NATs

Area de Ingeniería Telemática
http://www.tlm.unavarra.es

Grado en Ingeniería en Tecnologías de Telecomunicación, 3º

Temas de teoría

0. Introducción
1. QoS
2. Encaminamiento dinámico en redes IP
3. Tecnologías móviles

Objetivos

- Comprender el funcionamiento general de los NAT

NATs: Introducción

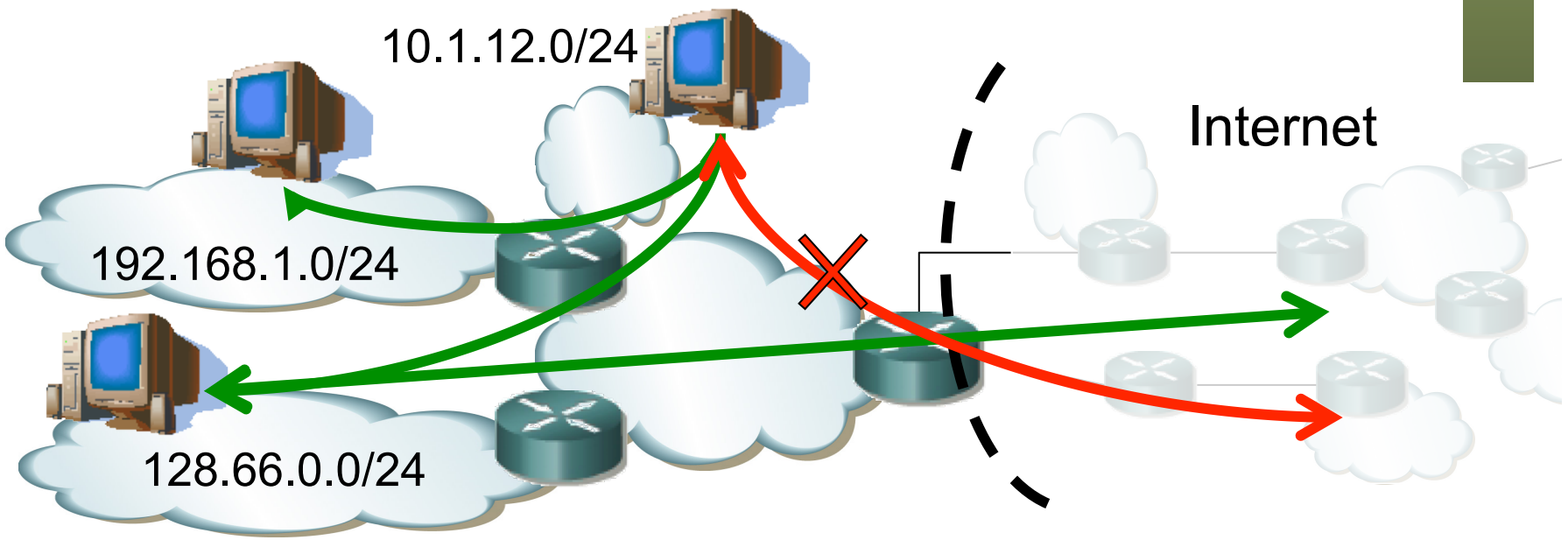
Problemas de IPv4

- Escasez de direcciones
  - Desaprovechamiento con Classful:
    - Clase A: Más de 16M de direcciones
    - Clase B: 64K direcciones
  - Con CIDR:
    - Hemos llegado de nuevo al problema de agotamiento
    - También PCs que se usen esporádicamente

- Complejidad innecesaria en los routers
- Algunas soluciones:
  - DHCP (escasa solución)
  - IPv6 (lejana solución)
  - NAT (vino a nuestro rescate… según cómo se mire)

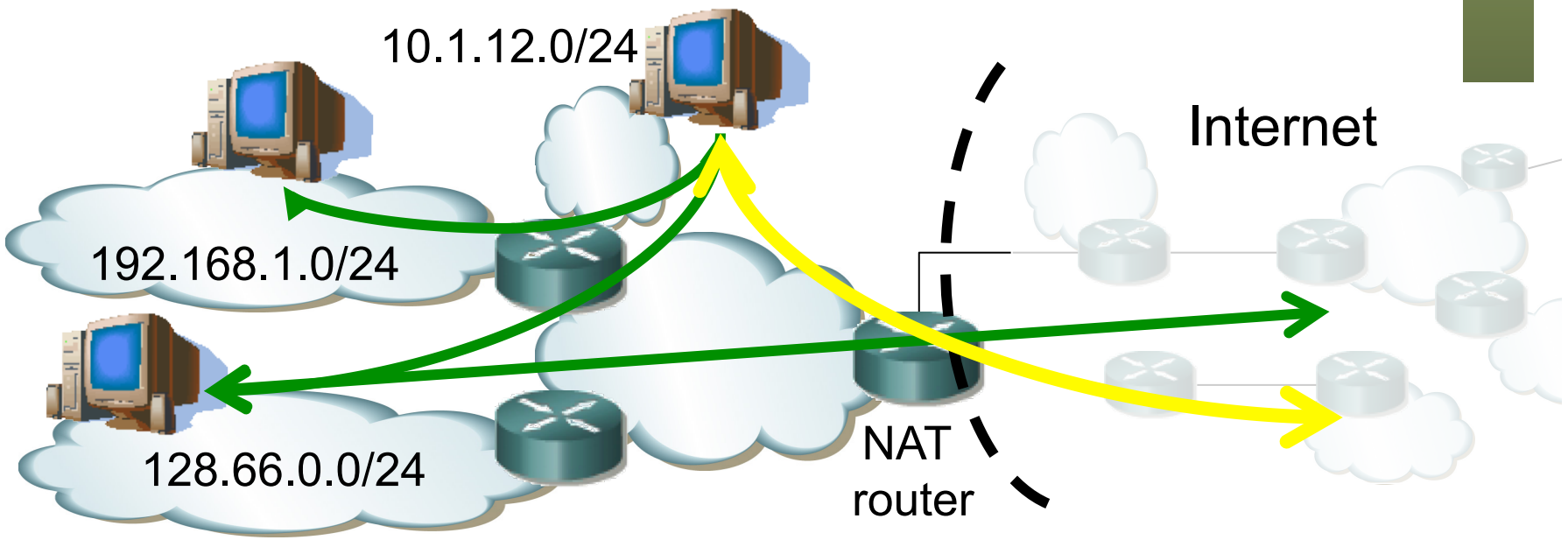
Direccionamiento privado

- 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12
- Pueden comunicarse con cualquier máquina de la red interna
- Al exterior solo pueden salir paquetes IP con direcciones públicas únicas



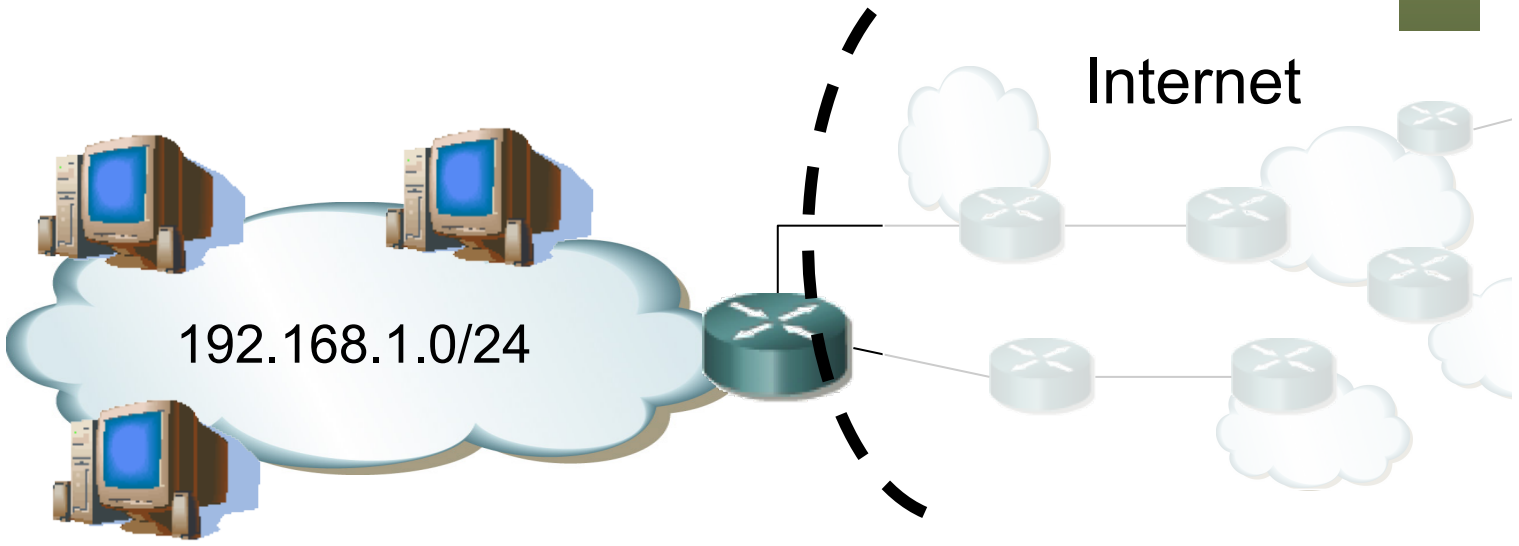
NATs

- Habilitan esa comunicación
- En los paquetes IP el NAT cambiará la dirección privada por una pública
- Escenario más conocido (…)



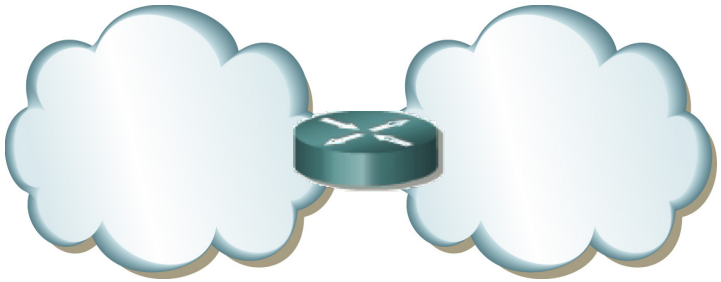
NATs

- Habilitan esa comunicación
- En los paquetes IP el NAT cambiará la dirección privada por una pública
- Escenario más conocido: Usuario residencial



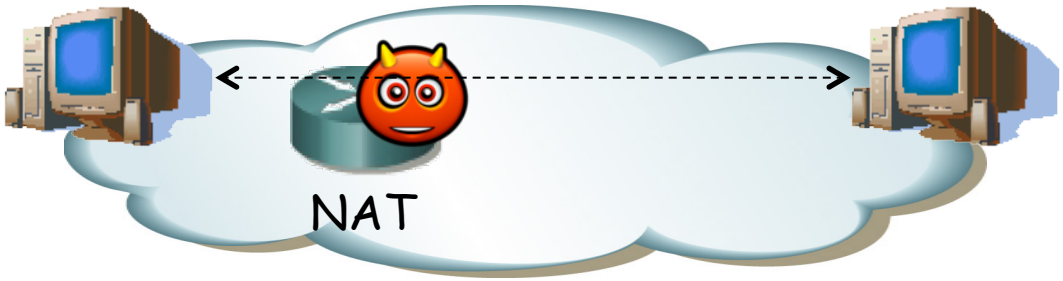
Introducción

- Hoy en día hay ya varias RFCs tratando el tema de los NATs
- Por ejemplo:
  - RFC 3022 “Traditional IP Network Address Translator (Traditional NAT)
  - RFC 2663 “IP Network Address Translator (NAT) Terminology and Considerations”
  - Y otras que comentaremos más adelante
- Un NAT mapea direcciones entre dos dominios
- Se habla de NATs y NAPTs (a veces PATs) aunque por extensión se les suele llamar a ambos NATs
- Se dice que hacen *transparent routing,* enrutando paquetes entre dos dominios



End-to-end principle

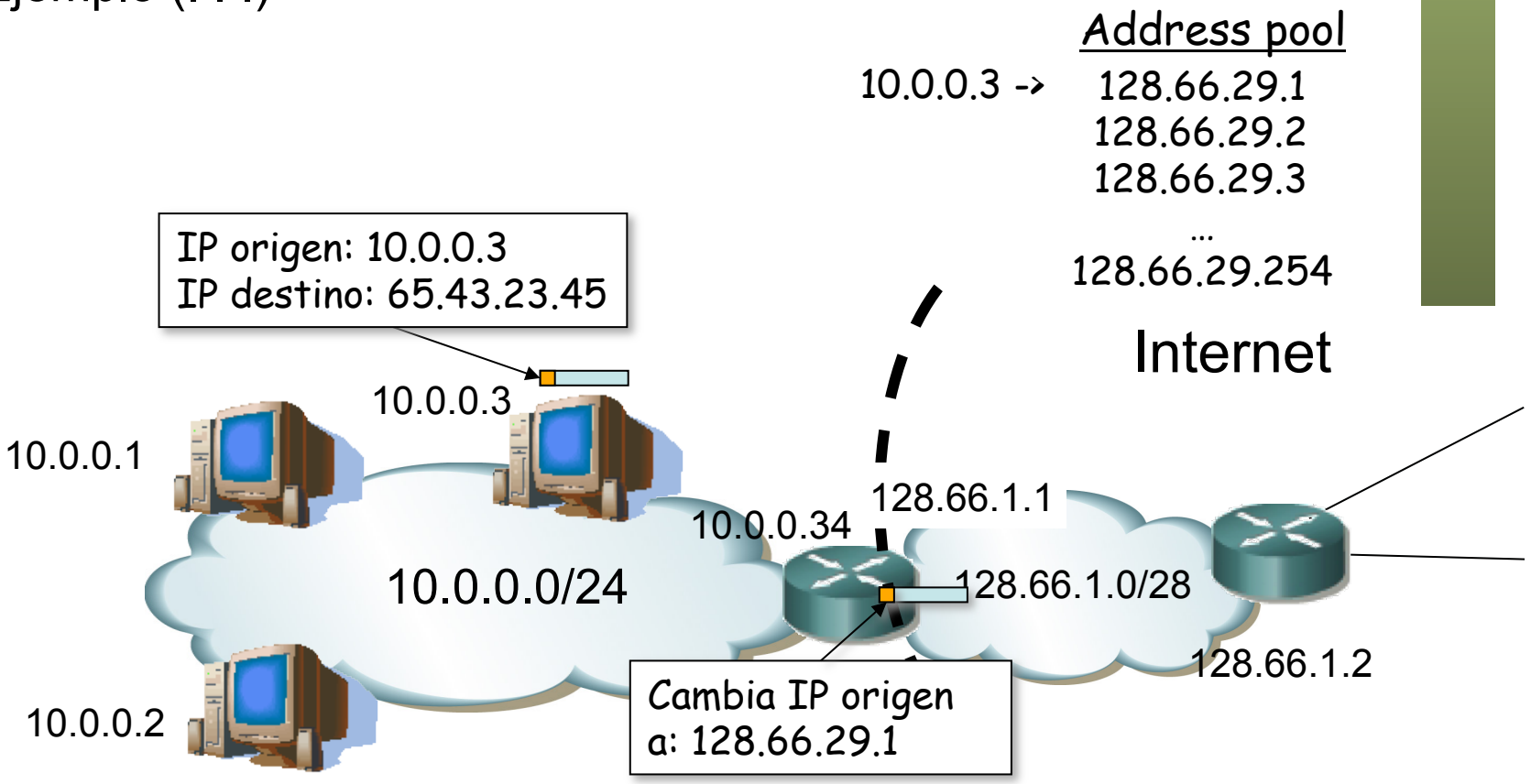
- Siempre que sea posible, implementar los protocolos en los extremos de la red
- Implementar en la red lo menos posible
- Red con mínima inteligencia (la red es difícil de cambiar)
- Inteligencia en los extremos (es más sencillo añadir nueva funcionalidad)
- La Internet es un ejemplo, con IP en la red y el resto de protocolos solo en los extremos
- NATs rompen el funcionamiento extremo-a-extremo de la Internet
- Eso va a dar problemas a las aplicaciones, a su funcionamiento y a su despliegue



NATs: Funcionamiento básico

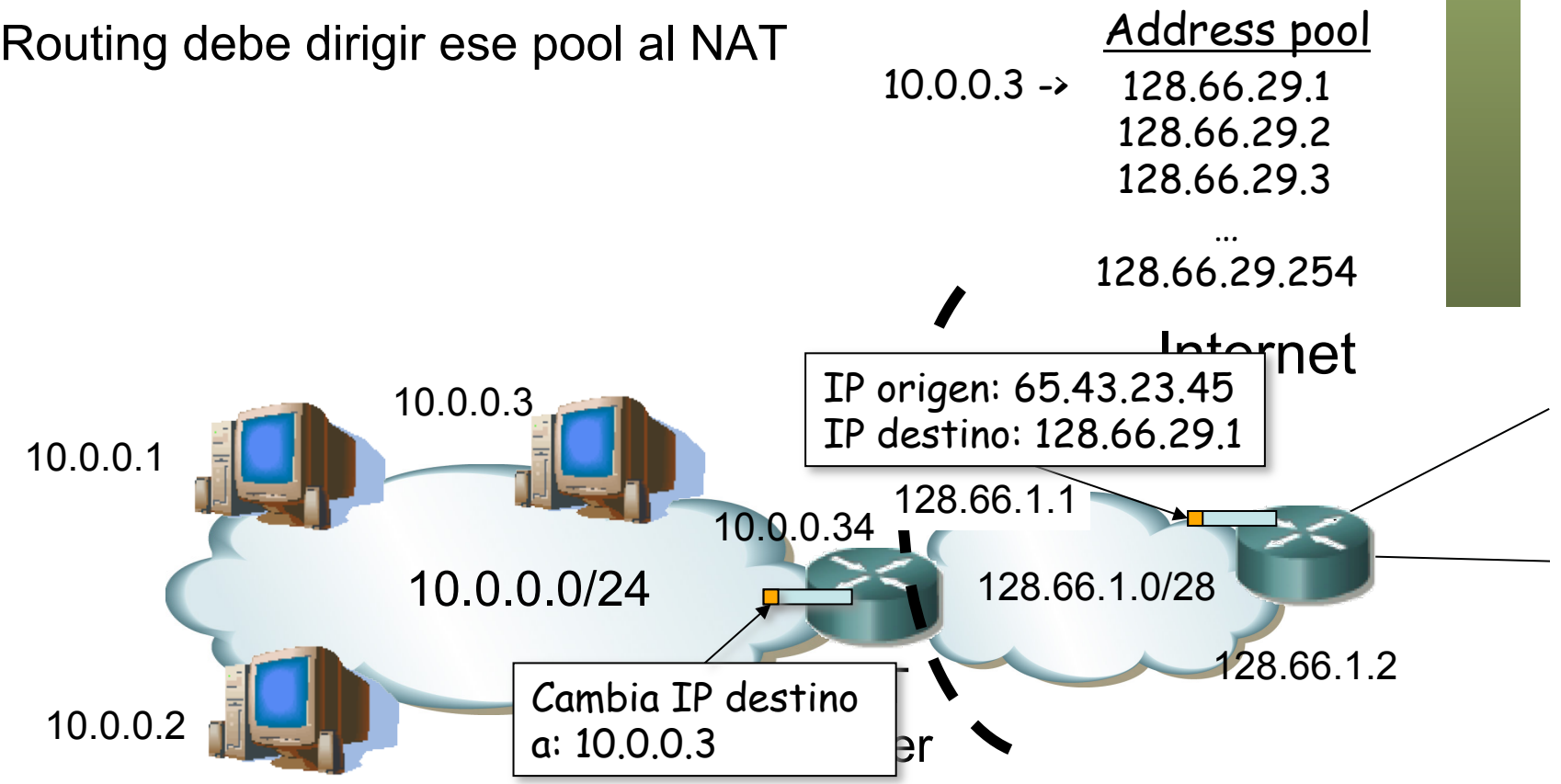
NATs

- NAT tiene asignado un bloque (*pool*) de direcciones públicas
- Cuando reenvía al exterior un paquete cambia la dirección origen por una del pool
- Apunta el *mapeo* para aplicarlo en sentido contrario
- Ejemplo (. . .)



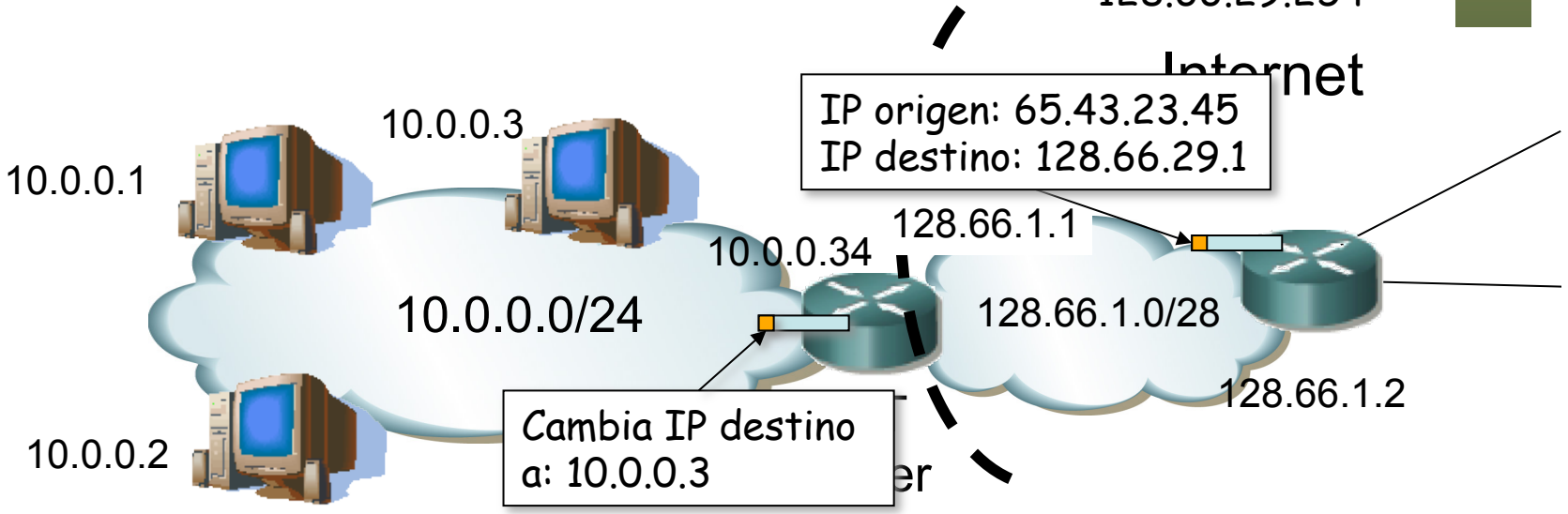
NATs

- Cuando venga un paquete de esa dirección IP externa vendrá dirigido a la dirección que colocó como origen el router NAT
- La tabla de mapeos indica el cambio a hacer (… …)
- Para el host remoto el flujo es con la dirección pública pues nunca ve la privada
- Routing debe dirigir ese pool al NAT



NATs: mapeo

- Estático
  - Preconfigurado 1 a 1
  - Requiere tantas direcciones como hosts con direccionamiento privado
- Dinámico
  - Mapea bajo demanda
  - Requiere menos direcciones públicas
  - Un timer de inactividad para eliminar el mapeo



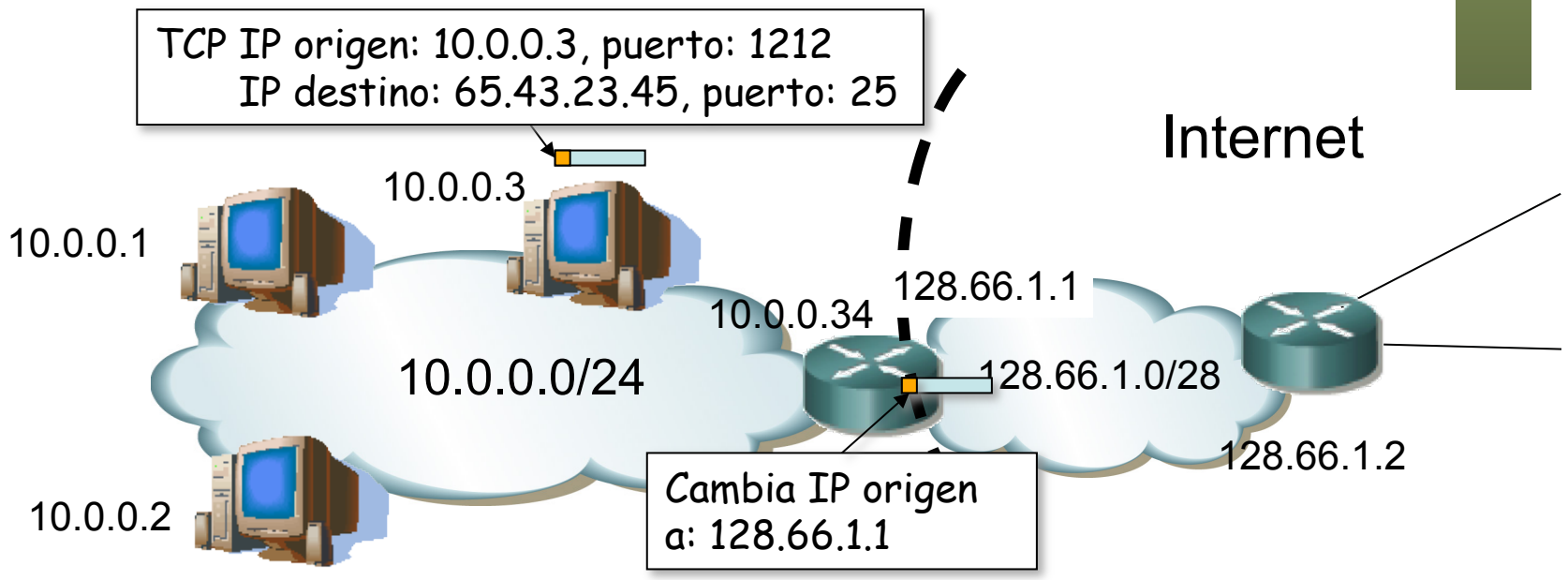
NAPT

- Network Address/Port Translator
- Va a poder modificar también la cabecera del protocolo de transporte
- Solo para TCP, UDP e ICMP
- "Sesiones"
  - TCP/UDP (TU): {(IP-1, Port-1), (IP-2, Port-2)}
  - ICMP: (IP-1, queryID, IP-2)
  - En TCP termina tras intercambio de FINs/RST aunque pueden perderse y se mantiene durante un tiempo (recomendado 4min)
  - El concepto de sesión a nivel de aplicación puede diferir e incluir varias de éstas
  - Hosts pueden reiniciarse así que siempre deben caducar los mapeos tras un tiempo de inactividad

NAPT

- Pocas direcciones públicas, por ejemplo solo una (que puede ser la de su interfaz exterior)
- Paquete hacia el exterior provoca nuevo mapeo (. . .)

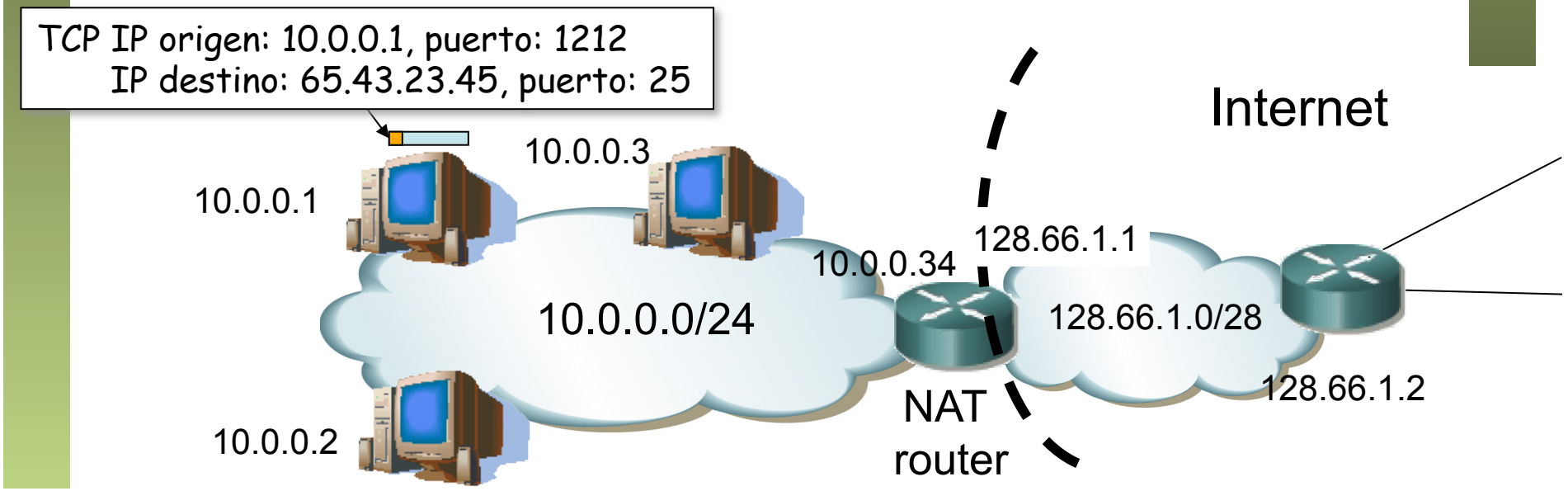
Proto.	Interno	Pública	Exterior
TCP	10.0.0.3:1212	128.66.1.1:1212	65.43.23.45:25



NAPT

- Otro host podría ir al mismo servidor y servicio empleando el mismo puerto local (no hay coordinación entre ellos)
- El mapeo provoca una colisión (. . .)

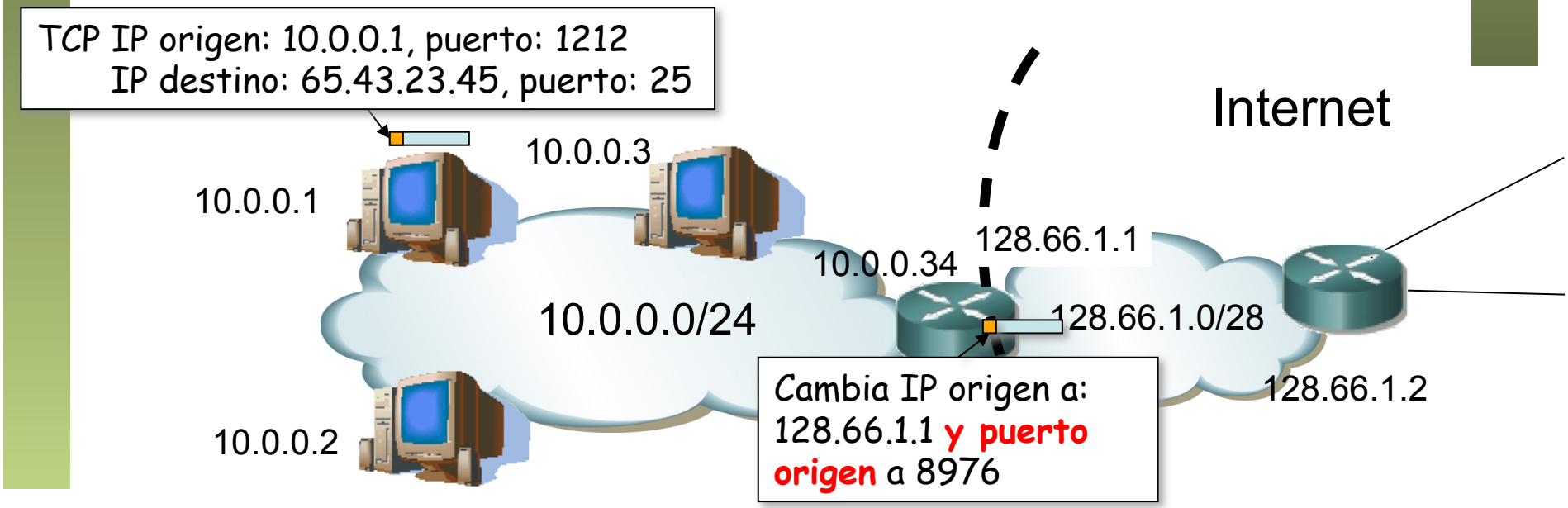
Proto.	Interno	Pública	Exterior
TCP	10.0.0.3:1212	128.66.1.1:1212	65.43.23.45:25
TCP	10.0.0.1:1212	128.66.1.1:1212	65.43.23.45:25



NAPT

- El NAPT va a cambiar también el puerto origen

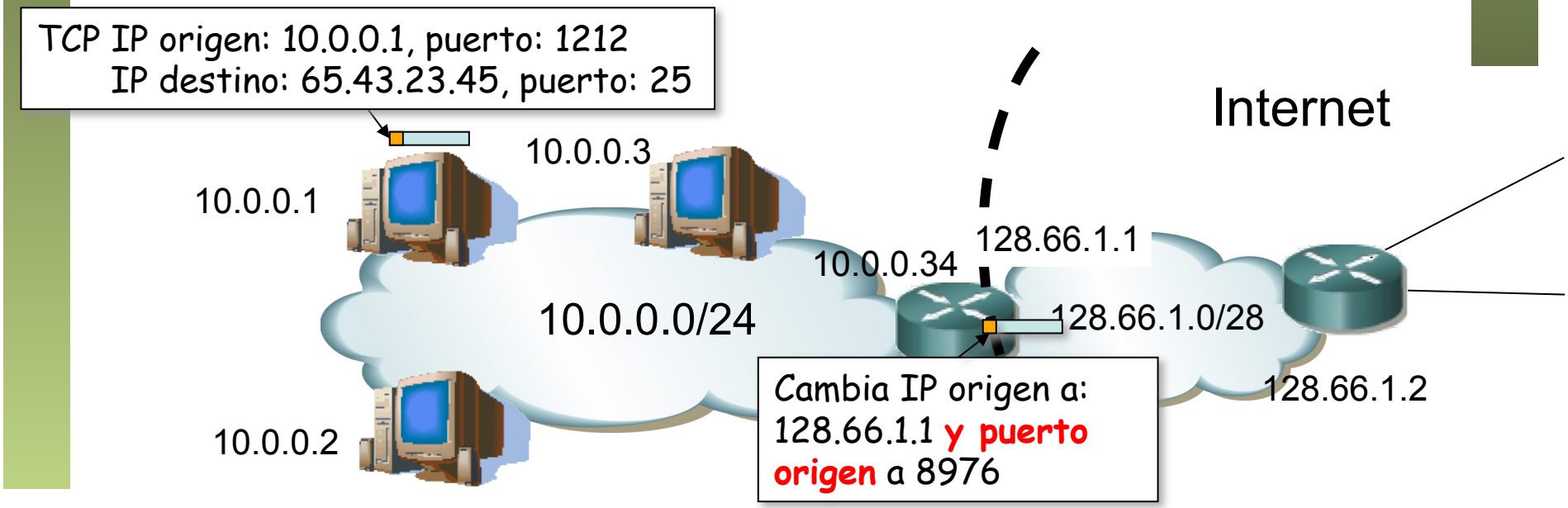
Proto.	Interno	Pública	Exterior
TCP	10.0.0.3:1212	128.66.1.1:1212	65.43.23.45:25
~~TCP~~	~~10.0.0.1:1212~~	~~128.66.1.1:1212~~	~~65.43.23.45:25~~
TCP	10.0.0.1:1212	128.66.1.1:**8976**	65.43.34.45:25



NAPT: problema

- Ante una dirección IP y puerto externo muy popular hay un límite de mapeos
- Se debe al límite de puertos TCP disponibles (16 bits)

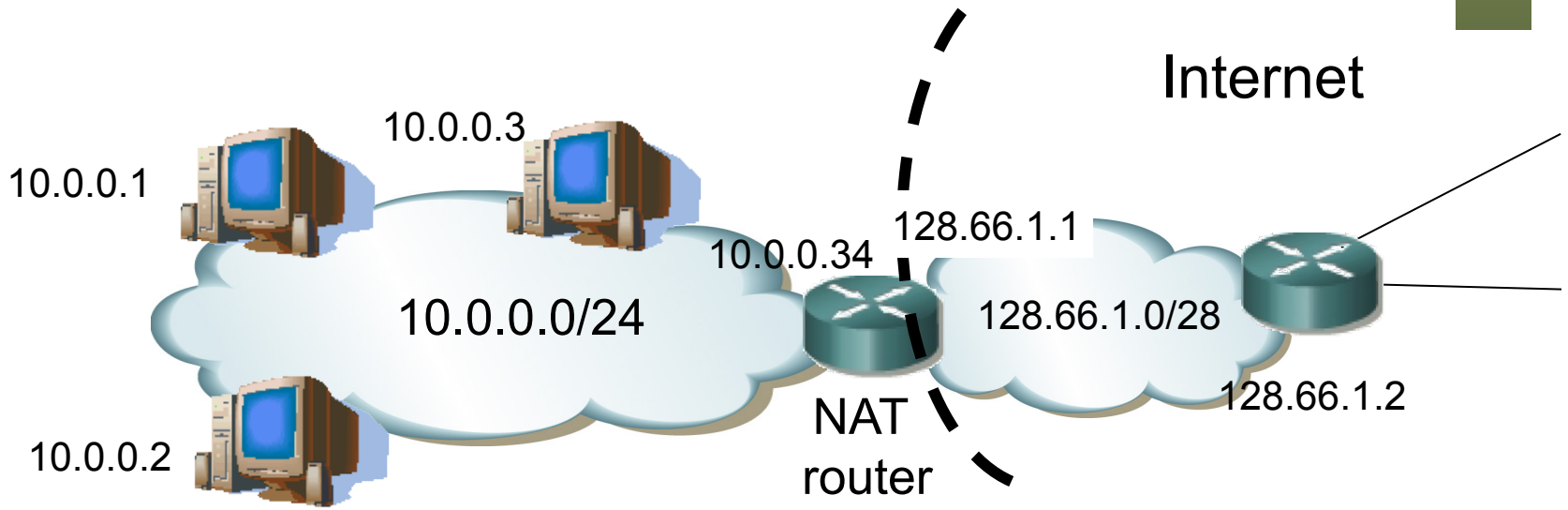
Proto.	Interno	Pública	Exterior
TCP	10.0.0.3:1212	128.66.1.1:1212	65.43.23.45:25
~~TCP~~	~~10.0.0.1:1212~~	~~128.66.1.1:1212~~	~~65.43.23.45:25~~
TCP	10.0.0.1:1212	128.66.1.1:**8976**	65.43.34.45:25



Conexiones entrantes

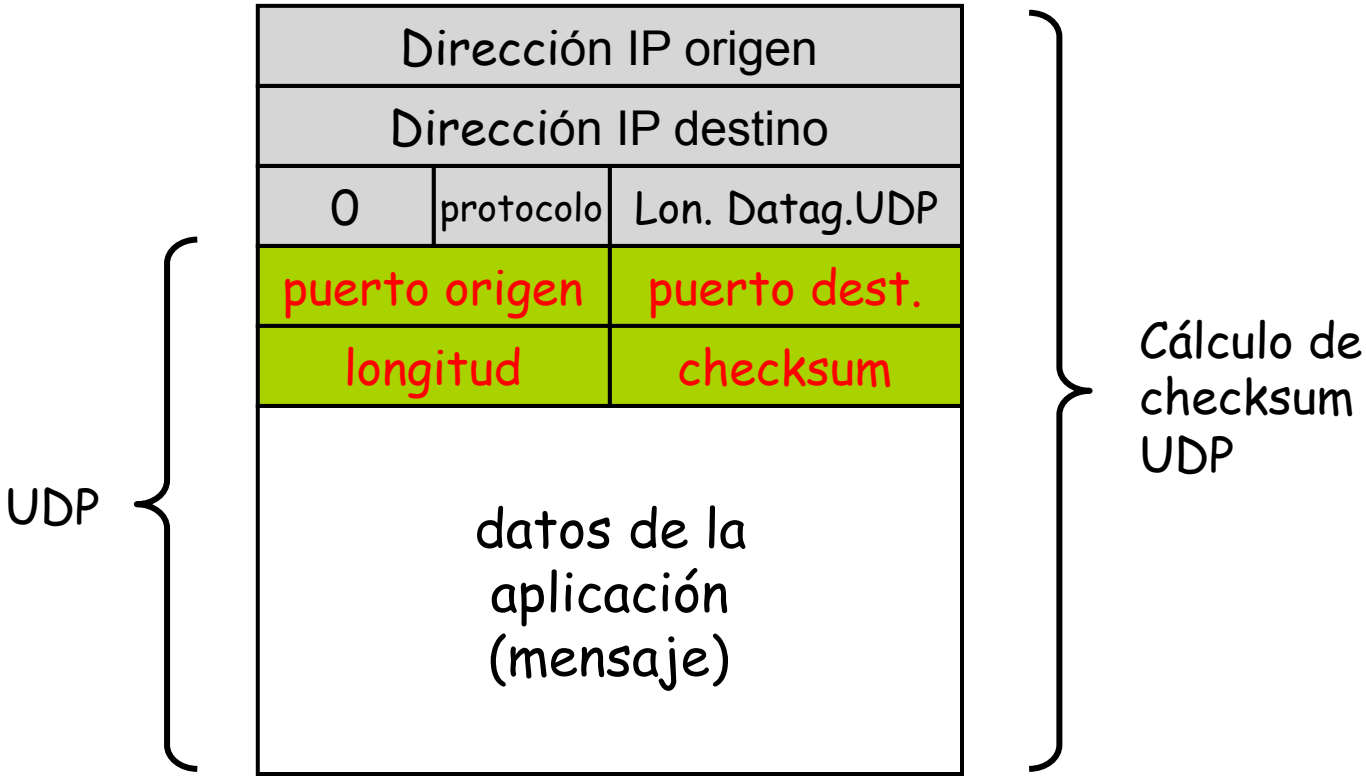
- Normalmente mediante mapeo estático
- Cambiando o no el puerto local

Proto.	Interno	Pública	Exterior
TCP	10.0.0.3:1212	128.66.1.1:80	65.43.23.45:80



Checksums

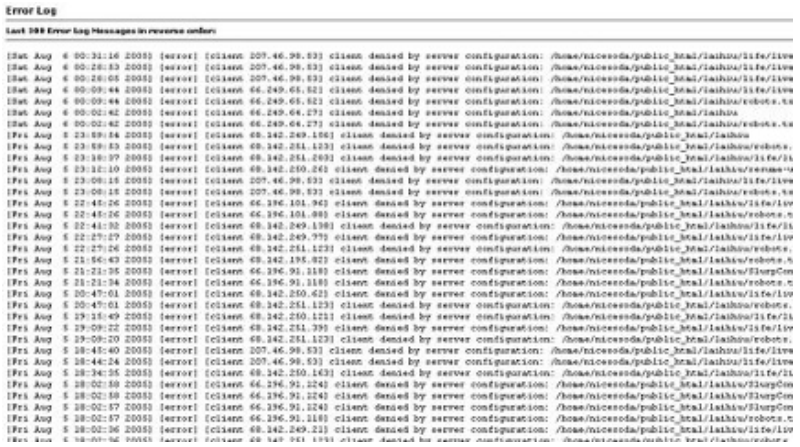
- Cambio en dirección IP requiere recalcular checksum IP
- También requiere recalcular checksum TCP/UDP pues protege también a las direcciones IP



NATs y las aplicaciones

NATs y logs

- Problemas con logs y estadísticas en servidores
  - El mismo host puede aparecer en el exterior con diferente dirección en diferente momento
  - Varios hosts pueden aparecer con la misma dirección
  - Con datos de red+transporte no se pueden distinguir
  - Dificulta hacer estadísticas por usuario o identificar responsables de abusos



NATs y aplicaciones

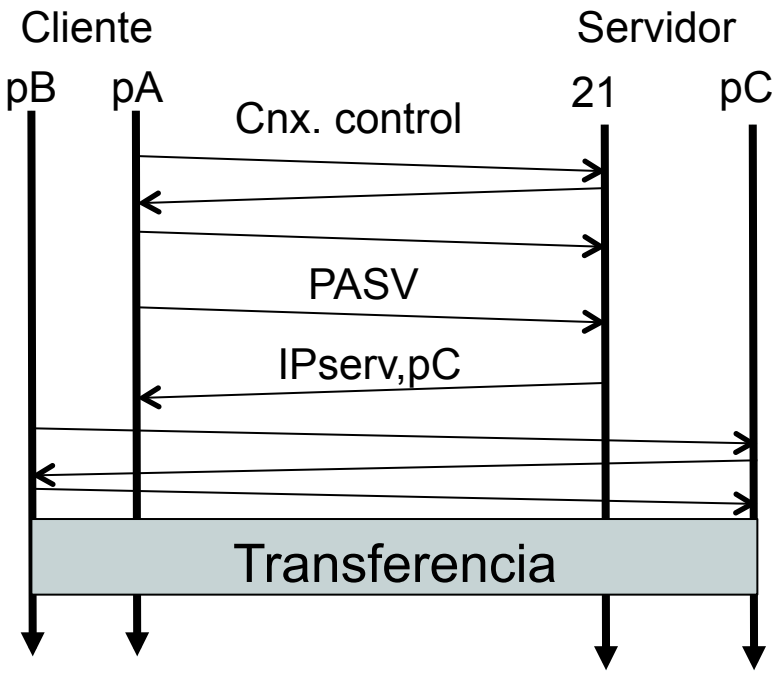
- Problemas con aplicaciones que
  - En la comunicación de datos hablan de direcciones IP y/o puertos (FTP, SIP, H.323, juegos online…)
  - Esa información es necesaria para establecer otras sesiones
  - Se emplean entonces ALGs (…)

ALGs

- *Application Level Gateways*
- Parte del NAT/NAPT
- Monitoriza y modifica el payload (datos TCP/UDP)
- Deben conocer el protocolo de nivel de aplicación
- No debe estar encriptado (o el ALG debe tener la clave)
- Ejemplo: FTP

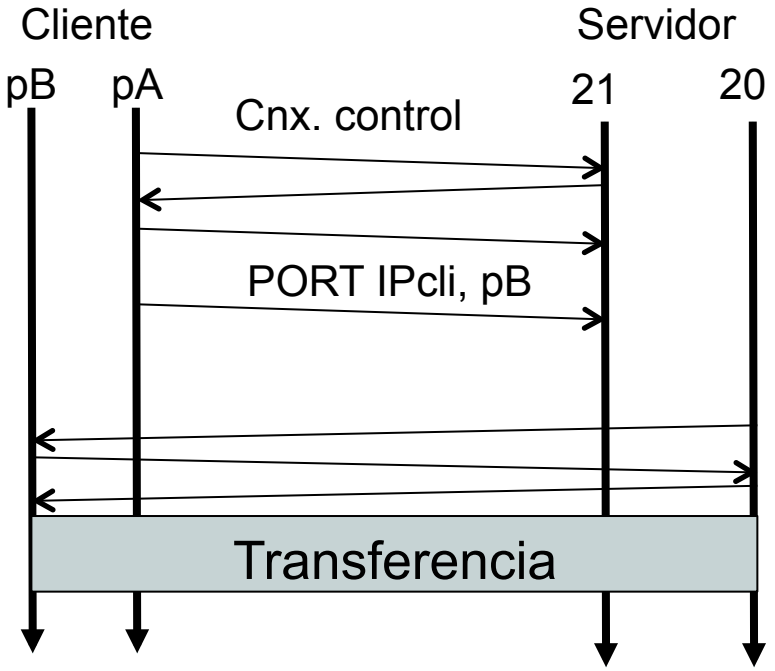
FTP: File Transfer Protocol

- RFC 959
- Servidor emplea puerto TCP 21
- Cliente establece una conexión de control con el servidor
- Transferencia en modo **pasivo**
  - Cliente envía comando a servidor
  - Servidor contesta indicando la dirección IP y puerto en que espera conexión
  - Cliente establece una conexión con el servidor a ese puerto
  - Se produce la transferencia
  - El servidor tiene que aceptar conexiones en múltiples puertos
  - Podría ser un problema con firewalls



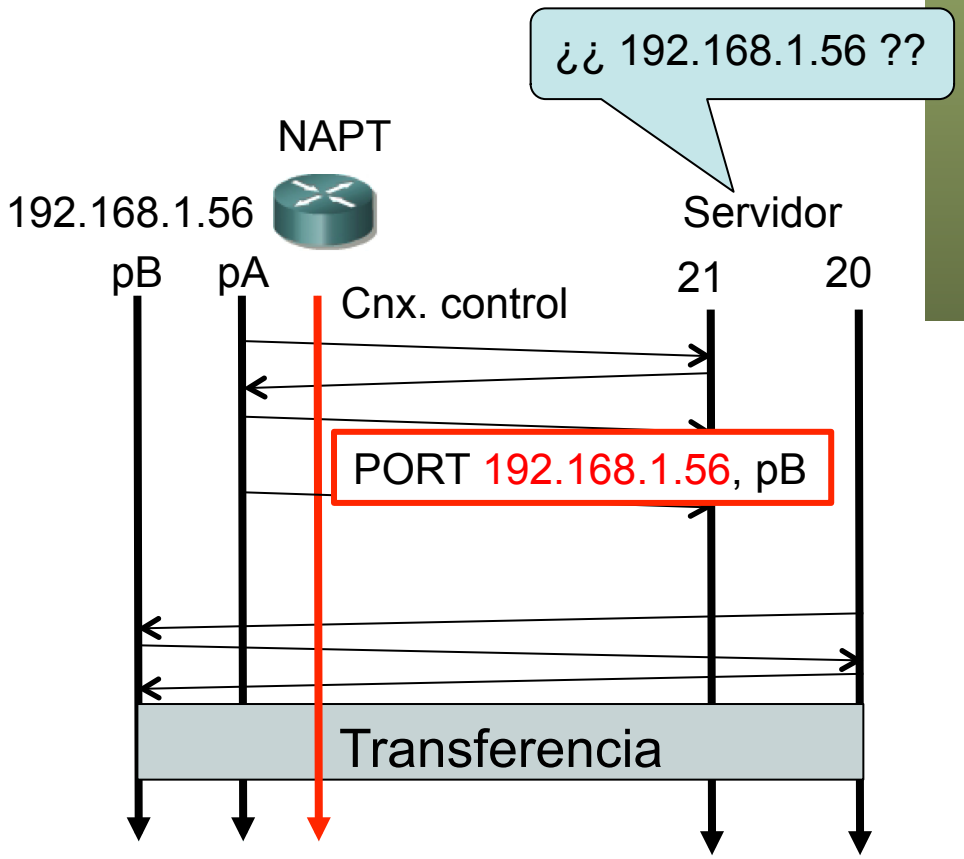
FTP: File Transfer Protocol

- RFC 959
- Servidor emplea puerto TCP 21
- Cliente establece una conexión de control con el servidor
- Transferencia en modo **activo**
  - Cliente envía comando a servidor indicando dirección IP y puerto en que espera conexión (…)
  - Servidor establece una conexión con el cliente a ese puerto (…)
  - Se produce la transferencia (…)



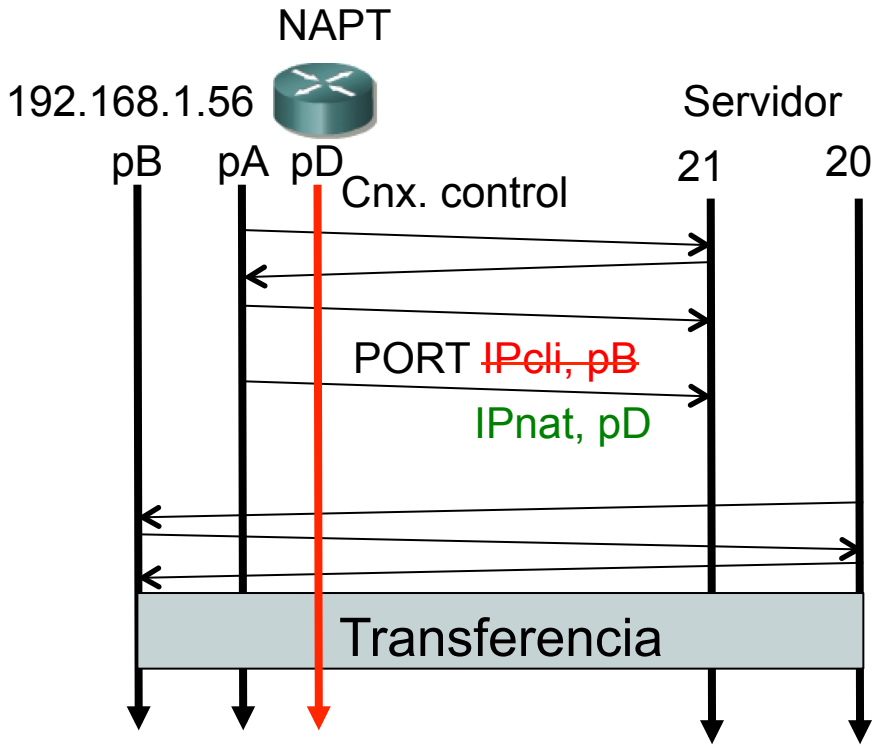
NAT y FTP activo

- ¿Y si el cliente está tras un NAT?
- El cliente ha especificado un puerto local, así como su dirección
- ¡ Esa dirección no es alcanzable para el servidor !
- (…)



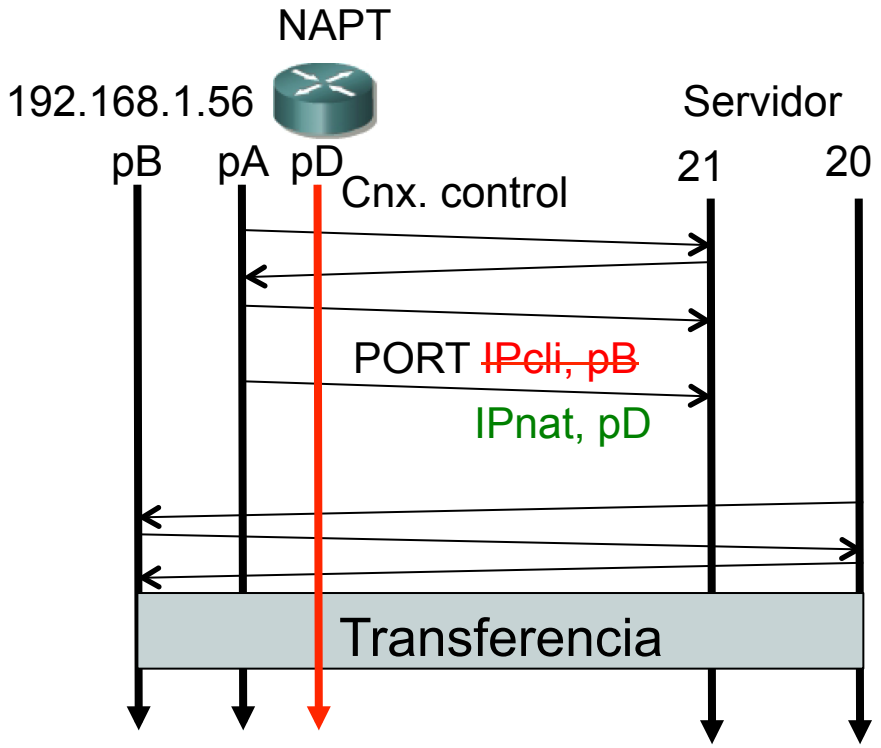
NAT y FTP activo

- Modificarlo con dirección externa y puerto que seleccione
- Introducir mapeo para esa (dirección,puerto)
- ¿Eso es sencillo, no? (…)



NAT y FTP activo

- NAT debe seguir el stream de datos para reconocer el comando
- Hay que reconstruir el stream si el comando está fragmentado
- La modificación puede introducir más o menos bytes en el comando FTP (son ASCII)
- ¡ Entonces debe modificar los números de secuencia TCP y de ACK a partir de ahí !



Resumen

- NATs modifican cabecera de red y transporte
- Necesarios debido al agotamiento de direcciones
- Dan problemas a protocolos de nivel de aplicación que comuniquen direcciones/ puertos