Sistemas Distribuídos - MIEEC **13 de Novembro de 2015**
Teste (Com consulta de "cheat sheet") **Duração: 120 min**

---

1. **Justifique todas as respostas.**
2. **Responda às perguntas 1 e 2 numa folha e às restantes noutra.**

---

1 [3v] - Relativamente a sistemas distribuídos.
1.1- Refira dois **problemas** causados pela utilização de **distribuição** na concepção de aplicações. Justifique.
1.2- Diga o que entende por **middleware** e dê **dois exemplos** de tecnologias de *middleware* de distribuição.
1.3- Não existindo nenhum tipo de sincronização é possível obter **informação de ordem** apenas com troca de mensagens num sistema distribuído? Justifique.

2 [7v] - Considere uma célula num sistema industrial onde existem várias máquinas que cooperam numa determinada aplicação distribuída. Os requisitos de comunicação são heterogéneos, desde partilha de estado entre várias máquinas com períodos de 10ms até troca de ficheiros de configuração e histórico, trocados esporadicamente mas com uma dimensão que pode chegar a alguns MBs.
2.1- Numa primeira abordagem vai tentar usar uma rede com protocolos *standard* da Internet. Que **protocolo de transporte** usaria para esses tipos de mensagens, nomeadamente partilha de estado e troca de ficheiros? Justifique.
2.2- Para facilitar a ordenação de eventos decidiu usar um **relógio de Lamport**. Olhando apenas para as marcas temporais (*timestamp*) de Lamport que afirmação pode fazer quanto à precedência de eventos?
2.3- Entretanto decidiu criar um serviço de **sincronização de relógio distribuído** para fornecer uma base temporal global. Quais são os factores que **limitam a precisão** que se consegue atingir?
2.4- Considere que para melhorar a pontualidade do sistema decidiu implementar um **protocolo de rede** do tipo **TDMA** em que os vários nodos transmitem em *slots* fixas consecutivas, organizadas sequencialmente num ciclo periódico. Cada nodo reconhece a sua slot por tempo, usando o relógio global. Quais as implicações de uma **precisão temporal limitada**? É relevante a **exatidão** do relógio global, neste contexto?
2.5- Para implementar o relógio global decidiu usar a técnica conhecida como **Fault-Tolerant Average (FTA)**. Descreva como a usaria. Considere ainda que cada nodo adquire uma marca temporal (*timestamp*) do seu relógio logo no início da sua *slot* e a difunde (*broadcast*) com uma mensagem de tamanho fixo. O atraso de rede deste mensagem é de $100\mu s$ e o mecanismo de transmissão pode gerar um *jitter* de $10\mu s$. Qual a precisão que se pode alcançar?

3 [1v]- Considere a aplicação da técnica **Triple Modular Redundancy** a um sistema com 3 andares/estágios. Indique o número máximo de componentes avariados, incluindo dispositivos de voto, tolerado por esta técnica. Justifique.
Dica- Use uma figura.

4 [1.5v]- Algoritmos de **eleição de *leader*/coordenador** são um bloco básico em muitos outros algoritmos distribuídos. Dê **dois exemplos** de algoritmos que estudou que podem usar algoritmos de eleição, descrevendo como esses algoritmos fariam uso do algoritmo de eleição e o porquê desse uso.

5 [1.5v]- Diga, justificando, se a seguinte afirmação é verdadeira ou falsa:

> Qualquer serviço replicado deverá ser **determinista**, independentemente da replicação usada ser do tipo primário-apois (*primary-backup*) ou do tipo máquina de estados replicada (*state machine replication*.

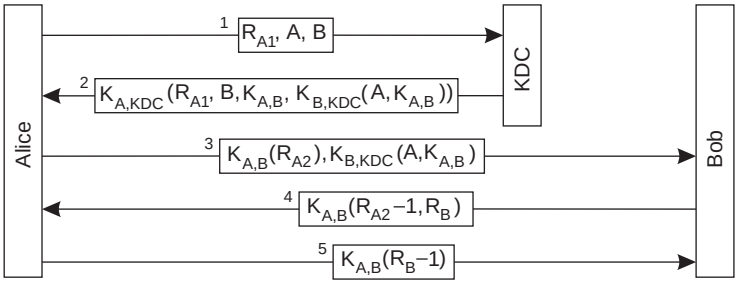
6 [3v] - O algoritmo de replicação **quorum consensus** deve satisfazer as seguintes desigualdades:

$$N_R + N_W < N \tag{1}$$

$$N_W + N_W < N \tag{2}$$

Explique através de exemplos a necessidade de cada uma das desigualdades.

7 [3v] - A figura abaixo exemplifica o protocolo para autenticação em sistemas de chave partilhada proposto por Needham e Schroeder em 1978.



7.1- Explique para que servem os parâmetros R_{A1}, R_{A2} e R_B.
7.2- Em 1981, Denning e Sacco descrobriram uma **vulnerabilidade** neste algoritmo. Explique-a. **Dica-** Use uma figura.