Planificación y Administración de Redes: IP – Internet Protocol (II)

IES Gonzalo Nazareno
CONSEJERÍA DE EDUCACIÓN

Jesús Moreno León
Raúl Ruiz Padilla

j.morenol@gmail.com

Septiembre 2010

Estas diapositivas son una obra derivada de las transparencias del Grupo de Sistemas y Comunicaciones de la Universidad Rey Juan Carlos
Puede encontrarse una versión de este documento en
http://gsyc.es/moodle

Encaminamiento

Cualquier máquina IP puede estar o no configurada como encaminador:

- Si NO lo está, los datagramas IP que recibe que no son para ella, se descartan
- Si SÍ lo está, se tratan de encaminar (es decir, se intenta reenviarlos para que progresen hacia su destino final)

Encaminamiento

Cuando una máquina quiere enviar un datagrama IP a un destino, consulta su **tabla de encaminamiento**.

En la tabla se busca si encaja la IP destino en la primera columna de alguna entrada (buscando en este orden):

1. Una entrada con una dirección IP de máquina igual a la IP destino
2. Una entrada con una dirección IP de red igual a la parte de red de la IP destino
3. Una entrada por defecto (0.0.0.0, *default* o * en la primera columna)

Si no existe ninguna entrada adecuada, el datagrama se descarta

Tablas de encaminamiento

Las tablas de encaminamiento tienen el siguiente aspecto:

```
% netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS  Iface
193.147.71.0    0.0.0.0         255.255.255.0   U       1500 eth0
212.128.4.0     0.0.0.0         255.255.255.0   U       1500 eth1
145.154.12.0    193.147.71.2    255.255.255.0   UG      1500 eth0
145.154.12.14   212.128.4.2     255.255.255.255 UG      1500 eth1
0.0.0.0         193.147.71.1    0.0.0.0         UG      1500 eth0
```

ARP (Address Resolution Protocol)

El Protocolo ARP permite averiguar la dirección Ethernet de una máquina sabiendo su dirección IP

Cuando el nivel IP va a envíar un datagrama a una cierta dirección IP destino:

- Si la dirección IP de destino es de la misma subred, esa máquina es directamente a quien hay que enviar la trama Ethernet que contenga el datagrama
- Si no, la tabla de encaminamiento da la dirección IP del siguiente salto, que es el encaminador a quien hay que enviar la trama Ethernet que contenga el datagrama

En cualquiera de los dos casos sólo sabemos la dirección IP de la máquina adyacente → necesitamos su dirección Ethernet

ARP

Para conocer la dirección Ethernet de una máquina de su misma subred, dada su dirección IP, una máquina hace lo siguiente:

- Envía una trama Ethernet de *broadcast* consistente en una solicitud ARP, conteniendo la dirección IP destino
- Aquella máquina que reciba la solicitud ARP preguntando por su propia dirección IP, contesta con una trama Ethernet dirigida a quien hizo la pregunta, conteniendo una respuesta ARP indicando la dirección pedida

ARP

Cada máquina mantiene una caché de correspondencias direcciones IP a direcciones Ethernet

Caché de ARP		
IP	Ethernet	Interfaz

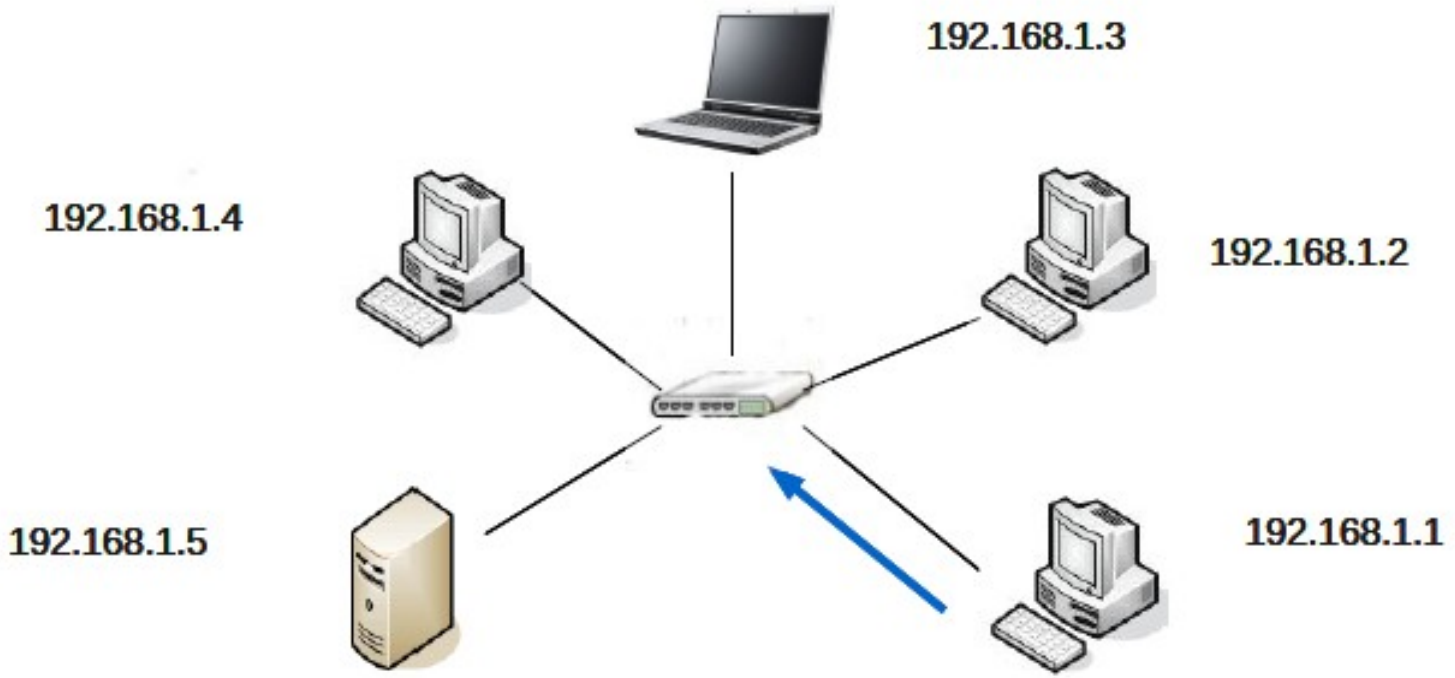
ARP

Formato de solicitud/respuesta ARP:

Solicitud/Respuesta	Eth. Origen	IP Origen	Eth. Destino	IP Destino

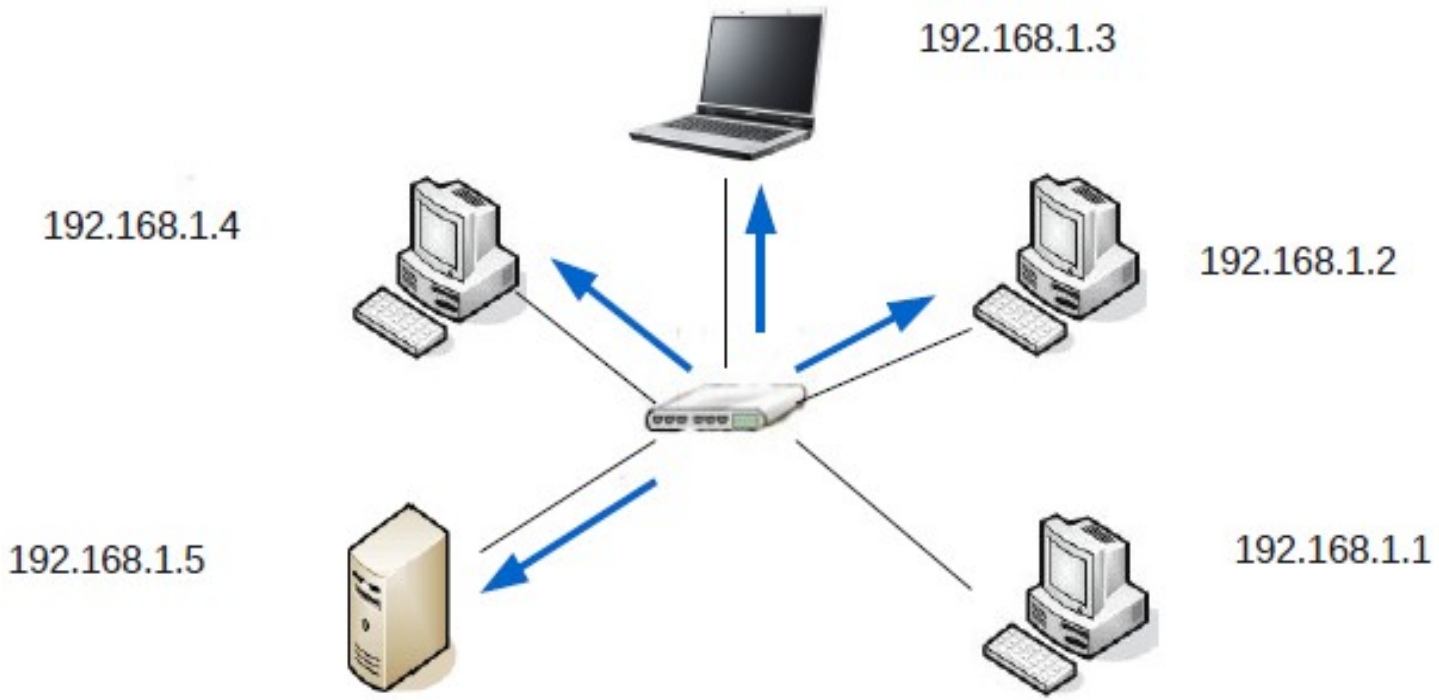
No hay que olvidar que el paquete de ARP viaja dentro de una trama Ethernet (si ese es el nivel de enlace)

ARP



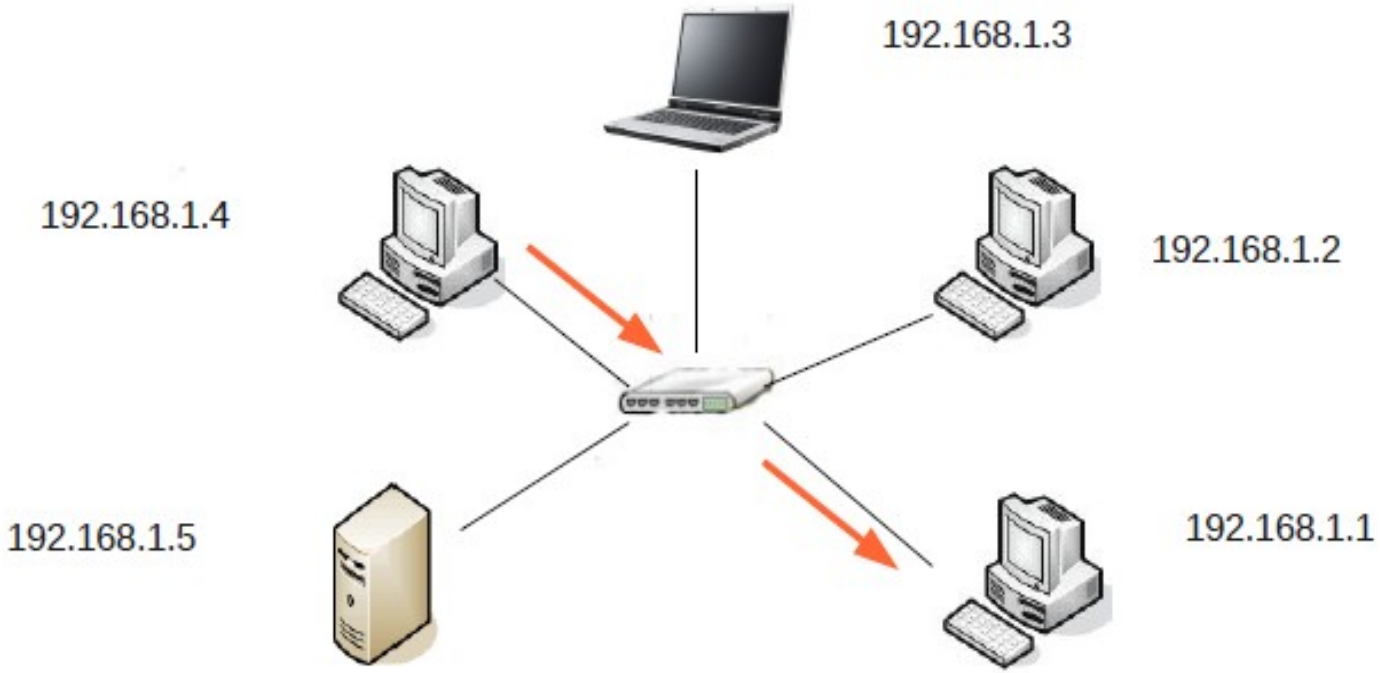
TIPO	Dir ethernet ORIGEN	IP ORIGEN	Dir ethernet DESTINO	IP DESTINO
SOLICITUD	1	192.168.1.1		192.168.1.4

ARP



TIPO	Dir ethernet ORIGEN	IP ORIGEN	Dir ethernet DESTINO	IP DESTINO
SOLICITUD	1	192.168.1.1		192.168.1.4

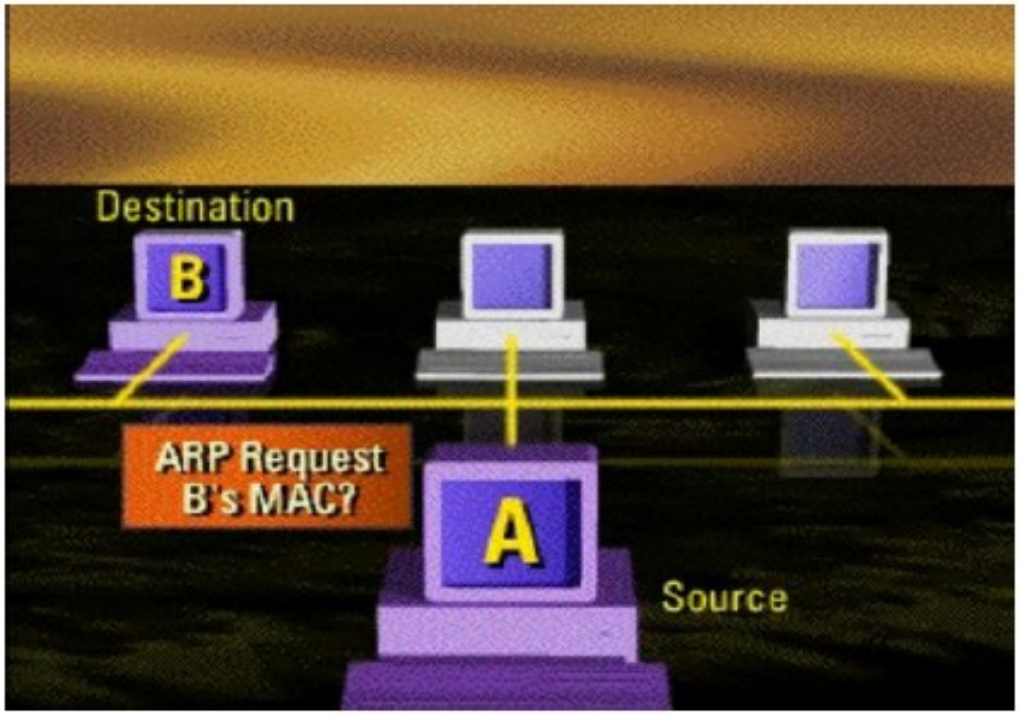
ARP



TIPO	Dir ethernet ORIGEN	IP ORIGEN	Dir ethernet DESTINO	IP DESTINO
RESPUESTA	4	192.168.1.4	1	192.168.1.1

ARP

Vídeo:



ARP

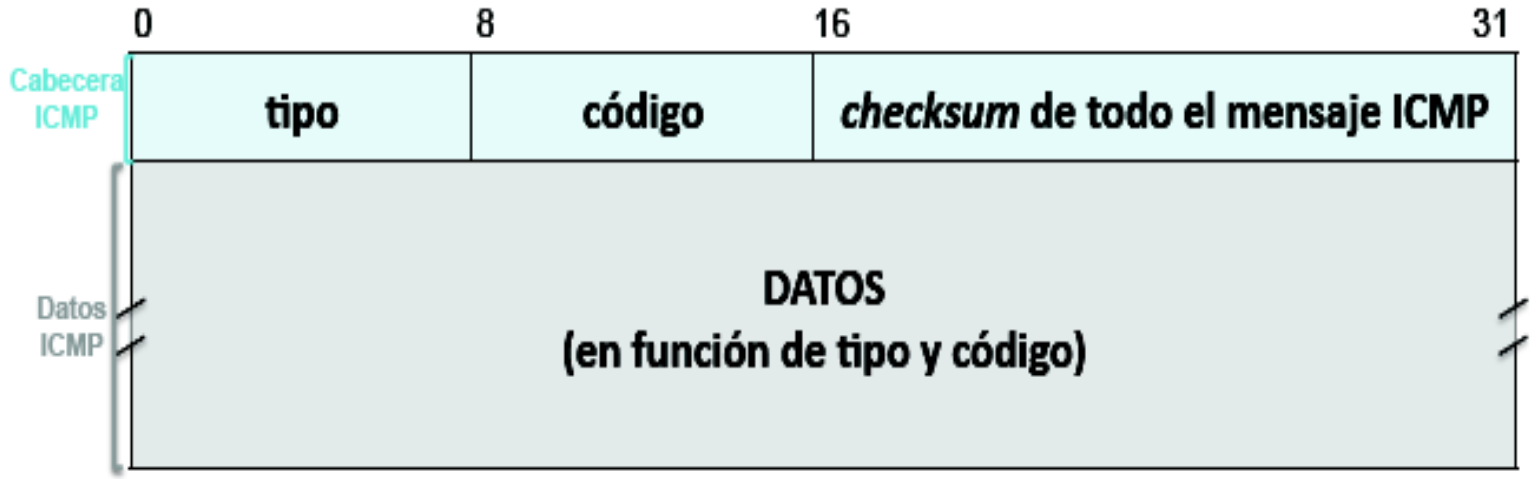
ARP gratuito: una máquina puede enviar una solicitud de ARP preguntando por su propia dirección IP

- Para detectar IP duplicadas
- Forzar a que todos actualicen la entrada de la tabla de caché correspondiente

ICMP

Este protocolo se utiliza para interrogar y/o comunicar condiciones de error entre máquinas

Los mensajes ICMP se transmiten encapsulados en datagramas IP



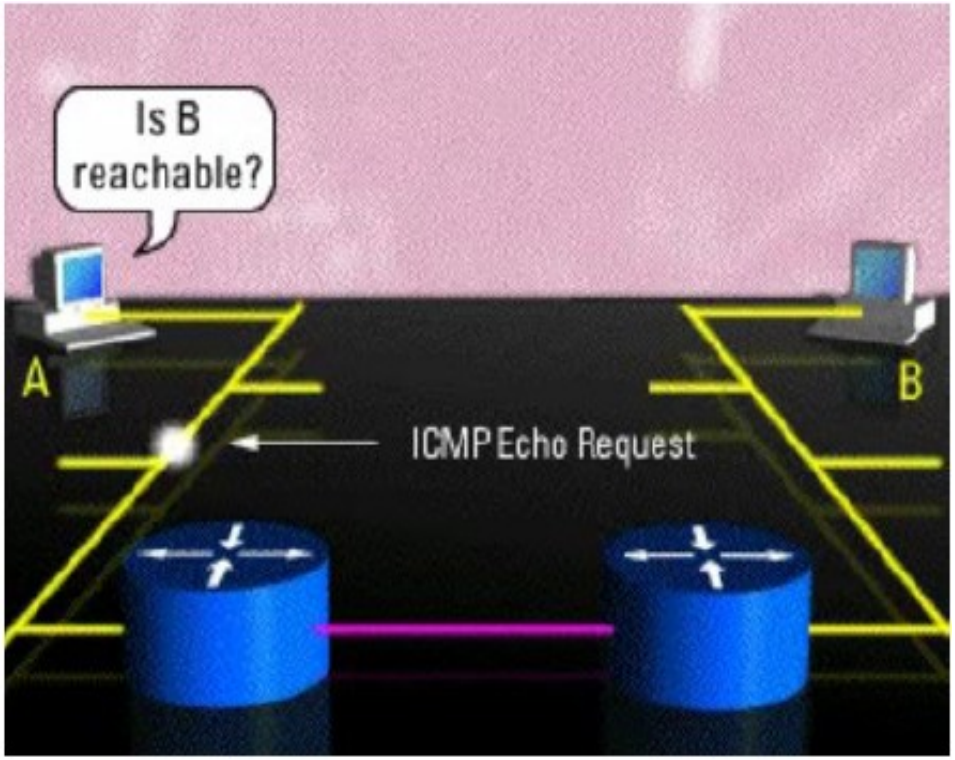
ICMP

Ejemplos de mensajes ICMP:

tipo	código	descripción
0	0	respuesta de eco
3	0	destino inalcanzable: red inalcanzable
3	1	destino inalcanzable: máquina inalcanzable
3	3	destino inalcanzable: puerto inalcanzable
8	0	solicitud de eco
11	0	tiempo excedido: TTL = 0
12	1	cabecera IP mal: falta una opción
13	0	solicitud de marca de tiempo
14	0	respuesta de marca de tiempo

ICMP

Vídeo de ejemplo: ping



Congestión en Internet

El nivel de red IP ofrece un servicio basado en datagramas

La principal fuente de pérdida de paquetes en Internet se debe a la congestión de encaminadores, que actúan descartando los paquetes que no caben en sus buffers

IP ofrece un servicio no fiable: no se recupera de las pérdidas por congestión (lo harán, en su caso, protocolos de niveles superiores)

IP no toma medidas para prevenir la congestión (será labor de protocolos de niveles superiores)

Direcciones privadas

Existen unos rangos de direcciones IP privadas, reservadas para ámbito local, y que no son utilizables en Internet:

Desde	10.0.0.0	hasta	10.255.255.255
Desde	169.254.0.0	hasta	169.254.255.255
Desde	172.16.0.0	hasta	172.31.255.255
Desde	192.168.0.0	hasta	192.168.255.255

Los encaminadores de Internet descartan los datagramas con destino a una de estas direcciones IP

Estas direcciones suelen denominarse direcciones IP privadas. Por oposición, el resto se denominan direcciones IP públicas.

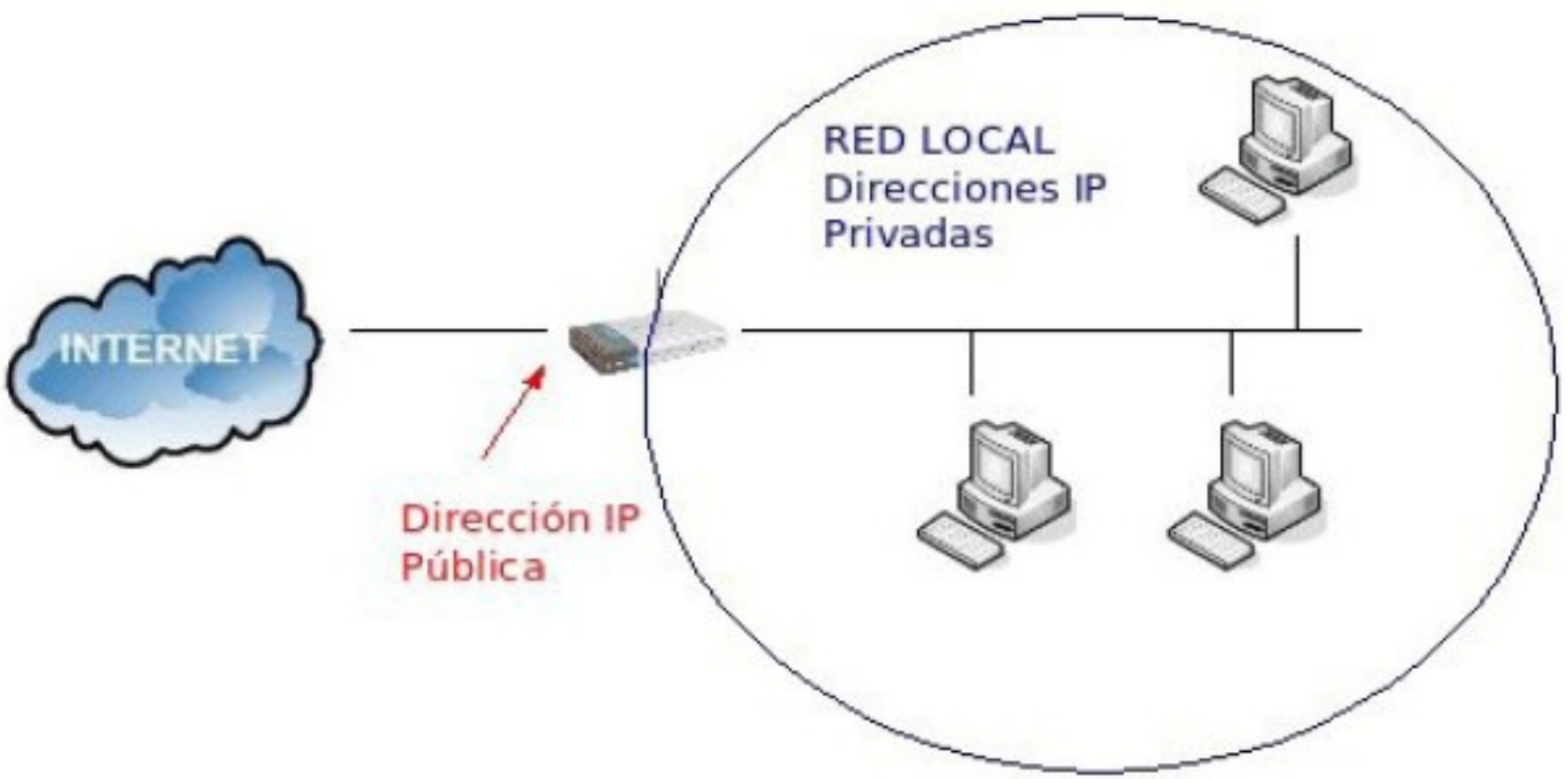
NAT (Network Address Traslation)

Para paliar la escasez de direcciones IP, una organización puede utilizar internamente direcciones privadas, y tener una sóla dirección IP global (pública) en la máquina que da salida a Internet

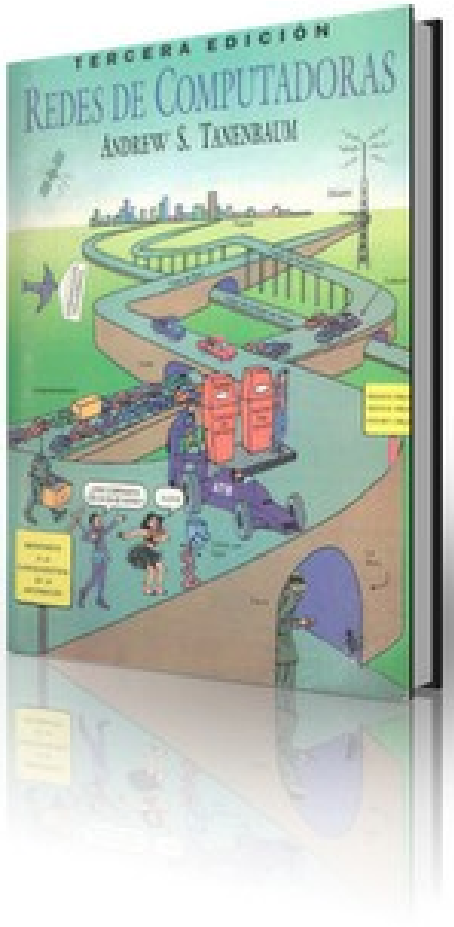
La máquina que da salida a Internet utiliza NAT para que los datagramas puedan entrar/salir de/a las máquinas internas

Muy resumidamente, lo que hace es cambiar las direcciones IP privadas de los datagramas por la suya pública

NAT (Network Address Traslation)



Bibliografía



A. Tanembaum, Redes de Computadores (4a ed.): Capítulo 5

Apartados: 5.6.1, 5.6.2 y 5.6.3