1(a): RPC is Remote Procedure Call that used to call other processes on the remote systems like a local system. Or we can say RPC is if one process is suspended and other is started then when it’s finished at that time the previous one I mean the suspended one is again will restart his work this technique is called RPC.

RPC operations:

1. The client procedure calls the client stub in the normal way.

2. The client stub builds a message and calls the local operating system.

3. The client's OS sends the message to the remote OS.

4. The remote OS gives the message to the server stub.

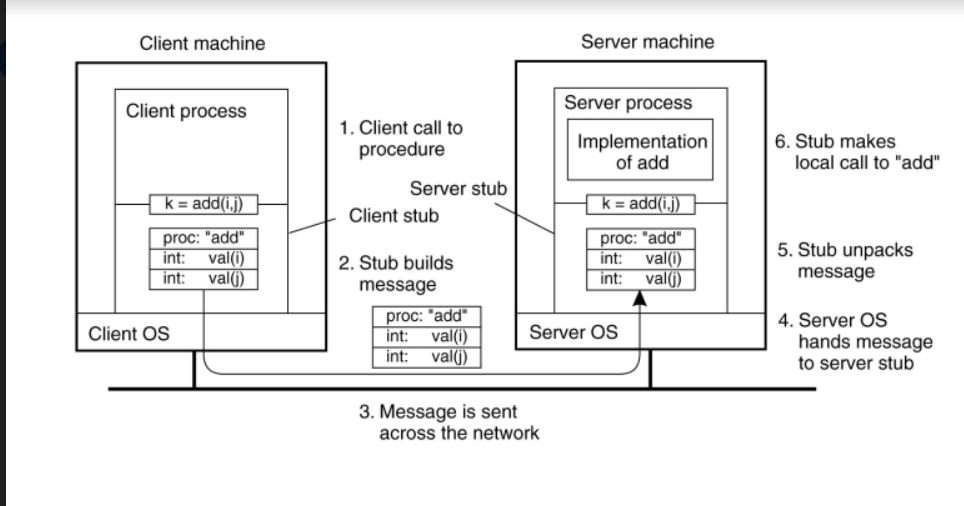
5. The server stub unpacks the parameters and calls the server.

6. The server does the work and returns the result to the stub.

7. The server stub packs it in a message and calls its local OS.

8.The server's OS sends the message to the clients OS.

9.The client's OS gives the message to the client stub.

10.The stub unpacks the result and returns to the client. 

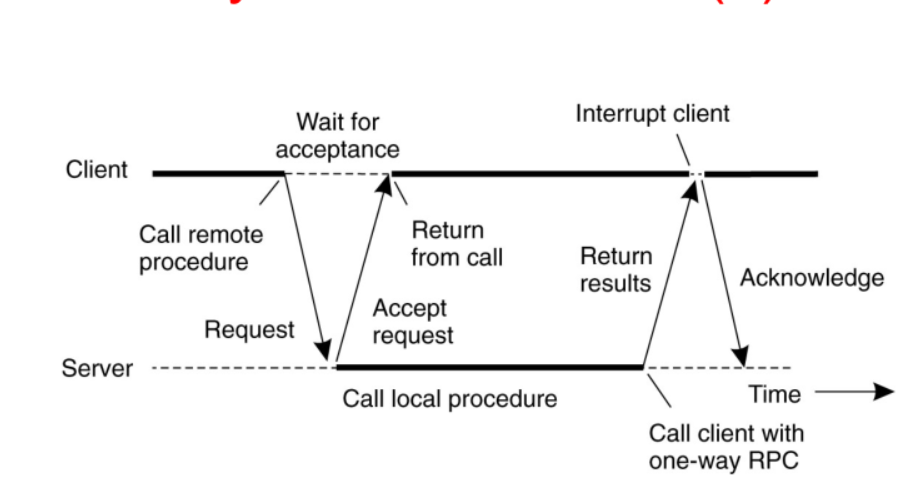
1(b): in this case of message /data passing in rpc system for full combination on waiting and conference

We can say the suitable Explanation and fig will be Defered asynchoronous

This is the easy its all about the when the client get the ecceptence then the client user will decide to reply as thanks message this can always reply comes out from the client

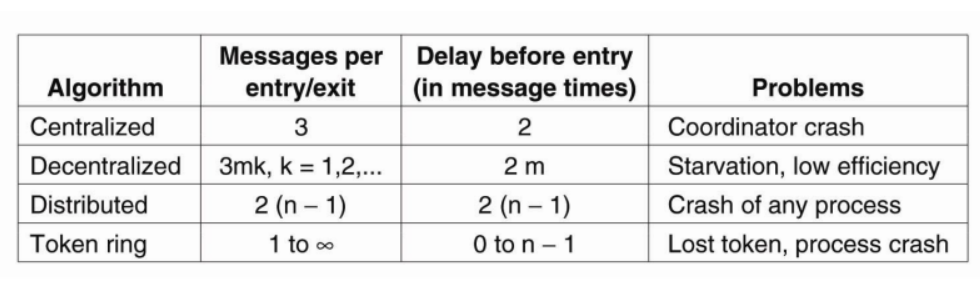
And three rpc process are done through Deferred algorithm

In here also theres two simultaneous Asynchronous RPC Working here



2(b): Barkley Algorithm is a clock synchronization technique used in distributed systems. Here the time is active, polling every machine from time to time to ask what time it is there. Based on the answers, it computes an average time and tells all the other machines to advance their clocks to the new time or slow their clocks down until some specified reduction has been achieved

3(a):



3(b): There are two problems in lamport’s algorithm and there solutions

(1): if sender and receiver times are same that is a problem and the solution is

Solution: sender+0.1 add the sender time + 0.1

Receiver+0.2 and add the receiver time + 0.2

(2): if the sender time is greater than the receiver time the solution is

Solution: receiver = sender time + 1

And we will use process by lamport’s algorithm

4(a):

1. Availability

2. Reliability

3. Safety

4. Maintainability

**Availability** is defined as the property that a system is ready to be used

immediately. In general, it refers to the probability that the system is operating

correctly at any given moment and is available to perform its functions on behalf

of its users. In other words, a highly available "system is one that will most likely

be working at a given instant in time.

**Reliability** refers to the property that a system can run continuously without failure.

In contrast to availability, reliability is defined in terms of a time interval instead of an instant in time. A highly reliable system is one that will most likely continue to work without interruption during a relatively long period of time.

This is a subtle but important difference when compared to availability. If a system goes down for one millisecond every hour, it has an availability of over 99.9999 percent, but is still highly unreliable.

**Safety** refers to the situation that when a system temporarily fails to operate correctly, nothing catastrophic happens.

For example, many process control systems, such as those used for controlling nuclear power plants or sending people into space, "are required to provide a high degree of safety. If such control systems temporarily fail for only a very brief moment, the effects could be disastrous.

Many examples from the past (and probably many more yet to come) show how

hard it is to build safe systems.

**maintainability** refers to how easy a failed system can be repaired' A highly maintainable system may also show a high degree of availability, especial if failures can be detected and repaired automatically recovering from failures is easier said than done.

Often, dependable systems are also required to provide a high degree of security, especially when it comes to issues such as integrity.

4(b):

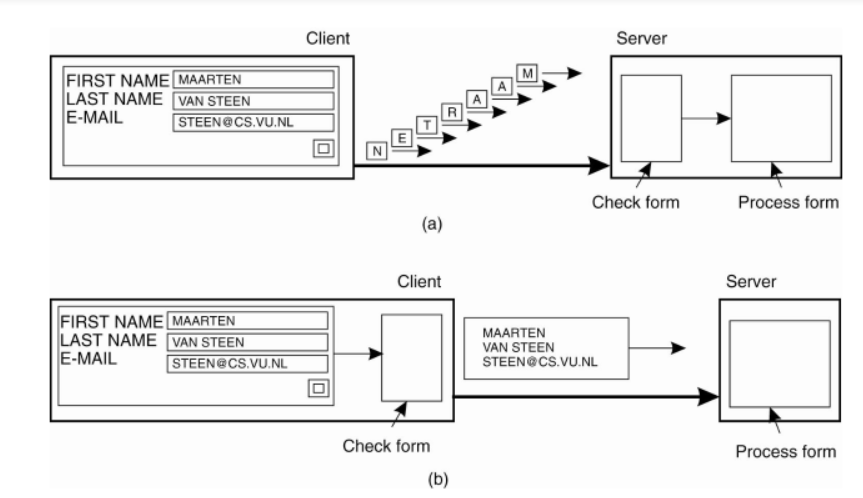
**why the server-side checking is not better than client-side checking**

In the Client Side Validation you can provide a better user experience by responding quickly at the browser level.

When you perform a Client Side Validation, all the user inputs validated in the user's browser itself.

Client Side validation does not require a round trip to the server, so the network traffic which will help your server perform better.

For example, if the user enter an invalid email format, you can show an error message immediately before the user move to the next field, so the user can correct every field before they submit the form.



(5): **Security Treats and prevention of mechanism**

•       Security Treats  Way of looking at security in computer systems is that we attempt to protect the services and data it offers against security threats.

Types of security threats:

Interception

Interruption

Modification

Fabrication

**An interception** is where an unauthorized individual gains access to confidential or private information.

**Interruption** is services or data becoming unavailable, unusable, destroyed.

**Modification**: Modify some existing information.

**Fabrication**: Fully Change the existing information.

**Security Mechanisms:**

•       Encryption

•       Authentication

•       Authorization

•       Auditing