

TP : Configuration de réseau local sous Linux

Analyse de trafic

Le but de ce TP est d'utiliser les outils de base de configuration d'un réseau local sous Linux (Ubuntu)

1) Fixation du nom de la machine

- a. Regarder le manuel des différentes commandes suivante : `ifconfig`, `hostname`
- a. Quel est le nom actuel de votre machine
- b. Que contient le fichier `/etc/hostname`
- c. Changer le nom dans le fichier `/etc/hostname`
- d. Prendre en compte la modification en redémarrant le service

2) Interface réseau

- a. Pour avoir une documentation sur les interfaces faites : `man interfaces`
- b. Les informations relatives aux interfaces sont citées dans le fichier `/etc/network/interfaces` ou bien « `/etc/netplan/01-network-configuration.yaml` »
- c. Configurer l'adresse IP d'une façon automatique (DHCP)
- d. Configurer manuellement les interfaces
- e. Redémarrer le service réseau

3) Netstat

- a. Afficher les informations détaillées sur le réseau (affiche une liste des sockets ouverts)
- b. Utiliser les options de `netstat` (`-r`, `-t`, `-c`, `nr`, etc)
- c. Utiliser la commande `netstat -at`
- d. Quel est la passerelle par défaut

4) Traceroute

Il fournit des informations sur le nombre de routes présentes entre la source et la destination

- a. Tester `traceroute` www.google.com
- b. Quelle est la version de Traceroute
- c. Regarder d'autres options de `traceroute`

5) Créer votre réseau LAN

- a. Connectez-vous au même réseau LAN
- b. Tester l'interconnexion en utilisant `ping`

- c. Ajouter une passerelle vers un réseau
- d. Vérifier la mise à jour de la table de routage
- e. Configurer le fichier /etc/hosts
- f. Configurer le fichier de mise à jour de DNS (/etc/resolv.conf)
- g. Supprimer le serveur DNS
- h. Tester ping 8.8.8.8
- i. Tester ping www.google.com
- j. Conclure

6) Wireshark

- a. Télécharger et installer Wireshark Démarrez Wireshark. Accédez au menu Capture - Options.
- b. Cliquez sur la ligne correspondant à l'interface Ethernet. Déclenchez une capture de trames en cliquant sur Démarrer :Faites un ping vers 8.8.8.8
- c. Après quelques secondes, arrêtez la capture.
- d. Tapez dans Filter le mot icmp (Internet Control Message Protocol)
- e. Développez les informations relatives au protocole icmp.
- f. Un ping correspond à deux trames : *Echo request* (aller) et *Echo reply* (retour).
- g. Quelle est la version de IP
- h. Quelle est la taille l'en-tête IP ?
- i. Quelle est la valeur du champ TTL de l'en-tête IP ? Justifiez votre réponse.
- j. Quel est le protocole de niveau supérieur ? Par quelle valeur est-il identifié ?