Número: Nome:

LEIC/LERC – 2009/10
2º Exame de Sistemas Distribuídos

9 de Julho de 2010
Responda no enunciado, apenas no espaço fornecido. Identifique todas as folhas.
Duração: 2h30m

Grupo I [1,9 v]

1) Considere a seguinte IDL do Sun RPC de um serviço de votação em sugestões (versão modificada e muito simplificada do sistema FeaRS do IST).
A interface deste serviço fornece apenas um método remoto. O método permite ao cliente votar numa sugestão indicando a sugestão e um código de voto. O servidor retorna ao cliente os votos totais dessa mesma sugestão. A implementação do método no servidor é idempotente.

```
enum vote_error {
   CALL_OK = 0,          /* No error */
   CALL_ID_NOT_FOUND = 1   /* Suggestion ID not found */
};

struct vote_args {
    long ID;
    long vote_code;
};

struct vote_result {
    vote_error error;
    double value;
};

program VOTE_PROG {
    version VOTE_VERS {
        vote_result POSTVOTE(vote_args);
    };
} = 100400;
```

a) [0,3 v] Quais são os parâmetros de entrada e de saída da função POSTVOTE? Escreva o protótipo da função em C equivalente à função do RPC explicitando todos os parâmetro da função

b) [0,4 v] Com base nestes parâmetros ilustre com um exemplo o problema da heterogeneidade numa arquitectura distribuída.

c) [0,4 v] Considere que este serviço de votação está disponibilizado em vários servidores. Pretende-se que a aplicação cliente se ligue a cinco destes servidores, e que seleccione alternadamente a ligação a utilizar para cada pedido de invocação remota.
Será possível o programador da aplicação cliente cumprir este requisito? Justifique.

2) Em relação ao IDL anterior
   a) [0,4 v] Um voto deve ser registado na base de dados do servidor sempre que o cliente efectuar uma votação. Responda, justificando, se uma semântica de invocação "Pelo-menos-uma-vez" seria aceitável para este serviço, ou seria recomendado uma semântica de invocação "No-máximo-uma- vez"?

   b) [0,4 v] (Resposta errada desconta ¼ da pergunta) Na invocação remota de POSTVOTE, um RPC que ofereça a semântica de invocação "Talvez" é capaz de oferecer uma semântica equivalente à semântica local de chamada de procedimentos mesmo quando as seguintes faltas ocorram (indique a resposta mais forte):
      i) Falha do servidor, duplicação de mensagens, perda de mensagens.
      ii) Duplicação de mensagens, perda de mensagens.
      iii) Perda de mensagens.
      iv) Nenhuma das anteriores.

Grupo II [3,1 v]

1. A figura seguinte indica um ficheiro de uma implementação de WebServices em que se define-se a classe Java, anota-se esta para gerar um Web Service, e finalmente o WSDL e os ties são gerados usando a ferramenta wsgenerate.

```
@WebService(name = "VotePortType", targetNamespace = "urn:exemploExame2SD.com:vote",
wsdlLocation = "file:///D:/IST/SD/2010/ex2/ExemploExame2SDWS/build/config/jax-ws-server/Vote.wsdl")
@SOAPBinding(style = Style.RPC)
public interface VotePortType {
    /**
     * @param voteCode
     * @param id
     * @return
     *     returns vote.ws.ties.VoteResult
     */
    @WebMethod
    @WebResult(name = "VoteResult", targetNamespace = "urn:exemploExame2SD.com:vote", partName
= "VoteResult")
    public VoteResult postVote(
        @WebParam(name = "id", partName = "id")
        long id,
        @WebParam(name = "voteCode", partName = "voteCode")
        long voteNumber);
}
```

a) [0,4 v] A abordagem indicada é chamada contract-first ou implementation-first? Justifique, descrevendo a abordagem de implementação ***alternativa*** à indicada.

b) Considere a implementação em que se constrói primeiro o WSDL.

i) [0,4 v] Indique, justificando, se identifica alguma razão para a definição do portType no WSDL ser separada da definição das mensagens e da definição dos bindings

ii) [0,6 v] Considere que se pretende duas concretizações deste portType: sobre transporte por HTTP e por SMTP. Isso seria possível? Se não, justifique. Se sim, indique como.

c) [0,5 v] Considere que existe a possibilidade de a invocação do método remoto postVote falhar porque o utilizador já votou, e que se pretende ter uma forma de o assinalar ao cliente. Que alterações teria que efectuar no WSDL?

d) [0,4 v] Descreva as duas principais diferenças que levaram à forte implantação dos Web Services nos sistemas actuais, em contraste com os RPCs SUN/DCE.

2. O seguinte excerto é retirado do contrato WSDL do serviço:

```
<definitions name="Vote"
  xmlns:tns="urn:exemploExame2SD.com:vote"
  xmlns="http://schemas.xmlsoap.org/wsdl/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
<types>
  <xsd:schema elementFormDefault="qualified"
    targetNamespace="urn:exemploExame2SD.com:vote">
    ...
      <xsd:complexType name="VoteResult">
        <xsd:sequence>
          <xsd:element name="voteError" type="tns:VoteError"/>
          <xsd:element name="value" type="xsd:double"/>
        </xsd:sequence>
      </xsd:complexType>
    ...
```

a) [0,4 v] Concretamente tns: está associado a um uri do documento wsdl. Explique porquê a associação a este uri.

b) [0,4 v] Este uri poderá ser usado para obter o wsdl por parte dos clientes? Justifique.

Grupo III [3,1 v]

```
public interface Shape extends Remote {
   int getVersion() throws RemoteException;
// getALLState obtem os valores de todas as propriedades do objecto da //class GraphicalObject
   GraphicalObject getAllState() throws RemoteException;
}

public interface ShapeList extends Remote {
        //GraphicalObject and Vector are classes whose interface //extends Serializable but not Remote
        Shape newShape(GraphicalObject g) throws RemoteException;
        Vector allShapes()throws RemoteException;
        int getVersion() throws RemoteException;
}

public class ShapeListServant extends UnicastRemoteObject implements ShapeList{
   private Vector theList;
   private int version;

   public ShapeListServant()throws RemoteException{
      theList = new Vector();
      version = 0;
   }
    public Shape newShape(GraphicalObject g) throws
   RemoteException{
   version++;
            Shape s = new ShapeServant( g, version);
      theList.addElement(s);
      return s;
    }
    public Vector allShapes()throws RemoteException{
      return theList;
   }
    public int getVersion() throws RemoteException{
      return version;
   }
}
```

1. Considere as duas interfaces definidas acima e o código da classe servant que implementa a interface ShapeList (extractos do exemplo do livro da cadeira). Considere ainda a seguinte sucessão de eventos, que envolvem um Servidor S1 e três clientes C1, C2,C3.

    1. O servidor S1 inicializa-se e regista-se com o nome MyShapeList.
    2. O cliente C1 obtém do servidor de nomes uma referência Sl para o objecto MyShapeList..
    3. O cliente C1 cria um objecto G1 do tipo GraphicalObject e invoca shape1 = Sl.newShape (G1).
    4. O cliente C2 obtém do servidor de nomes uma referência Sl para o objecto MyShapeList..
    5. O cliente C2 cria um objecto G2 do tipo GraphicalObject e invoca shape2=Sl.newShape (G2).
    6. O cliente C2 invoca GX= shape2.getAllState ().
    7. O cliente C3 obtém do servidor de nomes uma referência Sl para o objecto MyShapeList.
    8. O cliente C3 invoca version =Sl.getVersion.
    9. O cliente C3 invoca MyVect = Sl.allShapes.

a) [0,3 v] No final da etapa 6, quantas referências remotas tem o cliente C2? Justifique.

b) [0,2 v] Qual o valor devolvido pelo método *getVersion* na etapa 8? Justifique.

c) [0,3 v] Os métodos remotos devolvem objectos por valor ou por referência. O que sucede na invocação da etapa 8? Porquê?

d) [0,5 v] No final da etapa 9, quantos proxies terão sido criados no espaço de endereçamento do cliente C3?

e) [0,6 v] O cliente C3 poderia criar uma nova instância de Shape a partir de G2 criado pelo cliente C2? Explique como, fazendo um pequeno programa.

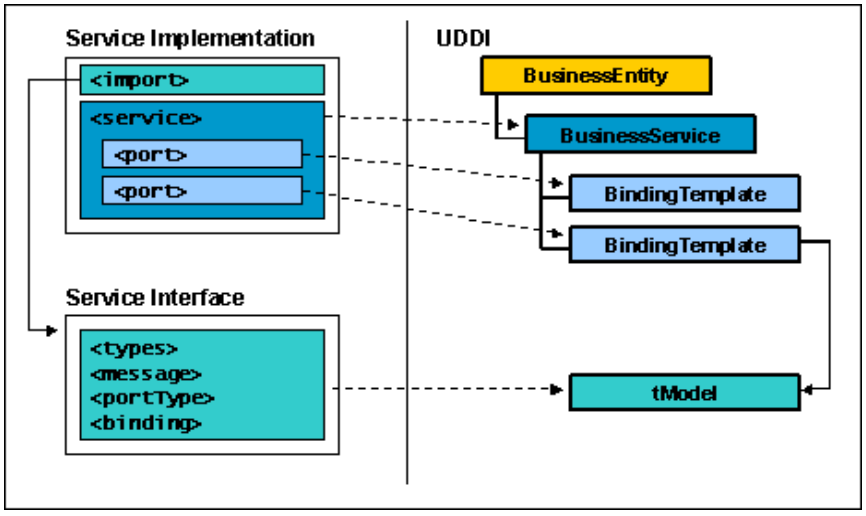
2. Admita que o garbage collector utiliza leases.
   a) [0,6 v] Desde a etapa 1 ao fim da etapa 8, Preencha a tabela do servidor, indicando quais os objectos e para que cliente existe uma lease.

Objecto	Cliente

b) [0,3 v] Que alteração, se alguma, introduz a etapa 8 no estado das leases? Justifique.

c) [0,3 v] Considere que os clientes C1 e C3 terminam e o restante cliente se mantém activo O que implica a terminação dos clientes relativamente ao protocolo de gestão de memória no servidor? Justifique

Grupo IV [1,9 v]



1) A figura 1 descreve os tipos de dados de um registo UDDI e a sua correspondência com um documento WSDL.

a) [0,3 v] Justifique com base no esquema a afirmação "o UDDI é um serviço de directório e não apenas um serviço de nomes"

b) [0,3 v] Deve ter utilizado o UDDI no seu projecto. Explique qual o principal objectivo dessa utilização.

2) Considere o cabeçalho da definição de um serviço escrito na IDL do Sun-RPC e do DCE-RPC respectivamente. Em ambas existe um identificador do serviço.

```
program BANCOPROG {
  version BANCOVERS {
    criarRet CRIAR(criarIn) = 1;
    …….
  } = 1;
} = 0x20000005;
```

IDL – SUN- RPC

```
[
uuid(00918A0C-4D50-1C17-9BB3-92C1040B0000),
version(1.0)
]
interface banco
{
…..
resultado criar([in] handle_t     h,
                [in] long         valor,
                [in, string] char nome[],
                [in, string] char morada[],
                [out] long        *numero);
……..
```

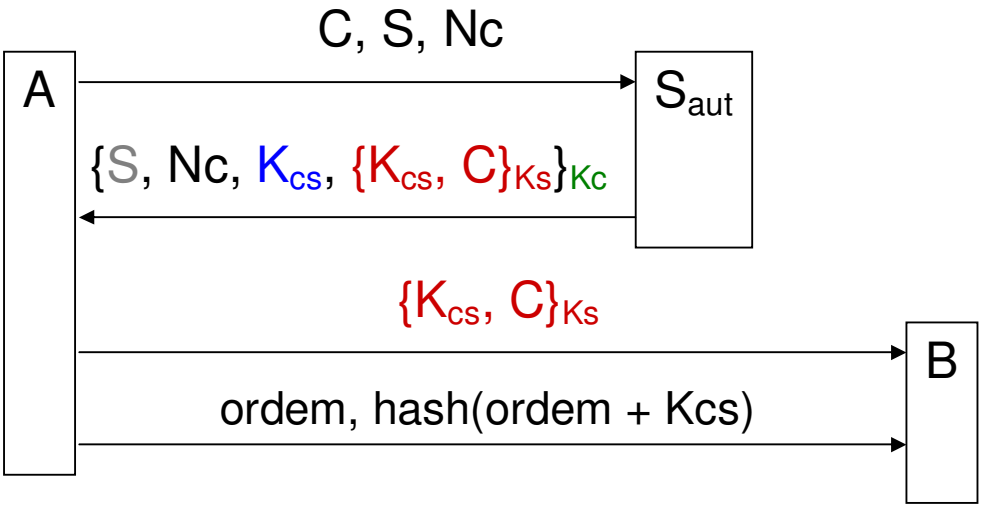
IDL – DCE-RPC

a) [0,3 v] Classifique ambos os nomes quanto ao âmbito - global ou local ao servidor?

b) [0,5 v] Como afecta a propriedade anterior o algoritmo de criação dos nomes? Justifique.

c) [0,5 v] Um sistema correcto de nomes não pode ter colisões de nomes porque violaria o princípio da unicidade referencial. Como são evitadas as colisões nos dois casos?

Grupo V [5,1 v]



1. A Alice (A) é cliente de um banco, e interage com o seu gestor de conta, Bob (B), remotamente, enviando ordens através de uma rede insegura.
   Ambos utilizam a variante simplificada do protocolo Needham-Schroeder apresentada acima para interagir. Cada vez que A quer enviar ordens a B, cria uma sessão a partir de um servidor de autenticação do banco (Saut) e durante essa sessão envia ordens a B.
   Assuma que as chaves envolvidas (Kc, Ks, Kcs) são **practicamente impossíveis de quebrar** e que A, B e Saut **não têm relógios sincronizados**.

a. [0,6v] Indique quem sabe qual chave, assinalando na seguinte tabela (com X):

	A	B	Saut
Kc			
Ks			
Kcs			

b. Em cada mensagem de ordem, vai anexado *hash(ordem+Kcs)*.
   i. [0,5v] Que propriedades visa garantir este anexo da mensagem?

   ii. [0,6v] Descreva um exemplo de ataque que seria possível caso tal anexo não fosse enviado (e que não é possível se o anexo for enviado).

c. [0,8v] É possível ao atacante escutar uma mensagem enviada por A com uma ordem e repeti-la na mesma sessão (replay attack)? Se sim, indique o que alteraria no protocolo para evitar esse ataque. Se não, justifique.

d. Mesmo assumindo que não é possível ao atacante repetir uma mensagem durante a sessão durante a qual a mensagem foi enviada por A, é ainda possível ao atacante repetir sessões antigas (i.e. repetir todas as mensagens de uma sessão antiga, incluindo as mensagens de estabelecimento da sessão) levando B a re-executar ordens antigas sem o saber.

   i. [0,5v] Indique como o protocolo Needham-Schoeder previne esse ataque.

   ii. [0,5v] Indique como o Kerberos previne esse ataque.

2. Considere que as notas finais de uma cadeira eram enviadas à secretaria da universidade e aos alunos da cadeira por email, através da Internet. Para garantir a autenticidade, integridade e não repúdio das notas enviadas, o responsável da cadeira **assina digitalmente cada par <nº aluno, nota>**. Os receptores, que conhecem a chave pública do responsável da cadeira (Kpresp), podem então validar cada par <nº aluno, nota> recebido.

   a. [0,5v] Sendo M=<nº aluno, nota>, indique o que é que o responsável da cadeira envia, de facto, pela rede quando quer anunciar a nota de um aluno.

   b. Para que os receptores (secretaria e alunos) possam validar as mensagens recebidas do responsável da cadeira, precisam conhecer a sua chave pública.

      i. [0,6v] Assuma que essa chave pública é previamente enviada num email contendo apenas *Kpresp* (em claro e sem qualquer informação adicional), o que não é seguro. Ilustre porquê, dando um exemplo de um ataque em que o aluno nº 12345 consegue convencer a secretaria de que passou com 20 valores.

ii. [0,5v] Como modificaria o método anterior para passar a ser seguro (apesar de executado sobre um canal inseguro)?

Grupo VI [2,5 v]

1. Considere um sistema que usa replicação passiva, constituído por dois servidores (a cada momento, um é primário, outro é secundário). Os clientes deste sistema invocam procedimentos remotos e esperando pela respectiva resposta. No caso de expirar um temporizador no cliente antes da resposta chegar, o cliente re-envia o pedido para o servidor que é primário nesse momento.

   Assuma que:
   - Cada servidor tem uma thread única que trata um pedido remoto de cada vez, por ordem de chegada, demorando tservice=10s por cada pedido
   - O período de envio de provas de vida (P) é P=30s
   - A comunicação é fiável,e o tempo de tramsnissão máximo é limitado, garantindo que qualquer mensagem enviada é entregue no máximo ao fim de tmax=2s
   - Os servidores falham silenciosamente;
   - Um servidor que se torne primário demora, em média, 1h até falhar silenciosamente
   - Em qualquer momento, pelo menos um dos servidores está correcto

   a. [0,5v] Na **ausência de falhas** e no caso em que **apenas um cliente está a usar o sistema**, qual o tempo máximo de execução do procedimento remoto (tempo desde que cliente enviou pedido até receber a resposta) ? Justifique.

   b. [0,6v] Continuando a assumir o cenário de um cliente apenas mas em que **um dos servidores pode falhar**, qual o tempo de de execução do procedimento remoto máximo? Justifique.

c. [0,8v] No geral, pode dizer-se que este sistema é síncrono? Se sim, justifique. Se não, que restrição(ões) não indicadas no enunciado seria necessário referir para considerar o sistema síncrono?

d. [0,6v] Se o meio físico que liga primário e secundário for alterado e passar a ter um **tempo de transmissão ilimitado**, o sistema replicado funcionará correctamente? Se sim, justifique. Se não, descreva uma execução que ilustre uma situação incorrecta.

Grupo VII [2,8v]

Considere uma hipotética variante descentralizada do 2-Phase Commit:
- Os participantes executam o protocolo de confirmação atómico comunicandodirectamente entre eles, em vez de indirectamente através do coordenador.
- Na primeira fase, o coordenador envia a mensagem canCommit? A todos os participantes.
- Na segunda fase, cada participante envia o seu voto (sim/não) **a todos os outros participantes** (assuma que a lista de participantes é previamente conhecida por todos).
- Cada participante espera pelos votos dos restantes participantes. Caso **todos sejam *sim***, confirma a transacção local; mal receba o primeiro voto *não*, aborta a transacção local.
- Tendo tomado a decisão localmente, cada participante envia uma mensagem *ack* a todos os participantes. Assim que cada participante receba *ack* de todos os participantes, eliminam o estado local sobre a transacção.

Nas restantes alíneas, considere uma transacção distribuída envolvendo **3 participantes (X, Y, Z)**, executada num **sistema assíncrono em que as mensagens podem atrasar-se arbitrariamente**.

1. No caso de não haver falhas de nenhum dos participantes e de todos votarem sim:
   a. [0,6v] Quantas mensagens troca o 2PC centralizado? Enumere-as num diagrama de mensagens.

Coord	X	Y	Z

b. [0,6v] Quantas mensagens troca o 2PC descentralizado? Enumere-as num diagrama de mensagens.

Coord	X	Y	Z

3.a) [0,6v] No caso do 2PC-centralizado, se o coordenador não receber os votos de todos os participantes ao fim de um tempo razoável, como reage?

i. Decide abortar a transacção, enviando essa decisão a todos os participantes.
ii. Decide confirmar a transacção, enviando essa decisão a todos os participantes.
iii. Continua a esperar pelos votos em falta.

3.b) [0,6 v] No caso do 2PC-descentralizado, é cada participante que, unilateralmente, recebe os votos suficientes e toma a decisão. Das três reacções mencionadas na alínea anterior, indique qual(is) o participante do 2PC-descentralizado pode tomar correctamente.
Para aquelas que considerar incorrectas, justifique apresentando uma execução em que tal reacção leve a um comportamento errado do 2PC; para as que considerar correctas, escreva simplesmente "correcta".

i. Decide abortar a transacção, enviando essa decisão a todos os participantes.

Coord	X	Y	Z

ii. Decide confirmar a transacção, enviando essa decisão a todos os participantes.

Coord	X	Y	Z

iii. Continua a esperar pelos votos em falta.

Coord	X	Y	Z