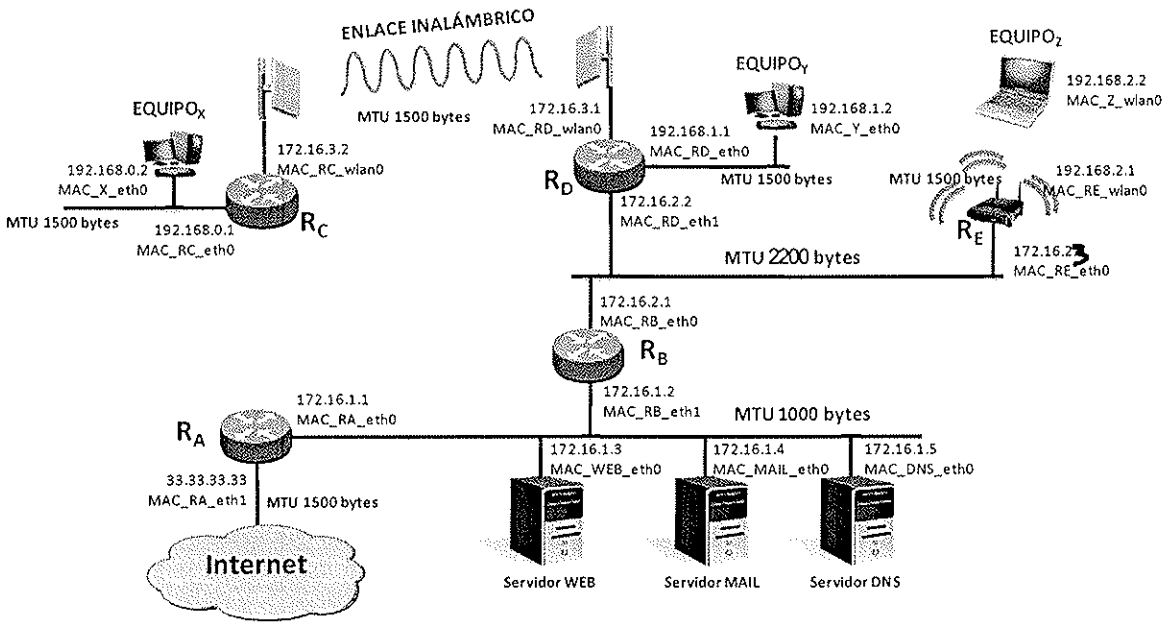
TRANSMISIÓN DE DATOS Y REDES DE COMPUTADORES II

– 4º curso de Ingeniería Informática –

Examen de teoría[1] – 5 de Diciembre de 2008

Apellidos y nombre: JORGE NAVARRO ORTIZ

1. (*2,5 puntos*) Una red tiene la topología y configuración (direcciones físicas e IP, MTU de cada red) mostrada en la figura.



Las tablas de encaminamiento de los componentes de esta red son las siguientes:

TABLA DE ENRUTAMIENTO DEL EQUIPO X

Red destino	Máscara	Sig. salto	Interfaz
172.16.3.2	/24	*	eth0
default	0.0.0.0	192.168.0.1	eth0

TABLA DE ENRUTAMIENTO DEL EQUIPO Y

Red destino	Máscara	Sig. salto	Interfaz
192.168.1.0	/24	*	eth0
default	0.0.0.0	192.168.1.1	eth0

TABLA DE ENRUTAMIENTO DEL EQUIPO Z

Red destino	Máscara	Sig. salto	Interfaz
192.168.2.0	/24	*	~~eth0~~ wlan0
default	0.0.0.0	192.168.2.1	~~eth0~~ wlan0

TABLA DE ENRUTAMIENTO DEL ROUTER R_A

Red destino	Máscara	Sig. salto	Interfaz
172.16.1.0	/24	*	eth0
192.168.0.0	/22	172.16.1.2	eth0
default	0.0.0.0	IP_GW_operador	eth1

TABLA DE ENRUTAMIENTO DEL ROUTER R_B

Red destino	Máscara	Sig. salto	Interfaz
172.16.1.0	/24	*	eth1
172.16.2.0	/24	*	eth0
192.168.0.0	/23	172.16.2.2	eth0
default	0.0.0.0	172.16.2.1	eth1

TABLA DE ENRUTAMIENTO DEL ROUTER R_C

Red destino	Máscara	Sig. salto	Interfaz
192.168.0.0	/24	*	eth0
default	0.0.0.0	172.16.3.1	wlan0

TABLA DE ENRUTAMIENTO DEL ROUTER R_D

Red destino	Máscara	Sig. salto	Interfaz
192.168.1.0	/24	*	eth0
default	0.0.0.0	172.16.2.1	eth1

TABLA DE ENRUTAMIENTO DEL ROUTER R_E

Red destino	Máscara	Sig. salto	Interfaz
192.168.2.0	/24	*	wlan0
default	0.0.0.0	172.16.2.1	eth0

TABLA DE ENRUTAMIENTO DE LOS SERVIDORES WEB, MAIL Y DNS

Red destino	Máscara	Sig. salto	Interfaz
192.168.0.0	/22	172.16.1.2	wlan0
default	0.0.0.0	172.16.1.1	wlan0

a) Muestre el intercambio de tramas entre el *equipo Z* y el servidor *MAIL*. Suponga que las tablas ARP están actualizadas, que el *equipo Z* sólo conoce el nombre de dominio del servidor ~~*WEB*~~ MAIL, y

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

que tanto la solicitud como la respuesta ocupan 1460 bytes. Para cada trama generada detalle la siguiente información:

- Direcciones hardware origen y destino.
- Direcciones IP origen y destino.
- En su caso, los puertos origen y destino.
- En su caso, los *flags* activos y campos de secuencia y ACK.
- El tipo de mensaje del que se trata.

b) ¿Sería posible realizar un *ping* entre el *equipo X* y el *equipo Y*? ¿Y la conexión del *equipo Y* a Internet? Justifique las respuestas.

c) ¿Qué problemas ha detectado en las tablas de encaminamiento? ¿Cómo los solucionaría?

2. (*1 punto*) ¿Cuántos sockets como mínimo se necesitan abrir en un servidor HTTP? Justifique la respuesta.

3. (*1 punto*) Suponga una conexión TCP entre dos entidades ¿Qué ocurre en las dos entidades al detectarse una pérdida?

4. (*2,5 puntos*) Suponga un posible escenario para la entrega telemática de la Declaración del Impuesto de la Renta de Personas Físicas (I.R.P.F.) que contempla su pago inmediato a través de Internet. Los agentes implicados serán la persona que presenta la declaración (P), la Agencia Estatal de Administración Tributaria (AT) y el banco donde la persona tiene una cuenta (BP).

En este escenario hipotético se intercambian los mensajes indicados debajo, donde ***certificado_digital***$_X$ se refiere al certificado digital de X, ***Kpriv***$_X$**()** al cifrado mediante la clave privada de *X*, ***Kpúb***$_X$**()** al cifrado mediante la clave pública de *X*, ***datos_fiscales***$_X$ a los datos de la declaración de I.R.P.F. de *X*, ***importe*** a la cantidad a pagar como resultado de la declaración de I.R.P.F. de *X*, ***código_para_pagar_IRPF*** es un código indicado por la AEAT para que la persona realice el pago en su banco y ***código_IRPF_pagado*** es un código indicado por el banco a la persona como comprobante de su pago.

P → AT: *certificado_digital*$_P$
AT → P: *certificado_digital*$_{AT}$
P → AT: *Kpriv*$_P$ (*Kpúb*$_{AT}$ (*datos_fiscales*$_P$, *importe*))
AT → P: *Kpriv*$_{AT}$ (*Kpúb*$_P$ (*código_para_pagar_IRPF*))
P → BP: *certificado_digital*$_P$
BP → P: *certificado_digital*$_{BP}$
P → BP: *Kpriv*$_P$ (*Kpúb*$_{BP}$ (*importe*, *código_para_pagar_IRPF*))
BP → P: *Kpriv*$_{BP}$ (Kpúb$_P$ (*código_IRPF_pagado*))
P → AT: *Kpriv*$_P$ (*Kpúb*$_{AT}$ (*certificado_digital*$_{BP}$, *código_IRPF_pagado*))
AT → BP: *Kpriv*$_{AT}$ (*Kpúb*$_{BP}$ (*identidad*$_P$, *código_para_pagar_IRPF*))
BP → AT: *Kpriv*$_{BP}$ (*Kpúb*$_{AT}$ (*identidad*$_P$, *código_IRPF_pagado*))
AT → P: *Kpriv*$_{AT}$ (*Kpúb*$_P$ (*mensaje_declaración_correcta*))

Todos los certificados digitales han sido expedidos por una Autoridad de Certificación fiable (e.g. la Fábrica Nacional de Moneda y Timbre). Además, la AEAT conoce la identidad de los bancos a través de los cuales se puede realizar el pago telemático de la declaración de I.R.P.F. Responda **razonadamente** las siguientes cuestiones:

a) ¿Qué servicios de seguridad se proporcionan en la transacción indicada?
b) ¿Qué debilidades/vulnerabilidades presenta el esquema y, en su caso, cómo podrían solucionarse?

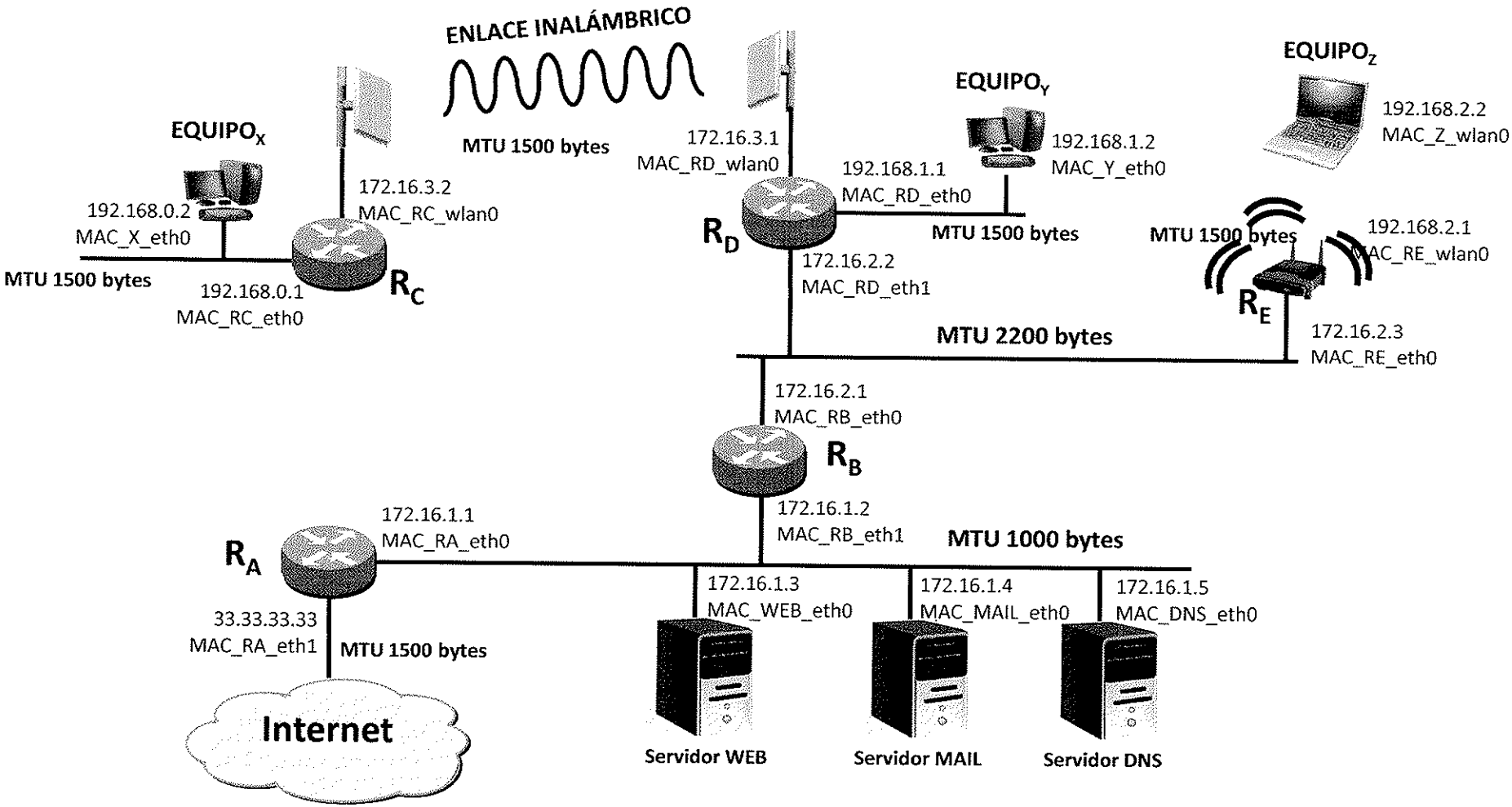

ENLACE INALÁMBRICO
MTU 1500 bytes
EQUIPO$_X$
192.168.0.2
MAC_X_eth0
MTU 1500 bytes
192.168.0.1
MAC_RC_eth0
172.16.3.2
MAC_RC_wlan0
R_C
172.16.3.1
MAC_RD_wlan0
R_D
EQUIPO$_Y$
192.168.1.2
MAC_Y_eth0
192.168.1.1
MAC_RD_eth0
MTU 1500 bytes
172.16.2.2
MAC_RD_eth1
EQUIPO$_Z$
192.168.2.2
MAC_Z_wlan0
MTU 1500 bytes
192.168.2.1
MAC_RE_wlan0
R_E
172.16.2.3
MAC_RE_eth0
MTU 2200 bytes
172.16.2.1
MAC_RB_eth0
R_B
172.16.1.2
MAC_RB_eth1
MTU 1000 bytes
R_A
172.16.1.1
MAC_RA_eth0
33.33.33.33
MAC_RA_eth1
MTU 1500 bytes
Internet
172.16.1.3
MAC_WEB_eth0
172.16.1.4
MAC_MAIL_eth0
172.16.1.5
MAC_DNS_eth0
Servidor WEB
Servidor MAIL
Servidor DNS

TABLA DE ENRUTAMIENTO DEL EQUIPO X

Red destino	Máscara	Sig. salto	Interfaz
192.168.0.0	/24	*	eth0
default	0.0.0.0	192.168.0.1	eth0

TABLA DE ENRUTAMIENTO DEL EQUIPO Y

Red destino	Máscara	Sig. salto	Interfaz
192.168.1.0	/24	*	eth0
default	0.0.0.0	192.168.1.1	eth0

TABLA DE ENRUTAMIENTO DEL EQUIPO Z

Red destino	Máscara	Sig. salto	Interfaz
192.168.2.0	/24	*	eth0
default	0.0.0.0	192.168.2.1	eth0

TABLA DE ENRUTAMIENTO DE LOS SERVIDORES WEB, MAIL Y DNS

Red destino	Máscara	Sig. salto	Interfaz
172.16.1.0	/24	*	eth0
192.168.0.0	/22	172.16.1.2	eth0
default	0.0.0.0	172.16.1.1	eth0

despiste

TABLA DE ENRUTAMIENTO DEL ROUTER R_A

Red destino	Máscara	Sig. salto	Interfaz
172.16.1.0	/24	*	eth0
192.168.0.0	/22	172.16.1.2	eth0
default	0.0.0.0	IP_GW_operador	eth1

TABLA DE ENRUTAMIENTO DEL ROUTER R_B

Red destino	Máscara	Sig. salto	Interfaz
172.16.1.0	/24	*	eth1
172.16.2.0	/24	*	eth0
192.168.0.0	/23	172.16.2.2	eth0
192.168.2.0	/24	172.16.2.3	eth0
default	0.0.0.0	172.16.1.1	eth1

TABLA DE ENRUTAMIENTO DEL ROUTER R_C

Red destino	Máscara	Sig. salto	Interfaz
192.168.0.0	/24	*	eth0
172.16.3.0	/24	*	wlan0
default	0.0.0.0	172.16.3.1	wlan0

olvido

TABLA DE ENRUTAMIENTO DEL ROUTER R_D

Red destino	Máscara	Sig. salto	Interfaz
192.168.1.0	/24	*	eth0
172.16.3.0	/24	*	wlan0
192.168.0.0	/24	172.16.3.2	wlan0
default	0.0.0.0	172.16.2.1	eth1

olvido

TABLA DE ENRUTAMIENTO DEL ROUTER R_E

Red destino	Máscara	Sig. salto	Interfaz
192.168.2.0	/24	*	wlan0
172.16.2.0	/24	*	eth0
default	0.0.0.0	172.16.2.1	eth0

olvido

¡¡¡TABLAS BIEN!!!

Entradas que faltan en el examen.

TABLA DE ENRUTAMIENTO DEL EQUIPO X

Red destino	Máscara	Sig. salto	Interfaz
172.16.3.2	/24	*	eth0
default	0.0.0.0	192.168.0.1	eth0

TABLA DE ENRUTAMIENTO DEL EQUIPO Y

Red destino	Máscara	Sig. salto	Interfaz
192.168.1.0	/24	*	eth0
default	0.0.0.0	192.168.1.1	eth0

TABLA DE ENRUTAMIENTO DEL EQUIPO Z

Red destino	Máscara	Sig. salto	Interfaz
192.168.2.0	/24	*	eth0
default	0.0.0.0	192.168.2.1	eth0

TABLA DE ENRUTAMIENTO DE LOS SERVIDORES WEB, MAIL Y DNS

Red destino	Máscara	Sig. salto	Interfaz
192.168.0.0	/22	172.16.1.2	~~wlan0~~ eth0
default	0.0.0.0	172.16.1.1	~~wlan0~~ eth0

despiste

TABLA DE ENRUTAMIENTO DEL ROUTER R_A

Red destino	Máscara	Sig. salto	Interfaz
172.16.1.0	/24	*	eth0
192.168.0.0	/22	172.16.1.2	eth0
default	0.0.0.0	IP_GW_operador	eth1

TABLA DE ENRUTAMIENTO DEL ROUTER R_B

Red destino	Máscara	Sig. salto	Interfaz
172.16.1.0	/24	*	eth1
172.16.2.0	/24	*	eth0
192.168.0.0	/23	172.16.2.2	eth0
default	0.0.0.0	172.16.2.1	eth1

TABLA DE ENRUTAMIENTO DEL ROUTER R_C

Red destino	Máscara	Sig. salto	Interfaz
192.168.0.0	/24	*	eth0
default	0.0.0.0	172.16.3.1	wlan0

olvido ruta directa a 172.16.3.0

TABLA DE ENRUTAMIENTO DEL ROUTER R_D

Red destino	Máscara	Sig. salto	Interfaz
192.168.1.0	/24	*	eth0
default	0.0.0.0	172.16.2.1	eth1

olvido ruta directa a 172.16.3.0

TABLA DE ENRUTAMIENTO DEL ROUTER R_E

Red destino	Máscara	Sig. salto	Interfaz
192.168.2.0	/24	*	wlan0
default	0.0.0.0	172.16.2.1	eth0

olvido ruta directa a 172.16.2.0

¡¡¡TABLAS MAL!!! → A propósito en el examen

TDRC2 Diciembre 2008

Ejercicio 1

a) Tramas entre Z y MAIL. Tablas ARP actualizadas. Se conoce el nombre de dominio de MAIL. Solicitud y respuesta de 1460 bytes.

Primero veamos si las distintas tramas llegarían bien a su destino, usando las tablas de encaminamiento.

Petición DNS:
- IP origen = IP_Z = 192.168.2.2
- IP destino = IP_{DNS} = 172.16.1.5

Z => ruta por defecto a través de 192.168.2.1 (Router R_E)

R_E => ruta por defecto a través de 172.16.2.1 (Router R_B)

R_B => ruta directa a través del interfaz eth1 a la red 172.16.1.0/24

=> llega el mensaje a 172.16.1.5 (DNS)

Respuesta DNS:
- IP origen = IP_{DNS} = 172.16.1.5
- IP destino = IP_Z = 192.168.2.2.

DNS => ruta a 192.168.0.0/22 por 172.16.1.2 (Router R_B)

R_B => ruta por defecto a 172.16.2.1 (Router R_B)

No se puede llegar a 172.16.2.1 a través de eth1 → mensaje ICMP de red inalcanzable.

Ruta circular (R_B ⇄ R_B) => no llega la respuesta DNS al equipo Z → se generaría un mensaje ICMP al origen de este mensaje (DNS) de ICMP tiempo excedido (tras un cierto tiempo el campo TTL se haría 0).

Como la respuesta DNS no llega, no se puede establecer una comunicación (establecimiento TCP + envío solicitud + recepción de respuesta) entre el equipo Z y el servidor MAIL.

Las tramas generadas serían:

	MAC origen	MAC destino	IP origen	IP destino	Puerto origen	Puerto destino	Flags	Mensaje
Petición DNS	MAC_Z_wan0	MAC_Rc_wan0	192.168.2.2	172.16.1.5	(*1) ~~53~~	53	—	Consulta DNS sobre UDP (suponemos longitud menor que 1000 bytes)
	MAC_Rc_eth0	MAC_RB_eth0	"	"	"	"	"	"
	MAC_RB_eth1	MAC_DNS_eth0	"	"	"	"	"	"
Respuesta DNS	MAC_DNS_eth0	MAC_RB_eth1	172.16.1.5	192.168.2.2	53	(*2)	—	Respuesta DNS (longitud < 1000 bytes)

No se puede enviar ese mensaje a 172.16.2.1 por el interfaz eth1 (ruta por defecto) =>
=> se genera un mensaje hacia el origen de destino inalcanzable (ICMP).

MAC_RB_eth1	MAC_DNS_eth0	172.16.1.2	172.16.1.5	—	—	—	Mensaje ICMP de destino inalcanzable (red inalcanzable).

Sin puerto porque ICMP va encima de IP, no de un protocolo de transporte.

b) => ¿Es posible un ping entre el equipo X y el equipo Y?

Mensaje ICMP echo-request { IP origen ≡ IP_X ≡ 192.168.0.2
IP destino ≡ IP_Y ≡ 192.168.1.2.

Encaminamiento:

X => ruta por defecto a través de 192.168.0.1 (Router Rc)

Rc => ruta por defecto a través de 172.16.3.1 (Router RD)

(En realidad no sabría llegar a RD porque no está la ruta directa a la red 172.16.3.0)

RD => ruta directa a la red 192.168.1.0 =>
=> llega al equipo Y.

Mensaje ICMP echo-reply { IP origen ≡ IP_Y ≡ 192.168.1.2
IP destino ≡ IP_X ≡ 192.168.0.2.

Y => ruta por defecto a través de 192.168.1.1 (RD)

RD => ruta por defecto a través de 172.16.2.1 (RB)

RB => ruta a través de 172.16.2.2 (RD)

↳ Ruta circular. Cuando TTL se haga 0, se mandará

un mensaje ICMP de tiempo excedido por TTL.

⇒ Como no llega la respuesta del PING,

NO SE PODRÍA REALIZAR UN PING ENTRE EL EQUIPO X y EL EQUIPO Y

⇒ ¿Se podría conectar Y a Internet (intercambiar datos con un equipo externo)?

Un equipo externo necesariamente tendrá una IP pública.

Veamos si el encaminamiento de paquetes es posible.

Envío de datos → { IPorigen = IP_Y = 192.168.1.2
IPdestino = IP pública.

Encaminamiento:

Y ⇒ ruta por defecto a través de 192.168.1.1 (R_D)

R_D ⇒ ruta por defecto a través de 172.16.2.1 (R_B)

R_B ⇒ ruta por defecto a través de 172.16.2.1 (R_B) sobre el interfaz eth1 ⇒

⇒ no sabe llegar ⇒ destino inalcanzable.

En realidad falta la ruta directa a la red 172.16.2.0

En realidad esa ruta debería ser a 172.16.1.1 (R_A).

En ese caso,

R_A ⇒ ruta por defecto a la pasarela del operador (se supone que sabe encaminar correctamente hacia Internet).

Si seguimos suponiendo que esa ruta (a través de R_A) estuviese correcta:

Recepción de datos { IPorigen = IP pública
IPdestino = IP_Y = 192.168.1.2

R_A ⇒ ruta a través de 172.16.1.2 (R_B)

R_B ⇒ ruta a través de 172.16.2.2 (R_D)

R_D ⇒ ruta directa a la red 192.168.1.0

↳ En ese caso sí llegaría al equipo Y.

c) ¿Qué problemas ha detectado en las tablas de encaminamiento? ¿Cómo los solucionaría?

→ Añadir rutas directas que faltan (R_C, R_D y R_E).

→ WEB, MAIL y DNS han de tener una ruta directa a 172.16.1.0.

→ R_B necesita una ruta a 192.168.2.0/24 a través de 172.16.2.3 (R_E) (interfaz eth0)

→ R_D necesita una ruta a 192.168.0.0/24 a través de 172.16.3.2 (R_C) (interfaz wlan0)

NOTA: En el enunciado, la dirección de R_E en el interfaz eth0 está mal. Pone 172.16.2.2 y debería ser 172.16.2.3, ya que la primera es la dirección de R_D.

→ R_B por defecto a 172.16.1.1, no a 172.16.2.1. (para salir a Internet).

Ejercicio 2

Número mínimo de sockets en un servidor HTTP.

a) Un socket de control para escuchar peticiones en el puerto 80.

b) Un socket de datos por cliente.

↝ Si es un servidor iterativo, sólo serviría a un cliente a la vez ⇒ 2 SOCKETS EN TOTAL

↝ Si es un servidor concurrente, abriría un socket por cliente ⇒ (N+1) SOCKETS EN TOTAL

Como preguntan por el mínimo, sería el caso del servidor iterativo y la respuesta sería 2.

Ejercicio 3

Conexión TCP entre dos entidades. ¿Qué ocurre al detectarse una pérdida?

Detección del error:

* Llega paquete al receptor con CRC erróneo (poco probable)
* Llegan al emisor 3 ACK fuera de orden
  (si llega sólo 1 puede ser que el paquete tiene más retardo por usar otra ruta).
* Expira timer en emisor sin llegar ACK

Acciones:

* Control de errores: reenvío la trama.
* Control de congestión: depende del tipo de TCP. En TCP Tahoe, se iniciaría el inicio lento y se cambiaría el valor del umbral a la mitad.
* Control de flujo = NO SE VE AFECTADO.

Ejercicio 4

a) Servicios proporcionados.

Veamos cada servicio de seguridad por separado:

* Confidencialidad: todos los mensajes están encriptados con la clave pública del receptor, por lo que sólo el receptor puede desencriptarlos con su clave privada ⇒ {SÍ SE SOPORTA CONFIDENCIALIDAD}

* Autenticación: todos los mensajes van encriptados con la clave privada del emisor, por lo que el receptor puede desencriptar esta primera encriptación con la clave pública del emisor.
Como se desencripta con su clave pública del emisor, sólo lo pudo encriptar con su clave privada el emisor → se fidedignamente que el mensaje lo envía el emisor. ⇒ {SÍ SE SOPORTA AUTENTICACIÓN}

NOTA: las claves públicas y privadas están garantizadas por una autoridad fiable, ya que los certificados digitales (que incluyen la identidad y la clave pública entre otras cosas) han sido expedidos por una Autoridad de Certificación fiable (como dice el enunciado).

* Integridad: No hay forma de comprobar si un tercero ha modificado los mensajes. Habría que incluir un compendio o resumen del mensaje (normalmente generado por una función HASH).
{NO SE SOPORTA INTEGRIDAD.}

* NO REPUDIO: Al hacer un doble cifrado, el que cifra con su clave privada no puede decir después que no mandó ese mensaje (ya que nadie más tiene su clave privada) ⇒ (SÍ SE SOPORTA EL NO REPUDIO)

* DISPONIBILIDAD: El protocolo de aplicación visto no tiene nada que ver con la disponibilidad. Serán otras técnicas las que permitan garantizar la disponibilidad.
  → Ejemplo: si cortan el cable de red no tengo disponible el servicio.

b) Vulnerabilidades y soluciones.

⇒ No se soporta la integridad. Se podría añadir un resumen del mensaje, de forma que si éste es modificado, el resumen calculado con el nuevo mensaje no coincide con el resumen enviado ⇒ me doy cuenta de que ha sido modificado.

⇒ Respecto a la disponibilidad, hay muchos factores que influyen. Habría que proporcionar redundancia de conexiones a red (e.g. otra red de acceso alternativa). También aplicar técnicas que eviten los ataques de denegación de servicio (DoS).
(Entre otras cuestiones).