Computer Sciences
159334 – Computer Networks - Sample Questions

Application Layer

1 - Explain the difference between passive and active modes in the standard FTP protocol.

2- Which application layer protocols are used for email?

3- Which application layer protocol is used to translate URL into IP addresses?

4- What transport layer protocol does HTTP normally uses?

5- A user wants to access a server via command line. Which application would you advice him to use, *telnet* or *ssh*? Why?

6- What is a Web-cache? What are the advantages in using it?

7 – What is conditional GET in HTTP protocols?

8 – FTP requires two TCP connections when transferring files. How are these connections used? Soon after a file is transferred, which one of these connections are still active?

Transport Layer

1 – What is the difference, in terms of the services provided, between TCP and UDP?

2- Explain the difference between passive and active modes in the standard FTP protocol.

3- Explain the difference between Go-back-N and Selective Repeat.

4- Using a simple diagram, show how the sequence numbers and acknowledgement numbers are updated in TCP.

5- In order to establish a TCP connection, which process should be started first, the server or the client?

6 – What are the two most important *fields* in TCP's segment headers?

7 – How does TCP achieve flow control?

8 – What are RTTs? How does TCP use them to calculate the timeout for each segment?

9 – Show a diagram with the *three way handshake* used by TCP.

10 - Briefly explain how TCP congestion control works.

Network Layer

1 -

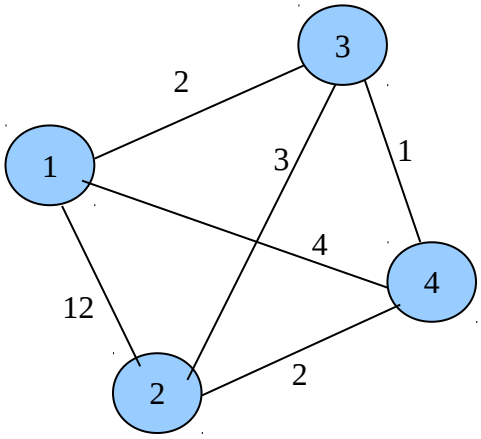

Figure 1

a) In Figure 1, the nodes represent routers, and it shows the time cost for each link between the 4 routers. Use the Distance Vector algorithm to find the minimum path between the routers. Show all the intermediate states for the tables in each router.

2- A certain network has a mask 255.255.248.0. Show, in binary, which one is the network and the host parts of the IP address for 130.123.107.128.

3 – What are the services provided by the Network Layer?

4 – Explain the strategy of 'poisoned reverse' to boost performance in Distance Vector algorithms.

5 – Why is it more efficient to use “families” of IP addresses (continuous range of IP adresses) to organise routing?

6 – Draw a diagram showing the three types of switching fabrics for routers.

7 – Explain how packet *losses* occur due to *buffer overflow* in routers.

Data Link and Physical Layer

1 - Briefly explain how errors are found and how they are corrected using two-dimensional parity.

2 - Explain how collisions are dealt with in the following protocols:

a) ALOHA
b) Slotted ALOHA
c) CSMA
d) CSMA/CD
e) CSMA/CA (wireless)

3 - What is the relationship between *physical addresses* (also called MAC addresses (Media Access Control), stored permanently in the host's network adapter) and *IP addresses*?

4 - How does ARP works? What is the motivation for its existence?

5 - If the ARP table is restricted to a certain LAN, how can a packet be sent to a PC that sits on another LAN?

6 – Briefly explain the difference between a Hub, a Bridge and a Switch.

7 - Considering that both the bridge and the router are 'store-and-forward' devices, what is the fundamental difference between them? Draw a diagram to show it.

8 - Calculate the CRC value (in binary and hexadecimal) for the character “1111 1001” considering that the polynomial is the standard 16 bit CRC (0x8005).

Network security

1 - What advantages does public key encryption schemes (like the RSA algorithm) offer over symmetric key schemes?

2 – Explain how 'packet sniffing' works in an Ethernet network.

3 – Why is important that RSA keys have a minimum length?

4 - Why MD5 is used to compute digital signatures instead of the simpler CRC?

5 - Why is authentication an important requirement for network security?

6 - Explain the *'man-in-the-middle' attack* and why this form of attack is related to the need of trusted intermediaries to certify public keys.

7 - Discuss the following statement: 'confidential information should not be sent by email without strong encryption methods.'

8 - Explain the following threats in the Internet: IP spoofing and DoS

9 - Why is it not advisable to implement protocols that encrypt a text message *character by character*?

10 – Show in a simple diagram how PGP uses encryption, authentication and message integrity for email messages.

11 – A firewall can filter packets based on protocols, port numbers, and even IP addresses. What are the limitations for a firewall?

12 – Compute a new pair of keys for RSA: p = q =
n =
z =
e =
d = final pair: private key (,) public key (,)