Soluciones a los problemas de direccionamiento

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

Programación de Redes
Grado en Ingeniería Informática, 3º

Temas de teoría

1. Introducción
2. Campus LAN
3. Encaminamiento
4. Tecnologías de acceso y WAN

Problemas de IPv4

- Escasez de direcciones
  - Desaprovechamiento con Classful:
    - Clase A: Más de 16M de direcciones
    - Clase B: 64K direcciones
  - Con CIDR:
    - PCs que se usen esporádicamente
- Complejidad innecesaria en los routers
- Algunas soluciones:
  - DHCP
  - NAT
  - IPv6

DHCP

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

DHCP

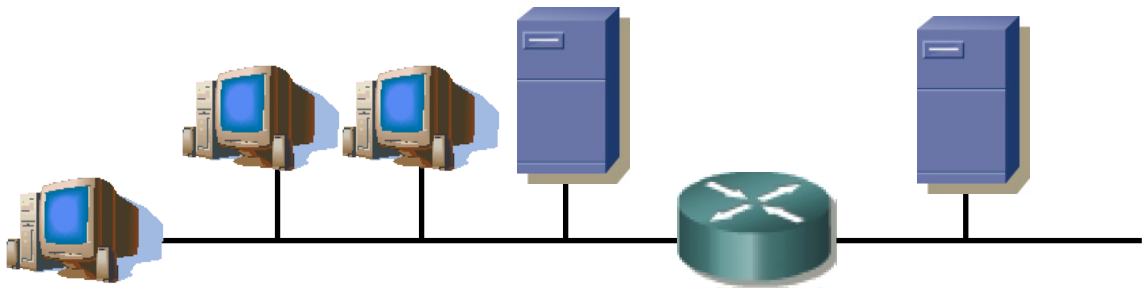
- Dynamic Host Configuration Protocol
- RFC 2131
- Basado en BOOTP (RFC 951)
- Permite a un host obtener configuración IP de forma automática
  - Dirección IP
  - Máscara de red
  - Router por defecto
  - Servidor de DNS
- El host solicita la configuración a un servidor de DHCP
- Emplea UDP
- Simplifica cambios en el direccionamiento

Mecanismos de asignación de dirección IP:

- Manual allocation
  - IP fijada por el administrador para la máquina
  - DHCP sirve para comunicarla a la máquina
- Automatic allocation
  - Asigna una IP de un *pool*
  - Asignación permanente
- Dynamic allocation
  - Asigna por un periodo de tiempo limitado (*lease*)
  - O hasta que el host la libera

DHCP: Funcionamiento

- El cliente es el nuevo host conectado a la red
- Necesita configuración de red
- Para ello preguntará a un servidor de DHCP
- Normalmente habrá un servidor en cada subred
- Si no hay servidor en una subred se puede configurar un *relay*
  - Conoce la dirección del servidor
  - Ve las peticiones del cliente y las reenvía
  - Es normalmente un router



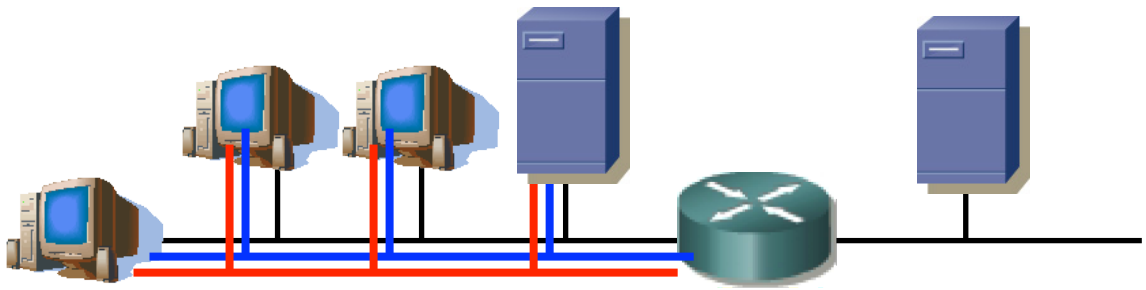
DHCP: Funcionamiento

DHCP Server Discovery

- Envía un datagrama UDP al puerto 67
- No conoce la dirección IP del servidor: lo dirige a la IP de **Broadcast** (255.255.255.255)
- No tiene dirección IP: emplea como origen la dirección IP "este host" (0.0.0.0) (…)

DHCP Server Offer

- El cliente puede recibir respuesta de uno o varios servidores (…)
- El servidor ofrece una dirección al cliente
- Ofrece también una duración durante la cual le cede la dirección
- Si hay varios ofrecimientos el cliente puede elegir



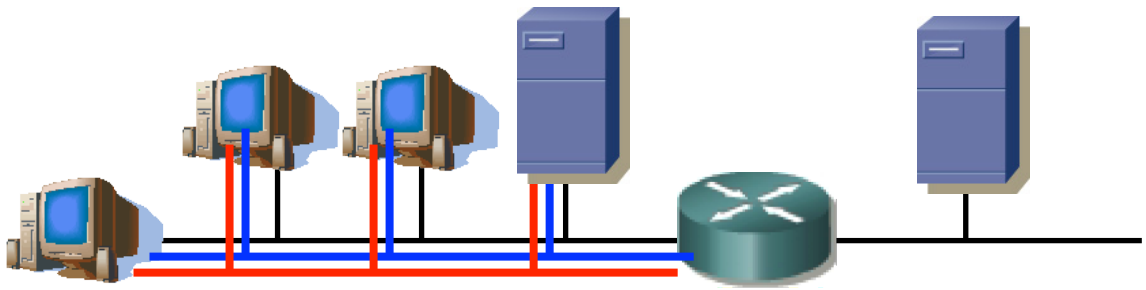
DHCP: Funcionamiento

DHCP Request

- El cliente ha escogido una oferta y hace la solicitud al servidor correspondiente (…)

DHCP ACK

- El servidor confirma la asignación al cliente (…)

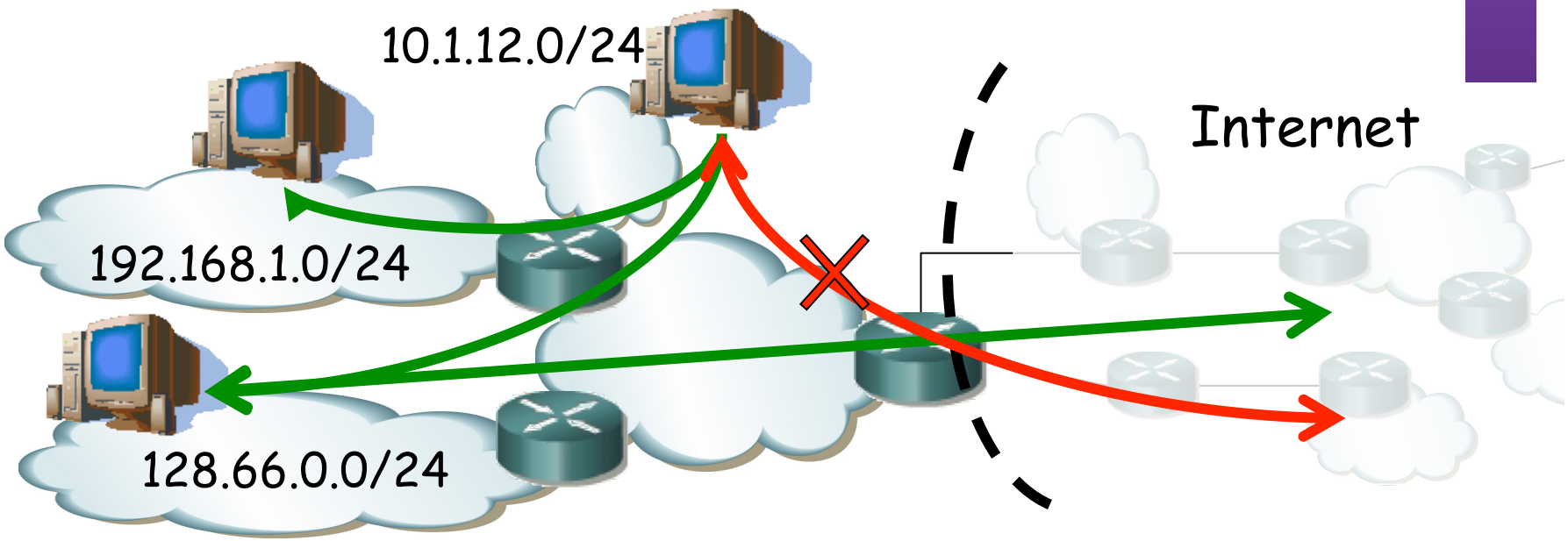


NAT

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

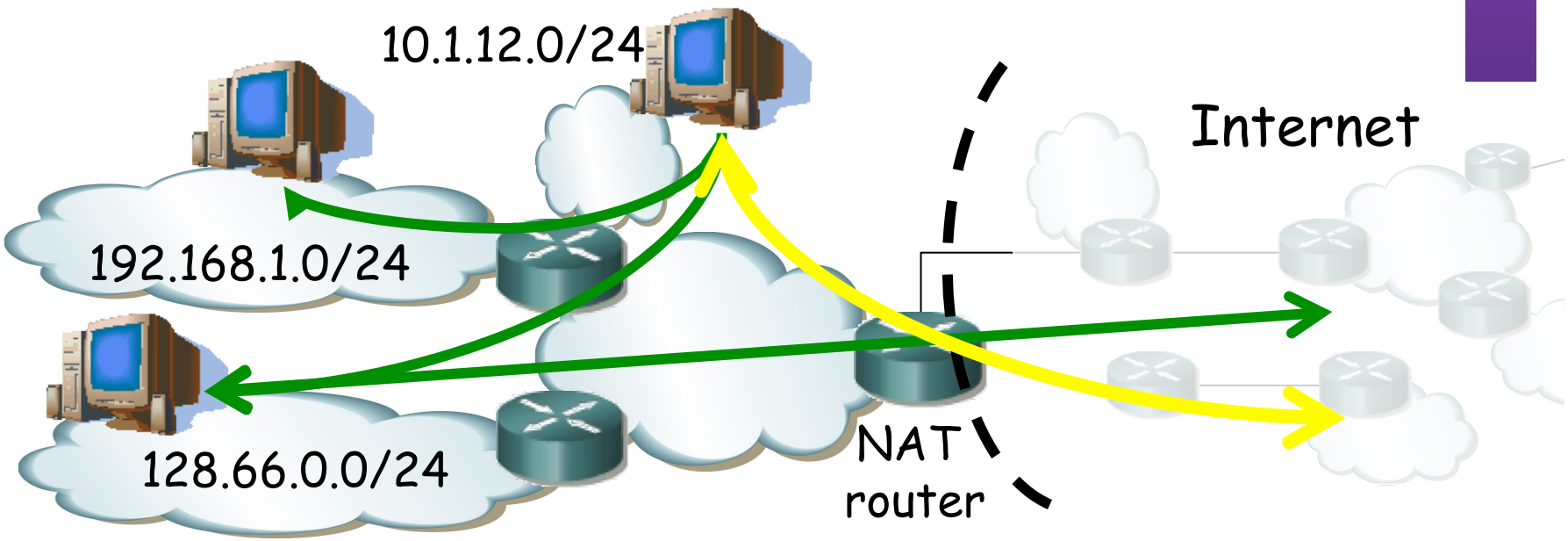
Direccionamiento privado

- 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



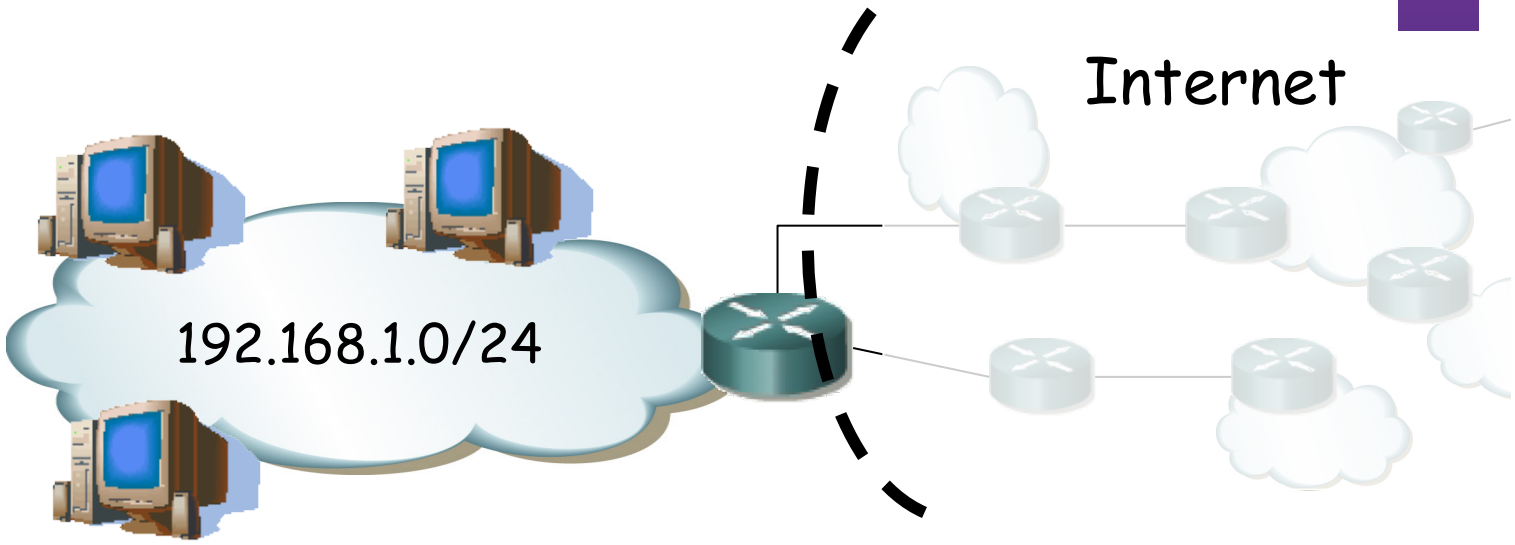
NATs

- 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

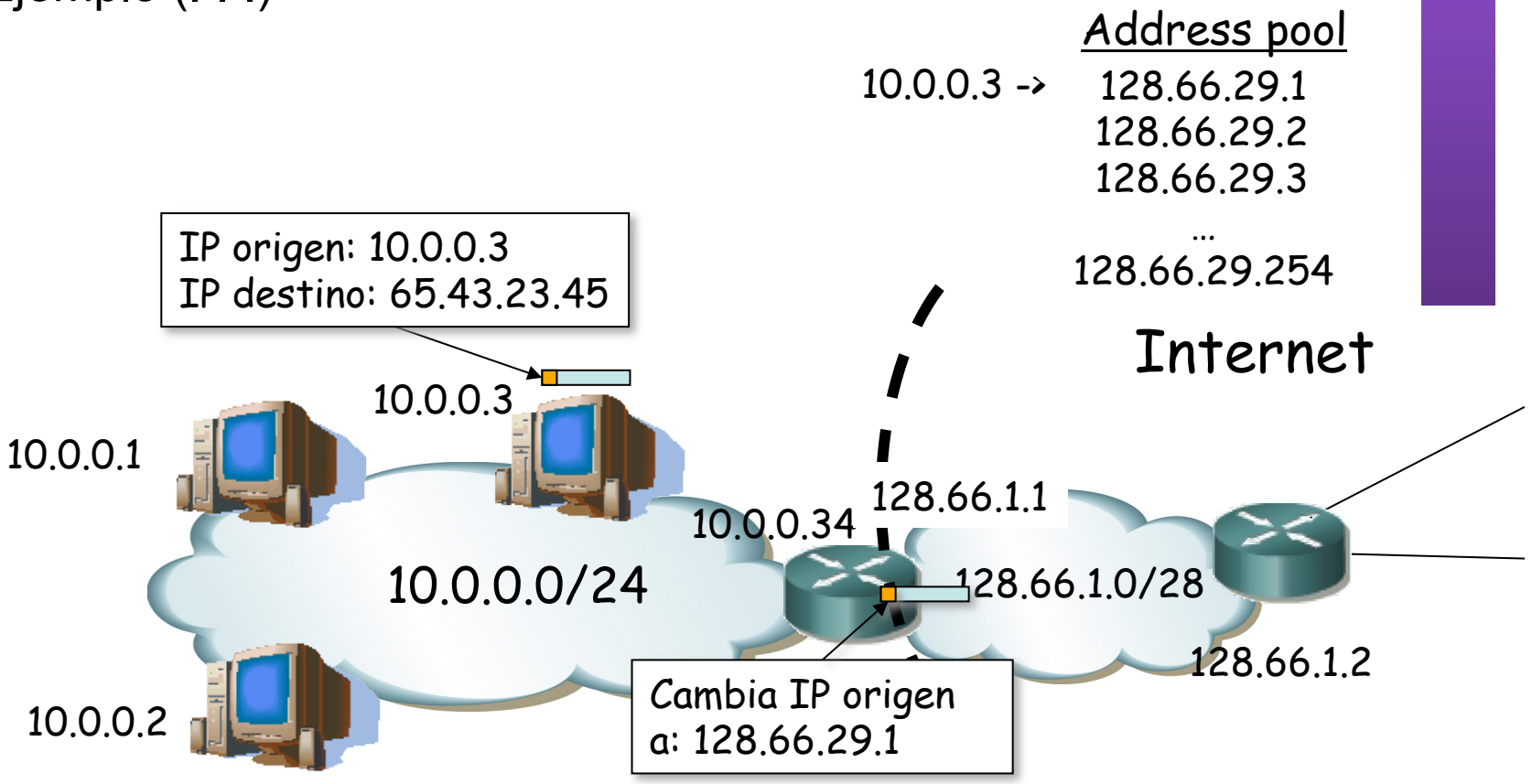


Introducción

- RFC 3022 “Traditional IP Network Address Translator (Traditional NAT)
- RFC 2663 “IP Network Address Translator (NAT) Terminology and Considerations”
- BCP 127 “Network Address Translation (NAT) Behavioral Requirements for Unicast UDP”
- Un NAT mapea direcciones entre dos dominios
- Se habla de NATs y NAPTs aunque por extensión se les suele llamar a ambos NATs
- Se dice que hace *transparent routing,* enrutando paquetes entre dos dominios
- Rompen el funcionamiento extremo-a-extremo de la Internet
- Eso va a dar problemas a aplicaciones, así como al despliegue de nuevas
- Veremos varios escenarios con ejemplos

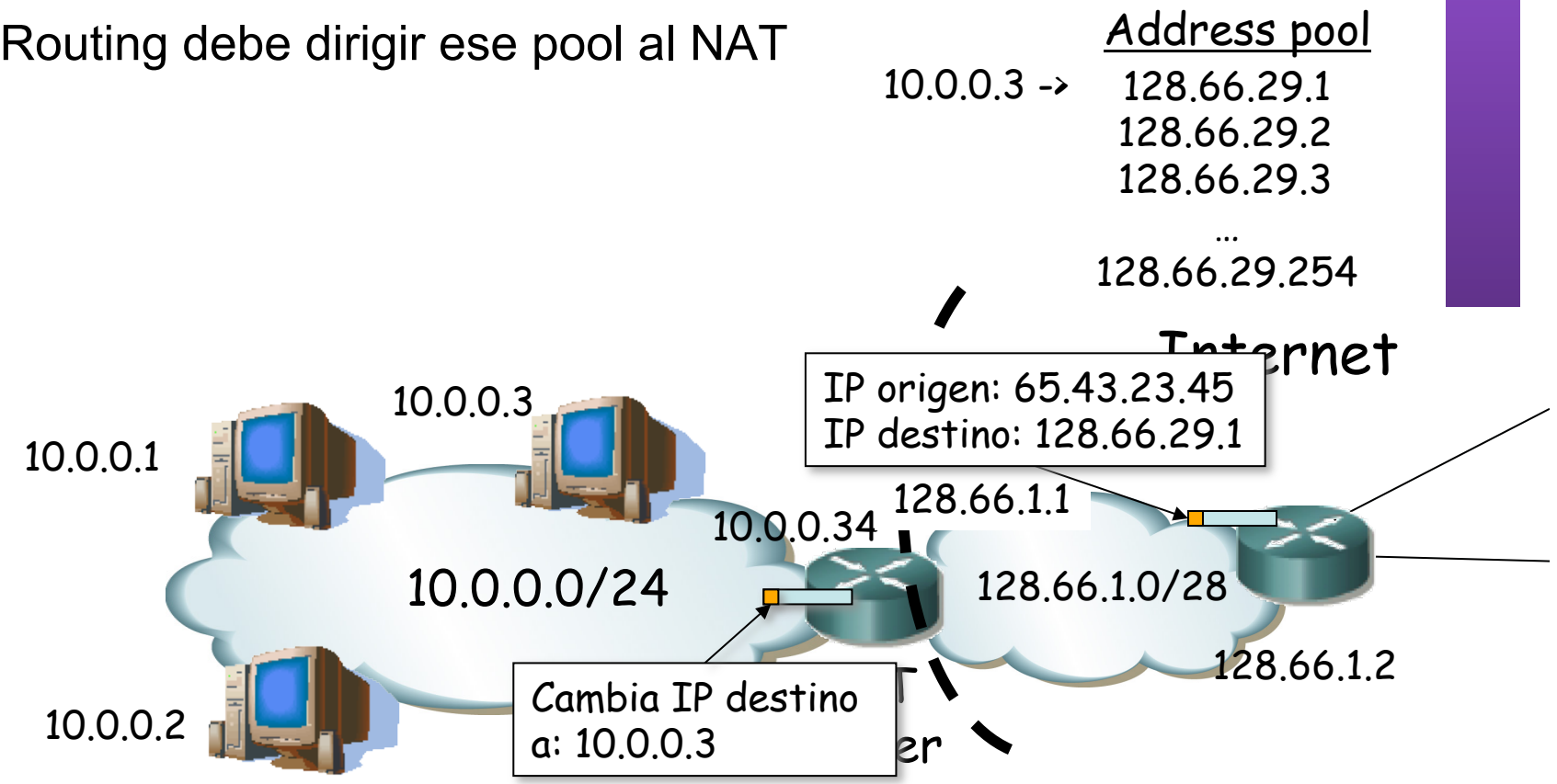
NATs

- 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 (. . .)



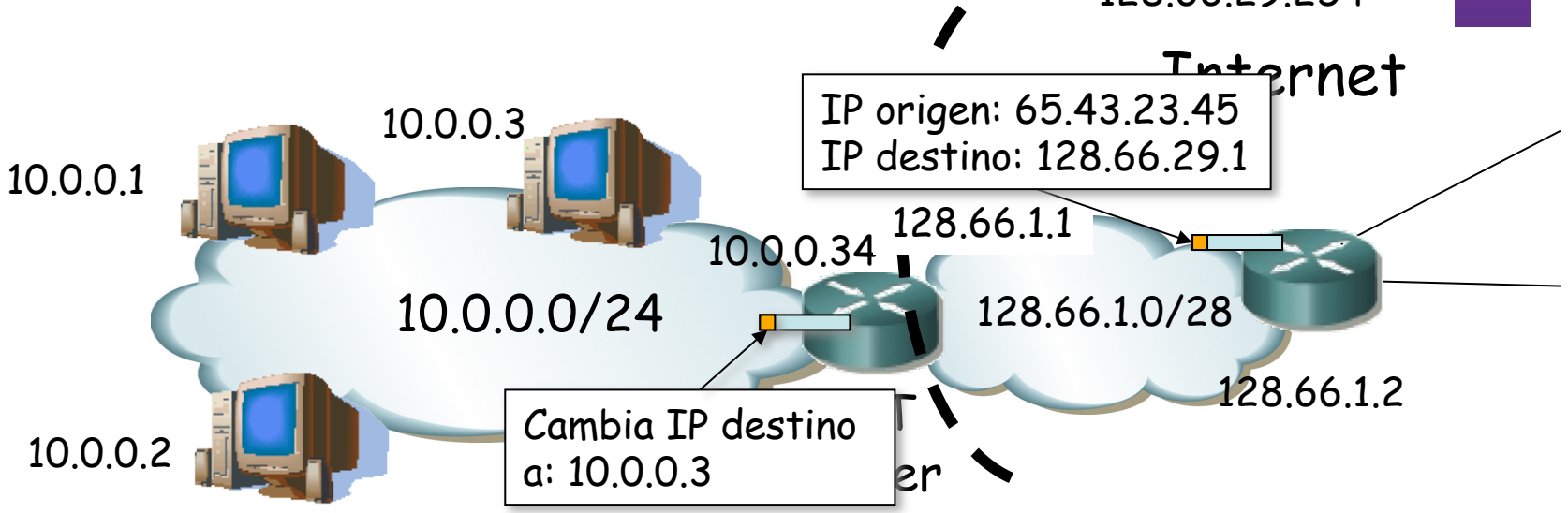
NATs

- 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



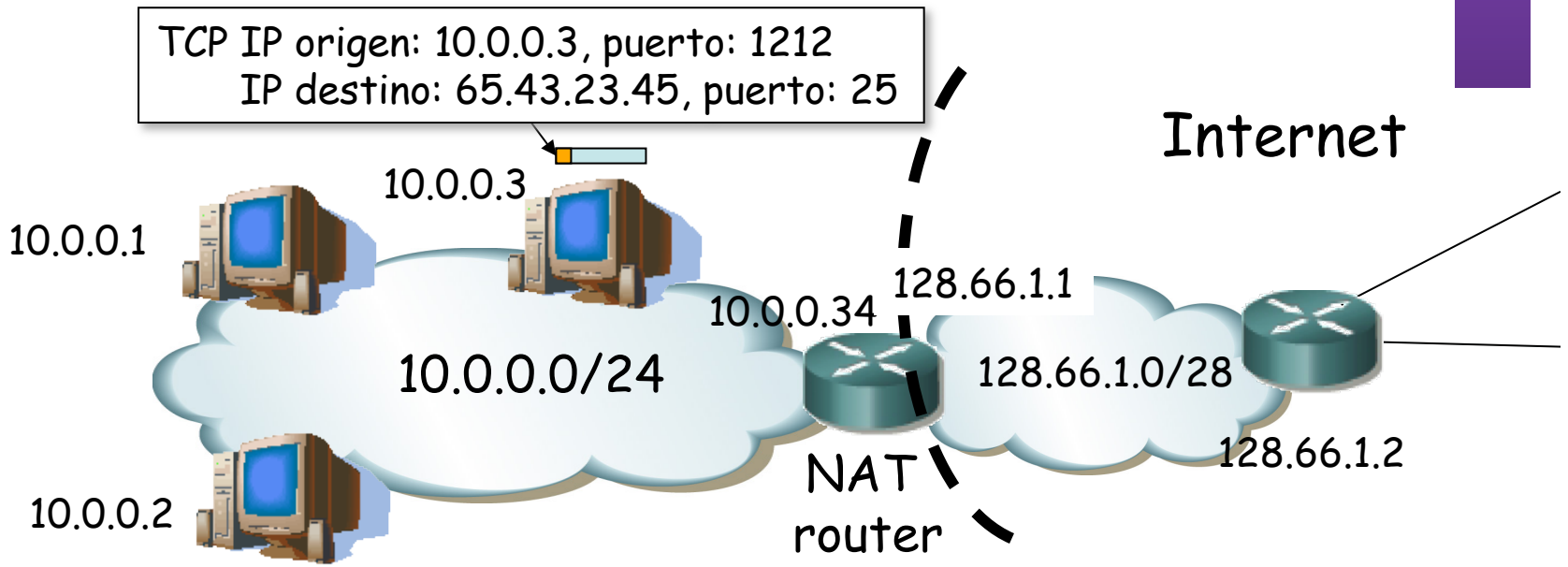
NAPT

- 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)
  - El concepto de sesión a nivel de aplicación puede diferir e incluir varias de éstas
  - En TCP termina tras intercambio de FINs/RST aunque pueden perderse y se mantiene durante un tiempo (recomendado 4min)
  - 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 (. . .)

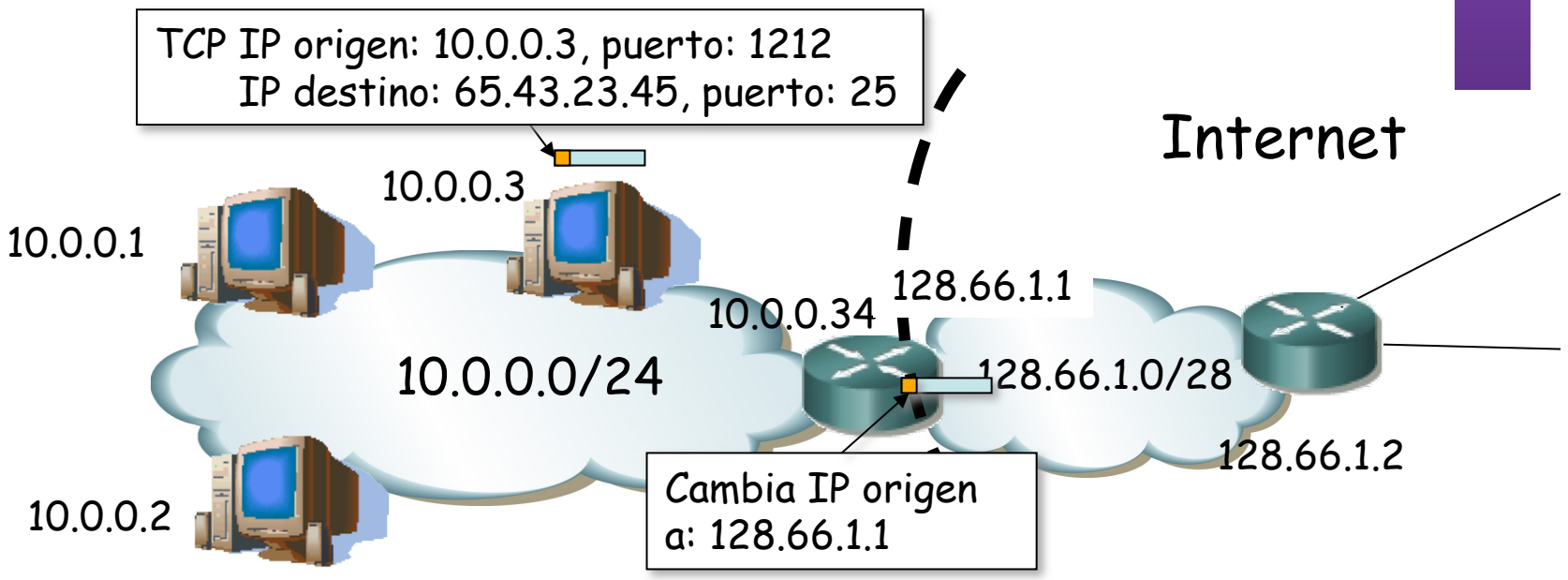
Proto.	Interno	Pública	Exterior



NAPT

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

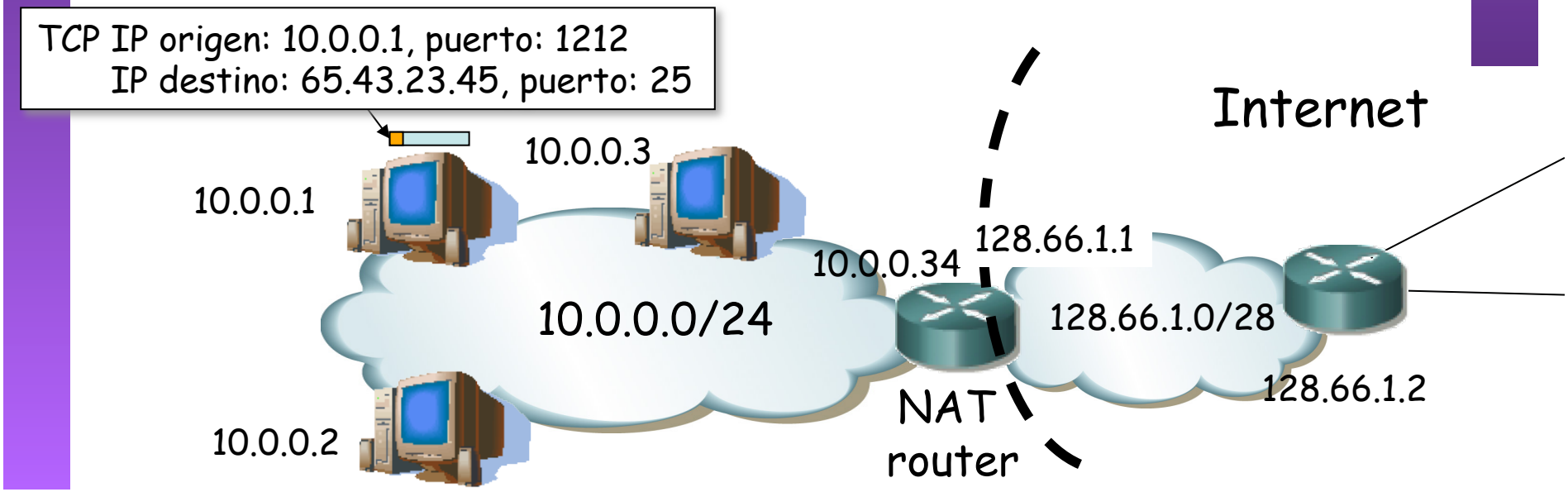
Proto.	Interno	Pública	Exterior
TCP	10.0.0.3:1212	128.66.1.1:1212	65.43.23.45:25



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 (. . .)

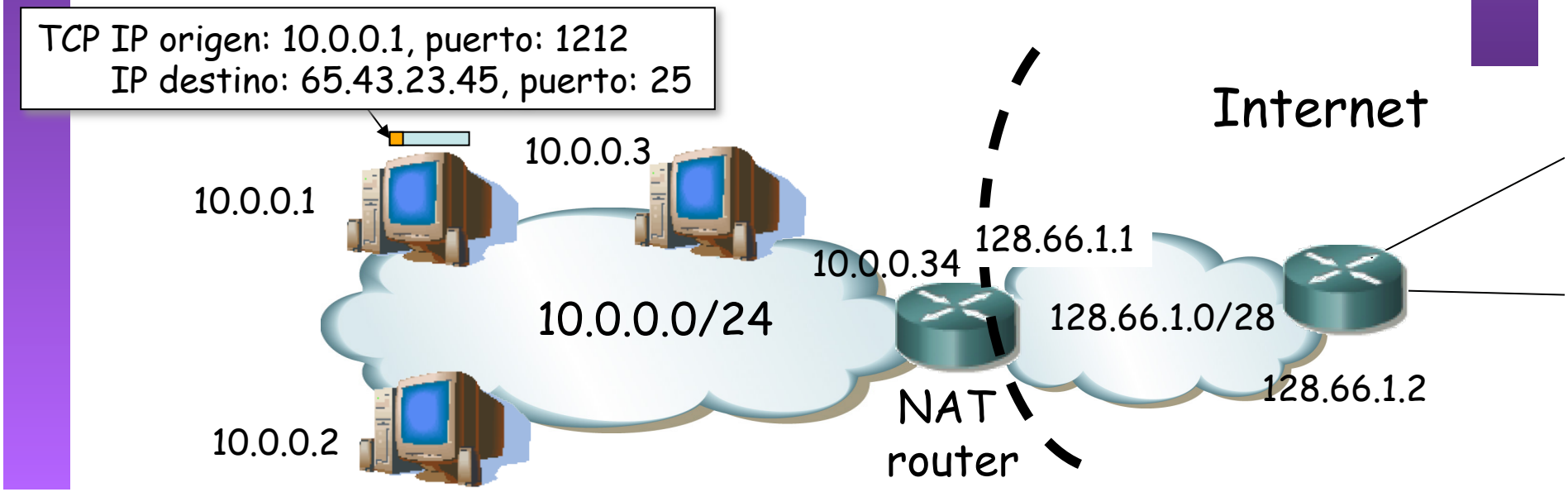
Proto.	Interno	Pública	Exterior
TCP	10.0.0.3:1212	128.66.1.1:1212	65.43.23.45:25



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 (. . .)

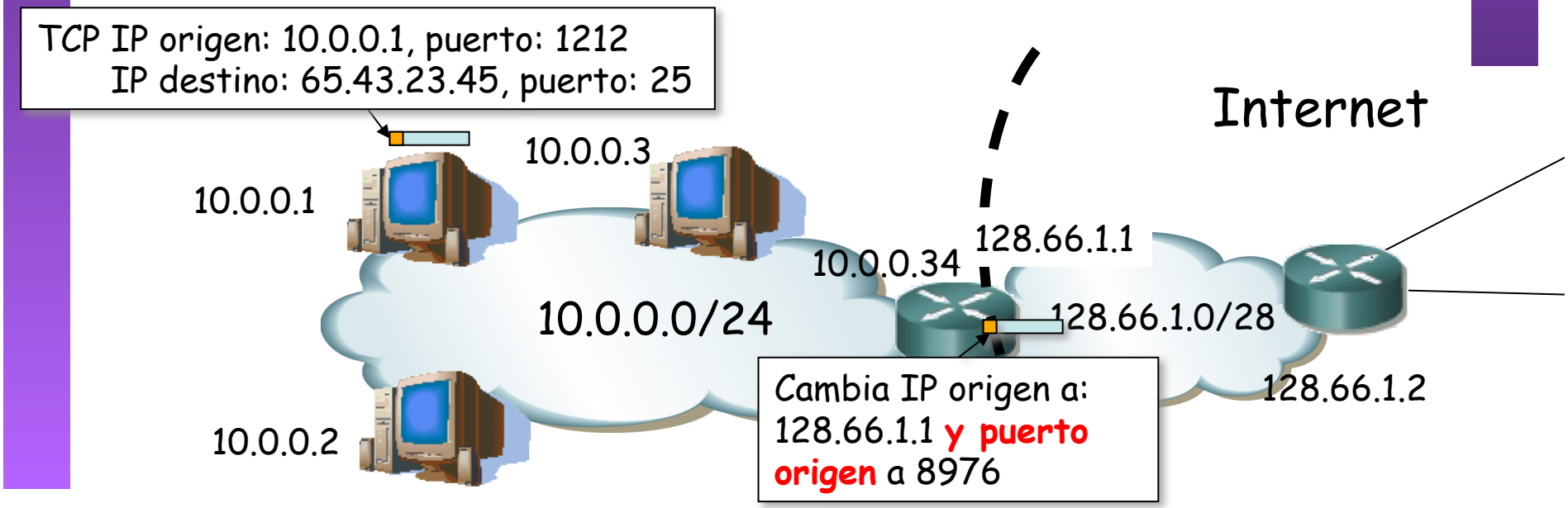
Proto.	Interno	Pública	Exterior
TCP	10.0.0.3:1212	128.66.1.1:1212	65.43.23.45:25
TCP	10.0.0.1:1212	128.66.1.1:1212	65.43.23.45:25



NAPT

- El NAPT va a cambiar también el puerto origen

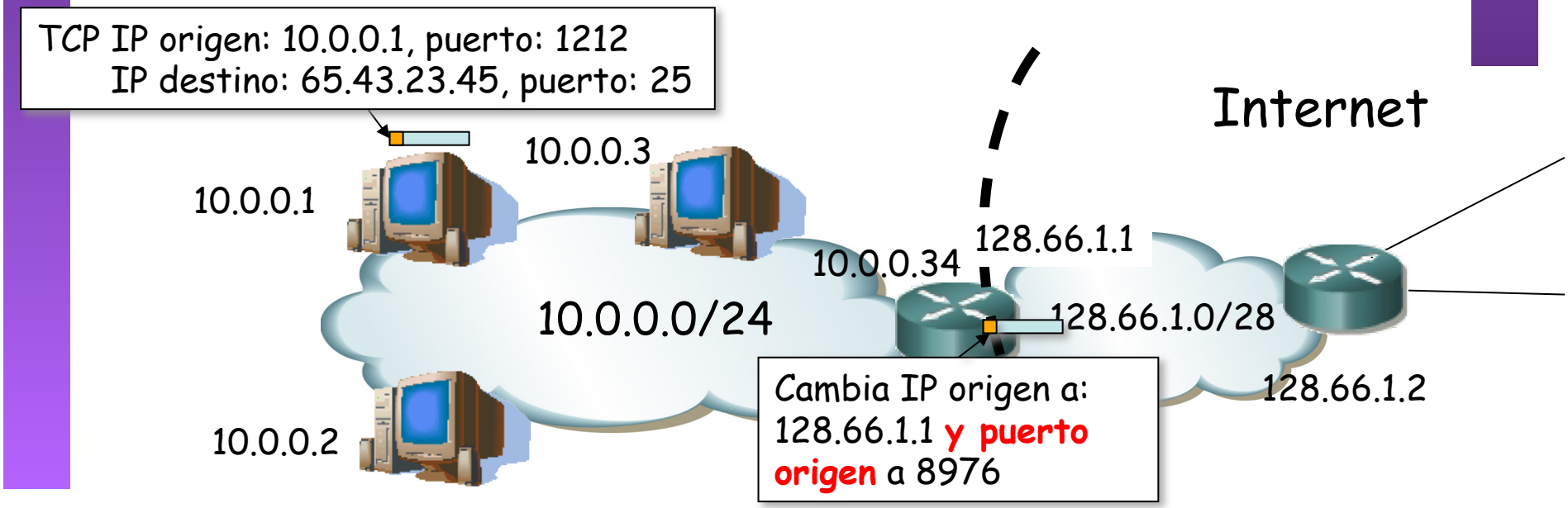
Proto.	Interno	Pública	Exterior
TCP	10.0.0.3:1212	128.66.1.1:1212	65.43.23.45:25
~~TCP~~	~~10.0.0.1:1212~~	~~128.66.1.1:1212~~	~~65.43.23.45:25~~
TCP	10.0.0.1:1212	128.66.1.1:**8976**	65.43.34.45:25



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)

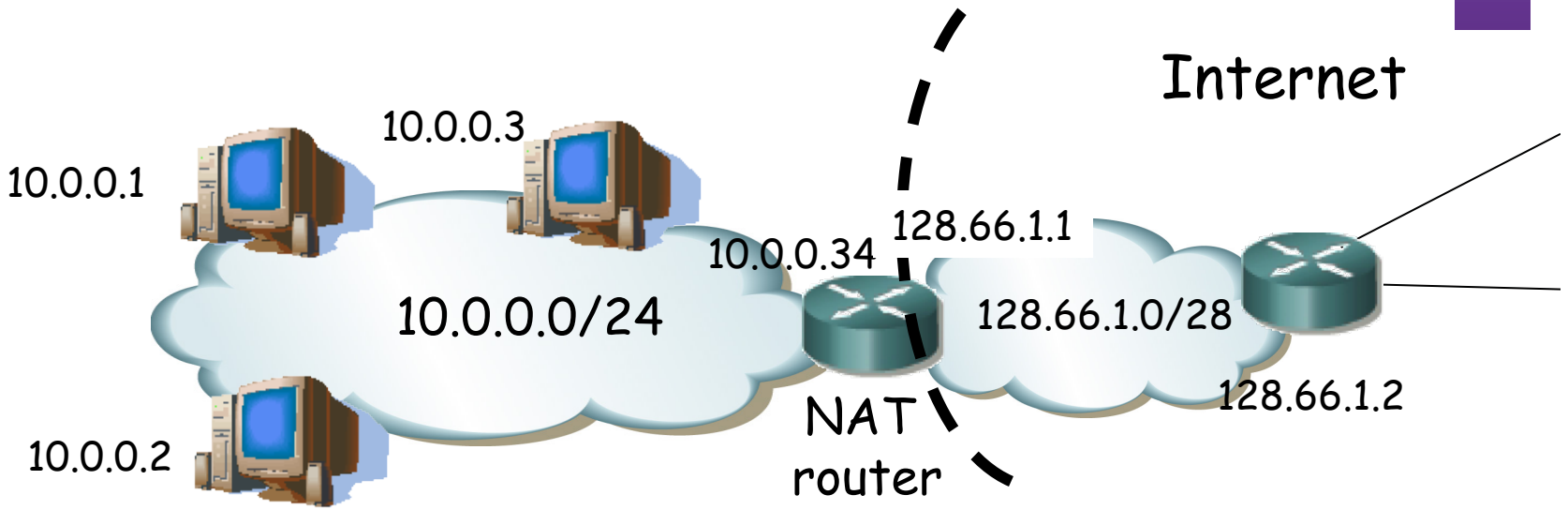
Proto.	Interno	Pública	Exterior
TCP	10.0.0.3:1212	128.66.1.1:1212	65.43.23.45:25
~~TCP~~	~~10.0.0.1:1212~~	~~128.66.1.1:1212~~	~~65.43.23.45:25~~
TCP	10.0.0.1:1212	128.66.1.1:**8976**	65.43.34.45:25



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



NATs y aplicaciones

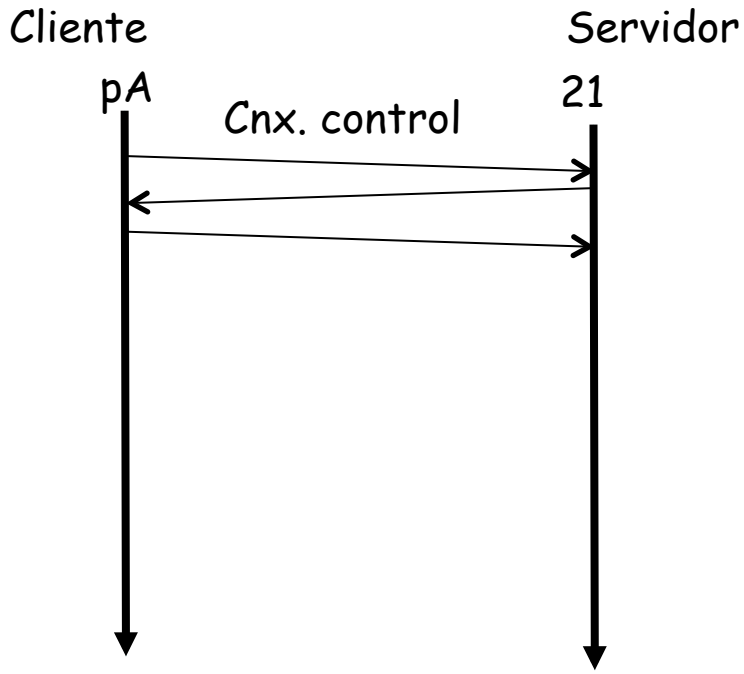
- Problemas con logs y estadísticas en servidores
  - El mismo host puede aparecer en el exterior con diferente dirección en diferente momento
  - Varios hosts pueden aparecer con la misma dirección
  - Con datos de red+transporte no se pueden distinguir
  - Dificulta hacer estadísticas por usuario o identificar responsables de abusos
- Problemas con aplicaciones que
  - En la comunicación de datos hablan de direcciones IP y/o puertos
  - Esa información es necesaria para establecer otras sesiones
  - Se emplean entonces ALGs (…)

ALGs

- *Application Spacific 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

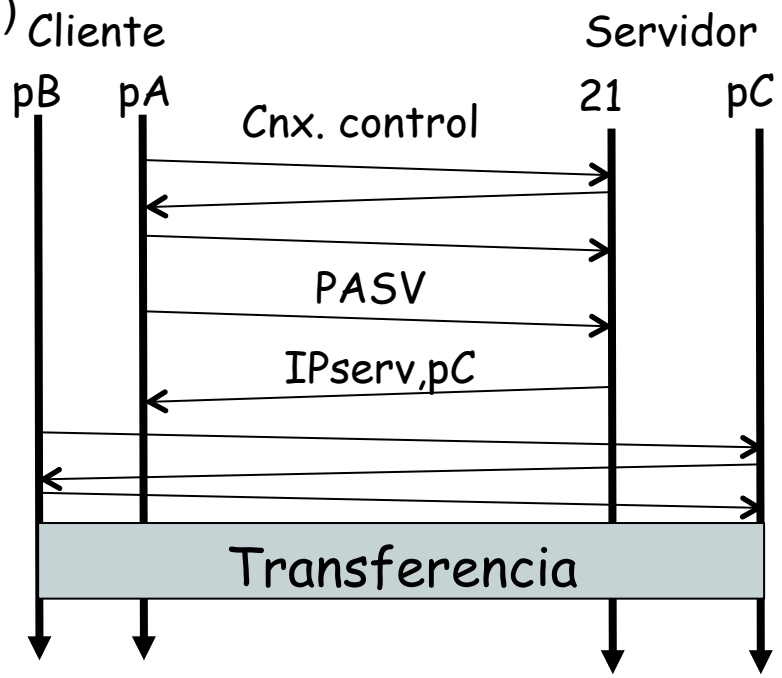
FTP: File Transfer Protocol

- RFC 959
- Servidor emplea puerto TCP 21
- Cliente establece una conexión de control con el servidor



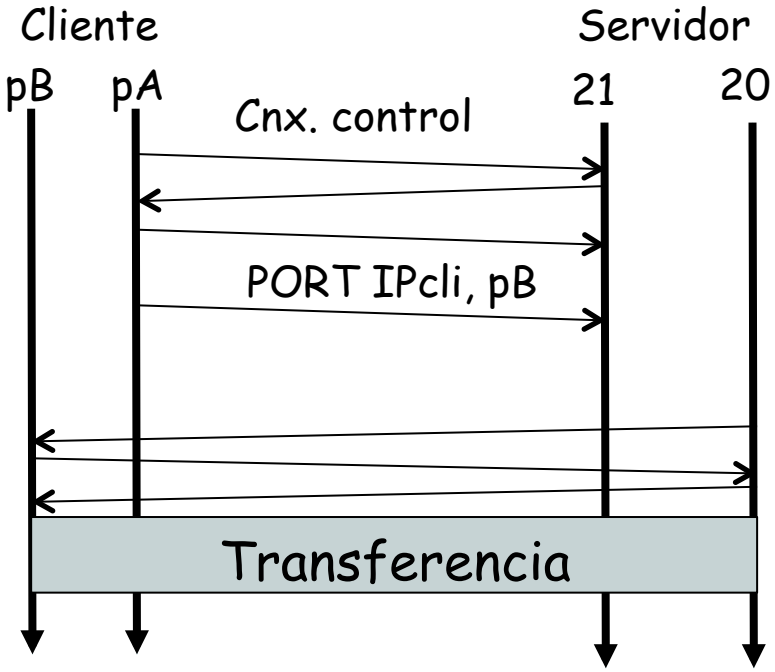
FTP: File Transfer Protocol

- 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



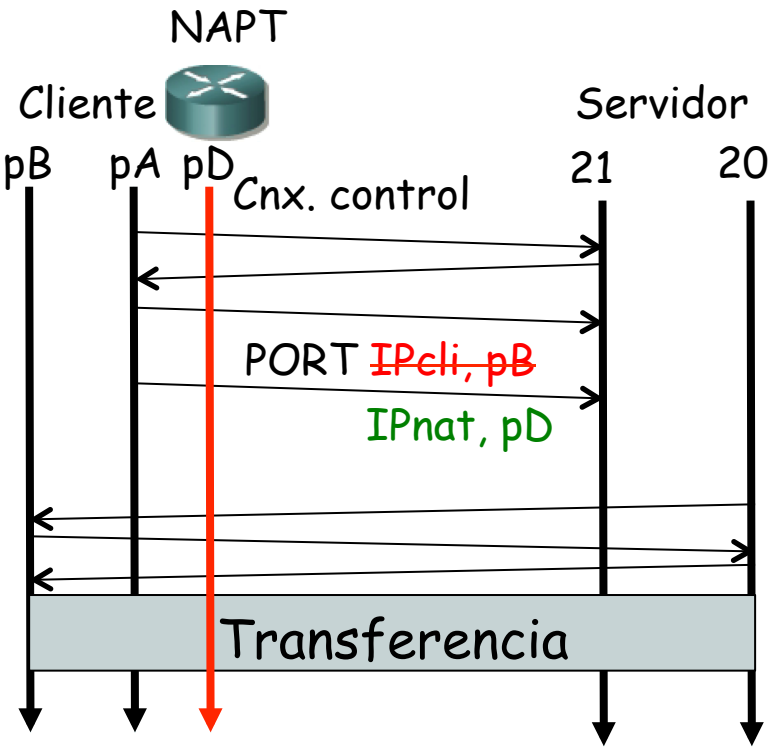
FTP: File Transfer Protocol

- 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

- El cliente ha especificado un puerto local, así como su dirección
- NAT debe seguir el stream de datos para reconocer el comando
- Reconstruir el stream si el comando está fragmentado
- Modificarlo con dirección externa y puerto que seleccione
- Introducir mapeo para esa (dirección,puerto)
- 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

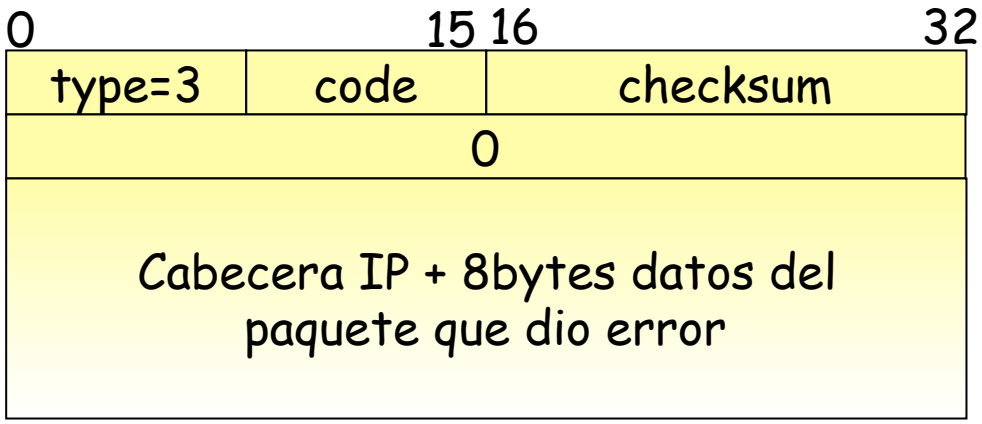


NATs y detalles de IP

- Opciones como *Record Route, Strict/Loose Source Route* puede traducir o no las direcciones
- No soporta fragmentos pues solo el primero lleva al cabecera de transporte
- Cambio en dirección IP requiere recalcular checksum IP
- También requiere recalcular checksum TCP/UP pues protege también a las direcciones IP
- Empleando direccionamiento privado+NAT se puede cambiar de ISP sin requerir redireccionar los hosts

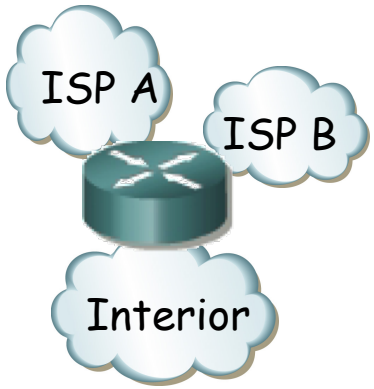
NAT e ICMP

- Ejemplo: envío de un ICMP *query*
  - No hay puertos, pero hay un identificador
  - Se cambia el identificador
- Ejemplo: recepción de ICMP de puerto inalcanzable
  - Viene dirigido a la dirección IP pública
  - El NAT debe reconocer el paquete UDP en el error y hacer la traslación en el paquete IP y en el UDP
  - Eso incluye corregir dos checksums



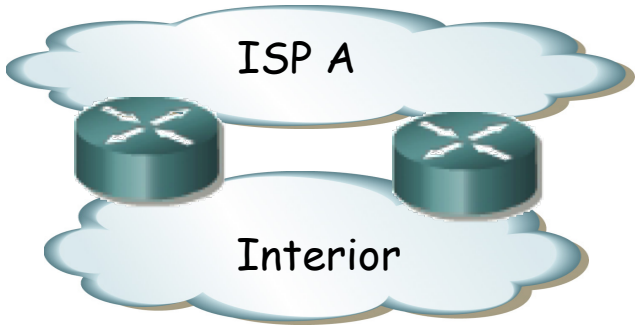
Protección y NATs

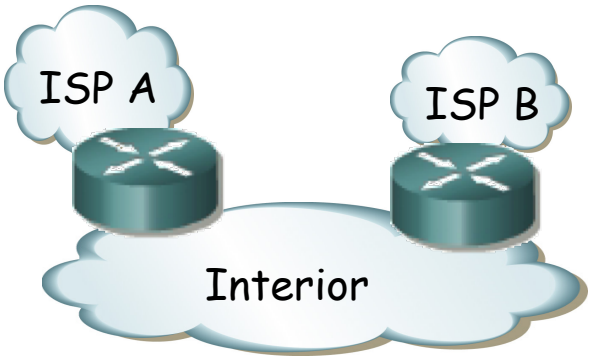
- Mantiene el mapeo para una sesión así que todo el tráfico debe pasar por él
- No debe haber asimetría, los dos sentidos de la comunicación deben pasar por el NAT
- Normalmente el NAT está en la frontera de un *stub*
- Es un punto único de fallo
- ¿ Multihomed ?
  - Protección con enlaces a varios operadores
  - La dirección externa será diferente así que los mapeos fallarán salvo que se enrute de vuelta al NAT por el segundo operador



Protección y NATs

- Mantiene el mapeo para una sesión así que todo el tráfico debe pasar por él
- No debe haber asimetría, los dos sentidos de la comunicación deben pasar por el NAT
- Normalmente el NAT está en la frontera de un *stub*
- Es un punto único de fallo
- ¿ Múltiples NATs ?
  - Protección ante fallo del equipo y de enlace si van a diferente ISP
  - Podría emplearse para cada sesión el más cercano al destino
  - Si uno falla debería encaminarse el tráfico por el otro
  - Las sesiones entonces deben estar sincronizadas
  - De nuevo problema con la dirección externa





Seguridad y NATs

- Hosts internos no son directamente accesibles si no inician ellos la comunicación
- Cambian direcciones y puertos así que no funcionan con mecanismos de seguridad basados en ellos (IPSec)
- Sí funcionan con aplicaciones que no basen la seguridad en direcciones IP o puertos (SSH, TLS)

Protocolos sobre IP

- Campo protocolo 1 byte (256 valores)
- Hay ya 142 reservados (2013)
- Pero un NAPT soporta traslación solo para TCP/ UDP/ICMP
- Con el despliegue que hay de NATs, el empleo de otros protocolos hoy en día no tendría alcance global
- Nuevos protocolos acaban implementándose sobre UDP que da un servicio de datagramas como IP

IPv6

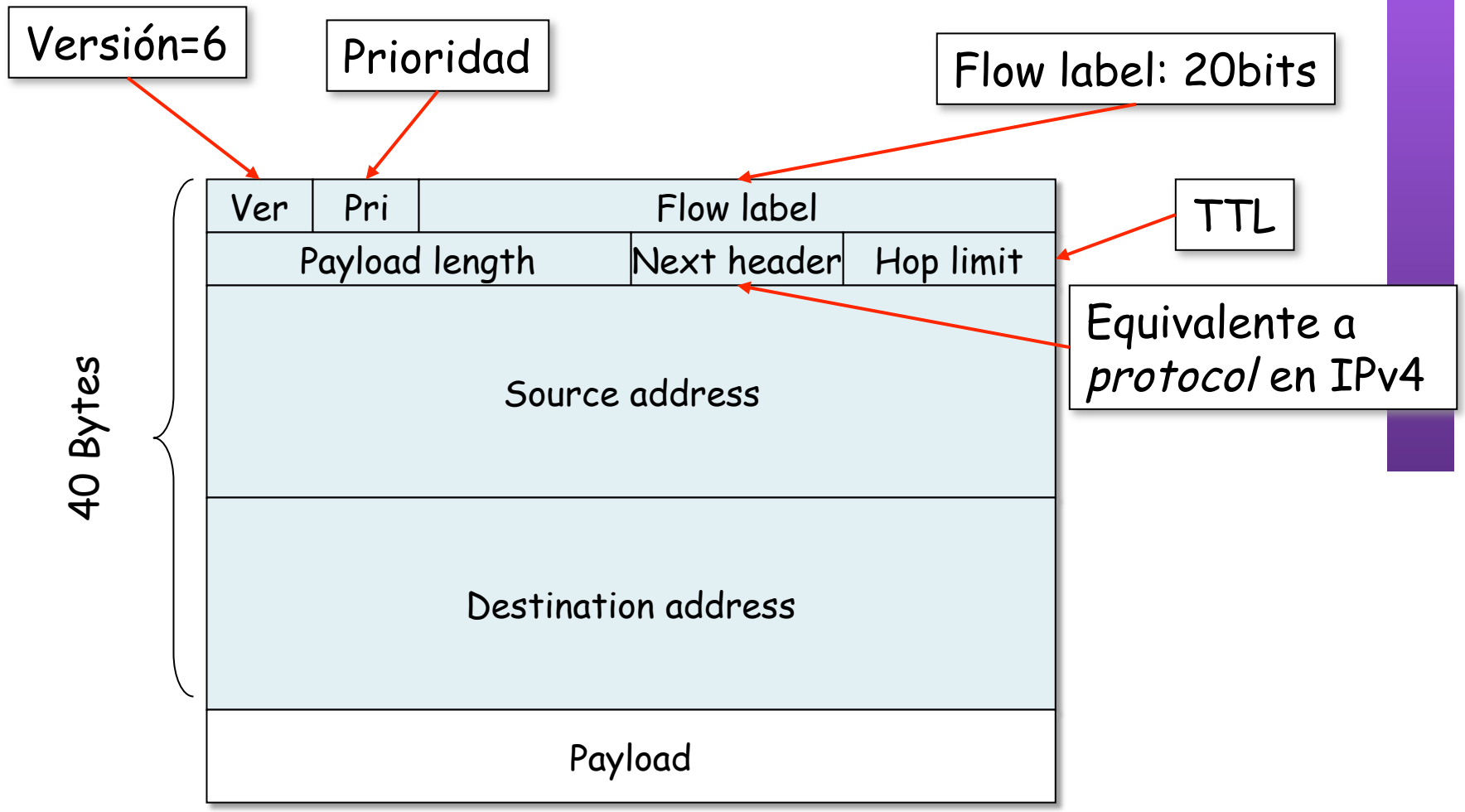
IPv6

- **Motivación inicial:**
  - El espacio de direcciones de 32bits se estaba (y se está) agotando
- **Motivación adicional:**
  - Formato de la cabecera que ayude en el procesamiento, acelerándolo
    - Que la cabecera no sea de tamaño variable
    - Eliminar el checksum
    - Eliminar la posibilidad de fragmentación en los routers
  - Cambios en la cabecera que faciliten ofrecer QoS

Cambios con IPv6

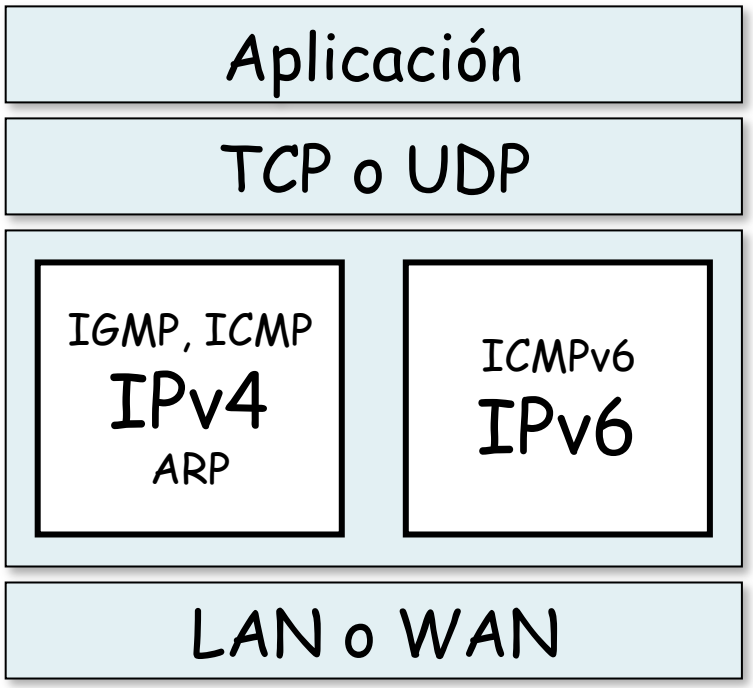
- Direcciones de 128bits
- Introduce un nuevo tipo de direcciones: ***anycast***
- Cabecera de **tamaño fijo** (40 Bytes)
- Para QoS: posibilidad de etiquetar paquetes como pertenecientes a un "flujo"
- No hay fragmentación y reensamblado
- No hay checksum de la cabecera
- Las opciones aparecen como otro protocolo sobre IP
- Seguridad (IPSec)
- ICMPv6

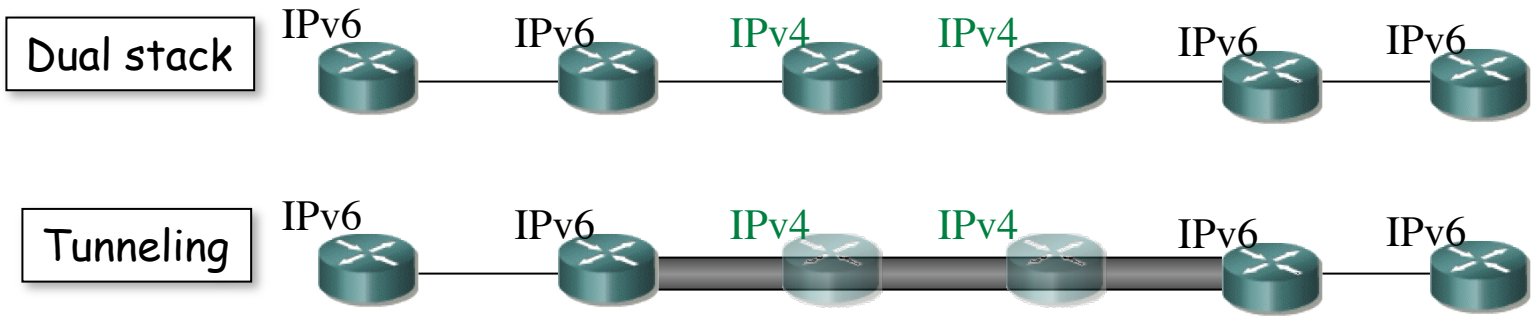
Cabecera IPv6



Transición de IPv4 a IPv6

- Es complejo cambiar los protocolos del nivel de red
- Alternativas:
  - Flag day
    - ¿¿Con cientos de millones de máquinas??
  - Dual-Stack
    - Nodos IPv4/IPv6
    - Problema: Pérdida de campos
  - Tunneling
  - Header translation





Resumen

- Escasez de direcciones:
  - Mal reparto
  - Uso esporádico
- Asignación dinámica a host: DHCP
- Traslación de direcciones en router: NAT
- Aumentar el espacio de direcciones: IPv6