Department of Computer Science
Computer Networks
Due: Sunday 27th October (23.59)

Your name:
TA Name:
Time Taken:
Estimated Time: 20 hours

This is a paired assignment - you may choose to work with one other person if you wish, and submit the assignment together.

This assignment can be submitted as a pdf using Canvas. For those who like to dabble in the dark arts, the latex version is also available, but you may submit in any legible form you wish. Marks are awarded for question difficulty. While there is typically a relationship between difficulty and length of answer, it may not be a strong one.

Explain your answer or give full derivation of results where appropriate. Solitary solutions without explanation risk receiving 0 points, even when correct. In particular if there are 2 points for a short question, 1 of them will be for the explanation.

Optional: Please include a rough estimate of how long it took you do the assignment so that we can calibrate the work being assigned for the course. (The estimated time is provided purely as a guideline.)

Question:	1	2	3	4	5	6	7	Total
Points:	23	14	10	13	8	18	14	100
Score:								

Network Trivia

1 . . . . *23 points*

(a) (2 points) What is a Media Access Control(MAC) Address?

(b) (2 points) How does Wireshark know the manufacturer of the device sending a packet?

(c) (2 points) Why is a random interval added to the CSMA backoff and try again protocol?

(d) (2 points) Why is it a good idea to keep the size of individual messages sent across the open Internet to less than 1450 bytes?

(e) (2 points) What is an open DNS amplification attack?

(f) (2 points) What is an Autonomous System(AS) and how are they identified as part of the internet.

(g) (2 points) Where are the routing tables for the backbone routers of the Internet calculated?

(h) (2 points) What is the Internet Control Message Protocol (ICMP) used for?

(i) (2 points) Why is it ill-advised to look directly into the end of a fibre optic cable?

(j) (3 points) Explain the differences between symmetric and asymmetric encryption?

(k) (2 points) Why is flow control important at all levels of the network stack?

Queuing Theory

2 . . . . *14 points*

(a) (4 points) In the Kendall Queuing System Notation (X/X/x/X), what do the first four terms stand for?

(b) An IT help desk is available 8 hours a day, with a single person to provide help. Assume the average exponentially distributed service time for each person needing help is 10 minutes, and there are 4 arrivals an hour.

i. (3 points) How long on average will each person have to wait in the queue?

ii. (3 points) How many IT specialists will need to be provided to prevent anybody queueing?

iii. (2 points) What critical assumption does the answer to part ii depend on?

iv. (2 points) At what particular time of the day is this assumption likely to be incorrect?

Information Theory

3 . . . . *10 points*

(a) (4 points) Shannon's limit on the communication of information in a single channel, places a hard mathematical limit on the amount of information that can be communicated over a single channel for a given amount of bandwidth, power and noise. Consider 5 devices that are connected via copper wires, versus 5 devices that are connected via WiFi. Assume that the bandwidth, power, and noise of the communication medium (i.e. copper vs wireless) are identical.

Is the amount of information that can be transmitted to the end devices the same in both scenarios? Explain.

(b) You are asked to audit a real time networked system, with a full mesh topology. Each node in the system can receive and process 100 messages/second from other nodes in the system. What is the maximum number of nodes the system can support, when:

i. (2 points) On receipt of any message, a node sends a message to at most one other node in the mesh.

ii. (2 points) On receipt of any message, a node sends a message to all the other nodes in the mesh.

iii. (2 points) Pick one of the two cases above, and explain how it could be rearchitected to have more nodes than the limit you calculated.

TCP/IP

4 . . . . *13 points*

(a) (3 points) The table below shows the sequence of events that happen during a TCP connections between two hosts A and B, when A opens a connectiion to B, sends a single data segment, and then closes the connection. Order the events as they occur as part of the connection, and indicate which host or hosts they occur at.

Order	A	B	Event
			Send an ACK segment
			Do the rest of the data exchange
			Close the connection
			Send an ACK segment
			Send a FIN segment
			Send a SYN segment
			Send a FIN segment
			Send a SYN-ACK segment
			Enter the TIME-WAIT state
			Send an ACK+DATA segment
			Close the connection

(b) (2 points) Draw a labelled diagram of the three part opening handshake of a TCP/IP connection, showing the sequence, acknowledgement values and type of each segment sent.

(c) (2 points) What is the purpose of a SYN cookie?

(d) (2 points) What guarantee does TCP/IP provide for connections which are made using it?

(e) (2 points) What is the advantage of TCP Selective Acknowledgements (SACK) over the original cumulative acknowledgement scheme?

(f) (2 points) What is silly window syndrome?

Networks and Addressing

5 . . . . *8 points*

(a) (3 points) For each of the following subnet addresses, provide the range of of IP Addresses that can be assigned to that subnet, and the broadcast address for that subnet.

Subnet	IP Address Range in the Subnet	Broadcast address
44.36.35.0/27		
10.12.13.0/24		
18.0.0.0/8		

(b) (2 points) What addressing problem does Network Address Translation(NAT) solve for IPv4 network addresses?

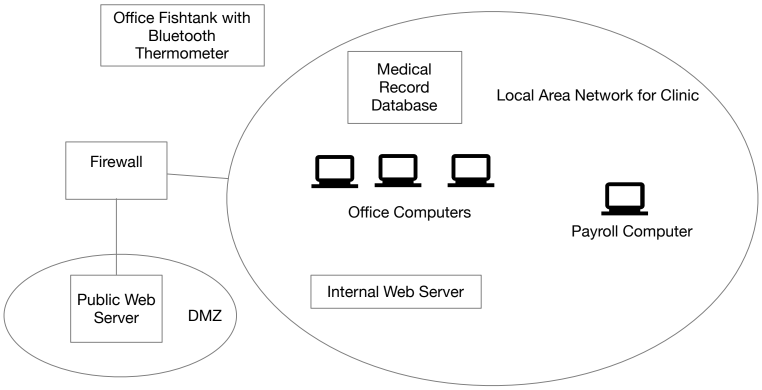
(c) (3 points) Because NAT violates the end to end principle of the Internet, initiating connections to addresses behind NAT routers is problematic. Name one of the techniques that can be used used to overcome this problem, and briefly describe how it works.

Network Design and Security

6 . . . . *18 points*

You have been asked to consult on the network security of the small health clinic shown in the diagram below. All computers in the clinic are on the same Local Area Network(LAN), which uses a small cisco router to connect to the Internet. The medical record database is stored on a dedicated linux computer also on the LAN, and is accessed by all the office computers except the payroll computer. A WiFi Network is used by employees to access the LAN with their cell phones, and to provide a guest network for patients. The fishtank is not on any network, but a manufacturer supplied cellphone APP is used to monitor its temperature by staff.

The clinic also supports a public web server which is used for patient appointments, to advertise times for Flu shots and other public announcements.



(a) (2 points) What is the purpose of the Demilitarized Zone(DMZ)?

(b) (2 points) Is one firewall sufficient?

(c) (4 points) The clinic's WWW address was recently used in a phishing attack, after attackers altered its public DNS record via a DNS cache poisoning exploit. Explain what happened, and how the clinic could prevent this from happening again.

(d) The Blueborne(CVE-2017-1000251) attack, announced in September 2017, allows an attacker to install and run malicious code on affected bluetooth devices without any interaction with the user. The attack has been sucessfully demonstrated on all major computer and mobile phone platforms, and many other bluetooth devices. The attack can also propagate itself to other bluetooth devices.

Assume that none of the Bluetooth devices in the Clinic have been patched.

i. (2 points) Explain how an attacker on the Guest network could probe for local bluetooth devices.

ii. (4 points) Explain all the steps in a plausible attack that uses the office fishtank to attack the payroll computer and extract data to a visitor's laptop.

(e) (4 points) Given that the Cisco router provides support for Virtual Lans (VLAN), draw and label a diagram showing how to reorganise the network to provide better security for the payroll computer. You may add additional named devices if you wish, and should provide a brief explanation for the reasons for your changes.

Bluetooth

7 . . . . *14 points*

(a) An American company is selling a personalised, Bluetooth 5.0 toothbrush, which measures heartrate, brushing frequency, and duration of brushing. It uploads this information to a company server. The product is marketed specifically towards children, under the age of 12, to help their parents monitor their brushing habits. The devices use a commodity chip which supports the full bluetooth stack, and pairs with an Android phone acting as a master.

i. (2 points) What is the bluetooth Generic Access profile(GAP)?

ii. (2 points) Explain how two Bluetooth LE devices from different manufacturers can share information.

iii. (2 points) How will the toothbrushes pair with a phone?

iv. (4 points) The company also sells a blue tooth enabled smart lightbulb, which is controlled with the same software. A household using both products will typically have over 20 light bulbs and several toothbrushes.
Describe using a labelled diagram, and stating clearly any restrictions on connectivity, how these bluetooth 5.0 devices can network together.

v. (4 points) A large number of dentists have been given these toothbrushes as part of a marketing campaign to distribute to customers. Unknown to either the dentists or the manufacturer, hackers have found a way to use the firmware in the toothbrushes to create a botnet for industrial espionage. Describe a plausible way this could be done, assuming that each household has at least one mobile phone which has not been updated to fix the Blueborne attacks. Include an explanation of how the toothbrushes could be identified, and also how information can be extracted from the toothbrushes back to Hacker HQ.