SECTION A

Q1

a) From administrator's point of view, what is a network? (2 marks)
b) Outline Four advantages of a network (4 marks)
Resource sharing: Networks allow users to share resources, such as printers, files, and applications, which can be more cost-effective than purchasing these resources for individual users.

Improved communication: Networks enable communication between users, which can improve collaboration and productivity.

Centralized management: Networks can be centrally managed, allowing administrators to monitor and control access to resources and data.

Scalability: Networks can be expanded easily to accommodate additional users or devices as needed.
c) What is the role of physical layer? (2 marks)

transmission of bits
synchronization of bits

d) What is a virtual LAN (2 marks)
A virtual LAN (VLAN) is a logical network that is created by grouping devices together based on their function, location, or other criteria, regardless of their physical location on the network. VLANs allow network administrators to isolate traffic between different groups of users, improving security and network performance.

e) What is hybrid topology? State its main advantage (3 marks)
A hybrid topology is a combination of two or more different types of network topologies. Its main advantage is that it can provide the benefits of multiple topologies, such as the scalability of a star topology and the redundancy of a mesh topology.
f) What is transmission media? (3 marks)

Transmission media refers to the physical communication channels used to transmit data from one device to another. Examples of transmission media include copper wire, fiber optic cable, and wireless radio waves.

Q2

a) What is secret key encryption? (4 marks)

Secret key encryption, also known as symmetric-key encryption, is a type of encryption technique that uses the same key for both encryption and decryption of data. In secret key encryption, the sender and receiver of a message share a common secret key, which is used to encrypt and decrypt the message. This key is kept secret and must be known by both the sender and the receiver to exchange encrypted messages.

b) State three factors affecting channel capacity (3 marks)
Bandwidth: The bandwidth of a communication channel is the range of frequencies that the channel can carry. The greater the bandwidth, the higher the channel capacity, as more information can be transmitted in a given amount of time.

Noise: Noise is any unwanted signal that interferes with the transmission of the message. The presence of noise in the communication channel reduces the channel capacity, as it increases the error rate and decreases the reliability of the transmission.

Modulation technique: Modulation is the process of encoding the information onto the carrier signal. The modulation technique used affects the channel capacity, as some modulation techniques allow for higher data rates than others. For example, quadrature amplitude modulation (QAM) can transmit more data than amplitude modulation (AM).

c) Give the three kinds of digital-to-analog conversion (3 marks)
Pulse Width Modulation (PWM): In PWM, the width of a pulse signal is varied to represent the amplitude of the analog signal. A digital signal is used to control the width of the pulses, which are then passed through a low-pass filter to obtain the corresponding analog signal.

Delta-Sigma Modulation: In delta-sigma modulation, a high-frequency digital signal is used to encode the analog signal by generating a stream of 1s and 0s. The output of the delta-sigma modulator is then passed through a low-pass filter to obtain the corresponding analog signal.

Digital-to-Analog Converter (DAC) Chip: A DAC chip is a specialized electronic circuit that converts digital signals into analog signals. The chip takes in a digital signal as input and produces an analog signal as output. There are different types of DAC chips, including binary-weighted DAC, R-2R ladder DAC, and segmented DAC.

d) What is multiplexing? (3 marks)
Multiplexing is the technique of combining multiple signals into a single signal for transmission over a communication channel. In multiplexing, each signal is assigned a unique identifier or address, which is used to demultiplex the combined signal at the receiving end.

e) A switch can be divided into two major categories. Name them (2 marks)

Circuit Switches: Circuit switches create a dedicated physical connection between two communication devices for the duration of the communication session. The connection remains fixed until the session is complete and is released only when the devices disconnect.

Packet Switches: Packet switches transmit data in the form of small data packets across a shared network. The packets are individually addressed and transmitted independently, and they may

take different routes to reach their destination. Packet switches dynamically allocate bandwidth to each packet as needed, and they can handle multiple communications simultaneously.

SECTION B

Q3

a) With the aid of diagrams, explain the following types of computer network topologies

i. Bus topology

In a bus topology, all nodes are connected to a common communication channel or bus. The communication channel is typically a coaxial cable, twisted pair cable, or optical fiber. Each node in the network communicates directly with the bus, and data is transmitted in both directions along the bus.

ii. Tree topology

In a tree topology, multiple star topologies are connected together in a hierarchical or tree-like structure. The central hub or switch of each star topology is connected to a main bus or backbone cable, which serves as the main communication channel for the entire network.

b) What is the computer system? (3 marks)

A computer system is a combination of hardware, software, and peripheral devices that work together to perform specific tasks or operations. The hardware component of a computer system includes the physical components such as the processor, memory, storage devices, input/output devices, and other peripheral devices. The software component includes the operating system, application programs, and utility programs that allow users to perform tasks on the computer system. Peripheral devices such as printers, scanners, and cameras are also part of a computer system as they provide additional functionality to the system. Together, the hardware, software, and peripheral devices of a computer system work together to provide users with a functional and productive computing experience.

c) State four ways in which networks are classified (4 marks)

Scale: Networks can be classified based on their size or scale, ranging from a small local area network (LAN) that connects devices within a small geographic area to a wide area network (WAN) that connects devices across a large geographic area.

Topology: Networks can also be classified based on their physical or logical topology, such as a bus, star, ring, or mesh topology.

Transmission medium: Networks can be classified based on the type of transmission medium used to transmit data, such as wired (e.g. Ethernet, fiber optic) or wireless (e.g. Wi-Fi, cellular) networks.

Ownership: Networks can be classified based on their ownership or control, such as private networks that are owned and operated by a single organization, or public networks that are owned and operated by a service provider or government agency.

d) State two advantages of star topology (2 marks)

Centralized management: In a star topology, all nodes are connected to a central hub or switch, which makes it easier to manage and troubleshoot the network. The centralized architecture allows network administrators to monitor the network and quickly identify and resolve any issues that arise.
Scalability: Star topology is a scalable network architecture, as new nodes can be added to the network easily by simply connecting them to the central hub or switch. This makes it easy to expand the network as the organization grows or as new devices are added to the network.

Q4

a) all security threats are intentional. What is the meaning of this statement? (1 mark)

The statement "all security threats are intentional" means that every security threat or attack is carried out with the intent of causing harm or gaining unauthorized access to a system, network, or device. This statement implies that security threats are not accidental, but rather are planned and executed by attackers with malicious intent. However, it is important to note that some security threats can also result from unintentional actions, such as human error or software bugs, which can create vulnerabilities that attackers can exploit.

b) State and explain five security threats (12 marks)

1. Malware: Malware refers to any malicious software that is designed to damage or disrupt computer systems, networks, or devices. Malware can include viruses, worms, trojans, ransomware, and other types of malicious code. Malware can spread through email attachments, downloads, or through vulnerabilities in software or operating systems.
2. Phishing: Phishing is a social engineering attack where an attacker attempts to trick a user into providing sensitive information, such as usernames, passwords, or credit card numbers. Phishing attacks can occur through email, instant messaging, social media, or other channels. Phishing attacks can be difficult to detect, as the attacker may use legitimate-looking websites or emails to deceive the user.
3. Denial of Service (DoS) attacks: DoS attacks are a type of cyber attack that is designed to overload a system, network, or website with traffic, making it inaccessible to users. DoS attacks can be launched by sending a large number of requests to a website or network, or by exploiting vulnerabilities in software or operating systems. DoS attacks can disrupt business operations, cause financial losses, and damage reputations.
4. Man-in-the-middle (MitM) attacks: MitM attacks are a type of cyber attack where an attacker intercepts and modifies communication between two parties. MitM attacks can

occur in email, instant messaging, social media, or other communication channels. The attacker can modify or steal sensitive information, such as login credentials, credit card numbers, or personal data.

5. Insider threats: Insider threats refer to security threats that come from within an organization. Insider threats can be intentional, such as an employee stealing sensitive data, or unintentional, such as an employee accidentally sharing sensitive information. Insider threats can be difficult to detect, as the attacker may have legitimate access to the systems and data they are targeting. Organizations can mitigate insider threats through employee training, access controls, and monitoring systems.

Q5

a) Understanding analog transmission, explain the following:
i) Bandpass (2 marks)

i) Bandpass refers to a range of frequencies within a signal that are transmitted or processed. In analog transmission, bandpass refers to the frequency range of the analog signal that is transmitted over a communication channel. The bandpass of an analog signal is typically defined as the difference between the highest and lowest frequencies that are transmitted over the channel. Bandpass filtering is used to select or isolate a specific range of frequencies within an analog signal. In communication systems, bandpass filters are used to remove unwanted frequencies and noise from the signal, ensuring that the transmitted signal remains within the specified bandpass range.

ii) Low-pass (2 marks)

ii) Low-pass filtering is a signal processing technique that removes all frequencies above a certain cut-off frequency, allowing only low-frequency components to pass through. In analog transmission, a low-pass filter is used to remove high-frequency components from the transmitted signal, ensuring that the signal remains within the specified bandwidth and does not interfere with other channels. Low-pass filtering is commonly used in communication systems to remove noise and interference from the signal and to ensure that the signal is transmitted without distortion. For example, in an AM radio system, a low-pass filter is used to remove high-frequency noise and interference, allowing only the low-frequency audio signal to be transmitted.

b) State three characteristics of an analog signal (3 marks)

Q6

a) Explain the following switching techniques
i) connectionless (2 marks)

i) Connectionless switching is a communication technique where data packets are transmitted independently without establishing a dedicated connection between the sender and receiver. In connectionless switching, each packet contains all the information required to route it to its destination, including the source and destination addresses. Each packet is transmitted independently, and the routing information is used to forward the packet through the network. Connectionless switching is commonly used in applications where a small amount of data is transmitted, and the cost of establishing a dedicated connection is too high.

ii) Connection oriented (2 marks)

ii) Connection-oriented switching is a communication technique where a dedicated connection is established between the sender and receiver before transmitting data. In connection-oriented switching, a virtual circuit is established between the sender and receiver, and all data packets are transmitted over this circuit. Once the communication is complete, the virtual circuit is terminated. Connection-oriented switching is commonly used in applications where a large amount of data is transmitted, and the cost of establishing a dedicated connection is justified by the performance benefits. Connection-oriented switching provides better reliability and performance than connectionless switching, as the dedicated connection ensures that data is transmitted in the correct order and that all packets are received without errors.

b) Explain the following
i) circuit switching (3 mks)

Circuit switching is a method of establishing a dedicated communication path between two nodes in a network. In circuit switching, a connection is established between the two nodes, and the entire communication channel is reserved for their use until the communication is complete. During the communication, the resources used to establish the connection remain dedicated to that connection and are not available to other users. Circuit switching is commonly used in telephone networks, where a dedicated circuit is established between two callers for the duration of their conversation.

ii) Message switching (3 marks)

Message switching is a communication method where messages are sent from one node to another through intermediate nodes. In message switching, the entire message is transmitted from one node to another, and each intermediate node temporarily stores the message until it can be forwarded to the next node. This process continues until the message reaches its destination node. Message switching is a slower method of communication than circuit switching, as each node must store and forward the entire

message. However, it is more efficient than circuit switching for transmitting messages to multiple nodes.

iii) Packet switching (3 marks)

Packet switching is a communication method that divides data into small packets and sends them individually from one node to another. In packet switching, each packet is transmitted from one node to another independently, and each packet can take a different path to its destination. Intermediate nodes forward each packet based on routing information contained in the packet header. Once all the packets arrive at the destination node, they are reassembled into the original message. Packet switching is a more efficient method of communication than circuit switching or message switching, as it allows multiple users to share network resources and can dynamically adjust to network congestion. Packet switching is the basis for modern computer networks, including the Internet.

Q7

a) with the aid of diagrams state and explain THREE types of errors (9 marks)

b)Explain the following error correction mechanisms:

i) Error detection (2 marks)

Error detection refers to the process of detecting whether errors have occurred during data transmission, storage or processing. Error detection is an essential part of reliable communication and data storage systems, as it helps ensure that data is transmitted and stored accurately. There are various error detection techniques, such as checksums, cyclic redundancy checks (CRCs), and error-correcting codes.

ii) Parity check (2 marks)

Parity check is a simple error detection technique that involves adding an extra bit to a block of data. The parity bit is set to 1 or 0 depending on the number of 1s in the data block. If an error occurs during transmission, the receiver can detect the error by checking the parity bit. If the number of 1s in the received data block is odd and the parity bit is even, or if the number of 1s is even and the parity bit is odd, then an error has occurred. Parity check is a basic error detection technique and is commonly used in computer memory systems.