ITEC451 Network Design and Analysis

Pre-Test

Name:

1. True or False: The International Organization for Standardization (ISO)'s Open System Interconnection (OSI) reference model partitions the communications process into seven layers and provides a framework for talking about the overall communications process. OSI reference model consists of (1) physical layer; (2) data link layer; (3) multiplexing layer; (4) network layer; (5) transport layer; (6) presentation layer; and (7) application layer.

2. True or False: Routing is included in the data link layer of OSI reference model.

3. True or False: Transmission Control Protocol/Internet Protocol (TCP/IP) network architecture consists of five layers.

4. True or False: User Datagram Protocol (UDP) is a reliable connection-oriented transfer of a byte stream.

5. True or False: Line coding is the method used for converting a binary information sequence into a digital signal in a digital communication system.

6. True or False: A simple method to improve the error-detection capability of a single parity check code is to arrange columns that consist of k information bits followed by a check bit at the bottom of each column.

7. True or False: Packet-switching networks provide dedicated circuits that enable the flow of information between users.

8. True or False: Wavelength-division multiplexing (WDM) can be viewed as an optical-domain version of time-division multiplexing (TDM) in which multiple information signals modulate optical signals at different optical wavelengths (colors).

9. True or False: Automatic Repeat Request (ARQ) combines error detection and retransmission to ensure that data is delivered accurately to the user despite errors that occur during transmission.

10. True or False: In centralized routing, each node continuously learns the state of the network by communicating with its neighbors. Thus a change in a network topology is eventually propagated to all nodes.

11. True or False: The principle of multicasting calls for a packet switch to forward an incoming packet to all ports except the one the packet was received from. Thus, multicasting may easily swamp the network as one packet creates multiple packets that in turn create multiples of multiple packets, generating an exponential growth rate.

12. True or False: The Bellman-Ford algorithm is based on the following principle: If each neighbor of node A knows the shortest path of node Z, then node A can determine its shortest path to node Z by calculating the cost/distance to node Z through each of its neighbors and picking the minimum.

13. True or False: Dijkstra's algorithm is an algorithm for finding the shortest paths from a source node to all other nodes in a network.

14. True or False: Using classless interdomain routing (CIDR) notation, a prefix 205.100.0.0 of length 22 is written as 205.100.0.0/22. The /22 notation indicates that the network mask is 22 bits, or 255.255.252.0.

15. True or False: Using Reverse Address Resolution Protocol (RARP), a host maps the IP address to the MAC address.

16. True or False: The Internet Control Message Protocol (ICMP) is the protocol that handles error and other control messages.

17. True or False: The Open Shortest Path First (OSPF) protocol is an Internet Gateway Protocol (IGP) protocol that was developed to fix some of the deficiencies in Routing Information Protocol (RIP).

18. True or False: The Dynamic Host Configuration Protocol (DHCP) automatically configures hosts that connect to a TCP/IP network.

19. True or False: Network Address Translation (NAT) refers to a method for mapping packets generated by machines in a private network into packets that can traverse the global Internet.

20. True or False: Mobile IP allows portable devices called mobile hosts (MHs) to roam from one area to another while maintaining the communication sessions. One requirement in mobile IP is that a legacy host communicating with an MH and the intermediate routers should not be modified.

21. True or False: Symmetric cryptography relies on two different keys, a public key and a private key. A sender encrypts the plaintext by using a public key, and a receiver decrypts the ciphertext by using a private key.