Sistemas Distribuídos - LEIC/LEEC **16 de Janeiro de 2006**
Época Normal **Duração: 90+15min**

- **Pense antes de responder**, a estrutura das suas respostas será também um critério de avaliação.
- **Seja sintético** ("*tudo o que escrever pode ser usado contra si*").
- **Justifique todas as respostas.**
- Use o tempo indicado em cada pergunta como uma **estimativa** do tempo necessário para lhe responder. Os 15 minutos de tolerância, **já** indicados no **cabeçalho**, servem para compensar possíveis erros nas estimativas.

1- [2v/20min] Considere um serviço de transferência de ficheiros muito simples suportando as seguintes operações sobre ficheiros: lêr, escrever, renomear e apagar. Note que as operações de leitura e de escrita operam sobre ficheiros inteiros e não partes desses ficheiros. Por exemplo, lêr transfere todo o conteúdo do ficheiro do servidor para o cliente.

1.1- Que propriedades deverá ter um canal de comunicação para facilitar o desenvolvimento deste serviço? Justifique.

1.2- Defina um possível protocolo baseado em mensagens para este serviço. Não se esqueça de considerar a possibilidade de erros.

2 - [1,5v/10min] A implementação de métodos remotos pelo próprio sistema Java RMI pode usar múltiplos *threads*. Descreva sinteticamente uma possível implementação *multithreaded*. Que precauções, se alguma, deverá ter um programador que desenvolve objectos remotos usando essa implementação de Java RMI?

3 - [1v/5min] Considere a resolução de nomes em DNS. Um servidor duma zona precisa manter pelo menos 2 *resource records* de tipo diferente por cada zona cuja administração delegou directamente. Descreva a informação contida em cada um desses *resource records* e como ela é usada no processo de resolução de nomes DNS.

4 - [1v/10min] Um dos mecanismos fundamentais usados em Jini é o de *lease*.

4.1- Explique o que é um *lease* e dê um exemplo duma sua aplicação.

4.2- A interface `net.jini.core.lease.Lease` define duas constantes DURATION e ABSOLUTE. Para que servem? Em que casos o uso de uma é vantajoso em relação ao da outra? Justifique.

5 - [1,5v/10min] Considere o problema da sincronização de relógios físicos.

5.1- Descreva o algoritmo de Cristian para sincronização externa de relógios. Qual é o erro máximo de sincronização, no instante em que o relógio é actualizado? Justifique, recorrendo, se necessário, a um desenho.

5.2- Este algoritmo foi apresentado como um algoritmo de sincronização para sistemas assíncronos. Pode também ser usado para sincronização de relógios em sistemas síncronos? Justifique.

6 - [1,5v/10min] Na Web recorre-se frequentemente à replicação.

6.1- Nomeie dois tipos de nós da Web onde é comum fazer *cacheing*, e explique em que medida estas podem ser consideradas uma forma de replicação. Que razões justificam o recurso a *cacheing* por esses nós?

6.2- Para cada uma dos tipos de nós acima mencionados, descreva um mecanismo ou algoritmo usado para manter a coerência da *cache* respectiva. Indique, justificando, o modêlo de consistência, se algum, suportado por estes mecanismos ou algoritmos.

7 - [2v/15min] Duas técnicas de replicação muito usadas são replicação activa e replicação passiva.

7.1- Explique a diferença entre elas.

7.2- Descreva uma implementação de replicação passiva usando grupos estáticos com *multicast* fiável com ordem total.

8 - [1,5v/10min] Em sistemas criptográficos assimétricos faz-se uso de dois tipos de chaves – chaves públicas e chaves privadas.

8.1- Mostre, dando exemplos da sua aplicação na implementação de mecanismos de segurança, que qualquer destas chaves pode ser usada quer em operações de codificação quer em operações de descodificação.

8.2- Na Internet normalmente prefere-se criptografia assimétrica para autenticação e criptografia simétrica para garantir confidencialidade. Explique porquê.