Las debilidades se han explicado en los párrafos anteriores. Las posibles soluciones serían conseguir confidencialidad en todos los mensajes (e.g. usando la clave pública del receptor), autenticación (e.g. usando la clave privada del emisor), integridad (e.g. añadiendo resúmenes con MD5 de los mensajes enviados) y no repudio (se consigue también al usar, por ejemplo, la clave privada del emisor).

UNIVERSIDAD DE GRANADA

Departamento de Teoría de la Señal, Telemática y Comunicaciones

FUNDAMENTOS DE REDES

– 3er curso del Grado en Ingeniería Informática (y dobles grados) –

Convocatoria ordinaria (1 de febrero de 2021)

Apellidos y nombre:

Titulación / grupo:

ENTREGA:

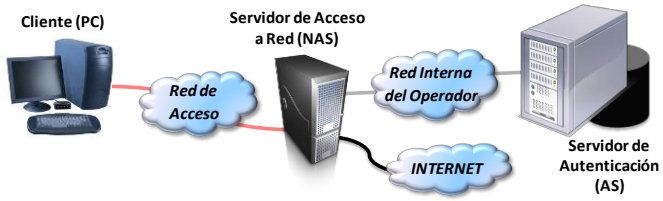
Haga la resolución de cada ejercicio en papel, escrito con bolígrafo de su puño y letra.

Después escanee o fotografíe los folios que desee que se evalúen, **INCLUYENDO SU DNI FÍSICO EN TODAS LAS PÁGINAS**. Preferiblemente todos juntos en un documento PDF.

Súbalo a la entrega en PRADO que se habrá habilitado durante la duración del examen, en los 10 minutos habilitados para la entrega.

PROBLEMA 1-A (3 puntos sobre 10)

La figura y mensajes siguientes describen un protocolo utilizado para permitir el acceso de un cliente a Internet a través de un Servidor de Acceso a Red (NAS). El Servidor de Autenticación (AS) guarda en una base de datos las claves secretas que se solicita a los usuarios para poder acceder a Internet.



PC → NAS: peticion_acceso + usuario
NAS → PC: desafio
PC → NAS: usuario + K_{PC-AS}(desafio)
NAS → AS: peticion_autenticacion + usuario + K_{PC-AS}(desafio)
AS → NAS: peticion_aceptada + $Ksesion_{PC-NAS}$ + K_{PC-AS}($Ksesion_{PC-NAS}$)
(o peticion_rechazada)
NAS → PC: peticion_aceptada + K_{PC-AS}($Ksesion_{PC-NAS}$)
(o peticion_rechazada)
PC → NAS: $Ksesion_{PC-NAS}$ (datos_a_enviar) + MD5($Ksesion_{PC-NAS}$ (datos_a_enviar))
NAS → hacia Internet: datos_a_enviar
Desde Internet → NAS: datos_de_respuesta
NAS → PC: $Ksesion_{PC-NAS}$ (datos_de_respuesta) + MD5($Ksesion_{PC-NAS}$ (datos_de_respuesta))

Siendo:

- $Kpub_X$ (P) → cifrado de P con la clave pública de X
- $Kpriv_X$ (P) → cifrado de P con la clave privada de X
- K_{X-Y} (P) → cifrado de P con la clave secreta entre X e Y
- K_{X-Y} → clave secreta entre X e Y
- MD5 → función *hash*

a) Indique qué servicios de seguridad se proporcionan (confidencialidad, autenticación, integridad y no repudio) y entre qué elementos (PC, NAS, AS). Explique detalladamente su respuesta.
b) ¿Qué debilidades presenta el esquema propuesto? En su caso, ¿cómo podrían evitarse?

NOTA: Responda razonadamente a las cuestiones.

Ejercicio de Seguridad

Los aspectos de seguridad son 5: confidencialidad, autenticación, integridad, no repudio y disponibilidad. Respecto a este último punto, disponibilidad, no se puede dar información porque no se conocen aspectos como la infraestructura física, elementos redundantes, etc.

Este procedimiento persigue que un usuario (cliente) se autentique frente a un servidor de autenticación (AS) para ver si tiene derecho a acceder a Internet a través de un servidor de acceso a red (NAS). Es un esquema típico que utilizan los ISPs. Básicamente el cliente le manda una petición al NAS, que le responde con un desafío. El cliente manda dicho desafío cifrado con la clave secreta entre el PC y el AS, que es reenviado por el NAS al AS. Si este desafío cifrado coincide con lo que calcula el AS, le devuelve que la petición ha sido aceptada. Si no, se rechaza. En el mensaje de sesión aceptada, AS manda a NAS la clave de sesión entre el PC y el NAS (sin cifrar y cifrada con la clave secreta entre PC y AS). NAS se la reenvía a PC (cifrada con la clave secreta entre PC y AS). Así, tanto PC como NAS conocen dicha clave de sesión que usarán después para enviar entre ellos los datos que van/vienen de Internet.

Respecto a confidencialidad:

- La petición inicial entre PC y NAS va sin cifrar, por lo que cualquiera puede ver esos datos (petición y usuario).
- La respuesta al desafío (K_{PC-AS}(desafio)) no incluye ningún *nonce* o elemento que no se repita, por lo que es susceptible de ataques por repetición.
- La información entre NAS y AS va sin cifrar, por lo que un trabajador del ISP podría ver todos esos mensajes y la información enviada.
- La clave de sesión sí se envía cifrada entre NAS y PC, por lo que no podría ser vista por alguien externo en ese enlace (sí entre AS y NAS, donde se envía sin ir cifrada).
- Los datos desde el PC al NAS y viceversa (respuestas) sí van cifradas con una clave de sesión. Hacia Internet estos datos van sin cifrar.

Respecto a la autenticación:

- El procedimiento persigue que el PC se autentique frente al AS enviando una prueba de ello (el desafío cifrado con la clave secreta compartida entre el PC y el AS).
- El NAS se fía de la respuesta (peticion_aceptada o peticion_rechazada) enviada por el AS. Esto puede ser problemático porque el AS no se autentica frente al NAS (no hay ningún procedimiento para ello, ni cifra los mensajes con su clave privada para que el otro descifre con la pública, ni nada similar).
- NAS no se autentica con el PC. Tampoco se autentican NAS y AS entre ellos.

Respecto a la integridad: solo se incluye un resumen (a través de la función *hash* MD5) de los datos enviados y sus respuestas entre PC y NAS. Eso significa que esos mensajes no pueden ser modificados sin que nos demos cuenta. El resto de mensajes no tienen ningún resumen por lo que podrían ser modificados sin que nos diésemos cuenta.

Respecto al no repudio: no hay ninguna prueba (e.g. por haber cifrado algo con mi clave pública y que pueda ser descifrado por cualquiera con mi clave privada) de que hemos participado en esta transacción. Incluso los mensajes cifrados con la clave secreta o de sesión no servirían, ya que puede haberlos cifrado cualquiera de los dos extremos (no serviría de prueba frente a un juez).

UNIVERSIDAD DE GRANADA

Departamento de Teoría de la Señal, Telemática y Comunicaciones

FUNDAMENTOS DE REDES

– 3er curso del Grado en Ingeniería Informática (y dobles grados) –

Convocatoria ordinaria (1 de febrero de 2021)

Apellidos y nombre:
Titulación / grupo::

INSTRUCCIONES:

En la resolución indique su nombre, apellidos, DNI/Pasaporte (que comprobaremos en su ficha de estudiante) y la IP DE DNI DE ESTUDIANTE.

Partiendo de su DNI, construya una dirección IP de la siguiente forma:

- Cada par de dígitos serán uno de los números en formato decimal de la IP. Por ejemplo, si su DNI es 77330055-G, la dirección IP será 77.33.0.55.
- La máscara se le indicará en el ejercicio, a partir de la cual podrá calcular la dirección de red correspondiente a esa IP (tendrá todos los bits a 0 según indican los bits de la máscara).

** Los estudiantes con pasaporte pueden construir la IP de la misma forma (usando los primeros 8 dígitos del mismo) **

ENTREGA:

Haga la resolución de cada ejercicio en papel, escrito con bolígrafo de su puño y letra.

Después escanee o fotografíe los folios que desee que se evalúen, **INCLUYENDO SU DNI FÍSICO EN TODAS LAS PÁGINAS**. Preferiblemente todos juntos en un documento PDF.

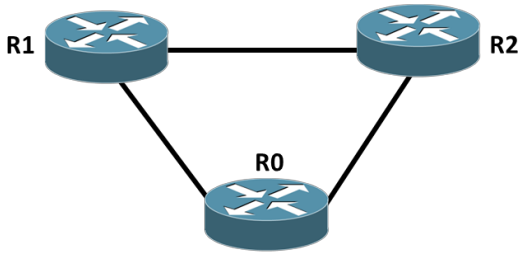
Súbalo a la entrega en PRADO que se habrá habilitado durante la duración del examen, en los 10 minutos habilitados para la entrega.

PROBLEMA 2 (3 puntos sobre 10)

Una empresa tiene cuatro subredes, cada una de ellas tiene conectados el siguiente número de equipos (indicado entre paréntesis): A(55), B(28), C(12), D(7). Se dispone del rango público indicado por SU IP DE DNI DE ESTUDIANTE con máscara /24.

a) Proponga un **esquema de asignación de direcciones** que cubra a todos los equipos de cada subred y a los routers que tenga conectados. Intente crear redes agrupables para minimizar el tamaño de las tablas de encaminamiento.

b) Muestre una **topología con las subredes** y sus direcciones (y máscara) correspondientes a partir de este esquema de 3 routers. Conéctelas como prefiera a R0, R1 y R2, hasta un máximo de dos subredes por router. Dibuje también Internet y conecte uno de los routers.



c) Asigne **direcciones a cada una de las interfaces** de los routers. Para el router conectado a Internet puede elegir una dirección IP pública cualquiera.

d) Defina las **tablas de encaminamiento** de los tres routers, suponiendo que se ha seguido el esquema de direccionamiento definido anteriormente. Minimice el número de entradas en las mismas haciendo agrupaciones.

NOTA: Responda razonadamente a las cuestiones.

ASIGNACIÓN IPs (EXAMEN)

11.22.33.0/24

a) La red más pequeña es D - 7 hosts + $\begin{cases} \text{red} \\ \text{difusión} \end{cases}$ + router = 10 IPs

$2^4 = 16$ IPs

A (55) ⇒ 4 subredes × 16 IPs = 64 IPs

11.22.33.0 /28
11.22.33.16 /28
11.22.33.32 /28
11.22.33.48 /28
} 11.22.33.0/26

red: 11.22.33.0 /28
difusión: 11.22.33.63 /28

B (28) ⇒ 2 × 16 IPs = 32 IPs

11.22.33.64 /28
11.22.33.80 /28
} 11.22.33.64/27

red: 11.22.33.64/28
difusión: 11.22.33.95/28

A y B
11.22.33.0/25

C (12) ⇒ 1 × 16 IPs = 16 IPs

11.22.33.96 /28

red: 11.22.33.96/28
df.: 11.22.33.111/28

D (7) ⇒ 1 × 16 IPs = 16 IPs

11.22.33.112 /28

red: 11.22.33.112 /28
df: 11.22.33.127/28

C y D
11.22.33.96/26

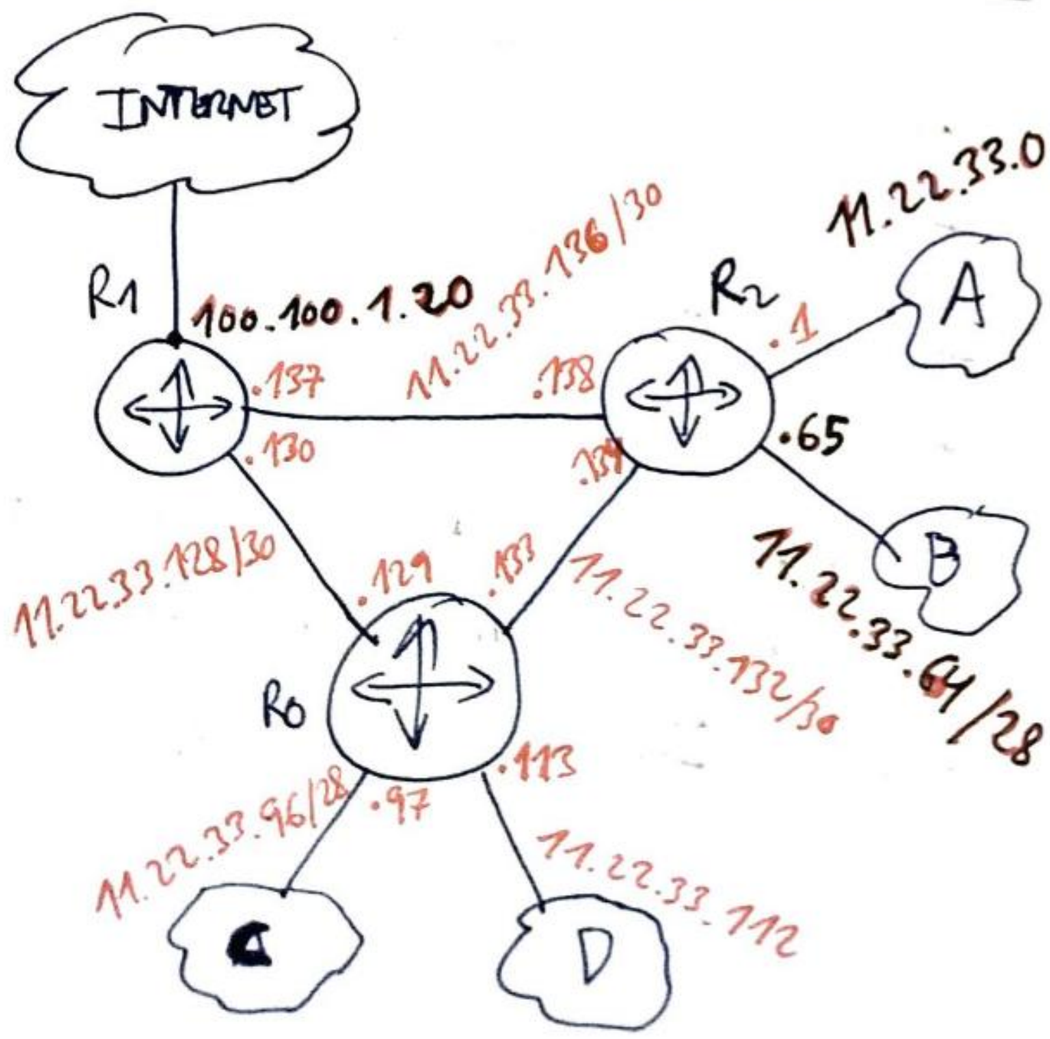
R0-R1
11.22.33.128/30

R0-R2
11.22.33.132/30

R1-R2
11.22.33.136/30

b)

c)



d)

TABLA R0

Destino	Máscara	Siguiente	
11.22.33.96	/28	*	Red C
11.22.33.112	/28	*	Red D
11.22.33.128	/30	*	Red R0-R1
11.22.33.132	/30	*	Red R0-R2
11.22.33.0	/25	11.22.33.134 (R2)	Redes A y B
11.22.33.136	/30	11.22.33.130 (R1)	Red R1-R2 } se podrían agrupar en 'default'
default	—	11.22.33.130 (R1)	Internet }

TABLA R1

Destino	Máscara	Siguiente	
100.100.1.0[illegible]	/24	*	[illegible] Internet (ISP)
11.22.33.128	/30	*	Red R0-R1
11.22.33.136	/30	*	Red R1-R2
11.22.33.0	/25	11.22.33.138(R2)	Redes A y B
11.22.33.96	/26	11.22.33.129(R0)	Redes C y D } se podrían agrupar en
11.22.33.132	/30	11.22.33.129(R0)	Red R0-R2 } 11.22.33.0/24 ⇒ para toda el rango de direcciones disponibles

TABLA R2

Destino	Máscara	Siguiente	
11.22.33.132	/30	*	Red R0-R2
11.22.33.136	/30	*	Red R1-R2
11.22.33.0	/28	*	Red A
11.22.33.64	/28	*	Red B
11.22.33.96	/26	11.22.33.133(R0)	Redes C y D } se podrían agrupar en
11.22.33.128	/30	11.22.33.133(R0)	Red R0-R1 } 11.22.33.0/24 ⇒ IDEM
default	—	11.22.33.137(R1)	Internet / cambiando 'siguiente' por R1, se podrían agrupar en 'default'