Tema 4

Mecanismos de traducción de direcciones

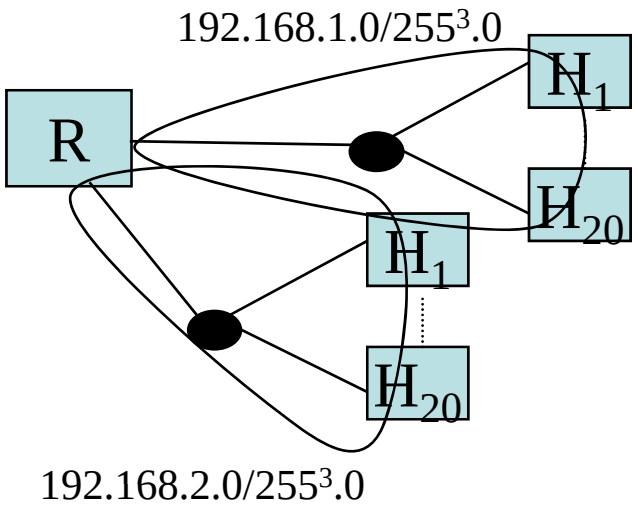
NAT (*Network Address Translation*)

Índice

Introducción (I)

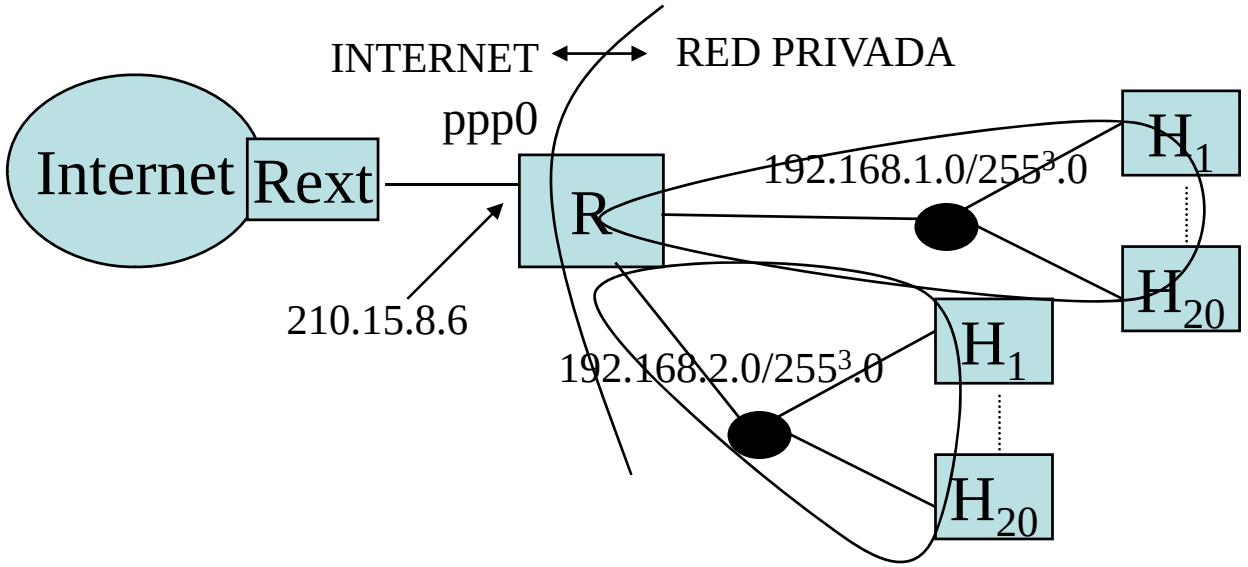
- La IANA (*Internet Assigned Numbers Authority*) ha reservado una serie de direcciones IP "de direccionamineto privado":
  - No han sido otorgadas a ninguna organización de Internet => no pueden existir en Internet datagramas con estas direcciones en el campo origen o destino.
  - Se recomienda su utilización en redes IP privadas (distintas a Internet).

1 dirección de red de clase A:10.0.0.0 / 255.0.0.0
16 direcciones de red de clase B:
172.16.0.0/255.255.0.0
...
172.31.0.0/255.255.0.0
256 direcciones de red de clase C:
192.168.0.0 / 255.255.255.0
...
192.168.255.0 / 255.255.255.0



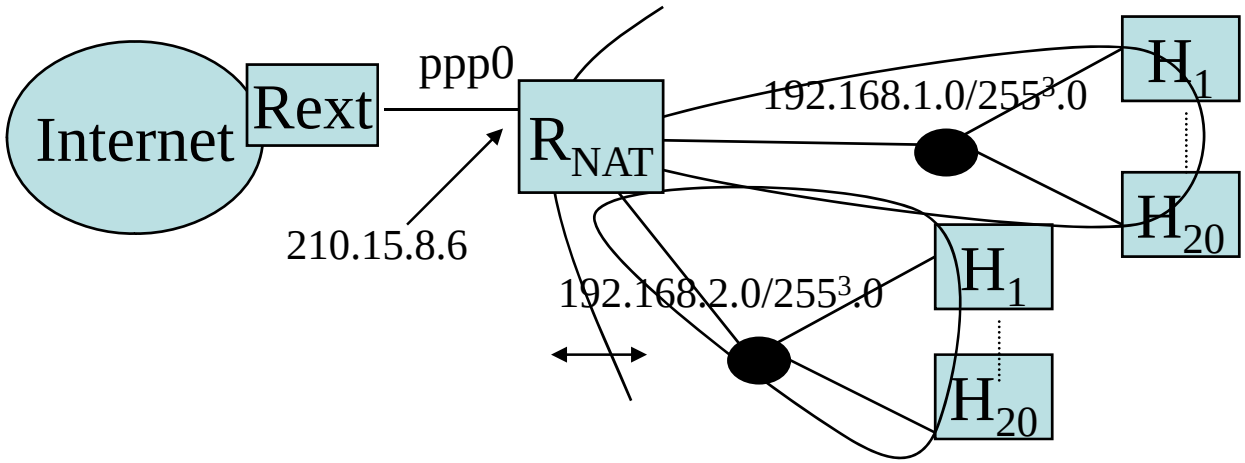
Introducción (II)

- ¿Qué pasa si conectamos nuestra red privada a Internet?. ¡Los dispositivos con IP privada no pertenecen a Internet!
  - *Routers* de Internet no saben cómo encaminar datagramas con dirección IP privada => desechan esos datagramas.
- Conclusión: Necesidad de traducción de direcciones IP!!!



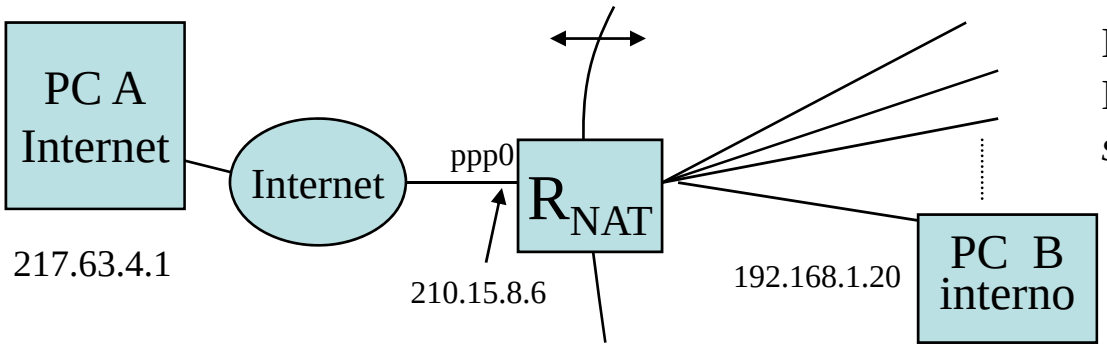
Introducción (III)

- NAT = *Network Address Translation* = conjunto de procedimientos de traducción de direcciones.
- Implementados en routers frontera entre dos redes IP, con espacios de direccionamiento distintos (típicamente Internet, y red con direccionamiento privado)
  - *Router* frontera con 1 o varias interfaces a red IP 1 y 1 o varias interfaces a red IP 2.
  - **Requisito imprescindible: exista un único *router* frontera**
    - Todo el tráfico entre ambas redes IP atraviesa ese *router*.
    - Único dispositivo a configurar. El proceso de traducción de direcciones es transparente al resto de dispositivos de ambas redes IP.



NAT estático (multidirección) (I)

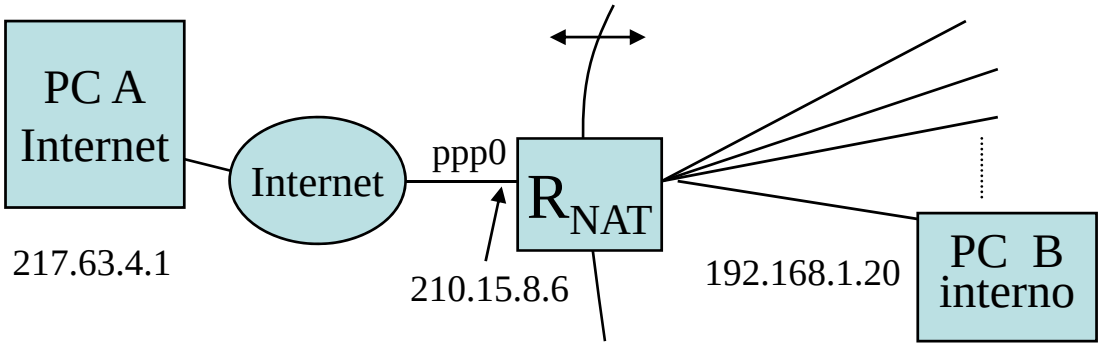
- Ejemplo: *Router* de proveedor de servicios (ISP) entre Internet y usuarios a los que asigna una dirección privada dinámicamente.
  - *Router* dispone de una dirección de clase C para sus usuarios => 254 direcciones IP externas.
  - Admite 254 usuarios conectados simultáneamente. A cada uno de ellos le asigna una dirección IP del *pool* de 254 direcciones, durante su conexión.



Nº usuarios del ISP > 254
Nº máx. usuarios conectados *simultáneamente* = 254

Dirección de clase C externa: 200.1.1.0 / 255.255.255.0
Dirección de clase C interna: 192.168.1.0 / 255.255.255.0

NAT estático (multidirección) (II)



- Traducción de campos **IP origen e IP destino** mediante información almacenada en la tabla (modificada con *login/logout* de usuarios).
- Traducción transparente para PC A y PC B.

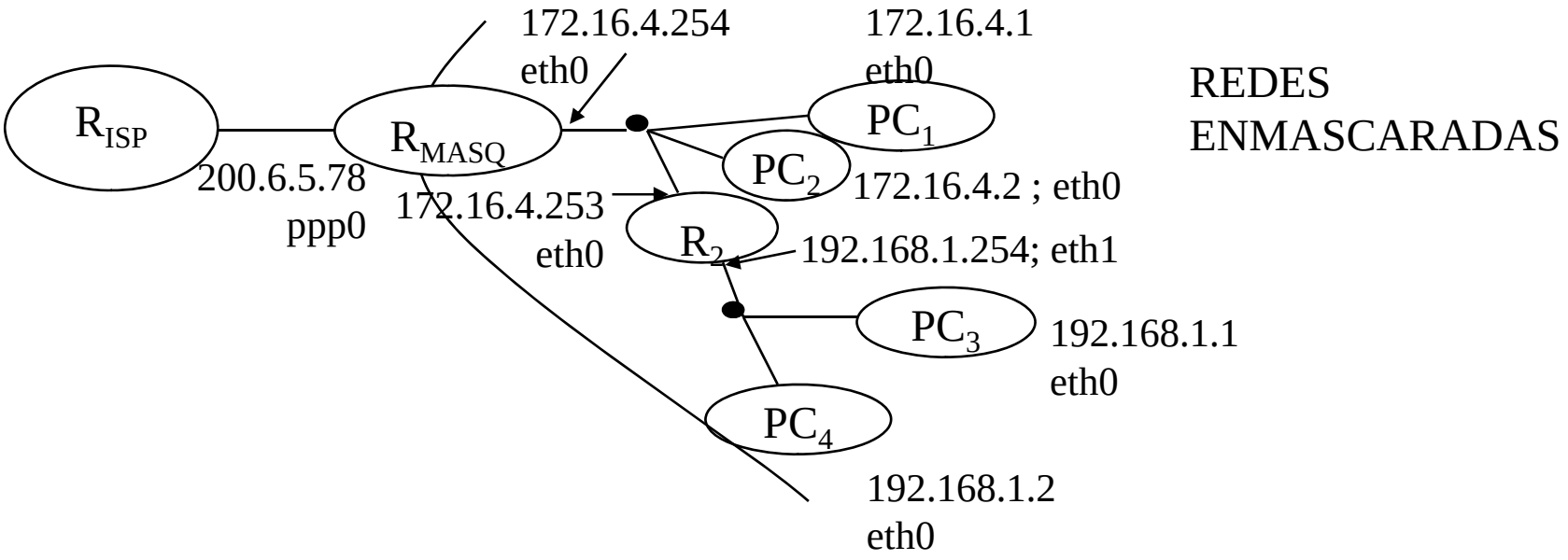
	IP origen	Porigen	IPdestino	Pdestino
B→R	192.168.1.20	3000	217.63.4.1	80
R →A	200.1.1.20	3000	217.63.4.1	80
A →R	217.63.4.1	80	200.1.1.20	3000
R →B	217.63.4.1	80	!92.168.1.20	3000

Tabla traducción NAT

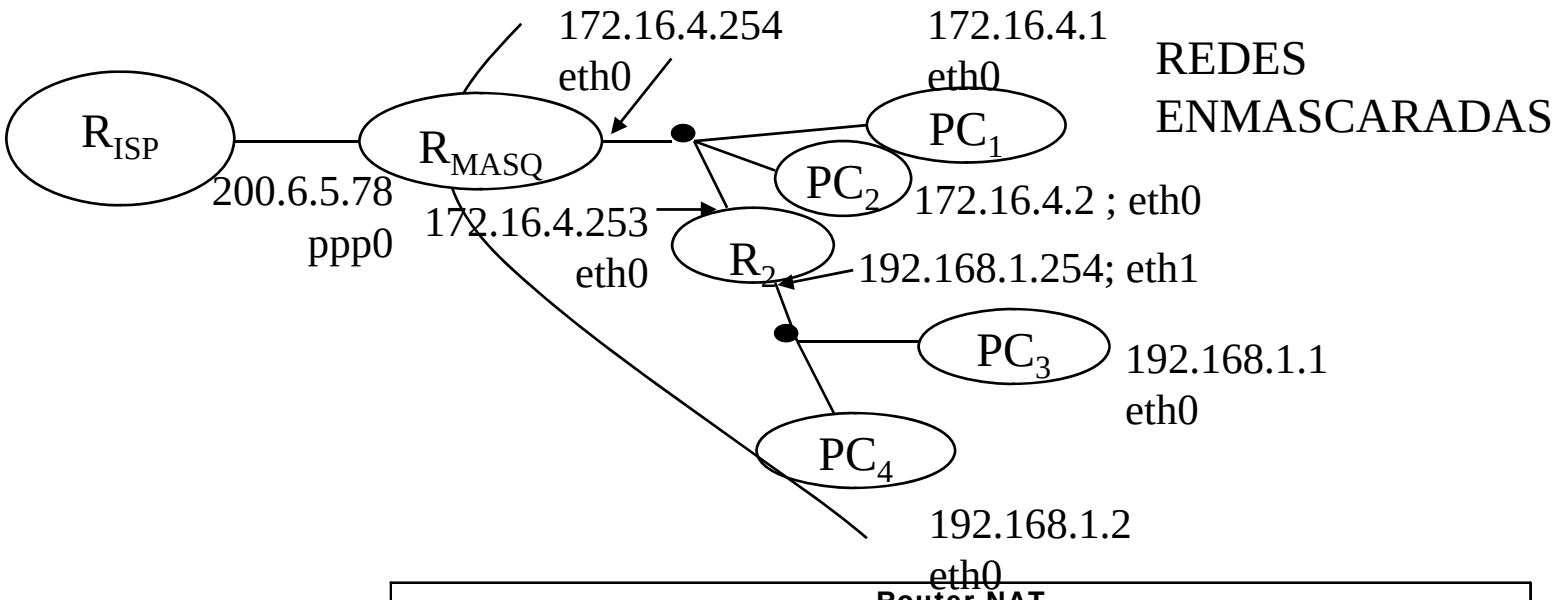
IP externa	IP interna
200.1.1.20	192.168.1.20
200.1.1.1	192.168.1.1
200.1.1.72	192.168.1.72
200.1.1.3	192.168.1.3
200.1.1.4	192.168.1.4
200.1.1.75	192.168.1.75
200.1.1.6	192.168.1.6

NAPT (*Port-Mapped NAT*) (I)

- NAPT (IP-Masquerading, “Conexión compartida a Internet”) = Traducción de direcciones empleando el puerto TCP/UDP como soporte.
- Ejemplo: Router ADSL da salida a Internet a una red Ethernet privada.
  - *Router* dispone de una única dirección IP, asignada por el ISP durante el arranque (dinámicamente, o estáticamente): p.e. 210.15.8.6
  - Red interna de número arbitrario de usuarios, con direccionamiento privado.
  - Una única dirección IP externa compartida por todos. Transparentemente a dispositivos en Internet y a red interna. ¿Cómo?



NAPT (*Port-Mapped NAT*) (II)

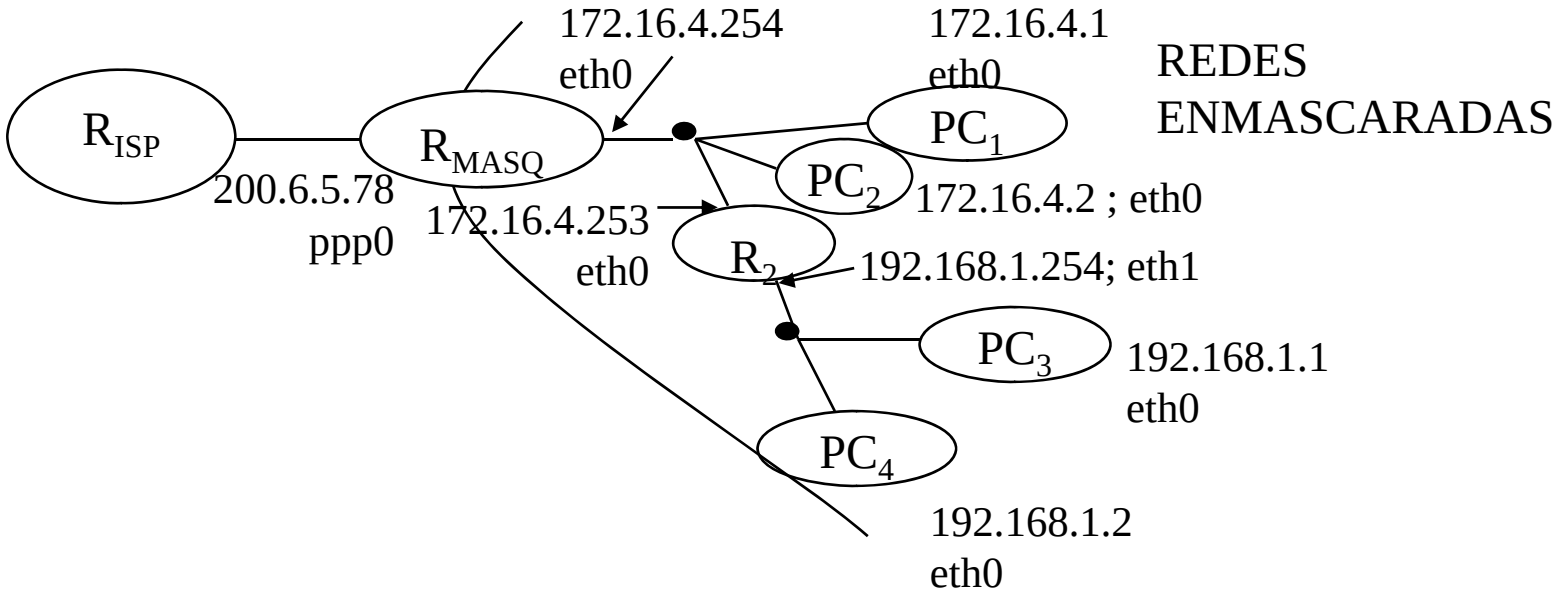


Tablas de encaminamiento: no se ven modificadas por la existencia de NAPT.

Router NAT			
IP dest	**Máscara**	**Interfaz**	**Gateway**
172.16.0.0	255.255.0.0	eth0	---
192.168.1.0	255.255.255.0	eth0	172.16.4.253
0.0.0.0	0.0.0.0	ppp0	---

Router 2			
IP dest	**Máscara**	**Interfaz**	**Gateway**
172.16.0.0	255.255.0.0	eth0	---
192.168.1.0	255.255.255.0	eth1	---
0.0.0.0	0.0.0.0	eth0	172.16.4.254

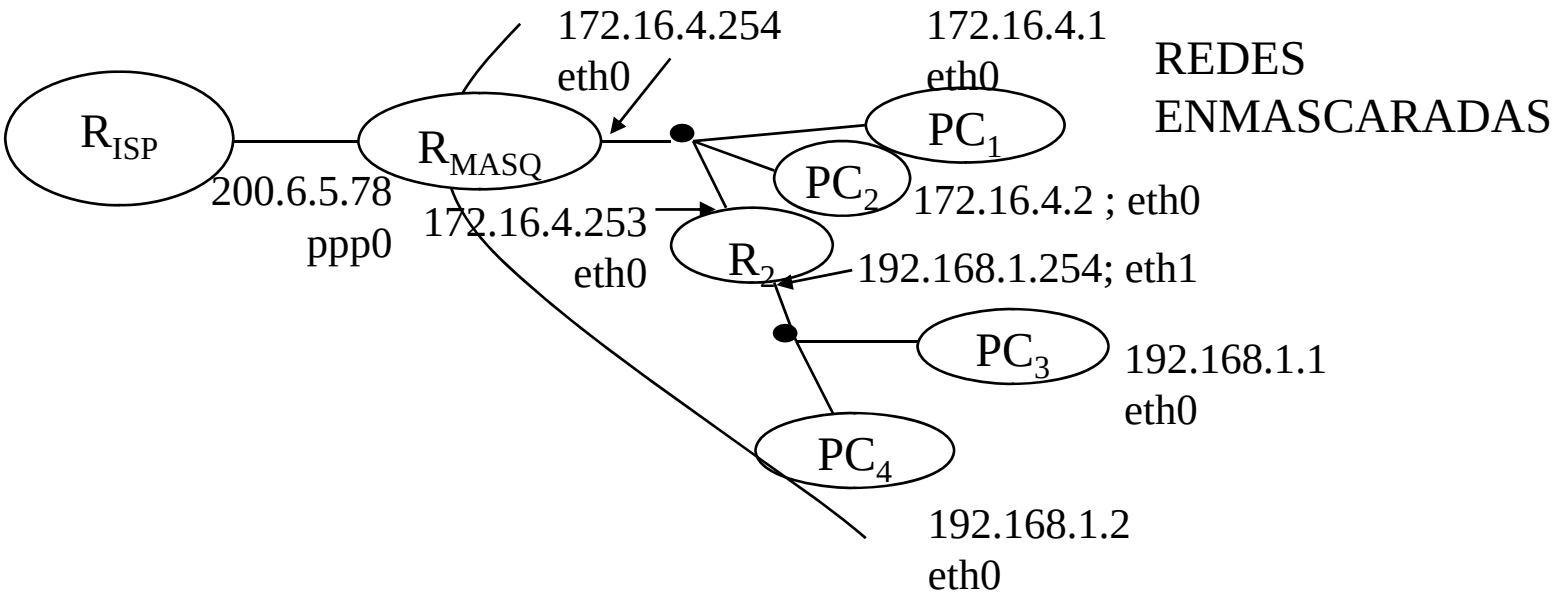
NAPT (*Port-Mapped NAT*) (III)



PC1-PC2			
IP dest	**Máscara**	**Interfaz**	**Gateway**
172.16.0.0	255.255.0.0	eth0	---
192.168.1.0	255.255.255.0	eth0	172.16.4.253
0.0.0.0	0.0.0.0	ppp0	172.16.4.254

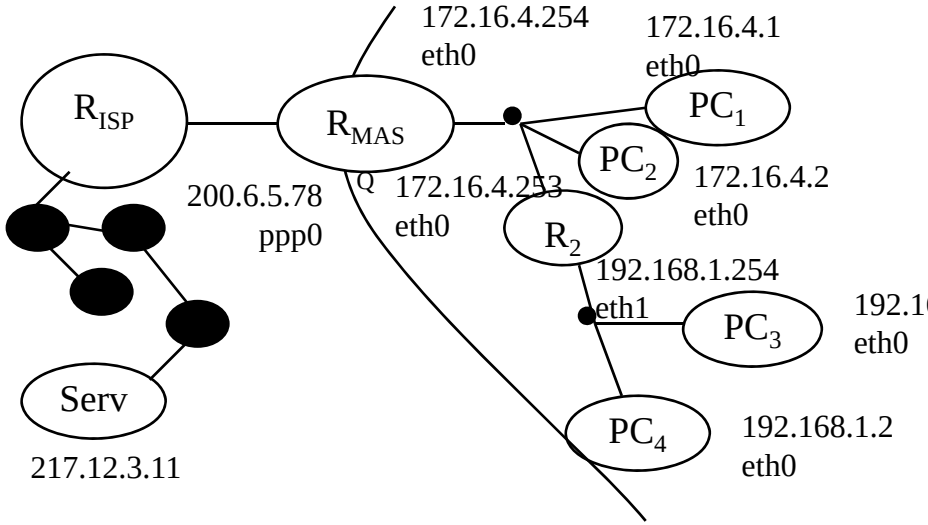
PC3-PC4			
IP dest	**Máscara**	**Interfaz**	**Gateway**
192.168.1.0	255.255.255.0	eth0	---
0.0.0.0	0.0.0.0	eth0	192.168.1.254

NAPT (*Port-Mapped NAT*) (IV)



Router ISP			
IP dest	**Máscara**	**Interfaz**	**Gateway**
200.6.5.78	255.255.255.255	Int	---
...	...	...	...

NAPT (*Port-Mapped NAT*) (V)

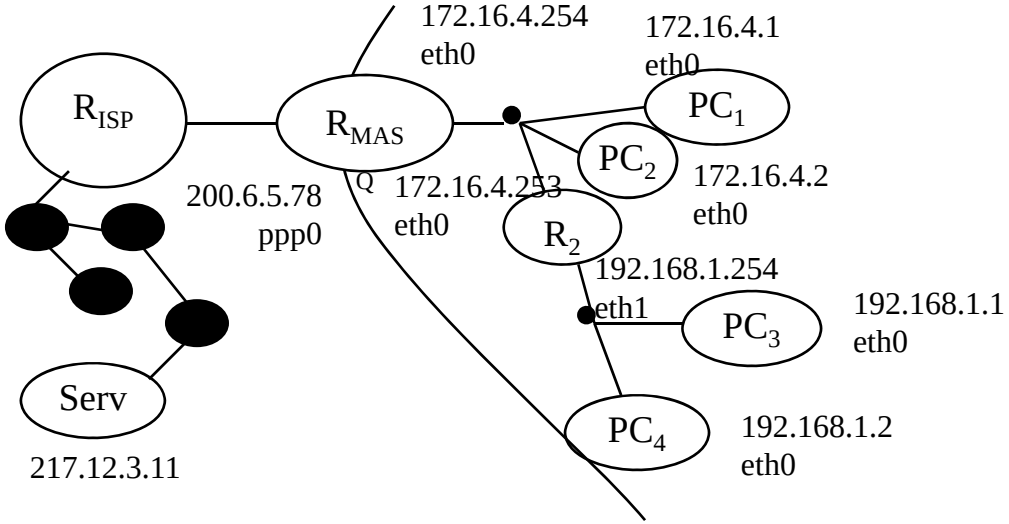


Ejemplo:

- Conexión TCP entre navegador en PC3 (192.168.1.1) y servidor Web en Internet (217.12.3.11)

1. PC 3 genera datagrama con segmento TCP de inicio de conexión:
   - Origen = (192,168,1.1 ; puerto origen (puerto efímero) = 2000)
   - Destino = (217.12.3.11 ; puerto destino = 80
2. Datagrama encaminado por R_2 hacia R_{Masq}.
3. R_{Masq} recibe datagrama por interfaz interna.
   - Observa IP destino => lee tabla encaminamiento => sabe debe transmitirse por interfaz externa => debe hacer traducción de dirección origen.

NAPT (*Port-Mapped NAT*) (VI)

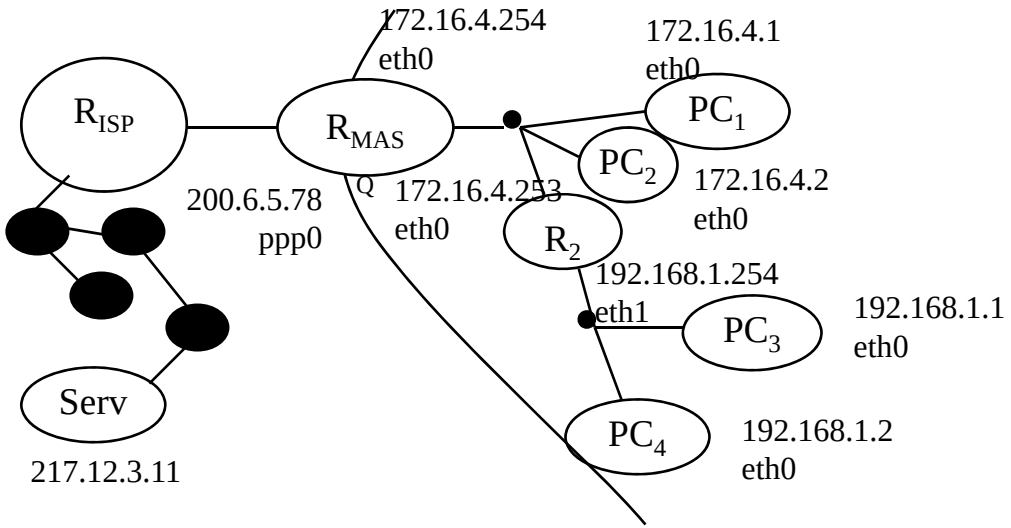


IP origen	Puerto origen inicial	Puerto origen traducido (P_{NAPT})

IP origen	Puerto origen inicial	Puerto origen traducido (P_{NAPT})
192.168.1.1	2000	61000

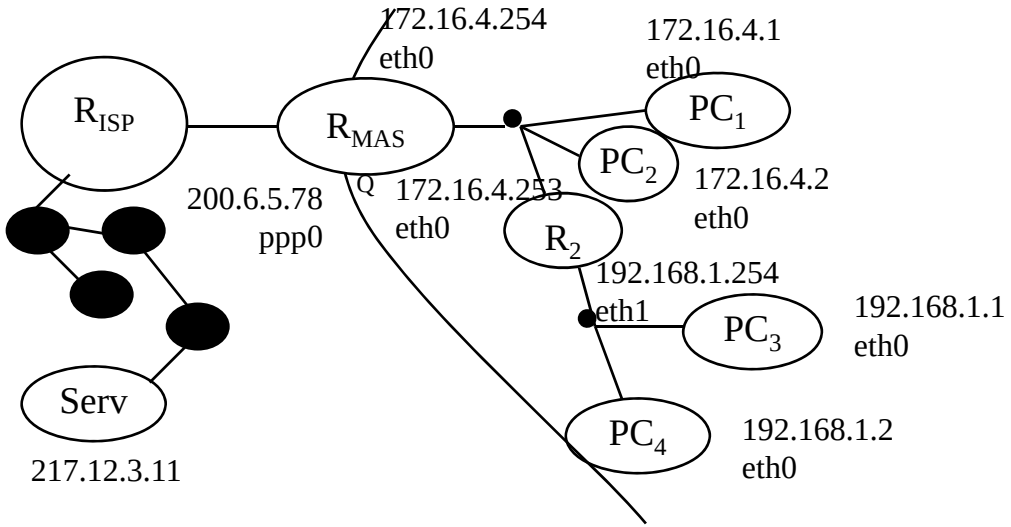
- Busca en tabla Masquerading TCP (192.168.1.1;2000) en campos IP_o, P_o
  - Encuentra => conexión TCP ya está siendo enmascarada
  - No encuentra => no está siendo enmascarada => reserva puerto TCP libre (en general, numeración > 61000) y añade a la tabla
- Transmite datagrama:
  - Origen (200.6.5.78;61000)
  - Destino (217.12.3.11;80)

NAPT (*Port-Mapped NAT*) (VII)



4. Datagrama viaja hacia servidor. Al ser recibido. Servidor responde con datagrama
   - Origen (217.12.3.11;80)
   - Destino (200.6.5.78;61000)
5. Datagrama llega a R_{Masq} (dirigido a´200.6.5.78)
   - ¿Puerto 61000 en tabla NAPT (campo “puerto origen traducido“)?
     - Sí => paso (6)
     - No => ¿hay alguna apliicación escuchando en puerto 61000? (Si no => error => descarta)

NAPT (*Port-Mapped NAT*) (VIII)



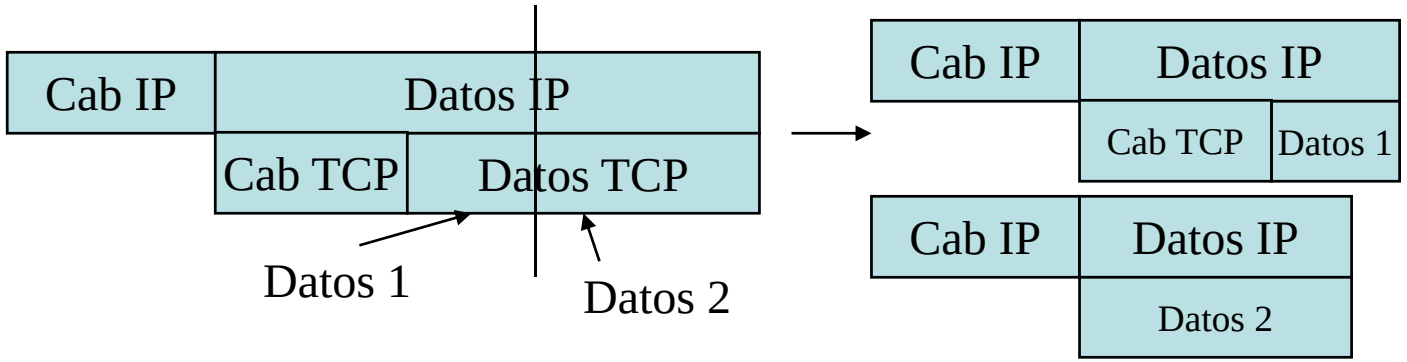
6. Realiza función NAPT => cambia destino datagrama utilizando valores de la entrada de la tabla NAPT:
   - Origen: (217.12.3.11 ; 80)
   - Destino: (192.168.1.1 ; 2000)
7. Observa tabla de encaminamiento, y determina por dónde debe transmitirlo (192.168.1.1 => eth0 con GW = 172.16.4.253)

NAPT (*Port-Mapped NAT*) (IX)

- Exactamente mismo procedimiento para enmascarar:
  - conexiones TCP con tabla NAPT-TCP (emplea puertos TCP).
  - "conexiones" UDP con tabla NAPT-UDP (emplea puertos UDP)
  - mensajes ICMP con tabla NAPT-ICMP (emplea *Identifier* y *Sequence Number* ICMP)
- Ventajas:
  - Es transparente a red interna y a red externa. Ejemplo:
    - PC interno cree que la conexión TCP es (192.168.1.1,2000 ; 217.12.3.11 , 80)
    - Servidor cree que la conexión TCP es (217.12.3.11 , 80 ; 200.6.5.78 , 61000)
- Desventajas NAPT:
  1. Procedimiento requiere que iniciador de conexión sea interno: típicamente, cliente en red interna, servidor en red externa.
     - Ejemplo: ¿Cómo podemos poner servidor Web en red interna y que sea accesible desde el exterior?

NAPT (*Port-Mapped NAT*) (X)

2. R_{Masq} hace procesamiento relativamente costoso:
   - Cada conexión enmascarada ocupa un puerto TCP/UDP/ICMP y una entrada en la tabla NAPT correspondiente
   - Necesario mecanismo de temporizadores que lleven la cuenta de las conexiones enmascaradas no utilizadas para liberar recursos.
   - Pb con fragmentación. P.e. fragmento con segmento TCP por recibido por interfaz externa =>
     - Únicamente primer fragmento contiene cabecera TCP
     - ¿Qué se hace con la llegada del segundo fragmento, sin cabecera TCP?
     - Conclusión: R_{Masq} debe capturar fragmentos y almacenar información para poder deshacer Masquerading.



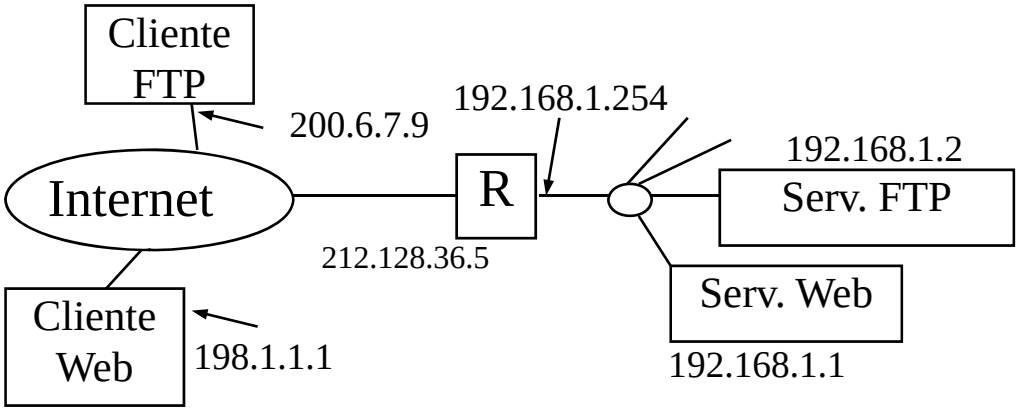
NAPT (*Port-Mapped NAT*) (XI)

- Se realizan cambios en la cabecera IP y TCP => recalcular *checksum* IP y *checksum* TCP.
- ¿Qué pasa si aplicaciones transmiten IP origen / puerto origen como datos de aplicación?
  - => Masquerading debe leer datos de aplicación y hacer la traducción. Puede que esto exija recalcular número de secuencia TCP!!!
  - Imposible comprobar datos de todas las aplicaciones. Se implementa esta funcionalidad para algunas aplicaciones conocidas.
  - Ejemplo: cliente FTP transmite número de puerto origen como datos de aplicación => R_{Masq} debe traducir ese número de puerto.
  - Ejemplo: algunos mensajes ICMP incluyen direcciones IP en los datos ICMP. También deben ser traducidos.

NAPT (*Port-Mapped NAT*) (XII)

Funcionalidad de puertos visibles

- Funcionalidad añadida a R_{Masq} que permita la colocación de servidores dentro de la red interna.
- Ejemplo:



Servidor FTP:

Real: 192.168.1.2 ; 21

Exterior: 212.128.36.5 ; 3001

Servidor Web:

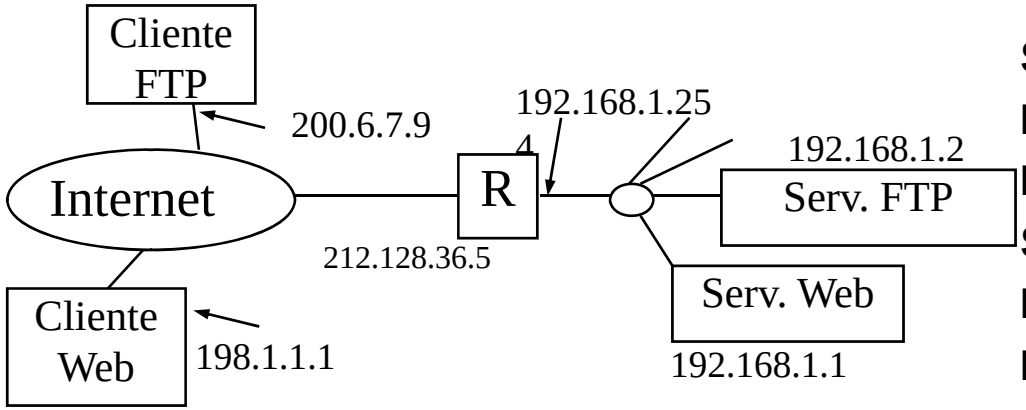
Real: 192.168.1.1 ; 80

Exterior: 212.128.36.5 ; 3000

Tabla de puertos visibles		
IP servidor interno	*Puerto servidor interno*	*Puerto público (externo)*
192.168.1.1	*80*	*3000*
192.168.1.2	*21*	*3001*

NAPT (*Port-Mapped NAT*) (XIII)

Funcionalidad de puertos visibles



Servidor FTP:

Real: 192.168.1.2 ; 21

Exterior: 212.128.36.5 ; 3001

Servidor Web:

Real: 192.168.1.1 ; 80

Exterior: 212.128.36.5 ; 3000

Tabla de puertos visibles		
IP servidor interno	*Puerto servidor interno*	*Puerto público (externo)*
192.168.1.1	*80*	*3000*
192.168.1.2	*21*	*3001*

	IP origen	Porigen	IPdestino	Pdestino
CW→R	198.1.1.1	1702	212.128.36.5	3000
R →SW	198.1.1.1	1702	192.168.1.1	80
SW →R	192.168.1.1	80	198.1.1.1	1702
R →CW	212.128.36.5	3000	198.1.1.1	1702

Puerto 3000 en tabla puertos => traduce IP/puerto origen

(192.168.1.1;80) en tabla puertos => traduce IP/puerto origen

NAPT (*Port-Mapped NAT*) (XIV)

Funcionalidad de puertos visibles

- Características:
  - Objetivo: Proporcionar servicio en servidor (IP_{serv},P_{serv}) en red interna, aunque de cara al exterior aparece como proporcionado por ($IP_{RMasq-ext}$, $P_{RMasq-reservado}$).
  - Procesamiento sencillo:
    - Se requiere únicamente una tabla para cada protocolo (en general, sólo para protocolo TCP).
    - **No es necesario almacenar información específica para cada conexión (al contrario que NAPT).**
    - No es necesario que la conexión se inicie desde la red interna.
    - Sí es necesario recalcular *checksum* IP y TCP de todos datagramas.

NAPT (*Port-Mapped NAT*) (XV)

Funcionalidad de red interna visible

- Funcionalidad añadida a R_{Masq} que permite la colocación de redes internas con direcciones IP reales (no privadas).
- Objetivo: datagramas a y desde esta red no sufran traducción de direcciones.

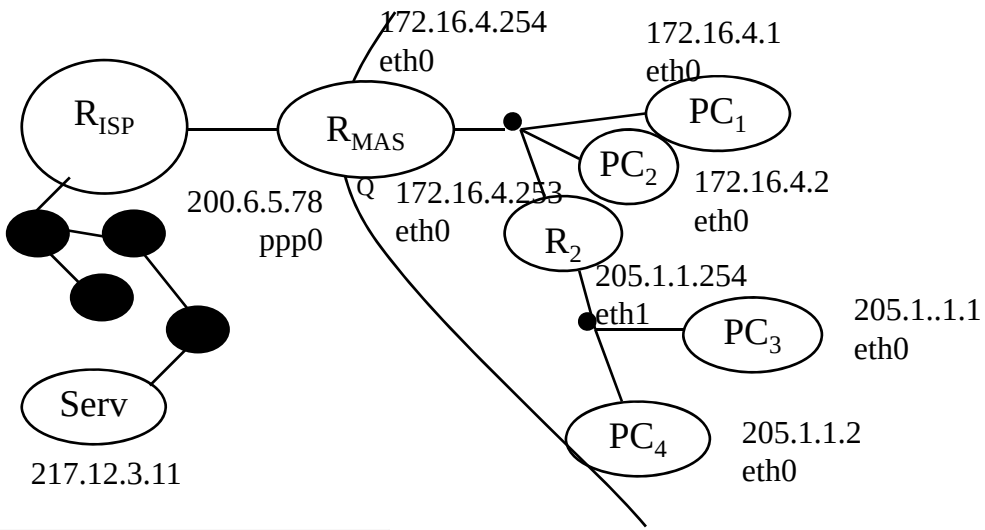
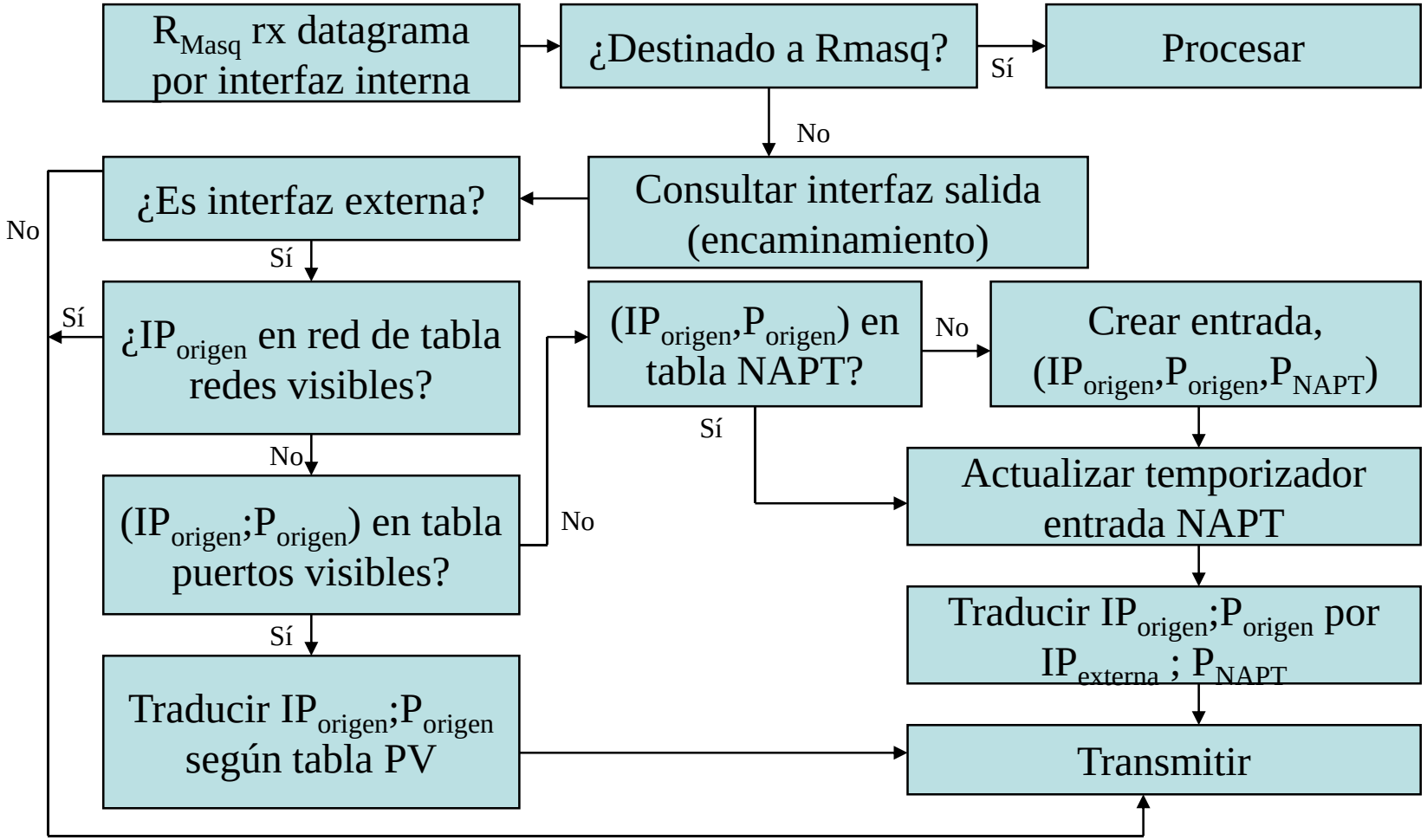


Tabla de Subredes visibles	
IP subred	Máscara de subred
205.1.1.0	255.255.255.0

	IP origen	Porigen	IPdestino	Pdestino
$PC_3 \rightarrow R$	205.1.1.1	2100	217.12.3.11	80
$R \rightarrow Serv$	205.1.1.1	2100	217.12.3.11	80
$Serv \rightarrow R$	217.12.3.11	80	205.1.1.1	2100
$R \rightarrow PC_3$	217.12.3.11	80	205.1.1.1	2100

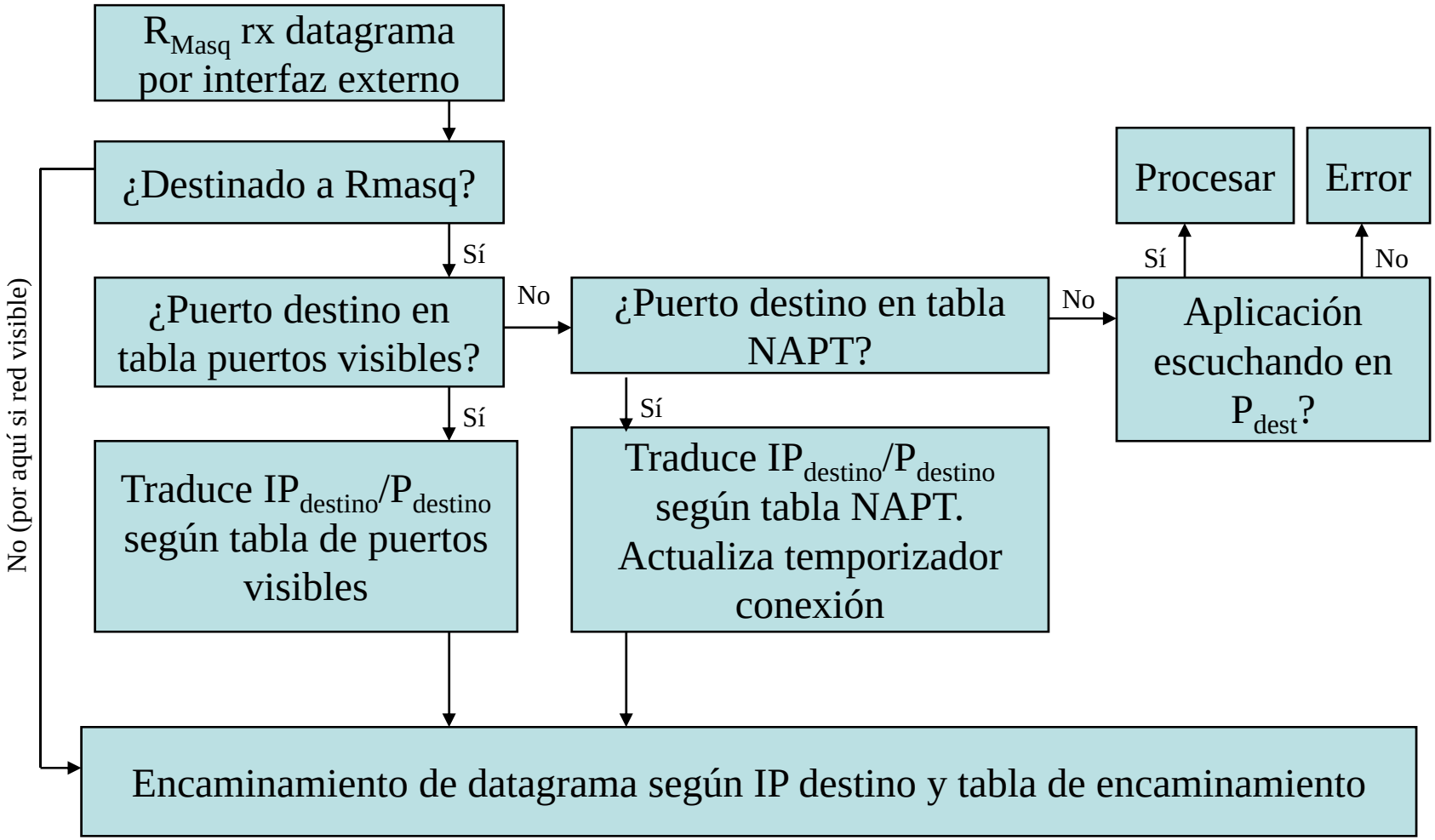
NAPT (*Port-Mapped NAT*) (XVI)

Algoritmo completo (TCP)



NAPT (*Port-Mapped NAT*) (XVII)

Algoritmo completo (TCP)



Bibliografía recomendada

- Douglas E. Comer, “Internetworking with TCP/IP Vol. 1: Principles, Protocols, and Architecture. 5th Edition”, Prentice Hall 2006.
  - Capítulo 19: *Private Network Interconnection (NAT, VPN).*
- NAT (*The IP Network Address Translator):* RFC 1631.
- Bibliografía complementaria:
  - (1998) RFC 2391. *Load Sharing using IP Network Address Translation (LSNAT)*.
  - (2000) RFC 2766. *Network Address Translation – Protocol Translation (NAT-PT).*