What is the difference between a client and an end user?

Step 1:

Any computer hardware or software device that seeks access to a service offered by a server is referred to as a client in home and business networks. In a client-server architecture, clients are often thought of as the requesting programme or user. Clients are defined as customers or those who use services. A student receiving tutoring at a college writing centre is an example of a client.

The word "end user" is used in information technology to distinguish between the individual for whom a hardware or software product is built and the people who create, install, and maintain the product.

Step 2:

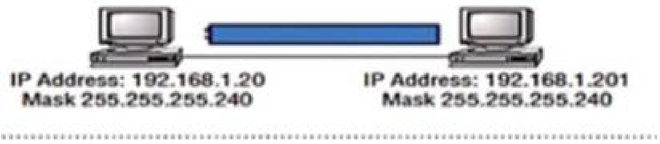
"Customer" is frequently used to refer to this function; the term "client" is typically reserved for people who use professional services (and a few others, like hotel guests). The service or product is directly provided to an end user or end consumer.

A customer is someone who pays you directly for your good or service. While a customer is a more general phrase, it is typically used in B2B (Business to Business) context. If a business approaches you about developing an app for an online marketplace where other SME companies can pay to be listed, that firm becomes your client, and other companies become that client's customers as well as end users of your app.

Any person who purchases a good, service, or subscription is referred to as a customer. He might or might not be the customer.

The individual who will utilise the product or service on a daily basis is the end user. The students and teachers who will be utilising your product, such as an online study course app, are its end users. The buyer of such thing may or may not be the final consumer (example, its a free app and you are getting money from the advertisers, thus, end users are not paying for the app).

A network administrator is connecting hosts A and B directly through their Ethernet interfaces, as shown in the illustration. Ping attempts between the hosts are unsuccessful. What can be done to provide connectivity between the hosts? IP Address: 192.168.1.20 Mask 255.255.255.240 IP Address: 192.168.1.201 Mask 255.255.255.240



Step 1: Answer

The straight-through wire has to be replaced with a crossover cable.

255.255.255.0 should be used as the subnet mask.

Step 2:

Explanation:

First, a crossover cable is required if two hosts are linked directly, as in the case of the graphic. Straight-through cables are ineffective. Second, the hosts are in various subnets because of their various masks. The easy solution is just to set both masks to 255.255.255.0 (/24).

You need to configure a server that is on the subnet 192.168.10.56/29. The router has the last available host address. Which IP will you assign to the server?

Step 1: Answer

192.168.19.26 255.255.255.248

Step 2: m

A /29, or the fourth octet's block size of 8, is 255.255.255.248. These are the subnets: 0, 8, 16, 24, 32, etc. The broadcast address for the 24 subnet is 31 because 192.168.19.24 is the 24 subnet and 32 is the following subnet. Only 192.168.19.26 is the correct answer

What kind of access method is CSMA/CD?

Answer: **option a contention**

Explanation for correct answer:

Contention-based media access refers to a method of transferring data over a network in which computers "contend for" or share media. When more than one system discovers a free network and tries to communicate, a data collision occurs, and the systems must retransmit. Because computers compete for the right to transmit data into the network media, CSMA/CD is known as a contention mechanism. For Ethernet networks, CSMA/CD is the standard access mechanism.

Explanation for incorrect answer

The administrator can assign a priority to requests for media access using **demand priority.** When there is a tie for media access, the highest-priority connection wins, making the demand priority approach ideal for time-sensitive applications. Demand priority networks necessitate the employment of a specialised network device to govern access. As a result, demand priority installation is more costly than alternatives like CSMA/CD.

In computer networking, carrier-sense multiple access with **collision avoidance** (CSMA/CA) is a network multiple access approach in which nodes use carrier sensing but only begin transmission after the channel is sensed to be "idle."

Collisions are possible in both CSMA/CD and CSMA/CA. As the number of hosts in the network grows, the likelihood of collisions grows as well. When using **token passing**, a host must hold the token, which is an empty packet, while transmitting data. The token is cycling the network at high speed.

The second most prevalent media access technique is tocken ring, which is specified in IEEE 802.5. However, due to Ethernet networking's dominance, tocken ring is a distant second.

A company is looking to share data between two platforms in order to extend their functionality. which feature enables communication between the platforms?

Step 1: Answer

application programming interface (API)

Application Programming Interface (API) feature is an option that permits platform connection.

Step 2: Explanation

Explanation:

An application programming interface is a piece of software that facilitates communication between two programmes (API). Application programming interfaces, or APIs, make it easier for apps to communicate data and functionalities in a secure and convenient way, which promotes innovation in software development.

By moving data from one interface to another, an API acts as a virtual middleman. A software platform's various components are connected by APIs to make sure that data gets to where it needs to be.

All the following statements about Approved Change Requests are true except which of the following?

Step 1: Answer

Approved change requests are an output of the Perform Integrated Change Control process.

Step 2: Explanation

The results of ANY procedure DO NOT include authorised change requests. A change request that has been submitted by the requestors, reviewed by the necessary parties via the integrated change control process, and been given permission to occur is referred to as an approved change request.

The team will be informed of the change. The project deliverables will be revised to account for the modification. On the CID Log, the change request will be closed.

The written request for the execution of a change by a project participant, a client, or a user is known as a change request or problem report.

What is cryptanalysis? Summarize the various types of cryptanalytic attacks on encrypted messages.

Step 1:

Cryptanalysis is the technique of examining cryptographic systems for flaws or information leakage.

Cryptanalysts, for example, aim to decipher cipher texts without having access to the plaintext source, encryption key, or encryption algorithm; they also attack safe hashing, digital signatures, and other cryptographic procedures.

Step 2:

Types of Attacks

- Known-Plaintext Analysis (KPA) : In this type of attack, some plaintext-ciphertext pairs are already known. ...
- Chosen-Plaintext Analysis (CPA) :
- Ciphertext-Only Analysis (COA) :
- Man-In-The-Middle (MITM) attack : ...
- Adaptive Chosen-Plaintext Analysis (ACPA) :

Step 3:

Known-Plaintext Analysis (KPA): Some plaintext-ciphertext pairs are already known in this sort of attack. In order to find the encryption key, the attacker maps them. This assault is simpler to execute because a large amount of data is already available.

CPA (Chosen-Plaintext Analysis): In this sort of attack, the attacker selects random plaintexts, obtains the accompanying cipher texts, and attempts to decrypt the data. It's similar to KPA in that it's easy to execute, but the success rate is low.

COA (Cipher Text-Only Analysis): In this form of attack, the attacker only knows a portion of the cipher text and attempts to deduce the encryption key and plaintext. It is the most difficult to implement, but it is also the most likely attack because just cipher text is required.

Man-In-The-Middle (MITM) attack:

The attacker intercepts the message/key between two communicating parties through a secured channel in a Man-In-The-Middle (MITM) attack.

ACPA (Adaptive Chosen-Plaintext Analysis)

It is a variant of CPA. After obtaining cipher texts for certain plaintexts, the attacker requests the cipher texts of further plaintexts.

List the parameters of a symmetric block cipher for greater security.

Step 1:

A symmetric cypher is one that encrypts and decrypts using the same key. Asymmetric or symmetric cyphers or algorithms exist. Symmetric ones employ the same key (sometimes referred to as a secret key or private key) to convert plaintext into ciphertext and vice versa.

Step 2:

The symmetric block cypher is determined by the parameters and design elements used.

• Block size: Larger block sizes provide more security but slow down encryption and decoding.

• Key size: A larger key size provides more security, but it may slow down encryption and decoding. In current algorithms, the most frequent key length is 128 bits.

• Number of rounds: A symmetric block cipher's essential is that a single round provides insufficient security, but numerous rounds provide increased security. 16 rounds is a common size.

• Subkey generation algorithm: A higher level of complexity in this process should make cryptanalysis more challenging.

• Round function: Once again, increased complexity equates to better cryptanalysis resistance.

• Fast software encryption/decryption: As a result, the algorithm's speed of execution and hardware implementation become a factor.

What is a block cipher? Name the important symmetric block ciphers.

Step 1:

A block cypher is an encryption method that encrypts a block of text using a deterministic algorithm and a symmetric key, rather than encrypting one bit at a time like stream cyphers. AES, for example, is a popular block cypher that encrypts 128-bit blocks with a key length of 128, 192, or 256 bits.

Step 2:

The symmetric block cyphers Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are both used to encrypt data. IBM created the DES block cypher in 1975, which consisted of 64-bit blocks and a 56-bit key.

Step 3:

DES is a symmetric key block cypher that uses a 64-bit block size and a 64-bit key size. It is vulnerable to some types of attacks, hence it isn't widely used.

The Advanced Encryption Standard (AES) is a symmetric block cypher that the United States government has chosen to safeguard confidential information. AES is used to encrypt sensitive data in software and hardware all over the world. It's critical for government computer security, cybersecurity, and data security.

There are two applications for public-key cryptography:

Step 1:

1) Encryption with the recipient's public key (the message is encrypted with the recipient's public key and can only be decoded with the recipient's private key)

The approach of encrypting data with two separate keys and making one of the keys, the public key, available for anybody to use is known as public key encryption or public key cryptography. The private key is the other of the two keys.

Step 2:

Every user's public key is stored in the Public Key Register. If B wants to transmit a confidential message to C, B uses C's public key to encrypt the message. When C receives the message from B, it can use its own Private key to decrypt it.

Because users never have to transmit or reveal their private keys to anyone, public key cryptography remains the most secure protocol (over private key cryptography). This reduces the odds of cyber criminals discovering an individual's secret key during transmission.

2)Digital signature

A mathematical algorithm is frequently used to confirm the validity and integrity of a message using a digital signature, which is a sort of electronic signature (e.g., an email, a credit card transaction, or a digital document).

Public key cryptography, often known as asymmetric cryptography, is used to create digital signatures. Two keys are produced using a public key algorithm like RSA (Rivest-Shamir-Adleman), resulting in a mathematically connected pair of keys, one private and one public.

It has been suggested that an independent certification authority should be established. Vendors would submit their components to this authority, which would validate that the component was trustworthy What would be the advantages and disadvantages of such a certification authority?

Step 1:

A reputable organisation that issues Secure Sockets Layer (SSL) certificates is known as a certificate authority (CA). These digital certificates are data files that are used to link an entity cryptographically to a public key. They enable trust in online content delivery by allowing web browsers to validate material sent from web servers.

Comodo, GeoTrust, and Symantec are a few examples. Simply put, becoming a Certificate Authority (CA) involves taking control of the process of producing cryptographic pairs of private keys and public certificates.

Step 2:

The benefits of having a reliable third party guarantee that a component is reliable are obvious. Providing The quality of a system that indicates the level of user confidence that it will perform as intended is called trustworthiness. A trustworthy person must be accessible, dependable, safe, and secure.

Disadvantage: A certificate authority serves as a third-party issuer to guarantee the certificate's acceptance. In order to continue using the component, certification authorities often require a membership to their services. As a result, the cost of the component is a consideration.

What is Communication? Describe the Effectiveness of Data Communication

Step 1:

Data and communication are the two words that make up the phrase "data communication." Any text, image, music, video, or multimedia file can be considered data. Sending and receiving data constitutes the act of communication. Data exchange between two or more networked or connected devices is referred to as data communication.

The communicating devices must be a part of a communication system composed of a mix of hardware (physical equipment) and software for data communications to take place (programs). Delivery, accuracy, timeliness, and jitter are the four key qualities that determine how well a data communications system performs.

Step 2:

Overall, by exchanging data and common resources among numerous computers, data communication enables firms to save costs and increase efficiency. In addition, the network may be linked together using cables, phone lines, or infrared beams, which is less expensive and lowers costs.

Delivery, accuracy, timeliness, and jitter are the four key qualities that determine how well a data communications system performs. I. Delivery: Data must be delivered to the proper location by the system. The designated device or user must get the data, and only that device or user.

Delivery:

Data must be sent to the right location by the system. The designated device or user must get the data, and only that device or user.

Accuracy:

The data must be accurately sent by the system. Data that has been tampered with during transmission and is not restored is useless.

Timeliness:

Data delivery from the system must be prompt. Late data delivery is meaningless. When it comes to video and audio, timely delivery entails sending the data as soon as it is created, in the same order, and without any noticeable delays. Real-time transmission is the term for this type of distribution.

Jitter:

The term "jitter" describes the variance in packet arrival times. It is the uneven delay in audio or video packet delivery. For illustration, suppose that video packets are transmitted every 3D millisecond. Uneven video quality results if some packets arrive with a 3D-ms delay while others arrive with a 4D-ms delay.

What is Network? Describe the Network Criteria

Step 1:

A group of devices joined by media links is referred to as a "network." A computer, printer, or any other device that can send and/or receive data produced by other nodes on the network is referred to as a "node." Communication channels are a common name for the connections between the devices.

A network is a collection of connected devices.

Communication between connected devices is referred to as networking.

Step 2:

Network criteria:

A network must be able to satisfy a variety of requirements. mainly because it enhances network performance. Performance, Reliability, and Security are the most crucial.

Performance: Transit and reaction times are two examples of performance metrics.

The length of time needed for a message to get from one device to another is known as the transit time.

The period of time between a request and a response is known as the response time.

A network's performance is influenced by a variety of variables, such as:

How many people utilise it

The medium of transmission

Hardware and software connected

Reliability:

Network dependability is measured in addition to delivery accuracy by failure frequency, the amount of time it takes a link to recover from a failure, and the network's resilience in a disaster.

Security

Data protection from viruses and unauthorised access is a concern for network security.

There are various levels at which protection can be achieved. User identification codes and passwords are at the bottom of the hierarchy. Techniques for encrypting data are at a higher level.

Since the network can be accessed from numerous locations, computer viruses may be present.

c) What is WAN? Write a Short note about it

step 1:

Wide area network, usually referred to as WAN, is a sizable information network that is not connected to a particular location. Through a WAN provider, WANs can make it easier for devices all around the world to communicate, share information, and do much more.

A wide area network (WAN) is a privately owned, geographically dispersed telecommunications system that links numerous local area networks (LANs). A local area network, or LAN, is made up of a number of connected computers and networking hardware that are often located close together geographically.

Step 2:

Voices, data, photos, and videos can all be transmitted across a wide geographic area using the WAN (Wide Area Network) network type. Combinations of LAN and MAN are used to produce WAN. Hubs, switches, routers, fibre optics, and modems are used to convey the data.

WANs are not geographically constrained in the same way that a LAN would be. A WAN is not restricted to a single location because a LAN can be established anywhere in the world and connected to it.

WAN connection types

Both wired and wireless technologies can be used for WAN connections. The following are examples of wired WAN services:

Multiprotocol Label Switching (MPLS)

T1s

Carrier Ethernet

commercial broadband internet links

When is compaction of secondary storage beneficial from the File Manager's perspective? Give several examples. List some problems that could be a result of compaction, and explain how they might be avoided.

Step 1:

Compaction refers to the shrinking or combining of hardware in order to make better use of physical memory space.

Compaction of secondary storage:

Compaction of secondary storage is advantageous from the standpoint of the file manager because of the following:

• The file manager is in charge of secondary storage upkeep.

• When compared to memory compaction, secondary storage compaction can take seconds, while disc compaction can take hours.

• In general, compaction is prompted by user complaints about having to wait a long time to retrieve data from files.

The files are scattered over the disc, generating a long chain of connections that must be viewed in order.

Step 2:

Disk compaction can take several hours compared to memory compaction, which can take seconds. As a result, it should be done infrequently. Compaction is usually prompted by user complaints about excessive wait times while getting data from files scattered over the disc, generating a long chain whose links must be retrieved in order.

Data files and databases that grow with time are good examples of files that must be compacted on a regular basis.

If the system crashes while compaction is in progress, the files in transit may be lost. This could be avoided by performing a full backup of the disc to be compressed before beginning the process. This, however, would increase the overhead.

Software copyright is the legal defence for computer-readable code. It is a tool used by software creators and owners to prevent unauthorised copies and other unauthorised uses of their intellectual property.

Computer software or programmes are sets of commands that the machine follows. Software is protected by copyright legislation, while software-related inventions are protected by patent legislation.

The problem with copyright is that it only protects the creator's expression of ideas, not the underlying idea. A form of intellectual property known as copyright is used to protect creative work. It is a legal privilege that allows the author of an original work to use and distribute it without restriction. 05

The mission of the Software & Information Industry Association and the Business Software Alliance is to ………………...

a. protects the trade secrets of world’s largest software and hardware manufacturers
b. encourages disgruntled employees to report misdeeds by their employers
c. stop the unauthorized copying of software produced by its members
d. provides recommendations on how to develop software code that is unhackable

Step 1: Answer
c. stop the unauthorized copying of software produced by its members

Step 2: Explanation

To demonstrate to the world that the software and digital information industry is the fastest-growing industry sector and a significant contributor to the global economy, according to the mission statement of the Software & Information Industry Association (SIIA).

Mission of the Business Software Alliance The BSA promotes progressive legislation and regulations that foster trust between citizens, businesses, and governments. Our goal is to make sure that ethical software innovation may flourish everywhere. We have locations, personnel, and operations in more than 30 nations. Software piracy is a copyright violation that carries both civil and criminal sanctions. Using, distributing, or selling software that has been duplicated is prohibited. And aiding piracy by providing unauthorized access to software or to serial numbers used to register software can also be illegal.

Explain the main concepts in DES.

Step 1:

The National Institute of Standards and Technology (NIST) published the Data Encryption Standard (DES), a symmetric-key block cypher (NIST).

Step 2:

Because the Data Encryption Standard (DES) has been discovered to be vulnerable to extremely powerful attacks, its popularity has been on the wane.

DES is a block cypher that encrypts data in 64-bit blocks. This implies that 64 bits of plain text are fed into DES, which outputs 64 bits of ciphertext. Encryption and decryption employ the same algorithm and key, with slight variations. The key is 56 bits long.

How can the same key be reused in triple DES?

Step 1:

The usage of a double-length DATA key made up of two 8-byte DATA keys is supported by a variant of the triple DES algorithm. The first 8-byte key is reused in the final encoding step in this method. Triple-DES encryption may not be available on your processor due to export constraints.

Step 2:

Rather of employing a single key as in DES, 3DES uses three 56-bit keys to perform the DES algorithm three times: The plaintext is encrypted using key one. The text that was encrypted by key one is decrypted using key two. The text decrypted by key two is encrypted using key three.

Explain the principles of the IDEA algorithm

Sep 1:

IDEA was created at ETH Zurich, a research university in Zurich, Switzerland, and is widely regarded as safe. The IDEA cypher encrypts text under the notion that security in IDEA is based on ignorance of the secret key rather than keeping the algorithm secret.

Step 2:

IDEA operates on 64-bit blocks and employs a 128-bit key. It converts a 64-bit block of plaintext into a 64-bit block of ciphertext in essence. This plaintext input block is broken into four 16-bit subblocks. It consists of a set of eight identical transformations, each of which is referred to as a round, as well as an output transformation referred to as a half-round. Similar to the 16-bit plaintext block, the ciphertext block is also the exact same size.

A block cypher works in round blocks, with each round including a portion of the encryption key, known as the round key, and additional mathematical operations. The ciphertext for that block is generated after a specific number of rounds.

Describing the data's contents

The Application layer sits down with the Transport layer and adds any necessary information to the header regarding the presentation and formatting of the data. This PDU is simply referred to as data when it is given to the Transport layer.

Describing each segment's content

The data that was passed down from the Application layer is supplemented by the Transport layer with port number information. You learnt earlier in this chapter that this information comprises of the requested service or application's port number and the Transport protocol (either TCP or UDP). This is included as a Transport header, which means it comes before the data and is read by the destination device before the actual data is read. The PDU that follows after this information has been added is referred to as a segment.

Describe the packets' contents

The Transport layer transmits this segment PDU to the Internet layer. The segment receives the necessary logical address information from the Internet layer. The IP addresses of the source and destination devices make up this data. The PDU is now referred to as a packet after this data has been added to the segment in the form of a Network header. You can now see that, despite the fact that it is frequently used in everyday discourse, calling the entire unit a packet is actually extremely imprecise. In this stage of the process, it is just referred to as a packet. The Network Access layer is now given control of the packet.

Defining the Frames' contents

After receiving the packet, the Network Access Layer adds the physical address data in the form of a frame header, also known as a Data Link header. The media access control (MAC) addresses of the source and destination device are contained in this data.

Detailed note on IGMP

Internet Group Management Protocol (IGMP) is the last Internet layer protocol in the TCP IP suite (IGMP). The multicasting protocol is utilised. The protocol works between hosts that are a part of multicast groups and routers. For routine communications, multicast groups of devices preserve their unicast IP addresses, but they also share a single multicast address collectively.

Dedicated to this use and not available to individual devices, multicast IP addresses are a particular range of IP addresses. Any multicast communication for the group will be forwarded to the IP address that is assigned a multicast address. As soon as the devices in the group register with the routers, the routers on the network will be aware of the devices that are members of the group. Following that, the routers will deliver any traffic sent to the multicast address to each group member.

Multicasting has the advantage of reducing network traffic. The server transmits a unique message to each unique device when unicasting. As a result, the network receives a large number of communications. However, while using multicasting, the server just sends one signal to the router through the network. That increases the strain on the network. The group members are then sent broadcasts by the router to complete the communication.

Generation of mobile network

The five generations of mobile networks are 1G, 2G, 3G, 4G, and 5G, where G stands for Generation and the number signifies the generation number. 5G is the most recent iteration, while 1G networks are no longer in use. GSM, UMTS, LTE, and NR are cellular technologies that enable 2G, 3G, 4G, and 5G, respectively.

Step 2: 4G and 5G

After 3G and before 5G, 4G is the fourth generation of broadband cellular network technology. A 4G system must support the ITU's IMT Advanced capabilities. Modified mobile online access, IP telephony, gaming services, high-definition mobile TV, video conferencing, and 3D television are some of the potential and present applications.

Fifth-generation wireless (5G) is the most recent iteration of cellular technology, designed to boost the speed and responsiveness of wireless networks dramatically.

Step 3: Packet switching technology

The transfer of small chunks of data across many networks is known as packet switching. These data chunks, or "packets," make data transfer faster and more efficient. When a user transfers a file across a network, it is frequently sent in smaller data packets rather than all at once.

Step 4:

Circuit-switching enables voice calls and text messages using dedicated circuits in 2G and 3G mobile networks; packet-switching is more efficient and uses shared circuits to enable IP-based mobile data in all mobile networks, as well as IP voice calls and texts in 4G LTE and 5G NR networks.

Step 6:

The whole network of LTE (4G) is packet switched, with no support for circuit switched networks. As a result, when using the LTE (4G) network, voice and SMS services must be moved to a packet switched network.

To satisfy users, the voice service in 5G is also packet-switched, and the service should be of equal or better quality than in 4G. Voice capability is required for a 5G smartphone to connect to a mobile network.

Step 7:

4G LTE and 5G NR networks lack circuit-switched nodes, they are data-only networks.

Packet-switching is used to provide voice, text, and data services. Voice over LTE (VoLTE) is a technology that uses the packet-switched component of the network to offer voice calls and SMS in 4G LTE networks.

Voice over New Radio (VoNR), a comparable technology for 5G networks, works on the same premise as VoLTE to provide voice and text services across the packet-switched portion of the network.

The type of 5G network implementation, i.e. non-standalone or standalone, determines whether a mobile network uses VoLTE or VoNR. Whether a mobile network uses an LTE core network (EPC) or a 5G core network affects VoLTE and VoNR technologies.

Packet-Switching (PS) is a technique that allows mobile networks to send and receive data without using the radio network resources for each user on a permanent basis.

PS provides data bursts in packets at various intervals, sharing the available channel capacity with several users.

These packets have a 'header' that carries the packet's destination information and a payload that contains the actual data or information being transferred.

These headers are used by switching nodes to detect the source and destination of packets, allowing data packets to be delivered to the desired subscribers (devices) through the most efficient route.

Step 8: Conclusion

Mobile networks use circuit-switching and packet-switching as two essential communication techniques to provide voice, SMS, and data services to their consumers.

The older of the two approaches used in 2G and 3G networks for making and receiving voice calls and sending and receiving text messages is circuit-switched.

Hence, Circuit-switched voice (voice and SMS over 2G and 3G networks) and packet-switched voice services in 4G and 5G networks are the major technological network migration steps.

This transformation enables service providers to give consumers, businesses, and industries with more useful and advanced voice and communication services.

List several different types of end systems. Is a Web server an end system?

Step 1:

A computer linked to a network is frequently referred to as an end system or end station. The end user interacts directly with a system that provides data or services.

End systems connected to the Internet are also known as online hosts because they host (or run) internet programmes like a web browser or an email retrieval tool.

Step 2:

Mail servers, web servers, and database servers are examples of these. Household goods (such as toasters and refrigerators), as well as portable, handheld computers and digital cameras, are all being connected to the internet as end systems with the rise of the internet of things.

PCs, workstations, Web servers, mail servers, PDAs, Internet-connected game consoles, and other end devices are examples. R2.

Step 3:

The end systems of the Internet include some computers with which the end user does not interface directly. Mail servers, web servers, and database servers are examples of these.

A web server is, thus, an end system.

Which of the words in the fully qualified domain name (FQDN)
www.paris.mydomain.org
represents the topmost layer in the DNS namespace hierarchy?

A. www
B. paris
C. mydomain
D. org

Step1:

A namespace is a context where all object names have to be clearly resolvable. For instance, all network devices with a DNS name on the internet can be resolved to a specific address within a single DNS name space (for example, www.microsoft.com resolves to 207.46. 131.13).

Step 2: Answer with Explanation

Answer D. org

Explanation

The top-level domain org is used to represent the DNS hierarchy's top tier. Mydomain is a second-level domain that has been registered by a specific company. www is the name of a specific host in the paris.mydomain.org domain, and Paris is a subdomain of Mydomain.

Generation of mobile network

The five generations of mobile networks are 1G, 2G, 3G, 4G, and 5G, where G stands for Generation and the number signifies the generation number. 5G is the most recent iteration, while 1G networks are no longer in use. GSM, UMTS, LTE, and NR are cellular technologies that enable 2G, 3G, 4G, and 5G, respectively.

Step 2: 4G and 5G

After 3G and before 5G, 4G is the fourth generation of broadband cellular network technology. A 4G system must support the ITU's IMT Advanced capabilities. Modified mobile online access, IP telephony, gaming services, high-definition mobile TV, video conferencing, and 3D television are some of the potential and present applications.

Fifth-generation wireless (5G) is the most recent iteration of cellular technology, designed to boost the speed and responsiveness of wireless networks dramatically.

Step 3: Packet switching technology

The transfer of small chunks of data across many networks is known as packet switching. These data chunks, or "packets," make data transfer faster and more efficient. When a user transfers a file across a network, it is frequently sent in smaller data packets rather than all at once.

Step 4:

Circuit-switching enables voice calls and text messages using dedicated circuits in 2G and 3G mobile networks; packet-switching is more efficient and uses shared circuits to enable IP-based mobile data in all mobile networks, as well as IP voice calls and texts in 4G LTE and 5G NR networks.

Step 6:

The whole network of LTE (4G) is packet switched, with no support for circuit switched networks. As a result, when using the LTE (4G) network, voice and SMS services must be moved to a packet switched network.

To satisfy users, the voice service in 5G is also packet-switched, and the service should be of equal or better quality than in 4G. Voice capability is required for a 5G smartphone to connect to a mobile network.

Step 7:

4G LTE and 5G NR networks lack circuit-switched nodes, they are data-only networks.

Packet-switching is used to provide voice, text, and data services. Voice over LTE (VoLTE) is a technology that uses the packet-switched component of the network to offer voice calls and SMS in 4G LTE networks.

Voice over New Radio (VoNR), a comparable technology for 5G networks, works on the same premise as VoLTE to provide voice and text services across the packet-switched portion of the network.

The type of 5G network implementation, i.e. non-standalone or standalone, determines whether a mobile network uses VoLTE or VoNR. Whether a mobile network uses an LTE core network (EPC) or a 5G core network affects VoLTE and VoNR technologies.

Packet-Switching (PS) is a technique that allows mobile networks to send and receive data without using the radio network resources for each user on a permanent basis.

PS provides data bursts in packets at various intervals, sharing the available channel capacity with several users.

These packets have a 'header' that carries the packet's destination information and a payload that contains the actual data or information being transferred.

These headers are used by switching nodes to detect the source and destination of packets, allowing data packets to be delivered to the desired subscribers (devices) through the most efficient route.

Step 8: Conclusion

Mobile networks use circuit-switching and packet-switching as two essential communication techniques to provide voice, SMS, and data services to their consumers.

The older of the two approaches used in 2G and 3G networks for making and receiving voice calls and sending and receiving text messages is circuit-switched.

Hence, Circuit-switched voice (voice and SMS over 2G and 3G networks) and packet-switched voice services in 4G and 5G networks are the major technological network migration steps.

This transformation enables service providers to give consumers, businesses, and industries with more useful and advanced voice and communication services.

Discuss some of the technical and nontechnical issues that might come up in trying to establish a large grid computing project such as the World Computing Grid.

The first problem is that there is no clear standard to follow.

The first thing that needs to be worked out in order to hide the diverse properties of different resources in a grid environment is a standard.

The most significant goal for the Global Grid Forum (GGF) has been standardisation since its inception. Until date, more and more people have recognised Open Grid Systems Architecture (OGSA), and more and more voices from industry have advocated for Web Services Resource Framework (WSRF). Even so, there are still distinct tones for future grid computing standards.

The more grid applications produced without broadly acknowledged standards, the more resource islands will arise.

Grid computing's challenges include the following:

In order to establish the Grid, a large amount of heterogeneous hardware is utilised, and these devices are not maintained by just one person, but by several system administrators in each of the companies.

Grid follows the problems that must be overcome in order to fully utilise the grid's potential.

There is no clear standard:-

Grid computing employs a variety of standards, although not all grids adhere to the same ones. For instance, all grid operating systems such as Linux, Apache, and others. My SQL is based on the standards of WSRF, UDDI, WWW, SOAP, and XML. Without WSRF, Oracle 10g Enterprise cannot be implemented. Grid middleware is developed by IBM and is based on J2EE. In grid computing, we can't run many operating systems on the same computer at the same time.

Grid computing vs. Distributed Computing:

Grid computing entails resource sharing, dynamic virtual organisation, and peer-to-peer computing.

The Grid aims to make access to computer power, scientific data archives, and experimental equipment as simple as access to information on the Web. Same all facilities provide the grid computing.so it is a challenge for grid computing.

Lack of grid-enabled software: The software that enables grid computing is insufficient, and there is only limited software on the grid. Many pieces of software do not have copyright issues or licence source code. There is a need for more companies to develop grid-enabled versions, more developers to work on grid development, and more open source software to be developed.

Grid is used to share resources between different types of services. -Grid is used to share resources between different sites and grid hosts. As a grid platform, it manages a large amount of data. There are a lot of sites and multiple servers grouped there, thus the infrastructure is quite complicated. It makes it harder to share hardware resources within a virtual organisation.

Difficult to develop: -

Grid programming employs Java and XML, as well as web services such as WSDD, WSDL, UDDI, WSRF, and GT3 development standards. It is a question of who will be building grid applications. Basically, senior computer science experts and enterprise developers have access to this.

Identifying the Source Device's Process

The data is obtained by Layer7 as an HTML page.

The formatting information is added in Layer 6.

Layer 5 adds the data necessary to establish a session between the laptop's web browser and the web server.

The transport protocol and source and destination port numbers are added at Layer 4, in this case TCP (which is a unicast protocol) and port 80. (HTTP).

The source and destination IP addresses, in this case 192.168.5.1 and 192.168.5.2, are part of Layer 3.

Layer 2 combines the source and destination MAC addresses, in this case 5-5-5-5-5-5 and 6-6-6-6-6-6, after learning the destination MAC address.

Layer 1 breaks the entire packet down into bits and transmits them to the laptop over the network.

Identifying the Destination Device's Process

The bits are received by layer 1 in electrical format, who then transforms them such that layer 2 can read them.

Layer 2 checks the target MAC address to determine if it is directed to it; upon identifying its own MAC address, 6-6-6-6-6, it removes that portion of the transmission and gives the remaining data to layer 3.

Layer 3 checks the target IP address (192.168.5.2) to make sure it is its own, drops that portion, and hands the remaining package to Layer 4.

Layer 4 evaluates port 80 as the destination port, notifies the browser that HTTP data is arriving, drops that portion, and passes the remaining package to Layer 5.

Layer 5 passes the remaining data to Layer 6 after creating the session between the web server and the web browser using the data that was provided on this layer by the web server.

Layer 6 does any necessary format translation and sends the HTML document's core contents to layer 7.

The web browser, a layer7 application, receives the HTML document and displays it in the browser window.