TD5
SI4 - Politique d'accès internet

La direction de la société CCCP souhaite appliquer au sein de l'entreprise, toutes filiales confondues, une politique d'accès au réseau internet. Plus précisément, la direction désire pouvoir appliquer des droits d'accès soit à un utilisateur en particulier, soit directement à un groupe d'utilisateurs, sachant qu'un utilisateur peut appartenir à plusieurs groupes.

Quatre types de droit sont envisagés : Aucun, Super-Restreint, Restreint, Libre

- **Aucun** : L'utilisateur ne peut pas accéder au réseau intranet/internet.
- **Super-Restreint** : L'utilisateur ne peut accéder qu'au réseau intranet de l'entreprise.
- **Restreint :** L'utilisateur ne peut accéder qu'au réseau intranet de l'entreprise et aux services *web* des fournisseurs référencés.
- **Libre** : L'utilisateur peut accéder librement à internet.

La société CCCP s'est dotée d'un routeur avec des fonctions de pare-feu (*firewall*) notamment dans le but d'appliquer sa politique de droits d'accès au réseau internet.

Le système est confié à l'administrateur du réseau de l'entreprise qui, après avoir étudié la documentation, découvre qu'il peut aisément, par programmation, appliquer la politique en question.

Pour cela il dispose d'une liste de droits, nommée ACL (*Access Control List*), un droit étant une instance de la structure nommée ACE (*Access Control Entry*), définie ainsi :

Structure ACE **{** userId **: chaîne de caractères,** unDroit **: entier }**.

Le rôle de chacun des champs est :

- *userId* : Identifiant unique d'un utilisateur ou d'un groupe d'utilisateurs au sein de l'entreprise.
- *unDroit* : Un entier parmi {**0**, **1**, **2**, **3**}, correspondant respectivement à ***aucun, super-restreint, restreint*** et ***libre***.

Il envisage d'écrire une fonction respectant les spécifications suivantes :

Interface

Fonction chercheDroit**(** tabIds **: tableau de chaînes de caractères,**
tabACL **: tableau d'**ACE**) : entier**

Où :

- *tabIds* est un tableau dont la première case contient toujours l'identifiant de l'utilisateur ; le cas échéant, les cases suivantes contiennent les identifiants des groupes auxquels appartient cet utilisateur.

- *tabACL* : représente une *ACL,* c'est-à-dire une liste d'ACE. Cette liste n'est pas triée.
- Valeur retournée : droit d'accès (0, 1, 2 ou 3) à appliquer à l'utilisateur dont la liste des identifiants est dans *tabIds*.

NB : On dispose d'une fonction, nommée *nombreÉléments(),* qui permet de connaître le nombre d'éléments d'un tableau passé en paramètre :

Fonction nombreÉléments(*t* : **tableau**) : **entier**

Règles de gestion

- **R1**

  Le droit le moins contraignant prime sur les autres, sauf application de la règle R2.

  Par exemple, si les droits *Restreint* et *Super-Restreint* sont affectés à un même utilisateur (directement ou par l'intermédiaire des groupes auxquels il appartient), le droit retenu sera le droit *Restreint*.

- **R2**

  Le droit *Aucun* est prioritaire sur tous les autres.

  Par exemple, si les droits *Libre* et *Aucun* sont affectés à un même utilisateur, le droit retenu sera le droit *Aucun*.

- **R3**

  Par défaut (en absence d'affectation de droits), le droit *Aucun* est alloué.

Exemple d'utilisation

tabIds1

0	CCCP
1	Comptabilité
2	Projet PACA

tabIds2

0	Grimaud
1	Commercial
2	Projet P2P
3	Projet PACA

tabIds3

0	Dumortier

ACL

0	Grimaud	0
1	CCCP	1
2	Topaze	3
3	Comptabilité	2
4	Informatique	3
5	Commercial	2
6	Projet PACA	2
7	Projet P2P	1
8	Projet R2D2	3

nombreÉléments (tabIds1) retourne 3
nombreÉléments (tabIds2) retourne 4
nombreÉléments (tabIds3) retourne 1
nombreÉléments (ACL) retourne 9

chercheDroit(tabIds1, ACL) retourne 2, soit le maximum des droits de CCCP (1), et des groupes Comptabilité (2) et Projet PACA (2) *(Application de la règle R1).*

Travail à faire

1. Indiquer la valeur que doit retourner la fonction ***chercheDroit***(tabIds2, ACL), en justifiant la règle appliquée.

2. Rédiger l'algorithme correspondant à la fonction ***chercheDroit***.