LEIC/LERC – 2012/13, 1º Exame de Sistemas Distribuídos, 5 de Junho de 2013

Responda no enunciado, apenas no espaço fornecido. Identifique todas as folhas. Duração: 2h30m

Grupo I [3v]

Considere o stub cliente do SUN RPC correspondente a uma função de soma.

```
calc_result *
sum_2(calc_args *argp, CLIENT *clnt)
{
        static calc_result clnt_res;
        if (clnt_call(clnt, SUM,
                    xdr_calc_args, argp,
                    xdr_calc_result, &clnt_res,
                    TIMEOUT) != RPC_SUCCESS) {
         return (NULL);
        }
        return (&clnt_res);
}
```

1. O cliente que utiliza esta função tem de obter previamente a localização do servidor.
   a) [0,4v] Descreva a forma como a localização do servidor é obtida.

   b) [0,4v] Depois de conhecer a localização, tem de ser estabelecido um canal de comunicação e este tem de ser utilizado pelo procedimento *sum_2.* Explique detalhadamente como é que esta associação do canal à função é efectuada e identifique no stub se existe alguma estrutura de dados que o represente.

   c) [0,3v] A função tem a designação sum_2. Se existir uma função _3, o que potencialmente pode mudar nesta função? A sua resposta deve ser concreta utilizando os elementos do programa.

2) [0,4v] A função clnt-call chama duas funções xdr_calc_args e xdr_calc_result, cuja função é efectuar o *marshalling* dos parâmetros. Explique concretamente para a função xdr_calc_result, qual é o input e o respectivo formato.

3) A função tem um retorno que trata potenciais situações de excepção (erro).
   a) [0,3v] Indique 3 situações com causas diferentes que podem conduzir a uma excepção.

   b) [0,3v] Compare este tratamento de excepção com o existente em RMI e em Web-Services, explicitando a principal diferença.

4) Considere as seguintes situações num protocolo de RPC e **indique qual a semântica de invocação, justificando**.
   a) [0,3v] Ligação TCP e perante ausência de resposta ou quebra de canal o cliente não repete.

   b) [0,3v] Ligação UDP e perante ausência de resposta repete a mensagem. As mensagens têm identificadores únicos e o servidor mantém as respostas até *acknowledge* do cliente.

   c) [0,3v] Ligação TCP e perante quebra de canal o cliente tenta nova ligação e repete a mensagem até obter resposta.

Grupo II [2,7v]

Considere a seguinte interface Java, que permite gerir um catálogo de uma loja:

```
public interface ICatalogo extends Remote {
  public IProduto consultaProduto(String idProduto) throws RemoteException;
  public void apagaProduto(String idProduto) throws RemoteException;
  public void adicionaProduto(IProduto novoProduto) throws RemoteException;
}
```

Assuma que um servidor S1, a correr na máquina “sd.ist.utl.pt”, tem uma instância da classe CatalogoServant, que implementa ICatalogo. Essa instância foi registada no *rmiregistry* com o nome “meuCatalogo”.

1) [0,6v] Apresente agora o extrato do programa de um cliente (remoto) que tenta consultar um produto identificado por "livro-sd" no catálogo da alínea anterior e apresenta o conteúdo do produto no ecrã chamando o método toString() da interface IProduto.
   Nota: por simplicidade, omita a preparação do SecurityManager da sua resposta.

2) [0,4v] No caso da consulta ter sucesso, o retorno do método consultaProduto chamado na alínea anterior pode ser passado por valor ou por referência. Como distingue o RMI se a passagem do retorno do método é por valor ou por referência?

3) [0,4v] No caso de ser passagem por valor, que classe(s) é/são carregada(s) no cliente para que o retorno de consultaProduto se concretize?

4) Assuma agora que o retorno do método consultaProduto é passado por referência.
   a) [0,4v] Que classe é carregada no cliente?
   b) [0,4v] Onde é armazenada a informação que associa a referência remota ao objecto no servidor remoto?
   c) [0,5v] O retorno desta referência remota no cliente causa alguma alteração do garbage collector do servidor S? Se não, justifique. Se sim, explique o que acontece.
      Nota: assuma que, antes deste momento, o cliente não tinha qualquer referência remota para S.

Grupo III [2,7v]

```
1 package example.ws.handler;
2 public class HeaderHandler implements SOAPHandler<SOAPMessageContext> {

3    public boolean handleMessage(SOAPMessageContext smc) {

4        try {
5                SOAPMessage msg = smc.getMessage();
6                SOAPPart sp = msg.getSOAPPart();
7                SOAPEnvelope se = sp.getEnvelope();
8                SOAPHeader sh = se.getHeader();
9                if(sh == null)
10                    sh = se.addHeader();
11                Name name = se.createName("myHeader", "d", "http://demo");
12                SOAPHeaderElement element = sh.addHeaderElement(name);
13                int value = 20;
14                String valueString = Integer.toString(value);
15                element.addTextNode(valueString);

16        } catch (Exception e) {
17            out.println(this + "> Caught exception in handleMessage: ");
18            out.println(e.getClass().toString());
19            out.println(e.getMessage());
          }
20        return true;
    }
}
```

O excerto de código acima faz parte do programa de um handler para Web Services e foi um dos exemplos que estudou para realizar o seu projecto.

1) [0,4v] Descreva a estrutura de um envelope SOAP com todos os seus elementos constitutivos. Indique a função da cada uma, relacionando com as linhas em que essa estrutura é referida no handler.

2) [0,4v] Genericamente, para que serve um handler?

3) [0,4v] Este handler de demonstração o que faria?

4) [0,3v] Como é que, na execução, o *application server* sabe que deve executar um handler?

5) [0,4v] A função Integer.toString usada no programa relaciona-se com uma das vantagens mais relevantes do SOAP e genericamente dos Web Services. Qual? Justifique claramente.

6) O header deve ter servido no projecto para transmitir um certificado X509 entre o serviço PagaAmigo e o Serviço LargaCaixa, analise as seguintes frases indica **se concorda ou discorda e justifique.**
   a. [0,4v] "Os cerificados são enviados no header porque como têm valores cifrados e não podem ser enviados como parâmetros das funções"

   b. [0,4v] "Os certificados poderiam ser parâmetros das funções descritos no WSDL mas as funções ficavam menos genéricas"

Grupo IV [2,6v]

Considere o endereço de email *leic-alameda-sod@disciplinas.ist.utl.pt*.

1) [0,5v] Como classifica o nome acima quanto à pureza, âmbito e homogeneidade? Justifique.

2) [0,4v] O nome acima é hierárquico, sendo gerido por diferentes autoridades. Enumere 3 dessas autoridades, indicando qual a porção do nome que cada entidade gere.

3) [0,5v] Um aluno da cadeira envia uma mensagem de correio electrónico para o endereço acima. Para que a mensagem possa ser entregue à caixa de correio associada ao endereço acima, ocorrem um ou mais passos de resolução de nome. Indique-os abaixo (não precisa preencher todas as linhas da tabela):

Traduz deste nome:	Para este nome:

4) Pelo menos um dos passos acima usa o DNS. Justifique as seguintes afirmações ilustrando com aspectos relacionados com a arquitectura do DNS.

a. [0,4v] "Quando o serviço de correio electrónico foi criado, havia poucas dezenas de servidores de correio electrónico no mundo. Hoje existem milhões de contas, espalhadas por milhares de servidores. No entanto, o serviço continua hoje a exibir bom desempenho."

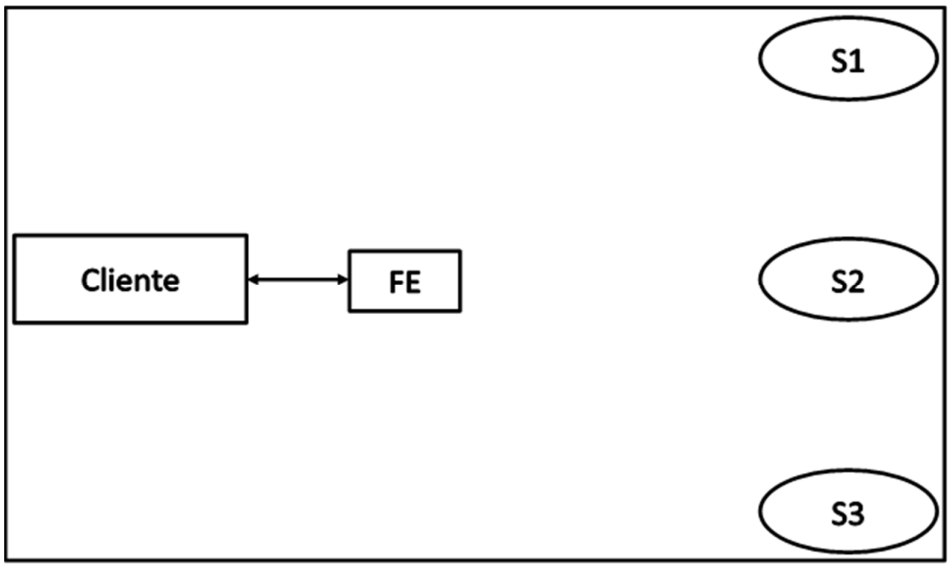
b. [0,4v] "O servidor DNS primário do domínio ist.utl.pt esteve indisponível durante a noite de ontem. No entanto, não há registos de falhas na entrega de emails para contas do mesmo domínio."

c. [0,4v] "O servidor de email do domínio disciplinas.ist.utl.pt mudou de IP. Durante as primeiras horas após a mudança não houve mensagens entregues a este servidor. No entanto, a entrega normal de mensagens foi automaticamente retomada após esse período."

Grupo V [5,3v]

1) Considere um sistema replicado em que um cliente (C) interactua através de um Front-End (FE) com um conjunto de três servidores (S1, S2, S3). As operações sobre os servidores são apenas de leitura (R) e escrita (W). O protocolo usado é o de p*rimary-backup.* Assuma que os servidores são de **falha silenciosa**, que o sistema é síncrono, que a rede não tem falhas permanentes e garante uma ordem FIFO das mensagens.

a) [0,5v] Considere que o cliente efectua uma escrita na variável A (W(A,10)) e depois lê o valor da mesma variável R(A). Complete o diagrama indicando as operações que são realizadas, descrevendo-as através de setas com a legenda das operações (W(A, 10), R(A)). Escreva as legendas que achar necessárias, indique todas as mensagens trocadas entre cliente e os servidores, e entre estes.

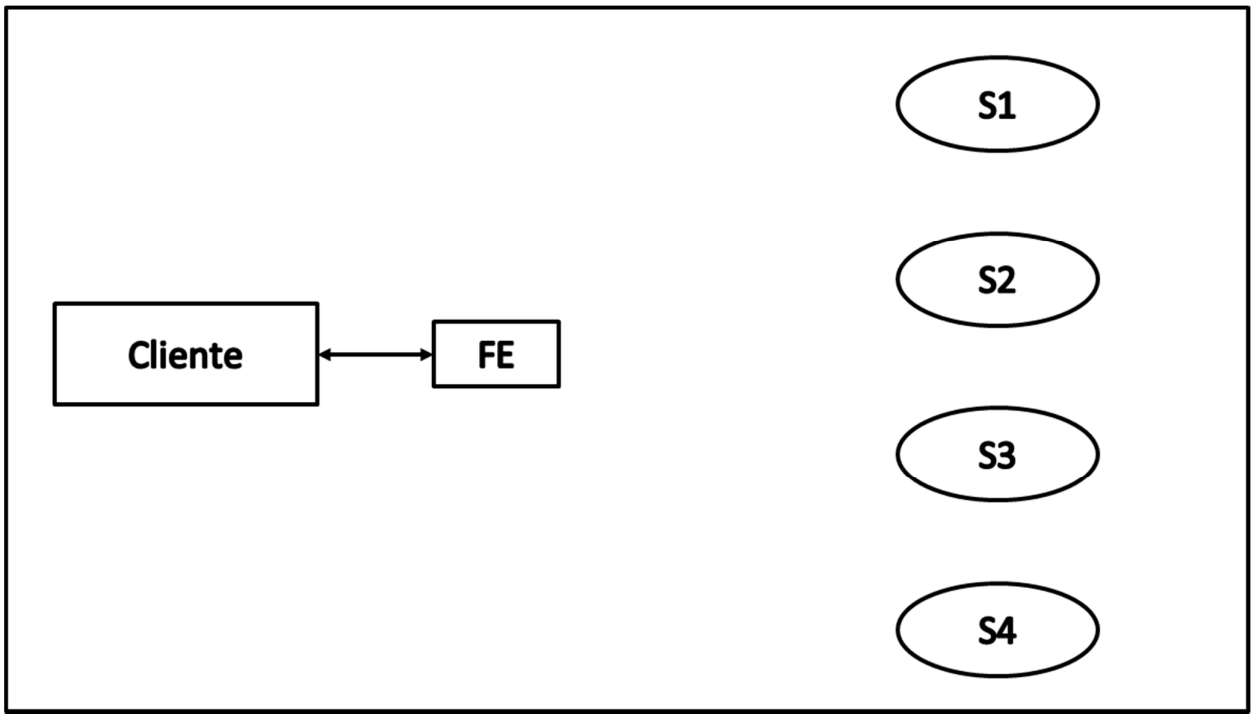


b) [0,4v] Explique quantas falhas de servidores pode tolerar este sistema. Justifique.

2) Considere agora que a **rede é assíncrona** e que utiliza um protocolo de quórum de maioria.

a) [0,4v] O que significa o pressuposto que o sistema é assíncrono e o que muda em relação ao sistema da pergunta 1?

b) [0,5v] Pressupondo que executa a operação (W(A, 10), R(A)). Complete o diagrama com todas as interacções entre o cliente e os servidores, admitindo que S2 não recebe a mensagem de write e S3 falha depois aquando da execução de R(A).



c) [0,4v] Quantas falhas silenciosas dos servidores tolera este sistema? Justifique.

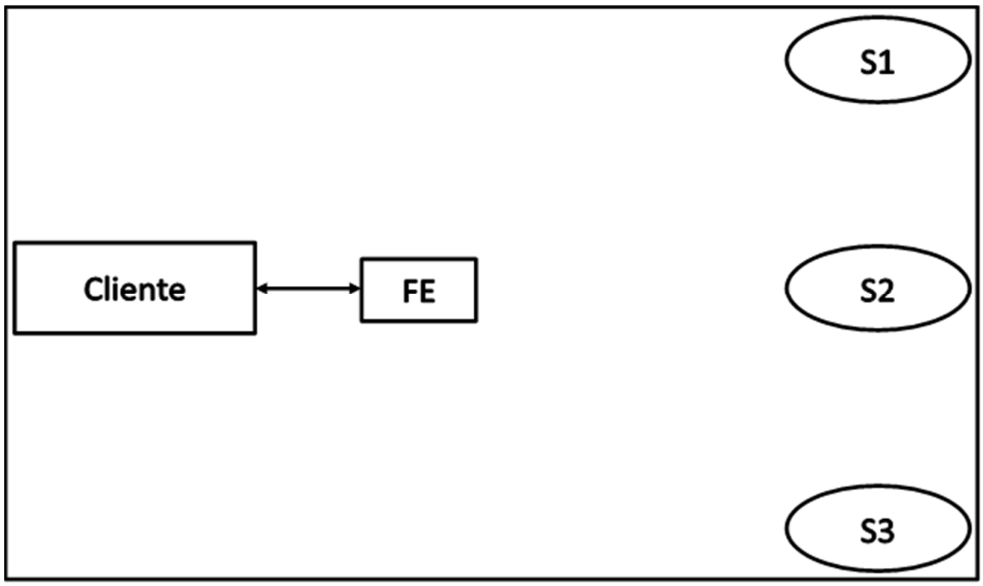
d) Considere que o servidor S1 está ligado a um *backbone* de rede com elevada banda passante, e os restantes têm ligações idênticas e mais lentas à rede (para exemplo a ligação é 3 vezes mais rápida). Como poderia optimizar o funcionamento do sistema para acelerar as estruturas, passando a usar um **protocolo de quóruns com pesos variáveis**?

i) [0,5v] Explique como definiria os pesos de cada servidor e os valores RT e WT

ii) [0,4v] Justifique com um exemplo qual a melhoria que esta proposta apresenta em relação ao quórum de maioria.

3) Mantendo a configuração da alínea 1), mas pressupondo outra aplicação em que o cliente quer executar sobre os 3 servidores operações de leitura e escrita sobre **dados diferentes** e garantindo transacções atómicas distribuídas, usando 2-phase commit (2PC).

a) [0,4v] Adicione ao diagrama seguinte um componente indispensável para poder executar as transacções distribuídas.



b) [0,4v] Represente no diagrama acima, através de setas, todas as interacções que desencadeia a execução da operação *openTransaction.*

c) [0,4v] Represente no diagrama acima, através de setas, todas as interacções que desencadeia a execução da transação distribuída composta pela escrita da variável X no servidor S1 e pela leitura da variável Y no servidor S2. Considere só a representação até esse momento; a evolução subsequente e em particular o 2PC não fazem parte desta representação

d) [0,5v] Depois desta operação o servidor S1 falha.
   i) Como será detectado?

   ii) O que irá suceder à transacção global nesse caso?

e) [0,5v] Considere agora uma execução alternativa em que a transacção decorre normalmente até ao cliente fazer closeTransaction e o servidor S1 falha depois de ter respondido ao *canCommmit* (*prepare)* com *yes* (*ready)*. O que irá suceder à transacção global? Justifique.

Grupo VI [3,7v]

1) Considere dois interlocutores, A e B.
Assuma que, após distribuição através de um canal seguro, A conhece a sua chave privada, KsA, e a chave pública de B, KpB; e vice-versa.
Por vezes, A e B pretendem trocar múltiplas mensagens entre si e para tal seguem o seguinte protocolo:

- O nó (A ou B) que tomar a iniciativa primeiro, gera uma chave simétrica secreta, K.
- Se for o nó A que gerou a chave K, A envia {K}KpB a B; B decifra com KsB e obtém K. (Procedimento inverso para o caso em que B toma primeiro a iniciativa.)
- Sempre que A queira enviar mensagem M a B, ou vice-versa, é enviado {M}K pela rede.

Nas alíneas seguintes assuma que o atacante não consegue quebrar as chaves secretas (KsA, KsB e K).

a) [0,5v] Quando A quer enviar M a B, A poderia optar pela alternativa de enviar {M}KpB. Que desvantagens encontra nesta solução, comparativamente à solução descrita acima?

b) O protocolo proposto na alínea 1) é vulnerável a ataques de repetição (*replay*).

i) [0,6v] Descreva de que forma um atacante T pode concretizar esse ataque. Ilustre com um exemplo em que B é um servidor de contas bancárias e permite aos clientes debitarem/creditarem as suas contas.

ii) [0,7v] Proponha uma correcção ao protocolo que previna este ataque.

2) Para cada mensagem M recebida por A ou B, o receptor pretende ter forma de garantir confidencialidade, integridade e não repúdio da mensagem.

a) [0,6v] Apresente detalhadamente uma solução que garanta esses 3 requisitos.

b) [0,6v] Apresente agora uma solução mais eficiente que não ofereça a garantia de não repúdio.

3) [0,7v] Uma forma de A ter tomado conhecimento da chave pública de B foi através de um certificado digital de chave pública. A obteve o certificado da chave pública de B a partir de um site desconhecido na Web. Pode A confiar na chave que vem no certificado? Se sim, que passos deve A efectuar para confirmar que a chave é realmente a chave pública actual de B? Se não, justifique.