

## Final U.V. RE51

Sans documents

20 Janvier 2012

gaber@utbm.fr

### Exercice 1 : Les protocoles de transfert de données PTD (4 points)

Les protocoles de transfert des données dans un système distribué dans le contexte d'un environnement non fiable nécessitent des mécanismes pour assurer l'acheminement des messages. Donner et justifier les fondements de solution qui peuvent permettre de résoudre les problèmes soulevés par les environnements non fiables.

### Exercice 2 (5 points)

a) L'algorithme de Naimi-Tréhel utilise une structure arborescente pour résoudre le problème de l'exclusion mutuelle. Considérons le scénario suivant. On dispose d'un système distribué contenant 5 sites. On suppose que le graphe (i.e., le réseau) connectant les sites est complet. Considérons le scénario suivant :

- 1) Initialement, le site 1 possède le privilège et utilise la section critique, le site 3 demande à entrer en section critique et le site 1 quitte la section critique,
- 2) Le site 4 demande à entrer en section critique,
- 3) Le site 3 quitte la section critique,
- 4) Le site 2 demande à entrer en section critique.

Pour chacun de ces cas, donner l'arborescence associée (en indiquant tous les pointeurs concernés).

b) On dispose d'un système distribué pour lequel le système de communication est un anneau. Quel est l'algorithme d'exclusion mutuelle le plus adapté que l'on pourrait utiliser ?

### Exercice 3 : Topologies virtuelles (6 points)

Nous avons vu en cours que les topologies virtuelles peuvent être classées en trois catégories selon qu'elles sont basées sur une approche orientée nœuds de couverture, liens inter-nœuds ou encore hybride. Parmi les approches orientées nœuds de couverture, nous avons celle basée sur le concept relais multipoint (Multi-Point Relays ou MPR).

- a) Donner le principe de l'approche MPR (vous pouvez illustrer votre propos par une figure)
- b) Montrer l'intérêt de cette approche.

### Exercice 4 : Sécurité des systèmes distribués (5 points)

Un protocole d'authentification permet à une entité de vérifier l'identité d'une autre dans un environnement distribué. Le protocole Kerberos permet à un utilisateur de vérifier l'identité d'un serveur, à un serveur de vérifier l'identité d'un autre serveur, et à l'utilisateur de vérifier son identité sur le serveur, dans un réseau non sécurisé. Les échanges de messages se déroulent selon trois étapes. Décrivez ce protocole en donnant les séquences d'échanges des messages de chacune de ces étapes.

**Exercice 5 (facultatif) : Tendances actuelles**

Nous avons vu en cours que la conception des algorithmes distribués est basée sur l'utilisation de concepts propres qui ont été proposés pour remédier aux problèmes soulevés par les systèmes distribués à cause de l'absence de mémoire commune et d'horloge globale.

a) Ces concepts sont-ils toujours valables dans le contexte actuel de réseaux sans fil et des réseaux mobiles ? Dresser une liste de problèmes soulevés par ce nouveau contexte ainsi que leurs causes.

b) Proposer une solution alternative pour une meilleure exploitation de ces réseaux.

Bon courage !