Soluciones a los problemas de direccionamiento

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

Laboratorio de Programación de Redes
3º Ingeniería Técnica en Informática de Gestión

Objetivo

- Ver diferentes soluciones al problema de la escasez de direcciones IP

Contenido

- Introducción
- El problema
- Algunas soluciones
  - DHCP
  - NAT
  - IPv6

Contenido

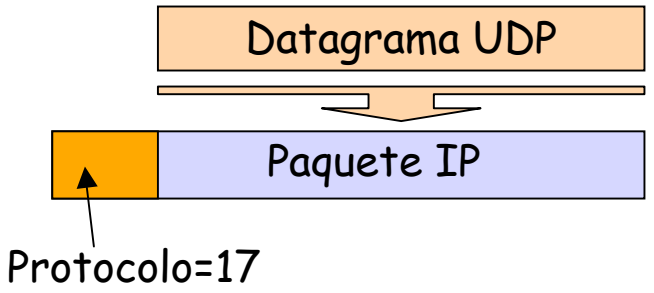
- **Introducción**
- El problema
- Algunas soluciones
  - DHCP
  - NAT
  - IPv6

UDP: User Datagram Protocol

- RFC 768
- Protocolo de transporte simple, sin gran inteligencia
- Servicio “best effort”
- Datagramas
- Los datagramas UDP se pueden:
  - Perder
  - Llegar desordenados a la aplicación
- ¿Transferencia fiable sobre UDP?
  - Añadir fiabilidad en el nivel de aplicación
  - ¡Recuperación ante errores específica de cada aplicación!
- Sin conexión:
  - No hay handshaking entre emisor y receptor
  - Cada datagrama UDP es procesado de forma independiente a los demás
- Empleado frecuentemente para aplicaciones de streaming multimedia
  - Soportan pérdidas
  - Sensibles a la tasa de envío
- Otros usos de UDP:
  - DNS
  - SNMP

UDP: User Datagram Protocol

- ¿Por qué existe UDP?
  - Es simple: no hay que mantener estado
  - Un establecimiento de conexión añadiría retardo no deseado
  - Cabecera pequeña
  - No hay control de congestión: puede enviar tan rápido como desee
- Encapsulado en paquetes IP, protocolo 17
- Cuando un host recibe un datagrama UDP :
  - Comprueba el puerto destino en el mismo
  - Dirige el segmento a la aplicación esperando datos a ese puerto
- Diferentes IP origen o puertos origen van al mismo punto de acceso al servicio (SAP)



Cabecera UDP

Puerto origen

- Normalmente lo escoge el sistema operativo
- Suele ser un puerto efímero

Puerto destino

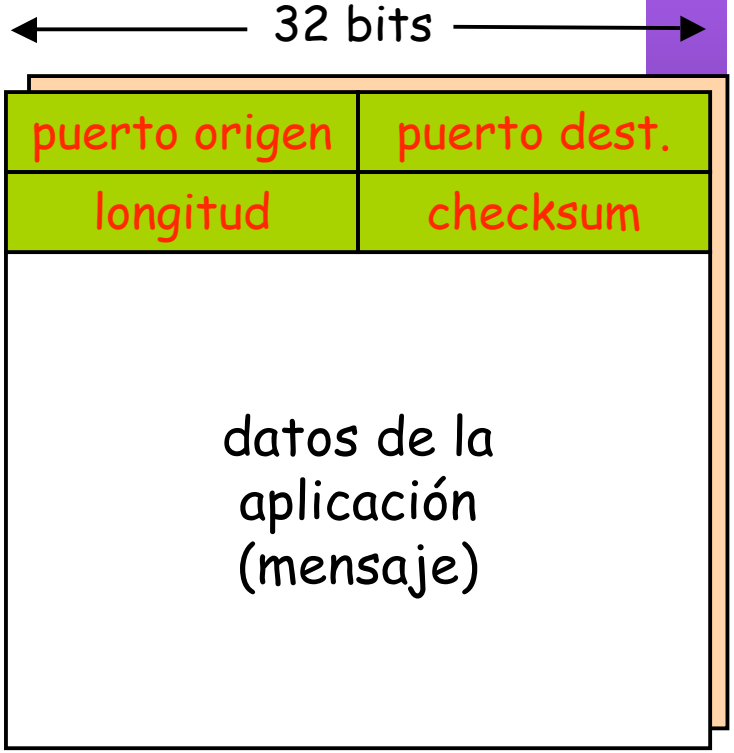
- Puerto del servidor
- *Well known* o se debe conocer por algún medio

Respuesta servidor→cliente

- Sentido contrario
- Puerto origen es el del servidor (*well known*)
- Puerto destino el efímero del cliente

Longitud

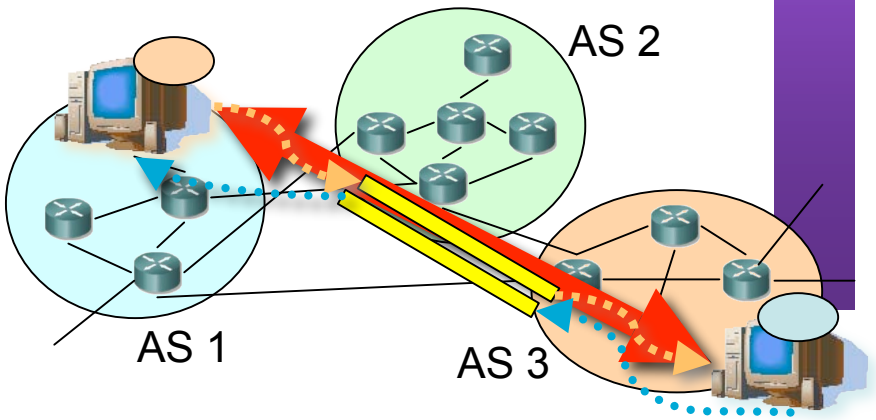
- Bytes del datagrama UDP

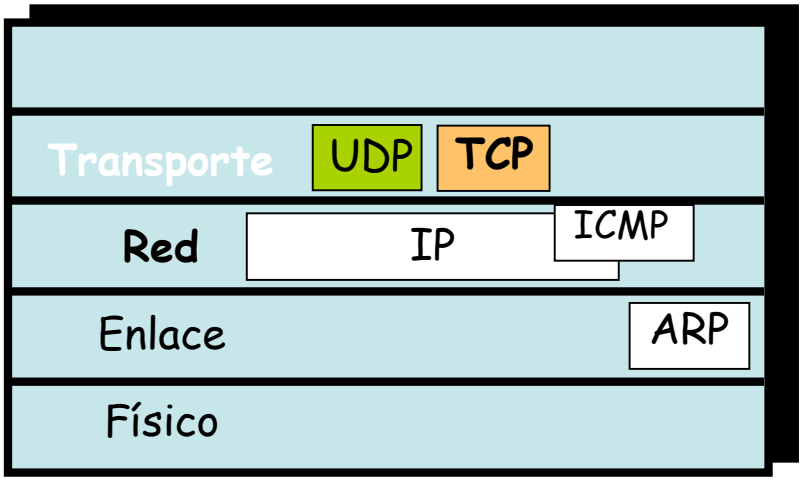


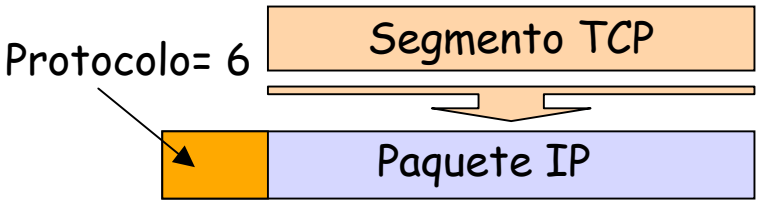
TCP

- *Transmission Control Protocol*
- Nivel de transporte
- RFCs 793, 1122, 1323, 2018, 2581
- Orientado a conexión
- Flujo de datos:
  - *Stream* de bytes
  - Fiable
  - Ordenado
  - Full duplex

- Control de flujo
  - Evitar congestionar al receptor
- Control de congestión
  - Evitar congestionar la red

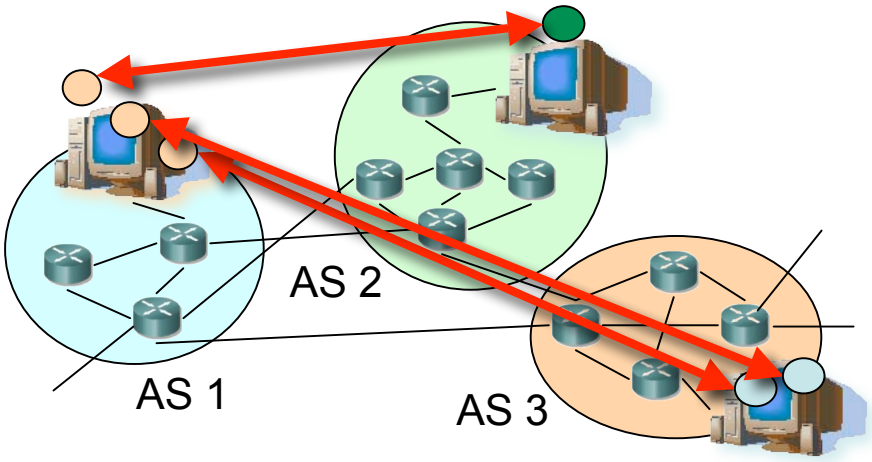


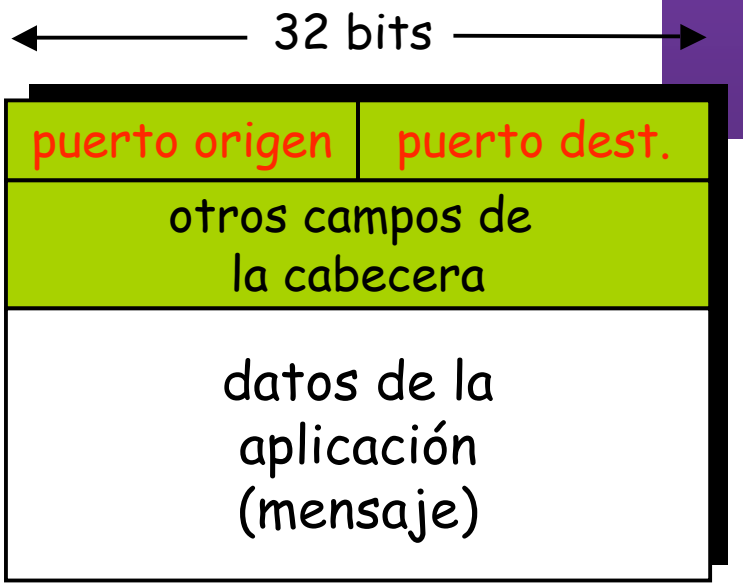




Demultiplexación con conexión

- Conexión identificada por 2 sockets
- Cada socket identificado por: Dirección IP y Puerto TCP
- Es decir, la conexión viene identificada por:
  - Dirección IP (1), Puerto TCP (1)
  - Dirección IP (2), Puerto TCP (2)
- El receptor emplea la cuaterna para demultiplexar
- Cada host soporta múltiples conexiones TCP simultáneas
- Con que uno de los 4 valores sea diferente la conexión ya es diferente
- Well-known ports, registrados, efímeros, igual que para UDP





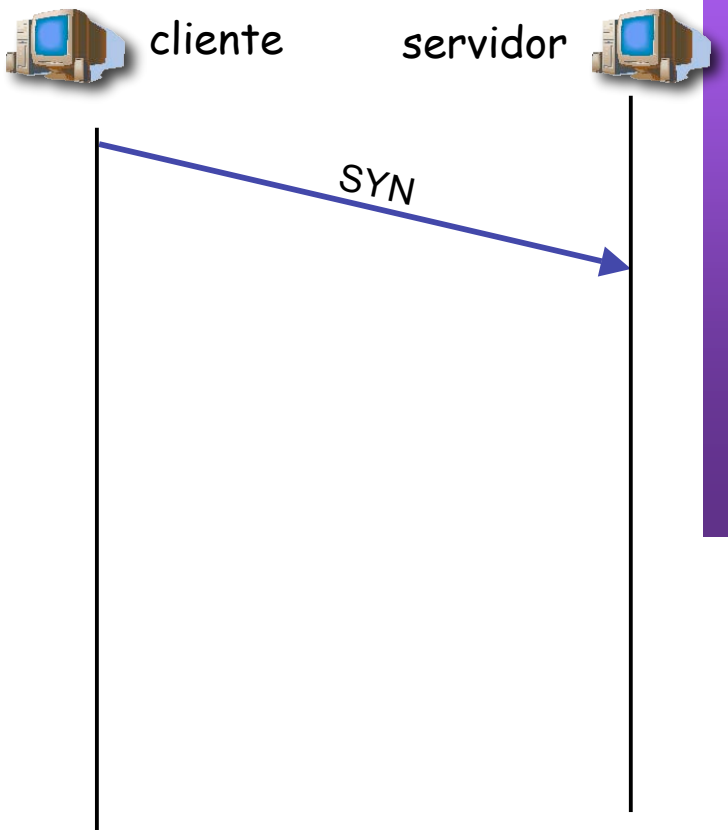
Gestión de conexiones

Estableciendo una conexión:

- *Three way handshake*

Paso 1:

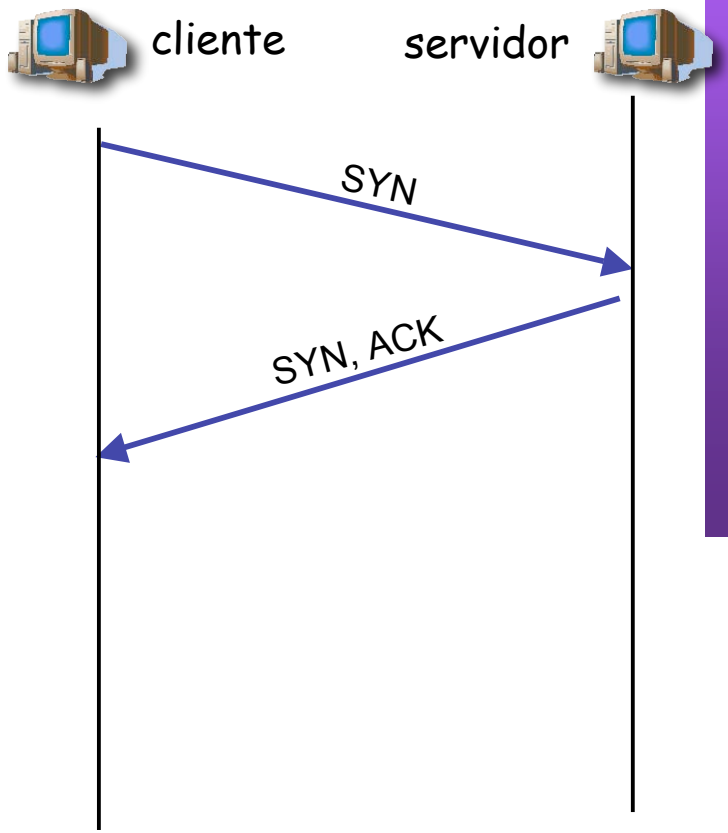
- El extremo **cliente** envía un segmento solicitando una conexión al servidor
- El segmento **no tiene datos**, solo cabecera
- **SYN**



Gestión de conexiones

Paso 2:

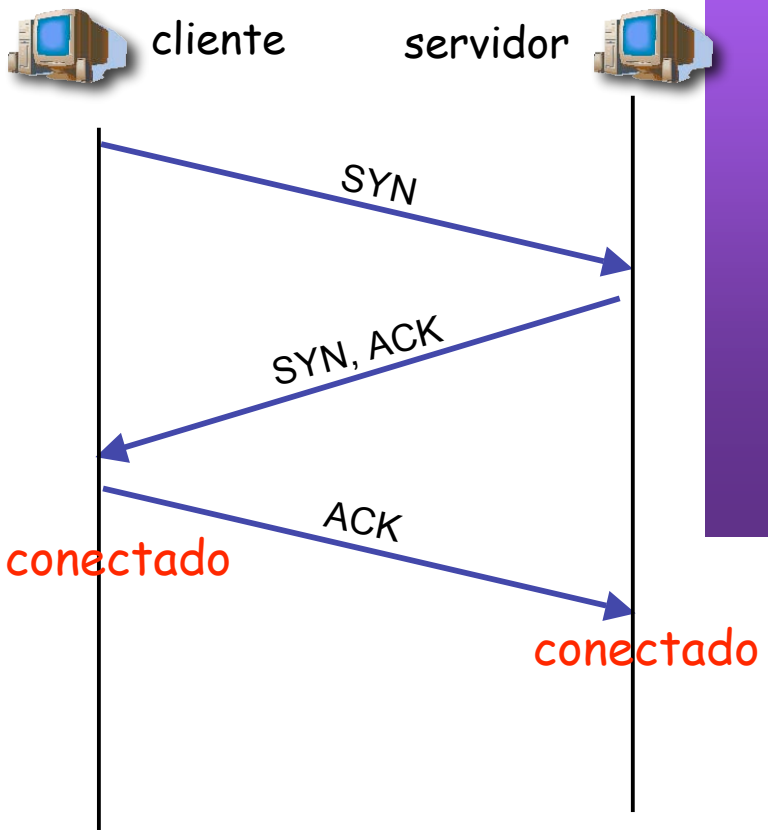
- El extremo **servidor** envía un segmento al cliente confirmando (acknowledgement) la recepción del SYN
- En el mismo segmento el servidor indica su deseo de establecer la conexión (SYN)
- El segmento **no tiene datos**, solo cabecera



Gestión de conexiones

Paso 3:

- El extremo **cliente** envía una confirmación al SYN del servidor
- El segmento **no tiene datos**, solo cabecera
- Conexión establecida



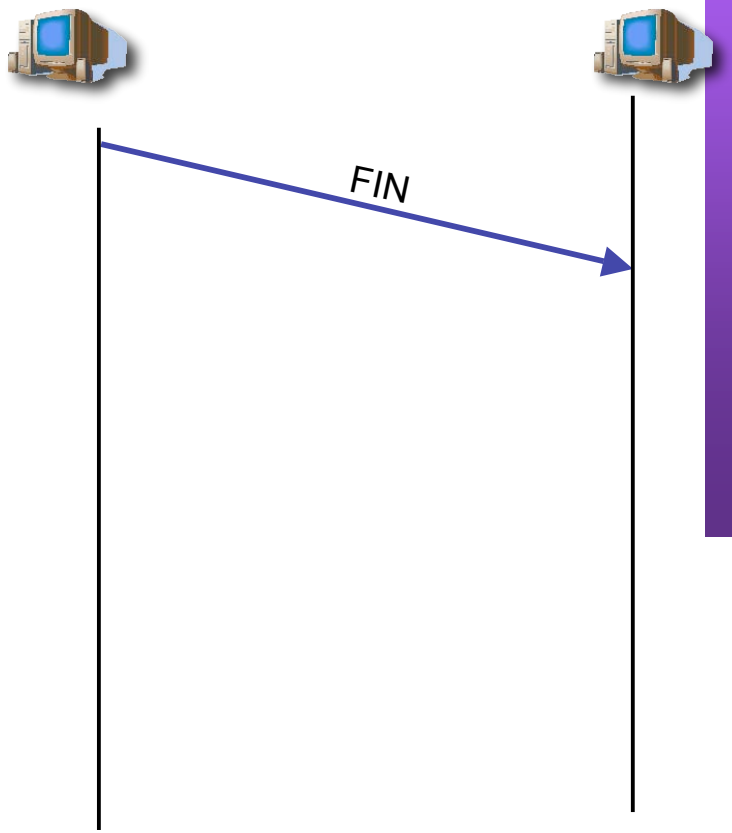
Transferencia de datos…

Gestión de conexiones

Cerrando una conexión

Paso 1:

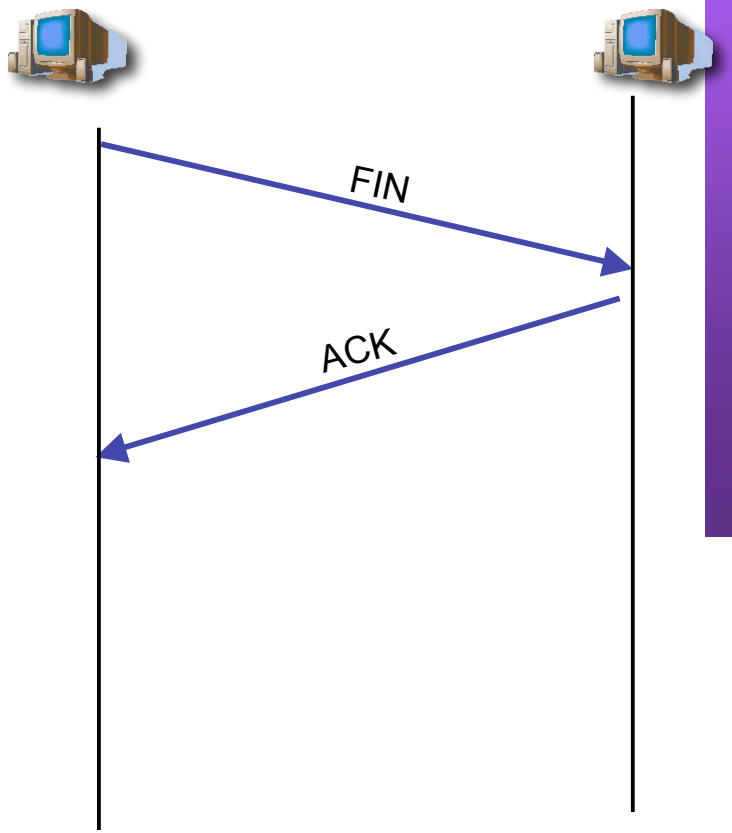
- **Un extremo** envía un segmento solicitando el cierre de la conexión
- El segmento **no tiene datos**, solo cabecera
- **FIN**



Gestión de conexiones

Paso 2:

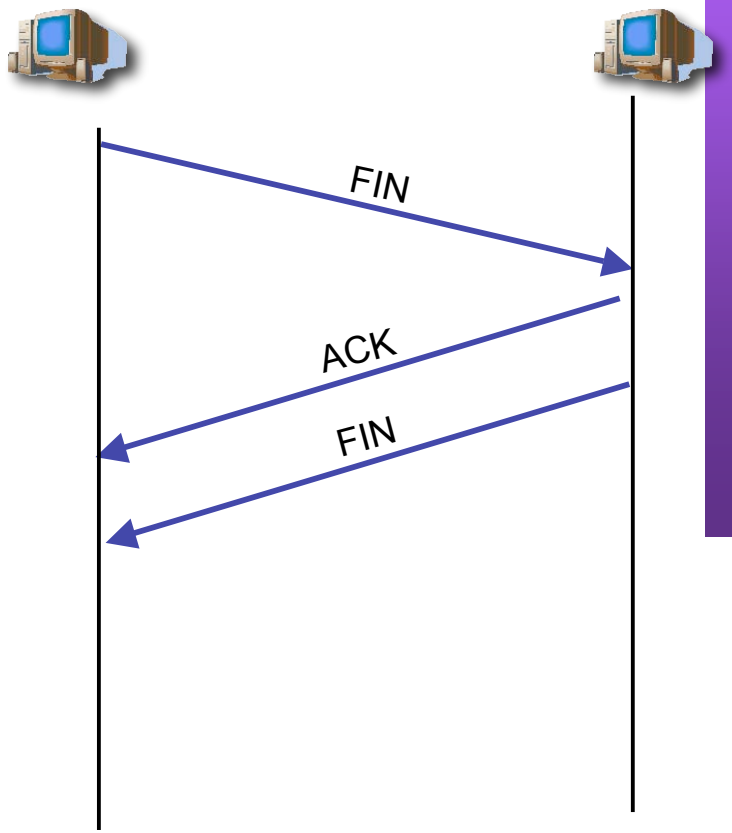
- El otro extremo confirma (ACK) la recepción del FIN
- El extremo que ha enviado el FIN ya no puede enviar más datos nuevos
- **Cierre solo de un sentido** de la comunicación



Gestión de conexiones

Paso 3:

- El otro extremo envía un segmento solicitando el cierre de la conexión
- El segmento no tiene datos, solo cabecera



Gestión de conexiones

Paso 4:

- Confirmación de ese segundo FIN
- Por si ese último ACK se pierde, el que lo envió espera un tiempo (podría tener que volverlo a enviar)
- Conexión cerrada

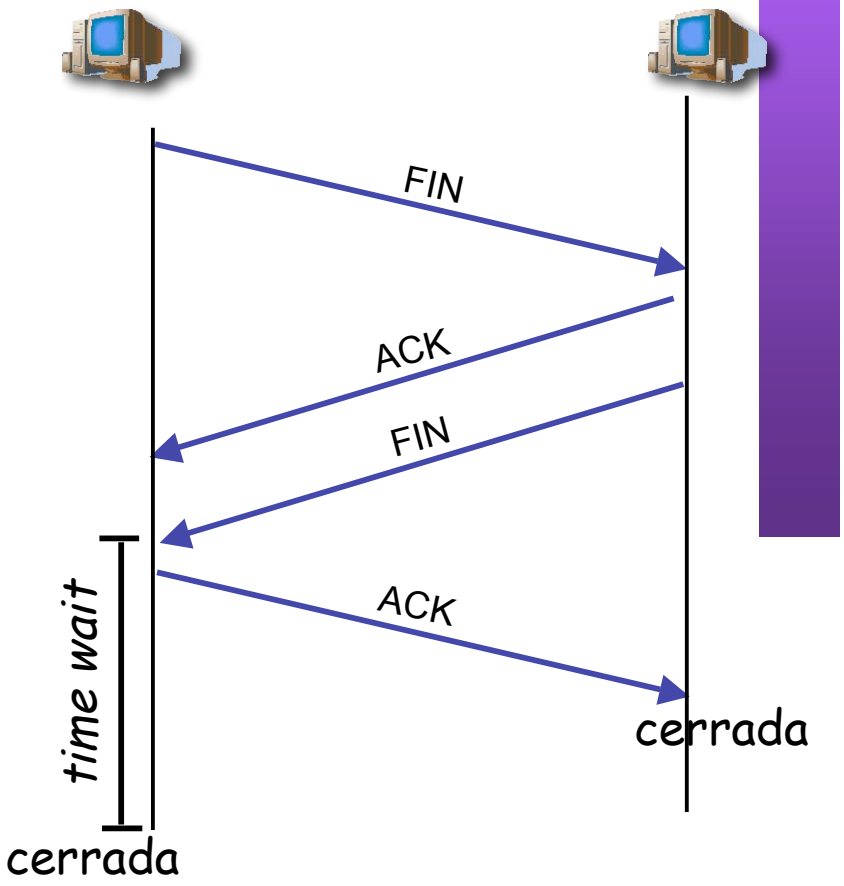
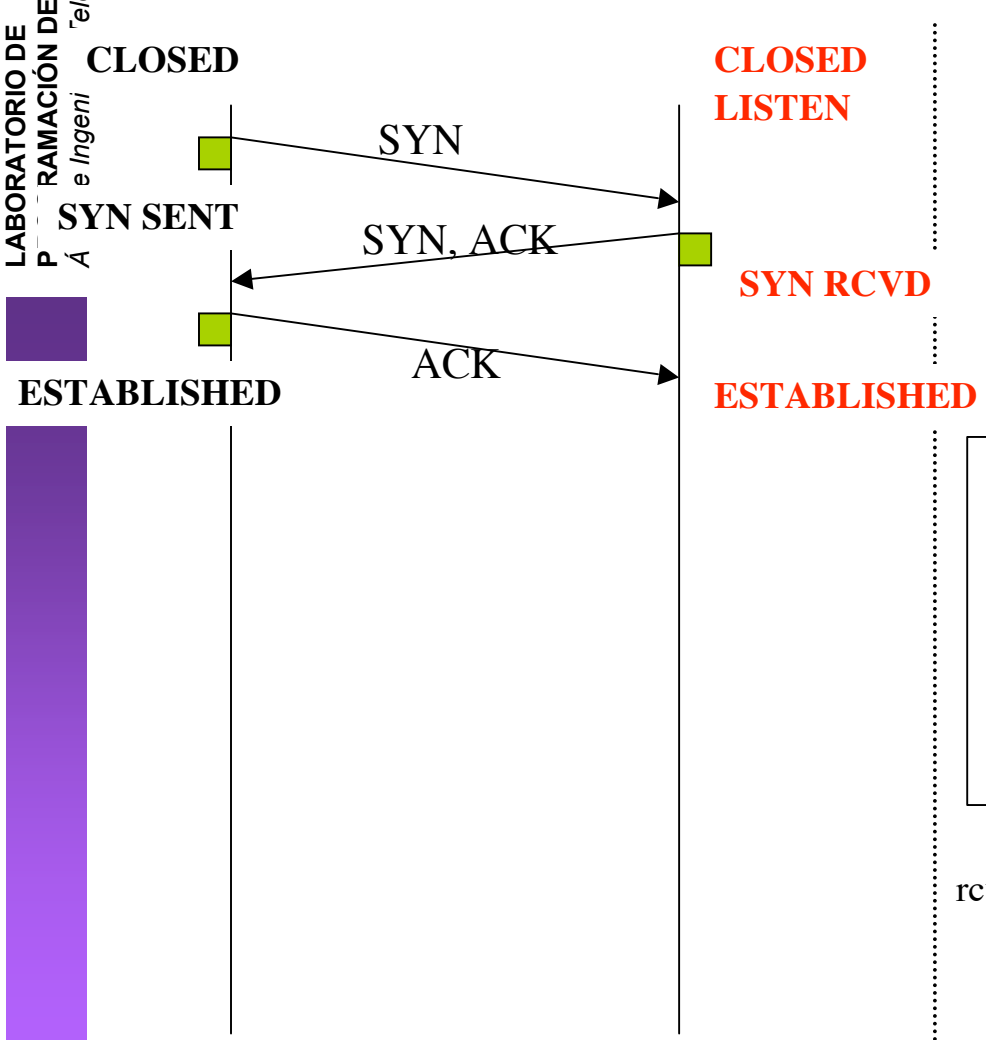


Diagrama de estados



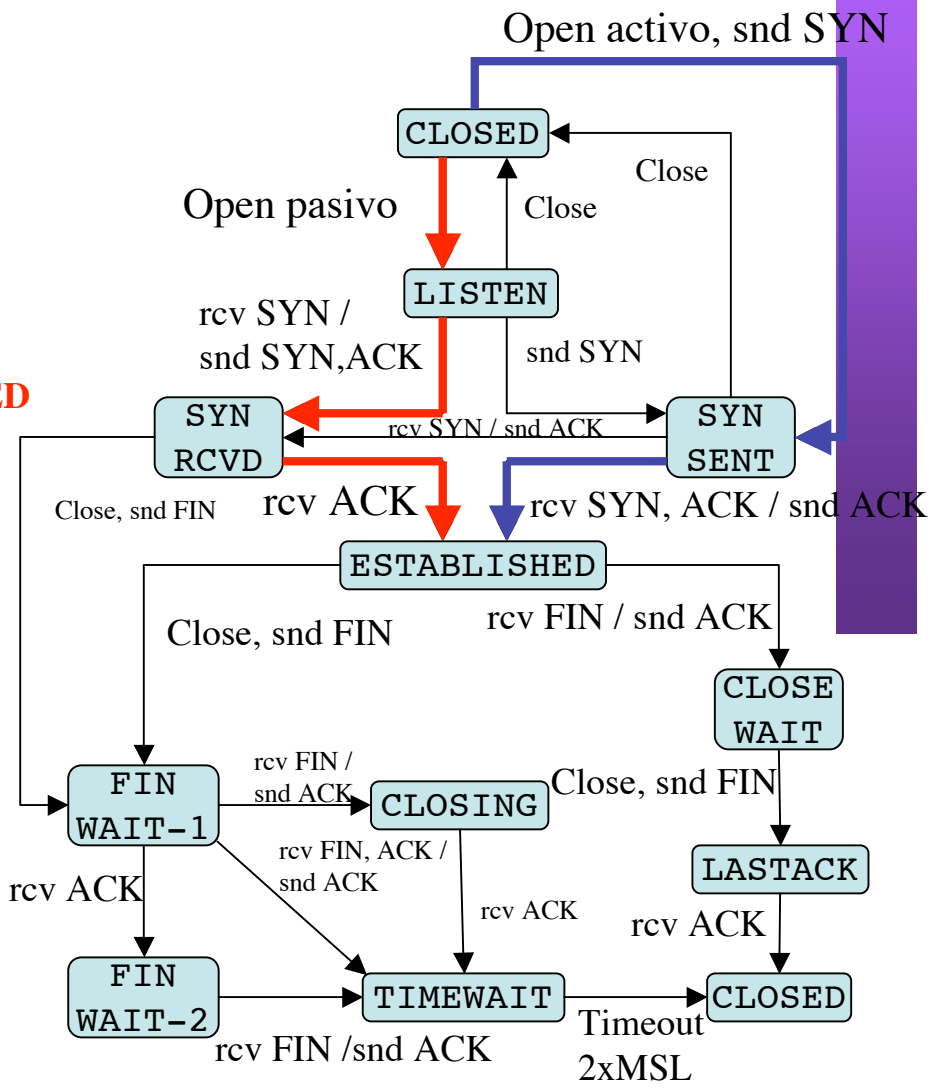
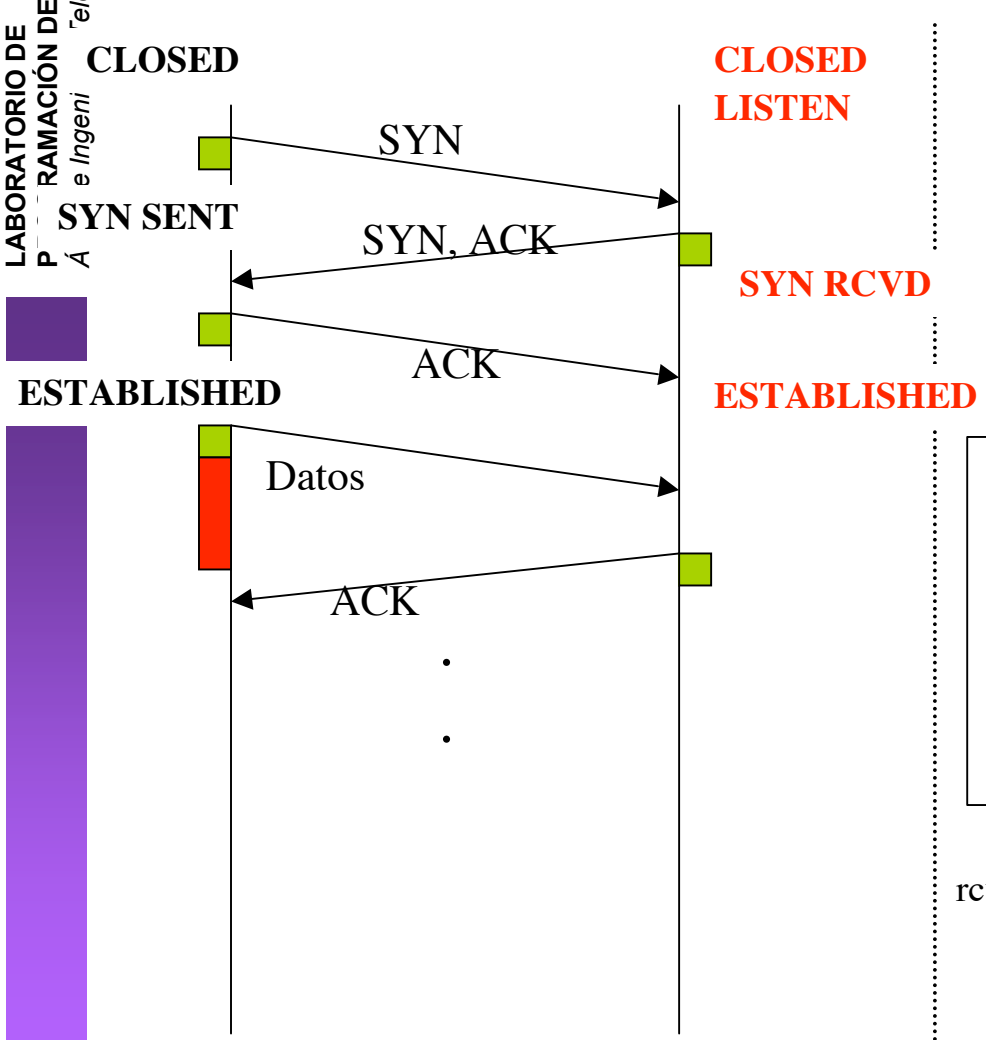


Diagrama de estados



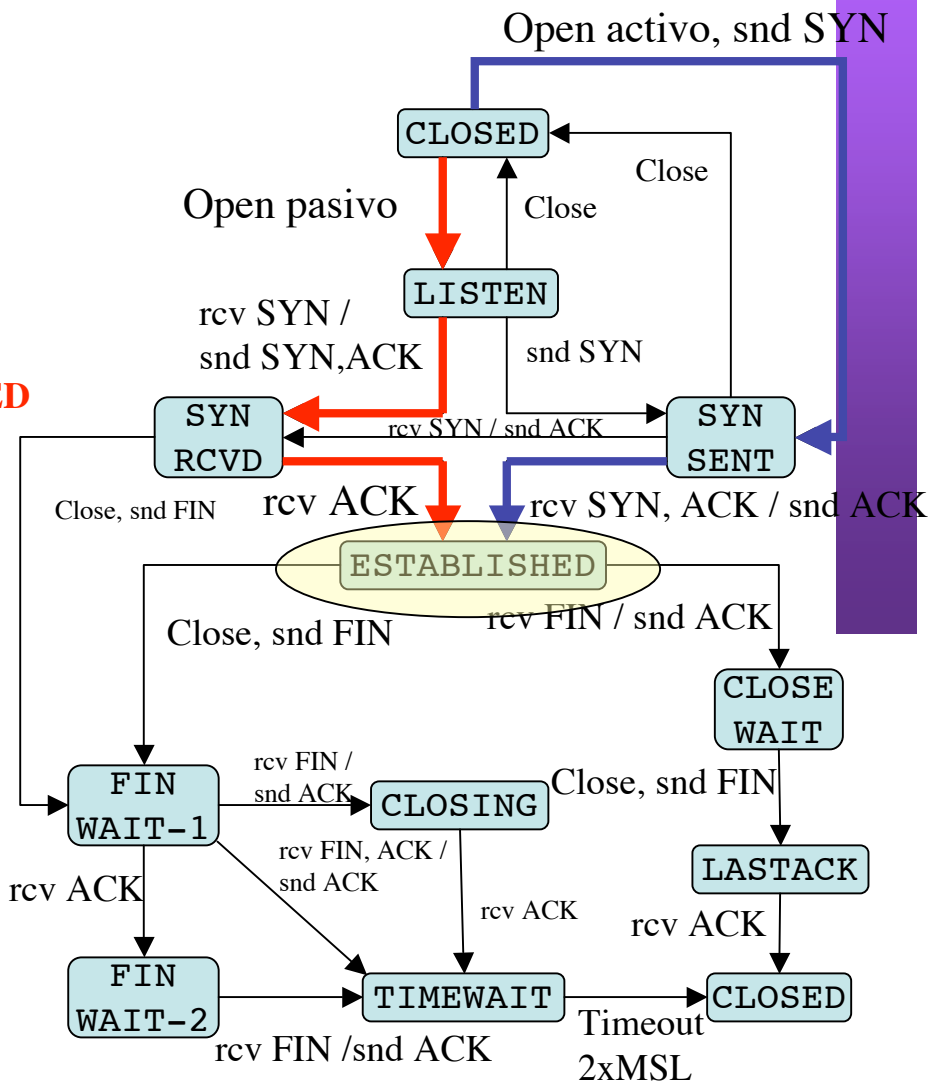
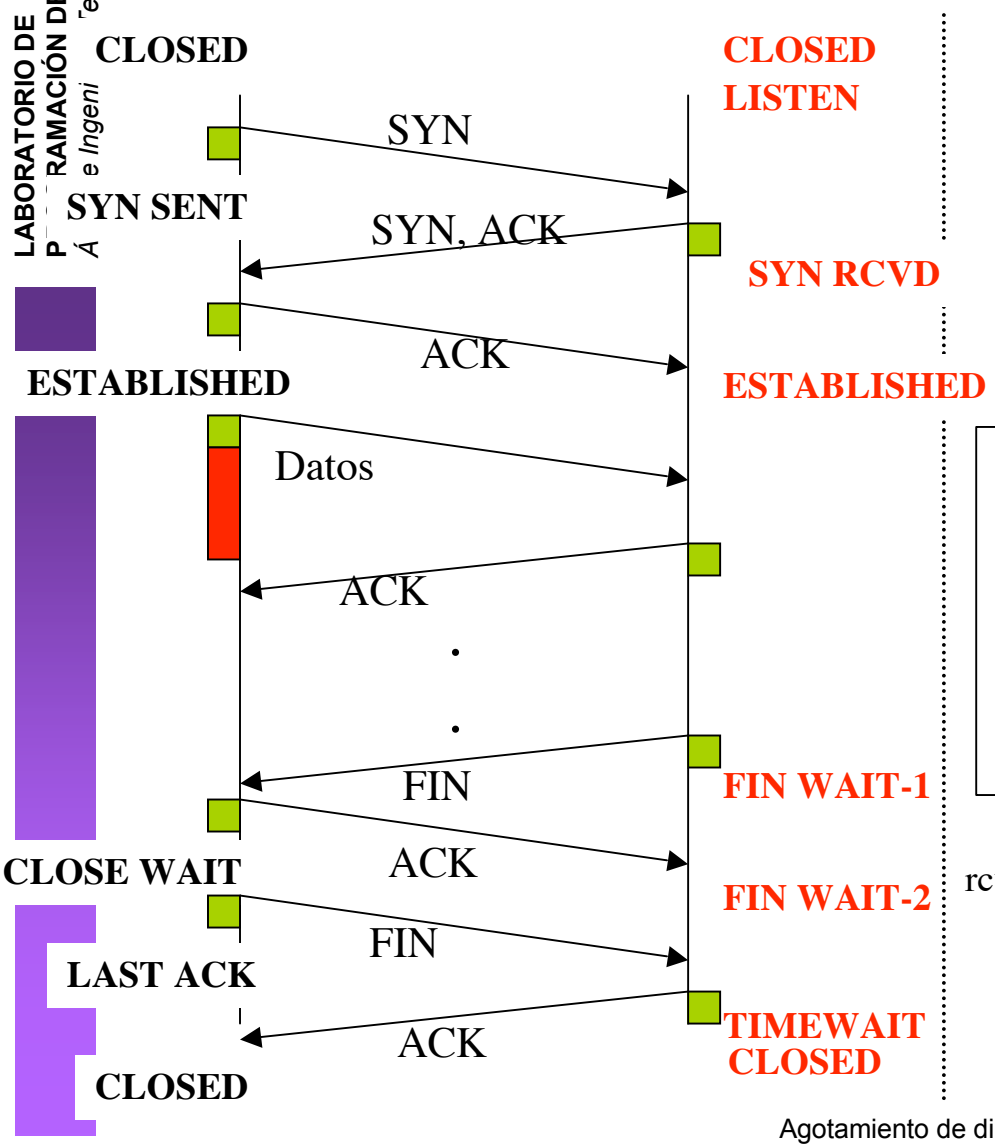
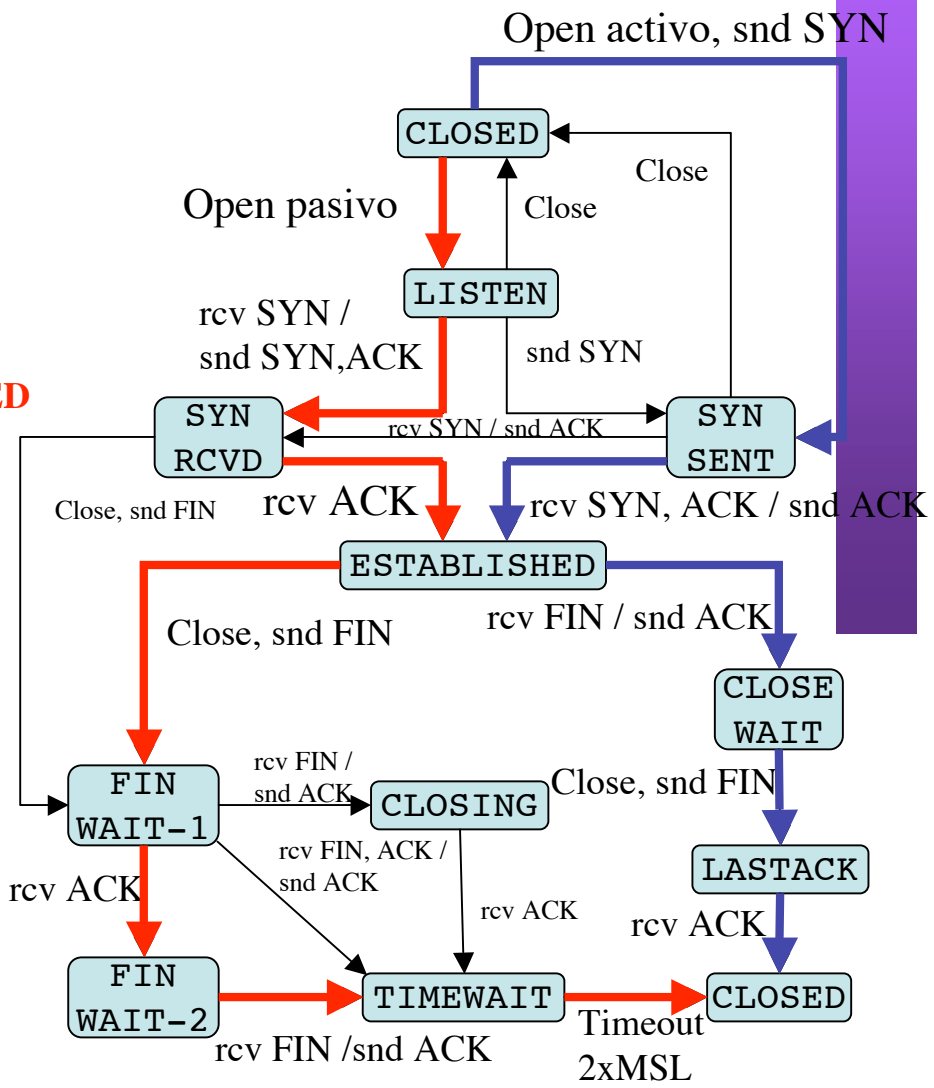
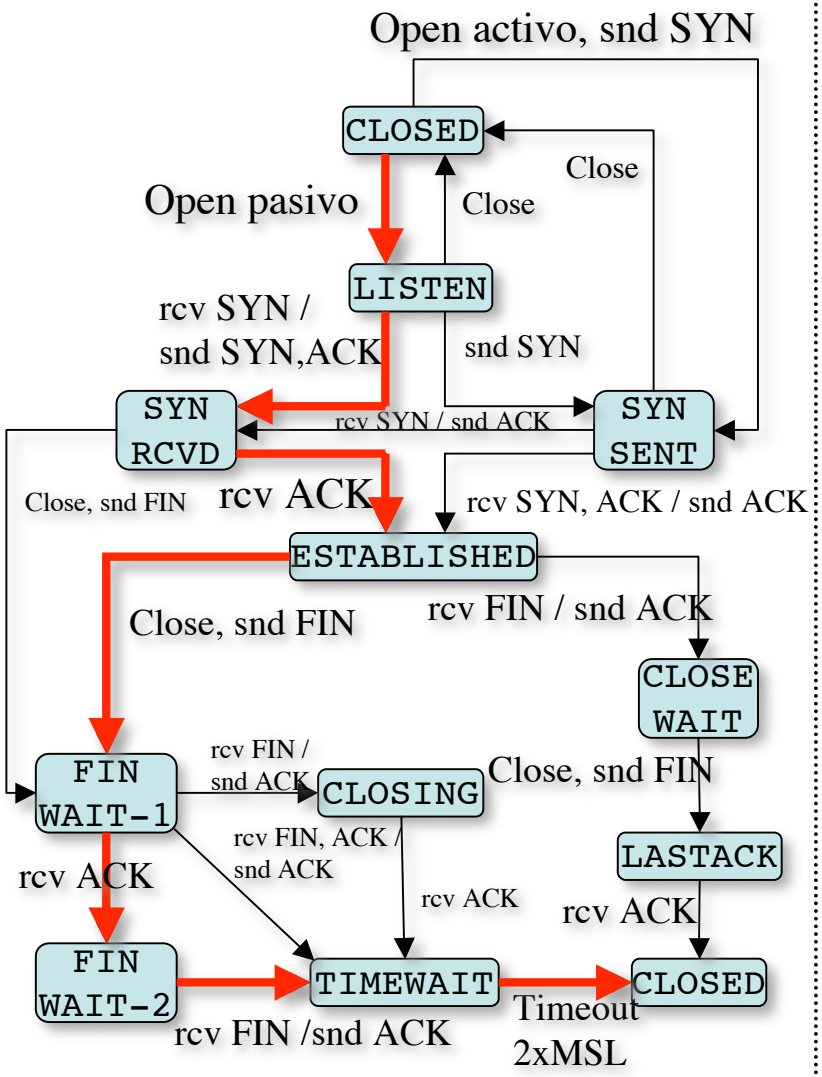


Diagrama de estados

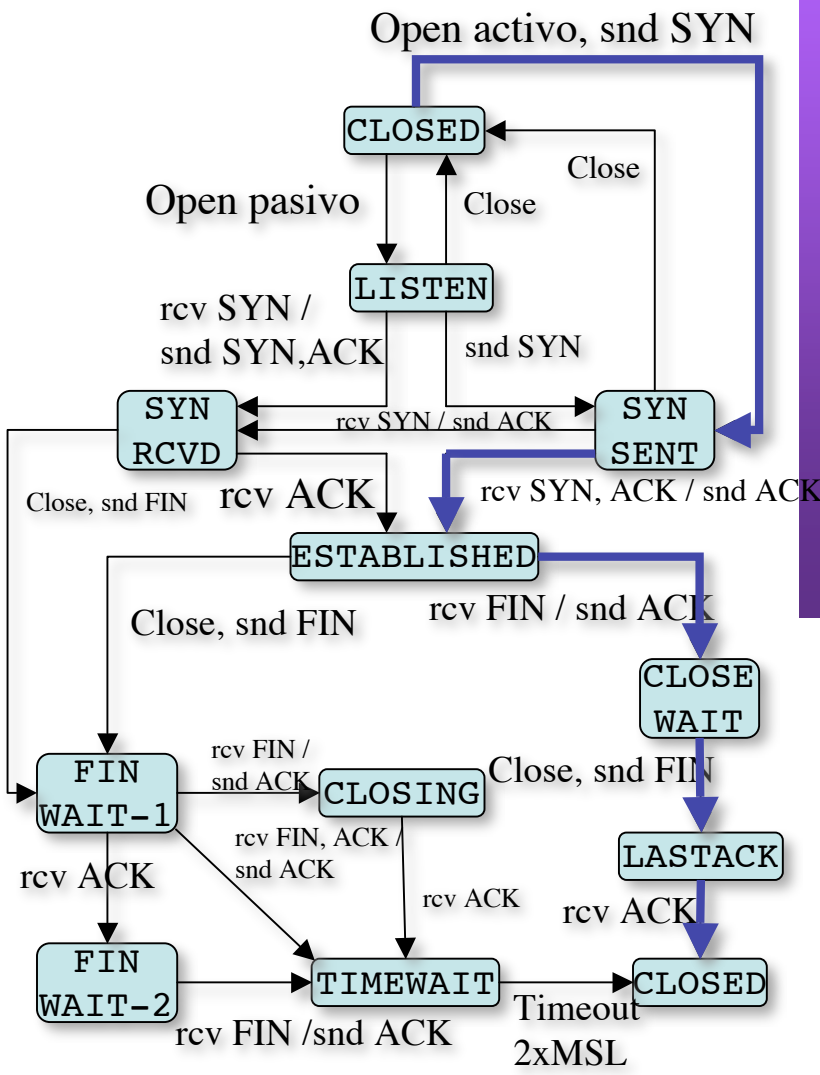




Servidor



Cliente



Ejemplo

```
$ tcpdump -ttnlS tcp and host 10.1.11.1
Kernel filter, protocol ALL, datagram packet socket
tcpdump: listening on all devices
54.171 1.1.1.12.1798 > 10.1.11.1.telnet: S 3462181145:3462181145(0)
54.175 10.1.11.1.telnet > 1.1.1.12.1798: S 1997882026:1997882026(0) ack 3462181146
54.175 1.1.1.12.1798 > 10.1.11.1.telnet: . 3462181146:3462181146(0) ack 1997882027

54.177 1.1.1.12.1798 > 10.1.11.1.telnet: P 3462181146:3462181173(27) ack 1997882027
54.178 10.1.11.1.telnet > 1.1.1.12.1798: . 1997882027:1997882027(0) ack 3462181173
...

66.816 10.1.11.1.telnet > 1.1.1.12.1798: FP 1997882551:1997882559(8) ack 3462181333
66.816 1.1.1.12.1798 > 10.1.11.1.telnet: . 3462181333:3462181333(0) ack 1997882560
66.817 1.1.1.12.1798 > 10.1.11.1.telnet: F 3462181333:3462181333(0) ack 1997882560
66.818 10.1.11.1.telnet > 1.1.1.12.1798: . 1997882560:1997882560(0) ack 3462181334
```

Contenido

- Introducción
- El problema
- Algunas soluciones
  - DHCP
  - NAT
  - IPv6

Contenido

- Introducción
- **El problema**
- Algunas soluciones
  - DHCP
  - NAT
  - IPv6

Problemas de IPv4

- Escasez de direcciones
- Complejidad innecesaria en los routers

¿Dónde se desperdician direcciones?

- Redes con clases:
  - Clase A: Más de 16M de direcciones
  - Clase B: 64K direcciones
- PCs que se usen esporádicamente

Contenido

- Introducción
- El problema
- **Algunas soluciones**
  - **DHCP**
  - NAT
  - IPv6

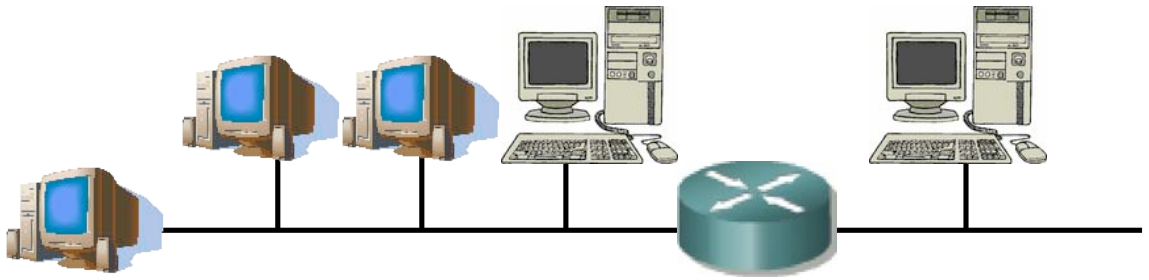
DHCP

- Dynamic Host Configuration Protocol
- RFC 2131
- Basado en BOOTP
- 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

- Mecanismos de asignación de dirección IP:
- Automatic allocation
  - Asigna una IP permanente
- Dynamic allocation
  - Asigna por un periodo de tiempo limitado (lease)
  - O hasta que el host la lebera
- Manual allocation
  - IP fijada por el administrador

DHCP: Funcionamiento (I)

- 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



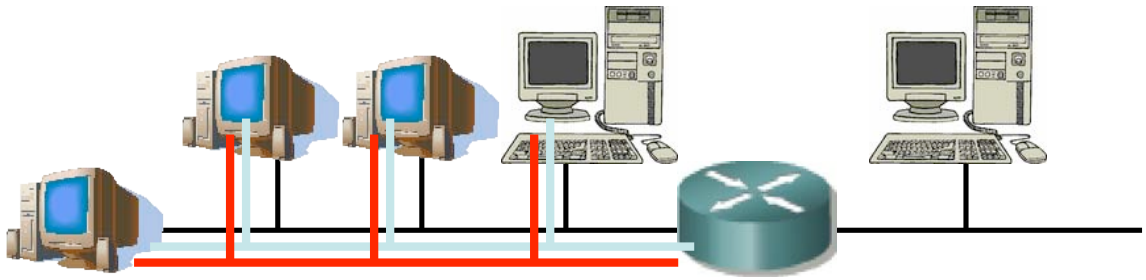
DHCP: Funcionamiento (II)

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



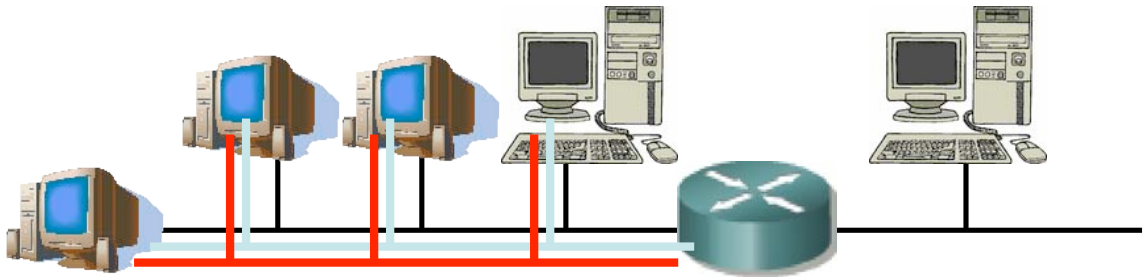
DHCP: Funcionamiento (y III)

DHCP Request

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

DHCP ACK

- El servidor confirma la asignación al cliente (…)



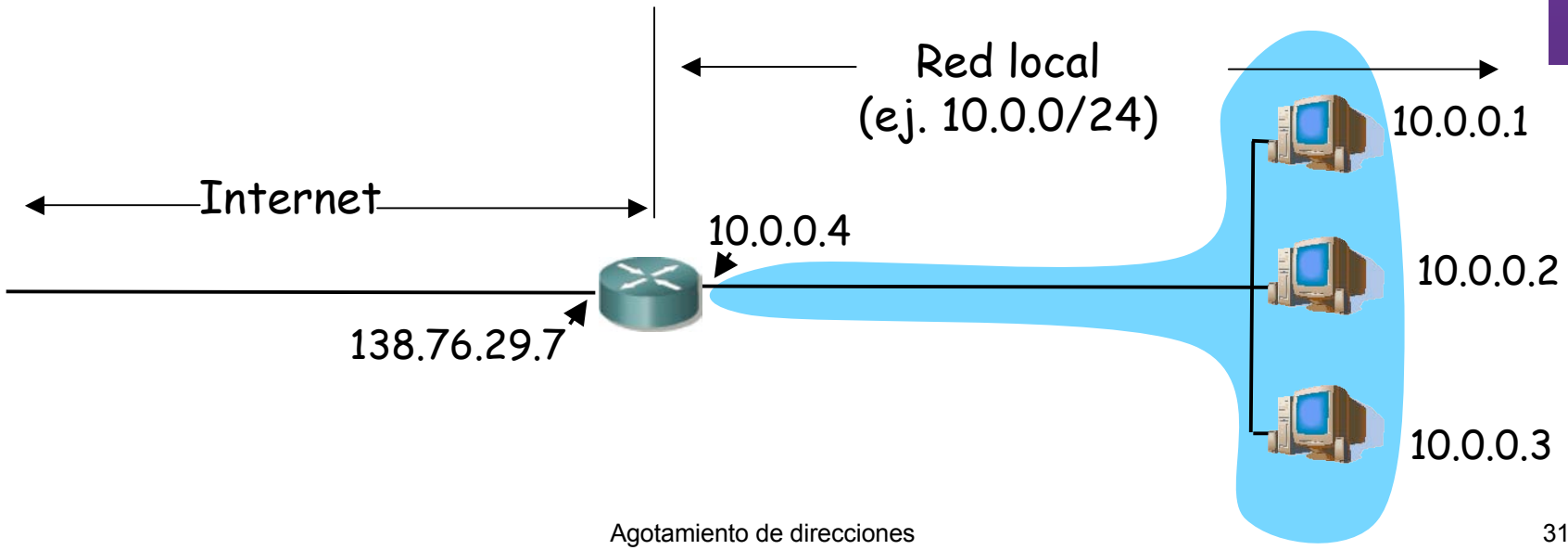
Contenido

- Introducción
- El problema
- **Algunas soluciones**
  - DHCP
  - **NAT**
  - IPv6

NAT

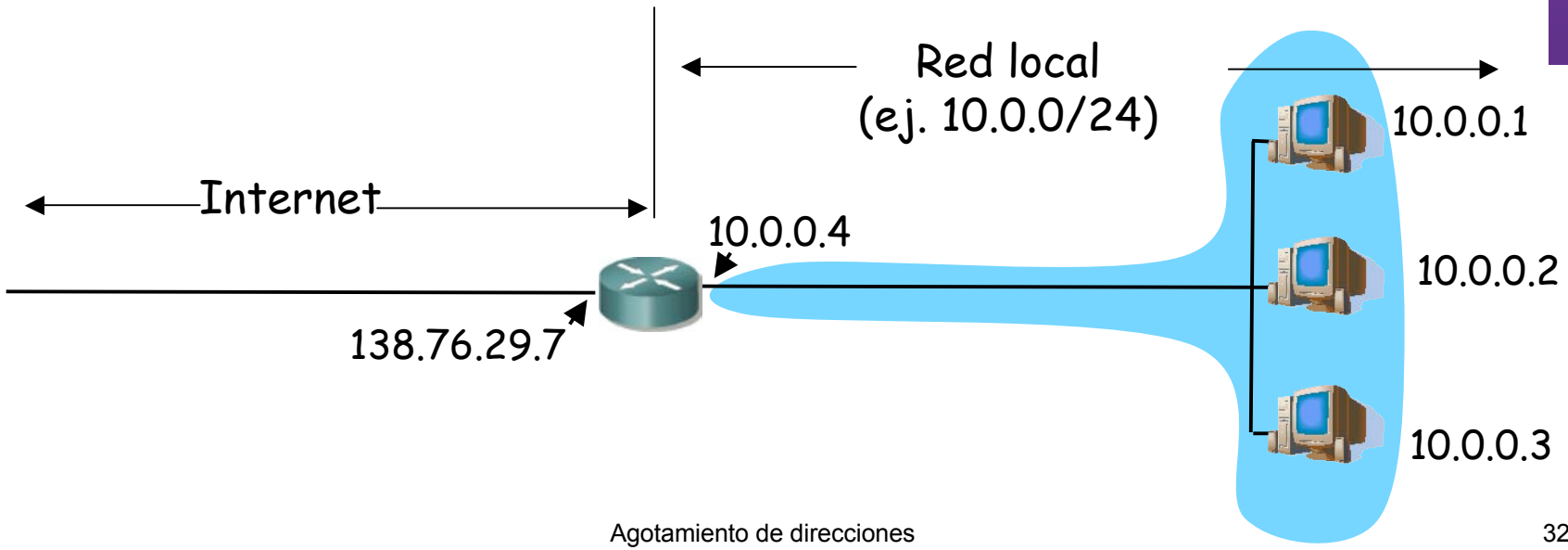
- Network Address Translation
- Otra propuesta de solución al problema del agotamiento del espacio de direcciones
- Permite que una red que emplee **direccionamiento privado** se conecte a Internet

- El router que conecta la red a Internet:
  - Cambia la dirección IP privada por una dirección pública al reenviar un paquete hacia el exterior
  - Cambia la dirección IP pública por la correspondiente privada al reenviar un paquete hacia el interior



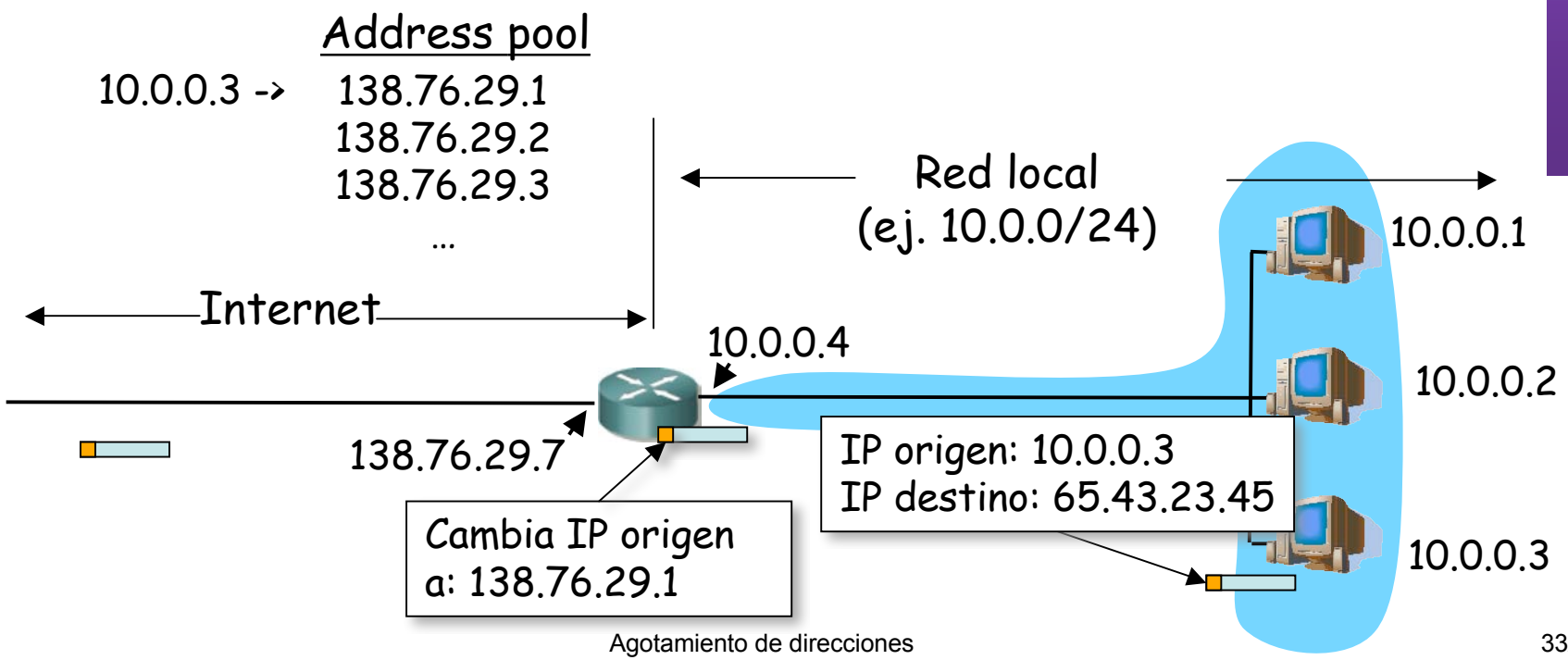
NAT

- El cambio puede ser:
  - **Estático**: una IP interna siempre se cambia por la misma IP pública
  - **Dinámico**: existe un pool de IPs públicas y se establece una relación entre las IPs internas y las de ese pool
- No se necesita reconfigurar los hosts de la red
- Si no todos los hosts de la red desean cursar tráfico con Internet "simultáneamente" no hacen falta tantas direcciones como hosts.



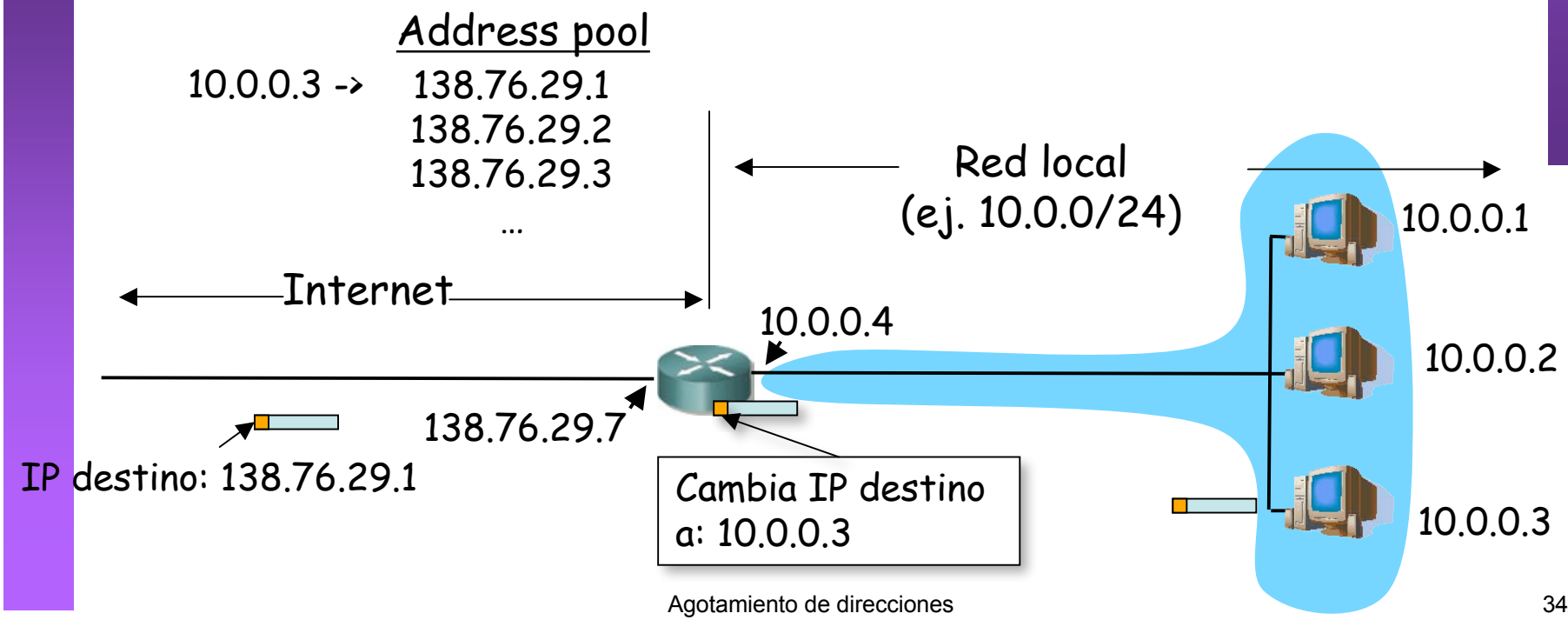
NAT (Ejemplo)

- La red interna tiene direccionamiento privado
- El interfaz del router tiene una dirección pública
- Además tiene un **pool de direcciones** publicas disponibles
- Cuando un host quiere enviar un paquete IP a un destino en Internet el router NAT cambia la dirección IP origen antes de reenviarlo (…)
- El router NAT apunta la dirección por la que la ha cambiado (…)



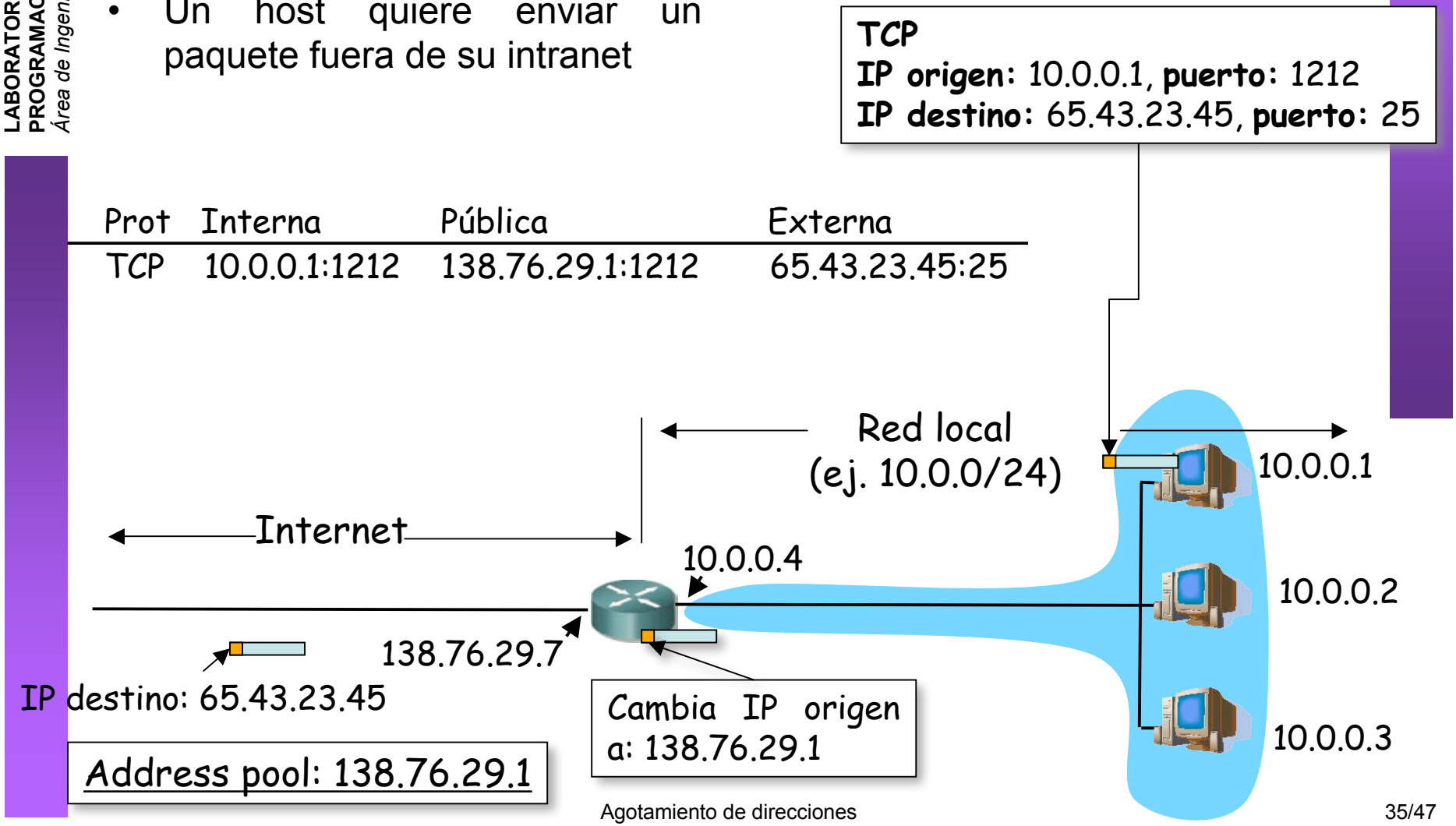
NAT (Ejemplo)

- Cuando venga un paquete de esa IP destino vendrá dirigido a la IP que colocó el router NAT
- El router NAT ve en su tabla la dirección IP interna a la que corresponde y la cambia (… …)



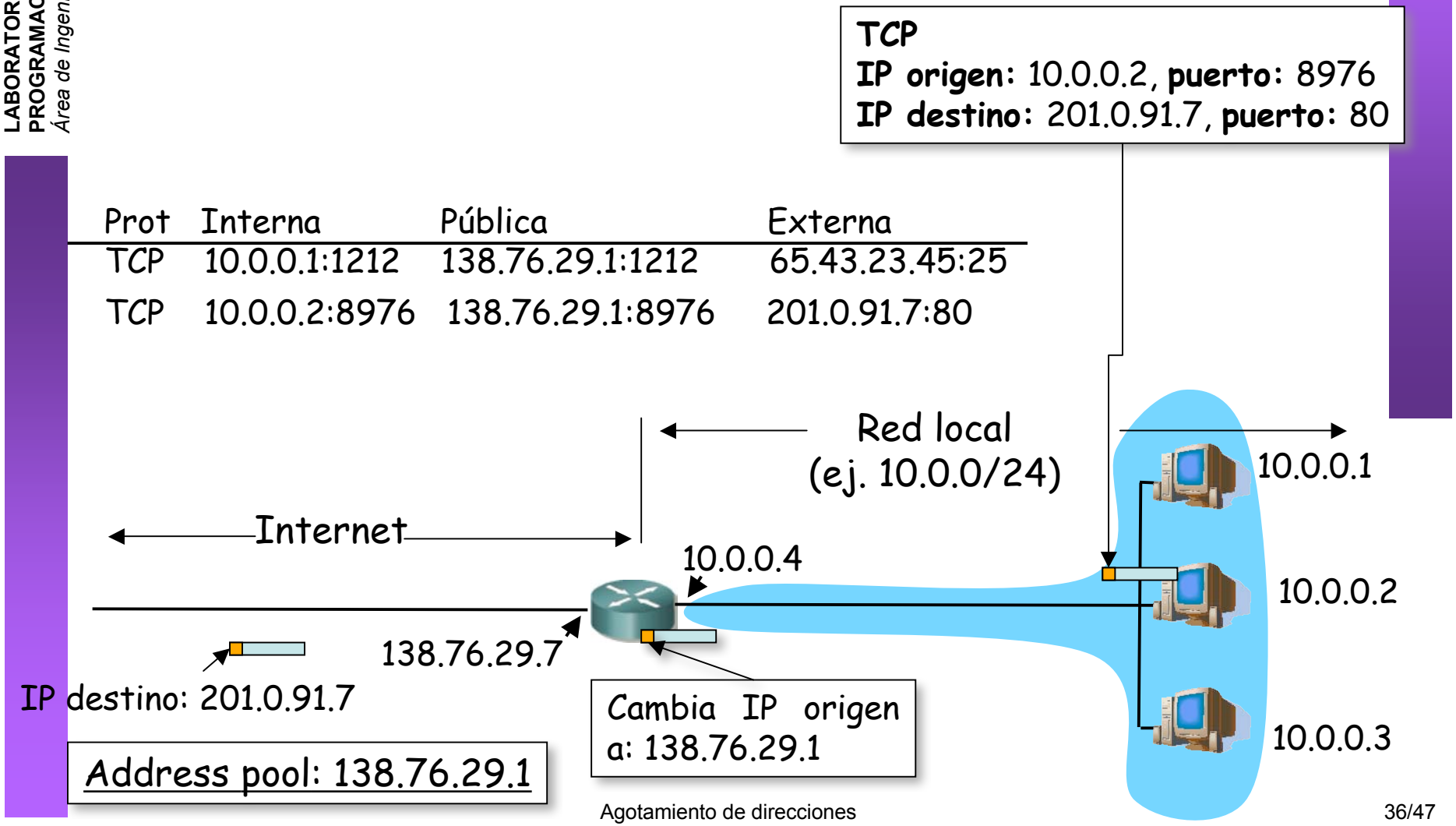
NAT (Ejemplo 2: Sobrecarga)

- Supongamos que solo hay una dirección pública
- Un host quiere enviar un paquete fuera de su intranet



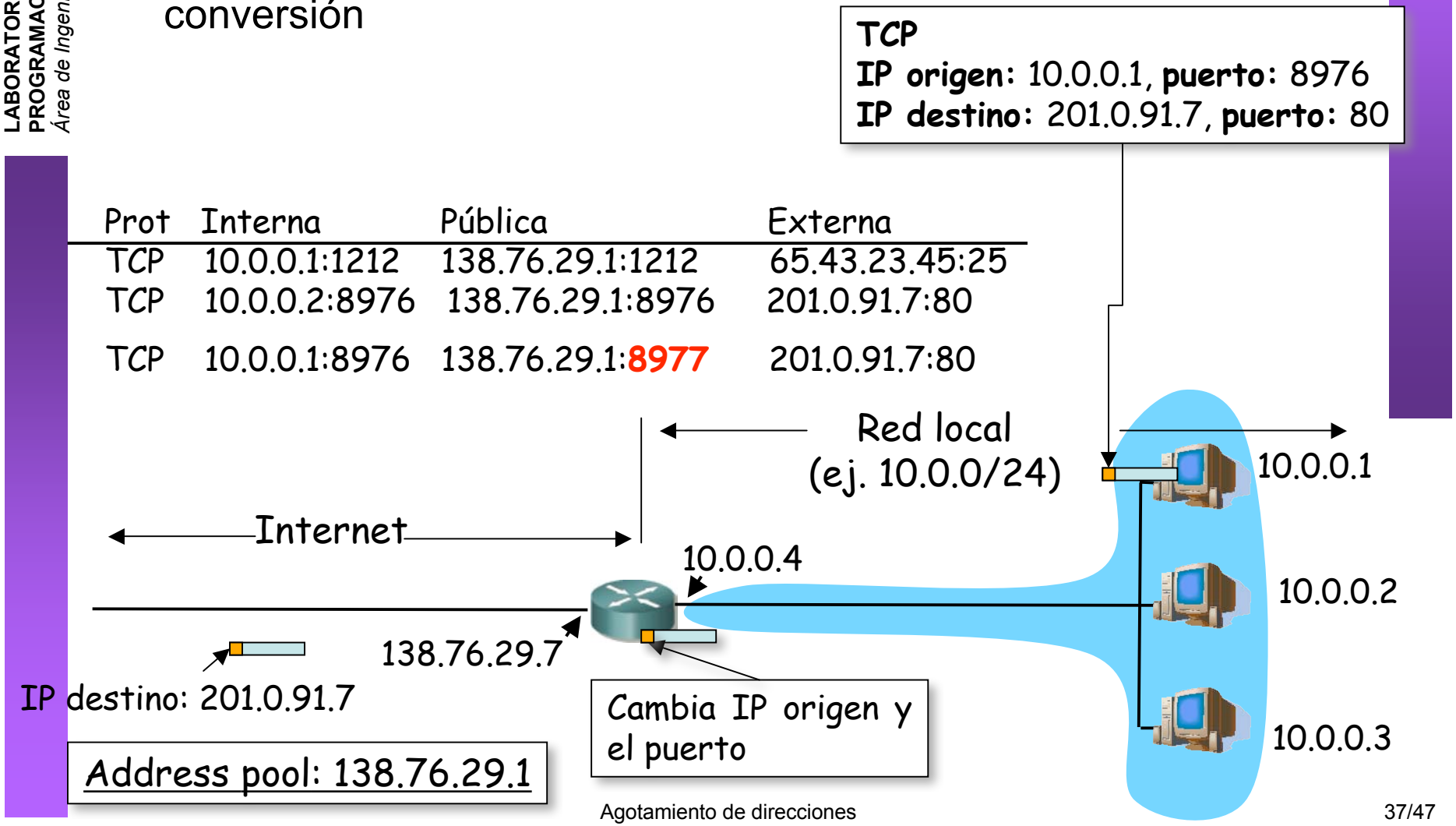
NAT (Ejemplo 2: Sobrecarga)

- Otro host también envía tráfico al exterior



NAT (Ejemplo 2: Sobrecarga)

- Se puede producir una colisión en la tabla de conversión



NAT

Ventajas

- Se puede cambiar el rango de direcciones sin notificar
- Puede cambiar de ISP sin cambiar las direcciones
- Máquinas no accesibles desde el exterior (seguridad)
- ¿Una sola IP en el pool? La del router

Inconvenientes

- El puerto es de 16bits:
  - 64K conexiones con una sola dirección
- Consume memoria
- Controvertido:
  - Los routers solo hasta el nivel de red
  - Servidores no accesibles desde el exterior
  - Rompe el esquema extremo a extremo
  - Los diseñadores de aplicaciones deberán tener en cuenta la posibilidad de existencia de NATs entre cliente y servidor

Contenido

- Introducción
- El problema
- **Algunas soluciones**
  - DHCP
  - NAT
  - **IPv6**

IPv6

- **Motivación inicial:**
  - El espacio de direcciones de 32bits se estaba 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
- ICMPv6

Direcciones

- 16 bytes
- Notación:
  - Pares de bytes en hexadecimal
  - Separados por ":"
  - Simplificar 0s a la izquierda
  - Bloques de pares de bytes de 0s
  - Notación CIDR
  - Notación mezclada

- Unicast
- Multicast
- Anycast
  - Conjunto de interfaces
  - Se entrega el paquete a uno de ellos

FDEC:0:0:0:0:BBFF:0:FFFF

FDEC::BBFF:0:FFFF

FDEC:BA98:7654:3210:ADBF:BBFF:2922:FFFF

FDEC:0:0:0:0:BBFF:0:FFFF/60

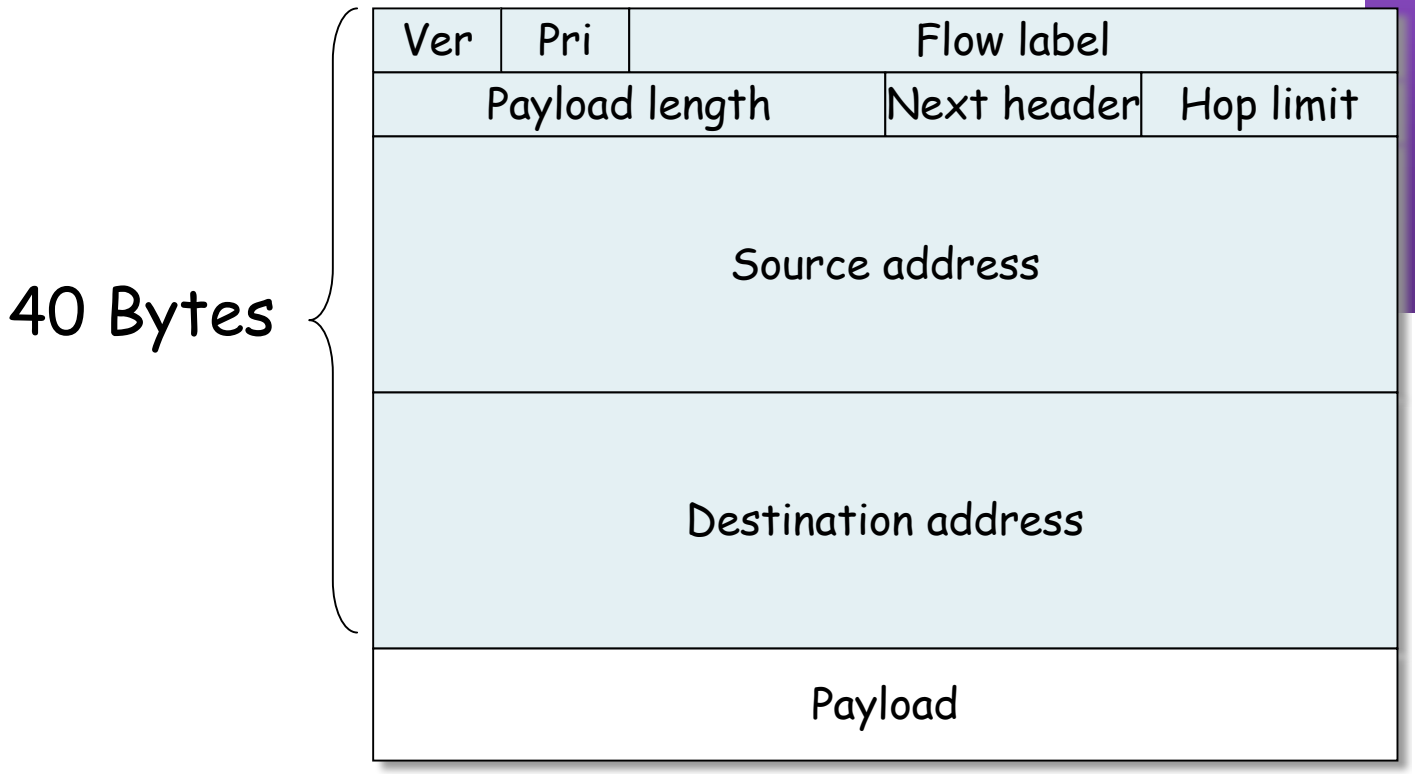
FDEC:BA98:0054:3210:000F:BBFF:0000:FFFF

FDEC:BA98:54:3210:F:BBFF:0:FFFF

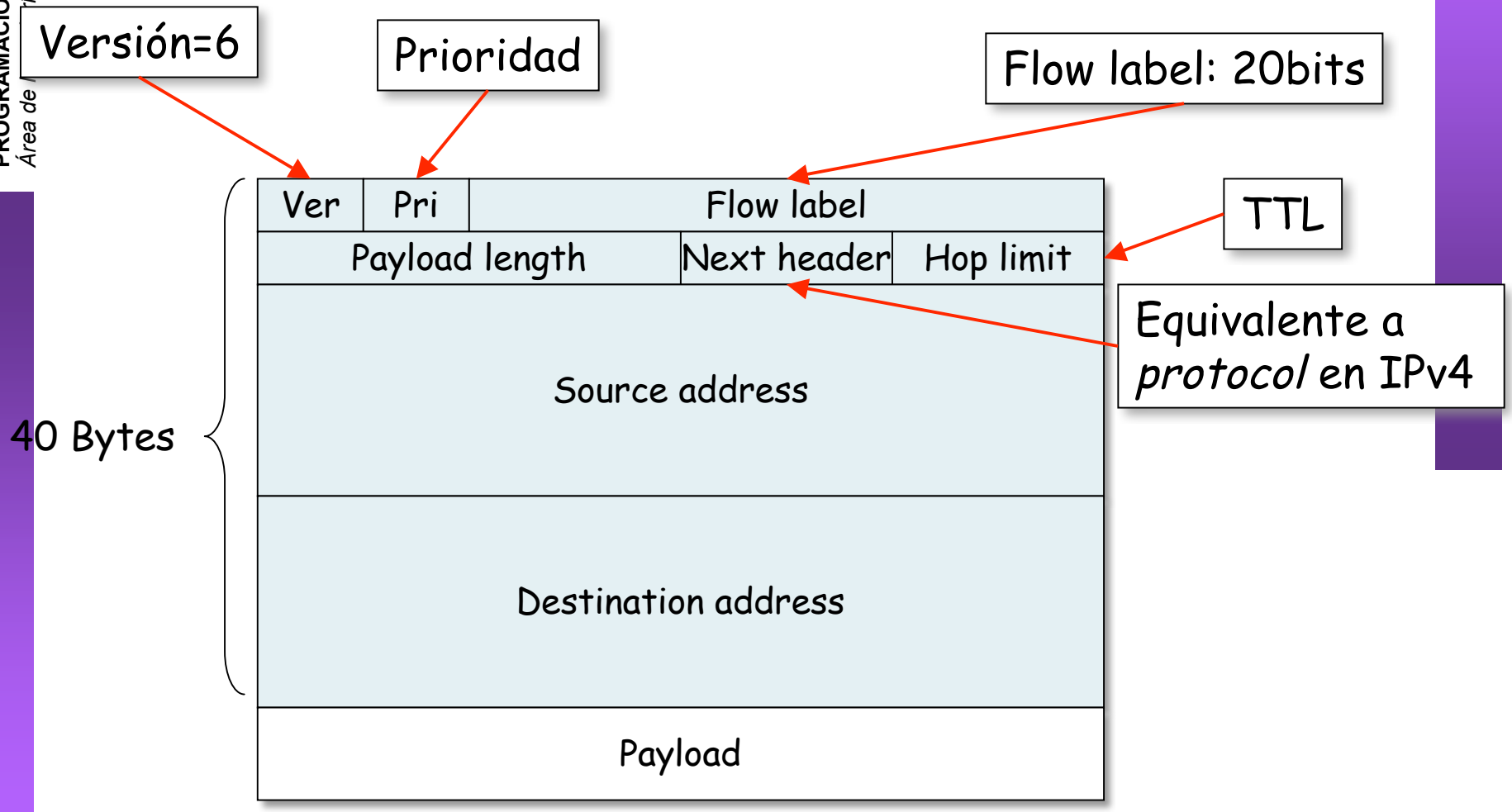
::FFFF:130.206.160.45

Cabecera IPv6

Versión = 6
Priority
Flow label: 20bits
Next header = *protocol* en IPv4
Hop limit: Como TTL

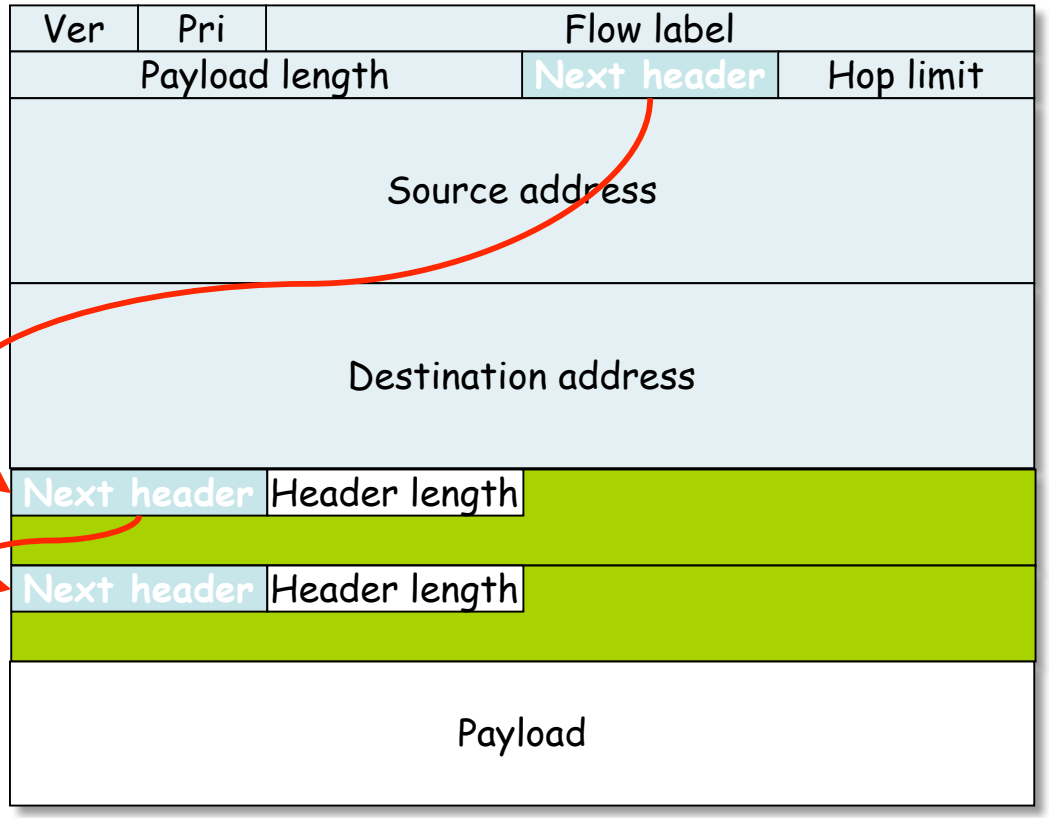


Cabecera IPv6



Opciones

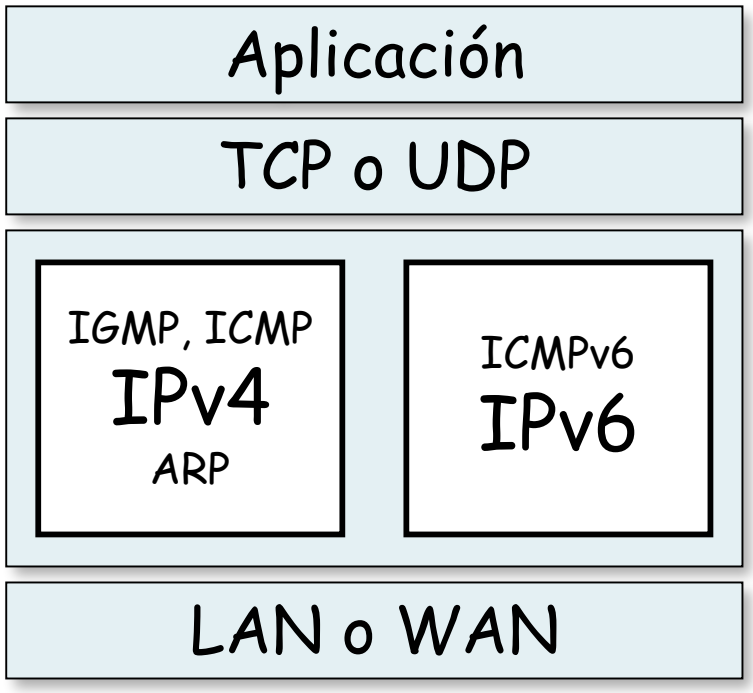
Extension Headers

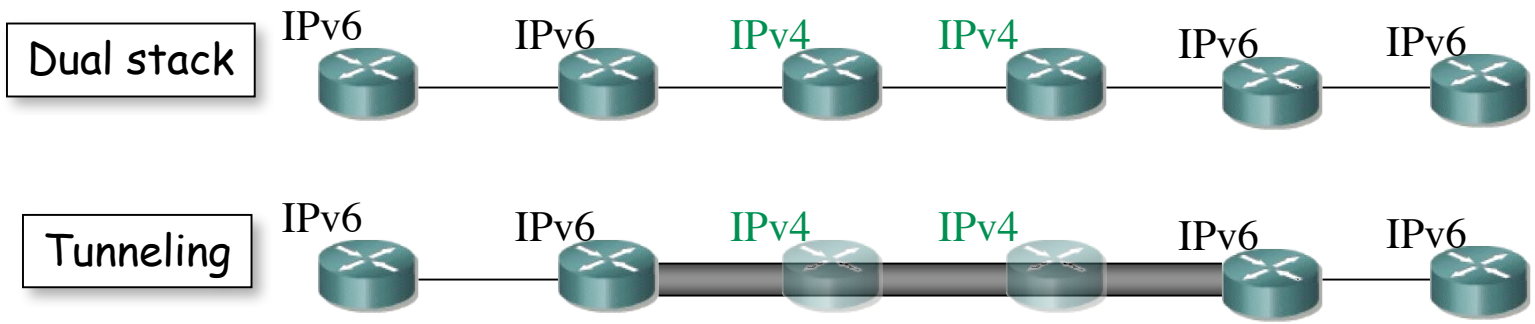


- *Source Routing*
- Fragmentación
- Autentificación
- *Encrypted Security Payload*
- *Etc.*

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

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