

Objectifs : Maîtriser les commandes basiques de gestion du réseau

Notions abordées : Commandes réseau de Linux : ip, route, ping, dns, traceroute, whois, tcpdump, wireshark, etc.

Les commandes sont à exécuter depuis un serveur de l'IUT (connexion en SSH ou bureau à distance). Cependant, il est intéressant d'exécuter les mêmes commandes depuis votre environnement personnel et de comparer les résultats.

N'hésitez pas, tout au long du TP et pour ceux qui disposent d'une machine avec des droits d'administrateur, à utiliser un logiciel de capture de trame comme `wireshark` (interface graphique) et/ou `tcpdump` (pour le scripting). Regardez le contenu des trames à chaque niveau d'encapsulation.

Pour chaque commande étudiée, consultez sa page de manuel (commande `man` ou option `--help`).

1 Commande ping

Question 1 - Testez avec un navigateur web si vous parvenez à accéder aux sites suivants. Lesquels, parmi ces serveurs, répondent à la commande `ping`?

- `www.unistra.fr`
- `web.mit.edu`
- `www.dgse.gouv.fr`
- `www.hoola.hp`

Question 2 - Lequel de ces domaines répond le plus rapidement?

- `encrypted.google.com`
- `www.baidu.com`
- `yandex.ru`

2 Commande traceroute

La commande `traceroute` permet de visualiser le chemin emprunté par un paquet à travers le réseau en envoyant un `ping` sur chaque nœud jusqu'à la destination, en utilisant un TTL décroissant.

Question 3 - Effectuez un `traceroute` vers la machine `phoenix.u-strasbg.fr`. Combien de passerelles (ou routeurs) sont traversées? Pourquoi?

Question 4 - Même question pour la machine `lactu.unistra.fr`. Pouvez-vous en déduire son emplacement physique?

Question 5 - Observez le résultat de la commande vers `www.renater.fr`.

Question 6 - Combien de routeurs se trouvent entre votre machine et celle hébergeant le site `washington.edu`?

Question 7 - À quel moment traverse-t-on l'Atlantique? Utilisez <https://fr.geoipview.com/> pour vérifier la localisation des routeurs.

Question 8 - Le site `www.traceroute.org` propose une liste de serveurs distribués dans le monde et depuis lesquels il est possible d'initier un `traceroute` vers un autre hôte de l'internet. Pour un serveur donné, comparez les résultats d'un `traceroute` depuis votre machine vers ce serveur ou depuis ce serveur vers votre machine. Que remarquez-vous?

Utilisez par exemple `noc.thunderworx.net` (Chypre) ou `www.terra-byte.com` (Canada).

3 Configuration IP

Pour rejoindre un réseau et exister sur internet, il faut une adresse IP et implémenter TCP et/ou UDP au minimum... Avant de communiquer sur le réseau, il faut donc configurer la machine hôte pour qu'elle le rejoigne, soit manuellement avec la commande `ip`, soit automatiquement à l'aide du protocole DHCP par exemple.

La commande `ip`

`ip` est une commande fournie par le paquet `iproute2`. Elle contient un ensemble de sous-commandes pour manipuler le réseau sur une machine Linux avec une distribution récente.

`ip link`

La sous-commande `ip link` permet de configurer les interfaces. L'action par défaut d'une sous-commande est `show`. Les trois commandes suivantes sont identiques :

- `ip link show`
- `ip link`
- `ip l`

Question 9 - Quel est le nom de votre interface Ethernet ? Son adresse MAC ?

Question 10 - À quoi correspond l'interface `lo` ?

Une interface s'allume et s'éteint de la manière suivante :

```
| sudo ip link set <interface> up  
| sudo ip link set <interface> down
```

Il est même possible d'utiliser `ip link` pour changer *logiciellement* son adresse MAC (à condition que l'interface soit éteinte) :

```
| sudo ip link set <interface> address <MAC>
```

`ip addr`

`ip addr` permet d'attribuer les adresses IP aux interfaces. Nous verrons cette commande plus en détail au prochain TP.

Question 11 - Quelle est l'adresse IPv4 de votre interface Ethernet ? IPv6 ?

Question 12 - Quelle est l'adresse IPv4 de l'interface de *loopback* ?

Question 13 - Pour les étudiants ayant un ordinateur portable, connectez-vous sur Osiris puis sur Eduroam. Comparez les adresses IP de votre interface.

`ip route`

`ip route` sert à manipuler la table de routage du noyau Linux. Nous verrons cette commande plus en détail au dernier TP.

Question 14 - Affichez simplement la table de routage et trouvez quelle est l'adresse IP de votre passerelle ? Donnez aussi l'adresse du réseau et son masque ainsi que l'adresse de broadcast dans ce réseau.

`ip neigh`

Le cache ARP permet de stocker les associations entre adresse MAC (niveau 2) et adresse IP (niveau 3). Ce cache est mis à jour par le noyau et est consultable via la commande `ip neigh`.

Question 15 - Quelle est l'adresse MAC de votre passerelle ? Est-il possible d'obtenir l'adresse MAC d'un routeur ?

Question 16 - Faites un ping vers une autre machine de la salle qui n'est pas actuellement dans le cache ARP puis constatez que la table a bien été mise à jour.

Attention : Les questions suivantes ne sont réalisables que sur une machine avec un compte administrateur.

Videz votre cache ARP :

```
| sudo ip -s neigh flush all
```

Puis faites une requête ping vers une destination quelconque. Cette action aura pour effet de remplir le cache.

Question 17 - Décrivez tous les échanges de trames ARP qui ont eu lieu pour remplir ce cache.

Le service DHCP

Question 18 - Observez le contenu du fichier `/etc/resolv.conf`. Que contient-il?

La commande nslookup

Les serveurs de noms (DNS) assurent la traduction de noms de sites distants en adresses IP. Pour effectuer des requêtes sur le serveur DNS, il faut utiliser la commande `nslookup`.

Question 19 - Quel est le nom du serveur `130.79.192.134`?

Question 20 - Quelle est l'adresse IP du site de Google? Lancez plusieurs fois la commande. Pourquoi obtenez-vous des réponses différentes?

Cas particulier : *loopback*

Question 21 - Exécutez un `nslookup` sur l'adresse `127.0.0.1`. Quel est le nom associé à cette adresse? Qu'est-ce que cela signifie?

4 La commande netstat

Question 22 - Affichez, grâce à la commande `netstat`, les connexions TCP actuellement actives depuis votre machine. Initiez une connexion `ssh` vers un serveur de l'IUT. Quelles sont les connexions TCP maintenant actives?

5 Renater et Geant

Actuellement, vous accédez à l'internet via le réseau Renater (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche) et le réseau Geant. Les pages suivantes vous fournissent des informations sur ces réseaux, parcourez-les afin de comprendre leur architecture et leur fonctionnement :

- <https://www.renater.fr/reseau>
- <https://www.renater.fr/fr/geant>
- <http://pasillo.renater.fr/weathermap>
- <https://osiris.unistra.fr/osiris/infra>
- <https://osiris.unistra.fr/osiris/ipv6/>
- carte mondiale GEANT

Question 23 - Quelles sont les bandes passantes types pour ces différents réseaux (au niveau régional, national, international)?

Question 24 - Trouvez le débit actuel vers l'île de Mayotte sur le réseau Renater.

Question 25 - Que sont les GIX?

Question 26 - Testez la commande `traceroute` vers une université européenne et essayez de voir les correspondances entre le résultat et la topologie du réseau.

6 Adresses IP

Question 27 - Écrivez une commande `addnet` en langage C permettant d'afficher, à partir d'une adresse IPv4 et un masque de sous-réseau, la classe du réseau, l'adresse du réseau, l'adresse de la station, l'adresse de broadcast et le nombre de machines adressables dans le sous-réseau.

Pour vérifier vos calculs, vous pouvez vous aider de cet outil : [calculateur CRIC](#).

Exemple :

```
| # addnet 130.79.81.129/23
```

| Classe B
| adresse du réseau : 130.79.80.0
| adresse du broadcast : 130.79.81.255
| adresse de la station : 0.0.1.129
| nombre de machines : 510