

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN
REDES DE COMPUTADORES
SEGUNDA EVALUACIÓN - I TÉRMINO 2014

Nombre: _____ **Matrícula:** _____

Sección A

1. Con respecto al servicio que proveen los protocolos *Transmission Control Protocol* (TCP) y *User Datagram Protocol* (UDP):
 - a. ¿Cuál es la diferencia en el servicio ofrecido a aplicaciones por los protocolos TCP y UDP? **[4%]**
 - b. Para cada una de las siguientes aplicaciones determine si usted usaría TCP o UDP y explique las razones para su selección. **[8%]**
 - i. Transferencia de archivos
 - ii. Ver un video transmitido en tiempo real
 - iii. Navegar por la Web
 - iv. Una conversación telefónica de voz sobre IP (VoIP)
 - c. Tanto TCP como UDP proveen números de puerto. ¿Para qué se usan estos números de puerto? **[4%]**
 - d. Un usuario desea establecer una conexión desde su laptop hacia un servidor por medio del Internet usando el protocolo TCP. Considerando los mensajes que TCP genera, explique ¿cómo se establece un circuito virtual entre la laptop y el servidor usando TCP? **[4%]**
2. Explique en qué consiste el mecanismo *network address translation* (NAT). Describa la estructura de la tabla de traducción para cada una de las estrategias de traducción. Señale las limitaciones en cada caso. **[12%]**
3. Identifique y explique brevemente tres protocolos para mapeo de direcciones físicas a lógicas. **[6%]**
4. Indique las razones por las cuales el protocolo *Internet Control Message Protocol* (ICMP) fue diseñado. Esquematice la clasificación de tipos de mensaje y describa un tipo de mensaje ICMP en cada categoría. **[10%]**
5. Explique el uso del servicio DNS y describa los diferentes tipos de resolución. **[6%]**

Sección B

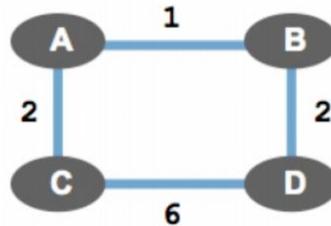
6. Confidencialidad, integridad y autenticación son tres características de comunicaciones seguras. Un sistema de red podría estar sujeto a amenazas a estas características por atacantes que explotan vulnerabilidades en el sistema de red. A fin de prevenir estos ataques nosotros implementamos controles sobre los servicios de seguridad.

Asuma que dos comunicadores, Alice y Bob, nunca se han conocido antes, ellos no confían entre sí y que Alice y Bob pueden usar cualquier sistema criptográfico y funciones de hash criptográficas. Ahora, Alice quiere enviar un mensaje largo a Bob. Conteste las siguientes preguntas (en su protocolo de diseño, usted debe indicar claramente cualquier asunción que realice y las operaciones desarrolladas por cada uno de los comunicadores).

- a. Diseñe un protocolo en el cual Alice pueda enviar este mensaje a Bob y solo Bob pueda descifrar el mensaje y los procesos de encriptación/descifrado sean los más eficientes. **[6%]**
- b. Diseñe un protocolo mediante el cual Alice pueda enviar un mensaje a cualquiera, y cualquiera que reciba el mensaje pueda estar seguro que el mensaje no es un *replay* de un mensaje previamente enviado y si es en verdad de Alice. **[6%]**
- c. Diseñe un protocolo en el que Alice pueda enviar un mensaje a Bob. El diseño del protocolo debe satisfacer los siguientes requerimientos: confidencialidad del mensaje, autenticación del origen, integridad y frescura están protegidos durante la transmisión, el protocolo es el

más eficiente en términos de costos de comunicación y Bob es menos vulnerable a ataques DoS (Denial of Service). En su diseño, usted debe justificar claramente cómo satisface cada requerimiento de diseño especificado. **[8%]**

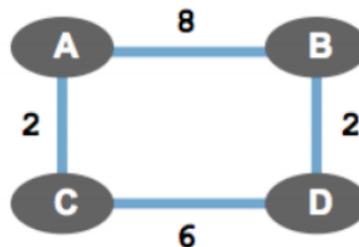
7. La siguiente pregunta considera una red de cuatro routers (A, B, C, D) que corren un protocolo de *distance vector* entre ellos. Los costos de los enlaces entre cada router son mostrados en la siguiente figura:



Dada la figura en la parte superior, calcule el camino más corto para cada router al router D. En la tabla en la parte inferior, escriba el siguiente salto en el camino más corto desde cada router hacia D, también conocido como camino más corto. **[12%]**

Router	Router del siguiente salto en el camino más corto a D	Costo del camino más corto desde el router hacia D
A		
B		
C		
D	D	0

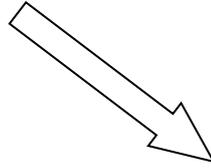
Ahora, asuma que el costo del enlace $A \leftrightarrow B$ se incrementa de 1 a 8. Escriba la serie de cambio de costos que A y C calculan (al calcular su camino más corto a D) mientras el protocolo converge nuevamente. Asuma que en una ronda dada, un nodo considerará cualquier actualización que reciba desde la ronda anterior, recalcula cualquier cambio de costo del camino y de ser necesario entrega la actualización a sus vecinos.



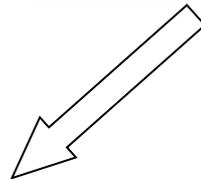
Inmediatamente después del cambio de costo del enlace, A actualiza su matriz de distancia y tabla de ruteo. En la parte inferior están cálculos que los nodos A y C harán durante cada ronda del algoritmo de *distance vector* basados en su cambio de costo del enlace o actualizaciones de vectores de distancia provenientes de sus vecinos. Para este problema, usted podría ignorar actualizaciones desde B y D y solo enfocarse en los intercambios de actualizaciones de vectores de distancia entre A y C.

Llene la serie de cálculos que pueden darse para A y C al calcular sus matrices de distancia y tablas de ruteo. Usted podría NO usar todas las tablas dadas. **[14%]**

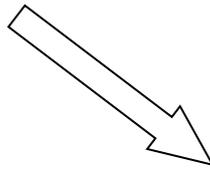
Costo del camino de A hacia D	Costo del camino
Por B	10
Por C	



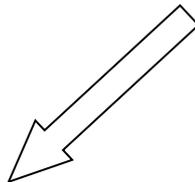
Costo del camino de C hacia D	Costo del camino
Por A	
Por D	



Costo del camino de A hacia D	Costo del camino
Por B	
Por C	



Costo del camino de C hacia D	Costo del camino
Por A	
Por D	



Costo del camino de A hacia D	Costo del camino
Por B	
Por C	