TRANSMISIÓN DE DATOS Y REDES DE COMPUTADORES II

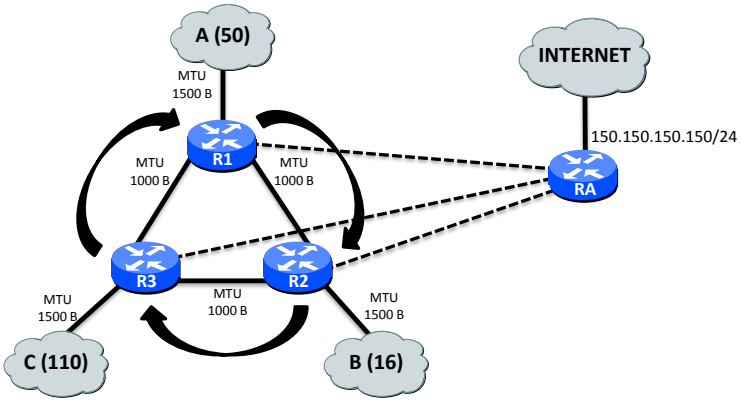
Examen de Teoría[1]

Septiembre de 2011

APELLIDOS, NOMBRE: **GRUPO:**

---

1. (*2.5 puntos*) La siguiente figura muestra la topología de red de una empresa, que tiene contratado con su ISP el rango de direcciones 15.16.17.0/24. El número de ordenadores conectados a las redes A, B y C están indicados en la figura entre paréntesis.



a) Realice la asignación de direcciones IP tanto de equipos como de routers (incluyendo las redes entre los routers), utilizando direcciones públicas siempre que sea posible.

b) Indique las tablas de encaminamiento de todos los routers de forma que, para el tráfico entre las redes A, B y C, se encamine de acuerdo a las flechas en la figura). Debe haber conectividad completa entre estas redes y hacia Internet.

c) Suponga que el router R_A tiene funcionalidad de servidor DNS. Describa el intercambio de tramas si un ordenador de la red A quiere enviar un *ping* a un ordenador de la red C a través de su nombre de dominio (petición y respuesta con tamaño inferior a 1000 bytes). Tanto el mensaje de petición como el de respuesta del *ping* tienen un tamaño de 2000 bytes (incluyendo las cabeceras del nivel de red). Indique (si procede): direcciones físicas de origen y destino, direcciones IP de origen y destino, protocolo, puertos de origen y destino, flags, números de secuencia y acuse, y el tipo de mensaje.

2. (*2 puntos*) Explique las diferencias en objetivos y funcionamiento entre el control de flujo y el control de congestión en TCP. ¿Cómo ayudan los routers en el control de congestión de TCP? ¿Y en el control de flujo?

3. (*2.5 puntos*) 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: $Kpub_{NAS}$ (peticion_acceso + usuario)
NAS → PC: desafio
PC → NAS: $Kpub_{NAS}$(MD5(usuario:K_{PC-AS}:desafio))
NAS → AS: peticion_autenticacion + usuario + desafio + MD5(usuario:K_{AS-PC}:desafio))
AS → NAS: peticion_aceptada + $Ksesion_{PC-NAS}$ + K_{PC-AS}($Ksesion_{PC-NAS}$)
(ó peticion_rechazada)
NAS → PC: $Kpriv_{NAS}$ (peticion_aceptada + K_{PC-AS}($Ksesion_{PC-NAS}$))
(ó $Kpriv_{NAS}$ (peticion_rechazada))
PC → NAS: $Ksesion_{PC-NAS}$ (datos_a_enviar)
NAS → hacia Internet: datos_a_enviar
Desde Internet → NAS: datos_de_respuesta
NAS → PC: $Ksesion_{PC-NAS}$ (datos_de_respuesta)

Siendo:

- $Kpub_X$ cifrado con la clave pública de X
- $Kpriv_X$ cifrado con la clave privada de X
- K_{X-Y} la clave secreta entre X e Y
- MD5 es una función *hash*

Suponiendo que las claves públicas corresponden a certificados digitales emitidos por una autoridad reconocida,

a) ¿Qué servicios de seguridad se proporcionan en el protocolo descrito?
b) ¿Qué debilidades presenta el esquema propuesto? En su caso, ¿cómo podrían evitarse?

[1] Esta prueba supone el 70% de la calificación final de la asignatura.