

No part of the candidate's evidence in this exemplar material may be presented in an external assessment for the purpose of gaining an NZQA qualification or award.



Level 3 Digital Technologies 2024

91908 Analyse an area of computer science

EXEMPLAR

Achievement

TOTAL 03

INSTRUCTIONS

There are three questions in this assessment, on the topics of:

- big data ([page 3](#))
- complexity and tractability ([page 12](#))
- network communication protocols ([page 20](#)).

Choose only ONE question to answer. Copy and paste the name of the question you will answer in the box below.

Read all parts of your chosen question before you begin. Do not repeat your response in different parts of the question.

Candidates must complete their assessments individually under teacher supervision, in accordance with the NCEA Assessment and Examination Rules and Procedures. The material submitted for assessment must be the candidate's own work.

Candidates are not permitted to access any resources (either in hard copy or online) other than those supplied in the assessment itself.

Schools, teachers, and candidates are not permitted to share or discuss the assessment or their assessment responses with any other schools, teachers, or candidates until after the final date for submission (30 October 2024).

The use of chatbots, generative AI, paraphrasing tools, or other tools that can automatically generate content is not permitted and material generated by these tools should not be submitted as part of the candidate's work.

(Assessment Specifications, NZQA 2024)



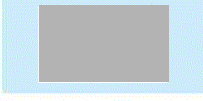

OR: QUESTION THREE: Network communication protocols

The table below shows four layers of the internet protocol suite.

- (a) Complete the table below by placing the correct protocol into each cell. Two of the protocols have been completed for you.

Protocols

HTTP, Ethernet, IPv4, UDP, Wireless LAN, DNS, TCP, IPv6, SCTP, FTP, HDLC.

Layer	Protocol 1	Protocol 2	Protocol 3
	HTTP	DNS	FTP
	SCTP	UDP	TCP
		IPv6	IPv4
	HDLC	Ethernet	Wireless LAN

Source: <https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:the-internet-protocol-suite/a/the-internet-protocols>

- (b) Explain HTTP and HTTPS.

In your response:

- compare and contrast them
- highlight the implications for data transmission(what does this mean??)
- provide specific examples of how each protocol should be used.

HTTPS is how it makes a secure connection to the server while HTTP is the process of sending the data through the connection. Its better to ensure a safe connection with HTTPS and then be able to send fast messages with HTTP. HTTPS should be used to create a safe connection, while HTTP should be used to send data through the connection.



RESOURCE A

Encapsulation and de-encapsulation



Source: <https://www.computernetworkingnotes.com/ccna-study-guide/data-encapsulation-and-de-encapsulation-explained.html>

Refer to Resource A to support your response to part (c) below.

- (c) (i) How are encapsulation and de-encapsulation utilised in network communication protocols?

Encapsulation is used by adding on headers to data that tells it important instructions like telling it how and where it needs to send and actually sending it while decapsulation is the opposite, see resource A, as it removes the headers and trailer and leaves only the data. This method allows for secure communication in the network.

- (ii) Explain why they are important features of network communication protocols.

It is extremely important to tell data how and where it needs to be sent. If you wanted to send a letter to somebody, would you just write down the message and just hope it somehow makes it to its destination? You need to tell the data how it needs to be sent, if its better to send it faster or safer, and where it needs to go, otherwise it obviously won't make it where you want it to go. Which is what the encapsulation process does. Decapsulation is just as important, otherwise you could end up receiving all of the data, including the headers which could make it impossible to determine which data is actually the piece you want, so its important to remove them after you get the data.

- 
- (iii) What problems could occur at the **transport layer** and **network layer** of the internet protocol suite if a packet was not de-encapsulated?

You would end up getting the data mixed in with both the network headers and the transport headers data and it could end up a mess and impossible to read.

RESOURCE B

'First in, first out' (FIFO) or 'First come, first serve scheduling' (FCFS) queuing



Source: <https://book.systemsapproach.org/congestion/queuing.html>

Refer to Resource B to support your response to part (d) below.

- (d) (i) What would likely occur within the UDP protocol if UDP packets were to arrive at a FIFO or FCFS queue with no free buffer space?

The would likely get lost as the place it needs to go is full and it doesn't have as good file loss detection as TCP as seen in Resource B (b).

- 
- (ii) Explain the process that the TCP protocol would likely undertake if TCP packets were to arrive at a FIFO or FCFS queue with no free buffer space.

It would keep checking if the data was transmitted properly, and if it wasn't, it would send the data again until there is free space for it to join the queue, as seen in Resource B (a)

- (iii) Compare and contrast what the end user would likely experience at the application level if they were using TCP or UDP protocols for video conferencing and the FIFO or FCFS queue had limited buffer space.

A TCP user would experience a secure connection and if the packets are all being sent slowly, it would be unlikely for the queue to fill up and cause buffering.

A UDP user would have a pretty terrible time because the queue would be overloaded with fast data packets and would end up losing a lot of them, making the end result a mess with lots of lag and buffering.



RESOURCE C

The CIA triad



Source: <https://www.linkedin.com/pulse/cia-triad-joseph-stephen/>

The CIA triad has three components: Confidentiality, Integrity, and Availability.



Source: <https://securityscorecard.com/blog/what-is-the-cia-triad/>

Refer to Resource C to support your responses to parts (e) and (f) below.

Secure sockets layer (SSL) and transport layer security (TLS) are foundational technologies for securing communications over computer networks. With the evolution from SSL to TLS, understanding these protocols is crucial for ensuring secure data transmission.


- (e) (i) Explain the purpose of SSL/TLS and how it contributes to secure communications over the internet.

TLS encrypts the sent data to make sure that communications are not compromised, especially when sending confidential data.

- (ii) Explain the process of a TLS handshake, including the steps involved and the purpose of each step. Be sure to mention the roles of certificates and keys in this process.

The 3 way handshake involves the client sending a syn (Synchronise) bit to the server it wants to connect with. The server send both the syn bit as well as an ack (acknowledge) bit which confirms the connection. Finally the client sends the ack bit which finalises the connection.

Then the server will generate some random data and will create a key and then send the data and a copy of the key to the client. Once the client receives the key, it will encrypt the data using the key and sent it back towards the server which will decrypt the data using its own key, to make sure that the connection is working. Then you can begin sending data to the server without worrying about people stealing it.

- 
- (iii) Consider a scenario where an attacker is capable of intercepting and altering communications between a client and a server. Explain how SSL/TLS can protect against such an attack, specifically focusing on the aspects of confidentiality, integrity, and authentication.

Using the previous method, TLS makes sure that even if the data is intercepted, it will only be able to be decrypted by the people with the key, which the interceptor won't have. So the hacker won't be able to access the data, but the keyholders will be able to access the reliable data at any time.

- (f) Critically analyse how network communication protocols contribute to ensuring the confidentiality, integrity, and availability of data within a connected environment. You may discuss areas from your studies where maintaining the confidentiality, integrity, and availability of data during network transmission is important.

You can use the options below as prompts, or you can discuss an area that you have studied in class:

- quantum computing
- artificial intelligence (AI)
- edge computing and IoT
- 5G technology
- blockchain technology
- machine learning in security.

By encrypting data in such a way that only quantum computers would be able to decrypt, making sure that there is no data loss during transmission, and making it only accessible to individuals with the right key, these network communication protocols ensure the confidentiality, integrity and availability of the data. It is especially useful in cases such as entering your bank information into a website to pay for something, as it will prevent the private data from being stolen and looked at, and you definitely don't want strangers learning all of your credit card information.

Achievement

Subject: Digital Technologies

Standard: 91908

Total score: 03

Question	Grade score	Marker commentary
Network communication protocols	A3	<p>The candidate has provided a basic description of network communication protocols. However, most explanation was at surface level, lacking in-depth, technical detail or advanced analysis. While they mentioned some protocols like TLS and SSL, they did not deeply explore these or connect them to broader contexts or implications.</p> <p>The responses were straightforward, and greater complexity and more detailed scrutiny would be needed to gain a higher grade.</p> <p>The analysis remained basic, focusing on general facts about network security, without delving into the complexities or offering deeper insights into how various protocols interact or are implemented in varying scenarios.</p> <p>The response could have been further improved with insightful conclusions, imaginative connections, or justified predictions about the future of network communication protocols.</p>