Réseaux 2
ping, traceroute, tracert et MyTraceRoute (mtr)

Nicolas Baudru, Nicolas Durand

Année 2011-2012 — 2e année IRM – ESIL

Exercice 1. Tester la présence et le bon fonctionnement d'une machine

Cette commande permet de tester l'acheminement des trames sur le réseaux et, accessoirement, de vérifier qu'une machine est bien présente sur le réseau. Elle permet aussi de réaliser des statistiques sur les temps de réponse ainsi que sur le pourcentage de paquets perdus. Pour cela, elle utilise le protocole ICMP en envoyant des messages (ICMP) de type "Demande d'ECHO" qui requière de la part de l'ICMP destinataire de répondre par un "Réponse d'ECHO".

Sur la plupart des systèmes, ping effectue plusieurs envois puis s'arrête en fournissant des statistiques sur le temps de propagation aller-retour (Round Trip Time) . Sur d'autres systèmes, il faut arrêter ping en tapant Ctrl-C. Ainsi, lorsqu'une réponse arrive, on est assuré que l'ordinateur qu'on utilise est correctement configuré, de même que l'ordinateur intérrogé, et que le réseau qui les sépare est opérationnel.

Consulter le manuel en ligne Linux de ping puis, à partir de votre machine, tester l'accessibilité et la présence :

1. de son interface loopback (une des adresses 127.x.y.z). Taper Ctrl-C pour arrêter la commande
2. de la machine d'un de vos camarades
3. d'une autre machine de votre réseau local, en précisant 10 tentatives
4. de toutes les stations du réseau local accessibles en broadcast (diffusion). Pour cela, préciser uniquement 2 tentatives.
5. du serveur orangead
6. de www.google.com. Quelle est son adresse IP ?

Exercice 2. Le cache ARP

1. Qu'est-ce que le cache ARP ? A quel moment est-il utilisé par la suite de protocoles TCP/IP ?
2. A l'aide de la commande arp, obtenir toutes les associations présentes dans le cache ARP de votre machine.
3. A l'aide de la commande arp, effacer le cache de votre machine (Certaines entrées sont réactualisées trop rapidement pour que l'effacement soit visible).
4. Effectuer maintenant quelques ping vers les machines des autres groupes tout en visualisant le cache ARP de votre station après chaque ping. Que s'est-il passé ?
5. Vider de nouveau le cache, puis envoyer un ping vers l'adresse IP 87.248.113.14 (celle de www.yahoo.com). Que s'est-il passé au niveau du cache ?
6. Que se passe-t-il au niveau du cache si vous envoyez un ping vers une adresse non joignable de votre réseau ?
7. A l'aide de la commande arp, retirer du cache les lignes correspondantes aux machines des autres groupes.
8. Ajouter une entrée comprenant l'adresse IP publique d'une machine d'un des autres groupes avec l'adresse MAC de votre machine. Cette nouvelle entrée est évidemment erronée. On appelle cela "corrompre le cache arp".
9. Tenter alors d'envoyer un ping vers la machine précédemment ajoutée dans le cache. Que se passe-t-il ? Vérifier votre hypothèse avec wireshark. Normalement, le ping a été détourné vers votre machine. Vous venez en fait de réaliser une attaque réseau connue sous le nom "arp cache poisoning".
10. Effacer de votre cache la ligne précédemment ajoutée. Effectuer de nouveau un ping vers la même machine que celle de la question précédente. Cela devrait marcher à nouveau.

Exercice 3. tracert, traceroute et mtr

Les commandes traceroute (sous Linux) et tracert (sous Windows) permettent de connaître la route que suivra un datagramme que vous enverrez vers une machine donnée. Elles permettent ainsi de savoir à quel endroit bloque la transmission d'un paquet que l'on tente d'envoyer sans succès (malheureusement, ça arrive).

Sous Windows : Après avoir consulter l'aide Windows de tracert, répondre aux questions suivantes :

1. Expliquer le fonctionnement général de tracert.
2. Indiquer la route permettant de contacter un serveur de votre réseau.
3. A l'aide de la commande tracert, indiquer la route permettant de contacter www.yahoo.com.
4. A l'aide du logiciel disponible en ligne à l'adresse http ://geotool.servehttp.com/ et des résultats obtenus à la question 2), déterminer le chemin parcouru par vos paquets IP lorsque vous contactez www.yahoo.com.
5. Reprendre la question 2) en demandant à ce que les cinq premiers routeurs n'apparaissent pas (il faut agir sur le TTL du premier datagramme envoyé par tracert).

Sous Linux :

6. Vérifier que la commande traceroute ne fonctionne pas correctement lorsque vous essayez de contacter un site distant comme www.yahoo.com .
7. A l'aide la commande mtr, indiquer la route permettant de contacter www.yahoo.com.
8. Reprendre la question 6) en demandant à ce que les cinq premiers routeurs n'apparaissent pas (il faut agir sur le TTL du premier datagramme envoyé par traceroute).
9. Recommencer la question 6) mais en utilsant cette fois-ci la commande traceroute, puis examiner les paquets UDP et IP envoyés et reçus à l'aide de wireshark.
10. Déterminer à l'aide de whireshark la différence entre les paquets envoyés par traceroute et ceux envoyés par mtr. En déduire pourquoi les paquets de traceroute sont filtrés alors que ceux de mtr ne le sont pas.
11. Vérifier votre hypothèse en consultant le manuel en ligne Linux de traceroute et mtr.