CITS 3002 Test “mock” questions

LAYERED PROTOCOLS

*1. Name the seven layers of the OSI Networking Reference model, from the lowest to the highest.*

The seven layers: Physical, Data Link, Network, Transport, Session, Presentation, Application

*2. List 2 advantages and 2 disadvantages of strictly conforming to a layered networking standard, such as the OSI/ISO networking model.*

Advantages: Each layer has a specific set of features.

A layered networking standard provides some order in regards to networking.

A layered approach reduces a set of complex things into smaller, interrelated groupings

Disadvantages: Users must now conform to a layered standard that they may not necessarily agree with.

A layered networking standard provides a lot of extra overhead and computation. The overhead may be more than that of the actual computation required to, for e.g. send a message, as the message has to pass through levels of abstraction (i.e. adding headers to the message).

*3. Data encryption of network traffic can, arguably, be employed in a number of layers of the OSI/ISO Reference model. If you were to employ encryption in exactly 2 layers, which layers would you choose, and why?*

*I would employ encryption in the Data Link layer and the Session layer. Data link layer encryption provides lower overhead on data packets, lower maintenance costs and support for legacy hardware – these facts do not really affect performance of the network.*

Encryption should be employed in

4. A system uses an n-layer protocol hierarchy. Applications generate messages of M bytes each. At each of the layers, an h byte header is added. What fraction of the network bandwidth is filled with headers?

h = header

nh / M + nh

Data Link Layer Protocols

5. Knowing that some typical checksums are only 16 bits long, it appears that a corrupted data frame has a 1 in 2^16 chance of having the same checksum as its original data frame. Discuss this idea with respect to the design of checksum algorithms.

6. Provide 3 distinct reasons why a stream of data is broken into frames by the data-link layer?

7. Under what circumstances would the use of Data-Link Layer frame pipelining be unnecessary (a waste of either time or effort)?

8. What is the primary motivation for piggy-backed acknowledgements in a Data-Link layer protocol?

9. In some protocol stacks, such as the Internet Protocol (IP) and Asynchronous Transfer Method (ATM) networks, the checksum of network-layer information covers only the header, and not the data. Why do you suppose that this design was chosen?

10. Consider a stop-and-wait protocol that uses only negative acknowledgments (NACKs), and no positive acknowledgments (ACKs). Describe what timeouts would need to be scheduled. Explain why an ACK-based protocol is usually preferred to a NACK-based protocol.

11. Within a sliding window Data-Link layer protocol, is it meaningful for the receiver's maximum window size to be larger than the sender's maximum window size? Why or why not?

NETWORK LAYER PROTCOLS

12. Given that Data Link Layer protocols already employ sequence numbers, provide 2 distinct motivations for Network Layer protocols also employing sequence numbers.

13. Why doesn't each node in a virtual circuit use the same number to identify the circuit?

14. Briefly, in a sentence or two, distinguish between the terms flow control and congestion control.

15. Briefly describe the intended effects of employing the leaky bucket and token bucket flow control algorithms.

16. As a brute-force form of congestion control, the Network Layer may choose to deliberately discard some packets when its maximum permissible memory allocation is reached. Which packets are the best candidates for removal? What effects will their removal have on the total network's congestion?

LOCAL AREA NETWORKS

17. Explain the need for both a minimum frame length and a maximum frame length in the IEEE 802.3 Ethernet specification.

18. What is the primary difference between an Ethernet hub and an Ethernet switch?

19. Although only a relatively low-level device, a network bridge has a number of important and difficult tasks to perform. List 3 distinct tasks that must be performed by a bridge connecting dissimilar hardware technologies.

20. Why must IEEE 802.11 wireless networks employ collision avoidance instead of simply collision detection?

21.Must all MAC addresses employed worldwide by IEEE 802.11 interface cards in mobile devices and fixed access points, be unique? Why or why not?

22. Briefly describe three distinct types of denial-of-service (DOS) attacks that may be performed on IEEE802.11 wireless networks. Each of the three attacks should be at a different layer of the protocol stack.

23. In an effort to reduce the likelihood of intruders employing passive scanning to assess the security of an IEEE802.11 wireless network, the owner of a wireless access point enables a facility so that only registered MAC addresses may use the access point. Explain why this measure would be ineffective against a determined intruder assessing the network's security.