Número: _____ Nome: _____

LEIC/LERC – 2008/09

2º Exame de Sistemas Distribuídos

25 de Julho de 2008

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

Duração: 2h30m

Grupo I [3 v]

```
#define PORT          0x1234
#define HOST_IP       0xC1880810
#define PROGRAM       9999
#define VERSION       5
#define ARGUMENT      10
#define MEASURE_TEMPERATURE 1

struct request_type {
       int program;
       int version;
       int function_number;
       int argument;
}

main(argc, argv)
int argc; char **argv;
{
       int    sd;
       struct sockaddr_in serv_addr;

       struct request_type request;
       int result;

       memset(&serv_addr, 0, sizeof(serv_addr));
       serv_addr.sin_family = AF_INET;
       serv_addr.sin_addr.s_addr = htonl(HOST_IP);
       serv_addr.sin_port = htons(PORT);

       if ((sd = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
              perror("socket");
              exit(1);
       }

       if (connect(sd,(struct sockaddr *) & serv_addr, sizeof(serv_addr)) == -1) {
              perror("connect");
              exit(1);
       }

       request.argument = htons(ARGUMENT);
       request.program = htons(PROGRAM);
       request.version = htons(VERSION);
       request.function_number = htons(MEASURE_TEMPERATURE);

       if (send(sd, &request, sizeof(request), 0) == -1) {
              perror("send");
              exit(1);
       }

      if (recv(sd, &result, sizeof(int), 0) == -1) {
            perror("recv");
            exit(1);
      }
       result = ntohs(result);

       printf("Resultado: %d\n", result);
       close(sd);
}
```

Considere o programa de cliente de um serviço remoto que monitoriza temperaturas de um edifício, apresentado acima. O programa foi codificado usando directamente a interface de comunicação dos

sockets, no entanto o programador teria várias vantagens se tivesse optado por usar RPC para programar o cliente e servidor desta aplicação distribuída.

1. [0,6 v] Qual a semântica de execução da chamada feita no programa acima? Justifique.

2. [0,6 v] Classifique a abordagem de conversão de dados usada no programa acima quanto a: estrutura das mensagens (implícita/explícita) e política de conversão (canónica/receptor-converte). Refira linhas do programa que sustentam a sua resposta.

3. [0,8 v] Como é obtido o endereço do porto do servidor no programa acima e como seria com SUN RPC? Que vantagem encontra no segundo caso?

4. [1 v] Esboce o IDL da interface remota do serviço remoto invocado no programa acima caso pretendesse re-implementar esta aplicação distribuída em SUN RPC.

Grupo II [3 v]

Considere os seguintes excertos de programas que descrevem uma interface, e uma classe utilizada nesse método.

```
public interface RemoteBankInterface extends Remote {
    public Account getAccount (String username,String password) throws RemoteException;
}

public class Account implements Serializable {
       private String fullName = null;
       private int amount = -1
       public Account () {}
       public void setFullName (String fullName) {
                 this.fullName = fullName;
       }
       public void setAmount (int amount) {
                 this.amount = amount;
              }
       public String getFullName() {
                 return fullName;
       }
       public int getAmount() {
           return amount;
       }
}
```

1. Definição das classes e interfaces.
   a. [0,4 v] A classe Account tem o qualificador Serializable. O que quer isto dizer? Em que situações pode ser usado?

   b. [0,5 v] Descreva as principais características da interface RemoteBankInterface.

Suponha a seguinte invocação por parte de um cliente ao método getAccount da interface acima, em que serv é a referência a um servidor remoto que implementa a interface RemoteBankInterface:

```
Account a = (Account) serv.getAccount (args[0], args[1]);
```

   c. [0,4 v] Onde é que esta operação é executada?

   d. [0,4 v] Como são transferidos os parâmetros de entrada?

   e. [0,5 v] Descreva com algum detalhe o que se passa no espaço de endereçamento do cliente quando este método retorna.

2. O cliente invocada agora

```
a.setAmount (45);
```

a. [0,4 v] Onde é que a operação é executada?

b. [0,4 v] Onde é que o estado é modificado?

Grupo III [3 v]

1. O exemplo apresenta um extracto de um xsd e de um wsdl semelhantes ao que utilizou no trabalho prático.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    targetNamespace="urn:suid:view" xmlns:tns="urn:suid:view"
    elementFormDefault="qualified" xmlns:jaxb="http://java.sun.com/xml/ns/jaxb"
    jaxb:version="1.0" jaxb:extensionBindingPrefixes="xjc"
    xmlns:xjc="http://java.sun.com/xml/ns/jaxb/xjc">

    <!-- ... -->

    <xsd:complexType name="LoginView">
        <xsd:sequence>
            <xsd:element name="validado" type="xsd:boolean" />
            <xsd:element name="numeroMecanografico" type="xsd:int"/>
        </xsd:sequence>
    </xsd:complexType>
    <xsd:element name="loginView" type="tns:LoginView" />

    <!-- ... -->
</xsd:schema>


<?xml version="1.0" encoding="UTF-8"?>
<definitions name="SUID" targetNamespace="urn:suid:wsdl"
    xmlns:tns="urn:suid:wsdl" 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:suid:wsdl"
                    xmlns:ns1="urn:suid:view">

            <xsd:import namespace="urn:suid:view" schemaLocation="suid-view.xsd" />

            <xsd:complexType name="Login">
                <xsd:sequence>
                    <xsd:element name="user" type="xsd:string" />
                    <xsd:element name="password" type="xsd:string" />
                </xsd:sequence>
            </xsd:complexType>
            <xsd:element name="login" type="tns:Login" />

            <xsd:complexType name="LoginResponse">
                <xsd:sequence>
                    <xsd:element name="loginVista" type="ns1:LoginView" />
                </xsd:sequence>
            </xsd:complexType>
            <xsd:element name="loginResponse" type="tns:LoginResponse" />

            <!-- ... -->
        </xsd:schema>
    </types>
```

```
    <message name="login">
        <part name="parameters" element="tns:login" />
    </message>
    <message name="loginResponse">
        <part name="result" element="tns:loginResponse" />
    </message>

    <!-- ... -->

    <portType name="SUIDPortType">
        <operation name="login">
            <input message="tns:login" name="login" />
            <output message="tns:loginResponse" name="loginResponse" />
            <fault message="tns:suidFault" name="suidFault" />
            <fault message="tns:serviceError" name="serviceError" />
        </operation>

        <!-- ... -->
    </portType>
.....................
```

a. [0,5 v] No campo types existe a importação de um ficheiro. Que vantagens vê nesta possibilidade para o desenvolvimento dos serviços? Justifique.

b. [0,7 v] Explique o serviço descrito no wsdl detalhando o conteúdo do campo portType.

c. [0,6 v] A estrutura do WSDL parece ser mais complicada do que necessário. Vê alguma razão para a secção Port Type estar separada da secção Message e não ter uma forma declarativa mais próxima da habitual nas linguagens procedimentais? Justifique

d. [1,2 v] Procure extrair do contrato a estrutura do envelope da mensagem SOAP `loginResponse`.

Grupo IV [3 v]

O seguinte texto é extraído da página inicial do Fénix:

O nome de utilizador (username) tradicionalmente usado no IST e também adoptado no sistema Fénix é da forma fxxxx, dxxxx ou lyyyyy, onde xxxx é o número mecanográfico de docentes e funcionários e yyyyy é o número de aluno.

Apesar desta tradição, este sistema de numeração apresenta alguns inconvenientes. De facto, alguns utilizadores têm simultaneamente vários papéis dentro da escola: um aluno pode simultaneamente ser funcionário da escola, ou um docente ser simultaneamente um estudante de Doutoramento. Por outro lado, um estudante de Licenciatura, Mestrado ou Doutoramento pode evoluir, ao longo da sua vida académica, de estudante para docente. Em casos como estes, é conveniente que, quer os registos pessoais, quer as credenciais de autenticação, não tenham que ser duplicados. Tal permite que o utilizador mantenha acesso aos mesmos serviços básicos e à mesma informação pessoal, ainda que a alteração de estatuto lhe permita eventualmente o acesso a serviços adicionais específicos do seu novo perfil (e, eventualmente, o fim de outros serviços anteriormente disponíveis).

De modo a facilitar esta identificação única do utilizador, o CIIST criou o ISTID, a qual é invariante e independente do estatuto do utilizador na escola. O ISTID é da forma ***istxxxxxx****, onde xxxxx é derivado do seu primeiro estatuto dentro do IST. O ISTID é obtido da seguinte forma:*

Docentes: *Somar 10000 ao número mecanográfico;*
Funcionários: *Somar 20000 ao número de funcionário;*
Alunos: *Somar 100000 ao número de aluno.*

1. Considere o espaço de nomes ISTID
   a. [0,4 v] É um nome hierárquico ou simples?

   b. [0,4 v] Homogéneo ou heterogéneo?

   c. [0,4 v] Se se considerar que o fenix pode vir a ser estendido a outras faculdades, que propriedade pretende garantir o prefixo IST?

2. Considere que existem dois servidores, um que mantém a identificação dos alunos e outro a dos docentes+funcionários e que a identificação ficaria sempre no servidor onde foi inicialmente criado o utilizador.
   a. O principal objectivo da proposta é fazer com o nome seja imutável neste contexto e relativamente às propriedades do nomes o que lhe parece
      i. [0,4 v] O nome é puro ou impuro?

      ii. [0,4 v] O nome é persistente?

3. O extracto seguinte é de um programa das aulas práticas de utilização do UDDI

```
public static void main(String[] args) {
   try{
       Registry registry = null;
       ClassificationQuery query = null;
       Registration[] registrationArray = null;
       try {
            registry = new Registry("/Registry.properties");
            query = new ClassificationQuery("/ClassificationQuery.properties");
            registry.connect(false);
            registrationArray = registry.query(query);
           if(registrationArray == null) {
             System.out.println("No web service registrations found in
                    registry server " + registry.getURL());
             return;
            } else {
             System.out.println("Found " + registrationArray.length + " web
service registrations in registry server " + registry.getURL());
       }
       } finally {if(registry != null) registry.disconnect();
    }
```

a. [0,4 v] O resultado é um array. Porquê?

b. [0,6 v] No trabalho prático tinha uma arquitectura tolerante a faltas com um primário e um ou mais secundários. Este mecanismo seria útil nessa situação? Justifique.

Grupo V [4 v]

1. Considere uma versão simplificada do projecto realizado nesta disciplina, onde se pretende implementar um sistema de avaliação de alunos online. Este sistema de avaliação é composto por um servidor de identificação/autenticação designado de SID, cuja chave pública é conhecida, um servidor que serve de repositório de exames designado por SAval e um cliente (não confiável) onde os alunos se autenticam com o seu cartão de aluno e realizam as avaliações. Cada cartão contém um par de chaves assimétricas único atribuído ao aluno.
   Os passos seguidos por um aluno para realizar o exame são os seguintes:
   1) Autentica-se junto do SID, que conhece as chaves públicas dos alunos e do SAval.
   2) Pede um exame ao SAval. O SAval envia o exame, não mantendo qualquer estado sobre a que alunos entregou exames. O exame contém as perguntas e a duração máxima para resposta.
   3) Após a realização da prova as respostas são enviadas para o SAval, que responde com a nota obtida.

   Fica ao seu critério a especificação de características do sistema que não foram definidas nesta descrição.
   O protocolo de autenticação tem que ser baseado em cifra assimétrica e deve garantir a autenticidade, a integridade e a validade temporal do exame e das respostas.

   a) [1 v] Descreva toda as mensagens necessárias, e o seu conteúdo, desde que um aluno se autentica no sistema até imediatamente antes de pedir um exame ao *SAval.*

   b) [0,7 v] Descreva toda as mensagens necessárias, e o seu conteúdo, entre o pedido de um exame ao *SAval* pelo cliente até a sua recepção nesse mesmo cliente.

   c) [0,7 v] Descreva a mensagem enviada pelo cliente ao *SAval*, e o seu conteúdo, com o exame preenchido.

   d) [0,4 v] Descreva a mensagem de resposta recebida pelo cliente com a nota final.

3 – Considere o acesso a uma página web remota por https a um servidor (Serv1) que detém um certificado de chave pública emitido por uma dada autoridade certificadora (CA) de um sistema hierárquico de CAs. Assuma que o cliente obtém o certificado de Serv1 através de um servidor não confiável.

a) [0,6 v] Identifique os campos fundamentais de um certificado digital.

b) [0,6 v] Para se assegurar a chave pública de Serv1 que está indicada no certificado é a chave legítima de Serv1, o cliente precisa de mais informação (para além do certificado)? Se sim, qual? Justifique.

Grupo VI [2 v]

1. Considere uma variante do algoritmo de replicação activa dado nas aulas em que cada cliente **C** executa os seguintes procedimentos para ler ou escrever de um objecto replicado.

Assuma apenas um objecto replicado e 3 réplicas, **R1, R2** e **R3**.

```
ler() {
        envia pedido de leitura a todas as réplicas;
        aguarda que a primeira resposta <valor,(numSeq,idUltimoEscritor)> chegue;
        retorna valor à aplicação;
}

escrever(novoValor) {
        envia pedido de leitura a todas as réplicas;
        aguarda que a primeira resposta <valor,(numSeq, idUltimoEscritor)> chegue;
        envia pedido de escrita <novoValor,(numSeq+1,idC)> a todos as réplicas;
        espera que a resposta Ack chegue de todos as réplicas;
    retorna à aplicação;
}
```

O comportamento das réplicas é exactamente o mesmo das réplicas na solução de replicação activa dada nas aulas teóricas (protocolo por quoruns de maioria).

a) [0,6 v] Assuma que todas as réplicas se desligam devido a uma falha na rede eléctrica regional. Do ponto de vista do sistema replicado, classifique esta falta da forma mais completa possível usando a terminologia dada nas aulas.

b) [0,6 v] Indique quantas réplicas falhadas são toleradas no novo algoritmo e no protocolo de quoruns de maioria. Analise as operações de leitura e escrita separadamente.

Réplicas em falta toleradas	Leitura	Escrita
Algoritmo novo		
Quoruns maioria		

c) [0,8 v] As réplicas R1, R2 e R3 são pouco fiáveis e podem falhar de forma independente e recuperável. Ao longo de um dia de operação, cada réplica está, em média, 10% do tempo indisponível. Com base nos valores que indicou na alínea anterior, calcule a disponibilidade de cada algoritmo para cada operação (leitura e escrita).
Para simplificar, assuma que, para eventos independentes A e B, P(A ou B)=P(A) + P(B).
Nota: Caso não tenha respondido à alínea anterior, assuma os seguintes valores hipotéticos:

Réplicas em falta toleradas	Leitura	Escrita
Algoritmo novo	1	2
Quoruns maioria	2	1

Respostas:

Disponibilidade	Leitura	Escrita
Algoritmo novo		
Quoruns maioria		

Apresente os cálculos:

Grupo VII [2 v]

1. Considere o seguinte protocolo de confirmação:

Coordenador	Participante
1. Envia *Confirmar* a todos os participantes	
	2. Ao receber Confirmar, responde *Ack* de imediato. Entretanto, executa *confirmar* na transacção local.
3. Espera por *Acks* de todos.	

a. [0,6 v] O protocolo de confirmação apresentado acima assegura a atomicidade da transacção distribuída? Justifique, ilustrando com um exemplo.

2. Considere o protocolo 2PC. Assuma que apenas sabe que:
   - um participante que está no estado "Preparado/Em espera"
   - até ao momento, não houve falhas de processos nem mensagens a chegar (a qualquer processo) após o seu temporizador expirar.

   a. [0,7 v] Indique, de entre os estados Inicial, Preparado/Em Espera, Abortar e Confirmar, em qual(is) é é possível algum outro participante estar. Justifique.

   Estado(s) possíveis:

   Justificação:

   b. [0,7 v] Na mesma situação da alínea anterior, responda considerando agora o protocolo 3PC (neste caso considere os estados Inicial, Preparado/Em Espera, Abortar, Pré-confirmado e Confirmar).

   Estado(s) possíveis:

   Justificação: