Atelier1 - Configuration réseau

Exercice1 : La commande ping

La commande ***ping*** teste la présence d'un hôte distant. Cette commande est à la fois très simple et très utile.

Son principe est trivial : la commande envoie des données dans des messages ICMP « echo request » que le système distant renvoie à l'intérieur de messages ICMP « echo reply ». La commande envoie plusieurs paquets et teste l'égalité entre les données envoyées et les données reçues. Elle peut donc détecter non seulement l'absence du poste distant mais également une mauvaise transmission et par conséquent mesure la qualité du réseau.

La commande mesure le temps de transit et l'ordre d'arrivée des paquets. Des paquets qui reviennent dans le désordre et qui mettent longtemps à revenir ou qui sont simplement perdus, mettent en évidence une charge du réseau.

Syntaxe : ***ping [parametres] host***

- ✓ **-c** count Spécifie le nombre de paquets à émettre.
- ✓ **-b** Autorise à spécifier une adresse de diffusion.
- ✓ **-M do** Positionne le bit «Don't fragment ».
- ✓ **-f** Mode « flood » : on émet les paquets aussi vite qu'on reçoit les réponses ou au moins 100 par seconde. Ce mode est réservé à **root**.
- ✓ **-l** preload Essaye d'envoyer le plus de paquets possible avant de fonctionner normalement. Ce mode est réservé à **root**.
- ✓ **-I** ifaddr Spécifie par quelle interface le paquet est émis.
- ✓ **-i** wait On spécifie l'intervalle de temps entre deux émissions de paquets.
- ✓ **-n** Affichage numérique, pas de résolution DNS-inverse.
- ✓ **-s** size Spécifie la taille des données.
- ✓ **-p** pattern Spécifie un modèle (en hexadécimal) pour remplir le paquet.
- ✓ **-q** Mode silencieux.
- ✓ **-R** Enregistre la route. Toutes les passerelles ne suivent pas cette injonction.
- ✓ **-r** Envoie directement un paquet sans utiliser les tables de routage (certaines routes pouvant être désactivées).
- ✓ **-t** ttl Spécifie le ttl.
- ✓ **-Q** tos
- ✓ **-T** tos Spécifient le TOS.
- ✓ **-v** Mode verbeux. Les paquets ICMP reçus différents de echo-reponse sont affichés.
- ✓ **-w** maxwait Selon la version, ce paramètre indique le temps d'attente d'une réponse avant d'envoyer le paquet suivant ou bien, le paramètre précise la durée d'exécution de la commande.

Exemple : ping 41.229.121.1 (Utilisation de l'adresse IP pour spécifier la cible).

1. Émettez un seul ping vers l'adresse du serveur google.com.
2. En utilisant la commande **echo $?** vérifiez le code retour de la commande ping sachant que Le code retour 0 indique que la machine distante a répondu.
3. Ecrire un script shell **verifhost** qui permet de vérifier l'état de la connexion d'une machine distante sur le réseau (tester si la machine répond, et si non de sortir du programme avec un message d'erreur).

Exercice 2 : La commande ifconfig

La commande ***ifconfig*** permet la configuration locale ou à distance des interfaces réseau de tous types d'équipements (unité centrale, routeur). Sans paramètres, la commande ifconfig permet d'afficher les paramètres réseau des interfaces.

Syntaxe : *ifconfig interface adresse [parametres].*

Exemple : *ifconfig* eth0 192.168.1.2 (affecte l'adresse 192.168.1.2 à la première interface physique).

Les principaux arguments utilisés :

- ✓ ***Interface :*** logique ou physique, il est obligatoire,
- ✓ **up :** active l'interface
- ✓ ***down*** : désactive l'interface
- ✓ ***mtu*** : définit l'unité de transfert des paquets
- ✓ ***netmask*** : affecter un masque de sous-réseau
- ✓ **broadcast** : définit l'adresse de broadcast
- ✓ ***arp*** ou ***-arp*** : activer ou désactiver l'utilisation du cache arp de l'interface
- ✓ ***metric*** : paramètre utilisé pour l'établissement des routes dynamiques, et déterminer le " coût " (nombre de sauts ou " hops ") d'un chemin par le protocole RIP.
- ✓ ***multicast*** : active ou non la communication avec des machines qui sont hors du réseau.
- ✓ ***promisc*** ou ***-promisc*** : activer ou désactiver le mode promiscuité de l'interface. En mode promiscuous, tous les paquets qui transitent sur le réseau sont reçus également par l'interface. Cela permet de mettre en place un analyseur de trame ou de protocole.

Description du résultat de la commande ***ifconfig eth0*** :

```
1   eth0 Link encap:Ethernet HWaddr 00:80:C8:32:C8:1E
2   inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
3   UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
4   RX packets:864 errors:0 dropped:0 overruns:0 frame:0
5   TX packets:654 errors:0 dropped:0 overruns:0 carrier:0
6   collisions:0
7   Interrupt:10 Base address:0x6100
```

Explications :

Ligne 1: l'interface est de type Ethernet. La commande nous donne l'adresse MAC de l'interface.

Ligne 2 : on a l'adresse IP celle de broadcast, celle du masque de sous-réseau

Ligne 3 : l'interface est active (UP), les modes broadcast et multicast le sont également, le MTU (Message Transfert Unit détermine l'unité de transfert des paquets) est de 1500 octets, le Metric de 1

Ligne 4 et 5 : RX (paquets reçus), TX (transmis), erreurs, suppressions, engorgements, collision

1. Relevez le nombre total d'interfaces (logique et physique) de votre machine à l'aide de la commande **ifconfig**.
2. Tapez la commande suivante ***ifconfig eth0*** et veuillez compléter le tableau suivant :

Adresse MAC	……
Adresse IP de la machine	……
Masque de sous-réseau	……
Adresse IP de broadcast	……
Etat de l'interface (activé ou non)	……
Mode broadcast (activé ou non)	……
Modes multicast (activé ou non)	……
MTU (octets)	……
Metric	……
Paquets reçus	……
Paquets transmis	……

3. Désactivez les 2 interfaces **lo** et **eth0**.
4. Tapez les commandes suivantes et expliquer les résultats obtenus.

```
ping localhost
ping 41.229.121.1
telnet localhost
```

5. Activez l'interface de loopback et retaper les commandes précédentes de nouveau. Expliquez ?
6. Affecter l'adresse IP 10.0.2.20 et le masque de sous-réseau 255.255.255.0 à la première interface physique eth0.
7. Tapez la commande **ping 10.0.2.2** et expliquer les résultats obtenus.
8. Tapez la commande **ping google.com** et expliquer les résultats obtenus.
9. Tapez la commande **route add default gw 10.0..2.2** pour ajouter l'adresse de la passerelle par défaut.
10. Tapez la commande **ping google.com** et expliquer les résultats obtenus.
11. Modifier le MTU par défaut à 1500, pour le mettre à 300.

Exercice 3 : La commande arp

La commande ***arp*** permet de visualiser ou modifier la table du cache arp de l'interface. Cette table peut être statique et (ou) dynamique. Elle donne la correspondance entre une adresse IP et une adresse **MAC** (Ethernet).

Syntaxe : ***arp [parametres].***

- ✓ -a : Affiche les tables en cours du cache ARP de toutes les interfaces.
- ✓ -d : Supprime une entrée correspondant à une adresse IP spécifique.
- ✓ -s : Ajoute dans le cache ARP une entrée statique qui résout l'adresse IP en l'adresse physique.

1. Affichez le contenu de la table ARP avec la commande **arp –a.**
2. Supprimez chaque ligne avec la commande **arp -d @ip**, où @ip est l'adresse IP de chaque hôte apparaissant dans la table.
3. Vérifier que la commande **arp -a** ne devrait plus afficher de ligne.
4. Faites un **ping**, sur une station du réseau local 10.0.2.2.
5. Tapez la arp **–a** et expliquer les résultats obtenus.
6. Ouvrez une session ftp anonyme sur un serveur distant en utilisant la commande **ftp ftp.cdrom.com.**
7. Affichez le nouveau contenu de la table avec **arp -a**. Le cache ARP contient-il l'adresse Ethernet du site distant ? Expliquer les résultats obtenus.

Exercice 4 : La commande route

La commande **route** a déjà été entrevue un peu plus haut, avec la commande **ifconfig**. Le routage définit le chemin emprunté par les paquets entre son point de départ et son point d'arrivée.

Il existe deux types de routages :

- le routage statique : consiste à imposer aux paquets la route à suivre.

- le routage dynamique : met en œuvre des algorithmes, qui permettent aux routeurs d'ajuster les tables de routage en fonction de leur connaissance de la topologie du réseau.

Exemple de table de routage :

```
Kernel IP routing table
Destination Gateway Genmask    Flags  Metric  Ref Use  Iface
192.168.1.0    *  255.255.255.0 U      0       0   2    eth0
127.0.0.0      *  255.0.0.0     U      0       0   2    lo
default  192.168.1.9 0.0.0.0    UG     0       0   10   eth0
```

- ✓ **Destination** : adresse de destination de la route
- ✓ **Gateway** : adresse IP de la passerelle pour atteindre la route, * sinon
- ✓ **Genmask** : masque à utiliser.
- ✓ **Flags** : indicateur d'état (U - Up, H - Host - G - Gateway, D - Dynamic, M - Modified)
- ✓ **Metric** : coût métrique de la route (0 par défaut)
- ✓ **Ref** : nombre de routes qui dépendent de celle-ci
- ✓ **Use** : nombre d'utilisation dans la table de routage
- ✓ **Iface** : interface eth0, eth1, lo

Syntaxe : ***route add [net | host] addr [gw passerelle] [métric coût] [netmask masque] [dev interface]***

- ✓ ***-net*** ou ***-host***: indique l'adresse de réseau ou de l'hôte pour lequel on établit une route
- ✓ **add :** ajoute une route.
- ✓ **del :** supprime une route.
- ✓ ***gw :*** adresse de la passerelle,
- ✓ ***métric :*** valeur métrique de la route,
- ✓ ***netmask :*** masque de la route à ajouter,
- ✓ ***dev :*** interface réseau à qui on associe la route.
- ✓ **-n :** Affiche les adresses numériques, au lieu d'essayer de déterminer les noms d'hôtes.

Exemple : ***route add default gw 192.168.1.254 eth0*** (ajoute une route par défaut pour la machine sur l'interface eth0 avec l'adresse IP 192.168.1.254).

1. Afficher votre table de routage avec des adresses numériques.
2. Veuillez compléter le tableau suivant :

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
……	……	……	…….	…….	…….	…….	…….
……	……	……	…….	…….	…….	…….	…….

3. Quel est l'adresse IP de votre passerelle par défaut ?
4. Taper ping 41.229.121.1 et vérifier si le réseau 41.229.121.0/8 existe ou non dans votre table de routage. Expliquer les résultats obtenus.
5. Supprimer la route par défaut en utilisant la commande route.

Exercice 5 : La commande netstat

La commande ***netstat***, permet de tester la configuration du réseau, visualiser l'état des connexions, établir des statistiques, notamment pour surveiller les serveurs.

Liste des paramètres utilisables avec ***netstat*** :

- ✓ Sans argument, donne l'état des connexions,
- ✓ **-a** : afficher toutes les informations sur l'état des connexions,
- ✓ **-i** : affichage des statistiques,
- ✓ **-c** : rafraîchissement périodique de l'état du réseau,
- ✓ **-n** : affichage des informations en mode numérique sur l'état des connexions,
- ✓ **-r** : affichage des tables de routage,
- ✓ **-t** : informations sur les sockets TCP
- ✓ **-u** : informations sur les sockets UDP.

1. Afficher votre table de routage en utilisant la commande **netstat**.
2. Si vous rajoutez le paramètre -**ei**, le résultat que vous obtiendrez est-il le même que celui de la commande **ifconfig –a** ?
3. Le paramètre **-a** permet de visualiser toutes les connexions, pour tous les protocoles, y compris les ports en écoute de la machine. Tapez la commande **netsat –a | wc –l** et expliquer les résultats obtenus.
4. Comparer le résultat obtenu des deux paramètres **–at** et **–au**.
5. Tapez la commande netstat –s qui permet d'afficher des statistiques. Donner le nombre total des paquets ICMP reçus.

Exercice 6 : La commande traceroute

La commande **traceroute** permet de visualiser chacun des points de passage (routeur) de vos paquets IP à destination d'un hôte donné.

1. Installer **traceroute** en utilisant la commande : **sudo apt-get install traceroute.**
2. Tapez la commande **sudo traceroute –I www.google.com.**
    a. Quel est le nombre total des routes empruntées pour se rendre sur le serveur google.
    b. Déterminer l'adresse ip du serveur google.

Exercice 7 : La commande iptraf

La commande **iptraf** permet de visualiser en temps réel l'activité du réseau via un outil texte interactif ou non (ligne de commande).

1. Installer **iptraf** en utilisant la commande : **sudo apt-get install iptraf.**
2. Tapez la commande **sudo iptraf -d eth0** pour visualiser l'affichage détaillé des statistiques de trafic de la carte eth0. (ctrl +X pour quitter)

Exercice 8 : La commande nmap

Nmap est un scanner de ports libre. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant.

1. Installer **nmap** en utilisant la commande : **sudo apt-get install nmap.**
2. Déterminer les ports réseau ouverts TCP/UDP sur votre machine en utilisant la commande : **sudo nmap 127.0.0.1.** Si vous souhaitez scanner un port en particulier, vous pouvez utilisez l'option **–p.**
3. Identifier toutes les machines présentes sur votre réseau comprises entre 10.0.2.1 et 10.0.2.20, en utilisant la commande : **sudo nmap –sP 10.0.2.1-20**