Commandes de base réseau Internet

But

Le but de ce TP est de prendre contact avec le réseau Internet en manipulant diverses commandes disponibles sous Unix. Le TP peut donc être refait à partir de toute machine UNIX bien configurée.

Le TP comporte donc différentes questions auxquelles vous devez répondre en exécutant des commandes Unix et rédiger ensuite un compte rendu. Des précisions concernant les commandes sont disponibles dans les manuels en ligne (commande man) ou en allant sur le WEB.

Vous devrez rédiger un compte rendu de ce TP. Votre compte rendu devra, pour chaque question concernant une commande, décrire brièvement le rôle de la commande, décrire si possible comment elle marche et pour les résultats obtenus commenter la signification des résultats.

Il est recommandé de rédiger pendant la session un bref compte rendu des réponses à chaque question. Vous devrez sauvegarder la liste des commandes utilisées pour chaque question, le résultat obtenu pour chaque commande. Pour ces résultats il est recommandé de créer, pendant le TP, un fichier contenant les listes de réponses aux commandes exécutées (au moyen des mécanismes UNIX comme les redirections) de façon à les présenter ultérieurement dans votre compte rendu.

Selon les variantes de systèmes UNIX (Linux) et les environnements installés (machines karkov, kirov), les différentes commandes peuvent se trouver dans des répertoires différents (/bin, /sbin, /usr/bin, /usr/sbin etc).

1 La commande ping *(protocole ICMP)*

La commande Unix/Internet `ping` permet de savoir si une machine connectée au réseau Internet est accessible en IP. Ping utilise les paquets du protocole ICMP. Voici quelques adresses possibles. Essayez d'en trouver d'autres.

Utilisez **`ping -c 4`** (ceci envoie seulement 4 paquets ICMP et s'arrête ensuite).

```
deptinfo.cnam.fr (CNAM Paris)
renater.sfinx.tm.fr (Réseau Renater France)
cs.toronto.edu (Université de Toronto Canada)
ns1.2day.co.nz(Serveur de noms DNS en Nouvelle Zélande)
gatekeeper.dec.com (USA-Cote ouest -Digital equipments)
209.85.129.147 ???
163.173.228.28
163.173.229.166
```

Options

En demandant un « man ping » vous avez différentes options, recherchez les options qui vont être utiles pour répondre aux questions suivantes.

1.1 Question

Commentez la réponse à une requête ping (commentez les différents champs des lignes de réponse et ce que l'on peut en déduire concernant le site testé)?

1.2 Question

Ping permet d'enregistrer la route utilisée jusqu'à la machine cible. Essayez cette commande (pourquoi n'enregistrons nous pas plus de 9 routeurs intermédiaires)?

2 La commande traceroute *(protocole ICMP)*

La commande Unix/Internet **`traceroute`** permet de résoudre les problèmes posés par ping et permet de connaître quelles sont les machines visitées dans le routage des paquets entre un site émetteur et un site destinataire. La commande est utilisable pour détecter des problèmes sur les différentes machines traversées entre un émetteur et un destinataire. La commande traceroute comporte comme principal paramètre une adresse IP ou d'une adresse de nom de domaine DNS. Il est difficile maintenant d'utiliser cette commande, en effet les différents matériels traversés (routeur, firewall, ...) sont bloqués et ne répondent plus correctement.

Quelques sites utiles

Vous allez utiliser des sites spécifiques qui vont permettre de répondre à la commande, vous pouvez vous connecter sur un des sites suivant, ou choisir d'autres sites, testez en au maximum 3 :

http://visualroute.visualware.com/

http://www.traceroute.org/

http://www.supporttechnique.net/traceroute.ihtml

http://www.france-citevision.com/aide-technique/traceroute.php

2.1 Question

Effectuez différentes traceroute vers différentes destination. Commentez la réponse à une requête traceroute (commentez les différents champs des lignes de réponse, que pouvez vous en déduire concernant le chemin emprunté)?

2.2 Question

Voici un exemple d'une trace obtenue il y a quelques années. Le chemin emprunté par les paquets vous semble-t-il cohérent ? Donner une explication pour ce routage.

```
/usr/etc/traceroute cyr.culture.fr
traceroute to cyr.culture.fr (143.126.201.251), 30 hops max, 40 byte
packets
1 internet-gw (163.173.128.2) 0 ms 0 ms 0 ms
2 renater-gw (192.33.159.1) 0 ms 10 ms 0 ms
3 danton1.rerif.ft.net (193.48.58.113) 110 ms 80 ms 90 ms
4 stlamb3.rerif.ft.net (193.48.53.49) 100 ms 130 ms 100 ms
5 stamand1.renater.ft.net (192.93.43.115) 90 ms 60 ms 50 ms
6 stamand3.renater.ft.net (192.93.43.17) 70 ms 100 ms 90 ms
7 rbs1.renater.ft.net (192.93.43.170) 130 ms 120 ms *
8 Paris-EBS2.Ebone.NET (192.121.156.226) 110 ms 90 ms 100 ms
9 icm-dc-1.icp.net (192.121.156.202) 220 ms 110 ms 220 ms
10 icm-dc-1-F0/0.icp.net (144.228.20.101) 200 ms 230 ms 290 ms
11 Vienna1.VA.Alter.Net (192.41.177.249) 250 ms 210 ms 240 ms
12 Falls-Church4.VA.ALTER.NET (137.39.100.33) 330 ms 220 ms 180 ms
13 Falls-Church1.VA.ALTER.NET (137.39.8.2) 270 ms 290 ms 230 ms
14 Amsterdam2.NL.EU.net (134.222.35.1) 380 ms 410 ms 460 ms
15 Amsterdam1.NL.EU.net (193.242.84.1) 350 ms 380 ms 310 ms
16 134.222.30.2 (134.222.30.2) 150 ms 490 ms 530 ms
17 Rocquencourt.FR.EU.net (193.107.192.18) 340 ms 340 ms 330 ms
18 143.126.200.203 (143.126.200.203) 300 ms 410 ms *
19 cyr.culture.fr (143.126.201.251) 460 ms 220 ms 290 ms
```

3 La commande ifconfig *(configuration des interfaces)*

La commande Unix/Internet ifconfig permet de gérer les voies physiques de l'ordinateur. Elle est donc très protégée et inaccessible aux utilisateurs standards. La variante **`ifconfig [-a]`** permet cependant à tout le monde de connaître l'état de la configuration à un instant donné (commande accessible dans le répertoire /sbin).

3.1 Question

Commentez les différents champs de la réponse aux commandes :

```
/sbin/ifconfig

/sbin/ifconfig -a
```

4 La commande route *(routage statique avec IP)*

La commande Unix/Internet route permet de définir un routage statique (uniquement utilisable en mode privilégié) et de visualiser les routes (possible pour tous les usagers). Une variante le la commande route liste les différentes routes établies c'est à dire la table de routage (autre façon de connaître l'état de la table de routage Internet de l'hôte netstat -r). La commande est dans le répertoire **`/sbin`**

4.1 Question

Commentez les différents champs de la réponse à la commande.

5 La commande whois *(Internic)*

La commande Unix/Internet whois permet de connaître les informations maintenues par l'Internic dans la base de données centrale des noms de l'Internet (voir www.internic.net). Exemple de noms de domaines utilisables: awl.com (.com, .net, .edu).

On peut ainsi par exemple connaître les serveurs de noms pour un domaine mais aussi d'autres renseignements. La qualité des réponses dépend de la mise à jour de cette base de données. Il y a normalement un enregistrement par nom de domaine principal.

Quelques liens utiles

Comme pour la commande traceroute, vous n'aurez pas d'informations probantes en utilisation normale, il faut aller sur un des sites suivant qui vous permettra de répondre à la question :

http://www.afnic.fr/outils/whois

http://www.whois.net/

http://www.whoislookup.be/

5.1 Question

Commentez la réponse à une requête whois (commentez les différents éléments de la réponse).

6 Les commandes host ou dig *(Domain Name System DNS)*

Avant de contacter un site distant connu par son nom logique (nom de domaine FQDN 'Fully Qualified Domain Name'), l'émetteur doit convertir le nom logique du serveur en une adresse IP numérique qui est utilisée dans les paquets échangés. C'est la principale application du DNS mais de manière plus générale cette application de serveur d'annuaire réparti permet de récupérer différentes

informations concernant les hôtes du réseau Internet. Par exemple les serveurs de courrier d'un domaine (enregistrement mail exchanger [MX]); l'adresse IP d'un hôte (enregistrement de type [A]); les alias ou 'canonical names' [CNAME]; etc.).

6.1 Question

En Unix le fichier **`/etc/resolv.conf`** est le principal fichier de configuration du DNS sur un hôte du réseau Internet. Que contient ce fichier?

6.2 Question

Cherchez avec **`host`** (**`dig`**) l'adresse IP de la machine **`cedric.cnam.fr`**, puis l'adresse IP de la machine **`www.cnam.f`**r.

6.3 Question

Recherche inverse: quel le nom de domaine de la machine d'adresse IP **`163.173.136.2`**?

6.4 Question

Quel est le nom de la machine serveur de courrier pour le domaine **`cnam.fr, free.fr`**?

7 Niveau transport: les services et les numéros de port

Les services Internet sur une machine sont associés à un numéro de port qui est un point d'accès de service au transport TCP ou au transport UDP. Un service a donc pour adresse, l'adresse IP de la machine et un numéro de port.

7.1 Question

Commentez le contenu du fichier **`/etc/services`**.

7.2 Question

Quels sont les numéros de port attribués au protocole **`whois`** (utilisez la commande **`grep`**).

8 La commande netstat *(les connexions de transport en cours)*

La variante **`netstat`** sans paramètre donne comme première information un état des connexions en cours.

8.1 Question

Commentez le résultat de la commande **`netstat`**.

8.2 Question

Utilisez les paramètres permettant de connaître les ports ouverts en **`UDP`** et **`TCP`** (**`man netstat`** vous donnera la solution). Parmi les ports ouverts (ils sont nombreux car vous êtes sur la même machine) indiquez ceux qui sont associés à des services ouverts sur la machine?

9 Le protocole d'application telnet *(ouverture de session à distance)*

Les principaux paramètres de la commande telnet sont un nom de domaine ou une adresse IP suivi d'un numéro de port TCP qui définit le service.

9.1 Question

Quel est le numéro de port du service telnet.

9.2 Question

Ouvrez une session telnet sur une autre machine (à distance).

10 Le protocole d'application SMTP *(messagerie)*

Les éléments principaux du protocole **SMTP** ('Simple Mail Transfer Protocol') sont décrits comme un échange entre un client de messagerie et un serveur de messagerie. Les principaux messages qui permettent d'envoyer un courrier sont codés sous la forme de chaînes de caractères.

Un modèle de l'échange pour émettre un courrier est donné ci après (selon les serveurs les textes des réponses diffèrent), les commandes du protocole sont en **GRAS**:

Client de messagerie Commande	Serveur de messagerie Réponse
Etablir une session	
	220 cnam.fr Service Ready
HELO cnam.fr	
	250 cnam.fr OK
MAIL FROM: michel@cnam.fr	
	250 OK
RCPT TO: pierre@cnam.fr	
	250 OK
DATA	
	354 Start mail input, end with CRLF.CRLF
Contenu du courrier	
CRLF	
.	
CRLF	
	250 OK
QUIT	221 cnam.fr Closing Connection

Liste des commandes et signification :

Commande	Exemple	Description
HELO (désormais EHLO)	EHLO 193.56.47.125	Identification à l'aide de l'adresse IP ou du nom de domaine de l'ordinateur expéditeur
MAIL FROM:	MAIL FROM: expediteur@domaine.com	Identification de l'adresse de l'expéditeur
RCPT TO:	RCPT TO: destinataire@domaine.com	Identification de l'adresse du destinataire
DATA	DATA message	Corps du mail
QUIT	QUIT	Sortie du serveur SMTP
HELP	HELP	Liste des commandes SMTP supportées par le serveur

L'ensemble des spécifications du protocole SMTP sont définies dans le RFC 821 (depuis avril 2001, les spécifications du protocole SMTP sont définies dans le RFC 2821).

10.1 Question

Quel est le numéro de port attribué au service **SMTP** ?

10.2 Question

Quel est le nom de domaine de la machine serveur de courrier du domaine **cnam.fr** (comment l'obtenez vous)?

10.3 Question

Ouvrez une session telnet avec un serveur de messagerie du CNAM. Pourquoi le logiciel telnet ne demande pas d'authentification ?

Pourquoi pouvez vous dialoguer avec un serveur SMTP en telnet?

Envoyez sur votre boite de courrier un courrier électronique en exécutant manuellement avec telnet le protocole SMTP d'accès à votre serveur de messagerie.

11Le protocole de relève de courrier POP3 *('Post Office Protocol')*

Il existe plusieurs protocoles de relève de courrier dont fait partie le protocole POP (la version courante est la version 3). **POP** fonctionne entre un client **POP3** qui souhaite lire du courrier électronique et un serveur POP3 de consultation de courrier. Un fois établie la connexion avec le serveur POP on peut utiliser les commandes :

```
user nom_de_boite_a_lettre_de_courrier
pass mot_de_passe
list (la commande list donne la liste des messages en instance non détruits avec
        un numéro d'ordre)
retr n (donne le contenu du message numéro n)
dele n (détruit le message n dans la file d'attente des messages en instance)
quit (sort du serveur pop3)
```

Commande	Exemple	Description
USER	USER nom_user	Cette commande permet de s'authentifier. Elle doit être suivie du nom de l'utilisateur, c'est-à-dire une chaîne de caractères identifiant l'utilisateur sur le serveur. La commande USER doit précéder la commande *PASS*.
PASS	PASS mot_de_passe	La commande *PASS*, permet d'indiquer le mot de passe de l'utilisateur dont le nom a été spécifié lors d'une commande *USER* préalable.
STAT		Information sur les messages contenus sur le serveur DELE
RETR	RETR n	Numéro du message à récupérer
DELE	DELE n	Numéro du message à supprimer
LIST	LIST [msg]	Numéro du message à afficher
NOOP		Permet de garder les connexion ouverte en cas d'inactivité
TOP	TOP <messageID> <n>	Commande affichant *n* lignes du message, dont le numéro est donné en argument. En cas du réponse positive du serveur, celui-ci renvoie les en-têtes du message, puis une ligne vierge et enfin les *n* premières lignes du message.
UIDL	UIDL [msg]	Demande au serveur de renvoyer une ligne contenant des informations sur le message éventuellement donné en argument. Cette ligne contient une chaîne de caractères, appelée *listing d'identificateur unique*, permettant d'identifier de façon unique le message sur le serveur, indépendamment de la session. L'argument optionnel est un numéro correspondant à un message existant sur le serveur POP, c'est-à-dire un message non effacé).
QUIT		La commande *QUIT* demande la sortie du serveur POP3. Elle entraîne la suppression de tous les messages marqués comme effacés et renvoie l'état de cette action.

11.1 Question

Quel est le numéro de port standard de **POP3.** Lancez telnet pour vous connecter sur le serveur **POP**.

11.2 Question

Exécutez le protocole **POP** pour lire le courrier émis à la question précédente. Pourquoi le protocole pop demande t'il une authentification ?

12 Le protocole d'application HTTP *(le WEB)*

Le protocole de communication du WEB est le protocole **http**. Il utilise un mécanisme de type requête-réponse : le client demande au serveur le document HTML et le serveur lui renvoie. Le protocole de transport utilisé est TCP. La commande pour charger une page HTML est GET <chemin fichier> <version du protocole>. Une commande comporte une ligne ou un ensemble de lignes de texte suivies de deux retour chariot (deux CRLF).

12.1 Question

Quel est le numéro de port standard HTTP. Lancer le logiciel telnet et connectez vous sur la machine serveur du site web du cnam **`www.cnam.fr`**. Pourquoi le logiciel telnet ne demande pas d'authentification ?

Pourquoi pouvez vous dialoguer avec un serveur HTTP en telnet?

12.2 Question

Lancez une commande GET en version 1.0 (HTTP/1.0):

```
GET /index.html HTTP/1.0 <CRLF> <CRLF>
```

Que constatez vous?

12.3 Question

Avec la version actuelle HTTP 1.1 il faut absolument ajouter une ligne d'entête HOST donnant le nom de domaine du site serveur.

```
GET /index.html HTTP/1.1 CRLF
HOST: www.cnam.fr
CRLF CRLF
.
```

Refaites la même commande en HTTP 1.1?

12.4 Question

Lancez une commande GET sur la page /**`faq.html`**. Commentez la réponse du serveur?

13 Rapport

Rappel vous devez fournir un rapport avec l'ensemble des réponses aux questions posées. Remplissez au fur et à mesure votre rapport pendant la séance de TP. Utilisez l'outil « OpenOffice » qui est accessible sur la machine sur laquelle vous êtes connecté. Le travail peut être fait en binôme, un seul rapport par groupe. Vous indiquez correctement dans le rapport vos Nom Prénom. Le nom donné au rapport doit être :

13.1 Personne seule

`TP1-Reseau-NomGrooupeEI2-Nom`

`NomGrooupeEI2` : le nom du groupe EI2 (**`EI2AD, EI2AG, ou EI-I2B`**)

`Nom1` votre nom si seul,

13.2 Binôme

`TP1-Reseau-NomGrooupeEI2-Nom1-Nom2`

`NomGrooupeEI2` : le nom du groupe EI2 (**`EI2AD, EI2AG, ou EI-I2B`**)

`Nom1` le nom d'un des membres du binôme

`Nom2` le nom de l'autre membre du binôme

Vous envoyez votre rapport par courrier électronique à l'adresse : **`gerard.benay@cnam.fr`** au plus tard le vendredi d'après la séance soit :

EI-I2AD : Vendredi 21 mars 2008

EI-I2AG : Vendredi 28 mars 2008

EI-I2B : Vendredi 4 avril 2008