4 UNIT

Transport Layer

CONTENTS

PART-1

Transport Layer-Design Issues.

CONCEPT OUTLINE

- UDP is a connectionless protocol which is suitable for application that needs fast, efficient transmission.
- TCP is a connection oriented protocol which rearranges data packets in the specified order.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.1. **Write a short note on process-to-process delivery.**

OR

How transport layer is meant for process-to-process delivery ?

Answer

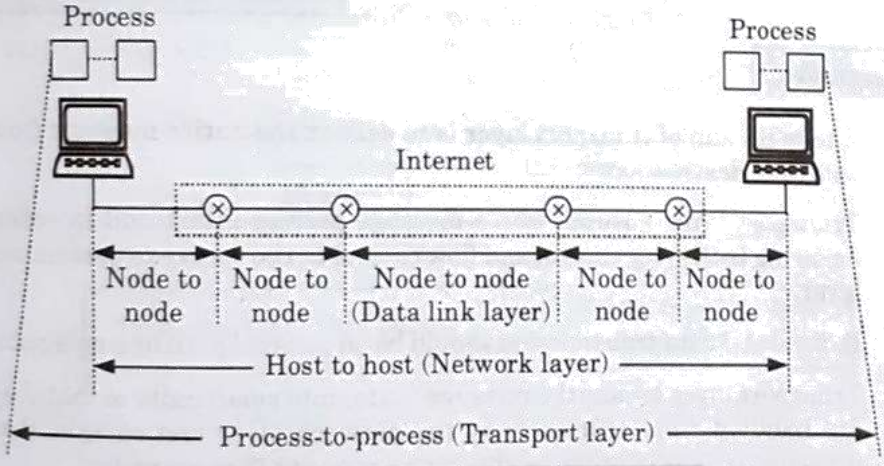

Fig. 4.1.1. Types of data deliveries.

1. The data link layer performs a node to node delivery. The network layer carries out the datagram delivery between two hosts (host to host delivery).
2. The real communication takes place between two process application programs for which we need the process-to-process delivery.
3. The transport layer takes care of the process-to-process delivery. In this a packet from one process is delivered to the other process.

4. The relationship between the communicating processes is the client-server relationship.

Que 4.2. **What are the design issues in transport layer ?**

Answer

Design issues with transport layer :

1. Accepting data from session layer, split it into segments and send to the network layer.
2. Ensure correct delivery of data with efficiency.
3. Error control and flow control.
4. End-to-end delivery of the packet.
5. Combining packets into message segment at receiver side.
6. Connection management.

Que 4.3. **Enumerate how the transport layer ensures that the complete message arrives at the destination and in the proper order.**

AKTU 2016-17, Marks 7.5

AKTU 2017-18, Marks 10

Answer

1. The main aim of transport layer is to deliver the entire message from source to destination.
2. Transport layer ensures whole message arrives intact and in order, ensuring both error control and flow control at the source to destination level.
3. It decides if data transmission should be on parallel path or single path.
4. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer and ensures that message arrives in order by checking error and flow control.
   a. **Flow control :** Flow control is performed end to end in this layer.
   b. **Error control :** Error control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error correction is done through retransmission.

Que 4.4. **Write a short note on User Datagram Protocol (UDP).**

Answer

1. User Datagram Protocol (UDP) provides a connectionless packet service that offers unreliable 'best effort' delivery.
2. Applications that do not require an acknowledgement of receipt of data, for example, audio or video broadcasting uses UDP.
3. UDP is also used by applications that typically transmit small amounts of data at one time, for example, the Simple Network Management Protocol (SNMP).
4. UDP provides a mechanism that application programs use to send data to other application programs.
5. UDP provides protocol port numbers to distinguish between multiple programs executing on a single device.
6. That is, an addition to the data sent, each UDP message contains both a destination port number and a source port number. This makes it possible for the UDP software at the destination to deliver the message to the correct application program, and for the application program to send a reply.
7. UDP packets are called as user datagram.

Que 4.5. Discuss the header format of UDP.

Answer

UDP have a fixed size header of 8-bytes. The format of user datagram is as shown in Fig. 4.5.1.

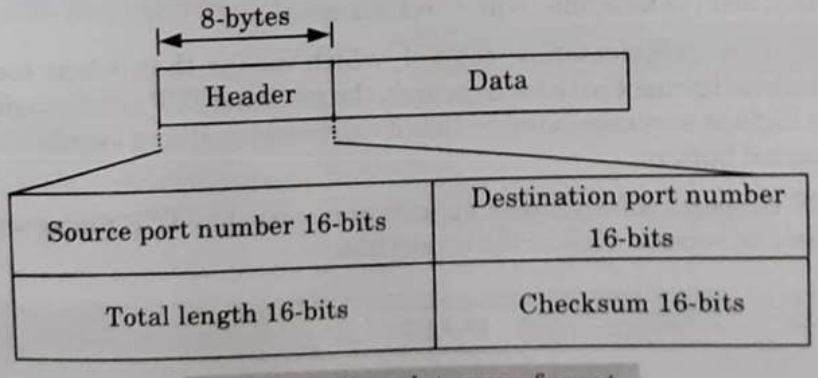

Fig. 4.5.1. User datagram format.

The UDP header is divided into the following four 16-bit fields :

1. **Source port :** Source port is an optional field, which indicates that port of the sending process and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.

2. **Destination port :** Destination port has a meaning within the context of a particular internet destination address.
3. **Length :** This is the size in bytes of the UDP packet, including the header and data. The minimum length of the header is 8-bytes.
4. **Checksum :** This is used to verify the integrity (*i.e.*, to detect errors) of the UDP header. The checksum is performed on a "pseudo header" consisting of information obtained from the IP header (source and destination address) as well as the UDP header.

Que 4.6. **What do you mean by Transmission Control Protocol (TCP) ?**

Answer

1. TCP (Transmission control protocol) is a connection-oriented protocol.
2. The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model.
3. Among the services, TCP provides stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.
4. With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers.
5. TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork.
6. The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate, or misread packets. A time-out mechanism allows devices to detect lost packets and request retransmission.
7. TCP offers efficient flow control, which means that, when sending acknowledgement back to the source, the receiving TCP process indicates the highest sequence number that it can receive without overflowing its internal buffers.
8. TCP supports a full-duplex operation means that TCP processes can send and receive both at the same time.

PART-2

Connection Management.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.7. **Differentiate between connection-oriented services with connectionless services.**

Answer

S. No.	Connection-oriented service	Connectionless service
1.	In connection-oriented service authentication is needed.	Connectionless service does not need any authentication.
2.	Connection-oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs.	Connectionless service protocol does not guarantee a delivery.
3.	Connection-oriented service is more reliable.	Connectionless service is less reliable.
4.	Connection-oriented service interface is stream based.	Connectionless service interface is message based.
5.	Packets travel sequentially.	Packets travel randomly.

Que 4.8. **Explain the three-way handshaking protocol to establish the transport level connection.**

AKTU 2016-17, 2017-18; Marks 10

Answer

Connection establishment in TCP :

1. To establish a connection, TCP uses a three-way handshake.
2. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections, this is called a passive open.
3. Once the passive open is established, a client may initiate an active open.
4. To establish a connection, the three-way (or 3-step) handshake occurs :
   a. **SYN :** The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value *A*.
   b. **SYN-ACK :** In response, the server replies with a SYN-ACK. The acknowledgement number is set to one more than the received

sequence number $(A + 1)$, and the sequence number that the server chooses for the packet is another random number, B.

c. **ACK :** Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value *i.e.*, $A + 1$, and the acknowledgement number is set to one more than the received sequence number *i.e.*, $B + 1$.

5. At this point, both the client and server have received an acknowledgement of the connection.
6. The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged.
7. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged.
8. With these, a full-duplex communication is established.

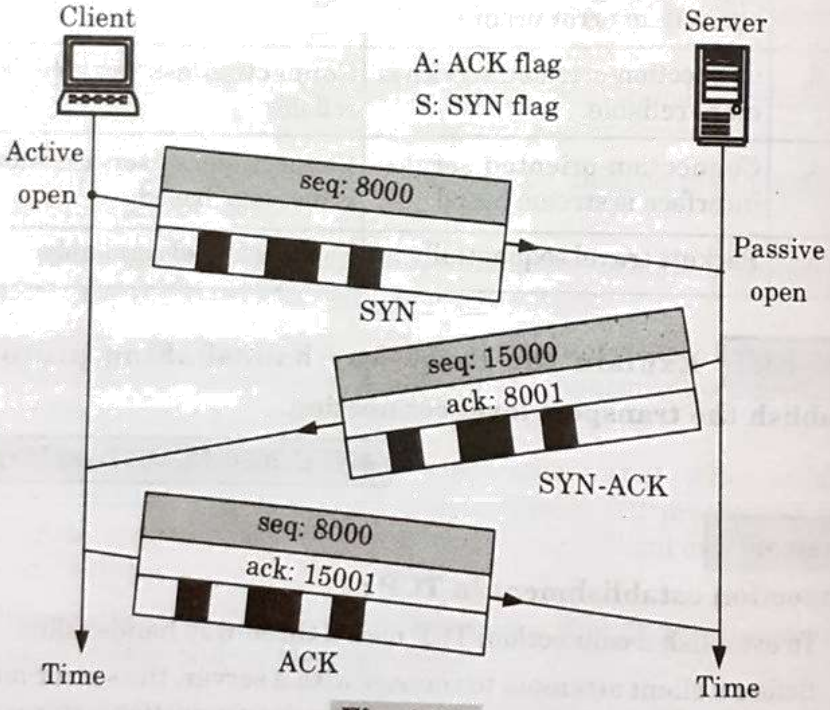

Fig. 4.8.1.

Que 4.9. Explain about the TCP header and working of TCP protocol and differentiate between TCP and UDP with frame format.

AKTU 2013-14, 2016-17, 2017-18; Marks 10

Answer

The segment consists of a 20 to 60 byte header, followed by data from the application program. The header is 20 bytes if there are no options and upto 60 bytes if it contains options.

1. **Source port :** A 16-bit number identifying the application that TCP segment originated from within the sending host.

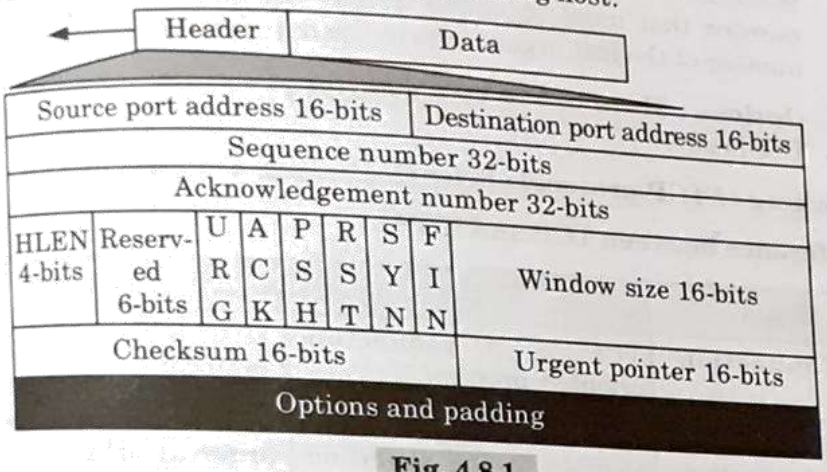

Fig. 4.8.1.

2. **Destination port :** A 16-bit number identifying the application that TCP segment is destined for on a receiving host.
3. **Sequence number :** A 32-bit number identifying the current position of the first data byte in the segment within the entire byte stream for the TCP connection.
4. **Acknowledgement number :** A 32-bit number identifying the next data byte that the sender expects from the receiver.
5. **Header length :** This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be in between 20 and 60.
6. **Reserved :** This is a 6-bit field reserved for future use.
7. **Control :** This field defines six different control bits or flags. One or more of these bits can be set at a time.
   i. **URG :** The value of urgent pointer field is valid.
   ii. **ACK :** The value of acknowledgement field is valid.
   iii. **PSH :** Push the data.
   iv. **RST :** Reset the data.
   v. **SYN :** Synchronize the sequence numbers during connection.
   vi. **FIN :** Terminate the connection.
8. **Window size :** This field defines the size of the window, in bytes, that the other party must maintain. The length of this field is 16-bits, which means that the maximum size of the window is 65,535 bytes.
9. **Checksum :** This 16-bit field contains the checksum. However, the inclusion of the checksum in the UDP datagram is optional, whereas the inclusion of the checksum for TCP is mandatory.

10. **Urgent pointer :** This 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data. It defines the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.

11. **Options :** There can be upto 40-bytes of optional information in the TCP header.

Working of TCP protocol : Refer Q. 4.8, Page 4–6A, Unit-4.

Difference between TCP and UDP :

Basis	TCP	UDP
Connection	TCP is a connection oriented protocol.	UDP is a connectionless protocol.
Ordering of data packets	TCP rearranges data packets in the specified order.	UDP has no inherent order as all packets are independent of each other.
Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because there is no error-checking for packets.
Reliability	There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent would reach at all.
Header size	TCP header size is 20-bytes.	UDP header size is 8-bytes.
Error checking	TCP does error checking.	UDP does error checking, but has no recovery option.

Que 4.10. **Draw the diagram of TCP header and explain the use of the following :**

i. **Source and destination port addresses**
ii. **Sequence and acknowledgement numbers**
iii. **Control bits**
iv. **Window size**
v. **Urgent pointer**

Describe the role of checksum field and option pad bytes.

AKTU 2014-15, Marks 10

Answer

TCP header : Refer Q. 4.9, Page 4–7A, Unit-4.

Use :

i. **Use of source and destination port address :** This field is used to identify the source and destination address of the host.

ii. **Use of sequence number :** The sequence number field is used to set a number on each TCP packet so that the TCP stream can be properly sequenced .

Use of acknowledgment number : This field is used when we acknowledge a specific packet a host has received.

iii. **Use of control bit :** This field is used to relay information between TCP peers.

iv. **Use of window size :** This field is used to indicate to the sender the amount of data that it is able to accept.

v. **Use of urgent pointer :** This field is used when the segment contain urgent data.

Role of checksum : The role of TCP/IP checksum is to detect corruption of data over a TCP or IPv4 connection.

Role of option pad bytes : Role of option pad byte is to ensure that the data part of the packet begins on a 32-bit boundary, and no data is lost in the packet.

Que 4.11. Explain TCP congestion control algorithm in internet. What is TCP segment header ? Also, discuss TCP connection management. **AKTU 2015-16, Marks 10**

Answer

TCP congestion control algorithm in internet :

1. Initialization for a given connection sets cwnd (congestion window) to one segment and ssthresh (when a loss occurs, fast retransmit is sent, half of the current cwnd is saved as ssthresh) to 65535 bytes.
2. The TCP output routine never sends more than the lower value of cwnd or the receiver's advertised window.
3. When congestion occurs (timeout or duplicate ACK), one-half of the current window size is saved in ssthresh. Additionally, if the congestion is indicated by a timeout, cwnd is set to one segment.
4. When new data is acknowledged by the other end, increase cwnd, but the way it increases depends on whether TCP is performing slow start or congestion avoidance. If cwnd is less than or equal to ssthresh, TCP is in slow start; otherwise, TCP is performing congestion avoidance.

TCP segment header : Refer Q. 4.9, Page 4–7A, Unit-4.

TCP connection management :

1. Connections are established in TCP using the three-way handshake.
2. To establish a connection, one side, the server, passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives, either specifying a specific source or nobody in particular.
3. The other side, the client, executes a CONNECT primitive, specifying the IP address and port to which it wants to connect, the maximum TCP segment size it is willing to accept, and optionally some user data (for example, a password).
4. The CONNECT primitive sends a TCP segment with the SYN bit on and ACK bit off and waits for a response.
5. When this segment arrives at the destination, the TCP entity checks to see if there is a process that has done a LISTEN on the port given in the destination port field. If not, it sends a reply with the RST bit on to reject the connection.

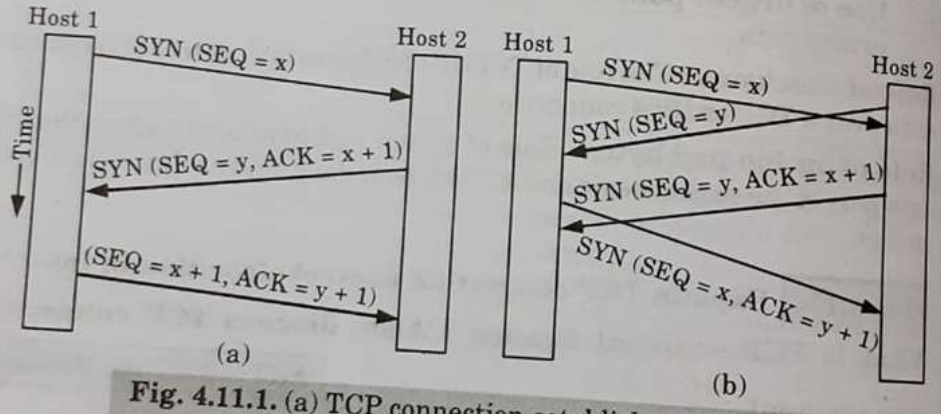

Fig. 4.11.1. (a) TCP connection establishment in the normal case. (b) call collision.

Que 4.12. Why TCP is preferred over UDP in some applications ? Explain the reasons and also mention those applications.

Answer

TCP is preferred over UDP in some application because of following reasons :

1. TCP ensures ordered delivery of a stream of bytes from user to server.
2. TCP is more reliable since it manages message acknowledgment and retransmissions in case of lost parts.
3. TCP transmissions are sent in a sequence and they are received in the same sequence.
4. TCP uses both error detection and error recovery.
5. TCP is a heavy weight connection requiring three packets for a socket connection and handles congestion control.

TCP are preferred over UDP in applications like multiplayer online games.

PART-3

Session Layer-Design Issues, Remote Procedure Call.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.13. Discuss the design issues of session layer. List the services provided by session layer.

Answer

Design issues with session layer :

1. To allow machines to establish sessions between them in a seamless fashion.
2. Provide enhanced services to the user.
3. To manage dialog control.
4. To provide services such as token management and synchronization.

List of session layer services :

1. **Authentication :**
   a. Authentication is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true.
   b. This involves confirming the identity of a person, the origins of an artifact, or assuring that a computer program is a trusted one.
2. **Permissions or access control :**
   a. Use of authentication and authorization is access control.
   b. Access is controlled by insisting on an authentication procedure to identity the user.
3. **Checkpoints :** Session layer is responsible for creating several checkpoints that are also treated as recovery points *i.e.*, in case of failure the system rollback to its previous checkpoint configuration or action.

Que 4.14. Write a short note on Remote Procedure Call (RPC).

Answer

1. When a process on machine-1 calls a procedure on machine-2, then the calling process on machine-1 is suspended and execution of the called

procedure takes place on machine-2 and no message passing is visible to the programmer. This technique is called as RPC (Remote Procedure Call).

2. The calling procedure is known as client and the called procedure is known as the server.
3. The principle behind RPC is to make a remote procedure call look like as a local call.
4. To call a remote procedure, the client program should be bound with a small library procedure called as client-stub which represents the server procedure in the client's address space.
5. Similarly a server is bound with a procedure called as the server-stub.
6. Fig. 4.14.1 shows the actual steps in making RPC.

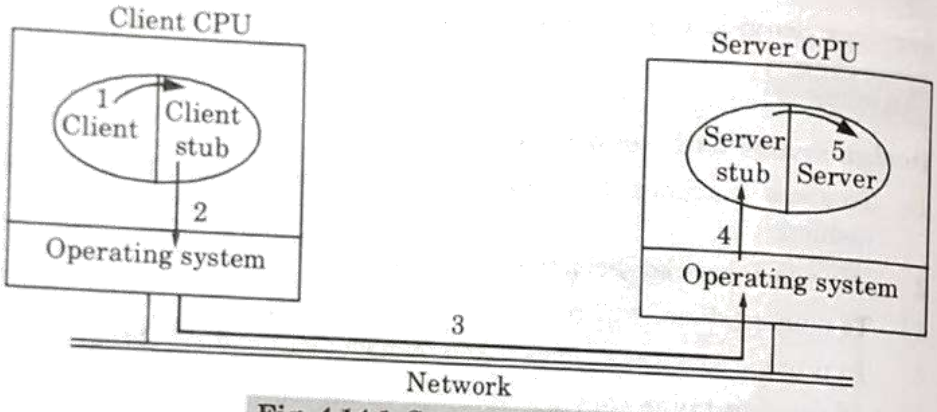

Fig. 4.14.1. Steps in making RPC.

Step 1 : Client calls the client-stub. This is a local procedure call with the parameters pushed on to the stack in the normal way.

Step 2 : Client-stub packs the parameters into a message and makes a system call to send the message. Packing the parameters is called as marshaling.

Step 3 : The message is sent from client machine to server machine.

Step 4 : The incoming packet is passed to the server-stub.

Step 5 : Server-stub calls the server procedure with the unmarshaled parameters.

7. The reply from server to client traces the same path in the opposite direction.

Que 4.15. Discuss the problem related to RPC.

Answer

Problems related to RPC :

1. It is not possible to pass pointers because client and server are in different address space.

2. It becomes impossible for the client-stub to marshal the parameters, the size of which is not known.
3. The problem is that it is not always possible to find out the types of the parameter, not even from a formal specification or code itself.
4. Generally the calling and called procedures can communicate by using global variables in addition to using parameters. But if the called procedure is moved to a remote machine, then the code will fail because the global variables are not being shared anymore.

Que 4.16. Discuss the RPC design and implementation issues.

AKTU 2014-15, Marks 05

Answer

Design and implementation issues in RPC :

1. **Structure :**
   i. A widely used organization for RPC mechanisms is based on the concept of stub procedures.
   ii. When a program (client) makes a remote procedure call, say $p(x, y)$ it actually makes a local call on a dummy procedure or a client-stub procedure corresponding to procedure P.
   iii. The client-stub procedure constructs a message containing the identity of the remote procedure and parameters, if any, to be passed.
   iv. It then sends the message to the remote server machine.
   v. When the remote procedure completes execution, the control returns to the server-stub procedure.
   vi. The server-stub procedure passes the results back to the client-stub procedure at the calling machine, which returns the results to the client.
2. **Binding :**
   i. Binding is a process that determines the remote procedure, and the machine on which it will be executed, upon a remote procedure invocation.
   ii. The binding process may also check the compatibility of the parameters passed and the procedure type called with what is expected from the remote procedure.
   iii. One approach for binding in the client-server model makes use of a binding server.
3. **Parameter and result passing :**
   i. To pass parameters or results to a remote procedure, a stub procedure has to convert the parameters and results into an appropriate representation first and then pack them into a buffer in a form suitable for transmission.

ii. After the message is received, the message must be unpacked.

iii. This approach requires the machine to know how to convert all the formats that can possibly be used. This approach also has poor portability because whenever a new representation is introduced into the system, existing software needs to be updated.

4. **Error handling, semantics and correctness :** A remote procedure call can fail for at least two reasons : computer failures and communication failures. Handling failures in distributed systems is difficult.

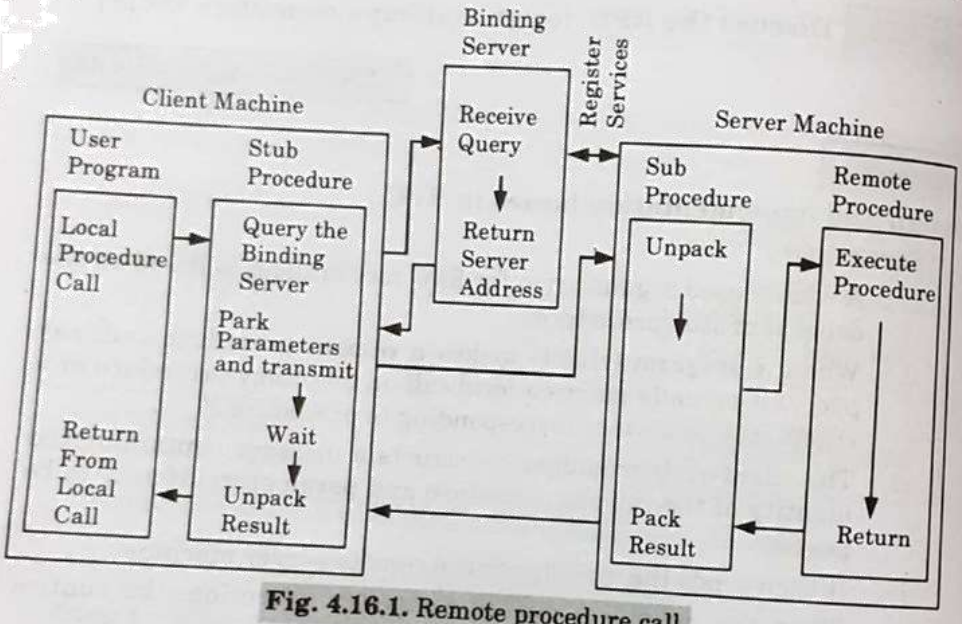

Fig. 4.16.1. Remote procedure call.

PART-4

Presentation Layer : Design Issues.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.17. **Discuss the design issues in presentation layer. Write the functions of presentation layer.**

Answer

Design issues in presentation layer :

1. To manage and maintain the syntax and semantics of the information transmitted.

2. Encoding data in a standard agreed upon way. For example : String, double, date, etc.
3. Perform standard encoding on wire.

Functions of presentation layer :

1. **Translation :** It translates data between the formats the network requires and the format the computer expects.
2. **Encryption :** It carries out encryption at the transmitter and decryption at the receiver.
3. **Compression :** It carries out data compression to reduce the bandwidth of the data to be transmitted. The primary role of data compression is to reduce the number of bits to be transmitted. It is important in transmitting multimedia such as audio, video, text etc.

The presentation layer has following issues :

1. **Data format :** Converting the complex data structures used by an application - strings, integers, structures, etc., into a byte stream transmitted across the network, representing information in such a way that communicating peers agree to the format of the data being exchanged.
2. Compressing data to reduce the amount of transmitted data (for example, to save money).
3. **Security and privacy issues :**
   i. **Encryption :** Scrambling the data so that only authorized participants can unscramble the messages of a conversation.
   ii. **Authentication :** Verifying that the remote party really is the party they claim to be rather than an impostor.

PART-5

Data Compression Techniques.

CONCEPT OUTLINE

- Data compression techniques :
  i. Lossless compression
  ii. Lossy compression

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.18. Describe data compression. What are the techniques/ types of data compression ?

Answer

Data compression :

1. Data compression is the way of downloading the compressed form of text, audio and video data using the computer.
2. Data compression is essential for efficient storage and transmission of different type of data.
3. A data compression system consists of an encoder and a decoder.
4. The encoder performs compression of the incoming data and decoder is used for decompression and reconstruction as shown in Fig. 4.18.1.

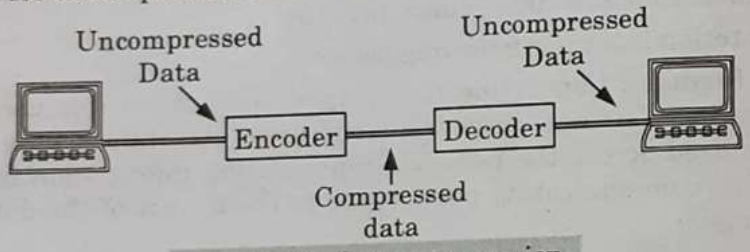

Fig. 4.18.1. Data compression.

Types of compression :

1. **Lossless compression (or data compaction) :**
   a. In lossless compression, the redundant information contained in the data is removed.
   b. In lossless compression, there is no loss of information.
   c. Lossless compression has lower compression ratio.
2. **Lossy compression :**
   a. In lossy compression, there is a loss of information in a controlled manner.
   b. The lossy compression is not completely reversible.
   c. The lossy compression has higher compression ratio.

Que 4.19. Write short notes on :

i. Digital audio
ii. Audio compression
iii. Streaming audio

AKTU 2013-14, Marks 10

Answer

i. Digital audio :

1. Digital audio is a technology that is used to record, store, manipulate, generate and reproduce sound using audio signals that have been encoded in digital form.

2. It also refers to the sequence of discrete samples that are taken from an analog audio waveform.
3. A digital audio signal may be stored or transmitted.
4. Digital audio can be stored on a CD, a digital audio player, a hard drive, a USB flash drive, or any other digital data storage device.
5. Digital audio can be carried over digital audio interfaces.
6. Digital audio can be carried over a network using audio over Ethernet, audio over IP or other streaming media standards and systems.

ii. Audio compression :

1. Before audio can be transmitted over a computer network, it must be digitized and compressed.
2. Audio compression is important because uncompressed audio consumes tremendous amount of storage and bandwidth.
3. Two techniques used for audio compression :

a. Predictive encoding :

i. In predictive encoding the difference between the samples are encoded instead of encoding all the sampled values.

ii. This type of compression is normally used for speech. Several standards have been defined such as GSM (13 Kbps), G.729 (8 Kbps) etc.

b. Perceptual encoding (MP3) :

i. The most common compression technique that is used to create CD-quality audio is based on the perceptual encoding technique.

ii. MP3 (MPEG audio layer 3) uses this technique.

iii. MP3 uses two phenomena, frequency and temporal masking, to compress audio signal.

iv. MP3 produces three data rates : 96 Kbps, 128 Kbps and 160 Kbps.

v. The rate is based on the range of the frequencies in the original analog audio.

iii. Streaming audio : To understand the concept of streaming audio we have following four approaches :

a. Using a web server :

i. A compressed audio file can be downloaded as a text file.

ii. The client (browser) can use the services of HTTP and send a GET message to download the file.

iii. The web server can send the compressed file to the browser.

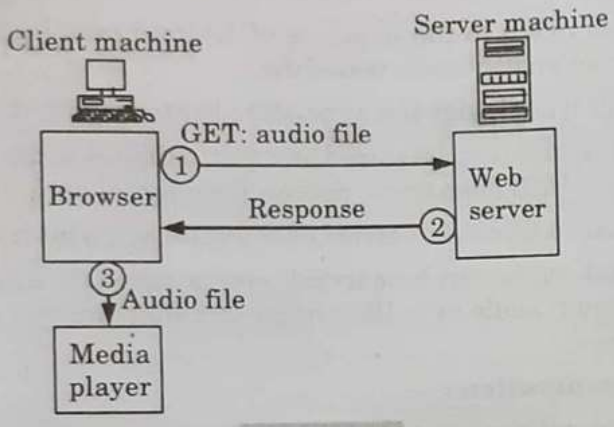

Fig. 4.19.1.

iv. The browser can then use a help application, normally called a media player, to play the file as shown in Fig. 4.19.1.

v. This approach is very simple and does not involve streaming.

b. Using a web server with a metafile :

i. In another approach, the media player is directly connected to the web server for downloading the audio file.

ii. The web server stores two files : the actual audio file and a metafile that holds information about the audio file. Fig. 4.19.2 shows the steps in this approach.

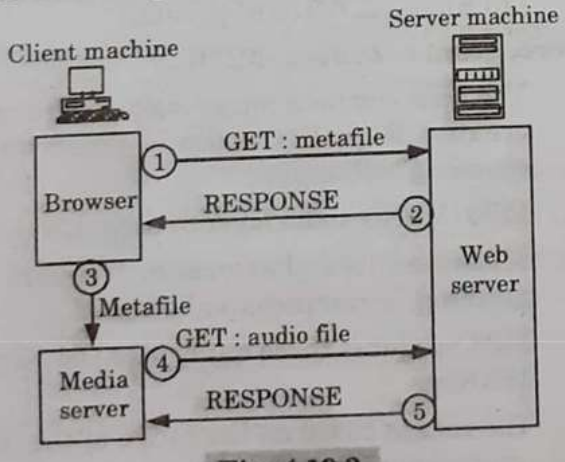

Fig. 4.19.2.

c. Using a media server :

i. The problem with the second approach is that the browser and the media player both use the services of HTTP. HTTP is designed to run over TCP.

ii. This is appropriate for retrieving the metafile, but not for retrieving the audio file.

iii. The reason is that TCP retransmits a lost or damaged segment, which is counter to the philosophy of streaming.

iv. We need to dismiss TCP and its error control; we need to use UDP.

v. However, HTTP, which accesses the web server, and the web server itself are designed for TCP; we need another server, a media server, as shown in Fig. 4.19.3.

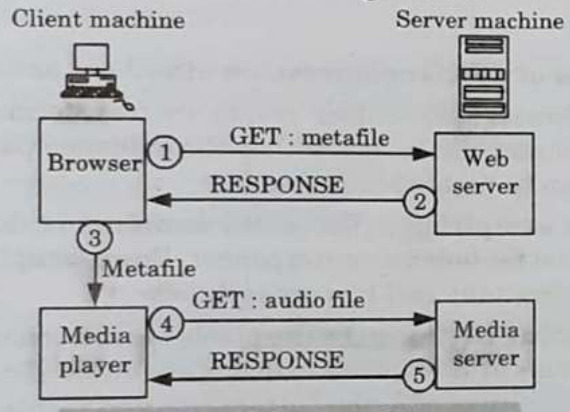

Fig. 4.19.3. Using a media server.

d. Using a media server and RTSP :

i. The Real Time Streaming Protocol (RTSP) is a control protocol designed to add more functionalities to the streaming process.

ii. Using RTSP, we can control the playing of audio.

iii. RTSP is an out-of-band control protocol that is similar to the second connection in FTP. Fig. 4.19.4 shows a media server and RTSP.

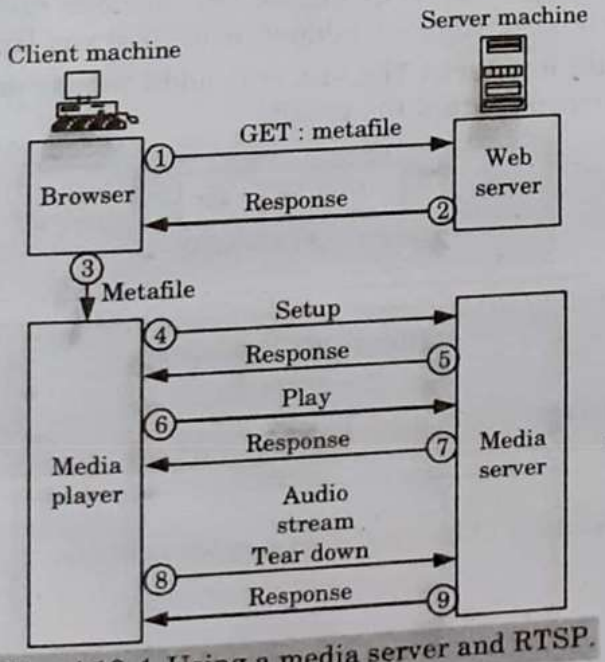

Fig. 4.19.4. Using a media server and RTSP.

Que 4.20. **Discuss the different steps of JPEG compression standard.** **AKTU 2014-15, Marks 05**

Answer

Different steps of JPEG compression standard are :

Step 1 (Transformation) : Colour images are transformed from RGB into a luminance/chrominance image so that chrominance part can lose much data and thus can be highly compressed.

Step 2 (Down sampling) : The down sampling is done for coloured component and not for luminance component. Down sampling is done either at a ratio 2:1 horizontally and 1:1 vertically.

Step 3 (Organizing in groups) : The pixels of each colour component are organized in groups of 8×2 pixels called "data units" if number of rows or column is not a multiple of 8, the bottom row and rightmost columns are duplicated.

Step 4 (Discrete Cosine Transform) : Discrete Cosine Transform (DCT) is then applied to each data unit to create 8×8 map of transformed components.DCT involves some loss of information due to the limited precision of computer arithmetic.

Step 5 (Quantization) : Each of the 64 transformed components in the data unit is divided by a separate number called its 'Quantization Coefficient (QC)' and then rounded to an integer.

Step 6 (Encoding) : The 64 quantized transformed coefficients of each data unit are encoded using a combination of RLE and Huffman coding.

Step 7 (Adding header) : The last step adds header and all the JPEG parameters used and output the result.

PART-6

Cryptography.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.21. **Write a short note on cryptography.**

Answer

1. Cryptography is the study of secret (crypto) writing (graphy).
2. It is concerned with developing algorithms that may be used to :

a. Conceal the context of some message from all except the sender and recipient (privacy or secrecy).
b. Verify the correctness of a message to the recipient (authentication).

3. It forms the basis of many technological solutions to computer and communications security problems.
4. Cryptography is the encoding of messages to render them unreadable by anyone other than their intended recipient(s).
5. Caesar cipher is one of the traditional cryptography techniques.
6. In modern cryptography it is essential to secure the computer network which is done using complex algorithms implemented on high speed computer systems.

Que 4.22. Define cryptography with the help of block diagram of symmetric and asymmetric key cryptography.

AKTU 2013-14, Marks 10

Answer

Cryptography : Refer Q. 4.21, Page 4–21A, Unit-4.

Symmetric key cryptography :

1. In symmetric key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

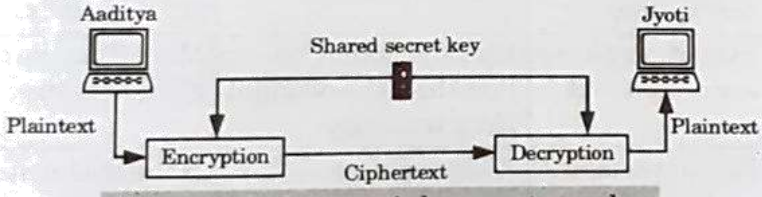

Fig. 4.22.1. Symmetric key cryptography.

2. The sender uses this key and an encryption algorithm to encrypt data, the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

Asymmetric key cryptography :

1. In asymmetric or public key cryptography, there are two keys : a private key and a public key.
2. The private key is kept by the receiver. The public key is announced to the public.
3. In Fig. 4.22.2 imagine Aaditya wants to send a message to Jyoti. Aaditya uses the public key to encrypt the message. When the message is received by Jyoti, the private key is used to decrypt the message.
4. In public key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption.

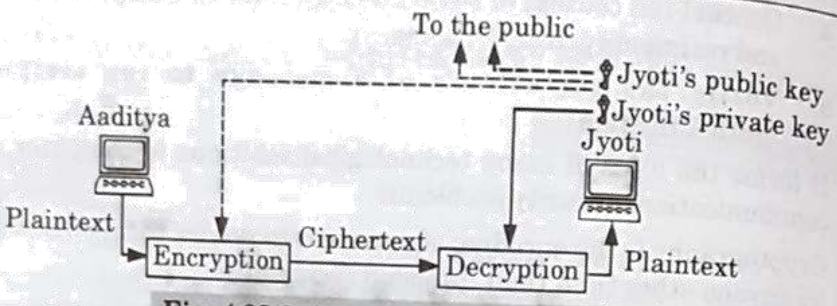

Fig. 4.22.2. Asymmetric key cryptography.

Que 4.23. **Distinguish between symmetric and asymmetric key cryptography.**

Answer

S. No.	Characteristic	Symmetric key cryptography	Asymmetric key cryptography
1.	Key used for encryption/ decryption	Same key is used for encryption and decryption.	One key used for encryption and another different key is used for decryption.
2.	Speed of encryption/ decryption	Very fast.	Fast, but less than symmetric key cryptography.
3.	Size of resulting encrypted text	Usually same as or less than the original clear text size.	More than the original clear text size.
4.	Key agreement/ exchange	A big problem.	No problem at all.
5.	Number of key required as compared to the number of participants in the message exchange	Equals about the square of the number of participants, so scalability is an issue.	Same as the number of participants, so scales up quite well.
6.	Usage	Mainly for encryption and decryption (confidentiality), cannot be used for digital signatures (integrity and non-repudiation checks)	Can be used for encryption and decryption (confidentiality) as well as for digital signatures (integrity and non-repudiation checks).

Que 4.24. **Write a short note on RSA encryption algorithm.**

Answer

i. RSA is the most widely used public key algorithm.

ii. The principle of RSA is based on a fact that it is easy to multiply two prime numbers but it is very difficult to factor the product and get them back.

iii. The algorithm is as follows :

1. Take two very large prime numbers A and B of equal lengths and obtain their product (N).

$$\therefore \quad N = A \times B \qquad ...(4.24.1)$$

2. Subtract 1 from A as well as B and take the product T.

$$\therefore \quad T = (A - 1)(B - 1) \qquad ...(4.24.2)$$

3. Choose the public key (E) which is a randomly chosen number such that it has no common factors with T.

4. Obtain the private key (D) as follows :

$$D = E^{-1} \bmod T \qquad ...(4.24.3)$$

5. The rule (algorithm) for encryption of a block of plaintext M into ciphertext C is as follows :

$$C = M^E \bmod N \qquad ...(4.24.4)$$

That means the plaintext M is raised to the power of E (public key) and then divided by N. The mod term in equation (4.24.4) tells us that the remainder of this division is sent as the ciphertext C as shown in Fig. 4.24.1.

6. The received message C at the receiver is decrypted to obtain the plaintext back by using the following rule (algorithm).

$$M = C^D \bmod N \qquad ...(4.24.5)$$

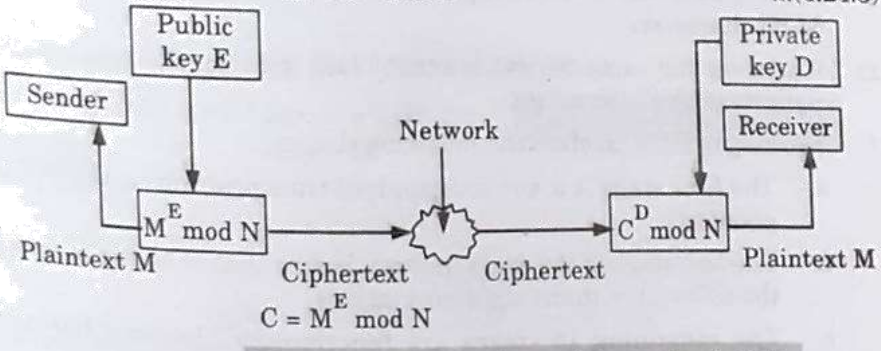

Fig. 4.24.1. Encryption and decryption in RSA.

Que 4.25. **Explain data encryption standard algorithm and its working in detail.**

Answer

1. The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption.
2. DES is based on a symmetric key algorithm that uses a 56-bit key as shown in Fig. 4.25.1.

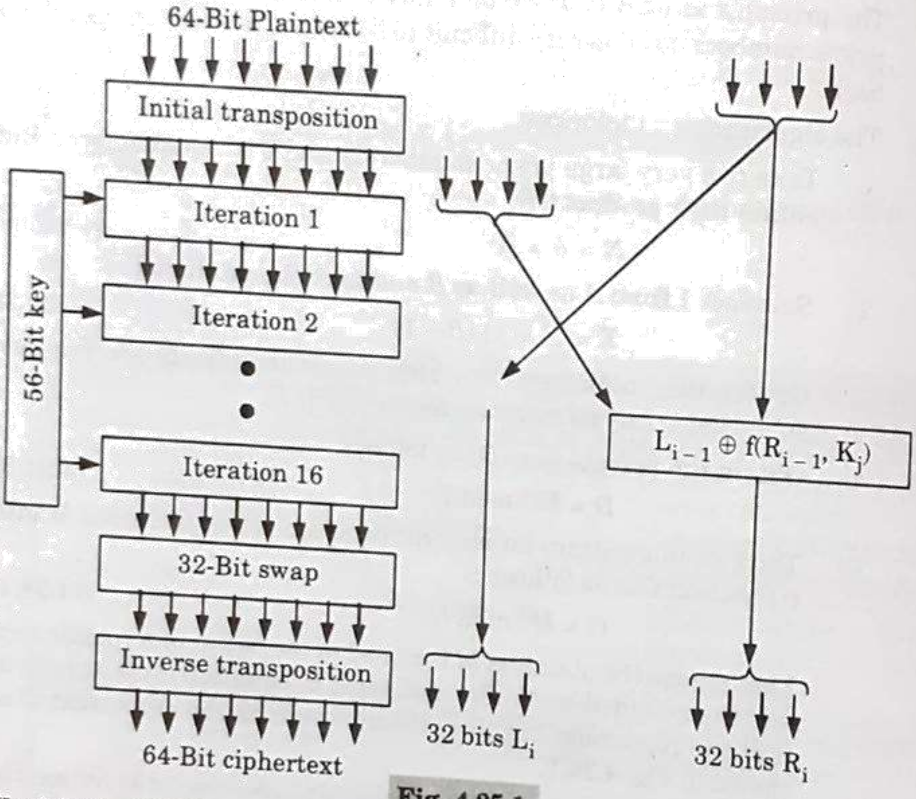

Fig. 4.25.1.

Working of DES :

1. DES is basically a mono-alphabetic substitution cipher using a 64-bit character.
2. Whenever the same 64-bit plaintext block goes in, the same 64-bit ciphertext block comes out.
3. Working of DES involves the following stages :
   a. The first stage is a key independent transposition on the 64-bit plaintext.
   b. The last stage is the exact inverse, before that is an exchange of the leftmost with the rightmost 32 bits.
   c. The remaining 16 stages are functionally identical but are parameterized by different functions of the key.
   d. The left output of an iteration stage is simply a copy of the right input. The right output is the exclusive OR of the left input and a

function of the right input and the key for this iteration. All the complexity lies in this functions which consists of four sequential steps.

Que 4.26. Differentiate between the block cipher with transposition cipher. **AKTU 2014-15, Marks 05**

Answer

S. No.	Block cipher	Transposition cipher
1.	A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.	Transposition cipher is the cipher in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
2.	Errors in transmitting one block generally do not affect other blocks.	Error in one letter will affect the whole ciphertext.
3.	Encryption process is slow.	Encryption process is fast.
4.	Security of block cipher depends on the design of encryption function.	Transposition cipher can be made more secure by performing more than one transposition.
5.	Algorithm breaks the plaintext into blocks and operates on each block independently.	Algorithm breaks the plaintext into letters and operates on each letter independently.

Que 4.27. Using the RSA public key cryptosystem with $a = 1, b = 2$ etc.

I. If $p = 7$ and $q = 11$, list five legal values for d.

II. If $p = 13$ and $q = 31$ and $d = 7$, find e. **AKTU 2014-15, Marks 05**

Answer

I. $p = 7 \quad q = 11$

$$n = p \times q = 7 \times 11 = 77$$

$$\phi(n) = (7 - 1) \times (11 - 1) = 6 \times 10 = 60$$

Choose a number relatively prime to $\phi(n)$ and satisfy the condition $1 < e < 60$ such that $gcd(\phi, e) = 1$

i.e., $e = \{13, 17, 19, 23, 29. 31, 37, 41, 43, 47, 53, 59\}$

Now, taking $e = 13$

$ed \bmod \phi(n) = 1$

$d = e^{-1} \bmod \phi(n)$

$d = 13^{-1} \bmod 60$

$d = 13^{\phi(77)-1} \bmod 60$

$d = 13^{59} \bmod 60$

$d = [[(13 \bmod 60)^4]^{13} ((13)^7 \bmod 60)] \bmod 60$

$d = 37 \bmod 60$

$d = 37$

Now, taking $e = 17$

$d = e^{-1} \bmod \phi(n)$

$d = 17^{-1} \bmod 60$

$d = 17^{59} \bmod 60$

$d = [[(17 \bmod 60)^3]^{17} ((17)^8 \bmod 60)] \bmod 60$

$d = (53 \times 1) \bmod 60$

$d = 53$

Taking $e = 19$

$d = e^{-1} \bmod \phi(n)$

$d = 19^{-1} \bmod 60$

$d = 19^{59} \bmod 60$

$d = [[(19 \bmod 60)^3]^{19} ((19)^2 \bmod 60)] \bmod 60$

$d = (19)^{19} \times 1 \bmod 60$

$d = [((19 \bmod 60)^1)^{18} \times 19 \times 1] \bmod 60$

$d = 1 \times 1 \times 19$

$d = 19$

Similarly by taking $e = 29$, we get $d = 29$

and $e = 37$, we get $d = 13$

Five legal value of d are 37, 53, 19, 29, 13.

II. $p = 13 \quad q = 31 \quad d = 7$

$n = p \times q = 13 \times 31 = 403$

$\phi(n) = (13 - 1) \times (31 - 1) = 12 \times 30 = 360$

$ed \bmod \phi(n) = 1$

$e = d^{-1} \bmod \phi(n)$

$= 7^{-1} \bmod 360$

$= 7^{\phi(403)-1} \bmod 360$

$= 7^{359} \bmod 360$

$= [(7^{11} \bmod 360)^{32} \times (7^7 \bmod 360)] \bmod 360$

$= [(103)^{32} \bmod 360 \times 223] \bmod 360$

$= [(103^4 \bmod 360)^8 \times 223] \bmod 360$

$$= [(121^4 \bmod 360)^2 \times 223] \bmod 360$$
$$= [(121)^2 \bmod 360 \times 223] \bmod 360$$
$$= (241 \times 223) \bmod 360$$
$$= 103$$

Que 4.28. Write a short note on voice over IP.

AKTU 2015-16, 2017-18; Marks 05

Answer

1. Voice over Internet Protocol (VoIP) is a technology used for delivering different kinds of data from a source to a destination using IP (Internet Protocol).
2. The data may be in many forms, including files, voice communication, pictures, fax or multimedia messages. VoIP is most often used for telephone calls, which are almost free of charge.
3. VoIP uses codes to encapsulate audio into data packets, transmit the packets across an IP network and unencapsulate the packets back into audio at the other end of the connection.
4. By eliminating the use of circuit-switched networks for voice, VoIP reduces network infrastructure costs, enables providers to deliver voice services over their broadband and private networks, and allows enterprises to operate a single voice and data network

Que 4.29. What are the problems for full implementation of voice over IP ? Did you think we will stop using the telephone network very soon ?

AKTU 2014-15, Marks 05

Answer

Problem for full implementation of VoIP are :

1. The computer must always be available in on mode with the internet connected.
2. Even if any one of the entities *i.e.*, the computer or internet fails to work, the telephone system will also not work.
3. There may be some delay in the voice due to problems in the internet.
4. The connection may lose in the middle if the internet connection is disconnected.
5. It may be susceptible to attacks.
6. The susceptibility of phone service to power failures can also occur.
7. The nature of IP makes it difficult to locate network users geographically and hence emergency calls cannot be routed easily.

No, we will not stop using telephone network.

PART-7

TCP, Window Management.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.30. **Compare and contrast TCP with RTP. Are both doing the same things ?**

AKTU 2014-15, Marks 05

Answer

S. No.	TCP	RTP
1.	TCP stands for Transmission Control Protocol.	RTP stands for Real Time Transport Protocol.
2.	It is a lossless protocol.	RTP is a stateless protocol,
3.	It is a slow process.	It is a faster than TCP.
4.	It cannot tolerate packet loss.	It can tolerate packet loss.
5.	TCP is not generally used for "real-time" streaming.	RTP is used for "real-time" streaming.

No, they are not doing the same things.

Que 4.31. **What is the total delay (latency) for a frame size of 10 million bits that is being set up on link with 15 routers, each having queuing time of 2 μs and a processing time of 1 μs ? The length of link is 3000 km. The speed of light inside the link 2×10^8 m/sec. The link has bandwidth of 6 Mbps.**

AKTU 2015-16, Marks 10

Answer

We have, Latency = processing time + queuing time + transmission time + propagation time

Processing time = $15 \times 1\ \mu s = 15\ \mu s = 0.000015$ s

Queuing time = $15 \times 2\ \mu s = 30\ \mu s = 0.000030$ s

Transmission time = $(10{,}000{,}000)/(6\ \text{Mbps}) = 1.67$ s

Propagation time = $(3000\ \text{km})/(2 \times 10^8\ \text{m/s}) = 0.015$ s

$\therefore$ Latency = $0.000015 + 0.000030 + 1.67 + 0.015 = 1.685045$ s

Que 4.32. **A rectangular wave-guide ($a = 2$ cm, $b = 1$ cm) filled with deionized water ($\mu = 1$, $\xi = 81$) operates at 3 GHz. Determine all propagating modes and corresponding cut-off frequencies.**

AKTU 2015-16, Marks 10

Answer

For a general transverse electric (TE) or transverse magnetic (TM) mode, the cut-off frequency is given as :

$$f_c = \frac{v_0}{2\sqrt{\mu\xi}}\sqrt{\left(\frac{m}{a}\right)^2 + \left(\frac{n}{b}\right)^2} = \frac{3\times10^8}{2\sqrt{1\times81}}\sqrt{\left(\frac{m}{0.02}\right)^2 + \left(\frac{n}{0.01}\right)^2}$$

$$= 1.667\sqrt{0.25m^2 + n^2} \text{ GHz}$$

The cut-off frequencies as calculated from the equation for different values of m and n are given in the Table 4.32.1.

Table 4.32.1.

Cut-off frequency (in GHz) for TM modes				Cut-off frequency (in GHz) for TE modes				
	$n = 1$	$n = 2$	...		$n = 0$	$n = 1$	$n = 2$	
$m = 1$	1.863	3.436	...	$m = 0$	×	1.667	3.333	...
$m = 2$	2.357	3.727	...	$m = 1$	0.833	1.863	3.436	...
$m = 3$	3.005	⋱		$m = 2$	1.667	2.357	3.727	...
	⋮			$m = 3$	2.500	3.005	⋱	
				$m = 4$	3.333	⋮		
					⋮			

Since the operating frequency is 3 GHz, all the propagating modes and their cut-off frequencies are given in the Table 4.32.2.

Table 4.32.2.

Mode	Cut-off frequency (GHz)
TE_{10}	0.833
TE_{01}, TE_{20}	1.667
TE_{11}, TM_{11}	1.863
TE_{21}, TM_{21}	2.357
TE_{30}	2.500