TD 1

L'objectif de ce td est de se familiariser avec les commandes réseaux du système d'exploitation. Ces outils sont particulièrement utiles lorsque nous souhaitons vérifier les paramètres réseaux d'un ordinateur, d'un serveur ou d'un site web.

Le Ping est un outil d'administration de réseau accessible depuis **la fenêtre d'invite de commande Windows**. Dans le cadre de l'administration de réseau, cette ligne de commande permet de vérifier la disponibilité d'un autre ordinateur dans un réseau local associé ou dans un réseau public.
La commande ping est lancée au moyen de la commande du même nom, associée soit à **l'adresse IP** de l'ordinateur-cible, soit à **son nom d'hôte**. Si l'ordinateur-cible ne se trouve pas dans le même réseau local que l'ordinateur-source, vous devez en plus préciser le domaine.

1. Dans un premier temps ,nous devons vérifier si notre carte réseau fonctionne.
   Pour cela vous devez faire un ping sur l'adresse local de l'ordinateur : 127.0.0.1
   Dans un invité de commande, saisissez la commande suivante :

   ping 127.0.0.1
   ping localhost

2. Vérifiez que la connexion Internet fonctionne en faisant un ping sur google.Fr

3. Sur chaque pc, vous avez accès à un fichier **hosts**. Il sert à faire le mapping entre les adresses IP et les noms d'hosts.
   Sous Windows il est présent dans : *C:\Windows\System32\drivers\etc*
   Sous Linux il est présent dans : */etc/*
   Ouvrez le fichier **hosts** avec un éditeur de texte.

4. Dans ce même répertoire, vous trouverez un fichier **networks**. Ce fichier permet d'associer des noms de réseaux aux adresses des réseaux.
   Ouvrez le fichier **networks** avec un éditeur de texte.

5. Dans ce même répertoire, vous trouverez un fichier **services**.Ce fichier contient les numéros et les protocoles de l'ensemble des services Web fournis par l'IANA.
   Ouvrez le fichier **services** avec un éditeur de texte.

IANA

Pour appeler une page Internet précise, il est nécessaire de saisir le nom de domaine correspondant dans le navigateur. Le nom est acheminé vers un serveur qui le traduit alors en adresse IP et vous achemine vers le site Internet. Ces noms et numéros, appelés identificateurs uniques, sont comparés à un ensemble normalisé de paramètres du protocole Internet pour permettre la communication entre ordinateurs. Une des tâches de l'Internet Assigned Numbers Authority (IANA) est de gérer ces identificateurs uniques. Cependant, l'IANA assume également d'autres tâches dans l'administration du Web.

Qu'est-ce que l'IANA ?

L'Internet Assigned Numbers Authority a un rôle administratif important à jouer. Il est en effet responsable de l'allocation des noms uniques et des systèmes de numérotation, qui sont attribués conformément aux normes techniques comme le protocole réseau et constituent la base de l'adressage des pages Web. Bien qu'Internet ne soit pas un réseau géré de manière centralisée, certains éléments essentiels doivent cependant être coordonnés au niveau mondial en raison de contraintes techniques. L'IANA s'est déjà chargé de cette tâche pour le prédécesseur du Web actuel. Cela en fait ainsi l'une des plus anciennes institutions de l'Internet.

De ARPANET à Internet : l'histoire de l'IANA

À l'origine, les tâches de l'IANA étaient assumées par une seule personne : Jon Postel. En 1972, Postel, alors étudiant à l'Université de Californie à Los Angeles (UCLA), propose de créer une administration pour la gestion des numéros de sockets du tout nouvellement développé ARPANET. Bien que le prédécesseur d'Internet d'aujourd'hui soit relativement clair, il fallait toutefois s'assurer que les mêmes numéros de sockets ne soient pas utilisés pour des applications différentes. J. Postel s'est donc chargé lui-même de cette tâche et a ainsi préparé un catalogue adéquat.

Note

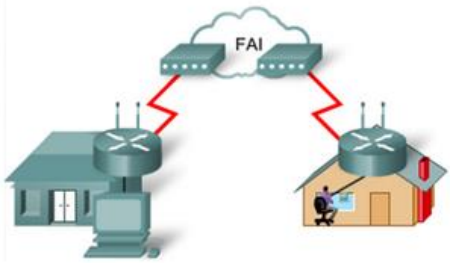
*un **socket** est la combinaison de l'adresse IP et du numéro de port. Il est utilisé pour adresser une application particulière sur un ordinateur particulier. L'adresse IP détermine le réseau et l'ordinateur, le numéro de port de l'application respective.*

6. Maintenant , il est nécessaire de vérifier si notre poste est en réseau.
   Pour cela , il faut lancer l'invité de commande.
   Dans un invité de commande, saisissez la commande suivante :
   ipconfig /all

Le système doit vous afficher :

- **l'adresse IP**
- **l'adresse MAC**
- **le masque de sous-réseau**
- **la passerelle**
- **L'adresse Ip du serveur DHCP**
- **L'adresse Ip du serveur DNS et si netbios est activé.**

7. La passerelle permet de sortir du réseau local pour accéder à internet.
   A l'aide de la commande **ping**, saisissez la commande suivante :
   ping @ip passerelle



Lorsqu'un ordinateur émet un message vers un ordinateur situé sur un réseau différent, il transmet le message à "son" routeur (dit passerelle par défaut), qui à son tour le fait suivre à un autre routeur et ainsi de suite jusqu'à atteindre l'hôte de destination.
Que ce soit l'ordinateur émetteur ou tous les routeurs intermédiaires, tous consultent leur table de routage pour savoir à qui transmettre le paquet afin d'atteindre la cible.
Table de routage :

```
C:\Users\sen>route print
===========================================================================
Liste d'Interfaces
 11...74 f0 6d 5d da 16 ......Atheros AR2427 Wireless Network Adapter
 10...20 cf 30 6d 50 c1 ......Atheros AR8132 PCI-E Fast Ethernet Controller (N
S 6.20)
  1...........................Software Loopback Interface 1
 14...00 00 00 00 00 00 00 e0 Carte Microsoft ISATAP
 13...00 00 00 00 00 00 00 e0 Carte Microsoft ISATAP #2
 12...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
===========================================================================

IPv4 Table de routage
===========================================================================
Itinéraires actifs :
Destination réseau    Masque réseau  Adr. passerelle   Adr. interface Métrique
          0.0.0.0          0.0.0.0    192.168.8.254     192.168.8.16     20
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    306
      192.168.8.0    255.255.255.0         On-link      192.168.8.16    276
     192.168.8.16  255.255.255.255         On-link      192.168.8.16    276
    192.168.8.255  255.255.255.255         On-link      192.168.8.16    276
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link      192.168.8.16    276
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link      192.168.8.16    276
===========================================================================
Itinéraires persistants :
  Aucun
```

Cette table peut se décomposer de la manière suivante :

- Destination : Plage d'adresse de destination déterminée par le couple Destination réseau / Masque réseau
- Adresse passerelle : Adresse du routeur qui permet d'atteindre le réseau de destination.
- Adresse interface : Carte réseau à utiliser pour contacter le routeur mentionné dans "Adresse passerelle".
- Métrique : Indique le coût relatif de l'itinéraire pour atteindre la destination.Cela peut correspondre aux nombre de sauts IP, ou un cout numérique qui dépend de la bande passante des liens franchis.

8. Exécuter la commande **route print** dans l'invité de commande.

DNS

Le Domain Name System (DNS) joue un rôle essentiel dans le succès d'Internet et du World Wide Web puisqu'il sert de service de répertoire central pour les adresses réseau. Le **réseau de serveurs DNS** (également appelé serveurs de noms) **répartis dans le monde entier** garantit que les noms des différents **utilisateurs du réseau et des applications réseau** comme *example.org* soient détaillés dans les adresses IP qui se basent sur des chiffres lisibles par l'ordinateur (et vice versa). Ceci permet d'être toujours sûr d'atteindre le bon ordinateur ou le site Web désiré, même sans connaissance de l'IP réelle.
Cependant, dans certaines situations (en cas de problèmes de résolution de noms par exemple), il peut être judicieux de regarder derrière les coulisses et de rechercher l'**adresse IP pour un nom de domaine** ou le **nom de domaine pour une adresse IP**. Pour ce faire, le programme nslookup, installé par défaut sous Windows, macOS et Linux, est un outil utile.
nslookup est un outil en ligne de commande simple mais très pratique qui est principalement utilisé pour trouver l'**adresse IP** d'un hôte spécifique ou le nom de domaine d'une adresse IP spécifique (recherche DNS inverse). nslookup peut être exécuté dans l'interface en ligne de commande du système d'exploitation utilisé. Les utilisateurs de Windows démarrent le service à partir de l'**invite de commandes**, les utilisateurs Unix à partir du **terminal**. De plus, il existe aujourd'hui un certain nombre de services Web qui permettent d'utiliser nslookup en ligne.

Comment fonctionne nslookup?
Pour utiliser nslookup sur Mac, Windows ou Linux, ouvrez la ligne de commande du système d'exploitation respectif. Vous retrouvez alors les deux modes déjà brièvement énumérés pour l'utilisation de l'outil DNS à vos propres fins :

- **Mode interactif** : démarrez nslookup avec la commande du même nom puis ajoutez les paramètres **séparément**

- **Mode non interactif** : entrez **directement** la commande nslookup et les paramètres désirés

9. Tapez la commande **nslookup** dans un invité de commande .Puis tapez la commande « help ».

Si une « **réponse non autorisée** » a été retournée, le serveur DNS local ne pouvait pas répondre lui-même à la requête, mais devait contacter un ou plusieurs autres serveurs de noms. Les contenus de la réponse nslookup sont les adresses IPv4 (quatre chiffres) et IPv6 (plus longues, séparées par deux points) du domaine d'exemple.

Le type de requête souhaité est saisi sous « TYPE D'ADRESSE », :
`set type=ADRESSTYP`

où les types suivants peuvent entre autres être utilisés :

Paramètres nslookup	Type de requête
A	Adresse IPv4
AAAA	Adresse IPv6
MX	Nom(s) de domaine du serveur de messagerie (Mail Exchanger)
NS	Serveur de nom de domaine
PTR	Requête « Pointer » (affiche le(s) nom(s) d'hôte sur une adresse IP)
SOA	Requête « Start of Authority » (informations sur la gestion de la zone DNS)

Par défaut, nslookup contacte le serveur DNS local, qui est généralement fourni par le **routeur** ou le **fournisseur d'accès Internet**. Cependant, si vous l'utilisez pour la requête, il est possible que les résultats ne soient pas toujours exacts car le serveur que vous recherchez n'est pas répertorié dans le **cache du serveur de noms local**, par exemple. Cependant, l'outil en ligne de commande vous permet de sélectionner le serveur DNS sur lequel la requête doit être exécutée. Si vous prenez le serveur qui est lié au domaine correspondant, vous obtenez même des **réponses d'autorisation**. La première étape consiste à **trouver le(s) serveur(s) de noms attribué(s)** en définissant le **type de requête« NS »** et en affichant cette entrée DNS en entrant le nom de domaine :

```
  set type=NS
  lamy.mobi
Reponse ne faisant pas authorité :

lamy.mobi       nameserver = ns100.ovh.net
lamy.mobi       nameserver = dns100.ovh.net
```

10. Faites une recherche de serveur DNS pour le domaine leboncoin.fr afin de récupérer l'adresse du serveur dns du domaine leboncoin.fr

L'un des deux serveurs de noms présentés doit maintenant être **défini comme serveur par défaut** pour que les requêtes s'exécutent à l'avenir. La commande correspondante se compose du **paramètre « serveur »** et **du nom du serveur souhaité**. Ces deux commandes sont possibles pour l'exemple nslookup choisi :

```
server ns100.ovh.net
```

Lors de la dernière étape, l'utilisateur change le type de requête, qui est toujours configuré pour la recherche par serveur de noms, par la requête d'adresse désirée telle que « A » pour le domaine, « MX » pour le contrôle IP du serveur de messagerie ou « ANY » pour un contrôle complet (utilisé ici) :

```
set type=ANY
```

11. Entrez à nouveau leboncoin.fr pour lancer la requête, nslookup fournit des informations DNS détaillées sur le domaine , le serveur de noms sélectionné comme serveur par défaut (serveur dns leboncoin) servant de source d'information .

12. Saisissez l'adresse IP (TYPE A) dans votre navigateur.

13. Identifiez les serveurs de messagerie (TYPE MX).

14. Chez quel hébergeur est stocké le site leboncoin.fr ?

15. Faites la même chose pour les domaines suivants :
    1. Education.gouv.fr
    2. Elysee.fr
    3. Nasa.gov

L'AFNIC est une association à but non lucratif et gestionnaire historique du .fr, l'Afnic est un opérateur multi-registres au service des domaines de premier niveau correspondant au territoire national (*.fr*) et de plusieurs projets français de nouvelles extensions Internet.
Elle est l'office d'enregistrement désigné par l'État pour la gestion des noms de domaine sous l'extension *.fr*. Elle gère également les extensions ultramarines *.re* (Ile de la Réunion), *.pm* (Saint-Pierre et Miquelon), *.tf* (Terres australes et antarctiques Françaises), *.wf* (Wallis et Futuna), *.yt* (Mayotte).
L'AFNIC propose des services comme (Whois) qui permet de remonter des renseignements techniques et administratifs sur les domaines en .fr.

16. Allez sur le lien suivant :
    https://www.afnic.fr/fr/produits-et-services/services/whois/
    Saisissez les domaines (leboncoin.fr, education.gouv.fr,elysee.fr ,Nasa.gov)

17. L'AFNIC propose un service convertisseur IDN. A quoi sert ce service ?

18. Qu'est-ce que DNSSEC ?

Afin de connaitre l'itinéraire entre votre ordinateur votre site web, la commande **tracert** peut nous aider. Le programme utilitaire de Windows **Tracert** ainsi que son pendant sous Linux Traceroute permettent de suivre les chemins de paquets de données. En fonction des résultats, l'utilisateur découvre par quelles stations individuelles les paquets sont envoyés lors de leurs parcours vers leurs destinations. Ainsi le problème peut être débloqué. Les détours compliqués ou les routeurs défaillant sont identifiés.

19. Dans un invité de commande, tapez la commande **tracert** pour connaitre le chemin emprunté entre votre ordinateur et le site web leboncoin.fr.
    Renouvelez l'opération afin de vérifier si vous empruntez toujours le même chemin.

20. Faites la même chose avec les domaines suivants :yahoo.fr, nasa.gov et elysee.fr

Nmap est un scanner de ports. Il est disponible pour la plupart des systèmes d'exploitation. Il peut être très utile pour vérifier qu'un service est ouvert sur un serveur ou pour retrouver une machine sur un réseau. Les cibles peuvent être désignées par leur adresse ou par leur nom DNS.

21. Dans l'invité de commande, saisissez la commande nmap.
    Demandez l'adresse IP de l'ordinateur de votre voisin et scannez les ports ouverts de son ordinateur.Quels sont les ports ouverts ?

La commande **netstat** permet d'afficher les statistiques des protocoles et des connexions réseau TCP/IP actives sur la machine.

22. Afficher les fichiers exécutables à l'origine des connexions ou des ports d'écoute en saisissant la commande : C:\> **netstat -b**
    Couplée avec l'option -v, cela permet d'actualiser la liste automatiquement toutes les n secondes : C:\> **netstat -b -v 5**

23. Afficher les statistiques ethernet : C:\> **netstat -e**

24. Afficher les adresses et les numéros de ports : C:\> **netstat -n**

25. Afficher toutes les connexions et les ports d'écoute actifs : C:\> **netstat -a**

26. Le systeme d'exploitation mémorise les valeurs des requêtes DNS dans un cache , afin d'éviter de de réexécuter la même requête DNS plusieurs fois.
    Afficher le cache DNS en saisissant la commande suivante : **ipconfig /displaydns**

27. Videz le cache DNS en saisissant la commande suivante : **ipconfig /flushdns**

DHCP

La connexion d'appareils à un réseau TCP/IP existant est désormais très facile. Auparavant il fallait **attribuer manuellement** des adresses IP et les saisir dans les différents systèmes, mais de nos jours la gestion des adresses est automatique. Le protocole DHCP (Dynamic Host Configuration Protocol, en français : protocole de configuration dynamique des hôtes) permet au **matériel de communication** (comme les routeurs, les commutateurs et les hubs) d'attribuer automatiquement une adresse individuelle aux dispositifs de recherche de connexion et de les intégrer dans un réseau.

L'attribution d'adresses avec le DHCP fonctionne selon le principe du client-serveur : les appareils qui recherchent une connexion demandent la configuration de l'adresse IP à un serveur DHCP, qui accède à son tour à une base de données dans laquelle sont saisies les **paramètres réseau** à définir. De plus, ce serveur, qui fait partie intégrante de tout routeur DSL moderne, peut assigner les paramètres suivants au client en utilisant ses informations de base données :

- **Adresse IP** unique
- **Masque de sous-réseau**
- **Passerelle** standard
- Serveur **DNS**
- **Configuration du proxy** via WPAD (Web Proxy Auto-Discovery Protocol)

L'attribution automatiques des adresses via le protocole de configuration dynamique de l'hôte (DHCP) se déroule en quatre étapes consécutives :

1. Pour commencer, le client envoie un paquet **DHCPDISCOVER** avec l'adresse cible 255.255.255.255 et l'adresse source 0.0.0.0. Avec cette diffusion, il contacte **tous les participants du réseau** pour localiser les serveurs DHCP disponibles et les informer de la demande d'adresse. Dans le meilleur des cas, seul un serveur existe, ainsi il n'y a pas de complications avec l'attribution.

2. Tous les serveurs DHCP qui écoutent les requêtes du port 67 répondent à la demande du client avec un paquet **DHCPOFFER**. Cette réponse, en plus d'une

éventuelle adresse IP libre et l'adresse MAC du client, contient aussi le masque de sous-réseau ainsi que l'adresse IP et ID du serveur.

3. Le client DHCP en sélectionne un à partir des données d'adresse reçues et informe le serveur concerné via **DHCPREQUEST**. Tous les autres serveurs reçoivent aussi ce message et savent ainsi que le choix a été fait en faveur d'un autre serveur. De plus, le client demande au serveur d'activer les données proposées. Le DHCPREQUEST est aussi utilisé pour confirmer les paramètres reçus précédemment.

4. Enfin, le serveur confirme les paramètres TCP/IP et va les transmettre à nouveau au client à l'aide d'un paquet **DHCPACK** (*DHCP acknowledged,* pour « reconnu »). Il contient des informations supplémentaires, par exemple sur les serveurs DNS, SMTP ou POP3. Le DHCP client enregistre maintenant toutes les données reçues localement et se connecte au réseau. Si le serveur n'est plus disponible ou si l'adresse IP a été attribuée à un autre client au cours du processus de configuration, il répond alors avec **DHCPNAK** (*DHCPnot acknowledged* « non reconnu »).

28. Afin de libérer l'adresse IP défini par le DHCP sur votre machine, et libérer toutes les connexions réseaux, tapez la commande suivante : **ipconfig /release**

29. Pour rétablir les connexions et obtenir un bail du serveur DHCP, Tapez la commande : **ipconfig /renew**

30. Vérifiez par la commande ping, que vous avez acces à Internet :
    ping www.google.Fr