

# Examen d'administration réseau

(première session)

**Documents autorisés :** supports de cours, documents manuscrits.

Calculatrices autorisées. Téléphones portables interdits.

**Durée :** 2h.

Toutes les réponses doivent être détaillées (techniquement si possible) et justifiées. Le sujet comporte trois pages.

## 1 Syndrome de la fenêtre folle dans TCP (7.5 points)

Le contrôle de flux de TCP empêche à un émetteur trop rapide d'envoyer trop de paquets à un receveur trop lent. Rappelons que dans TCP, tous les segments ont une taille limitée à MSS (pour *maximum segment size*). Nous supposons que MSS vaut 600 dans la suite.

**Question 1 (0.5 point)** *Rappelez comment le contrôle de flux est implémenté sous TCP.*

**Question 2 (1.5 points)** *Considérons le scénario suivant. A désire transmettre 800 octets à B. B possède un buffer de réception de 600 octets. De plus, B traite les données lentement : à chaque fois que A envoie quatre octets de données, B n'est capable d'en extraire du buffer qu'un seul. En supposant que la connexion est déjà établie entre A et B, représentez les échanges de paquets en vous concentrant sur l'évolution du buffer de réception de B. Est-ce que la communication selon ce scénario est efficace ?*

**Question 3 (1.5 points)** *L'algorithme de David D. Clark interdit à un récepteur de transmettre une taille de buffer de réception inférieure à  $\min\{MSS, w_0/2\}$ , où  $w_0$  est la taille initiale du buffer de réception. Reprenez le scénario précédent, et montrez que l'algorithme de David D. Clark résout le problème.*

**Question 4 (1.5 points)** *Considérons le scénario suivant. A désire transmettre 800 octets à B. A produit les données 80 octets par 80 octets. Le délai entre A et B est long et on supposera que B traite les données rapidement. En supposant que la connexion est déjà établie entre A et B, représentez les échanges de paquets (en supposant que A commence en mode démarrage lent avec une fenêtre de congestion égale à 1, et sans l'algorithme de Nagle). Est-ce que la communication selon ce scénario est efficace ?*

**Question 5 (1.5 points)** *Reprenez le scénario précédent, et montrez que l'algorithme de Nagle résout le problème.*

**Question 6 (1 point)** *Le syndrome de la fenêtre folle apparaît quand la taille de la fenêtre de TCP conduit à des envois de données inefficaces. L'algorithme de David D. Clark et l'algorithme de Nagle sont deux solutions au syndrome de la fenêtre folle. Expliquez en quoi ces solutions sont complémentaires.*

## 2 Routage avec RIP (4.5 points)

Considérons le réseau représenté sur la figure 1, sur lequel le protocole de routage RIP est utilisé.

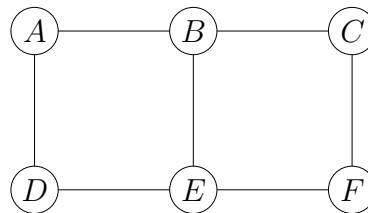


FIGURE 1 – Un réseau sur lequel le protocole de routage RIP est utilisé.

**Question 7 (0.5 point)** *Pourquoi est-ce RIP qui est utilisé sur ce réseau, plutôt qu'OSPF ?*

**Question 8 (2 points)** *Représentez les échanges de messages échangés par RIP jusqu'à ce que le routage converge. On supposera que les routeurs transmettent leur vecteur dans l'ordre A, B, C, D, E et F.*

**Question 9 (0.5 point)** *À quoi servent les messages poison updates dans RIP ?*

**Question 10 (1.5 point)** *Supposons que le lien entre C et F tombe en panne. Représentez les messages poison updates envoyés et la conséquence immédiate (c'est-à-dire, avant que le routage ne converge à nouveau) sur les décisions de routage ?*

## 3 Étude de cas sur les proxys (8 points)

Vous êtes administrateur réseau d'une entreprise, et vous souhaitez mettre en place du contrôle d'accès au niveau des communications webs pour autoriser ou interdire certains sites à certains utilisateurs.

### 3.1 Utilisation d'un proxy interne

**Question 11 (0.5 point)** *Pourquoi est-il préférable de faire le contrôle d'accès en un seul point du réseau ?*

**Question 12 (1 point)** *Si le contrôle d'accès est fait à la sortie du réseau privé, doit-il être fait juste avant la traduction d'adresses ou juste après la traduction d'adresses ?*

Faire le contrôle d'accès web sur la machine faisant la traduction d'adresses peut surcharger inutilement cette machine. En général, il est préférable d'utiliser un proxy, c'est-à-dire une machine du réseau interne qui agit comme intermédiaire.

**Question 13 (1 point)** *Comment forcer les utilisateurs à accéder aux services webs par l'intermédiaire du proxy ?*

**Question 14 (0.5 point)** *Où faire le contrôle d'accès web ?*

**Question 15 (1.5 points)** *Représentez l'architecture résultante, en indiquant la machine réalisant le NAT, la DMZ (et ses serveurs webs), le proxy et les utilisateurs. Faites apparaître les communications autorisées par des flèches.*

### 3.2 Fonctionnement du proxy au niveau HTTP

Au niveau HTTP, une requête sans proxy sur l'adresse `http://www.google.fr/` se fait en envoyant la commande HTTP GET / sur le serveur `www.google.fr`. Une requête avec proxy sur l'adresse `http://www.google.fr/` se fait en envoyant la commande HTTP GET `www.google.fr/` sur le proxy.

**Question 16 (0.5 point)** *Pourquoi ces deux requêtes sont-elles légèrement différentes ? Faut-il configurer le client de manière particulière pour qu'il gère le proxy ? Comment ?*

**Question 17 (1 point)** *Que fait le programme du proxy ? Est-ce un programme compliqué à implémenter ?*

### 3.3 Utilisation d'un proxy externe

Certains utilisateurs cherchent à contourner le contrôle d'accès en utilisant un proxy externe. Un proxy externe fonctionne de la manière suivante : lorsqu'un utilisateur se connecte sur ce proxy externe, un formulaire HTML avec une zone à remplir est affiché. Quand l'utilisateur tape une adresse dans cette zone et valide le formulaire, le proxy externe affiche la page.

**Question 18 (1 point)** *Pourquoi les proxys externes permettent de contourner le contrôle d'accès mis en place en interne ?*

**Question 19 (0.5 point)** *Pourquoi un proxy externe ne supporte-t'il pas les communications HTTPS ? Rappelons qu'HTTPS fournit la confidentialité et l'authentification.*

**Question 20 (0.5 point)** *Est-ce qu'un proxy externe peut sauvegarder les informations confidentielles (comme le mot de passe) que l'utilisateur utilise pour se connecter à des sites via ce proxy externe ?*