Examen de RE 202 : Réseaux

2h, documents de cours autorisés, aucun livre n'est autorisé.

Toutes les réponses aux exercices devront être justifiées. Il sera tenu compte de la clarté, des explications et de la présentation dans le barème final.

Exercice 1

Questions diverses réflexion / cours :

1. Comment le protocole IP peut-il faire pour estimer lui même le MTU d'un chemin ?
2. Quels sont les différents mécanismes qui rentrent en jeu (à tous niveaux) pour détecter et gérer la congestion sous TCP/IP ?
3. On s'accorde à dire que le protocole ARP n'est pas très sécurisé. Expliquez pourquoi. Proposez brièvement une solution qui permette d'éviter le piratage utilisant cette faiblesse.

Exercice 2

On utilise pour une transmission avec détection d'erreurs un Code de Redondance Cyclique (CRC) de polynôme générateur $x^4 + x + 1$. L'émetteur veut envoyer la suite 1101101101. Quelle suite va effectivement être envoyée dans le canal ?

Exercice 3

Dans cet exercice, on considère une carte réseau sans fil ayant un débit de 56 Mbits/s.

1. On estime que la vitesse de propagation dans l'air du signal émis par la carte réseaux est de 200000 km/s, et que la distance entre la station émettrice et la station réceptrice est de 2500m. Combien de bits l'émetteur émet avant que le récepteur ne reçoive le premier ?
2. Sur combien de mètres le codage d'un bit s'étale-t-il ?
3. Rappelez le principe du CSMA-CD. A votre avis, est-ce possible de l'utiliser tel quel dans le cadre des transmissions sans fil ? Justifiez.

Exercice 4

La trame suivante a été enregistrée avec la commande `tcpdump -XX`. On précise qu'ici il s'agit du protocole Ethernet.

```
0x0000:  0018 fe85 2580 000a 5e1f 51a3 0800 4500  ....%...^.Q...E.
0x0010:  0028 a635 4000 4006 e339 93d2 093c d8ef  .(.5@.@..9...<..
0x0020:  3b63 b9fd 0050 6b59 99d8 8040 e9e0 5010  ;c...PkY...@..P.
0x0030:  4e34 869e 0000                           N4....
```

Répondez en justifiant aux questions suivantes :

1. Quel est le protocole de niveau 3 (réseau) utilisé ?
2. Quelle est l'adresse IP de destination en notation décimale pointée ?
3. Quel est le protocole de niveau 4 (transport) utilisé ?
4. Quel est le port de la machine destinatrice ? Que peut-on en déduire ?

Indisponible (schema a rendre)

4. En respectant le masque de la question précédente, donnez un plan d'adressage de votre bâtiment, c'est à dire les adresses IP de toutes les machines et routeurs de la figure 1. Attention, n'oubliez pas de commencer par donner une adresse à chaque sous-réseau. Dans notre cas, il y a 5 sous-réseaux : celui correspondant à l'hôte A, celui de l'hôte B, celui de l'hôte C, le lien Routeur1/Routeur2, et enfin le lien Routeur1/Routeur3. Après avoir justifié vos choix, vous écrirez la réponse directement sur la figure. On rappelle que les cinq sous-réseaux doivent avoir le même masque (celui trouvé à la question précédente).
5. Pour chacun des cinq sous-réseaux, donnez l'adresse de diffusion.
6. Donnez la table de routage du routeur 3, ainsi que celle de l'hôte C.
7. Donnez les commandes permettant de configurer la table de routage de l'hôte C.
8. En supposant que le routeur 3 soit en fait une machine sous Unix, avec trois interfaces, donnez les commandes permettant de configurer sa table de routage.

Exercice 6

On rappelle que toutes les réponses doivent être justifiées. Il est fortement recommandé de lire l'énoncé en entier avant de commencer à répondre aux questions.

- Rappelez à quoi servent les numéros de séquences dans le protocole TCP. Vous insisterez sur le rôle des premiers numéros de séquences lors de l'ouverture d'une connexion TCP.
- Le déni de service (Deny Of Service ou DOS) est une attaque faite par une personne malveillante qui a pour but de faire tomber un service réseau contre la volonté du propriétaire de ce dernier. Les implémentations de TCP doivent être raisonnablement robustes contre le déni de service (DOS). Entre autres, ceci signifie que toutes les implémentations de TCP jettent régulièrement des paquets dont les numéros de séquences sont erronés. Selon vous, pourquoi ces paquets sont-ils ignorés ?
- Les numéros de séquence TCP sont des nombres de 32 bits. Ainsi, si un attaquant peut produire 2^{32} paquets, chacun avec une prévision différente pour le prochain numéro de séquence, l'attaquant serait assuré qu'un de ses paquets malveillants contiendrait le numéro de séquence correct. Une attaque en force brute vous semble-t-elle possible ? Donner des arguments concrets tels la bande passante nécessaire pour effectuer une attaque dans le pire des cas (tous les numéros de séquence doivent être envoyés).
- Les implémentations récentes de TCP génèrent les numéros de séquence de façon aléatoire. Pouvez-vous expliquer pourquoi ?

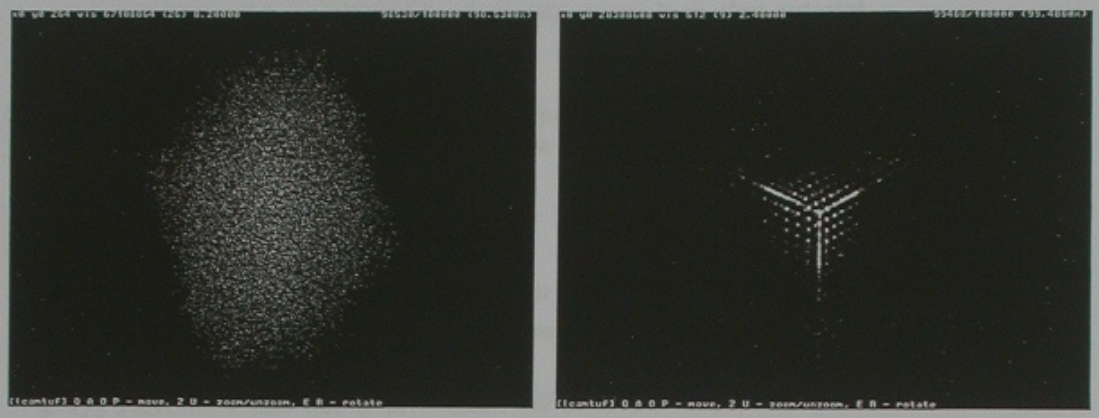
Une tentative d'usurpation prédéfinie est un ensemble de valeurs bien choisies selon certaines caractéristiques du générateur de numéro de séquence. Le but à atteindre est de faire suffisamment de prédictions "assez juste" pour pouvoir espérer toucher le "jack-pot" sans toutefois rendre l'échantillon de prédiction trop important.
La technique des "coordonnées différées" permet de représenter en trois dimensions une séquence de chiffres. Cette technique est couramment utilisée pour étudier les systèmes chaotiques. Pour utiliser cette technique on calcule des séquences de trois coordonnées par la formule suivante :

$$x[n] = s[n-2] - s[n-3]$$
$$y[n] = s[n-1] - s[n-2]$$
$$z[n] = s[n] - s[n-1]$$

où s identifie la liste de numéros de séquences que nous voulons étudier. La figure 2 présente les résultats obtenus pour *Windows 98*© et pour *Linux 2.2* respectivement.

- Intuitivement, lequel de ces deux systèmes vous semble le plus sûr face à une tentative d'usurpation de numéro de séquence ? Pourquoi ?

- Admettons que l'on puisse inonder une machine de paquets forgés avec des numéros de séquences de nos prédictions avec l'adresse IP d'une machine déjà connectée, puis que l'une d'entre elles corresponde au paquet attendu. Quel type de paquet TCP forgeriez vous afin de provoquer un déni de service ? (Pensez aux différents drapeaux TCP).
- Proposez une autre utilisation de l'analyse des numéros de séquences.



(a) linux (b) win98

FIG. 2 – Coordonnées différées obtenues à partir des numéros de séquences générés par linux (a) et Windows 98© (b).