UNIVERSIDAD DE GRANADA

Dpto. Teoría de la Señal, Telemática y Comunicaciones
E.T.S. Ingeniería Informática y de Telecomunicación
C/ Periodista Daniel Saucedo Aranda, S/N
18071- Granada

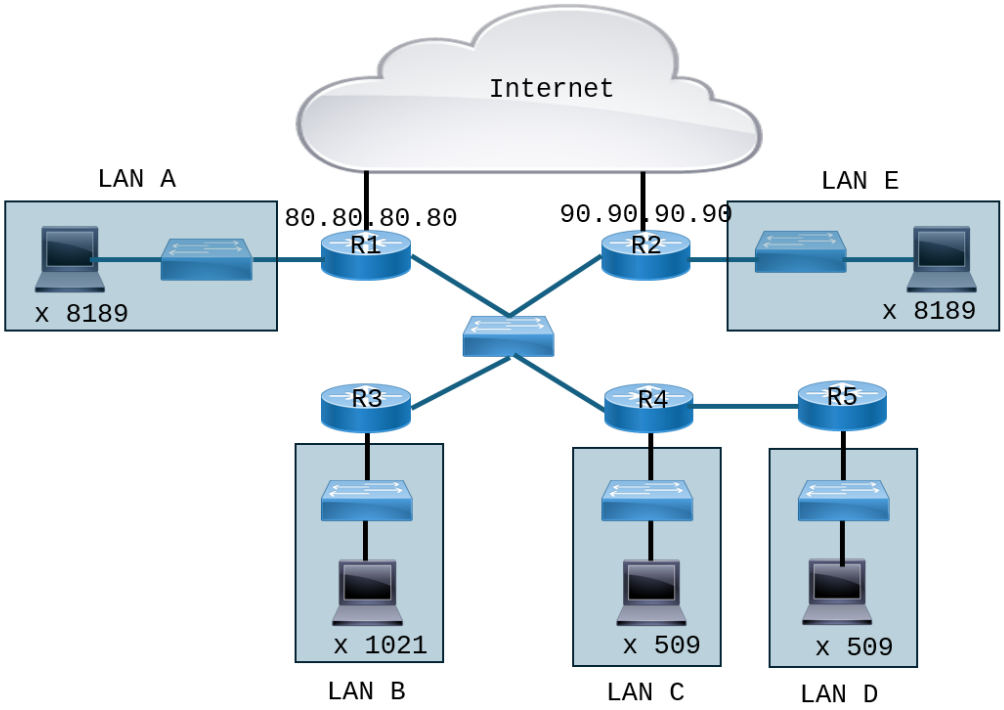
FUNDAMENTOS DE REDES. Examen de Teoría.
Convocatoria Extraordinaria. Febrero 2024.

Apellidos y nombre: _____ **GRUPO:** _____

PROBLEMA 1 (3 puntos sobre 10)

En la intranet de la figura, **sólo puede usar las direcciones 172.16.0.0/16.**

a) **Asigne direcciones** a todos los equipos en las LAN A, B, C, D y E así como a todas las interfaces de los routers R1, R2 R3 R4 y R5, **especifique las máscaras** tal que se desperdicien el número mínimo de direcciones.
b) ¿**Cuántas** redes LAN adicionales con 8189 hosts cada una y con su correspondiente *router* se podrían añadir? **Justifique** la respuesta.
c) **Muestre las tablas** de encaminamiento de R1 y de R2.
d) **Muestre la tabla** de R3 para que los hosts de LAN B puedan acceder a todas las redes y accedan a internet por R1
e) **Muestre la tabla** de encaminamiento de un host de LAN E para que **sólo** pueda acceder a los hosts de LAN C y LAN D



a) Realizamos la siguiente asignación de direcciones comprobando que las máscaras son lo más restrictivas posibles y que no aparezcan 1's en binario en la parte de equipo al definir las redes.

Las máscaras se calculan considerando el número de equipos + dirección del router + dirección de red + dirección de difusión <= 2^x, donde x es el número de bits a 0 en la máscara de red. Por ejemplo, la LAN A tiene 8189 + 1 + 1 + 1 = 8192 <= 2^13, por lo que el número de bits a 1 será 32-13 = 19 y la máscara será /19. De forma similar se calcula para el resto de equipos. Además, habrá que coger el rango siguiente que no tenga ningún bit a 1 en la parte de equipo ya que, si no, no estaríamos definiendo bien la red.

Si asignásemos las direcciones ordenándolas de menor a mayor número de equipos, podríamos asignar las direcciones de la siguiente manera:

LAN C: 172.16.0.0/23 → de 172.16.0.0 (dirección de red, i.e. todos los bits de la parte de equipo a 0) a 172.16.1.255 (dirección de difusión, i.e. todos los bits de la parte de equipo a 1). Asignamos 172.16.0.1 a R4.
LAN D: 172.16.2.0/23 → de 172.16.2.1 (dirección de red) a 172.16.3.255 (dirección de difusión). Asignamos 172.16.2.1 a R5.
LAN B: 172.16.4.0/22 → de 172.16.4.0 (dirección de red) a 172.16.7.255 (dirección de difusión). Asignamos 172.16.4.1 a R3.

Si utilizáramos para la LAN E direcciones consecutivas, i.e. 172.16.8.0/19, aparecerían 1's en la parte de equipo (10101100.00010000.00001000.0000000, bits de red en rojo y bits de equipo en verde). Por tanto, estaría mal definida y, si se usara esa definición en una tabla de encaminamiento, aparecería la dirección 172.16.0.0 al hacer el AND lógico entre cualquier dirección de destino de dicha red y la máscara /19, lo que solaparía con las redes anteriores.

Por tanto, la siguiente dirección que podríamos utilizar sin solapar con las redes anteriores y que estuviese bien definida sería 10101100.00010000.001**1**00000.0000000, es decir, 172.16.32.0/19.

LAN E: 172.16.32.0/19 → de 172.16.32.0 (dirección de red) a 172.16.63.255 (dirección de difusión). Asignamos 172.16.32.1 a R2.

De forma similar, continuaríamos por la LAN A y tendríamos que asignarle la dirección de red 10101100.00010000.0**10**00000.0000000, es decir, 172.16.64.0/19.

LAN A: 172.16.64.0/21 → de 172.16.64.0 (dirección de red) a 172.16.95.255 (dirección de difusión). Asignamos 172.16.64.1 a R1.

Faltaría asignar las direcciones entre los routers R1-R2-R3-R4 (es una única red ya que estos routers están conectados a través de un switch, que funciona a nivel de enlace) y la red entre los routers R4 y R5. Podríamos utilizar el rango no usado de 172.16.8.0 a 172.16.31.255, como se muestra a continuación.

Red R1-R2-R3-R4: necesitamos 4 direcciones de los routers + dirección de red + dirección de difusión = 6 direcciones → necesito 3 bits para direccionarlas (2^3 = 8 >= 6) → máscara /29 (32 – 3 = 29). Así, podríamos asignar la red 172.16.8.0/29 con e.g. R1 = 172.16.8.1, R2 = 172.16.8.2, R3 = 172.16.8.3, R4 = 172.16.8.4, dirección de red 172.16.8.0 y dirección de difusión 172.16.8.7. Se puede comprobar fácilmente que los bits de la parte de equipo están a 0, por lo que la red está bien definida.

Red R4-R5 → necesitamos 2 direcciones de los routers + dirección de red + dirección de difusión = 4 → máscara /30. Podríamos asignar la red 172.16.8.8/30, con R4 = 172.16.8.9, R5 = 172.16.8.10, dirección de red 172.16.8.8 y dirección de difusión 172.16.8.11. Se puede comprobar fácilmente que los bits de la parte de equipo están a 0, por lo que la red está bien definida.

De esta forma, las redes estarían bien definidas, aunque observamos que hay direcciones no utilizadas en el rango 172.16.8.12 a 172.16.31.255.

Para evitar esto (algo que indica el problema expresamente, al decir "*que se desperdicien el número mínimo de direcciones*"), la forma más sencilla es asignar las direcciones ordenando las redes de mayor a menor número de equipos. Se puede comprobar fácilmente que, siguiendo este orden, los bits de la parte de equipo están a 0 (red bien definida) y que se pueden asignar rangos consecutivos sin desperdiciar direcciones. Así, quedaría:

LAN A: 172.16.0.0/19 → de 172.16.0.0 (dir. de red) a 172.16.31.255 (dir. difusión), con R1 = 172.16.0.1.
LAN E: 172.16.32.0/19 → de 172.16.32.0 (dir. red) a 172.16.63.255 (dir. difusión), con R2 = 172.16.32.1
LAN B: 172.16.64.0/22 → de 172.16.64.0 (dir. red) a 172.16.67.255 (dir. difusión), con R3 = 172.16.64.1
LAN C: 172.16.68.0/23 → de 172.16.68.0 (dir. red) a 172.16.69.255 (dir. difusión), con R4 = 172.16.68.1
LAN D: 172.16.70.0/23 → de 172.16.70.0 (dir. red) a 172.16.71.255 (dir. difusión), con R5 = 172.16.70.1
Red R1-R2-R3-R4: 172.16.72.0/29, de 172.16.72.0 (dir. red) a 172.16.72.7 (dir. difusión), con R1=172.16.72.1, R2=172.16.72.2, R3=172.16.72.3, R4=172.16.72.4
Red R4-R5: 172.16.72.8/30, de 172.16.72.8 (dir. red) a 172.16.72.11 (dir. difusión), con R4=172.16.72.9, R5=172.16.72.10

Como se observa, de esta forma no se desperdicia ningún rango de direcciones y se puede comprobar fácilmente que las redes están correctamente definidas (todos los bits de la parte de equipo a 0).

b) Como se ha explicado, para redes de 8192 direcciones necesitamos 13 bits para equipo (2^13 = 8192). Como tenemos asignado un rango (172.16.0.0/16) con 16 bits para equipo (32 - 16 bits para red = 16 bits para equipo), tenemos 16 - 13 = 3 bits para definir redes. Para visualizarlo mejor, ponemos este rango con colores: 10101100.00010000.XYZ00000.0000000. XYZ son esos 3 bits que nos permiten definir las redes de 8192 direcciones. Con la asignación de direcciones indicada en el apartado a), ya hemos utilizado XYZ =000 (de 172.16.0.0 a 172.16.31.255), XYZ =001 (172.16.32.0 a 172.16.63.255) y parte de XYZ=010 (172.16.64.0 a 172.16.72.10). Es decir, de 2^3 = 8 posibles redes, ya hemos utilizado 3. Eso hace que podamos definir 8 - 3 = 5 redes de 8192 direcciones que aún quedan libres (las correspondientes a XYZ = 011, 100, 101, 110 y 111). Estas corresponderían con las direcciones de red 172.16.96.0/19, 172.16.128.0/19, 172.16.160.0/19, 172.16.192.0/19 y 172.16.224.0/19.

c) Tabla de encaminamiento de R1:

Hay que incluir las rutas a las redes directamente conectadas (rutas directas), las rutas para llegar al resto de las redes en la topología (rutas indirectas) y una ruta por defecto para llegar al resto de redes en Internet. En este ejercicio, el único posible agrupamiento (que no exigía el enunciado del problema) sería el de las LANs C y D, ya que el siguiente salto es común (router R4). El resto de redes no tiene un siguiente salto común, por lo que no se podrían agrupar rutas.

Dir. destino	Máscara	Siguiente salto	Comentario
172.16.0.0	/19	*	LAN A, ruta directa
172.16.72.0	/29	*	Red R1-R2-R3-R4, ruta directa
80.80.80.0	/24	*	Red entre R1 y la pasarela del operador. Suponemos, por ejemplo, máscara /24.
172.16.32.0	/19	172.16.72.2	LAN E a través de R2
172.16.64.0	/22	172.16.72.3	LAN B a través de R3
172.16.68.0	/22	172.16.72.4	LANs C y D a través de R4
0.0.0.0	/0	80.80.80.x	Ruta por defecto a través de la pasarela del operador, cuya dirección no indica el enunciado del problema pero debe estar en la misma red que el router R1 en su interfaz hacia Internet, por lo que le suponemos la dirección 80.80.80.x.

d) Tabla de encaminamiento de R3

Siguiendo la misma lógica que en el apartado anterior:

Dir. destino	Máscara	Siguiente salto	Comentario
172.16.64.0	/22	*	LAN B, ruta directa
172.16.72.0	/29	*	Red R1-R2-R3-R4, ruta directa
172.16.0.0	/19	172.16.72.1	LAN A a través de R1
172.16.32.0	/19	172.16.72.2	LAN E a través de R2
172.16.68.0	/22	172.16.72.4	LANs C y D a través de R4
0.0.0.0	/0	172.16.72.1	Ruta por defecto a través de R1

e) Tabla de encaminamiento de un host de la LAN E para que solo pueda acceder a los hosts de las LANs C y D.

Si pusiésemos una ruta por defecto a través de R2, no podríamos garantizar que se cumplen los requisitos que indica el enunciado (solo acceder a los equipos de las LANs C y D), ya que se dependería de lo que contuviese la tabla de encaminamiento del router R2, que no conocemos. Por tanto, tenemos que incluir:

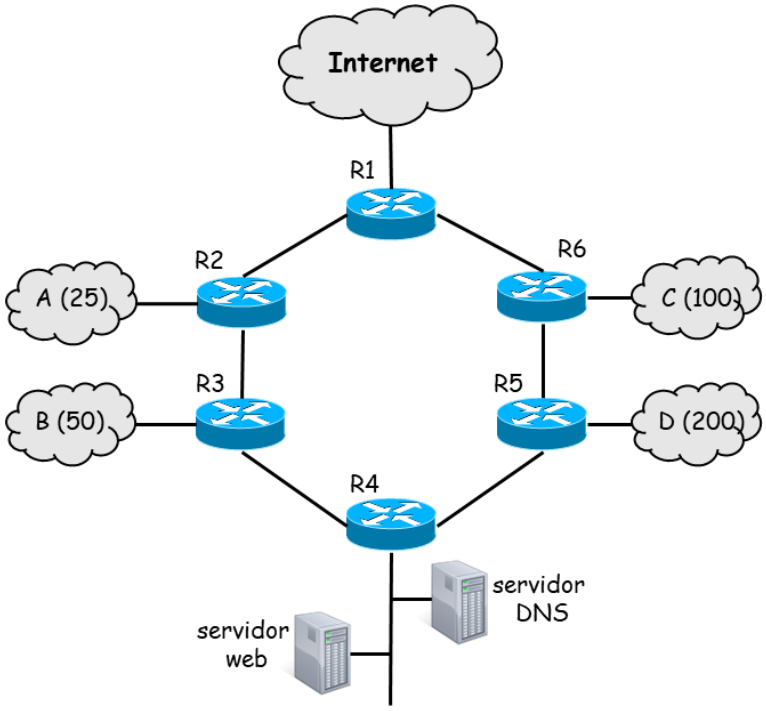
- Una entrada para llegar a la red directamente conectada
- Una entrada para llegar a las LANs C y D a través de R2 (se podrían poner dos entradas, el enunciado no indica que se agrupen)

Así, la tabla sería:

Dir. destino	Máscara	Siguiente salto	Comentario
172.16.32.0	/19	*	LAN E, ruta directa
172.16.68.0	/22	172.16.32.1	LANs C y D a través de R2

PROBLEMA 2 (3 puntos sobre 10)

En la imagen se muestra la topología de una red que incluye varias LAN, cada una de ellas con el número de equipos expresado entre paréntesis. Respecto a esta red, responda **razonadamente** a los siguientes apartados:



a) Indique los **errores que detecta** en la siguiente asignación de direcciones:

- Red A: 192.168.0.0/27
- Red B: 192.168.0.32/26
- Red C: 192.168.0.96/25
- Red D: 192.168.0.224/24
- Red R1-R2: 192.168.1.224/30
- Red R2-R3: 192.168.1.228/30
- Red R3-R4: 192.168.1.232/30
- Red R4-R5: 192.168.1.236/30
- Red R5-R6: 192.168.1.240/30
- Red R6-R1: 192.168.1.244/30
- Red R4-servidores: 192.168.1.248/30

b) Ahora suponga que **los routers solo incluyen en sus tablas de encaminamiento cómo llegar a las redes directamente conectadas**. En t=0 todos los routers activan **RIP**, el router R4 tiene configurado cómo llegar a una red X con un coste 5 y R5 tiene configurado cómo llegar a la misma red X con un coste 10. Indique **cómo llegará el router R1 a la red X**, incluyendo coste y a través de qué router, en los **instantes t=0, t=30, t=60 y t=90 segundos**.

Solución:

a) En este apartado:

- La red A es correcta. Iría de 192.168.0.0 a 192.168.0.31.
- La red B es incorrecta, ya que contiene un 1 (en binario) en la parte de equipo según la máscara /26 à 26 bits para definir la red y los 6 restantes para definir el equipo. 32 en binario es 00100000 (bits de red bits de equipo), por lo que no es una dirección de red válida (que debe tener a 0 todos los bits de equipo). De hecho, esta red se utilizara en una tabla de encaminamiento, al hacer AND con la máscara y una dirección de destino perteneciente

a dicha red, saldría la dirección de red 192.168.0.0/26 (que solaparía con la red A, ya que iría de 192.168.0.0 a 192.168.0.63).
- La red C también es incorrecta por el mismo motivo (96 en binario es 01100000, por lo que hay dos bits a uno en la parte de equipo). Haciendo la AND con la máscara saldría 192.168.0.0/25, errónea como en el caso anterior.
- Ídem para la red D (224 en binario es 11100000, por lo que hay tres bits a uno en la parte de equipo en esta red mal definida).
- Las redes entre routers son correctas (con una máscara /30 hay sitio para dos routers y todas las direcciones de red tienen los dos últimos bits a 0, como debe ser con dicha máscara).
- La red R4-servidores es incorrecta porque se necesitan 2 (servidores) + 1 (router) + 1 (red) + 1 (difusión) = 5 direcciones, por lo que la máscara debería ser /29. Con esa máscara sí sería correcta, ya que el último byte (248) tiene los tres últimos bits a 0 (11111000).

b) Veamos cómo RIP iría propagando las rutas al mandar sus mensajes periódicos cada 30 segundos y usar como métrica el número de saltos (entre routers) para llegar a la red X:

- En t=0, R5 manda su información a sus vecinos R6 y R4. R6 aprende que puede llegar a través de R5 a la red X con un coste 11 (10+1). R4 no actualiza su entrada para llegar a la red X ya que sabía llegar con un coste inferior (solo se aprende una ruta nueva si se mejora el coste, no si se iguala o se empeora). Seguidamente, R4 manda su información a sus vecinos R3 y R5, que aprenden que pueden llegar a la red X a través de R4 con un coste 6 (5+1). R5 lo aprende porque sí mejora el coste en dicha ruta. En este punto, R1 todavía no sabe llegar a la red X.
- En t=30, R6 manda su información a sus vecinos R1 y R5. R1 aprende que llega a la red X a través de R6 con un coste 12 (11+1) y R5 no aprende esta información porque sabe llegar con un coste inferior. Seguidamente, R3 manda esta información a sus vecinos R2 y R4. R2 aprende esta ruta (llegar a la red X por R3 con un coste 7=6+1). Igualmente, R5 manda una información similar a R6 y R4. Así, R6 aprende que puede llegar a la red X por R5 con un coste 7 (6+1). R4 no actualiza la ruta porque su ruta actual tiene un coste inferior. Al final de este punto, como se ha comentado, R1 sabe llegar a la red X a través de R6 con un coste 12.
- En t=60, el proceso es similar, y R1 aprende (de R2 o R6, quien mande primero el mensaje RIP) a llegar a la red X con un coste 8 (7+1).
- En t=90 ya no hay más actualizaciones por parte de R1 (no aprende nada nuevo con un coste inferior), por lo que la ruta se mantiene.
Siguiendo este razonamiento para todos los nodos, tenemos:

	R1		**R2**		**R3**		**R4**		**R5**		**R6**	
	coste	**siguiente salto**	**coste**	**siguiente salto**	**coste**	**siguiente salto**	**coste**	**siguiente salto**	**coste**	**siguiente salto**	**coste**	**siguiente salto**
t=0	**-**	**-**	**-**	**-**	**6**	**R4**	**5**	[en su tabla inicialmente]	**10**	[en su tabla inicialmente]	**11**	**R5**
t=30	**12**	**R6**	**7**	**R3**	**6**	**R4**	**5**	[en su tabla inicialmente]	**6**	**R4**	**11**	**R5**
t=60	**8**	**R2**	**7**	**R3**	**6**	**R4**	**5**	[en su tabla inicialmente]	**6**	**R4**	**7**	**R5**
t=90	"	"	"	"	"	"	"	"	"	"	"	"

Si alguien supone que en t=0 no se envía ningún mensaje, todo se movería 30 segundos hacia delante.

Contestar las siguientes preguntas usando exclusivamente los huecos reservados.

P1 (1 punto sobre 10) Enumere las diferencias y similitudes entre los protocolos HTTP y IMAP.
Diferencias:

- HTTP se utiliza para solicitar y servir páginas web y IMAP para recepción de e-mails
- HTTP es stateless e IMAP no
- HTTP puede ser persistente o no. IMAP no es ni persistente ni no persistente
- HTTP usa puerto 80, IMAP puerto 143
- HTTP usa cookies, IMAP no
- HTTP gestiona proxies/cache, IMAP no
- HTTP es orientado a conexión, IMAP no

Similitudes:

- Son orientados a texto
- No son seguros/no proporcionan confidencialidad
- Son cliente/servidor
- Usan TCP
- Son de la capa de aplicación
- Son in-band
- Ambos usan extensiones MIME

P2 (1,5 puntos sobre 10). Explique cómo funciona el control de errores en TCP. ¿Qué parámetro es fundamental en el rendimiento del control de errores y cómo se adapta durante una conexión?

TCP numera todos los segmentos y exige confirmaciones ACK positivas y acumulativas con piggyback. El emisor guarda una copia local de cada segmento enviado en la ventana de emisión, e inicia un temporizador, si el temporizador expira, el emisor vuelve a retransmitir el segmento correspondiente. Además, el emisor por cada segmento calcula un checksum (un código de paridad) que es añadido en la cabecera, tal que el receptor pueda descartar errores simples. El receptor habilita una ventana de recepción abierta para los números de secuencia que espera recibir. Si se recibe un segmento con número de secuencia fuera de la ventana de recepción, el segmento se descarta. Si se recibe el segmento dentro de la ventana de recepción se acepta y si llega en orden y sin errores se pasa a la aplicación y se confirma. En régimen estacionario TCP confirma acumulativamente de 2 en 2 segmentos, aunque puede confirmar segmentos aislados tras esperar 500 msegundos en el receptor a que llegue otro segmento contiguo. Si se recibe un segmento desordenado pero sin errores se almacena temporalmente en la ventana de recepción, no se pasa a la aplicación pero se confirma el último segmento correctamente recibido. [Aquí habría que explicar bien los 4 casos para la generación de ACKs vistos en teoría.]
El parámetro fundamental que impacta en el rendimiento es el timeout del emisor. Este por cada segmento enviado habilita un temporizador y por cada ACK recibido estima el RTT como una media móvil
RTT_Estimado = alfa * RTT_Old + (1 - alfa) * RTT_Medido, alfa y beta en [0, 1]
Error_Estimado = beta * Error_Old + (1- beta) * | RTT_Estimado – RT_Medido|
Finalmente, se calcula TIME-OUT = RTT_estimado * 4 Error_Estimado

Para evitar ambigüedades, cuando se produce un timeout el algoritmo de karn especifica que el TIMEOUT se doble.

P3 (1,5 puntos sobre 10). A y B no se conocen y quieren intercambiar mensajes a través de un canal no seguro. Suponga que disponen de certificados digitales expedidos por una autoridad de confianza.
A) Explique el procedimiento para autenticarse mutuamente identificando claramente los mensajes que deban intercambiar. ¿Qué es y qué debe contener el certificado digital?
B) Si no dispusieran de certificados, pero sí de una clave secreta compartida, ¿cómo podrían autenticarse? Identifique claramente los requisitos y posibles debilidades.

a) Para autenticarse mutuamente A envía a B el mensaje cifrado con su clave privada (K_PRIV_A) y B hace los mismo hacia A cifrando con su clave privada (K_PRIV_B). El certificado digital es la asociación fehaciente e irrevocable de una entidad A con su clave pública. Debe contener la identidad A, su clave pública, y una fecha de expiración (validez) todo ello cifrado con la clave privada de una autoridad reconocida K_PRIV_AUT(A, K_PUB_A, validez). En este caso A y B quedan autenticadas ya que se supone la hipótesis de que la clave privadas solo las conocen las entidades correspondientes y al usar el certificad la AUTORIDAD nos garantiza la asociación fehaciente e irrevocable de la entidad con su clave pública y por ende con su clave privada

b) Suponiendo la hipótesis de la existencia de una clave secreta compartida se pueden autenticar con RETO_RESPUESTA, pero ojo hay que tomar medidas para evitar los ataques por reflexión, usando conjuntos de retos disjuntos y marcas de tiempo (*nonce*) que eviten los ataques por repetición.