TRANSMISIÓN DE DATOS Y REDES DE ORDENADORES

Examen de Teoría[1]

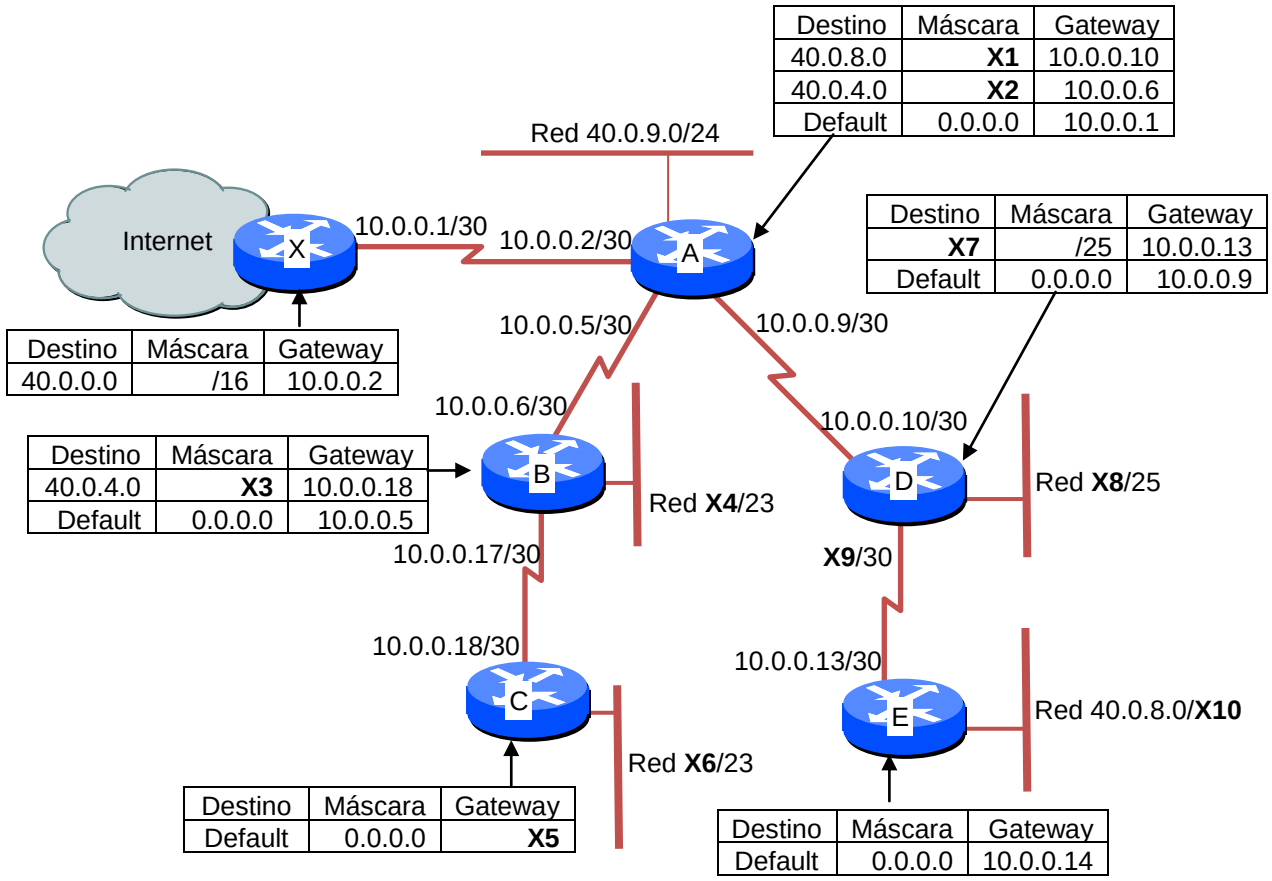
Junio de 2013

APELLIDOS, NOMBRE:

PROFESOR DE TEORÍA:

---

1. (*3 puntos*) En la red de la siguiente figura se muestra la configuración incompleta de una red:



a) Complete los datos marcados en la figura como **X1** a **X10**. Justifique las respuestas.
b) Los *routers* A,B,C,D,E,X ¿Necesitarán más entradas en sus tablas de encaminamiento? En caso afirmativo indíquelas.
c) Suponga que instala un servidor de HTTP con dirección 40.0.9.1. ¿Es necesario instalar un NAT? En caso afirmativo indique dónde y cómo sería su tabla de asignación de puertos.
d) Suponga que ejecuta ping 40.0.9.1 desde una máquina en 40.0.8.1. Indique las IPs origen y destino, y el contenido de los paquetes generados.

Solución: expuesta en el examen de Junio de 2012 (ejercicio 1)

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?

Solución: expuesta en el examen de Septiembre de 2011 (ejercicio 2)

3. (*2 puntos*) Suponga un protocolo que por cada mensaje en texto plano M, envía $(M, H(M) \oplus K_S)$, donde
H(x) es un compendio o Hash de x
$(a \oplus b)$ es la X-OR de a y b
K_s es una clave secreta compartida entre los dos extremos.

---

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

¿Qué aspectos de seguridad y cuáles no garantiza? Justifique la respuesta y proponga en su caso una alternativa –con las mismas herramientas– que sea más segura.

Confidencialidad: No, ya que el mensaje se envía en texto plano

Autenticación: Inicialmente se podría pensar que sí, ya que es necesario conocer la clave de sesión para realizar la operación ⊕. Pero cualquiera puede obtener esa clave a partir de escuchar mensajes de este tipo, ya que cualquiera puede calcular H(M) (M se envía como texto plano), y realizando la operación ⊕ con el dato enviado en el mensaje (H(M) ⊕ Ks) se obtiene Ks directamente. Por tanto, hay un problema de seguridad serio ya que cualquiera ve el mensaje en texto plano y cualquiera puede obtener Ks a partir de un mensaje escuchado.

Integridad: Igual que en la autenticación, se podría pensar que sí ya que se envía un resumen. Pero si alguien modifica el mensaje, también es capaz de modificar la función hash y hacer la operación ⊕ con la clave Ks obtenida, por lo que no se garantiza la integridad.

No repudio: No hay nada que implique el no repudio (prueba que confirme que se participó en la transacción), aunque no fuese posible obtener la clave Ks (que sí se puede obtener).

Disponibilidad: No hay datos sobre redundancia de redes, de equipos, … No podemos decir nada de este aspecto.

Alternativa más segura:

En primer lugar, no enviaremos el texto plano. De esta forma, no se puede calcular su función hash y por tanto no se puede conseguir la clave secreta Ks. Sin embargo, tendríamos que incluir algo ya que, si no, no estamos mandando el mensaje (sólo un resumen del que es imposible obtener el mensaje).

Para enviar el mensaje cifrado (y conseguir así la confidencialidad), se podría realizar la función ⊕ con Ks (repitiendo Ks las veces necesarias para que tuviese el mismo número de bits que el mensaje en texto plano). Esto proporcionaría confidencialidad, aunque sería susceptible de un ataque estadístico (si bien, al no conocerse la longitud de Ks, puede que fuese complicado).

Al ser necesario conocer Ks, se proporciona autenticación (sólo la conocen el emisor y el receptor).

Al incluir un resumen (H(M), sea operado o no con Ks mediante ⊕), se consigue integridad.

El no repudio no sería sencillo de conseguir únicamente con estas herramientas (⊕, Ks y H()). Harían falta otras herramientas como entidades fiables (e.g. Big Brother) o claves públicas.

Sobre disponibilidad no se puede decir nada con los datos dados.