Universidad de Granada
Departamento de Teoría de la Señal,
Telemática y Comunicaciones

ETSIIT
C/ Periodista Daniel Saucedo Aranda, s/n
18071 - Granada
Tf: 958 240840 - Fax: 958 240831

TRANSMISIÓN DE DATOS Y REDES DE COMPUTADORES II

– 4º curso de Ingeniería Informática –

Examen de teoría[1] – Junio 2007

Apellidos y nombre: JORGE NAVARRO ORTIZ **Grupo:** PROFESOR GRUPO C

1 *(2 puntos: 2×1)* Suponga que administra una intranet en un hotel de 4 plantas. Por cada planta dispone de un router inalámbrico –red de infraestructura- con un servidor de DHCP. Cada planta tiene 33 habitaciones. Se disponen de 2 routers adicionales, uno de ellos conectado a los routers inalámbricos de las plantas 1 y 2, y el otro conectado a los routers de las plantas 3 y 4. Finalmente considere que dispone de un router de acceso a Internet. Suponga que se ha contratado un rango de direcciones públicas 199.199.199.128/25

a) Proponga un esquema de asignación de direcciones tal que el router de acceso tenga una tabla de encaminamiento con sólo 3 entradas.
b) Si se exige que los hosts tengan una IP pública ¿cómo lo haría?

2 *(2 puntos: 2×1)* Suponga una transacción comercial en Internet con cuatro entidades involucradas, identificadas como *C* (cliente), *P* (proveedor), *Bc* (entidad bancaria del cliente) y *Bp* (entidad bancaria del proveedor). Entre ellas se intercambian los siguientes mensajes:

C→P: $Kpb_P(producto, importe, datos\_C)$
P→Bp: $Kpb_{Bp}(importe, datos\_C, P)$
Bp→P: $Kpb_P(datos\_P, R)$
P→Bp: $Kpb_{Bp}(datos\_P, K_{P\text{-}Bp}(R))$
Bp→Bc: $Kpb_{Bc}(importe, datos\_C, P)$
Bc→C: $Kpb_C(importe, datos\_C, P, R')$
C→Bc: $Kpb_{Bc}(importe, datos\_C, P, K_{C\text{-}Bc}(R'))$
Bc→Bp: $Kpb_{Bp}(importe, datos\_C, P)$
Bp→P: $Kpb_P(importe, datos\_C)$
P→C: *...entrega del producto...*

siendo
- Kpb_X: cifrado con clave pública de *X*,
- $K_{X\text{-}Y}$: cifrado con clave secreta compartida entre *X* e *Y*,
- *producto*: identificación del producto o servicio provisto,
- *importe*: valor económico del producto,
- *R*: reto, y
- *datos_X*: información bancaria correspondiente a *X-Bx*.

Aceptadas la disponibilidad y validez de las claves públicas involucradas en base a la existencia de una entidad superior confiable, responda justificadamente a las dos siguientes cuestiones:

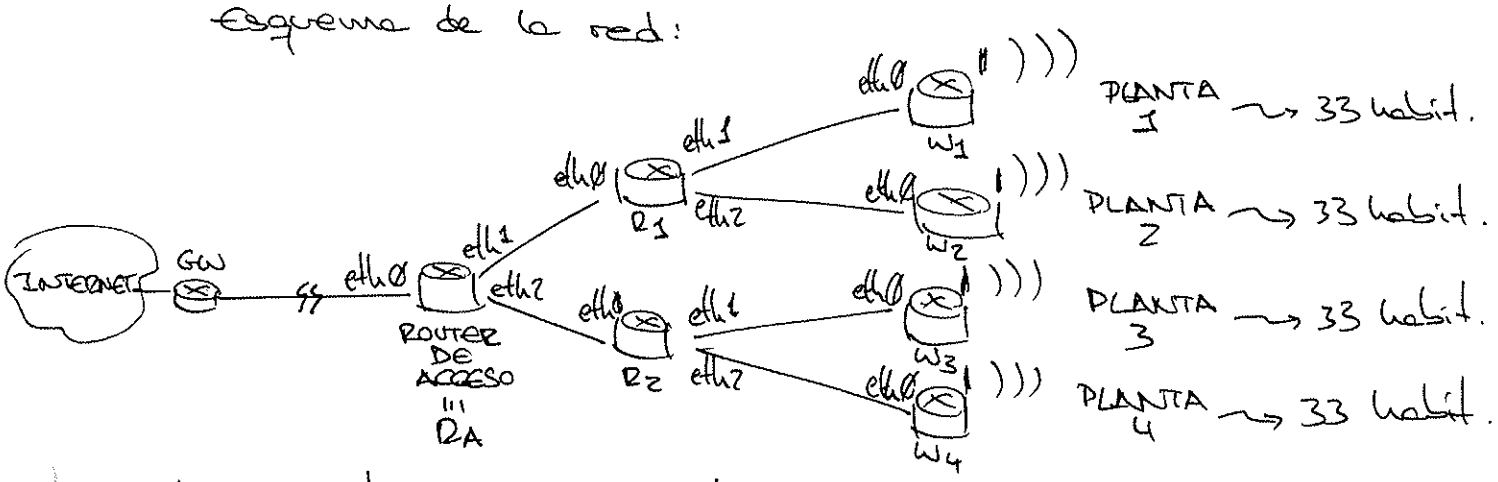
a) ¿Qué servicios de seguridad se proporcionan en la transacción mencionada?
b) ¿Qué debilidades y vulnerabilidades frente a posibles ataques presenta el esquema propuesto y, en su caso, cómo podrían evitarse?

[1] → La calificación de esta parte de la asignatura supondrá 7 puntos sobre el total de 10.

Ejercicio 1

a) Como no exigen nada, se pueden utilizar direcciones privadas para evitar problemas por falta de recursos (direcciones IP).

Esquema de la red:



Piden 3 entradas en la tabla de encaminamiento de R_A ↝ ↝ en realidad se refiere a rutas (finales) indirectas, ya que las rutas directas (a R_1 y R_2) también han de estar.

3 rutas indirectas → INTERNET
→ REDES CONECTADAS A R_1 ↝ las de W_1 y W_2
→ u R_2 ↝ las de W_3 y W_4

⇓

Los equipos conectados a W_1 y W_2 han de estar en la misma subred vista por R_A. Por ejemplo:

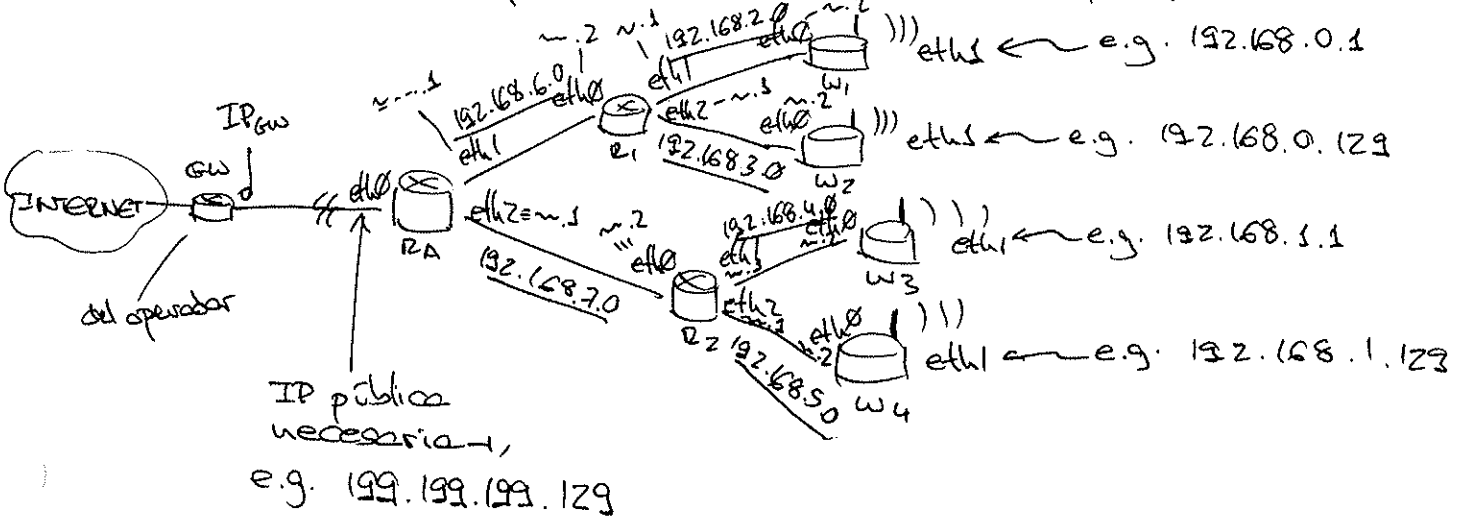
192.168.0.0/24 → 192.168.0.0/25 para equipos en W_1
→ 192.168.0.128/25 para equipos en W_2

Idem para W_3 y W_4:

192.168.1.0/24 → 192.168.1.0/25 para equipos en W_3
→ 192.168.1.128/25 para equipos en W_4

Así, R_A distinguiría entre las redes 192.168.0.0/24 y 192.168.1.0/24, y serían R_1 y R_2 los que distinguirían entre las subredes de W_1, W_2, W_3 y W_4 (con máscaras /25).

Las direcciones entre routers no son importantes, salvo que hay subredes entre routers directos conectadas. Se pueden usar direcciones privadas también. Por ejemplo:



La tabla de encaminamiento del router de acceso quedaría:

	destino	máscara	sig. salto	interfaz
3 RUTAS INDIRECTAS	192.168.0.0	255.255.255.0	192.168.6.2 (R_1)	eth1
	192.168.1.0	255.255.255.0	192.168.7.2 (R_2)	eth2
	default	——	IP_{GW}	eth0
RUTAS DIRECTAS	192.168.6.0	255.255.255.0	*	eth1 → a R_1
	192.168.7.0	255.255.255.0	*	eth2 → a R_2

b) Para usar direcciones públicas hay 2 opciones.

1) Utilizar direcciones públicas en los hosts. Como no hay suficientes ($33 \times 4 > 128 - (\text{direcciones de subred} + \text{difusión})$) se utilizaría DHCP para asignarlas y se supondría que no se conectan todos simultáneamente.

Esas direcciones hay que dividirlas entre los 4 routers wireless.

4 routers ⇒ 4 subredes ⇒ 2 bits para diferenciarlas.

Había 7 bits para hosts (32 bits - 25 bits de máscara)

⇒ 2 para subredes { 00 ≡ w_1, 01 ≡ w_2, 10 ≡ w_3, 11 ≡ w_4 }, 5 para hosts → $2^5 \equiv 32$

Equipos por subred → 32 − 2 (dir. subred 00000, dir. difusión 11111)

Además hay que quitar una dirección para ese interfaz (inalámbrico) del router wireless de esa red ⇒

⇒ 32 − 2 − 1 = 29 equipos por router wireless con IP públicas.

Así, las direcciones serán:

subred w_1 { w_1: 199.199.199.129 ; resto: 199.199.199.130 — 158 } subred 199.199.199.128/27

subred w_2 { w_2: 199.199.199.161 ; resto: 199.199.199.162 — 190 } subred 199.199.199.160/27

subred w_3 { w_3: 199.199.199.193 ; resto: 199.199.199.194 — 222 } subred 199.199.199.192/27

subred w_4 { w_4: 199.199.199.225 ; resto: 199.199.199.226 - 254 } subred 199.199.199.224/27

2) Utilizar NAT en el router de acceso, con todas las IP públicas disponibles.

En ambos casos, ~~el dir~~ la asignación de direcciones entre routers ~~no~~ podría seguir siendo igual (dir. privadas).

2...

a) Los servicios de seguridad provistos en la transacción descrita son básicamente dos:

- *Confidencialidad*, habida cuenta del cifrado de todos los mensajes intercambiados con la clave pública del receptor. Ello garantiza que sólo éste disponga de la clave necesaria para descifrar el mensaje: la propia privada.
- *Autenticación* $C \rightarrow Bc$ *y* $P \rightarrow Bp$, gracias al respectivo cifrado de un "reto" (con clave secreta compartida) por parte de C y P.

  Es de señalar, sin embargo, que la autenticación es sólo de C y P frente a Bc y Bp; o sea, Bc y Bp sabrían que C y P son quienes dicen ser. En cambio, Bc y Bp podrían no ser auténticos. Por supuesto, tampoco Bc y Bp están autenticados entre sí; ni C y P.

b) Más allá de una *autenticación* total entre las entidades, también pueden proveerse mecanismos para *integridad* y *no repudio*. Ambos aspectos pueden conseguirse mediante el uso de funciones *hash* y cifrado asimétrico con la clave privada del emisor.

Adicionalmente, es de significar una debilidad y/o vulnerabilidad importante. Los mensajes, independientemente de que puedan estar o no cifrados con claves públicas y/o privadas y/o secretas compartidas, son susceptibles de ser capturados y replicados por potenciales atacantes. Con objeto de dificultar este hecho, se recomienda utilizar identificativos unívocos o *nonces* para todos y cada uno de los mensajes intercambiados. Este aspecto, conjuntamente con todos los anteriores mencionados, cabrían ser provistos a través del empleo de una entidad intermediaria de tipo *Big Brother* por la que "fluyese" toda la información.

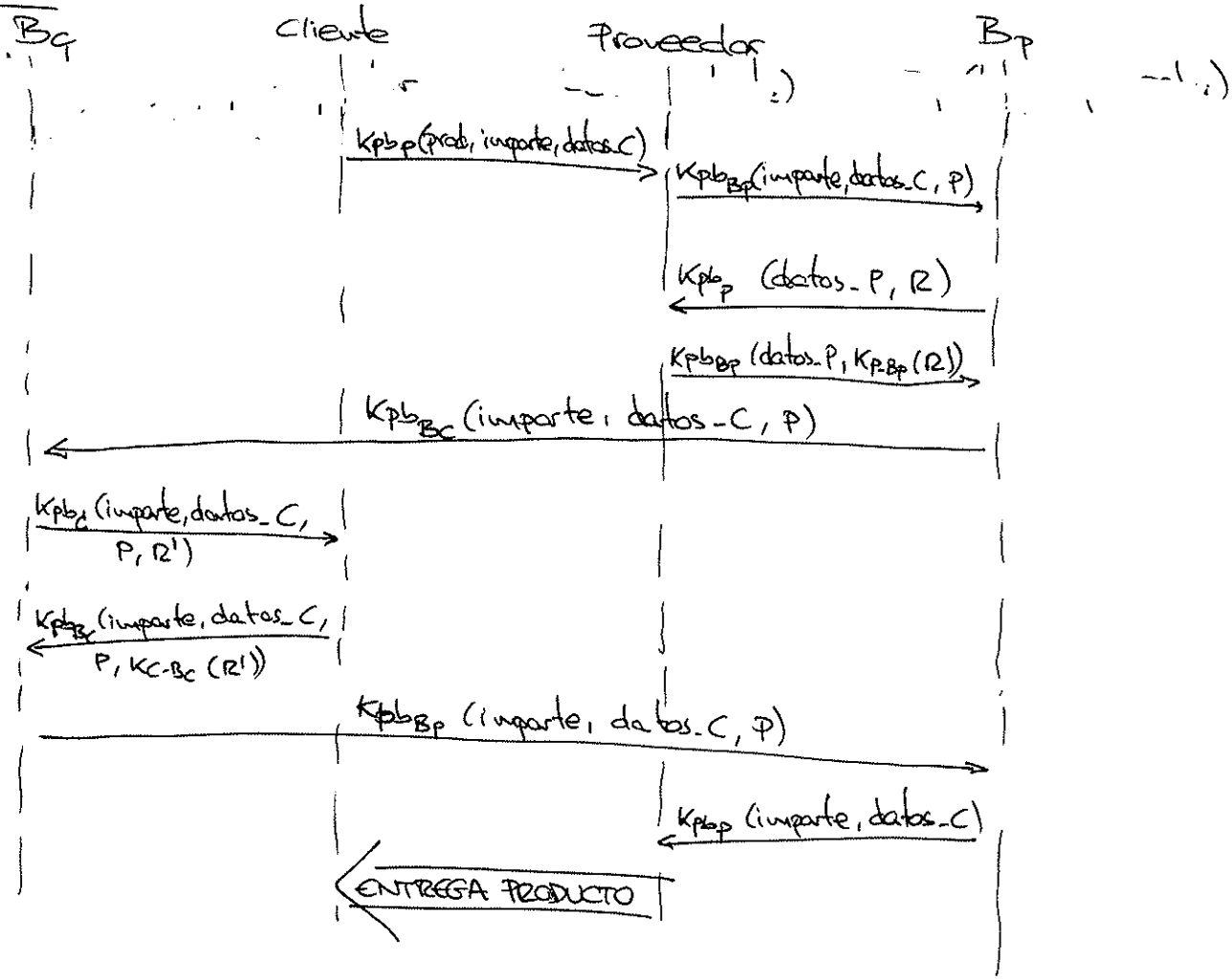
TDRC 2 — EXAMEN JUNIO 2007

2 Transacción comercial en Internet.

C = cliente B_C = banco del cliente
P = proveedor B_P = banco del proveedor
AGENTES INVOLUCRADOS

Mensajes:
- Kpb_X ≡ cifrado con clave pública de X
- K_{X-Y} ≡ cifrado con clave secreta compartida de X e Y.
- producto ≡ identificación del producto o servicio
- importe ≡ valor económico del producto
- R ≡ reto
- datos_X ≡ información bancaria de X – B_X

Protocolo:



Se acepta la validez y disponibilidad de las claves públicas utilizadas.

a) ¿Qué servicios de seguridad se proporcionan?

* Confidencialidad: ya que todos los mensajes están cifrados con clave pública, sólo el dueño de la clave privada puede obtener su contenido.

* Integridad: no, ya que no se usa firma digital (ni usando compendios ni con doble cifrado).

* Autenticación: sólo del cliente/proveedor con sus bancos respectivos, mediante el envío cifrado del reto. Sin embargo, los bancos no se autentican entre ellos ni con sus clientes.

* No repudio: no, ya que el cliente no tiene ninguna prueba de que el proveedor haya aceptado la transacción que implica un cierto producto y su importe. Ni siquiera de que ha realizado el pago, ~~ya que cualquiera podría suplantar al banco~~ ya que su banco no le envía la confirmación de la operación con algún campo que sólo hubiese podido realizar él.

* Disponibilidad: no, ya que la red podría dejar de funcionar en cualquier momento, por ataques en otras capas inferiores o por fallos de la red.

b) Vulnerabilidades y soluciones.

Integridad
Autenticación
No repudio
} Uso de firmas digitales ← BB, doble cifrado, compendios

↳ Uso de Big Brother

Ataques por repetición → uso de "nonces"

Retos → ataques por repetición (si bien van cifrados)

↳ Sd: ~~[illegible]~~ nonces

ataques por reflexión

Alguien podría suplantar a otro, si bien los datos se envían cifrados y no se deberían conocer. E.g. alguien suplanta a un banco. Si los datos se conociesen, no hay ningún mecanismo de autenticación.

Autenticación total

3 Los *routers* de la figura adjunta tienen definidas las rutas a las redes que tienen conectadas directamente. El administrador de la red decide utilizar en dichos *routers* el protocolo RIP (en los interfaces hacia otros *routers*) y activa dicho servicio siguiendo la secuencia temporal indicada a la derecha de la figura (en segundos).

a) Explique el funcionamiento del protocolo de encaminamiento dinámico RIP, describiendo los mensajes intercambiados entre los *routers* (indique origen/destino del mensaje, redes conocidas por el receptor tras recibir el mensaje, coste para alcanzar cada red y cuál es el primer *router* en la ruta hacia dicha red) hasta que las rutas se mantienen estables.
Suponga que sólo se utilizan actualizaciones periódicas, y que el primer mensaje periódico enviado por cada *router* se envía a los 30 segundos de haber arrancado el servicio RIP. Incluya en la descripción sólo la accesibilidad a las redes A, B, C, D, E y F.

Notación aconsejada: X → Y: J(c_J / X), K(c_K / X), L(c_L / Z), ...

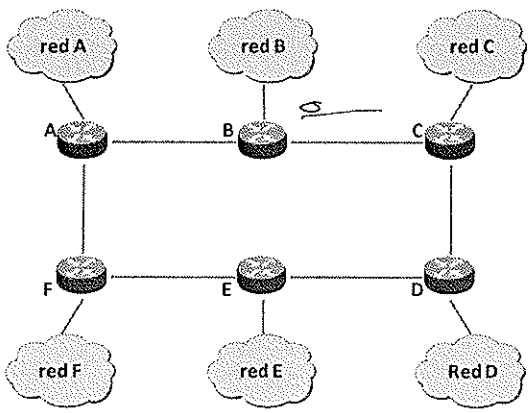
Significado: el *router* X le manda un mensaje al *router* Y, y tras procesarlo, el *router* Y conoce cómo acceder a la red J con un coste c_J a través del *router* X, a la red K con un coste c_K a través del *router* X, a la red L con un coste c_L a través del *router* Z, ...

Ejemplo (ficticio): B → C: A(2 / B), B(1 / B), C(0 / C)

Significado: el *router* B envía un mensaje al *router* C, y tras procesarlo, el *router* C sabe cómo acceder a la red A con un coste 2 a través del *router* B, a la red B con un coste 1 a través del *router* B, y a la red C con un coste 0 a través del *router* C (o sea, directamente).

Se aconseja hacer un resumen de las redes accesibles desde cada *router* (indicando para cada red su coste asociado y el primer *router* en la ruta hacia dicha red, siguiendo la notación comentada) tras cada período.

b) Calcule el tiempo que pasa hasta que la situación de toda la red se ha estabilizado (desde el instante t_0).



- $t = t_0$ → activación RIP en *router* A
- $t = t_0+5$ → activación RIP en *router* B
- ~~$t = t_0+10$ → activación RIP en *router* C~~
- $t = t_0+15$ → activación RIP en *router* D
- $t = t_0+20$ → activación RIP en *router* E
- $t = t_0+25$ → activación RIP en *router* F

Solución:

a) RIP es un protocolo para el intercambio de información sobre enrutado, que funciona sobre UDP (puerto 520). Una entidad que utilice RIP envía mensajes periódicos (cada 30 segundos) a sus vecinos, para informarles sobre las rutas que tiene disponibles (red destino, máscara, coste=distancia a dicha red) y así los vecinos podrán actualizar sus tablas de encaminamiento. Si no llega ningún mensaje periódico desde un enlace en 180 segundos, se supondrá que dicho enlace ha dejado de funcionar.
El intercambio de mensajes se puede utilizando la dirección 224.0.0.9 (dirección multicast para nodos RIP), o bien utilizando las direcciones de los vecinos (e.g. en redes que no soporten multicast).
En este ejercicio se supone que sólo se envían mensajes periódicos, por lo que no habrá mensajes de petición/respuesta (e.g. cuando se inicia el servicio RIP, dependiendo de la implementación).
Considerando que el primer mensaje periódico se envía 30 segundos después de iniciar RIP en cada *router*, esto significa que todos los *routers* tendrán RIP activo cuando se reciba el primer mensaje periódico (véase la secuencia de activación de RIP en los diferentes *routers*). Así, los mensajes intercambiados serán (se incluye entre paréntesis el coste de alcanzar a la red destino y a través de qué *router*):

- A manda su mensaje periódico informando a B y F. **B** ahora sabe acceder a las redes A (1,A) y B(0,B). **F** sabe acceder ahora a las redes A(1,A) y F(0,F).
- B informa a A y C. **A** conoce ahora a las redes A(0,A), B(1,B). **C** conoce ahora a las redes A(2,B), B(1,B) y C(0,C).
- C informa a B y D. **B** conoce ahora a las redes A(1,A), B(0,B), C(1,C). **D** conoce ahora a las redes A(3,C), B(2,C), C(1,C) y D(0,D).
- D informa a C y E. **C** conoce ahora a las redes A(2,B), B(1,B), C(0,C), D(1,D). **E** conoce ahora a las redes A(4,D), B(3,D), C(2,D), D(1,D), E(0,E).
- E informa a D y F. **D** conoce ahora a las redes A(3,C), B(2,C), C(1,C), D(0,D), E(1,E). **F** conoce ahora a las redes A(1,A), B(4,E), C(3,E), D(2,E), E(1,E), F(0,F).
- F informa a A y E. **A** conoce ahora a las redes A(0,A), B(1,B), C(4, F), D(3, F), E(2, F), F(1, F). **E** conoce ahora a las redes A(2, F), B(3, D), C(2, D), D(1, D), E(0, E), F(1, F).

Resumiendo las redes conocidas tras la primera iteración de mensajes periódicos (entre paréntesis se indica el coste para llegar a dichas redes):

- **A** conoce a las redes A(0,A), B(1,B), C(4,F), D(3,F), E(2,F), F(1,F)
- **B** conoce a las redes A(1,A), B(0,B), C(1,C)
- **C** conoce a las redes A(2,B), B(1,B), C(0,C), D(1,D)
- **D** conoce a las redes A(3,C), B(2,C), C(1,C), D(0,D), E(1,E)
- **E** conoce ahora a las redes A(2,F), B(3,D), C(2,D), D(1,D), E(0,E), F(1,F)
- **F** conoce ahora a las redes A(1,A), B(4,E), C(3,E), D(2,E), E(1,E), F(0,F)

Tras la siguiente iteración, la situación quedaría:

- [redacted] conoce a las redes A(0,A), B(1,B), C(2,B), D(3,F), E(2,F), F(1,F)
- [redacted] conoce a las redes A(1,A), B(0,B), C(1,C), D(2,C), E(3,A), F(2,A)
- [redacted] conoce a las redes A(2,B), B(1,B), C(0,C), D(1,D), E(2,D), F(3,B)
- [redacted] conoce a las redes A(3,C), B(2,C), C(1,C), D(0,D), E(1,E), F(2,E)
- [redacted] conoce ahora a las redes A(2,F), B(3,D), C(2,D), D(1,D), E(0,E), F(1,F)
- [redacted] conoce ahora a las redes A(1,A), B(2,A), C(3,E), D(2,E), E(1,E), F(0,F)

Como las distancias obtenidas ya son las mínimas, las siguientes iteraciones no incluirían cambios en las tablas de encaminamiento. En realidad, los últimos mensajes de F hacia E y A no actualizarían nada (se ve mirando los mensajes concretos, como se hizo en la 1ª iteración).

(revisar, puede haber errores en alguna actualización)

b) Tiempo hasta que se estabilizan las rutas:
30 segundos (inicio de RIP, sin intercambio de mensajes) + 30 segundos (1ª iteración) + 30 segundos (2ª iteración) = 90 segundos

(en realidad serían 80 ya que E es el último que manda algún mensaje que actualizaría alguna tabla, i.e. t=20 de la 2ª iteración)