Número: Nome:

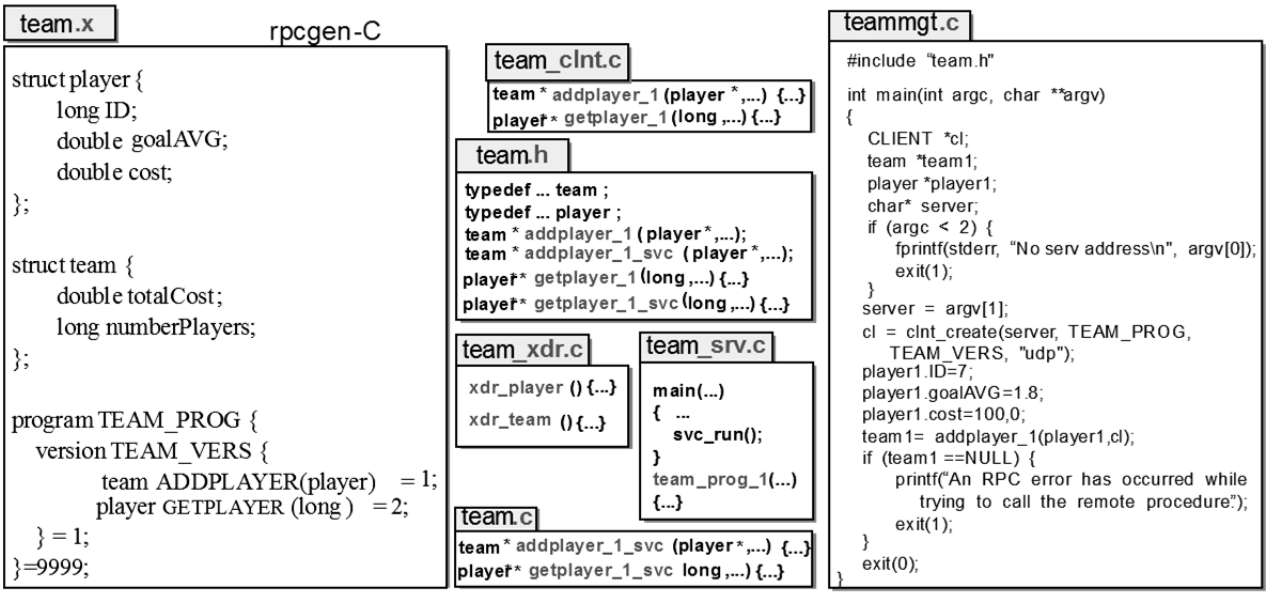
LEIC/LERC – 2011/12 - 2º Exame de Sistemas Distribuídos

29 de Junho de 2012

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

Grupo I RPC [2,5v]

1. Considere o seguinte código fonte de uma aplicação cliente-servidor programado em Sun RPC.



a. [0,5v] Indique, em relação à Figura, qual/quais dos ficheiros apresentados:

Onde está implementada a função de despacho	
Não incluem código introduzido manualmente pelo programador	
São necessários para compilar a aplicação cliente	
Onde é efectuado o Binding do cliente ao servidor (ficheiro(s) e instrução(ões))	
Onde é efectuada a chamada do procedimento remoto no programa cliente (ficheiro e instrução).	
Onde é efectuada a conversão dos parâmetros	

b. [0,4v] Considere a invocação remota do método *addplayer:* *team1=addplayer_1(player1,cl)*, no ficheiro *teammgt.c*. A partir deste ficheiro e da IDL da figura em cima, preencha a seguinte tabela para o pedido enviado ao servidor (para os campos não definidos, poderá definir um valor à sua escolha):

Campo	Valor
XID	
Número Programa	
Número Versão	
Número procedimento	
Parâmetros	

c. [0,5v] A operação *addplayer* muda o estado de uma equipa adicionando um jogador desta, enquanto a operação *getplayer* consulta uma base de dados (sem alterar esta) e retorna informação de um dado jogador da equipa.
Considere o IDL da figura que descreve as operações disponibilizadas pelo serviço e o programa principal do servidor. É seguro invocar as operações *addplayer* e *getplayer* com base na forma como o servidor disponibiliza os serviços? Justifique.

d. Considere que a implementação da função addplayer incrementa o valor da variável numberPlayers da estrutura team (variável global) em uma unidade, quando a mesma é invocada de forma distribuída através da plataforma de RPC, sendo **o valor inicial de 11**.
Considere que a estrutura team é global.

Responda às seguintes questões indicando o valor da variável numberPlayers no contexto da invocação do RPC apresentado em cada alínea.
No caso de não poder deterministicamente definir o valor indique **ND**.

i. [0,3v] Assuma uma semântica de invocação Talvez.

O RPC retornou o resultado à aplicação cliente	
O RPC retornou erro ao cliente	

ii. [0,8v] Assuma agora as seguintes semânticas de invocação.

	Semântica de invocação pelo-menos-uma-vez	Semântica de invocação no máximo-uma-vez	Semântica de invocação exactamente-uma-vez
O pedido foi reenviado três vezes pelo run-time, sendo sempre executado pelo servidor mas perdendo-se sempre a resposta. Só à 4ª vez a resposta chegou ao cliente.			
O RPC foi repetido 4 vezes e o servidor nunca respondeu tendo o cliente considerado que o RPC falhou			
O pedido foi reenviado três vezes pelo run-time, mas perdendo-se sempre a resposta devido a falta temporária do servidor a meio da execução. Só à 4ª vez a resposta chegou ao cliente.			

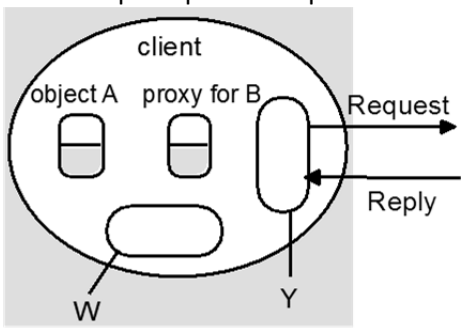
Número:

Grupo II [2,5v]

1) Considere o seguinte extracto de um programa que descreve a classe do programa cliente de uma aplicação de armazenamento de objetos gráficos (exemplo do livro da cadeira).

```
1    public class GraphicalObject implements Serializable{...}
2    public class ShapeServant extends UnicastRemoteObject implements Shape{...}
3
4    public class ShapeListClient{
5      public static void main(String args[]){
6        String shapeType = "Rectangle";
7            ...
8           aShapeList  = (ShapeList) Naming.lookup("//Jean.torriano.net/ShapeList");
9           GraphicalObject g = new GraphicalObject(shapeType,
10          new Rectangle(50,50,300,400),Color.red,Color.blue, false);
11          aShapeList.newShape(g);
12          Shape s = aShapeList.getLastCreatedShape();
13           ...
14     }
15   }
```

a. Considere a figura com os elementos principais da arquitetura do Java RMI no cliente:



i. [0,4v] Preencha a seguinte tabela com os nomes dos componentes W e Y e qual a sua função

Componente	Nome	Função
W		
Y		

ii. [0,3v] Na linha 8 o cliente invoca o serviço de nomes (assuma que corresponde à primeira invocação remota do programa). Descreva, em função dos componentes RMI, que objetos são instanciados no cliente, e como.

iii. [0,3v] Na linha 11, g é passado por valor ou por referência? Justifique.

iv. [0,3v] Na linha 12 é invocado um método remoto. *Shape s* é retornado por valor ou por referência? Justifique.

b. [0,4v] O Java RMI Garbage Collector usa o mecanismo de contagem de referências distribuído. Descreva o estado dos contadores do Garbage Collector distribuído do RMI em `"//Jean.torriano.net"`, ignorando referências a objectos locais. Assuma apenas as invocações da linha 8 à linha 12, inclusive.

c. [0,3v] Considere a classe `GraphicalObject`, e as linhas 9-11. Uma instância da classe `Rectangle` é criada no cliente, sendo `Rectangle` uma subclasse da classe `GraphicalObject`, mas a classe `Rectangle` não pode ser encontrada localmente na CLASSPATH no servidor.
Como poderá a aplicação no servidor obter a classe `Rectangle` durante a execução da instrução `aShapeList.newShape(g)`? Justifique.

2) Considere o seguinte CORBA IDL (OMG IDL):

```
module Accounts
{
      interface Account
      {
          readonly attribute string number;
          readonly attribute float balance;
          exception InsufficientFunds (string detail);

          float debit (in float amount) raises (insufficientFunds);
          float credit (in float amount);
      }
 }
```

a. [0,2v] Assinale a resposta correta: numa invocação a um método remoto, Account é:

	passado por valor
	passado como referência a objecto remoto

b. [0,3v] Comparativamente com a questão 2bI, em CORBA como pode uma aplicação obter a classe de um objecto durante a execução? Justifique.

Grupo III [3,0v]

1) Considere o seguinte pedido HTTP, que inclui um pedido SOAP para um dado web service:

```
1  POST /InStock HTTP/1.1
2  Host: www.example.org
3  Content-Type: application/soap+xml; charset=utf-8
4  Content-Length: nnn
5
6  <?xml version="1.0"?>
7  <soap:Envelope
8  xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
9  soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">
10  <soap:Body xmlns:m="http://www.example.org/catalogo">
11    <m:GetPrice>
12      <m:Envelope>A4 Envelope</m:Envelope>
13    </m:GetPrice>
14  </soap:Body>
15 </soap:Envelope>
```

Número:

a) [0,4v] Os nomes "*Envelope*" que aparecem nas linhas 7 e 12 referenciam o mesmo elemento? Justifique.

b) [0,4v]Em que namespace está o elemento "`m:GetPrice`" definido?

c) Para as linhas indicadas abaixo, indique que secção do WSDL é que a(s) define. Caso ache que não faz parte do WSDL responda "NA":

i) [0,2v] Linhas 1 e 2

ii) [0,2v] Linha 4

iii) [0,2v] Linha 11

iv) [0,2v] Linha 12

2) Classifique a abordagem seguida pelo SOAP para a resolução da heterogeneidade no que toca a:

a) [0,3v] A **estrutura das mensagens**. Justifique.

b) [0,3v] A **política de conversão dos dados**. Justifique.

3) O protocolo SOAP tem as seguintes propriedades. Justifique-as, indicando qual o elemento do protocolo ou da sua definição no WSDLque o justifica:

a) [0,2v] Extensível.

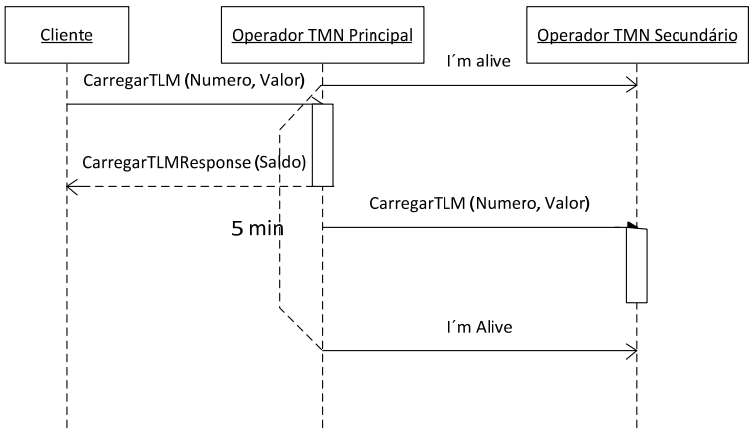
b) [0,2v] Tratamento de exceções remotas.

c) [0,2v] Funcionamento pedido-resposta ou mensagem(one-way).

d) [0,2v] Multiprotocolo de transporte.

Grupo IV [2,5v]

Considere que lhe apresentam o seguinte diagrama de sequência de um protocolo de replicação de servidores.



1) [0,3]Da análise do diagrama, que tipo de falta dos servidores tolera este sistema? Justifique.

2) Suponha que depois da 2ª mensagem "I´m Alive" o Operador TMN Principal não envia mais nenhuma mensagem durante os próximos:
   a) [0,4] 3 min – O que sucede? Justifique.
   b) [0,4] 10 min - O que sucede? Justifique.

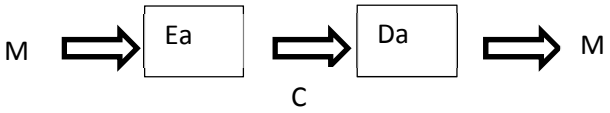
3) O Operador TMN Principal pode falhar depois de enviar a resposta (Carregar TLMResponse) e antes de enviar a mensagem para o secundário.
   a) [0,3] O que sucederá neste caso?
   b) [0,3] Como classifica esta situação em termos da tolerância a faltas?

4) Suponha que a rede de comunicação entre os servidores pode ter uma latência que varia entre 100 ms e valores muito elevados que não foi possível quantificar.
   a) [0,3] O protocolo funciona? Justifique com base nas asserções habituais em que se fundamenta este tipo de protocolos.
   b) [0,5] Como poderia resolver o problema para garantir o correto funcionamento independentemente da latência da rede? Justifique e diga que impacto teria na solução.

Número:

Grupo V [3,7v]

1) Considere um algoritmo de cifra simétrica a, sendo E_a a função de encriptação e D_a a de desencriptação, de acordo com a figura, sendo M a mensagem original em claro e C a mensagem cifrada com a chave secreta k.



a) [0,3v] De forma a ter uma solução de cifra segura, o algoritmo "a" deverá ser secreto.
Verdadeiro ou Falso?

Verdadeiro	Falso

Justifique.

b) Considere um alfabeto apenas com 11 letras. Alice, uma guarda prisional, enviou a seguinte mensagem para Bob: JA FECHEI A CADEIA
usando um método de cifra mono-alfabético baseado numa chave (a chave usada é "ACKE"). Assim, o alfabeto seria convertido de acordo com a figura da esquerda, e o texto original seria portanto convertido de acordo com a figura da direita em baixo:

I. [0,4v] Diga como a atacante Trudy, apanhando a mensagem cifrada, poderia obter a mensagem original. Justifique sucintamente.

II. [0,2v] Este algoritmo utiliza substituição. Que outra operação utilizam os algoritmos de cifra simétrica atualmente como o DES?

III. [0,3v] Os algoritmos de cifra assimétrica, são baseados no mesmo tipo de operações que os algoritmos de cifra simétrica? Justifique.

2) Pretende-se a utilização de mecanismos de autorização.

a) [0,4v] É possivel um agente transferir direitos de acesso para outro agente transmitindo-lhe uma capacidade? Justifique.

b) [0,4v] Considere a seguinte matriz de acessos:

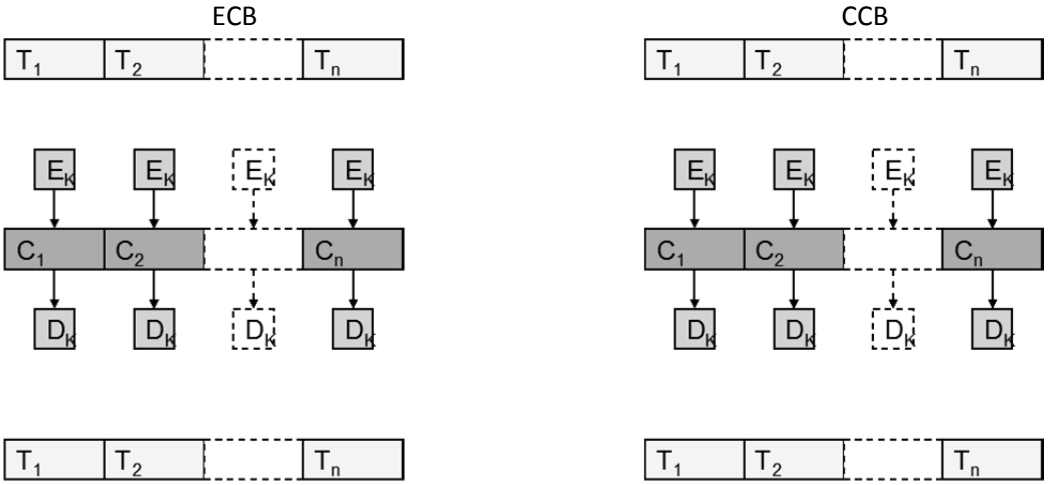
	Objectos			
Agentes	O1	O2	O3	O4
A1	R	RW	RX	---
A2	RX	---	RW	R

Indique explicitamente as capacidades para o agente A2 e a ACL para o objecto O3:

Capacidades Agente A2	
ACL objecto O3	

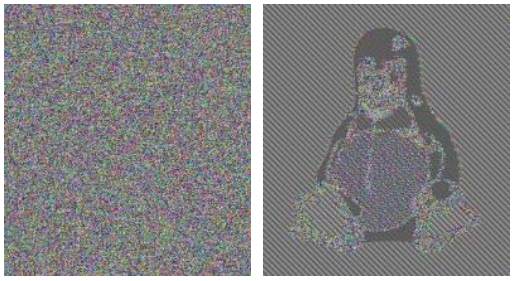
c) [0,4v] Uma forma de impedir um atacante de forjar as capacidades é o monitor de controlo de referências criar uma assinatura digital destas. Assuma que é usada uma função de resumo $H(M)=[car(m)]^2$, em que car(m) é o número de caracteres de m, para criar a assinatura. Diga como um atacante pode alterar uma capacidade com o valor original "O5,RW", e poderá substituir pela mensagem "O6,X" usando a mesma assinatura digital do emissor.

3) Considere os modos de cifra ECB (Electronic Code Book) e CCB (Cipher Block Chaining)



a) [0,4v] Complete as figuras em cima para cada um dos modos de cifra indicados.

b) [0,3v] Considere a cifra da imagem de um pinguim. Legendar com o modo de cifra utilizado (ECB ou CCB) as figuras em baixo.



4) Distribuição de chaves

a. [0,2v] A que tipo de ataque é vulnerável o protocolo Diffie-Helmann?

b. [0,4v] Considere o protocolo Kerberos V5. Que mecanismo existe no protocolo para garantir que um atacante que se apodere de um ticket quando ele circula na rede não o reutiliza?

Número:

Grupo VI [3,2v]

Um cliente pretende executar uma transação, cujo pseudo código está abaixo

```
OpenTransaction
        valor = read (ServA, conta);
        write (ServB, saldo, valor/3);
        write (ServC, saldo, valor/3);
Closetransaction
```

O Diário (log) do coordenador desta transação, num determinado instante é o seguinte:

OpenTransaction	Join	Join	OpenTransaction	CloseTransaction	canCommit	canCommit	Yes	
TID = 1234	1234 ServA.x.pt	1234 ServB.x.pt	TID = 5678	1234	1234 ServA.x.pt	1234 ServB.x.pt	1234 ServA.x.pt	

1) [0,5v] O que está incoerente no diário? Justifique.

2) Admitindo que o diário está coerente com o programa, suponha na situação descrita na figura que expira o timeout do coordenador relativo à transação 1234.
   a) [0,4v]O que poderá isto indicar? Justifique.
   b) [0,5v] Qual a evolução do protocolo? Descreva para todos os intervenientes.

3) [0,6v] Considere agora que não se verifica qualquer timeout. Complete abaixo os valores do diário necessários para que a transação 1234 termine com sucesso. Considere todas as mensagens até final do protocolo.

4) O programa interatua com 3 servidores em que existem variáveis que vão ser alteradas e que consequentemente tem de respeitar a propriedade do isolamento. Admitindo que todos usam um método pessimista de sincronização, responda às seguintes alíneas:
   a) [0,4v] Descreva quantos trincos e em que servidores estão antes da transação fazer CloseTransaction.
   b) [0,4v] Suponha que no ServB a variável "saldo" já está a ser lida numa outra transação que ainda não terminou. O que sucede?
   c) [0,4v] Justifique se esta pode ser uma razão para o protocolo de 2PC decidir abortar.

Grupo VII [2,6v]

O sistema bancário internacional já dispõe de um identificador de bancos o IBAN criado pela União Europeia e depois tornado norma internacional, o IBAN.

O IBAN consta de um máximo de 34 caracteres alfanuméricos. Os dois primeiros são de carácter alfabético e identificam o país. Os dois seguintes são dígitos de controle e são o elemento legitimador da totalidade do IBAN. Segue-se o número de conta, que na maioria dos casos identifica também a entidade bancária e a agência. No caso português, depois dos quatro primeiros caracteres aparecem os 21 caracteres numéricos do NIB.

1) [0,3v] Como é que este nome garante a unicidade referencial?

2) [0,3v] O nome tem diversas informações que poderiam permitir localizar o servidor com a conta bancária. Por esta característica é necessariamente um nome impuro? Justfique.

3) Suponha também que o Banco Central Europeu normaliza a componente mínima de serviços bancários eletrónicos disponíveis através de um conjunto de Web Services que publica num WSDL (EUBanking.wsdl). Os serviços devem poder ser invocados por HTTPS e por SMTP. Explique como poderia usar o UDDI como diretório deste sistema.
   a) [0,2v] Quem seriam as business entities?
   b) [0,2v] Como as poderia identificar?
   c) [0,2v] Que serviços deveriam constar dos Business Services?
   d) [0,2v] Que informação deveria estar na BindingTemplate de cada banco?
   e) [0,2v] Como resolve o problema de existir um WSDL único e numerosos bancos a operar com servidores diferentes?

4) O DNS tem várias alternativas para a resolução de um nome.
   a) [0,2]Indique quais.
   b) Qual o impacto, se existir, destas alternativas na:
      i) [0,2v] Na disponibilidade do DNS.
      ii) [0,2v] No desempenho global.
      iii) [0,2v] Na complexidade do cliente.
      iv) [0,2v] Na complexidade do servidor.