Pablo Rauzy <pr@up8.edu>
https://pablo.rauzy.name/teaching/sr

Systèmes et réseaux

TP 5 : ICMP (`ping` et `traceroute`)

L'objectif de ce TP est de vous faire manipuler le protocole ICMP à travers les outils `ping` et `traceroute`.
Pour faire au plus simple, on se limite au support d'IPv4 uniquement (il n'y a que ça à Paris 8 de toutes façons).
N'hésitez pas à consulter les pages de manuel et le guide de Beej : `https://beej.us/guide/bgnet/`.
Répondez aux questions dans un fichier `reponses.txt`.

Exercice 0.

ICMP.

1. Le protocole ICMP fait parti de la suite de protocole fondamentaux d'Internet. Il se place au niveau de la couche 3 du modèle OSI, comme IP. Il sert à envoyer des messages, par exemple des messages d'erreur, qui ne sont pas pris en charge par le protocole IP directement.

   Les différents types de messages transmissibles par ICMP sont listés sur la page Wikipédia du protocole : `https://fr.wikipedia.org/wiki/Internet_Control_Message_Protocol`.

2. La commande `ping`, dont une version simplifiée vous est fournit avec ce TP, fait usage d'ICMP pour entre autre vérifier qu'un hôte lui répond. Pour cela, elle envoie un message de type `ECHO` et attends en retour un message de type `ECHOREPLY`.

   → Familiarisez avec la commande `ping` de votre système et consultez sa page de manuel.

3. La commande `traceroute`, dont vous allez produire une version simplifiée lors de ce TP, fait également usage d'ICMP. L'objectif de la commande `traceroute` est d'identifier le chemin que prennent les paquets pour arriver à une destination.

   → Familiarisez avec la commande `traceroute` de votre système et consultez sa page de manuel.

Exercice 1.

Analyse du code de ping.

1. La commande `ping` faisant usage de socket "raw", elle doit être exécutée en tant que root.

   → Vérifiez que vous pouvez bien compiler et exécuter le code.

2. → Comment se fait-il que la commande `ping` de votre système ne nécessite pas `sudo` ?

3. → Donnez la liste des fonctions et structures utilisées pour chaque entête inclus dans le fichier.
   Par exemple : `stdio.h: printf, fprintf, perror`

4. → Expliquez de manière détaillée le fonctionnement du programme, en faisant une analyse pas à pas de ce qui se passe et pourquoi dans les fonctions `main`, puis `send_echo_requests`, puis `listen_echo_replies`.

Exercice 2.

Implémentation d'un traceroute.

1. → Copiez le fichier `ping.c` vers un nouveau fichier `traceroute.c`, et remplacez dans le code du nouveau fichier l'affichage de "PING" par "TRACEROUTE TO" à la ligne 50.

2. La fonction `setsockopt` permet de modifier les options d'une socket.

   Cette fonction prend en argument :
   — la socket à manipuler,
   — le niveau auquel on veut toucher (le niveau IP est représenté par la constante `SOL_IP`),
   — le nom de l'option à changer (le temps de vie d'un paquet IP est représenté par la constante `IP_TTL`),
   — un pointeur vers la nouvelle valeur de l'option,
   — la taille de la valeur en question.
   Quand tout s'est bien passé, `setsockopt` renvoie 0, sinon une autre valeur.

   → Étant donné ces informations et ce que vous avez pu voir du protocole ICMP, quelle stratégie pouvez-vous utiliser pour mettre en œuvre traceroute ?

3. → Éditez le fichier `traceroute.c` pour mettre en œuvre cette stratégie. N'hésitez pas à ajouter des commentaires pour expliquer/justifier vos modifications. Pensez à tester votre code !