**Ollscoil Mhá Nuad**

**Maynooth University**

**SEMESTER 1**

**2023-2024**

# CS320

**Computer Networks**

Dr. P. Healy, Prof. R. J. Farrell, Dr. B. Hennelly

Time allowed: 2 hours

You must answer Question 1 and any three other questions.

Your mark will be based on Question 1 and your best three answers from the remaining questions

**All questions** carry equal marks

**Instructions**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** | **No** | **N/A** |
| Formulae and Tables book allowed *(i.e. available on request)* |  | X |  |
| Formulae and Tables book required *(i.e. distributed prior to exam commencing)* |  | X |  |
| Statistics Tables and Formulae allowed *(i.e. available on request)* |  | X |  |
| Statistics Tables and Formulae required *(i.e. distributed prior to exam commencing)* |  | X |  |
| Dictionary allowed *(supplied by the student)* |  | X |  |
| Non-programmable calculator allowed | X |  |  |
| Students required to write in and return the exam question paper |  | X |  |

Enter any other instructions here or delete the box.

**[25 marks]**

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | (a)  (b)  (c)  (d)  (e)  (f)  (g)  (h)  (i)  (j) | **Short Questions**  Suppose two hosts, A and B, are separated by 50,000km and  are connected by a direct link of R = 2Mbps. Suppose the  propagation speed over the link is 2.5x108 meters/sec. How long  does it take to send a file of 1.5Mbytes from A to B? *Answer: File Size Conversion: 1.5 Megabytes = 1.5 x 8 x 1,000,000 bits (as 1 Byte = 8 bits, 1 Megabyte = 1,000,000 Bytes). Transmission Time is the file size in bits divided by the link speed. This gives 1.5 x 8 x 1,000,000 bits / (2 x 1,000,000 bits/second) = 6 seconds. Propagation Delay: The propagation delay is the distance divided by the speed of light in the medium = 50,000 x 1,000 / (2.5 x 10^8) seconds ≈ 0.2 seconds. Total 6.2 seconds.​*  Explain in a few sentences what are the fundamental differences between the client-server and peer-to-peer network architectures. *Answer: In a client-server architecture, the system is centralized with a dedicated, always-on server having a fixed IP address. This model faces scalability challenges. In contrast, a peer-to-peer (P2P) network is decentralized; each peer adds and consumes resources when joining, enhancing scalability and resource distribution.*  Suppose that Alice wants to send an email message to Bob. This will involve four entities: Alice’s mail client (for email composition and sending ), Alice’s outgoing mail server, Bob’s incoming mail server, and Bob’s mail client (for email retrieval and viewing ). Between which of these four entities does the SMTP protocol operate? What about the IMAP protocol? *Answer: SMTP runs between Alices mail client and her server, and also (separately ) between her server and Bob’s server. IMAP runs between Bob’s server and his mail client to retrieve messages from Bob’s server.*  What is meant by demultiplexing a protocol data unit up to an upper level (app layer) protocol? *Answer: this refers to passing the decapsulated data unit up to the appropriate higher level protocol. This is done by looking at the upper--‐layer protocol field.*  Consider a server socket that is used to communicate from server to client. In the case of a TCP socket, can data being read from the server socket have been sent by more than one client? Explain briefly. In the case of a UDP socket, can data being read from the server socket have been sent by more than one client? Explain briefly. *Answer: With TCP, the client--‐to--‐server socket is created by the return from the accept( ) call at the server, binding the client that was accepted to the server via the newly created socket. Thus only one client is associated with the TCP socket. With UDP, any client can send to the (same ) UDP socket on the server.*  What is the role of the “control plane” and the role of the “data plane” in a router? *Answer: the control plane is responsible for executing the routing algorithms. The data plane is responsible for forwarding datagrams according to the forwarding table.*  What is the purpose of the DHPC protocol? *Answer: the get an IP address. The IP address will be in the same subnetwork (LAN ) as the router to which it is attached via the LAN.*  Briefly in just a few sentences explain the difficulties in developing a protocol for a shared access network. *Answer: Collision Management: Implementing methods to detect and resolve data collisions among multiple users. Fair Access: Ensuring all users have equal opportunity to access the network. Scalability: The protocol must adapt to different user numbers and traffic without performance loss. Balancing Latency and Throughput: Optimizing for low delay and high data transfer rates simultaneously.*  Briefly explain the key differences between the ALOHA and slotted ALOHA protocols. *Answer:* *Time Synchronization: ALOHA does not require synchronization, while Slotted ALOHA operates on synchronized time slots. Collision Rate: ALOHA has a higher collision rate due to unsynchronized transmissions, whereas Slotted ALOHA's aligned time slots reduce collision chances. Efficiency: Slotted ALOHA is more efficient due to structured transmission times, as opposed to ALOHA's more random approach.*  Suppose that Bob and Alice have access to a public key system that makes their public keys available to each other. Each knows its own private key. 1. Suppose Bob has a document, m, that he wants to digitally sign. How does he do so? Efficiency is not a concern here, any digital signature technique is fine. *Answer: Bob will encrypt the document, m, using his private key. This serves as Bob’s digital signature on the document. If we want to be more efficient, Bob could compute a hash of m, and then encrypt hash(m).* 2. What does Alice do to verify Bob’s digital signature? *Answer: Alice applies Bob’s public key to the signed version of m, i.e., computes KB+(KB-(m)). If that yields the message m, then Alice knows that Bob has signed the document.* | [2.5 marks]  [2.5 marks]  [2.5 marks]  [2.5 marks]  [2.5 marks]  [2.5 marks]  [2.5 marks]  [2.5 marks]  [2.5 marks]  [2.5 marks] |

|  |  |  |  |
| --- | --- | --- | --- |
| **3** | (a)  (b)  (c)  (d) | **Content Distribution Network, Caching, DNS, and delay**  In Fig. 1 below, a simplified model for a CDN is shown with three networks each with a 1 Gbps LAN. One of these is an ISP with two clients A and B as well as a HTTP cache and a local DNS server. The clients are both using the Netflix streaming service, which is hosted at Netflix.com, while the content is hosted on a third-party server KingCDN.com.  **Figure 1: Simplified model of a CDN**  You may assume the following:   * All TCP connection segments can be ignored * The transmission delay of small packets such as DNS or HTTP GET is negligible. * The throughput between routers R1 and R2 is 10Mbps * All files on KingCDN.com are 2Gb in size. * The propagation delay between any two nodes on the internet is 0.25 seconds * The HTTP cache is initially empty.   Assume Client A has already accessed Netflix.com and is now browsing. He clicks on a file and waits for it to begin downloading. Starting from the moment he clicks on the file, list all of the messages that will be sent by all nodes involved.  How long does it take for the file to be downloaded; you need only consider propagation delays and transmission delays.  Some time after the download is complete, a second client, B, accesses Netflix.com using their browser and clicks on the same file. List all of the messages that are sent.  How long before Client B has downloaded the file. | [8 marks]  [6 marks]  [6 marks]  [5 marks] |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | *Solution: This is taken from a tutorial I did on the same question with slightly different values for delay (a) and (b)*    *(c) and (d)*    *Please note there is a mistake in Q1 (a) and (b) I should have included 4 messages after step (3) and before Step 4 (4) : i>local DNS->root ii>root->local DNS, iii>local DNS\_>.com TLD, iv>.com TLD->local DNS - this adds 1 full second to question (b)* |  |

**[25 marks]**

|  |  |  |  |
| --- | --- | --- | --- |
| **3** | (a) | **TCP Congestion**  For this problem you should familiarise yourself with Figure 2 first. Now assume that in the network shown in Figure 2 two parallel TCP transmissions are performed. TCP1 is a transmission between Source A and Sink A that uses TCP Tahoe. TCP2 is a transmission between Source B and Sink B that uses TCP Reno. Initial *ssthresh* for both TCP transmissions is set to 32. In this specific scenario no additional delay through forwarding is introduced. Thus, the RTT is only composed of the sums of the delay indicated on each link, times two.  A diagram of a router  Description automatically generated  **Figure 2: Two Parallel TCP Connections A and B**  For the *TCP 1* transmission, draw the resulting congestion window, assuming that a packet loss (triple duplicate ACKs) is detected at time t=900ms. Use Figure 3 to answer. | [7 marks] |
|  | (b) | For the *TCP 2* transmission, draw the resulting congestion window, assuming that a packet loss (triple duplicate ACKs) is detected at time t=650ms. Use Figure 3 to answer.    **Figure 3: You can write on this figure to answer (a) and (b)** | [7 marks] |
|  | (c) | Describe the benefit of TCP Reno over TCP Tahoe. | [6 marks] |
|  | (d) | TCP is more similar to the *Go-Back-N* protocol compared with the *Selective Repeat* protocol; do you agree or disagree with this statement and why? | [5 marks] |
|  |  |  |  |

*Solution*

*For (a) and (b)*

**

*(c)* *TCP Reno adds the Fast Recovery algorithm, which is a significant enhancement over TCP Tahoe. When TCP Reno detects packet loss via the reception of three duplicate ACKs (Triple Duplicate ACKs), it performs the Fast Retransmit like Tahoe does, retransmitting the lost packet. However, instead of going into Slow Start (like TCP Tahoe), it enters Fast Recovery. In Fast Recovery, TCP Reno cuts the congestion window size in half (instead of reducing it to 1 as in TCP Tahoe) and then begins transmitting new packets again if the congestion window allows for it, without waiting for a timeout or the retransmission to be acknowledged.*

*This means that TCP Reno can recover from losses without reducing the congestion window to a single MSS (Maximum Segment Size) as TCP Tahoe does, which allows for higher throughput and better utilization of the network under conditions of multiple packet losses within a single window of data.*

*By avoiding the Slow Start after a loss event indicated by three duplicate ACKs, TCP Reno improves overall throughput in networks with high bandwidth-delay products, where recovering from a reduced congestion window is particularly costly in terms of time and bandwidth*

*(d) TCP incorporates aspects of both Go-Back-N and Selective Repeat. Like Go-Back-N, TCP uses cumulative acknowledgments, which can lead to the retransmission of multiple packets if a single packet loss is detected. However, with features like selective acknowledgments (SACK), TCP can also exhibit behavior similar to Selective Repeat, where it can acknowledge non-contiguous blocks of packets and only the missing segments are retransmitted. Thus, TCP can adapt its behavior to the situation, taking on characteristics of both protocols.*

**[25 marks]**

|  |  |  |  |
| --- | --- | --- | --- |
| **4** | (a) | **Routing Algorithms – Distance Vector**  Consider the network shown below, and assume that each node initially knows the cost to each of its neighbors. Consider the distance--‐vector algorithm and show the distance table entries at node z over the three iterations that are highlighted with the empty tables in the next page. You can use these empty tables to answer your question.    **Figure 4: Use the Bellman-Ford Equation to determine the distance vectors at Node z** | [15 marks] |
|  | (b) | For each of the three iterations, does Z send any updates to its neighbors, and if so, will any of these result in changes in the neighbors tables? | [5 marks] |
|  | (c) | What do you understand by the term *poisoned reverse* in the context of distance vector routing? | [5 marks] |
|  |  |  |  |
|  |  | 1. First Iteration. Z only knows about its immediate links      1. Second Iteration. Z receives an update from its immediate neighbours x and v and updates its tables accordingly      1. Third iteration. Z receives more updates from its immediate neighbours x (re cost to u) and v (re cost to y and z) and Z updates its tables accordingly |  |

*Solution: 1. First Iteration. Z only knows about its immediate links*

*u v x y z*

*v inf inf inf inf inf*

*x inf inf inf inf inf*

*z inf 7 3 inf 0*

*2. Second Iteration. Z receives an update from its immediate neighbours x and v and updates its tables accordingly*

*u v x y z*

*v 2 0 2 inf 7*

*x inf 2 0 4 inf*

*z inf****->7******7->5*** *3 inf->7 0*

*3. Third iteration. Z receives more updates from its immediate neighbours x (re cost to u) and v (re cost to y and z) and Z updates its tables accordingly*

*u v x y z*

*v 2 0 2 inf->5 7*

*x inf->4 2 0 4 inf*

*z* ***7******5*** *3 7 0*

*(b) it sends updates every time its values change – so yes after each iteration*

*(c) Poisoned reverse is a technique used in distance vector routing protocols to prevent routing loops. When a router sends out its routing table, it sets the distance to any route learned from a neighbor to infinity if it is sending that information back to the neighbor. This "poisoning" informs the neighbor that the route through that router is no longer viable, effectively reversing the route advertisement. By doing this, the algorithm aims to quickly propagate route failures through the network and thus avoid the possibility of counting-to-infinity problems.*

**[25 marks]**

|  |  |  |  |
| --- | --- | --- | --- |
| **5** | (a) | **Network and Link Layer Addressing**  An ISP owns 123.16.0.0/17 address block. The ISP has five customers A, B, C, D, E with requirements for the following numbers of IP address.  A 4000  B 2000  C 4000  D 8000  E 2000  Address ranges are allocated first to A, then to B, then to C, and finally to D. In each case the lowest possible starting point that you can for the range is selected. What address ranges and subnet masks are allocated to each organization? Use notation similar to 123.16.0.0/17) for each of these customers.  *Solution:*  *A needs 12 bit block (4096) and will need /20 mask so we give 123.16.0000\*\*\*\*.\*\*\*\*\*\*\*\*=123.16.0.0/20*  *B needs 11 bits (2048) and will need /21 mask so we give:*  *123.16.00010\*\*\*.\*\*\*\*\*\*\*\*=123.16.16.0/21*  *C needs 12 bit block (4096) and will need /20 mask so we give 123.16.0010\*\*\*\*.\*\*\*\*\*\*\*\*=123.16.32.0/20*  *Notice at this point we have not used the 11 bit range 123.16.0011\*\*\*.\*\*\*\*\*\*\* - This can be used for an additional customer that needs 2048 address – lets give to E.*  *D needs 13 bit block (8192) and will need /19 mask*  *123.16.01\*\*\*\*\*.\*\*\*\*\*\*\*=123.16.64.0/19*  *And E is as above = 123.16.48.0* | [12 marks] |
|  | (b) | Consider the figure below. The IP and MAC addresses are shown for nodes A, B, C and D, as well as for the router's interfaces. Consider an IP datagram being sent from node C to node B. Give the source and destination Ethernet addresses, as well as the source and destination addresses of the IP datagram encapsulated within the Ethernet frame at points (6), (4), and (3) in the figure above.    *Solution: At point (6): Ethernet source, destination address: A5--‐C5--‐FA--‐3B--‐FF--‐0A, 9D--‐EB--‐5B--‐5A--‐BA--‐A5 IP source, destination address: 128.119.54.168, 128.119.227.32 At point (4): Same as as point (6) At point (3): Ethernet source, destination address: 5E--‐27--‐7D--‐58--‐94--‐3A, 7D--‐A5--‐F5--‐0A--‐8B--‐1F IP source, destination address: 128.119.54.168, 128.119.227.32* | [8 marks] |
|  | (c) | Consider an ARP query that is sent by A. Assume all switches are learning switches but have empty tables. How many nodes will receive this ARP message, and how many will receive the response.  *Solution: Since the switch table is empy the message will be broadcast – all 4 interfaces adapters in A’s subnet will receive (no other subnets will receive) and only A will receive the response due to learning switch* | [5 marks] |

**[25 marks]**

|  |  |  |  |
| --- | --- | --- | --- |
| **6** | (a) | **The RSA encryption algorithm**  Briefly explain how the RSA algorithm works. Make sure to cover key generation, encryption, and decryption processes. | [10 marks] |
|  | (b) | Discuss why RSA is considered secure and what role prime numbers play in ensuring this security. | [5 marks] |
|  | (c) | Imagine a scenario where two parties, Alice and Bob, want to securely communicate over a network using RSA encryption. Alice has chosen two prime numbers p = 17 and q = 19 to generate her public and private keys. Calculate the public key (n, e) and the private key (n, d). You may choose a small value of e for simplicity. | [5 marks] |
|  | (d) | Bob wants to send the message 'HI' to Alice. Based on your previous answer, convert the message to a numerical format, encrypt it using Alice’s public key, and send it over the network. (You may represent the message in ASCII format and work with a simplified version of the encryption to fit the time constraint.) Hint: "H" in ASCII is 72, "I" in ASCII is 73. Combining these, we get the message as 7273.  *Solution*  *(a) RSA Basics: The RSA algorithm involves three main steps: key generation, encryption, and decryption.*  *Key Generation:*  *Choose two distinct large random prime numbers p and q.*  *Compute n = pq. n is used as the modulus for both the public and private keys.*  *Compute the totient φ(n) = (p-1)(q-1).*  *Choose an integer e such that 1 < e < φ(n) and e is coprime with φ(n).*  *Compute d to satisfy the congruence relation d \* e = 1 (mod φ(n)).*  *Public Key: The public key is (e, n).*  *Private Key: The private key is (d, n).*  *Encryption (performed by the sender):*  *Represent the plaintext message as an integer m in the interval 0 <= m < n.*  *Compute the ciphertext c using the recipient’s public key (e, n) with the formula c = m^e (mod n).*  *Decryption (performed by the receiver):*  *Use the private key (d, n) to compute m = c^d (mod n).*  *Convert the integer m back to the plaintext message.*  *(b). Role of Prime Numbers in RSA’s Security*  *Prime numbers play a crucial role in ensuring the security of RSA encryption. The difficulty of factoring the product of two large prime numbers ensures the security of the private key. The RSA algorithm's security is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.*  *(c). Key Generation with Alice’s Chosen Prime Numbers (5 mins)*  *Let p = 17 and q = 19.*  *Calculate n = pq = 17 \* 19 = 323*  *Calculate φ(n) = (p-1)(q-1) = 16 \* 18 = 288*  *Choose e such that 1 < e < 288 and e is coprime with 288. Let’s choose e = 5.*  *Calculate d, the modular multiplicative inverse of e (mod φ(n)). For example, d = 173, as 5 \* 173 = 865 = 1 (mod 288).*  *The public key is (5, 323) and the private key is (173, 323).*  *(d) Let's encrypt the message "HI" using Alice's public key. First, we need to convert the message to an integer. A common approach is to use ASCII values.*  *"H" in ASCII is 72, "I" in ASCII is 73. Combining these, we get the message as 7273.*  *Now, let's encrypt the message:*  *m = 7273*  *c = m^e mod n = 7273^5 mod 323*  *Calculate c to get the encrypted message.*  *Now, the sender can send c to Alice.*  *3. Decrypting the Message (5 mins)*  *Upon receiving the encrypted message c, Alice can use her private key to decrypt it:*  *m = c^d mod n*  *Substitute c, d, and n with their respective values to find m.*  *Convert the integer m back to the ASCII characters to retrieve the original message "HI".*  *Through this process, Alice successfully decrypts the message using her private key, showcasing the RSA encryption and decryption process.* | [5 marks] |
|  |