1. Preocupações de um sistema distribuído deve ser transparente mantendo aspetos invisiveis para o utilizador. As outras formas de transparência são:o acesso a recursos locais e remotos com operações idênticas, a localização que permite a utilizacr recursos sem conhecimento da sua localização exacta, a concorrência permite executar simultâneamente vários processos partilhando recursos sem que haja interferências entre eles, a replicação que utiliza múltiplas instâncias de recursos para aumentar a fiabilidade e a performance, sem que o utilizador ou aplicações cliente tenham conhecimento das réplicas, o tratamento de falhas para que o utilizador e as aplicações completem a sua tarefa, independentemente da ocorrência de um problema de hardware ou software, a mobilidade de recursos e clientes dentro de um sistema sem afectar as operações de utilizadores e programas, a performance que permite a reconfigurar o sistema aumentando o desempenho à medida que as cargas variam, tudo isto sem afetar a estrutura do sistema.
2. Distinga Modelo Cliente-Servidor de Modelo Peer Processes. Modelo Cliente-Servidor, os clientes invocam um servidor e um servidor pode ser cliente para se ligar a outro servidor. Modelo Peer Processes baseado em processos que comunicam entre si para realizar uma tarefa em que estes desempenham papéis idênticos, não existe separação prévia entre clientes e servidores. Existem processos que podem comportar-se como clientes ou como servidores.
3. Descreva o comportamento das operações send e receive (na transmissão de uma mensagem), relativamente ao bloqueio, em cenários de comunicação síncrona e assíncrona.Comunicação síncrona os processos emissor e receptor sincronizam-se a cada mensagem, onde o send e o receive são operações bloqueantes. O emissor fica parado no send até que o receive seja efectuado, e ao efectuar um receive, o receptor fica bloqueado até a mensagem chegar. Comunicação assíncrona não há sincronização, ou seja, o send não é bloqueante, o emissor prossegue assim que a mensagem passa ao buffer local de saída e o receive pode ser bloqueante ou não, visto que o processo prossegue com um buffer que será preenchido em background, existindo uma notificação quando o buffer é preenchido.
4. Explique a diferença entre sistemas síncronos e assíncronos. Sis.Si.- existem limites para: tempo de execução de cada passo d um processo, tempo que demora até à recepção d uma mensagem enviada e para o clock drift rate em cada máquina. Sis.Assi - não há limite definido ou garantias para a veloci de execução de um processo, para o tempo de transmissão de uma mensagem, esta pode ter atraso (delay), nem para o clock drift rate a taxa deste é arbitrária.
5. Descreva o processo designado por Marshalling e justifique a sua utilização. consiste na tradução de estruturas e tipos primitivos para uma representação externa de dados (formato usado para a representação de estruturas e tipos primitivos) adequada para a sua transmissão. Marshalling é utilizado para que uma estrutura d dados possa ser usada em RPC ou RMI, ou seja, para qu possa ser representado de modo flattened e os tipos primitivos num formato acordado.
7. Indique uma diferença entre Marshalling em CORBA assume-se que o emissor e receptor conhecem os tipos de cada elemento da mensagem, por isso o tipo não é passado (apenas o valor)e o usado em Java RMI, a aplicação que recebe a mensagem pode não conhecer o tipo de dados logo a representação serializada tem info sobre a classe do objecto
8. Descreva as vantagens fornecidas pela camada Middleware são: Transparência face à localização; - Independência dos protocolos de comunicação , do Hardware e dos Sist Opera; - Utilização de diferentes linguagens de programação.
abstracções que disponibiliza ao programador de sistemas distribuídos são: RPC descreve procedimentos disponíveis e respectivos argumentos, não se podem passar pointers como argumentos
RMI tem métodos de objecto disponíveis para Invocação Remota e podem passar-se referências para objectos remotos.
9. Quais os 3 tipos de medidas de tolerância a falhas desejáveis para primitiva doOperation, no protocolo Request-Reply. São 1-reenvio do pedido que reenvia a mensagem com o pedido para o servidor até a resposta chegar ou se detectar que o servidor está com problemas,2-filtragem de duplicados que decide se o duplicado deve ser processado para reenvio ou ignorado 3-retransmissão de resultados que através d histórico destes evita nova execução da operação.
b) Quais são usadas pelas semânticas de invocação Maybe, At-least-once e At-most- once.
A Maybe não reenvia o pedido, a filtragem de duplicados e a retransmissão de resultados não são aplicáveis.
O At-least-once reenvia o pedido, não filtra os duplicados e executa de novo a retransmissão de resultados.
O At-most-once reenvia o pedido, filtra os duplicados e retransmite do histórico os resultados.
c) Quando estão envolvidas operações não idempotentes. mais apropriada é o Maybe.
10. O mecanismo de invocação CORBA num cenário de diferentes Ling. Progr. E aplicações permite que objetos distribuídos e implementados em diferentes Ling.Prog. possam comunicar. E necessita duma Interface Definition Language que forneça a notação para as interfaces que poderão ser usadas pelas diferentes aplicações.
11. Em Java RMI, que operações devem ser obrigatoriamente efectuadas pela aplicação Servidor, é ter as classes dispatcher e skeleton, para que um cliente possa invocar métodos remotamente sobre o objecto remoto classes Servant ou Impl, que presta um serviço? tem-se de criar pelo menos um objecto remoto e inicializá-lo, registar objecto no binder, e para evitar demoras cada invocação remota é tratada numa nova thread.
12. Descreva o papel de Proxy, Dispatcher e Skeleton na abstracção RMI. Papel do Proxy torna a invocação remota transparente para o cliente, faz o marshalling de argumentos e o unmarshalling do resultado da invocação, é unico para cada objecto remoto que um processo referencie e implementa os métodos da interface remota do objecto, mas cada método faz marshall da referência do objecto, methodid, e argumentos, aguardando a resposta para o unmarshall.
O Dispatcher é unico para cada classe de objecto remoto, no servidor. Recebe a mensagem e pelo methodId selecciona o método apropriado no Skeleton. O Skeleton é um por cada classe que representa um objecto remoto, no servidor implementa os métodos na interface remota, efectua unmarshall a argumentos no pedido, invocando o método no objecto remoto (localmente) e devolvendo o marshall do resultado e eventual excepção na resposta ao proxy.
13. Distinga os modos de sincronização interna e externa de relogios num sistema. Relogios sincronizados de modo interno não estão necessariamente sincronizados de modo externo, ou seja, se cada nó de um sistema está sincronizado de modo externo (com a mesma fonte) com limite D, então esse sistema está internamente sincronizado com limite 2D.
14. Algoritmo de sincronização de Cristian sincroniza se o tempo para a troca de mensagens cliente-servidor é suficientemente pequeno quando comparado com a precisão desejada e o servidor de tempo é UTC S.O processo p envia pedido mr e recebe um tempo t em mt, p regista o tempo de viagem de mr e mt onde T = Tmr + Tmt. Daqui estima-se o tempo em p com t + T/2.

15. Algoritmo de sincronização de Berkeley é para sincronização interna de um grupo de computadores, onde uma máquina é escolhida para coordenar (master). O master pede periodicamente uma leitura aos restantes (slaves) e estima a hora em cada slave, pela observação do tempo de viagem das mensagens e pelo valor recebido (como em Cristian) e faz a média de todos os valores (incluindo o seu próprio tempo). O master em vez de enviar o tempo actualizado aos slaves (o que estaria sujeito ao tempo de envio variável), o master envia a cada um o valor exacto que deve usar para ajustar o seu relógio. Se o master falhar, outro será escolhido para assumir a sua função.
16. Algoritmo GC - Garbage Collection, do lado do servidor mantém uma lista com o conjunto de processos com referências para os seus objectos e quando um cliente cria um Proxy para um objecto, é adicionado ao conjunto de processos com referências para aquele objecto. Quando o GC do cliente detecta que o Proxy do objecto já não é necessário, este envia uma mensagem ao servidor e elimina o proxy, onde o servidor remove o processo da lista e quando a lista estiver vazia, o GC do servidor recupera o espaço do objecto, excepto se existirem referências locais.
b) Vulnerabilidades do algortimo GC face a falhas no cliente são que o servidor (com objectos remotos) atribui um intervalo de tempo ao cliente e a contagem é válida até que o tempo expire ou o cliente remova a referência do objecto.
17.O protocolo NTP permite três modos para sincronização de relógios em servidores são: 1-multicast é de baixa precisão é usado em redes locais de alta velocidade, onde um ou mais servidores enviam periodicamente o tempo num broadcast e os servidores noutras máquinas acertam o relógio assumindo um pequeno delay. 2-Procedure-call onde um servidor aceita pedidos de outros computadores, aos quais responde com a informação horária que tem. É utilizado quando se pretende maior precisão que no modo multicast, ou quando não é possível multicast. 3-Simétrico que serve para sincronizações entre servidores que fornecem a informação em redes locais e em níveis mais altos da NTP subnet, onde se pretende a máxima precisão. Aqui um par de servidores trabalha de modo simétrico, troca mensagens com informação horária e o tempo das mensagens também é considerado.
b) Qual o método onde se consegue a precisão máxima? é no modo simétrico.
18)Na assinatura digital de chave pública, qual a chave usada para encriptar? A chave usada para encriptar é a chave privada. É usada esta, porque o objectivo não é a confidencialidade da mensagem, para além de ser mais simples e dispensar comunicação entre os intervenientes.
19)Vantagem da assinatura digital de chave secreta (MAC), nos contextos em que se pode utilizar, face à assinatura digital de chave pública. É a performance porque não há encriptação e porque as funções de hash são 3 a 10 vezes mais rápidas que os algoritmos simétricos.
20)No contexto do Sistema de Ficheiros Distribuído NFS, o papel do sistema de ficheiros virtual (virtual file system) relativamente às aplicações de utilizador, do lado do cliente é integrar este no Kernel permitindo o acesso aos ficheiros através de system calls, servir como único módulo cliente todos os processos user-level, com uma cache dos blocos em uso.Chave usada na encriptação do uid fica protegida a nível do kernel, a salvo de aplicações user-level.
21)No Sistema de Ficheiros Distribuído NFS o servidor é stateless. porque tem vantagem para a consistência, ou seja, o servidor tem de validar a identidade do utilizador junto dos atributos de acesso a cada pedido e os clientes enviam informação sobre a autenticação do utilizador, a cada pedido, em campos próprios nas RPCs. Como consequência, tem-se um problema de segurança, pois um utilizador podia alterar o uid passado por RPC.
22)No serviço de nomes, a navegação é o processo de pesquisa por vários servidores. Descreva as diferentes formas possíveis de navegação são as controladas pelo cliente ou pelo servidor. Cliente podem ser iterativas (se um servidor não tem a resposta, o cliente liga-se ao seguinte) ou multicast (o cliente faz um multicast com o nome a resolver para um grupo de servidores. O servidor que tem a informação responde-lhe em unicast). Servidor podem ser recursivas ou não recursivas. As não recursivas podem ser iterativas ou em multicast entre os servidores.
23)Uma empresa decidiu replicar o servidor de backend do seu serviço, que se encontrava numa única máquina com probabilidade 0,06 de falhar ou ficar incontactável, para uma segunda máquina idêntica. Apresente uma estimativa para a taxa de disponibilidade do serviço com as duas máquinas no backend.P = 0,06; N = 2 máquinas 1 – p^N = 1 – (0,06)^2 = 99,64% **24)ndique existe consistência linear?**Um objecto replicado é linearmente consistente se, para qualquer execução, existe algum encadeamento/sequência das operações desencadeadas por todos os clientes que permita a sequência de alcançar uma única cópia correcta dos objectos e a ordem das operações na sequência está de acordo com o tempo real a que efectivamente ocorreram.**25)indique, se existe consistência sequencial** um objecto replicado obedece à consis. sequencial se: para cada execução, existe sequência de operações desencadeadas por todos os clientes que permita a sequência de alcançar uma única cópia correcta dos objectos e a ordem das operações na sequência está de acordo com a ordem no código do programa do cliente que as executa.
26)Uma empresa pretende um sistema replicado e com tolerância a falhas, apto para continuar a prestar um serviço correcto mesmo na presença de 4 falhas bizantinas. Deve-se optar por um modelo de replicação activa porque o modelo de replicação passiva não tolera falhas bizantinas. **Quantos RM devem existir no backend do serviço?** 2N + 1 RM = 2*4 + 1 = 9 RM
27)Com o tipo de replicação passiva, que tipo de falhas pode o sistema tolerar e quantas podem ocorrer sem que o serviço teja fechado? permite sobreviver a N crashes de servidores com N+1 RM e não tolera falhas bizantinas.
28)funcionamento do AFS quando uma aplicação do utilizador pretende aceder (faz open)a um ficheiro remoto, o servidor respectivo é localizado e envia uma cópia que é armazenada no file system do cliente e aberta, sendo devolvido ao utilizador o respectivo file descriptor unix. As operações de leitura e escrita ocorrem sobre essa réplica. Ao efectuar um close se a réplica foi alterada o conteúdo é enviado ao servidor AFS que actualiza a sua e a réplica permanece junto do cliente para eventual uso por outro utilizador da workstation.
29)Definição para autenticação e descreva um processo de autenticação baseado em criptografia. Autenticação é a garantia sobre a identidade de um interveniente ou a origem de uma mensagem. Um processo de autenticação simples baseado em criptografia é o algoritmo de Needham-Schroeder onde há um servidor de autenticação que conhece a identificação e a chave secreta de cada principal no sistema. Essa chave secreta é conhecida apenas pelo principal e pelo servidor S, servindo para autenticação do principal junto do servidor e para cifrar mensagens entre os mesmos.

30)Se um principal A não deseja partilhar (desde início e secretamente) uma chave com o seu interlocutor B, que tipo de algoritmo criptográfico deve usar-se neste cenário?usa-se um algoritmo assimétrico, dado que nos algoritmos simétricos existe partilha de chave secreta.
31)Aplicando o algortimo RSA ou IDEA para encriptar dados, tendo como objectivo a confidencialidade dos mesmos quando enviados de A para B. Indique quais as chaves envolvidas nos processos de encriptação e desencriptação.RSA: Encriptação: chave pública de B, Desencriptação: chave privada de B
IDEA: Encriptação: chave secreta partilhada entre A e B, Desencriptação: chave secreta escondida de todos os outros
32)Descreva a sequência de mensagens para a autenticação de um utilizador junto de um servidor, utilizando o algoritmo Kerberos. 1-O primeiro nível de autenticação (AS) consiste numa verificação segura de utilizador/password. O cliente pede ao servidor de autenticação A que lhe forneça um Ticket para a comunicação com o servidor TGS
2-Em resposta obtém um ticket e a chave de sessão para comunicar com o TGS, tudo encriptado com a sua chave secreta. Esta mensagem inclui um Nonce encriptado com Kc, o que significa que é proveniente do servidor. O Ticket está encriptado com a chave do servidor TGS, contendo as identidades C e TGS, timestamps de validade e a chave de sessão entre C e TGS, Kct **3**-C comunica com servidor TGS, enviando um Token de Autenticação (encriptado com chave secreta Kct), o ticket para TGS, a identificação do servidor S para o qual pretende o Ticket e nounce **4**-TGS verifica o ticket apresentado. Se é válido então gera uma chave de sessão Kcs e devolve a chave de sessão Kcs e nounce, encriptados com Kct e o ticket para S(encriptado com chave secreta do servidor S, Ks) 5-C comunica com o servidor S (do serviço pretendido), enviando o token de autenticação (cifrado com a chave de sessão secreta Kcs), o ticket para S (cifrado com Ks, secreta do servidor S), o nonce (encriptado com Kcs) e o pedido ao servidor (encriptado com Kcs quando se requer confidencialidade) **6**-S responde. A resposta pode incluir o nonce N, encriptado com Kcs
33)Como se valida uma assinatura digital de um documento? Chave secreta – só pode ser verificada por quem possuir a chave secreta Chave pública – verificada por qualquer principal com a chave pública do signer
34)Dois tipos de Uniform Resource Identifier (URI), e suas caracteristicas chaves. URLocator tem o esquema (http, mail, ftp), hostname e pathname até ao documento e tem problemas em dangling links (se o objecto é movido podem ficar apontadores inválidos. **URName** o identificador é persistente, mesmo que o recurso mude de localização, regista-se o nome URN, incluindo atributos do documento, se o URL mudar basta actualizar o URL registado para aquele URN e a pesquisa faz-se pelo URN e resulta sempre no URL correcto.
35)"Resolução de Nomes"é o processo em que se apresenta um nome a um contexto, que tem um binding directo desse nome num conjunto de atributos ou efectua a procura de um binding num outro contexto.
36)As callbacks promise no Sistema de Ficheiros Distribuídos AFS? garantem a passagem de Vice para Venus de que notificará a actualização do ficheiro sempre que outro cliente o alterar. Armazenadas do lado do cliente, junto à réplica do file, 2estados (válida e cancelada) são revistas quando servidor recebe operação close de um file actualizado.
37)Ataques são: Eavesdropping – obter cópias de mensagens sem autorização. Masquerading – envio ou recepção de mensagens utilizando uma identidade de outro principal sem o seu consentimento. Message Tampering intercepção e alteração de mensagens, que em seguida são enviadas para o destinatário original .Replaying – guardar uma mensagem interceptada para enviar mais tarde. Denial of Service congestionamento de um canal ou recurso para impedir o acesso por parte dos utilizadores comuns**Medidas para evitar Ataques**:Firewalls, Controlo de Acesso, Certificados, Credenciais e Criptografia, com o propósito de conseguir autenticação, integridade, confidencialidade, assinaturas digitais e não repúdio.
38)Assinatura digital de chave secreta ou MAC. requer um processo seguro para transmitir a chave secreta até ao verifier, pode ser necessário verificar a assinatura numa fase posterior à sua criação.A partilha da chave secreta traz fraqueza pois um detentor da chave pode forjar a assinatura do signer original. Utiliza um canal seguro para transmitir mensagens não encriptadas mas para as quais é necessário verificar a autenticidade. O canal seguro permite a transmissão de chave secreta para uso nestas AD "de baixo custo computacional".
39)Funcionalidade nos serviços de Directoria que não exista nos serviços de Nomes? Serviços nomes existem pares (nome, atributos) e a pesquisa efectua-se pelo nome mas em determinados cenários pode interessar a pesquisa pelos atributos, enquanto que o serviço de directoria guarda associações (bindings) entre nomes e atributos e permite pesquisa de entradas baseada nos atributos, logo podemos afirmar que os serviços de directorios têm mais funcionalidades que os serviços de nomes.
40)Mecanismo de segurança híbrido? Vantagens face ao uso de um algoritmo criptográfico simétrico ou assimétrico?O propósito é que resolvem o problema de exigência computacional dos algoritmos assimétricos e são robustos. Este combina técnicas de encriptação simétrica e assimétrica como a criptografia de chave pública para autenticar os intervenientes e para transmissão de chaves secretas, assim como algortimos simétricos de chave secreta para restante encriptação.
41)Componentes genéricos da arquitectura de um serviço de ficheiros, e suas respectivas funções. As componentes são os Serviços Flat File, Directorias e Módulo Cliente. Flat File são operações sobre o conteúdo dos ficheiros, os pedidos referem ficheiros com identificadores únicos no SD (UFIDs) e ao criar um ficheiro, é gerado um novo UFID. Directorias mapeia nomes (texto) de ficheiros em UFIDs e cria directorias, adiciona ficheiros a directorias. Módulo cliente é executado em cada computador cliente, integra e estende as operações das componentes anteriores, disponibiliza uma interface de programação aos programas (user-level) e guarda informação sobre a localização na rede dos serviços de directorias e flat file.
42)Motivo de usar replicação num sistema distribuído SD? Num SD espera-se que os serviços tenham alta disponibilidade, a melhor performance possível e que o efeito das falhas seja mínimo, assim replicação é fundamental, na medida em que contribui para a performance, alta disponibilidade e tolerância a falhas.