Número: Nome:

LEIC/LERC – 2011/12

Primeiro Exame de Sistemas Distribuídos

5 de Junho de 2012, Duração: 2h30m

Responda no enunciado, apenas no espaço fornecido. Identifique todas as folhas.

Grupo I RPC [2,5v]

1. Em Unix, a rotina *clnt_create* permite a programas escritos em C criar ligações com servidores remotos (por exemplo, através do SUN RPC ou outros RPCs). A descrição das man pages é a seguinte:

CLIENT *clnt_create(char *host, unsigned long prog, unsigned long vers, char *proto);
Generic client creation routine. host identifies the name of the remote host where the server is located. proto indicates which kind of transport protocol to use. The currently supported values for this field are "udp" and "tcp". Default timeouts are set, but can be modified using clnt_control().
Warning: Using UDP has its shortcomings. Since UDP-based RPC messages can only hold up to 8 Kbytes of encoded data, this transport cannot be used for procedures that take large arguments or return huge results.

a) [0,4v] Esta função retorna uma estrutura de dados que contém (marque com uma cruz todas as afirmações correctas):

	Identificação do Program (interface) e sua versão
	O endereço IP e porto do socket do servidor os quais identificam o canal de comunicação para interactuar com o servidor
	Stub para comunicação com o servidor remoto

b) [0,3v] Assuma que se pretende enviar uma mensagem M de tamanho 20Kbytes usando apenas a função call do RPC. Deveria previamente invocar *clnt_create* com a variável *proto* instanciada a que valor (selecione de entre as 3 opções e justifique)?

UDP	TCP	HTTP	Justificação:

c) [0,4v] Considere:

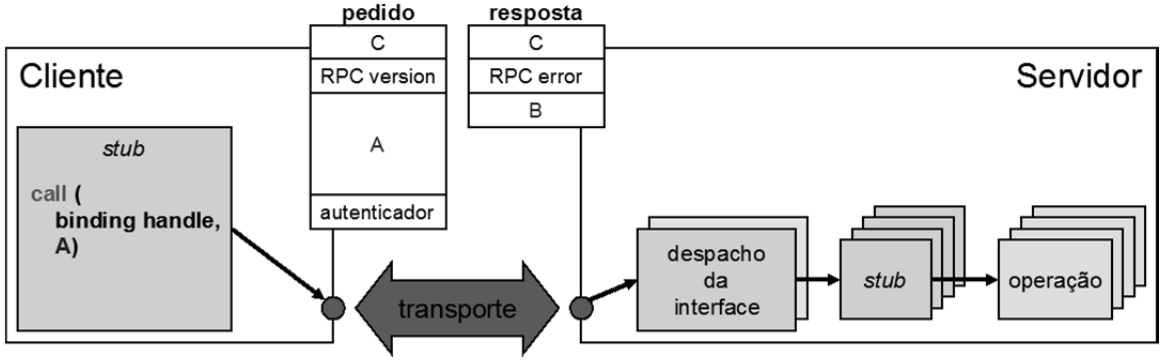
```
CLIENT *cl;
cl=clnt_create(...);
```

e que o sistema de RPC lhe permitia 2 alternativas para uma invocação:

I. `shop_item item = getitem(10110, cl);`
II. `shop_item Item = getItem(10110);`

Compare as vantagens e desvantagens de ambas as alternativas.

2. A mensagem enviada com o pedido e a mensagem retornada com a resposta podem ser vistas como tipos estruturados, contendo múltiplos campos.
   a) [0,4v] Indique na tabela em baixo os campos em falta que a mensagem de pedido e a mensagem de retorno incluem.



A	
B	
C	

   b) [0,3v] Se se pretendesse cifrar os parâmetros enviados no pedido, a cifra deveria acontecer depois da conversão dos parâmetros. Porquê?

3. O IDL do DCE RPC permite que programador associe ao procedimento remoto o atributo *idempotent*, que indica que a implementação do procedimento é idempotente.
   a) [0,3v] O que é um procedimento idempotente?

   b) [0,4v] Indique (assinalando com uma cruz) quais das seguintes funções são idempotentes

	Função Copy, a qual copia um ficheiro para uma directoria diferente. Se ficheiro com mesmo nome já existir, é substituído.
	Função Append, a qual acrescenta um conjunto de dados no final do ficheiro
	Função ReadAfterInc, a qual retorna a leitura de um valor de timestamp após incrementar este.
	Função SetValue(int t), a qual instancia uma variável value com o valor de t.
	Função DecValue(int t), a qual decrementa uma variável value com o valor de t.

Número:

Grupo II [2,5 v]

Considere as seguintes declarações de interfaces e classes em Java:

```
public interface SoccerManager extends Remote {...}

public class SoccerManagerServant extends UnicastRemoteObject implements SoccerManager{
     private ManagerGroup father=null;
     private int id;
     public SoccerManagerServant(int id, IManagerGroup mg) throws RemoteException{
        this.id = id; father = mg;}
     public ManagerGroup getManagerGroup() throws RemoteException{return father;}
     public void setId(int id) throws RemoteException {this.id=id;}
     public int getId() throws RemoteException {return this.id;}
}

public interface IManagerGroup extends Serializable{...}

public class ManagerGroup implements IManagerGroup{
       private Vector theList; //contains the list of SoccerManager private
       private int groupId;
       public ManagerGroup(){groupId=0; theList=null;}
       public SoccerManager newSoccerManager(){
             SoccerManager s = new SoccerManagerServant(groupId, this);
             theList.addElement(s);
             groupId++;
             return s;
       }
       public Vector allSoccerManagers(){return theList;}
       public int getGroupId(){return groupId;}
}
```

E a execução das seguintes instruções de código em duas máquinas A e B (considere que os números representam a ordem com que são executadas):

	A	B
1		ManagerGroup mgB=new ManagerGroup();
2		SoccerManager aSM=mgB.newSoccerManager());
3		Naming.bind("SoccerManager", aSM);
4	SoccerManager sSM= (SoccerManager) Naming.lookup("//hostB/SoccerManager");	
5	sSM.setId(sSM.getId()+10);	
6	IManagerGroup mg = sSM.getManagerGroup();	
7		int id_1=aSM.getId();
8	SoccerManager bSM=mg.newSoccerManager();	
9	Vector sList = mg.allSoccerManagers();	
10	int id_0=bSM.getId();	
11	bSM. setId(id_0+1);	
12	Naming.bind("NewSoccerManager", bSM);	
13		int id_2=aSM.getId();
14		SoccerManager cSM=(SoccerManager) Naming.lookup("//hostA/NewSoccerManager");
15		unt id_3=bSM.getId();

1) Considere as linhas 4 e 8:

   a) [0,3v] Na linha 4, o SoccerManager aSM é retornado na invocação a Naming.lookup por:

Valor	Referência

   b) [0,4v] Que objetos são criados na máquina A na linha 4 e na linha 8? Justifique.

2) [0,4v] Considere as variáveis (id_0, id_1, id_2 ,id_3) constantes do programa . Indique o respetivo valor no final da execução:

ID	id_0	id_1	id_2	id_3
Valor				

3) [0,4v] Acha possível o registo da linha 12 e o lookup da linha 14, ou são bugs do código? Justifique sucintamente.

4) [0,5 v] Descreva o estado dos contadores de referência do Garbage Collector de B no passo 15.

5) [0,5v] Considere a instrução na linha 6: o compilador na máquina A precisa de ter acesso à classe ManagerGroup para compilar a aplicação?

SIM	NÃO

Se respondeu SIM, justifique. Se respondeu NÃO, então diga como a máquina A obtém o ficheiro da classe ManagerGroup.

Grupo III [2,5 v]

Considere a seguinte assinatura de um serviço que recebe linhas da fatura descritas em XML, os métodos para efetuar a assinatura e produz uma fatura assinada. As linhas constituintes da fatura `List` são descritas por um XML schema e `SignedInfo` também é descrito por um XML Schema.

```
public abstract SignedInfo newSignedInfo(CanonicalizationMethod cm, SignatureMethod sm, List references)
```

1) [0,7v] Explique a como a partir desta assinatura procede para desenvolver um Web service usando:
   a) Contract first

   b) Implementation first

Número:

2) [0,3v] Indique uma **desvantagem** clara da primeira abordagem

3) [0,3v] Indique uma **desvantagem** clara da segunda abordagem

4) [1,2v] Considere a seguinte mensagem SOAP

```
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <m:GetEndorsingBoarder xmlns:m="http://namespaces.snowboard-info.com">
      <manufacturer>K2</manufacturer>
      <model>Fatbob</model>
    </m:GetEndorsingBoarder>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

a) A mensagem tem dois parâmetros cuja definição não é patente apenas analisando-a. Em que secção ou secções do WSDL poderia encontrar informação sobre a definição da estrutura de dados

b) Apesar de não se saber o tipo dos parâmetros qualquer que este seja a heterogeneidade vai ser tratada. Explique como.

c) A mensagem GetEndorsingBoarder pode ser invocado com o protocolo de transporte HTTP e SMTP? Se respondeu NÃO, justifique. Se respondeu SIM, diga em que secção ou secções do WSDL deveria especificar esta característica?

Grupo IV [2,5 v]

Considere que implementa um servidor (ServX) que disponibiliza dois serviços `AtualizarSaldo` e `LerSaldo` e pretende que este serviço cumpra os seguintes requisitos:

1) [0,7v] Deve tolerar uma falta de paragem, o sistema é síncrono, o cliente deve ser o mais simples possível.
   a) Faça um diagrama da arquitetura

a)

b) Justifique.

2) [0,3v] Explique como funciona `Lersaldo` com 1 falta de paragem.

3) [1,1v] Deve tolerar uma falta de paragem, o sistema é assíncrono, pretendendo-se que o cliente consiga concluir a invocação o mais rápido possível respeitando o modelo de faltas.

a) Faça um diagrama da arquitetura.

b) Explique o protocolo para LerSaldo.

c) Explique o protocolo para ActualizarSaldo.

4) [0,4v] A arquitetura que definiu na pergunta 3 toleraria uma falta bizantina?

Sim		Não	

Se resposta for Sim justifique,se for Não o que modificaria

Grupo V [3,7 v]

1) Uma empresa de software foi encarregue pela Troika de desenhar um website para Troika.pt. Um dos requisitos do cliente é que os utilizadores deverão utilizar as suas credenciais (username, password) para fazerem login no website remoto. Não será necessário autenticar o servidor.

a) [0,3v] A empresa propõe usar um protocolo simples de autenticação, usando um desafio que consiste na criação da chave Kcs, a partir um hash da password do cliente, para cifrar um desafio (um nounce) enviado pelo servidor:

1) C ->S: "Iniciar Sessão"
2) S ->C: D
3) C ->S: $\{D\}_{K_{cs}}$

A Troika rejeita. Indique sucintamente quais as limitações desta solução proposta pela empresa.

Número:

b) [0,4v] A empresa propõe agora usar o protocolo de Needham-Schroeder, usando chaves secretas construídas a partir de uma função de hash da password do cliente. A password é distribuída previamente usando mais do que um meio de comunicação (e.g. metade da password é enviada por telefone, e a outra metade por carta selada como os PIN de multibanco). A Troika rejeita. Indique uma razão que justifique a decisão, descrevendo como essa vulnerabilidade poderia ser explorada por um atacante.

c) [0,4v] A empresa propõe finalmente usar o protocolo de Kerberos V5. A Troika ACEITA. No entanto, pede à empresa uma explicação da razão da utilização de dois servidores: Saut e TGS. Forneça essa explicação.

2) Mecanismos de autorização: considere os Agentes A1 e A2 com as seguintes capacidades
A1 [(O1;"R","W") (O3;"R","X")]
A2[(O2;"X")(O3,"W,X")]

a) [0,4v] Como proceder se o agente descobrir que as capacidades foram obtidas por um atacante? Compare com um problema semelhante nos certificados de chave pública.

b) [0,4v] Se utilizasse listas de controlo de acesso, quais seriam as ACLs resultantes? Indique-as explicitamente.

3) Considere o algoritmo de **cifra híbrida**. Alice quer enviar uma mensagem confidencial (com uma imagem do novo visual de uma estrela de cinema) para Bob.

a) Ambos têm a chave pública do outro.

i. [0,4v] Descreva de forma sucinta como a Alice deverá proceder para enviar a mensagem ao Bob, e como este último deverá proceder para conseguir ler a mensagem de Alice.

ii. [0,4v] A cifra simétrica é efetuada em modo bloco (ECB). Qual o problema de segurança que poderá ocorrer pela utilização do modo de cifra ECB?

b) [0,6v] Assuma agora que ambos não têm a chave pública dos correspondentes pelo que enviam a sua chave pública com a mensagem.

A que tipo de ataque ficam vulneráveis?

Descreva como seria efectuado o ataque.

c) [0,4v] Como poderiam ambos obter a chave pública do outro de forma segura?

Grupo VI [3,4 v]

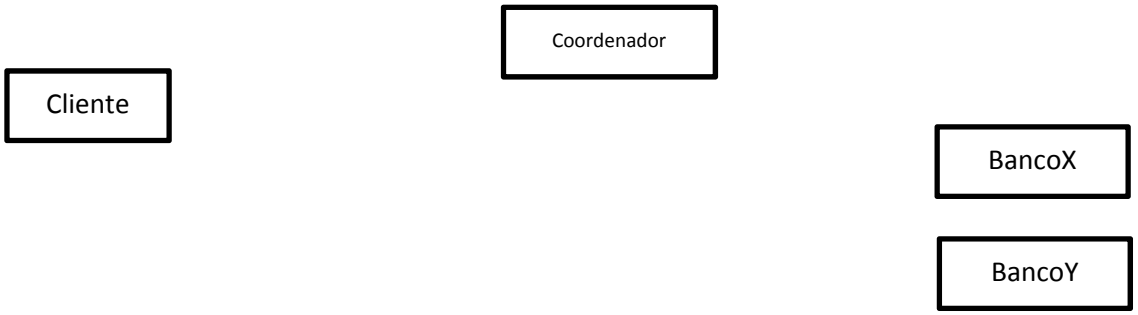


Figura 1 - Sistema transaccional

1) [0,5 v] Considere o sistema da figura 1 em que o cliente pretende executar serviços nos Banco X e Banco Y de forma transacional.
   a) O cliente inicia uma transação distribuída. Desenhe na figura qual a entidade que invoca. Justifique.
   b) Que valor é retornado e qual o seu significado?

Número:

2) [0,6v] O cliente efetua em seguida `Depositar (BancoX, contaX1, valor);`
Complete a figura com esta invocação. Represente todas as ações que esta chamada desencadeia. Justifique a sua resposta.

3) [0,6v] O cliente efetua depois

```
Depositar (BancoY, contaY1, valor);
Saldo = LerSaldo (BancoX, conta 1,);
```

E depois pretende confirmar (commit) a transação.

a) A que entidade se dirige para iniciar o protocolo de confirmação?

b) Na 1ª fase do protocolo de 2PC, que serviços e em que entidades são invocados?

4) [0,6v] Suponha que, depois da fase descrita na pergunta 3.b), o BancoX está em baixo (falha por paragem) e que levará a recuperar um tempo significativo, fazendo com que um temporizador associado ao protocolo no coordenador expire. Descreva a evolução do protocolo. Seja claro e exaustivo na resposta, considerando todos os intervenientes.

5) [0,6v] Considera agora que não há faltas na 1ª etapa do protocolo, mas que depois de ter respondido "sim" o BancoX falha por paragem. Descreva a evolução do protocolo. Seja claro e exaustivo na resposta explicando a evolução em todos os intervenientes.

6) [0,5v] Considere que o BancoY responde "Não" na fase 1 do protocolo 2PC. Indique **duas** razões plausíveis e realistas.

Grupo VII [2,9 v]

Considere a secção *service* descrita neste fragmento de um documento WSDL:

```
<wsdl:service name="EndorsementSearchService">
  <wsdl:documentation>snowboarding-info.com Endorsement Service</wsdl:documentation>
  <!-- connect it to the binding "EndorsementSearchSoapBinding" above -->
  <wsdl:port name="GetEndorsingBoarderPort"
             binding="es:EndorsementSearchSoapBinding">
    <!-- give the binding an network address -->
    <soap:address location="http://www.snowboard-info.com/EndorsementSearch"/>
  </wsdl:port>
</wsdl:service>
```

1) [0,3 v] A localização do serviço é efetuada através de um URL. Classifique este nome quanto a:

Âmbito	
Pureza	
Homogeneidade	

2) [0,4 v] O documento WSDL pode ser publicado e qualquer cliente na Internet poderá, em princípio invocá-lo. Explique porquê relacionando com as propriedades referidas na pergunta 1.

3) [0,4v] O serviço poderia executar-se noutro sítio e o cliente poderia usar o UDDI para descobri-lo em tempo de execução e depois invocá-lo. Como usaria o UDDI para fazê-lo? Explique detalhadamente.

4) [1,0v] No mesmo documento tem outro nome `binding="es:EndorsementSearchSoapBinding">` em que a es poderia estar definido como

```
xmlns:es="http://www.snowboard-info.com/EndorsementSearch.wsdl"
```

   a) Considere o nome `es:EndorsementSearchSoapBinding`.
      i) Qual é a função deste nome?

      ii) Como se garante a propriedade de unicidade referencial?

   b) O nome es é especificado também por um URL que em princípio serve para localizar. É assim neste caso? Justifique

5) [0,8v] O DNS é utilizado para resolver parte do URL mencionado na alínea 1.
   a) Comente a frase "a disponibilidade do serviço pode ser limitada pela disponibilidade do DNS".

   b) Que aspetos da arquitetura do DNS conhece relacionados com o problema que levanta esta frase e que procuram resolvê-lo?
