

# Ingeniería Técnica de Telecomunicación, Especialidad Telemática

## Laboratorio de Redes y Servicios de Comunicaciones



### **Cuestiones y Ejercicios de Teoría**

**María Victoria Bueno Delgado**  
**Pablo Pavón Mariño**



# INDICE

---

## **BLOQUE TEMÁTICO 1. ICMP, TCP Y UDP -----7**

1.1	IP -----	7
	Cuestión 1 (Diciembre 2001-cuestión 3) -----	7
1.2	TCP y UDP -----	7
	Cuestión 1 (Diciembre 2001-cuestión 2) -----	7
	Cuestión 2 (Septiembre 2002-cuestión 1) -----	7
	Problema 1 (Septiembre 2001-cuestión 1) -----	8
	Problema 2 (Septiembre 2004-problema 1) -----	8
	Problema 3 (Diciembre 2004-problema 1) -----	9
	Problema 4 (Junio 2005-problema 1) -----	9
	Problema 5 (Septiembre 2005-problema 2) -----	10
	Problema 6 (Diciembre 2005-problema 2) -----	11
	Problema 7 (Junio 2006-problema 2) -----	11
	Problema 8 (Septiembre 2006-problema 2) -----	12
	Problema 9 (Febrero 2007-problema 1) -----	13
	Problema 10 (Junio 2007-problema 1) -----	13
	Problema 11 (Septiembre 2007-problema 1) -----	14
	Problema 12 (Febrero 2008-problema 1) -----	15
	Problema 13 (Junio 2008-problema 1) -----	16
	Problema 14 (Septiembre 2008-problema 1) -----	17

## **BLOQUE TEMÁTICO 2. EXTENSIONES DE DIRECCIONAMIENTO IPV4 - 19**

2.1	Proxy ARP -----	19
	Problema 1. (Junio 2003-cuestión 2) -----	19
	Problema 2 (Junio 2004-problema 1) -----	20
	Problema 3 (Septiembre 2005-problema 1) -----	21
	Problema 4 (Diciembre 2005-problema 1) -----	23
	Problema 5 (Junio 2006-problema 1) -----	24
	Problema 6 (Septiembre 2006-problema 1) -----	26
2.2	Direccionamiento de subred, CIDR y líneas punto a punto -----	27
	Problema 1 (Junio 2003-problema 2) -----	27
	Problema 2 (Junio 2004-problema 3) -----	29
	Problema 3 (Septiembre 2004-problema 3) -----	32

Problema 4 (Junio 2003-cuestión 1)-----	33
Problema 5 (Junio 2003-problema 2) -----	33
Problema 6 (Septiembre 2003-problema 2) -----	35
Problema 7 (Diciembre 2004-problema 3) -----	38
Problema 8 (Febrero 2007-problema 2) -----	40
Problema 9 (Junio 2007-problema 2) -----	41
Problema 10 (Septiembre 2007-problema 2)-----	42
Problema 11 (Febrero 2008-problema 2) -----	44
Problema 12 (Junio 2008-problema 2)-----	45
Problema 13 (Septiembre 2008-problema 2)-----	47

**BLOQUE TEMÁTICO 3. ALGORITMOS DE ENCAMINAMIENTO  
DINÁMICO. SISTEMAS AUTÓNOMOS ----- 49**

Cuestiones (Diciembre 2001-cuestión 1) -----	49
Problema 1 (Septiembre 2002-cuestión 3) -----	49
Problema 2 (Junio 2005-problema 2) -----	52
Problema 3 (Septiembre 2005-problema 3) -----	53
Problema 4 (Diciembre 2005-problema 3) -----	55
Problema 5 (Junio 2006-problema 3) -----	56
Problema 6 (Septiembre 2006-problema 3) -----	57
Problema 7 (Febrero 2007-problema 3) -----	59
Problema 8 (Junio 2007-problema 3) -----	61
Problema 9 (Septiembre 2007-problema 3) -----	63
Problema 10 (Febrero 2008-problema 3)-----	64
Problema 11 (Junio 2008-problema 3)-----	66
Problema 12 (Septiembre 2008-problema 3)-----	68

**BLOQUE TEMÁTICO 4. MECANISMOS DE TRADUCCIÓN DE  
DIRECCIONES (NAT) ----- 71**

Problema 1 (Septiembre 2002-cuestión 2) -----	71
Problema 2 (Junio 2003-problema 1) -----	72
Problema 3 (Septiembre 2003-problema 1) -----	74
Problema 4 (Junio 2004-problema 2) -----	77
Problema 5 (Septiembre 2004-problema 2) -----	81
Problema 6 (Diciembre 2004-problema 2) -----	85
Problema 7 (Junio 2005-problema 3) -----	88
Problema 8 (Septiembre 2005-problema 4) -----	93

Problema 9 (Junio 2006-problema 4) -----	95
Problema 10 (Septiembre 2006-problema 4)-----	98
Problema 11 (Febrero 2007-problema 4)-----	100
Problema 12 (Junio 2007-problema 4)-----	102
Problema 13 (Septiembre 2007-problema 4)-----	105
Problema 14 (Febrero 2008-problema 4)-----	108
Problema 15 (Junio 2008-problema 4)-----	111
Problema 16 (Septiembre 2008-problema 4)-----	113



# Bloque temático 1. ICMP, TCP y UDP

---

## 1.1 IP

### Cuestión 1 (Diciembre 2001-cuestión 3)

- 1) Describa el formato de un paquete IP (explicación de todos los campos).

## 1.2 TCP y UDP

### Cuestión 1 (Diciembre 2001-cuestión 2)

- 1) Defina brevemente “*Maximum Segment Size* del protocolo TCP”.

- 2) Defina brevemente “Ventana de transmisión del protocolo TCP”.

### Cuestión 2 (Septiembre 2002-cuestión 1)

- 3) Para una conexión TCP entre las máquinas A y B, responde clara y brevemente a las siguientes preguntas:

- ¿Para qué utiliza A el campo *Window Size* (tamaño ventana) de la cabecera TCP de los segmentos que transmite a B?

- A envía un segmento a B con el campo *Sequence* = 24587653. ¿En qué afecta esto al campo *Sequence* de los datagramas que B envía a A?. ¿Por qué?

- A envía un segmento a B con el campo ACK = 21344366. ¿En qué afecta esto al campo ACK de los datagramas que B envía a A?. ¿Por qué?

### Problema 1 (Septiembre 2001-cuestión 1)

Un cliente HTTP establece una conexión TCP con un servidor HTTP. El extremo cliente informa de que el tamaño máximo de segmento que está dispuesto a recibir es de 1460, mientras que el extremo servidor informa que el tamaño máximo de segmento que está dispuesto a recibir es 576. Escriba el contenido de los campos de la cabecera TCP vacíos en la siguiente secuencia de intercambio de segmentos, suponiendo que no existe pérdida ni desorden en la entrega.

P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
1116	80	3779	---		Petición de inicio de conexión
		665			2º mensaje de inicio de conexión
					3º mensaje de inicio de conexión
					Cliente envía 200 bytes de datos
					Servidor envía 300 bytes de datos
					Cliente envía 200 bytes de datos
					Cliente envía 100 bytes de datos
					Servidor envía 100 bytes de datos

### Problema 2 (Septiembre 2004-problema 1)

Un cliente FTP establece una conexión TCP con un servidor FTP. El extremo cliente informa de que el tamaño máximo de segmento que está dispuesto a recibir es de 576, mientras que el extremo servidor informa que el tamaño máximo de segmento que está dispuesto a recibir es 1460. Escriba el contenido de los campos de la cabecera TCP vacíos en la siguiente secuencia de intercambio de segmentos, suponiendo que no existe pérdida ni desorden en la entrega, salvo en las ocasiones que se indica lo contrario.

P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
2001	21	2600	---		Petición de inicio de conexión
		6000			2º mensaje de inicio de conexión
					3º mensaje de inicio de conexión

					Cliente envía 150 bytes de datos
					Servidor envía 300 bytes de datos (segmento perdido)
					Cliente envía 200 bytes de datos
					Cliente envía 100 bytes de datos (segmento perdido)
					Servidor envía 100 bytes de datos
					Servidor reenvía 300 bytes de datos de segm. perdido
					Cliente reenvía 100 bytes de datos de segm. perdido

### Problema 3 (Diciembre 2004-problema 1)

Una aplicación A establece una conexión TCP con una aplicación B. El extremo iniciador informa de que el tamaño máximo de segmento que está dispuesto a recibir es de 1460, mientras que el extremo aceptador de la conexión informa que el tamaño máximo de segmento que está dispuesto a recibir es 576. Escriba el contenido de los campos de la cabecera TCP vacíos en la siguiente secuencia de intercambio de segmentos, suponiendo que no existe pérdida ni desorden en la entrega, salvo en las ocasiones que se indica lo contrario.

P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
1200	8000	790			Petición de inicio de conexión
		46500			2º mensaje de inicio de conexión
					3º mensaje de inicio de conexión
					B envía 100 bytes de datos (segmento perdido)
					A envía 200 bytes de datos (segmento perdido)
					B envía 200 bytes de datos
					A envía 100 bytes de datos (segmento perdido)
					B reenvía el segmento perdido
					A reenvía 1º segmento perdido
					B envía segmento de 300 bytes
					A reenvía 2º segmento perdido

### Problema 4 (Junio 2005-problema 1)

Una aplicación A establece una conexión TCP con una aplicación B. El extremo iniciador informa de que el tamaño máximo de segmento que está dispuesto a recibir es

de 576, mientras que el extremo aceptador de la conexión informa que el tamaño máximo de segmento que está dispuesto a recibir es 1460. Escriba el contenido de los campos de la cabecera TCP vacíos en la siguiente secuencia de intercambio de segmentos, suponiendo que no existe pérdida ni desorden en la entrega, salvo en las ocasiones que se indica lo contrario.

P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
8000	1200	100			Peticion de inicio de conexión
		2000			2º mensaje de inicio de conexión
					3º mensaje de inicio de conexión
					<i>B</i> envía 100 bytes de datos nuevos (segmento perdido)
					<i>A</i> envía 200 bytes de datos nuevos (segmento perdido)
					<i>B</i> reenvía 100 bytes de datos (segmento perdido)
					<i>A</i> envía 200 bytes de datos nuevos (recibido)
					<i>B</i> envía 200 bytes de datos nuevos (recibido)
					<i>A</i> reenvía 1º segmento perdido (recibido)
					<i>B</i> envía 300 bytes de datos nuevos (recibido)
					<i>B</i> reenvía segmento perdido

### Problema 5 (Septiembre 2005-problema 2)

Una aplicación A establece una conexión TCP con una aplicación B. El extremo iniciador informa de que el tamaño máximo de segmento que está dispuesto a recibir es de 1460, mientras que el extremo aceptador de la conexión informa que el tamaño máximo de segmento que está dispuesto a recibir es 400. Escriba el contenido de los campos de la cabecera TCP vacíos en la siguiente secuencia de intercambio de segmentos, suponiendo que no existe pérdida ni desorden en la entrega, salvo en las ocasiones que se indica lo contrario.

P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
1200	8000	2000	---		Peticion de inicio de conexión
		100			2º mensaje de inicio de conexión
					3º mensaje de inicio de conexión
					<i>A</i> envía 200 bytes de datos nuevos (segmento perdido)
					<i>A</i> envía 500 bytes de datos nuevos (segmento perdido)
					<i>B</i> envía 100 bytes de datos (recibido)
					<i>A</i> reenvía 200 bytes de datos de 1º segm. perdido (también se pierde)

					A reenvía 500 bytes de datos de 2° segm. perdido (recibido)
					B envía 300 bytes de datos (recibido)
					A reenvía 200 bytes de datos de 1° segm. perdido (también se pierde)
					B reenvía segmento de 300 bytes anterior

### Problema 6 (Diciembre 2005-problema 2)

Una aplicación A establece una conexión TCP con una aplicación B. El extremo aceptador informa de que el tamaño máximo de segmento que está dispuesto a recibir es de 1460, mientras que el extremo iniciador de la conexión informa que el tamaño máximo de segmento que está dispuesto a recibir es 550. Escriba el contenido de los campos de la cabecera TCP vacíos en la siguiente secuencia de intercambio de segmentos, suponiendo que no existe pérdida ni desorden en la entrega, salvo en las ocasiones que se indica lo contrario.

P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
3000	4000	200			Peticion de inicio de conexión
		1000			2° mensaje de inicio de conexión
					3° mensaje de inicio de conexión
					B envía 500 bytes de datos nuevos (segmento perdido)
					B envía 200 bytes de datos nuevos (segmento perdido)
					A envía 150 bytes de datos (recibido)
					B reenvía 500 bytes de datos de 1° segm. perdido (también se pierde)
					B reenvía 200 bytes de datos de 2° segm. perdido (recibido)
					A envía 300 bytes de datos (recibido)
					B reenvía 500 bytes de datos de 1° segm. perdido (también se pierde)
					A reenvía segmento de 300 bytes anterior

### Problema 7 (Junio 2006-problema 2)

Una aplicación A establece una conexión TCP con una aplicación B. El extremo aceptador informa de que el tamaño máximo de segmento que está dispuesto a recibir es de 5000, mientras que el extremo iniciador de la conexión informa que el tamaño máximo de segmento que está dispuesto a recibir es 1460. Escriba el contenido de los campos de la cabecera TCP vacíos que aparecen en la tabla, en la siguiente secuencia de intercambio de segmentos, suponiendo que no existe pérdida ni desorden en la entrega, salvo en las ocasiones que se indica lo contrario.

P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
4000	3000	6000			Petición de inicio de conexión
		1000			2º mensaje de inicio de conexión
					3º mensaje de inicio de conexión
					A envía 300 bytes de datos nuevos (segmento perdido)
					A envía 400 bytes de datos nuevos
					B envía 100 bytes de datos nuevos
					A envía 100 bytes de datos nuevos (segmento perdido)
					B envía 300 bytes de datos nuevos (segmento perdido)
					A reenvía 300 bytes de datos de 1º segmento perdido (recibido)
					B reenvía 300 bytes de datos de 1º segmento perdido (recibido)
					A envía segmento de 1000 bytes de datos nuevos

Suponga que los mecanismos de control de congestión no afectan en este ejemplo al tamaño de la ventana de transmisión. Suponga que en el extremo A, el tamaño inicial de su ventana de transmisión no varía durante la transmisión de los segmentos. Suponga lo mismo en el extremo B. ¿Cuál es el tamaño mínimo de la ventana de transmisión que tiene el extremo A? (es decir, tal que si su tamaño hubiera sido menor, esta secuencia de segmentos no se podría haber producido).

### Problema 8 (Septiembre 2006-problema 2)

Una aplicación A establece una conexión TCP con una aplicación B. El extremo aceptador informa de que el tamaño máximo de segmento que está dispuesto a recibir es de 5000, mientras que el extremo iniciador de la conexión informa que el tamaño máximo de segmento que está dispuesto a recibir es 1460.

Escriba el contenido de los campos de la cabecera TCP vacíos que aparecen en la tabla, en la siguiente secuencia de intercambio de segmentos, suponiendo que no existe pérdida ni desorden en la entrega, salvo en las ocasiones que se indica lo contrario.

P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
7100	2000	1000			Petición de inicio de conexión
		6000			2º mensaje de inicio de conexión
					3º mensaje de inicio de conexión
					A envía 300 bytes de datos nuevos (segmento perdido)

					A envía 400 bytes de datos nuevos
					B envía 100 bytes de datos nuevos
					A envía 100 bytes de datos nuevos (segmento perdido)
					B envía 300 bytes de datos nuevos (segmento perdido)
					A reenvía 300 bytes de datos de 1º segmento perdido (recibido)
					B reenvía 300 bytes de datos de 1º segmento perdido (recibido)
					A envía segmento de 1000 bytes de datos nuevos

### Problema 9 (Febrero 2007-problema 1)

Una aplicación A establece una conexión TCP con una aplicación B. El extremo aceptador informa de que el tamaño máximo de segmento que está dispuesto a recibir es de 1460, mientras que el extremo iniciador de la conexión informa que el tamaño máximo de segmento que está dispuesto a recibir es 2100. Escriba el contenido de los campos de la cabecera TCP vacíos que aparecen en la tabla, en la siguiente secuencia de intercambio de segmentos, suponiendo que no existe pérdida ni desorden en la entrega, salvo en las ocasiones que se indica lo contrario.

P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
31200	2000	15000			Peticion de inicio de conexión
		31000			2º mensaje de inicio de conexión
					3º mensaje de inicio de conexión
					A envía 300 bytes de datos nuevos (segmento perdido)
					A envía 400 bytes de datos nuevos
					B envía 100 bytes de datos nuevos
					A envía 100 bytes de datos nuevos (segmento perdido)
					B envía 300 bytes de datos nuevos (segmento perdido)
					A reenvía 300 bytes de datos de 1º segmento perdido (recibido)
					B reenvía 300 bytes de datos de 1º segmento perdido (recibido)
					A envía segmento de 1000 bytes de datos nuevos

### Problema 10 (Junio 2007-problema 1)

Una aplicación A establece una conexión TCP con una aplicación B. El extremo aceptador informa de que el tamaño máximo de segmento que está dispuesto a recibir es de 1000, mientras que el extremo iniciador de la conexión informa que el tamaño

máximo de segmento que está dispuesto a recibir es 1460. Escriba el contenido de los campos de la cabecera TCP vacíos que aparecen en la tabla, en la siguiente secuencia de intercambio de segmentos, suponiendo que no existe pérdida ni desorden en la entrega, salvo en las ocasiones que se indica lo contrario. Rellene la siguiente tabla.

P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
2750	80	15000			Petición de inicio de conexión
		31000			2º mensaje de inicio de conexión
					3º mensaje de inicio de conexión
					B envía 100 bytes de datos nuevos (segmento perdido)
					A envía 400 bytes de datos nuevos
					B envía 100 bytes de datos nuevos (segmento perdido)
					B envía 100 bytes de datos nuevos (segmento perdido)
					A envía 300 bytes de datos nuevos (segmento perdido)
					A reenvía 400 bytes de datos de 1º segmento enviado (B lo recibe)
					B reenvía 100 bytes de datos de 1º segmento perdido (segmento perdido)

Suponga que ni en el extremo A ni en el extremo B, las aplicaciones han hecho llamadas a la función *read ()*. ¿Cuál es número de bytes almacenados en el buffer de recepción del extremo A? ¿Cuál es número de bytes almacenados en el buffer de recepción del extremo B? Rellene la siguiente tabla

Bytes en buffer de recepción de extremo A	
Bytes en buffer de recepción de extremo B	

### Problema 11 (Septiembre 2007-problema 1)

Una aplicación A establece una conexión TCP con una aplicación B. El extremo aceptador informa de que el tamaño máximo de segmento que está dispuesto a recibir es de 800, mientras que el extremo iniciador de la conexión informa que el tamaño máximo de segmento que está dispuesto a recibir es 1000. Por coincidencia, el primer segmento de establecimiento de conexión que el extremo A transmite, y el primero que el extremo B transmite, tienen el valor 10000 en el campo SN (Sequence Number). Escriba el contenido de los campos de la cabecera TCP vacíos que aparecen en la tabla, en la siguiente secuencia de intercambio de segmentos, suponiendo que no existe pérdida ni desorden en la entrega, salvo en las ocasiones que se indica lo contrario. Rellene la siguiente tabla.

P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
2750	80				Petición de inicio de conexión

					2º mensaje de inicio de conexión
					3º mensaje de inicio de conexión
					B envía 100 bytes de datos nuevos (segmento perdido)
					A envía 200 bytes de datos nuevos
					B envía 100 bytes de datos nuevos
					B reenvía 100 bytes de datos de primer segmento enviado (segmento perdido)
					A envía 300 bytes de datos nuevos (segmento perdido)
					A reenvía 200 bytes de datos de 1º segmento enviado (B lo recibe)
					B reenvía 100 bytes de datos de 1º segmento enviado (segmento perdido)

Suponga que el tamaño de la ventana de transmisión ( $tamaño = \min\{snd\_wnd, snd\_cwnd\}$ ) en ambos extremos es de 8092 bytes. ¿Cuál es número de bytes *libres* en la ventana del extremo A? Lo mismo para extremo B. Rellene la tabla.

Bytes libres en ventana transmisión A	
Bytes libres en ventana transmisión B	

### Problema 12 (Febrero 2008-problema 1)

Una aplicación A establece una conexión TCP con una aplicación B. El extremo aceptador informa de que el tamaño máximo de segmento que está dispuesto a recibir es de 1460, mientras que el extremo iniciador de la conexión informa que el tamaño máximo de segmento que está dispuesto a recibir es 2100. Escriba el contenido de los campos de la cabecera TCP vacíos que aparecen en la siguiente tabla, suponiendo que no existe pérdida ni desorden en la entrega, salvo en las ocasiones que se indica lo contrario.

P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
2000	31200	10000			Petición de inicio de conexión
		40000			2º mensaje de inicio de conexión
					3º mensaje de inicio de conexión
					A envía 300 bytes de datos nuevos (segmento perdido)
					A envía 400 bytes de datos nuevos
					B envía 100 bytes de datos nuevos
					A envía 100 bytes de datos nuevos (segmento perdido)

					<i>B</i> envía 300 bytes de datos nuevos (segmento perdido)
					<i>A</i> reenvía 300 bytes de datos de 1º segmento perdido (recibido)
					<i>B</i> reenvía 300 bytes de datos de 1º segmento perdido (recibido)
					<i>A</i> envía segmento de 1000 bytes de datos nuevos

Suponga que ni en el extremo A ni en el extremo B, las aplicaciones han hecho llamadas a la función *read* (). ¿Cuál es número de bytes almacenados en el buffer de recepción del extremo A y B al final de la secuencia? Rellene la siguiente tabla.

Bytes en buffer de recepción de extremo A	
Bytes en buffer de recepción de extremo B	

### Problema 13 (Junio 2008-problema 1)

Una aplicación A establece una conexión TCP con una aplicación B. Ambos extremos informan de que el tamaño máximo de segmento que están dispuestos a recibir es de 1000 bytes. El tamaño máximo del buffer de recepción tanto del extremo aceptador como del iniciador es de 1500 bytes. Escriba el contenido de los campos de la cabecera TCP vacíos que aparecen en la tabla suponiendo que no hay desorden en la entrega ni pérdida de segmentos, salvo en las ocasiones donde se indique.

t	P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
0	2000	42000	10000		<i>MSS=1000</i>	Petición de inicio de conexión
1			20000		<i>MSS=1000</i>	2º mensaje de inicio de conexión
2						3º mensaje de inicio de conexión
3						<i>A</i> envía 500 bytes de datos nuevos
4						<i>B</i> envía 400 bytes de datos nuevos (segmento perdido)
5						<i>A</i> envía 700 bytes de datos nuevos
6						<i>B</i> envía 100 bytes de datos nuevos (segmento perdido)
7						<i>A</i> reenvía 500 bytes de datos de 1º segmento
8						<i>B</i> reenvía 400 bytes de datos del primer segmento perdido.
9						<i>B</i> envía 900 bytes de datos de datos nuevos

a) ¿Cuál es el número de bytes almacenados en el buffer de transmisión del extremo A y B al final de la secuencia? Rellene la siguiente tabla.

Bytes en buffer de transmisión de extremo A	
---	--

Bytes en buffer de transmisión de extremo B	
---	--

- b) Suponga que el extremo A hace una llamada a la función *read()* en el instante  $t=5$  que lee todos los datos del posibles, y el extremo B hace una llamada a la función *read()* en el instante  $t=8$ , que también lee todos los datos posibles. ¿Cuál es número de bytes almacenados en el buffer de recepción del extremo A y B al final de la secuencia? Rellene la siguiente tabla.

Bytes en buffer de recepción de extremo A	
Bytes en buffer de recepción de extremo B	

### Problema 14 (Septiembre 2008-problema 1)

Una aplicación A establece una conexión TCP con una aplicación B. Ambos extremos informan de que el tamaño máximo de segmento que están dispuestos a recibir es de 1000 bytes. El tamaño máximo del buffer de recepción del extremo aceptador es de 1500 bytes y el del extremo iniciador de 1200 bytes. Escriba el contenido de los campos de la cabecera TCP vacíos que aparecen en la siguiente tabla, suponiendo que no existe desorden en la entrega ni pérdida de segmentos, salvo en las ocasiones que se indica lo contrario.

t	P <sub>origen</sub>	P <sub>destino</sub>	Seq. Number	ACK	Options	Comentarios
0	2200	4200	1200			Petición de inicio de conexión
1			2000			2º mensaje de inicio de conexión
2						3º mensaje de inicio de conexión
3						A envía 500 bytes de datos nuevos
4						B envía 400 bytes de datos nuevos (segmento perdido)
5						A envía 700 bytes de datos nuevos
6						A reenvía 500 bytes de datos de 1º segmento
7						B envía 100 bytes de datos nuevos
8						B reenvía 400 bytes de datos del 1º segmento
9						A envía 700 bytes de datos nuevos (el segmento llega correctamente)

- a) ¿Cuál es el número de bytes eliminados del buffer de transmisión del extremo A y B al final de la secuencia? Rellene la siguiente tabla.

Bytes eliminados del buffer de transmisión de extremo A	
Bytes eliminados del buffer de transmisión de extremo B	

- b) Un instante antes de  $t=8$  los extremos A y B hacen una llamada a la función *read()* que lee todos los datos posibles. Rellene la siguiente tabla con el número de bytes leídos en A y en B.

Bytes leídos del buffer de recepción de extremo A	
Bytes leídos del buffer de recepción de extremo B	

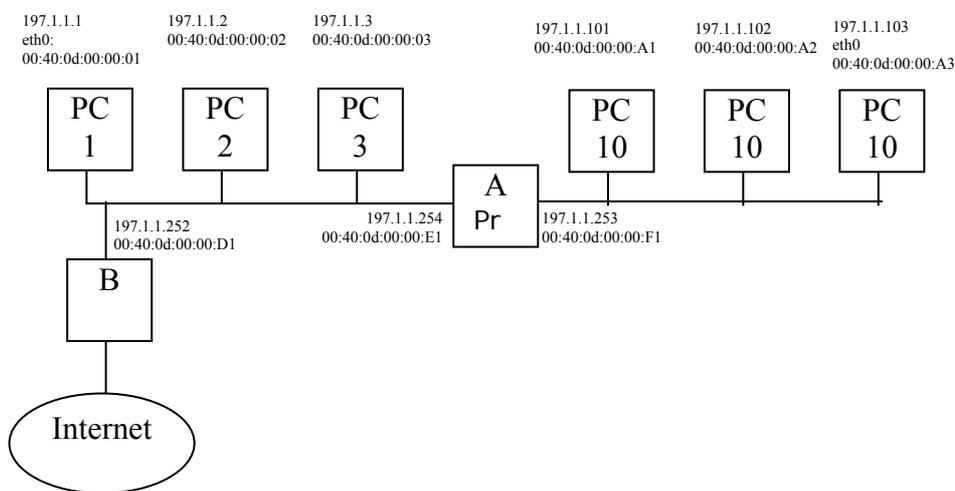
## Bloque temático 2. Extensiones de direccionamiento IPv4

Para realizar la mayoría de los problemas que se plantean en este bloque temático es necesario tener un conocimiento previo de direccionamiento IP así como de los protocolos TCP, UDP (bloque temático 1).

### 2.1 Proxy ARP

#### Problema 1. (Junio 2003-cuestión 2)

El router A ha sido configurado para implementar la funcionalidad Proxy ARP entre las dos redes físicas Ethernet a las que se encuentra conectado. Las tablas de traducción ARP de los PCs 1, 2, 3, 101, 102, 103 se encuentran inicialmente vacías.



(a) Indique la tabla de encaminamiento del PC 1 y del PC 103. Un error en una tabla de encaminamiento supone la pérdida de los puntos correspondientes a dicha tabla.

Tabla encaminamiento PC 1		
IP destino / Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC 103		
IP destino / Máscara	Interfaz de salida	Gateway

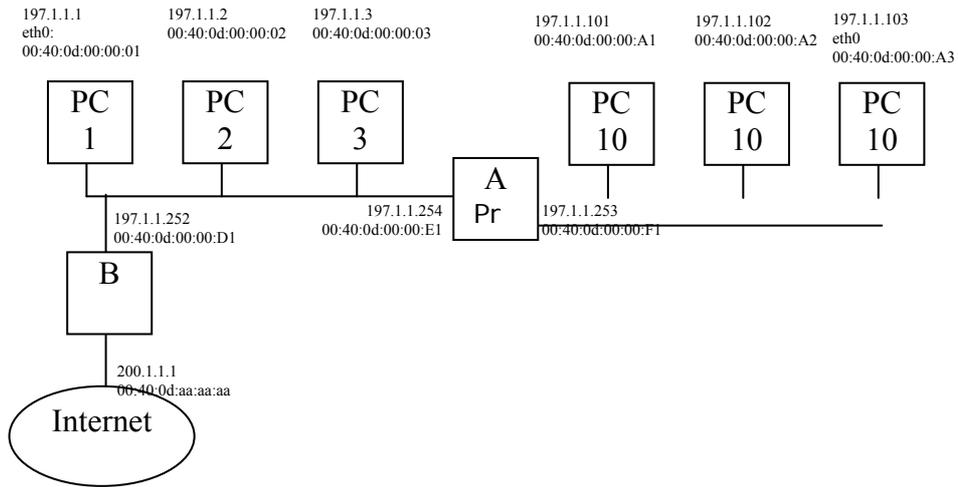

(b) Describa, rellenando la siguiente tabla, la evolución de las tramas transmitidas, involucradas en la transmisión de un mensaje ICMP echo request desde PC 1 a PC 103, y el mensaje ICMP echo reply correspondiente.

Campos cabecera Ethernet (rellenar siempre)		Campos mensaje ARP (rellenar en caso de mensaje ARP)		Campos mensaje ICMP (rellenar en caso mensaje ICMP)
MACorigen (3 últimos bytes)	MACdestino (3 últimos bytes)	Consulta/ Respuesta ARP	IP Consultada (consulta ARP) / MAC resuelta (respuesta ARP)	Echo Request / Echo Reply

**Problema 2 (Junio 2004-problema 1)**

El *router* A ha sido configurado para implementar la funcionalidad Proxy ARP entre las dos redes físicas *Ethernet* a las que se encuentra conectado. Las tablas caché ARP de los PCs 1, 2, 3, 101, 102, 103 y del *router* B se encuentran inicialmente vacías. La tabla caché ARP del *router* A contiene las entradas correspondientes a las direcciones IP 197.1.1.{1,2,3}, 197.1.1.{101,102,103}, 197.1.1.252. Las tablas de encaminamiento de todos los dispositivos han sido correctamente configuradas.

Describa, rellenando la siguiente tabla, la evolución de las tramas transmitidas, involucradas en la transmisión de un mensaje ICMP *echo request* desde PC 103 a la dirección 200.1.1.1, y el mensaje ICMP *echo reply* correspondiente.



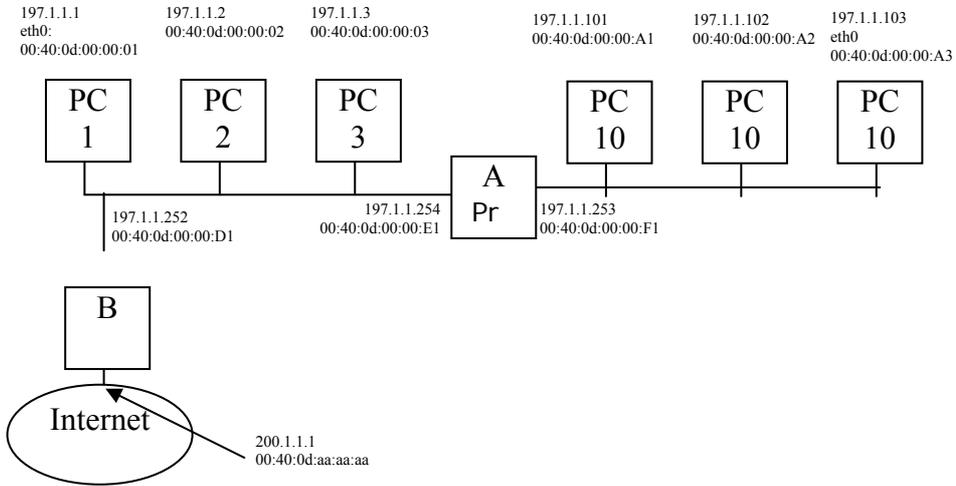
Campos cabecera Ethernet (rellenar siempre)		Campos mensaje ARP (rellenar en caso de mensaje ARP)		Campos mensaje ICMP (rellenar en caso mensaje ICMP)
MACorigen (3 últimos bytes)	MACdestino (3 últimos bytes)	Consulta/ Respuesta ARP	IP Consultada (si consulta ARP)	Echo Request / Echo Reply

### Problema 3 (Septiembre 2005-problema 1)

El *router* A ha sido configurado para implementar la funcionalidad Proxy ARP entre las dos redes físicas *Ethernet* a las que se encuentra conectado.

Las tablas de encaminamiento de todos los dispositivos han sido correctamente configuradas. La tabla caché ARP del *router* A contiene las entradas correspondientes a las direcciones IP 197.1.1.{1,2,3}, 197.1.1.{101,102,103}, 197.1.1.252. El resto de dispositivos, tiene inicialmente vacías las tablas caché ARP, salvo en los siguientes casos:

Tabla Caché ARP Router B		Tabla Caché ARP PC 102	
Dirección MAC	Dirección IP	Dirección MAC	Dirección IP
00:40:0d:00:00:02	197.1.1.2	00:40:0d:00:00:A1	197.1.1.101



a) Describa, rellenando la siguiente tabla, la evolución de las tramas transmitidas, involucradas en la transmisión de un mensaje ICMP *echo request* desde el router B hacia el PC 102, y el mensaje ICMP *echo reply* correspondiente.

Campos cabecera Ethernet (rellenar siempre)		Campos mensaje ARP (rellenar en caso de mensaje ARP)		Campos mensaje ICMP (rellenar en caso mensaje ICMP)
MACorigen (3 últimos bytes)	MACdestino (3 últimos bytes)	Consulta/ Respuesta ARP	IP Consultada (si consulta ARP)	Echo Request / Echo Reply

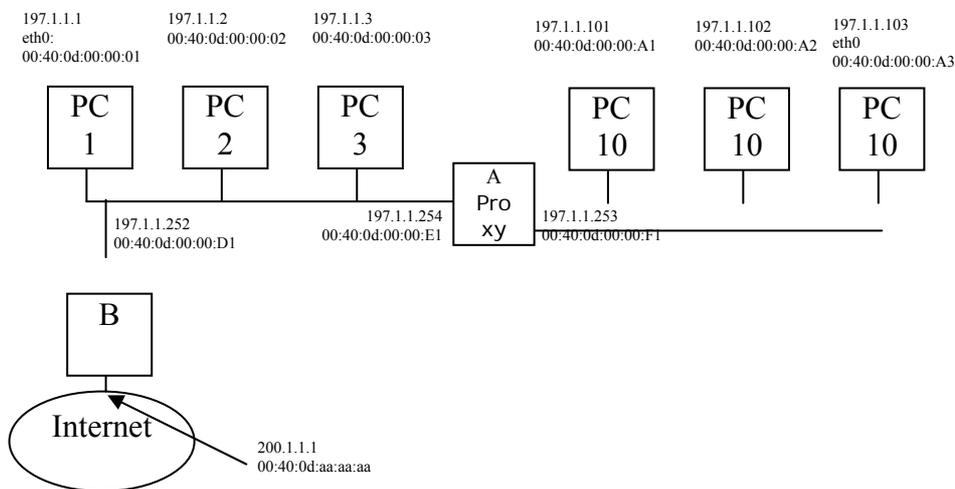
b) Escriba el estado final de las tablas caché ARP de los dispositivos que se le indican, teniendo en cuenta que ninguna de las entradas ha caducado.

Tabla Caché ARP Router B	
Dirección MAC	Dirección IP

Tabla Caché ARP PC 102	
Dirección MAC	Dirección IP

### Problema 4 (Diciembre 2005-problema 1)

El *router* A ha sido configurado para implementar la funcionalidad Proxy ARP entre las dos redes físicas *Ethernet* a las que se encuentra conectado.



Las tablas de encaminamiento de todos los dispositivos han sido correctamente configuradas. La tabla caché ARP del *router* A contiene las entradas correspondientes a las direcciones IP  $197.1.1.\{1,2,3\}$ ,  $197.1.1.\{101,102,103\}$ ,  $197.1.1.252$ . El resto de dispositivos, tiene inicialmente vacías las tablas caché ARP, salvo en los siguientes casos:

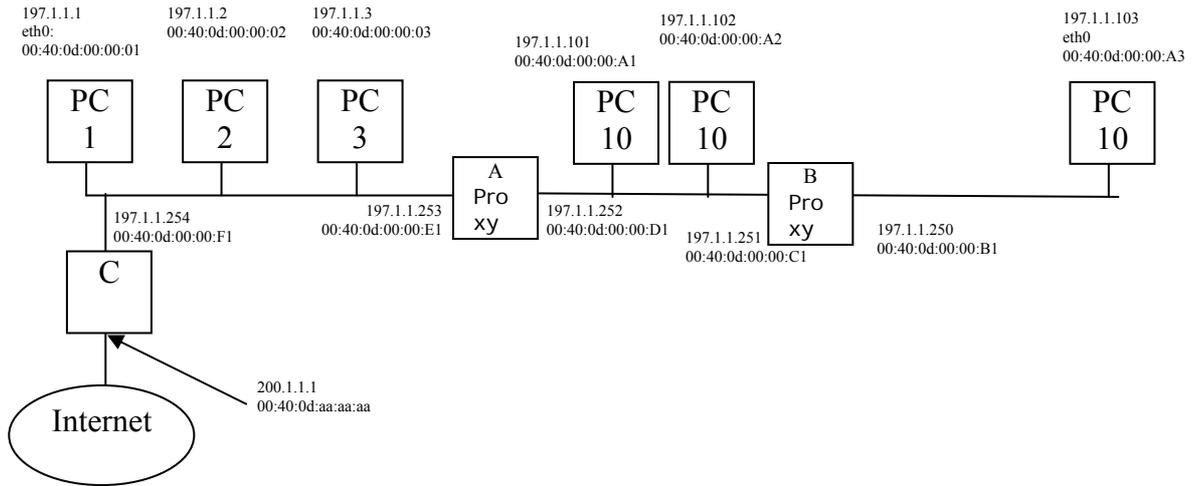
Tabla Caché ARP PC 1	
Dirección MAC	Dirección IP
00:40:0d:00:00:02	197.1.1.254
00:40:0d:00:00:03	197.1.1.103

Tabla Caché ARP PC 103	
Dirección MAC	Dirección IP
00:40:0d:00:00:A1	197.1.1.101
00:40:0d:00:00:F1	197.1.1.1

Note que la tabla caché ARP del PC 1 tiene almacenados valores incorrectos (quizá porque haya sido configurada manualmente de esa manera). La tabla caché ARP del *router* A ha sido correctamente configurada.

- a) Describa, rellenando la siguiente tabla, la evolución de las tramas transmitidas, involucradas en la transmisión de un mensaje ICMP *echo request* desde el PC 1 hacia el PC 103, y el mensaje ICMP *echo reply* correspondiente.





a) Escriba los contenidos de las tablas caché ARP de los dispositivos indicados:

Tabla Caché ARP Router C	
Dirección MAC	Dirección IP

Tabla Caché ARP PC 1	
Dirección MAC	Puerto

Tabla Caché ARP PC 101	
Dirección MAC	Dirección IP

Tabla Caché ARP PC 103	
Dirección MAC	Puerto



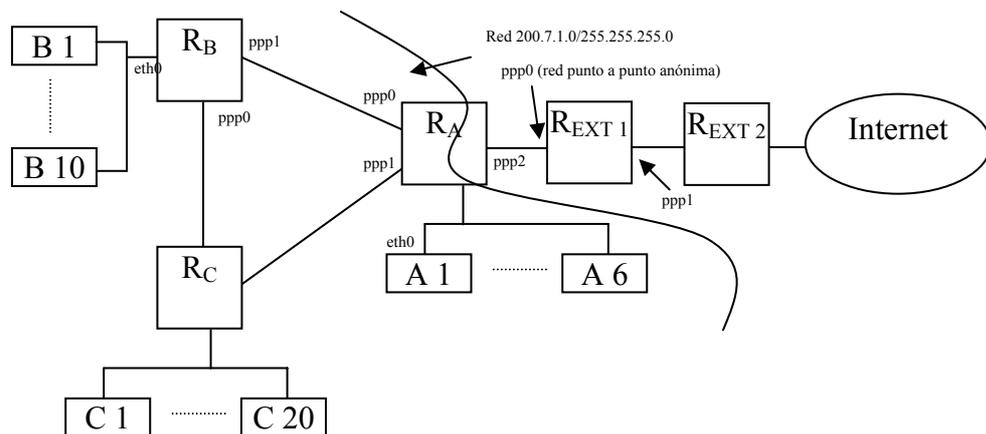
- b) Escriba el estado final de las tablas caché ARP de los dispositivos que se le indican, teniendo en cuenta que ninguna de las entradas ha caducado. Escriba la palabra “vacía” si considera que la tabla está vacía.

Tabla Caché ARP PC 1		Tabla Caché ARP PC 101	
Dirección MAC	Dirección IP	Dirección MAC	Dirección IP

## 2.2 Direccionamiento de subred, CIDR y líneas punto a punto

### Problema 1 (Junio 2003-problema 2)

La figura muestra una organización con tres redes Ethernet conectadas a través de enlaces punto a punto, a la que le ha sido otorgada una dirección de clase C (200.7.1.0/255.255.255.0). Para resolver el problema de asignación de direcciones, se pide utilizar la técnica de direccionamiento de subred (no direccionamiento CIDR), teniendo en cuenta que todas las subredes deben ser del mismo tamaño (mismo tamaño de porción de red/subred y porción de host).



Tenga en cuenta las siguientes consideraciones:

- Otorgue a las redes físicas las subredes en el siguiente orden (de dirección de subred más baja a más alta): 1) Ethernet A, 2) Ethernet B, 3) Ethernet C, 4) Punto a punto A-B, 5) Punto a punto B-C, 6) Punto a punto A-C. [Nota: por comodidad, se trata del orden de aparición en las tablas de respuesta encontradas más abajo].

- Las direcciones de los PCs deben otorgarse ordenadamente en función del número del PC: la más baja utilizable dentro de la subred para el PC A/B/C 1, la siguiente para el PC A/B/C 2, y así consecutivamente para el resto de PCs.
- Las direcciones de las interfaces Ethernet de los routers A, B, C deben emplear la última dirección asignable dentro de la subred.
- Los enlaces punto a punto deben emplear las dos últimas direcciones utilizables dentro de las asignables de subred, dando la dirección más baja a la de orden alfabético menor en cada enlace (por ejemplo, en el enlace A-C, la dirección más baja al extremo A, y la siguiente a C).

a) Rellene las siguientes tablas:

Red física	@ Subred	@ Bcast. subred	@ PC (Primero)	@ PC (Último)	@Interfaz R <sub>A/B/C</sub>
Ethernet A					
Ethernet B					
Ethernet C					

Red física	@ Subred	@ Extremo 1	@ Extremo 2
Punto a punto A-B			
Punto a punto B-C			
Punto a punto A-C			

b) Con la información anterior, rellene las tablas de encaminamiento que aparecen a continuación, siguiendo las siguientes normas:

- Reducir al máximo el número de entradas (sin aplicar agregación de rutas).
- No poner nada en el campo *gateway* cuando sea conexión punto a punto.
- Incluir las entradas de las redes (punto a punto o Ethernet) directamente conectadas.
- En caso de igualdad en número de saltos a una red destino, preferir el camino a través del router A frente a B y C, y el camino a través del router B, frente a router C.

Tabla encaminamiento PC A-1			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento R <sub>B</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento R <sub>A</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento R <sub>EXT 1</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

**Problema 2 (Junio 2004-problema 3)**

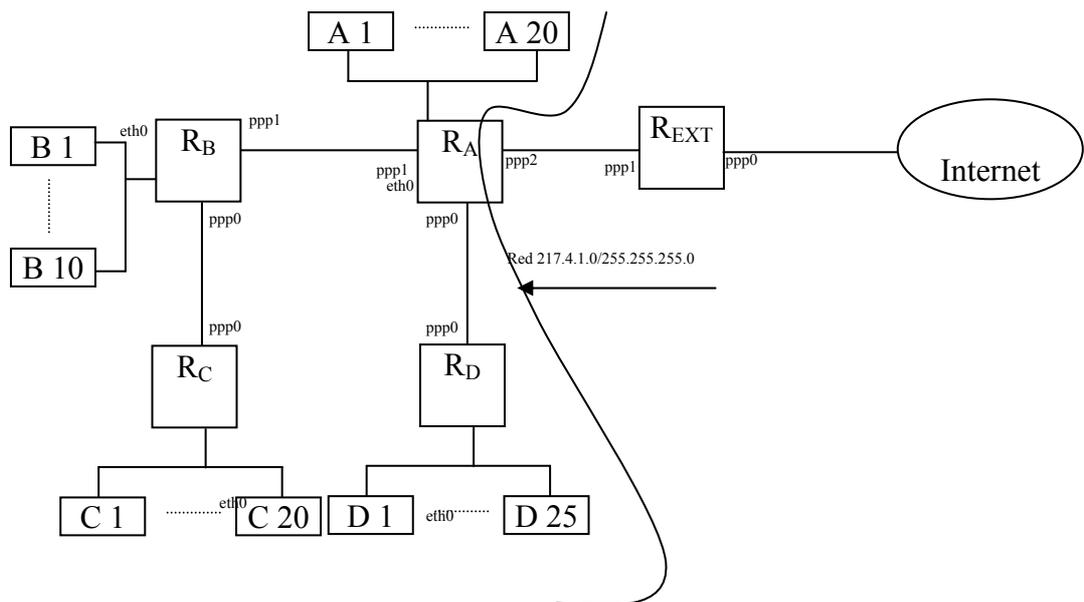
La figura muestra una organización con cuatro redes Ethernet conectadas a través de enlaces punto a punto, a la que le ha sido otorgada una dirección de clase C (217.4.1.0/255.255.255.0). Para resolver el problema de asignación de direcciones, se pide utilizar la técnica de direccionamiento de subred (no direccionamiento CIDR), teniendo en cuenta que todas las subredes deben ser del mismo tamaño (mismo tamaño de porción de red/subred y porción de host).

Tenga en cuenta las siguientes consideraciones:

- Otorgue a las redes físicas las subredes en el siguiente orden (de dirección de subred más baja a más alta): 1) Ethernet A, 2) Ethernet B, 3) Ethernet C, 4) Ethernet D.
- Las direcciones de los PCs deben otorgarse ordenadamente en función del número del PC: la más baja utilizable dentro de la subred para el PC A/B/C/D 1, la siguiente para el PC A/B/C/D 2, y así consecutivamente para el resto de PCs.
- Las direcciones de las interfaces Ethernet de los routers A, B, C y D deben emplear la última dirección asignable dentro de la subred.
- Los enlaces punto a punto aplican la técnica de IP no numerado (enlaces anónimos), por lo que no deben ser reservados direcciones de subred para ellos.

a) Rellene las siguientes tablas:

Red física	@ Subred	Máscara de subred	1° @ IP utilizable	@Interfaz R <sub>A/B/C</sub>	@Broadcast de subred
Ethernet A					
Ethernet B					
Ethernet C					
Ethernet D					



b) Con la información anterior, rellene las tablas de encaminamiento que aparecen a continuación, siguiendo las siguientes normas:

- Reducir al máximo el número de entradas.
- No poner nada en el campo *gateway* cuando el interfaz de salida sea punto a punto.
- Incluir las entradas de las redes (punto a punto o Ethernet) directamente conectadas.
- Cada tabla de encaminamiento suma 0,2 ptos en caso de ser correcta, y 0 ptos. en caso de no serlo.

Tabla encaminamiento R <sub>A</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento R <sub>B</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento R <sub>C</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento R <sub>D</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento R <sub>EXT</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

c) Observe las direcciones de subred no utilizadas en el apartado 1. Escoja la *menor* de estas direcciones IP de subred libres, y subdivídala a su vez en subredes que proporcionen direcciones a los enlaces punto a punto anónimos por este orden (dirección de subred menor a mayor) R<sub>C</sub>-R<sub>B</sub>, R<sub>D</sub>-R<sub>A</sub>, R<sub>B</sub>-R<sub>A</sub>. El tamaño de las subredes (número de bits de la porción de *host*) **debe ser el menor posible**.

Red física	@ Subred	Máscara	Primera @ IP	Segunda @IP	@ Bcast. subred
R <sub>C</sub> -R <sub>B</sub>					
R <sub>D</sub> -R <sub>A</sub>					
R <sub>B</sub> -R <sub>A</sub>					

### Problema 3 (Septiembre 2004-problema 3)

Dispone de la dirección 203.4.7.0/255.255.255.0, para asignar direcciones a 6 redes físicas. El número de interfaces a los que asignar dirección IP en cada red es: (Red 1) 60, (Red 2) 30, (Red 3) 10, (Red 4) 2, (Red 5) 2, (Red 6) 2.

Para ello, rellene la siguiente tabla con los datos que se le pide, teniendo en cuenta que:

- No se permite utilizar las direcciones de subred que creen ambigüedades con la dirección de red 203.4.7.0 y con la dirección de difusión 203.4.7.255.
- Todas las direcciones y máscaras de subred de la tabla deben rellenarse con los tres primeros bytes en decimal, y *último byte en binario* (lo que hará más sencilla la resolución del problema)
- La numeración de las redes debe realizarse en orden (dirección de subred de red 1, menor que de red 2, etc.)

Red	Dirección de subred	Máscara de subred	Primera dirección subred utilizable	Última dirección subred utilizable	Dirección <i>broadcast</i> de subred
1					
2					
3					

4					
5					
6					

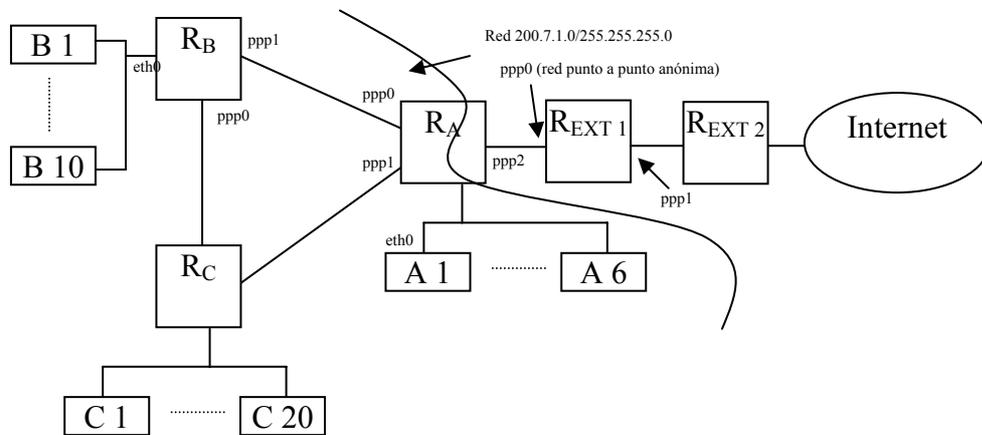
**Problema 4 (Junio 2003-cuestión 1)**

Rellene la siguiente tabla para el bloque CIDR 20.96.0.0/12

- Dirección IP del bloque:
- Dirección más baja asignable:
- Dirección más alta asignable:
- Dirección de broadcast:

**Problema 5 (Junio 2003-problema 2)**

La figura muestra una organización con tres redes Ethernet conectadas a través de enlaces punto a punto, a la que le ha sido otorgada una dirección de clase C (200.7.1.0/255.255.255.0). Para resolver el problema de asignación de direcciones, se pide utilizar la técnica de direccionamiento de subred (no direccionamiento CIDR), teniendo en cuenta que todas las subredes deben ser del mismo tamaño (mismo tamaño de porción de red/subred y porción de host).



Tenga en cuenta las siguientes consideraciones:

- Otorgue a las redes físicas las subredes en el siguiente orden (de dirección de subred más baja a más alta): 1) Ethernet A, 2) Ethernet B, 3) Ethernet C, 4) Punto a punto A-B, 5) Punto a punto B-C, 6) Punto a punto A-C. [Nota: por comodidad, se trata del orden de aparición en las tablas de respuesta encontradas más abajo].
- Las direcciones de los PCs deben otorgarse ordenadamente en función del número del PC: la más baja utilizable dentro de la subred para el PC A/B/C 1, la siguiente para el PC A/B/C 2, y así consecutivamente para el resto de PCs.

- Las direcciones de las interfaces Ethernet de los routers A, B, C deben emplear la última dirección asignable dentro de la subred.
- Los enlaces punto a punto deben emplear las dos últimas direcciones utilizables dentro de las asignables de subred, dando la dirección más baja a la de orden alfabético menor en cada enlace (por ejemplo, en el enlace A-C, la dirección más baja al extremo A, y la siguiente a C).

a) Rellene las siguientes tablas:

Red física	@ Subred	@ Bcast. subred	@ PC 1	@ PC (Último)	@Interfaz R <sub>A/B/C</sub>
Ethernet A					
Ethernet B					
Ethernet C					

Red física	@ Subred	@ Extremo 1	@ Extremo 2
Punto a punto A-B			
Punto a punto B-C			
Punto a punto A-C			

b) Con la información anterior, rellene las tablas de encaminamiento que aparecen a continuación, siguiendo las siguientes normas:

- Reducir al máximo el número de entradas (pero sin aplicar agregación de rutas).
- No poner nada en el campo *gateway* cuando el interfaz de salida sea punto a punto.
- Incluir las entradas de las redes (punto a punto o Ethernet) directamente conectadas.
- En caso de igualdad en número de saltos a una red destino, preferir el camino a través del router A frente al B y C, y el camino a través del router B, frente al router C.

Tabla encaminamiento PC A-1			
Dirección	Máscara	Interfaz de salida	Gateway

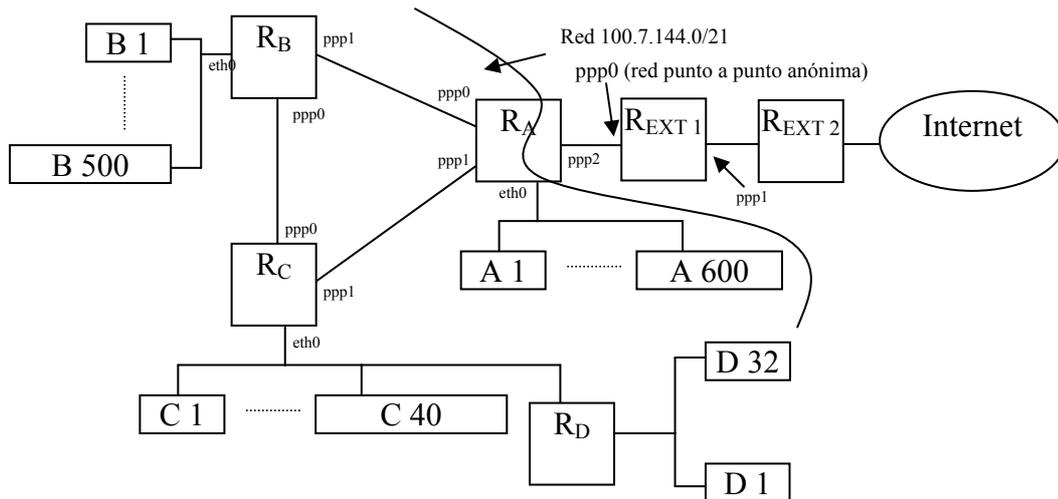
Tabla encaminamiento R <sub>B</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento R <sub>A</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento R <sub>EXT 1</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

**Problema 6 (Septiembre 2003-problema 2)**

La figura muestra una organización con tres redes Ethernet conectadas a través de enlaces punto a punto, a la que le ha sido otorgada una dirección de clase B (100.7.0.0/21). Para resolver el problema de asignación de direcciones, se pide utilizar la técnica de direccionamiento y encaminamiento CIDR. Todas las interfaces *ppp* entre los routes A, B y C son anónimas (y por lo tanto, corresponden a redes a las que no se asigna dirección de subred).



Tenga en cuenta las siguientes consideraciones:

- Otorgue a las redes físicas los bloques de direcciones de tamaño mínimo necesario, en el siguiente orden (de dirección de bloque más baja a más alta): 1) Ethernet A, 2) Ethernet B, 3) Ethernet C. [Nota: por comodidad, se trata del orden de aparición en las tablas de respuesta encontradas más abajo].
- Las direcciones de los PCs deben otorgarse ordenadamente en función del número del PC: la más baja utilizable para el PC A/B/C 1, la siguiente para el PC A/B/C 2, y así consecutivamente para el resto de PCs.
- Las direcciones de las interfaces Ethernet de los routers A, B, C y D a las redes Ethernet A, B, C y D respectivamente, deben ser las últimas direcciones asignables. La dirección de R<sub>D</sub> a la red C debe ser la penúltima asignable.

a) ¿Es correcto el bloque otorgado a R<sub>A</sub>? ¿Por qué?

b) Rellene la siguiente tabla:

Red física	@ Bloque (Formato A.B.C.D / N)	@ PC 1	@ Interfaz R <sub>A/B/C/D</sub>
Ethernet A			
Ethernet B			
Ethernet C			
Ethernet D			

c) Con la información anterior, rellene las tablas de encaminamiento que aparecen a continuación, siguiendo las siguientes normas:

- Reducir al máximo el número de entradas (aplicando agregación de rutas si es beneficioso).
- No escriba nada en el campo *gateway* cuando la interfaz de salida sea punto a punto.
- Incluir las entradas de las redes (punto a punto o Ethernet) directamente conectadas.
- En caso de igualdad en número de saltos a una red destino, elija el camino a través del router A frente al B y C, y el camino a través del router B, frente al router C.
- Cada tabla de encaminamiento suma 0,25 ptos en caso de ser correcta, y 0 ptos. en caso de no serlo.

Tabla encaminamiento PC R <sub>C</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento R <sub>B</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

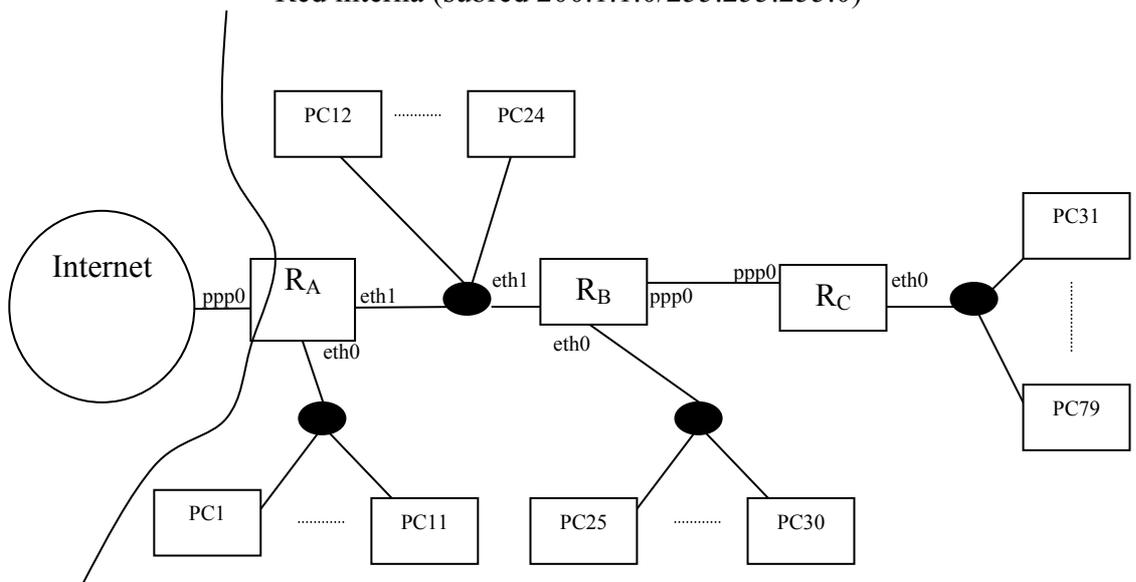
Tabla encaminamiento R <sub>A</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento R <sub>EXT 1</sub>			
Dirección	Máscara	Interfaz de salida	Gateway

**Problema 7 (Diciembre 2004-problema 3)**

Dispone de la dirección 200.1.1.0/255.255.255.0, para asignar direcciones a las redes físicas de la figura.

Red interna (subred 200.1.1.0/255.255.255.0)



● Conmutador *Ethernet*

- a) Rellene la siguiente tabla con los datos que se le pide, teniendo en cuenta que:
- No se permite utilizar las direcciones de subred que creen ambigüedades con la dirección de red 200.1.1.0 y con la dirección de difusión 200.1.1.255.
  - La numeración de las redes debe realizarse de tal manera que las direcciones correspondientes a las subredes con más interfaces, deben tener direcciones menores.
  - Los rangos de direcciones utilizados deben ser contiguos (entre dos subredes consecutivas no debe haber direcciones que no pertenezcan a ninguna subred)

- Deben desaprovecharse la menor cantidad posible de direcciones. Esto implica ajustar la máscara de subred al tamaño más adecuado de cada subred.
- Muestre las direcciones IP y máscaras en formato decimal por puntos: A.B.C.D.

Sub Red	Lista de PCs dentro de esa red (si hay alguno)	Dirección de subred	Máscara de subred	Rango de direcciones utilizables	Dirección <i>broadcast</i> de subred
1					
2					
3					
4					
5					

- b) Asigne sobre la figura, direcciones IP a todas las interfaces de los routers A, B y C, siguiendo las asignaciones que ha propuesto en la tabla anterior, y las convenciones habituales para asignar direcciones a los *routers*. **Nota:** No asigne ninguna dirección a la interfaz ppp0 de R<sub>A</sub>.
- c) Escriba la tabla de encaminamiento de los dispositivos que se le indica, minimizando el número de entradas.

Tabla encaminamiento <i>router A</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>Router B</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>Router C</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC 12			
Dirección	Máscara	Interfaz de salida	Gateway

**Problema 8 (Febrero 2007-problema 2)**

Dispone de la dirección 172.16.0.0/255.255.0.0, para asignar direcciones a 6 redes físicas. El número de interfaces a los que asignar dirección IP en cada red es: (Red 1) 16000, (Red 2) 1000, (Red 3) 990, (Red 4) 290, (Red 5) 280, (Red 6) 256. Para ello, rellene la siguiente tabla con los datos que se le pide, teniendo en cuenta que:

- No se permite utilizar las direcciones de subred que creen ambigüedades con la dirección de red 172.16.0.0 y con la dirección de difusión 172.16.255.255.
- Todas las direcciones y máscaras de subred de la tabla deben rellenarse en decimal (formato A.B.C.D), no en binario.
- La numeración de las redes debe realizarse en orden (dirección de subred de red 1, menor que de red 2, etc.).
- Deben desaprovecharse la menor cantidad posible de direcciones. Esto implica ajustar la máscara de subred al tamaño más adecuado de cada subred, y no dejar rangos de direcciones sin utilizar entre subredes.

Red	Dirección de subred	Máscara de subred	Primera dirección subred utilizable	Última dirección subred utilizable	Dirección <i>broadcast</i> de subred
1					
2					
3					

4					
5					
6					

**Problema 9 (Junio 2007-problema 2)**

La figura muestra una organización que dispone del rango de direcciones 87.36.0.0/18. Escriba las tablas de encaminamiento de los dispositivos que se le indican. Las tablas deberán aplicar la técnica de agregación de rutas en los casos en que esto permita disminuir el número de entradas en la tabla de encaminamiento. Todos los enlaces punto a punto son anónimos.

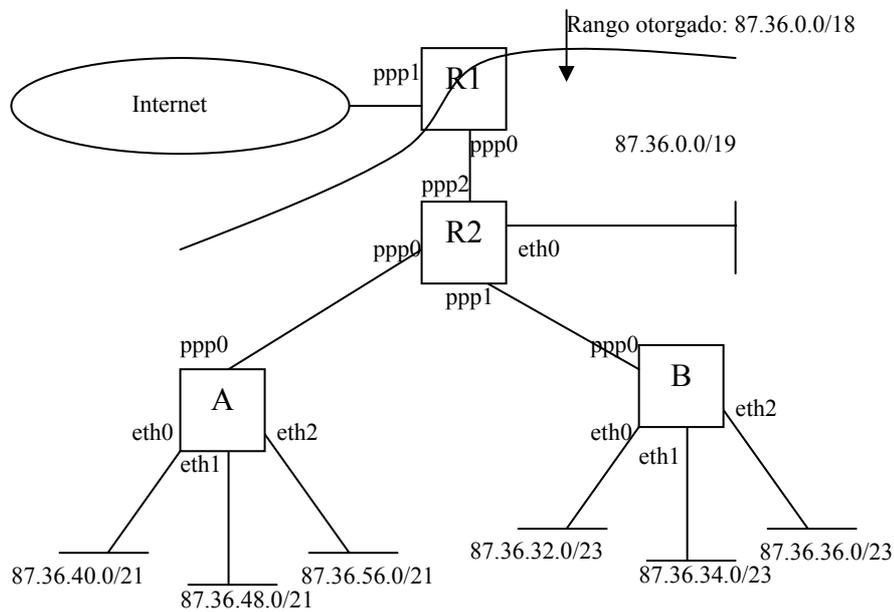


Tabla encaminamiento router A		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway

Tabla encaminamiento router B		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway


Tabla encaminamiento router R2		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway

Tabla encaminamiento router R1		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway

### Problema 10 (Septiembre 2007-problema 2)

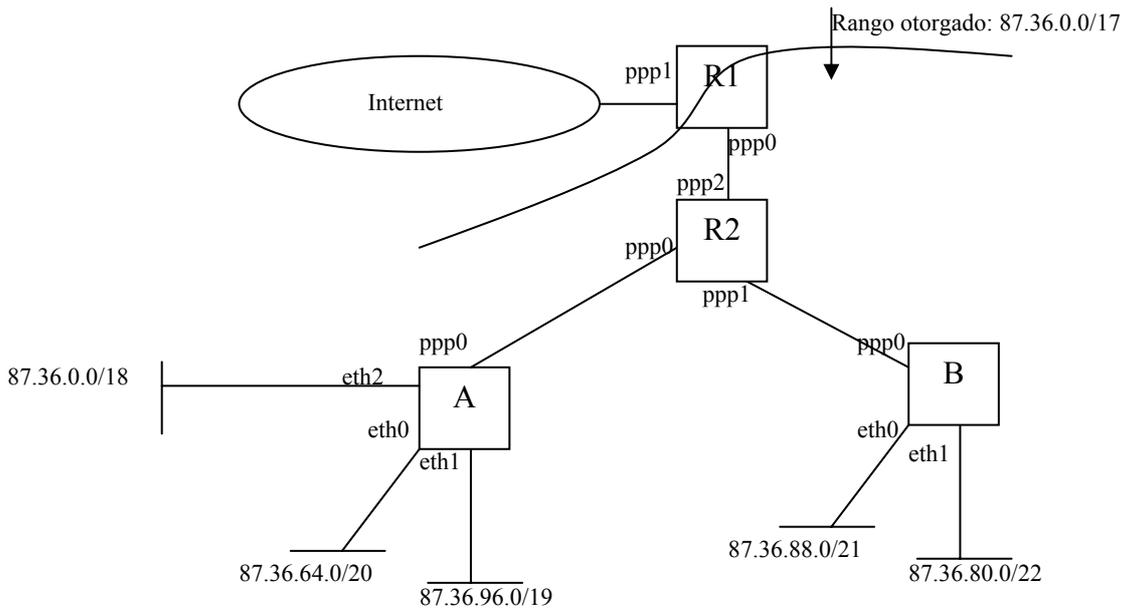
La figura muestra una organización que dispone del rango de direcciones 87.36.0.0/17. Escriba las tablas de encaminamiento de los dispositivos que se le indican. Las tablas deberán aplicar la técnica de agregación de rutas en los casos en que esto permita disminuir el número de entradas en la tabla de encaminamiento. Todos los enlaces punto a punto son anónimos.

Tabla encaminamiento router A		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway

Tabla encaminamiento router B		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway


Tabla encaminamiento router R2		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway

Tabla encaminamiento router R1		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway



**Problema 11 (Febrero 2008-problema 2)**

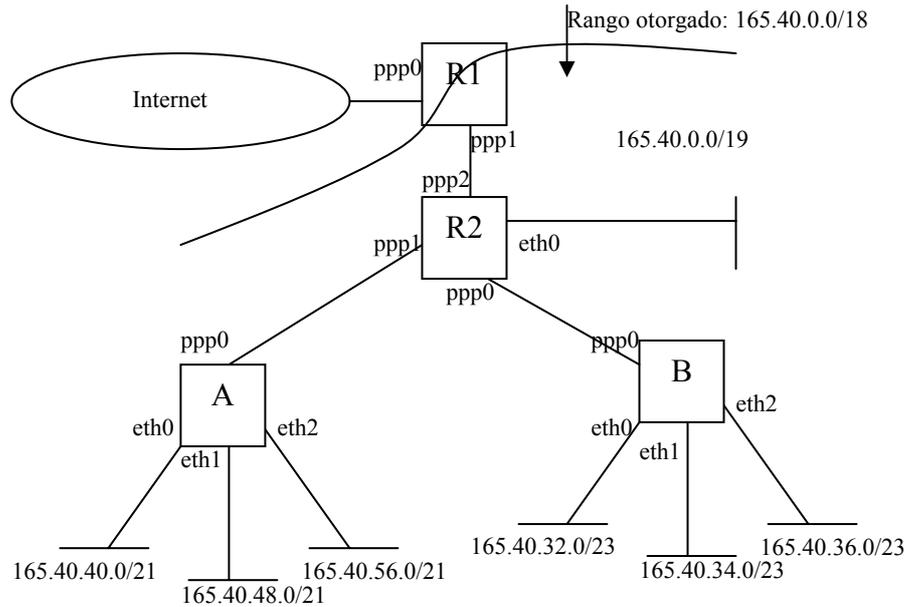
La figura muestra una organización que dispone del rango de direcciones 165.40.0.0/18. Escriba las tablas de encaminamiento de los dispositivos que se le indican. Las tablas deberán aplicar la técnica de agregación de rutas en los casos en que esto permita disminuir el número de entradas en la tabla de encaminamiento. Todos los enlaces punto a punto son anónimos.

Tabla encaminamiento router A		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway

Tabla encaminamiento router B		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway

Tabla encaminamiento router R2		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway

Tabla encaminamiento router R1		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway



### Problema 12 (Junio 2008-problema 2)

La figura muestra una organización que dispone del rango de direcciones 165.40.0.0/17. Escriba las tablas de encaminamiento de los dispositivos que se le indican. Las tablas deberán aplicar la técnica de agregación de rutas en los casos en que esto permita disminuir el número de entradas en la tabla de encaminamiento. Todos los enlaces punto a punto son anónimos.

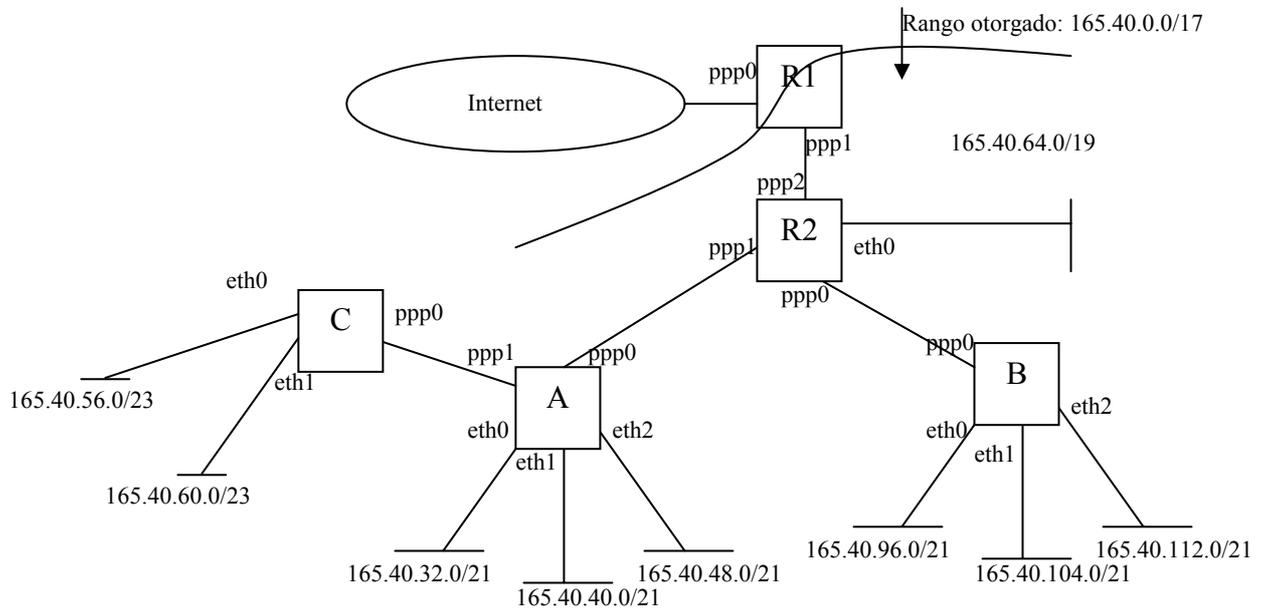


Tabla encaminamiento router C		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway


Tabla encaminamiento router A		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway

Tabla encaminamiento router B		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway

Tabla encaminamiento router R2		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway

Tabla encaminamiento router R1		
Dirección (formato A.B.C.D/prefijo)	Interfaz de salida	Gateway

### Problema 13 (Septiembre 2008-problema 2)

- a) Rellene la siguiente tabla para el bloque CIDR 135.32.0.0/14. En caso de no ser un bloque válido indíquelo.

Dirección IP del bloque:  
Dirección más baja asignable:  
Dirección más alta asignable:  
Dirección de broadcast:  
Número de direcciones utilizables:

- b) Rellene la siguiente tabla para el bloque CIDR 135.32.24.0/20. En caso de no ser un bloque válido indíquelo.

Dirección IP del bloque:  
Dirección más baja asignable:  
Dirección más alta asignable:  
Dirección de broadcast:  
Número de direcciones utilizables:



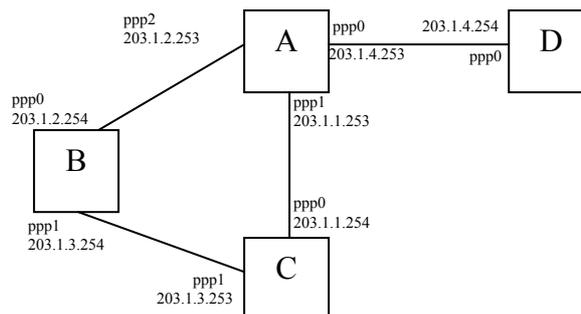
# Bloque temático 3. Algoritmos de encaminamiento dinámico. Sistemas autónomos

## Cuestiones (Diciembre 2001-cuestión 1)

- Definición de Algoritmos de encaminamiento dinámico dentro de un sistema autónomo:
- Algoritmos Bellman-Ford o vector-enlace: definición. Ventajas e inconvenientes
- Algoritmos enlace-estado: definición. Ventajas e inconvenientes.

## Problema 1 (Septiembre 2002-cuestión 3)

Las máquinas de la figura están ejecutando el protocolo de encaminamiento RIP v1.0. Todas las redes son de clase C, y se aplica una máscara de subred 255.255.255.0 en todas las entradas de las tablas de encaminamiento.



Escriba los mensajes periódicos RIP Response que generan cada una de las máquinas suponiendo lo siguiente:

- Se ha alcanzado la convergencia de rutas.
- En esta convergencia, el router A encamina los datagramas a la red 203.1.3.0 por C.
- En esta convergencia, el router B encamina los datagramas a la red 203.1.1.0 por A.
- En esta convergencia, el router C encamina los datagramas a la red 203.1.2.0 por B.
- Los mensajes Response indican con número de saltos 1 (no 0), aquellas redes a las que están directamente conectadas.

- La implementación de RIP v1.0 que ejecutan las máquinas involucradas, aplica el mecanismo de *split horizon* simple.

Mensaje Response generado por A por su interfaz ppp0	
IP origen del mensaje:	IP destino del mensaje:
Ruta	Número de saltos

Mensaje Response generado por A por su interfaz ppp1	
IP origen del mensaje:	IP destino del mensaje:
Ruta	Número de saltos

Mensaje Response generado por A por su interfaz ppp2	
IP origen del mensaje:	IP destino del mensaje:
Ruta	Número de saltos

Mensaje Response generado por B por su interfaz ppp0	
IP origen del mensaje:	IP destino del mensaje:
Ruta	Número de saltos

Mensaje Response generado por B por su interfaz ppp1	
IP origen del mensaje:	IP destino del mensaje:
Ruta	Número de saltos

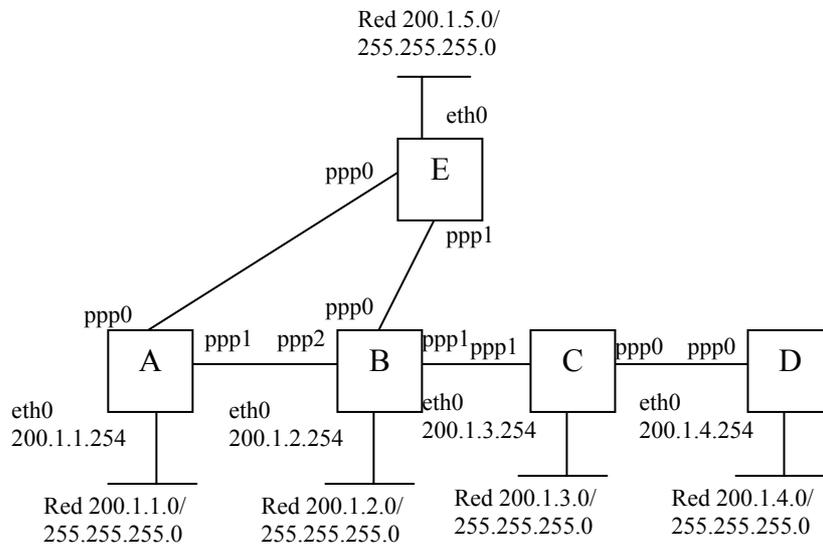
Mensaje Response generado por C por su interfaz ppp0	
IP origen del mensaje:	IP destino del mensaje:
Ruta	Número de saltos

Mensaje Response generado por C por su interfaz ppp1	
IP origen del mensaje:	IP destino del mensaje:
Ruta	Número de saltos

Mensaje Response generado por D por su interfaz ppp0	
IP origen del mensaje:	IP destino del mensaje:
Ruta	Número de saltos

## Problema 2 (Junio 2005-problema 2)

Las máquinas de la figura están ejecutando el protocolo de encaminamiento RIP v1.0.



Escriba los mensajes periódicos RIP Response que generan cada una de las máquinas suponiendo lo siguiente:

- Se ha alcanzado la convergencia de rutas.
- Todos los enlaces punto a punto son anónimos.
- Si considera que algún mensaje no se produce o está vacío, debe indicarlo explícitamente con la palabra “vacío” en la tabla.
- Los mensajes Response indican con número de saltos 1 (no 0), aquellas redes a las que están directamente conectadas.
- La implementación de RIP v1.0 que ejecutan las máquinas involucradas, aplica el mecanismo de *split horizon* simple, excepto la máquina E que implementa *split horizon* con inversión de ruta (*poisoned reverse*).

Mensaje Response generado por A por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por A por su interfaz ppp1	
Ruta	Número de saltos

Mensaje Response generado por B por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por B por su interfaz ppp1	
Ruta	Número de saltos



Mensaje Response generado por B por su interfaz ppp2	
Ruta	Número de saltos

Mensaje Response generado por D por su interfaz ppp0	
Ruta	Número de saltos

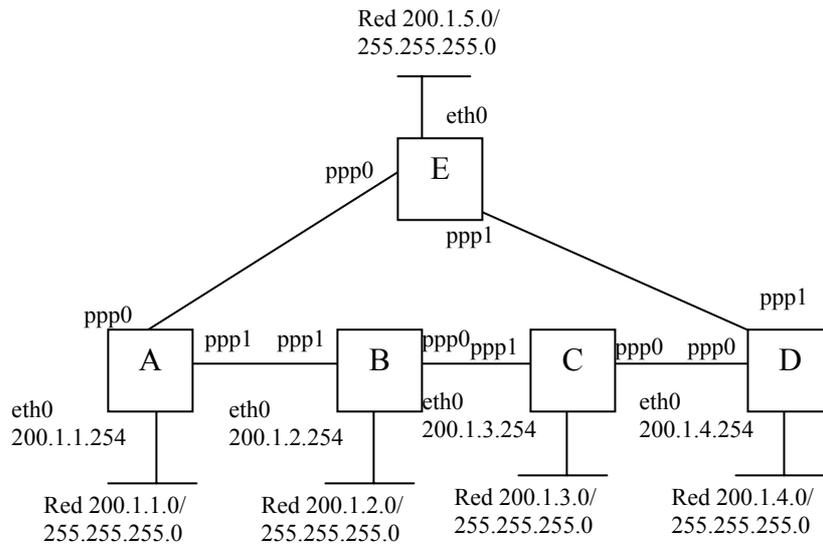
Mensaje Response generado por E por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por E por su interfaz ppp1	
Ruta	Número de saltos

**Problema 3 (Septiembre 2005-problema 3)**

Las máquinas de la figura inferior están ejecutando el protocolo de encaminamiento RIP v1.0. Escriba los mensajes periódicos RIP Response que generan cada una de las máquinas suponiendo lo siguiente:

- Se ha alcanzado la convergencia de rutas.
- Todos los enlaces punto a punto son anónimos.
- Si considera que algún mensaje no se produce o está vacío, debe indicarlo explícitamente con la palabra “vacío” en la tabla.
- Los mensajes Response indican con número de saltos 1 (no 0), aquellas redes a las que están directamente conectadas.
- La implementación de RIP v1.0 que ejecutan las máquinas involucradas, aplica el mecanismo de *split horizon* simple, excepto la máquina D que implementa *split horizon* con inversión de ruta (*poisoned reverse*).



Mensaje Response generado por A por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por A por su interfaz ppp1	
Ruta	Número de saltos

Mensaje Response generado por B por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por B por su interfaz ppp1	
Ruta	Número de saltos

Mensaje Response generado por D por su interfaz ppp0	
Ruta	Número de saltos

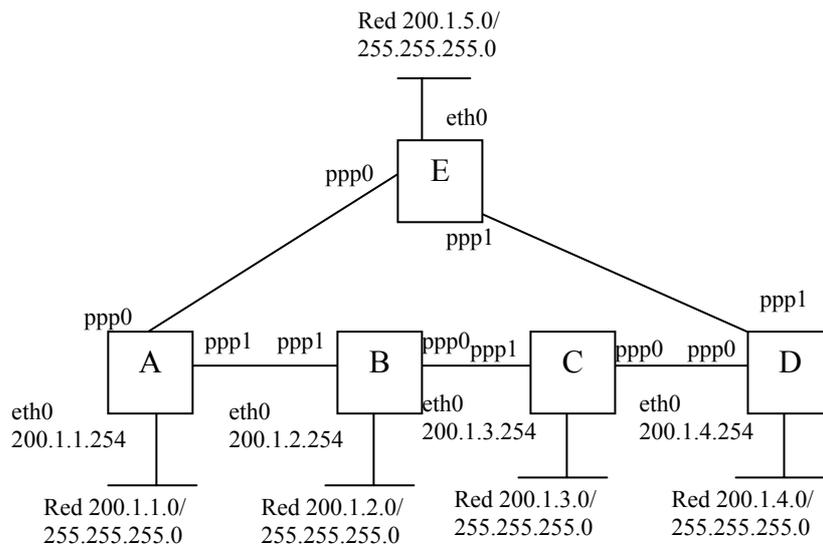
Mensaje Response generado por D por su interfaz ppp1	
Ruta	Número de saltos



**Problema 4 (Diciembre 2005-problema 3)**

Las máquinas de la figura están ejecutando el protocolo de encaminamiento RIP v1.0. Escriba los mensajes periódicos RIP Response que generan cada una de las máquinas suponiendo lo siguiente:

- Se ha alcanzado la convergencia de rutas.
- Todos los enlaces punto a punto son anónimos.
- Si considera que algún mensaje no se produce o está vacío, debe indicarlo explícitamente con la palabra “vacío” en la tabla.
- Los mensajes Response indican con número de saltos 1 (no 0), aquellas redes a las que están directamente conectadas.
- La implementación de RIP v1.0 que ejecutan las máquinas involucradas, aplica el mecanismo de *split horizon* con inversión de ruta (*poisoned reverse*).



Mensaje Response generado por A por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por A por su interfaz ppp1	
Ruta	Número de saltos

Mensaje Response generado por B por su interfaz ppp0	
Ruta	Número de saltos

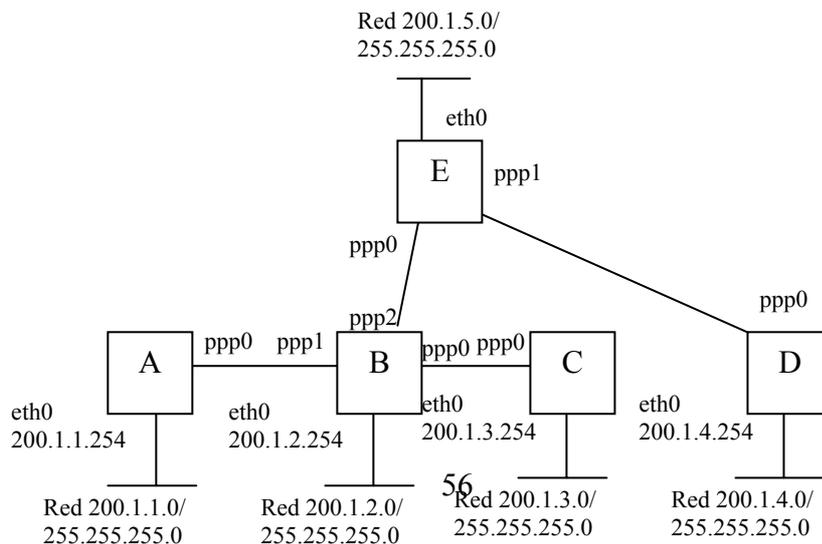
Mensaje Response generado por B por su interfaz ppp1	
Ruta	Número de saltos

Mensaje Response generado por D por su interfaz ppp0	
Ruta	Número de saltos

### Problema 5 (Junio 2006-problema 3)

Las máquinas de la figura están ejecutando el protocolo de encaminamiento RIP v1.0. Todos los nodos implementan la técnica de split horizon simple con inversión de ruta (*poisoned reverse*). Escriba los mensajes periódicos RIP Response que generan cada una de las máquinas suponiendo lo siguiente:

- Se ha alcanzado la convergencia de rutas.
- Todos los enlaces punto a punto son anónimos.
- Si considera que algún mensaje no se produce o está vacío, debe indicarlo explícitamente con la palabra “vacío” en la tabla.
- Los mensajes Response indican con número de saltos 1 (no 0), aquellas redes a las que están directamente conectadas.



Mensaje Response generado por A por su interfaz ppp0	
Ruta	Número de saltos

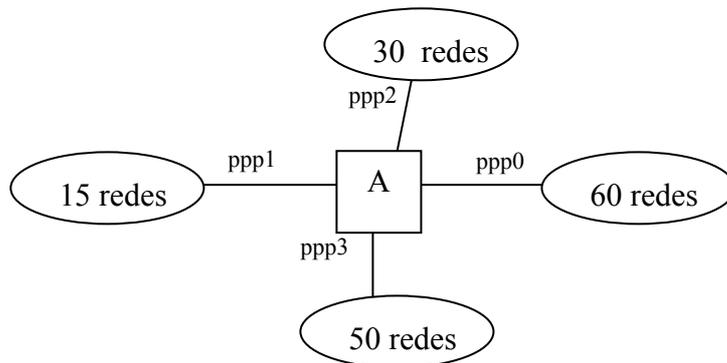
Mensaje Response generado por B por su interfaz ppp1	
Ruta	Número de saltos

Mensaje Response generado por C por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por E por su interfaz ppp0	
Ruta	Número de saltos

**Problema 6 (Septiembre 2006-problema 3)**

La siguiente figura muestra el *router A*, único punto que interconecta dentro de un sistema autónomo los 4 grupos de redes que se muestran (es decir, el tráfico entre los 4 grupos debe atravesar este router). El sistema autónomo emplea el protocolo RIP v1.0 como protocolo de encaminamiento dinámico. Responda justificadamente a las siguientes preguntas (deben incluirse los cálculos):



**Nota:** Tenga en cuenta que un envío periódico puede suponer el envío de 1 o más mensajes por cada interfaz. Cada mensaje RIP puede incluir un máximo de 25 rutas. Suponga que el tamaño en bytes de un mensaje RIP es igual a: 32 bytes, más 20 bytes por cada ruta que incluye.

- a) ¿Cuál es la suma del tamaño en bytes de los mensajes RIP que envía el router A por su interfaz ppp0, suponiendo que la técnica empleada por el router es la de *split horizon* sin inversión de ruta?

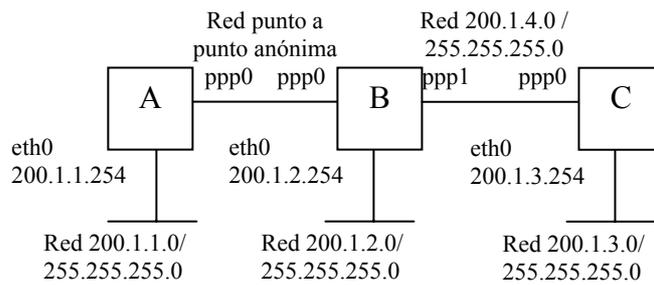
- b) ¿Cuál es la suma del tamaño en bytes de los mensajes RIP que envía el router A por su interfaz ppp1, suponiendo que la técnica empleada por el router es la de *split horizon* con inversión de ruta?

- c) ¿Cuál es la suma del tamaño en bytes de los mensajes RIP que envía el router A por su interfaz ppp2, suponiendo que la técnica empleada por el router es la de *split horizon* con inversión de ruta?

### Problema 7 (Febrero 2007-problema 3)

Las máquinas de la figura están ejecutando el protocolo de encaminamiento RIP v1.0. Todos los nodos implementan la técnica de split horizon simple con inversión de ruta (*poisoned reverse*). Inicialmente ( $t=0$ ), las tablas de encaminamiento de los nodos contienen únicamente las entradas de las redes a las que están directamente conectadas. Se produce la siguiente sucesión de eventos:

- En  $t=1$  el router A envía por cada uno de sus interfaces un mensaje Response.
- En  $t=2$  el router B envía por cada uno de sus interfaces un mensaje Response.
- En  $t=3$  el router C envía por cada uno de sus interfaces un mensaje Response.



Rellene las tablas indicadas a continuación teniendo en cuenta que:

- Si considera que algún mensaje está vacío, debe indicarlo explícitamente con la palabra “vacío” en la tabla.
- Los mensajes Response indican con número de saltos 1, aquellas redes a las que están directamente conectadas.

Mensaje Response generado por A en $t=1$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por B en $t=2$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por B en $t=2$ por su interfaz ppp1	
Ruta	Número de saltos

Mensaje Response generado por B en $t=2$ por su interfaz eth0	
Ruta	Número de saltos

Mensaje Response generado por C en $t=3$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por C en $t=3$ por su interfaz eth0	
Ruta	Número de saltos

Tabla encaminamiento <i>router A</i> en $t=4$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

Tabla encaminamiento <i>router B</i> en $t=4$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

Tabla encaminamiento <i>router C</i> en $t=4$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

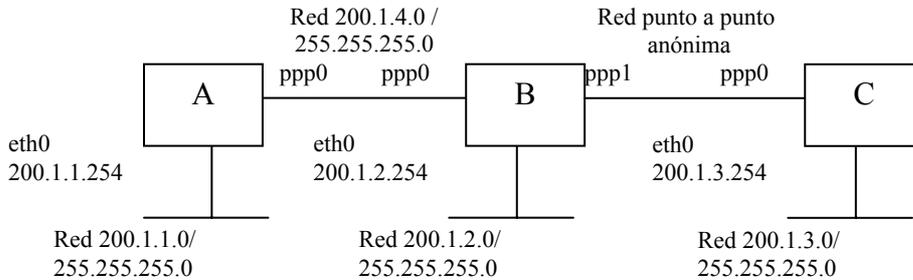
### Problema 8 (Junio 2007-problema 3)

Las máquinas de la figura están ejecutando el protocolo de encaminamiento RIP v1.0. Todos los nodos implementan la técnica de *split horizon* simple SIN inversión de ruta (sin *poisoned reverse*). Inicialmente ( $t=0$ ), las tablas de encaminamiento de los nodos contienen únicamente las entradas de las redes a las que están directamente conectadas. Se produce la siguiente sucesión de eventos:

- En  $t=1$  el router B envía por cada uno de sus interfaces un mensaje Response.
- En  $t=2$  el router A envía por cada uno de sus interfaces un mensaje Response.
- En  $t=3$  el router C envía por cada uno de sus interfaces un mensaje Response.

Rellene las tablas indicadas a continuación teniendo en cuenta que:

- Si considera que algún mensaje está vacío, debe indicarlo explícitamente con la palabra “vacío” en la tabla.
- Los mensajes Response indican con número de saltos 1, aquellas redes a las que están directamente conectadas.



Mensaje Response generado por B en $t=1$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por B en $t=1$ por su interfaz ppp1	
Ruta	Número de saltos

Mensaje Response generado por A en $t=2$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por A en $t=2$ por su interfaz eth0	
Ruta	Número de saltos

Mensaje Response generado por C en $t=3$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por C en $t=3$ por su interfaz eth0	
Ruta	Número de saltos

Tabla encaminamiento <i>router A</i> en $t=4$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

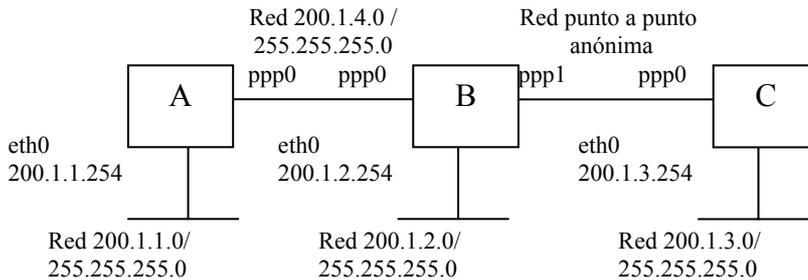
Tabla encaminamiento <i>router B</i> en $t=4$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

Tabla encaminamiento <i>router C</i> en $t=4$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

### Problema 9 (Septiembre 2007-problema 3)

Las máquinas de la figura están ejecutando el protocolo de encaminamiento RIP v1.0. Todos los nodos implementan la técnica de *split horizon* simple CON inversión de ruta (con *poisoned reverse*). Inicialmente ( $t=0$ ), las tablas de encaminamiento de los nodos contienen únicamente las entradas de las redes a las que están directamente conectadas. Se produce la siguiente sucesión de eventos:

- En  $t=1$  el router A envía por cada uno de sus interfaces un mensaje Response.
- En  $t=2$  el router C envía por cada uno de sus interfaces un mensaje Response.
- En  $t=3$  el router B envía por cada uno de sus interfaces un mensaje Response.



Rellene las tablas indicadas a continuación teniendo en cuenta que:

- Si considera que algún mensaje está vacío, debe indicarlo explícitamente con la palabra “vacío” en la tabla.
- Los mensajes Response indican con número de saltos 1, aquellas redes a las que están directamente conectadas.

Mensaje Response generado por A en $t=1$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por A en $t=1$ por su interfaz eth0	
Ruta	Número de saltos

Mensaje Response generado por C en $t=2$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por C en $t=2$ por su interfaz eth0	
Ruta	Número de saltos

Mensaje Response generado por B en $t=3$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por B en $t=3$ por su interfaz ppp1	
Ruta	Número de saltos

Tabla encaminamiento <i>router A</i> en $t=4$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

Tabla encaminamiento <i>router B</i> en $t=4$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

Tabla encaminamiento <i>router C</i> en $t=4$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

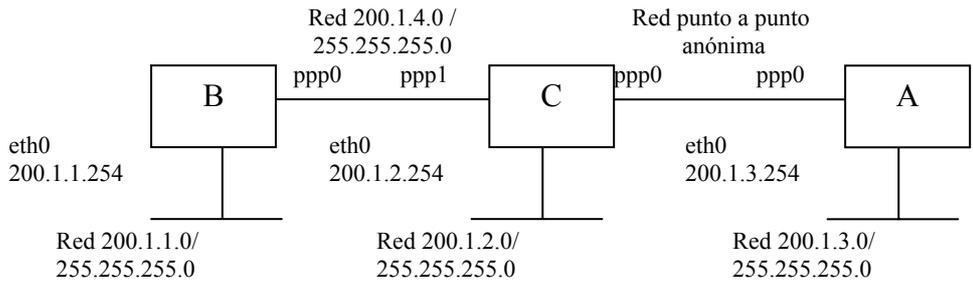
**Problema 10 (Febrero 2008-problema 3)**

Las máquinas de la figura están ejecutando el protocolo de encaminamiento RIP v1.0. Todos los nodos implementan la técnica de *split horizon* simple CON inversión de ruta (con *poisoned reverse*). Inicialmente ( $t=0$ ), las tablas de encaminamiento de los nodos contienen únicamente las entradas de las redes a las que están directamente conectadas. Se produce la siguiente sucesión de eventos:

- En  $t=1$  el router A envía por cada uno de sus interfaces un mensaje Response.
- En  $t=2$  el router C envía por cada uno de sus interfaces un mensaje Response.
- En  $t=3$  el router B envía por cada uno de sus interfaces un mensaje Response.

Rellene las tablas indicadas a continuación teniendo en cuenta que:

- Si considera que algún mensaje está vacío, debe indicarlo explícitamente con la palabra “vacío” en la tabla.
- Los mensajes Response indican con número de saltos 1, aquellas redes a las que están directamente conectadas.



Mensaje Response generado por A en $t=1$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por A en $t=1$ por su interfaz eth0	
Ruta	Número de saltos

Mensaje Response generado por C en $t=2$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por C en $t=2$ por su interfaz ppp1	
Ruta	Número de saltos

Mensaje Response generado por B en $t=3$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por B en $t=3$ por su interfaz eth0	
Ruta	Número de saltos

Tabla encaminamiento <i>router</i> A en $t=4$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

Tabla encaminamiento <i>router</i> B en $t=4$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

Tabla encaminamiento <i>router</i> C en $t=4$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

**Problema 11 (Junio 2008-problema 3)**

Las máquinas de la figura están ejecutando el protocolo de encaminamiento RIP v1.0. Todos los nodos implementan la técnica de *split horizon* simple SIN inversión de ruta (sin *poisoned reverse*). Inicialmente ( $t=0$ ), las tablas de encaminamiento de los nodos contienen únicamente las entradas de las redes a las que están directamente conectadas. Se produce la siguiente sucesión de eventos:

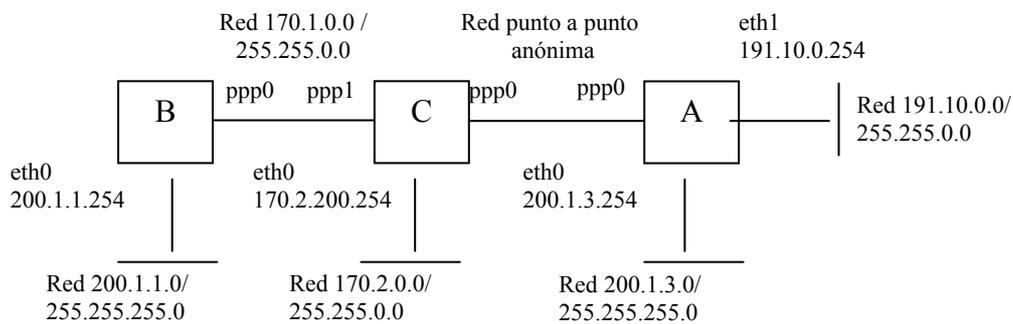
- En  $t=1$  el Router A y el Router B envían por cada una de sus interfaces un mensaje Response.
- En  $t=2$  se pierde la conectividad entre el Router C y A (caída del enlace asociado a la red anónima). Los dos extremos de esta enlace punto a punto (C y A),

instantáneamente detectan este hecho, y asocian una distancia 16 a todos los destinos que alcanzan a través de esa interfaz.

- En  $t=3$  el Router C envía por cada una de sus interfaces activas un mensaje Response. Nota: Cuando un router recibe un mensaje Response con una distancia infinita (16) a un destino, y ese destino era desconocido para él, no añade esa entrada a su tabla de encaminamiento.
- En  $t=4$  el Routers B envía por cada una de sus interfaces un mensaje Response.

Rellene las tablas indicadas a continuación teniendo en cuenta que:

- Si considera que algún mensaje está vacío, debe indicarlo explícitamente con la palabra “vacío” en la tabla.
- Los mensajes Response indican con número de saltos 1, aquellas redes a las que están directamente conectadas.



Mensaje Response generado por A en $t=1$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por B en $t=1$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por C en $t=3$ por su interfaz eth0	
Ruta	Número de saltos

Mensaje Response generado por C en $t=3$ por su interfaz ppp1	
Ruta	Número de saltos

Mensaje Response generado por B en $t=4$ por su interfaz eth0	
Ruta	Número de saltos

Mensaje Response generado por B en $t=4$ por su interfaz ppp0	
Ruta	Número de saltos



Tabla encaminamiento <i>router A</i> en $t=5$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

Tabla encaminamiento <i>router C</i> en $t=5$ (con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

**Problema 12 (Septiembre 2008-problema 3)**

Las máquinas de la figura están ejecutando el protocolo de encaminamiento RIP v1.0. Todos los nodos implementan la técnica de *split horizon* simple CON inversión de ruta (con *poisoned reverse*). Inicialmente ( $t=0$ ), las tablas de encaminamiento de los nodos contienen únicamente las entradas de las redes a las que están directamente conectadas. Se produce la siguiente sucesión de eventos:

- En  $t=1$  el Router A y el Router B envían por cada una de sus interfaces un mensaje Response.
- En  $t=2$  los Router B y A pierden la conectividad con el Router C. Los dos extremos de estos enlaces punto a punto instantáneamente detectan este hecho, y asocian una distancia 16 a todos los destinos que alcanzan a través de esa interfaz.
- En  $t=3$  el Router C envía por cada una de sus interfaces conectadas a un enlace activo un mensaje Response. Nota: Cuando un router recibe un mensaje Response

con destino cuya distancia es infinita (16) y ese destino es desconocido para él, no añade esa entrada a su tabla de encaminamiento.

- En  $t=4$  se restablece la conectividad de los Routers B y A con el Router C. Los extremos de estos enlaces punto a punto instantáneamente detectan este hecho, y asocian una distancia 1 a todas las redes directamente conectadas.
- En  $t=5$ , el Router B envía por cada una de sus interfaces un mensaje Response.

Rellene las tablas indicadas a continuación teniendo en cuenta que:

- Si considera que alguna tabla de encaminamiento está vacía, o algún mensaje está vacío debe indicarlo explícitamente con la palabra “vacío” en la tabla.
- Si considera que NO se envía o recibe algún mensaje Response por alguna interfaz debe indicarlo en su tabla correspondiente como “no Response”
- Los mensajes Response indican con número de saltos 1, aquellas redes a las que están directamente conectadas.

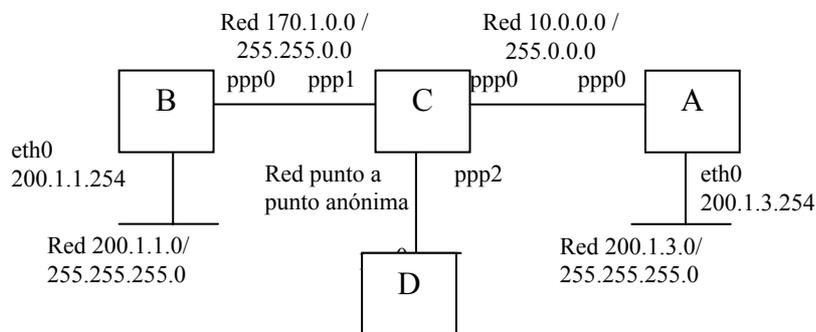


Tabla encaminamiento <i>router C</i> en $t=1.5$ (actualizada tras recibir los mensajes Response de sus routers vecinos en $t=1$ y con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

Mensaje Response generado por C en $t=3$ por su interfaz ppp0	
Ruta	Número de saltos

Mensaje Response generado por C en $t=3$ por su interfaz ppp2	
Ruta	Número de saltos

Tabla encaminamiento <i>router</i> D en $t=4.5$ (actualizada con los eventos sucedidos en $t=3$ y $t=4$ y con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

Tabla encaminamiento <i>router</i> A en $t=4.5$ (actualizada tras detectar la conectividad con su Router vecino C y con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

Tabla encaminamiento <i>router</i> C en $t=4.5$ (actualizada tras detectar la conectividad con su Router vecino C y con información de distancia en número de saltos)				
Dirección	Máscara	Interfaz de salida	Gateway	Distancia (saltos)

Mensaje Response recibido en C por su interfaz ppp1 en $t=5$	
Ruta	Número de saltos

Mensaje Response generado por B en $t=5$ por su interfaz eth0	
Ruta	Número de saltos

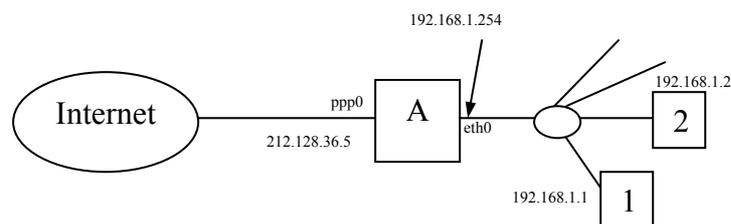
## Bloque temático 4. Mecanismos de traducción de direcciones (NAT)

Para resolver la mayoría de los problemas de este bloque el alumno debe tener conocimiento, no solo de NAT sino también de direccionamiento IP, protocolo TCP, mecanismos de extensión de direccionamiento IPv4: Proxy ARP, Subnetting, CIDR, etc.

### Problema 1 (Septiembre 2002-cuestión 2)

En la figura observamos una red local privada, en la que se ha configurado el mecanismo de IP-Masquerading en el router A para proporcionar conexión a Internet. Este router mantiene internamente una tabla para gestionar las conexiones TCP que está enmascarando. En un momento dado, los contenidos de esa tabla son los siguientes:

IP origen	Puerto origen	Puerto enmascarador
192.168.1.1	1700	61000
192.168.1.1	1701	61001
192.168.1.1	1702	61002
192.168.1.2	1700	61003
192.168.1.2	1701	61004
192.168.1.2	1702	61005



En este momento, el router A recibe por una de sus interfaces un datagrama IP, perteneciente a una conexión TCP, con las siguientes características:

IP origen	192.168.1.2
IP destino	200.4.6.1
Puerto TCP origen	1050
Puerto TCP destino	23

- a) ¿Se añadirá alguna entrada en la tabla de conexiones TCP enmascaradas? ¿Por qué?

b) Si la pregunta anterior es afirmativa escriba el contenido de esa entrada.

IP origen	Puerto origen	Puerto enmascarador

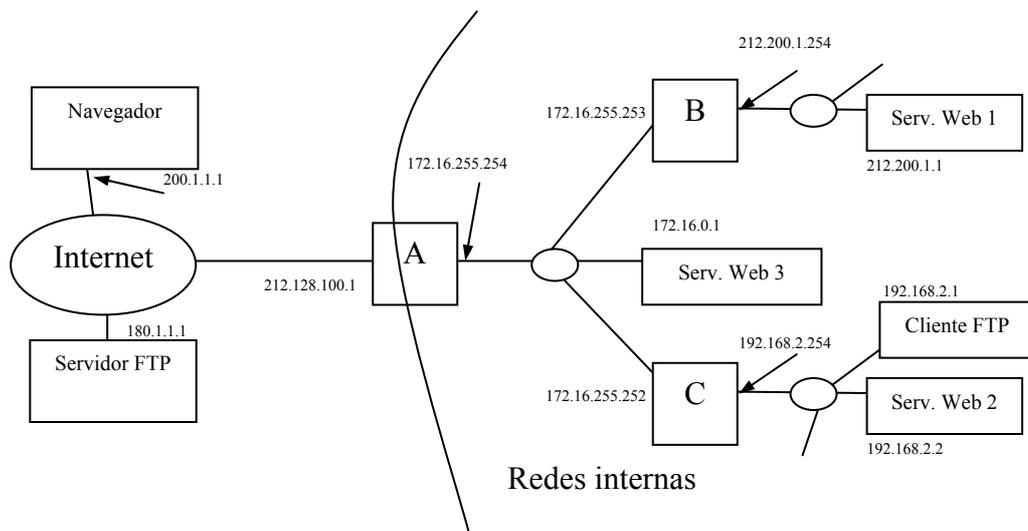
c) El mecanismo de IP-Masquerading realiza una serie de cambios en la cabecera IP y TCP de los datagramas pertenecientes a las conexiones TCP. El alumno debe rellenar la siguiente tabla en función de lo contestado en la cuestión anterior, lo que reflejará cuáles son esos cambios en los datagramas de la conexión TCP objeto de estudio.

Datagramas de la conexión TCP	IP origen	IP destino	Puerto TCP origen	Puerto TCP destino
Datagramas generados por 192.168.1.2				
Datagramas transmitidos por router A hacia 200.4.6.1				
Datagramas generados por 200.4.6.1				
Datagramas transmitidos por router A hacia 192.168.1.2				

### Problema 2 (Junio 2003-problema 1)

El router A de la figura implementa la funcionalidad NAT entre el dominio interno (en el que todas las redes físicas son de tecnología Ethernet) y la red IP Internet. Todos los servidores Web se encuentran dando servicio en el puerto 80 de los servidores donde se ejecutan. Se configuran las siguientes funcionalidades en router A:

- La red de clase C 212.200.1.0 se configura como red visible desde el exterior.
- El servidor Web 2 en la máquina 192.168.2.2 se hace accesible al exterior a través del puerto 80.
- El servidor Web 3 en la máquina 172.16.0.1 se hace accesible al exterior a través del puerto 8080.



a) Indique el contenido de la tabla de configuración de puertos visibles

Tabla de puertos visibles		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

b) Indique el contenido de la tabla de configuración de subredes visibles

Tabla de Subredes visibles	
IP subred	Máscara de subred

c) El router A recibe por su interfaz externa un datagrama que transporta un segmento TCP, con las siguientes características:

IP origen	Puerto origen	IP destino	Puerto destino
180.1.1.1	21	212.128.100.1	61000

En ese momento, su tabla de conexiones enmascaradas contiene los valores:

IP interna	Puerto Máquina interna	Puerto Externo
172.16.0.1	1900	61000
192.168.2.1	1500	61001

Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP a la que pertenece el segmento recibido.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Red interna → Router A				
Router A → Destino Externo				
Destino Externo → Router A				
Router A → Red interna				

d) Desde la máquina 200.1.1.1 se lanza un navegador que realiza una petición de una página al servidor Web 1 (puerto TCP origen 1301). Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de esta conexión TCP.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Navegador→Router A				
Router A→Serv. Web 1				
Serv. Web 1→Router A				
Router A→Navegador				

- e) Desde la máquina 200.1.1.1 se lanza otro navegador que realiza una petición de una página al servidor Web 2 (puerto TCP origen 1302). Rellene las siguientes tablas describiendo la traducción de direcciones y puertos que sufren los segmentos de esta conexión TCP.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Navegador→Router A				
Router A→Serv. Web 2				
Serv. Web 2→Router A				
Router A→Navegador				

- f) Desde la máquina 200.1.1.1 se lanza otro navegador que realiza una petición de una página al servidor Web 3 (puerto TCP origen 1303). Rellene las siguientes tablas describiendo la traducción de direcciones y puertos que sufren los segmentos de esta conexión TCP.

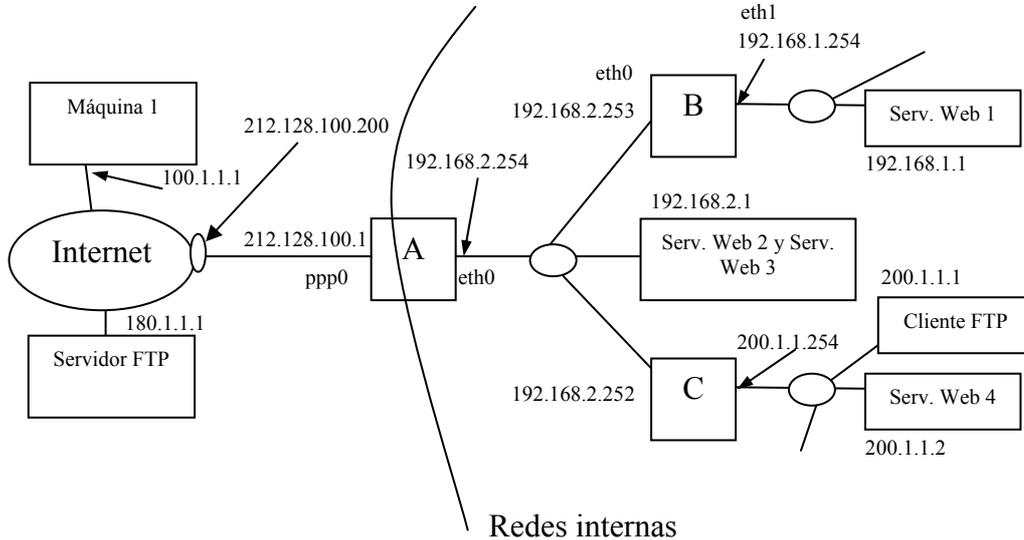
Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Navegador→Router A				
Router A→Serv. Web 3				
Serv. Web 3→Router A				
Router A→Navegador				

### Problema 3 (Septiembre 2003-problema 1)

El router A de la figura implementa la funcionalidad NAT entre el dominio interno (en el que todas las redes físicas son de tecnología Ethernet) y la red IP Internet. Se configuran las siguientes funcionalidades en el router A:

- La red de clase C 200.1.1.0 se configura como red visible desde el exterior.
- El servidor Web 1 en la máquina 192.168.1.1 recibe peticiones por el puerto 80 y se hace accesible al exterior a través del puerto 8080.

- El servidor Web 2 en la máquina 192.168.2.1 recibe peticiones por el puerto 80 y se hace accesible al exterior a través del puerto 8081.
- El servidor Web 3 en la máquina 192.168.2.1 recibe peticiones por el puerto 8080 y se hace accesible al exterior a través del puerto 8082.
- El servidor Web 4 en la máquina 200.1.1.2 recibe peticiones por el puerto 8080.



a) Indique el contenido de la tabla de configuración de puertos visibles

Tabla de puertos visibles		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

b) Indique el contenido de la tabla de configuración de subredes visibles

Tabla de Subredes visibles	
IP subred	Máscara de subred

c) Escriba el contenido de las siguientes tablas encaminamiento

Router B			
IP destino	Máscara	Interfaz Salida	Gateway


Router A			
IP destino	Máscara	Interfaz Salida	Gateway

d) El router A recibe por su interfaz externa un datagrama que transporta un segmento TCP, con las siguientes características:

IP origen	Puerto origen	IP destino	Puerto destino
100.1.1.1	1200	212.128.100.1	8080

En ese momento, su tabla de conexiones enmascaradas contiene los valores:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.1.1	1200	61000
192.168.2.1	1500	61001

e) Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP a la que pertenece el segmento recibido.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Red interna → Router A				
Router A → Destino Externo				
Destino Externo → Router A				
Router A → Red interna				

f) El router A recibe un datagrama con las siguientes características

IP origen	Puerto origen	IP destino	Puerto destino
192.168.2.1	1500	180.1.1.1	21

En ese momento, su tabla de conexiones enmascaradas contiene los valores:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.1.1	1200	61000
192.168.2.1	1500	61001

- g) Rellene las siguientes tablas describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP a la que pertenece el segmento recibido.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Red interna → Router A				
Router A → Destino Externo				
Destino Externo → Router A				
Router A → Red interna				

- h) El router A recibe un datagrama con las siguientes características

IP origen	Puerto origen	IP destino	Puerto destino
180.1.1.1	21	200.1.1.1	1500

- i) Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP a la que pertenece el segmento recibido.

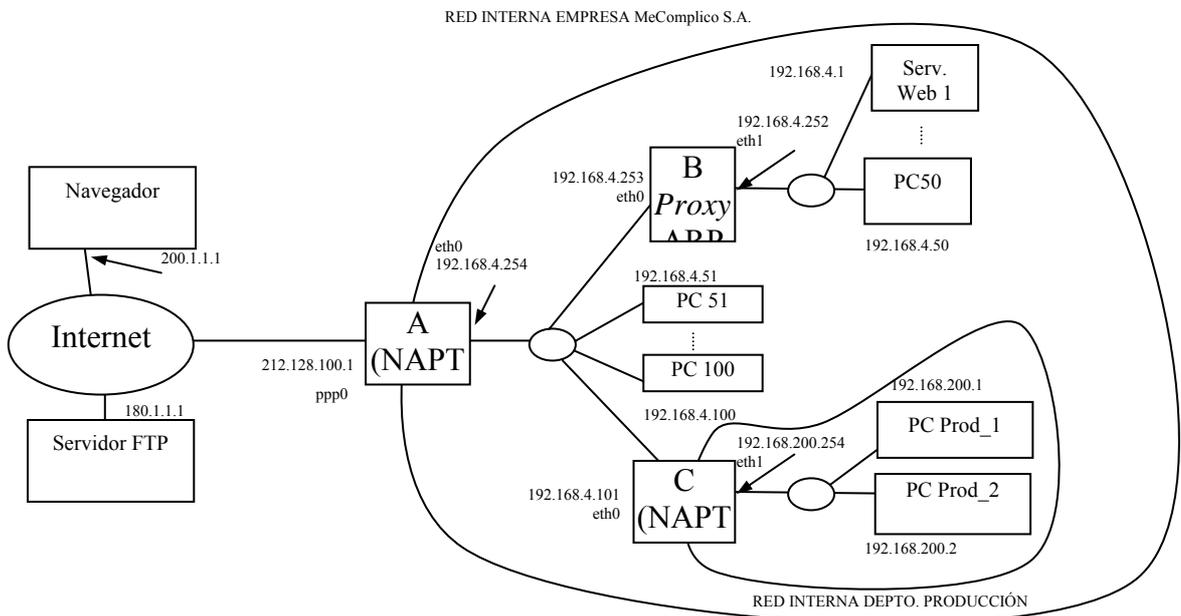
Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Red interna → Router A				
Router A → Destino Externo				
Destino Externo → Router A				
Router A → Red interna				

#### Problema 4 (Junio 2004-problema 2)

La empresa MeComplico S.A se dedica a servicios de consultoría IP. La red interna de la empresa (basada completamente en tecnología *Ethernet*), se muestra en la siguiente figura.

- La única conexión al exterior de la red es a través del *router* A, que implementa la funcionalidad de *Masquerading* (NAPT), con red interna 192.168.4.0/255.255.255.0, y dirección externa 212.128.100.1.
- El conjunto de PCs 1..51 se conecta a la red interna de la empresa a través del *router* B, que implementa la funcionalidad de *Proxy* ARP.
- El departamento de producción ocupa la red 192.168.200.0/255.255.255.0. Sin embargo, con el objetivo de **esconder la existencia de esta red al resto de la empresa**, se configura el *router* C para que implemente NAPT, considerando como red interna la red 192.168.200.0/255.255.255.0, y como dirección externa 192.168.4.1.

- El servidor Web de la empresa se sitúa en el PC 1 de dirección 192.168.4.1, en el puerto 80, y se hace accesible al exterior a través del puerto 80 del *router* A.



La tabla de conexiones enmascaradas del *router* A contiene los valores:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.4.101	61001	61000
192.168.4.1	1500	61001

La tabla de conexiones enmascaradas del *router* C contiene los valores:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.200.1	2000	61001
192.168.200.1	2100	61002
192.168.200.2	3450	61003

- a) Indique el contenido de la tabla de configuración de puertos visibles de *router* A.

Tabla de puertos visibles		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

- b) Escriba la tabla de encaminamiento de los dispositivos que se le indica.

Tabla encaminamiento <i>router</i> C			
Dirección	Máscara	Interfaz de salida	Gateway


Tabla encaminamiento <i>router A</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC 50			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC Prod 1			
Dirección	Máscara	Interfaz de salida	Gateway

- c) El *router A* recibe por su interfaz externa un datagrama que transporta un segmento TCP, con las siguientes características:

IP origen	Puerto origen	IP destino	Puerto destino
180.1.1.1	21	212.128.100.1	61000

- d) Rellene las siguientes tablas describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP a la que pertenece el segmento recibido. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
PC Prod → Router C				
Router C → Router A				
Router A → Destino Externo				

Destino Externo→Router A				
Router A→Router C				
Router C → PC Prod				

e) Desde la máquina 200.1.1.1 se lanza un navegador que realiza una petición de una página (puerto TCP origen 3100) al servidor Web 1. Rellene las siguientes tablas describiendo la traducción de direcciones y puertos que sufren los segmentos de esta conexión TCP. Fijese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Navegador→Router A				
Router A→Router B				
Router B→Serv Web 1				
Serv Web 1→Router B				
Router B→Router A				
Router A → Navegador				

f) El personal del departamento de producción, decide desarrollar una página web del departamento:

- que alojan en el servidor web en el PC Prod\_2, puerto 80,
- hacen accesible hacia el resto de la empresa en el puerto 80 del *router C*,
- y hacen accesible a Internet en el puerto 8080 del *router A*.

**Nota:** Esto implica que el *router A* debe redireccionar las consultas hacia el *router C*, y el *router C* hacia PC Prod\_2.

g) Escriba la tabla de puertos visibles del *router C*, y la nueva tabla de puertos visibles del *router A*, para que este servidor sea visible desde Internet.

Tabla de puertos visibles <i>Router C</i>		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles <i>Router A</i>		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

--	--	--

h) En la situación anterior, rellene la siguiente tabla describiendo la traducción de direcciones de una conexión TCP desde el navegador (200.1.1.1, puerto 1200) con el servidor web del departamento de producción. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Navegador→Router A				
Router A→Router B				
Router B→Serv Produc.				
Serv Produc.→Router B				
Router B→Router A				
Router A → Navegador				

### Problema 5 (Septiembre 2004-problema 2)

La siguiente figura muestra la red interna de una empresa, basada completamente en tecnología *Ethernet*.

- La única conexión al exterior de la red es a través del *router A*, que implementa la funcionalidad de *Masquerading* (NAPT).
- El conjunto de PCs 1..100 se encuentra situado dentro de la red visible 200.1.1.0/255.255.255.0. El *router B* implementa la funcionalidad de *proxy ARP*.
- Los PCs 101,..., 200 se encuentran dentro de la red 192.168.1.0, enmascarada por el *router A*.
- Todos los servidores de la empresa, son accesibles desde Internet y la red interna a través del *router C*, que implementa la funcionalidad de *Masquerading* (ocultando la red 192.168.200.0/255.255.255.0 al resto de la empresa). Los puertos TCP en los cuales estos servicios se hacen públicos son:

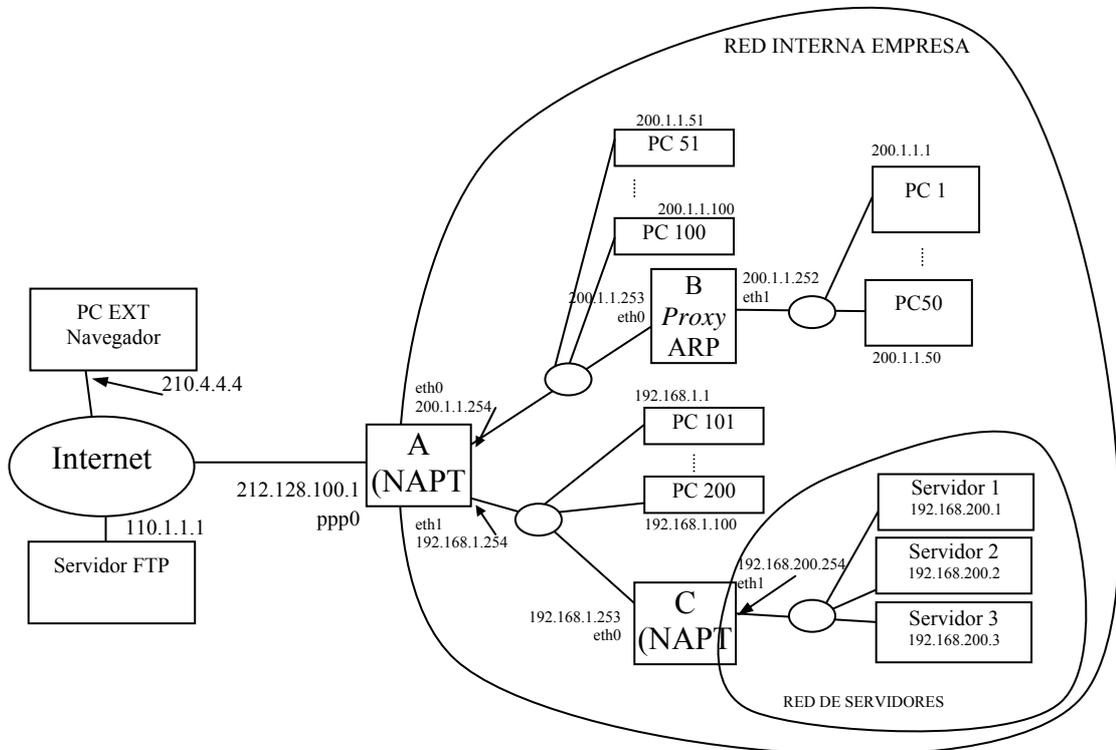
Servidor	Puerto en el servidor para acceso al servicio	Puerto del <i>router C</i> para el acceso al servicio	Puerto del <i>router A</i> para el acceso al servicio
1	80	6001	80
2	80	6002	8080
3	21	6003	21

La tabla de conexiones enmascaradas del *router A* contiene los valores:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.1.253	61001	61000
192.168.1.101	1500	61001

La tabla de conexiones enmascaradas del *router C* contiene los valores:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.200.1	2000	61001
192.168.200.1	2100	61002
192.168.200.2	3450	61003



a) Indique el contenido de la tabla de configuración de puertos visibles del *router A* y del *router C*.

Tabla de puertos visibles Router A		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles Router C		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

b) Escriba la tabla de encaminamiento de los dispositivos que se le indica, minimizando el número de entradas.

Tabla encaminamiento <i>router A</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>Router C</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC 1			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC 51			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC 101			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento Servidor 1			
Dirección	Máscara	Interfaz de salida	Gateway

- c) La aplicación navegador en el PC EXT de dirección 210.4.4.4, abre una conexión TCP desde el puerto 3000, en su acceso al servidor 2 (servidor web). Rellene las siguientes tablas describiendo la traducción de direcciones y puertos que sufren los segmentos de esa conexión TCP. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
PC EXT → Router A				
Router A → Router C				
Router C → Serv 2				
Serv 2 → Router C				
Router C → Router A				
Router A → PC EXT				

- d) Una aplicación cliente FTP en el PC1 establece desde el puerto 2000, una conexión con el puerto 21 del servidor FTP externo. Rellene las siguientes tablas describiendo la traducción de direcciones y puertos que sufren los segmentos de esta conexión TCP. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
PC 1 → Router B				
Router B → Router A				
Router A → Serv FTP				
Serv FTP → Router A				
Router A → Router B				
Router B → PC 1				

El router A recibe por una de sus interfaces internas un datagrama que transporta un segmento TCP, con las siguientes características:

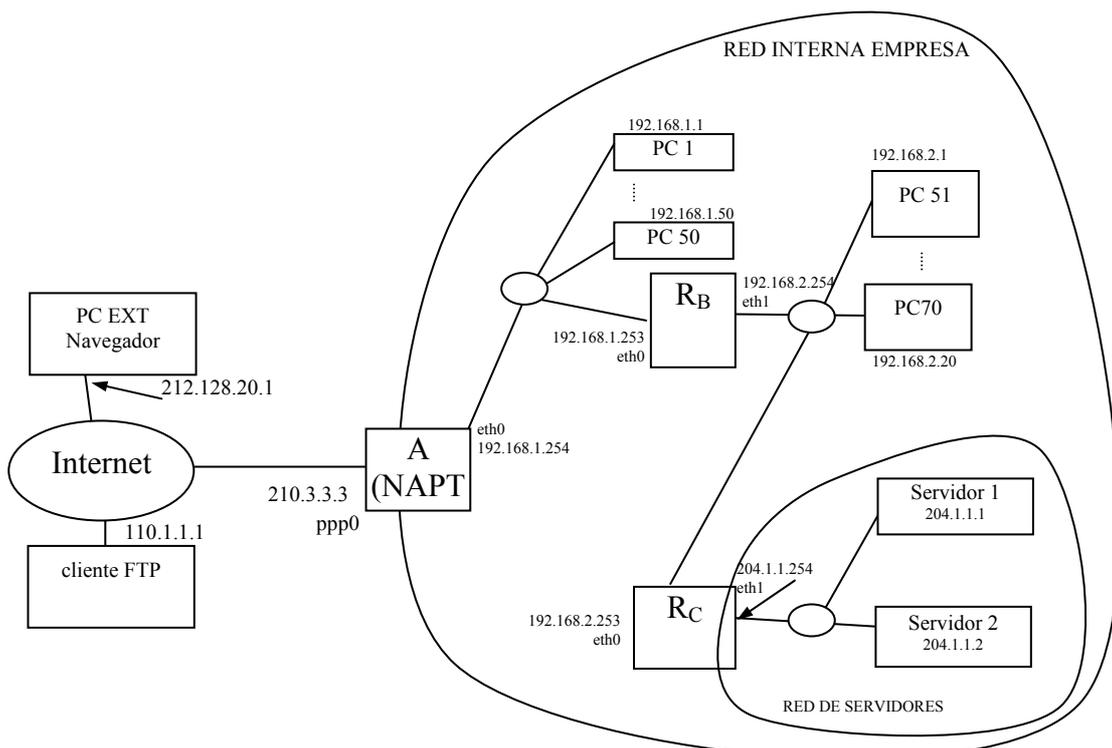
IP origen	Puerto origen	IP destino	Puerto destino
192.168.1.253	61001	100.1.1.1	21

e) Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP a la que pertenece el segmento recibido. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Serv interno → Router C				
Router C → Router A				
Router A → Serv FTP				
Serv FTP → Router A				
Router A → Router B				
Router B → Serv interno				

### Problema 6 (Diciembre 2004-problema 2)

La figura adjunta muestra la red interna de una empresa, basada completamente en tecnología *Ethernet*. La única conexión al exterior de la red es a través del router A, que implementa la funcionalidad de *Masquerading* (NAPT). Los servidores 1 y 2 son servidores web, activos en el puerto TCP 80. Observando las direcciones que tiene cada dispositivo, responda a las siguientes preguntas.



- a) Indique el contenido de la tabla de configuración de puertos visibles y la tabla de subredes visibles del *router A*.

Tabla de puertos visibles <i>Router A</i>		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de Subredes visibles <i>Router A</i>	
IP subred	Máscara de subred

- b) Responda razonadamente a la siguiente pregunta. ¿Cree usted que el *Router C* debe implementar la funcionalidad NATP?.

- c) En caso de que considere que sí es necesario, rellena las siguientes tablas.

Tabla de puertos visibles <i>Router C</i>		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de Subredes visibles <i>Router C</i>	
IP subred	Máscara de subred

- d) Escriba las tablas de encaminamiento de los dispositivos que se le indica, minimizando el número de entradas.

Tabla encaminamiento <i>Router R<sub>A</sub></i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>Router R<sub>B</sub></i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>Router R<sub>C</sub></i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento Servidor 1			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC 51			
Dirección	Máscara	Interfaz de salida	Gateway


Tabla encaminamiento PC 1			
Dirección	Máscara	Interfaz de salida	Gateway

- e) La aplicación navegador en el PC EXT de dirección 210.4.4.4, abre una conexión TCP desde el puerto 2100, en su acceso al servidor 2. Rellene las siguientes tablas describiendo la traducción de direcciones y puertos que sufren los segmentos de esa conexión TCP. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

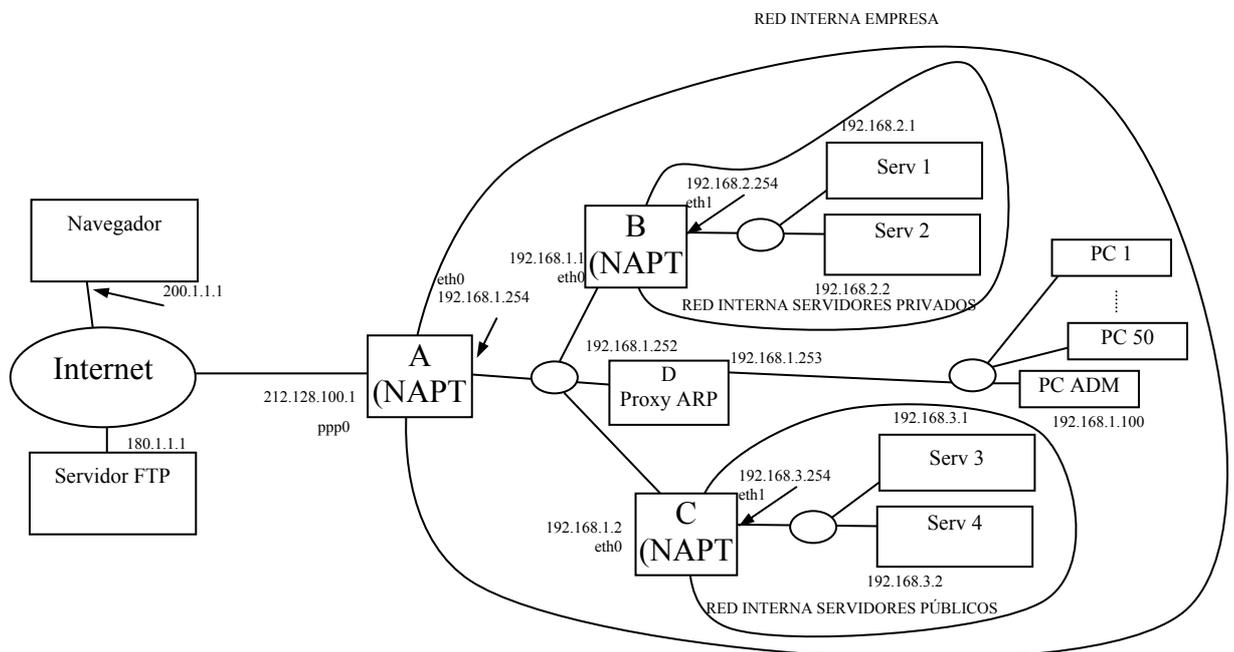
Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
PC EXT → Router A				
Router A → Router B				
Router B → Router C				
Router C → Servidor 2				
Servidor 2 → Router C				
Router C → Router B				
Router B → Router A				
Router A → PC EXT				

### Problema 7 (Junio 2005-problema 3)

La figura inferior muestra la red interna de la empresa AAA, basada completamente en tecnología *Ethernet*.

- Los routers A, B, C implementan la funcionalidad de *Masquerading*.
- Los servidores 1 y 2 proporcionan servicios que tienen que ser accesibles al resto de PCs de la red interna (incluidos los servidores 3 y 4). Ninguno de estos servicios debe ser accesible desde Internet.
  - o El servidor 1 proporciona dos servicios en los puertos 3000 y 3001 que deben ser accesibles en el puerto 3000 y 3001 del router B.

- El servidor 2 implementa un servicio en el puerto 3000, que debe ser accesible en el puerto 3002 del router B.
- Los servidores 1 y 2 implementan el servicio SSH (*Secure Shell*) en el puerto 22, que debe ser accesible a la red interna (incluidos los servidores 3 y 4) en los puertos 22 y 2222 respectivamente.
- Los servidores 3 y 4 proporcionan servicios que deben ser accesible al resto de PCs de la red interna (incluidos los servidores 1 y 2) y a los usuarios de Internet.
  - El servidor 3 proporciona el servicio Web en el puerto 80, que debe ser accesible en el router C y en el router A también en el puerto 80.
  - El servidor 4 proporciona el servicio FTP en el puerto 21, que debe ser accesible en el router C en el puerto 2121 y en el router A en el puerto 21.
- El router D implementa la funcionalidad de Proxy ARP.



a) Indique el contenido de las siguientes tablas de configuración de puertos visibles.

Tabla de puertos visibles Router A		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles <i>Router B</i>		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles <i>Router C</i>		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

b) Escriba la tabla de encaminamiento de los dispositivos que se le indica.

Tabla encaminamiento <i>router A</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>router B</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>router C</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC ADM			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento Servidor 1			
Dirección	Máscara	Interfaz de salida	Gateway

- c) El PC ADM abre una conexión SSH desde el puerto 2000 con el Servidor 2. Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP de esa conexión. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
PC ADM → Router D				
Router D → Router B				
Router B → Serv 2				
Serv 2 → Router B				
Router B → Router D				
Router D → PC ADM				

- d) ¿Existe alguna posibilidad de que un momento dado, la tabla de conexiones enmascaradas del *router* A sea la que muestra la figura?. ¿Por qué?

IP interna	Puerto Máquina interna	Puerto Externo
192.168.1.100	3560	61107
192.168.1.100	3800	61108
192.168.2.1	3560	61100

- e) ¿Existe alguna posibilidad de que un momento dado, la tabla de conexiones enmascaradas del *router* C sea la que muestra la figura?. ¿Por qué?

IP interna	Puerto Máquina interna	Puerto Externo
192.168.1.1	3560	61107
192.168.3.1	3800	61108

- f) Desde la máquina PC ADM se ha abierto una conexión TCP con el servidor FTP (puerto 21) en 180.1.1.1. Rellene las siguientes tablas describiendo la traducción de direcciones y puertos que sufren los segmentos de esta conexión TCP. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
PC ADM → Router D				
Router D → Router A				
Router A → Serv FTP				
Serv FTP → Router A				
Router A → Router D				
Router D → PC ADM				

**Nota:** La tabla de conexiones enmascaradas del *router* A, *después* de que se haya completado el establecimiento de conexión TCP, se muestra a continuación:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.1.100	3000	61002
192.168.1.1	4500	61000

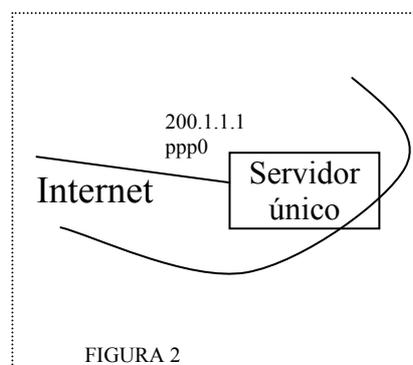
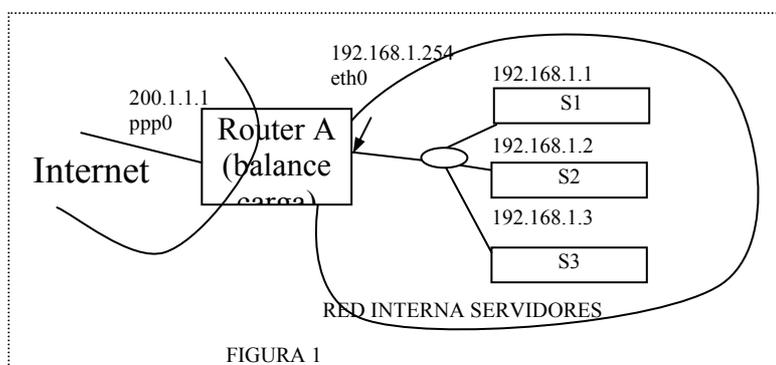
## Problema 8 (Septiembre 2005-problema 4)

La figura 1 muestra la sala de servidores de un portal de Internet <http://www.tuporaqui.es>. Todas las consultas de páginas web a este portal, vienen dirigidas al puerto 80 del router A, cuya dirección IP externa es 200.1.1.1 (la dirección IP asociada al nombre de dominio <http://www.tuporaqui.es>).

En su nacimiento, la empresa encargada del portal, inició su funcionamiento utilizando una única máquina servidora (configuración antigua, figura 2). Sin embargo, el excesivo volumen de consultas provocó la necesidad de actualizar el sistema. Entre las opciones de actualización, se encontraba la sustitución del servidor inicial por uno de mayor capacidad. Esta solución fue desechada por su alto precio, y poca flexibilidad ante posibles crecimientos futuros. La decisión adoptada implica la instalación de un router de balance de carga (*load sharing router*), que reparta las consultas a las páginas web, entre un grupo de servidores, tal y como indica la figura 1. Todos los servidores internos S1, S2, S3 emplean el puerto 80 para el servicio web.

El mecanismo de balance de carga implantado consiste en:

1. El router A se configura como el único dispositivo visible desde el exterior, tomando la dirección del portal en su interfaz externa (200.1.1.1), y atendiendo consultas web en el puerto 80.
2. Las conexiones TCP desde clientes externos, destinadas a la dirección 200.1.1.1, puerto 80, deben ser redireccionadas por el router, a uno de los servidores internos adquiridos (S1, S2, S3 en la figura).
3. La asignación de servidor a cada conexión TCP entrante nueva, se elige repitiendo un orden secuencial (S1, S2, S3, S1, S2, S3, ...).
4. La asignación (conexión TCP ; servidor) debe ser recordada, ya que los futuros segmentos de la conexión TCP deben ser redirigidos al mismo servidor.
5. La existencia del router de balance de carga debe ser transparente para cada uno de los servidores, que deben tener la ilusión de estar recibiendo conexiones directamente de los clientes externos. Esto implica un proceso de traducción de direcciones para el tráfico entrante (cliente→router→servidor).
6. La existencia del router de balance de carga debe ser transparente para los clientes, que deben tener la ilusión de que existe una única máquina 200.1.1.1 que atiende sus consultas. Esto implica un proceso de traducción de direcciones para el tráfico saliente (servidor→router→cliente).



Un usuario en Internet (dirección 100.1.1.1) abre un navegador y visita la página web <http://www.tuporaqui.es>. Esto implica un establecimiento de conexión TCP con

destino 200.1.1.1, puerto 80. El puerto efímero del cliente es el 2100. El router de reparto de carga, asigna el servidor 3 a esta conexión TCP.

- a) Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de esa conexión TCP. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Usuario → Router A				
Router A → Servidor S3				
Servidor S3 → Router A				
Router A → Usuario				

- b) Responda razonadamente a las siguientes preguntas. El objetivo de las mismas es guiar al alumno para que describa el procesamiento que el router A debe realizar para implementar el mecanismo de reparto de carga diseñado.

- En el caso de que considere necesario que el router A almacene una tabla con una fila para cada conexión TCP (tabla de reparto de carga), indique los campos de dicha tabla.
- Describa razonadamente el procesamiento que debe realizar el router A para el primer segmento de inicio de conexión por parte del usuario (100.1.1.1,2100 → 200.1.1.1,80). Indique las posibles lecturas/escrituras en la posible tabla de reparto de carga.
- Describa razonadamente el procesamiento que debe realizar el router A para el segundo y siguientes segmentos generados por el usuario externo, posteriores al inicio de la conexión anterior. Indique las posibles lecturas/escrituras en la posible tabla de reparto de carga.

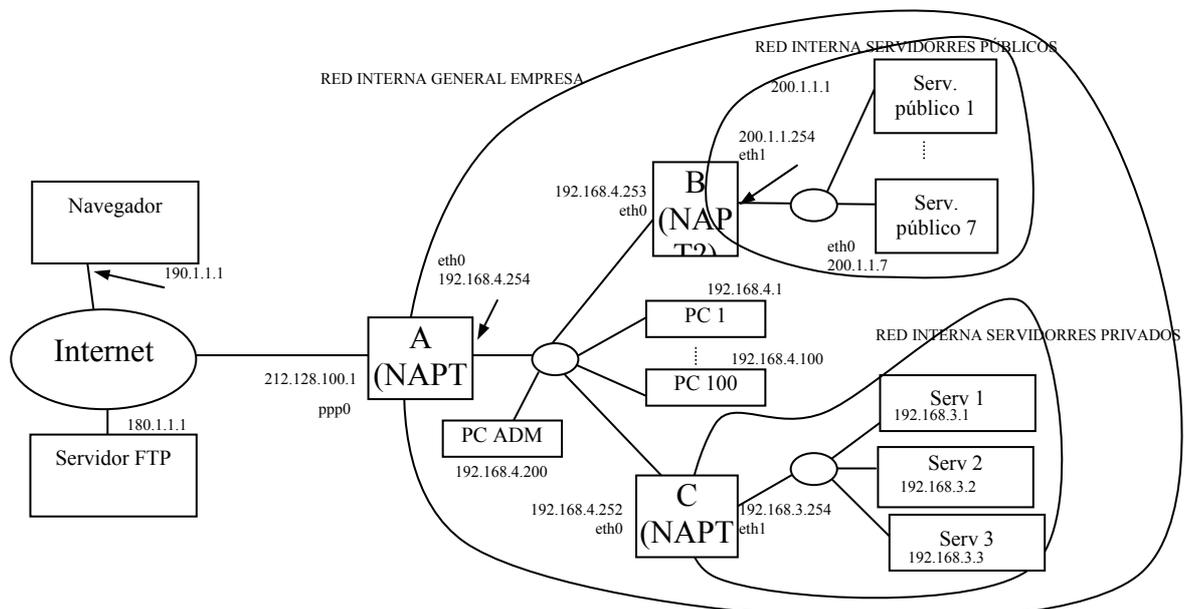
- Describa razonadamente el procesamiento que debe realizar el router A para el tráfico saliente de esa conexión TCP (originado en el servidor 3). Indique las posibles lecturas/escrituras en la posible tabla de reparto de carga.

### Problema 9 (Junio 2006-problema 4)

La figura inferior muestra la red de una empresa dedicada a servicios de consultoría IP:

- La única conexión al exterior de la red es a través del *router A*, que implementa la funcionalidad de *Masquerading* (NAPT), con red interna 192.168.4.0/255.255.255.0, y dirección externa 212.128.100.1.
- El conjunto de PCs 1..100 y el PC ADM se encuentran conectados directamente en la red general interna.
- La red incluye un conjunto de servidores públicos, con dirección IP pública de Internet. Estos servidores deben ser accesibles desde el exterior y desde el interior de la empresa.
- La empresa dispone de 3 servidores en una red interna, **oculta a la red general interna a través del router C**. Las conexiones originadas en estos servidores deben ser enmascaradas. Los siguientes servicios ofrecidos por los servidores, deben ser accesibles (únicamente a la red general interna):
  - Servidor 1: implementa dos servicios en los puertos 22 y 143, que deben ser accesibles desde la red general interna en los puertos 2222 y 143 respectivamente.
  - Servidor 2: implementa dos servicios en los puertos 22 y 80, que deben ser accesibles desde la red general interna en los puertos 2223 y 80 respectivamente.
  - Servidor 3: implementa dos servicios en los puertos 22 y 21, que deben ser accesibles desde la red general interna en los puertos 2224 y 21 respectivamente.

Nota: Si al rellenar una tabla, cree que debe estar vacía, debe indicarlo claramente con la palabra “vacía”.



- a) Indique el contenido de la tabla de configuración de puertos visibles del *router* A.

Tabla de puertos visibles		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

- b) Indique el contenido de la tabla de configuración de puertos visibles del *router* C.

Tabla de puertos visibles		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

- c) Indique razonadamente si el *router* B debe implementar la funcionalidad NAT.

- d) Escriba la tabla de encaminamiento de los dispositivos que se le indica.

Tabla encaminamiento <i>router</i> B			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>router A</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC ADM			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>router C</i>			
Dirección	Máscara	Interfaz de salida	Gateway

El PC ADM abre una conexión SSH para configurar remotamente el servidor 2 (que tiene el servidor SSH en su puerto 22). El puerto origen efímero que emplea el PC ADM es el 3000. Durante esta conexión SSH, la tabla de conexiones enmascaradas del router C tiene los siguientes valores:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.3.1	2000	61001
192.168.3.2	2223	61002

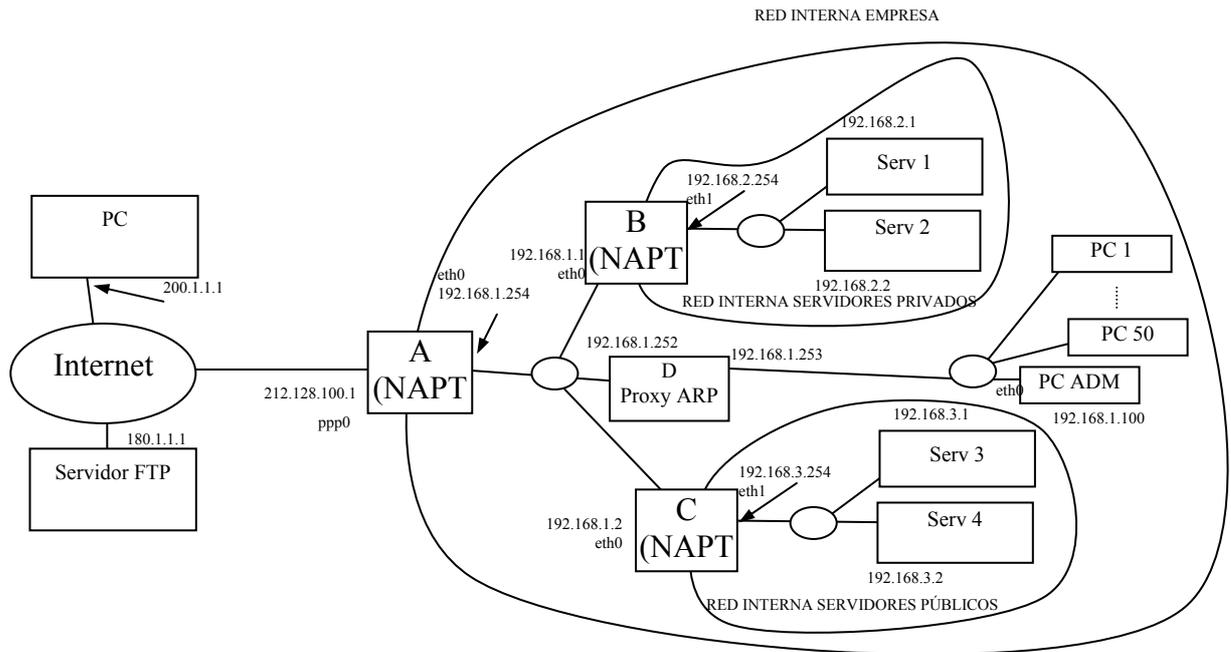
- e) Rellene la siguiente tabla con la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP a la que pertenece la conexión SSH. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
PC ADM→Router C				
Router C→Serv 2				
Serv 2→Router C				
Router C→PC ADM				

### Problema 10 (Septiembre 2006-problema 4)

La figura inferior muestra la red interna de la empresa AAA, basada completamente en tecnología *Ethernet*.

- Los *routers* A, B, C implementan la funcionalidad de *Masquerading*.
- Los servidores 1 y 2 proporcionan servicios en su puerto local 3000 que tienen que ser accesibles al resto de PCs de la red interna (incluidos los servidores 3 y 4) en los puertos 3000 y 3001. Ninguno de estos servicios debe ser accesible desde Internet.
- Los servidores 3 y 4 proporcionan servicios en el puerto 3000 que deben ser accesibles al resto de PCs de la red interna (incluidos los servidores 1 y 2) en los puertos 3000 y 3001 y a los usuarios de Internet en los puertos 3000 y 3001.
- El PC ADM se encarga de tareas de administración de red.
- Todos los servidores (1..4), todos los routers (A, B, C, D), y todos los PCs (1...50, ADM) tienen activado el servicio SSH en sus puertos 22.
- El PC de ADM es capaz de administrar remotamente con SSH todos los servidores, PCs y routers.
- El servicio SSH del PC ADM debe ser accesible desde Internet.



a) Indique el contenido de las siguientes tablas de configuración de puertos visibles. El alumno debe decidir sobre aquellos puertos que no aparezcan indicados en el enunciado, escogiendo números mayores a 1024.

Tabla de puertos visibles Router A		
IP servidor interno	Puerto servidor interno	Puerto público (externo)


Tabla de puertos visibles <i>Router B</i>		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles <i>Router C</i>		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

b) Escriba la tabla de encaminamiento de los dispositivos que se le indica.

Tabla encaminamiento <i>router A</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>router B</i>			
Dirección	Máscara	Interfaz de salida	Gateway


Tabla encaminamiento <i>router C</i>			
Dirección	Máscara	Interfaz de salida	Gateway

- c) El Servidor 3 abre una conexión TCP desde el puerto 15000 con el servicio proporcionado por el Servidor 1. Rellene las siguientes tablas describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP de esa conexión. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta. Si considera que no aparece en el enunciado algún número de puerto que le sea necesario, elíjalo dentro del rango de puertos mayores a 1024.

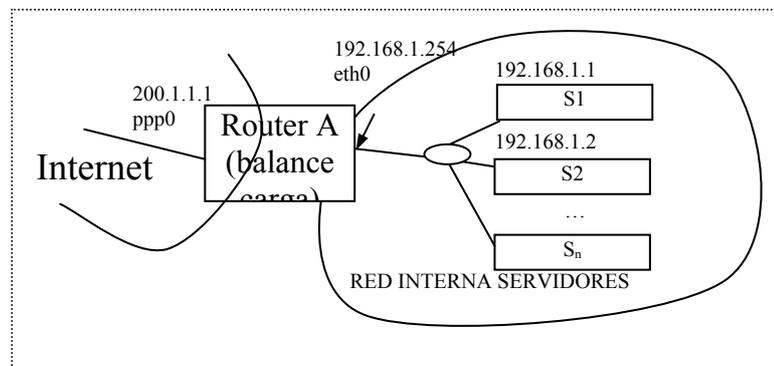
Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Serv 3 → Router C				
Router C → Router B				
Router B → Serv 1				
Serv 1 → Router B				
Router B → Router C				
Router C → Serv 3				

### Problema 11 (Febrero 2007-problema 4)

La figura muestra la sala de servidores de un portal de Internet. Todas las consultas de páginas web a este portal, vienen dirigidas al puerto 80 del router A, cuya dirección IP externa es 200.1.1.1. La empresa emplea un router de balance de carga (*load sharing router*), que reparte las consultas a las páginas web, entre un grupo de servidores ocultos al exterior, tal y como indica la figura 1. Todos los servidores internos S1, S2, S3 emplean el puerto 80 para el servicio web. El mecanismo de balance de carga implantado consiste en:

- El router A se configura como el único dispositivo visible desde el exterior, tomando la dirección del portal en su interfaz externa (200.1.1.1), y atendiendo consultas web en el puerto 80.

- Las conexiones TCP desde clientes externos, destinadas a la dirección 200.1.1.1, puerto 80, deben ser redireccionadas por el router, a uno de los servidores internos adquiridos (S1, S2, ... en la figura).
- La asignación de servidor a cada conexión TCP entrante nueva, se elige repitiendo un orden secuencial (S1, S2, ..., Sn, S1, S2, ...).
- La asignación (conexión TCP ; servidor) debe ser recordada, ya que los futuros segmentos de la conexión TCP deben ser redirigidos al mismo servidor.
- La existencia del router de balance de carga debe ser transparente para cada uno de los servidores, que deben tener la ilusión de estar recibiendo conexiones directamente de los clientes externos. Esto implica un proceso de traducción de direcciones para el tráfico entrante (cliente→router→servidor).
- La existencia del router de balance de carga debe ser transparente para los clientes, que deben tener la ilusión de que existe una única máquina 200.1.1.1 que atiende sus consultas. Esto implica un proceso de traducción de direcciones para el tráfico saliente (servidor→router→cliente).



Un usuario en Internet (dirección 222.2.2.2) abre un navegador y visita la página web de la empresa. Esto implica un establecimiento de conexión TCP con destino 200.1.1.1, puerto 80. El puerto efímero del cliente es el 3200. El router de reparto de carga, asigna el servidor 1 a esta conexión TCP.

- a) Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de esa .conexión TCP. Fijese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Servidor S1 → Router A				
Router A → Usuario				
Uusuario → Router A				
Router A → Servidor S1				

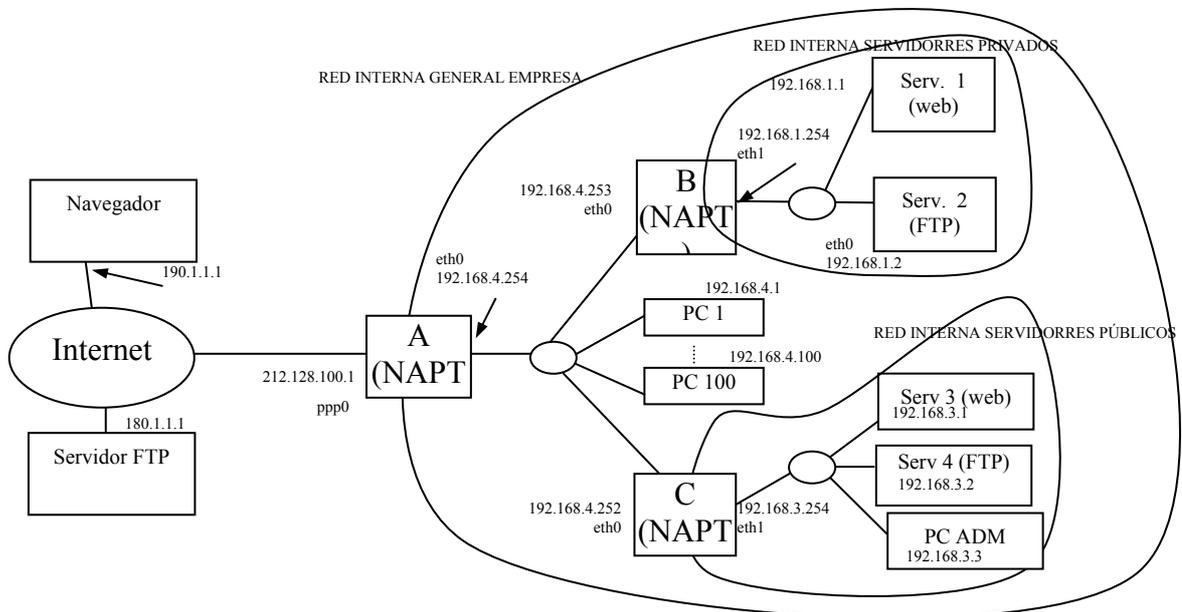
- b) Responda razonadamente a las siguientes preguntas.

- En el caso de que considere necesario que el router A almacene una tabla con una fila para cada conexión TCP (tabla de reparto de carga), indique los campos de dicha tabla.

- Escriba los valores que tendría esta tabla si la única conexión TCP que se establece corresponde a la del apartado anterior.

### Problema 12 (Junio 2007-problema 4)

La figura muestra la red de una empresa dedicada a servicios de consultoría IP:



La única conexión al exterior de la red es a través del *router* A, que implementa la funcionalidad de *Masquerading*. Los routers B y C también implementan la funcionalidad de *Masquerading*.

La red incluye dos conjuntos de servidores. Los dos servidores detrás del router B (servidores 1 y 2), deben ser accesibles únicamente desde la red general interna. Los dos servidores detrás del router C (servidores 3 y 4), deben ser accesibles desde la red general interna y desde Internet.

Los servidores web (1 y 3) están accesibles siempre en el puerto 80, y los servidores FTP (2 y 4) en el puerto 21. Los routers que exporten servicios web y FTP, deberán hacerlo en sus puertos 80 y 21.

Todas las máquinas de la red general interna tienen un servidor SSH en el puerto 22. El PC ADM del administrador debe poder administrar todas las máquinas de la red general interna accediendo a su puerto 22. Para el caso de los servidores ocultos por el router B, debe configurarse la red de manera que el administrador acceda al puerto 2222 y 2223 del router B, para configurar respectivamente los servidores 1 y 2.

Rellene las tablas. Si al rellenar una tabla, cree que debe estar vacía, debe indicarlo claramente con la palabra “vacía”.

Tabla de puertos visibles Router A (0,25 pts.)		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles Router B (0,25 pts.)		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles Router C (0,25 pts.)		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla encaminamiento <i>router A</i> (0,25 ptos)			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>router B</i> (0,25 ptos)			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC ADM (0,25 ptos)			
Dirección	Máscara	Interfaz de salida	Gateway

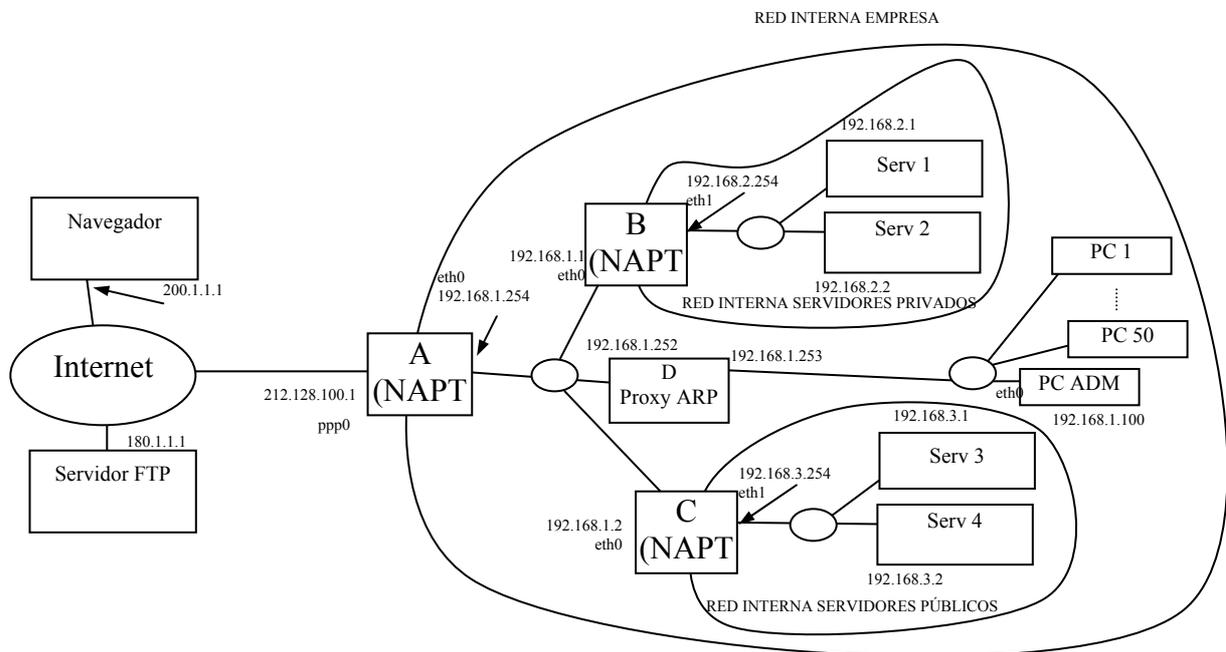
- a) El navegador en la máquina 190.1.1.1 abre una conexión TCP desde su puerto 2100, que le permite ver una página web en el servidor web público de la empresa. Rellene las siguientes tablas describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP. Fijese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Navegador→Router A				
Router A→Router C				
Router C→Serv. 3				
Serv. 3→Router C				
Router C→Router A				
Router A→Navegador				

### Problema 13 (Septiembre 2007-problema 4)

La figura muestra la red interna de una empresa, basada completamente en tecnología *Ethernet*.

- Los routers A, B, C implementan la funcionalidad de *Masquerading*.
- Los servidores 1 y 2 proporcionan servicios que tienen que ser accesibles al resto de PCs de la red interna (incluidos los servidores 3 y 4). Ninguno de estos servicios debe ser accesible desde Internet.
  - El servidor 1 proporciona dos servicios en los puertos 3000 y 3001 que deben ser accesibles en el puerto 3000 y 3001 del router B.
  - El servidor 2 implementa un servicio en el puerto 3000, que debe ser accesible en el puerto 3002 del router B.
- Los servidores 1 y 2 implementan el servicio SSH (*Secure Shell*) en el puerto 22, que debe ser accesible a la red interna (incluidos los servidores 3 y 4) en los puertos 22 y 2222 respectivamente.
- Los servidores 3 y 4 proporcionan servicios que deben ser accesible al resto de PCs de la red interna (incluidos los servidores 1 y 2) y a los usuarios de Internet.
  - El servidor 3 proporciona el servicio Web en el puerto 80, que debe ser accesible en el router C y en el router A también en el puerto 80.
  - El servidor 4 proporciona el servicio FTP en el puerto 21, que debe ser accesible en el router C en el puerto 2121 y en el router A en el puerto 21.
- El router D implementa la funcionalidad de Proxy ARP.



a) Indique el contenido de las siguientes tablas de configuración de puertos visibles.

Tabla de puertos visibles <i>Router A</i>		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles <i>Router B</i>		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles <i>Router C</i>		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

b) Escriba la tabla de encaminamiento de los dispositivos que se le indica.

Tabla encaminamiento <i>router A</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>router B</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>router C</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC ADM			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento Servidor 1			
Dirección	Máscara	Interfaz de salida	Gateway

- c) Desde la máquina PC ADM se ha abierto una conexión TCP con el servidor FTP (puerto 21) en 180.1.1.1. Rellene la siguientes tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de esta conexión TCP. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
PC ADM → Router D				
Router D → Router A				
Router A → Serv FTP				
Serv FTP → Router A				
Router A → Router D				
Router D → PC ADM				

**Nota:** La tabla de conexiones enmascaradas del router A, *después* de que se haya completado el establecimiento de conexión TCP, se muestra a continuación:

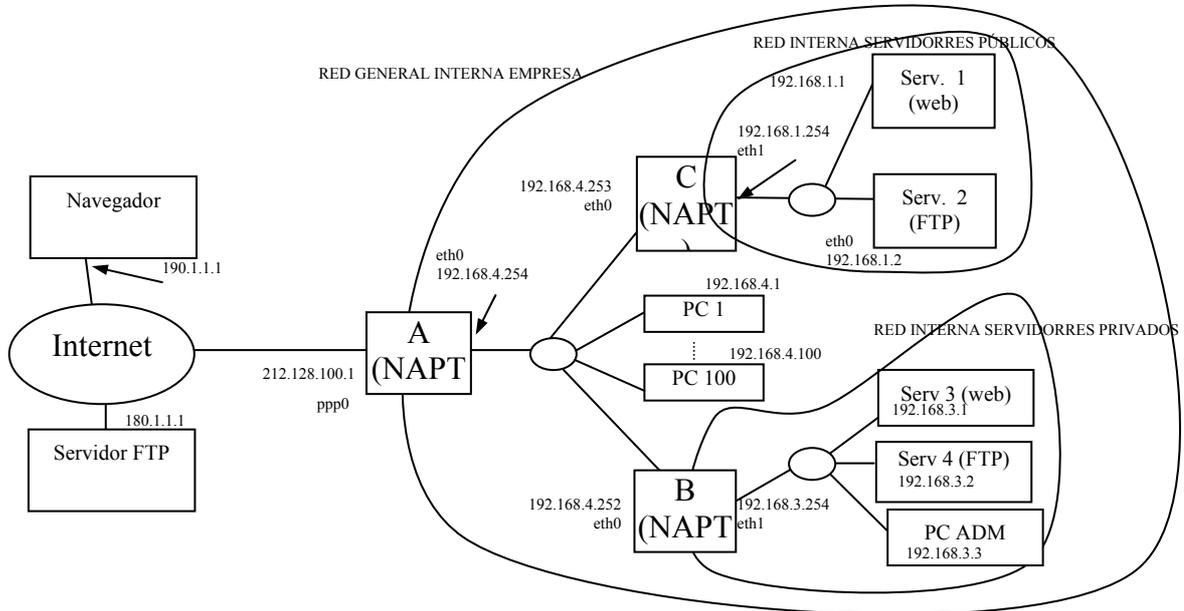
IP interna	Puerto Máquina interna	Puerto Externo
192.168.1.100	3000	61002
192.168.1.1	4500	61000

d) ¿Existe alguna posibilidad de que en un momento dado, la tabla de conexiones enmascaradas del *router* C sea la que muestra la figura?. ¿Por qué?

IP interna	Puerto Máquina interna	Puerto Externo
192.168.1.1	3560	61107
192.168.3.1	3800	61108

#### Problema 14 (Febrero 2008-problema 4)

La figura muestra la red de una empresa dedicada a servicios de consultoría IP:



- La única conexión al exterior de la red es a través del *router* A, que implementa la funcionalidad de *Masquerading*. Los routers B y C también implementan la funcionalidad de *Masquerading*.

- La red incluye dos conjuntos de servidores. Los dos servidores detrás del router B (servidores 3 y 4), deben ser accesibles únicamente desde la red general interna. Los dos servidores detrás del router C (servidores 1 y 2), deben ser accesibles desde la red general interna y desde Internet.
- Los servidores web (1 y 3) están accesibles siempre en el puerto 80, y los servidores FTP (2 y 4) en el puerto 21.
- Los routers (A, B, C) que exporten servicios web y FTP, deberán hacerlo en sus puertos 8080 y 2121.
- Todas las máquinas de la red general interna *salvo el PC ADM* tienen un servidor SSH en el puerto 22. El PC ADM del administrador debe poder administrar todas las máquinas de la red general interna accediendo a su puerto 22. Para el caso de los servidores ocultos por el router C, debe configurarse la red de manera que el administrador acceda al puerto 2222 y 2223 del router C, para configurar respectivamente los servidores 1 y 2.

Rellene las tablas. Si al rellenar una tabla, cree que debe estar vacía, debe indicarlo claramente con la palabra “vacía”.

Tabla de puertos visibles Router A		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles Router B		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles Router C		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla encaminamiento <i>router A</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento <i>router B</i>			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento PC ADM			
Dirección	Máscara	Interfaz de salida	Gateway

El navegador en la máquina 190.1.1.1 abre una conexión TCP desde su puerto 2100, que le permite ver una página web en el servidor web público de la empresa. Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Navegador → Router A				
Router A → Router C				
Router C → Serv. 1				
Serv. 1 → Router C				
Router C → Router A				
Router A → Navegador				

### Problema 15 (Junio 2008-problema 4)

La figura muestra la red de una empresa dedicada a servicios de consultoría IP:

- Los routers A y B implementan la funcionalidad NAPT (*masquerading*).
- Los servidores Web A y B están ejecutándose en el puerto 80, y se hacen públicos en el puerto 80 de sus respectivos routers NAPT. El servidor FTP está ejecutándose en el puerto 21, y se hace público en el puerto 21 del router B.
- Los tres servidores tienen un servicio SSH escuchando en el puerto 22. El servidor Web A publica el servicio SSH del servidor web en el puerto 2222 del router A. Los servicios SSH de los servidores Web B y FTP B no deben ser públicos fuera de la red interna B.

Rellene las. Si al rellenar una tabla, cree que debe estar vacía, debe indicarlo claramente con la palabra “vacía”.

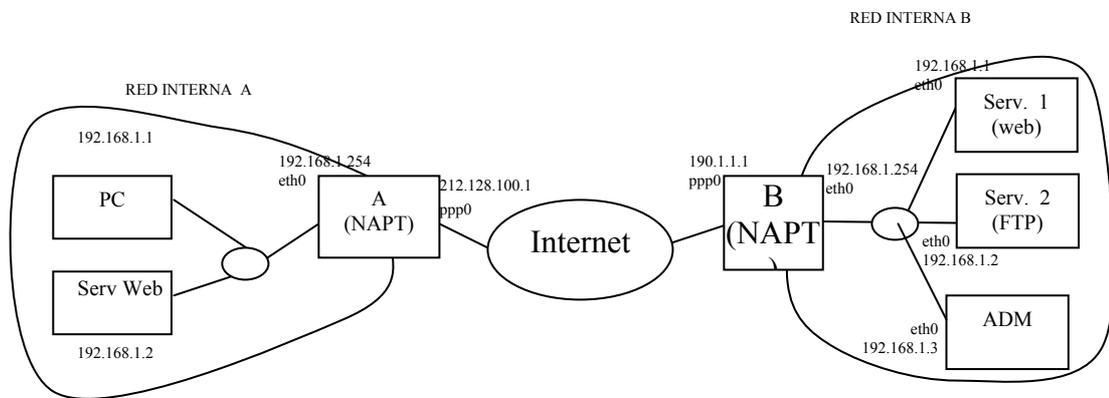


Tabla de puertos visibles Router A		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles Router B		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla encaminamiento Router B			
Dirección	Máscara	Interfaz de salida	Gateway

En un determinado momento, la tabla de conexiones enmascaradas del router A es:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.1.1	3000	61000
192.168.1.2	2100	61001
192.168.1.2	2222	61003

Y la del router B es:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.1.1	3000	61000
192.168.1.2	2100	61001
192.168.1.3	2200	61003

En este momento, un usuario en el PC de la red interna A está viendo una página web en el servidor web público de la red interna B. Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
Navegador→Router A				
Router A→Router B				
Router B→Serv. Web B				
Serv. Web B→Router B				
Router B→Router A				
Router A→Navegador				

En este momento, un usuario en el PC ADM de la red interna B está configurando por SSH el servidor Web A. Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
ADM→Router B				
Router B→Router A				
Router A→Serv. Web A				
Serv. Web A→Router A				
Router A→Router B				
Router B→ADM				

### Problema 16 (Septiembre 2008-problema 4)

La figura muestra la red de una empresa con dos sedes: Los routers A, B y C implementan la funcionalidad NAPT (*masquerading*). Los servidores S1, S2, S3, S4 tienen un servidor web que escucha peticiones en el puerto 80.

- El servidor S1 es accesible desde Internet a través del puerto 80 del router A.
- El servidor S2 es accesible desde Internet a través del puerto 8080 del router A.
- El servidor S3 es accesible desde Internet a través del puerto 80 del router B.
- El servidor S4 es accesible desde la red interna B a través del puerto 80 del router C. No es accesible desde Internet.

Las máquinas A, B, C, S1, S2, S3, S4 tienen un servidor SSH en su puerto 22 para poder ser administradas remotamente desde ADM. Los servicios SSH de S1 y S2 son accesibles desde Internet en los puertos 2222 y 2223 respectivamente. Rellene las siguientes tablas Si al rellenar una tabla, cree que debe estar vacía, debe indicarlo claramente con la palabra “vacía”.

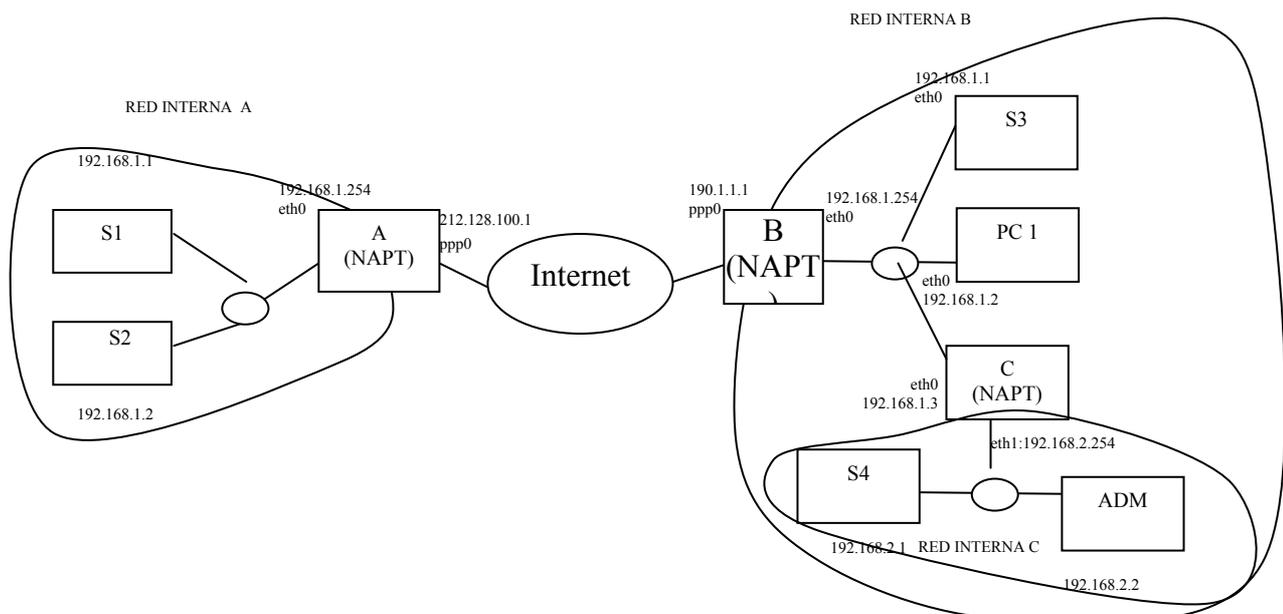


Tabla de puertos visibles Router A		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles Router B		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla de puertos visibles Router C		
IP servidor interno	Puerto servidor interno	Puerto público (externo)

Tabla encaminamiento Router B			
Dirección	Máscara	Interfaz de salida	Gateway

Tabla encaminamiento Router C			
Dirección	Máscara	Interfaz de salida	Gateway

En un determinado momento, la tabla de conexiones enmascaradas del router B es:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.1.2	2100	61001
192.168.1.3	61001	61002
192.168.1.3	61002	61003
192.168.1.1	3500	61004

Y la del router C es:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.2.2	2000	61001
192.168.2.2	2001	61002

En este momento, un usuario en el PC1 está viendo una página web servida por S1. Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
PC1→Router B				
Router B→Router A				
Router A→S1				
S1→Router A				
Router A→Router B				
Router B→PC1				

En este momento, un usuario en la máquina ADM está configurando por SSH la máquina S2, con una conexión TCP iniciada en el puerto 2000. Rellene la siguiente tabla describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
ADM→Router C				
Router C→Router B				
Router B→Router A				
Router A→S2				
S2→Router A				
Router A→Router B				
Router B→Router C				
Router C→ADM				