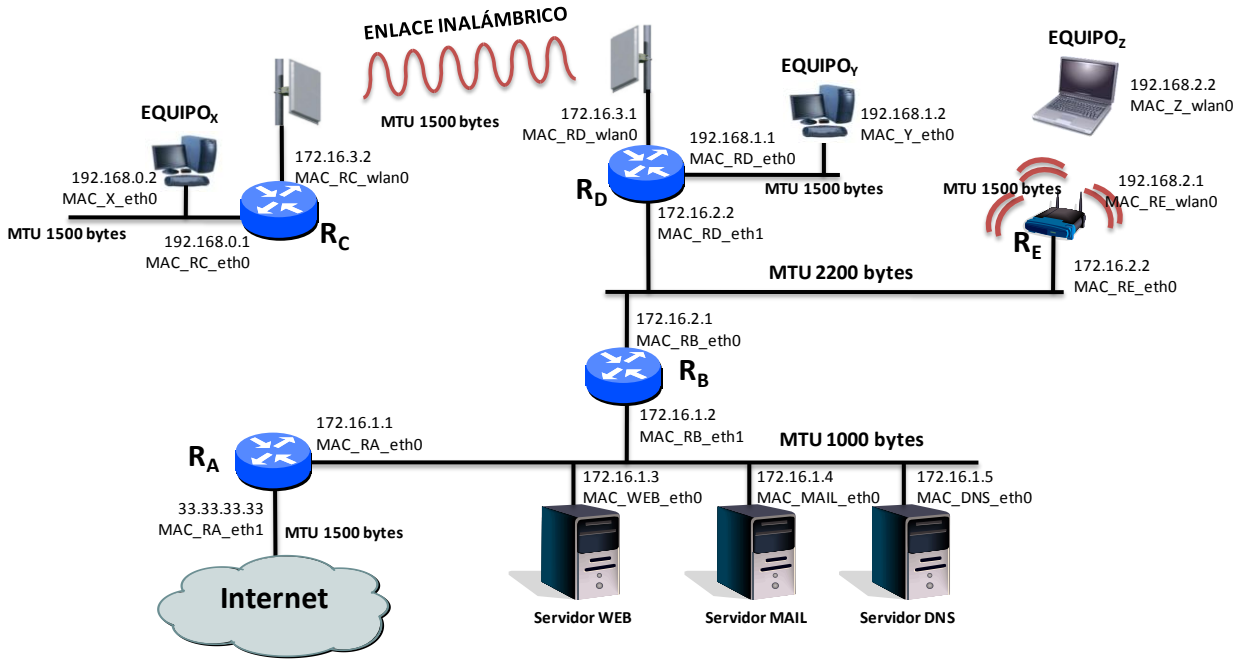
TRANSMISIÓN DE DATOS Y REDES DE COMPUTADORES II

– 4º curso de Ingeniería Informática –

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

Apellidos y nombre: _____

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
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
default	0.0.0.0	172.16.1.1	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

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*, 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?