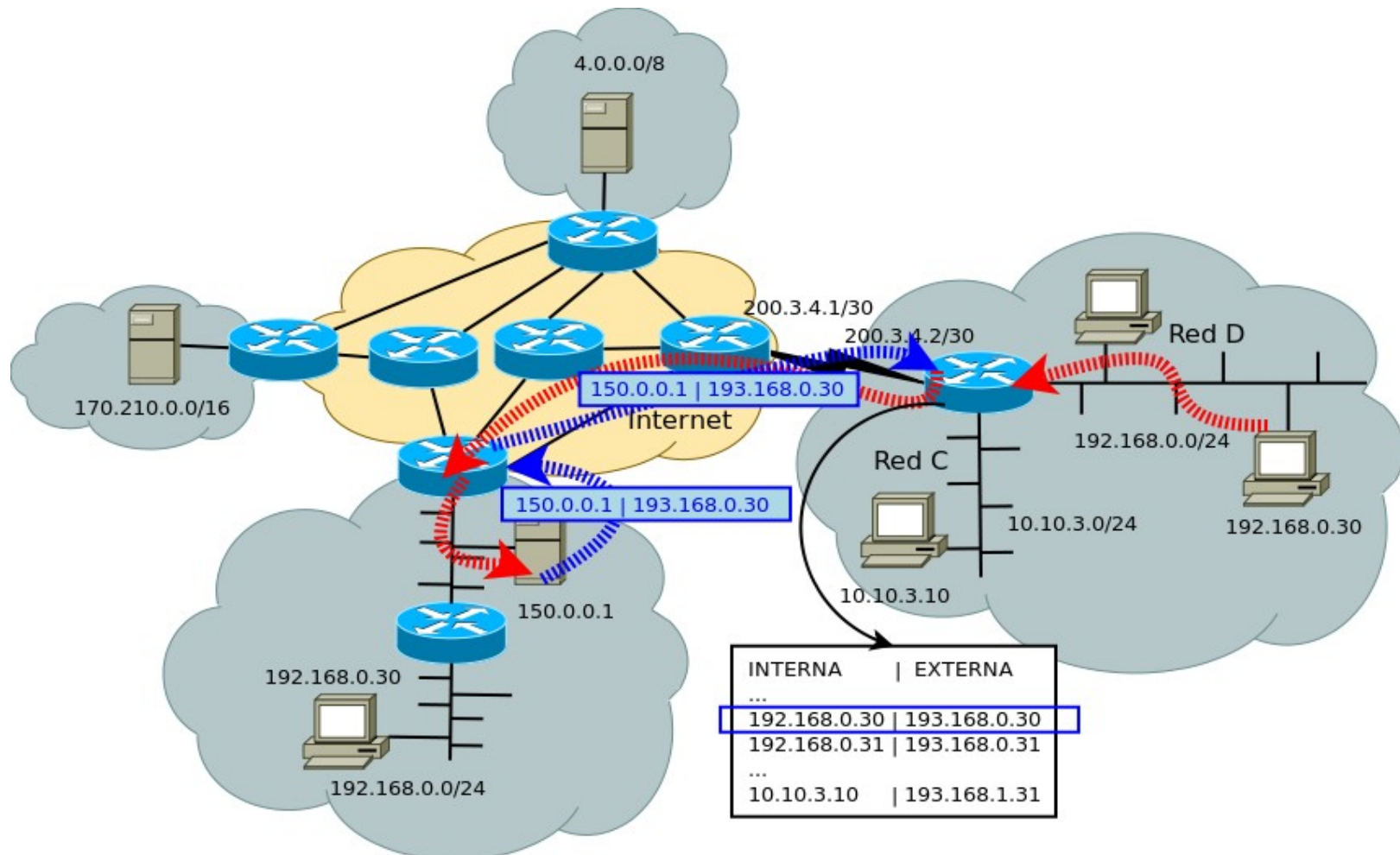
Ejemplo NAT estático (5)



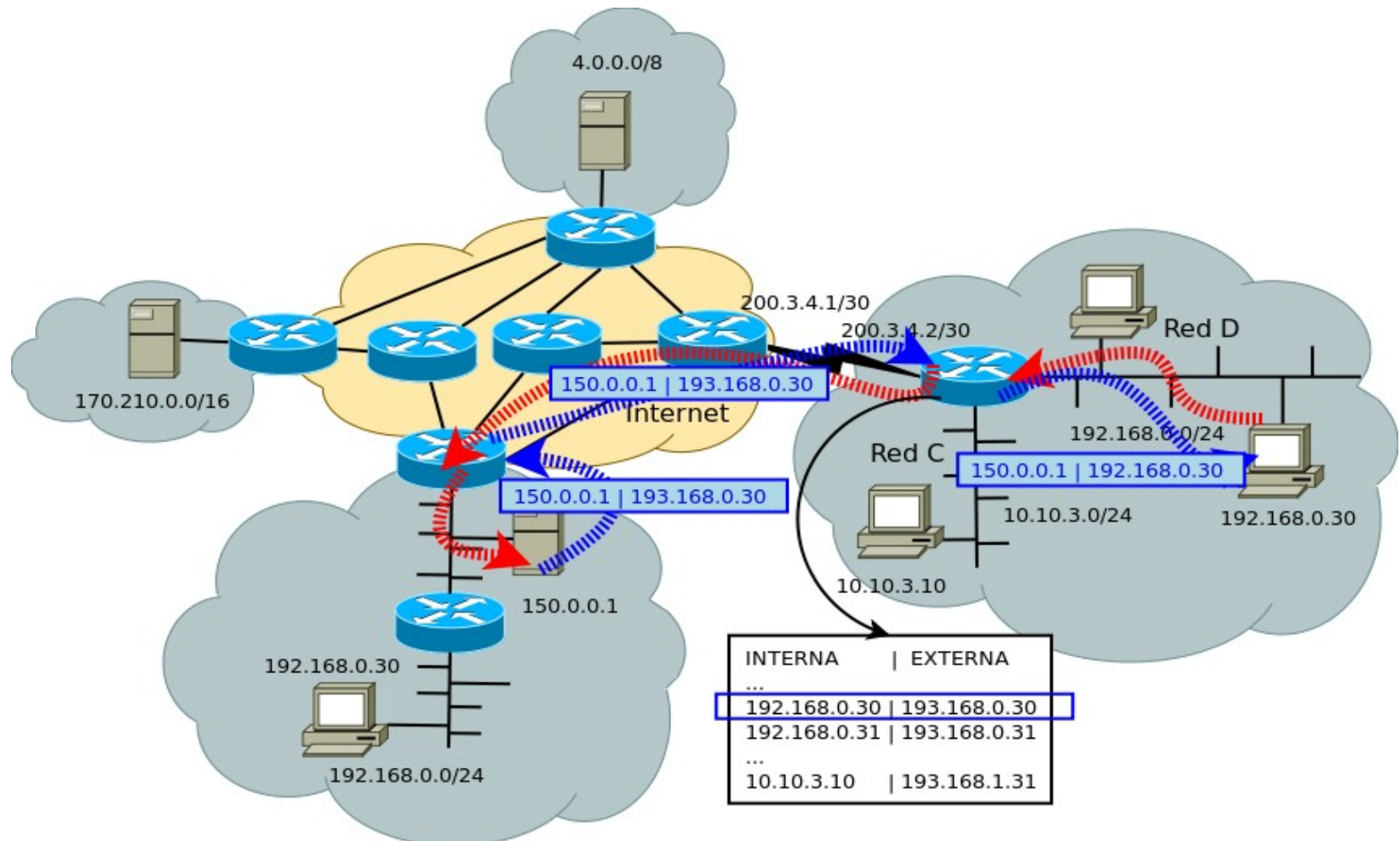
Ejemplo NAT estático (6)



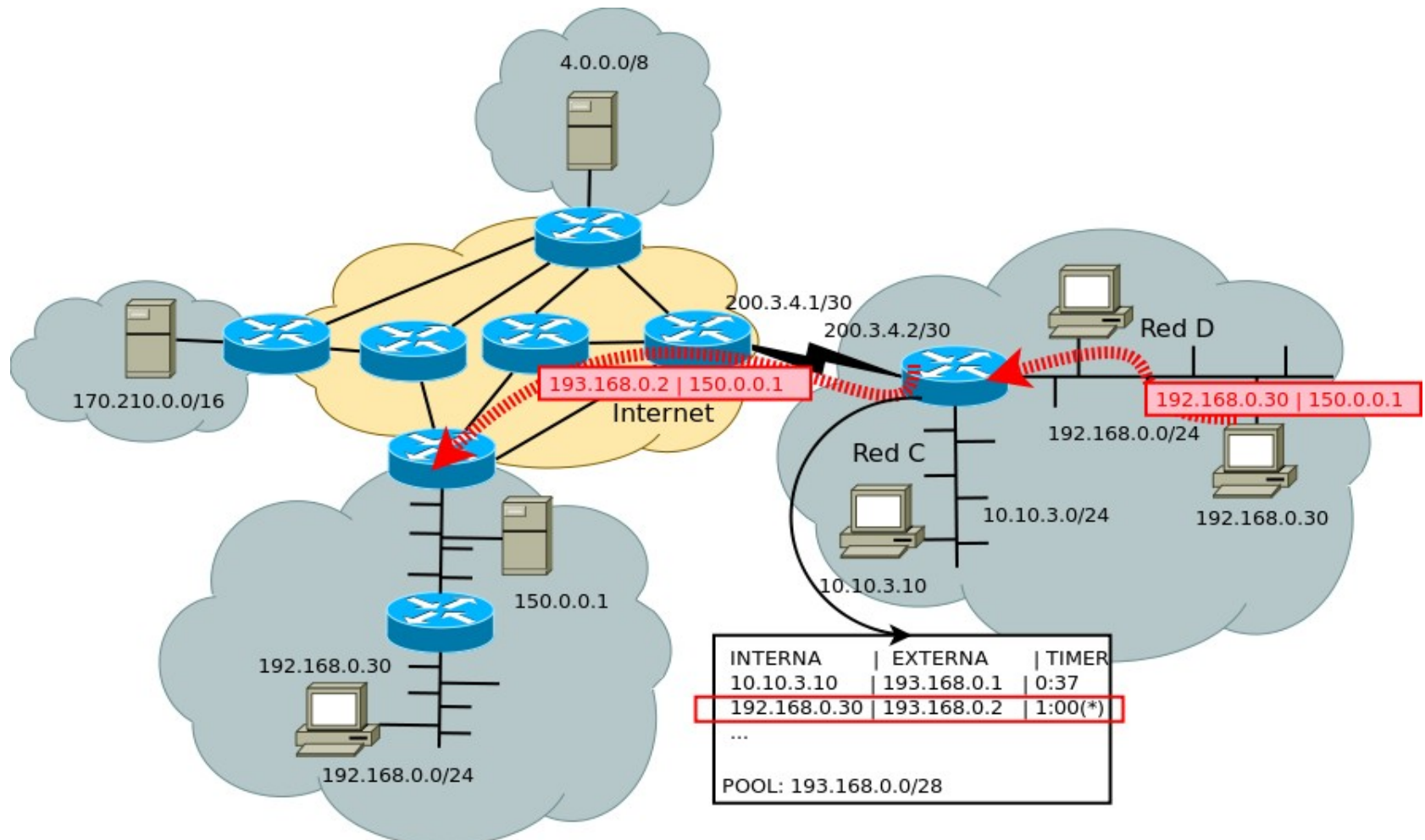
Ejemplo NAT estático (7)



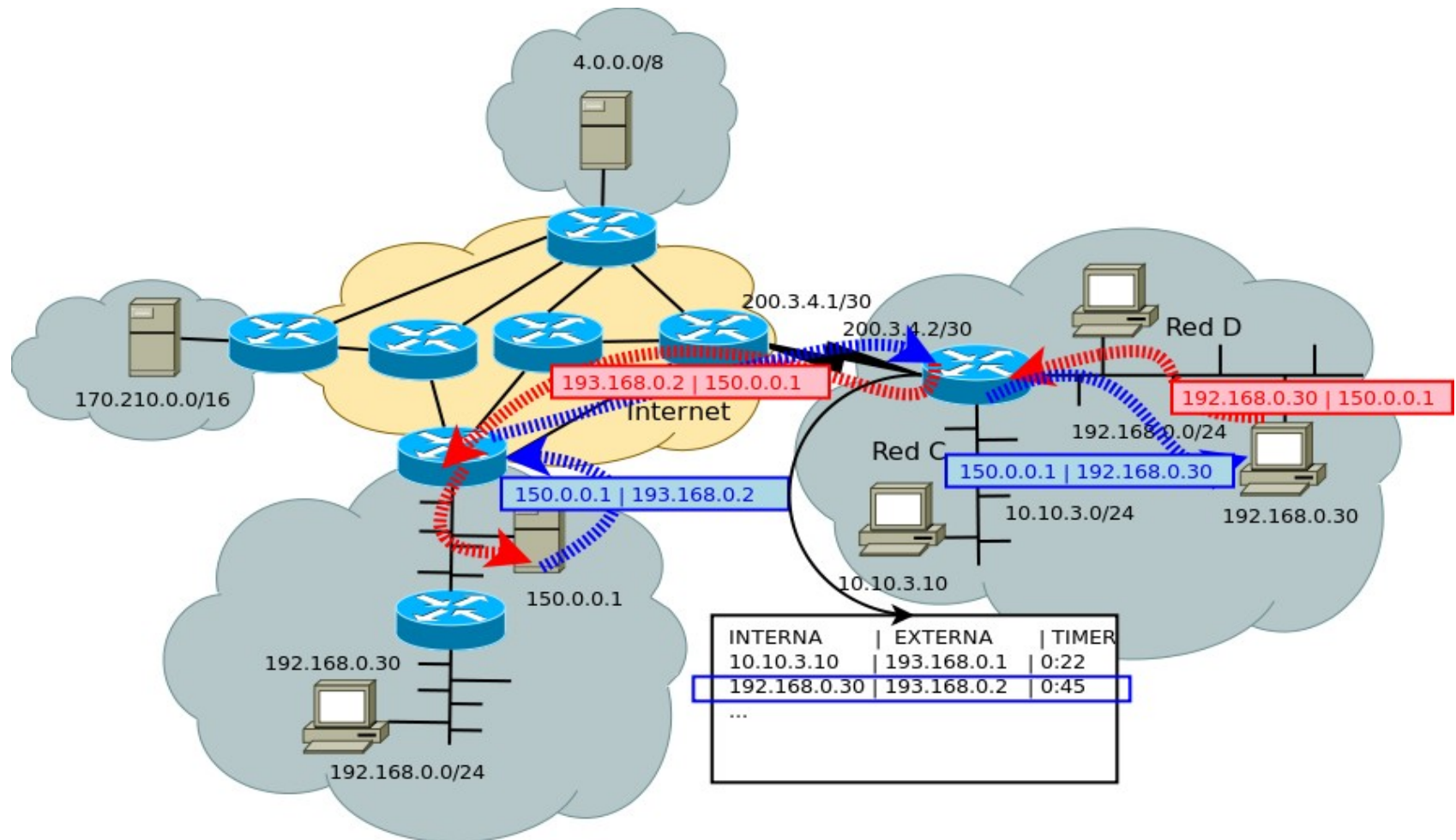
Ejemplo NAT estático (8)



Ejemplo NAT dinámico (1)



Ejemplo NAT dinámico (2)



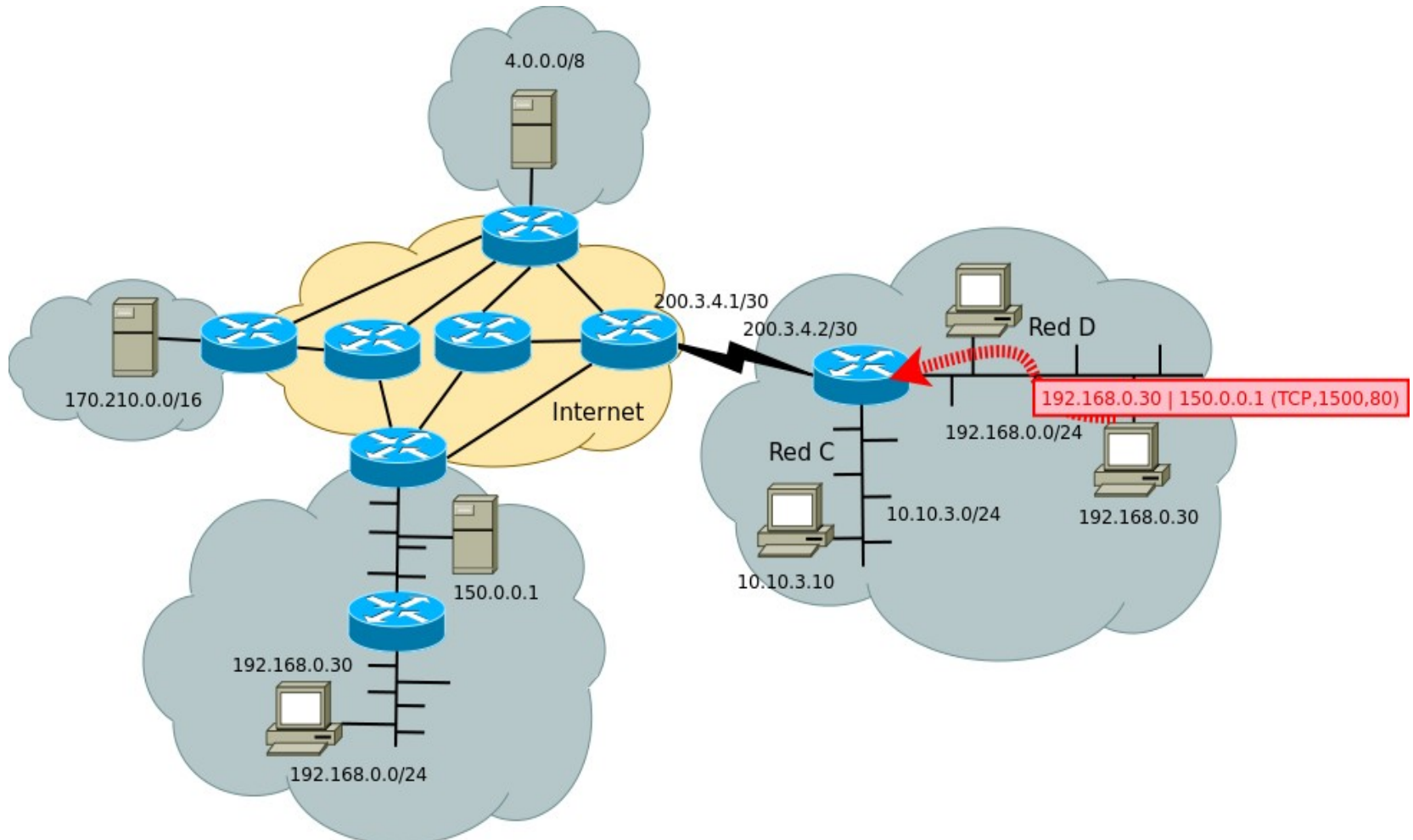
NAPT (Network Address Port Translation)

- NAT no es implementable cuando se tiene un **pool chico** de direcciones o no se posee direcciones publicas asignadas.
- En ese caso se debe trabajar con campos de la capa de transporte o del payload.
- **NAPT** es conocido como **PAT (Port Address Translation): “one-to-many”**.
- Se utilizan los **puertos** de los protocolos u otros valores como ICMP **Identifier** para resolver el mapeo.
- Se pueden usar timers y sesión del protocolo.

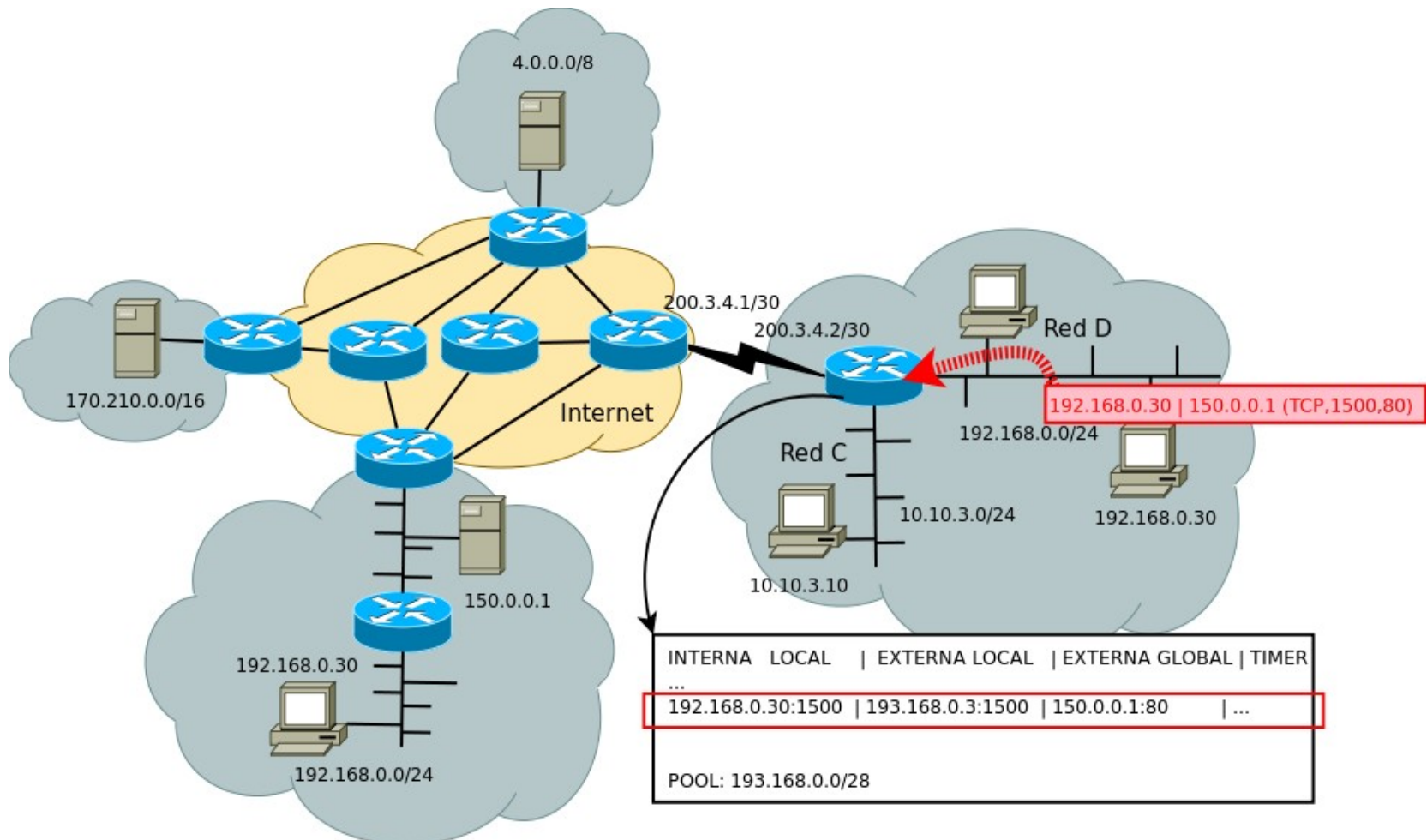
NAPT (Network Address Port Translation)

- En la tabla de traslaciones se mantienen el **protocolo y los puertos origen y destino.**
- Se intenta conservar el puerto origen, pero si esta “ocupado” se debe reemplazar por otro.
- El dispositivo se debe “violar” los límites impuestos por la división en capas.
- Dos alternativas:
 - Utilizando un pool y haciendo PAT sobre este.
 - Utilizando la dir. IP externa y haciendo **overloading/masquerading** sobre esta.

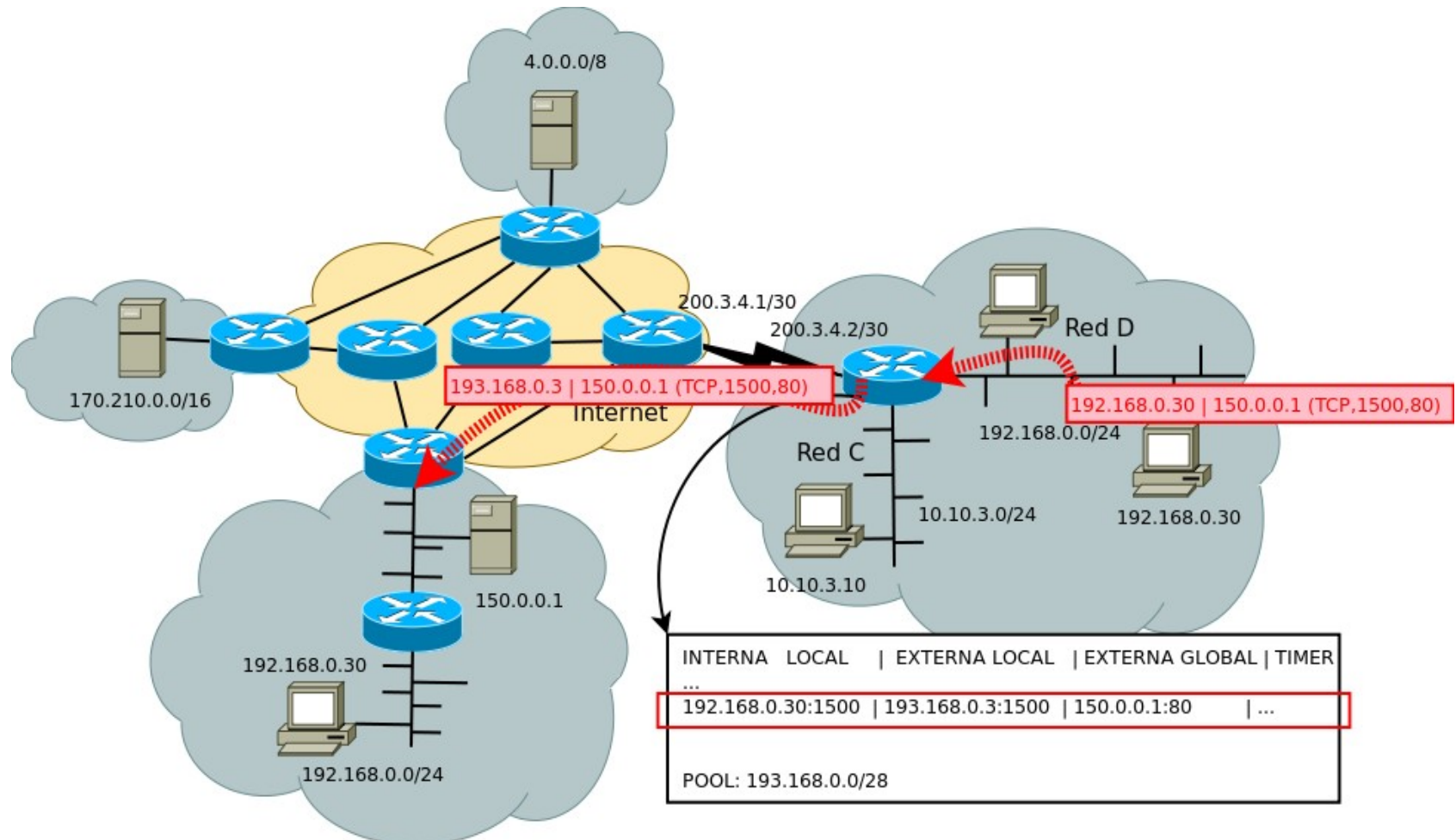
Ejemplo de NAT (Pool) (1)



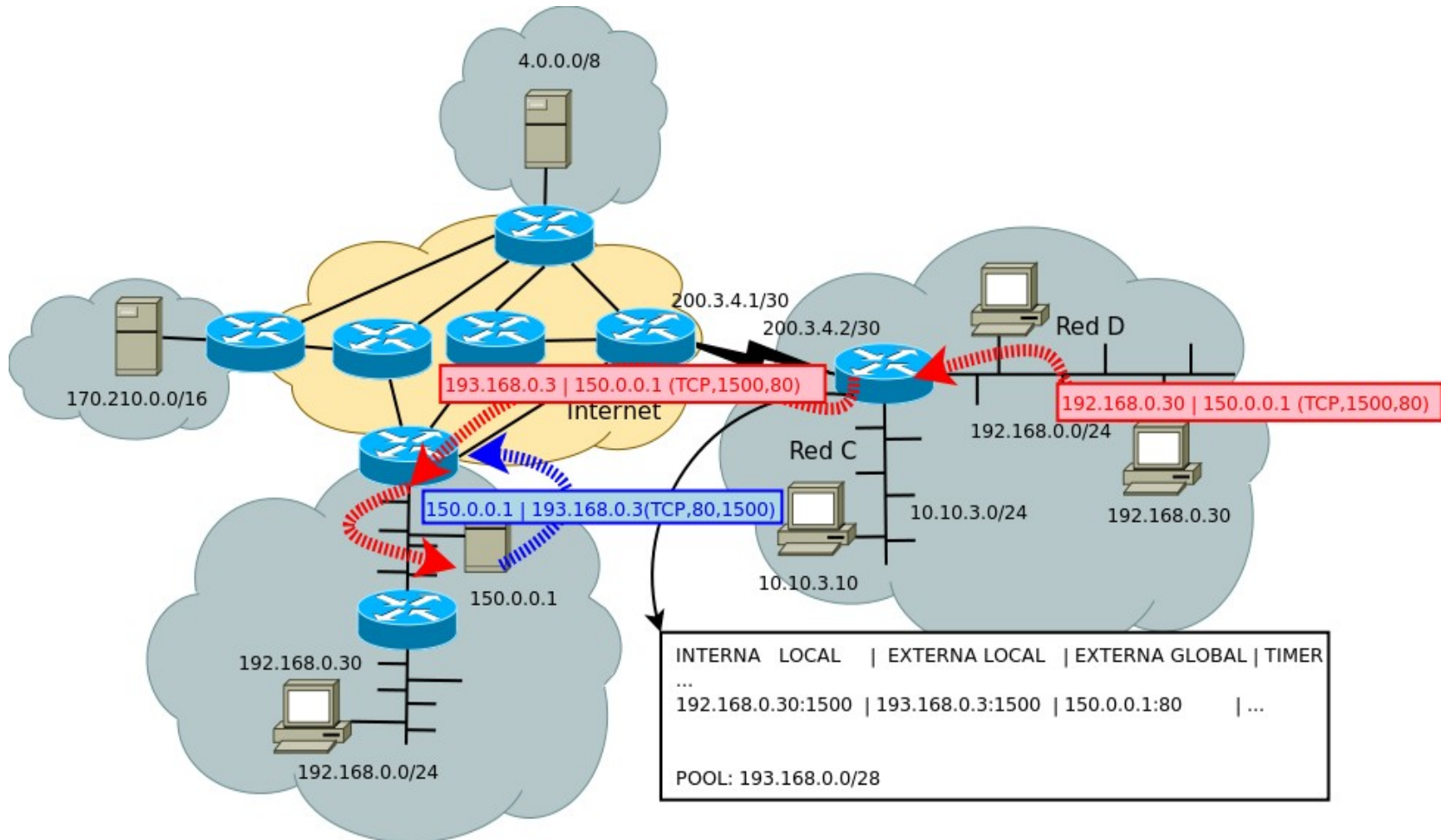
Ejemplo de NAT (Pool) (2)



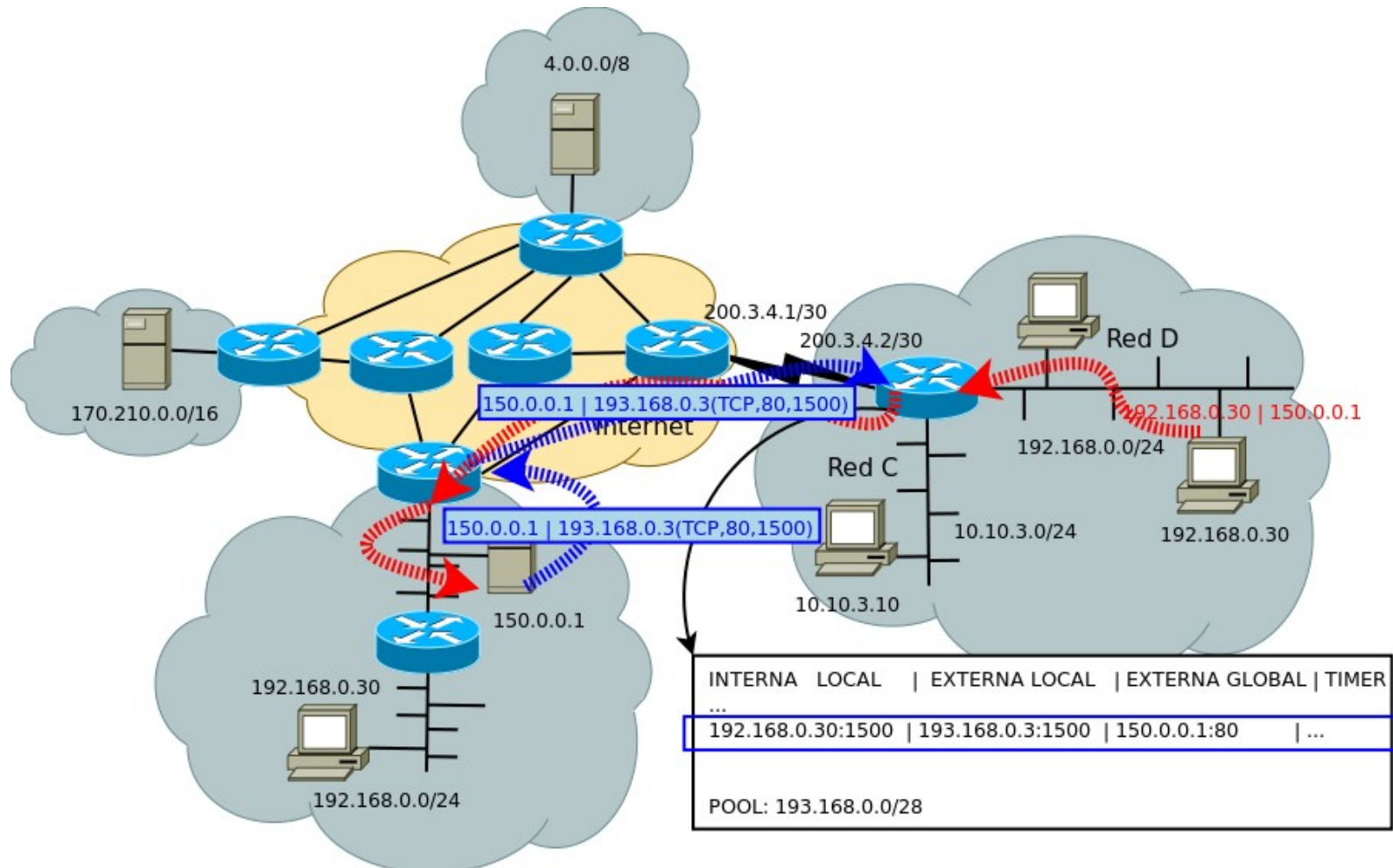
Ejemplo de NAT (Pool) (3)



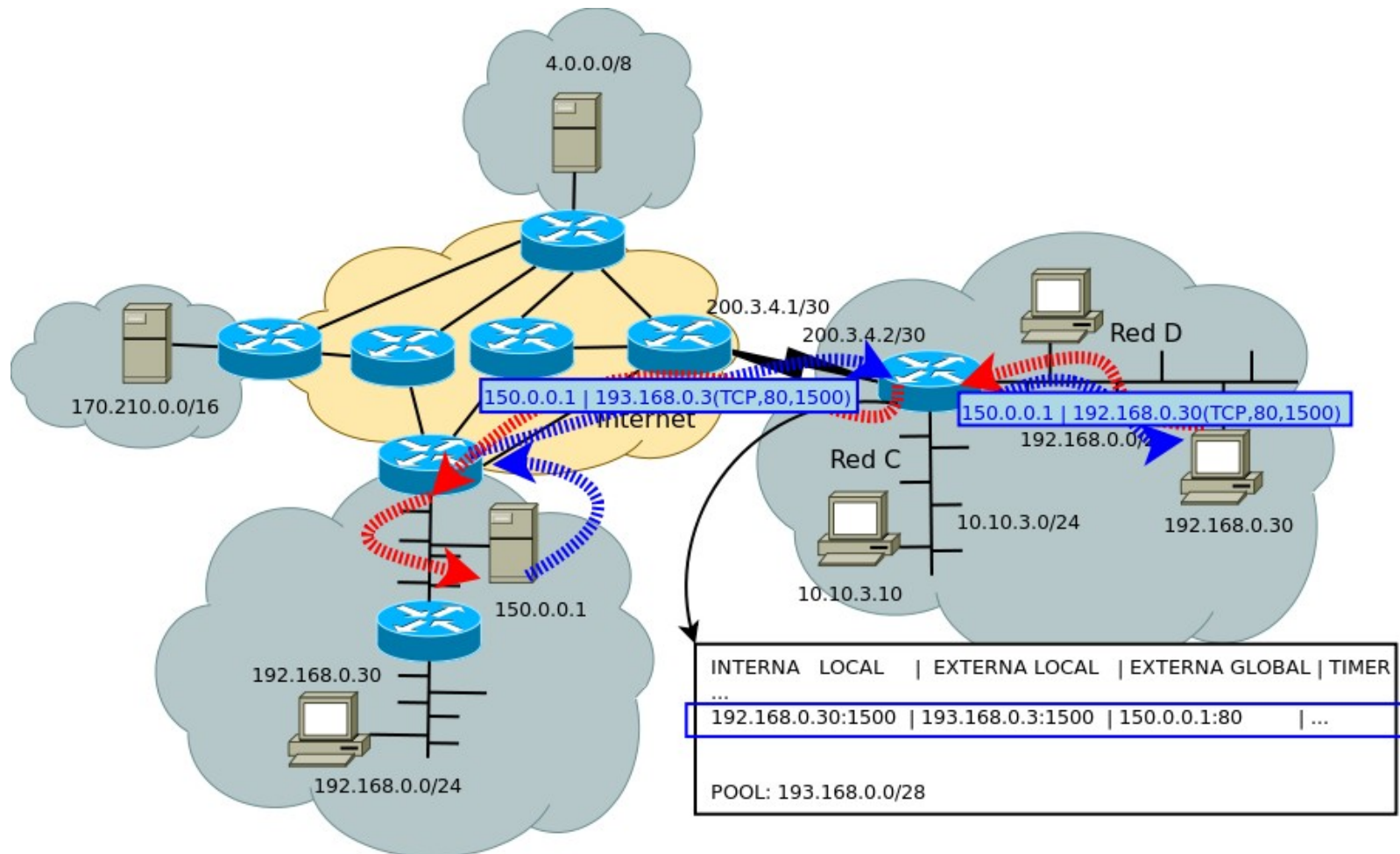
Ejemplo de NAT (Pool) (4)



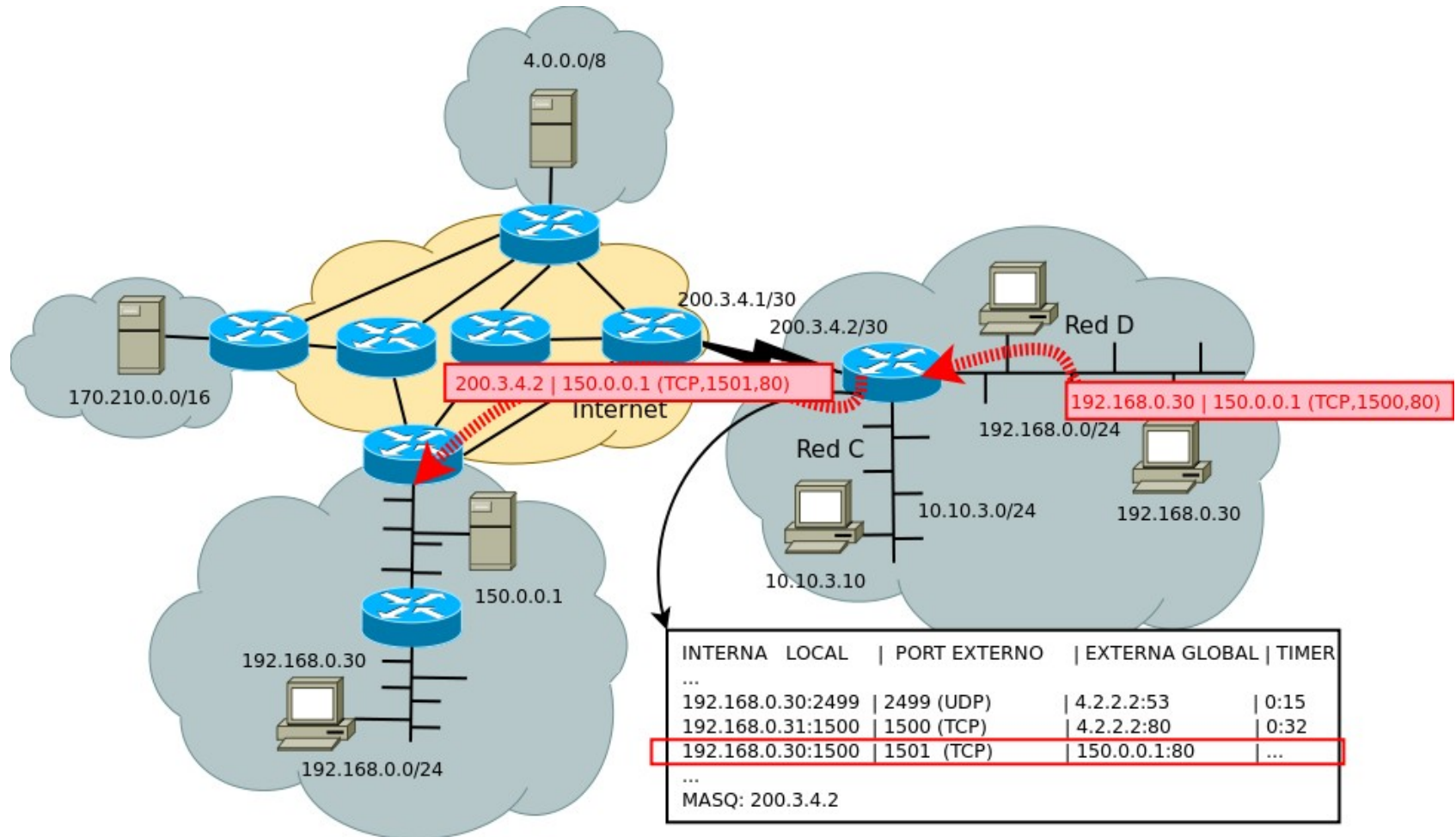
Ejemplo de NAT (Pool) (5)



Ejemplo de NAT (Pool) (6)



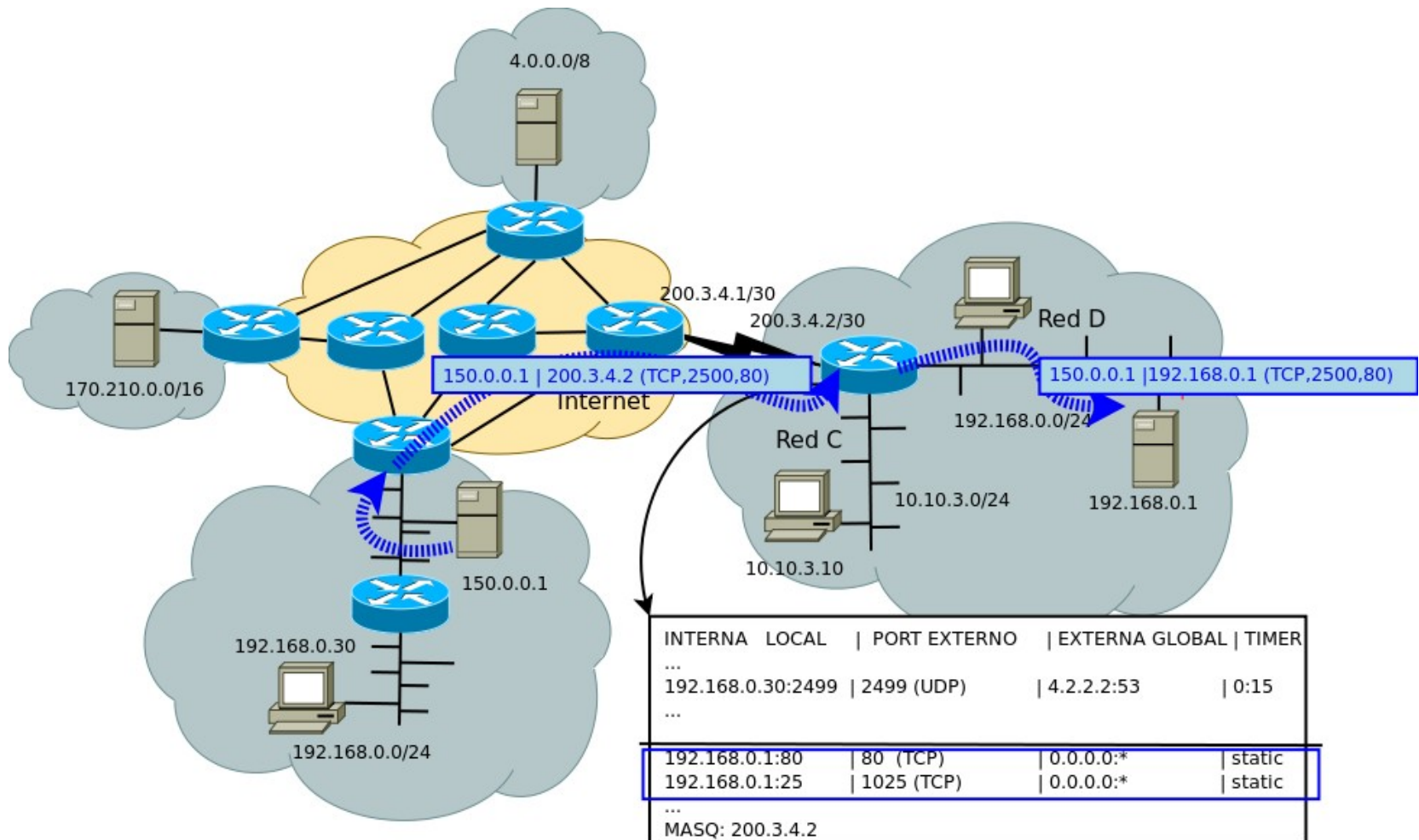
Ejemplo de NAPT (OVERLOAD/MASQ)



Port Forwarding

- Overloading/Masq no permiten acceso desde “afuera” hacia “adentro”.
- Solo se permiten entrar tráfico de conexiones generadas internamente.
- Mediante **Port Forwarding** (Re-envío de puerto) se permite poder tener servicios en una red privada accesibles desde “afuera”.
- No se requiere NAT estático, se implementa con NAT y mapeo reverso estático de puertos.

Ejemplo de Port Forwarding



Conclusiones

- NAT/NAPT resuelve temporalmente la escasez de direcciones Ipv4.
- Algunos servicios no funcionan.
- Da una “sensación” de seguridad, aunque no siempre es verdad.
- Se pierde la idea de IP end-to-end.
- Firewalls más complejos.

Referencias:

- Kurose/Ross: Computer Networking (5th Edition).
- Cisco CCNAv3.1.
- Cisco CCNA v4.0 exploration.
- RFC-1918 - Address Allocation for Private Internets.
- RFC-3022 - Traditional IP Network Address Translator (Traditional NAT).
- RFC-2663 - IP Network Address Translator (NAT) Terminology and Considerations