Q1) What is SDLC?

Ans) Software Development Life Cycle is a step-by-step process for developing software. We can say that it is a structured way to make sure software projects are successfully completed. Below are the key stages in it. They are as follows:

1.Planning

2.Designing

3.Building

4.Testing

5.Deployment

6.Maintenance

Q2) Why SDLC?

Ans) SDLC provides a structured approach to software development & its step-by-step process helps manage the complexities of software development and minimizes the risk of issues or failures. So, following such framework will lead to a much higher quality software that is also way more reliable.

Q3) What are the different stages of SDLC?

Ans) The Software Development Life Cycle (SDLC) consists of several key phases that guide the software development process. The core stages include:

1. Planning and Requirements Gathering: This initial phase involves collecting customer requirements and planning the project approach.

2. Design: After requirements are gathered, the software solution is designed.

3. Development/Coding: This stage involves the actual building of the software.

4. Testing: The software undergoes thorough testing to ensure quality and functionality.

5. Deployment: Once tested, the software is implemented and released.

6. Maintenance and Monitoring: The final phase involves maintaining and monitoring the software after deployment.

Q4) What are the different models of SDLC? Please list them with description (4 lines minimum)?

Ans) Below are the main SDLC models listed as well:

1. Waterfall Model:

The Waterfall model is one of the traditional SDLC models that follows a sequential development process. It is a linear model in which the development process is divided into distinct phases, such as requirements gathering, design, implementation, testing, and deployment. Each phase must be completed before moving on to the next, and there is little to no overlap between the phases. This model is best suited for projects with well-defined and stable requirements.

2. Spiral Model:

The Spiral model is another established model in software development methodologies. It combines the features of the Waterfall and Prototyping models, incorporating an iterative approach with a focus on risk management. The model divides the development process into multiple cycles, each of which includes planning, risk analysis, engineering, and evaluation. This model is particularly useful for large, complex projects where the requirements are not well-defined and may change over time.

3. Agile Model:

The Agile model is the most common model used in today's software industry. It combines iterative and incremental process models, focusing on process adaptability and customer satisfaction through rapid delivery of working software products. The Agile model involves cross-functional teams working simultaneously on various areas, including planning, design, development, and testing. This approach emphasizes collaboration, frequent feedback, and the ability to respond to changing requirements.

4. Prototyping Model:

The Prototyping model incorporates prototypes of software components into the development process. It is particularly useful when gathering and implementing user requirements, as it allows for early testing and feedback. In this model, a basic version of the software is developed, and then iteratively refined based on user feedback until the final product is achieved. This approach helps to identify and address user requirements more effectively, reducing the risk of developing a product that does not meet the user's needs.

Q5) What are the different Network Types?

Ans) There are several main types of computer networks:

1. Local Area Network (LAN): A LAN is a network that interconnects devices within a relatively small geographical area, such as a home, school, computer laboratory, or office building.

2. Wide Area Network (WAN): A WAN is a network that covers a large geographical area, such as a country or continent. WANs are used to connect LANs and other networks together.

3. Metropolitan Area Network (MAN): A MAN is a network that covers an area larger than a LAN but smaller than a WAN, such as a city or a large campus.

4. Personal Area Network (PAN): A PAN is a network for interconnecting devices centered around an individual person's workspace. Bluetooth and infrared are common PAN technologies.

5. Wireless Local Area Network (WLAN): A WLAN is a type of LAN that uses wireless technologies, such as Wi-Fi, to connect devices.

6. Storage Area Network (SAN): A SAN is a dedicated high-speed network that provides access to consolidated, block-level data storage.

7. Campus Area Network (CAN) : A CAN is a network that interconnects multiple LANs within a limited geographical area, such as a university or corporate campus.

8. Home Area Network (HAN): A HAN is a residential network that connects devices within a home, such as computers, smartphones, and home automation systems.

The specific network type chosen depends on factors such as the geographical area to be covered, the number of devices, the required speed and bandwidth, and the available infrastructure and resources.

Q6) What are the types of servers?

Ans) There are several main types of servers:

1. Web Servers: These servers store and deliver web pages, files, and other content in response to requests from web browsers and other clients over the internet or a local network.

2. Application Servers: These servers run business logic and application code, processing requests and delivering dynamic content, such as web applications, e-commerce platforms, and content management systems.

3. File Servers: These servers store and manage access to shared files, documents, and other data over a network. They allow multiple users to access the same files.

4. Database Servers: These servers host and manage database systems, processing queries and data requests from applications and users.

5. Email Servers: These servers handle the sending, receiving, and storage of email messages, as well as related functions like spam filtering.

6. Print Servers: These servers manage and distribute print jobs to networked printers, allowing multiple users to access shared printing resources.

7. DNS Servers: These servers translate human-readable domain names into the IP addresses needed for computers to communicate over the internet.

8. FTP Servers: These servers facilitate the transfer of files between computers over a network using the File Transfer Protocol (FTP).

9. Media Servers: These servers store and stream multimedia content, such as videos, music, and images, to client devices on demand.

10. Virtual Servers: These are servers that run on virtual machine software, allowing a single physical server to host multiple virtual servers and operating systems.

Q7) What do you know about DNS?

Ans) DNS stands for Domain Name System. It is an hierarchical decentralized naming system for computers, services & other resources connected to the internet. It translates human-readable domain names into the IP addresses that computers use to identify and communicate with each other.

Q8) What is TCP & UDP? What is the difference?

Ans) TCP is a reliable, connection-oriented protocol. UDP is a fast, connectionless protocol. The key differences are as follows:

TCP ensures reliable, ordered data transfer, while UDP does not guarantee delivery or order.

TCP is slower but more reliable, while UDP is faster but less reliable.

TCP is used for applications that require reliability, UDP for those that prioritize speed.

Q9) What do you know about mac address? What is the difference between Mac address and IP address?

Ans) MAC address is a unique hardware identifier for a network device, used for local communication. IP address is a logical identifier used for routing and communication across networks. The key difference is that MAC addresses are local while IP addresses are used for broader network communication.

Q10) What is OSI Model?

Ans) OSI stands for Open Systems Interconnection. This model has a 7-layer framework for network communication. It is a conceptual framework used to describe the functions of a networking system. This model provides a standardized way to understand and discuss how different network components and protocols work together. The layers are:

1. 1. Physical Layer: It deals with the physical equipment involved in network such as cables & connectors.
2. 2. Data Link Layer: It is responsible for reliable data transfer between directly connected devices including error detection/Correction.

3. Network Layer: It handles the logical addressing and routing of data between different networks such as IP addressing & routing protocols

1. 4. Transport Layer: This layer ensures that end-of-end reliable data delivery including flow control, segmentation & error correction. (Ex : TCP/UDP)

5. Session Layer: Here, this layer establishes communication sessions between applications & also maintains as well as synchronizes these sessions.

1. 6. Presentation Layer: It involves formatting & encrypting data that is to be shared between applications ensuring compatibility.

7. Application Layer: The final layer represents the interface between the network & end user applications such as web browsers, email clients & file transfer protocols.

Q11) What is an IPv4 address? What are the different classes of IPv4?

Ans) An IPv4 (Internet Protocol version 4) address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves as a unique identifier for that device on the network.

The different classes of IPv4 addresses are:

1. Class A: These addresses are used for very large networks and have the first bit set to 0. The network portion of the address consists of the first 8 bits, leaving 24 bits for host addresses.

2. Class B: These addresses are used for medium-sized networks and have the first two bits set to 10. The network portion consists of the first 16 bits, leaving 16 bits for host addresses.

3. Class C: These addresses are used for smaller networks and have the first three bits set to 110. The network portion consists of the first 24 bits, leaving 8 bits for host addresses.

4. Class D: These addresses are used for multicast purposes and have the first four bits set to 1110.

5. Class E: These addresses are reserved for experimental and future use and have the first four bits set to 1111.

The different classes of IPv4 addresses are like different-sized buckets used to hold the devices on a network. Class A is a very large bucket, Class B is a medium-sized bucket, and Class C is a smaller bucket. The size of the bucket determines how many devices can be connected to the network.­­

Q12) What are the advantages of using VPN?

Ans) VPN stands for Virtual Private Network. Below are the different advantages of using VPN. They are listed as follows:

1. Enhanced privacy and security by encrypting your internet traffic

2. Access to geo-restricted content by connecting to servers in different countries

3. Protection on public Wi-Fi networks from eavesdropping and attacks

4. Bypassing internet censorship in countries with restrictions

5. Improved online anonymity by masking your IP address

6. Simultaneous protection for multiple devices

Q13) What are the different types of VPN? Explain the following with 1 statement each.

Ans) The main types of VPNs are:

1. Remote Access VPN (Access VPN): Allows remote users to securely connect to a private network.

2. Site-to-Site VPN: Connects two networks, such as branch offices, over a public network.

3. Intranet VPN: Securely connects employees within an organization's private network.

4. Extranet VPN: Securely connects an organization with its external partners or clients.

5. SSL/TLS VPN: Uses Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols to provide secure remote access.

6. Internet-based VPN: Utilizes the public internet to establish a secure connection between devices or networks.

7. Trusted VPN: Connects networks using a service provider's private, dedicated network infrastructure.

8. Untrusted VPN: Connects networks over the public internet, with the VPN provider serving as an intermediary.

Q14) What is Node & Link in terms of VPN?

Ans) Node: Nodes are the individual components that make up the VPN. Any device that is part of the VPN, including clients, servers, and network equipment.

- Remote client devices (e.g., laptops, smartphones, tablets) that connect to the VPN

- VPN servers or gateways that facilitate the VPN connection

- Network devices like routers, switches, or firewalls that are part of the VPN infrastructure

Link: A link in a VPN refers to the communication pathway or connection between the nodes. The links allow the nodes to communicate with each other securely over the public internet or other untrusted networks.

- The encrypted tunnel between a remote client and the VPN server

- The secure connection between two VPN sites or networks

- The data flow between different elements of the VPN infrastructure

Q15) What does network topology mean?

Ans) Network topology refers to the physical and logical arrangement of the components in a computer network, including a VPN. It describes how nodes (devices) are interconnected and how data flows between them.

Q16) What are the different types of network topologies?

Ans) Below listed are the different types of VPN network topologies.

1. Point-to-Point: Connects two remote sites directly over a VPN link.

2. Hub-and-Spoke: Centralized VPN server (hub) with multiple remote clients (spokes).

3. Mesh: All nodes interconnected, forming a fully meshed network.

4. Hybrid: Combines elements of other topologies for flexibility.

5. Cloud-Based: VPN hosted and managed in the cloud.

Q17) What is extended bus topology?

Ans) This topology extends basic bus topology by connecting multiple bus segments using repeaters/bridges for larger coverage and scalability. It is a Tree Topology.

Q18) What is the use of a router & how is it different from a gateway?

Ans) Routers connect and enable communication between different computer networks. Their primary function is to analyze data packet destinations and determine the optimal routing paths.

Gateways, on the other hand, serve as access points and bridges between disparate network environments. Their main role is to translate between different network protocols and standards to facilitate connectivity and data exchange across distinct networks.

While gateways may incorporate routing capabilities, the core difference is that routers are focused on internal network traffic flow, while gateways enable connectivity and translation between separate network domains.

Q19) Explain SMTP Protocol with diagram

Ans) SMTP (Simple Mail Transfer Protocol) is a standard protocol used for sending and delivering emails across the internet. It defines the communication between email clients (such as Outlook or Gmail) and email serves to facility the transfer of messages.

SMTP (Simple Mail Transfer Protocol):

- Standard protocol for sending and delivering emails over the internet

- Defines communication between email clients and servers to facilitate message transfer

- Email client initiates SMTP session with sending server, which then forwards message to receiving server

- Receiving server stores message in recipient's mailbox

- Key features include specifying sender/recipient, handling errors, supporting attachments, and enabling authentication/encryption

Q20) Differentiate between OSI & TCP/IP.

Ans) The OSI model provides a theoretical framework for network communication, while the TCP/IP model reflects the actual protocols and practices used on the internet and other IP-based networks.

OSI Model:

- Theoretical 7-layer model (Physical, Data Link, Network, Transport, Session, Presentation, Application)

- Defines the standards and protocols for each layer

- Provides a framework for designing and understanding network communication

TCP/IP Model:

- Practical 4-layer model (Link, Internet, Transport, Application)

- Based on the actual protocols used on the internet

- Simpler and more flexible than the OSI model

- Widely adopted and the de facto standard for internet communication

Key Differences:

- OSI is a conceptual model, while TCP/IP is an implementation-focused model

- OSI has more distinct layers, while TCP/IP combines some of the OSI layers

- TCP/IP is more widely used and better aligned with real-world internet protocols

- OSI is more comprehensive, but TCP/IP is more practical and prevalent on the internet

Q21) What is HTTP & HTTPS?

Ans) Here's a brief comparison of HTTP and HTTPS with their definitions:

HTTP (Hypertext Transfer Protocol):

Definition: The standard protocol for transmitting data between a web browser and web server.

HTTPS (Hypertext Transfer Protocol Secure):

Definition: A secure extension of HTTP that uses encryption to establish a secure, authenticated connection.

Key Differences:

- HTTP uses port 80, HTTPS uses port 443

- HTTP is unencrypted, HTTPS uses SSL/TLS encryption

- HTTPS provides server authentication and optional client authentication

- HTTPS protects against eavesdropping and data tampering

Q22) What is Low Level Design & High-Level Design?

Ans) HLD is a high-level, conceptual view of the system, while LLD is a more detailed, technical design of the individual components. Both are essential phases in the SDLC to ensure a structured and organized system development process.

High-Level Design (HLD):

- Focuses on the overall system architecture and major components

- Defines functional requirements and component interactions

- Establishes the logical design and system modules

- Provides a high-level blueprint for development

Low-Level Design (LLD):

- Focuses on the detailed implementation of individual components

- Defines technical specifications like algorithms, data structures, and programming logic

- Provides a detailed roadmap for developers to implement the components

- Deals with more granular, implementation-specific details

Q23) What is SRS (Software Requirement Specification)

Ans) The SRS document is a crucial artifact in the Software Development Life Cycle, as it comprehensively defines the requirements for the software system to be built.

Definition:

- SRS is a document that defines the requirements for a software system.

Purpose:

- Captures the complete set of requirements.

- Serves as a contract between the client and development team.

- Enables estimation, design, implementation, and validation.

Key Components:

- Functional requirements

- Non-functional requirements

- System interfaces

- Data requirements

- Other requirements

Importance:

- Ensures understanding of system scope and capabilities.

- Manages stakeholder expectations and reduces project failure risk.

- Provides a baseline for planning, development, and testing.

- Facilitates communication between client and development team

MCQ :

**SDLC MCQ**

1. A feasibility study using the SDLC model is conducted to

determine whether or not the project is technically possible

determine whether the proposal is financially viable

Both a and b ☑️

None of the above

2.A well-documented life cycle model aids in the detection of what during the development phase?

Inconsistencies

Redundancies

Omission

All of the above ☑️

3.How many lines of code does the Build & Fix Model suit for programming exercises?

100-200

300-400 ☑️

600-700

Above 800+

4.In which life cycle does regression testing play a significant role?

Waterfall model

V model

Iterative model

All of the above ☑️

5.What determines if the project should go forward?

feasibility assessment ☑️

opportunity identification

system evaluation

program specification

6.What is the most significant disadvantage of employing the RAD Model?

Developers/designers that are highly specialized and skilled are required. ☑️

Component reusability is improved.

Encourages client/customer input.

Increases component reusability.

7.Which of the following developmental models is incremental?

Prototyping, V model, Agile

Prototyping, RAD, Agile, RUP

Prototyping, V model, RAD, Agile, RUP ☑️

All of the above

8.Which of the following is an Agile development characteristic?

Shared code ownership

Test-Driven Development

Implement the simplest solution to meet today's problem

Continual feedback from customer

All of the above ☑️

9.Which of the following steps in the SDLC framework are valid?

Requirement Gathering

Software Design

System Analysis

All of the above ☑️

10.Who is in charge of system development, staffing, budgeting, and reporting, as well as ensuring that deadlines are met?

Project managers ☑️

Network engineers

Graphic designers

Systems analysts