UNIVERSIDAD DE GRANADA

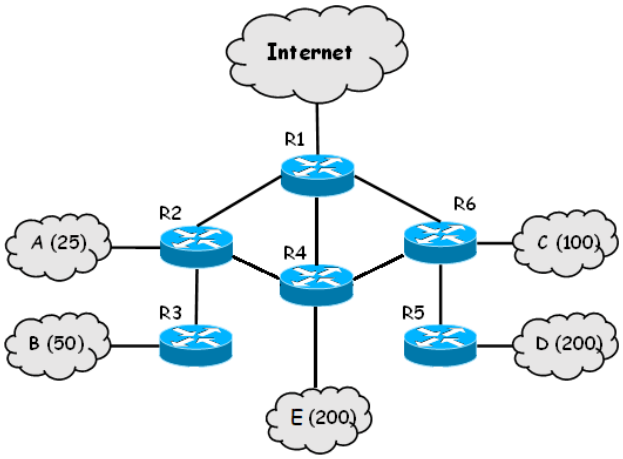
Departamento de Teoría de la Señal, Telemática y Comunicaciones

FUNDAMENTOS DE REDES

3er curso del Grado en Ingeniería Informática

Convocatoria extraordinaria – Examen Teoría (17 de febrero de 2022)

Apellidos y nombre/Grupo:



EJERCICIO 1 (3 puntos sobre 10)

La siguiente figura muestra la topología de una intranet. El ISP ha proporcionado únicamente una dirección pública 75.83.41.4, con la pasarela 75.83.41.5.

a) *(1,5 puntos)* Realice una asignación de direcciones IP privadas para todas las redes, incluyendo las redes entre routers, tal que se minimice el número de IPs no usadas.

b) *(1 punto)* Muestre el contenido de las tablas de encaminamiento de los routers R1, R3 y R4, intentando minimizar el número de entradas en las mismas.

c) *(0,5 puntos)* Si quisiera añadir una subred F con 2 equipos en cualquier punto, ¿cómo conseguiría que sólo los equipos de esa subred tuvieran acceso a Internet (y no los de las demás subredes) y dónde la ubicaría?.

Posible solución para el apartado a

Red E → 200 + red + difusión + router = 203 < 256 → 192.168.0.0/24 → de 192.168.0.0 (red) a 192.168.0.255 (difusión)
Red D → 200 + 3 < 256 → 192.168.1.0/24 → de 192.168.1.0 (red) a 192.168.1.255 (difusión)
Red C → 100 + 3 < 128 → 192.168.2.0/25 → de 192.168.2.0 (red) a 192.168.2.127 (difusión)
Red B → 50 + 3 < 64 → 192.168.2.128/26 → de 192.168.2.128 (red) a 192.168.2.191 (difusión)
Red A → 25 + 3 < 32 → 192.168.2.192/27 → de 192.168.2.192 (red) a 192.168.2.223 (difusión)

Las redes entre routers necesitan 2 IPs (2 routers) + red + difusión = 4 → máscara /30. Siguiendo con direcciones consecutivas, podría ser:
Red R1-R2 → 192.168.2.224/30 → .224 para red, .225 para el primer router (R1), .226 para el segundo router (R2), .227 para difusión
Red R2-R3 → 192.168.2.228/30 → .228 red, .229 R2, .230 R3, .231 difusión
Red R2-R4 → 192.168.2.232/30 → .232 red, .233 R2, .234 R4, .235 difusión
Red R4-R1 → 192.168.2.236/30 → .236 red, .237 R4, .238 R1, .239 difusión
Red R4-R6 → 192.168.2.240/30 → .240 red, .241 R4, .242 R6, .243 difusión
Red R6-R5 → 192.168.2.244/30 → .244 red, .245 R6, .246 R5, .247 difusión
Red R6-R1 → 192.168.2.248/30 → .248 red, .249 R6, .250 R1, .251 difusión

Apartado b

En general, hay que poner las rutas a las redes directamente conectadas (si no, no llegamos a ellas), poner las rutas a las redes con destinatarios (no hay que poner las rutas a todas las redes entre routers, salvo que queramos poder conectarnos a los routers, algo que habitualmente no es necesario y no se pide). Lo normal sería también añadir una entrada para las rutas por defecto (para poder salir al resto de redes en el mundo, i.e. Internet), pero en vista del apartado C, no la añadiremos en los routers interiores y sólo la incluiremos en R1.
Además, como se pide minimizar, habría que:

- Agruparemos las redes A-B: éstas se agruparían con 192.168.2.128/25. Es cierto que eso incluiría las redes entre routers, pero 1) normalmente no queremos acceder a ellas y 2) si quisiéramos acceder a ellas, pondríamos además las rutas a esas redes y no habría problema porque tienen una máscara más restrictiva.
- Agruparemos las redes C-D: éstas se agruparían con 192.168.0.0/22, que es una dirección que incluiría todas las subredes de la intranet, pero como habría entradas con máscaras más restrictivas para llegar a cada una de las subredes, no habría problema.

Tabla de encaminamiento de R1

Red destino	Máscara	Siguiente salto
192.168.2.224 (red R1-R2)	/30	*
192.168.1.236 (red R1-R4)	/30	*
192.168.1.248 (red R1-R6)	/30	*
default (o 0.0.0.0) (salida a Internet)	/0	75.83.41.5
192.168.0.0 (C y D, ver máscara)	/22	192.168.2.249 (R6)
192.168.2.128 (A y B, ver máscara)	/25	192.168.2.226 (R2)
192.168.0.0 (Red E)	/24	192.168.2.237 (R4)

Tabla de encaminamiento de R3

Red destino	Máscara	Siguiente salto
192.168.2.128 (red B)	/26	*
192.168.2.228 (red R2-R3)	/30	*
192.168.0.0 (todas las subredes de la intranet)	/22	192.168.2.229 (R2)

Tabla de encaminamiento de R4

Red destino	Máscara	Siguiente salto
192.168.0.0 (red E)	/24	*
192.168.2.236 (red R4-R1)	/30	*
192.168.2.232 (red R4-R2)	/30	*
192.168.2.240 (red R4-R6)	/30	*
192.168.2.128 (A y B, ver máscara)	/25	192.168.2.233 (R2)
192.168.0.0 (C y D, ver máscara)	/22	192.168.2.242 (R6)

Apartado c

Red F → 2 equipos + router + red + difusión = 5 < 8 → por ejemplo, de 192.168.3.0/29 → de 192.168.3.0 (red) a 192.168.3.7 (difusión)

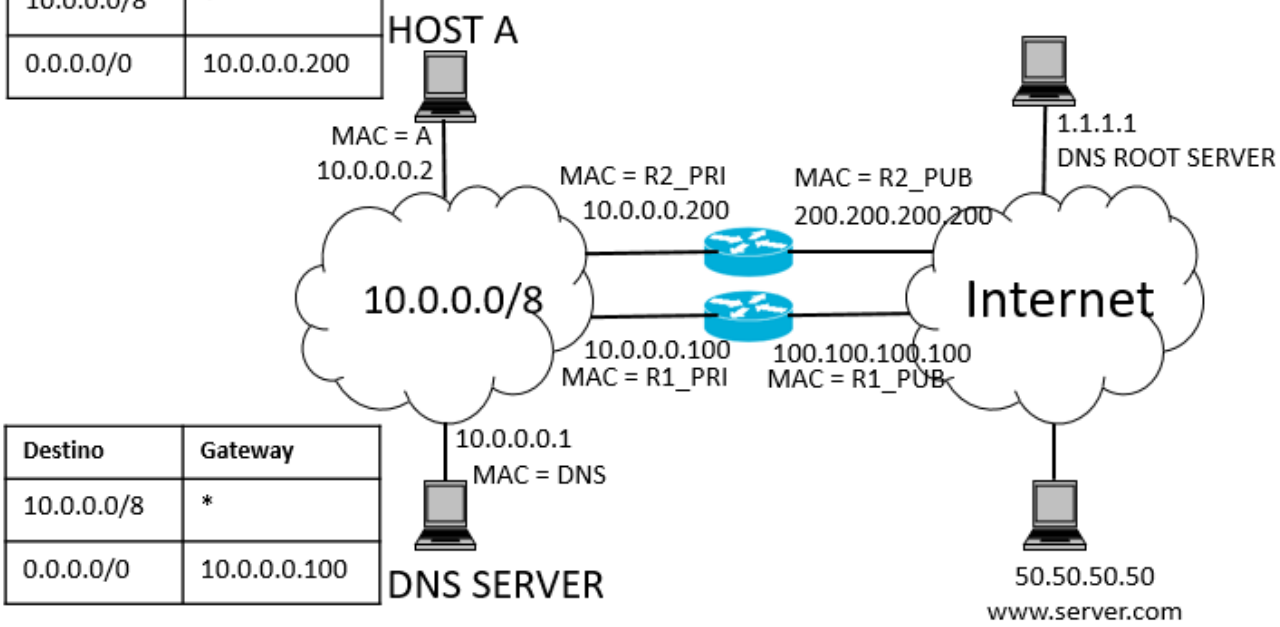
Podríamos conectar la red F directamente a R1. En ese caso, R1 debería tener una entrada 'default' para dirigir el tráfico hacia Internet proveniente de la Red F hasta la pasarela del ISP. R1 tendría también una entrada por conexión directa a la Red F.

Los demás routers sólo deberían dirigir tráfico hacia las demás subredes. No deberían tener entradas 'default' para así no poder llegar a destinos externos a la intranet.

EJERCICIO 2 (2 puntos sobre 10)

Con la ayuda de la tabla mostrada en la página 4 del examen, identifique secuencialmente salto a salto todo el tráfico que se generaría en 10.0.0.0/8 y a la salida de los routers, desde que un navegador situado en el **HOST A** solicita la URL http://www.server.com. Complete para cada fila de la tabla todos los campos que sean necesarios. Suponga que todas las tablas ARP están completas y que la cache del DNS SERVER contiene los registros necesarios.

Destino	Gateway
10.0.0.0/8	*
0.0.0.0/0	10.0.0.0.200



Destino	Gateway
10.0.0.0/8	*
0.0.0.0/0	10.0.0.0.100

En la siguiente página se muestra la tabla con las tramas intercambiadas. Algunos aspectos a tener en cuenta:

- Las direcciones MAC cambian salto a salto (origen quien transmite en ese segmento de red, destino quien recibe en ese segmento de red).
- Las direcciones IP son extremo a extremo (origen y destino finales), por lo que no cambian salto a salto. Solo cambian cuando se usa NAT, como es el caso de este ejercicio al pasar de una red privada a una red pública (se usa Source NAT). Cuando se vuelve (respuesta), se deshace dicho cambio de IPs.
- DNS funciona sobre UDP normalmente (también lo puede hacer sobre TCP). Si se usa UDP, que es lo habitual, no hay establecimiento ni cierre de conexión ni se utilizan flags.
- HTTP funciona sobre TCP, por lo que hay establecimiento de conexión (mensajes SYN, SYN+ACK y ACK), tiene confirmaciones (ACKs) y finalmente cierre de conexión (mensajes FIN, FIN+ACK y ACK).
- Los puertos de los clientes son asignados por el sistema operativo, estando por encima de 1024 y siendo en general aleatorios (se van asignando secuencialmente conforme muchos programas piden puertos al sistema operativo, no se puede saber el orden ni el valor a priori). Los puertos de los servidores son los habituales (53 en el caso de DNS, 80 en el caso de HTTP).

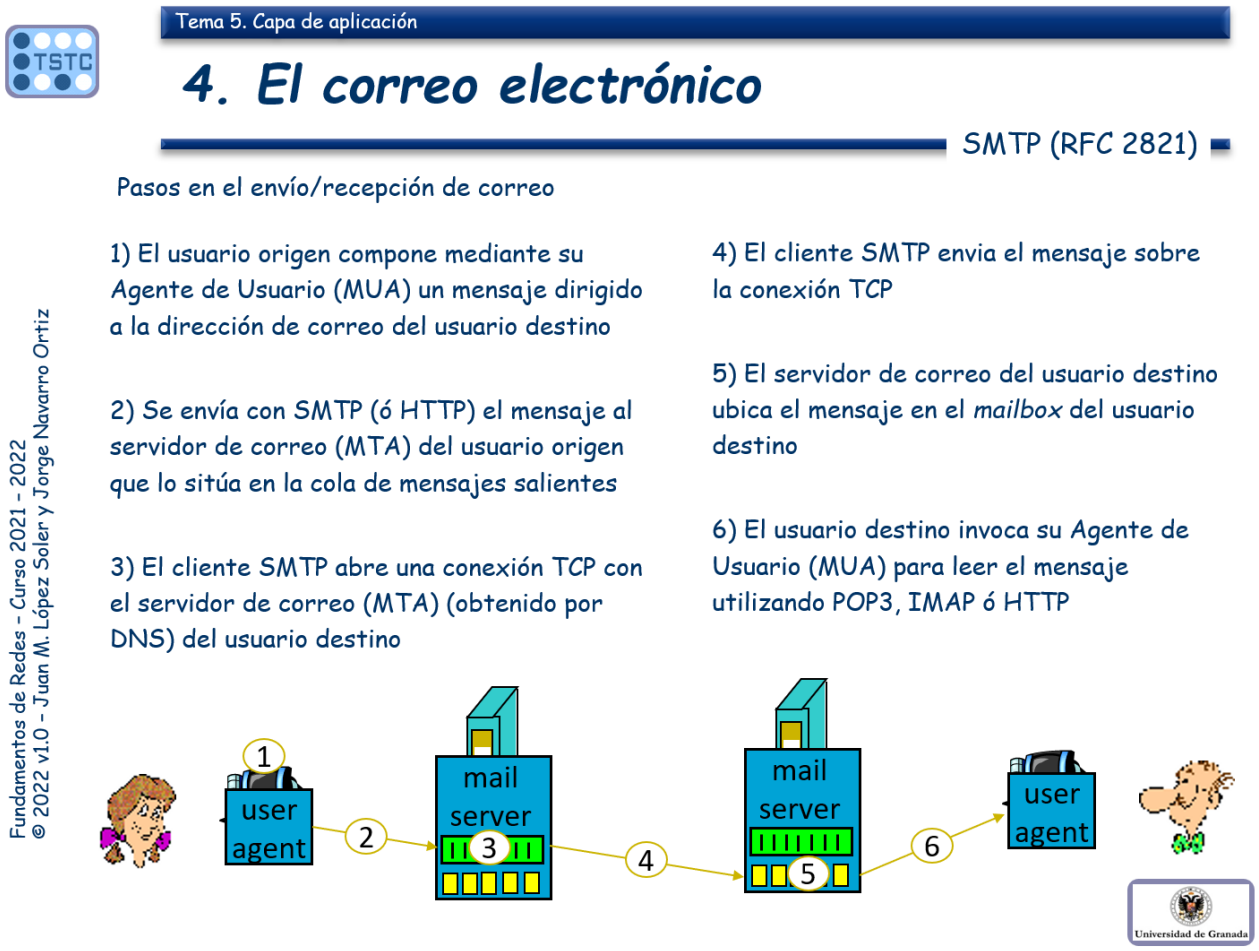
MAC ORIGEN	MAC DESTINO	IP ORIGEN	IP DESTINO	FLAGS	PUERTO ORIGEN	PUERTO DESTINO	MENSAJE	COMENTARIOS
A	DNS	10.0.0.2	10.0.0.1	-	X > 1024	53	CONSULTA DNS www.server.com	La cache de A está vacÍa. Usa UDP
DNS	A	10.0.0.1	10.0.0.2	-	53	X	RESPUESTA DNS: 50.50.50.50	La cache DNS tiene ese RR se resuelve.
A	R2_PRIV	10.0.0.2	50.50.50.50	SYN=1	Y > 1024	80	SYN DE TCP	Establecimiento de la conexión, #seq
R2_PUB	MAC_NEXT_HOP	200.200.200.200	50.50.50.50	SYN=1	Z > 1024	80	SYN DE TCP	NAT cambia IP y PORT origen
MAC_NEXT_HOP	R2_PUB	50.50.50.50	200.200.200.200	SYN=1, ACK=1	80	Z	SYN+ACK	Llega SYN+ACK al ROUTER NAT
R2_PRIV	A	50.50.50.50	10.0.0.2	SYN=1, ACK=1	80	Y	SYN+ACK	NAT cambia IP y PORT destino
A	R2_PRIV	10.0.0.2	50.50.50.50	ACK=1	Y	80	ACK DE TCP	ACK del HANDSHAKE
R2_PUB	MAC_NEXT_HOP	200.200.200.200	50.50.50.50	ACK=1	Z	80	ACK DE TCP	NAT cambia IP y port ORIGEN
A	R2_PRIV	10.0.0.2	50.50.50.50	-	Y	80	GET de HTTP	Datos TCP con #seq+1
R2_PUB	MAC_NEXT_HOP	200.200.200.200	50.50.50.50	-	Z	80	GET de HTTP	NAT cambia IP y PORT ORIGEN
MAC_NEXT_HOP	R2_PUB	50.50.50.50	200.200.200.200	ACK=1	80	Z	RESPUESTA al GET	Incluye index.html
R2_PRIV	A	50.50.50.50	10.0.0.2	ACK=1	80	Y	RESPUESTA al GET	NAT cambia IP y PORT destino
A	R2_PRIV	10.0.0.2	50.50.50.50	FIN=1, ACK=1	Y	80	FIN de la conexión y ACK del index.html	Llega FIN+ACK al ROUTER NAT
R2_PUB	MAC_NEXT_HOP	200.200.200.200	50.50.50.50	FIN=1, ACK=1	Z	80	FIN de la conexión y ACK del index.html	NAT cambia IP y port ORIGEN
MAC_NEXT_HOP	R2_PUB	50.50.50.50	200.200.200.200	FIN=1, ACK=1	80	Z	FIN de la conexión y ACK	Llega FIN+ACK al ROUTER NAT
R2_PRIV	A	50.50.50.50	10.0.0.2	FIN=1, ACK=1	80	Y	FIN de la conexión y ACK	NAT cambia IP y PORT destino
A	R2_PRIV	10.0.0.2	50.50.50.50	ACK=1	Y	80	ACK para el FIN	Llega ACK al ROUTER NAT
R2_PUB	MAC_NEXT_HOP	200.200.200.200	50.50.50.50	ACK=1	Z	80	ACK para el FIN	NAT cambia IP y PORT ORIGEN

PREGUNTA 1 (1.5 puntos sobre 10)

Si usuario1@lab1.es manda un correo electrónico a usuario2@lab2.es, identifique las entidades involucradas (ponga su nombre completo) para que dicho correo sea leido por el destinatario. Indique los protocolos utilizados entre dichas entidades y las peticiones DNS que realizarían las mismas.

Esta pregunta se responde parcialmente con la siguiente transparencia. A esta habría que añadir que MUA significa Mail User Agent y MTA significa Mail Transfer Agent (está en la primera transparencia sobre correo electrónico). Además, respecto al uso de DNS:

- El MUA de usuario1@lab1.es tiene que hacer una petición DNS preguntando por la IP de su servidor de correo electrónico (dominio lab1.es), cuyo nombre de dominio estará configurado en el propio cliente. Con esa IP, el MUA ya puede conectarse con su MTA y enviar el correo usando SMTP.
- El MTA de lab1.es mirará el destinatario (usuario2@lab2.es) y preguntará a su servidor DNS por el registro MX (Mail eXchange) del dominio lab2.es. Una vez obtenida la IP, se conectará a dicho servidor de correo electrónico y le mandará el mensaje usando SMTP.
- En algún momento, el MUA de usuario2@lab2.es querrá mirar los correos electrónicos recibidos. Para ello, preguntará a su DNS por la dirección IP de su MTA, cuyo nombre de dominio estará configurado en el propio cliente. Con esa IP, el MUA ya puede conectarse con su MTA y descargarse el correo usando POP3 o IMAP.



PREGUNTA 2 (1.5 puntos sobre 10)

Explique lo que son los números de secuencia en los protocolos de la capa de transporte, cómo se determinan y su utilidad.

Inicialmente se puede comentar lo que aparece en la siguiente transparencia (resumiendo la parte de ISN):

3.2. TCP. Control de conexión.

Control de la conexión. Números de secuencia.

- El número de secuencia es un campo de 32 bits que cuenta bytes en módulo 2^{32} (el contador se da la vuelta cuando llega al valor máximo).
- El número de secuencia no empieza normalmente en 0, sino en un valor denominado ISN (Initial Sequence Number) elegido "teóricamente" al azar; para evitar confusiones con solicitudes anteriores.
- El ISN es elegido por el sistema (cliente o servidor). El estándar sugiere utilizar un contador entero incrementado en 1 cada 4 μs aproximadamente. En este caso el contador se da la vuelta (y el ISN reaparece) al cabo de 4 horas 46 min.
- El mecanismo de selección de los ISN es suficientemente fiable para proteger de coincidencias, pero no es un mecanismo de protección frente a sabotajes. Es muy fácil averiguar el ISN de una conexión e interceptarla suplantando a alguno de los dos participantes.
- TCP incrementa el número de secuencia de cada segmento según los bytes que tenía el segmento anterior, con una sola excepción:
  - Los flags SYN y FIN, cuando están puestos, incrementan en 1 el número de secuencia.
- La presencia del flag ACK no incrementa el número de secuencia.

Además, sobre cómo se determina se debería indicar:

- Los mensajes SYN iniciales sirven para sincronizar los números de secuencia de cada lado (son diferentes para cada extremo). Aumentan en 1 al recibirse el ACK correspondiente al SYN (igual para el cierre de conexión con los mensajes FIN).
- El número de secuencia indica el primer byte del segmento, de forma que en cada segmento valdrá la suma del valor en el segmento anterior más el tamaño de dicho segmento anterior.

Utilidad:

- Sirve para mantener el orden de los segmentos recibidos. Como indica la posición del primer byte del segmento, si llegan varios segmentos desordenados (o retransmitidos) podemos colocarlos en su lugar adecuado.
- También sirve para detectar errores, usando para ello los campos de secuencia y de acuse. El acuse es el número de byte que espera recibir el receptor, que debería ser el último número de secuencia del receptor más el tamaño del segmento en el que se envió. Si no, significa que ha habido una discontinuidad y algún segmento no se ha recibido (bien porque se haya perdido, bien porque llegue más tarde desordenado).

PREGUNTA 3 (2 puntos sobre 10)

Describa el proceso del doble cifrado y explique los servicios de seguridad que proporciona dicho proceso.

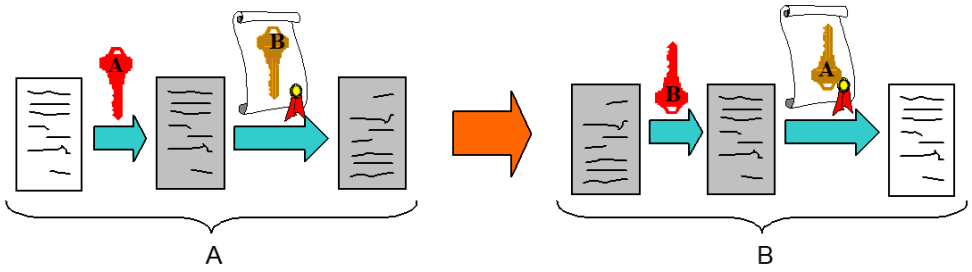
Esta pregunta se explica en la siguiente transparencia. Básicamente:

- Cifro con la clave pública del receptor → consigo confidencialidad porque solo el receptor puede descifrarlo con su clave privada.
- Cifro con la clave privada del emisor → consigo autenticación, porque solo el emisor conocía la clave privada (cualquiera descifra con la clave pública del emisor)
- No repudio: no se puede garantizar salvo que haya alguien me garantice la relación entre la identidad del emisor y su clave privada. En otro caso, no me serviría de prueba ante un juez. Si se garantiza esa relación (básicamente sería tener un certificado digital, donde una autoridad certificadora me garantiza con su firma que una identidad tiene una clave pública asociada), entonces sí se garantizaría el no repudio. Así que no se garantizaría en el caso general.

- No se garantiza la integridad (no hay ningún resumen o compendio que me permita comprobar si alguien ha modificado el mensaje).

5. Firma digital y certificados digitales

- Firma digital con clave asimétrica. *Doble cifrado*:
  - Uno para proporcionar privacidad, con KpubB
  - Otro, previo, para autenticación, con KpriA
  - Para firmar, enviar KpubB(KpriA (T) →
  - En el receptor KpubA (KpriB (KpubB(KpriA (T))))=T



  - Debilidad: para garantizar el no repudio se necesita garantizar la asociación fehaciente e indisoluble de la "identidad A" con su "clave pública KpubA" (A ←→ KpubA) … ?
    esto se consigue con un "certificado digital"