# The University of Melbourne
# School of Computing and Information Systems

# COMP90007 Internet Technologies
# Final Exam
# Semester 2, 2021

**Reading Time:** 15 minutes

**Total Time:** 3 hours 15 minutes (including reading time)

**Instructions to Students:**

This paper has 7 pages, including two cover pages.

- The exam has 16 questions worth a total of 60 marks, making up 60% of the total assessment for the subject.
- The value beside the Question number displays the marks allocated to each question.
- Please answer all questions using English in the given order. Please type your answers and **save as one PDF file**. Handwritten assignments using tablet or scanned will not be accepted.
- Submission should only contain the question number and the answer (do not repeat the text of questions in your submission).
- Partial marks will be available. No question requires writing lengthy answers. Please be clear and brief as you may lose points for unclear or redundant descriptions.
- Make sure to **save your progress locally and regularly** during the exam and at the end. **Upload the PDF file before due time.** We recommend not leaving the uploading of your file to the last minute.
- If you submit after the due date and time, your submission will be marked as late. Your exam will be available for 30 minutes after the due date and time to allow late submission due to any technical issues during the exam. Once this additional 30 minutes has passed, you will no longer be able to access your exam in the LMS.



**Authorised Materials:** This exam is open-book. The work you submit ***must be based on your own knowledge and skills, without assistance from any other person***.

While undertaking this exam you ***are permitted to***:

- make use of textbooks, lecture slides (including electronic versions), lecture recordings and material provided as part of tutorials in this subject.
- make use of your own personal notes.
- use calculators or mathematical software to compute numeric answers.
- make use of other materials with proper references.

**IMPORTANT!! Collusion, Plagiarism, Copying are not allowed under any circumstances.**

- **Collusion** includes, but is not limited to, talking to, phoning, emailing, texting or using the internet to communicate with other students. Similarly, you cannot communicate with any other person via any means about the content of this exam during the examination time. If another student contacts you during the examination period, please inform the subject coordinator immediately.
- Your answers to the exam **must be in your own words** and not directly copied from lecture notes, tutorial materials, the Internet or joint study notes you have prepared with your friends. You may refer to sources, but answers should be written in your own words.
- Any similarity detected between your answers, the answers from other students and/or from the Internet or other sources will be investigated and may result in severe penalties.

**Technical support**

- **During the exam**, if you have questions about the exam content, please use the Exam Support Chat (BigBlueButton).
- **Technical support** for this exam can be accessed at: https://students.unimelb.edu.au/your-course/manage-your-course/exams-assessments-and-results/exams/technical-support
  Additional information about **Canvas Assignment** including troubleshooting tips, can be found: https://students.unimelb.edu.au/your-course/manage-your-course/exams-assessments-and-results/exams/how-do-i-take-my-exam/formats/LMS-assignments



**Questions commence on the next page.**

1. (**4 marks**) In this subject, we followed a layered network reference model.
   (1) What are the advantages of having a layered model? Briefly explain using bullet points.
   (2) What are the potential issues if the network layer is removed? Briefly explain using bullet points.

2. (**2 marks**) The transmission media used in the physical layer can be wired or wireless. Compare satellite with wired medium coaxial cable, and list both the advantages and disadvantages of these two media using bullet points.

3. (**2 marks**) Data link layer aims to provide reliable and efficient communication of frames between two adjacent machines.
   (1) Compared to byte stuffing, what are the advantages of using bit stuffing for framing? Briefly explain the advantages using bullet points.
   (2) Briefly explain the differences between Stop-and-Wait and Go-Back-N protocols using bullet points.



4. (**4 marks**) The Cyclic Redundancy Check method is often used for error detection during data transmission. Given the original data 10001101 and generator polynomial $G(x) = x^5 + x^2 + x + 1$,
   (1) what is the final data to be sent? Show your calculations.
   (2) how does the receiver detect error after receiving the data? Briefly explain the process (2-3 sentences).





Instructions: When showing your calculations you can use the following format, but also note that the numbers given in the notation example below have nothing to do with the question above and the operations there should not be taken as an indication how your solution would be. This sample is simply to give you an example to easily enter solution without complicated drawings/diagrams.

Sample format:

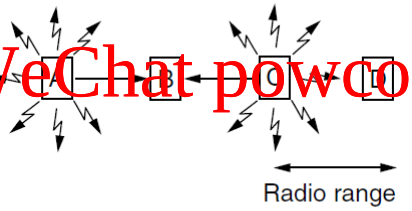
```
1 1 1 1 / 1 0 0 0 0 1 1 1 1 0 0
          1 1 1 1
         ------------------------
             ...
             operation continues
             …
```

5. (**3 marks**) There are 64 stations sharing a channel using binary countdown protocol. The addresses of these stations are from 0 to 63 in binary format. If the stations with addresses 12, 25, 33, 50 and 55 become ready to send at the same time, which station will get the channel to transmit its data in this round? Describe the process to determine which station will get the channel in this round by showing what happens at each slot of contention period.
   You can use a table like the following one to show the process, and briefly describe the process using bullet points.

| Stations | Time Slots | | | |
|---|---|---|---|---|
| | 1 | 2 | … | |
| | | | | |
| … | | | | |
| | | | | |

6. (**4 marks**) The Medium Access Control (MAC) sublayer is mainly to resolve transmission conflicts in shared channels.
   (1) Briefly explain why slotted ALOHA can achieve higher success rate than pure ALOHA.
   (2) Assuming Multiple Access with Collision Avoidance (MACA) is used in a wireless network as shown in the following figure, both A and C want to send data to station B. What will happen if C sends RTS to B? Briefly describe the behaviour of each station A, B, C and D in bullet point format. Will a collision occur at B if the CTS from B to C is lost? Why or why not?






7. (**3 marks**) A router has the following entries in its routing table:

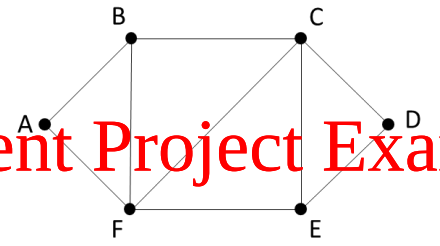
| Prefix | Next hop |
|---|---|
| 147.18.56.0/22 | Interface 0 |
| 147.18.60.0/22 | Interface 1 |
| 147.18.0.0/16 | Interface 2 |
| 186.102.40.0/23 | Interface 3 |
| default | Interface 4 |

   What are the next hops for the packets with the following IP addresses? Show all the steps taken to decide the next hop for these packets.
   (1) 147.18.63.140;
   (2) 147.18.52.12;
   (3) 186.102.42.112.

8. (**4 marks**) There are 4 departments A, B, C and D of a company requesting 1500, 700, 3200 and 900 addresses, respectively. Internet Service Provider has offered this company a large number of consecutive IP addresses starting from 115.36.0.0. The requirements for the allocation are: (i) each department needs a subnet with a block of consecutive addresses; (ii) the order of A, B, C and D must be kept, which means all the addresses of A must be before B, and B before C etc.; (iii) the allocation should be optimised to avoid allocating a huge subnet to a department, which is significantly more than it needs.

   How to assign addresses to these departments? Give the prefix of the block, the last address of the block and the number of addresses allocated to it using a table. Show reasoning of your allocations in bullet points (1-2 sentences for each department).

9. (**6 marks**) The link state routing is used in the following network as shown in the following figure. Given the current link state packet for each router in tables,






| A | |
|---|---|
| Seq. | 1 |
| Age | 20 |
| B | 1 |
| F | 2 |

| B | |
|---|---|
| Seq. | 1 |
| Age | 20 |
| A | 1 |
| C | 3 |
| F | 3 |

| C | |
|---|---|
| Seq. | 1 |
| Age | 20 |
| B | 3 |
| D | 1 |
| E | 2 |
| F | 6 |

| D | |
|---|---|
| Seq. | 1 |
| Age | 20 |
| C | 1 |
| E | 2 |

| E | |
|---|---|
| Seq. | 1 |
| Age | 20 |
| C | 2 |
| D | 2 |
| F | 3 |

| F | |
|---|---|
| Seq. | 1 |
| Age | 20 |
| A | 2 |
| B | 3 |
| C | 6 |
| E | 3 |

(1) what are the weights of shortest paths (using Dijkstra's algorithm) from router C to the other nodes, respectively? Show your calculation and the steps of using Dijkstra's algorithm in a table.

(2) if the link between C and E is broken, which routers' link state packets will be impacted? Show the new link state packets of these routers (the Sequence and Age fields can be ignored). Which routers should receive these updated link state packets?

10. (**5 marks**)
    a. If an application uses UDP and delivery guarantees are needed, in which layer (of the 5 layer model that we studied) is this achieved?
    b. Design a modification to RPC that uses UDP but guarantees that a remote procedure call is only invoked once if packets go missing. Your modification should be able to cope with the case where the request is not delivered and the case where the response is not delivered.

       **Hint**: your solution could add a request sequence number which is embedded in the UDP request packet.

11. (**2 marks**) What failures might occur if a host transmitting data ignored:
    a. The flow control window
    b. The congestion control window

12. (**2 marks**) How can a transmitter of data use the timing of the ACKs it receives to estimate the maximum rate at which it can transmit packets of data?



13. (**4 marks**) Designers of a videoconferencing application are considering two possible designs:
    a. Each party in the videoconference call sends their high quality video stream to every other party
    b. Each party sends their high quality video stream to a centralised server which sends a high quality image stream of the current speaker and low quality image streams of the other participant to every party.





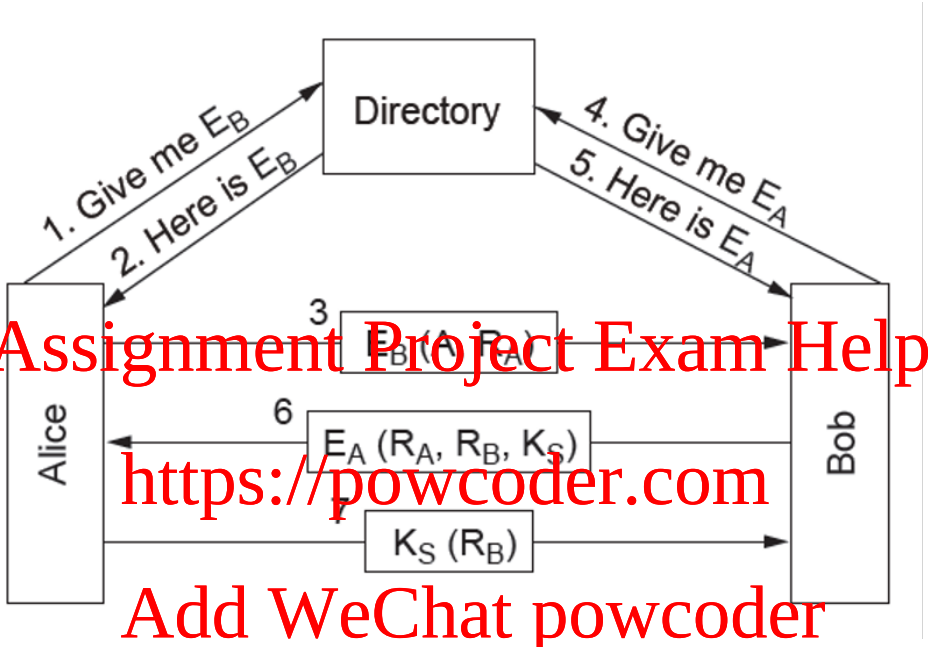
    Compare these two options in terms of their QoS requirements

14. (**6 marks**) A user types the address: 'https://www.unimelb.edu.au/' into the address bar of a web browser. Create a table that shows the sequence of packets that are sent and received by the web browser, up to and including the first packet containing part of the web page from the server. For each packet, you should indicate:
    a. Source host (e.g. 'User')
    b. Source port
    c. Destination host
    d. Destination port
    e. Transport layer protocol that is used
    f. Purpose of the packet.

    If the port is well-known, you should use that number and where the application chooses a port, you should make a suitable choice. You should assume that no packets are dropped during this process.

15. (**4 marks**) An RSA encryption scheme is operated using p=3, q=11 (hence n=33).
    a. If the public key is (7, 33), show all the steps proving that (3, 33) is the correct value for the private key.
    b. Add two (2) to the last digit of your University of Melbourne Student ID to obtain a number between 2 and 11. Show how this value can be encrypted using the public key (7, 33) and decrypted using the private key (3, 33).

16. (**5 marks**) The Figure below shows how public key cryptography can be used to establish the identities of two parties that wish to communicate and to establish a session key for the communication.






    a. How does Alice know that message 2 comes from the Directory?
    b. At what point can Alice be confident that she is communicating with Bob? How can she be sure?
    c. If Bob omitted $R_B$ from message 6, how could Alice still convince Bob that he is communicating with her?