Mana Tohu Mātauranga o Aotearoa
New Zealand Qualifications Authority

Level 3 Digital Technologies 2024

91908 Analyse an area of computer science

EXEMPLAR

Excellence

TOTAL 07

Instructions

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

- complexity and tractability (page 3)
- network communication protocols (page 11)
- big data (page 21).

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 TWO: 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	TCP	UDP
	IPv4	IPv6	
	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
- provide specific examples of how each protocol should be used.

HTTP(Hyperlink Transfer protocol) is a protocol in the application layer of the TCP/IP model. It involves communication between devices, software applications and the web. HTTPS is the same as HTTP, however it has a (S), meaning that is ensures a secure connection. HTTPS provides a more secure, safe, and reliable communication than HTTP. Through the use of TLS(Transport Layer Security), a protocol that ensures a encrypted, safe, reliable connection. Connection through HTTP becomes secure resulting in HTTPS.

When data is transmitted over the internet with HTTP, it is unencrypted, with a lack of security. It also doesn't make sure the communication between two devices is encrypted This results in data being susceptible to potential hackers and even unauthorised people intercepting the communication. A type of cyber attack like this is called the “Man in the middle attack”, which is when an unauthourised user is intercepting communication between two devices without them knowing, this results in the data being transmitted able to be seen by the unauthourised person. eg. if sensitive information like passwords were sent across through a unsafe and unencrypted communication, hackers could gain access to that.

HTTPS should be used to ensure a encrypted connection, to make sure that an unauthorized individual isn’t able to intercept a communication, gaining access to possible sensitive information. A good example is google, when a site can’t ensure a encrypted connection, then it

will display ‘Not secure’ at the top of the webpage.

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 and de-encapsulation are used to manage and organise data flow between network communication protocols. Each step of encapsulation and de-encapsulation process involves either adding or removing headers and trailers. Encapsulation involves adding data header/trailers as it goes down the TCP/IP stack(sending data). De-encapsulation involves removing the data header/trailer, with it going up the TCP/IP stack(receiving data). Encapsulation and de-encapsulation are used to send data in a reliable way.

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

Encapsulation and de-encapsulation are both important features of network communication protocols. Both features allow for good management of data flow, it allows for the separation of protocols in the layers of the TCP/IP model. The separation of protocols means that each protocol can be easily organised, manageable , and tracked. As each layer provides adding something different e.g. transport layer could involve adding a tcp header, and networ layer adding IP header. Therefore it allows for network communication protocols to be seperated, also making it easier to understand. Again resulting in a concise, manageable flow of 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?

De encapsulation involves the removing of headers and trailers of data, receiving the sent data. The network layer of the internet protocol suite involves adding an IP header, which indicates its source and destination IP address. While the transport layer involves adding a TCP header, which make sures there is a reliable communication, to get data sent effectively. If a packet was not de-encapsulated, it would mean it wouldn't goes through all the steps up to the application, thus meaning it would not be able to present the data effectively, and would not be readable. If a packet was not de-encapsulated it would result in data transmission being unreliable.

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?

UDP(User Datagram Protocol) is a connection less protocol in the transport layer. If UDP packets were to arrive at a FIFO queue with no buffer space, it would result in those UDP packets being lost, and thus not being received.

(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.

Latency

ensures in order packets, all packets to be there

Retransmits any lost packets

TCP(Transmission Control protocol) is a connection-based protocol in the transport layer. If TCP packets were to arrive at a FIFO with no free buffer space. It would queue and wait for the next available buffer. This is because TCP ensures that all packets are received, in order. TCP also has error checking, if there were to be a problem with a packet, it would ask for retransmission of the packet, to ensure that all packets are received. Flow control is also part of TCP, is able to manage packet flow, and doesn't care about how long it takes, it wants all the packets to be received. Therefore TCP packets would queue up, if there were to be no free buffer spaces as it ensures a reliable secure connection.

(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.

TCP and UDP are both protocols used to transmit data. However they both have their differences.

TCP

advantages

- reliable and accurate communication
- flow and congestion control
- retransmits any lost packets(error detection)
- Checksum
- Secure communication due to tcp 3 way handshake

Disadvantages

- can be slow due to it ensuring all packets are sent & received
- Latency
- Establishing a connection
- Unreliable, if fast transmission of data is required, eg, Gaming.

TCP being used for video conferencing with a limited buffer space would result in a secure, reliable connection. However it would be quite slow. At the application layer. the end user may experience buffering due to packets being transmitted at a slow rate.

UDP

advantages

- Fast, efficient flow of data.
- Doesn't require a connection

Diadvantages

- Loss of packets due to limited buffer flow
- No flow, congestion control

- Unreliable if accurate transmission of data is required, eg Files

UDP being used for video conferencing with a limited buffer space would result in fast transmission of data. However it would also lead to packet loss, due to the limited buffer space. As with UDP packets lost, will not be resent. At the application layer, the end user may experience a loss of data in some areas. However it may not be as noticeable if FIFO queue flows efficiently.

It can be seen that both protocols have their advantages and disadvantages and both would have effects at the application layer for the end user.

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 is a cryptographic protocol designed to ensure encrypted, and secure communication across the internet, it ensures that no unauthorized individual is intercepting the communication thus reducing the possibility of cyber attacks like the man in the middle happening TLS is able to be used with HTTP, which results in HTTPS. HTTPS is now widely used over the world and is able to ensure secure communication over the internet.

(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.

TLS handshake is used to set up a secure, encrypted connection, between two devices. TLS uses digital certificates, the use of digital certificates allow for a company authentication. We can demonstrate this by using Bob and the Bank.

1. Bob sends a client "Hello" message to the bank.
2. Bank responds with "Helllo" message aswell, and with it, is its digital certificate.
3. Bob server observers the digital certificate and decrypts with CA public key
4. Bob generates a session key and encrypted it with the Bank's public key and sends it to the bank.
5. The bank will now decrypt the session key with its private key.
6. Now both Bob and the bank have session key to communicate in a encrypted, and safe, to ensure there is no possibly of the unauthorised individual intercepting the communication

In step 2. we can see a digital certificate, digital certificates are granted by a CA(Certificate Authourity), it is when the Bank's public key gets encrypted with the CA's private key. This shows that the CA trusts that the Bank is authentic, and not someone else. As to get a digital certificate you need to prove they are a legitimate company. If Bob's browser were to get a different company public key or a different digital certificate, it would terminate the communication. Therefore it can be seen that TLS ensures a reliable, secure communication, making sure that no unauthorized individuals can intercept the communication.

(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.

TLS can protect against attackers. When setting up the TLS handshake the client makes sure that they are talking to who their suppose to be talking to(through the use of digital certificates). To get a digital certificate the server would need to prove they are a legitimate company to a Certificate Authourity. If clients browser were to get a different company public key or a different digital certificate, it would terminate the communication. Also at the end steps of a TLS handshake, a session key is generated, which ensures that the connection will only be for that time, impacting th confidentiality, of any data transmitted during the connection. Thus it can be seen that TLS protection against attackers is very strong and will terminate the connection, if it detects any false information supplied by the server. TLS also ensures that data sent across the internet is not in plain text, using hashing to prevent this.

(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.

Due to the growing world of technology, which will keep on growing, the transmission of data remains so important. Data that is not secure during transmission, showcases so many risks. For example, if someone were to send sensitive information like credit card, or passwords across a unprotected internet connection, it would result in a bad consequences if that data were to be taken by a unauthourised individual.

The use of ideas such as Artificial Intellingence and machine learning in security is able to give huge impacts on the internet,as it continuous to grow. Companies are able to use mathematical analysis through the use of AI and machine learning. As AI continues to keep growing, it can help with the management and availability of data flow within an environment. AI could be able to records on how well a company's network is performing, or even keep records about maintenance of companies systems. Systems across the internet will only keep better with the help with AI, such as being able to optimise and prevent failures happening across the internet. This wil keep helping the management of data flow across the internet to get quicker. Also helping the transmission of data across the internet to keep getting secure, quick and reliable.

Network protocols such as TCP make sure that data transmission is secure with a 3 way handshake, and reliable with error checking. While IPv4 or Ipv6 ensure that packets get to their destination, in the most efficient way. Thus all network communication protocols work together to ensure secure and quick data transmission, and will only keep getting better as modern techonology progresses.

Excellence

Subject: Digital Technologies

Standard: 91908

Total score: 07

Q	Grade score	Marker commentary
Network communication protocols	E7	The candidate employed specific examples like TCP/IP protocols ensuring secure data transmission and IPv4/IPv6 in network routing, showing a deep understanding of how the protocols function and are implemented in real-world scenarios. This fulfils the requirement for providing examples and offering a detailed explanation. The discussion on leveraging AI to analyse and secure networks demonstrated innovative thinking, connecting advanced technology with traditional network security methods. This approach aligns with the excellence criteria of exploring less obvious implications and making innovative connections. The student submission extended beyond basic description to explore how these protocols can adapt to upcoming challenges, such as increased data traffic and security threats. This foresight and predictive thinking utilise the higher-level cognitive skills that are required for an Excellence grade. The response went beyond simply explaining network communication protocols; it critically examined how these protocols support the maintenance of data confidentiality, integrity, and availability. This was achieved through detailed discussion of various protocols and mechanisms, such as AI and machine learning in security, which aligns with the criteria for a critical analysis that includes making justified generalisations and suggesting improvements. The analysis was clear, logically structured, and comprehensive, thoroughly covering the crucial roles of network communication protocols in security and efficiency, which is vital for achieving Excellence. To gain a score of 08, the candidate could have provided richer evidence of understanding, and linked with other areas – for example: • potential benefits of AI-driven anomaly detection for network security • quantum computing in breaking current encryption methods • zero trust architecture (ZTA). While these are not specifically asked for in the standard, they are examples of where more depth, breadth, and connections are more clearly apparent. The candidate's response showed some insightful conclusions, but these lacked innovative and imaginative connections and the exploration of less obvious implications, and therefore were not fully justified.