- TP 1 et 2-
Commandes Linux pour la gestion des réseaux

M. Le Lain – M. Dragone – G. Renault

Antoine Gicquel	**07/04/17**
Maxime Hervé	**Groupe A2**

1. Fichiers de configuration

1.1. Quelles sont les informations contenues dans le fichier /etc/hosts, A quoi servent-elles.

Le fichier hosts permet d'associer des adresses IP avec des noms de domaines de façon statique. Pour chaque ligne on met une adresse puis suivit d'un espace le nom de domaine.

1.2. Quelles sont les informations contenues dans le fichier /etc/services, A quoi servent-elles.

Le fichier services permet d'associer à chaque service internet un numéro de port et le protocole sur lequel il travail.

2. Commandes de gestion du réseaux

Pour toutes les commandes suivantes, donnez une brève description de ce qu'elles font et de leurs principaux paramètres. Donnez pour chacune d'entre-elles des exemples d'utilisation que vous aurez testés (Utilisez la commande man, le commutateur -h ou --help de la commande ou Internet) Votre réponse ne doit pas être un simple copié collé mais un commentaire de votre part. Ne listez pas l'ensemble des commutateurs d'une commande mais plutôt les 2 ou 3 commutateurs les plus courant ou d'usage le plus pratique.

2.1 Commandes réseaux – Partie A

- dig

  dig permet de tout savoir sur les resolveurs dns. On s'en sert notameent pour dignostiquer un probleme dans la resolution des noms :

  dig [option] adresse [option sur l'affichage]

  ```
  dig www.univ-ubs.fr +short
  ```

- host

  host permet de simplement convertir nom de domaine à une adresse IP et vice versa :

  host [option] adresse

  ```
  host www.univ-ubs.fr
  ```

- nslookup

  nslookup permet de rechercher des informations sur le dns de façon interactif.

  nslookup [option] adresse

  ```
  nslookup www.univ-ubs.fr
  ```

Quels concepts réseaux se cachent derrières ces commandes réseaux ? Définissez-les

DNS :

C'est entre autres, le service qui permet d'établir la correspondance entre le nom de domaine et son adresse IP.

IP :

Une adresse IP (avec IP pour Internet Protocol) est le numéro qui identifie chaque ordinateur connecté à Internet.

Domaine :

La notion de domaine définit un ensemble de machines partageant des informations d'annuaire.

2.2 Commandes réseaux – Partie B

- ethtool

  ethtool permet de configurer le matériel réseau filaire.

  ethtool [option] devname

- arp

  arp signifie Adress Resolution Protocol et permet de manipuler la table ARP du noyau. Les options principales permettent d'effacer une correspondance d'adresses et d'en définir une manuellement.

- ifdown

  ifdown permet de stopper une interface réseau

  ifdown (interface)

- ifconfig

  ifconfig permet d'afficher les différentes interfaces réseaux.

- ifup

  ifup permet de démarrer une interface réseau déjà configurée.

- route

  route permet d'affiche / manipule la table de routage IP.

- ip

  ip permet d'afficher et paramétrer la configuration réseau.

Quels concepts réseaux se cachent derrières ces commandes réseaux ? Définissez-les

IP:

Une adresse IP (avec IP pour Internet Protocol) est le numéro qui identifie chaque ordinateur connecté à Internet.

Carte réseaux :

La carte réseau est un périphérique permettant de connecter son ordinateur à un réseau. Elle sert d'interface entre la machine et le câble du réseau.

Routage :

Le routeur achemine les données jusqu'à destination le plus rapidement possible : RIP

et OSPF sont deux protocoles de routage.

2.3 Commandes réseaux – Partie C

- netstat

  netstat permet de d'afficher les connexions réseau, les tables de routage, les statistiques des interfaces, les connexions masquées, les messages netlink, et les membres multicast.

- ping

  ping permet d'envoyer une requette ping à une adresse. Cela est utile pour vérifier notre connexion internet ou de la visibilité d'une machine distante.

- traceroute -I

  traceroute permettant de déterminer le chemin suivi par un paquet. La commande traceroute permet ainsi de dresser une cartographie des routeurs présents entre une machine source et une machine cible.

  L'option -I permet quant à elle de choisir le protocole ICMP au lieu de TCP pour éviter le blocage de la passerelle.

- finger

  finger permet d'afficher simplement des informations sur l'utilisateur courant.

- tcpdump

  tcpdump permet de faire une sauvegarde du trafic sur le réseau.

- tcpdmatch

  tcpdmatch permet de simuler le comportement d'une interface.

Quels concepts réseaux se cachent derrières ces commandes réseaux ? Définissez-les

Paquet :

Le paquet est l'entité de transmission de la couche réseau (couche 3 du modèle OSI).

Accès :

Autorisé ou non selon l'utilisateur par rapport au serveur

Réseaux :

Un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies.

2.4 Commandes réseaux – Partie D

- lshw

  lshw permet de faire une liste de la configuration matériel exhaustive.

- mii-diag

  mii-diag permet de contrôler et monitorer une carte réseau.

- mii-tool

  mii-diag permet de configurer une carte réseau.

- lspci

  lspci permet d'afficher une liste des composants de la machine.

- udevinfo

  udevinfo permet d'afficher les informations sur udev qui est le gestionnaire dynamique de materiel.

3. Donnez pour chaque question suivante, la ou les commandes Linux qui permettent d'y répondre :

3.1. Vérifiez que la machine de votre voisin(e) est connectée sur le réseau

À l'aide la commande ping on peut versifier que la machine de notre voisin est connectée sur le réseau si celle ci répond au ping.

3.2. Quelle est l'adresse ETHERNET de votre machine ?

L'adresse mac de notre carte ethernet est 28:D2:44:04:C3:11

3.3. Quelle est l'adresse IP de votre machine ?

À l'aide de ifconfig ou ip address, on constate que mon adresse IPv4 est `10.2.132.228`

3.4. A quel serveur DNS (nom et @IP) vous connectez-vous pour une requête http ?

On peut voir à l'aide de la commande dig :

```
;; SERVER: 10.0.0.2#53(10.0.0.2)
```

3.5. Quels sont les ports ouverts sur votre machine ?

On peut les afficher à l'aide de la commande netstat -an

3.6. Quelle est l'adresse (ou les adresses) IP de www.google.fr ?

On utilise la commande host www.google.fr :

```
www.google.fr has address 216.58.205.131
```

3.7. Faites une commande qui affiche le service associé à un port que vous saisissez (Utilisez les commandes grep, cut, echo, vues lors des TP Linux précédents)

Voici la commande :

```
echo "Entre votre port :" && read port && netstat -ap | grep $port | cut -d/ -f2 | cut -d\  -f 1
```

Le résultat :

```
Entre votre port :
63307
(Tous les processus ne peuvent être identifiés, les infos sur les processus
non possédés ne seront pas affichées, vous devez être root pour les voir
toutes.)
thunderbird-bi
```

3.8. Quelle est l'adresse mail de votre enseignant (Utilisez une commande Linux qui l'affiche à partir du nom)

On peut l'afficher avec la commande finger Lain

3.9. Quelle est la configuration matérielle de votre machine ?

On peut l'afficher à l'aide la commande lscpi

3.10. Utilisez la commande tracert de windows équivalente à traceroute (sous Windows, démarrer->exécuter->cmd (mode console de windows) et commande tracert) pour identifier les machines traversées jusqu'à

3.10.1. **http://extranet.iut-info-vannes.net**

```
traceroute to extranet.iut-info-vannes.net (195.83.161.134), 30 hops max,
60 byte packets
1  10.0.0.4 (10.0.0.4)  9.906 ms  15.506 ms  15.524 ms
2  gw-ubs-gi0-0-2.univ-ubs.fr (193.52.32.33)  15.523 ms  15.525 ms  15.529
ms
3  hsrv-c7g63y1.univ-ubs.fr (195.83.161.134)  18.934 ms  18.964 ms  18.970
ms
```

3.10.2. **http://www.google.fr**

```
traceroute to www.google.fr (216.58.208.195), 30 hops max, 60 byte packets
1  10.0.0.4 (10.0.0.4)  14.274 ms  37.148 ms  43.558 ms
2  gw-ubs-gi0-0-2.univ-ubs.fr (193.52.32.33)  52.808 ms  52.836 ms  65.479
ms
3  gi8-2-vannes-rtr-021.noc.renater.fr (193.51.181.26)  65.509 ms  65.510
ms  65.511 ms
4  te2-1-nantes-rtr-021.noc.renater.fr (193.51.177.183)  87.965 ms  113.108
ms  113.141 ms
5  te1-2-bordeaux-rtr-021.noc.renater.fr (193.51.177.40)  113.144 ms
 120.049 ms  120.082 ms
6  te1-1-toulouse-rtr-021.noc.renater.fr (193.51.177.36)  116.146 ms
 27.639 ms  27.581 ms
7  te2-3-montpellier-rtr-021.noc.renater.fr (193.51.177.224)  27.492 ms
 27.528 ms  27.515 ms
8  te1-2-marseille1-rtr-021.noc.renater.fr (193.51.177.18)  27.498 ms
 33.222 ms  33.189 ms
9  te1-1-marseille2-rtr-021.noc.renater.fr (193.51.177.185)  33.165 ms
 30.924 ms  36.394 ms
10  72.14.223.254 (72.14.223.254)  40.380 ms  27.875 ms  27.866 ms
11  209.85.252.36 (209.85.252.36)  27.845 ms  32.998 ms  32.903 ms
12  209.85.142.249 (209.85.142.249)  43.747 ms  41.254 ms  41.232 ms
13  216.239.43.156 (216.239.43.156)  41.197 ms  30.663 ms  39.075 ms
14  108.170.244.161 (108.170.244.161)  39.082 ms  21.633 ms  21.508 ms
15  216.239.42.37 (216.239.42.37)  28.395 ms  26.558 ms  32.452 ms
16  par10s21-in-f195.1e100.net (216.58.208.195)  32.372 ms  33.052 ms
 33.040 ms
```

3.10.3. http://dell.fr

```
 traceroute to www.dell.fr (143.166.83.190), 30 hops max, 60 byte packets
1     10.0.0.4    (10.0.0.4)     5.802    ms     8.044    ms     12.549    ms
2   gw-ubs-gi0-0-2.univ-ubs.fr (193.52.32.33)  18.203 ms  20.782 ms  21.986 ms
3  gi8-2-vannes-rtr-021.noc.renater.fr (193.51.181.26)  26.692 ms  29.889 ms  34.239
ms
4  te2-2-nantes-rtr-021.noc.renater.fr (193.51.177.207)  41.088 ms  42.725 ms  46.536
ms
5  te1-2-rennes-rtr-021.noc.renater.fr (193.51.177.34)  40.042 ms  54.920 ms  52.747
ms
6  te4-1-caen-rtr-021.noc.renater.fr (193.51.177.33)  58.257 ms  18.401 ms  21.814 ms

7   te0-0-0-0-paris1-rtr-001.noc.renater.fr (193.51.177.162)  73.805 ms  73.819 ms
 73.796                                    ms
8    ae4-8-xcr1.prp.cw.net  (195.10.54.65)   25.473  ms   25.467  ms   25.444  ms
9    ae1-xcr1.ptl.cw.net  (195.2.10.90)   100.785  ms   100.800  ms   93.743  ms
10   et-7-1-0-xcr1.nyh.cw.net (195.2.24.241)  87.776 ms  85.892 ms  87.879 ms
11    ae13-xcr2.nyk.cw.net  (195.2.25.69)   87.885  ms   90.641  ms   90.617  ms
12  0.xe-0-2-3.GW14.NYC1.ALTER.NET (204.148.1.253)  95.625 ms  95.639 ms  95.638 ms
13                    *                   *                  *
14   dell-gw.customer.alter.net (63.65.121.2)  135.679 ms  131.994 ms  131.946 ms
15                    *                   *                  *
16                    *                   *                  *
17                    *                   *                  *
18                    *                   *                  *
19                    *                   *                  *
20                    *                   *                  *
21                    *                   *                  *
22                    *                   *                  *
23                    *                   *                  *
24                    *                   *                  *
25                    *                   *                  *
26                    *                   *                  *
27                    *                   *                  *
28                    *                   *                  *
29                    *                   *                  *
30                          *                       *                         *
```