UNIVERSITÉ D'ARTOIS

Quelques protocoles et outils réseaux

1 Adresses MAC et IP – ifconfig

Chaque point de connexion d'un réseau est identifié par une adresse MAC (physique) et une adresse IP (logique). Pour l'adresse MAC, il s'agit d'une séquence de 6 couples de chiffres hexadécimaux séparés par : et pour l'adresse IP (v4), il s'agit d'une séquence de 4 nombres (compris entre 0 et 255) séparés par un point.

1. En utilisant la commande whereis (qui permet de localiser l'emplacement d'une commande), indiquer comment exécuter la commande ifconfig.
2. Exécuter la commande ifconfig (en précisant le chemin comme indiqué par le résultat de la commande précédente, si nécessaire).
3. Quelle est l'adresse MAC de votre machine ? Quel est le constructeur de la carte réseau ? Voir `http://standards.ieee.org/develop/regauth/oui/public.html`. Attention, vous ne devez donner sur ce site que la valeur des trois premiers octets, en utilisant le caractère '-' comme séparateur.
4. Quelle est l'adresse IP de votre machine ?
5. Quelle est l'adresse IP v6 de votre machine ?
6. Que signifie la seconde adresse IP ?
7. Est-il possible d'associer d'autres adresses MAC et IP à une même machine ? Expliquer.

2 Noms de machines (domaines) – host, hostname, et ping

Pour simplifier la vie de l'utilisateur, des noms (de machines) peuvent être associés à des adresses IP. Ainsi, au lieu d'indiquer l'adresse IP d'une machine, on peut utiliser son nom.

Pour connaître l'adresse IP d'une machine dont vous connaissez le nom, ou pour faire le contraire (requête inverse), vous pouvez utiliser la commande host.

1. Utilisez cette commande en plaçant comme argument le nom de la machine de votre voisin.
2. Utilisez cette commande en plaçant comme argument l'adresse IP de la machine de votre voisin.
3. En observant le résultat des commandes précédentes, indiquer quel est le nom complet de la machine de votre voisin.
4. Utilisez cette commande en plaçant comme argument www.arte.fr.
5. Maintenant que vous connaissez l'adresse IP du site de Arte, placez-là dans le champ d'adresse de votre navigateur et valider.
6. Si vous avez un doute sur le nom de votre machine, tapez hostname. Essayez.
7. Vérifiez que la machine de votre voisin répond avec la commande ping nomMachine. Qu'observez-vous ? Stoppez avec **CTRL C**.
8. Essayer la commande ping avec des noms de machine extérieure à l'université. Que se passe-t-il ?

3 Résolution d'adresses – arp

ARP est un protocole de résolution d'adresses (que nous verrons en cours) permettant d'obtenir la correspondance entre une adresse logique (IP) et une adresse physique (MAC). Sous Linux, la commande arp permet de visualiser la table de correspondance courante de votre machine.

1. En utilisant la commande whereis (qui permet de localiser l'emplacement d'une commande), indiquer comment exécuter la commande arp.
2. Exécuter la commande arp et analyser le résultat.
3. En utilisant la manuel (commande man arp), trouver quelle option il faut utiliser pour obtenir les adresses IP en notation décimale pointée.
4. Quelle option faut-il utiliser pour connaître l'adresse MAC d'une machine dont vous donnez le nom (ou l'adresse IP).
5. Effectuer un ping sur une machine de la salle pour laquelle vous ne trouvez aucune information dans la table ARP. Notez les temps de réponse des 3 premières réponses.
6. Lancer la commande arp ensuite. Que constatez-vous ? En effectuant à nouveau un ping, comparez les nouveaux temps de réponse (les 3 premiers) avec les anciens.
7. Utilisez votre navigateur web pour accéder au site `www.arte.fr`. Y a-t-il de nouvelles entrées dans la table ARP ? Pourquoi ?
8. Lancer une requête de diffusion (avec ping) en utilisant 255.255.255.255 (et la bonne option – trouvez-là). Que constatez-vous ? Observez la table ARP.

4 Résolution de noms (DNS) – dig et host

Le but de DNS (Domain Name Service) est de réaliser/gérer l'association entre adresses IP et des noms plus compréhensibles pour l'être humain. Parfois, plusieurs noms sont associés à une même adresse IP. L'un de ces noms est gardé comme référence et est dit canonique tandis que les autres noms sont considérés comme des alias. Les commandes `host`, `dig` et `nslookup` interrogent des serveurs DNS. Les informations stockées par le DNS correspondent à des enregistrements (de ressources ou resource records) de la forme :

nom TTL classe type valeur

où :

1. le nom indique le domaine (ou la machine)
2. TTL (Time To Live) indique la stabilité de l'information
   - 86400 = 1 jour
   - 60 = 1 mn
3. classe identifie la structure (protocole) ; IN = internet
4. type donne la nature de l'enregistrement (et utilise le champ valeur)
   - A record (address record) fait correspondre un nom d'hôte à une adresse IPv4 de 32 bits
   - AAAA record (IPv6 address record) fait correspondre un nom d'hôte à une adresse IPv6 de 128 bits
   - CNAME record (canonical name record) permet de faire d'un domaine un alias vers un autre. Cet alias hérite de tous les sous-domaines de l'original
   - MX record (mail exchange record) définit un serveur de courriel pour le domaine (précédé de la préférence pour ce serveur)
   - PTR record (pointer record) associe une adresse IP à un enregistrement de nom de domaine, aussi dit « reverse » puisqu'il fait exactement le contraire du A record
   - NS record (name server record) définit un serveur DNS pour le domaine

- SOA record (Start Of Authority record) donne les informations générales de la zone : serveur principal, courriel de contact, différentes durées dont celle d'expiration, numéro de série de la zone
- HINFO donne une description de l'hôte
- TXT record permet à un administrateur d'insérer un texte quelconque dans un enregistrement DNS

Effectuez une lecture rapide du manuel concernant host et dig. Pour ces deux commandes, on peut en particulier utiliser l'option -t qui indique le type d'enregistrement (record) recherché. Par exemple,

```
host -t MX arte.fr
```

ou

```
dig -t MX arte.fr
```

fournit la liste des serveurs de courriels du domaine `arte`.

Comme autre exemple,

```
host -t NS arte.fr
```

ou

```
dig -t NS arte.fr
```

fournit la liste des serveurs DNS du domaine `arte`. Comme valeur de l'option -t, on peut également utiliser A (en fait, c'est la valeur par défaut), CNAME, SOA, ANY, ...

A l'aide de ces deux commandes, répondez aux questions suivantes :

1. Quel est le nom canonique de `www.yahoo.fr` ? Est-ce qu'il n'y en a qu'un seul ? Quelle est l'adresse IP de ce nom canonique ?
2. Chercher l'adresse IP correspondant à `www.arte.fr`.
3. Utiliser l'adresse IP correspondant à `www.arte.fr` dans la barre d'adresse de votre navigateur.
4. Effectuez la requête inverse pour la machine d'adresse IP 163.173.128.6.
5. Trouvez tous les serveurs de nom et de courriel de l'université d'artois (`univ-artois.fr`).
6. Trouvez tous les serveurs de nom et de courriel de `google.com`
7. En analysant le contenu (commande cat) du fichier de configuration `/etc/resolv.conf` qui fournit le nom de domaine ainsi que tous les serveurs de noms disponibles sur notre réseau (domaine `iut-lens.univ-artois.fr`), donnez le nom de domaine, le nom et l'adresse IP de chaque serveur de noms.
8. Il est possible (normalement) de visualiser le principe de requête itérative mis en place par le DNS. Tapez

   ```
   dig june.cs.washington.edu +trace
   ```

   Analyser le résultat... (et si cela ne fonctionne pas ici, testez chez vous).
9. Etudier d'autres traces de requêtes itératives, avec par exemple les domaines `www.nicta.com.au` ou `www.jnto.go.jp`
10. Effectuer vous-mêmes les requêtes précédentes en utilisant dig avec l'argument `@`. Par exemple :

    ```
    dig @a.root-servers.net edu
    ```

    interroge le serveur DNS racine `a.root-servers.net` sur les serveurs de noms disponibles sur `edu`.
11. Malheuresement, localement, on ne pourra qu'identifier indirectement les serveurs DNS utilisés successivement pour une requête en interrogeant le serveur DNS local (mailserv.univ-artois.fr). Ceci de la manière suivante :

    ```
    dig @mailserv.univ-artois.fr .
    dig @mailserv.univ-artois.fr edu
    ...
    ```

5 Connexion à des services distants – telnet

Avec telnet, on peut se connecter sur des machines distantes, et plus précisément à des services sur des machines distantes. Ces services sont identifiés par des numéros (de port). Par exemple, pour accéder à un serveur web, on utilise le port 80. Par exemple, pour le serveur web local (de bdd.iut-lens.univ-artois.fr), on peut taper :

telnet bdd.iut-lens.univ-artois.fr 80
GET /

Récupérer le texte et copier le dans un fichier "page.html", et utilisez ensuite un navigateur pour afficher cette page.

Pour un serveur web distant (ici, www.univ-lille1.fr), on tapera :

telnet www.univ-lille1.fr 80
GET /

Malheureusement, l'université nous force à passer par un proxy pour accéder aux sites web externes. Dans ce cas, il faut se connecter au proxy et lui soumettre la requète. Par exemple, pour obtenir la même page que ci-dessus, mais en passant par le proxy :

telnet cache-etu.univ-artois.fr 3128
GET http ://www.univ-lille1.fr

Pour le protocole de communication utilisé pour transférer le courrier électronique, SMTP (Simple Mail Transfer Protocol), on peut utiliser telnet sur un serveur à l'écoute du port 25. Voici ci-dessous la procédure type :

```
>> telnet smtp.xxxx.xxxx 25
Connected to smtp.xxxx.xxxx.
220 smtp.xxxx.xxxx SMTP Ready
>> HELO client
250-smtp.xxxx.xxxx
250-PIPELINING
250 8BITMIME
>> MAIL FROM: <auteur@yyyy.yyyy>
250 Sender ok
>> RCPT TO: <destinataire@xxxx.xxxx>
250 Recipient ok.
>> DATA
354 Enter mail, end with "." on a line by itself
Subject: Test

Corps du texte
.
250 Ok
>> QUIT
221 Closing connection
Connection closed by foreign host.
```

Trouver le nom d'un serveur de courriel chez votre hébergeur (par exemple, gmail ou yahoo) et envoyez-vous un message. Cela ne marche pas ? Essayer avec 127.0.0.1

6 Connexion à distance – ssh

ssh est une commande qui permet de se connecter (de façon sécurisée) sur une machine distante. La syntaxe est la suivante :

ssh user@serveur

Pour en savoir plus sur la commande ssh, consulter le manuel (man ssh).

1. Essayer de vous connecter sur la machine de votre voisin ; si la machine de votre voisin s'appelle bolide, alors tapez `ssh bolide`. Si c'est la première fois que vous vous connectez à distance sur cette machine, alors ssh vous demande de confirmer que vous authentifiez cette machine comme une source fiable. Répondez `yes`. Ensuite tapez votre mot de passe.

2. Constatez-vous que vous êtes connecté sur la machine de votre voisin ? Comment ?
3. Stoppez la connexion distante avec `logout` ou `CTRL D`. Constatez-vous que vous n'êtes plus connecté sur la machine de votre voisin ? Comment ?
4. Ouvrez le fichier .ssh/known_hosts. Par exemple, `cat .ssh/known_hosts`. Décrivez les différents champs.
5. Tentez une connexion sur la machine de votre voisin avec le nom complet de la machine puis avec l'adresse IP. Indiquer les commandes. Est-ce que cela fonctionne ?
6. Indiquez qui est connecté à un moment donné sur votre machine en utilisant la commande `who`.
7. Pour vérifier que ssh s'exécute bien sur la machine distante, après vous être connecté sur celle-ci, tapez :

   echo "coucou" > /tmp/coucouToto.txt

   Demander à votre voisin d'effectuer la même opération à distance sur votre machine mais avec un autre nom de fichier (par exemple, coucouTiti.txt) Constater le résultat en listant les fichiers dans `/tmp` de votre machine et celle de votre voisin.
8. On souhaite effectuer un ssh en précisant une commande à exécuter directement (par exemple, ls -l /tmp). Que devez-vous taper ?
9. Demandez à votre voisin de se connecter sur une machine distante quelconque avec ssh depuis un terminal de votre machine. Il devra intégrer à la commande son nom d'utilisateur. Quelle commande doit-il taper ?
10. Tentez une connection avec ssh sur une machine distante et lancer emacs. Que constatez-vous ?
11. Tentez une connection avec ssh -X sur une machine distante et lancer emacs. Que constatez-vous ? A quoi sert l'option -X ?
12. Sur la machine distante, tapez ps -aux. Que constate-t-on ?
13. De la même manière, tentez de lancer gcalctool sur la machine distante à l'aide de ssh avec et sans l'option -X.

ssh est un (processus) serveur qui fonctionne en mode connecté (TCP) en utilisant le port 22. On peut observer cela avec `netstat -ntl`.

7 Transfert de fichiers – scp

scp est une commande qui permet de copier des fichiers sur une machine distante. Il utilise `ssh` pour transférer des données et offre le même niveau de sécurité. Pour en savoir plus sur la commande `scp`, consulter le manuel. Tapez `man scp`.

1. Copier un fichier dans le répertoire /tmp de la machine voisine. Indiquer l'instruction.
2. Créer localement un répertoire et placez-y quelques fichiers. Copier en une seule instruction ce répertoire dans le répertoire /tmp de la machine voisine. Indiquer l'instruction.
3. Avec `scp`, copiez un fichier de votre compte sur le compte de votre voisin (sur sa machine) en indiquant lors de la copie le nom de login de votre voisin. Que doit effectuer votre voisin ? Est-ce sécurisé ?

8 Transfert de fichiers – ftp

Le protocole FTP (File Transfer Protocol) permet d'échanger des fichiers en garantissant une qualité de service (le fichier doit arriver correctement et en entier au récepteur). FTP n'est pas sécurisé. Aussi, quand cela est possible, il est fortement recommandé d'utiliser la commande `scp` à la place de la commande `ftp`. Néanmoins, `ftp` est assez souvent utilisé pour transférer des fichiers (pages web)

chez un fournisseur d'accès et il est également utilisé sous une forme dite anonyme (on se connecte en utilisant anonymous comme nom d'utilisateur et son adresse électronique comme mot de passe).

Pour savoir comment utiliser la commande `ftp`, consultez le manuel d'utilisation en ligne. Une fois connecté, les commandes `ascii` ou `binary` permettent de changer le type des fichiers échangés. La commande `get` permet de récupérer les fichiers, et la commande `put` de les déposer.

1. Connectez-vous sur la machine `ens` avec un `ftp` anonyme.
2. Comment lister le répertoire courant sur la machine distante ? la machine locale ?
3. Comment connaître le répertoire courant sur la machine distante ? la machine locale ?
4. Comment changer de répertoire courant sur la machine distante ? la machine locale ?
5. Pouvez-vous placer un fichier dans le répertoire /tmp de la machine `ens` ? Pourquoi ?
6. Passez en mode ascii et récupérer le fichier de commande ls ainsi que le fichier texte monFichier.
7. Tentez d'éxecuter localement le fichier ls (./ls) après avoir donné les droits d'éxecution sur le fichier. Par ailleurs, visualiser le fichier monFichier.
8. Passez en mode binaire et récupérer le fichier de commande ls
9. Tentez de l'éxecuter localement (./ls) après avoir donné les droits d'éxecution sur le fichier
10. En déduire la différence entre le mode ascii et le mode binaire
11. Comment récupérer plusieurs fichiers à la fois ?
12. Peut-on utiliser `ftp` par le biais d'une URL ? Essayer.

A l'IUT, il n'est pas possible de récupérer un fichier par ftp anonyme sur un serveur de votre choix (par exemple, le fichier README du répertoire jussieu sur le site ftp.lip6.fr).

9 Serveur FTP via telnet

Avant toute chose, récupérer la RFC 959. Ensuite, analyser ce qui se passe dans les deux terminaux ci-dessous. Essayer de reconstruire le scénario. Dans un dernier temps, reproduisez vous-même le scénario.

```
[Terminal 1]
toto@bidule> telnet ens.iut-lens.univ-artois.fr 21
Trying 172.31.144.4...
Connected to ens.iut-lens.univ-artois.fr.
Escape character is '^]'.
220 (vsFTPd 2.0.1)
USER anonymous
331 Please specify the password.
PASS toto
230 Login successful.
CWD pub
250 Directory successfully changed.
PASV
227 Entering Passive Mode (172,31,144,4,92,30)
LIST
150 Here comes the directory listing.
226 Directory send OK.
PASV
227 Entering Passive Mode (172,31,144,4,78,182)
RETR fichier
425 Failed to establish connection.
PASV
227 Entering Passive Mode (172,31,144,4,48,154)
RETR fichier
150 Opening BINARY mode data connection for fichier (467 bytes).
226 File send OK.
QUIT
221 Goodbye.
Connection closed by foreign host.
```

```
[Terminal 2]
toto@bidule> telnet ens.iut-lens.univ-artois.fr 23582
Trying 172.31.144.4...
Connected to ens.iut-lens.univ-artois.fr.
Escape character is '^]'.
-rw-r--r--    1 505      100           467 Mar 30  2005 fichier
-rwxr-xr-x    1 0        0           85232 Sep 12  2005 ls
Connection closed by foreign host.
toto@bidule> telnet ens.iut-lens.univ-artois.fr 20150
Trying 172.31.144.4...
telnet: Unable to connect to remote host: Connection refused
toto@bidule> telnet ens.iut-lens.univ-artois.fr 12442
Trying 172.31.144.4...
Connected to ens.iut-lens.univ-artois.fr.
Escape character is '^]'.
       Anacron  peut  etre utilise pour executer des commandes periodiquement,
       avec une periodicite donnee en jours. A la difference de cron, il ne
       suppose  pas  que  la  machine tourne en permanence. En consequence, il
       peut etre utilise sur des machines qui ne tournent pas  24  heures  sur
       24, pour controler journellement, hebdomadairement ou mensuellement des
       taches qui sont ordinairement controlees par cron.

Connection closed by foreign host.
```

10 URLs

Pour identifier les pages sur le web, chacune se voit attribuer une URL (Uniform Resource Locator) qui fait office de nom universel de la page. Les URLs se composent de trois parties :

- le protocole
- le nom DNS de la machine où la page se trouve
- le chemin d'accès unique conduisant à la page sur la machine

Lorsqu'aucun protocole n'est précisé, par défaut il s'agit de HTTP (Hypertext Transfer Protocol). Parmi les protocoles, on trouve :

- `http` est le protocole natif du web. Par exemple, une page chargée avec ce protocole est :

  `http://www.lemonde.fr`

  Dans un premier onglet sur votre navigateur, tapez `http://www.lemonde.fr` et dans un deuxième onglet tapez `/www.lemonde.fr`. Comparez.
- `https` est le protocole de transfert hypertexte sécurisé. C'est la combinaison de HTTP avec une couche de chiffrement comme SSL ou TLS. Pour constater que ce protocole est utilisé, rendez-vous sur la page de paypal.
- `file` est un schéma (protocol) URL qui est utilisé pour charger un fichier local. Par exemple, une URL de ce schéma peut être :

  `file:///home/toto/fichier.html`

  Essayer de charger une page html de votre compte en tapant une URL similaire dans la barre d'adresses de votre navigateur.
- `ftp` est un protocole de transfert de fichier. On peut l'utiliser via un navigateur. Par exemple,

  `ftp://ftp1.freebsd.org/pub/FreeBSD/README.TXT`

  Essayer cette URL.
- `about` est un schéma (protocol) URL qui permet de donner certaines informations sur les navigateurs. Essayer dans la barre d'adresses de votre navigateur :

  `about:about`
  `about:plugins`
  `about:cache`

  Attention : le comportement peut différer d'un navigateur à l'autre

11 Commande netstat

La commande netstat permet d'obtenir diverses informations comme celles concernant la table de routage d'une machine ou encore les interfaces d'une machine.

1. Lire le manuel concernant la commande netstat.
2. Quelle option permet d'obtenir la table de routage de votre machine ?
3. Quelle option faut-il utiliser pour obtenir les adresses IP en notation décimale pointée ?
4. Analyser la table de routage. Pour chaque ligne (entrée), indiquer précisément le rôle des champs Destination, Gateway et GenMask.
5. Quelle option permet d'obtenir des informations sur les interfaces de votre machine ?
6. A quoi correspondent RX, TX et MTU ?