**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**

**FACULTY OF ELECTRICAL AND COMPUTER ENGINEERING**
**COMPUTER NETWORKS**
**SECOND EVALUATION - II TERM 2013**

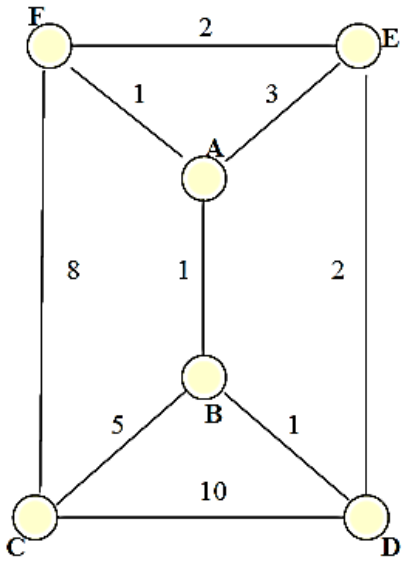
***Name:*** _____ ***Student ID:*** _____

***Section A***

1. Compare and contrast private, hybrid and virtual private networks. Show an example to represent each case. ***[12%]***
2. What was ICMP designed for? Briefly describe how each error reporting ICMP message type works. ***[12%]***
3. Briefly explain what is meant by IPSec and which its operating modes are. ***[6%]***
4. Name two well-known data transport protocols provided by the Internet Transport Layer. Provide a brief description of each service and indicate what type of application might use that service. ***[8%]***
5. What are cookies? Explain how they are used during a client-server HTPP exchange messages. Illustrate three usages for them. ***[8%]***
6. Briefly explain and illustrate with a diagram the components of an IDS architecture. Compare and contrast the schemes of the component responsible for analysing events to detect attacks. ***[8%]***

***Section B***

7. Suppose a distance vector algorithm is being run and it will converge to a stable solution on the network shown below. Describe step by step, how routing information is propagated between the different nodes. Draw the routing tables of all six nodes. ***[20%]***




Explain a couple of mechanisms used to solve the count-to-infinity problem. ***[6%]***



*MSc. Carlos Mera Gómez*

8. Alice (A) has decided to send a secure message (M) to Bob (B) by means of cryptographic methods. Alice has her own private ($SK_A$) and public ($PK_A$) keys. Bob also owns his corresponding private and public keys ($SK_B$ and $PK_B$). Analyse the following steps: ***[20%]***
   - Alice generates a session key $K_{AB}$
   - Alice encrypts the key $K_{AB}$ using her private key $SK_A$ and then she sends it to Bob: A→B: $\{K_{AB}\}SK_A$
   - Alice encrypts the message M with the key $K_{AB}$
   - Alice wants to provide non-repudiation (proof of data integrity and assert authentication). So, she calculates H = Hash (M) using a well-known hash function such as SHA-1.
   - Alice transmits the tuple ($\{M\}K_{AB}$, H)

   Identify two different errors Alice has made at using cryptographic methods and describe how to correct each of them.